Bull System Manager

BSM 2.4

User's Guide

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 and/or patent misuse.

Table of Contents

Preface

This guide explains how to monitor and manage Bull systems using Bull System Manager, and in particular via the Bull System Manager Console.

Note	You are advised to consult the Bull Support Web site for the most up-to-date product information, documentation, firmware updates, software fixes and service offers: http://support.bull.com

Intended Readers

This guide is intended for use by System Operators.

Highlighting

The following highlighting conventions are used in this guide:

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

```
Commands entered by the user
```

```
System messages displayed on the screen
```

⚠️ **WARNING**

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

Related Publications

- *BSM Installation Guide*, 86 A2 54FA
  explains how to install the Bull System Manager solution for monitoring and managing Bull systems. This guide is intended for use by System Administrators.

- *BSM Administrator's Guide*, 86 A2 56FA
  explains how to customize Bull System Manager to monitor specific environments. This guide intended for use by System Administrators.

- *BSM User's Guide*, 86 A2 55FA
  explains how to monitor and manage Bull systems using Bull System Manager, and in particular via the Bull System Manager Console. This guide is intended for use by System Operators.

- *BSM Remote Hardware Management CLI Reference Manual,* 86 A2 58FA
  describes the Hardware Management CLI (Command Line Interface) for Bull systems.

- *BSM Server Add-ons - Installation Guide*, 86 A2 59FA
  Bull System Manager Server Add-ons provide extensions for Bull System Manager to monitor specific system devices or products. This guide is intended for use by System Administrators.

- *Release Notes,* 86 A2 57FA
  describe the contents, system requirements, installation instructions, and known issues (with workarounds, where applicable) for the current Bull System Manager release.

Chapter 1. Bull System Manager Overview

Bull System Manager (BSM) is designed to simplify the management of Bull servers and external devices, including storage subsystems and switches.

It provides a single point of control for the integrated management of Bull servers and external devices, allowing administrators to see alerts quickly and to take the appropriate actions, thereby enhancing system availability and performance.

Bull System Manager integrates Open Source software, including **Nagios** and uses standard network protocols including **SNMP**, **CIM/WBEM** and **IPMI**.

1.1   Architecture

Based on a 3-tier architecture, Bull System Manager includes:

Management Console	installed on each end-user station (Windows or Linux)
Management Server and **Add-ons**	installed on the management server(s) (Windows or Linux)
Management Agents	**installed** on each managed hardware platform (Windows or Linux or AIX)
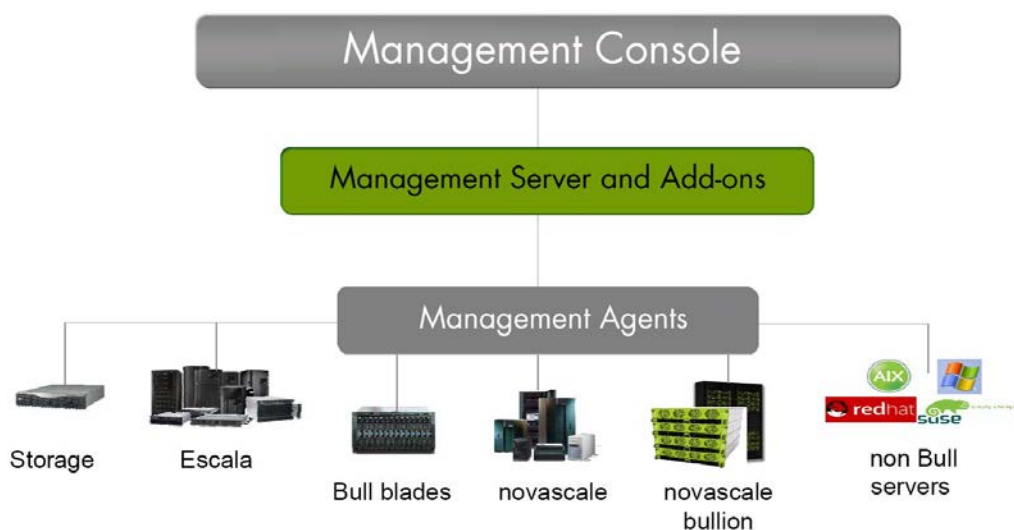
For large infrastructures, a distributed monitoring solution can be implemented allowing an overall view of managed system status via a Global Management Console. For more information, contact your Bull Customer Representative.

Bull System Manger is also delivered with a Hardware Management CLI package, providing an easy Command Line Interface (CLI) for local or remote hardware management and automation scripts.

A description of the key components and concepts for **BSM** is given in the *Glossary*.

1.1.1 Management Console

The Management Console is a web-based Graphical User Interface compatible with **Internet Explorer** and/or **FireFox**. **The Management Console allows you to graphically view, monitor and manage all the hosts configured for administration by the associated Management Server**.

If a distributed monitoring solution is implemented, a Global Management Console allows you to graphically view, monitor and manage all the hosts configured for administration on a set of Management Servers.
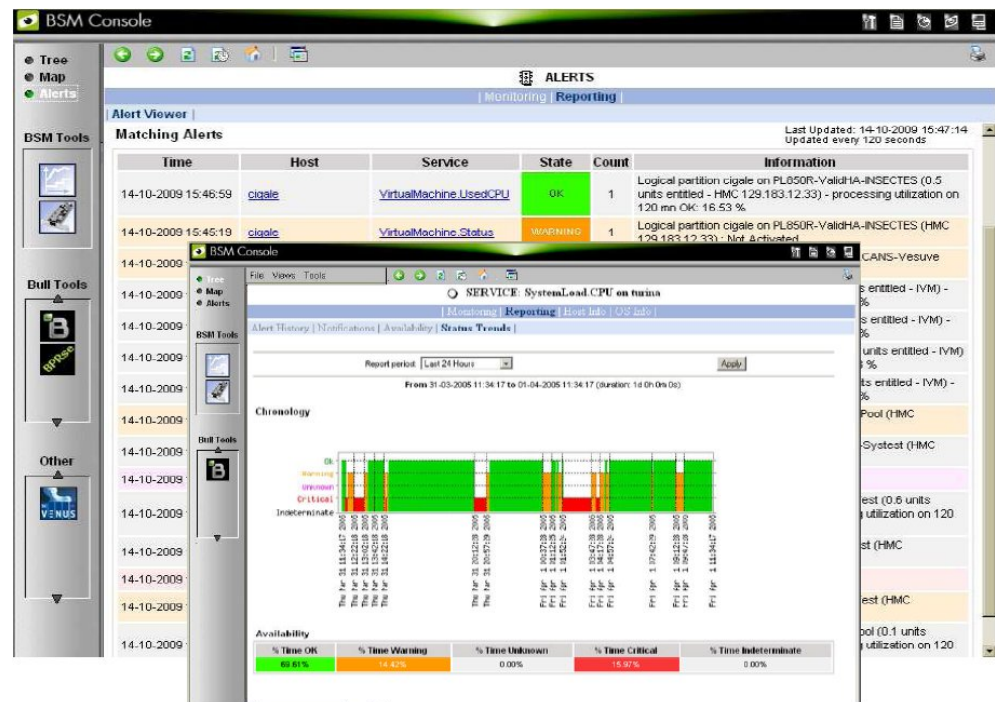
The Management Console provides access to the **Configuration GUI**, used to configure the monitoring of hosts, and to the **Control GUI**, used to stop and start the Management Server.

See The *BSM Administrator's Guide* for more details regarding the Configuration GUI and Control GUI.

1.1.2 Management Server

The **Management Server** provides the infrastructure and services required to collect, process and store operational and monitoring data.

Dedicated Add-ons provide extensions to Bull System Manager to manage specific devices or tools.

1.1.3 Management Agent

The **Management Agent** consists of the instrumentation and administration tools used to obtain monitoring and inventory information. The Management Agent is system specific and must be installed on each target server to be monitored by BSM.

1.1.4 Hardware Management CLIs

The **Hardware Management Command Line Interface** (CLI) package can be used for remote hardware management tasks including:

- Powering on/off

- Obtaining power status details

- Monitoring hardware components

- Inventory purposes for hardware, partition and module details

- Hardware discovery and topological verification

- Configuration and Maintenance

    – Updating firmware
    – Managing CPU allocation
    – Creating and modifying partitions
    – Configuring platform modules
    – Allowing a Support Online connection to be made

1.2 Features

Bull System Manager offers the following features:

- Monitoring

- Reporting

- Alerting

- Remote Operations and Inventory

1.2.1 Monitoring

The servers and external devices to be monitored are either explicitly specified by the Administrator or detected by a discovery mechanism:

- Specific elements and services such as **Power status**, **CPU load, memory usage, disk usage, number of users, processes** and **service execution, http** and **ftp services** can be monitored. When an anomaly occurs or when normal status is recovered, **alerts** (in a log file) and **notifications** (by e-mail, by Bull auto-call and/or by **SNMP** trap) are generated.

- Status thresholds (**OK, WARNING, CRITICAL, UNKNOWN**) can be defined for each element monitored.

- Monitored hosts and services can be grouped into entities that reflect your environment so that you can easily identify an anomaly for these entities.

- Instantiated services can be grouped into specific functional domains so that you can display monitoring information for that domain only.

Monitoring is based on communication with management modules embedded on the hardware.

1.2.2 Reporting

All events generated by the Operating Systems and hardware managers are automatically recorded.
The data is accessible in a graph format for a defined period so that system changes, such as load, can easily be detected.

1.2.3 Alerting

When hardware or software thresholds are reached, when an anomaly occurs **(alerts** in a log file), or when normal status is recovered, the Administrator is notified automatically by e-mail, or by Bull autocall and/or by SNMP traps:

E-mail Notification

A **Mail server** is needed to relay e-mails. E-mail notifications are sent to all the **Contacts** in a **Contactgroup**.

Bull Autocall Transmission

The **Autocall server** must be configured to define the **GTS** server that will relay autocalls to the Bull maintenance site.

SNMP Trap Alerting

The **SNMP manager** must be configured to define **SNMP** trap receivers.

1.2.4 Remote Operations

Remote Operation is used to configure target hosts and execute actions on these hosts via the Operating System or via Remote Hardware Management CLIs.

1.2.5 Inventory

The Inventory is used to display hardware and software information for hosts.

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 7* 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.

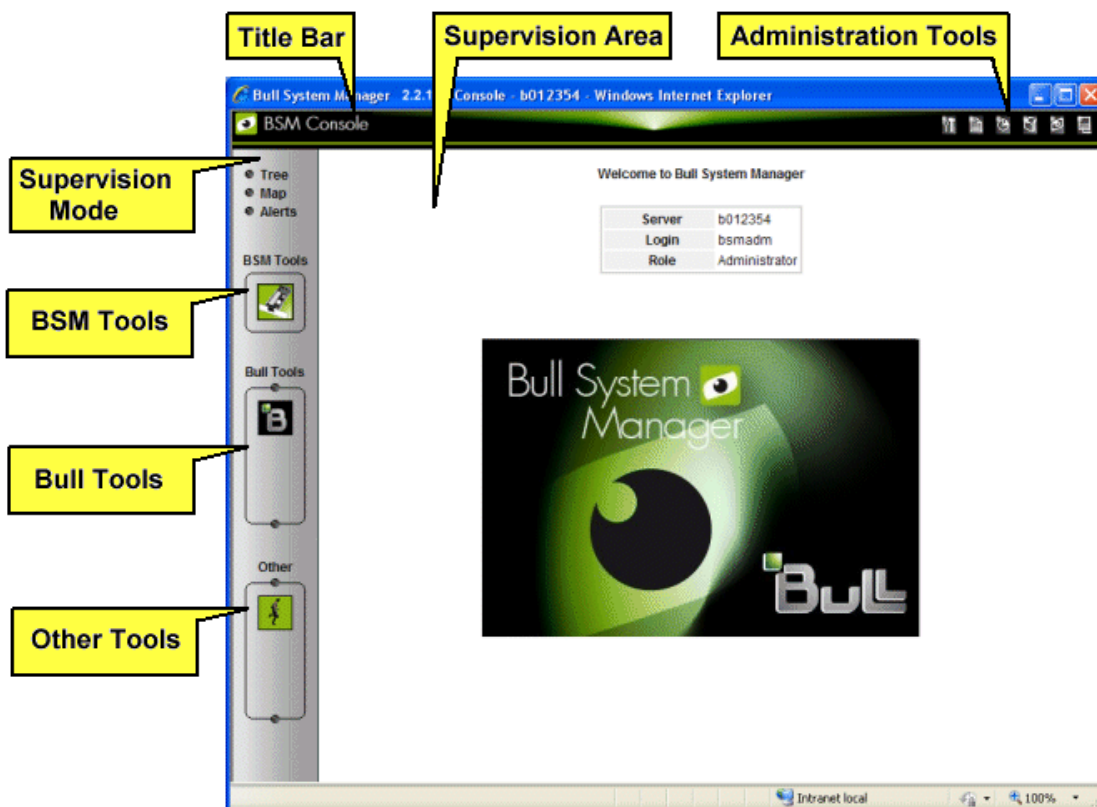### 2.1.2 Console Basics

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 agents deployment 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 52).

0The BSM Console provides different types of monitoring data.

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, 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

This section describes how to monitor your system using Tree Mode.

2.2.1 Starting with the Tree Mode

Notes

- Tree Mode concepts are explained in detail in *Erreur ! Source du renvoi introuvable.*.

- 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 sub trees.

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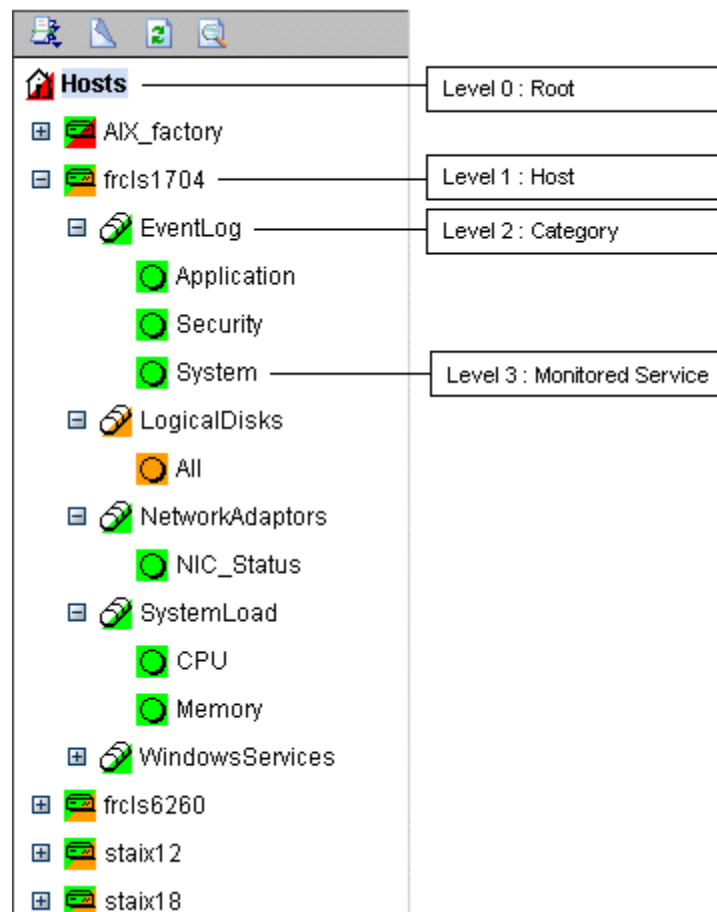
The color of the top left corner of a host icon indicates if this host is responding or not (following a **ping** command).

