Bull NovaScale Master

User’s Guide

ORDER REFERENCE
86 A2 49EG 04

Bull NovaScale Master

User's Guide

Software

July 2005

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

ORDER REFERENCE
86 A2 49EG 04

Printed in France

Suggestions and criticisms concerning the form, content, and presentation of this book are invited. A form is provided at the end of this book for this purpose.

To order additional copies of this book or other Bull Technical Publications, you are invited to use the Ordering Form also provided at the end of this book.

Trademarks and Acknowledgements

Preface

Table of Contents

Table of Figures

Scope and Audience of this Manual

This manual is intended for operators in charge of monitoring and managing Bull NovaScale and Express5800 servers with NovaScale Master, in particular via the NovaScale Master Console. It comprises the following chapters:

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

Highlighting

The following highlighting conventions are used in this manual:

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

Note: Important information

Related Publications

- For more information about NovaScale Master, please refer to:

  NovaScale Master Installation Guide (Ref. 86 A2 48EG)

  NovaScale Master Administrator's Guide (Ref. 86 A2 50EG)

  NovaScale Master Remote Hardware Management CLI Reference Manual (Ref. 86 A2 88EM)

- For more information about the Bull NovaScale 2000 and 4000 series, please refer to:

  Bull NovaScale Blade 2020 Installation and User's Guide (Ref. 86 A1 03EM)

  Bull NovaScale Blade 2040 Installation and User's Guide (Ref. 86 A1 34EM)

  Bull NovaScale 4020 User's Guide (Ref. 86 A2 72EG)

  Bull NovaScale 4040 User's Guide (Ref. 86 A1 26EG)

- For more information about the Bull NovaScale 5000 and 6000 series and PAM software, please refer to:

  Bull NovaScale 5xx0 & 6xx0 User's Guide (Ref. 86A194EM)

  Bull NovaScale 5xx0 & 6xx0 Guide Utilisateur (Ref. 86F194EM)

  Bull NovaScale 5xx5 & 6xx5 User's Guide (Ref. 86A141EM)

  Bull NovaSCale 5xx5 & 6xx5 Guide Utilisateur (Ref. 86F141EM)

- For information about the Intel Server Manager (ISM) management tool or Blade Chassis Management Module (CMM), please refer to the documentation provided by Intel.

- For information about the Open Source products used by NovaScale Master, please refer to:

  www.nagios.org (for Nagios product)

  www.webmin.com (for Webmin product)

  mrtg.hdl.com (for MRTG product)

Chapter 1. About NovaScale Master

Scope

NovaScale Master is the graphical interface tool used to manage Bull NovaScale and Express5800 servers. It provides two main functions:

Supervision (monitoring, reporting, information).
Supervises system resources.

Detects anomalies and notifies them to defined entities. It also provides the interface that displays all important information.

Administration (remote control).
Used to configure target hosts and to execute actions on these hosts via the OS or via a Hardware Management tool.

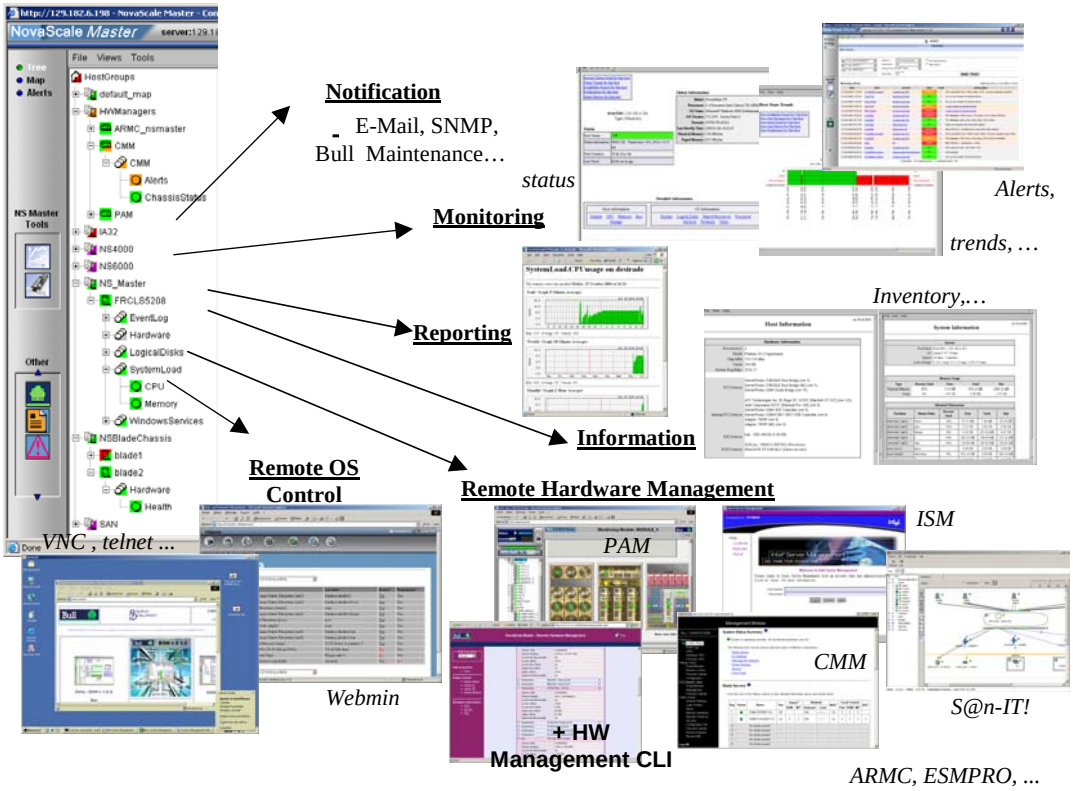


Figure 1. Overview of NovaScale Master functions

Two NovaScale Master user roles are pre-defined:

- O**perator Role:**
  An operator can read host and operating system information, but has no access to the administration tools.
- A**dministrator Role:**
  An administrator can perform administration, configuration, update, and remote control tasks on target hosts.

Supervision Features

- **Host Monitoring**:
  Checks if the target host is accessible (via the **ping** command).
- **Monitoring Services**:
  Monitors OS CPU load, memory usage, disk usage, number of users, processes and services execution, http and ftp services.
  Thresholds are used to assign a state (**ok, warning, critical, unknown**) to hosts and to each monitored element.
  Alerts (in a log file) and notifications (by email) are generated when anomalies occur or when normal states are recovered (return to ok state).
  Monitoring Services are classified into Monitoring Categories: **SystemLoad**, **Filesystems**, **EventLog**…
- **Hardware Monitoring:**
  NovaScale servers gets hardware health status via a call to CMM, ISM and PAM Hardware Managers.
  Express5800 servers gets power status via a call to the RMC Management Card.
- Selectable View Displays:
  Presentation of hosts and monitoring services through different **views**.
  A **view** is a tree structure that can display:
  - the entire list of hosts,
  - 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 user roles (Administrator or Operator).
- Group Definitions:
  Host groups and Group groups can be defined to organize server infrastructure as a tree.
- **Alerts:**
  Notifications of problems via email, SNMP traps or Bull format autocalls.
- **Selectable Map Displays:**
  Presentation of hostgroups (with the status of their hosts and monitoring services) through different maps.
  A **map** is a layout, in general with a background image, that displays associated hostgroups.
  Hostgroups are located at specified positions (x,y) on the map and are animated with the status of associated hosts and monitoring services.
  From a hostgroup, the user can display detailed information about all associated hosts.

Administration Features

- **Webmin** Management Tool for Linux hosts.
  Webmin is an OpenSource product that gives OS information (about users, filesystems…) or executes OS commands, in a graphical environment, locally on Linux target hosts.
- **Remote Operation Tools**:
  telnet to access Linux and Windows hosts.
  tightVNC to access Windows hosts.
  tightVNC is an Open Source product that allows you to take control of remote hosts as if you were in the remote host Windows environment.
- **Hardware Manager Calls:**
  PAM for NovaScale 5000 and 6000 Series platforms.
  CMM for NovaScale Blade Series Chassis 2000 platforms.
  ISM for NovaScale 4000 Series hosts.
  ARMC (or/and ESMPRO) for Express5800 platforms.
  For example, systems can be powered on / off via these managers and NovaScale Master provides a single Hardware Management GUI for basic tasks.

Basic Definitions

Service

A **service** is a monitoring check which supervises a monitored item.
Monitoring agents compute service status (OK, Warning, Critical, Unknown or Pending) and status information (a text giving more information on the service state) for each service.

Example:
The **CPU service**, which returns a status about CPU utilization, displays the following information on Windows:

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

Category

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

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

View

A **view** is how monitored hosts are displayed on the screen. Views differ in structure, but they all display hosts with an animation reflecting service status (ok, warning, critical, or unknown) and associated monitoring services, classified into categories, under the host node.

The advantage of views is to display only what the user wants to see at a given time. For example, if a user is interested in Hosts and not in Managers or Hostgroups, he can display the **Hosts** view.

As Administrator, you can create customized views for hosts and groups. Refer to the *Administrator's Guide* for details.

Notes:

- According to configuration, a category may or may not be present. For details, refer to the *Administrator's Guide*.
- Each type of node in a view has specific menus detailed later in this manual.

Map

A **map** can be used to display the status of a selection hostgroups (with their monitored hosts) on the screen.

In general, the map has a background image and hostgroups are located at specified positions (x,y) on the map. Maps differ in appearance, but they all display hostgroups with an animation reflecting service status computed from the status of the associated hosts and monitoring services.

When you zoom in on a hostgroup, you can view associated hosts and overall service status (the worst status of the associated monitoring services).

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

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

NovaScale Master Components

NovaScale Master is based on a 3-tier architecture:

- **Monitoring Console**
  This WEB-based application running in a browser (Internet Explorer or Mozilla) accesses collected monitoring data using WEB technology.
- Monitoring Server
  Collects, processes and stores monitoring and reporting data. It runs on both Windows and Linux platforms.
- Monitoring Agent
  Contains the basic programs used to obtain monitoring and inventory information. It is installed on each target system.

NovaScale Master comprises Open Source software:

- **Nagios**
  For the monitoring function.
- **MRTG**
  For the reporting indicators function.
- **Webmin**
  A Linux administration tool (a standard Webmin package and a NovaScale Master Webmin restricted to obtaining information).
- **TightVNC Server**
  For remote operation on Windows hosts.
- **IPMItool**
  For remote operation on hardware systems.

NovaScale Master also comprises an optional component for scripting applications on Linux platforms:

- **Hardware Commands**
  A Command Line Interface (CLI) for remote hardware management, providing an easy interface for automating scripts to power on/off or get the power status of a system. These commands can only be used on Express5800 or, NovaScale 4000, 5000 and 6000 series servers with a Linux Operating System.

NovaScale Master and Security

NovaScale Master security is based on a combination of secured applications using authentification and profiling (role based) mechanisms.

Authentication

Each NovaScale Master application uses a **user/password** or **single password** authentication mechanism for access. Users are defined on the NovaScale Master server.

Role-based Management

Each NovaScale Master Console user is associated to a role (or set of functionalities). There are two types of profiled users:

- **Operator**
  An operator can read host and operating system information, but has no access to the administration tools.
- Administrator
  An administrator can perform administration, configuration, update, and remote control tasks on target hosts.

Chapter 2. Getting Started

This chapter explains how to use NovaScale Master for basic monitoring and administration tasks.

