Bull System Manager

BSM 1.3

User's Guide

NOVASCALE & ESCALA

REFERENCE
86 A2 55FA 03

NOVASCALE & ESCALA

BSM 1.3
User's Guide

Software

August 2010

BULL CEDOC
357 AVENUE PATTON
B.P.20845
49008 ANGERS CEDEX 01
FRANCE

REFERENCE
86 A2 55FA 03

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 2008-2010

Printed in France

Trademarks and Acknowledgements

We acknowledge the rights of the proprietors of the 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

Table of Contents iii

List of Figures viii

List of Tables x

Preface xi

Chapter 1. About Bull System Manager 1

1.1 Scope 1
1.1.1 Supervision Features 2
1.1.2 Administration Features 3

1.2 Basic Definitions 5
1.2.1 BSM local Console 5
1.2.2 BSM global Console 5
1.2.3 Service 5
1.2.4 Category 5
1.2.5 Functional domain filter (or Servicegroup) 5
1.2.6 View 6
1.2.7 Map 6

1.3 Bull System Manager Components 7

1.4 Bull System Manager and Security 8
1.4.1 Authentication 8
1.4.2 Role-based Management 8

Chapter 2. Getting Started 9

2.1 Starting the Console 9
2.1.1 Differences between local and global Console 9
2.1.2 Console Basics 9
2.1.3 Bull System Manager Authentication and Roles 10
2.1.3.1 Role Based Management 10
2.1.3.2 Bull System Manager Server User Authentication – Linux & Windows 11

2.2 Displaying Monitoring Information 12
2.2.1 Starting with the Tree mode 12
2.2.2 Using a Functional domain filter with the Tree mode 13
2.2.3 Tracking Problems 15
2.2.3.1 Alert History 15
2.2.3.2 Status Trends 16
2.2.4 Viewing More Information 18

2.3 Receiving Alerts 20
2.3.1 Email Notifications 20
2.3.2 SNMP Trap Notifications 20

2.3.3 Viewing Notifications 20
2.4 Scheduling Downtime 21
2.4.1 Show scheduled downtime lists 21
2.4.2 How to schedule a downtime 21
2.4.3 How to cancel a scheduled downtime 23
2.5 Taking Remote Control of a Host 24
2.5.1 Windows Hosts 24
2.5.2 Linux and AIX Hosts 26
2.6 Managing Hardware 28
2.6.1 Using the System Native Hardware Manager 28
2.6.2 Using the Bull System Manager Hardware Management Application 31
2.7 Tracking a Performance Indicator over a Long Period 33
2.8 Configuring Bull System Manager 34
2.9 Bull System Manager Server Control 35
Chapter 3. Using Bull System Manager Console Supervision Modes 37
3.1 Working in the Tree Mode 37
3.1.1 Management Tree Basics 37
3.1.2 Management Tree Status Colors 39
3.1.3 Management Tree Nodes 41
3.1.3.1 Root Node 42
3.1.3.2 Hardware Manager Node and Status Levels 42
3.1.3.3 Storage Manager Node 44
3.1.3.4 Virtual Manager Node 44
3.1.3.5 Platform Node and Hostgroup Node 44
3.1.3.6 Host Node and Status Levels 45
3.1.3.7 Category Node 45
3.1.3.8 Services Node and Status Levels 46
3.1.4 Management Tree Views 47
3.1.4.1 Hosts View 48
3.1.4.2 HostGroups View 48
3.1.4.3 Hardware Managers View 49
3.1.4.4 Storage Managers View 50
3.1.4.5 Virtual Managers View 51
3.1.4.6 Functional Domains View 51
3.2 Working in the Map Mode 52
3.3 Working in Alerts Mode 53
3.3.1 Alert Basics 53
3.3.2 Alert Selection 54
3.3.3 Alert Information 56
3.4 Supervision Information 57
3.4.1 FOCUS area 57
3.4.2 Supervision Information Basics 58
3.4.3 Monitoring Information 59
3.4.3.1 Status Overview 59
3.4.3.2 Status GRID 61

3.4.3.3 Status Detail ... 62
3.4.3.4 Host Status ... 63
3.4.3.5 Service Status ... 63
3.4.3.6 Config ... 64
3.4.3.7 Log ... 65
3.4.3.8 Control ... 66
3.4.4 Reporting Information ... 69
3.4.4.1 Alert History ... 70
3.4.4.2 Notifications ... 71
3.4.4.3 Availability ... 72
3.4.4.4 Status Trends ... 73
3.4.4.5 Indicator Trends ... 74
3.4.5 Inventory Information ... 75
3.4.5.1 Platform Information ... 75
3.4.5.2 Operating System Information ... 77
3.4.6 Operations Menu ... 82
3.4.6.1 Platform Menu ... 82
3.4.6.2 Operating system Menu ... 83
3.4.6.3 Storage Menu ... 83
3.4.6.4 Consolidation Menu ... 83
3.4.6.5 Application Menu ... 83

Chapter 4. Using Bull System Manager Console Applications ... 85

4.1 Bull System Manager Hardware Management Application ... 85
4.1.1 Host Selection ... 86
4.1.1.1 Host Properties ... 86
4.1.2 Commands ... 88
4.1.2.1 Prerequisites ... 88
4.1.2.2 Command Outputs ... 89
4.2 Reports ... 92
4.3 Other Applications ... 94

Chapter 5. Categories and Services Reference List ... 95

5.1 Monitoring Hosts ... 95
5.1.1 Internet Category ... 95
5.1.1.1 HTTP ... 95
5.1.1.2 HTTP_BSM ... 95
5.1.1.3 FTP ... 96
5.1.1.4 TCP_n ... 96
5.1.1.5 UDP_n ... 96
5.1.2 Reporting Category ... 96
5.1.2.1 Perf_indic ... 96
5.2 Monitoring Linux or AIX Systems ... 97
5.2.1 FileSystems Category ... 97
5.2.1.1 All Service ... 97
5.2.2 LinuxServices Category (for Linux system) ... 98
5.2.2.1 Syslogd Service ... 98
5.2.3 AIXServices Category (for AIX system) ... 98

5.2.3.1 Syslogd Service 98
5.2.4 Syslog Category 99
5.2.4.1 AuthentFailures Service (for Linux system) 99
5.2.4.2 Errors Service (for AIX system) 100
5.2.4.3 Alerts Service (for Linux and AIX system 101
5.2.5 SystemLoad Category 101
5.2.5.1 CPU Service (for Linux system) 101
5.2.5.2 CPU Service (for AIX system) 102
5.2.5.3 Memory Service (for Linux system) 103
5.2.5.4 Processes Service (for Linux system) 103
5.2.5.5 Users Service (for Linux system) 104
5.2.5.6 PagingSpace Service (for AIX system) 104
5.2.5.7 Swap Service (for AIX system) 105
5.3 Monitoring Windows Systems 106
5.3.1 EventLog Category 106
5.3.1.1 Application Service 106
5.3.1.2 Security Service 107
5.3.1.3 System Service 108
5.3.2 LogicalDisks Category 109
5.3.2.1 All Service 109
5.3.3 SystemLoad Category 109
5.3.3.1 CPU Service 109
5.3.3.2 MemoryUsage Service 110
5.3.4 WindowsServices Category 111
5.3.4.1 EventLog Service 111
5.4 Hardware Monitoring 112
5.4.1 Hardware Category for Express 5800 112
5.4.1.1 PowerStatus Service 112
5.4.1.2 Alerts Service 112
5.4.2 Hardware Category for NovaScale 3000 Series 113
5.4.2.1 PowerStatus Service 113
5.4.2.2 Alerts Service 113
5.4.3 Hardware Category for NovaScale T800 & R400 Series 113
5.4.3.1 PowerStatus Service 113
5.4.3.2 Alerts Service 114
5.4.4 Hardware Category for NovaScale 4000 Series 114
5.4.4.1 Alerts Service 114
5.4.4.2 PowerStatus 115
5.4.4.3 Health Service 115
5.4.5 Hardware Category for NovaScale 5000 & 6000 Series 116
5.4.5.1 Health Service 116
5.4.6 Hardware Category for NovaScale 9006 Series 117
5.4.6.1 Alerts Service 117
5.4.6.2 PowerStatus Service 117
5.4.6.3 PowerConsumption Service 117
5.4.7 Hardware Category for Blade Series 117
5.4.7.1 Health Service 117
5.4.8 Hardware Categories for Escala Servers 118
5.4.8.1 CECStatus Service 118
5.4.8.2 Events 118

5.5 Blade Monitoring 119
5.5.1 CMM Category 119
5.5.1.1 ChassisStatus Service 119
5.5.1.2 Alerts Service 119
5.6 Storage and Virtualization Monitoring 120
Index 121

List of Figures

Figure 1-1 Overview of Bull System Manager functions 1
Figure 2-1 Bull System Manager console 9
Figure 2-2 bsmadm user authentication – Linux 11
Figure 2-3 Example of expanded Hosts tree 12
Figure 2-4 Example of functional filter menu 13
Figure 2-5 OperatingSystem domain filter use 14
Figure 2-6 Alert History window 15
Figure 2-7 Status Information for an instance of the EventLog.Application service 16
Figure 2-8 Example of Status Trends for EventLog.Application service (last 24 hours) - 17
Figure 2-9 Host status display - example 18
Figure 2-10 Host information - example 19
Figure 2-11 Scheduled downtime lists 21
Figure 2-12 Starting UltraVNC Viewer on a host 24
Figure 2-13 VNC Authentication window 25
Figure 2-14 Remote connection to a Windows host with VNC Viewer 25
Figure 2-15 Launching Webmin window 26
Figure 2-16 Webmin login window 27
Figure 2-17 Webmin interface on Linux hosts 27
Figure 2-18 HW Manager GUI menu 29
Figure 2-19 PAM Hardware Manager - Home Page 30
Figure 2-20 Launching the Remote Hardware Management Window 31
Figure 2-21 Remote Hardware Management window 32
Figure 2-22 Bull System Manager Reporting Indicators Home Page 33
Figure 2-23 Bull System Manager Reporting Indicators - example 34
Figure 2-24 Bull System Manager Server Control 35
Figure 2-25 Bull System Manager Server Status 35
Figure 3-1 Management Tree 37
Figure 3-2 A service node menu 38
Figure 3-3 Management Tree menu 38
Figure 3-4 Management Tree commands 38
Figure 3-5 Management Tree animation - example 39
Figure 3-6 Node icon menu 40
Figure 3-7 Deactivating supervision - example 40
Figure 3-8 Hosts view 48
Figure 3-9 HostGroups view 48
Figure 3-10 HW Managers view 49
Figure 3-11 Storage Managers view 50
Figure 3-12 Functional Domain view example 51
Figure 3-13 Map mode 52
Figure 3-14 Bull System Manager Alert Viewer 53
Figure 3-15 Alert Selection 54
Figure 3-16 Alert selection - example 54
Figure 3-17 Acknowledged alerts selection 55
Figure 3-18 BSM Focus windows example 57
Figure 3-19 Status detailed information from the BSM Focus window. 57
Figure 3-20 Supervision Window 58
Figure 3-21 Hostgroup Status Overview 59

Figure 3-22 Servicegroups Status Overview 60
Figure 3-23 Host Status Overview 60
Figure 3-24 Host Status GRID 61
Figure 3-25 Hosts Status Detail 62
Figure 3-26 Host Status 63
Figure 3-27 Service Status 63
Figure 3-28 Monitoring Server Configuration 64
Figure 3-29 Monitoring Server Log 65
Figure 3-30 Monitoring Server commands 66
Figure 3-31 Performance statistics 67
Figure 3-32 Scheduling Information 68
Figure 3-33 Monitoring Host commands 68
Figure 3-34 Alert History screen - example 70
Figure 3-35 Notifications screen - example 71
Figure 3-36 Availability screen - example 72
Figure 3-37. Status Trends on a Service 73
Figure 3-38 Indicator Trends on a Host 74
Figure 3-39 Hardware Inventory information – example 76
Figure 3-40 Storage information - example 76
Figure 3-41 Windows Memory screen - example 77
Figure 3-42 Windows Process screen - example 78
Figure 3-43 Windows Users screen - example 78
Figure 3-44 Windows Products screen - example 78
Figure 3-45 Windows Logical Disks screen - example 79
Figure 3-46 Windows Services screen - example 79
Figure 3-47 Linux Memory Usage screen - example 79
Figure 3-48 Linux Process screen - example 80
Figure 3-49 Linux Users screen - example 81
Figure 3-50 Linux RPM Products - example 81
Figure 3-51 Linux System Logs screen – example 82
Figure 4-1 Remote Hardware Management screen 85
Figure 4-2 NovaScale 5000 Server host properties - example 86
Figure 4-3 Power Status output - example 89
Figure 4-4 FRU output - example 90
Figure 4-5 SENSOR output - example 90
Figure 4-6 SEL output - example 91
Figure 4-7 PAM History output - example 91
Figure 4-8 Indicator Reports 92
Figure 4-9 Daily and Weekly Report Graphs - example 93
Figure 4-10 Other applications 94

List of Tables

Table 1-1. Users, Roles and Functions 2
Table 3-1. Management Tree nodes 41
Table 3-2. Root node menu 42
Table 3-3. PAM and CMM status levels 42
Table 3-4. RMC status levels 43
Table 3-5. Hardware Manager node menu 43
Table 3-6. Storage Manager node menu 44
Table 3-7. Virtual Manager node menu 44
Table 3-8. Platform node and Hostgroup node menus 44
Table 3-9 Host status levels 45
Table 3-10 Host node menu 45
Table 3-11. Category node menu 45
Table 3-12. Service status levels 46
Table 3-13. Service node menu 46
Table 3-14. Tree views 47
Table 3-15. Monitoring information 59
Table 4-1. NovaScale 4000 Server host properties 87
Table 4-2. NovaScale 5000 or 6000 Server host properties 87
Table 4-3. Express 5800 Server host properties 87

Preface

Scope and Audience of this Manual

This manual is intended for Operators who monitor and manage Bull servers using **Bull System Manager**, and in particular via the Bull System Manager Console. It comprises the following chapters:

Chapter 1	**About Bull System Manager** presents Bull System Manager architecture and components.
Chapter 2	**Getting Started** explains how to use Bull System Manager to perform basic monitoring and management tasks.
Chapter 3	**Using Bull System Manager Console** describes Bull System Manager Console functionalities and use.
Chapter 4	**Using Bull System Manager Console Applications** describes Bull System Manager Console applications and use.
Chapter 5	**Categories and Services Reference List** describes Bull System Manager monitored categories and default services, according to operating system and hardware

Highlighting

The following highlighting conventions are used in this manual:

Bold	Identifies commands, keywords, files, structures, directories, and other items predefined by the system. Also identifies graphical resources such as buttons, labels and icons that the user selects.
Italics	Identifies chapters, sections, paragraphs and book names to which the reader must refer for more information.
`Monospace`	Identifies examples of specific data values, examples of text similar to what you might see displayed, messages from the system, or information you should actually type.

Note Important information

Related Publications

For more information about Bull System Manager, please refer to:

- *Bull System Manager Installation Guide* (Ref. 86 A2 54FA)
- *Bull System Manager Administrator's Guide* (Ref. 86 A2 56FA)
- *Bull System Manager Remote Hardware Management CLI Reference Manual* (Ref. 86 A2 58FA)
- *Bull System Manager Server Add-ons Installation and Administrator's Guide* (Ref. 86 A2 59FA)

- Restrictions and known problems are described in the associated *Release Notes* document (Ref. 86 A2 57FA).
- For information about the Open Source products used by Bull System Manager, please refer to:
  http://www.nagios.org (for Nagios product)
  http://www.webmin.com (for Webmin product)
  http://www.mrtg.hdl.com (for MRTG product)

Chapter 1. About Bull System Manager

1.1 Scope

Bull System Manager is the graphical interface tool used to manage Bull servers. It provides two main functions:

Supervision (Monitoring, Reporting, Information)

System resources are supervised, and when any anomalies are detected, the entities defined for notification will be notified. An interface is also provided that displays all the important data.

Administration (Remote Control)

BSM can be used to configure target hosts, and to execute actions on these hosts via the Operating System or via a Hardware Management tool.

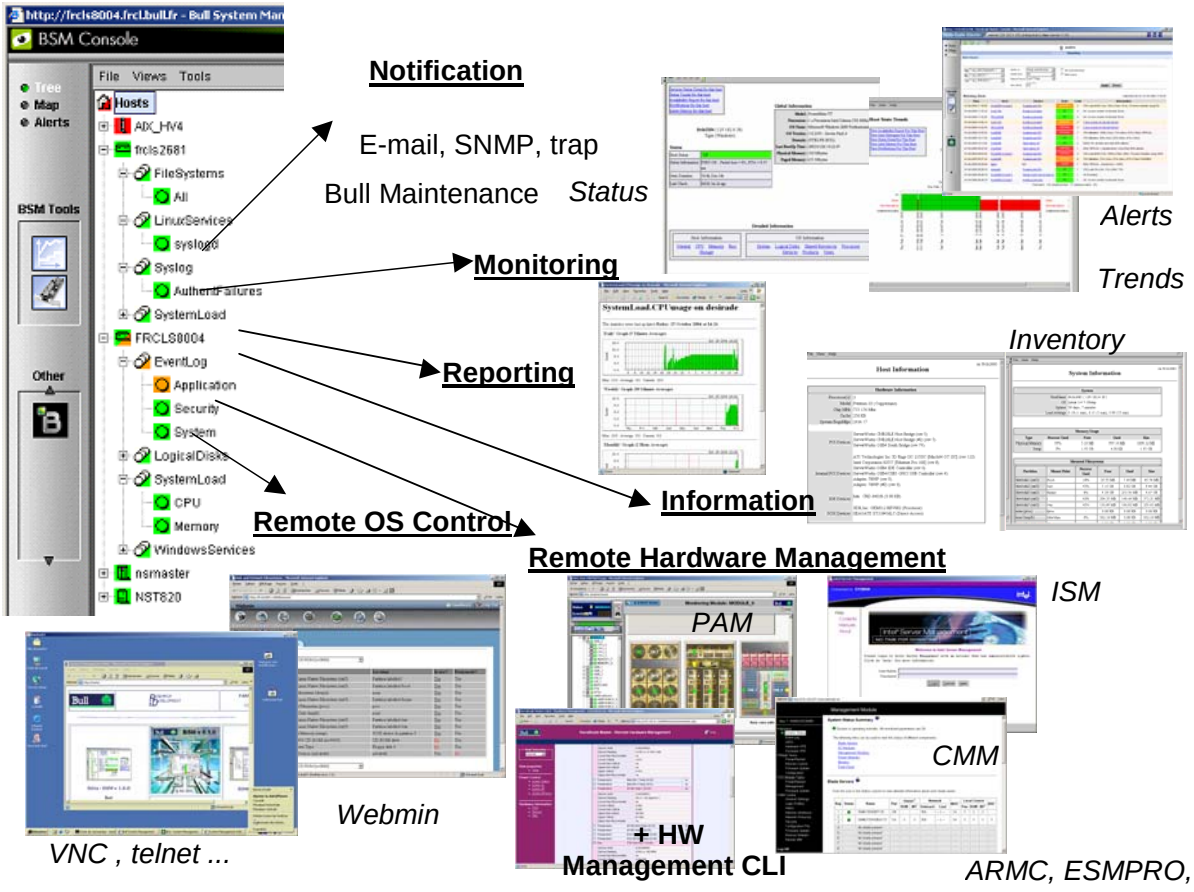


Figure 1-1 Overview of Bull System Manager functions

Four roles, with a different set of rights, are defined in Bull System Manager Server, as described below:

Role	BSM Configuration	BSM Control	BSM Console		
			Global monitoring control menu (at the tree root)	Host Monitoring control menu	Host Remote Operation menu
Administrator	Write	Yes	Yes	Yes	Yes
BSM-Administrator	Write	Yes	Yes	Yes	No
System-Administrator	ReadOnly	No	No	Yes	Yes
Operator	ReadOnly	No	No	Yes	No

Table 1-1. Users, Roles and Functions

1.1.1 Supervision Features

- **Host Monitoring**
  Checks if the target host is accessible (via the **ping** command).
- **Monitoring Services**
  Monitors OS CPU load, memory usage, disk usage, number of users, processes and services execution, HTTP and FTP services.
  Thresholds are used to assign a state (**OK**, **WARNING**, **CRITICAL**, **UNKNOWN**) to hosts and to each element monitored.
  Alerts (in a log file) and notifications (by email) are generated when anomalies occur or when normal states resume (return to **OK** state).
  Monitoring Services are classified into the following Monitoring Categories: **SystemLoad**, **Filesystems**, **EventLog**
- **Hardware Monitoring**
  - **NovaScale servers** obtain a hardware status via a call to the **IPMI** Out-of-Band access.
  - **novascale bullion servers obtain a hardware status via a call to EMM (IPMI).**
  - **Blade servers** obtain a hardware status via a call to CMM.
  - **Escala servers** obtain a hardware status via a call to HMC or IVM.
  - **Express 5800 servers** obtain a power status via a call to the RMC Management Card.
- **Virtualization Monitoring**
  - **Escala LPARs** obtain a virtualization status via a call to HMC or IVM.

- **Selectable View Displays**
  The presentation of different hosts and monitoring service views. A view is a tree structure that can display:
  - the entire host list
  - managers and the hosts they manage
  - host groups

  From each tree node, the user can display detailed information about a host or a service, according to the User role (Administrator or Operator).
- **Group Definitions**
  It is possible to define Host groups so the server infrastructure can be organized as a tree.
- **Functional domain filter Definitions**
  Service groups can be defined to filter topological trees and maps in order to obtain monitoring information for a specific functional domain (Hardware, Operating System, Network, Storage, etc.).
- **Alerts**
  Notification of problems via email, SNMP traps or Bull format autocalls.
- **Selectable Map Displays**
  Presentation of host groups (with the status of their hosts and monitored services) using different maps.
  A **map** is a layout, in general with a background image, which displays associated host groups. Host groups are located at specified positions (x, y) on the map, and display the status of associated hosts and monitoring services.
  From a host group, the user can display detailed information about all the associated hosts.

1.1.2 Administration Features

- **Eventhandling** mechanism based on status changes.
- **Webmin Management Tool for Linux hosts**
  Webmin is an Open Source product that gives OS information (regarding users, file systems, etc.) or executes OS commands, in a graphical environment, locally on the **Linux** target hosts.
- **Remote Operation Tools**
  - **telnet** to access Linux and Windows hosts.
  - **Rdesktop** or **UltraVNC** to access Windows hosts. UltraVNC is an Open Source product that allows you to take control of a remote host, within its own Windows environment.
- **Hardware Manager Calls**
  - **PAM** for NovaScale 5000 and 6000 Series platforms
  - **CMM** for NovaScale and EvolutiveLine Blade Series Chassis platforms
  - **HMC for Escala PL servers**
  - **BMC (or iDRAC) for NS T800 and NS R400 servers**
  - **ARMC** for Express 5800 servers

Targeted systems can be powered on/off via these managers and Bull System Manager provides a single Hardware Management GUI for basic tasks.

- Virtualization Manager Calls
  - **ESX web GUI or VirtualCenter** for VMware ESX platforms
  - **IVM or HMC** for Escala LPAR platforms
- Storage Manager Calls

  Embedded Storage Manager GUI for the storage bays.

1.2 Basic Definitions

1.2.1 BSM local Console

The BSM local Console is used to manage locally configured hosts on a BSM server node.

1.2.2 BSM global Console

The BSM global Console is used to manage all configured hosts on a set of BSM servers, linked between them via a centralized DataBase containing configuration and exploitation information.

1.2.3 Service

A **service** monitors specific system items. Monitoring agents compute the status (**OK**, **WARNING**, **CRITICAL**, **UNKNOWN** or **PENDING**) and status information (a message providing more details regarding the status) for each service.

Example
The **CPU** service monitoring the status of the CPU usage will display a message similar to that below:

```
CPU Load OK (1mn: 8%) (10mn: 5%)
```

1.2.4 Category

A **category** is a container for a group of services.

Example
The **SystemLoad** category for Windows systems contains both the CPU and Memory services.

1.2.5 Functional domain filter (or Servicegroup)

A **service group** is a list of instantiated services that can be used to filter topological views and maps.

Example
The **OperatingSystem** service group includes all services that monitor OS items (meaning all categories that monitor the Operating System).

By default, BSM provides the following list of functional domains: **Hardware, OperatingSystem, Storage and Network**.

Note These functional domains are not activated by default

Other functional filters are provided by BSM Server AddONs (e.g. Virtualization).

1.2.6 View

A **view** displays the monitored hosts as a set. Views differ in structure and granularity, but they all display hosts and the status (**OK**, **WARNING**, **CRITICAL**, or **UNKNOWN**) of their services, and associated services monitored, in a graphical format, classified into categories under the host node.

The views will display only what a user wants to see at a given time, for example, the **Host**s view, and not the **Managers** or **Host groups** views.

Notes

- According to the configuration, a category may or may not be present. For more details, refer to the *Administrator's Guide*
- The menus for each type of node in a view are described later in this manual.

1.2.7 Map

A **map** can be used to display the status for a grouping of host groups (and their monitored hosts) on the screen.

In general, the map has a background image and the host groups are located at specified positions (x, y) on the map. Maps differ in appearance, but they all display host groups graphically indicating the status for the service, calculated from the status of the associated hosts and services that are monitored.

When you zoom in on a host group, you can view the associated hosts and the overall service status (derived from the worst service status for all the associated services monitored).

The advantage of maps is that display only what a user wants to see for a given context.

As Administrator, you can create customized maps for host groups in different contexts. Refer to the *Administrator's Guide* for details.

1.3 Bull System Manager Components

Bull System Manager is based on a 3 tier architecture:

- **Monitoring Console**
  This web-based application running in a browser (**Internet Explorer** or **FireFox**) accesses the monitoring data collected using web technology. There are two types of BSM consoles: the local one and the global one. (see section 1.2)
- **Monitoring Server**
  Collects, processes, and stores monitoring and reporting data. It runs on both Windows and Linux platforms.
- **Monitoring Agent**
  Contains the basic programs, used to obtain monitoring and inventory information. It is installed on each target system.

Bull System Manager comprises the following Open Source software:

- **Nagios, SNMPTT, ...**
  For the monitoring functions
- **MRTG**
  For the reporting indicators functions
- **Webmin**
  A **Linux** administration tool (a standard Webmin package and a Bull System Manager **Webmin** restricted to obtaining information).
- **UltraVNC Server**
  For remote operation on **Windows** hosts.
- **IPMItool**
  For remote operation on hardware systems that contain **Intel BMC**s (Baseboard Management Controller).

Bull System Manager also comprises an optional component for scripting applications for Linux platforms:

- **Hardware Commands**
  A Command Line Interface (**CLI**) for remote hardware management, providing an easy interface for automating scripts to power on/off, or to obtain the power status for a system.
  These commands can only be used on:
  - Express 5800 servers
  - NovaScale series servers
  - novascale bullion servers
  - bullx servers
  - Bull Blade servers
  - Escala servers

1.4 Bull System Manager and Security

The security of Bull System Manager is ensured by a combination of secured applications that use authentication and profiling (role based) mechanisms.

1.4.1 Authentication

Each Bull System Manager application uses a user/password or single password authentication mechanism for access. Users are defined on the Bull System Manager server.

1.4.2 Role-based Management

Each Bull System Manager Console user is associated with a role (or set of functionalities). See section 1.1.

Chapter 2. Getting Started

This chapter explains how to use **Bull System Manager** for basic monitoring and administration tasks.

2.1 Starting the Console

See *Chapter 6* of the *Installation Guide* for details on how to launch the console and the applications.

2.1.1 Differences between local and global Console

Even if some contextual menu are absent in the global console (generally due to the localization of the associated URL), both consoles are very similar.

2.1.2 Console Basics

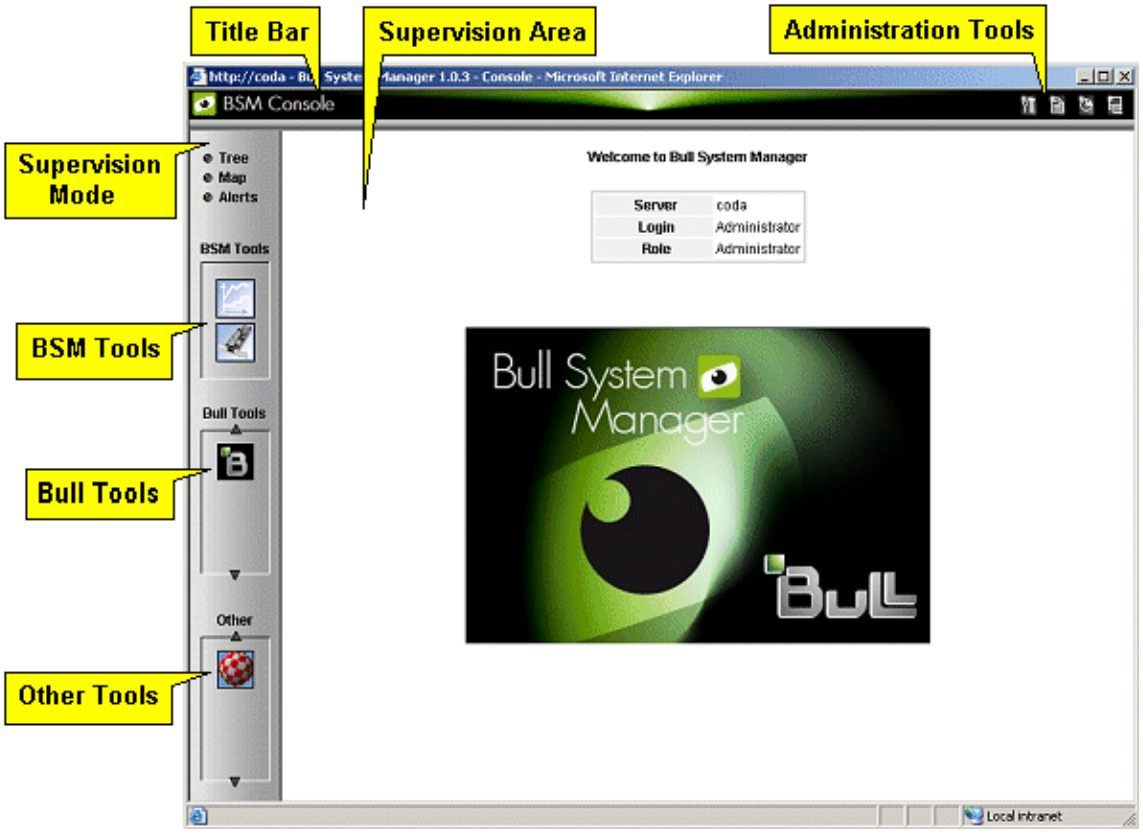


Figure 2-1 Bull System Manager console

The Bull System Manager console is divided into the following functional parts:

Title Bar Displays the server name.

Administration Tools Enable access to the following administration tools:

Bull system Manager focus (if needed, only in local console)
Bull System Manager configuration tool (only in local console)
Bull System Manager documentation
Bull System Manager download page
Bull System Manager Server control (only in local console)
Display of server information: Netname, Date/Time, Login, Role (and Global server for global console).

Supervision Mode Allows you to choose one of the three supervision modes:

Supervision using a tree
Supervision using a map
Supervision using alerts

Supervision Area Displays information about the resources monitored, related to the type of supervision (see *Supervision Information*, on page *57*)

BSM Tools Enables access to the Bull System Manager Tools (only in local console):
Reports, Hardware Management.

Bull Tools Enables access to the Bull Applications:
Bull Support, Cassatt Controller, Cassatt Manager, BPRSE, BPREE, ARF

Other Tools Enables access to external applications

2.1.3 Bull System Manager Authentication and Roles

Bull System Manager applications must be authenticated.
The authentication type varies according to the web Server (Apache) See the following paragraphs for more information.

Note To change the Bull System Manager authentication state, close all the web browser windows that are open, and start a new session for the browser. Otherwise, the browser will retain the existing authentication context.

2.1.3.1 Role Based Management

The authenticated user type will have a different user profile or role. See section 1.1

Note User roles can be only configured by the **Administrator**. Refer to the *Administrator's Guide* for more details.

2.1.3.2 Bull System Manager Server User Authentication – Linux & Windows

Apache server authentication

A default Apache user called **bsmadm** (password **bsmadm**) is created when Bull System Manager Server is installed. This user is not a Linux user and will only be used contextually by Apache Server.

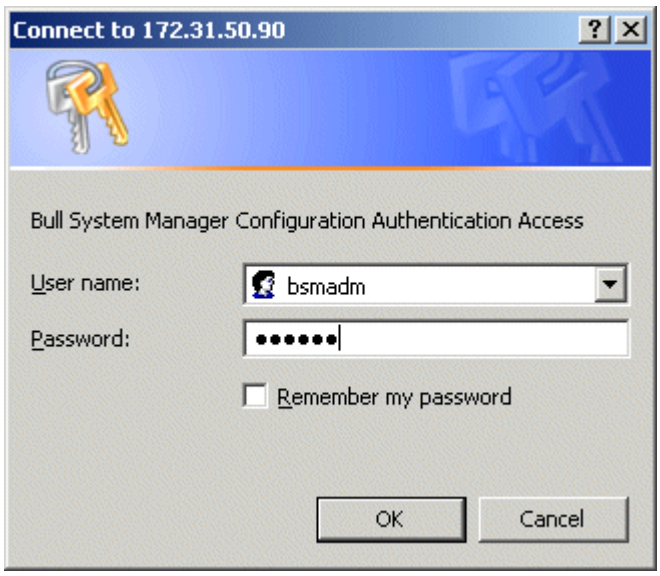


Figure 2-2 bsmadm user authentication – Linux

The users database is stored in the following file:
/opt/BSMServer/core/etc/htpasswd.users

Adding a New User / Modifying a Password

You can use the BSM configuration WEB GUI to add a new user or to modify a password on the Apache server:

2.2 Displaying Monitoring Information

2.2.1 Starting with the Tree mode

Notes

- Tree Mode concepts are explained in detail in *Chapter 3*.
- When the Console is started, the default view is opened, i.e. the **Hosts** view, displaying all the hosts declared at the same level.
  By clicking on , you can load four other views: the **Hostgroups** view, the **HardwareManager** view, **StorageManager** view or the **VirtualManager** view.
  As the Administrator, you can change the default view.

The left part of the console is a tree representing all the platforms managed. It can be expanded, as shown below:

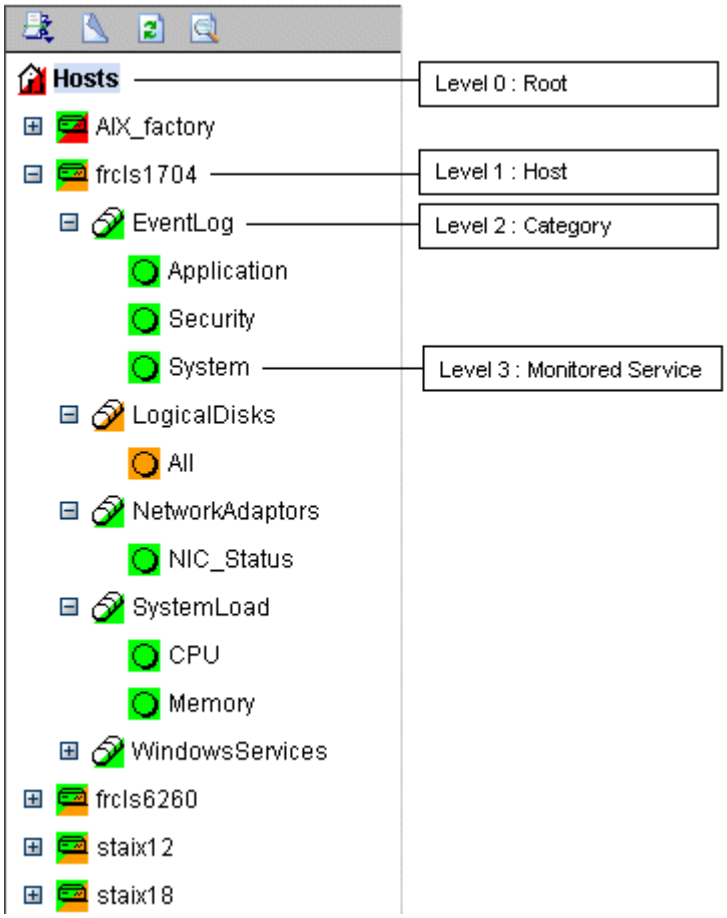


Figure 2-3 Example of expanded Hosts tree

A **Service** is a **Monitored Entity** and the color of the icon indicates the status for the service: red (critical), orange (warning), magenta (unknown) or green (OK).

Each icon is divided into two sections:

- The top left section indicates the status of the host or service,
- The bottom right cascades the subtrees.

For instance, for a Host node, when there is a service status change, the color of the bottom right corner of the category icon changes to reflect this change.

The color of the top left corner of a host icon indicates if this host is responding or not (following a **ping** command).

Example

The top left corner of the `nsmaster` host node is green because it responds to the ping command and the bottom right corner is green because all its services are ok.

A **Category** is a node that groups the services monitored logically. The overall Category status is determined by the most critical service status for the sub services or hosts.

2.2.2 Using a Functional domain filter with the Tree mode

For each tree, you can apply a functional domain filter from the menu, as shown in the graphic below:

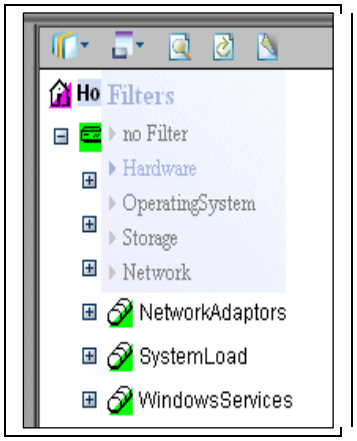


Figure 2-4 Example of functional filter menu

Thus, all contextual applicative frames will apply this functional domain filter for their content.