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:
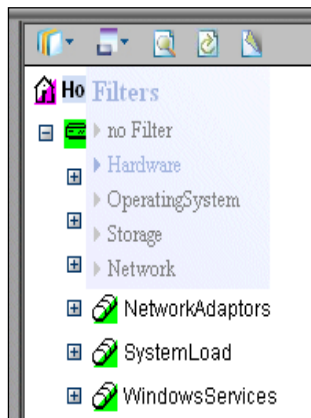
Figure 2-4   Example of Functional Filter Menu

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:
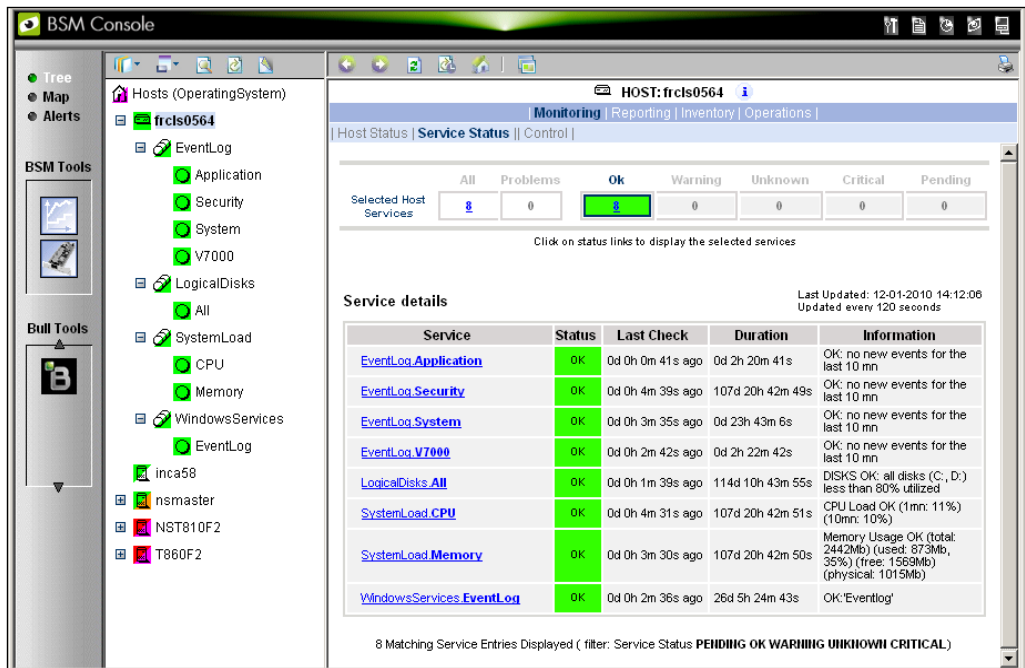
Figure 2-5   **OperatingSystem** Domain Filter Use

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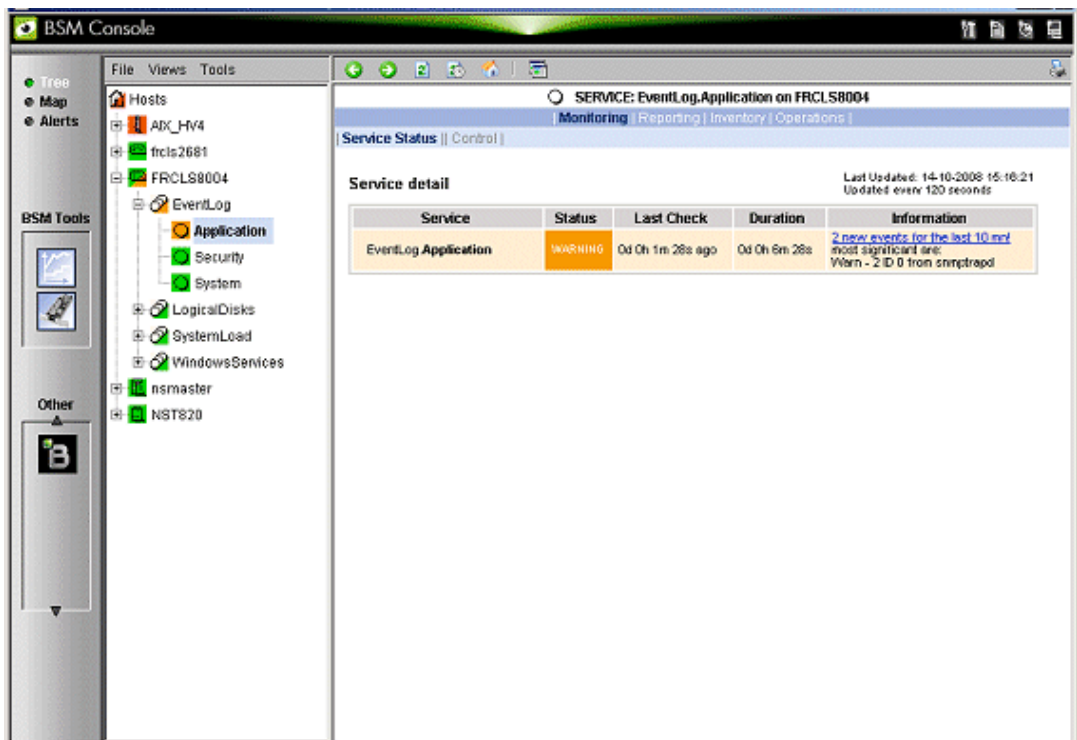
Figure 2-7　Status Information for an instance of the **EventLog.Application** Service

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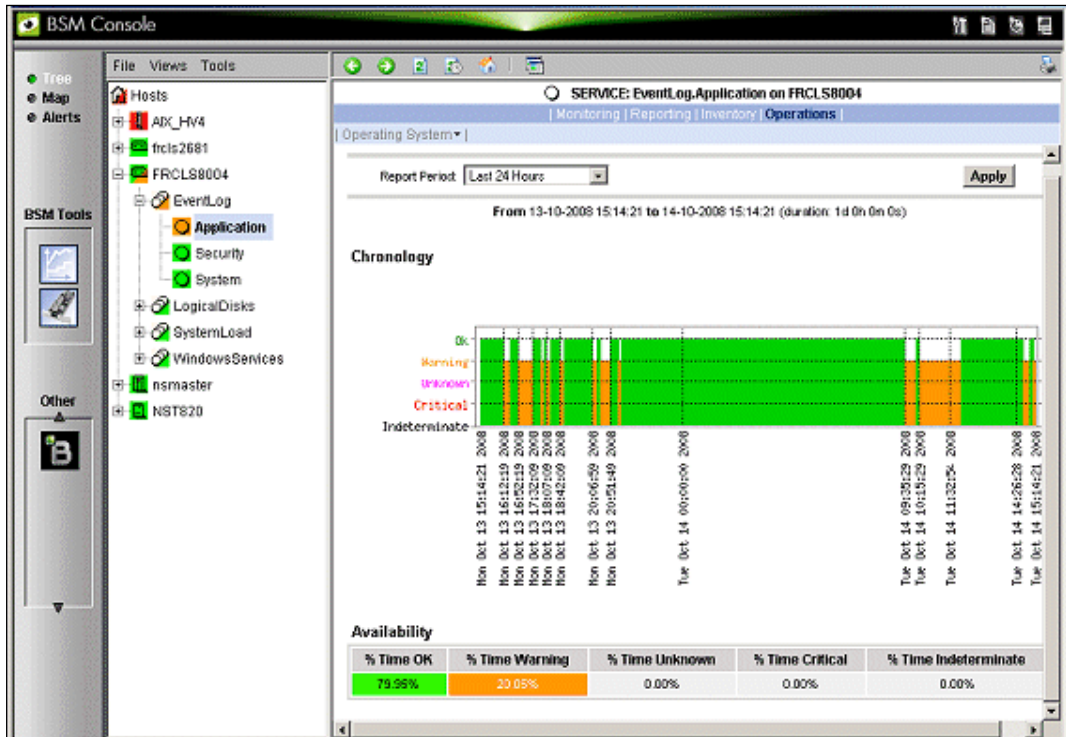
Figure 2-8   Example of Status Trends for **EventLog.Application** Service (last 24 hours)

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.
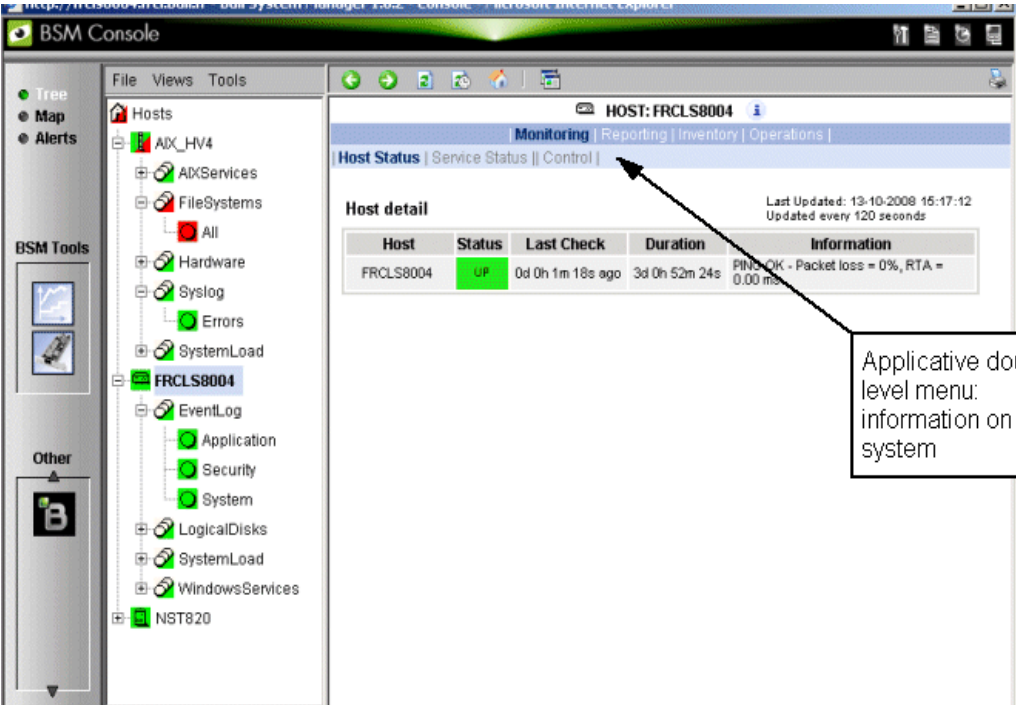
2.2.4 Viewing More Information

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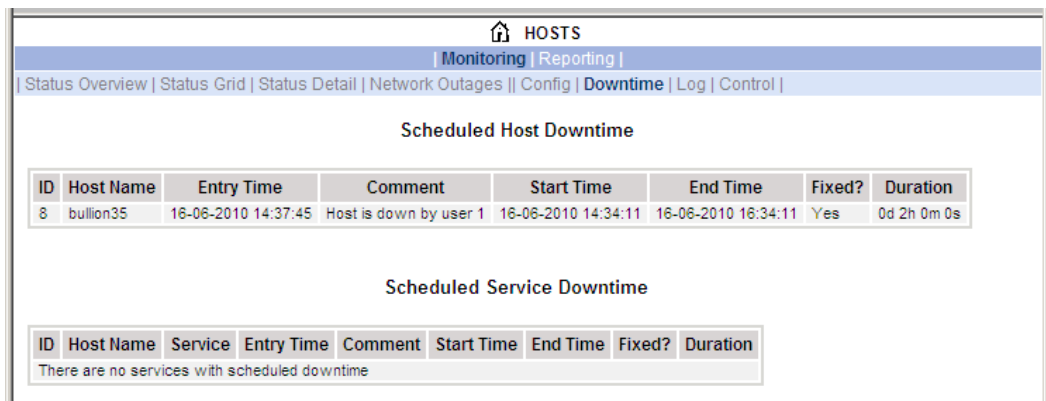
The Bull System Manager Console allows you to view all the notifications sent by the monitoring service.

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
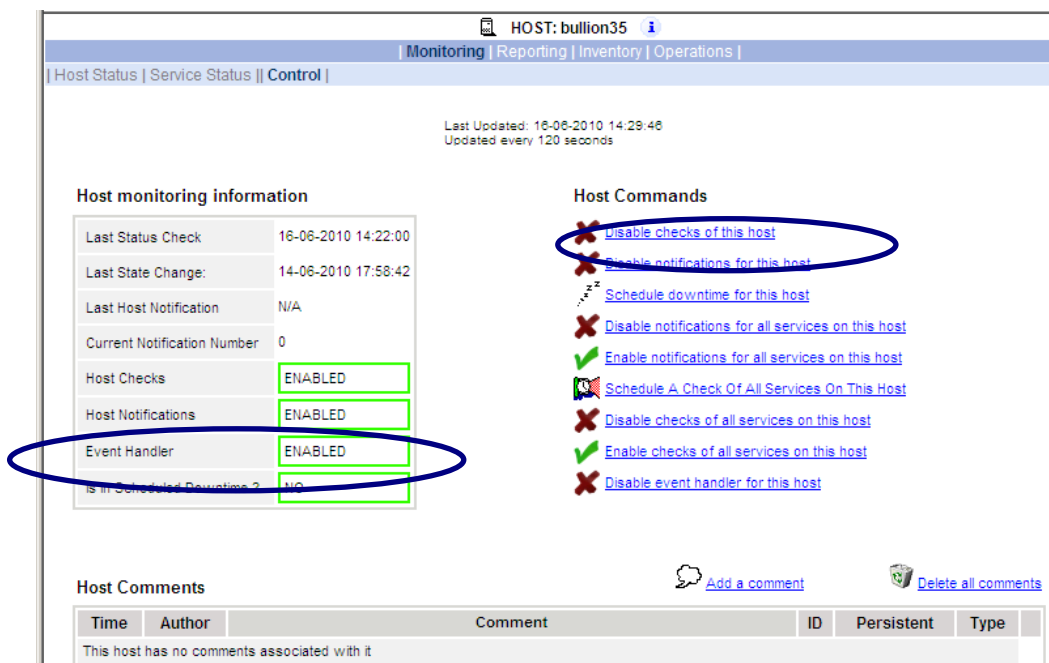
Figure 2-11 Scheduled Downtime Lists

2.4.2 How to Schedule a Downtime

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

Figure 2-12. Scheduling Downtime for Host Monitoring

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

Figure 2-13. Scheduling Downtime for a Particular Host

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:

Figure 2-14. Host Monitoring Information for Scheduled Downtime

When downtime period 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).

Figure 2-15. Canceling Scheduled Downtime for a Host

Then the following form must be completed and applied.

Figure 2-16. Information Details for Scheduled Downtime for a Host

Note   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**).
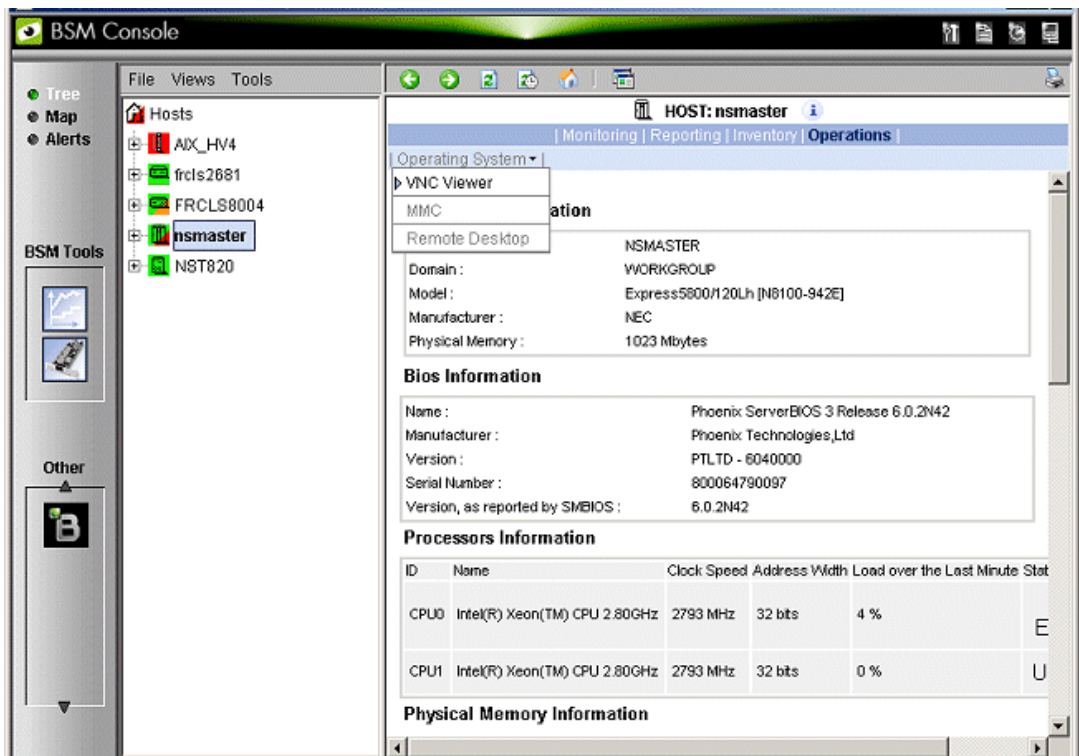
Figure 2-17 Starting UltraVNC Viewer on a Host