Starting the Console

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

Console Basics

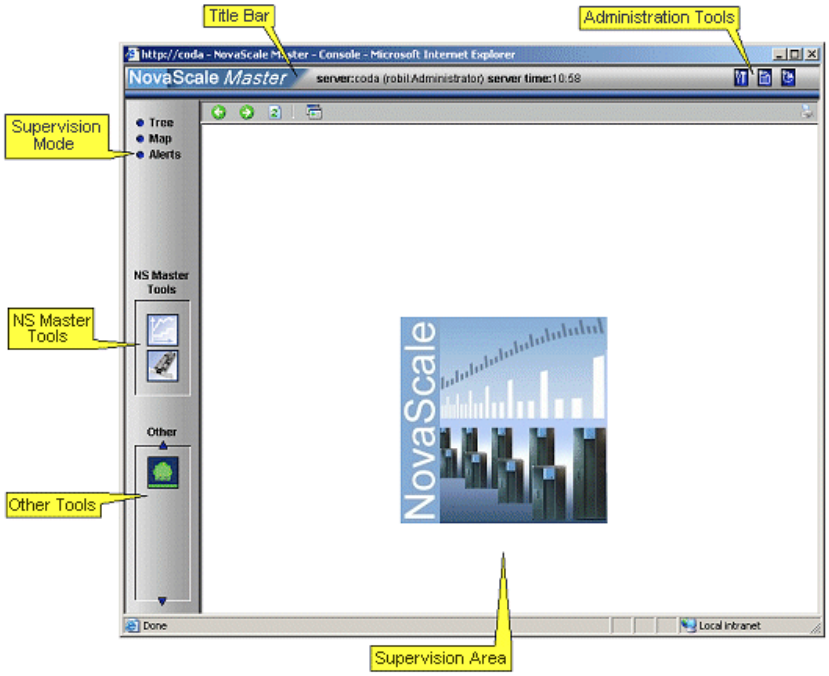


Figure 2. NovaScale Master console

The NovaScale Master console is divided into the following functional parts:

Title Bar	displays the server name, the server time, the user and the role.
Administration Tools	enables access to the administration tools: NovaScale Master configuration application, NovaScale Master documentation and NovaScale Master download page.
Supervision Mode	allows you to choose one of the three modes of supervision: supervision through a tree, supervision through a map and supervision through alerts.
Supervision Pane	displays information about the monitored resources, related to the type of supervision (see *Supervision Information*, on page 3-22).
NovaScale Master Tools	enables access to the NovaScale Master Tools: Reports and Hardware Management.
Other Tools	enables access to external applications.

NovaScale Master Authentication and Roles

NovaScale Master applications must be authenticated. They use common NovaScale Master users defined on the server part.

Authentication type varies according to the NovaScale Master Server operating system (Linux or Windows) and to the WEB Server (Apache or Microsoft IIS). (see next paragraphs).

Note:
In order to change the current authentification for NovaScale Master. You MUST close all the opened WEB browser windows. And relaunch a new session of this browser. Else, the browser will keep the previous authentification context.

Role Based Management

Moreover, the authenticated user is used to apply a user profile or role.

Two default roles have been defined for NovaScale Master:

- **Operator** with access only to supervision information.

- **Administrator** with access to supervision information, configuration tasks and Remote Control functions.

Applications	Roles	Functions
Monitoring and Reporting	Operator	Information access
	Administrator	+ server control access
Remote Control OS	Operator	None
	Administrator	Remote Control access
Hardware & Storage managers	Operator	Information access
	Administrator	+ Remote Control access

Table 1. Roles and Functions

Note:
User roles can be only configured by a user with Administrator role. For further details, refer to the *Administrator's Guide*.

NovaScale Master Server User Authentication - Linux

Apache server authentification

A default Apache user called **nsmadm** (password **nsmadm**) is created when NovaScale Master Server is installed. This user is not a Linux user and will only be used contextually by this WEB Server.

Figure 3. nsmadm user authentication - Linux

The users database is stored in the following file:
/usr/local/bull/SystemManagement/core/etc/htpasswd.users

Adding a New User / Modifying a Password

To add a new user or to modify a password on the Apache server:

1. Log on as **root** and launch the following command followed by the required user name:

   # htpasswd /usr/local/bull/SystemManagement/core/etc/htpasswd.users <USERNAME>

2. Enter the *n*ew password: *****
3. Re-type the new password: *****
   Adding password for user <USERNAME>

where <USERNAME> is the user name you want to add or modify.

Authenticated users are users declared in the Windows users database.

Using Internet Services Information WEB Server

The user can be a local user or a domain user. The domain must be specified for domain users (e.g **DOMAIN\User).**

Figure 4. User authentication with IIS WEB Server - Windows

Using Apache WEB Server

Any user in the Windows user database of the server, or any trusted domain to which the server belongs, will be granted access.

The user name must be entered in the following format: **DOMAINNAME\Username**, even for local users. The domain name must be fully qualified.

Figure 5. User authentication with Apache WEB Server - Windows

This chapter continues with the description of what you can do with the console.

Displaying Monitoring Information

Starting with the Tree mode

Notes:

- Tree Mode concepts are explained in detail in Chapter 2.
- When the Console is started, the default view is opened, i.e. the **Hosts** view, displaying all the declared hosts at the same level.
  By clicking in the File menu, you can load three other views: the **Hostgroups** view, the **HardwareManager** view or the **StorageManager** view.
  As Administrator, you can change the default view and advanced users can create customized views. Refer to the *Administrator's Guide* for details.

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

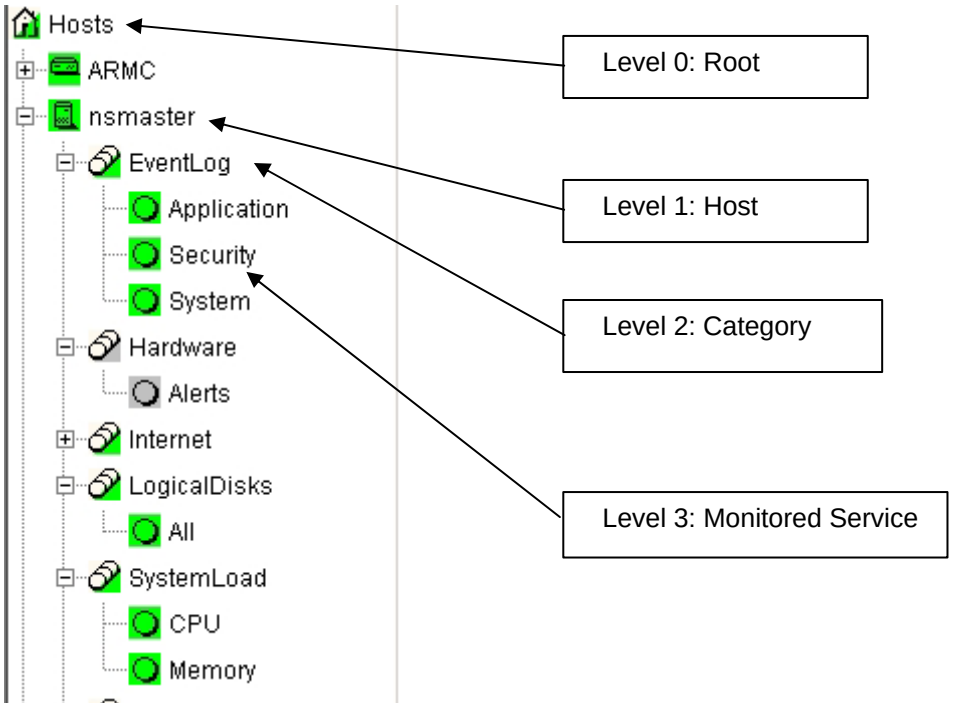


Figure 6. Example of expanded Hosts tree

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

Each icon is divided into two sections:

The top left is reserved for the animation for itself and the bottom right is reserved to cascade animation from its subtrees.

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

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

Example:

The top left corner of the nsmaster host node is green because it is alive and the bottom right corner is green because all its services are ok.

A **Category** is a node grouping monitored services logically. Category status reflects the worst status of its associated services..

Looking in the Past

When a problem occurs, it is interesting to know if it already occurred in the past, and how many times it occurred.

NovaScale Master offers many ways to analyze what occurred in the past.

Looking in the Past with Alert History

From the Applications pane, click **Reporting -> Alert History**. The following display appears (in this example, the host is called NSMASTER).

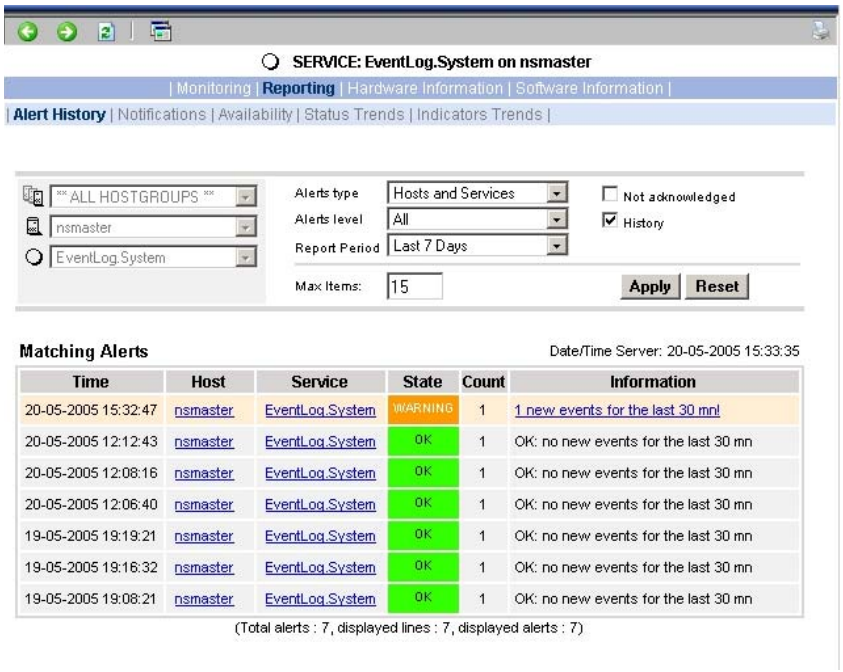


Figure 7. Alert History window

The history shows all the alerts that occurred for this service, in periods of time. Service information is also logged, providing all the information required to decide if a corrective action is needed.

Looking in the Past with Status Trends Information

The **Alerts** and **Trends** functions use monitoring logs to display past information:

- Alerts shows events.
- Trends shows a status graph for a given period of time.

In the example shown in Figure 8. the monitored system is FRCLS5208. The tree shows a **CRITICAL** state on **EventLog.Security. C**lick **Security** to display status information.

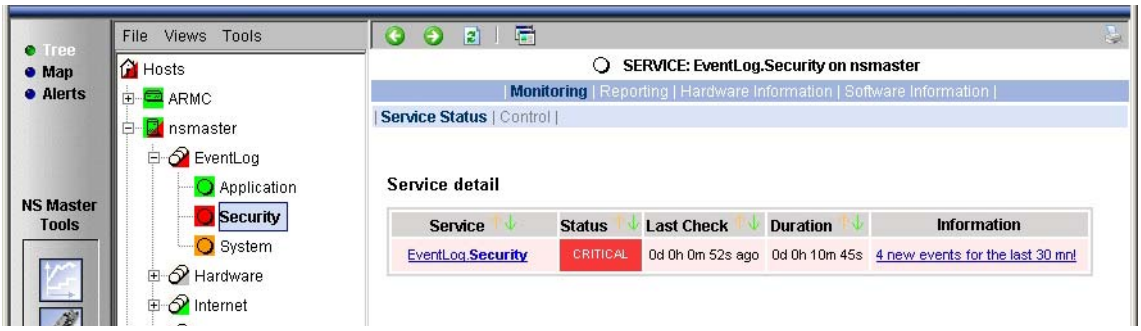


Figure 8. Status Information for EventLog.Security service

If you want to know if this situation often occurs, and when it occurs, click **Reporting** → **Status Trends**. The following display appears:

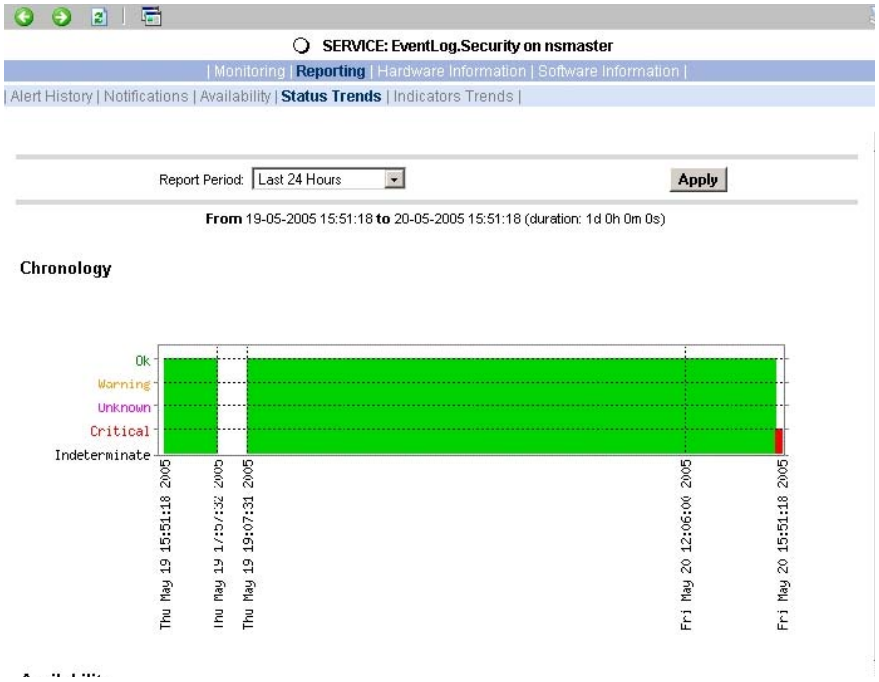


Figure 9. Status Trends for EventLog.Security service (last 24 hours) - example

The graph shows the situation for the last 24 hours and that nsmaster has detected a recent bad security access.