Notes

- The filter Menu can be used at any time, and applied to any topological level, in a tree or a map.
- Once selected, the filter will be active until it is unselected (**no Filter** setting)

The graphic below shows the use of the **OperatingSystem** filter for a NovaScale host:

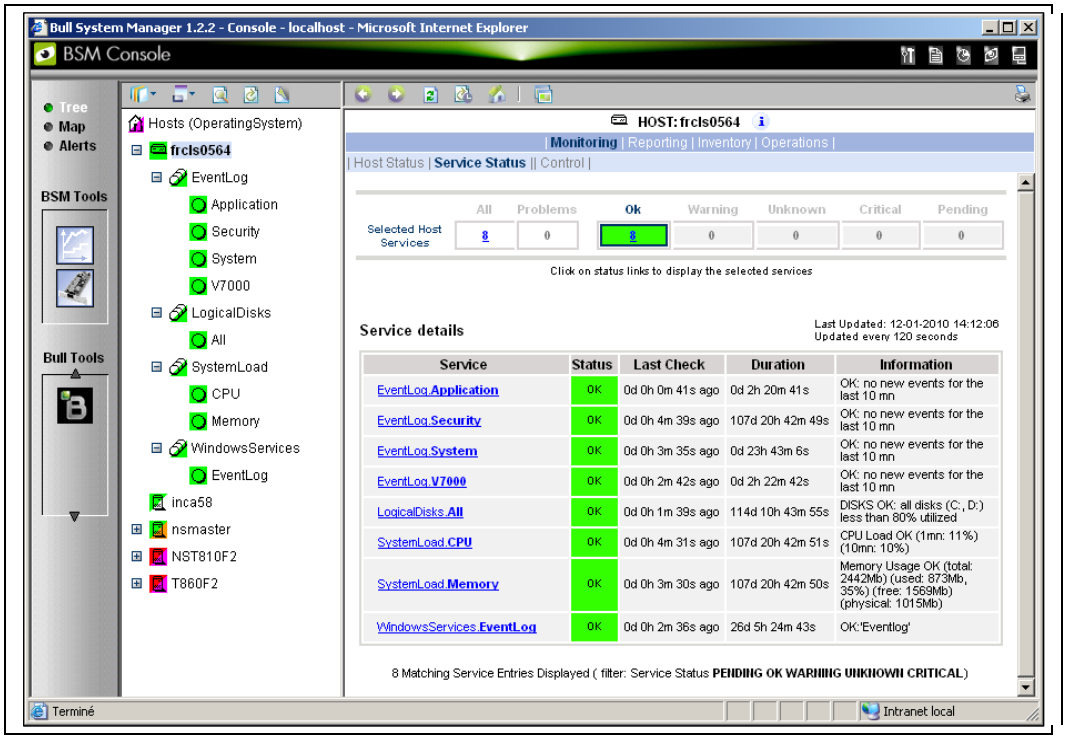


Figure 2-5 **OperatingSystem** domain filter use

Only Categories whose monitoring domain is **Operating System** are displayed.

2.2.3 Tracking Problems

When a problem occurs, it is useful to know if it has occurred previously, and if so, how often.

Bull System Manager provides several different ways to track and analyze problems.

2.2.3.1 Alert History

From the Applications Window, click **Reporting > Alert History**. The screen below appears (in this example, the host is called FRCLS8004).

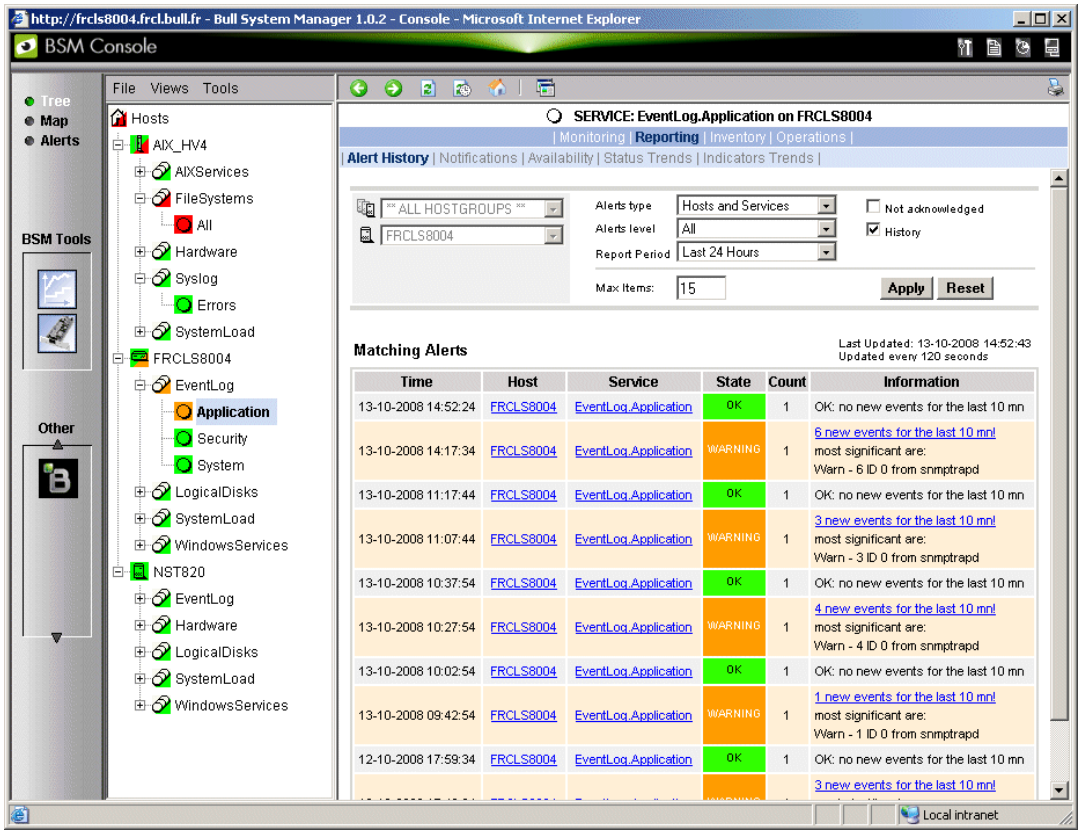


Figure 2-6 Alert History window

The **Alert History** shows all previous alerts for this service for different periods. Service information is also logged; this data can be used for the decision-making process regarding corrective actions.

2.2.3.2 Status Trends

The **Alerts** and **Trends** functions use monitoring logs to display the monitoring history:

- **Alerts** shows events.
- **Trends** shows a status graph for a defined period.

In the example shown in Figure 2-6, the monitored system is FRCLS8004. The tree displays **WARNING** states for the **EventLog.Application** service. Click **Application** to display additional status information.

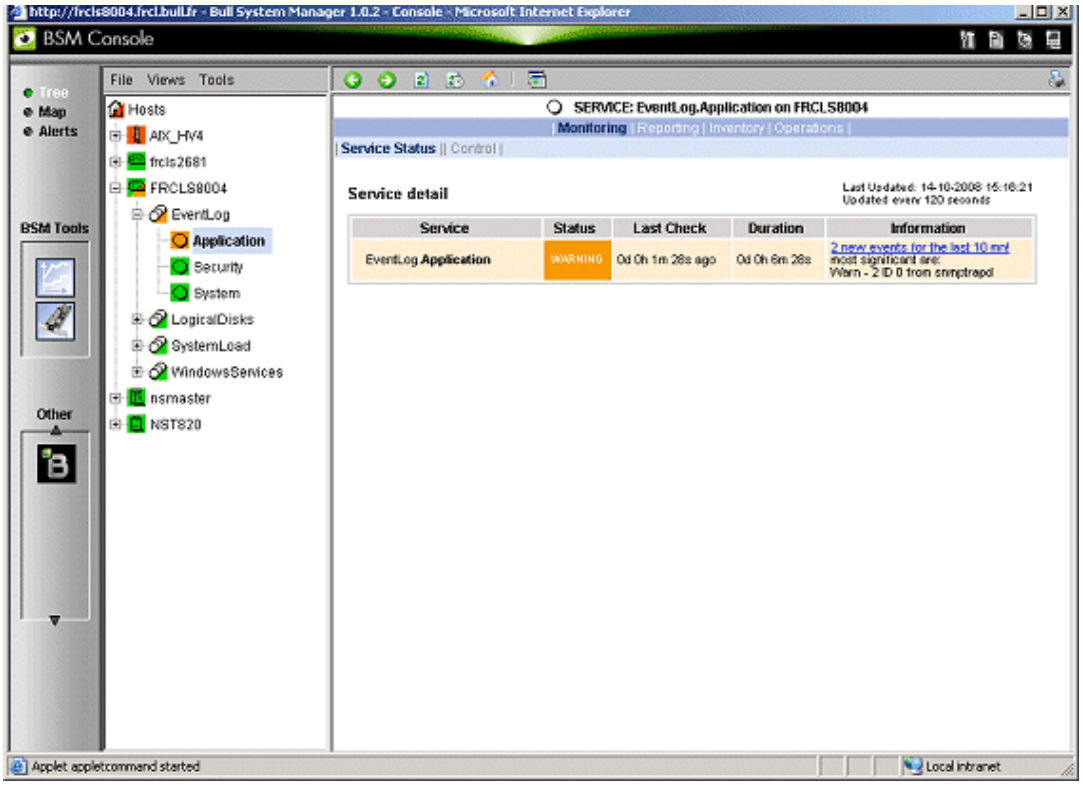


Figure 2-7 Status Information for an instance of the **EventLog.Application** service

Click **Reporting > Status Trends** if you would like to know how often, and when, this situation has occurred previously. A screen similar to that below will appear.

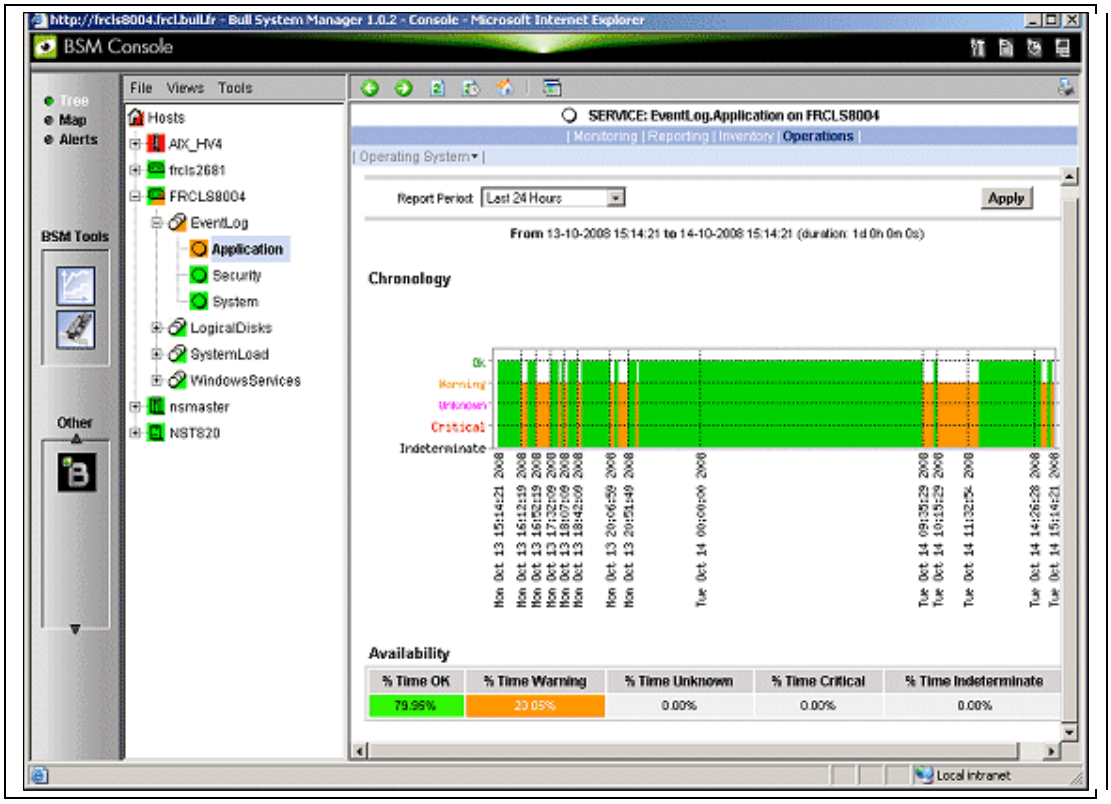


Figure 2-8 Example of Status Trends for **EventLog.Application** service (last 24 hours) -

The graph of the service for the previous 24 hours, in the example above, shows that **BSM** has registered some **EventLog.Application** warnings during this time.

2.2.4 Viewing More Information

The **Applications** Window displays more information, as and when requested by the Administrator via menu items or links.

- Click a **node** in the **Tree** Window to display basic monitoring information, according to the node type.
- Right-click a node in the **Tree** Window to display a pop-up menu giving access to all the operations available for that node.
- Click an option in the secondary level menu in the **Applications** Window to access additional information for that node.

Example

When you click the FRCLS8004 node, the following screen appears, indicating that the status for this host is UP:

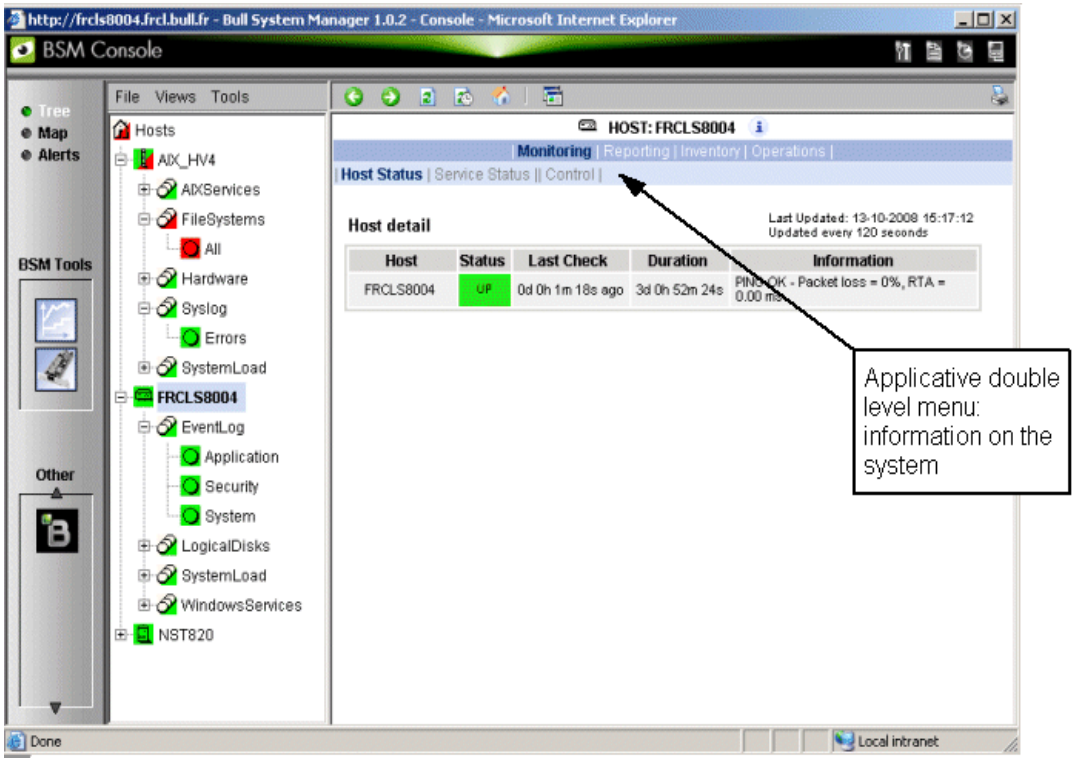


Figure 2-9 Host status display - example

From the **Applications** Window, click **Hardware Information > Inventory** to display the host hardware inventory.

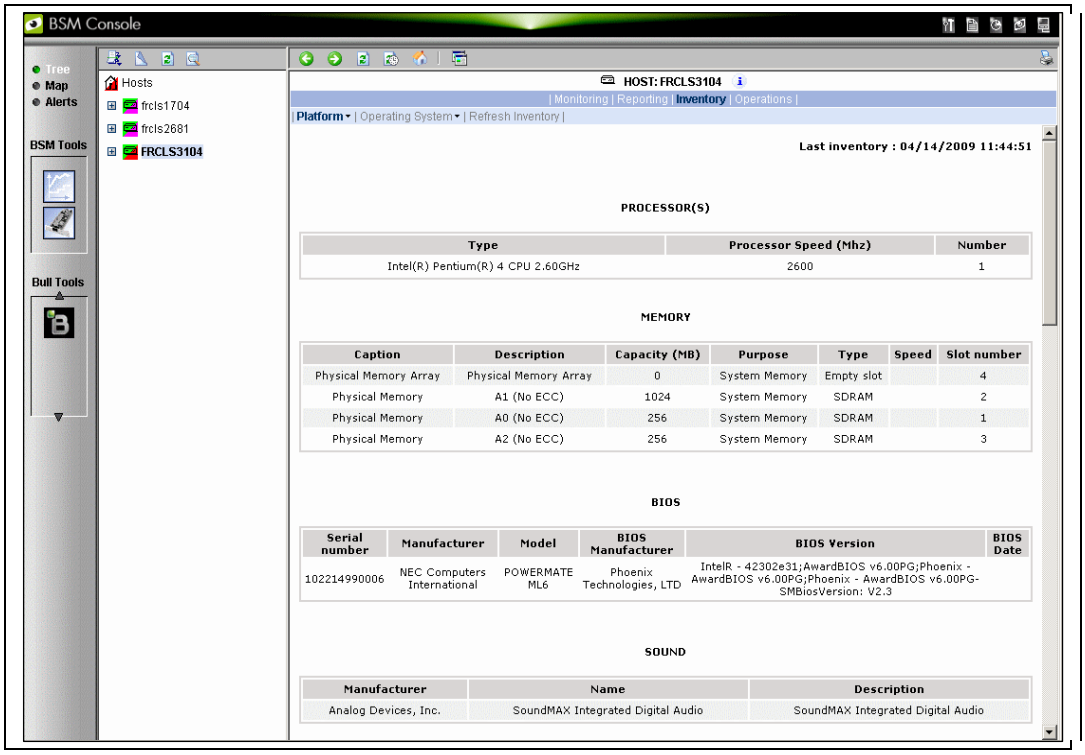


Figure 2-10 Host information - example

2.3 Receiving Alerts

The System Administrator can set up email and/or SNMP notifications, for enhanced operational monitoring.

2.3.1 Email Notifications

Configure email notifications as follows:

Step 1: Start the Bull System Manager Configuration window.

Step 2: Configure the Mail Server (only if Bull System Manager Server runs on a Windows system).

Step 3: Specify the mail address of the Alert receiver.

Step 4: Reload the monitoring service so that the modifications are taken into account.

Refer to the BSM *Administrator's Guide* for more details.

2.3.2 SNMP Trap Notifications

Configure SNMP notification as follows:

Step 1: Start Bull System Manager Configuration window.

Step 2: Specify the SNMP managers that will receive the traps.

Step 3: Reload the monitoring service so that the modifications are taken into account.

Refer to the BSM *Administrator's Guide* for details.

2.3.3 Viewing Notifications

In the following example, an authentication failure has generated an email notification:

```
***** Bull Bull System Manager *****
Notification Type: PROBLEM
Service: LogicalDisks.All
Host: w2k-addc01 Description: Portal DC (current network name: w2k-
addc01)
Address: w2k-addc01
State: CRITICAL
Date/Time: Wed May 18 16:26:21 GMTDT 2005
Additional Info:
DISKS CRITICAL: (Z:) more than 95% utilized.
```

The Bull System Manager Console allows you to view all the notifications sent by the monitoring service.

2.4 Scheduling Downtime

BSM (via Nagios) allows you to schedule periods of planned downtime for hosts and services that you are monitoring. This is useful in the case you know that you are going to be taking a server down for an upgrade, etc.

2.4.1 Show scheduled downtime lists

You can see all current scheduled downtime rules at the root menu: Monitoring/Downtime

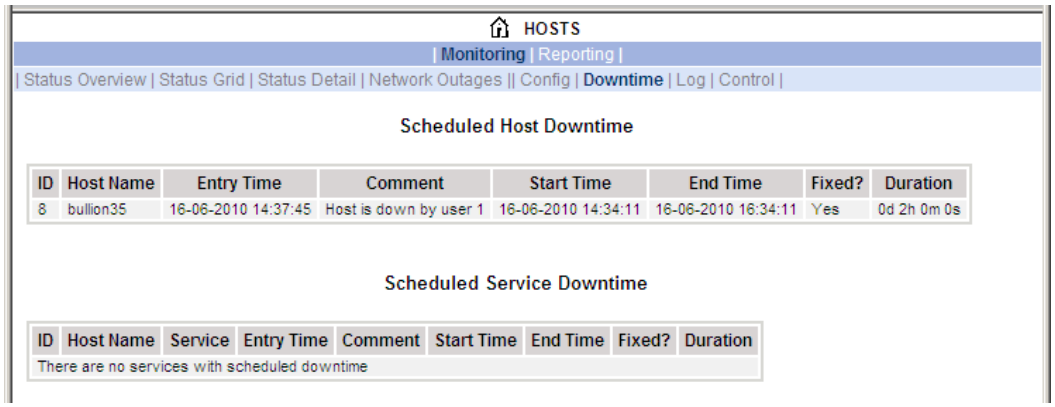
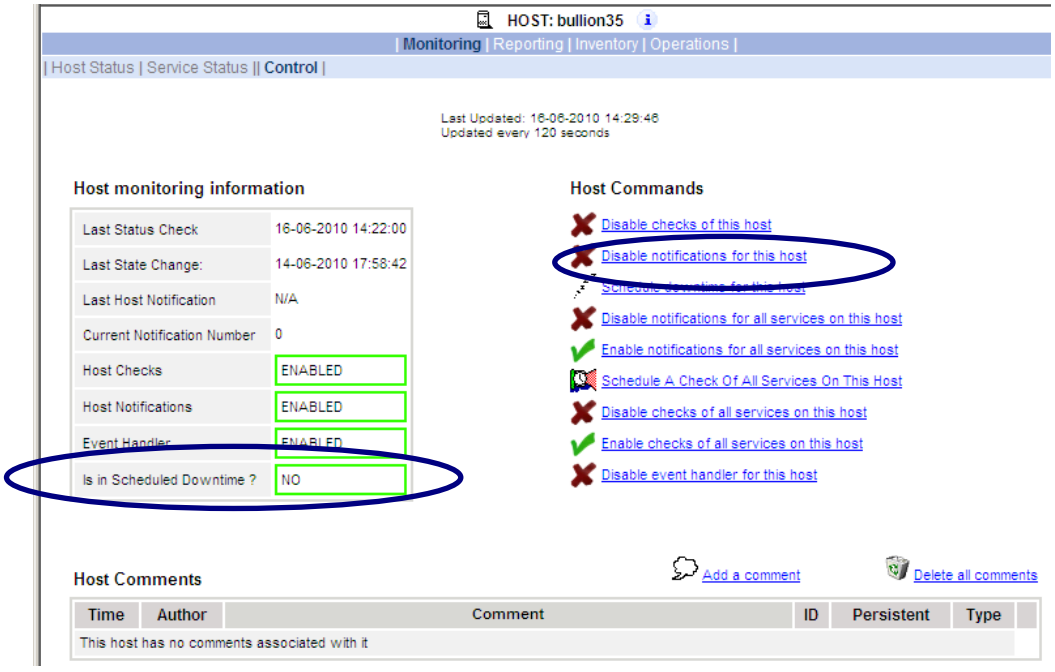


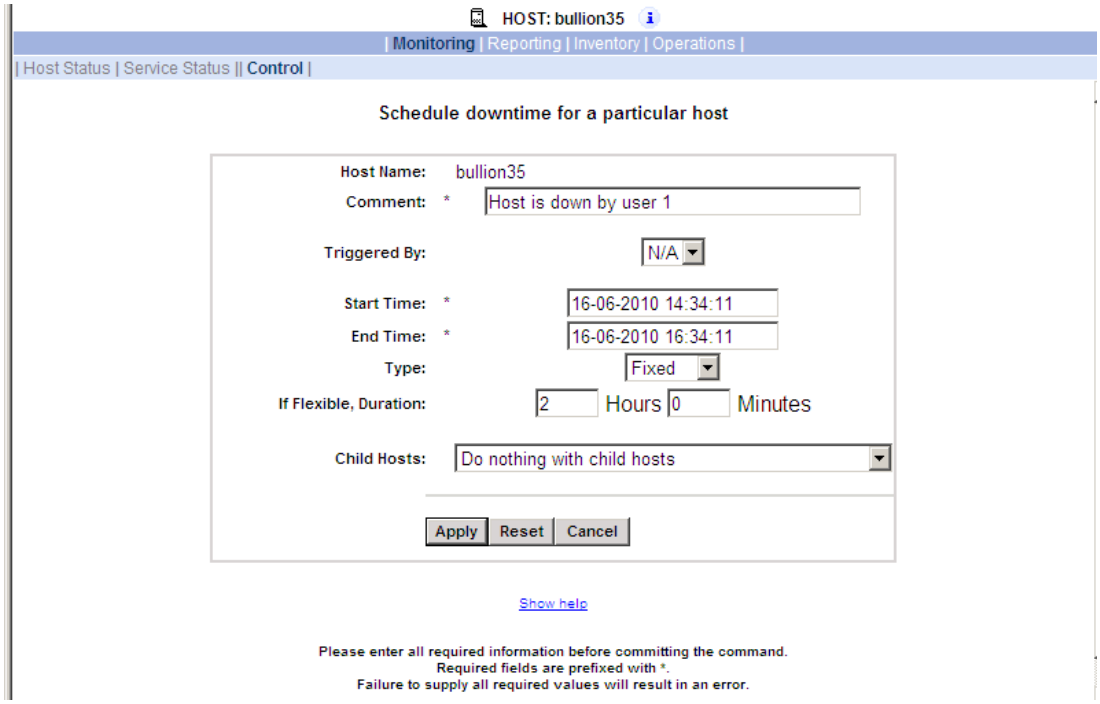
Figure 2-11 Scheduled downtime lists

2.4.2 How to schedule a downtime

You can schedule downtime for hosts and services through the Monitoring/Control menu:

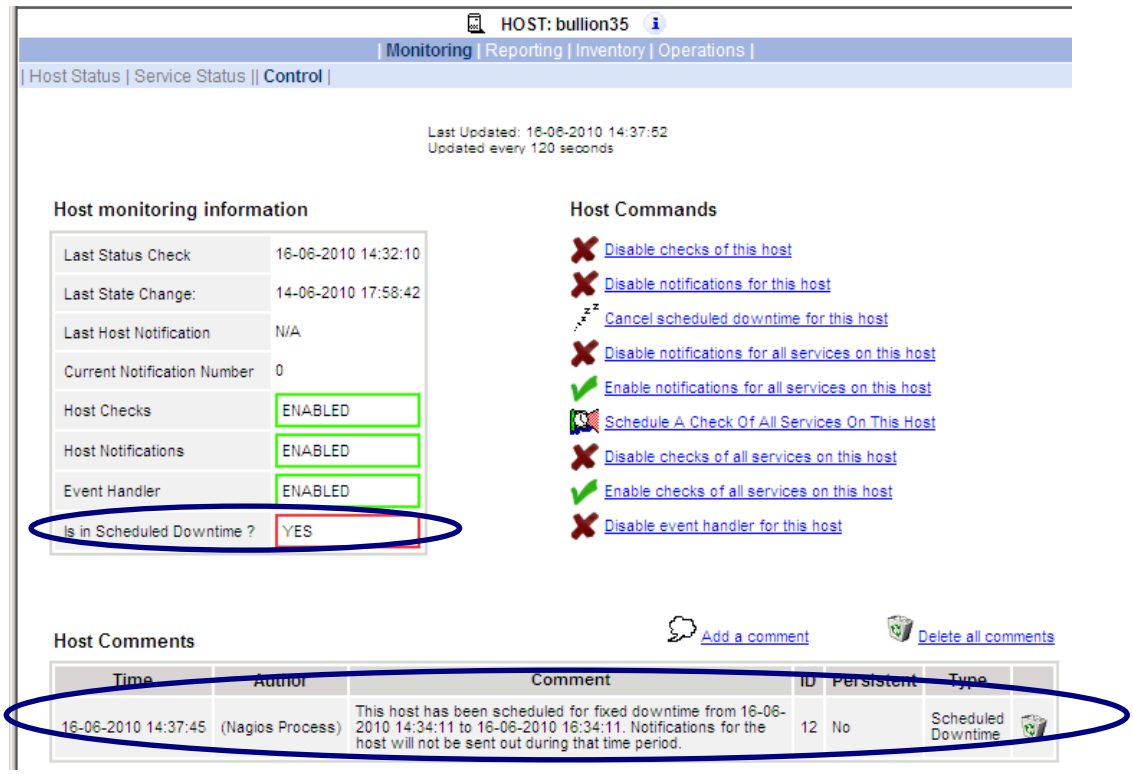


When you click on the hypertext link for this action, the following form must be completed and applied.



The "Show help" hypertext link gives more details for the fields list.

Once you schedule downtime for a host or service, BSM (Nagios) will add a comment to that host/service indicating that it is scheduled for downtime during the period of time you indicated. The following picture shows the Monitoring/Control CGI in a scheduled downtime state:

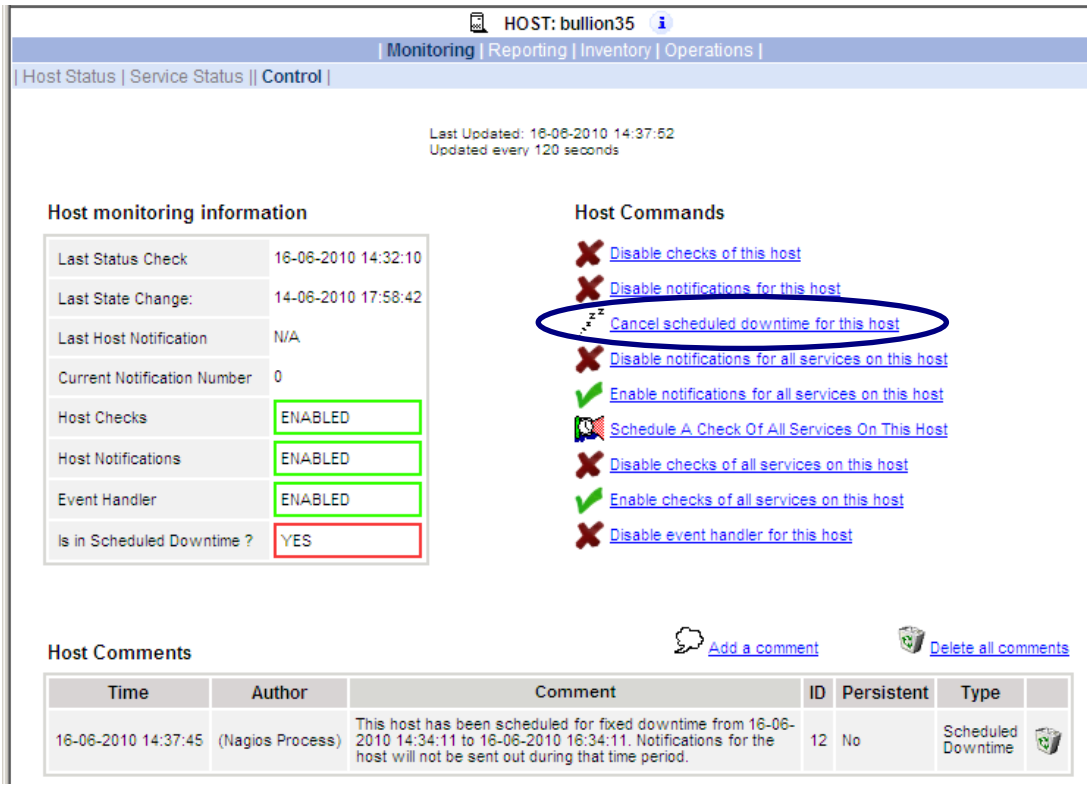


When that period of downtime passes or when the scheduled time is cancelled, BSM will automatically delete the comment that it added.

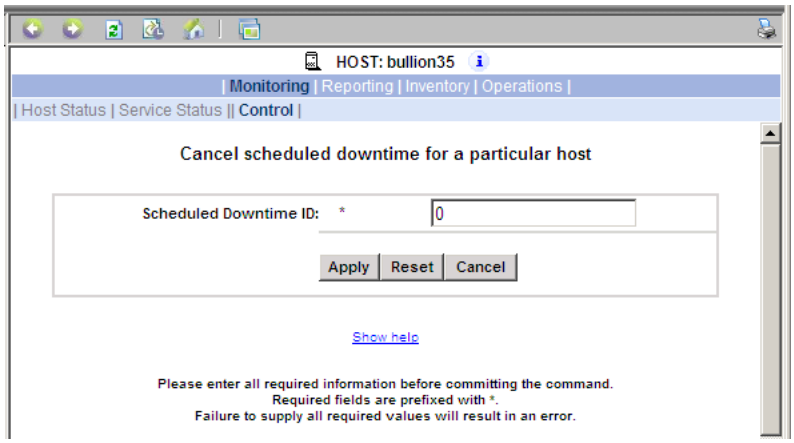
2.4.3 How to cancel a scheduled downtime

When the period of downtime passes, BSM will automatically delete the scheduled downtime rule and the comment that it added.

You can cancel a scheduled downtime via the Monitoring/Control menu associated to the related object (host or service).



Then the following form must be completed and applied.



NB: the Scheduled Downtime ID appears in the root Monitoring/Downtime web page (see Figure 2-11).

2.5 Taking Remote Control of a Host

As the Administrator, if you want to investigate a problem and fix it, you need to take a remote control of the platform concerned. Bull System Manager uses standard, commonly used tools to perform this function. These tools differ according to whether the remote Operating System is Windows or Linux.

2.5.1 Windows Hosts

UltraVNC Viewer is used to connect remotely to Windows hosts.

Note Prerequisite: The **VNC** package delivered with Bull System Manager must be installed and started on the remote host. Refer to the *Installation Guide* for details.

Example

Bull System Manager informs you that the **C:** disk is nearly full on the `nsmaster` Windows host, via the **LogicalDisks** node, and you decide to connect to `nsmaster` to see if you can free some disk space.

To connect to the remote host:

1. Start VNC Viewer from the `nsmaster` host menu (**Operations > Operating System > VNC Viewer**).

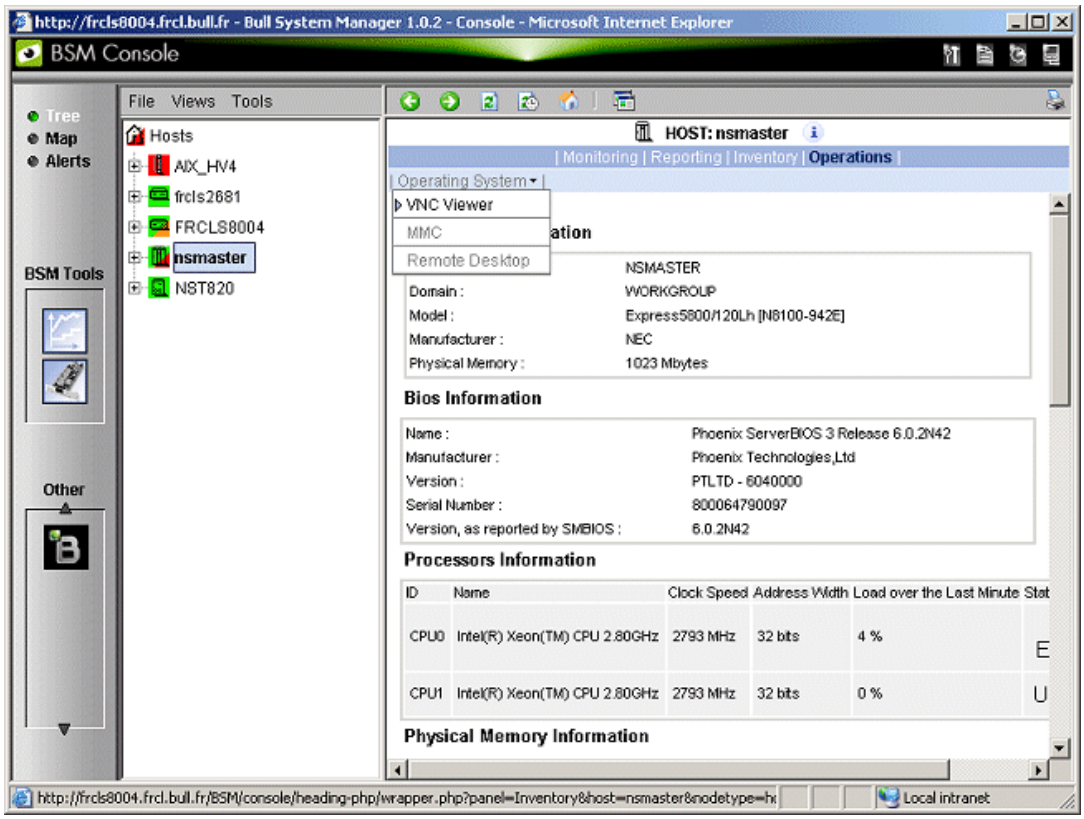


Figure 2-12 Starting UltraVNC Viewer on a host

2. When prompted, enter the password used when VNC Server was installed or configured on the target host (`nsmaster` in this example).