2. When prompted, enter the password used when VNC Server was installed or configured on the target host (`nsmaster` in this example).
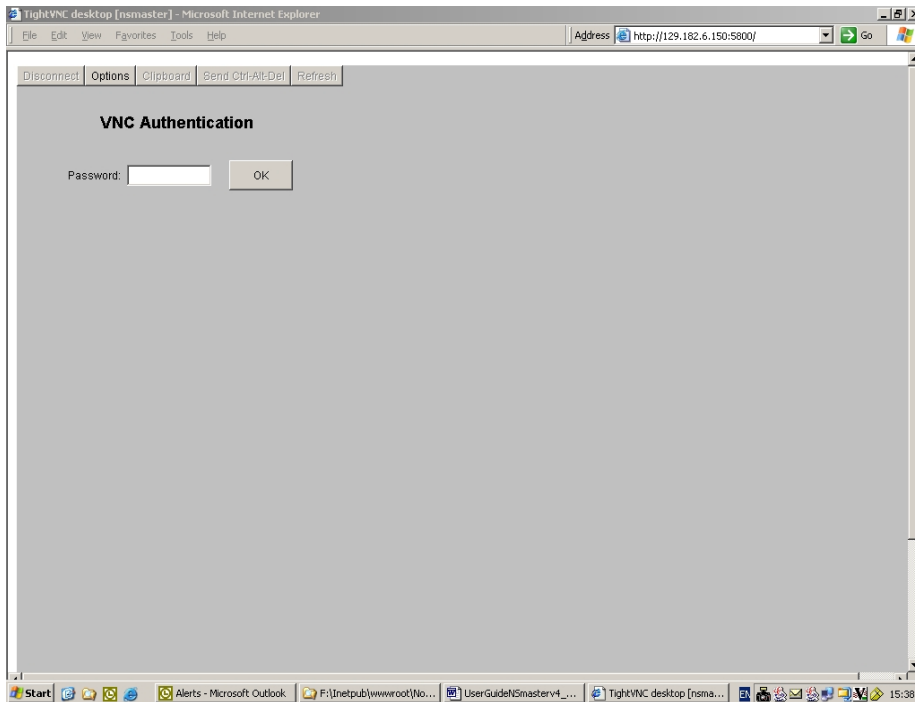
Figure 2-18 VNC Authentication Window

3. Click **OK**. You now have full access to the remote host (`nsmaster`), although response times may be longer.
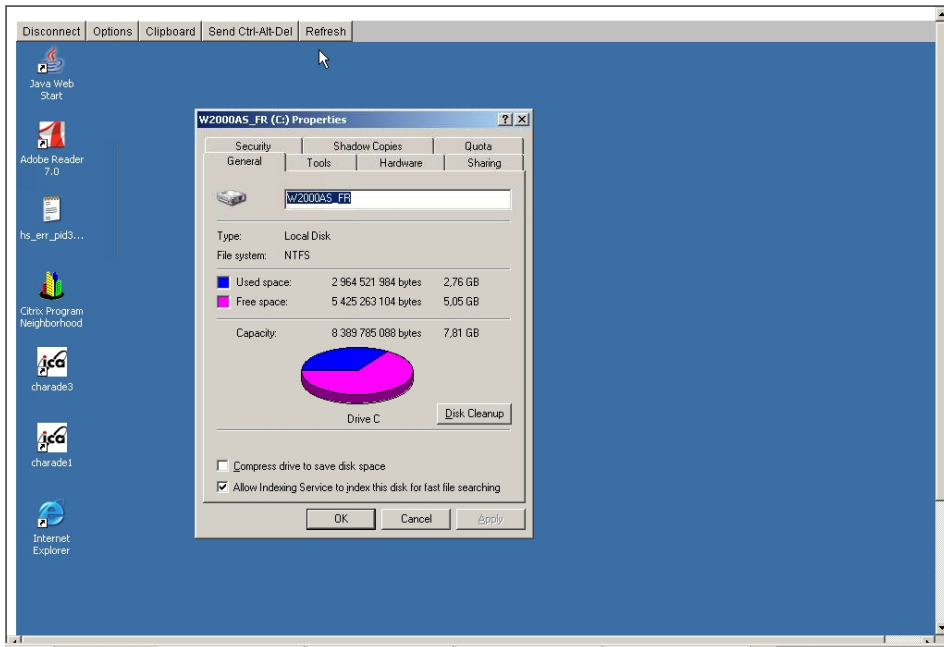
Figure 2-19 Remote Connection to a Windows Host with VNC Viewer

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.

From the `FRCLS2681` host menu, select **Operations > Operating System > Users**.
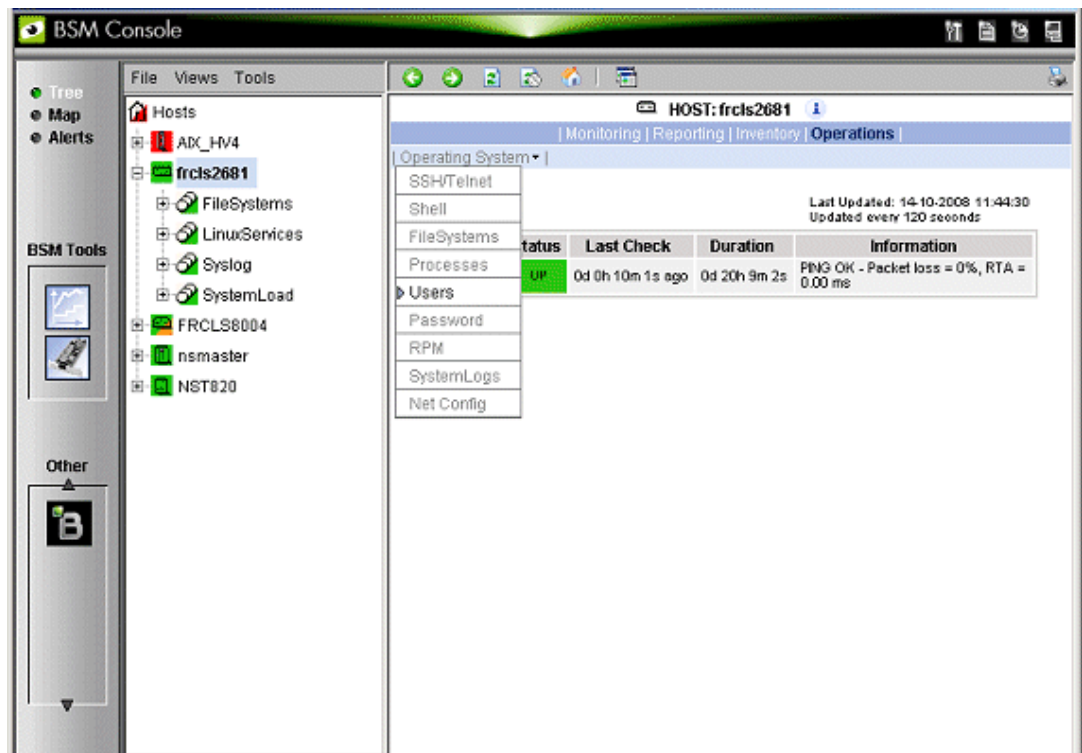
Figure 2-20 Launching Webmin Window

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

Figure 2-21 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 2-22 Webmin Interface on Linux Hosts

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

2.6 Managing Hardware

This section describes the different ways of 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:

- EMM for NovaScale bullion and GCOS series

- CMM for NovaScale Blade series

- HMC for Escala servers,

- iDRAC for NovaScale R400 or T800 series

- PAM for NovaScale 5000 and 6000 series

- ISM for NovaScale 4000 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, iDRAC, 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.
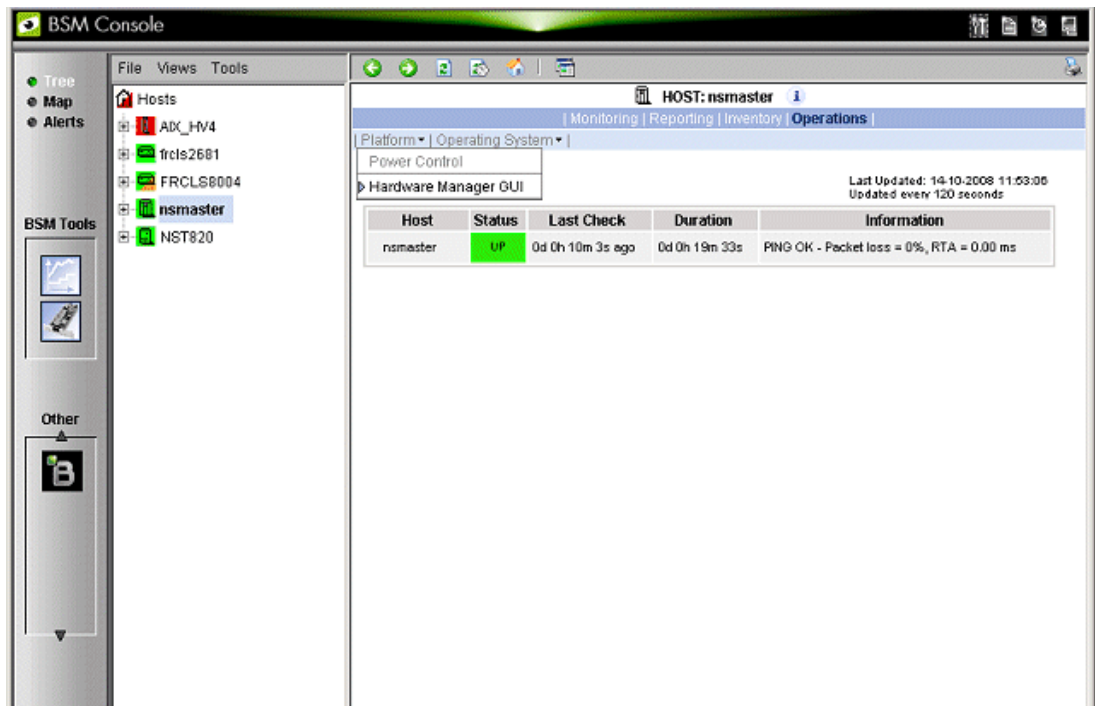
Figure 2-23 HW Manager GUI Menu

Starting the **Hardware Manager GUI** menu item calls the associated Hardware Manager, for instance for a ns bullion server:
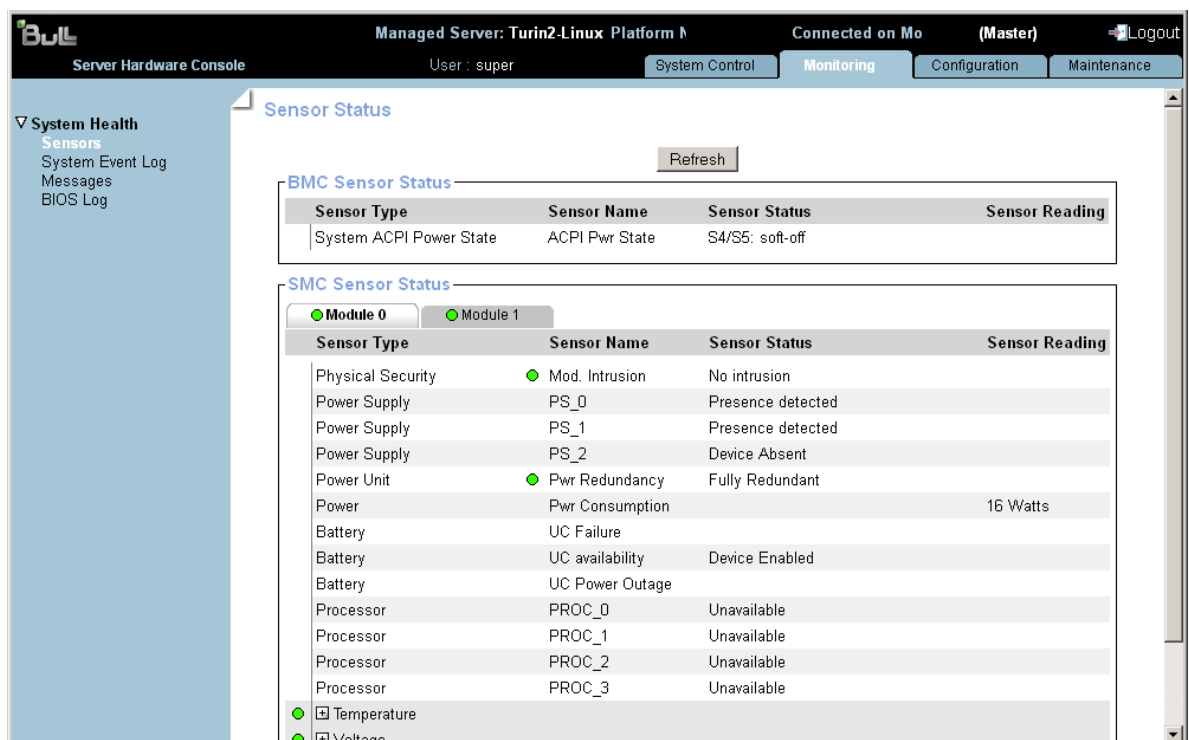
Figure 2-24 ns bullion Hardware Manager - Home Page

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 Bull systems.

To start the application:
From the Console Management Tree, click the **Operations > Platform > Power Control** items in the host menu.
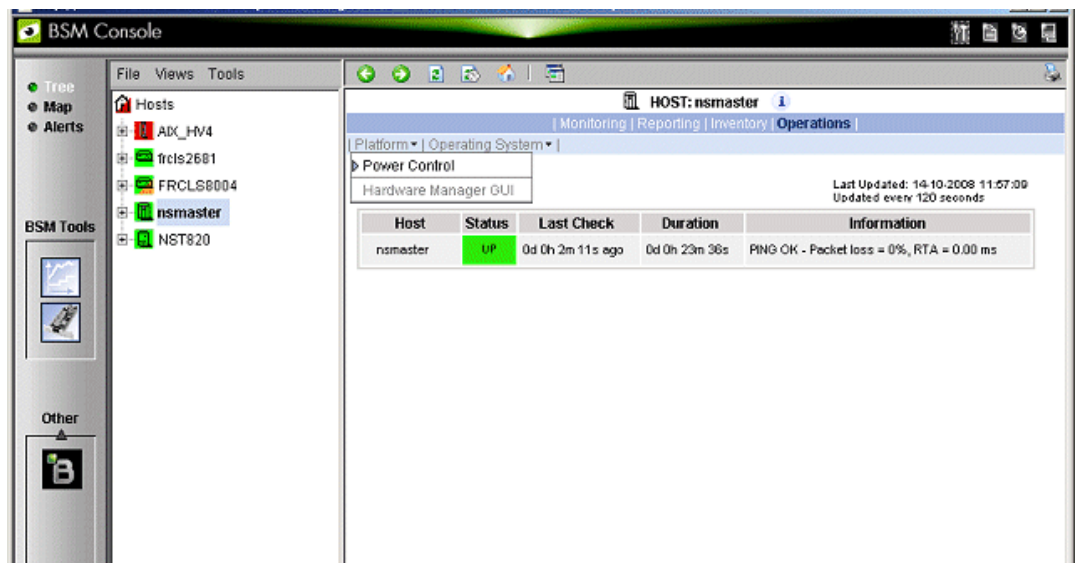
Figure 2-25 Launching the Remote Hardware Management Window
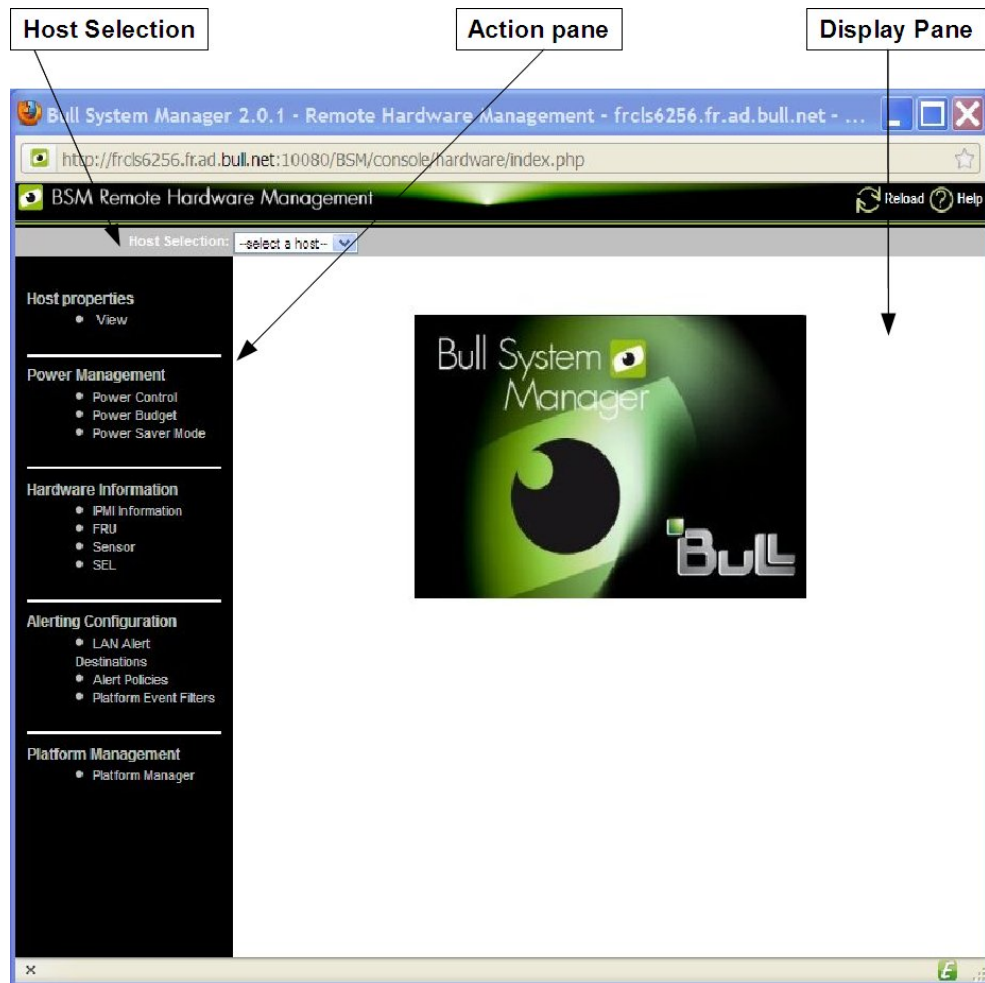
Figure 2-26 Remote Hardware Management Window

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 Bull systems listed.