Viewing More Information

The Applications pane is used to display information requested by menu items or links.

Click a node in the Tree pane to display basic monitoring information, according to node type.

Right-click a node in the Tree pane to display a popup menu giving access to all operations available for that node.

Click an option in the double level menu in the Applications pane to access to all information available for that node.

Example:

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

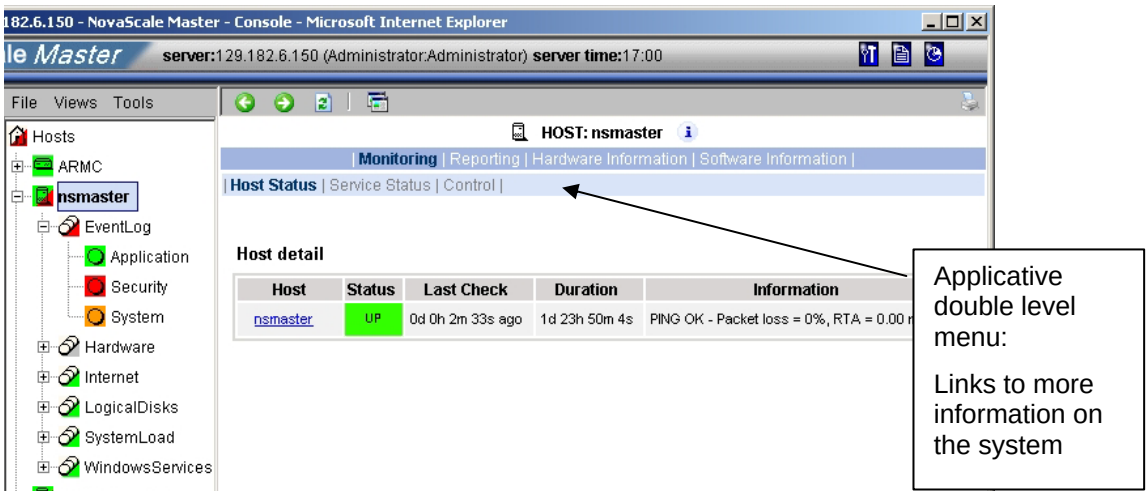


Figure 10. Host status display - example

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

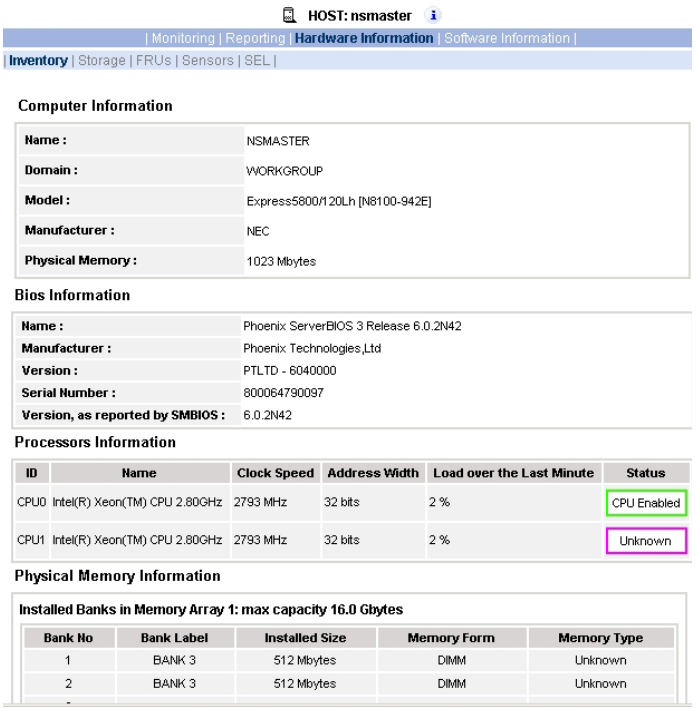


Figure 11. Host information - example

Receiving Alerts

As Administrator, once you have built your configuration, you can set up email and/or snmp notifications for enhanced operational monitoring

Sending Email Notifications

To configure the email notification mechanism, proceed as follows:

Step 1: Start NovaScale Master Configuration.

Step 2: Configure the Mail Server (only if NovaScale Master Server runs on a Windows system).

Step 3: Specify the mail address of the receiver.

Step 4: Reload the monitoring server to take the modifications into account.

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

Sending SNMP Traps Notifications

To configure the SNMP notification mechanism, proceed as follows:

Step 1: Start NovaScale Master Configuration.

Step 2: Specify the SNMP managers to which the traps will be sent.

Step 3: Reload the monitoring server to take the modifications into account.

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

Viewing Notifications

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

***** Bull NovaScale Master *****

Notification Type: PROBLEM

Service: LogicalDisks.Alls
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.

Figure 12. Example of email notification

The NovaScale Master Console allows you to view all the notifications sent by the monitoring server.

.

Taking Remote Control of a Host

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

Windows Hosts

tightVNC Viewer is used to to remotely connect to Windows hosts.

IPrerequisite:
The **VNC package** delivered with NovaScale Master must be installed and started on the remote host. Refer to the *Installation Guide* for details.

Example:
NovaScale Master 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 (**Remote Operation -> VNC Viewer**), .

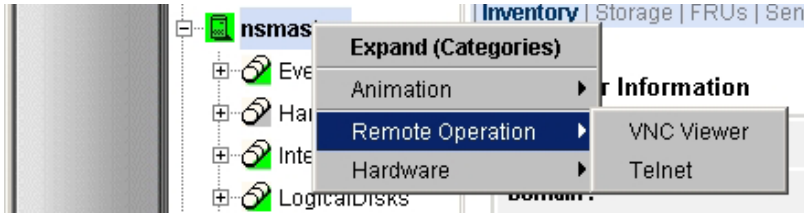


Figure 13. Starting tightVNC Viewer on a host

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

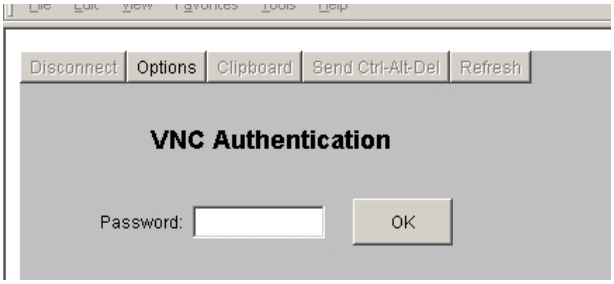


Figure 14. VNC Authentication window

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

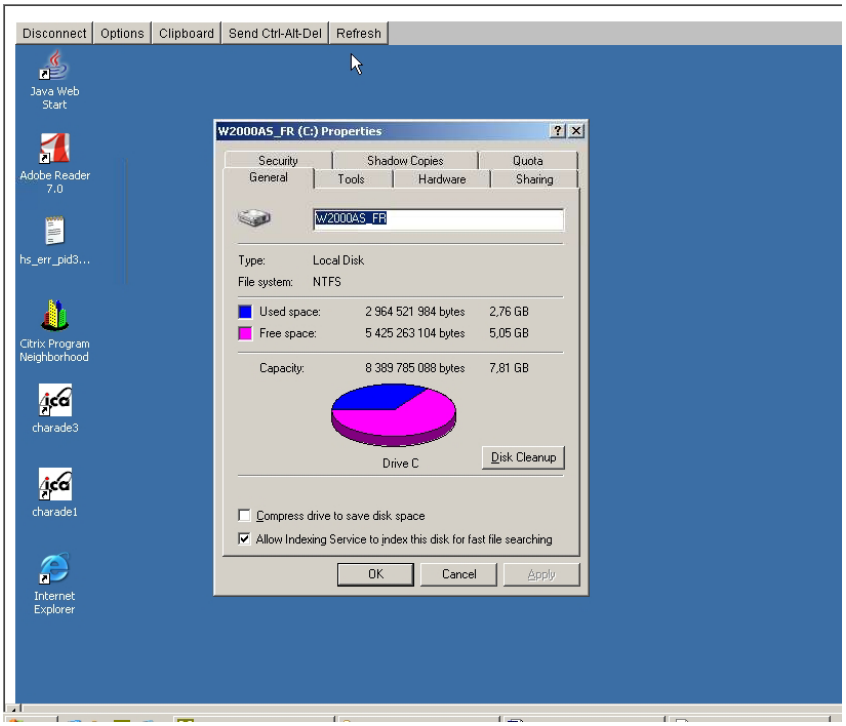


Figure 15. Remote connection to a Windows host with VNC Viewer

You can now display information related to disk C: and perform corrective actions.

Note:
If you do not require full access to the remote desktop, you can also open a **telnet** connection, if the **telnet service** is started on the remote host.

Linux Hosts

Webmin is used to remotely connect to Linux hosts.

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

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

1. From the FRCLS2681 host menu, select **Remote Operations->Actions->Users**.

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

Figure 16. Webmin login window

Note:
If the Linux host is running in SSL mode the following message appears, before the Webmin login page:
This web server is running in SSL mode. Try the URL https://FRCLS2681:10000/ instead.
You must click the link indicated in this message.

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

Username	User ID	Real name	Home directory	Shell
root	0	root	/root	/bin/bash
bin	1	bin	/bin	/sbin/nologin
daemon	2	daemon	/sbin	/sbin/nologin
adm	3	adm	/var/adm	/sbin/nologin
lp	4	lp	/var/spool/lpd	/sbin/nologin
sync	5	sync	/sbin	/bin/sync
shutdown	6	shutdown	/sbin	/sbin/shutdown
halt	7	halt	/sbin	/sbin/halt
mail	8	mail	/var/spool/mail	/sbin/nologin
news	9	news	/var/spool/news	
uucp	10	uucp	/var/spool/uucp	/sbin/nologin
operator	11	operator	/root	/sbin/nologin
games	12	games	/usr/games	/sbin/nologin
gopher	13	gopher	/var/gopher	/sbin/nologin
ftp	14	FTP User	/var/ftp	/sbin/nologin

Figure 17. Webmin interface on Linux hosts

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

Managing Hardware

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 NovaScale Master.

Each type of server has a dedicated hardware manager that NovaScale Master uses to perform these operations. NovaScale Master provides the appropriate menu item for each server type: , that is:

- PAM for NovaScale 5000 and 6000 series
- ISM for NovaScale 4000 series
- CMM for NovaScale Blade series
- ESMPRO for Intel based computers, running Windows
- RMC or ARMC for Intel based computers.
- 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 and CMM hardware managers **requires authentication.**
  Logins must be defined in the management modules before they can be used by NovaScale Master.
  CMM: only one session is allowed per user. You must therefore register one user for each NovaScale Master 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 NovaScale Master server as SNMP Manager when you configure the CMM.

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 to take the modifications into account.

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

Example:
Calling a configured PAM Manager:

The **Hardware -> PAM** item appears in the menu of the PF4B-10 host.