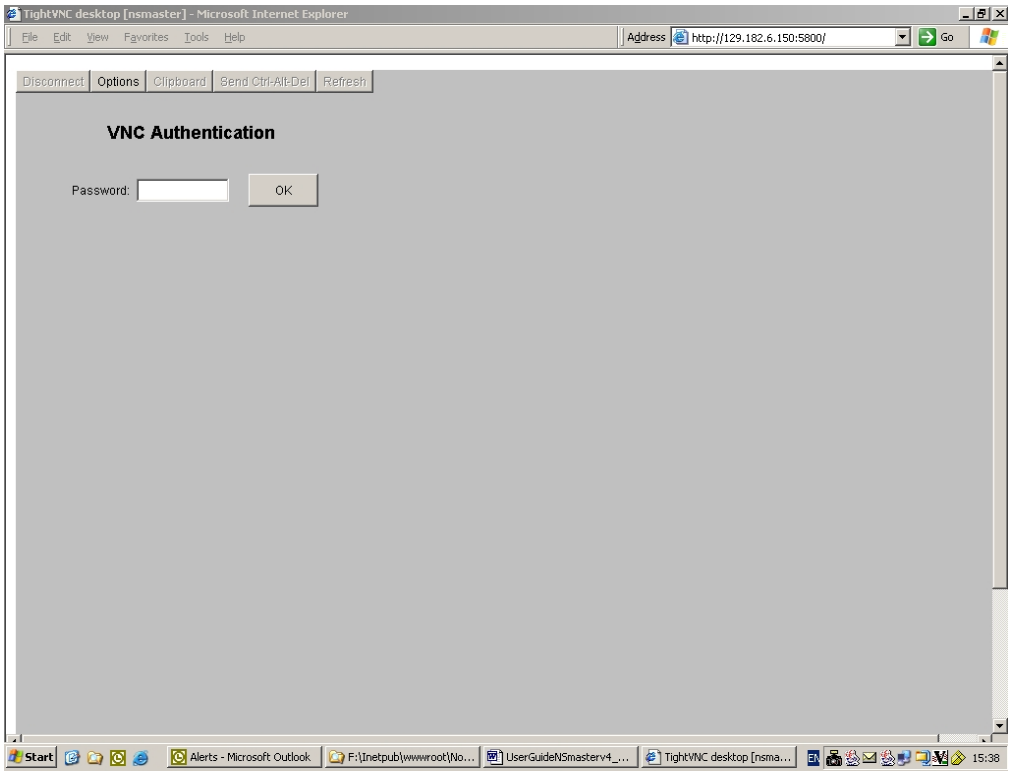


Figure 2-13 VNC Authentication window

3. Click **OK**. You now have full access to the remote host (`nsmaster`), although response times may be longer.

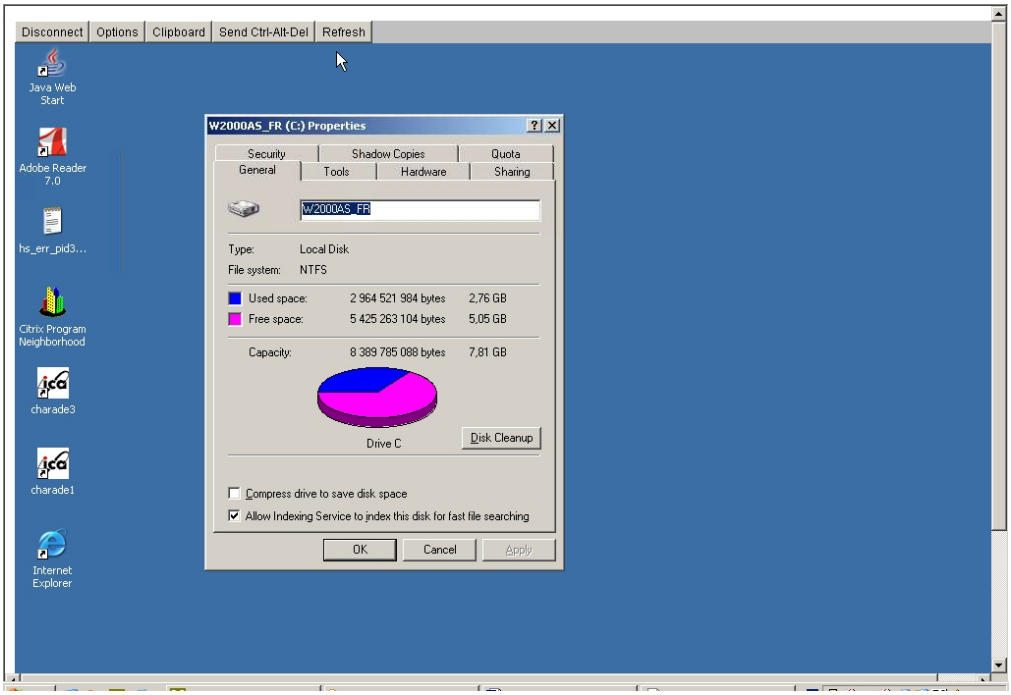


Figure 2-14 Remote connection to a Windows host with VNC Viewer

You can now display information related to disk C: and make changes.

Note If you do not require full access to the remote desktop, you can also open a telnet connection, as long as the telnet service has been started on the remote host.

2.5.2 Linux and AIX Hosts

Webmin is used to connect to Linux and AIX hosts remotely.

Note **Webmin** is a graphical tool for managing Linux and AIX systems and allows you to configure the system, application servers (http, mail, etc.), the network, and many other parameters. Webmin is Open Source software and the Open Source Community regularly adds new modules.

Example

You want to add a new user to your FRCLS2681 Linux host.

1. From the FRCLS2681 host menu, select **Operations > Operating System > UsersActions > Users**.

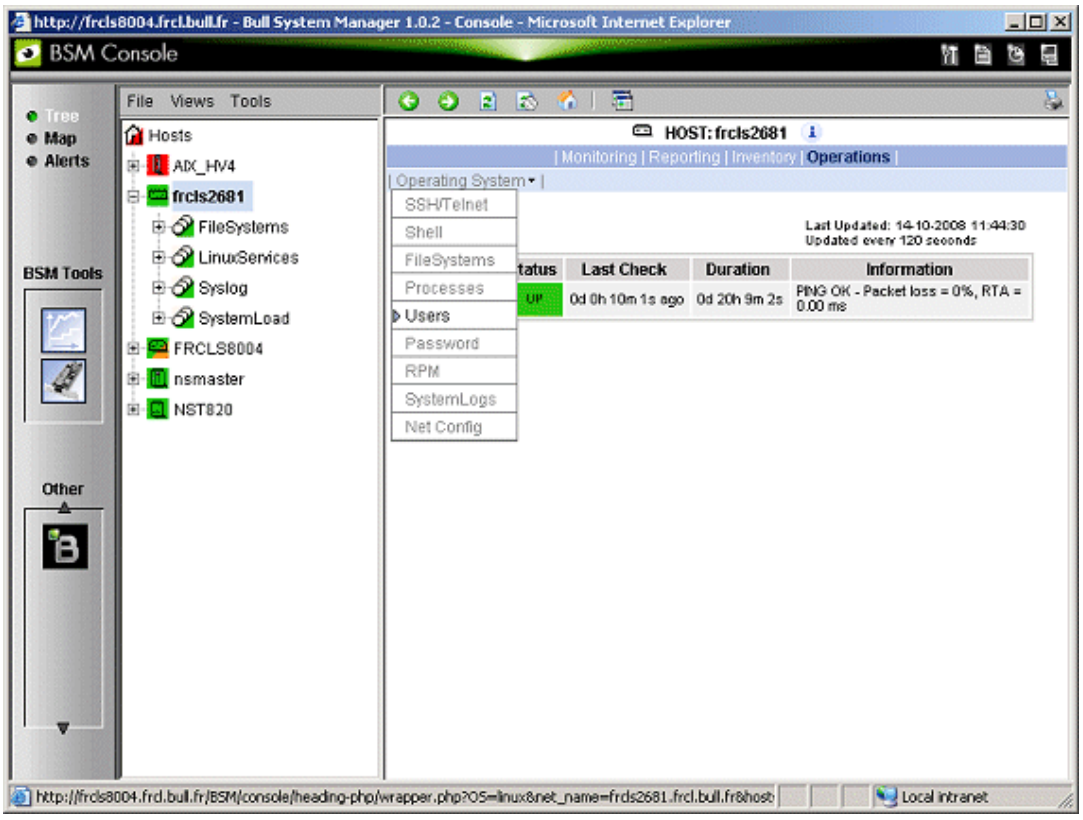


Figure 2-15 Launching Webmin window

A **Webmin** page opens and prompts you for a **Username / Password**. As Administrator, with the corresponding Linux password, you can connect as root.

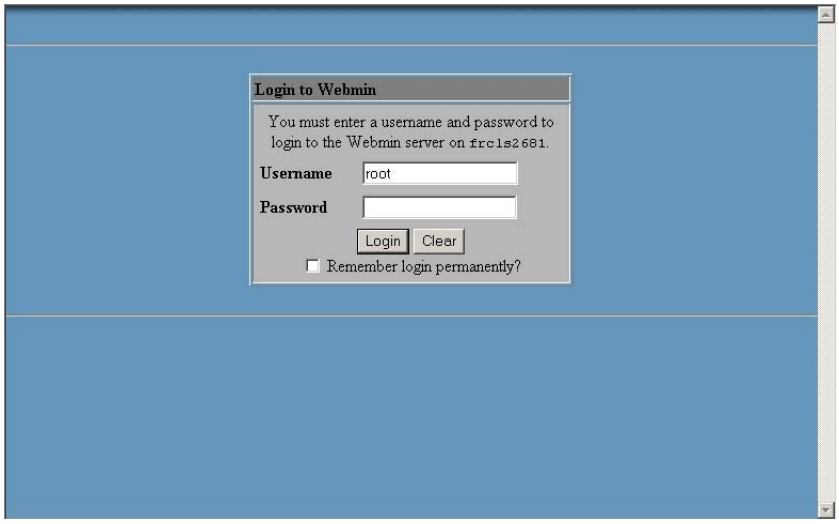


Figure 2-16 Webmin login window

Note If the Linux host is running in **SSL** mode the following message appears, before the Webmin login page is loaded:
`This web server is running in SSL mode. Try the URL https://<hostname>:10000/ instead.`
You must click the link indicated in this message.

You are now in the **Webmin** page that manages **Users** and **Groups**.

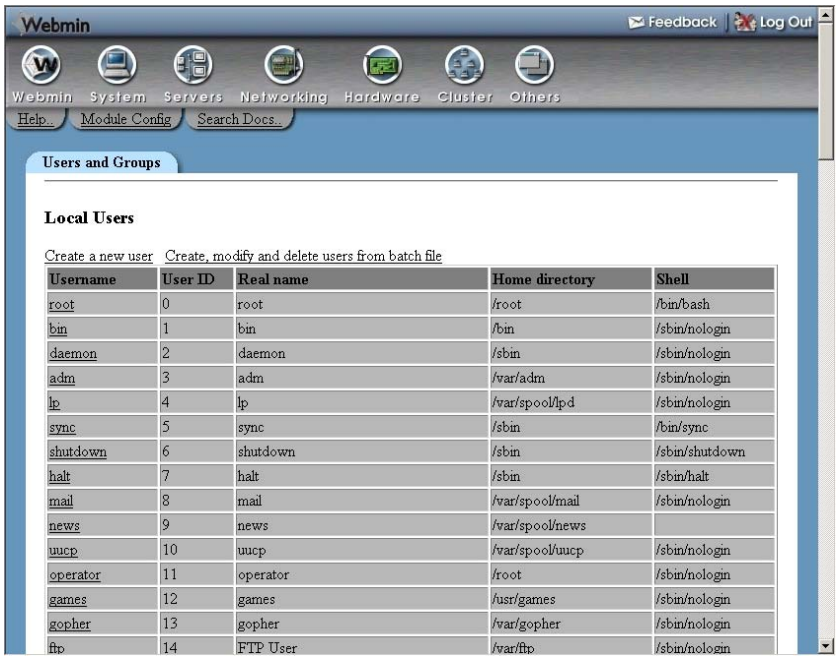


Figure 2-17 Webmin interface on Linux hosts

2. Add a new user by clicking **Create a new user**.

2.6 Managing Hardware

2.6.1 Using the System Native Hardware Manager

Hardware monitoring and management - such as temperature or voltage monitoring, remote power control, access to BIOS or system logs - is not directly performed from Bull System Manager.

Each type of server has a dedicated hardware manager that Bull System Manager uses to perform these operations. Bull System Manager provides the appropriate menu item for each server type, as follows:

- PAM for NovaScale 5000 and 6000 series
- ISM for NovaScale 4000 series
- CMM for NovaScale Blade series
- HMC for Escala servers,
- ExpressScope for NovaScale R400 or T800 series
- RMC or ARMC for Express5800 Series
- Any other manager that can be accessed via a URL.

Notes

- The corresponding Hardware Manager MUST be installed and configured. Please refer to the documentation delivered with the server for details.
- When the Hardware Manager is launched via a URL (Web GUI), the browser on the console must be configured to access this URL without using an HTTP proxy.
- Connection to PAM, ISM, RMC, ExpressScope, CMM and HMC hardware managers **requires authentication.**
  Logins must be defined in the management modules before they can be used by Bull System Manager.
  CMM: only one session is allowed per user. You must therefore register one user for each Bull System Manager Console (used when the Manager GUI is launched from the Management Tree).
- NovaScale **Blade hardware monitoring** is performed through the CMM SNMP interface. You must therefore declare the Bull System Manager server as the SNMP Manager when you configure the CMM.
- Escala monitoring is performed through a remote secure shell. You must therefore configure a non-prompted SSH connection between BSM and the HMC.

To manage hardware, proceed as follows:

Step 1: Declare a HW manager and the hosts, or platforms, it manages.

Step 2: Reload the monitoring server so that the modifications are taken into account.

Step 3: Call the HW Manager from the Tree Window.

Example: Calling a configured PAM Manager

The **Operations > Platform > Hardware Manager GUI** item is opened from the `nsmaster` host menus.

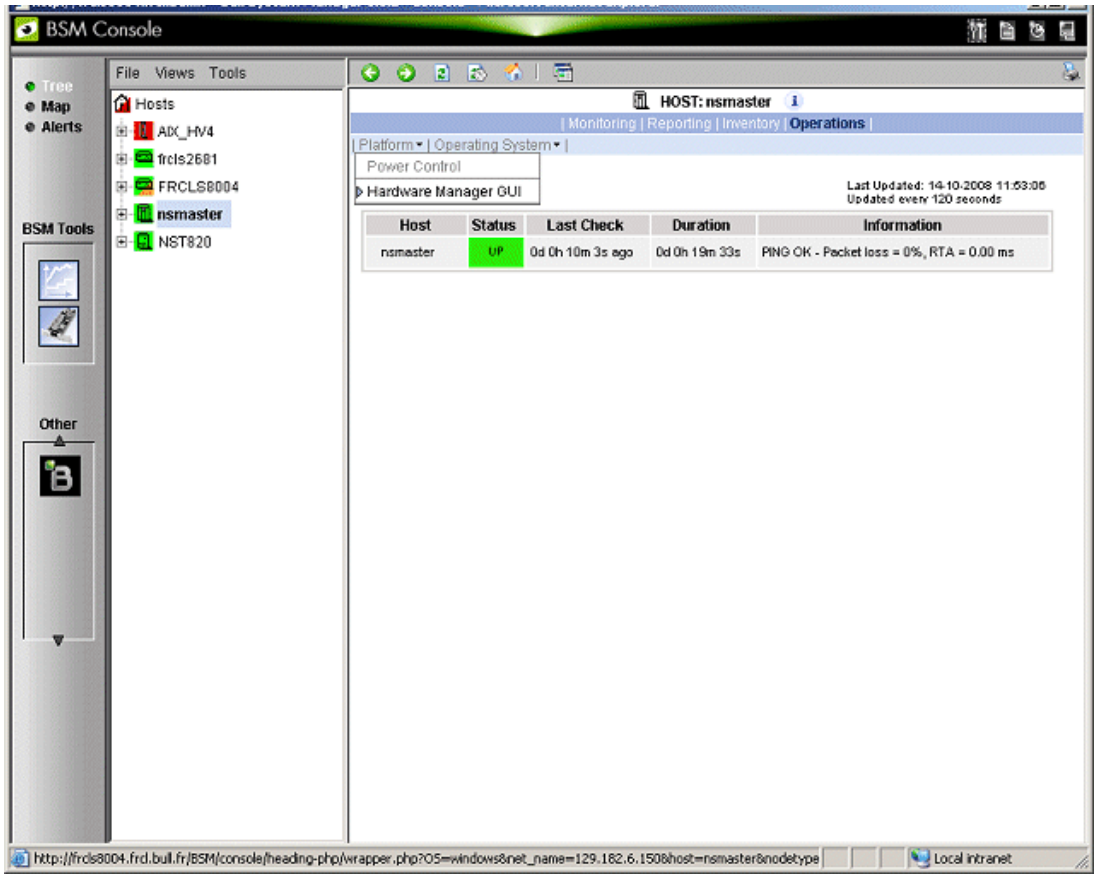


Figure 2-18 HW Manager GUI menu

Starting the **Hardware Manager GUI** menu item calls the associated PAM Hardware Manager:

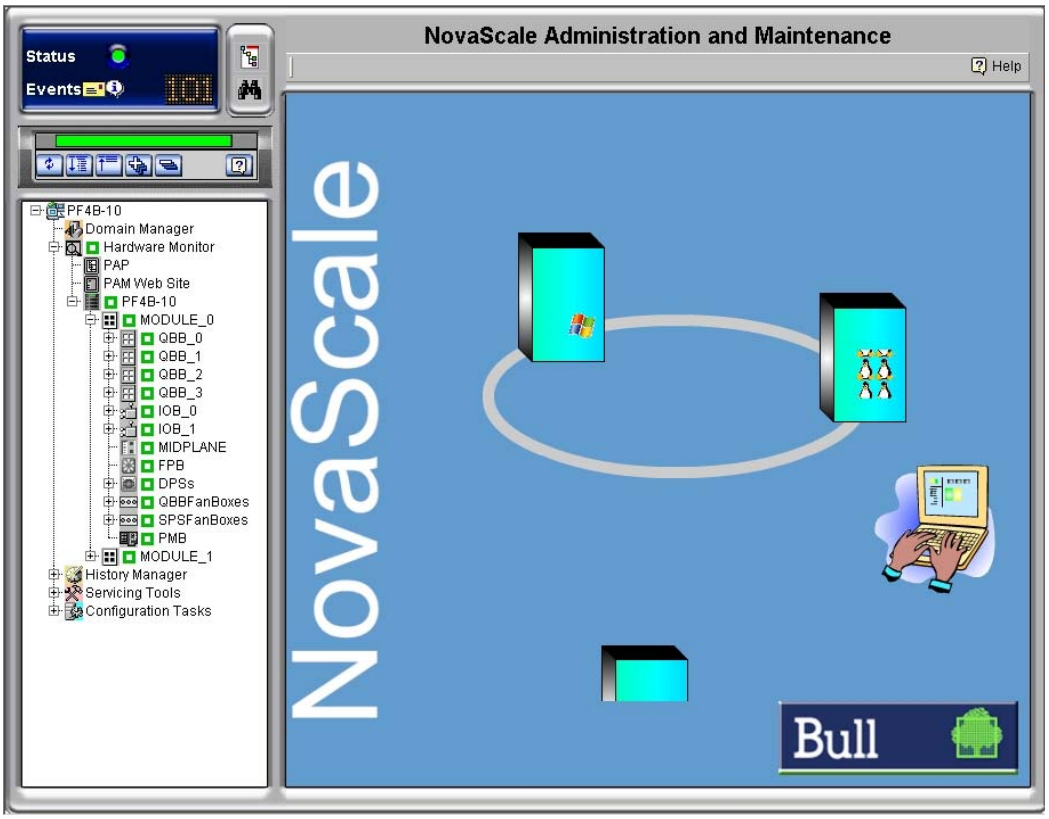


Figure 2-19 PAM Hardware Manager - Home Page

See the *Administrator's Guide* for details.

2.6.2 Using the Bull System Manager Hardware Management Application

Bull System Manager also provides its own Hardware Management application that can be used instead of the native hardware managers (e.g. PAM, CMM, etc.). The Bull System Manager Hardware Management application has the same look and feel for all hardware operations, independently of the target server type.

The application manages the Power Control, and displays FRUs, Sensors and System Event Logs for Express 5800, NovaScale R400 & T800 series and NovaScale 4000, 5000 and 6000 series servers.

To start the application:
From the Console Management Tree, click the **Operations > Platform > Power Control** items in the host menu.

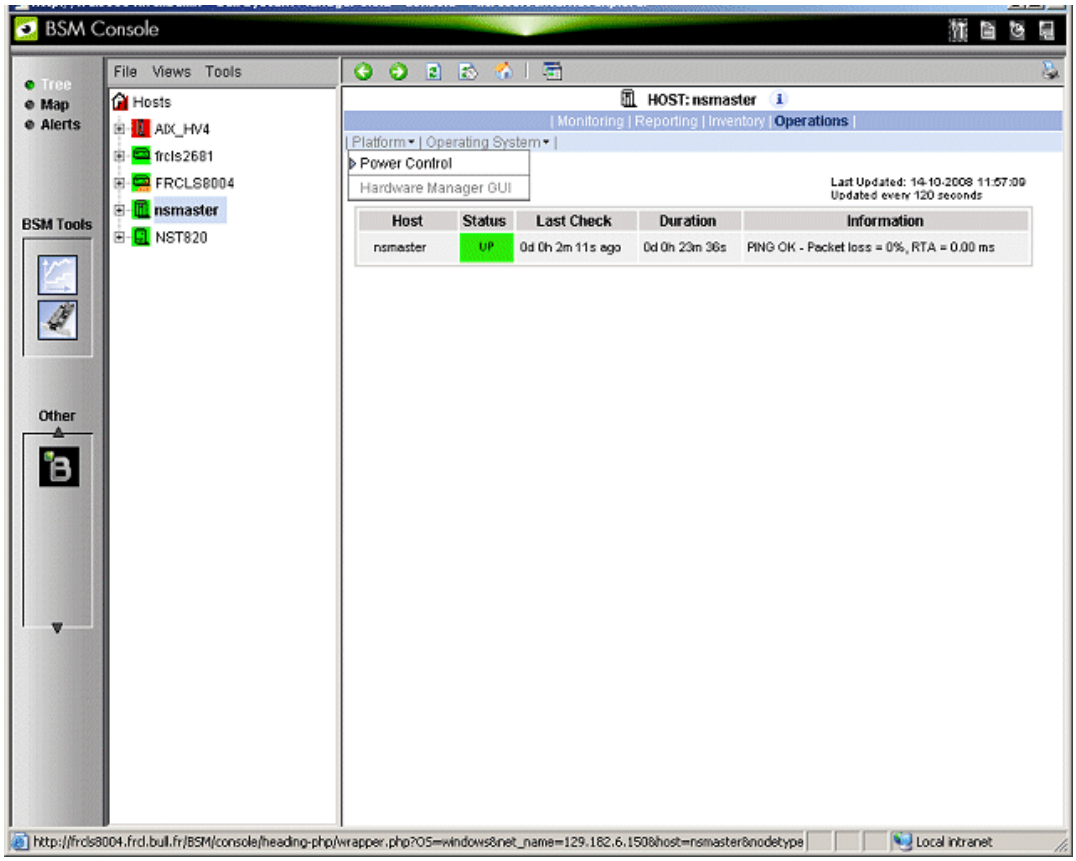


Figure 2-20 Launching the Remote Hardware Management Window

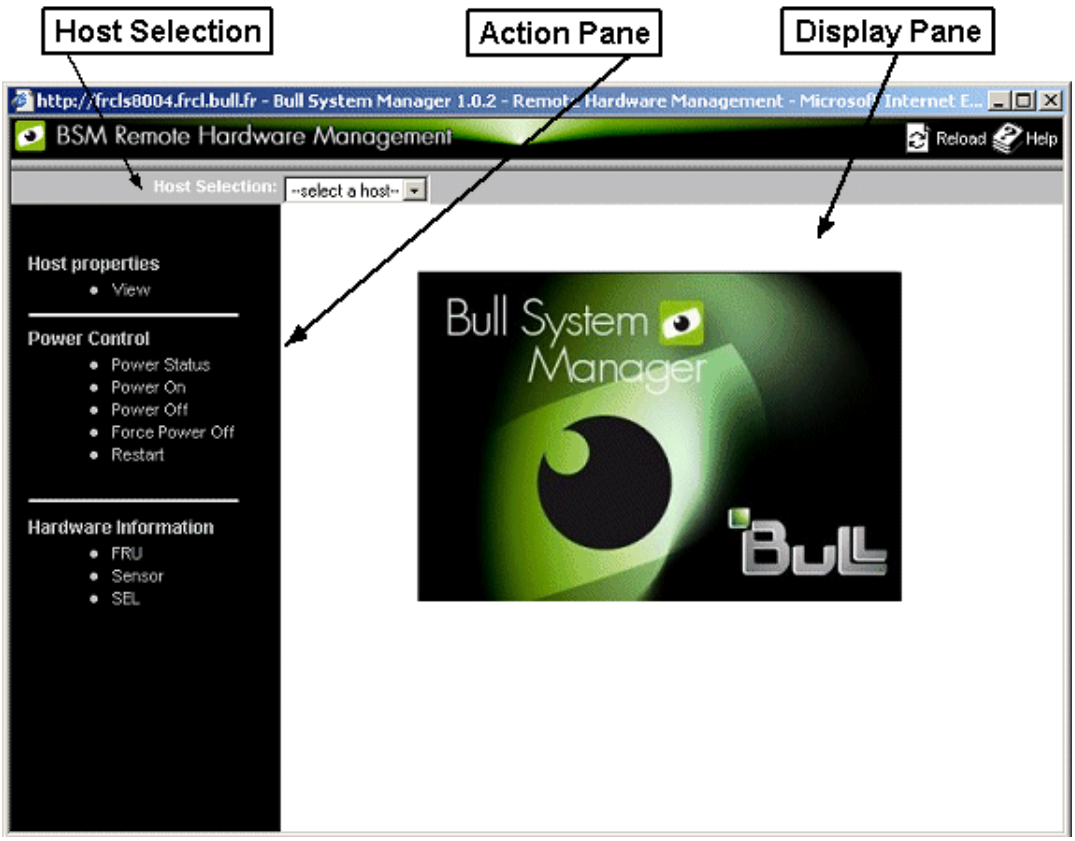


Figure 2-21 Remote Hardware Management window

The Bull System Manager Remote Hardware Management application Window is divided into the following functional parts:

Host Selection Bar Allows you to select a host from the Express 5800, NovaScale R400 or T800 series, and NovaScale 4000, 5000, 6000 or 6009 series servers, Blade servers and Escala servers listed.

Action Sub-Window Displays the hardware operations that can be performed:

- Power control functions
- FRU visualization
- Sensor visualization
- Event log visualization

Display Sub-Window Displays parameter forms, messages and command results.

2.7 Tracking a Performance Indicator over a Long Period

It may be useful to follow the evolution of certain performance indicators over a long period (e.g. the evolution of the memory use).

Performance indicators can be collected from Bull System Manager monitoring data or the SNMP protocol, as described below.

To collect and visualize performance indicator reports, proceed as follows:

1. Launch the Bull System Manager Console from the Bull System Manager Home Page.
2. Click the **Reports** icon to display the list of all the reports that are available.
3. Select the report you want to display from the indicators list.

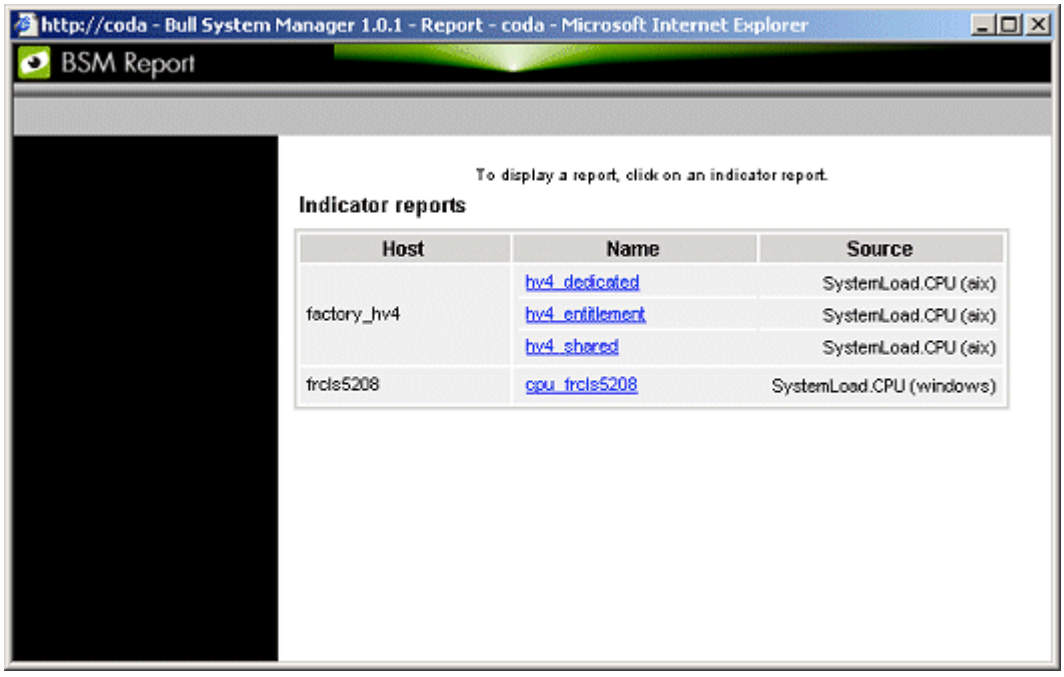


Figure 2-22 Bull System Manager Reporting Indicators Home Page

The following Window appears:

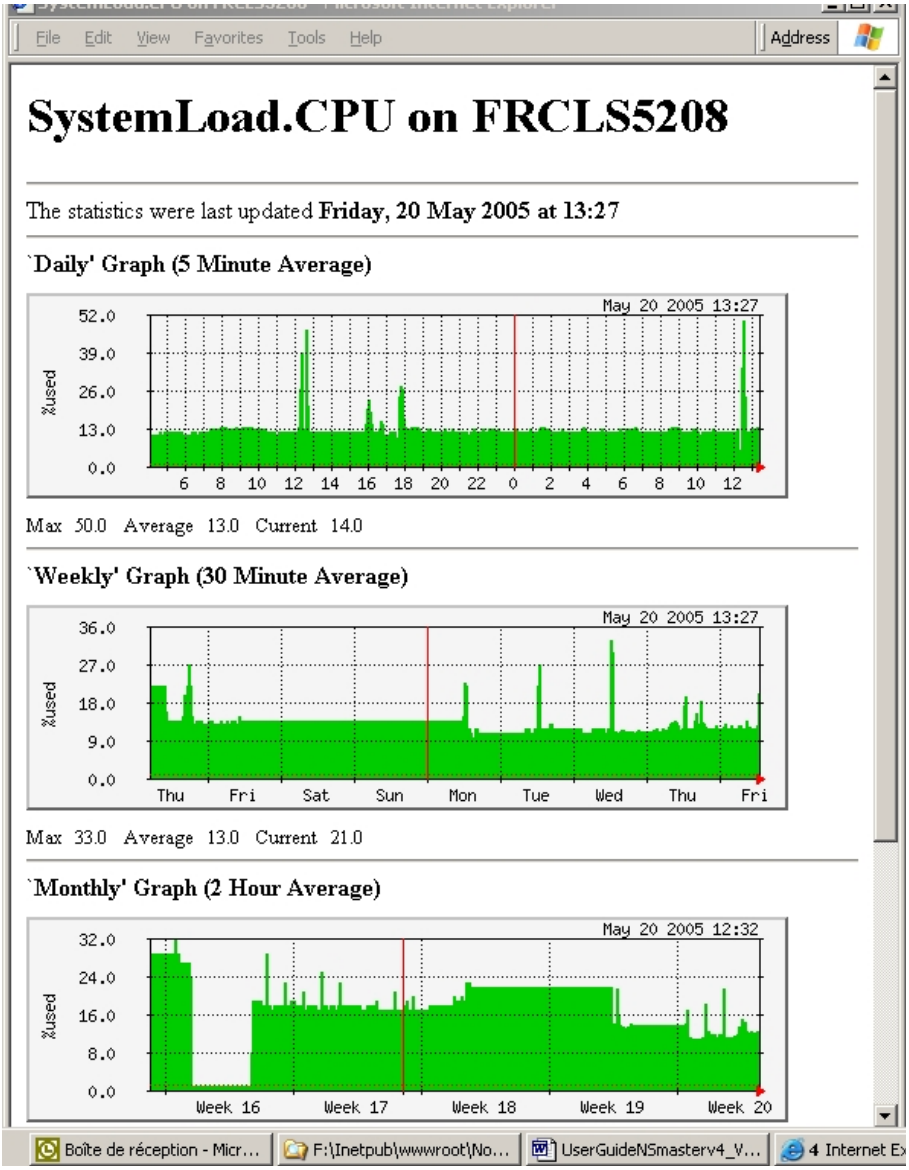


Figure 2-23 Bull System Manager Reporting Indicators - example

This display shows four graphs (three are visible in the example). Each graph shows the evolution of an indicator (CPU load in the example above) for different periods (daily, weekly, monthly and yearly).

2.8 Configuring Bull System Manager

Please refer to the *Administrator's Guide*, 86 A2 56FA, for details about configuration tasks.

2.9 Bull System Manager Server Control

The **Bull System Manager Server Control** application can be launched by clicking on the **control** icon in the Console **Administration Tools** toolbar.

Figure 2-24 Bull System Manager Server Control

The **Bull System Manager Server Control** application allows you to start, stop or restart BSM Server, as required.

When the BSM Server Control application is launched, the status of the server is displayed, as shown in the figure below:

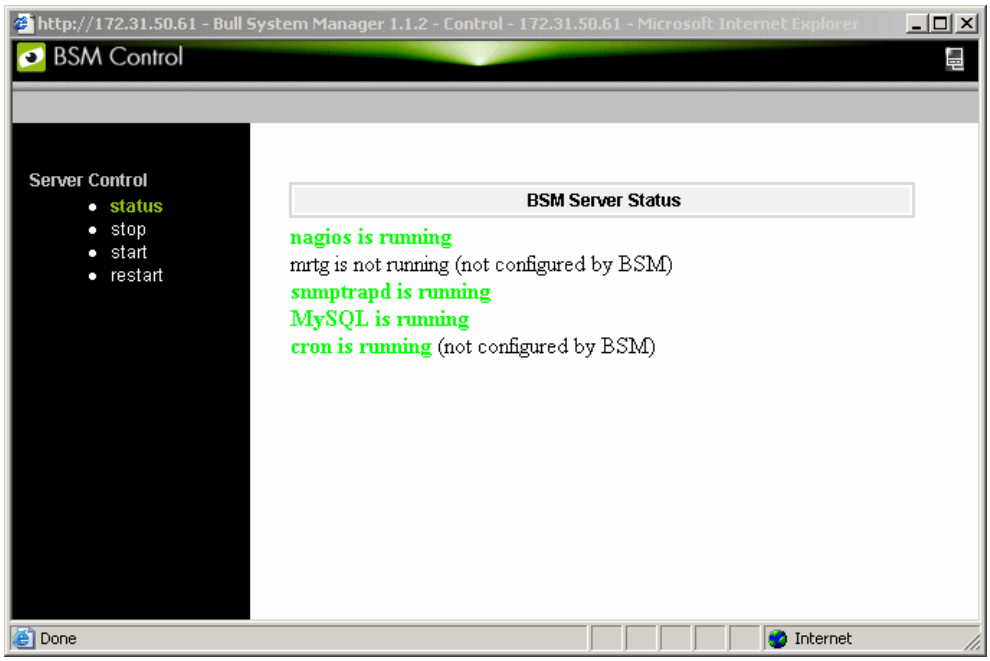


Figure 2-25 Bull System Manager Server Status

Chapter 3. Using Bull System Manager Console Supervision Modes

The Bull System Manager console provides three supervision modes, each providing its own representation of the resource monitored by Bull System Manager:

- Tree mode
- Map mode
- Alerts mode

Whatever the mode, the characteristics of the monitored resource selected are automatically displayed in the Supervision Window.

Note For more information about Console Basics and Console Security Access, refer to the sections on *Console Basics* and *Bull System Manager Authentication and Roles*.

3.1 Working in the Tree Mode

When you select the **Tree** radio button, a Management Tree is displayed in the Supervision Window.

3.1.1 Management Tree Basics

The Management Tree is a hierarchical representation of the resources defined in the Bull System Manager configuration. Each resource displayed in the tree is represented by a node that may have subnodes.

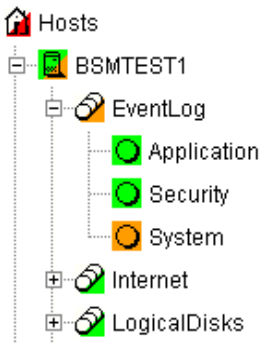


Figure 3-1 Management Tree

- Double-click a node or click the **+/-** expand/collapse icon to display subnodes.
- Select a node to display its characteristics in the Supervision Window.
- Right-click to display the specific node menu.