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

- Power management functions

- FRU visualization

- Sensor visualization

- Event log visualization

- LAN Alert Destinations visualization

- Alert Policies visualization

- Platform Event Filters visualization

- Platform management application

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

2.7 Tracking a Performance Indicator over a Long Period via PNP4Nagios
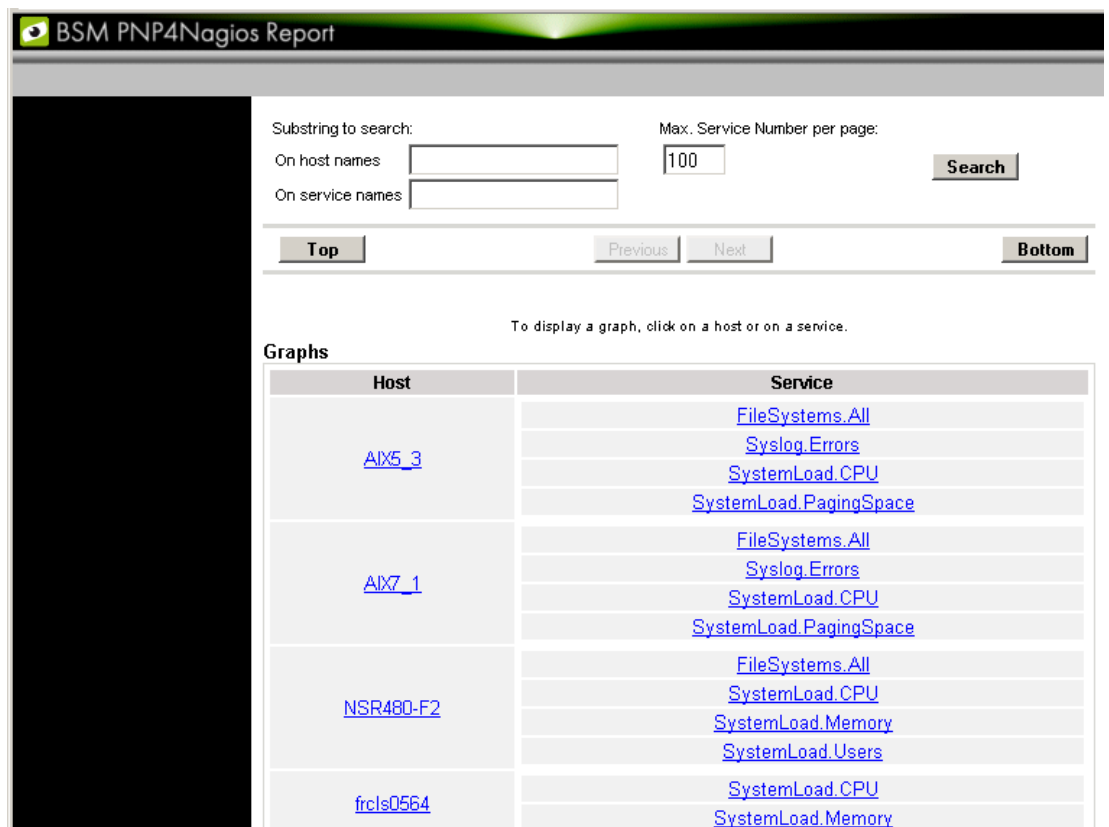
Note	The following items can be used only if the BSM PNP4Nagios (or PNP4Nagios04 on a RedHat 5.n) server extension package is installed.

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 are automatically collected from Bull System Manager monitoring data.

To visualize performance indicator reports, proceed as follows:

1. Launch the Bull System Manager Console from the Bull System Manager Home Page.

2. Click the **PNP4Nagios Reports** icon ![icon] to display the list of all the reports that are available.

3. Select the report you want to display from the services list or the host list.

Figure 2-27 Bull System Manager PNP4Nagios Reporting Indicators Home Page

Note	You can filter by substring the services list via the top form.

The following Window appears:
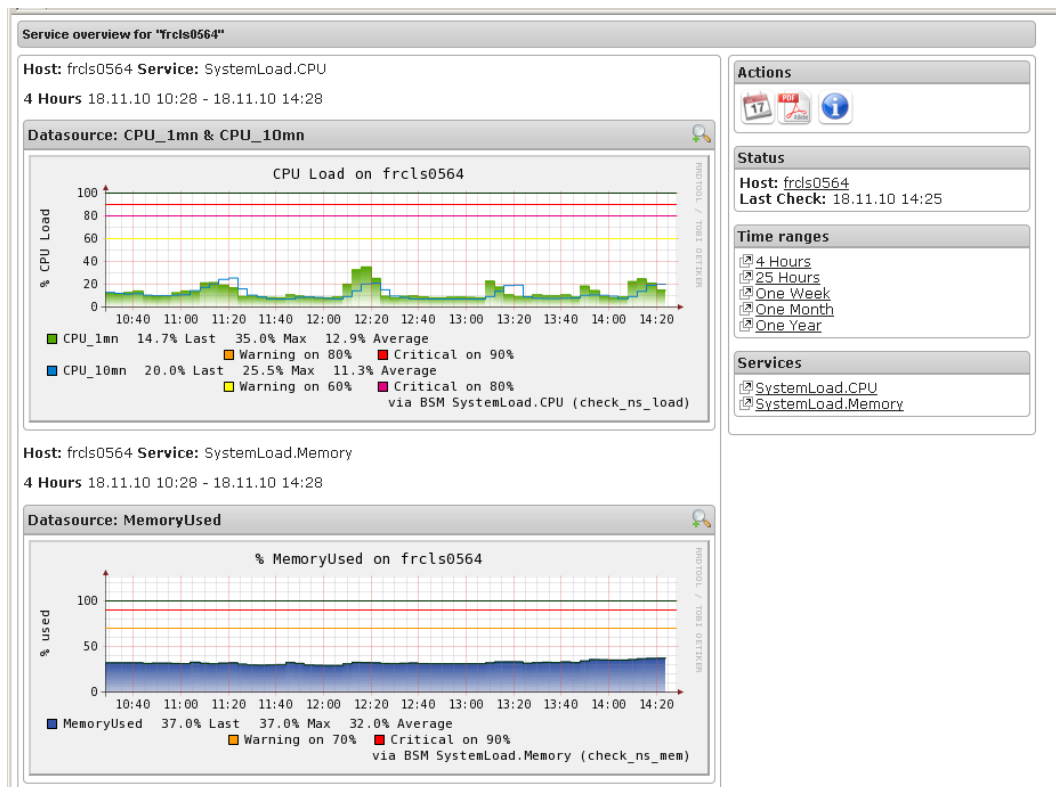
Figure 2-28 Bull System Manager PNP4Nagios Reporting Indicators - Example

This display shows 2 graphs. Each graph shows the evolution of a different indicator ("CPU load" and " % Memory used" in the example above) for one period of 4 hours.

Note   You can notify that the granularity is different between MRTG and PNP4Nagios. MRTG manages a set of indicators that can be associated to a host or a Nagios monitoring service. While PNP4Nagios manages a set of indicators that are necessarily associated with a Nagios monitoring service.

On the contrary of MRTG, the PNP4Nagios configuration does not contain a list of declared indicators. A generic mechanism collects automatically indicators that are exported by Nagios monitoring services.

2.8   Configuring Bull System Manager

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.
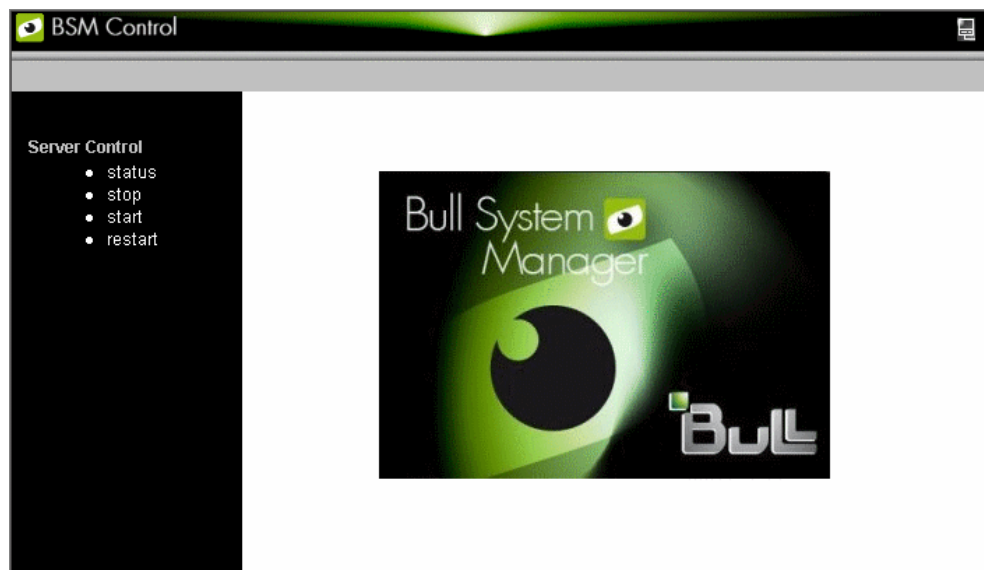
Figure 2-29 Bull System Manager Server Control

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:
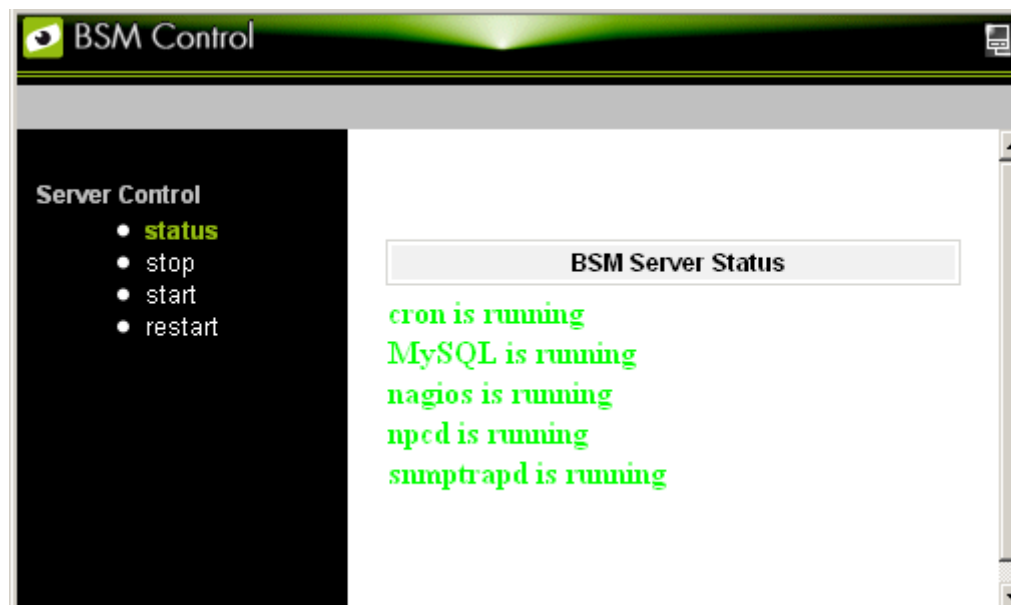
Figure 2-30 Bull System Manager Server Status

Chapter 3. Using Bull System Manager Console Supervision Modes

Three different supervision modes - **Tree mode**, **Map mode** and **Alerts mode** - are accessible from the radio buttons in the top left hand corner of the **BSM** console.

These provide contextual information for the resource selected within that mode.

Note   For more information about Console Basics and Access, refer to *Section 2.1.2 Console Basics*.

3.1   Working in the Tree Mode

The **Tree mode** displays hierarchically all the resources defined in the Bull System Manager configuration.

Figure 3-1.   BSM Console Tree Mode

On any configuration change, an alert Window is displayed as shown in the following figure:
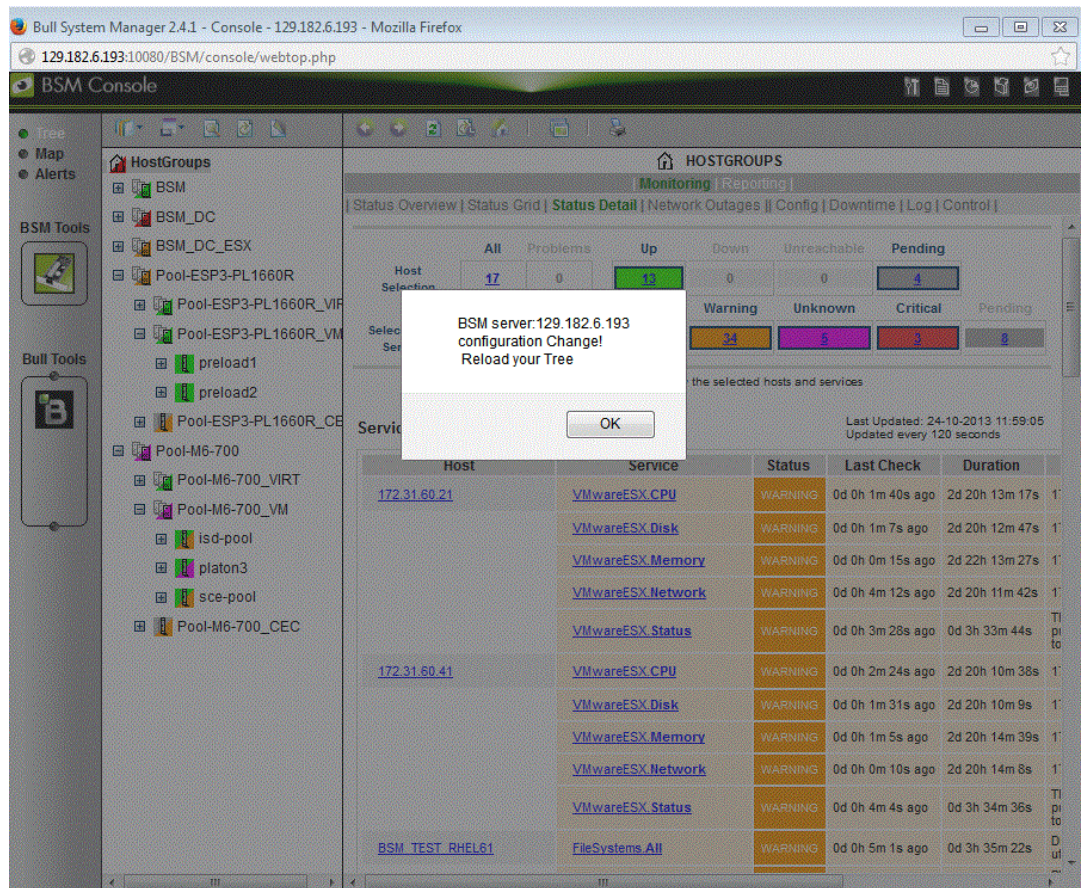
Figure 3-2   Tree Reload

Configuration change can result from:

- modification done with the BSM GUI Configuration
- modification automatically applied after change detected by the supervision engine if the dynamic configuration feature is enabled. Please refer to the *Administrator's Guide*, 86 A2 56FA, for details about configuration tasks.

3.1.1 Management Tree Basics

Each node in the tree may contain sub-nodes that can be selected for more specific information.
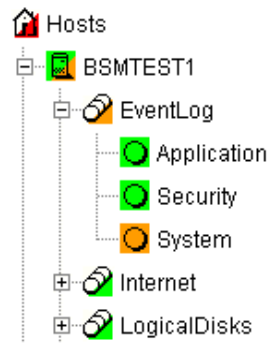
Figure 3-3   Management Tree

- Double-click a node or click the **+/-** expand/collapse icon to display sub-nodes.

- Select a node to display its characteristics in the Supervision Window.