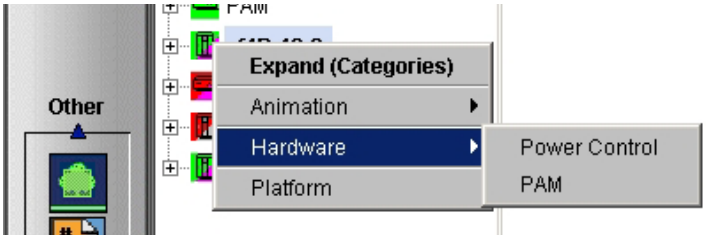


Figure 18. HW Manager GUI menu

Activating the **Hardware -> PAM** menu item calls the associated PAM HardWare Manager:

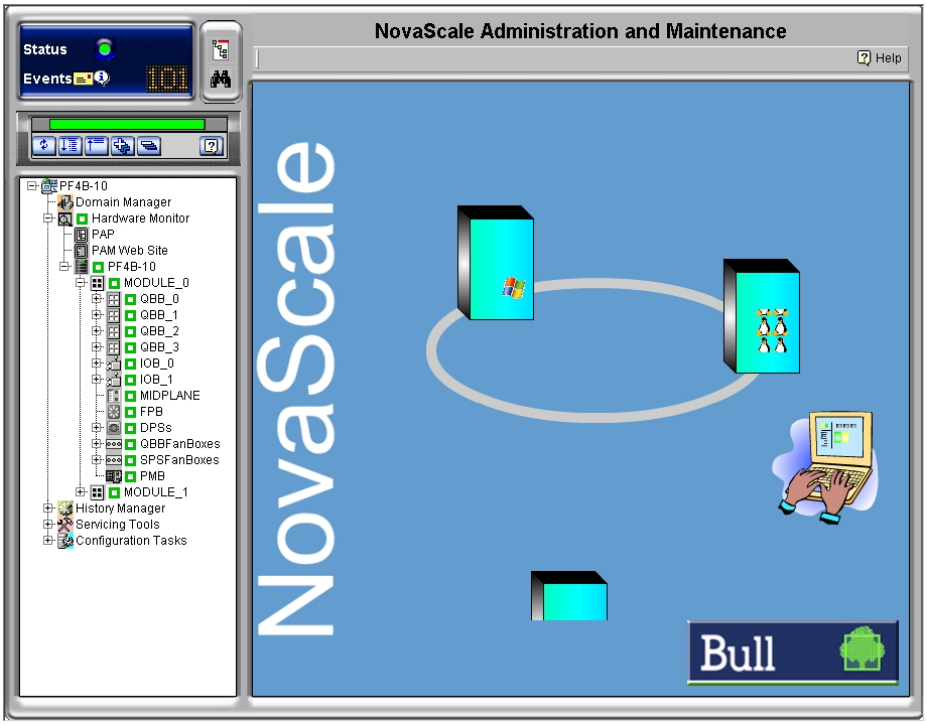


Figure 19. PAM Hardware Manager – Home Page

See the *Administrator's Guide* for details.

Using the NovaScale Master Hardware Management Application

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

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

To start the application:

1. From the Console Management Tree, click the **Hardware -> Remote Control** item in the host menu.

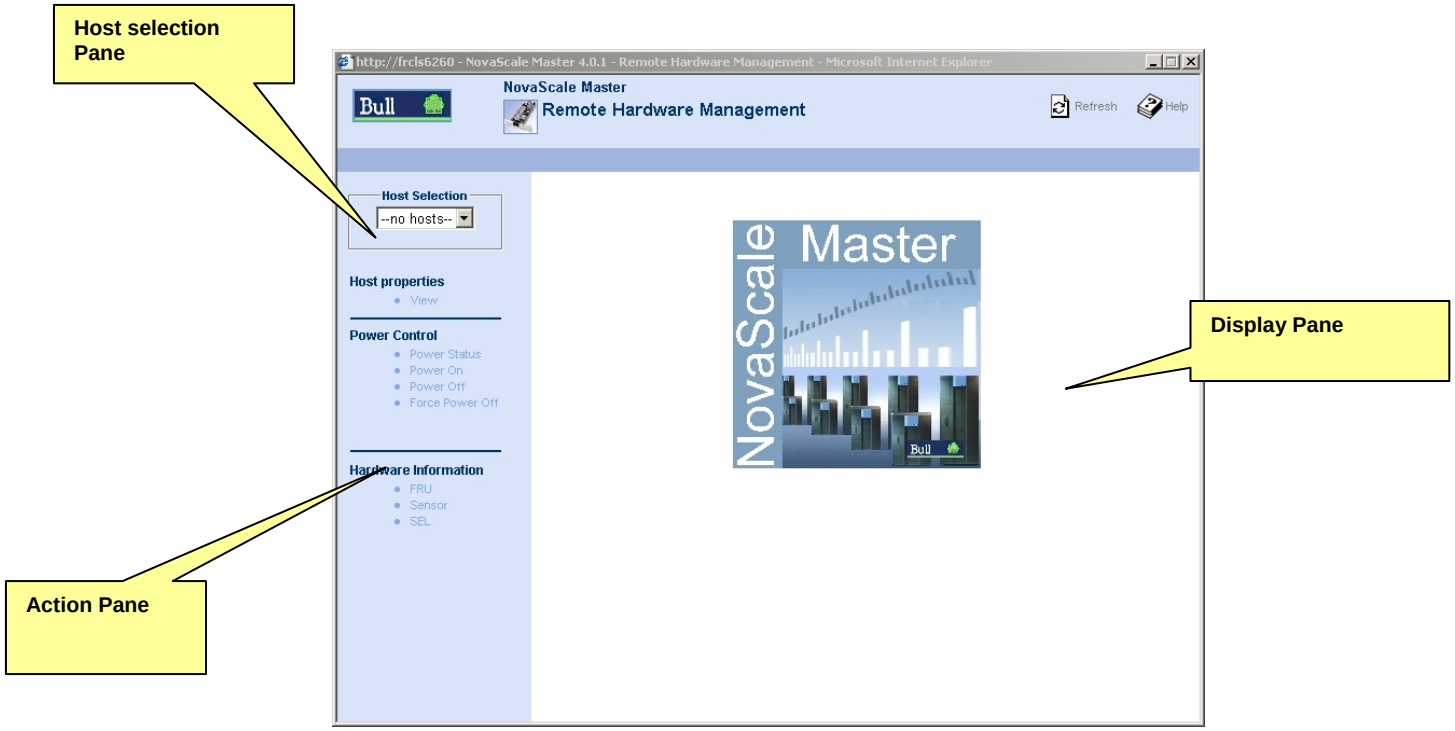


Figure 20. Remote Hardware Management window

The NovaScale Master Remote Hardware Management application window is divided into the following functional parts:

Host Selection Pane allows you to select the current host from all declared Express 5800 and NovaScale 4000, 5000 or 6000 series servers.

Action Pane displays the hardware operations that can be performed:

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

Display Pane displays parameters forms, messages and command results.

Following a Performance Indicator over a Large Period

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

Performance indicators can be collected from NovaScale Master monitoring data or SNMP protocol, as described below.

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

1. Launch NovaScale Master Console from the NovaScale Master Home Page.
2. Click the **Reports** icon to display the list of all available reports.
3. Select the report you want to display from the indicators list.

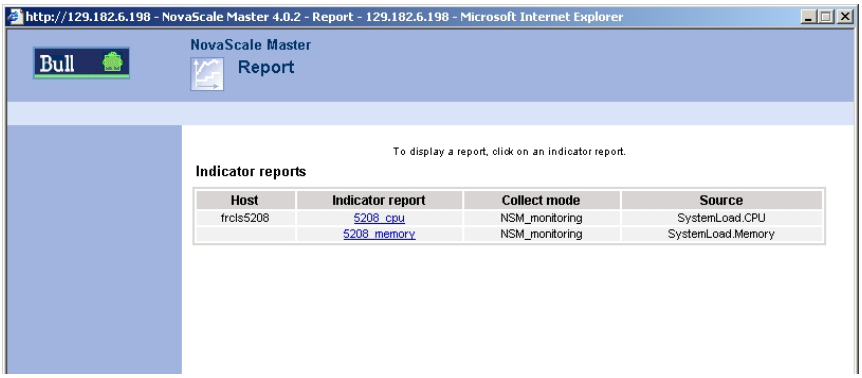


Figure 21. NovaScale Master Reporting Indicators Home Page

The following display appears:

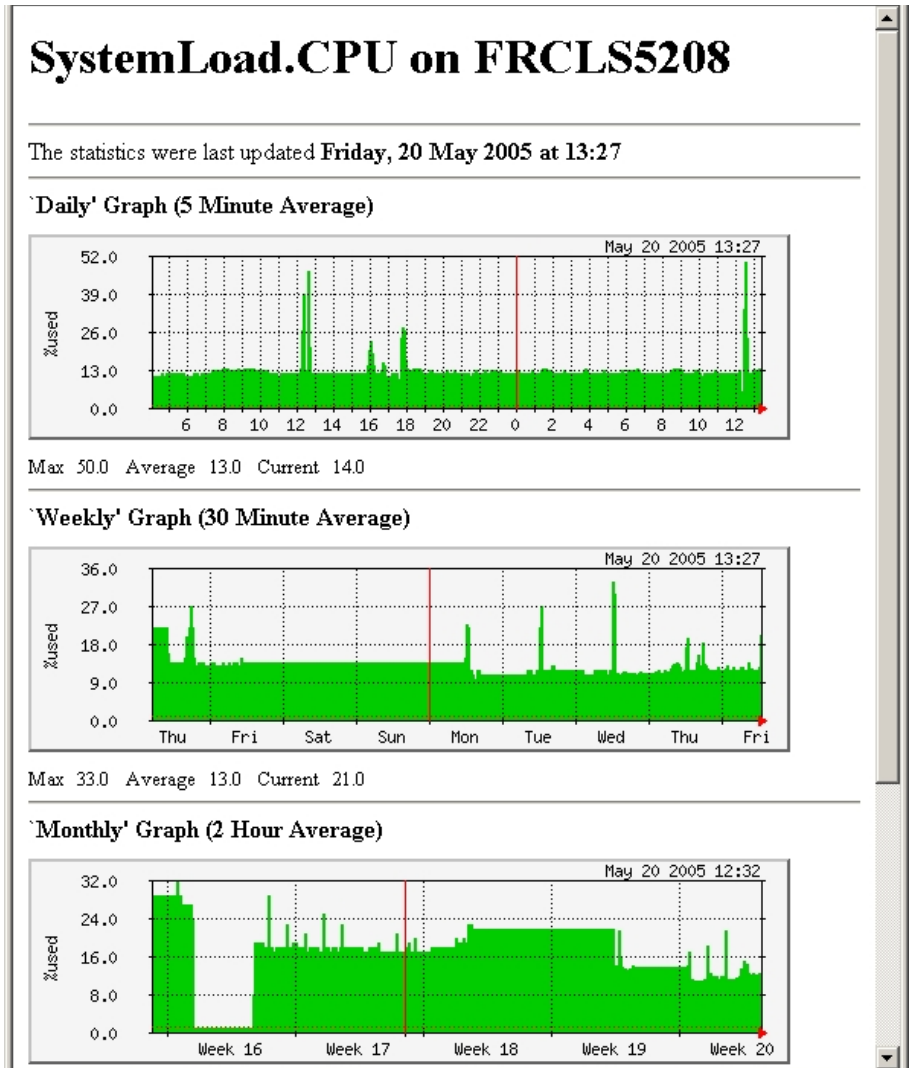


Figure 22. NovaScale Master Reporting Indicators - example

This display shows 4 graphs (3 visible in the example). Each graph shows the evolution of an indicator (here CPU load) for different periods (daily, weekly, monthly and yearly).

NovaScale Master Configuration

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

Chapter 3. Using NovaScale Master Console Supervision Modes

The NovaScale Master console provides three supervision modes, each providing its own representation of the NovaScale Master monitored resource:

- **Tree mode**
- **Map mode**
- **Alerts mode**

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

Note:
For further information about Console Basics and Console Security Access, refer to Console Basics and NovaScale Master Authentication and Roles

Working in the Tree Mode

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

Management Tree Basics

The Management Tree is a hierarchical representation of the resources defined in the NovaScale Master configuration. Each resource displayed in the tree is represented by a **node that may or may not have subnodes.**

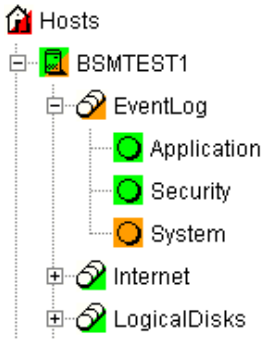


Figure 23. Management Tree

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

Select a node to automatically display its characteristics in the Supervision Pane.

Right-click the mouse to display the specific node menu.

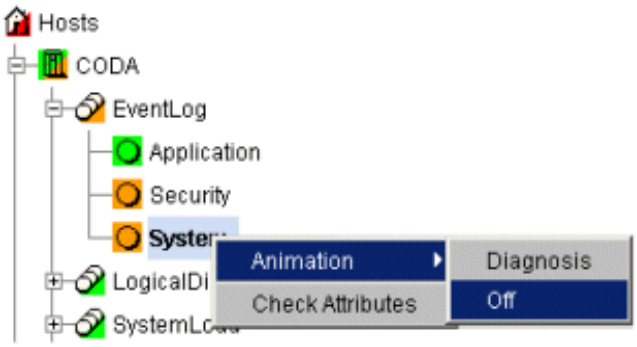


Figure 24. a service node menu

Upper the Management Tree, a menu provides the **File**, **Views** and **Tools** commands:

Figure 25. Management Tree menu

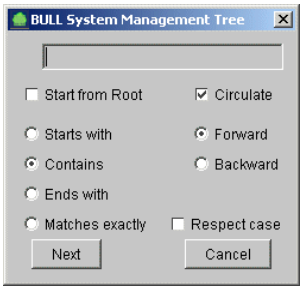
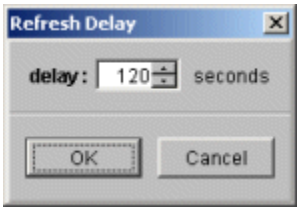
Management Tree Menu			
File	**-> Load**	Selects a view to be loaded.	
	-> Reload	Reloads the current view if the configuration has been modified.	
	-> Close	Closes the current view.	
	-> Hide Tree	Hides the tree to display the whole Supervision Pane	
Views		Displays the list of all loaded views: you can select one view.	
Tools	**-> Find**	Allows you to search a node in the current view according to its name or part of its name.	
	-> Refresh Delay	This dialog box allows you to modify the Management Tree animation refresh delay. The default refresh delay is 120 seconds.	