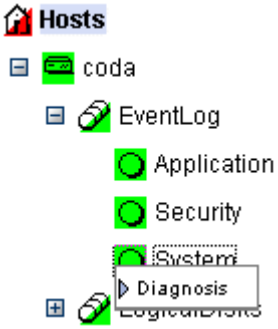


Figure 3-2 A service node menu

Above the Management Tree, a menu provides the Select View, Hide Tree, Refresh and Search commands:

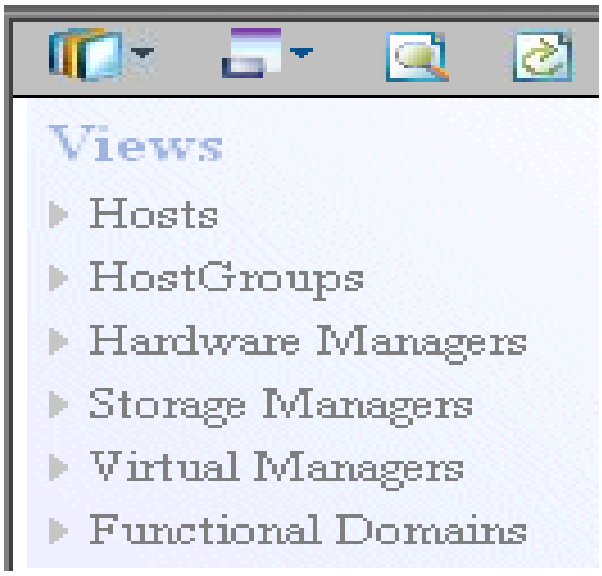


Figure 3-3 Management Tree menu

Management Tree Menu	
Select View	Selects a view to be loaded
Filter Select	Selects a Functional domain filter
Hide Tree	Hides the tree to display the whole Supervision Window
Refresh	Reloads the current view if the configuration has been modified.
Search	Allows you to search a node in its current view, according to its name, or part of its name.

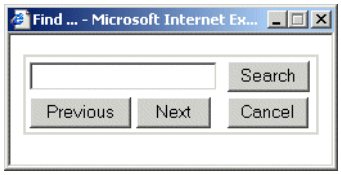


Figure 3-4 Management Tree commands

3.1.2 Management Tree Status Colors

The Management Tree is displays status information according to the following rules:

- The color coding is dependent on status:

Red	CRITICAL
Orange	WARNING
Magenta	UNKNOWN
Green	OK
Blank	UNMONITORED

  This color scheme is applicable to **hosts** and **services**.
- When a node has subnodes, the node icon is split in two. The top left triangle is colored to represent the node status and the bottom right triangle represents the subnode status (i.e. the node in the worst state).
- Host and associated monitoring services node icons are colored according to their status. All other node icons are colored according to the status of their subnodes (i.e. the node in the worst state).

Example:

SYSMAN (root node) and associated services are self-monitoring. The top left triangle is GREEN, showing that host status is OK (the **ping** operation is successful), but the bottom right triangle is RED, showing that **at least one service status is CRITICAL**.

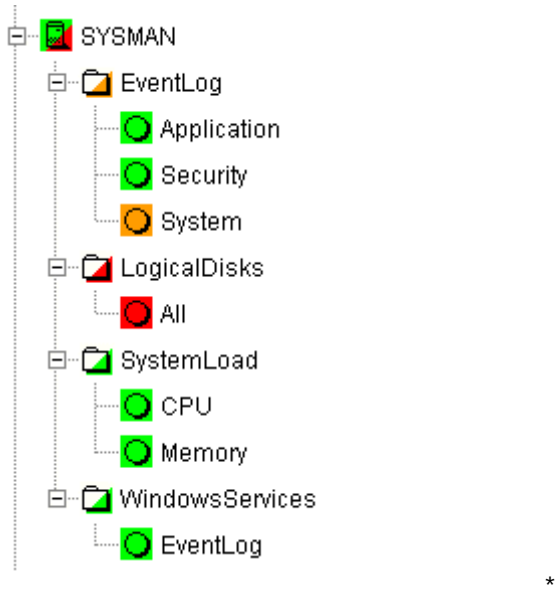


Figure 3-5 Management Tree animation - example

Right-click the colored node icon to display the **Diagnosis** and **On/Off** menus:

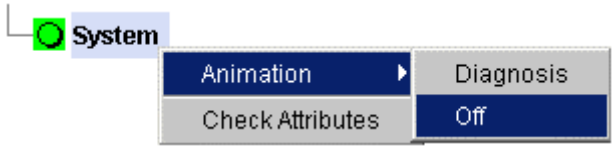


Figure 3-6 Node icon menu

Diagnosis	Displays the animation information Window
On	Activates node animation
Off	Deactivates node animation. This option is useful if you decide not to animate a specific service or host.

Example:

Animation of the **System** and **All** services nodes has been deactivated. As these nodes are no longer monitored, the status is not propagated (icons are BLANK) and SYSMAN (root node) status is now OK.

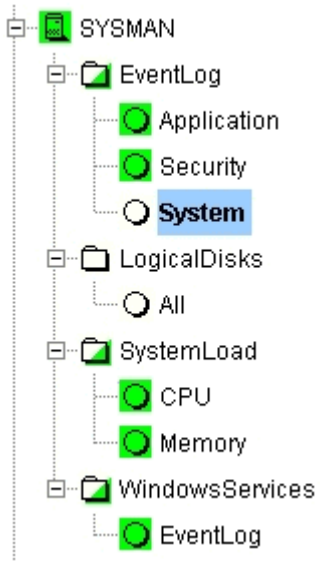


Figure 3-7 Deactivating supervision - example

Note Monitoring services are independent due to the server polling mechanism. This may create a temporary de-synchronization during an animation refresh.

3.1.3 Management Tree Nodes

Each Bull System Manager monitored resource is represented as a node with a specific icon in the dynamically colored Management Tree. Management Tree nodes are colored according to node status. When a node is selected, its characteristics are displayed automatically in the Supervision Window.

Monitored Resource	Icon	Description
Root Node		First node in the tree
Platform		A platform is a physical group of hosts of the same type.
Hardware Manager		Several hardware managers can be displayed: • PAM Manager for NovaScale 5000 and 6000 Series Platforms. • CMM Manager for NovaScale Blade Series Chassis. • ISM Manager for NovaScale 4000 series Platforms. • ESMPRO Manager for Express 5800 hosts. • RMC manager for Express 5800 hosts. • Any other hardware manager.
Storage Manager		Two storage managers can be displayed: S@N.IT! Manager for shared host storage via a SAN. Any other storage manager.
Virtual Manager		A Virtual Manager is composed of Virtual Platform.
Host	ia64 ia32 other	A host is composed of categories.
Category		A category contains specific monitoring services. For example, the SystemLoad category contains the CPU service and the Memory service.
Service		Each service belongs to a category.
ServiceGroup		Services can be organized into functional domain. For example the servicegroup for the Network domain (automatically generarted).

Table 3-1. Management Tree nodes

Note Currently, NovaScale 64 bits is applicable to NovaScale 4xxx, 5xxx and 6xxx servers and NovaScale 32 bits is applicable to NovaScale 2xxx and Express 5800 servers.

3.1.3.1 Root Node

The Root node is the first node in the tree. The top left triangle reflecting self-status is always blank (unmonitored). The bottom right triangle reflects the status for the subnode in the worst state (host and services).

Root node menu	
Expand	Shows a tree view of all hosts, hostgroups or managers in the configuration.
Animation	Indicates resource status.

Table 3-2. Root node menu

3.1.3.2 Hardware Manager Node and Status Levels

A Hardware Manager node represents one of the hardware managers listed in Table 3-5.

PAM and CMM Managers Status Levels

The top left triangle reflects self-status and the bottom right triangle reflects the worst subnode status (hosts and services), as shown in the following table:

Manager (PAM, CMM) Status Levels	
Status	Description
PENDING (gray)	The service has not been checked yet. Pending status occurs only when **nagios** is started. Status changes as soon as services are checked.
OK (green)	The manager is up and running.
WARNING (orange)	The manager has a problem, but is still partially up and running.
UNKNOWN (magenta)	An internal plug-in error has prevented status checking. An unknown status is considered as a warning status.
CRITICAL (red)	The manager has a serious problem or is completely unavailable.

Table 3-3. PAM and CMM status levels

RMC Manager Status Levels

The top left triangle reflects the power status and the bottom right triangle reflects the status for the subnode in the worst state (**hosts** and **services**), as shown in the following table:

Manager (RMC) Status Levels	
Status	**Description**
PENDING (gray)	The service has not been checked yet. Pending status occurs only when nagios is started. Status changes as soon as services are checked.
OK (green)	The power status is on.
UNKNOWN (magenta)	An internal plug-in error has prevented status checking. An unknown status is considered as a warning status.
CRITICAL (red)	The power status is off.

Table 3-4. RMC status levels

ISM and ESMPRO Managers Status Levels

The top left triangle reflecting self-status is always blank (unmonitored). The bottom right triangle reflects the status for the subnode in the worst state (**hosts** and **services**).

Hardware Manager node menu	
Expand -> PAM manager	Shows all NovaScale 5000 and 6000 Series platforms managed by this PAM manager.
-> CMM manager	Shows all NovaScale Blade Series Chassis managed by this CMM manager.
-> other managers	Shows all hosts managed by these managers.
Animation	Briefly explains resource status.

Table 3-5. Hardware Manager node menu

3.1.3.3 Storage Manager Node

The Storage Manager node represents either the S@N.IT! Manager or any other storage manager.

The top left triangle reflecting self-status is always blank (unmonitored). The bottom right triangle reflects the status for the subnode in the worst state (hosts).

Expand	Shows all hosts managed by this manager.
Animation	Briefly explains resource status.

Table 3-6. Storage Manager node menu

Note The S@NIT Web GUI is based on java applet technology. So, do not close the first browser Window launched, as this contains the java applet.

3.1.3.4 Virtual Manager Node

The Virtual Manager node represents the interface used to manage the virtual elements. The Virtual Manager administrates the Virtual Platform, which includes both the native host and the VM hosts.
The top left triangle reflecting self-status is always blank (unmonitored). The bottom right triangle reflects the status for the subnode in the worst state.

Virtual Manager node menu	
Expand	Shows all virtual Platforms managed by this manager.
Animation	Briefly explains resource status.

Table 3-7. Virtual Manager node menu

3.1.3.5 Platform Node and Hostgroup Node

A Hostgroup node represents a group of hosts. A platform node is a specific hostgroup node, which represents a group of hosts of the same type.

The top left triangle reflecting self-status is always blank (unmonitored). The bottom right triangle reflects the status for the subnode in the worst state (hosts and services).

Platform node and Hostgroup node menu	
Expand	Shows the hosts included in the hostgroup or platform.
Animation	Briefly explains resource status.

Table 3-8. Platform node and Hostgroup node menus

3.1.3.6 Host Node and Status Levels

A Host node represents a single host. The top left triangle reflects self-status and the bottom right triangle reflects the status for the subnode in the worst state (services).

Host Status Levels	
Status	Description
PENDING (gray)	Host status is unknown because no associated service has been checked yet. Pending status occurs only when NetSaint is started. Status changes as soon as an associated service is checked.
UP (green)	The host is up and running.
DOWN (red)	The host is down or unreachable.

Table 3-9 Host status levels

		Host node menu
Expand		Shows all monitoring categories associated with this host.
Animation	**-> Diagnosis**	Briefly explains resource status.
	->On / Off	Activates / deactivates node animation.

Table 3-10 Host node menu

3.1.3.7 Category Node

A Category node contains specific monitoring services.

The top left triangle reflecting self-status is always blank (unmonitored). The bottom right triangle reflects the status for the subnode in the worst state (services).

Category node	
Expand	Shows all monitoring services belonging to this category.
Animation	Briefly explains resource status.

Table 3-11. Category node menu

3.1.3.8 Services Node and Status Levels

A Services node is a leaf node.

The service node reflects the service status computed by the monitoring process, as shown in the following table:

Service Status Levels	
Status	**Description**
PENDING (gray)	The service has not been checked yet. Pending status occurs only after NetSaint is started. Status changes as soon as services are checked.
OK (green)	The monitored service is up and running.
WARNING (orange)	The monitored service has a problem, but it is still partially up and running.
UNKNOWN (magenta)	An unreachable or internal plug-in error has prevented service status checking. An unknown status is considered as a warning status.
CRITICAL (red)	The service has a serious problem or is completely unavailable.

Table 3-12. Service status levels

Service node menu		
Animation	**-> Diagnosis**	Briefly explains resource status.
	-> On / Off	Activates / deactivates node animation.

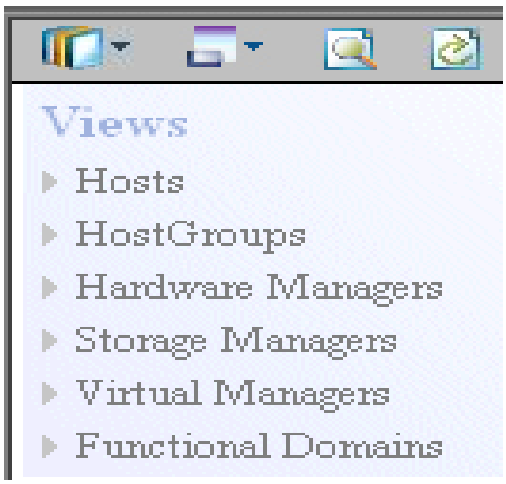
Table 3-13. Service node menu

3.1.4 Management Tree Views

Management Tree views allow you to represent monitored resources according to your needs at a given time. The Management Tree provides five standard views:

- Hosts
- HostGroups
- Hardware Managers
- Storage Managers
- Virtual Managers
- Functional Domains

The default view is the **Hosts** view, but you can load another view by clicking on and selecting the view:



Standard Tree Views	
Hosts View	All hosts are displayed under the root node.
HostGroups View	All hostgroups in the configuration plus all NovaScale 5000 and 6000 Series platforms and NovaScale Blade Chassis are displayed as hostgroup nodes with their associated hosts.
Hardware Managers View	All hardware managers in the configuration are displayed. Each manager node contains the hosts that it manages. For example, the PAM manager nodes contain the NovaScale 5000 and 6000 Series platforms and the CMM manager nodes contain the NovaScale Blade Chassis.
Storage Managers View	All storage managers in the configuration are displayed. Each manager node contains the hosts that it manages.
Virtual Manager View	All virtual managers in the configuration are displayed. Each manager node manages a set of virtual machines, viewed as Virtualization Platform.
Functional Domains	All service groups (functional domains) in the configuration are displayed.

Table 3-14. Tree views

3.1.4.1 Hosts View

The Hosts view is the default view. All the hosts in the configuration are displayed with their monitoring services classified by category (**EventLog**, **LogicalDisks, etc.**), as shown in the following figure.

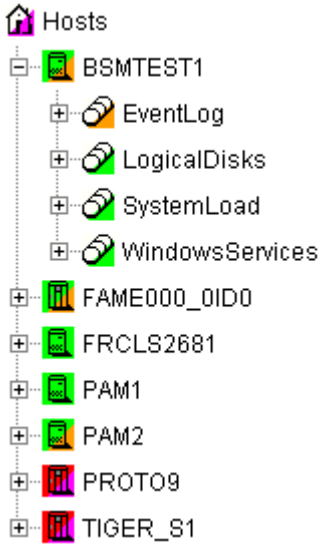


Figure 3-8 Hosts view

3.1.4.2 HostGroups View

The **HostGroups** view displays all the hostgroups in the configuration.

Hosts are displayed under each hostgroup, with their monitoring services classified by category (**EventLog**, **LogicalDisk, etc.**), as shown in the following figure.

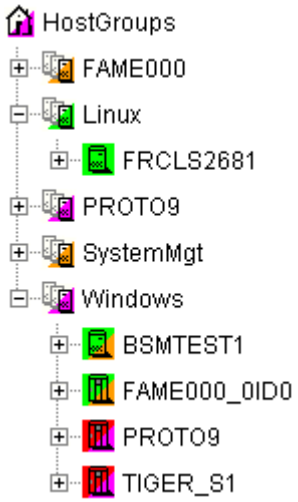


Figure 3-9 HostGroups view

In the example above, the administrator has defined a Windows HostGroups grouping all Windows servers. The bottom right triangle of a HostGroups icon is not green, meaning that a host or a service has a problem. The operator can expand the HostGroups icon to identify the host or service with a problem.

3.1.4.3 Hardware Managers View

The **HWManagers** view displays all the managers in the configuration:

- PAM Managers, displaying NovaScale 5000 and 6000 Series platforms with their hosts (domains)
- CMM Managers displaying NovaScale Blade Chassis with their hosts (NS 20x0)
- RMC, ISM or ESMPRO Managers displaying other hosts.

Hosts are displayed with monitoring services classified by categories supported (**Hardware**, **EventLog**, **LogicalDisk, etc.**), as shown in the following figure:

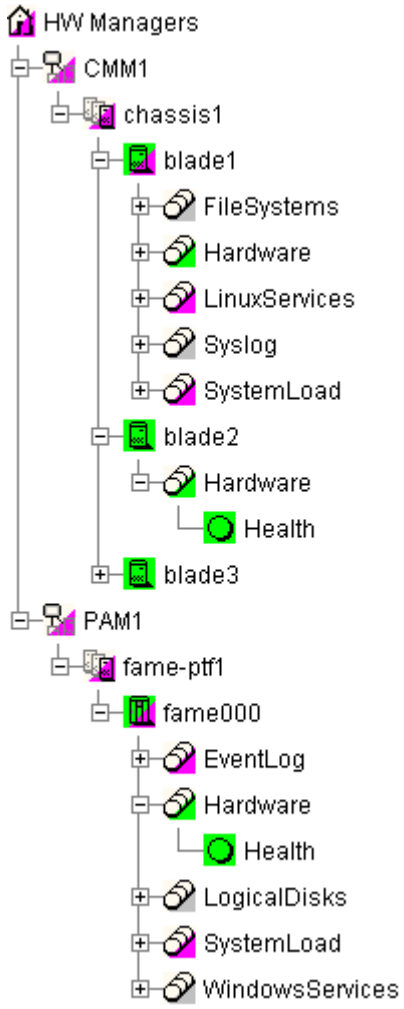


Figure 3-10 HW Managers view

3.1.4.4 Storage Managers View

The **Storage Managers** view displays all the storage managers in the configuration.

Hosts are displayed with monitoring services classified by the categories supported (**Storage**, **EventLog**, **LogicalDisk**, **etc.**), as shown in the following figure:

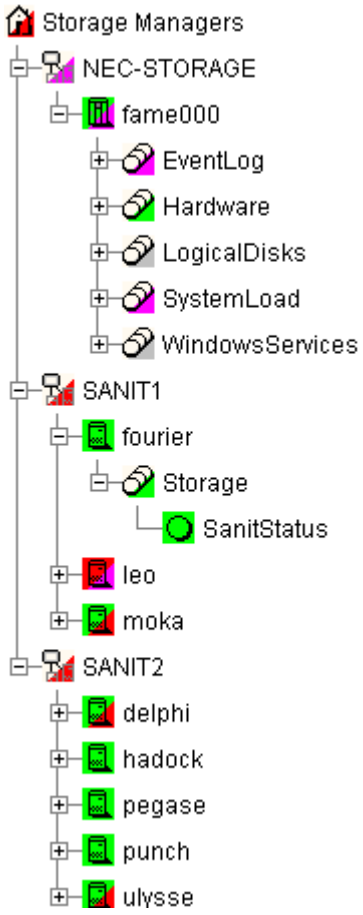
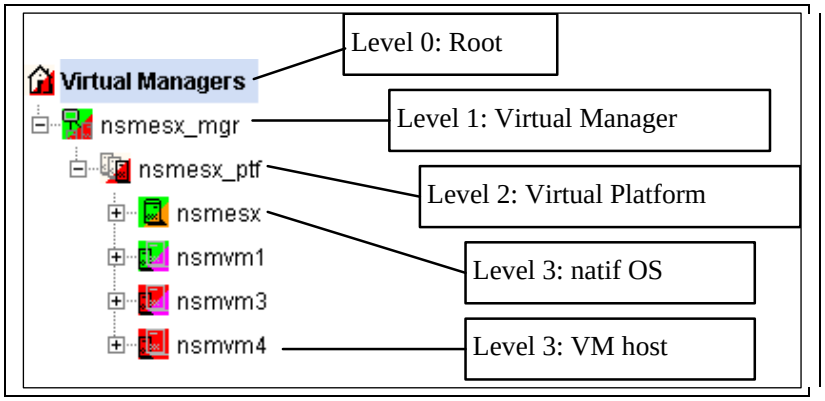


Figure 3-11 Storage Managers view

3.1.4.5 Virtual Managers View

The **Virtual Managers** view displays all the virtual managers in the configuration.

Under the root node, the first node is the Virtual Manager that administrates the Virtual Platform. The Virtual Platform contains the native host and the VM hosts. Hosts are displayed with the monitoring services sorted by supported category.



For details, refer to the *Bull System Manager Server Add-ons Installation and Administrator's Guide*, 86 A2 59FA.

3.1.4.6 Functional Domains View

The **Functional domains** view displays all the service groups in the configuration.

The following picture shows a functional domain view containing three domains (**Network**, **OperatingSystem** and **Storage** for a single host.

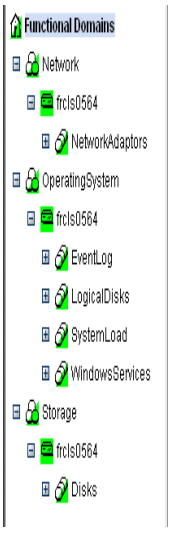


Figure 3-12 Functional Domain view example

3.2 Working in the Map Mode

When you select the Map radio button, the Map and Applicative Windows are displayed.

Note The **Map** and **Applicative** Windows are always synchronized.

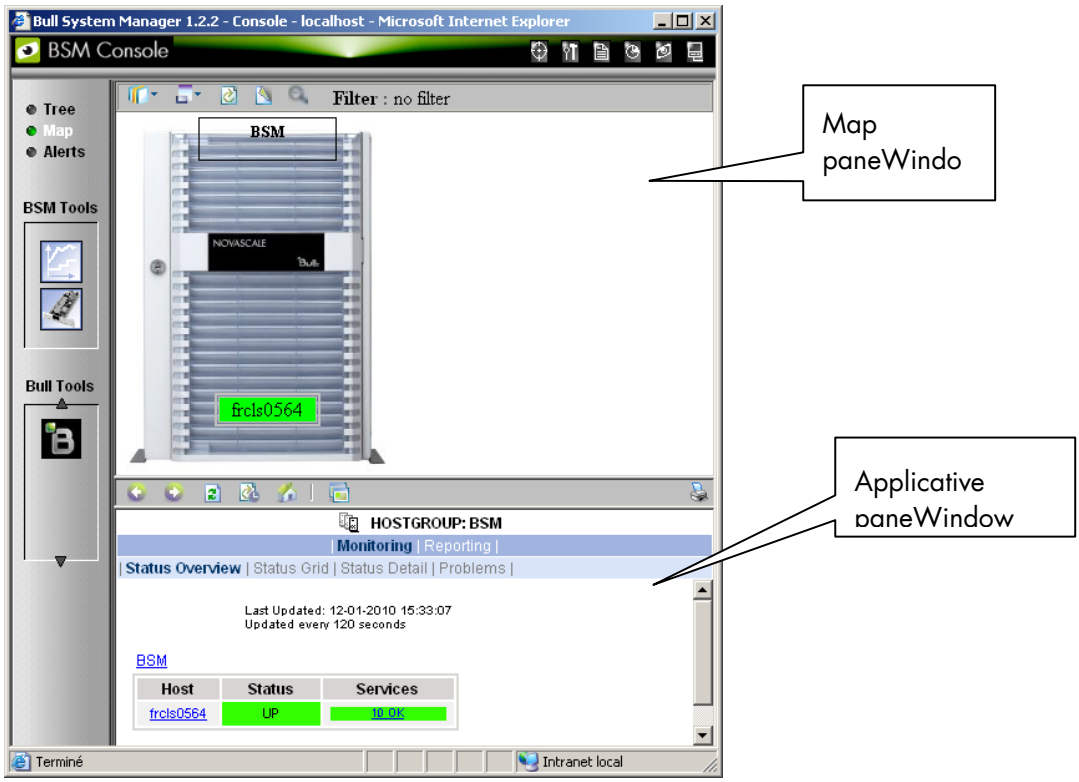


Figure 3-13 Map mode

In the **Map** Window, Hostgroups and Hosts are displayed, and are colour coded according to their status. Their positions (x, y) are specified in the Configuration GUI. The Hostgroup status is determined by the status of their corresponding hosts and monitoring services.

The **Applicative** Window lists all the information and functional menus for any host belonging to the Hostgroups on the map. You can navigate using the hyper-links and return using the **Back** button.

Note A map can contain other maps.

3.3 Working in Alerts Mode

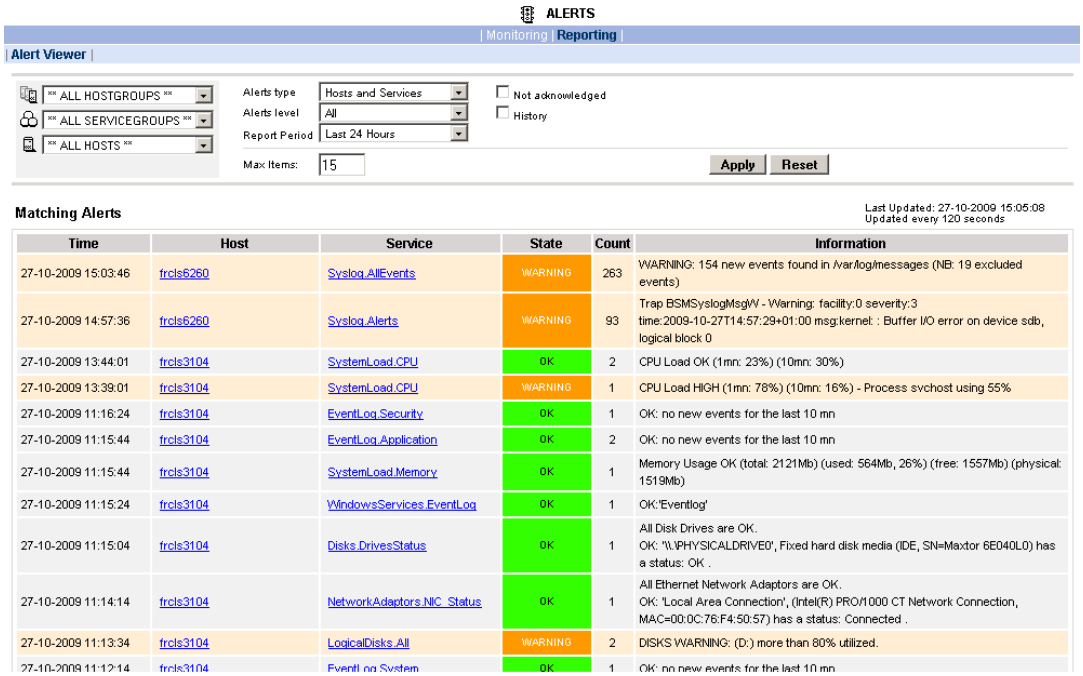
3.3.1 Alert Basics

The **Bull System Manager Alert Viewer** application displays monitoring alerts (also called events) concerning a set of Hostgroups, Hosts and Services.

The application provides filter functions in order to display alerts for all monitored resources or for a subset of these resources only.

Whenever a service or host status change takes place, the monitoring server generates an alert, even when the status passes from CRITICAL to RECOVERY and then to OK. Alerts are stored in the monitoring log in operation and are then archived.

The Bull System Manager Alert Viewer application scans the current monitoring log and archives according to filter report period settings.



Time	Host	Service	State	Count	Information
27-10-2009 15:03:46	frcls6260	Syslog.AllEvents	WARNING	263	WARNING: 154 new events found in /var/log/messages (NB: 19 excluded events)
27-10-2009 14:57:36	frcls6260	Syslog.Alerts	WARNING	93	Trap BSMSyslogMsgW - Warning: facility:0 severity:3 time:2009-10-27T14:57:29+01:00 msg:kernel: : Buffer I/O error on device sdb, logical block 0
27-10-2009 13:44:01	frcls3104	SystemLoad.CPU	OK	2	CPU Load OK (1mn: 23%) (10mn: 30%)
27-10-2009 13:39:01	frcls3104	SystemLoad.CPU	WARNING	1	CPU Load HIGH (1mn: 78%) (10mn: 16%) - Process svchost using 55%
27-10-2009 11:16:24	frcls3104	EventLog.Security	OK	1	OK: no new events for the last 10 mn
27-10-2009 11:15:44	frcls3104	EventLog.Application	OK	2	OK: no new events for the last 10 mn
27-10-2009 11:15:44	frcls3104	SystemLoad.Memory	OK	1	Memory Usage OK (total: 2121Mb) (used: 564Mb, 26%) (free: 1557Mb) (physical: 1519Mb)
27-10-2009 11:15:24	frcls3104	WindowsServices.EventLog	OK	1	OK:'Eventlog'
27-10-2009 11:15:04	frcls3104	Disks.DrivesStatus	OK	1	All Disk Drives are OK. OK: '\\.\PHYSICALDRIVE0', Fixed hard disk media (IDE, SN=Maxtor 6E040L0) has a status: OK .
27-10-2009 11:14:14	frcls3104	NetworkAdaptors.NIC_Status	OK	1	All Ethernet Network Adaptors are OK. OK: 'Local Area Connection', (Intel(R) PRO/1000 CT Network Connection, MAC=00:0C:76:F4:50:57) has a status: Connected .
27-10-2009 11:13:34	frcls3104	LogicalDisks.All	WARNING	2	DISKS WARNING: (D:) more than 80% utilized.
27-10-2009 11:12:14	frcls3104	EventLog.System	OK	1	OK: no new events for the last 10 mn

Figure 3-14 Bull System Manager Alert Viewer

Bull System Manager Alert Viewer is divided into two main functional parts:

- The **Alert Selection** Window, where all filters are taken into account like a logical AND. Exception: when the **Alert** level is set to **Display Current problems only**, the **Time Period** is automatically set to **This Year**, and cannot be modified.
- The **Information** Window, which displays the filtered alerts.

3.3.2 Alert Selection

Note By default, alerts for all Hostgroups, all Servicegroups and all Hosts are displayed.

Figure 3-15 Alert Selection

Selecting Hostgroups, Servicegroups and Hosts

You can filter Hostgroup, Servicegroup and host Alerts from the Selection Window, in any combination:

- When you select a specific **hostgroup**, only the hosts belonging to that hostgroup are selected.
- When you select a specific **servicegroup**, only the hosts belonging to the previously selected servicegroup and hostgroup are selected.
- When you select ****ALL HOSTS****, all the hosts belonging to the previously selected hostgroup and servicegroup are selected.

Example:

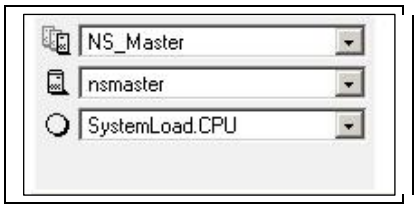


Figure 3-16 Alert selection - example

In this example, the user has decided to select all alerts concerning **SystemLoad.CPU** on the **nsmaster** host in the **NS_Master** hostgroup.

Note When the **servicegroup** filter field of the Alert Viewer is set to **ALL SERVICEGROUPS**, the resulting list will also contain Categories with no defined monitoring domain (= "none" or not set). In fact, the value "ALL * GROUP" means that this filter field is not used for the search. Therefore, the resulting list will contain all items, whether they have a defined monitoring domain or not.

Selecting Alert Type

You can filter alerts according to the following alert types:

- Hosts and Services
- Hosts
- Services

Note By default, **Hosts and Services** is selected.

Selecting Alert Level

You can filter Alerts according to the following alert levels:

- **All**
  Displays all alerts.
- **Major and Minor problems**
  Displays host alerts with DOWN or UNREACHABLE status levels.
  Displays service alerts with WARNING, UNKNOWN or CRITICAL status levels.
- **Major problems**
  Displays host alerts with DOWN or UNREACHABLE status levels.
  Displays service alerts with UNKNOWN or CRITICAL status levels.
- **Current problems**
  Displays alerts with a current non-OK status level.
  When this alert level is selected, the Time Period is automatically set to '**This Year**' and cannot be modified.

Note By default, **All** is selected.

Selecting Acknowledged Alerts

As Administrator, you can acknowledge alerts and decide whether they should be displayed or not.

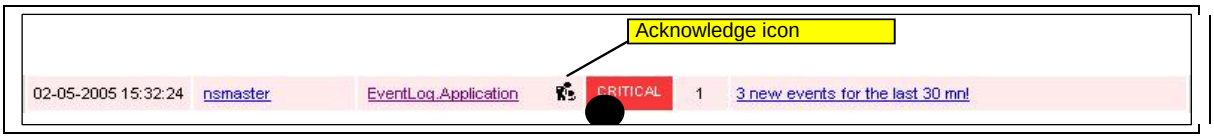


Figure 3-17 Acknowledged alerts selection

Note By default, **All** alerts is selected (acknowledged or not).

Selecting Alert History

By default, all the alerts concerning a particular service of a particular host with a given status level are displayed in a single line:

- The **Count** field lists the number of similar alerts over the specified Report Period.
- The **Time** field displays the time when the most recent alert was generated.
- The **Information** field details the most recent alert.

When you select this option, each alert is displayed in a different line:

- The **Time** field displays the time when the alert occurred.

Selecting Time Periods

The user can specify the period for which alerts are displayed:

- Last 24 Hours
- Today
- Yesterday
- This Week
- Last 7 Days
- Last Week
- This Month
- Last Month
- This Year
- Last Year
- *CUSTOM PERIOD*

When you select *CUSTOM PERIOD*, you can specify time period start and end dates. The default *CUSTOM PERIOD* setting is the beginning of the current month up to the current date.

Note By default, alerts over the **Last 7 Days** are displayed.

Selecting Max Items

This option allows you to specify the maximum number of lines displayed.

Note By default, the **Max Items** setting is 15.

3.3.3 Alert Information

Alerts provide the following information:

- **Time** when the alert occurred
- **Host Name** where the alert occurred
- **Service Name** where the alert occurred
- **Status Level**
- **Count**
- **Information**

Note The **Count** field is always set to **1** if the **History** option is set to **true**. Otherwise, the **Count** field indicates the number of alerts with the same status level. The **Time** and **Information** fields concern the most recent alert.

3.4 Supervision Information

3.4.1 FOCUS area

From the console menu , you can display a **BSM Focus** Window containing a set of monitoring services that can be surveyed in parallel to the BSM Console use. This list of services is configured via the BSM Configuration web GUI (See the *Administrator's Guide* for more information).

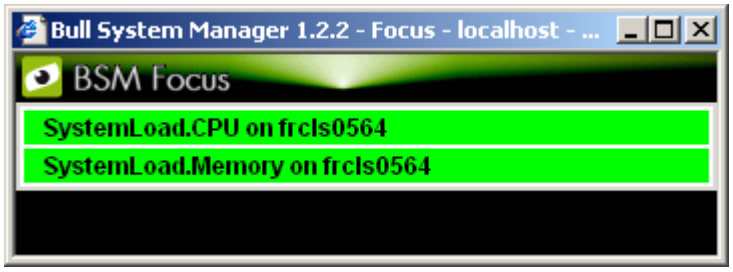


Figure 3-18 BSM Focus windows example

When you click on a service status line, a popup Window appears with more detailed information, as shown in the screen grab below:

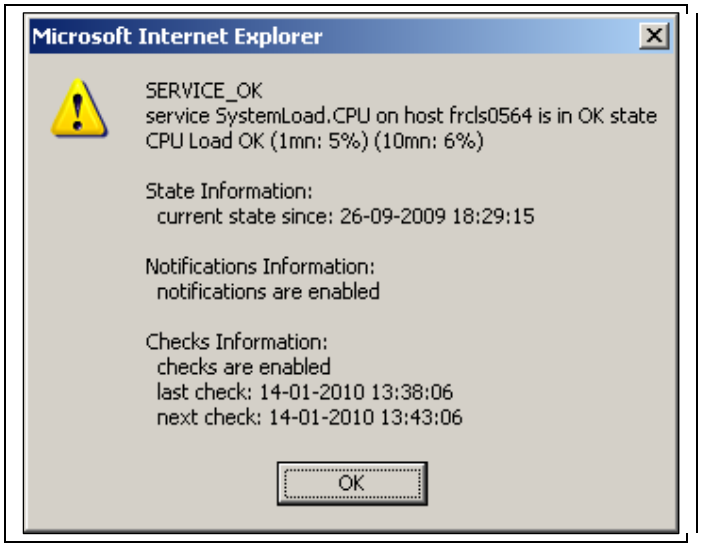


Figure 3-19 Status detailed information from the BSM Focus window.