- Right-click to display the specific node menu.
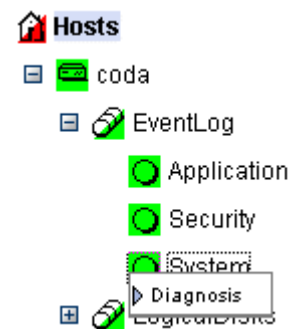
Figure 3-4   A Service Node Menu

Above the Management Tree, a menu provides the Select View, Hide Tree, Refresh and Search commands:
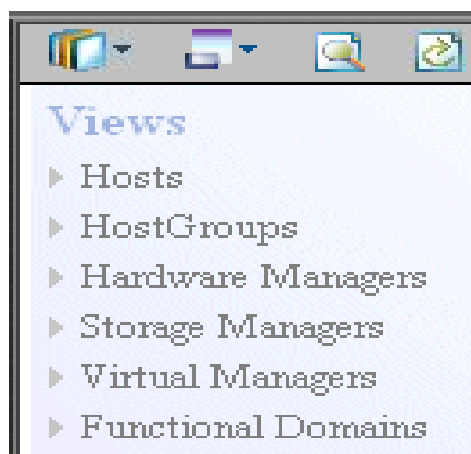
Figure 3-5   Management Tree Menu

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 3-6   Management Tree Commands

Note   The default view mode is the **topology & service** mode which allows the display of all hosts with their services. You can choose the **topology** mode which allows the display of hosts only. (See *Chapter 11: Customizing the Bull System Manager Console*, in the *Administrator's Guide*, 86 A2 56FA).

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 sub-nodes, 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 sub-node 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 sub-nodes (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**.
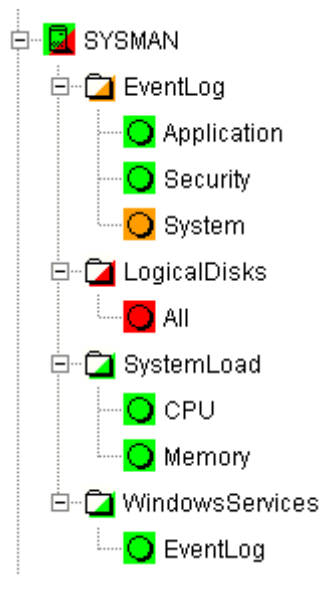
Figure 3-7   Management Tree Animation - example

Right-click the colored node icon to display the **Diagnosis** menu:
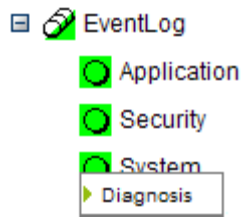
Figure 3-8   Node Icon Menu
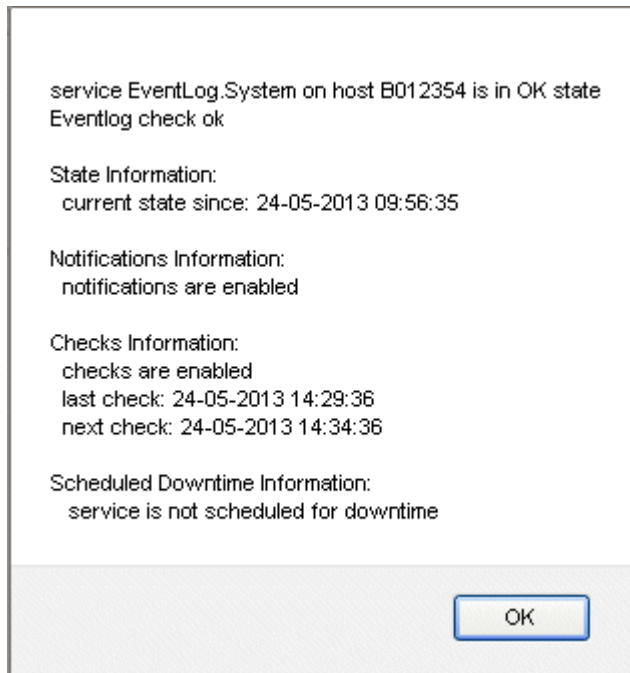
Figure 3-9   Diagnosis Window

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 generated).

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 sub-node 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 sub-node 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 sub-node 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

The top left triangle reflecting self-status is always blank (unmonitored). The bottom right triangle reflects the status for the sub-node 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 sub-node 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 sub-node 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 sub-node 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 sub-node 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 sub-node 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:
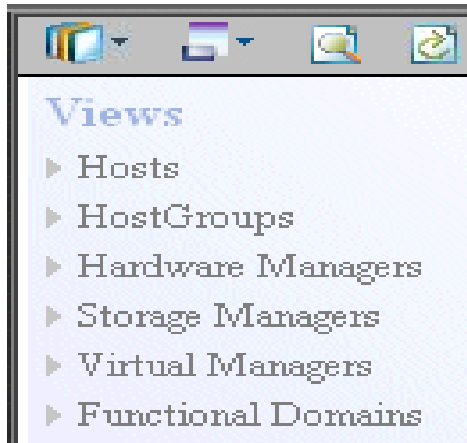
Standard Tree Views	
Hosts View	All hosts are displayed under the root node.
HostGroups View	All hostgroups in the configuration plus all NovaScale 5000 and 6000 Series platforms and NovaScale Blade Chassis are displayed as hostgroup nodes with their associated hosts.
Hardware Managers View	All hardware 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.
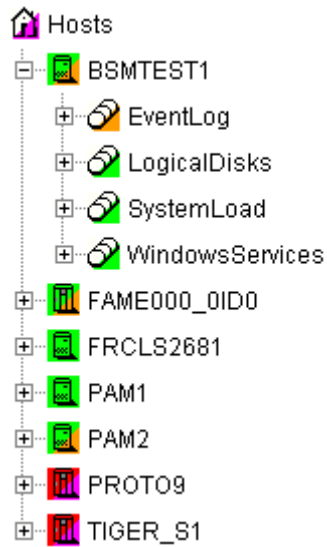
Figure 3-10 Hosts View

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.
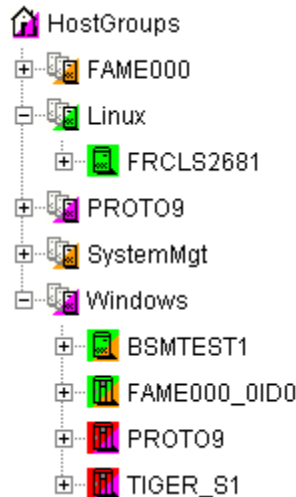
Figure 3-11 HostGroups View

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:
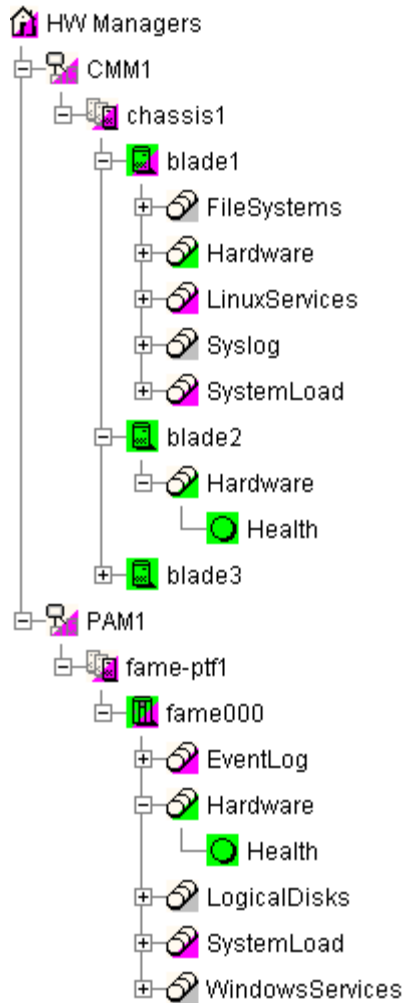
Figure 3-12 HW Managers View

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:
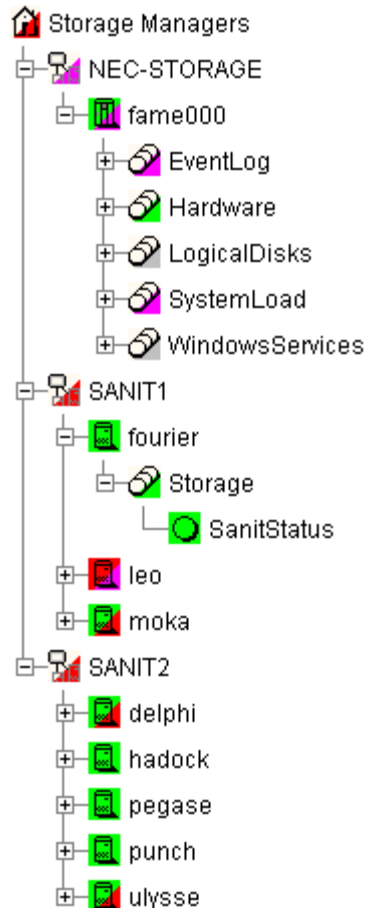
Figure 3-13 Storage Managers View

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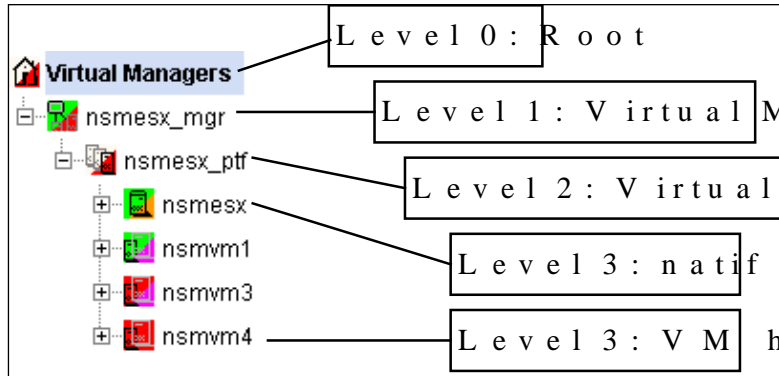
For details, refer to the *Bull System Manager Server Add-ons Installation and Administrator's Guide*, 86 A2 59FA.

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.
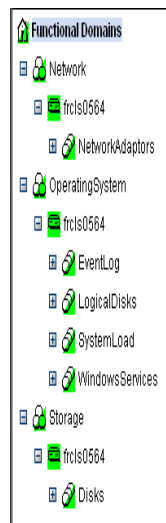
Figure 3-14 Functional Domain View Example

3.2   Working in the Map Mode

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

Map mode is used to display the status for a grouping of host groups (and their monitored hosts) on the screen.

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

Note   The **Map** and **Applicative** Windows are always synchronized.
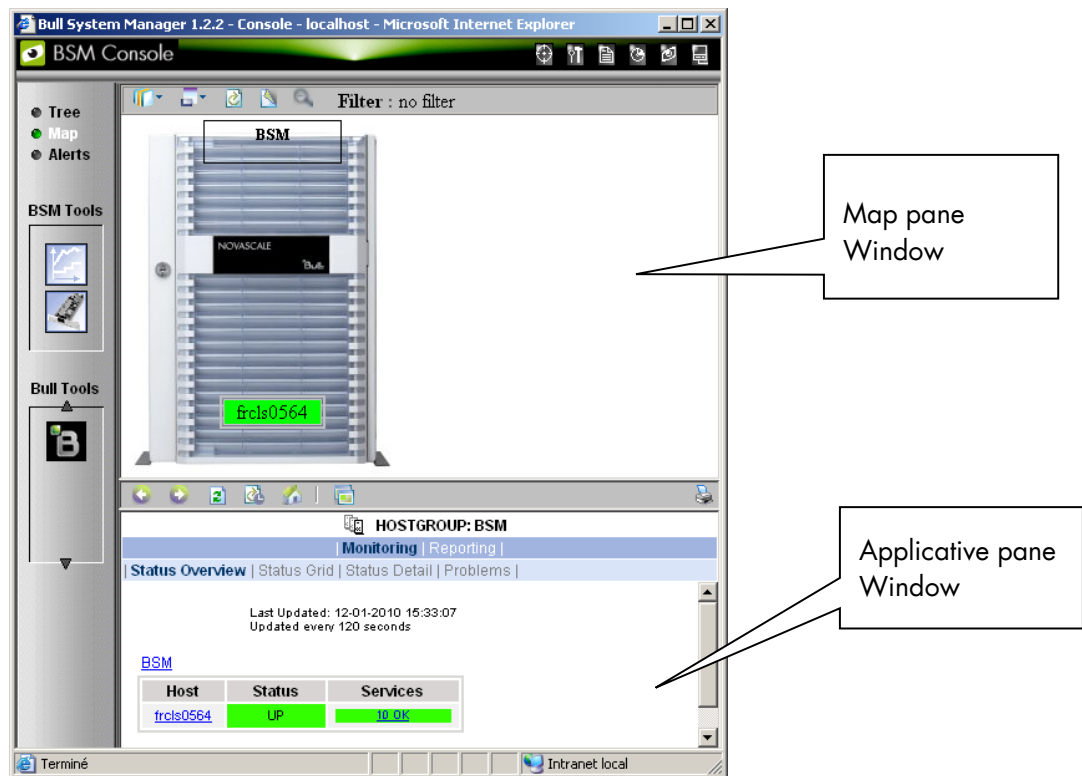
Figure 3-15 Map Mode

In the **Map** Window, Hostgroups, Hosts and Monitoring services are displayed, and are color coded according to their status.

In general, the map has a background image and the host groups are located at specified positions (x, y) on the map as specified in the Configuration GUI. Maps differ in appearance, but they all display host groups graphically indicating the status for the services.

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 **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

Alerts mode displays alerts (also called events) for a set of Hostgroups, Hosts and Services monitored by the **Alert Viewer** application.

3.3.1 Alert Basics

The **Alert Viewer** 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.

BSM Alert Viewer scans the alerts stored in the monitoring log and archives according to filter report period settings.

Figure 3-16 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 3-17 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:
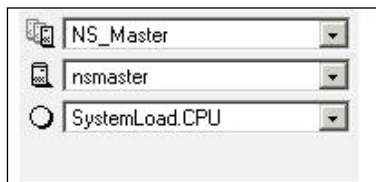
Figure 3-18 Alert Selection - Example

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.
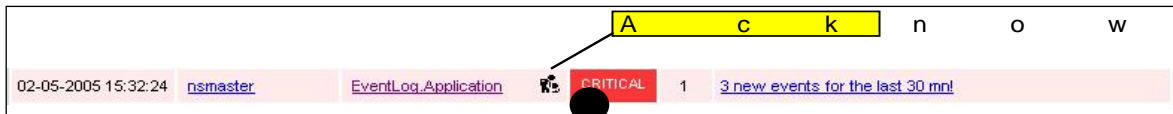
Figure 3-19 Acknowledged Alerts Selection

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

The BSM Console provides different types of monitoring data.

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 3-20 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:
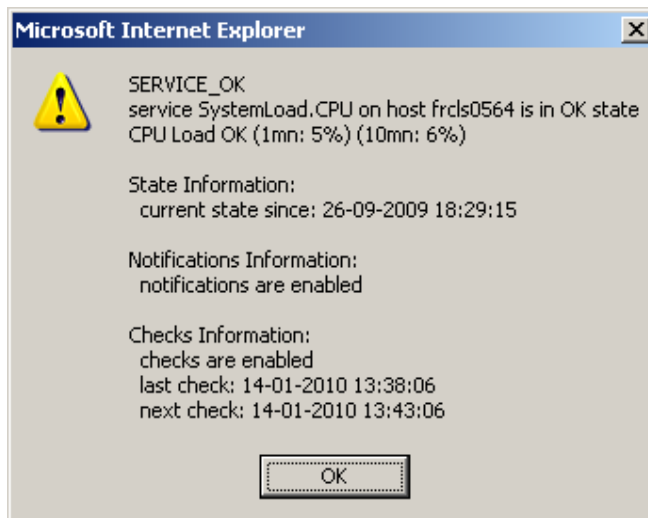
Figure 3-21 Status Detailed Information from the BSM Focus Window.