Figure 26. Management Tree commands

Note:
The refresh delay is only used by the Management Tree, not by applicative panes.

Management Tree Animation

The Management Tree is animated according to the following rules:

- Color is dependent on status:
  - Red: CRITICAL
  - Orange: WARNING
  - Magenta: UNKNOWN
  - Green: OK
  - Blank: UNMONITORED

  This color scheme is applicable to **hosts and services**.
- When a node has subnodes, the node icon is split in two. The top left triangle is animated to represent node status and the bottom right triangle to represent subnode status (i.e. most degraded status).
- Host and associated monitoring services node icons are animated to represent self-status. All other node icons are animated to represent subnode status (i.e. most degraded status).

Example:

SYSMAN (root node) and associated services are self-monitored. 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**.

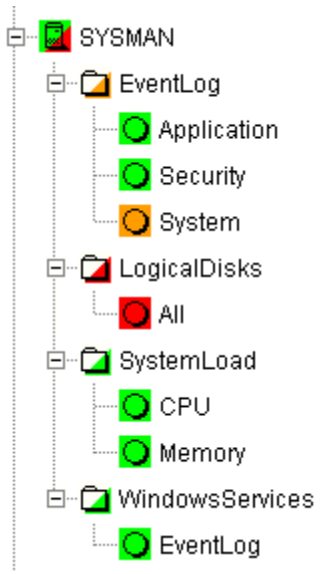


Figure 27. ManagementTree animation - example

Right-click the animated nodes to display the **Diagnosis** and **On/Off** menus:

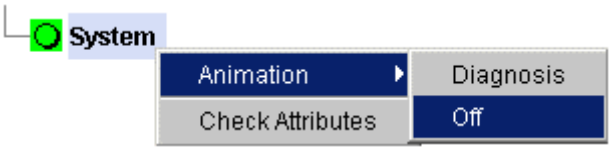


Figure 28. Animated node menu

Diagnosis	displays an animation information window.
On	activates node animation.
Off	deactivates node animation. This option is useful if you decide not to animate a specific service or host.

Example:

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

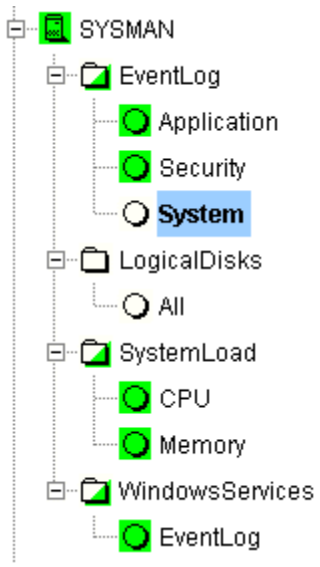


Figure 29. Deactivating supervision - example

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

Management Tree Nodes

Each NovaScale Master **monitored resource** is represented as a **node** with a specific icon in the animated Management Tree. Management Tree nodes are animated according to node status. When a node is selected, its characteristics are automatically displayed in the **Supervision Pane.**

Monitored Resourcest	Icons	Description
Root Node		First node in the tree.
HostGroup		Hosts can be grouped into hostgroups. For example, an administrator can define a hostgroup containing all NT servers. Doing so allows you to quickly identify a host in a degraded state, as host status is propagated up to the hostgroup node.
Group		Groups allow you to gather other groups and hostgroups in coherent entities. Refer to the *Administrator's Guide* for details.
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.
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.

Table 2. 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.

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 most degraded subnode status (host and services).

Root Node Menu	
Expand	Shows a tree view of all hosts, hostgroups or managers in the configuration.
Animation	Briefly explains resource status.

Table 3. Root node menu

HardwareManager Node and Status Levels

A HardwareManager node represents one of the five types of hardware managers listed in Table Management Tree Nodes above.

PAM and CMM Managers Status Levels

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

Manager (PAM, CMM) Status Levels	
Status	**Description**
PENDING (gray)	The service has not been checked yet. Pending status occurs only when **nagios** is started and disappears 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 plugin 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 4. PAM and CMM status levels

RMC Managers Status Levels

The top left triangle reflects power status and the bottom right triangle reflects the most degraded subnode status (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 and disappears as soon as services are checked.
OK (green)	The power status is on.
UNKNOWN (magenta)	An internal plugin error has prevented status checking. An unknown status is considered as a warning status.
CRITICAL (red)	The power status is off.

Table 5. RMC status levels

ISM and ESMPRO Managers Status Levels

The top left triangle reflecting self-status is always blank (unmonitored). The bottom right triangle reflects the most degraded subnode status (hosts and services).

 **HardwareManager 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.
->RMC, ISM or **ESMPRO**	Shows all hosts managed by these managers.
-> other managers	Shows all hosts managed by these managers.
Animation	Briefly explains resource status.
Hardware -> "manager GUI"	Calls the Manager GUI. This menu requires **Administrator rights**. The menu name changes according to manager type.

Table 6. Hardware Manager node menu

StorageManager Node

The StorageManager 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 most degraded subnode status (hosts).

StorageManager Node Menu	
Expand	Shows all hosts managed by this manager.
Animation	Briefly explains resource status.
Storage **-> Storage manager (Web)**	Calls the Manager GUI. The S@N.IT! Manager GUI is called **S@N.IT! GUI**.
-> S@N.IT! (local)	Calls the manager in local application mode. This menu is available only for the S@N.IT! manager configured to support local application launching.

Table 7. Storage Manager node menu

The S@NIT Web GUI is based on an java applet technology. So, don't close the first launched browser windows which doesn't contain the GUI but the applet itself.

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 most degraded subnode status (hosts and services).

Platform Node and Hostgroup Node Menus	
Expand	Shows the hosts contained in this hostgroup or this platform.
Animation	Briefly explains resource status.

Table 8. Platform node and Hostgroup node menus

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 most degraded subnode status (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, and disappears as soon as at least one associated service is checked.
UP (green)	The host is up and running.
DOWN (red)	The host is down or unreachable.

Table 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.
Remote Operation	See Table below.

Table 10. Host node menu

Remote Operation Menu for Windows	
… -> VNC Viewer	Starts VNC viewer to connect to this host.
… -> Telnet	Launches Telnet to connect to this host.
Remote Operation Menu for Linux	
… -> Telnet	Launches Telnet to connect to this host.
… -> Actions	Opens a Webmin page to:
-> Shell Command	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.
-> Change Password	to manage passwords.
-> RPM Products	to manage software packages.
-> System Logs	to manage system logs.
-> Network Configuration	to manage network configuration.

Table 11. Linux Remote operation menus

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 most degraded subnode status (services).

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

Table 12. Category node menu

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 and disappears 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 plugin 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 13. Service status levels

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

Table 14. Service node menu

Management Tree Views

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

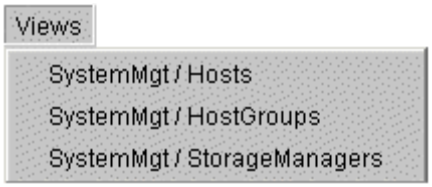
- Hosts
- HostGroups
- HardwareManagers
- StorageManagers

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

File -> Load -> SystemMgt -> *view name*

Once several views have been loaded, you can switch from a one view to another by selecting:

Views -> *view name*



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.
HardwareManagers 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.
StorageManagers View	All storage managers in the configuration are displayed. Each manager node contains the hosts that it manages.

Table Tree views

As Administrator, you can create customized views to meet your own criteria. Please refer to the *Administrator's Guide for details.*.

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**, **LogicalDisk**…), as shown in the following figure.

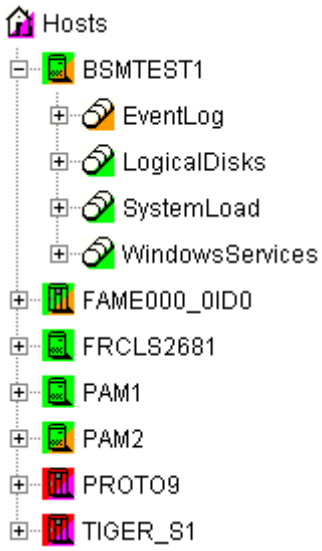


Figure 30. Hosts view

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**...), as shown in the following figure.

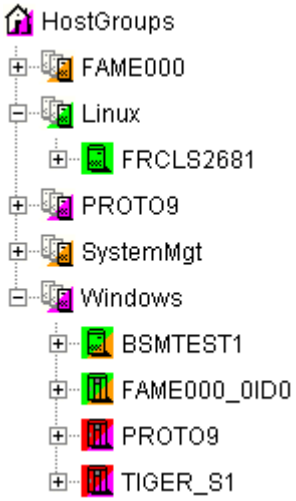


Figure 31. HostGroups view

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

HardwareManagers View

The **HardwareManagers** 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 supported category (**Hardware**, **EventLog**, **LogicalDisk**...), as shown in the following figure:

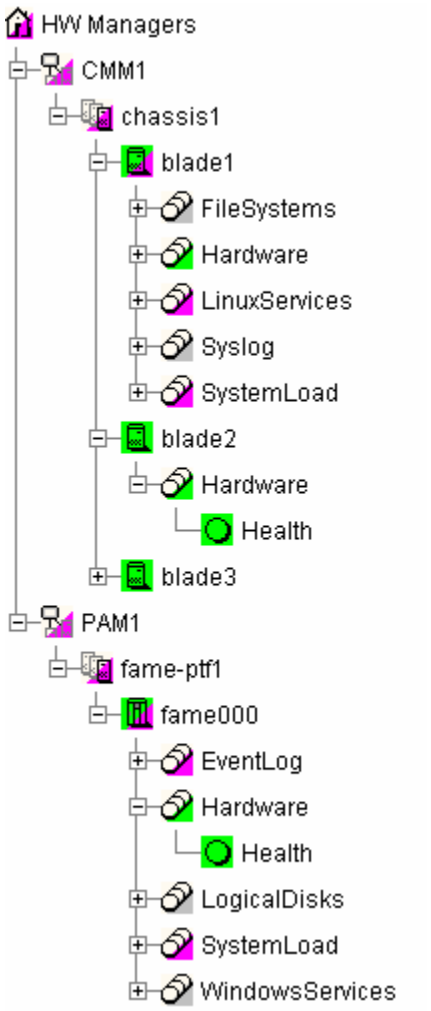


Figure 32. HardwareManagers view

StorageManagers View

The **StorageManagers** view displays all the storage managers in the configuration.

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

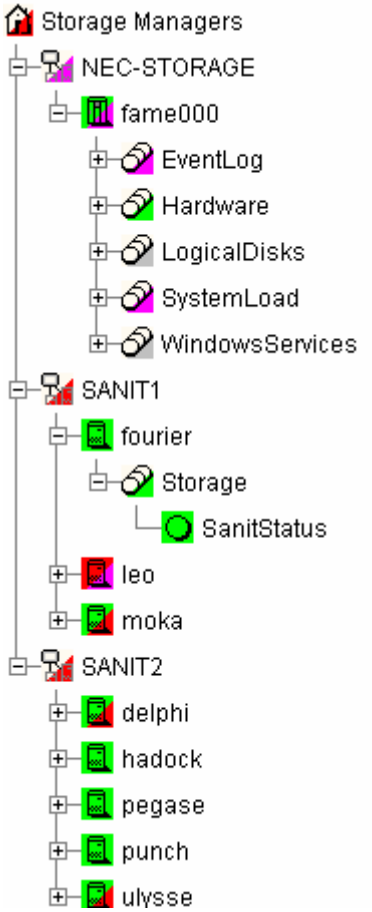


Figure 33. StorageManagers view

Working in the Map Mode

When you select the **Map** radio button, the **Map, Focus** and **Problem Panes** are displayed.