3.4.2 Supervision Information Basics

The Supervision Window displays information about the resources and works monitored, and functions exactly like a web browser. You can click a link, retrace your steps (back, forward), reload a page, detach a page and print a page. The Supervision Window is divided into five functional parts, as shown in the following figure:

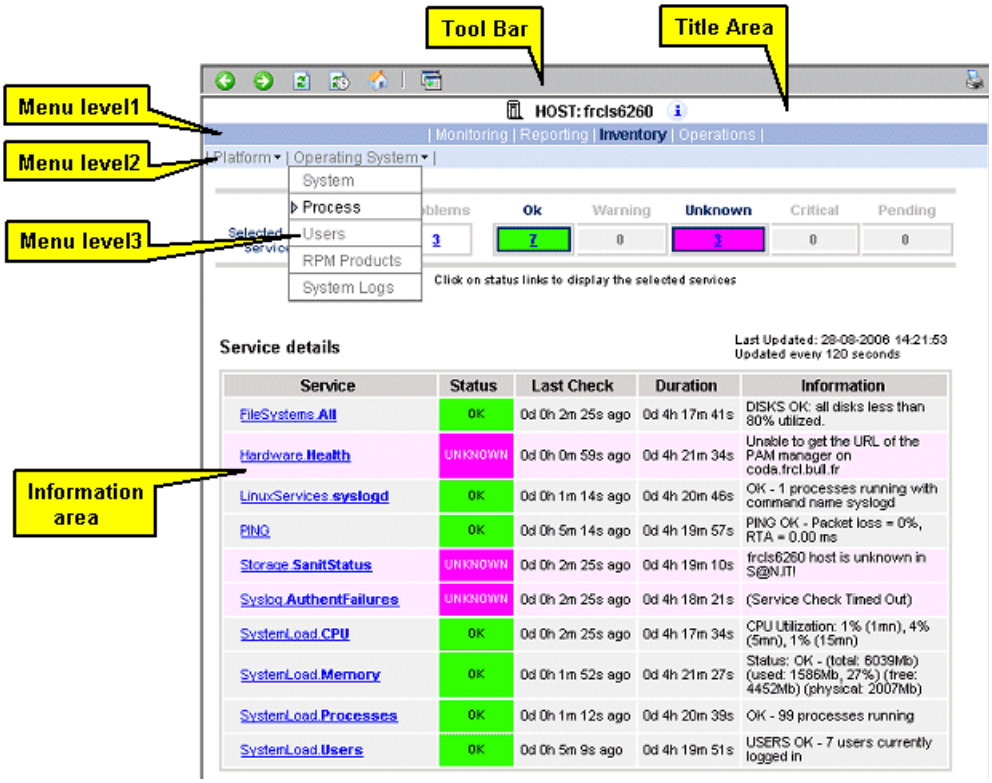


Figure 3-20 Supervision Window

Tool Bar

Go back one page

Go forward one page

Reload the current page

Modify the information Window refresh delay

Reload the first page

Detach the current page and insert it into a separate frame

Title Window

Displays the monitored resource icon selected, type and name.

Only available for hosts. Gives a short description of the selected host (name, model, OS, netname and domain).

Menu Level1

Allows you to select the type of functional domain you want to access, according to the resource selected: Monitoring, Reporting, Inventory, Operations.

Menu Level2 Allows you to select the information or operation you want to access, according to Level1 information selected.

Menu Level3 Allows you to select the information or operation you want to access, according to Level2 information selected.

Information Window Displays selected information about the selected resource.

3.4.3 Monitoring Information

The table below lists the information types available and the associated supervision scope.

Information Type	Supervision Scope
Status Overview	Root nodes of Hosts and Hostgroups Views (Tree) Hostgroup
Status GRID	Root nodes of Hosts and Hostgroups Views (Tree) Hostgroup
Status Detail	Root nodes of Hosts and Hostgroups Views (Management Tree) Hostgroup
Host Status	Host
Service Status	Service
Network Outages	Not yet supported
Config	Root nodes of Hosts and Hostgroups Views (Tree)
Log	Root nodes of Hosts and Hostgroups Views (Tree)
Control	Root nodes of Hosts and Hostgroups Views (Tree)

Table 3-15. Monitoring information

3.4.3.1 Status Overview

This screen allows you to view the status of all the monitored hosts and services.

- When you launch this screen from a hostgroup node, a status overview of all hostgroups (or a particular hostgroup) is displayed.

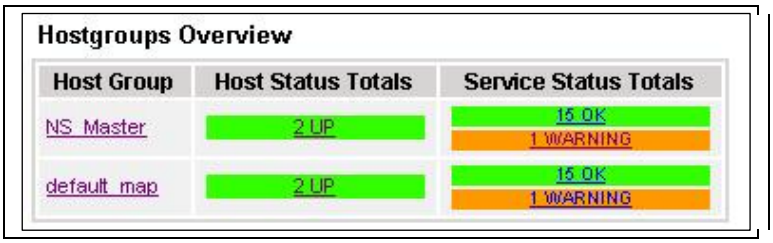


Figure 3-21 Hostgroup Status Overview

Host Group	Hostgroup name
Host Status Totals	Number of hosts classified by status level in the hostgroup
Service Status Totals	Number of services classified by status level in the hostgroup

- When you launch this screen from the Functional Domains node, a status overview of all servicegroups (or a particular servicegroup) is displayed.

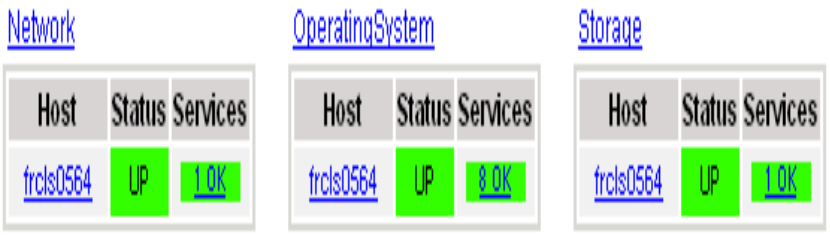


Figure 3-22 Servicegroups Status Overview

Host	Host name
Status	Hosts status level in the servicegroup
Services	Number of services classified by status level in the servicegroup

- When you launch this screen from the host node, a status overview of all hosts is displayed.

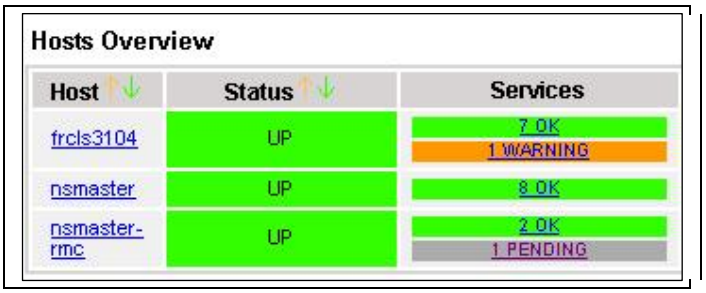


Figure 3-23 Host Status Overview

Host	Host name
Host Status	Host status level
Service Status	Number of services classified by status level

3.4.3.2 Status GRID

This screen displays the name of all the services monitored for each host.

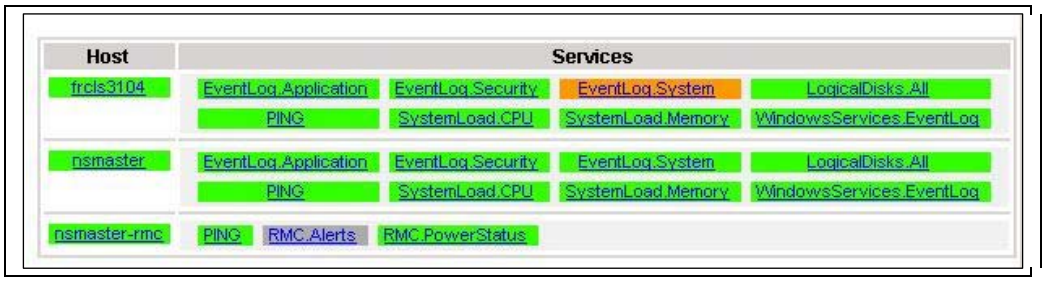
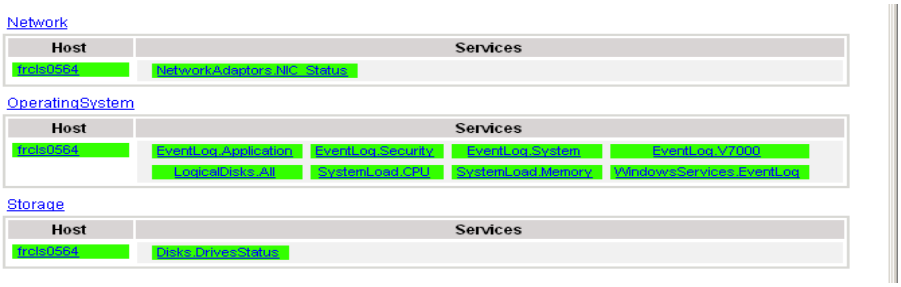


Figure 3-24 Host Status GRID

Host Host name

Service Status Host services colour coded according to status level.

- When you launch this screen from the Functional Domains node, you will obtain a grid overview by functional domain:



3.4.3.3 Status Detail

This screen gives detailed information about the hosts and/or services selected.

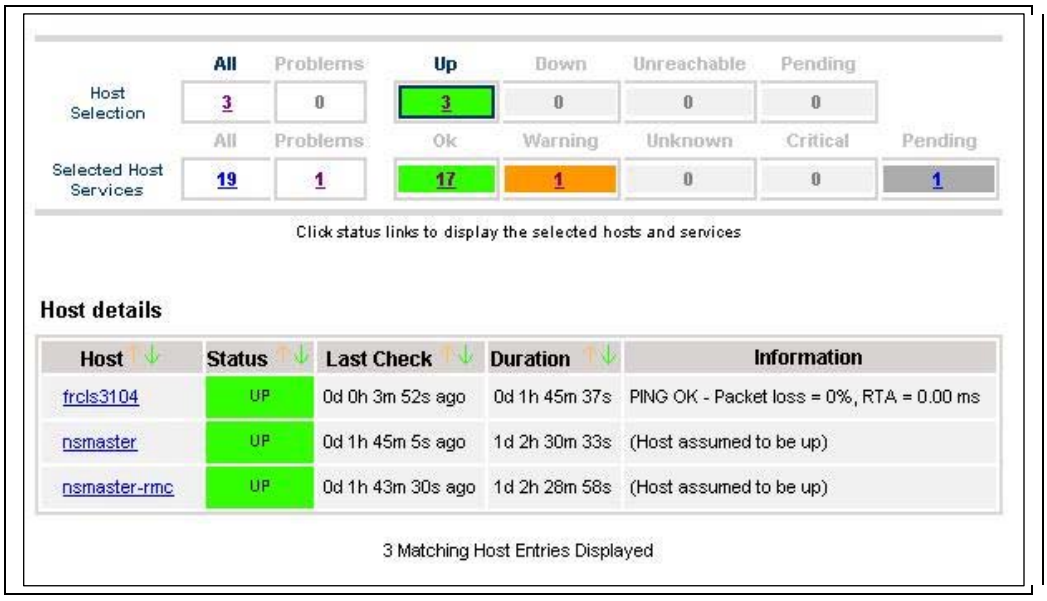


Figure 3-25 Hosts Status Detail

The Selection Window allows you to select the host and service according to status level:

Host Selection Number of hosts with Up, Down, Unreachable or Pending status. You can select hosts according to status: All hosts, Problem hosts, or Specific hosts.

Selected Host Services
Number of services with OK, Warning, Unknown, Critical or Pending status. You can select services according to status: All services, Problem services, or Specific services.

Information Gives host details if a host is selected and service details if host and service are selected.

See *Host Status* and *Service Status* below for more information.

3.4.3.4 Host Status

This screen gives a detailed view of the status of the host selected.

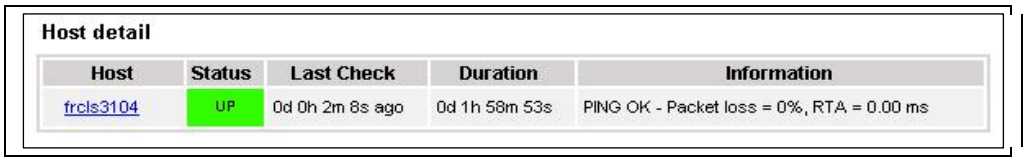


Figure 3-26 Host Status

Host	Host name
Host Status	Host status
Last Check	Time since the last check occurred
Duration	Time since the current state was set
Information	Additional information about the host state

3.4.3.5 Service Status

This screen gives a detailed view of the status of all the services associated with the selected host. Services can also be selected according to status level.

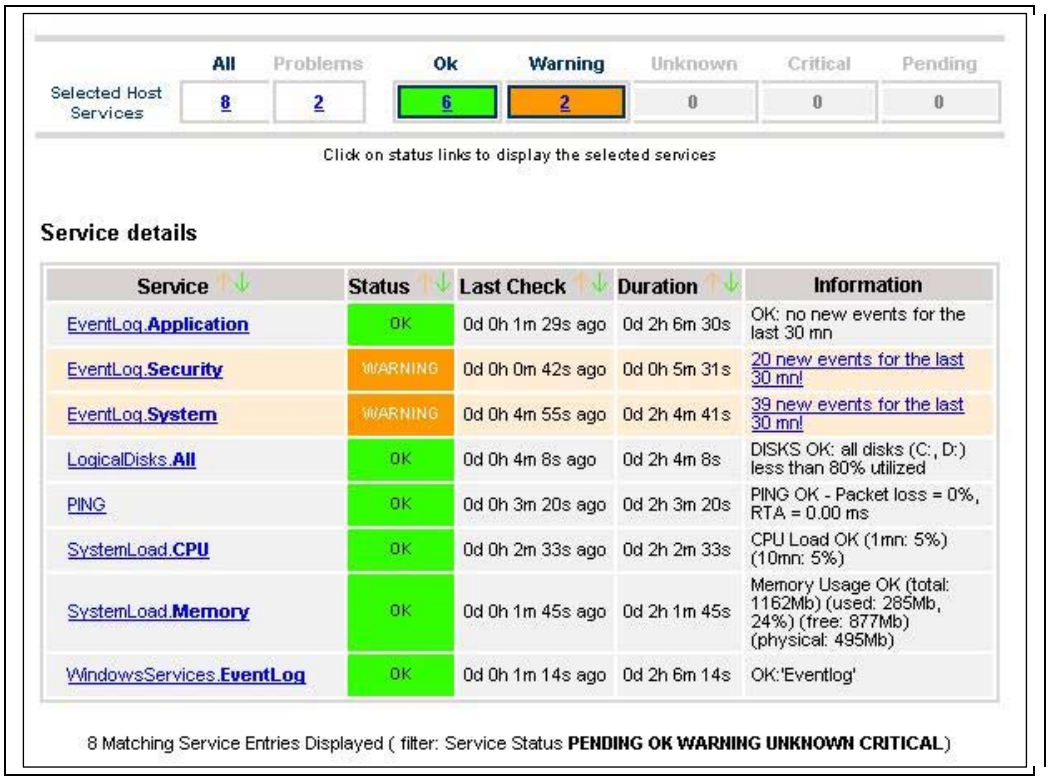


Figure 3-27 Service Status

The Selection Window allows you to select services according to status level:

Selected Host Services
: Number of services with OK, Warning, Unknown, Critical, or Pending status. You can select services according to status: All services, Problem services, or Specific services.

Service
: Service name

Status
: Service status

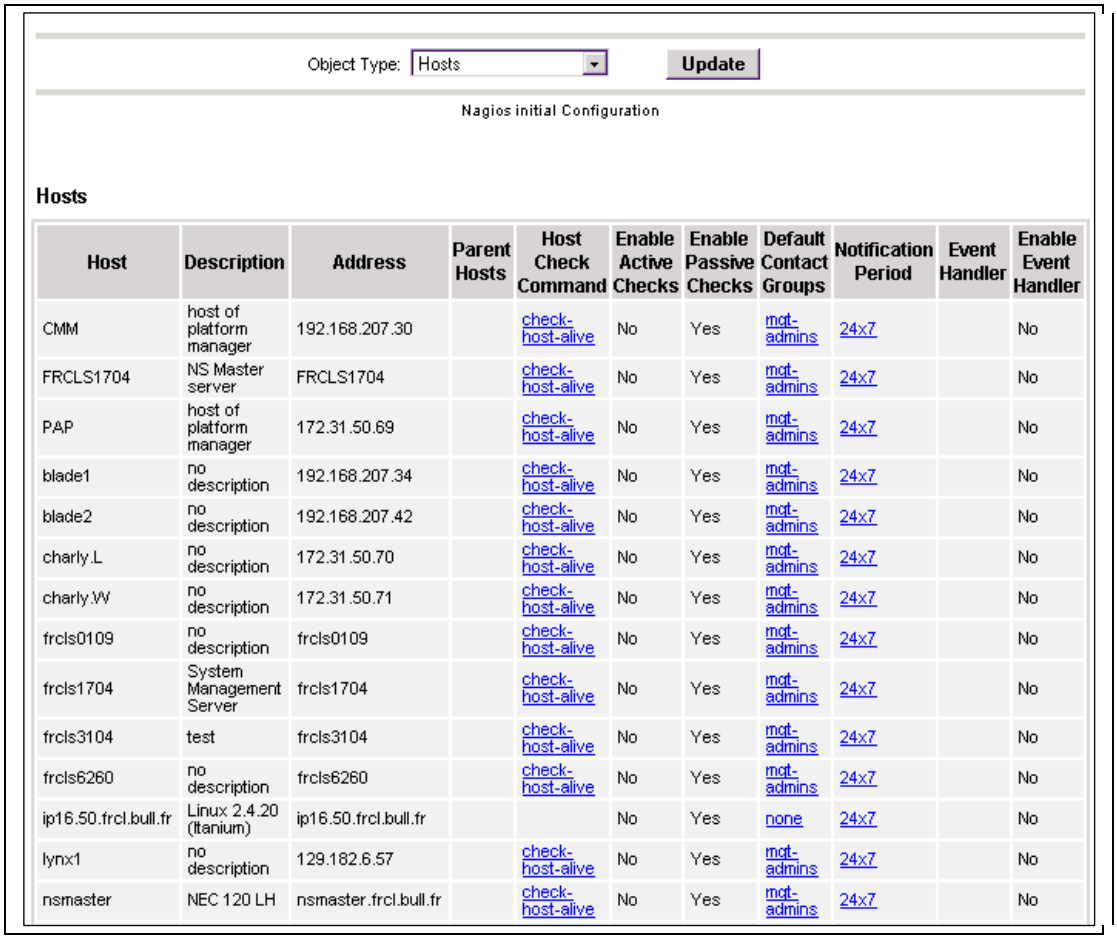
Last Check
: Time since the last check occurred

Duration
: Time since the current state was set

Information
: Gives status details for the selected services

3.4.3.6 Config

This screen displays the Monitoring Server (**nagios**) configuration objects (hosts, hostgroups, services, contacts, contactgroups, timeperiods and commands) that you have defined.


Object Type: Hosts Update

Nagios initial Configuration

Hosts

Host	Description	Address	Parent Hosts	Host Check Command	Enable Active Checks	Enable Passive Checks	Default Contact Groups	Notification Period	Event Handler	Enable Event Handler
CMM	host of platform manager	192.168.207.30		check-host-alive	No	Yes	mgt-admins	24x7		No
FRCLS1704	NS Master server	FRCLS1704		check-host-alive	No	Yes	mgt-admins	24x7		No
PAP	host of platform manager	172.31.50.69		check-host-alive	No	Yes	mgt-admins	24x7		No
blade1	no description	192.168.207.34		check-host-alive	No	Yes	mgt-admins	24x7		No
blade2	no description	192.168.207.42		check-host-alive	No	Yes	mgt-admins	24x7		No
charly.L	no description	172.31.50.70		check-host-alive	No	Yes	mgt-admins	24x7		No
charly.W	no description	172.31.50.71		check-host-alive	No	Yes	mgt-admins	24x7		No
frcls0109	no description	frcls0109		check-host-alive	No	Yes	mgt-admins	24x7		No
frcls1704	System Management Server	frcls1704		check-host-alive	No	Yes	mgt-admins	24x7		No
frcls3104	test	frcls3104		check-host-alive	No	Yes	mgt-admins	24x7		No
frcls6260	no description	frcls6260		check-host-alive	No	Yes	mgt-admins	24x7		No
ip16.50.frcl.bull.fr	Linux 2.4.20 (Itanium)	ip16.50.frcl.bull.fr			No	Yes	none	24x7		No
lynx1	no description	129.182.6.57		check-host-alive	No	Yes	mgt-admins	24x7		No
nsmaster	NEC 120 LH	nsmaster.frcl.bull.fr		check-host-alive	No	Yes	mgt-admins	24x7		No

Figure 3-28 Monitoring Server Configuration

3.4.3.7 Log

This screen displays the current Monitoring Server log file. You can also browse archived events.

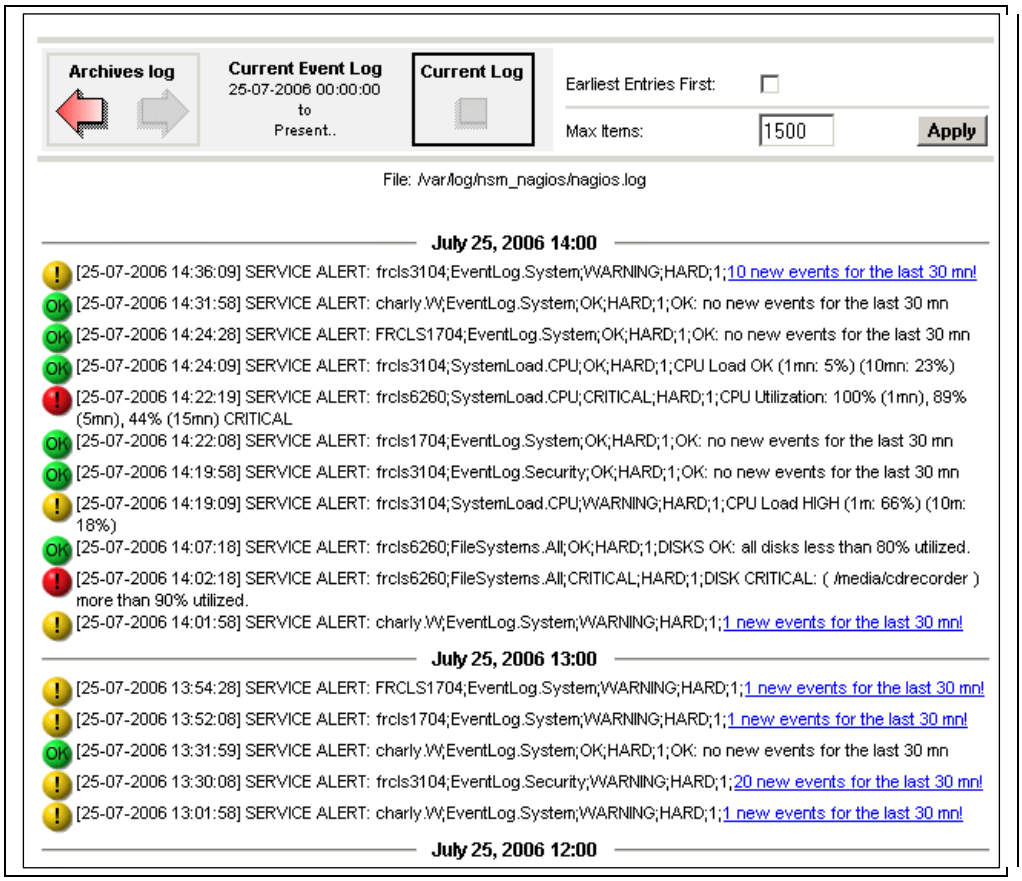


Figure 3-29 Monitoring Server Log

Bull System Manager Log shows all the events logged by the monitoring process:

The screen is divided into two parts:

- The top part of the screen allows you to modify the display according to the criteria selected:

  Event Log selection — By default, only the entries recorded in the current log are displayed. To see previous entries, select an archived log.

  Earliest Entries First — Used to change the order of the entries displayed. By default, the most recent entries are displayed first.

- The bottom part of the screen displays logged events:
  - Host and Service alerts
  - Alert notifications
  - Alert acknowledgements
  - New comments
  - Configuration information messages
  - Miscellaneous

3.4.3.8 Control

When you launch the Control screen from the Hosts or Hostgroups root nodes, the **Monitoring Server information** is displayed. You also have a launching point for the monitoring server commands and links to **Detailed Information**.

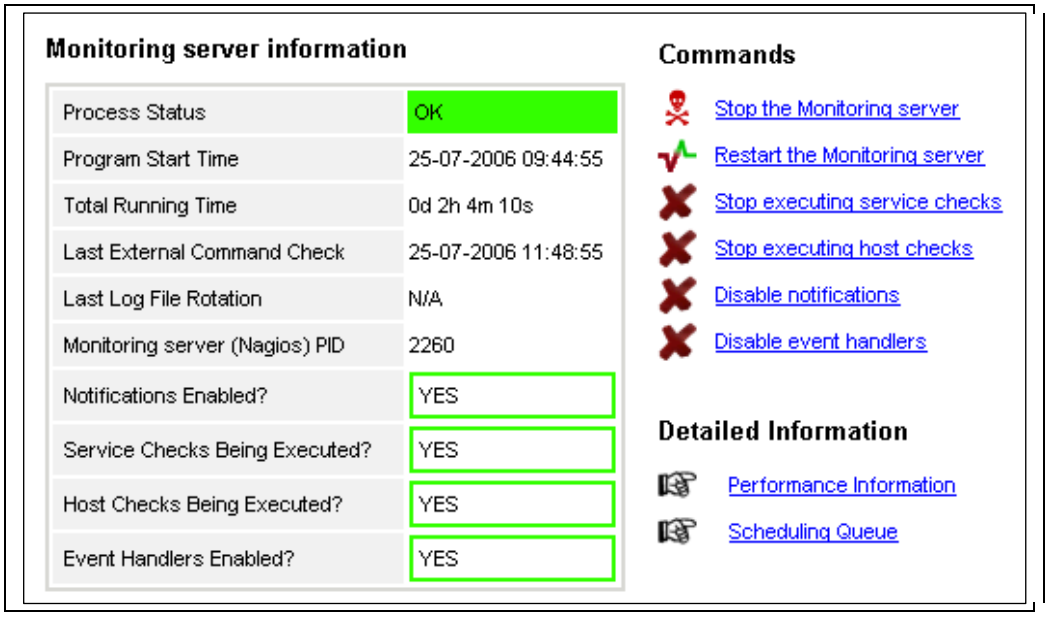


Figure 3-30 Monitoring Server commands

Monitoring Server Information

Gives general information about the Nagios monitoring process.

Commands

Allows you to manage the monitoring functions.
When you click a command, you are prompted to confirm by clicking **Commit** in the confirmation page. The command is dispatched for immediate execution by the Monitoring Server.

Note To process commands you must have Administrator rights.

Detailed Information

Allows you to access detailed information about the performance and scheduling queue.

Performance Information gives statistical information about the **Nagios** monitoring process for each kind of check:

- The minimum, maximum and average time recorded for each iteration of the check The minimum, maximum and average time recorded for check latency (check delay time due to monitoring server overload)
- The current number of active service checks
- The current number of passive service checks
- The current number of active host checks

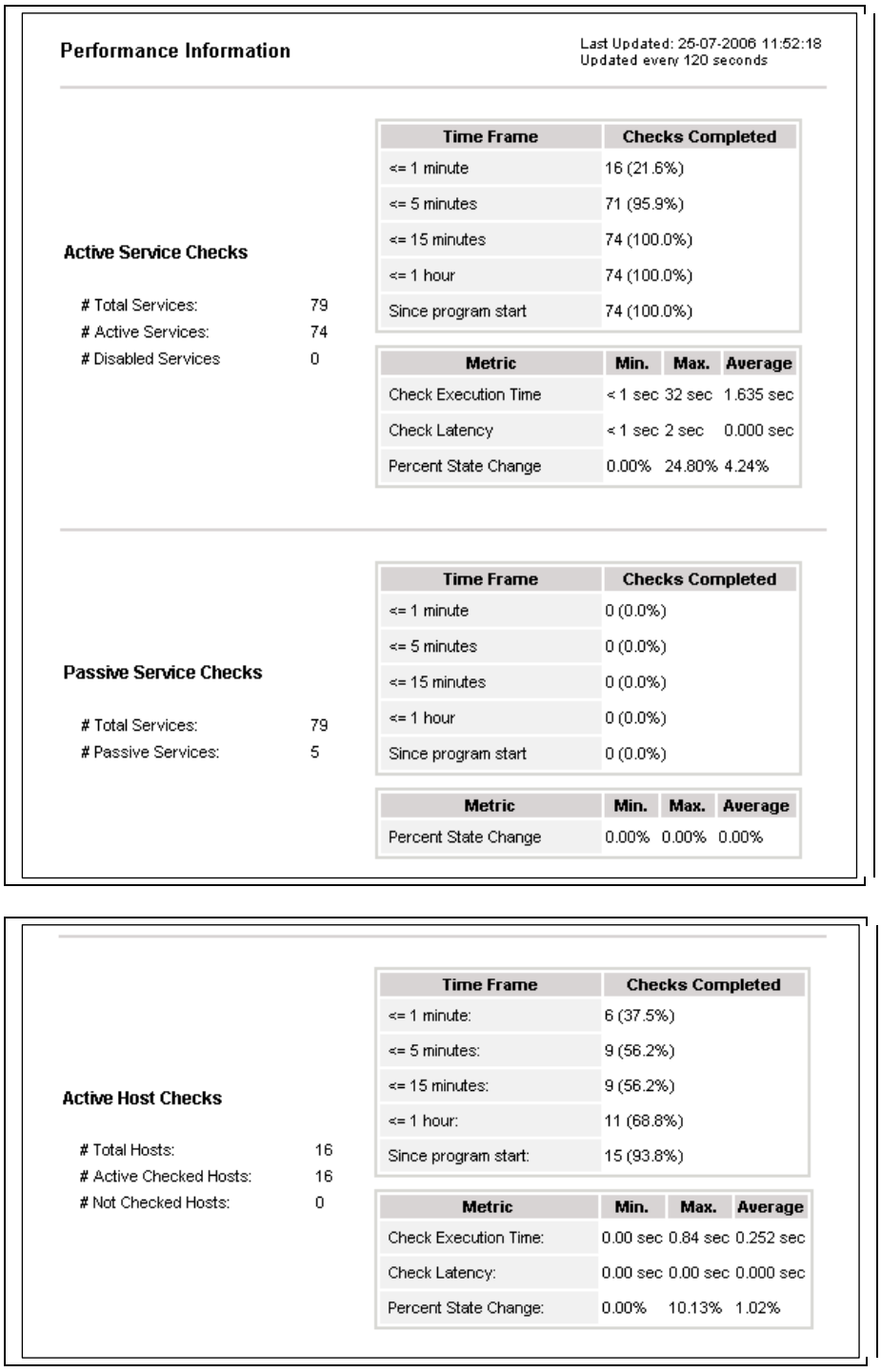
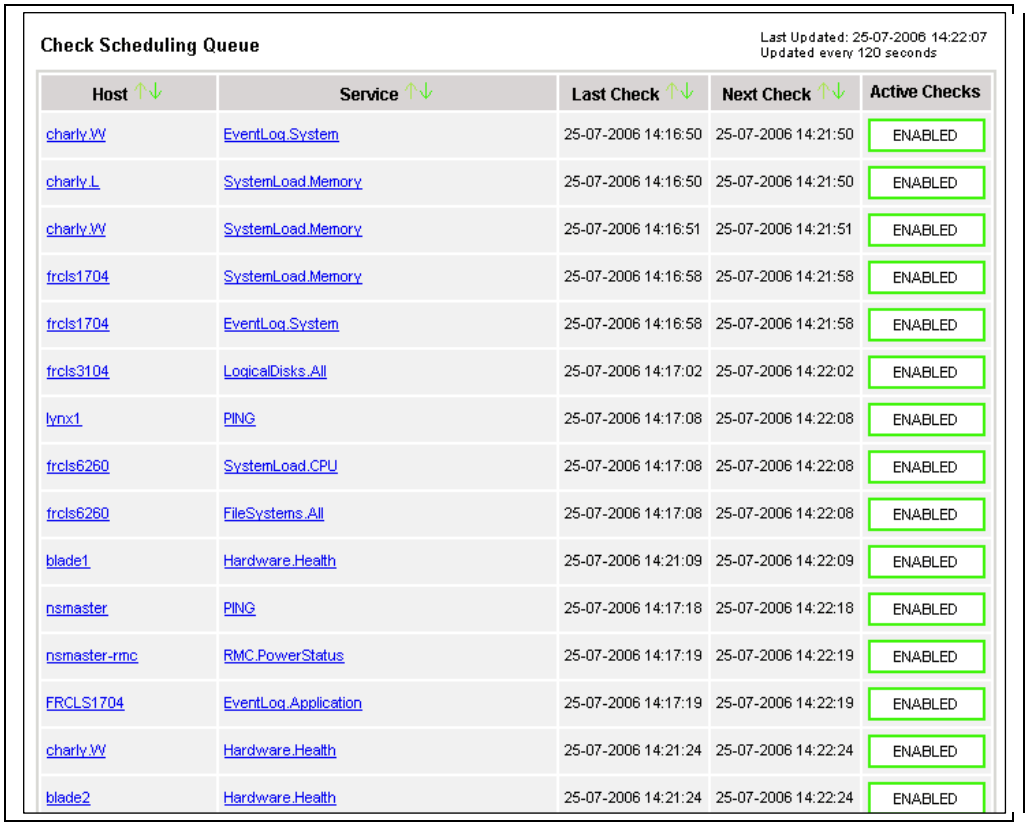


Figure 3-31 Performance statistics

Scheduling Queue displays the time of the last and next checks scheduled for each host or service that is monitored.



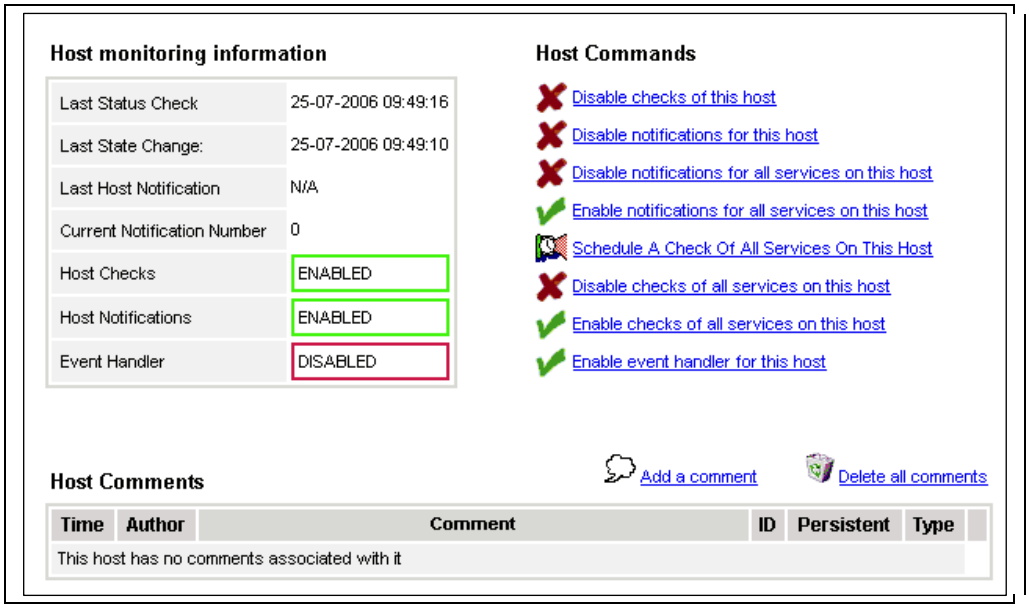
Check Scheduling Queue

Last Updated: 25-07-2006 14:22:07
Updated every 120 seconds

Host	Service	Last Check	Next Check	Active Checks
charly.W	EventLog.System	25-07-2006 14:16:50	25-07-2006 14:21:50	ENABLED
charly.L	SystemLoad.Memory	25-07-2006 14:16:50	25-07-2006 14:21:50	ENABLED
charly.W	SystemLoad.Memory	25-07-2006 14:16:51	25-07-2006 14:21:51	ENABLED
frcls1704	SystemLoad.Memory	25-07-2006 14:16:58	25-07-2006 14:21:58	ENABLED
frcls1704	EventLog.System	25-07-2006 14:16:58	25-07-2006 14:21:58	ENABLED
frcls3104	LogicalDisks.All	25-07-2006 14:17:02	25-07-2006 14:22:02	ENABLED
lynx1	PING	25-07-2006 14:17:08	25-07-2006 14:22:08	ENABLED
frcls6260	SystemLoad.CPU	25-07-2006 14:17:08	25-07-2006 14:22:08	ENABLED
frcls6260	FileSystems.All	25-07-2006 14:17:08	25-07-2006 14:22:08	ENABLED
blade1	Hardware.Health	25-07-2006 14:21:09	25-07-2006 14:22:09	ENABLED
nsmaster	PING	25-07-2006 14:17:18	25-07-2006 14:22:18	ENABLED
nsmaster-rmc	RMC.PowerStatus	25-07-2006 14:17:19	25-07-2006 14:22:19	ENABLED
FRCLS1704	EventLog.Application	25-07-2006 14:17:19	25-07-2006 14:22:19	ENABLED
charly.W	Hardware.Health	25-07-2006 14:21:24	25-07-2006 14:22:24	ENABLED
blade2	Hardware.Health	25-07-2006 14:21:24	25-07-2006 14:22:24	ENABLED

Figure 3-32 Scheduling Information

When you launch the **Control** screen from a host or a service, host or service monitoring information and host or service comments are displayed. You can also enable/disable notifications, and enable or disable service checks.



Host monitoring information

Last Status Check	25-07-2006 09:49:16
Last State Change:	25-07-2006 09:49:10
Last Host Notification	N/A
Current Notification Number	0
Host Checks	ENABLED
Host Notifications	ENABLED
Event Handler	DISABLED

Host Commands

- Disable checks of this host
- Disable notifications for this host
- Disable notifications for all services on this host
- Enable notifications for all services on this host
- Schedule A Check Of All Services On This Host
- Disable checks of all services on this host
- Enable checks of all services on this host
- Enable event handler for this host

Host Comments

Add a comment Delete all comments

Time	Author	Comment	ID	Persistent	Type
This host has no comments associated with it					

Figure 3-33 Monitoring Host commands

Host/Service Monitoring Information

Gives general information about host or service monitoring.

Host/Service Comments

Displays the comments associated with the host or service, and allows you to add or delete comments.

Host/Service Commands

Enables actions for the monitoring functions.

When you click a command, you are prompted to confirm by clicking **Commit** in the confirmation page. The command is posted for immediate execution by the Monitoring Server.

Note To process commands you must have Administrator rights.