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:
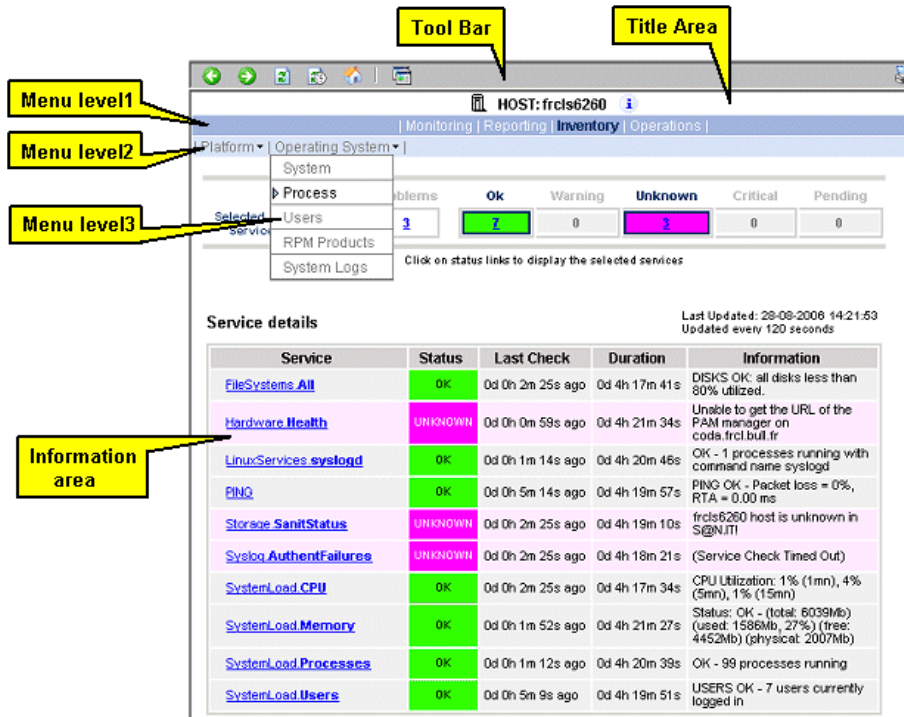
Figure 3-22 Supervision Window

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 3-23 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 3-24 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 3-25 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 3-26 Host Status Grid

| **Host** | Host name |
| **Service Status** | Host services color 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.
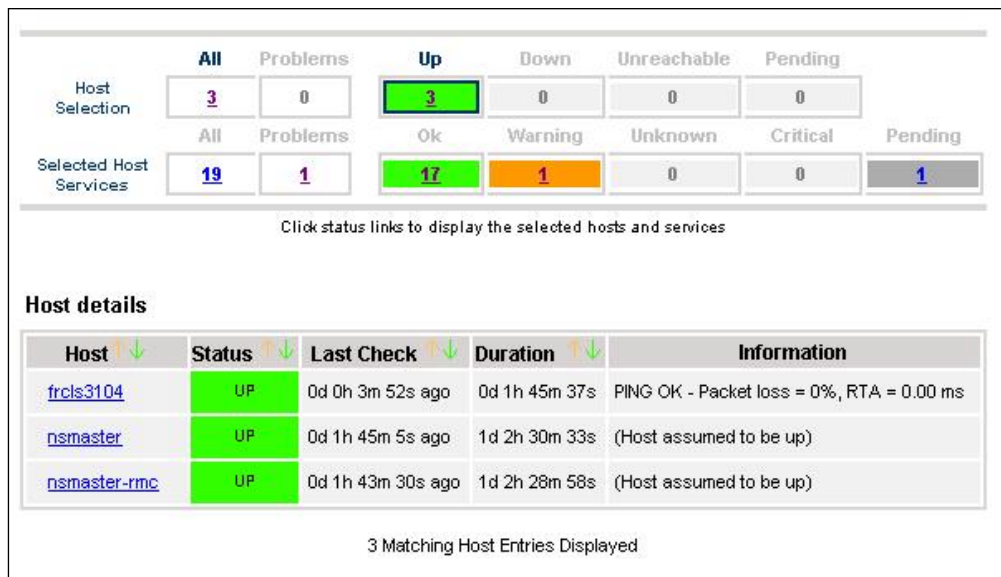
Figure 3-27 Hosts Status Detail

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 3-28 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.
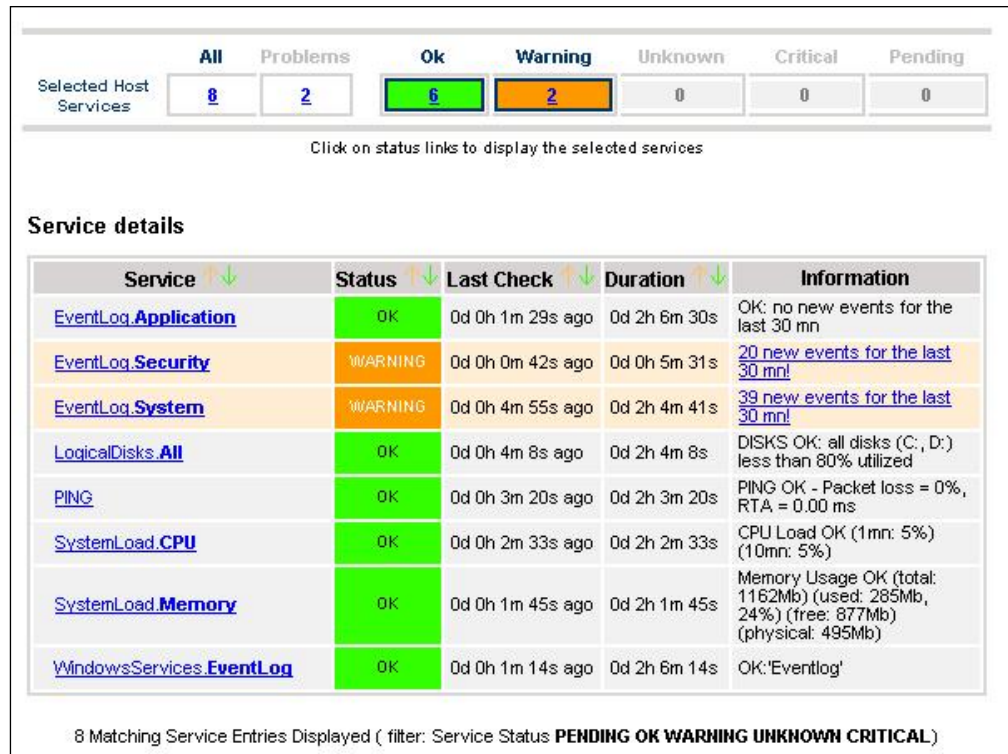
Figure 3-29 Service Status

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 Configuration

This screen displays the Monitoring Server (**nagios**) configuration objects (hosts, hostgroups, services, contacts, contact groups, time periods 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 3-30 Monitoring Server Configuration

3.4.3.7 Log

This screen displays the current Monitoring Server log file. You can also browse archived events.
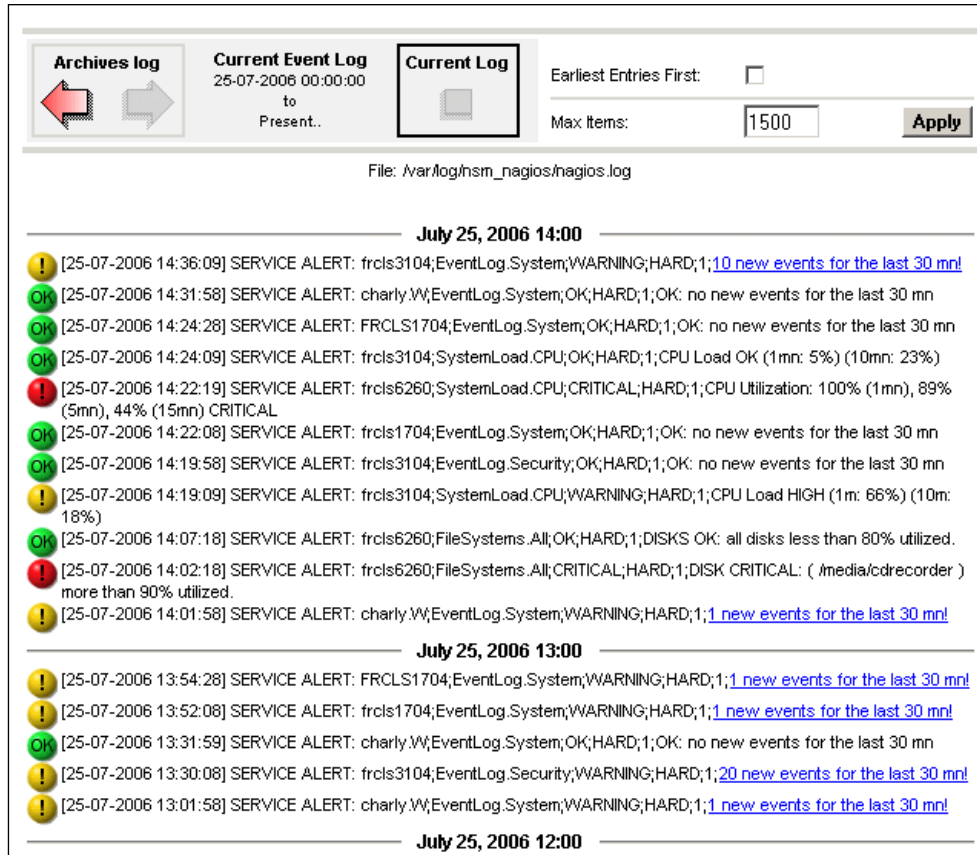
Figure 3-31 Monitoring Server Log

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 3-32 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

Performance Information

Active Service Checks

Total Services: 79
Active Services: 74
Disabled Services   0

Time Frame	Checks Completed
<= 1 minute	16 (21.6%)
<= 5 minutes	71 (95.9%)
<= 15 minutes	74 (100.0%)
<= 1 hour	74 (100.0%)
Since program start	74 (100.0%)

Metric	Min.	Max.	Average
Check Execution Time	< 1 sec	32 sec	1.635 sec
Check Latency	< 1 sec	2 sec	0.000 sec
Percent State Change	0.00%	24.80%	4.24%

Passive Service Checks

Total Services: 79
Passive Services: 5

Time Frame	Checks Completed
<= 1 minute	0 (0.0%)
<= 5 minutes	0 (0.0%)
<= 15 minutes	0 (0.0%)
<= 1 hour	0 (0.0%)
Since program start	0 (0.0%)

Metric	Min.	Max.	Average
Percent State Change	0.00%	0.00%	0.00%

Active Host Checks

Total Hosts: 16
Active Checked Hosts: 16
Not Checked Hosts: 0

Time Frame	Checks Completed
<= 1 minute:	6 (37.5%)
<= 5 minutes:	9 (56.2%)
<= 15 minutes:	9 (56.2%)
<= 1 hour:	11 (68.8%)
Since program start:	15 (93.8%)

Metric	Min.	Max.	Average
Check Execution Time:	0.00 sec	0.84 sec	0.252 sec
Check Latency:	0.00 sec	0.00 sec	0.000 sec
Percent State Change:	0.00%	10.13%	1.02%

Figure 3-33 Performance Statistics

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

Figure 3-34 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.

Figure 3-35 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
PNP Indicator Trends	Root nodes of Hosts views (Tree) 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 11.

Figure 3-36 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 3-37 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.
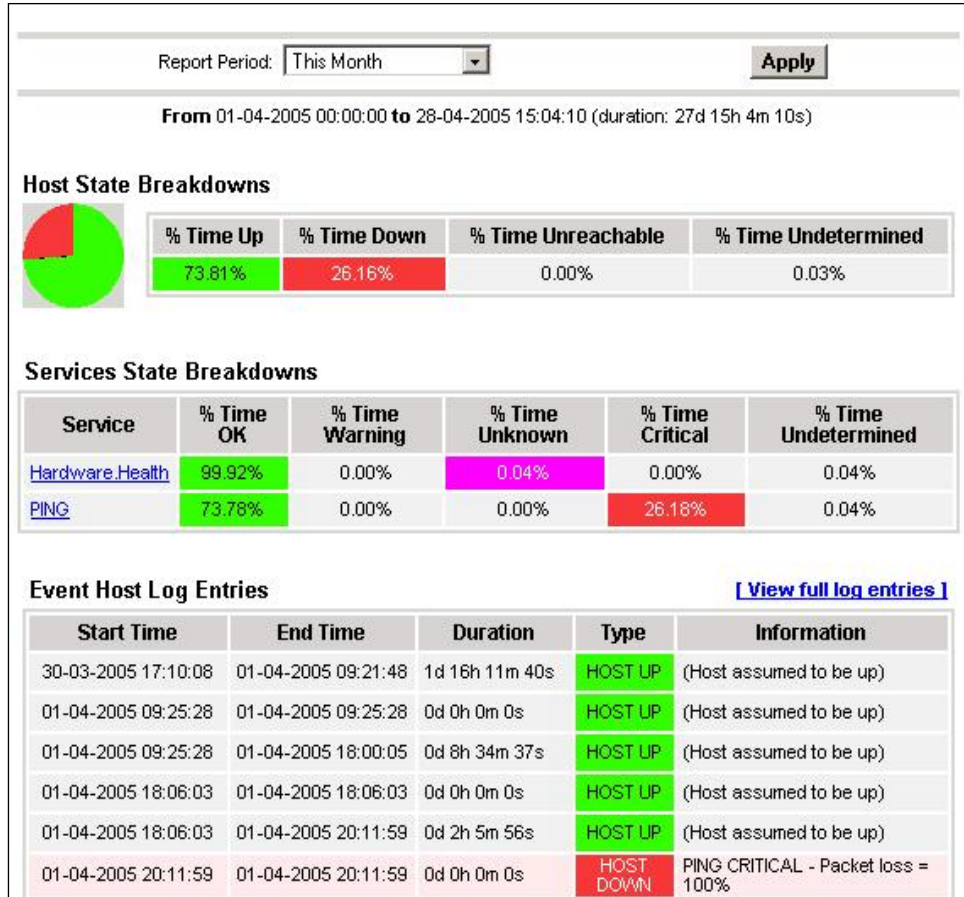
Figure 3-38 Availability Screen - Example

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 (the full log option can display Nagios core events: start, restart).

3.4.4.4   Status Trends

This screen displays a graph of host or service states over a defined period, as shown below.
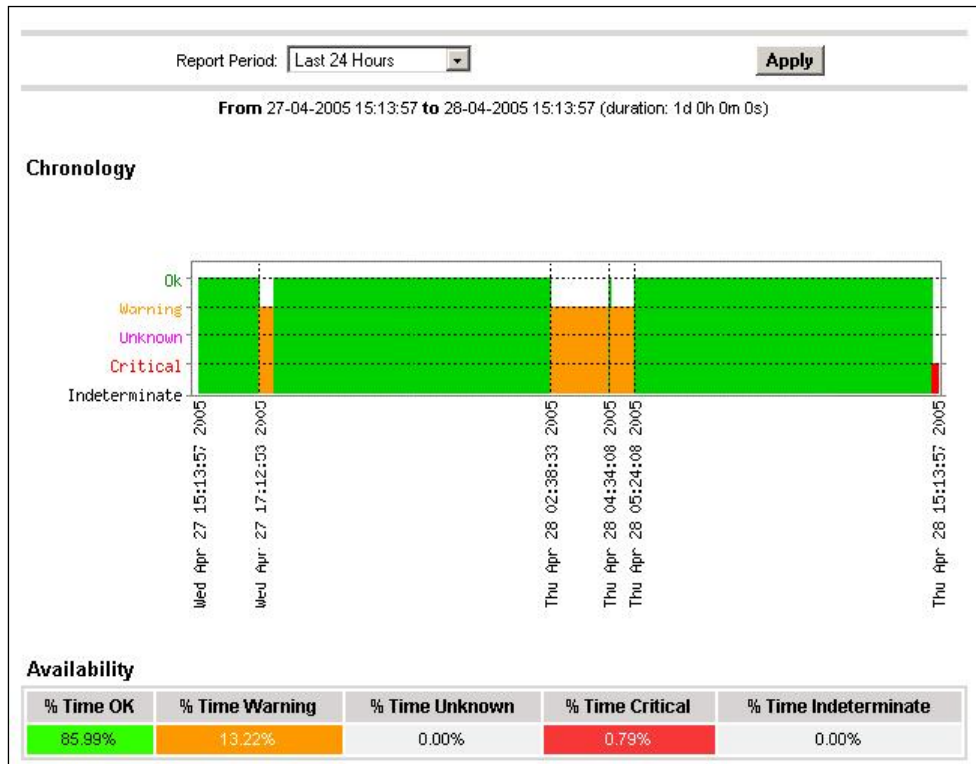
Figure 3-39 Status Trends on a Service

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   PNP4Nagios Indicator Trends

Note   The following items can be used only if the BSM PNP4Nagios (or PNP4Nagios04 on a RedHat 5.n) server extension package is installed.