Note:
The M**ap** and P**roblem panes** are always synchronized.

- The P**roblem pane** lists the problems that occurred on hosts belonging to hostgroups on the current map. Each hostgroup is represented by an animated rectangle (rectangle dimensions are specified in the Configuration GUI). The **Select a map** box allows you to select another configured map.
- The F**ocus Pane** lists all the services (with their status) configured to be displayed in this pane. As Administrator, these monitoring services are highly important and need to be displayed in a specific pane. This pane appears only when there exists configured focus services. (See Administration's guide for more information).

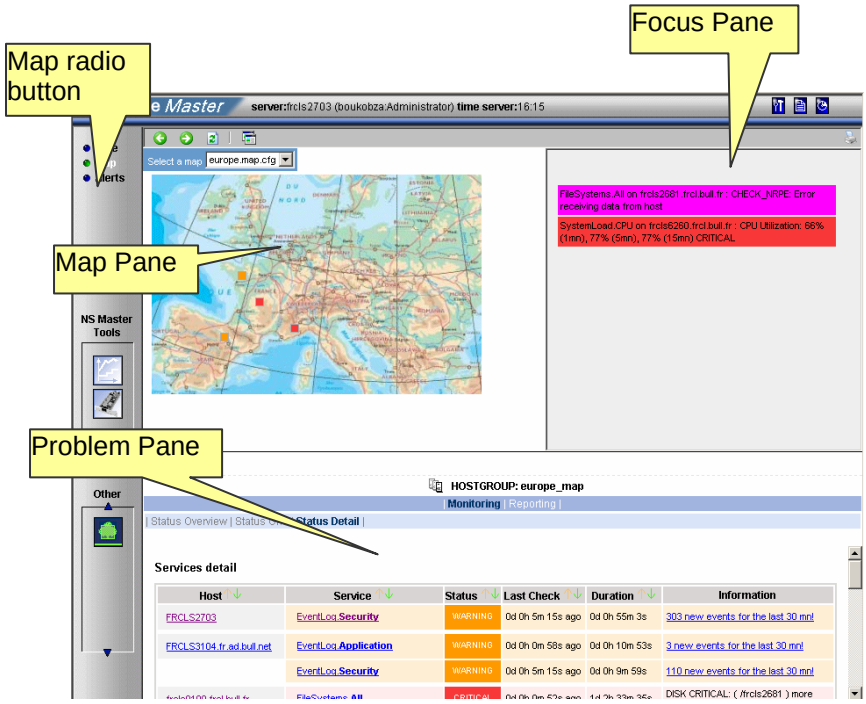


Figure 34. Map mode

In the M**ap Pane**, hostgroups are displayed and animated with their computed status. Their positions (x,y) are specified in the Configuration GUI.

Hostgroup status is the most degraded status of corresponding hosts and monitoring services.

The P**roblem Pane** lists all the problems that occurred on any host belonging to the hostgroups on the map. IYou can navigate thru internet links and return using the **Back** button.

Note:
For each Map, a corresponding internal hostgroup (with name “<MapName>_map” is generated for the monitoring server (used by the Problem Pane).

If you want to zoom a specific hostgroup, select it on the map. When the mouse is hovered over a square representing a hostgroup, an Infotip displays the hostgroup name and position (x,y). :

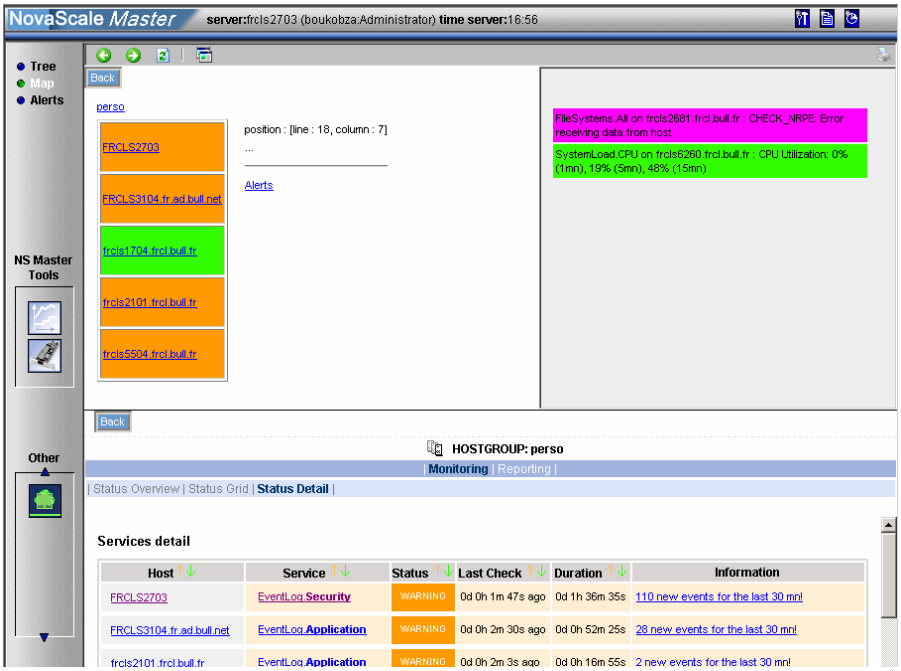


Figure 35. Hostgroup details

When a hostgroup is selected, the status of all the hosts belonging to that hostgroup are displayed, along with three links to more information:

- **Hostgroup name** link (**perso** in Figure):
  This link opens a new window giving grid status information about all current hostgroup host services.

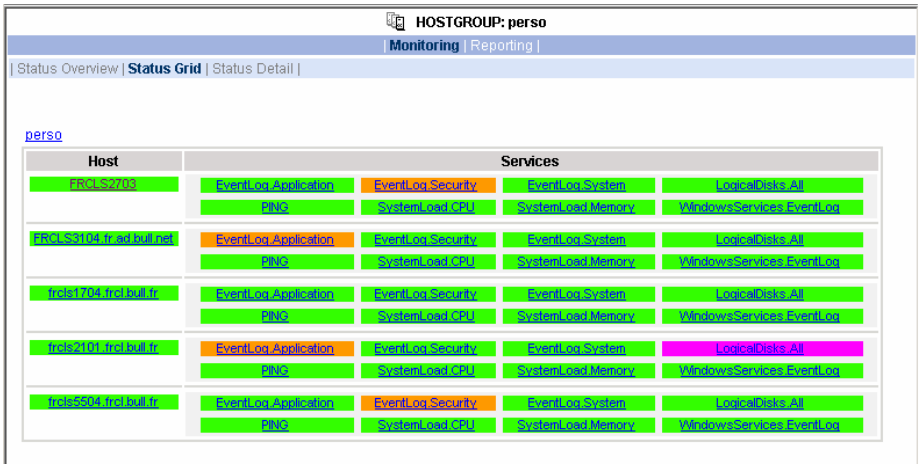


Figure 36. Hostgroup link information

- **Host name** link (**frcls2101.frcl.bull.fr** in Figure):
  This link opens a new window giving monitoring information about all current host services.

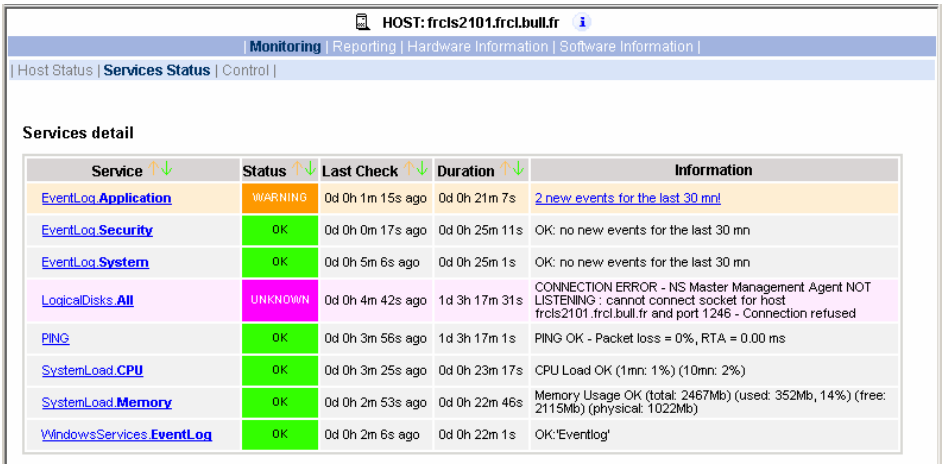


Figure 37. Host services

- **Alerts** link:
  This link opens a new window giving alert information about all current hostgroup host alerts.

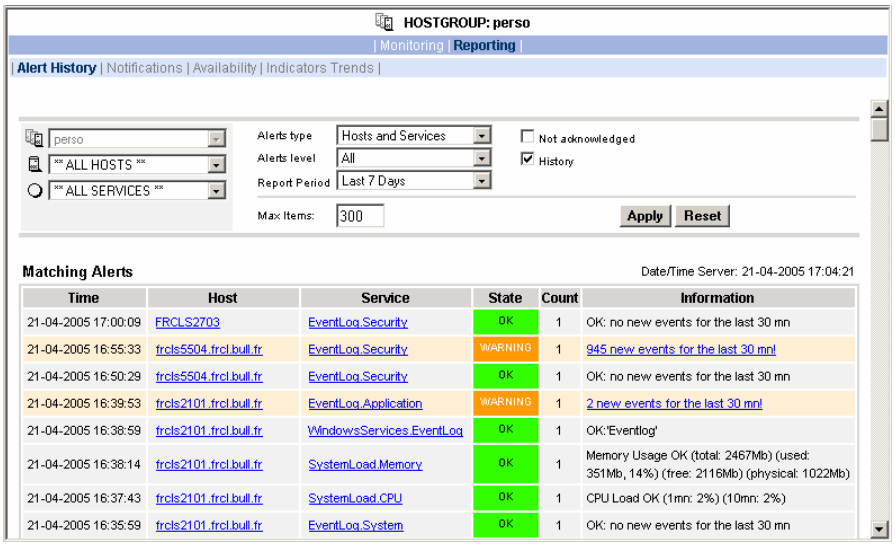


Figure 38. Hostgroup alerts

Working in the Alerts Mode

Alert Basics

The **Nova Scale Master Alert Viewer** application displays monitoring alerts (also called events) concerning a set of hostgroups, hosts and services.

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

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

The NovaScale Master Alert Viewer application scans the current monitoring log and archives according to filter **report period** settings.

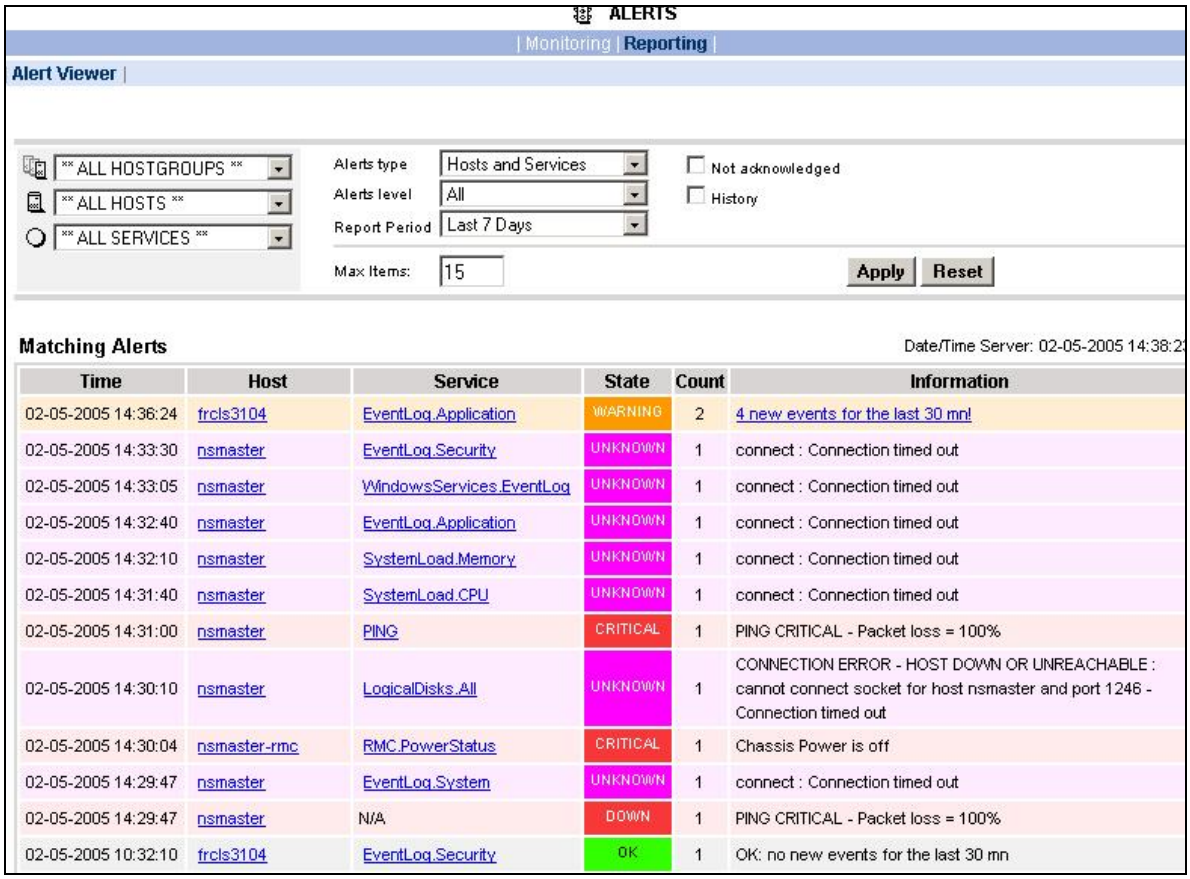


Figure 39. Nova Scale Master Alert Viewer

Nova Scale Master Alert Viewer is divided into two main functional parts:

- The **Selection Pane**, 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 Pane**, which displays filtered alerts.