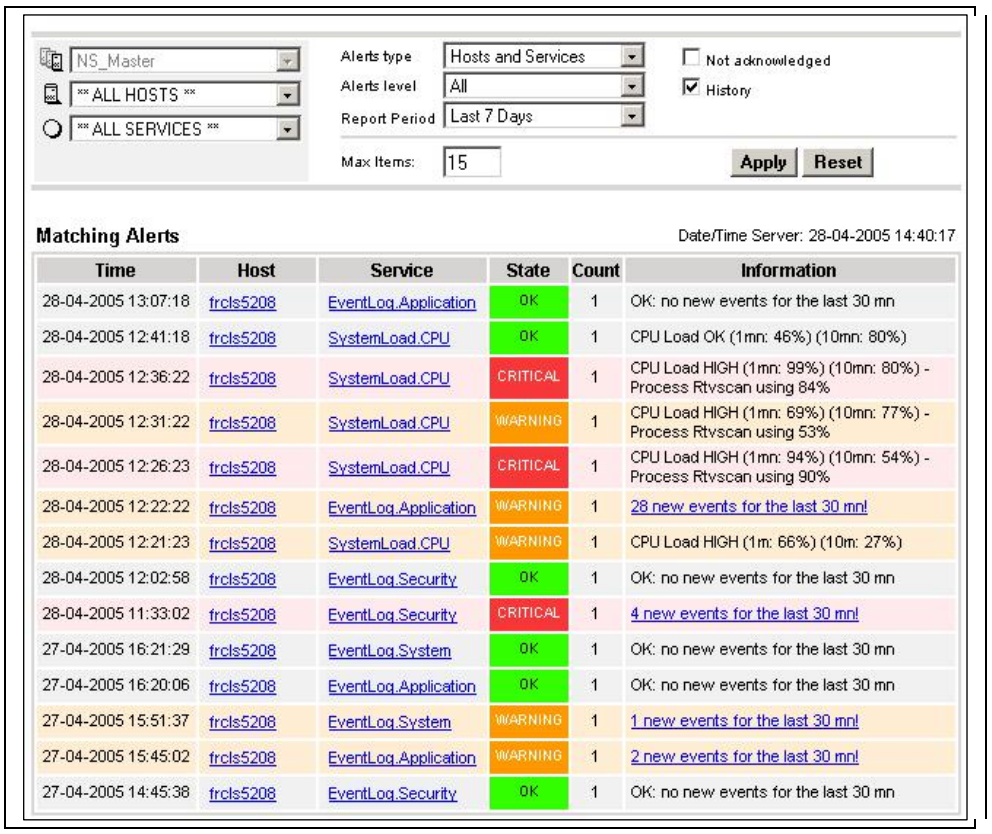
3.4.4 Reporting Information

The following table lists the information types available and associated supervision scope.

Information Type	Supervision Scope
Alert History	Root nodes of Hosts and Hostgroups views (Tree) Hostgroup Host Service
Notifications	Root nodes of Hosts and Hostgroups views (Tree), Hostgroup Host Service
Availability	Root nodes of Hosts and Hostgroups views (Tree), Hostgroup Host Service
Status Trends	Root nodes of Hosts and Hostgroups views (Tree) Host Service
Indicator Trends	Root nodes of Hosts and Hostgroups views (Tree) Hostgroup Host Service

3.4.4.1 Alert History

This screen displays host and service alerts according to the context selected. For example, when this screen is called from a Hostgroup, only the Alerts related to the hosts contained in the selected Hostgroup are given, as shown below. Information about **Alert History** is detailed in *Alert History*, on page 15.



Time	Host	Service	State	Count	Information
28-04-2005 13:07:18	frcls5208	EventLog.Application	OK	1	OK: no new events for the last 30 mn
28-04-2005 12:41:18	frcls5208	SystemLoad.CPU	OK	1	CPU Load OK (1mn: 46%) (10mn: 80%)
28-04-2005 12:36:22	frcls5208	SystemLoad.CPU	CRITICAL	1	CPU Load HIGH (1mn: 99%) (10mn: 80%) - Process Rtvscan using 84%
28-04-2005 12:31:22	frcls5208	SystemLoad.CPU	WARNING	1	CPU Load HIGH (1mn: 69%) (10mn: 77%) - Process Rtvscan using 53%
28-04-2005 12:26:23	frcls5208	SystemLoad.CPU	CRITICAL	1	CPU Load HIGH (1mn: 94%) (10mn: 54%) - Process Rtvscan using 90%
28-04-2005 12:22:22	frcls5208	EventLog.Application	WARNING	1	28 new events for the last 30 mn!
28-04-2005 12:21:23	frcls5208	SystemLoad.CPU	WARNING	1	CPU Load HIGH (1m: 66%) (10m: 27%)
28-04-2005 12:02:58	frcls5208	EventLog.Security	OK	1	OK: no new events for the last 30 mn
28-04-2005 11:33:02	frcls5208	EventLog.Security	CRITICAL	1	4 new events for the last 30 mn!
27-04-2005 16:21:29	frcls5208	EventLog.System	OK	1	OK: no new events for the last 30 mn
27-04-2005 16:20:06	frcls5208	EventLog.Application	OK	1	OK: no new events for the last 30 mn
27-04-2005 15:51:37	frcls5208	EventLog.System	WARNING	1	1 new events for the last 30 mn!
27-04-2005 15:45:02	frcls5208	EventLog.Application	WARNING	1	2 new events for the last 30 mn!
27-04-2005 14:45:38	frcls5208	EventLog.Security	OK	1	OK: no new events for the last 30 mn

Figure 3-34 Alert History screen - example

3.4.4.2 Notifications

This screen displays notifications that have been sent to various contacts, according to the context selected. When this screen is called from a Root node, it reports all the notifications for all the resources declared in the Bull System Manager application, as displayed below.

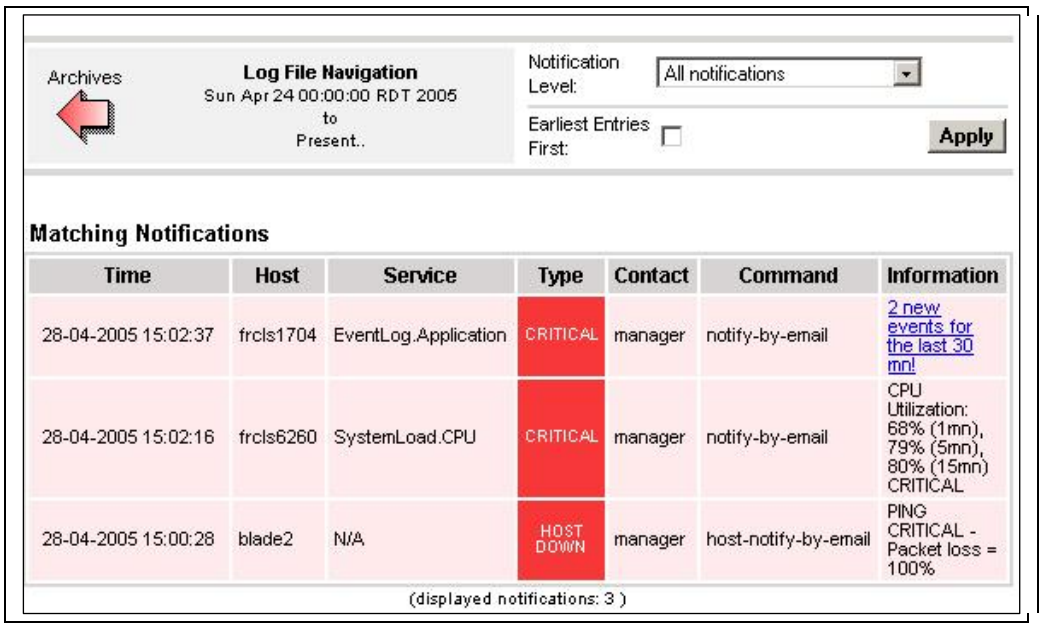


Figure 3-35 Notifications screen - example

The screen is divided into two parts:

- The top part of the screen allows you to modify the notifications reported, according to a set of criteria:

  Log File — By default, only the notifications recorded in the current log are displayed.
  To see older notifications, you can select an archived log.

  Notification Level — Allows you to select the type of Notifications displayed (Service notifications, Host notifications, Host Down, Service Critical, etc.).
  By default, all notifications are displayed.

  Earliest Entries First — Used to select the order of notifications displayed.
  By default, the most recent notifications are displayed first.

- The bottom part of the screen contains matching notification information according to the context and the criteria set in the top part of the screen.

Notifications and information about these notifications (Time, Type, Notified Contacts, etc.) are displayed according to the criteria previously set. Type information reflects the severity of the notification.

3.4.4.3 Availability

This screen reports the availability of hosts and services over a user-specified period. When called from a root node, it reports the availability summary for each host declared in the Bull System Manager application. When called from a Host context, the report will be more detailed as shown below.

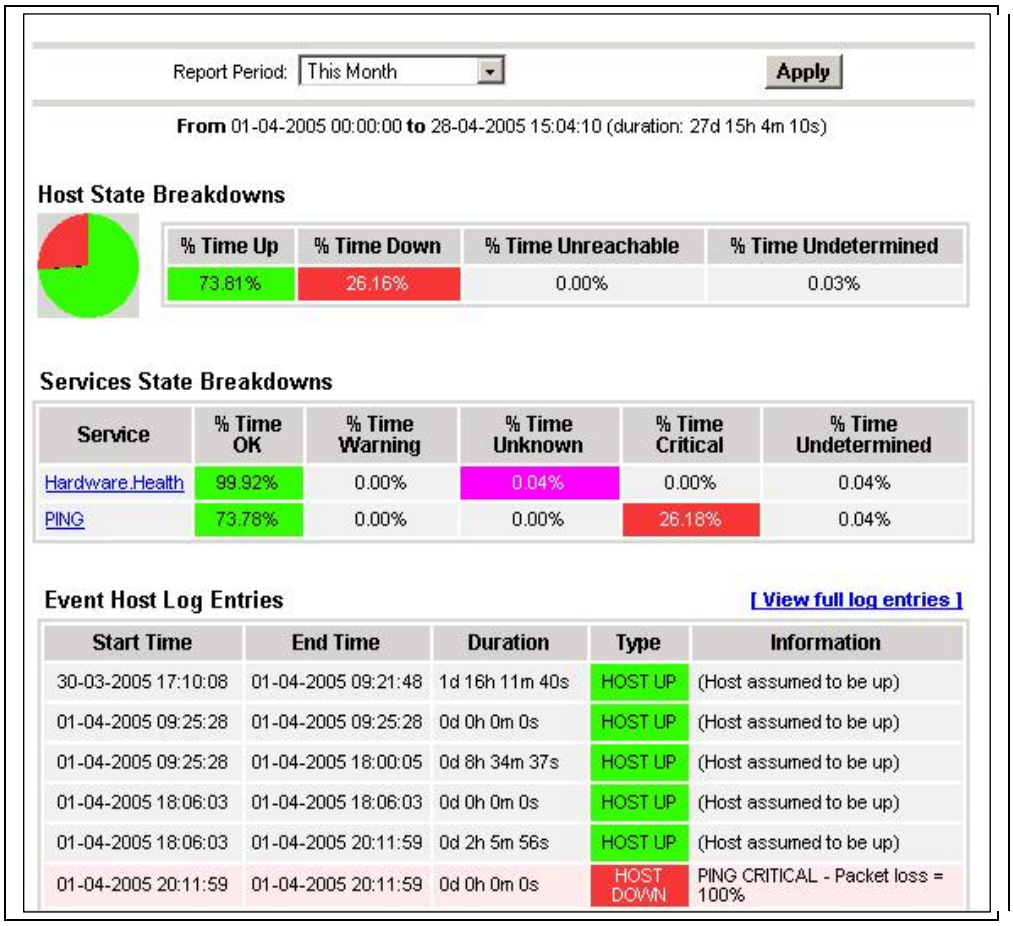


Figure 3-36 Availability screen - example

The screen is divided into two parts:

- The top part allows you to define the period over which the report is built (Report Period selection box). The default period is the last 24 hours.
- The bottom part displays reporting information, according to the context and the report period.

The following information is reported:

Host State Breakdowns or **Service State Breakdowns**	Represents the percentage of time spent by the host or service in each of its possible states. **Note:** **Time Unknown** is reported when the monitoring server cannot obtain information about the service (because, for instance, the host is down, or the monitoring agent is not running on the target). **Time Undetermined** is reported when no information was collected, mainly because the monitoring server was not running.
Services State Breakdowns	This information is available when a report is requested for a host. Availability report for all the services of the host.
Host Log Entries or **Service Log Entries**	List of all the Nagios events logged for the host or service during the chosen period.

3.4.4.4 Status Trends

This screen displays a graph of host or service states over a defined period, as shown below.

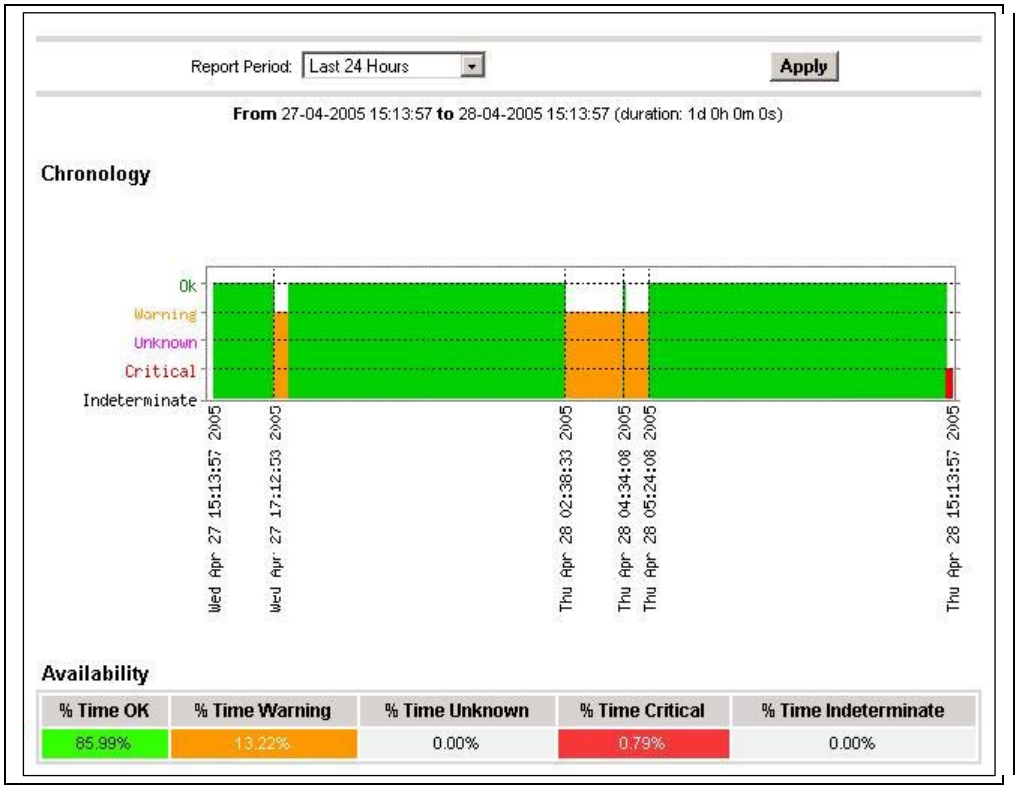


Figure 3-37. Status Trends on a Service

The screen is divided into two parts:

- The top part allows you to select the period for which the report is built (**Report Period** selection box). The default period is the last 24 hours.
- The bottom part displays information, according to the context and the Report Period selected.

The following information is reported:

Chronology	Represents the evolution of the host or service status over the selected period.
Availability	Represents the percentage of time spent in each state for the host or service.

3.4.4.5 Indicator Trends

The **Indicator Trends** screen lists the available indicator reports defined for a given resource, as displayed below.

Details on how to visualize reports associated with these indicators is detailed in *Reports*, on page 92.

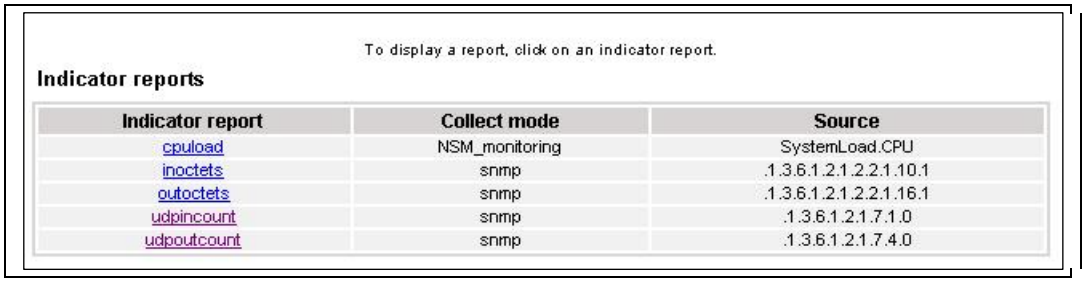


Figure 3-38 Indicator Trends on a Host

3.4.5 Inventory Information

The **Inventory** menu is divided into two submenus: **Platform** and **Operating System**.

Inventory information, which is sent by the **BSM** agent, is stored in a database on the BSM server. If the target host is down, the inventory data is always available.

The **Refresh Inventory** button is used to force a refresh of the inventory stored in the database.

The **BSM** server sends a request to the BSM agent installed on the target host, asking it to send an inventory (hardware and software):

- When the target host is defined in the BSM configurationWhen the target host reboots
- Manually when the operator clicks on **Refresh Inventory**
- Automatically if the **updateInventory** periodic task is enabled in the BSM configuration (See *Chapter 4: Configuring Inventory*, in the *Administrator's Guide*, 86 A2 56FA,)

3.4.5.1 Platform Information

These screens are available for Host or Service supervision. Information levels vary according to OS and host type.

Hardware Information

This information is only available for hosts with **Windows**, **Linux** or **AIX** Operating Systems.

- For Windows hosts, this screen displays the following information:
  - Processor, Memory, BIOS, SOUND, VideoCard, Input Devices, Monitor, Network, Ports, Printer, Controller and Slots Information

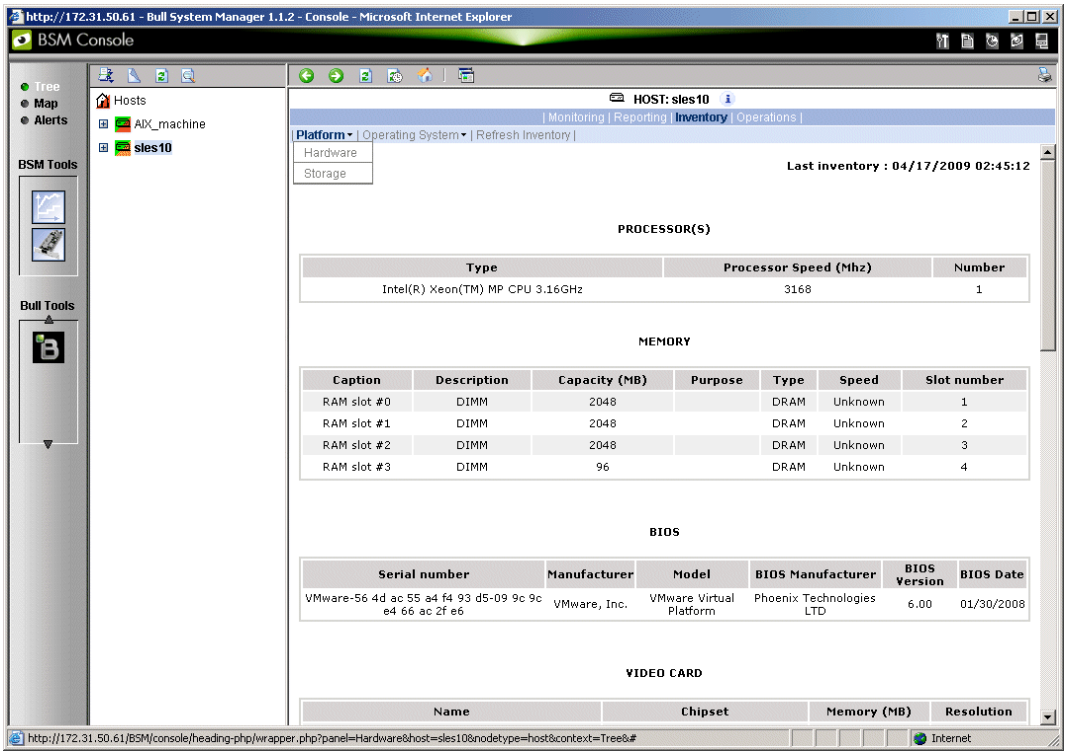


Figure 3-39 Hardware Inventory information – example

Storage Information

This information is only available for hosts with **Windows** or **Linux** Operating Systems.

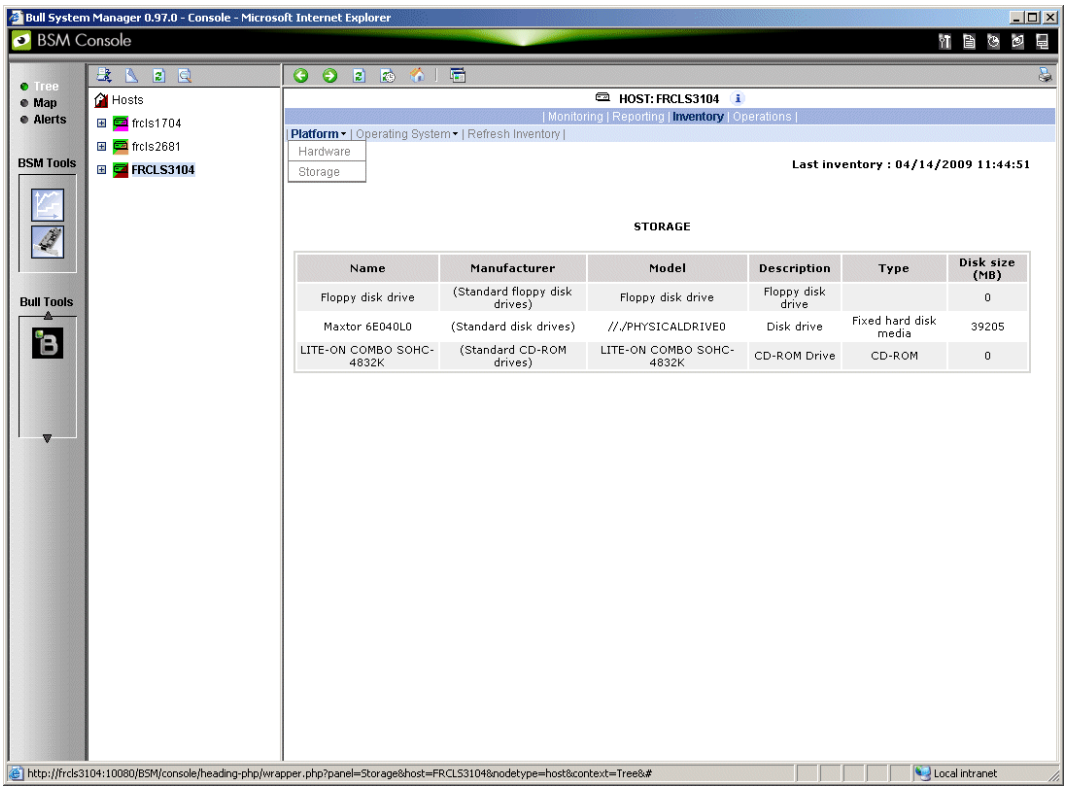


Figure 3-40 Storage information - example

FRU Information

This information is only available for Express 5800, R400, T800, NovaScale 3000, 4000, 5000, 6000 and 9006 series, Nova Scale Blade and Escala Blade hosts.
For details about the information displayed, refer to *Chapter 4*.

Sensor Information

This information is only available for Express 5800, R400, T800, NovaScale 3000, 4000 and 9006 series and Nova Scale Blade hosts.
For details about the information displayed, refer to *Chapter 4*.

SEL Information

This information is only available for Express 5800, R400, T800, NovaScale 3000, 4000, 5000 , 6000 and 9006 series, Nova Scale Blade and Escala Blade hosts.
For details about the information displayed, refer to *Chapter 4*.

3.4.5.2 Operating System Information

These screens are available for the supervision of Hosts or Services. Information levels vary according to OS and host type.

Windows Information

The Windows System screen displays the following information:

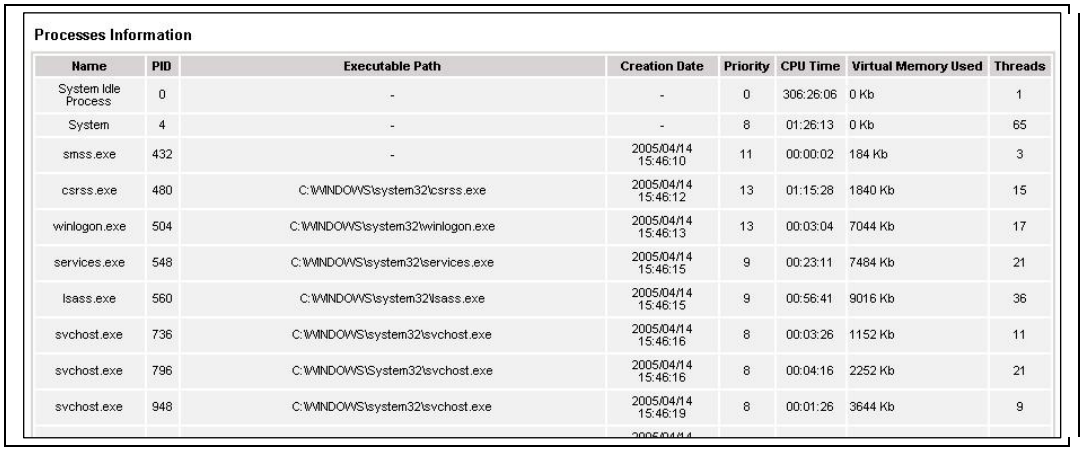
- System, Memory, Logical Disks Process, Users, Products installed, Shared resources and Services Information

Memory Usage

	Size	Used	Free
Physical	1.5 Gbytes	53 %	725 Mbytes
Paged	744 Mbytes	13 %	654 Mbytes
Total (Virtual)	2.1 Gbytes	30 %	1.5 Gbytes

Figure 3-41 Windows Memory screen - example

The **Windows Process** screen displays the processes running:

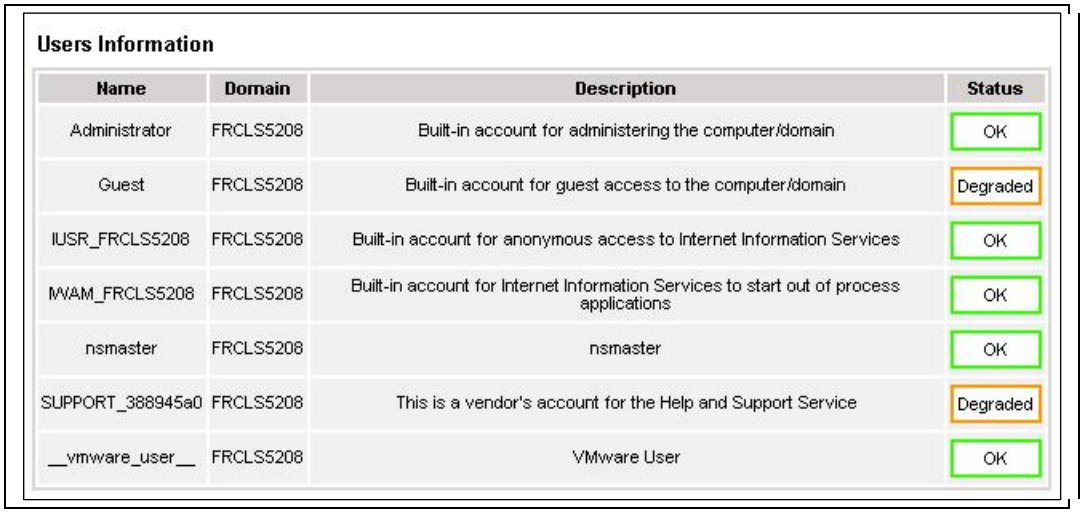


Processes Information

Name	PID	Executable Path	Creation Date	Priority	CPU Time	Virtual Memory Used	Threads
System Idle Process	0	-	-	0	306:26:06	0 Kb	1
System	4	-	-	8	01:26:13	0 Kb	65
smss.exe	432	-	2005/04/14 15:46:10	11	00:00:02	184 Kb	3
csrss.exe	480	C:\WINDOWS\system32\csrss.exe	2005/04/14 15:46:12	13	01:15:28	1840 Kb	15
winlogon.exe	504	C:\WINDOWS\system32\winlogon.exe	2005/04/14 15:46:13	13	00:03:04	7044 Kb	17
services.exe	548	C:\WINDOWS\system32\services.exe	2005/04/14 15:46:15	9	00:23:11	7484 Kb	21
lsass.exe	560	C:\WINDOWS\system32\lsass.exe	2005/04/14 15:46:15	9	00:56:41	9016 Kb	36
svchost.exe	736	C:\WINDOWS\system32\svchost.exe	2005/04/14 15:46:16	8	00:03:26	1152 Kb	11
svchost.exe	796	C:\WINDOWS\System32\svchost.exe	2005/04/14 15:46:16	8	00:04:16	2252 Kb	21
svchost.exe	948	C:\WINDOWS\system32\svchost.exe	2005/04/14 15:46:19	8	00:01:26	3644 Kb	9

Figure 3-42 Windows Process screen - example

The **Windows Users** screen displays information regarding the users:

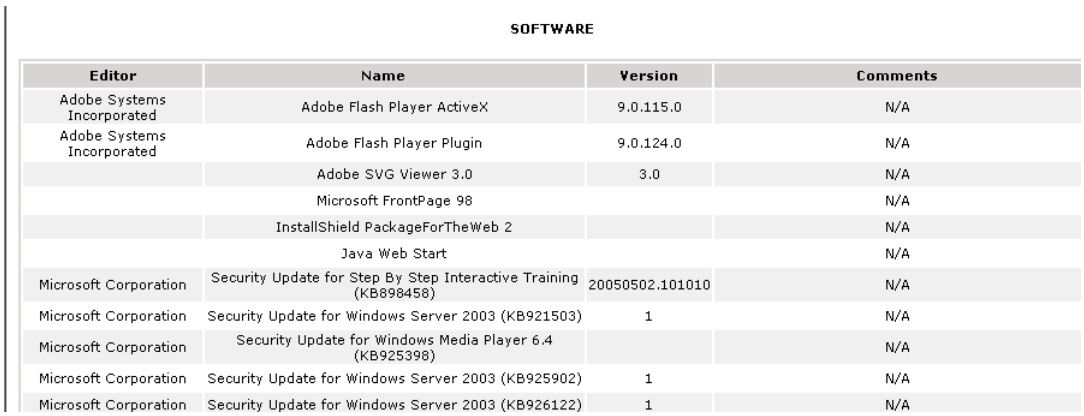


Users Information

Name	Domain	Description	Status
Administrator	FRCLS5208	Built-in account for administering the computer/domain	OK
Guest	FRCLS5208	Built-in account for guest access to the computer/domain	Degraded
IUSR_FRCLS5208	FRCLS5208	Built-in account for anonymous access to Internet Information Services	OK
IWAM_FRCLS5208	FRCLS5208	Built-in account for Internet Information Services to start out of process applications	OK
nsmaster	FRCLS5208	nsmaster	OK
SUPPORT_388945a0	FRCLS5208	This is a vendor's account for the Help and Support Service	Degraded
__vmware_user__	FRCLS5208	VMware User	OK

Figure 3-43 Windows Users screen - example

The **Windows Products** screen displays the products installed:



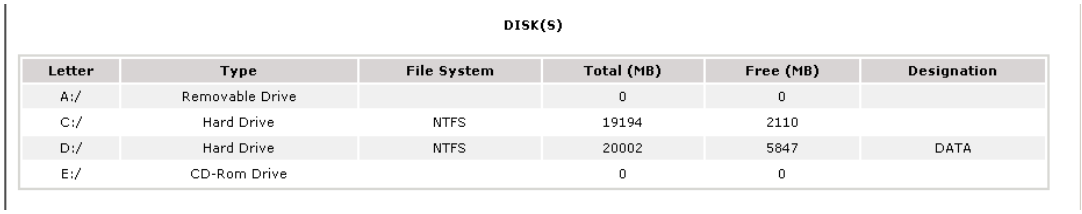
SOFTWARE

Editor	Name	Version	Comments
Adobe Systems Incorporated	Adobe Flash Player ActiveX	9.0.115.0	N/A
Adobe Systems Incorporated	Adobe Flash Player Plugin	9.0.124.0	N/A
	Adobe SVG Viewer 3.0	3.0	N/A
	Microsoft FrontPage 98		N/A
	InstallShield PackageForTheWeb 2		N/A
	Java Web Start		N/A
Microsoft Corporation	Security Update for Step By Step Interactive Training (KB898458)	20050502.101010	N/A
Microsoft Corporation	Security Update for Windows Server 2003 (KB921503)	1	N/A
Microsoft Corporation	Security Update for Windows Media Player 6.4 (KB925398)		N/A
Microsoft Corporation	Security Update for Windows Server 2003 (KB925902)	1	N/A
Microsoft Corporation	Security Update for Windows Server 2003 (KB926122)	1	N/A

Figure 3-44 Windows Products screen - example

Note On servers running the Windows Operating System, only the products installed that use a **.MSI** file are displayed.

The **Windows Logical Disks** screen displays information about the logical disks:

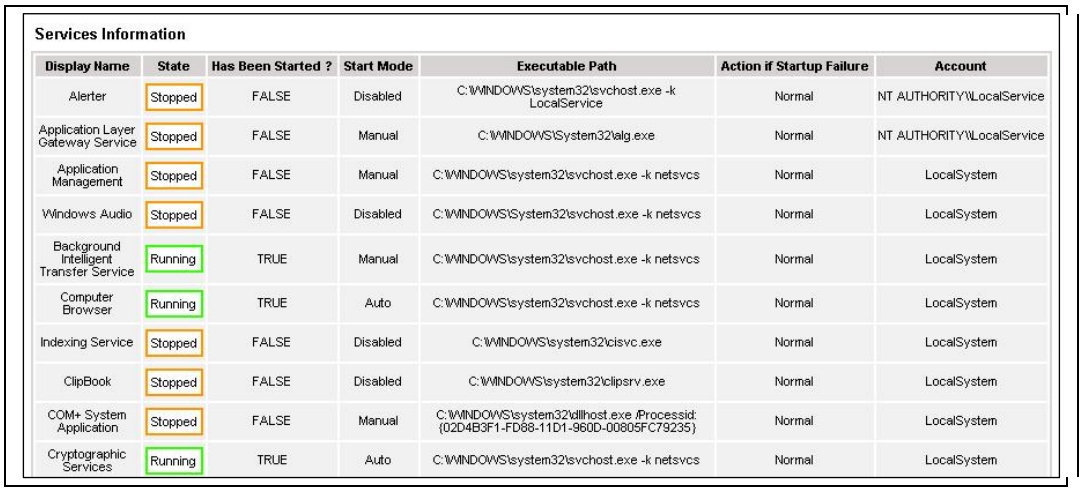


DISK(S)

Letter	Type	File System	Total (MB)	Free (MB)	Designation
A:/	Removable Drive		0	0	
C:/	Hard Drive	NTFS	19194	2110	
D:/	Hard Drive	NTFS	20002	5847	DATA
E:/	CD-Rom Drive		0	0	

Figure 3-45 Windows Logical Disks screen - example

The **Windows Services** screen displays information regarding the services:



Services Information

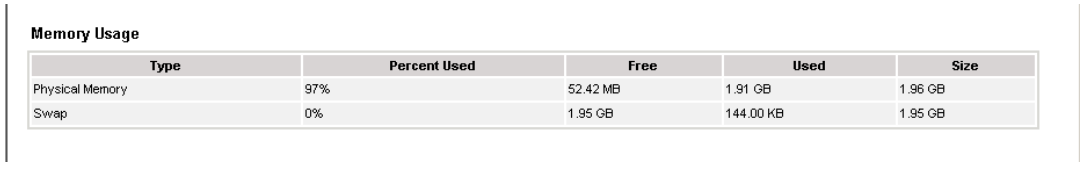
Display Name	State	Has Been Started ?	Start Mode	Executable Path	Action if Startup Failure	Account
Alerter	Stopped	FALSE	Disabled	C:\WINDOWS\system32\svchost.exe -k LocalService	Normal	NT AUTHORITY\LocalService
Application Layer Gateway Service	Stopped	FALSE	Manual	C:\WINDOWS\System32\alg.exe	Normal	NT AUTHORITY\LocalService
Application Management	Stopped	FALSE	Manual	C:\WINDOWS\system32\svchost.exe -k netsvcs	Normal	LocalSystem
Windows Audio	Stopped	FALSE	Disabled	C:\WINDOWS\System32\svchost.exe -k netsvcs	Normal	LocalSystem
Background Intelligent Transfer Service	Running	TRUE	Manual	C:\WINDOWS\system32\svchost.exe -k netsvcs	Normal	LocalSystem
Computer Browser	Running	TRUE	Auto	C:\WINDOWS\system32\svchost.exe -k netsvcs	Normal	LocalSystem
Indexing Service	Stopped	FALSE	Disabled	C:\WINDOWS\system32\cisvc.exe	Normal	LocalSystem
ClipBook	Stopped	FALSE	Disabled	C:\WINDOWS\system32\clipsrv.exe	Normal	LocalSystem
COM+ System Application	Stopped	FALSE	Manual	C:\WINDOWS\system32\dllhost.exe /Processid:{02D4B3F1-FD88-11D1-960D-00805FC79235}	Normal	LocalSystem
Cryptographic Services	Running	TRUE	Auto	C:\WINDOWS\system32\svchost.exe -k netsvcs	Normal	LocalSystem

Figure 3-46 Windows Services screen - example

Linux and AIX Information

The Linux System screen displays the following information:

- System, Memory, File Systems, Process, Users, RPM products and System Logs Information



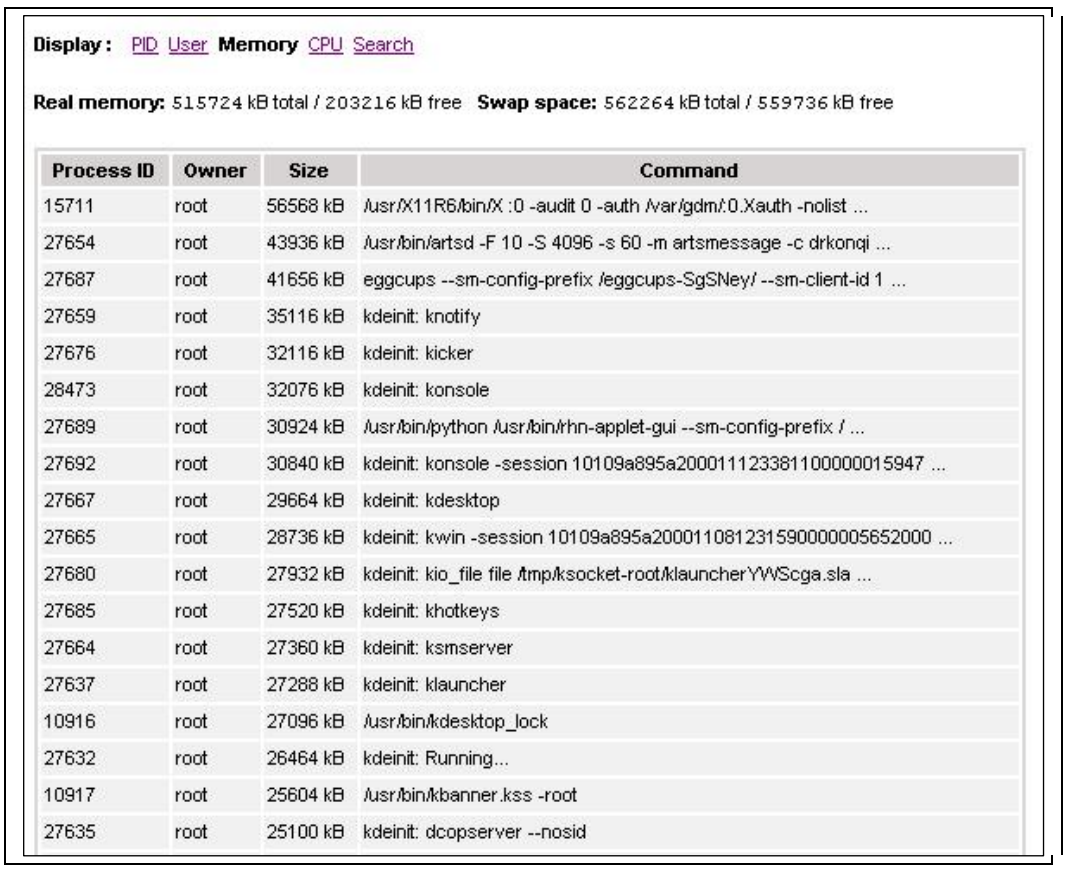
Memory Usage

Type	Percent Used	Free	Used	Size
Physical Memory	97%	52.42 MB	1.91 GB	1.96 GB
Swap	0%	1.95 GB	144.00 KB	1.95 GB

Figure 3-47 Linux Memory Usage screen - example

The **Linux Process** screen displays processes sorted by PID, User, Memory Usage or CPU Usage.