The **PNP Indicators Trends** screen lists the available indicator reports associated to a given resource, as displayed below.
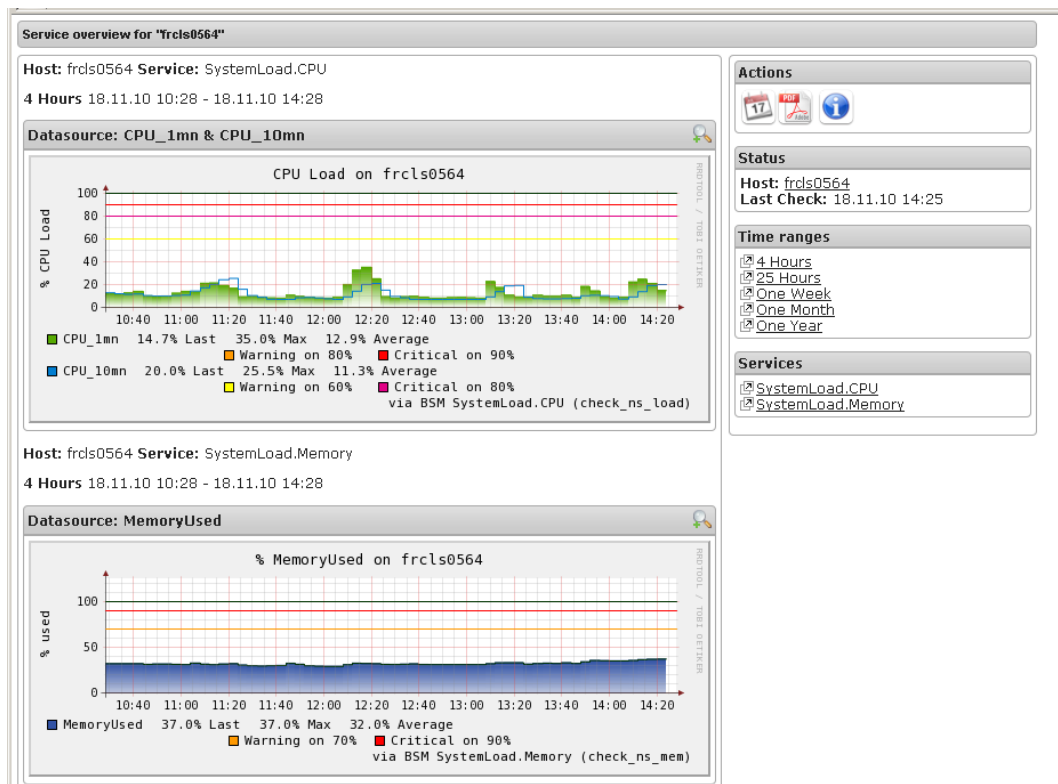
Figure 3-40 PNP4Nagios Indicator Trends on a Host

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 configuration.

- When 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
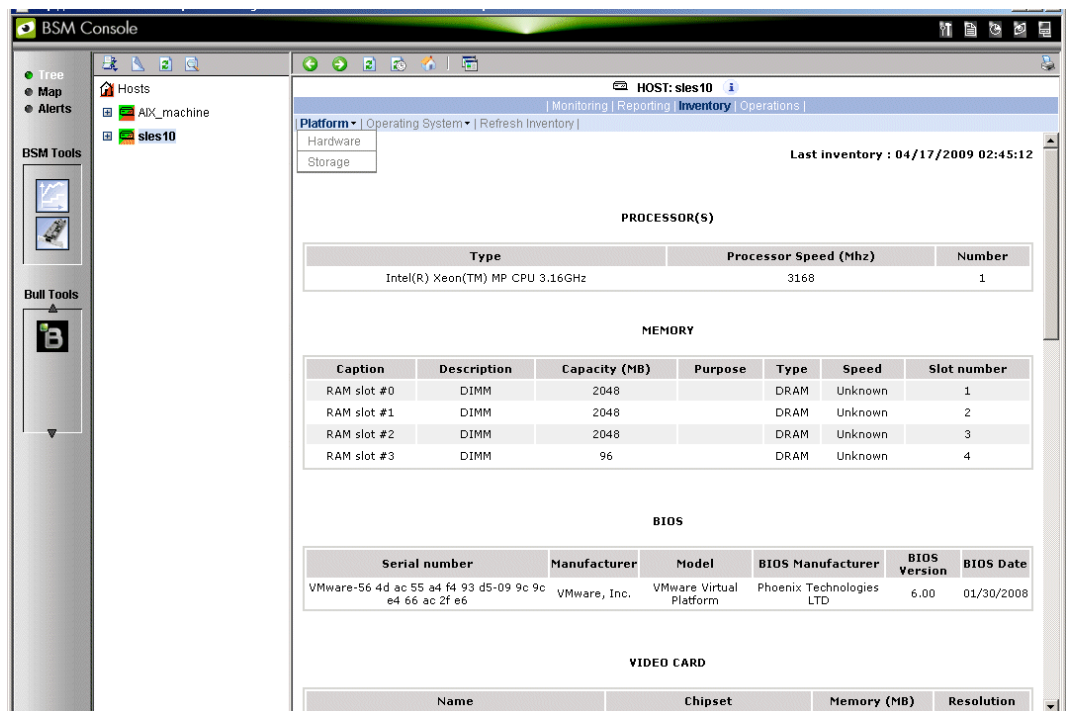
Figure 3-41 Hardware Inventory Information – Example

Storage Information

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

Figure 3-42 Storage Information - Example

FRU Information

This information is only available for NovaScale bullion and GCOS, Express 5800, R400, T800, NovaScale 3000, 4000, 5000, 6000 and 9010 series, NovaScale Blade and Escala Blade hosts.
For details about the information displayed, refer to *Chapter 4*.

Sensor Information

This information is only available for NovaScale bullion and GCOS, Express 5800, R400, T800, NovaScale 3000, 4000 and 9010 series and Nova Scale Blade hosts.
For details about the information displayed, refer to *Chapter 4*.

SEL Information

This information is only available for NovaScale bullion and GCOS, Express 5800, R400, T800, NovaScale 3000, 4000, 5000, 6000 and 9010 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 3-43 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
			2005/04/14				

Figure 3-44 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 3-45 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 3-46 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 3-47 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 3-48 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 3-49 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 10109a895a20001108123159000005652000 ...
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 3-50 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 3-51 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 3-52 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 3-53 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:

- EMM for NovaScale bullion and GCOS
- HMC for Escala series
- CMM for NovaScale Blade series
- iDRAC for NovaScale R400 or T800 series
- RMC or ARMC for Express5800 series.
- PAM for NovaScale 5000 and 6000 series
- ISM for NovaScale 4000 series
- 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.
... ->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

This chapter describes the applications available from the BSM console.

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 Bull systems.

This application manages **Power Management** for novascale R400, T800 servers.

This application manages **Power Saver Mode** for PL servers.

This application displays **Alerting Configuration** for all machine types.

This application also manages **Platform Management** for novascale bullion machines.

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.
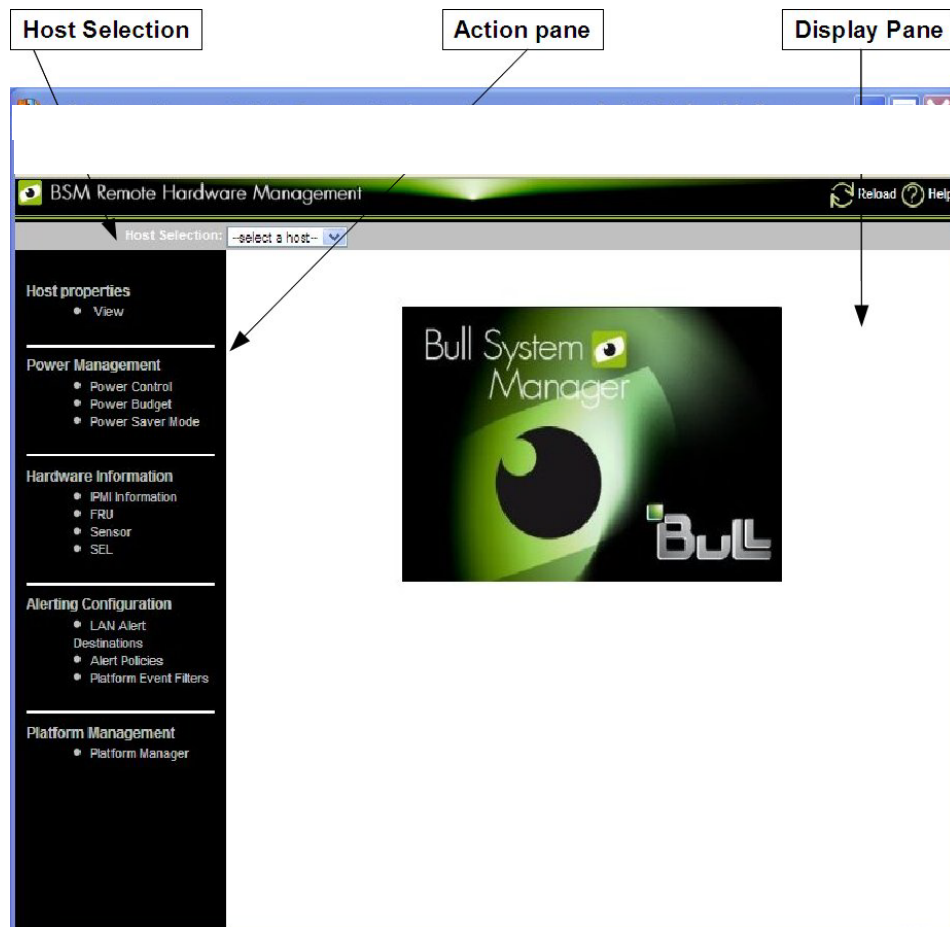
Figure 4-1   Remote Hardware Management Screen

Bull System Manager Remote Hardware Management comprises three functional parts:

Host Selection Window & Current Selected Host Window
Used to select and display the current host from the Bull systems declared in the Bull System Manager network.

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 Bullion Server Host Properties - Example

Host properties differ according to host type.

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 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*

NovaScale bullion/NS R400/NS T800

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

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.

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.
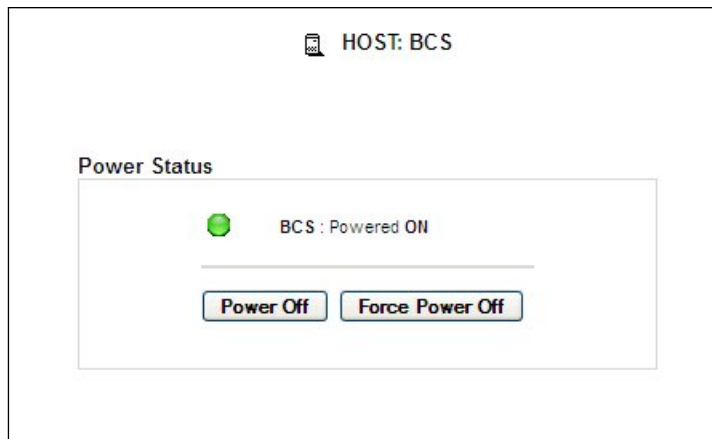
Figure 4-3   Power Status Output - Example
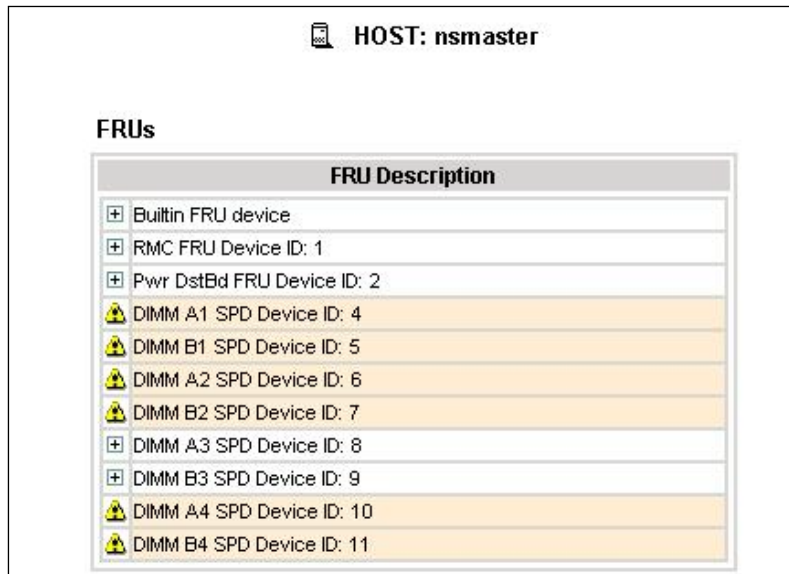
Note   In order for the **power off** command to be taken into account on a remote host running Windows 2000 / 2003 server, the *Shutdown: Allow system to be shut down without having to log on* security option must be enabled on the remote host.

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).
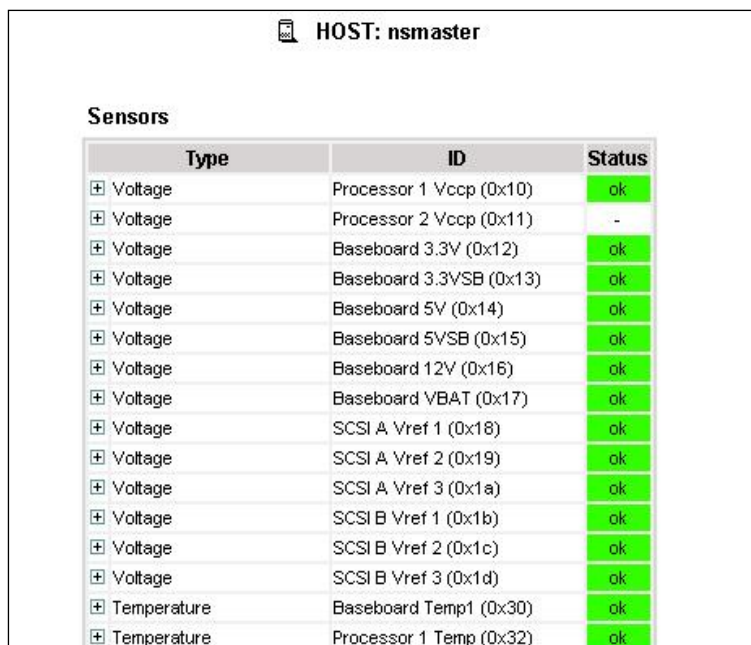
Figure 4-4   FRU Output - Example

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** (NovaScale bullion and GCOS, 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
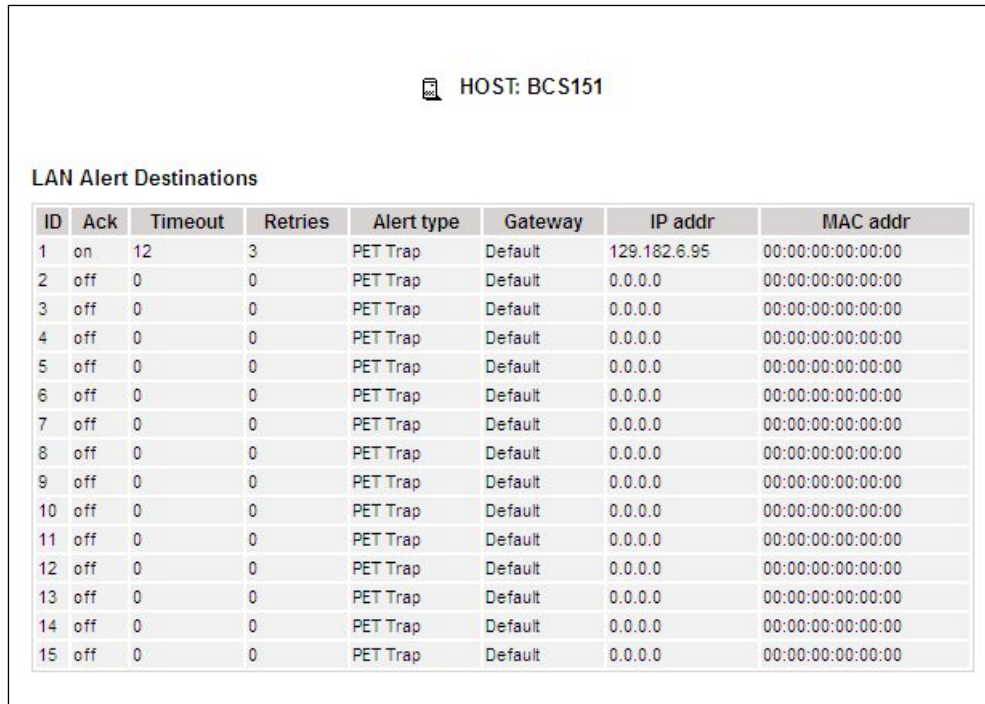
Figure 4-7   PAM History Output – Example

LAN Alert Destinations

Click **LAN Alert Destinations** to display the configured alert destinations.