Alert Selection

Note:
By default, alerts for all hostgroups, all hosts and all services are displayed.

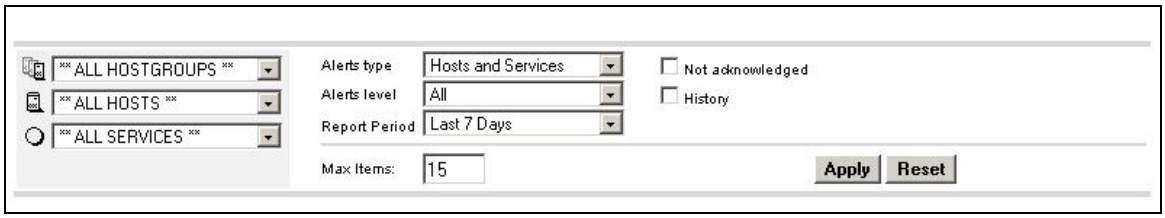


Figure 40. Alert Selection

Selecting Hostgroups, Hosts and Services

You can filter **hostgroup, host** and **service** Alerts from the Selection Pane, in any combination:

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

- When you select a **specific host**, only the services belonging to that host are selected.
- When you select ****ALL SERVICES****, all the services belonging to the previously selected host are selected.
- When you select ****ALL HOSTS**** and ****ALL SERVICES****, all the hosts belonging to the previously selected hostgroup (or all hostgroups) are selected and all the services belonging to those hosts are selected.

Example:

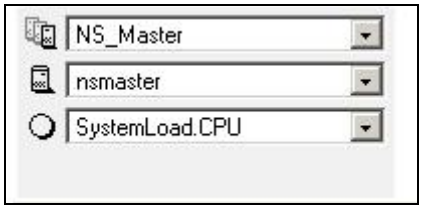


Figure 41. Alert selection - example

In Figure 39, the user decided to select all alerts concerning **SystemLoad.CPU on the nsmaster host** in the NS_Master hostgroup.

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 alerts**
  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 alerst with **UNKNOWN** or **CRITICAL** status levels.
- **Current problems**
  display 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 decid[illegible]e displayed or not.

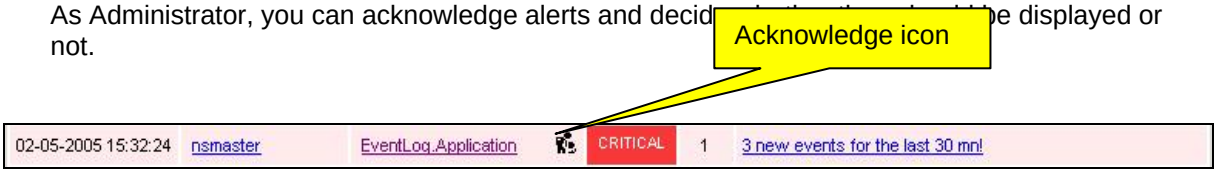


Figure 42. Acknowledged alerts selection

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

Selecting Alert Histories

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 of time over 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 through 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**.

Alert Information

Alerts give the following information:

- **Time:** i.e. when the alert occured
- **Host Name:** i.e. where the alert occured
- **Service Name**: i.e. where the alert occured
- **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.
Time and Information fields concern the most recent alert.

Supervision Information

Supervision Information Basics

The **Supervision Pane** displays information about monitored resources and works 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 Pane is divided into five functional parts, as shown in the following figure:

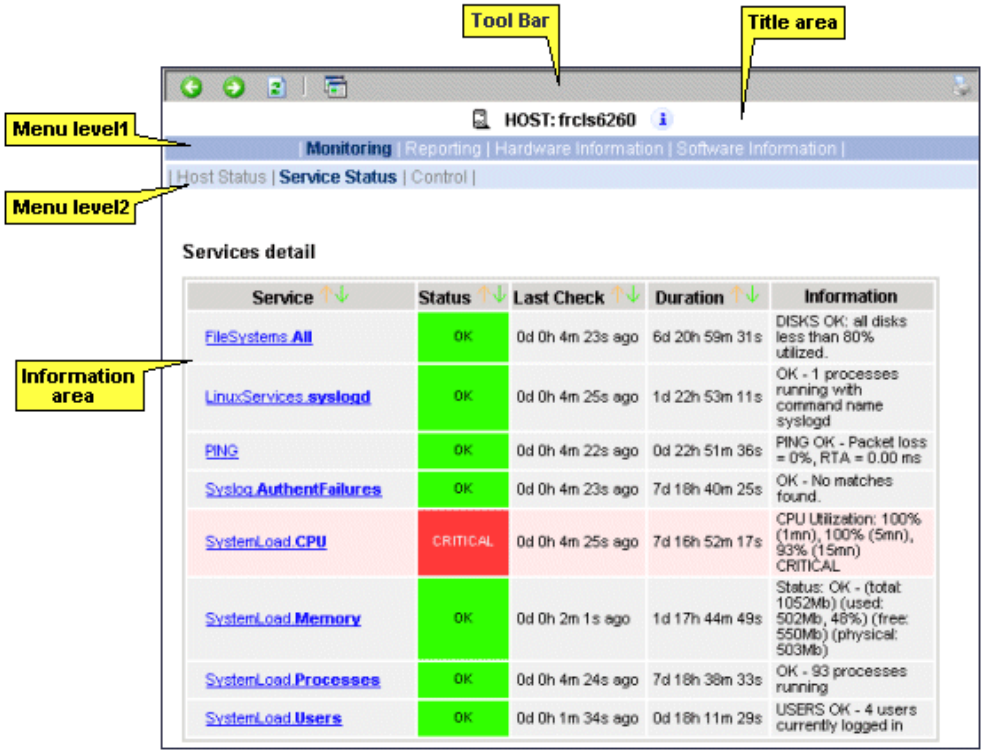


Figure 43. Supervision Pane

Tool Bar	Go back one page.
	Go forward one page.
	Reload the current page.
	Detach the current page to a separate frame.
	Print the current page.
Title Pane	Displays the selected monitored resource icon, 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 information you want to display, according to the selected monitored resource: Monitoring, Reporting, Hardware and Software information.
Menu Level2	Allows you to select the information you want to display, according to selected Level1 information.
Information Pane	Displays selected information about the monitored resource.

Monitoring Information

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

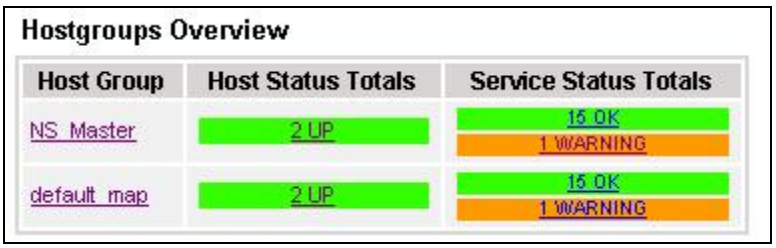
Information Type	Supervision Scope
Status Overview	Root nodes of Hosts and Hostgroups Views (Tree) Hostgroup
Status GRID	Root nodes of Hosts and Hostgroups Views (Tree) Hostgroup
Status Detail	Root nodes of Hosts and Hostgroups Views (Management Tree) Hostgroup
Host Status	Host
Service Status	Service
Log	Root nodes of Hosts and Hostgroups Views (Tree)
Commands	Root nodes of Hosts and Hostgroups Views (Tree)

Table 15. Monitoring information

Status Overview

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

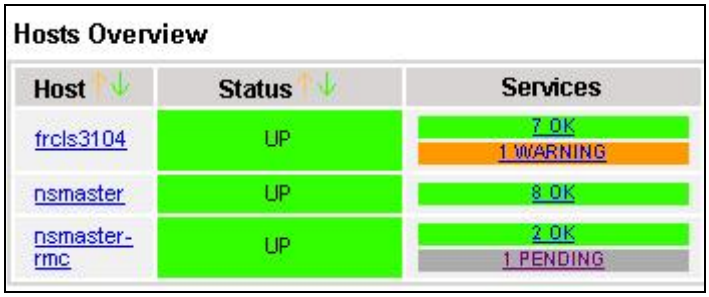
- When you launch this screen from the hostgroup node, a status overview of all hostgroups (or a particular hostgroup) is displayed.



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

Figure 44. Hostgroup Status Overview

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

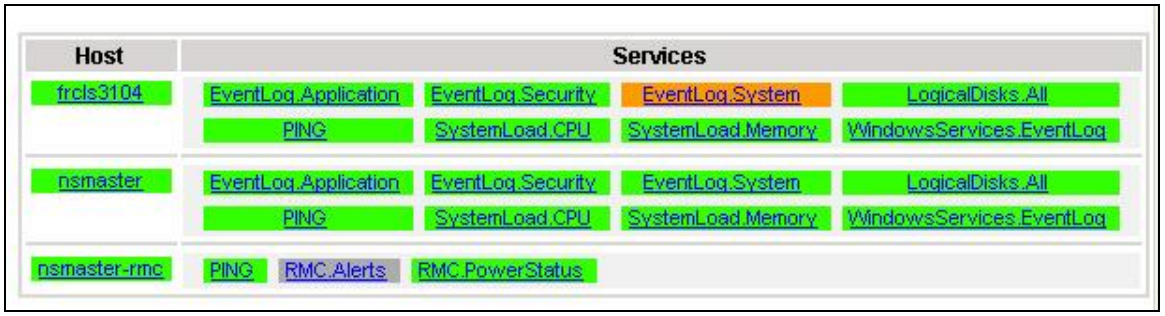


Host	Host name
Host Status	Host status level
Service Status	Number of services classified by status level

Figure 45. Host Status Overview

Status GRID

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

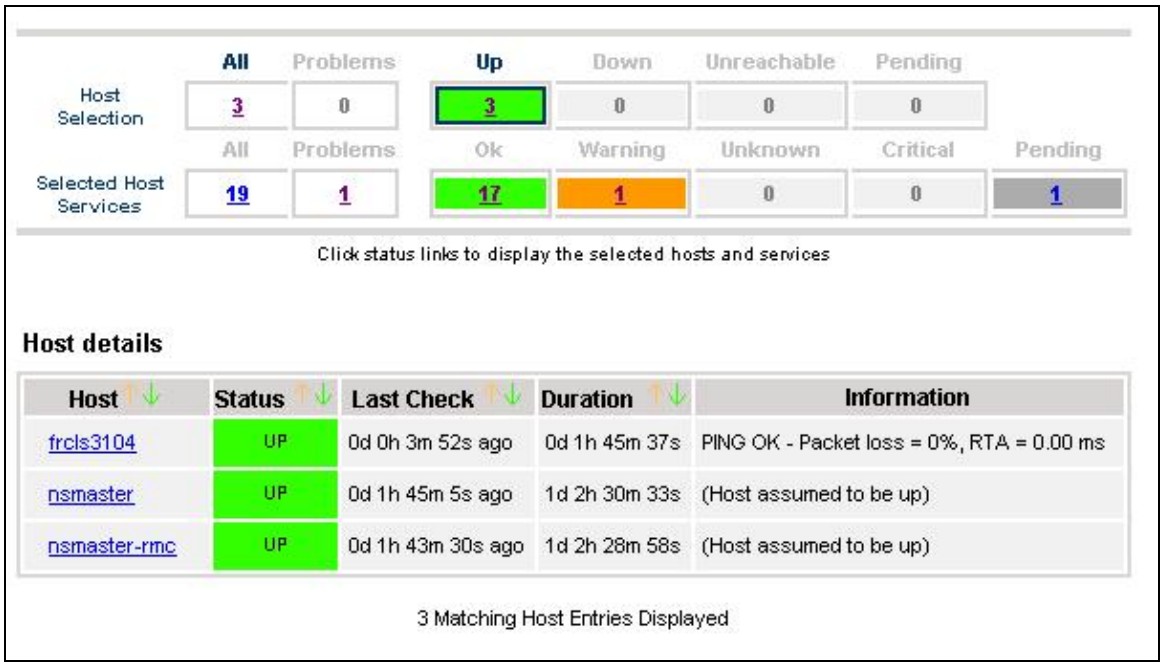


Host	Host name
Service Status	Host services animated by status level color

Figure 46. Host Status GRID

Status Detail

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



The S**election Pane** allows you to select 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.**

Figure 47. Hosts Status Detail

Information details gives host details if **host** is selected and service details if **host and service** are selected.