The following example shows processes sorted by **Memory Usage**. You can change the sort option by clicking the corresponding link.



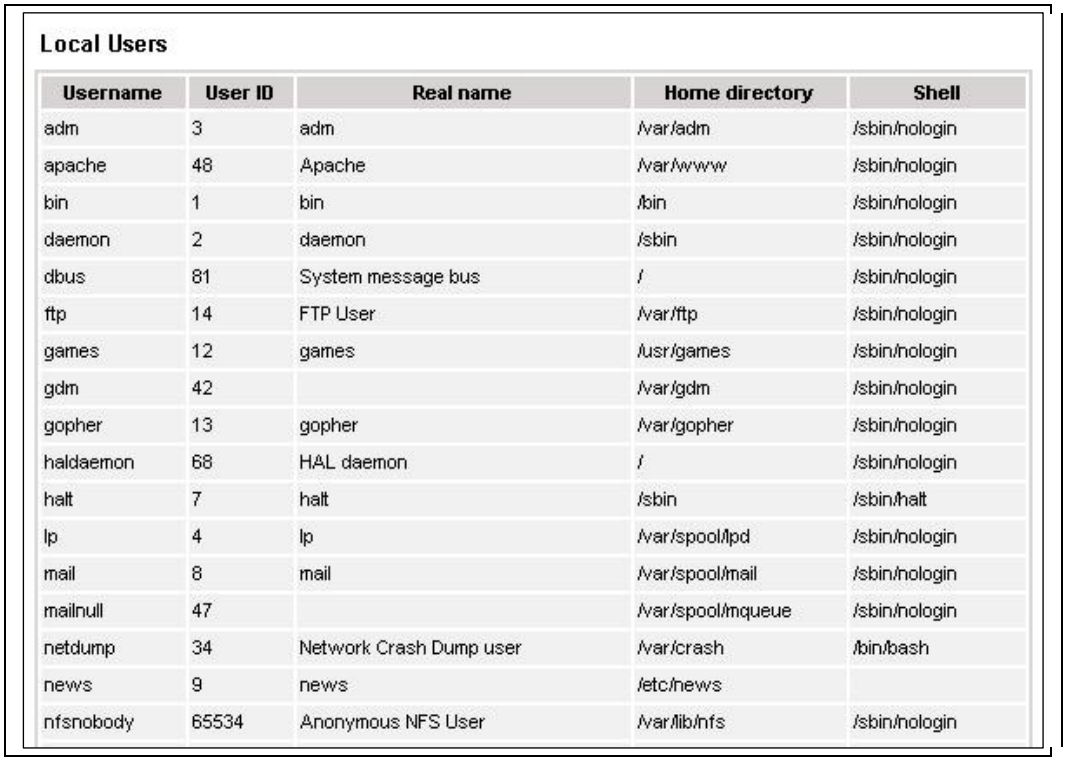
Display: PID User **Memory** CPU Search

Real memory: 515724 kB total / 203216 kB free **Swap space:** 562264 kB total / 559736 kB free

Process ID	Owner	Size	Command
15711	root	56568 kB	/usr/X11R6/bin/X :0 -audit 0 -auth /var/gdm/:0.Xauth -nolist ...
27654	root	43936 kB	/usr/bin/artsd -F 10 -S 4096 -s 60 -m artsmessage -c drkonqi ...
27687	root	41656 kB	eggcups --sm-config-prefix /eggcups-SgSNey/ --sm-client-id 1 ...
27659	root	35116 kB	kdeinit: knotify
27676	root	32116 kB	kdeinit: kicker
28473	root	32076 kB	kdeinit: konsole
27689	root	30924 kB	/usr/bin/python /usr/bin/rhn-applet-gui --sm-config-prefix / ...
27692	root	30840 kB	kdeinit: konsole -session 10109a895a2000111233811000000015947 ...
27667	root	29664 kB	kdeinit: kdesktop
27665	root	28736 kB	kdeinit: kwin -session 10109a895a2000110812315900000005652000 ...
27680	root	27932 kB	kdeinit: kio_file file /tmp/ksocket-root/klauncherYWScga.sla ...
27685	root	27520 kB	kdeinit: khotkeys
27664	root	27360 kB	kdeinit: ksmserver
27637	root	27288 kB	kdeinit: klauncher
10916	root	27096 kB	/usr/bin/kdesktop_lock
27632	root	26464 kB	kdeinit: Running...
10917	root	25604 kB	/usr/bin/kbanner.kss -root
27635	root	25100 kB	kdeinit: dcopserver --nosid

Figure 3-48 Linux Process screen - example

The **Linux Users** screen displays information regarding the users:

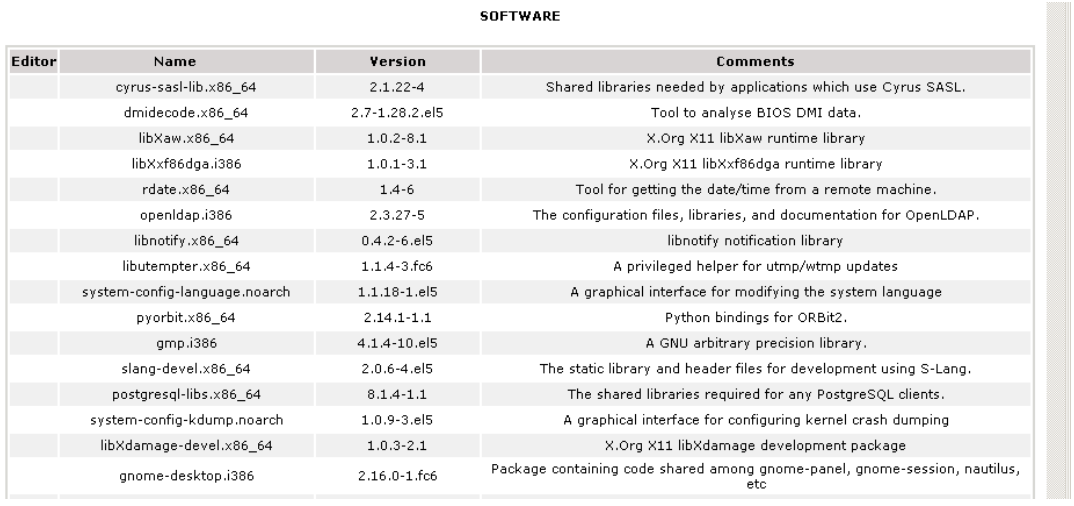


Local Users

Username	User ID	Real name	Home directory	Shell
adm	3	adm	/var/adm	/sbin/nologin
apache	48	Apache	/var/www	/sbin/nologin
bin	1	bin	/bin	/sbin/nologin
daemon	2	daemon	/sbin	/sbin/nologin
dbus	81	System message bus	/	/sbin/nologin
ftp	14	FTP User	/var/ftp	/sbin/nologin
games	12	games	/usr/games	/sbin/nologin
gdm	42		/var/gdm	/sbin/nologin
gopher	13	gopher	/var/gopher	/sbin/nologin
haldaemon	68	HAL daemon	/	/sbin/nologin
halt	7	halt	/sbin	/sbin/halt
lp	4	lp	/var/spool/lpd	/sbin/nologin
mail	8	mail	/var/spool/mail	/sbin/nologin
mailnull	47		/var/spool/mqueue	/sbin/nologin
netdump	34	Network Crash Dump user	/var/crash	/bin/bash
news	9	news	/etc/news	
nfsnobody	65534	Anonymous NFS User	/var/lib/nfs	/sbin/nologin

Figure 3-49 Linux Users screen - example

The **Linux RPM** Products screen allows you to display the packages installed by using a search tool or by browsing the package tree.



SOFTWARE

Editor	Name	Version	Comments
	cyrus-sasl-lib.x86_64	2.1.22-4	Shared libraries needed by applications which use Cyrus SASL.
	dmidecode.x86_64	2.7-1.28.2.el5	Tool to analyse BIOS DMI data.
	libXaw.x86_64	1.0.2-8.1	X.Org X11 libXaw runtime library
	libXxf86dga.i386	1.0.1-3.1	X.Org X11 libXxf86dga runtime library
	rdate.x86_64	1.4-6	Tool for getting the date/time from a remote machine.
	openldap.i386	2.3.27-5	The configuration files, libraries, and documentation for OpenLDAP.
	libnotify.x86_64	0.4.2-6.el5	libnotify notification library
	libutempter.x86_64	1.1.4-3.fc6	A privileged helper for utmp/wtmp updates
	system-config-language.noarch	1.1.18-1.el5	A graphical interface for modifying the system language
	pyorbit.x86_64	2.14.1-1.1	Python bindings for ORBit2.
	gmp.i386	4.1.4-10.el5	A GNU arbitrary precision library.
	slang-devel.x86_64	2.0.6-4.el5	The static library and header files for development using S-Lang.
	postgresql-libs.x86_64	8.1.4-1.1	The shared libraries required for any PostgreSQL clients.
	system-config-kdump.noarch	1.0.9-3.el5	A graphical interface for configuring kernel crash dumping
	libXdamage-devel.x86_64	1.0.3-2.1	X.Org X11 libXdamage development package
	gnome-desktop.i386	2.16.0-1.fc6	Package containing code shared among gnome-panel, gnome-session, nautilus, etc

Figure 3-50 Linux RPM Products - example

The **Linux System Logs** screen displays, and allows you to view, the logs that are available.

Log destination	Active?	Messages selected	
File /dev/console	No	kern.*	
File /var/log/messages	Yes	*.info ; mail.none ; authpriv.none ; cron.none	View..
File /var/log/secure	Yes	authpriv.*	View..
File /var/log/maillog	Yes	mail.*	View..
File /var/log/cron	Yes	cron.*	View..
All users	Yes	*.emerg	
File /var/log/spooler	Yes	uucp,news.crit	View..
File /var/log/boot.log	Yes	local7.*	View..

Figure 3-51 Linux System Logs screen – example

3.4.6 Operations Menu

The **Operations** menu allows an Administrator to take remote control of a platform or Operating System.

This menu is only available to Administrators and is divided into several potential submenus: **Platform**, **Operating System**, **Consolidation**, **Applications** and **Storage**.

3.4.6.1 Platform Menu

These menus are available for the **Hardware Manager** and **Host** (and **Services**) with a dedicated hardware manager.

Power Control

Allows the Administrator to manage the power control via the Bull System Manager Hardware Management application.

Manager GUI

Allows you to launch the appropriate hardware manager:

- PAM for NovaScale 5000 and 6000 series
- ISM for NovaScale 4000 series
- CMM for NovaScale Blade series
- RMC or ARMC, SIMSO+ for Intel based computers.
- All other managers that can be accessed via a URL.

3.4.6.2 Operating system Menu

These menus are available for **Host** or **Service** supervision. Information levels vary according to OS and host type.

Remote Operation Menu for Windows	
... ->VNC Viewer	Starts VNC viewer to connect to this host.
... ->MMC	
... ->Remote Desktop	
Remote Operation Menu for Linux	
... ->SSH	Launches SSH to connect to this host.
	The following items Open a Webmin page:
... ->Shell	• to execute a Unix shell command.
... -> FileSystem	• to manage disk and network file systems.
... -> Processes	• to manage running processes.
... -> Users	• to manage Users and Groups.
... -> Password	• to manage passwords.
... -> RPM	• to manage software packages.
... -> System Logs	• to manage system logs.
... -> NetConfig	• to manage network configuration.

Note **SSH** command calls a local SSH client console. This command runs only on **Linux** console machines.

3.4.6.3 Storage Menu

This menu is available for the Storage Manager, Host or Service supervision.

From this menu, you can call the storage manager GUI.

3.4.6.4 Consolidation Menu

This menu is available for **Host** supervision.

From this menu, you can call specific management tools for virtualization and/or consolidation (generally, these items come with specific Server Add-ons).

3.4.6.5 Application Menu

This menu is available for Host supervision.

From this menu, you can call specific management tools for a specific Bull applicative framework and/or applications (generally, these items come with specific Server Add-ons).

Chapter 4. Using Bull System Manager Console Applications

4.1 Bull System Manager Hardware Management Application

The **Bull System Manager Remote Hardware Management Application** provides the same look and feel for hardware operations, independently of the target machine type.

This application manages **Power Control**, and displays **FRUs**, **Sensors** and **System Event Logs** for Express 5800 and NovaScale 4000, 5000, 6000, R400, T800, 9600 or Blade series servers.

This application also manages Power Management for NovaScale R400, T800 servers.

There are two ways to start the application:

- Launch the **Hardware Management Application** from the application bar
- Activate the **Hardware > Remote Control** item in the Console Management Tree host menu.

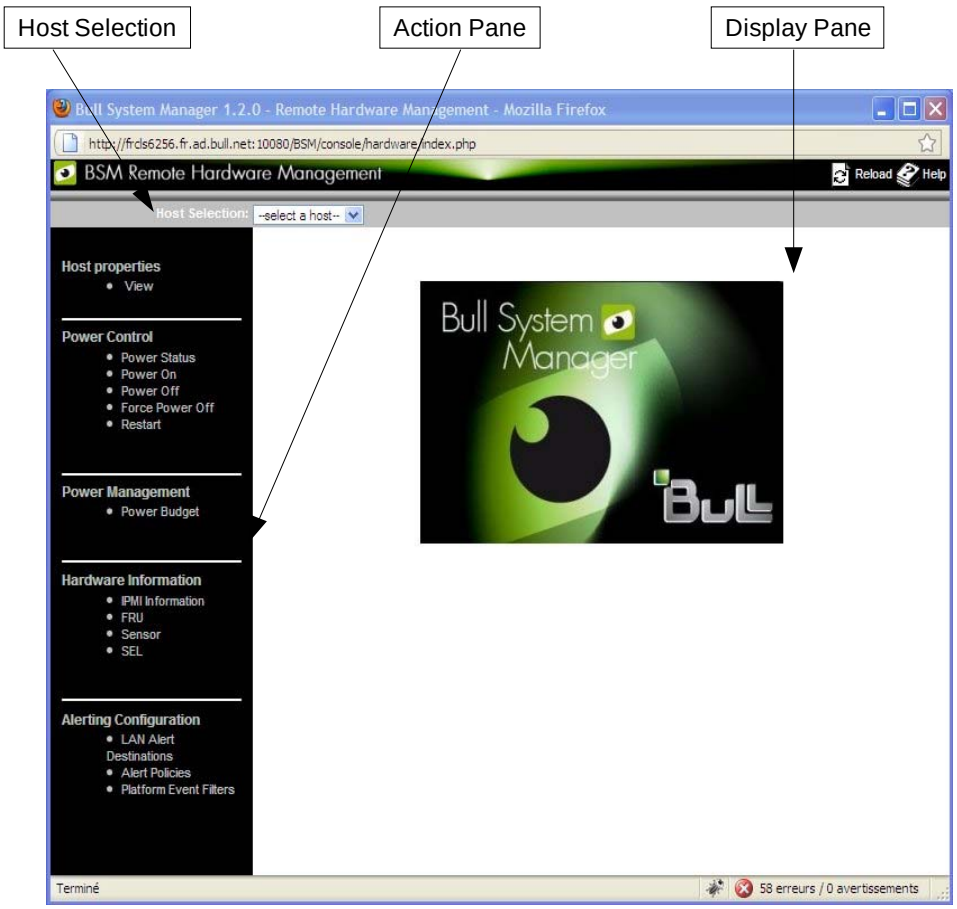


Figure 4-1 Remote Hardware Management screen

Bull System Manager Remote Hardware Management comprises three functional parts:

Host Selection Window & Current Selected Host Window
: Used to select the current host from all the Express 5800 and NovaScale 4000, 5000, 6000, R400, T800, 9600 or Blade servers declared in the Bull System Manager network and displays it.

Action Window
: Displays the hardware operations that can be executed.

Display Window
: Displays parameter forms, messages and command results.

4.1.1 Host Selection

Hardware commands only apply to the selected host. The selected host name is displayed in the **Current Selected Host** Window.

The application is launched contextually from the **Current Selected Host** in the **Console Management** Tree.

You can select another host from the list of available hosts in the **Host Selection** Window.

When a host is selected, the application reads the Bull System Manager configuration files to obtain the host properties.

4.1.1.1 Host Properties

You can display selected host properties by clicking **View**:

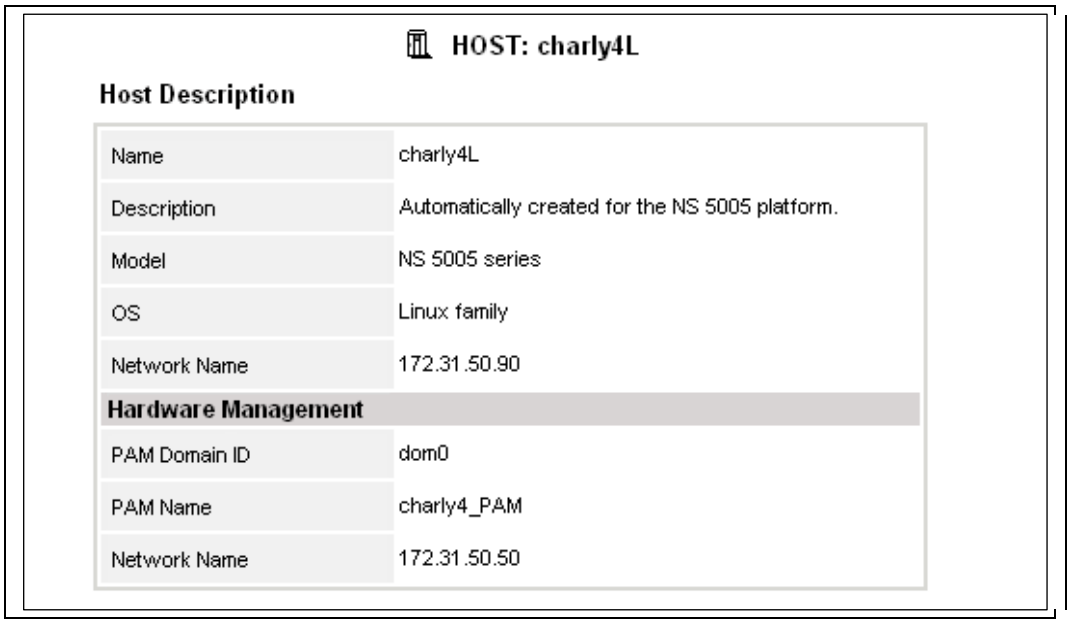


Figure 4-2 NovaScale 5000 Server host properties - example

Host properties differ according to host type, as shown in the following tables:

Name	Name of the current selected host to which commands are applied
Model	Host model
Network Name	Current selected host local network name or IP address
Operating System	Operating system type (Windows, Linux or any)
Out-Of-Band information	
Network name	network name

Table 4-1. NovaScale 4000 Server host properties

Name	Name of the current selected host to which commands are applied
Model	Host model
Operating System	Operating system type (Windows, Linux or any)
Network name	Current selected host local network name or IP address
Hardware Management	
PAM Domain ID	Current selected host domain name
PAM Name	PAM Manager name
Network Name	Local network name or IP address of the PAP server managing the selected host

Table 4-2. NovaScale 5000 or 6000 Server host properties

Name	Name of the selected host to which commands are applied.
model	Host model
Network Name	Selected host local network name or IP address
Operating System	Operating system type (Windows, Linux or any)
Out-Of-Band information	
Network Name	RMC network name

Table 4-3. Express 5800 Server host properties

Note These values always correspond with those found in the Bull System Manager Configuration.

4.1.2 Commands

Note All commands are applicable to the Host Selected.

4.1.2.1 Prerequisites

NovaScale 3000 Servers

The BMC (Baseboard Management Controller) on the managed host must be configured for remote control over LAN.

NovaScale 4000 Servers

An SMU (System Maintenance Utility) user must be declared for the managed host via the ISM (Intel Server Management) software delivered with NovaScale 4000 servers. User authentication must be declared in the Bull System Manager Configuration.

NovaScale 5000 and 6000 Servers

Bull System Manager Hardware commands are sent to the PAP server for execution. The only prerequisite is that the targeted host is managed by an operational PAP unit accessible from the Bull System Manager server.

NovaScale Blade Servers

Bull System Manager server must be declared as a SNMP Manager in the CMM configuration. For details, please refer to the *NovaScale Blade Chassis Management Module Installation and User's Guide*

NS R400/NS T800/Express 5800 Servers

The BMC (Baseboard Management Controller) on the managed host must be configured for remote control over LAN. This is done using the Intel **SysConfig** tool or **DOS** configuration tool available on the Bull EXPRESSBUILDER CD-ROM delivered with Express 5800 Series servers.

4.1.2.2 Command Outputs

A message indicating command failure or acceptance is displayed.

Power Control

As Power Control operations (except Power Status) are executed asynchronously, the output only indicates if the command is accepted and started. It does not indicate whether the command has been executed or not.

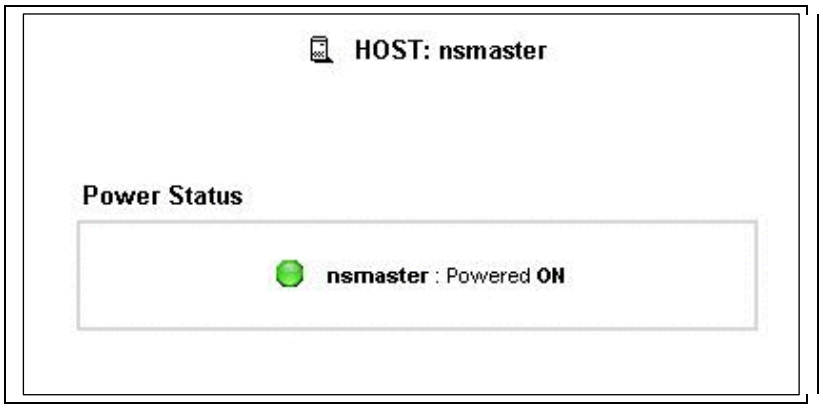


Figure 4-3 Power Status output - example

Note In order for the **power off** command to be taken into account on a remote host running Windows 2000 / 2003 server, the *Shutdown: Allow system to be shut down without having to log on* security option must be enabled on the remote host.

You can configure this security setting by opening the appropriate policy and expanding the console tree as such:

1. Click **Start**, and then click **Run**.
2. In the **Open** box, type **gpedit.msc**, and then click **OK**.
3. In the **Group Policy** window, expand **Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options**.
4. Set the shutdown security option to **enabled**.

FRU

Click **FRU** to display the FRUs (Field Replacement Unit).

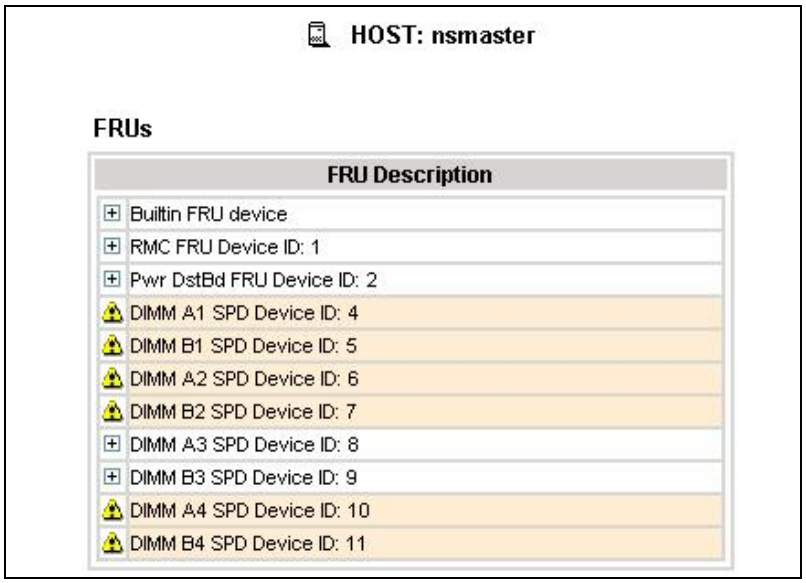


Figure 4-4 FRU output - example

SENSOR

Click **Sensor** to display the sensors.

Note This option is not available for NovaScale 5000, 6000 and Blade series servers.

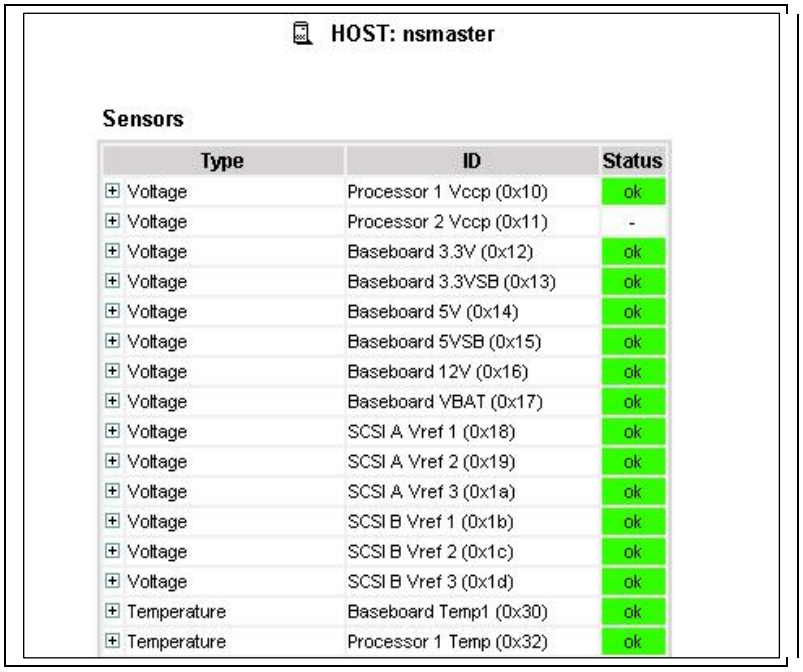


Figure 4-5 SENSOR output - example

SEL/PAM History

Click **SEL** (Express 5800 and NovaScale R400, T800, 3005, 4000 and Blade Series) or **PAM History** (Nova Scale 5000 and 6000 Series) to display the 20 most recent records for the **System Event Log**.

You can view records according to rank, or navigate to the next or previous records, and to view the oldest records.

The **Clear all SEL entries** button is used to clear all the **System Event Log** entries. This functionality is not present in **PAM** history.

Note The **Refresh** button is only enabled when the most recent records are displayed.

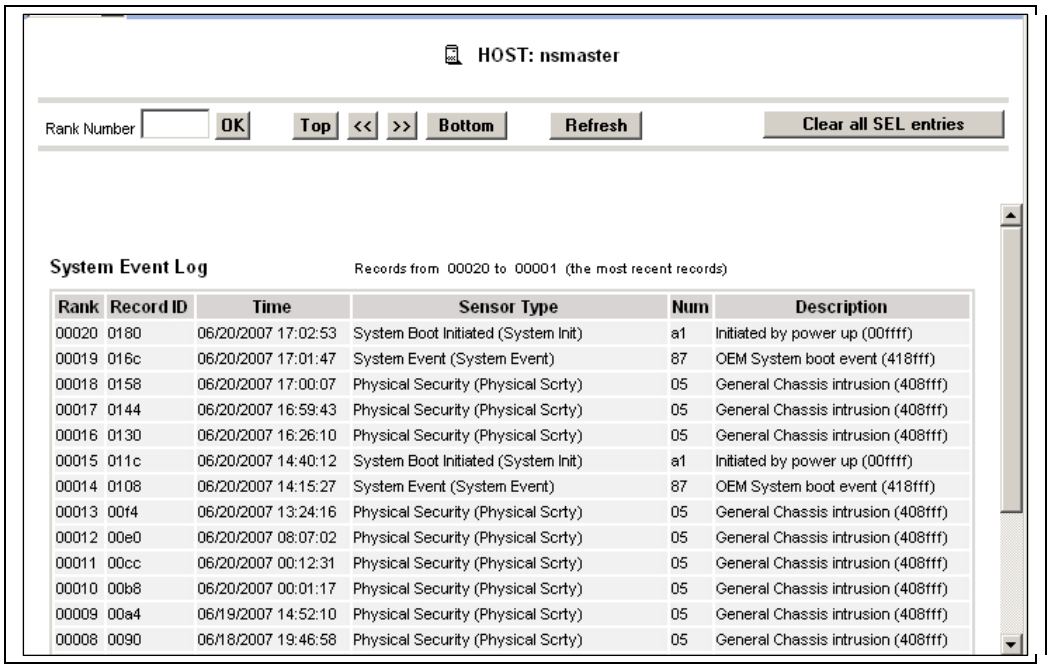


Figure 4-6 SEL output - example

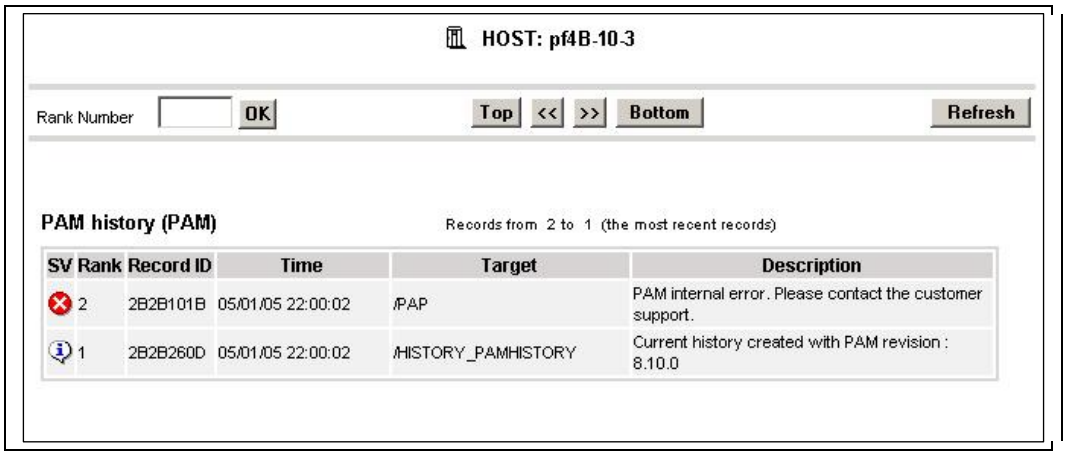


Figure 4-7 PAM History output - example

4.2 Reports

You can visualize the reports associated with these indicators, as follows:

1. Launch the Bull System Manager Console and click the **Reports** button to display the reports available.

2. Click the report required.

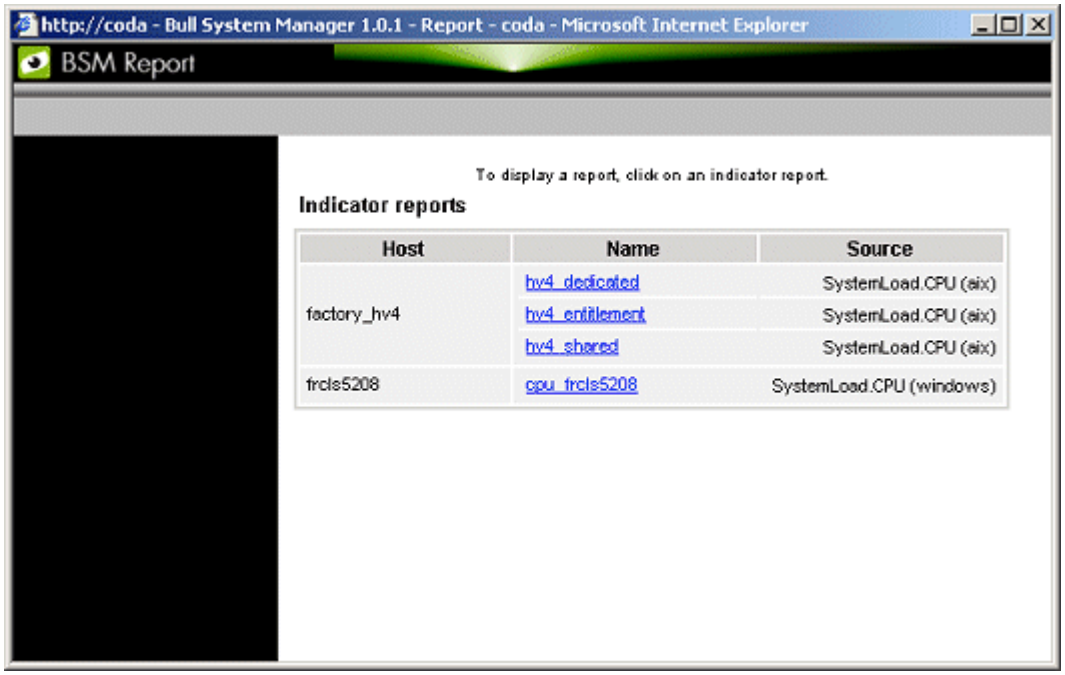


Figure 4-8 Indicator Reports

Each report includes four graphs:

- Daily
- Weekly
- Monthly
- Yearly

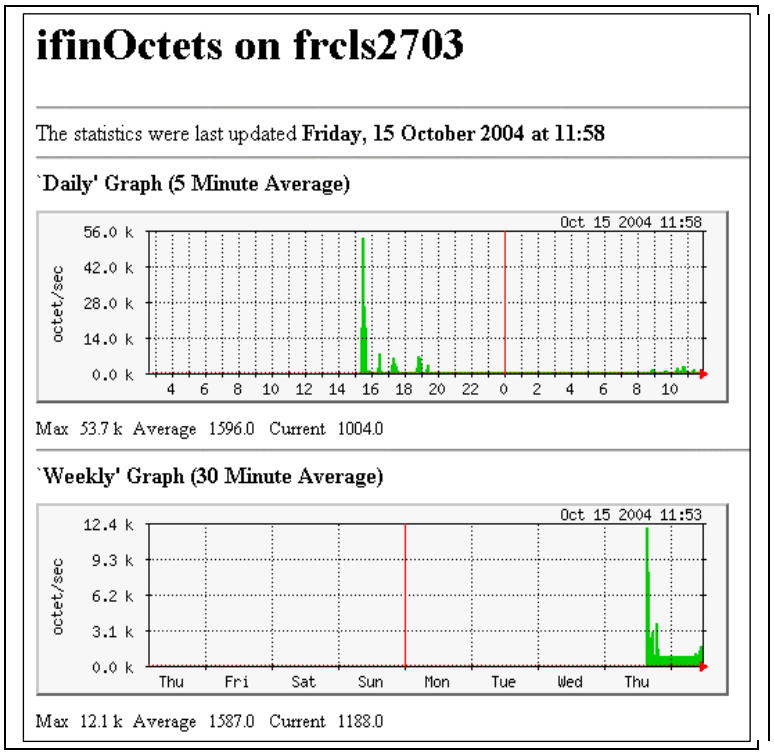


Figure 4-9 Daily and Weekly Report Graphs - example

4.3 Other Applications

You can launch external applications by clicking the appropriate icon in the **Other Tools** Window. Use the arrows to scroll through the list of applications. As the Administrator, you can add external applications. Please refer to the *Administrator's Guide* for details.