HOST: BCS151
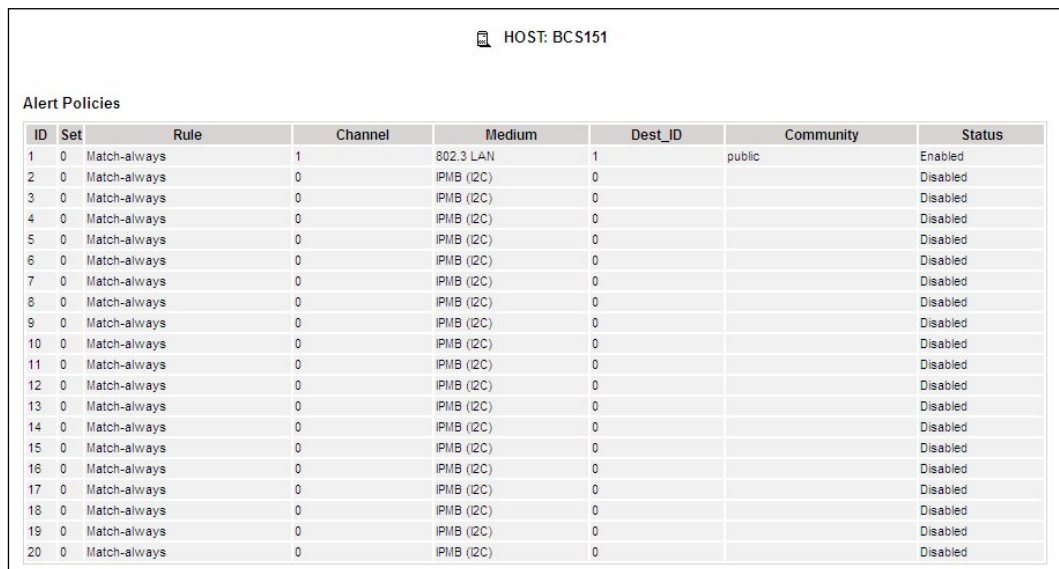
LAN Alert Destinations

ID	Ack	Timeout	Retries	Alert type	Gateway	IP addr	MAC addr
1	on	12	3	PET Trap	Default	129.182.6.95	00:00:00:00:00:00
2	off	0	0	PET Trap	Default	0.0.0.0	00:00:00:00:00:00
3	off	0	0	PET Trap	Default	0.0.0.0	00:00:00:00:00:00
4	off	0	0	PET Trap	Default	0.0.0.0	00:00:00:00:00:00
5	off	0	0	PET Trap	Default	0.0.0.0	00:00:00:00:00:00
6	off	0	0	PET Trap	Default	0.0.0.0	00:00:00:00:00:00
7	off	0	0	PET Trap	Default	0.0.0.0	00:00:00:00:00:00
8	off	0	0	PET Trap	Default	0.0.0.0	00:00:00:00:00:00
9	off	0	0	PET Trap	Default	0.0.0.0	00:00:00:00:00:00
10	off	0	0	PET Trap	Default	0.0.0.0	00:00:00:00:00:00
11	off	0	0	PET Trap	Default	0.0.0.0	00:00:00:00:00:00
12	off	0	0	PET Trap	Default	0.0.0.0	00:00:00:00:00:00
13	off	0	0	PET Trap	Default	0.0.0.0	00:00:00:00:00:00
14	off	0	0	PET Trap	Default	0.0.0.0	00:00:00:00:00:00
15	off	0	0	PET Trap	Default	0.0.0.0	00:00:00:00:00:00

Figure 4-8   LAN Alert Destinations – Example

Alert Policies

Click **Alert Policies** to display the configured alert policies.

HOST: BCS151

Alert Policies

ID	Set	Rule	Channel	Medium	Dest_ID	Community	Status
1	0	Match-always	1	802.3 LAN	1	public	Enabled
2	0	Match-always	0	IPMB (I2C)	0		Disabled
3	0	Match-always	0	IPMB (I2C)	0		Disabled
4	0	Match-always	0	IPMB (I2C)	0		Disabled
5	0	Match-always	0	IPMB (I2C)	0		Disabled
6	0	Match-always	0	IPMB (I2C)	0		Disabled
7	0	Match-always	0	IPMB (I2C)	0		Disabled
8	0	Match-always	0	IPMB (I2C)	0		Disabled
9	0	Match-always	0	IPMB (I2C)	0		Disabled
10	0	Match-always	0	IPMB (I2C)	0		Disabled
11	0	Match-always	0	IPMB (I2C)	0		Disabled
12	0	Match-always	0	IPMB (I2C)	0		Disabled
13	0	Match-always	0	IPMB (I2C)	0		Disabled
14	0	Match-always	0	IPMB (I2C)	0		Disabled
15	0	Match-always	0	IPMB (I2C)	0		Disabled
16	0	Match-always	0	IPMB (I2C)	0		Disabled
17	0	Match-always	0	IPMB (I2C)	0		Disabled
18	0	Match-always	0	IPMB (I2C)	0		Disabled
19	0	Match-always	0	IPMB (I2C)	0		Disabled
20	0	Match-always	0	IPMB (I2C)	0		Disabled

Figure 4-9   Alert Policies – Example

Platform Event Filters

Click **Platform Event Filters** to display configured filters applied to events.

Figure 4-10 Platform Event Filters – Example

Platform Manager

Click **Platform Manager** to open the platform management application. Look at BPM2.0_Install&UserGuide.

Figure 4-11 Platform Manager – Example

4.2 PNP4Nagios Reports

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

1. Launch the Bull System Manager Console from the Bull System Manager Home Page.

2. Click the **PNP4Nagios Reports** icon to display the list of all the reports.

Figure 4-12 Bull System Manager PNP4Nagios Reporting Indicators Home Page

Note   You can filter by substring the services list via the top form.

3. Select the report you want to display from:

  – The **Host** list
    To show an overview of all available services for a host.

  – The **Service** list
    To show all the available time range graphs for a service.

An example of the Window displayed when the host report is selected is shown below:

Figure 4-13 Bull System Manager PNP4Nagios Reporting Indicators - Example

This display shows 2 graphs. Each graph shows the evolution of a different indicator (**CPU load** and **% Memory used** in the example above) for a period of 4 hours.

The **Time ranges** box displays graphs for a given time interval.

The **Services** box toggles to display a detailed view of a service. Only available services are listed in the **Services** box.

Note   If you need more usage details for PNP4nagios, you can click on the following URL:
http://www.pnp4nagios.org/

4.3 Other Applications

You can launch external applications by clicking the appropriate icon in the **Other Tools** area. 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.

Figure 4-14 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 I**nternet.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 NSCP 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 10 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 Warning or Error event.

- Status is set to WARNING if there are at least 3 Warning or Error events.

Status Information

If the status is set to WARNING or CRITICAL, the following detailed information is indicated:

Event Type	Error or Warning or Information
Count	Number of events with the same type, source and id
Source	Event source
Id	Event id

Examples:

```
Eventlog check ok
error - 1 ID 13 from SescLU<br>, eventlog: 1 > warning
```

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 Failures, Error and Warning events generated in the Security event log for the last 10 minutes.

- Status is set to CRITICAL if there is at least 1 Audit Failure, Warning or Error event.

- Status is set to WARNING if there are at least 3 Audit Failure, Warning or Error events.

Status Information

If the status is set to WARNING or CRITICAL, the following detailed information is indicated:

Event Type	Error, Warning, Information, Audit Success or Audit Failure
Count	Number of events with the same type, source and id
Source	Event source
Id	Event id

Examples:

```
Eventlog check OK
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 10 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 following detailed information is indicated:

Event Type	Error, Warning or Information
Count	Number of events with the same type, source and id
Source	Event source
Id	Event id

Examples:

```
-------------------------------------------------------------------------------------------------------------------------
Eventlog check ok
error - 1 ID 13 from SescLU<br>, eventlog: 2 > warning
-------------------------------------------------------------------------------------------------------------------------
```

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.

Examples:

```
OK: 1m: average load 6%, 10m: average load 5%
WARNING: 1m: average load 85% > warning, 10m: average load 65% > warning
```

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 paged memory 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 paged memory size in Mbytes or Gbytes, the paged memory used in Mbytes or Gbytes and percentage, the paged free memory in Mbytes or Gbytes and percentage.

Examples:

```
OK: paged bytes: Total: 5.26G - Used: 1.59G (30%) - Free: 3.68G (70%)
WARNING: paged bytes: Total: 5.26G - Used: 3.79G (72%) - Free: 1.47G
(28%) > warning
```

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

The following service is available for the WindowServices 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 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: started
CRITICAL: Eventlog: stopped (critical)
```

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

The following categories are available for hardware monitoring.

5.4.1 Power Category for NovaScale bullion & GCOS, NovaScale T800 & R400 Series

The following category is available:

5.4.1.1 Status Service

The **Power.Status** 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.

5.4.2 Hardware Category for NovaScale bullion & GCOS, NovaScale T800 & R400 Series

The following category is available:

5.4.2.1 Alerts Service

The **Hardware.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.

5.4.3 Hardware Category for Blade Series

The following category is available:

5.4.3.1 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.

5.4.4 Hardware Categories for Escala Servers

The following categories are available:

5.4.4.1 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.

5.4.4.2 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.

5.4.5 Hardware Category for NovaScale 4000 Series

The following categories are available:

5.4.5.1 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 filtered previously 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.

5.4.5.2 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.

5.4.5.3　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.

5.4.6　Hardware Category for Express 5800

The following categories are available:

5.4.6.1　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. |

5.4.6.2 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.

5.4.7 Hardware Category for NovaScale 3000 Series

The following categories are available:

5.4.7.1 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.

5.4.7.2 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.

5.4.8 Hardware Category for NovaScale 5000 & 6000 Series

The following categories are available:

5.4.8.1 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.

5.4.9 Hardware Category for NovaScale 9010 Series

The following category is available:

5.4.9.1 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 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.

5.5 Blade Monitoring

The following category is available:

5.5.1 CMM Category

The following services are available:

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 Add-ons Guide* (Bull REF: 86A259FA) for more information about the storage and/or virtualization monitoring services.

Appendix A. Third Party License Agreements

The table below lists the license details for the third party software used by **Bull System Manager**.

Software Tool	License Type	More Information	License available from
Apache	Apache	www.apache.org/licenses/	www.apache.org/licenses/
IPMItool	BSD	ipmitool.sourceforge.net/	
MYSQL	GPL	hwww.mysql.com/about/legal/licensing//opensource-license.html	www.gnu.org/licenses/gpl.html
Net-SNMP	BSD	www.net-snmp.org/about/license.html	www.net-snmp.org/about/license.html
Nagios	GPL	www.nagios.com/legal/licenses	www.gnu.org/licenses/gpl.html
OCS Inventory	GPL	www.ocsinventory-ng.org/en/about/licence.html	www.gnu.org/licenses/gpl.html
Webmin	BSD	www.webmin.com/intro.html	
Cygwin	GPL	cygwin.com/licensing.html	www.gnu.org/licenses/gpl.html
SNMPTT	GPL	snmptt.sourceforge.net/license.shtml	www.gnu.org/licenses/gpl.html
UltraVNC	GPL	www.uvnc.com/general/license.html	www.gnu.org/licenses/gpl.html
PHP	PHP/BSD	www.php.net/license/	http://www.php.net/license/
winPcap	winPcap	www.winpcap.org/misc/copyright.htm	
RRDtool	GPL	oss.oetiker.ch/rrdtool/license.en.html	www.gnu.org/licenses/gpl.html
PNP4Nagios	GPL	www.pnp4nagios.org/	www.gnu.org/licenses/gpl.html
NSClient++	GPL	www.nsclient.org/nscp/	www.gnu.org/licenses/gpl.html

Note   Bull System Manager Remote Hardware Management CLIs use the following third party software tools: **IPMITool**, **Cygwin** and **NET-SNMP**. See the table above for license details for these tools.

Glossary

A

Add-on

Provides extensions to Bull System Manager to manage specific devices or tools.

Alert

Notification of a problem via e-mail, SNMP trap or Bull format autocall.

Alert Mode

Alerts Mode displays alerts (also called events) for a set of **Hostgroups, Hosts** and **Services** monitored by **Alert Viewer** application in the BSM Console.

Autocall Server

Used to relay notifications to Bull support.

B

BMC

Baseboard Management Controller. See Embedded Management Controller.

BSM

Bull System Manager.

BSM Console

See Management Console

C

Category

A **category** is a container for a group of services, for example, the **SystemLoad** category for Windows systems contains both the **CPU** and **Memory** services for a Windows host.

CIM

Common Information Model.

CLI

Bull Command Line Interface for local or remote hardware management and for automation scripts that can, for example, power on/off or obtain the power status for a system.

CMM

Chassis Management Module.

Configuration GUI

Used to configure BSM settings for Topology, Third-Party Applications, Supervision, Console, Local Settings and Global Settings.

Contact

Defines the target for BSM notifications

Contactgroup

Groups contacts together to be notified about the events (alerts/recoveries which occur for a host or service.

Control GUI

Used by the Administrator to start, stop, restart or obtain a status for **BSM Server**.

D

DHCP

Dynamic Host Configuration Protocol.

Distributed Solution

Used for a group of BSM servers that are linked together with a centralized database. The monitoring data is visible via the **Global Console**.

Domain

Hosts for **NovaScale 5000** and **6000** series.

E

EMM

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

Event Handler

An optional command executed when the status changes for a monitored **host** or **service**. These commands are executed locally on the BSM server.

Event Reception

Reception of SNMP traps, defined in a MIB, from SNMP agents.

F

Focus Pane

Used by the GUI to display monitoring services specified by the user.

FRU

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

G

Global Console

Used to manage all configured hosts for a set of BSM servers.

GTS

Global Transaction Server

GUI

Graphical User Interface

H

Hardware Manager

The **Hardware Manager** manages hardware for a server or a set of servers.

Hardware Partition

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

HMC

Hardware Management Controller.

Host

The **Host** is the main resource to be monitored and can be a physical server, workstation, hardware or virtual platform, device etc. The Administrator has to define the host properties (**Operating System, Model, Notification properties,** etc.) for all the hosts in the configuration.

Hostgroup

A **Hostgroup** structures hosts into logical entities that reflect your environment. Hostgroup statistics show the status for the Hostgroup elements.

Hostlist

List of hosts associated with a host group.

Hosts view

Window that displays all configured hosts with their status.

I

IPMI

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

IPMItool

For remote operations on hardware systems that contain **Intel BMC**s (Baseboard Management Controller).

J

No entries

K

No entries

L

LDAP

Lightweight Directory Access Protocol.

M

Management Agent

Instrumentation and administration tools used to obtain monitoring and inventory information.

Management Console

Used to graphically view, monitor and manage all the hosts configured for administration by the associated Management Server.

Management Server

Provides the infrastructure and services required to collect, process and store operational and monitoring data

Management Tree

A hierarchal 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 sub-nodes.

Map Mode

A representation of **hostgroup**s located at specified positions (x,y) and animated according to their status. Zooming in on a hostgroup displays the associated hosts and the overall service status (derived from the worst service status for all the associated services monitored).

MIB

Management Information Base.

Monitoring Service

A monitoring service defines how specific host elements are monitored. A service can be defined for all hosts or for a list of hosts, depending on the OS (**Windows**, **Linux**, **AIX** or any) and/or on the model.

MySQL

Structured Query Language Relational Database Management System (RDBMS) that runs as a server providing multi-user access to a number of databases.

N

Nagios

Open Source monitoring tool.

NDOutils

Used to store all the **Nagios** status information in a **MySQL** database.

NIC

Network Interface Controller.

NSCA

Nagios Service Check Acceptor is used to send service check results to the BSM server securely.

O

OCS Inventory Ng

For the inventory information collected via the Operating System and centralized in a database.

P

PAM

Platform Administration and Maintenance Software

Performance Indicators

Used as long-term counters reflecting specific functional qualities. The **PNP4Nagios** server extension is used to collect the performance indicators.

PDU

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

PHP

PHP: Hypertext Preprocessor. A server side scripting language.

Platform

A particular Hostgroup defined to represent a common set of hosts from the same series, for example, an **Escala** server might contain one or more hosts.

PNP4Nagios

Analyzes performance data provided by plug-ins and store it automatically in RRD databases.

Q

No entries

R

RRD

Round-robin database.

RRD Indicators

Monitoring service performance indicators collected and stored in RRD files in a defined RRD database by the PNP4Nagios Nagios extension.

S

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.

Service group

A **service group** is a list of instantiated services that can be used to filter topological views and maps, for example, the **OperatingSystem** service group includes all services that monitor OS items (meaning all categories that monitor the Operating System).

SNMP

Simple Network Management Protocol.

Storage Manager

The **Storage Manager** manages storage for one or a more servers and/or bays.

Supervision Mode

A **BSM Console** data resource viewing mode, either **Tree mode** or **Map mode** or **Alerts Mode.**

T

Timeperiod

Timeperiods are used to control when hosts and services are monitored or when contacts receive notifications.

Topology

A representation of the hosts, hostgroups, hardware managers, storage managers and virtualization managers that are monitored.

Tree mode

Hierarchical display of all the resources defined in the Bull System Manager configuration. Each node in the tree may contain sub-nodes that can be selected for more specific information.

U

UltraVNC Server

For remote operation on **Windows** hosts.

V

View

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 their User role (Administrator or Operator).

Virtualization Platform

A particular Hostgroup defined to represent a set of virtual machines. For example, the VMware ESX servers are commonly represented as a virtualization platform grouping the virtual machines together.

Virtualization Manager

The **Virtualization Manager** manages the virtual elements of a Virtualization platform.

W

WBEM

Web-Based Enterprise Management.

Webmin

A **Linux** administration tool (Bull System Manager **Webmin** restricted to obtaining information).

Bull Cedoc

357 avenue Patton

BP 20845

49008 Angers Cedex 01

FRANCE