Note The **Bull** icon gives you direct access to the Bull Support Web Site.

Figure 4-10 Other applications

Chapter 5. Categories and Services Reference List

This chapter describes the categories and default services for monitoring Linux, AIX or Windows systems.

As the Administrator, you can change, remove or add categories and services to the configuration. Please refer to the *Administrator's Guide* for details.

Notes

- Other Categories and Services are provided by NovaScale Server Add-Ons. They are described in the *Bull System Manager Server Add-ons Installation and Administrator's Guide*.
- A **PING** monitoring service allows you to monitor the presence of a targeted Host. This service is not represented by a service node in the Management tree but is represented in the Applications Window (Monitoring Status Details).

5.1 Monitoring Hosts

The following categories and services can be used to monitor items independently of the OS (network access and protocols for instance). By default, they appear under any declared host.

5.1.1 Internet Category

This category contains all the services for monitoring the IP port (TCP, UDP, HTTP, FTP, etc.).

5.1.1.1 HTTP

The **Internet.HTTP** service monitors the HTTP access of the hosts on port 80 (by default) on the '/' URL (i.e. `http://host:80/`). The timeout value is 10 seconds.

- Status is set to WARNING state for HTTP errors: 400, 401, 402, 403 or 404 such as 'unauthorized access'.
- Status is set to the CRITICAL state if the response time exceeds 10 seconds or for HTTP errors 500, 501, 502 or 503, or if the connection with the server is impossible.

5.1.1.2 HTTP_BSM

The **Internet.HTTP_BSM** service monitors the presence and status of the BSM URL.

5.1.1.3 FTP

The **Internet.FTP** service checks the FTP accessibility on its standard port (21).

- Status is set to the **WARNING** state if the connection is successful, but incorrect response messages are issued from the host.
- Status is set to **CRITICAL** state if the response time exceeds 10 seconds or if the connection with the server is impossible.

5.1.1.4 TCP_n

The **Internet.TCP_n** service monitors TCP access of the hosts for a port.

- Status is set to the **CRITICAL** state if the connection with the server is impossible.

5.1.1.5 UDP_n

The **Internet.UDP_n** service monitors UDP port access of the hosts.

- Status is set to CRITICAL state if the connection with the server is impossible.

5.1.2 Reporting Category

This category contains all the services for monitoring reporting indicators associated with a threshold.

5.1.2.1 Perf_indic

The **reporting.Perf_indic** service monitors defined reporting indicators.

Please refer to the *Administrator's Guide* for details.

5.2 Monitoring Linux or AIX Systems

The following categories and services can be used to monitor Linux or AIX systems. By default, they appear under any host, declared as a Linux or AIX system.

5.2.1 FileSystems Category

This category contains all the services for monitoring file systems.

5.2.1.1 All Service

The **FileSystems.All** service monitors the percentage of used space for each mounted file-system, except CD-ROM and floppy disks.

- Status is set to WARNING if there is at least one file-system with more than 80% space used.
- Status is set to CRITICAL if there is at least one file-system with more than 90% space used.

Status Information

If status is set to WARNING or CRITICAL, Status Information lists the file-systems concerned.

Examples:

```
DISKS OK: all disks less than 80% utilized
DISKS WARNING: /home more than 80% utilized
DISK CRITICAL: ( / ) more than 90% utilized - DISKS WARNING: ( /usr
/var ) more than 80% utilized
```

Correcting Status

- From the **Applications** Window, click **System** (**Detailed Information** box) to get information about host file-system size.
- From the **Applications** Window, click the **Operations** menu and select: **Operating System > FileSystems**.
  You now have access to the host and you can investigate and correct any problems.

5.2.2 LinuxServices Category (for Linux system)

This category contains all the services for checking the presence of Linux daemons.

5.2.2.1 Syslogd Service

The **Syslogd** service checks that there is one and only one **syslogd** process running on the system.

Note	Syslogd is a system utility daemon that provides support for system logging.

- Status is set to WARNING if the number of **syslogd** processes differs from 1.
- Status is only set to CRITICAL when a processing error occurs.

Status Information

Gives the number of processes running with the **syslogd** name.

Example:

```
OK - 1 processes running with command name syslogd
```

Correcting Status

- From the Applications Window, click Processes (Detailed Information box) to obtain the list of processes currently running on the system.
- From the Applications Window, click the **Operations** menu and select: **Operating System > SSH/Telnet**.
  You now have access to the host and can investigate and correct any problems.

5.2.3 AIXServices Category (for AIX system)

This category contains all the services for checking the presence of an **AIX** daemon.

5.2.3.1 Syslogd Service

The **Syslogd** service checks that there is one and only one **syslogd** process running on the system.

Note	Syslogd is a system utility daemon that provides support for system logging.

- Status is set to WARNING if the number of syslogd processes differs from 1.
- Status is only set to CRITICAL when a processing error occurs.

Status Information

Gives the number of processes running with the **syslogd** name.

Example:

```
OK - 1 processes running with command name syslogd
```

Correcting Status

- From the Applications Window, click **Processes** (Detailed Information box) to get the list of processes currently running on the system.
- From the **Applications** Window, click the **Operations** menu and select: **Operating System > SSH/Telnet**.
  You now have access to the host and can investigate and correct any problems.

5.2.4 Syslog Category

This category contains all the services for monitoring the content of the **syslog** files.

5.2.4.1 AuthentFailures Service (for Linux system)

The **AuthentFailures** service monitors the **/var/log/**messages file for the detection of authentication failure messages. It searches for the lines containing: *`authentication failure`* or *`FAILED LOGIN`* or *`Permission denied`*, but not containing *`login.*authentication failure`* (because such a line traps the same error as a **`FAILED LOGIN`** line that has already been detected).

Note Only new lines (if any) are checked each time. If the file has been truncated or rotated since the last check, then the search is started from the beginning.

- Status is set to WARNING if there is at least one new matching line since the last check.
- Status is only set to CRITICAL when a processing error occurs.

Important

The WARNING status can be very transitory in the console.
When a new matching line appears in the log file, status is only set to WARNING during the interval between the check that detects the error and the next check (if no new error appears). You are therefore advised to activate the notification mechanism for this service, and to consult the service history regularly.

Note The **notify_recovery** field is set to **no** because it is not applicable for this service.

Status Information

If status is set to WARNING, **Status Information** gives the number of lines and the last line matching the patterns searched.

Examples:

```
OK - No matches found
(3): Nov 26 15:31:32 horus login[4786]: FAILED LOGIN 3 FROM isis FOR
admin, Authentication failure
```

Note "(3):" indicates that 3 matching lines were found; the text that follows (Nov 26 15:31:32 horus...) includes the last matching line detected.

Correcting Status

- From the **Applications** Window, click the **System Logs** (**Detailed Information**) box to access the content of the **syslog** files for the system. Then click **View** for **/var/log/**messages to consult log file details.
- From the Applications Window, click the **Operations** menu and select: **Operating System > SSH/Telnet**.
  You have now access to the host and can investigate and correct any problems.

5.2.4.2 Errors Service (for AIX system)

The **Syslog.Errors** service monitors the number of error reports generated in the error log over the last 30 minutes (based on the **errpt** command).

- Status is set to WARNING if there is at least one new matching line since the last check.
- Status is only set to CRITICAL when a processing error occurs.

Important

WARNING status can be very transitory in the Console.
When a new matching line appears in the log file, status is only set to WARNING during the interval between the check that detects the error and the next check (if no new error appears). You are therefore advised to activate the notification mechanism for this service, and to consult the service history regularly.

Examples:

```
No new Error Reports since Tue Jan 29 15:02:11 CST 2008
1 New error reports generated since Tue Jan 29 15:02:11 CST 2008
```

Correcting Status

- From the **Applications** Window, click the **Operations** menu and select: **Operating System > SSH/Telnet**.
  You now have access to the host and can investigate and correct any problems.

5.2.4.3 Alerts Service (for Linux and AIX system

The **Alerts** Service is used to collect the hardware SNMP traps emitted by the host.
To enable this service, the **BSM-SYSLOG-MSG.mib** must be integrated in the Bull System Manager application, and SNMP trap reception must be enabled.
At installation time, the MIB is integrated and SNMP trap reception is enabled.
Traps are previously filtered, and only the traps emitted by **SyslogToBsm** on the Bull System Manager agent are used to animate this service. The Bull System Manager agent must be properly configured to send traps to the Bull System Manager_server host.

The status of this service depends on the trap severity:

- Status is set to OK if the trap severity is NORMAL.
- Status is set to WARNING if the trap severity is INFORMATION or WARNING.
- Status is set to CRITICAL if the trap severity is MAJOR or CRITICAL.

5.2.5 SystemLoad Category

This category contains all the services for monitoring system load.

5.2.5.1 CPU Service (for Linux system)

The CPU service monitors the total CPU load over three periods:

- 1 min
- 5 min
- 15 min.

CPU load is computed using the load average given by the **w** command, or in the **/proc/loadavg** file. The Load average is the average number of processes in the system run queue, that is, the number of processes able to run:
(load average / number of CPUs) * 100.

Therefore, CPU load should be equal to 100% when the average of running processes per CPU is 1 (all CPUs are busy).

- Status is set to WARNING if the average CPU load is higher than:
  - 80% over the last 1 minute
  - 70% over the last 5 minutes
  - 60% over the last 15 minutes.

- Status is set to CRITICAL if the average CPU load is higher than:
  - 90% over the last 1 minute
  - 80% over the last 5 minutes
  - 70% over the last 15 minutes.

Status Information

Displays the percentage of average CPU load for the last minute, the last 5 minutes, and the last 15 minutes respectively.

Examples:

```
CPU Utilization: 0% (1mn), 1% (5mn), 0% (15mn)
```

```
CPU Utilization: 86% (1mn), 51% (5mn), 33% (15mn) WARNING
```

Correcting Status

- From the **Applications** Window, click the **Inventory** menu and select: **Operating system > Processes** to get process CPU consumption.
- From the **Applications** Window, click the **Operations** menu and select: **Operating System > Processes**.

You have now access to the host and can investigate and correct any problems.

5.2.5.2 CPU Service (for AIX system)

This CPU service monitors the CPU load of an AIX system or an AIX partition.

The result depends on the partition type: shared (Uncapped or Capped) or dedicated.

- Status is set to WARNING if the average CPU load is higher than 80%.
- Status is set to CRITICAL if the average CPU load is higher than 90%.

Examples:

```
CPU OK - CPU load is 0 (idle:100.0% wait:0.0%) - type=Dedicated partition
CPU OK: Phys CPU load is 0.01 1% of 1 CPU (idle:99.0% wait:0%) - max_vp=2
type=Shared Uncapped partition
```

Correcting Status

- From the **Applications** Window, click on the **Inventory** menu and select: **Operating System > Processes** to get CPU consumption for the processes.
- From the **Applications** Window, click the **Operations** menu and select: **Operating System >** Processes.

You have now access to the host and can investigate and correct any problems.

5.2.5.3 Memory Service (for Linux system)

The **Memory** service monitors the percentage of used memory (physical + swap) for the system.

- Status is set to WARNING if used memory is higher than 70%.
- Status is set to CRITICAL if used memory is higher than 90%.

Status Information

Displays the total (physical + swap) memory size in Mbytes, the total amount of memory used in Mbytes and percent, the total free memory in Mbytes and the physical memory size in Mbytes.

Examples:

```
Status: OK - (total: 2996Mb) (used: 863Mb, 29%) (free: 2132Mb)
(physical: 1004Mb)
Status: WARNING - (total: 1097Mb) (used: 878Mb, 80%) (free: 219Mb)
(physical: 501Mb)
```

Correcting Status

- From the **Applications** Window, click **System** (Detailed Information box) to get memory consumption details.
  Click **Processes** to get information regarding the memory consumption for each process running on the system.
- From the **Tree** Window, display the host pop-up menu and select:
  Remote Operation > Actions, or **Remote Operations > Telnet**

You have now access to the host and can investigate and correct any problems.

5.2.5.4 Processes Service (for Linux system)

The Processes service monitors the number of processes running on the system.

- Status is set to WARNING if the number of processes is higher than 150.
- Status is set to CRITICAL if the number of processes is higher than 200.

Status Information

Displays the number of processes running on the system.

Examples:

```
OK - 101 processes running
WARNING - 162 processes running
```

Correcting Status

- From the **Applications** Window, click **Processes** (Detailed Information box) to get the list of the processes.
- From the **Applications** Window, click the **Operations** menu and select:
  Operating System > Processes
  You have now access to the host and can investigate and correct any problems.

5.2.5.5 Users Service (for Linux system)

The Users service monitors the number of users currently logged onto the system.

- Status is set to WARNING if the number of connected users is higher than 15.
- Status is set to CRITICAL if the number of connected users is higher than 20.

Status Information

Displays the number of users logged onto the system.

Examples:

```
USERS OK - 2 users currently logged in
USERS WARNING - 16 users currently logged in
```

Correcting Status

- From the **Applications** Window, click **Processes** (Detailed Information box) to get information on users running processes.
- From the **Tree** Window, display the host pop-up menu and select:
  Remote Operation > Actions or **Remote Operation > Telnet**
  You have now access to the host and can investigate and correct any problems.

5.2.5.6 PagingSpace Service (for AIX system)

The **PagingSpace** service monitors the current system paging space in relation with **paging space in** and **paging space out** parameters.

- Status is set to WARNING if the paging space used is higher than 80%.
- Status is set to CRITICAL if the paging space used is higher than 90%.

Example:

```
OK - Used paging space 0.72 % : paging-ins 0.00 pg/s paging-outs : 0.00 pg/s
```

Correcting Status

- From the **Applications** Window, click the **Operations** menu and select:
  Operating System > SSH/Telnet.

You have now access to the host and can investigate and correct any problems.

5.2.5.7 Swap Service (for AIX system)

The **Swap** service monitors the current swap space for the system.

- Status is set to WARNING if the swap space used is higher than 50%.
- Status is set to CRITICAL if the swap space used is higher than 80%.

Examples:

```
Swap ok - Swap used: 0% (5 out of 512)
```

Correcting Status

- From the **Applications** Window, click the **Operations** menu and select: **Operating System > SSH/Telnet**.

You have now access to the host and can investigate and correct any problems.

5.3 Monitoring Windows Systems

The following categories and services can be used to monitor Windows systems. By default, they appear under any host, declared as a Windows system.

Notes

- The Windows monitoring agent part is based on two Windows services:
  - **Bull System Manager Management agent**
    Its main function is to provide OS and HW information, but it also provides the **LogicalDisk.All** monitoring service.
  - **Bull System Manager Monitoring agent**
    This provides all the Windows monitored services, except **LogicalDisk.All**.

5.3.1 EventLog Category

This category contains all the services for monitoring the Windows Event Log.

5.3.1.1 Application Service

The **EventLog.Application** service monitors the number of Error, Warning and Information events generated in the Application Event log for the last 300 minutes.

- Status is set to WARNING if there are more than 10 Information events or at least 1 Warning event.
- Status is set to CRITICAL if there is at least 1 Error event.

Status Information

If the status is set to WARNING or CRITICAL, the number of events for the status are indicated. This message includes a link to an html file that contains the following detailed information:

Event Type	Error or Warning or Information
Last Time	Last time an event with the same type, source and id occurred
Count	Number of events with the same type, source and id
Source	Event source
Id	Event id
Description	Event message

Examples:

```
OK: no new events for the last 30 mn
WARNING: 1 new events for the last 30 mn!
```

The text "`1 new events for the last 30 mn!`" is a link that displays detailed information:

Correcting Status

- From the **Applications** Window, click **Events** (Detailed Information box) for more information.
- From the **Applications** Window, click the **Operations** menu and select: **Operating System > VNC Viewer** or **Remote Desktop**.
  You now have access to the host and can investigate and correct any problems.

5.3.1.2 Security Service

The **EventLog.Security** service monitors the number of Audit Success, Audit Failures, Error and Warning events generated in the Security event log for the last 30 minutes.

- Status is set to WARNING if there are more than 10 Audit Success events or at least 1 Warning event.
- Status is set to CRITICAL if there is at least 1 Audit Failure or Error event.

Status Information

If the status is set to WARNING or CRITICAL, the number of events for the status are indicated. This message includes a link to an html file that contains the following detailed information:

Event Type	Error, Warning, Information, Audit Success or Audit Failure
Last Time	Last time an event with the same type, source and id occurred
Count	Number of events with the same type, source and id
Source	Event source
Id	Event id
Description	Event message

Examples:

```
OK: no new events for the last 30 mn
WARNING: 4 new events for the last 30 mn!
```

Correcting Status

- From the **Applications** Window, click **Events** (Detailed Information box) for more information.
- From the **Applications** Window, click the **Operations** menu and select: **Operating System > VNC Viewer** or **Remote Desktop**.
  You now have access to the host and can investigate and correct any problems..

5.3.1.3 System Service

The **EventLog.System** service monitors the number of Error, Warning and Information events generated in the System event log over the last 300 minutes.

- Status is set to WARNING if there are more than 10 Information events or at least 1 Warning event.
- Status is set to CRITICAL if there is at least 1 Error event.

Status Information

If the status is set to WARNING or CRITICAL, the number of events for the status are indicated. This message includes a link to an html file that contains the following detailed information:

Event Type	Error, Warning or Information
Last Time	Last time an event with the same type, source and id occurs
Count	Number of events with the same type, source and id
Source	Event source
Id	Event id
Description	Event message

Examples:

```
OK: no new events for the last 30 mn
CRITICAL: 8 new events for the last 30 mn!
```

Correcting Status

- From the **Applications** Window, click **Events** (Detailed Information box) for more information.
- From the **Applications** Window, click the **Operations** menu and select: **Operating System > VNC Viewer** or **Remote Desktop**.
  Your now have access to the host and can investigate and correct any problems.

5.3.2 LogicalDisks Category

This category contains all the services for monitoring the logical disks.

5.3.2.1 All Service

The **All Service** monitors the percentage of used space for each local disk. The local disks list is dynamically established at each check.

- The status is set to WARNING if one of the disks has more than 80% space used.
- The status is set to CRITICAL if one of the disks has more than 90% space used.

Status Information

List the local disks checked.

Examples:

```
DISKS OK: all disks (C:, E:, F:) less than 80% utilized
DISK WARNING: (G:) more than 90% utilized - DISKS CRITICAL: (C:) more
than 80% utilized
```

Correcting Status

- From the **Applications** Window, click **Logical Disks** (Detailed Information box) to get all information about the size of the host disks. Then click **Storage** to get information on the physical storage devices for the host.
- From the **Applications** Window, click the **Operations** menu and select: **Operating System > VNC Viewer** or **Remote Desktop**.
  You now have access to the host and can investigate and correct any problems.

5.3.3 SystemLoad Category

This category contains all the services for monitoring the load for the system.

5.3.3.1 CPU Service

The CPU service monitors the total CPU load over two times: 1 minute and 10 minutes

- Status is set to WARNING if the average CPU load is higher than:
  - 80% over the last 1 minute
  - 60% over the last 10 minutes
- Status is set to CRITICAL if the average CPU load is higher than:
  - 90% over the last 1 minute
  - 80% over the last 10 minutes

Status Information

Displays the average CPU load percentage for the previous minute, and for the last 10 minutes. If the status is WARNING or CRITICAL, it displays the process with the highest CPU usage, with the percentage of use, for the check.

Examples:

```
CPU Load OK (1mn: 8%) (10mn: 5%)
CPU Load HIGH (1mn: 92%) (10mn: 56%) - Process cputest.exe using 100%
```

Correcting Status

- From the **Applications** Window, click **CPU** (Detailed Information box) to get CPU usage per processor. Then click **Processes** to get CPU time spent per process.
- From the **Tree** Window, display the host pop-up menu and select:
  Remote Operation > VNC Viewer or **Remote Operation > Telnet**.
  You have now access to the host and can investigate and correct any problems.

5.3.3.2 MemoryUsage Service

The **MemoryUsage** service monitors the total memory (physical + paged) used by the system. It is equivalent to the Commit Charge displayed in the Windows Task Manager.

- Status is set to WARNING if the memory used is higher than 70%.
- Status is set to CRITICAL if the memory used is higher than 90%.

Status Information

Displays the total (physical + paged) memory size in Mbytes, the total memory used in Mbytes and percentage, the total free memory in Mbytes and the physical memory size in Mbytes.

Examples:

```
Memory Usage OK - (total: 1480Mb) (used: 193Mb, 13%) (free: 1287Mb)
(physical: 511Mb)
Memory Usage WARNING - (total: 2462Mb) (used: 1773Mb, 72%) (free:
689Mb) (physical: 1023Mb)
```

Correcting Status

- From the **Applications** Window, click **Memory** (Detailed Information box) to get details of memory use.
  Then click **Processes** to get memory used per process.
  Then click **General** (Host Information box) to get information about the physical memory configuration and layout.
- From the **Applications** Window, click the **Operations** menu and select:
  Operating System > VNC Viewer or **Remote Desktop**.
  You have now access to the host and can investigate and correct any problems.

5.3.4 WindowsServices Category

5.3.4.1 EventLog Service

The **WindowsServices.EventLog** service monitors the state of the services involved in event logging functions:

Service Key	Display Name	Description
Eventlog	Event Log	Log event messages issued by programs and Windows. Event Log Reports contain information that can be useful in diagnosing problems. Reports are viewed in Event Viewer

- Status is set to WARNING if at least one of these services is paused and the others are running.
- Status is set to CRITICAL if at least one of these services does not exist or is not running.

Status Information

Displays service name and status.

Examples:

```
OK: 'EventLog'
NotActive: 'EventLog'
```

Correcting Status

- From the **Applications** Window, click **Memory** (Detailed Information box) to get detailed information about services.
- From the **Applications** Window, click the Operations menu and select: **Operating System > VNC Viewer** or **Remote Desktop**.
  You have now access to the host and can investigate and correct any problems.

5.4 Hardware Monitoring

5.4.1 Hardware Category for Express 5800

5.4.1.1 PowerStatus Service

The **PowerStatus** service indicates the power status of an Express 5800 server, as returned by the RMC management card.

- Status is set to CRITICAL if RMC has returned a power status off.
- Status is set to UNKNOWN if RMC is not accessible or if RMC has not been able to calculate the power status.

Correcting Status

- From the Tree Window, display the host pop-up menu and select RMC to launch the CMM tool and investigate and correct any problems.

Note For more information about RMC, please refer to the documentation delivered with your server.

5.4.1.2 Alerts Service

The **Alerts** Service is used to collect the hardware SNMP traps emitted by the manager.

This service uses the **bmclanpet** MIB, integrated in the Bull System Manager application. **SNMP** trap reception must be enabled.

The Hardware Management card must be correctly configured to send traps to the Bull System Manager_SERVER host.

The status of this service depends on trap severity:

- Status is set to OK if trap severity is NORMAL.
- Status is set to WARNING if trap severity is INFORMATION or WARNING.
- Status is set to CRITICAL if trap severity is MAJOR or CRITICAL.

As the Administrator, you can display and edit trap severity using the Configuration application. Please refer to the *Administrator's Guide* for details.

5.4.2 Hardware Category for NovaScale 3000 Series

5.4.2.1 PowerStatus Service

The **PowerStatus** service reflects the power status of a NovaScale server, as returned by the management card.

- Status is set to CRITICAL if the cardName has indicated a power off status.
- Status is set to UNKNOWN if the cardName is not accessible or if the cardName has not been able to obtain a power status.

5.4.2.2 Alerts Service

The **Alerts** Service is used to collect the SNMP traps for the hardware emitted by the manager.

This service uses the **bmclanpet** and **SMSmp** MIBs integrated in the Bull System Manager application. SNMP trap reception must be enabled.

The Hardware Management BMC must be correctly configured to send traps to the Bull System Manager_SERVER host.

The status of this service depends on trap severity:

- Status is set to OK if trap severity is NORMAL.
- Status is set to WARNING if trap severity is INFORMATION or WARNING.
- Status is set to CRITICAL if trap severity is MAJOR or CRITICAL.

As Administrator, you can display and edit trap severity using the Configuration tool. Please refer to the *Administrator's Guide* for details.

5.4.3 Hardware Category for NovaScale T800 & R400 Series

5.4.3.1 PowerStatus Service

The **PowerStatus** service reflects the power status of a NovaScale server, as returned by the management card.

- Status is set to CRITICAL if the cardName has assigned a power off status.
- Status is set to UNKNOWN if the cardName is not accessible or if the cardName has not been able to obtain the power status.

5.4.3.2 Alerts Service

The **Alerts** Service is used to collect the SNMP traps for the hardware emitted by the manager.

To enable this service, the **bmclanpet** MIB must be integrated in the Bull System Manager application. SNMP trap reception must be enabled.

At installation time, the **MIB** is integrated and SNMP trap reception is enabled.

The Hardware Management BMC must be correctly configured to send traps to the Bull System Manager_SERVER host.

The status of this service depends on trap severity:

- Status is set to OK if trap severity is NORMAL.
- Status is set to WARNING if trap severity is INFORMATION or WARNING.
- Status is set to CRITICAL if trap severity is MAJOR or CRITICAL.

As Administrator, you can display and edit trap severity using the **Configuration** application. Please refer to the *Administrator's Guide* for details.

5.4.4 Hardware Category for NovaScale 4000 Series

5.4.4.1 Alerts Service

The **Alerts** Service is used to collect the hardware SNMP traps emitted by the host.
To enable this service, the **basebrd5** MIB must be integrated in the Bull System Manager application and SNMP trap reception must be enabled.
At installation time, the MIB is integrated and SNMP trap reception is enabled.
Traps are previously filtered and only the traps emitted by the Hardware Management card are used to animate this service. The Hardware Management card must be properly configured with the Intel SMU tool to send traps to the Bull System Manager_server host.

The status of this service depends on trap severity:

- Status is set to OK if trap severity is NORMAL.
- Status is set to WARNING if trap severity is INFORMATION or WARNING.
- Status is set to CRITICAL if trap severity is MAJOR or CRITICAL.

As Administrator, you can display and edit trap severity through the Configuration application. Please refer to the *Administrator's Guide* for details.

Status Information

Trap description, as found in the trap MIB, is used as to indicate the status.

Example:

```
Trap systemHealthCriticalEvent – Server Health Critical: The overall
health of the server is critical
```

Correcting Status

From the Tree Window, display the host pop-up menu and select the HW Manager GUI to launch the ISM tool and investigate and correct any problems.

Note For more information about ISM, please refer to the documentation delivered with your server.

5.4.4.2 PowerStatus

The **PowerStatus** service reflects the power status of a NovaScale server, as indicated by the management card.

- Status is set to CRITICAL if the cardName has assigned an off power status.
- Status is set to UNKNOWN if the cardName is not accessible or if the cardName has not been able to obtain the power status.

5.4.4.3 Health Service

The **Health** service monitors hardware status, as returned by the Intel System Management (ISM) software tool.
To enable this service, a manager must be declared for the host (see the *Administrator's Guide* for details about how, as Administrator, you can declare a manager) and ISM must be installed and running on that manager.

Health is an ISM indicator that reflects the global state of hardware. The hardware components taken into account in Health can be configured in the ISM tool.

- Status is set to WARNING if the status of one of the hardware components described as a contributor to Health is in the WARNING state.
- Status is set to CRITICAL if the status of one of the hardware components described as a contributor to Health is in the CRITICAL state.

Correcting Status

From the **Tree** Window, display the host pop-up menu and select:
HW Manager GUI to launch the ISM tool, to investigate and correct any problems.

5.4.5 Hardware Category for NovaScale 5000 & 6000 Series

5.4.5.1 Health Service

The **Health** service monitors hardware status, as returned by the **PAM** software tool, for the host (or PAM domain).

To enable this service, a manager must be declared for the host (see the *Administrator's Guide* for details about how, as Administrator, you can declare a manager) and a **PAP** server must be installed and running on that manager.

- Status is set to WARNING if PAM has assigned a WARNING status to the domain.
- Status is set to CRITICAL if PAM has assigned a CRITICAL status to the domain.
- Status is set to UNKNOWN if PAM is not accessible or if PAM has not successfully computed domain status.

Status Information

Status information is set by PAM and represents host hardware status.

Example:

```
For the Domain FAME000_0ID0 of the CentralSubSystem FAME000, the functional
status is NORMAL (The domain state is "BIOS READY - STARTING EFI)
```

Correcting Status

From the **Tree** Window, display the host pop-up menu and select:
PAM to launch the PAM tool to investigate and correct any problems.

Note For more information about PAM, see the documentation delivered with your server.

5.4.6 Hardware Category for NovaScale 9006 Series

5.4.6.1 Alerts Service

5.4.6.2 PowerStatus Service

The **PowerStatus** service reflects the power status of a NovaScale server, as returned by the management card.

- Status is set to CRITICAL if the cardName has assigned an off power status.
- Status is set to UNKNOWN if the cardName is not accessible or if the cardName has not been able to obtain the power status.

5.4.6.3 PowerConsumption Service

5.4.7 Hardware Category for Blade Series

5.4.7.1 Health Service

The **Health** service monitors hardware status, as returned by the CMM software tool.

To enable this service, a CMM manager must be declared for the host and the hardware identifier (used to identify the host in the NovaScale Blade Chassis) must be provided when Bull System Manager is configured. Please refer to the *Administrator's Guide* for details.

- Status is set to WARNING if CMM has assigned a WARNING status to the host.
- Status is set to CRITICAL if CMM has assigned a CRITICAL status to the host.
- Status is set to UNKNOWN if CMM is not accessible or if the host has not been successfully mapped in the chassis (due, for example, to an incorrect hardware identifier).

Status Information

Status information is set by CMM and represents the host hardware status.

Examples:

```
Current status:       OK
Status Information    No critical or warning events
```

The hardware state of the host is OK.

```
Current status:       CRITICAL
Status information:   DASD Removed.
```

The hardware state of the host is CRITICAL.

```
Current status:       unknown
Status information:   Unable to get SNMP response [No response from
remote host '192.168.207.46'
```

The hardware state cannot be retrieved from the CMM manager due to a connection timeout. This issue can result from a bad declaration of the SNMP Manager in the CMM configuration.

Correcting Status

From the Tree Window, display the host pop-up menu and select HW Manager GUI, and then launch the CMM tool. This investigates any problems and will help to correct them.

Note For more information about CMM, please refer to the documentation delivered with your server.

5.4.8 Hardware Categories for Escala Servers

5.4.8.1 CECStatus Service

The **CECStatus** service monitors the **CEC** status, as returned by the **HMC** system.
To enable this service, the Escala server must be declared as a managed element of an HMC (see the *Administrator's Guide* for details about how, as Administrator, you can declare an HMC and systems it manages).

- Status is set to OK if the CEC status given by HMC has one of the following states: **Running**, **Operating**
- Status is set to WARNING if the CEC status given by HMC has one of the following states:
  Not Activated, Starting, Shutting Down, Initializing Standby, On Demand Recovery, Recovery, Version Mismatch, Open Firmware, Pending authentication, Failed authentication, Power Off, Power Off In Progress, Service Processor Failover In Progress.
- Status is set to CRITICAL if the CEC status given by HMC has one of the following states:
  No Connection, Incomplete, Error, Error - Dump in Progress, Error - Terminated, Not Available.

5.4.8.2 Events

The **Events** service monitoring is based on hardware events reported by the HMC for the server.

The status of this service depends on trap severity:

- Status is set to OK if no hardware event is reported for the server
- Status is set to WARNING if at least one hardware event is reported for the server.

5.5 Blade Monitoring

5.5.1 CMM Category

5.5.1.1 ChassisStatus Service

The **ChassisStatus** service reflects the functional status of the NovaScale Blade Chassis, as returned by the CMM manager. This state comprises the hardware status of the whole configuration managed by this CMM, as well as the status of the CMM manager itself.

This service exists only on a host that is declared as a CMM manager (see the *Administrator's Guide* for details about how, as Administrator, you can declare a manager).

- Status is set to WARNING if CMM has assigned a WARNING status to the host.
- Status is set to CRITICAL if CMM has assigned a CRITICAL status to the host.
- Status is set to UNKNOWN if CMM is not accessible or if CMM has not been able to compute global status.

Correcting Status

From the Tree Window, display the host pop-up menu and select HW Manager GUI, and then launch the CMM tool. This investigates any problems and will help to correct them.

Note For more information about CMM, please refer to the documentation delivered with your server.

5.5.1.2 Alerts Service

The **Alerts** Service is used to collect the hardware SNMP traps emitted by the manager. To enable this service, the **mmalert** MIB must be integrated in the Bull System Manager application and SNMP trap reception must be enabled.
At installation time, the MIB is integrated and SNMP trap reception is enabled.
The Hardware Management card must be correctly configured to send traps to the Bull System Manager_SERVER host.

The status of this service depends on trap severity:

- Status is set to OK if trap severity is NORMAL.
- Status is set to WARNING if trap severity is INFORMATION or WARNING.
- Status is set to CRITICAL if trap severity is MAJOR or CRITICAL.

As Administrator, you can display and edit trap severity through the Configuration application. Please refer to the *Administrator's Guide* for details.

5.6 Storage and Virtualization Monitoring

See document *BSM Server Addons Guide* (Bull REF: 86A259FA) for more information about the storage and/or virtualization monitoring services.

Index

/

/proc/loadavg file 101

/var/log/messages file 99

A

alerts 20

Alerts 16

alerts mode 53

Alerts service..... 101, 112, 113, 114, 117, 119

All Service (Linux) 97

All service (Windows) 109

Animation
  colors 39
  rules 39

Animation menu 43

Animation menu 40, 42

Animation menu 44

Animation menu 44

Animation menu 44

Animation menu 45

Animation menu 46

Application Service..... 106

ARMC 3

AuthentFailures service 99, 100

C

Category
  AIXServices 98
  definition 5
  Internet 95
  LinuxServices 98
  Reporting 96

Change Password menu 83

ChassisStatus service..... 119

CMM 3
  hardware manager 28, 82

CMM category..... 119

CMM manager menu 43

Color
  host icon 13
  service icon 12

console
  starting 9

console applications..... 85

console supervision modes 37

CPU service (AIX) 102

CPU service (Linux)..... 101

CPU service (Windows) 109

Create a new user..... 27

D

Diagnosis menu 40, 45

E

EventLog category..... 106

EventLog service..... 111

Expand menu 42, 43, 44, 45

ExpressScope
  hardware manager..... 28

F

File
  /var/log/messages..... 99

FileSystem menu..... 83

FileSystems category..... 97

FTP service 96

H

Hardware category (Express 5800) 112

Hardware category (NovaScale 3000) 113

Hardware category (NovaScale 4000) .. 114, 117

Hardware category (NovaScale 5000 & 6000) 116

Hardware category (NovaScale Blade) 117

Hardware Category (NovaScale T800 & R400) 113
hardware management..... 28
hardware management application..... 85
Hardware Manager
PAM, ISM, CMM, ExpressScope..... 28
Health service..... 115, 116, 117, 118
History 15
HTTP service 95
HTTP_NSMaster service..... 95

I

Intel based computers
RMC 82
RMC or AMRC..... 28
inventory information..... 75
IPMItool 7
ISM
hardware manager..... 28, 82

L

LogicalDisks category..... 109

M

Management Tree
presentation..... 37
management tree views 47
map mode 52
Memory service 103
MemoryUsage service 110
mode
alerts 53
map 52
tree 37
modes
console supervision..... 37
monitoring information 12
MRTG 7

N

Nagios 7
Network Configuration menu 83
Node
definition 37
notify_recovery parameter 99
NovaScale 4000
ISM 28, 82
NovaScale 5000
PAM 28, 82
NovaScale 6000
PAM 28, 82
NovaScale Blade Series
CMM 28, 82

O

Off menu 40, 45
On menu 40, 46
Open Source
Webmin 26
Operations
UsersActions / Users 26
VNC Viewer 24

P

PagingSpace service.....104
PAM 3, 4
hardware manager 28, 82
PAM manager menu 43
Perf_indic service.....96
performance indicator.....33
Ping command 2
PowerStatus service 113
Processes menu 83
Processes service 103

R

remote control 24
Remote control
VNC Viewer 24
Webmin 26
Remote Desktop.....83
Reporting category 96

reports 74, 92
RMC
hardware manager 28, 82
Root node 42
RPM Products menu..... 83

S

Security Service 107
server control 35
Service
definition 5
Perf_indic96
PowerStatus..... 112
Service state
color 12
Shell Command menu 83
SSH 83
starting the console 9
Status
ISM, ESMPRO 43
service 46
Status Trends for this service..... 17
supervision information..... 10, 57
Swap service..... 105
Syslog category..... 99
Syslogd service 98
System Logs menu..... 83
System service..... 108
SystemLoad category 101, 109

T

TCP_n service 96
telnet 26
Telnet 3
Telnet menu 83
Threshold 2
tree mode 37
Trends 16

U

UDP_n service..... 96
UltraNC Viewer 24
UltraVNC 3
UltraVNC Server 7
Users menu 83
Users service 104

V

View 3
default 47
definition 6
VNC Viewer
password25
VNC Viewer menu 83

W

Webmin 3, 7, 26
password27
WindowsServices category 111

BULL CEDOC
357 AVENUE PATTON
B.P.20845
49008 ANGERS CEDEX 01
FRANCE

REFERENCE
86 A2 55FA 03