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

Host Status

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

Host detail

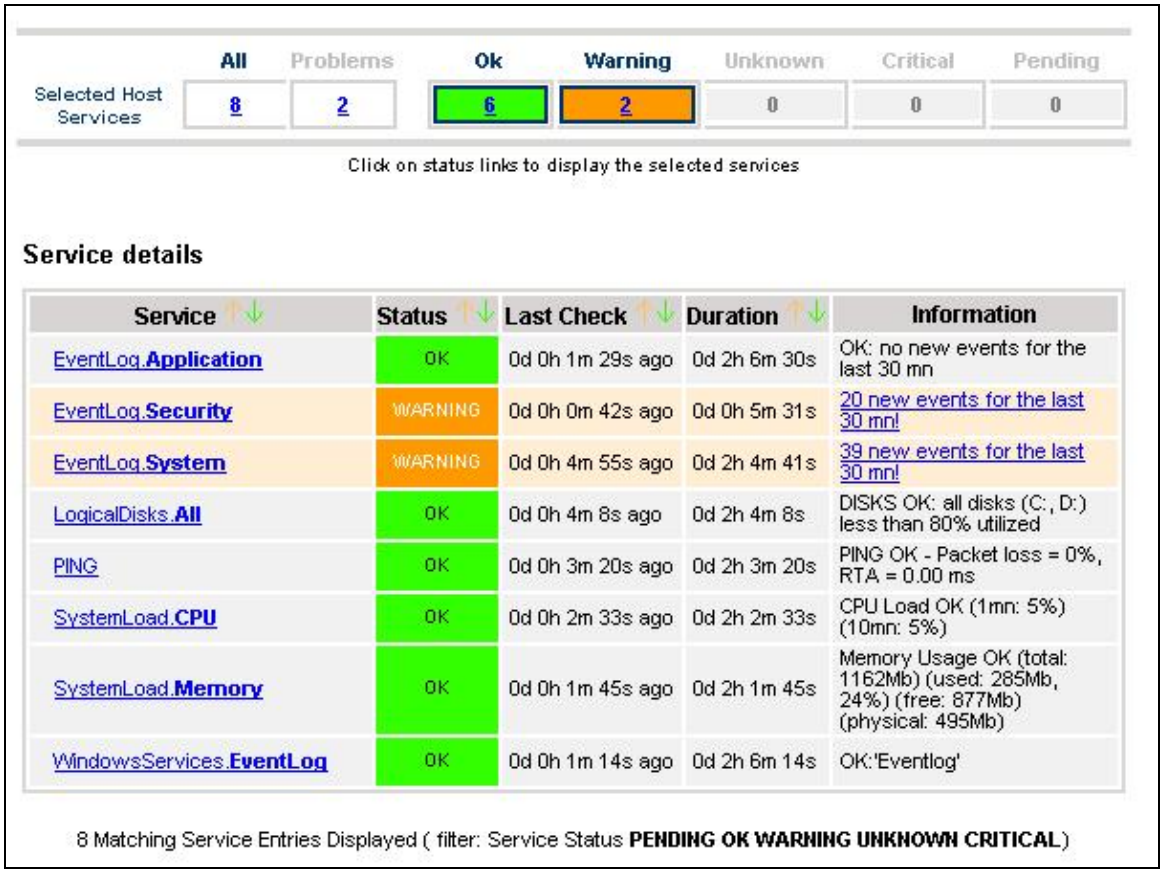
Host	Status	Last Check	Duration	Information
frcls3104	UP	0d 0h 2m 8s ago	0d 1h 58m 53s	PING OK - Packet loss = 0%, RTA = 0.00 ms

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

Figure 48. Host Status

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.



	All	Problems	Ok	Warning	Unknown	Critical	Pending
Selected Host Services	8	2	6	2	0	0	0

Click on status links to display the selected services

Service details

Service	Status	Last Check	Duration	Information
EventLog.**Application**	OK	0d 0h 1m 29s ago	0d 2h 6m 30s	OK: no new events for the last 30 mn
EventLog.**Security**	WARNING	0d 0h 0m 42s ago	0d 0h 5m 31s	20 new events for the last 30 mn!
EventLog.**System**	WARNING	0d 0h 4m 55s ago	0d 2h 4m 41s	39 new events for the last 30 mn!
LogicalDisks.**All**	OK	0d 0h 4m 8s ago	0d 2h 4m 8s	DISKS OK: all disks (C:, D:) less than 80% utilized
PING	OK	0d 0h 3m 20s ago	0d 2h 3m 20s	PING OK - Packet loss = 0%, RTA = 0.00 ms
SystemLoad.**CPU**	OK	0d 0h 2m 33s ago	0d 2h 2m 33s	CPU Load OK (1mn: 5%) (10mn: 5%)
SystemLoad.**Memory**	OK	0d 0h 1m 45s ago	0d 2h 1m 45s	Memory Usage OK (total: 1162Mb) (used: 285Mb, 24%) (free: 877Mb) (physical: 495Mb)
WindowsServices.**EventLog**	OK	0d 0h 1m 14s ago	0d 2h 6m 14s	OK:'Eventlog'

8 Matching Service Entries Displayed (filter: Service Status **PENDING OK WARNING UNKNOWN CRITICAL**)

The **Selection Pane** 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.**

Information Details gives status details for the selected services:

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

Figure 49. Services Status

Log

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

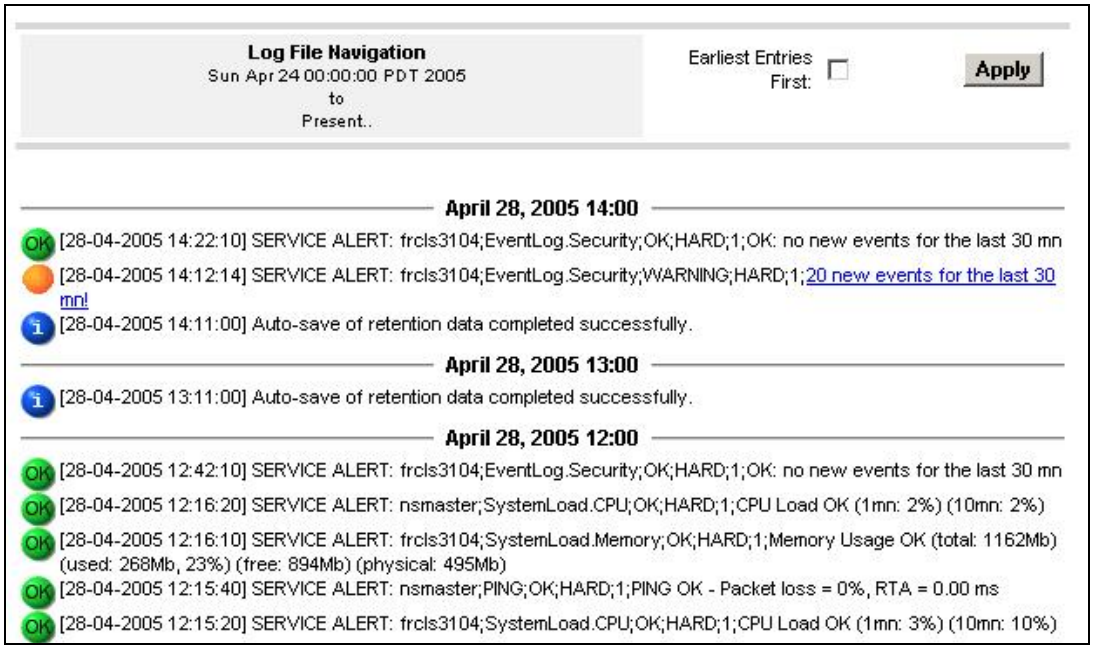


Figure 50. Monitoring Server Log

NovaScale Master Log shows all the events logged by the monitoring process:

- Host and Service alerts
- Alert notifications
- Alert acknowledgements
- New comments
- Configuration information messages
- Miscellaneous

Commands

- When you launch this screen from the Hosts or Hostgroups root nodes, Monitoring Server information and performance is displayed. You also have access to Process Commands.

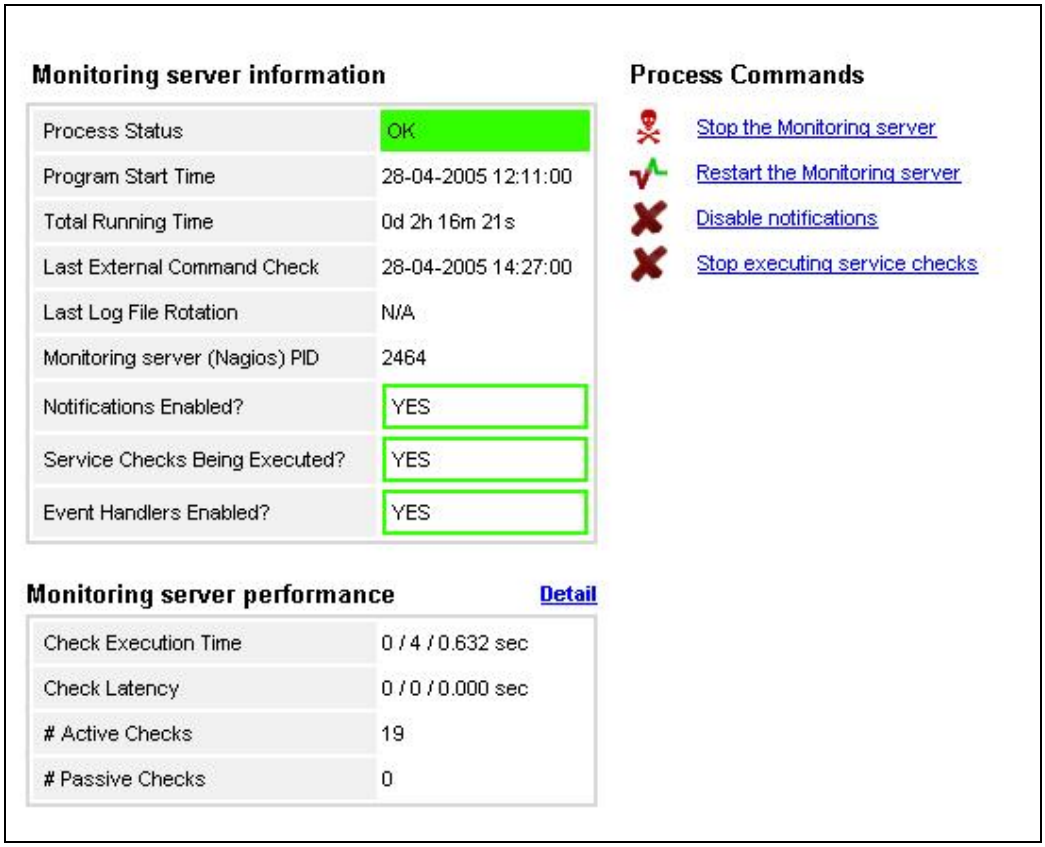


Figure 51. Monitoring Server commands

Monitoring Server Information

Gives general information about the Nagios monitoring process.

Monitoring Server Performance

Gives statistical information about the Nagios monitoring process:

- the min, max and average time recorded for the check execution
- the min, max and average time recorded for check latency (check delay time due to monitoring server overload)
- the current number of active checks
- the current number of passive checks.

Process Commands

Allows you to perform actions on 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.

☞ **Process Commands** require Administrator rights.

- When you launch this 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, enable or disable service checks.

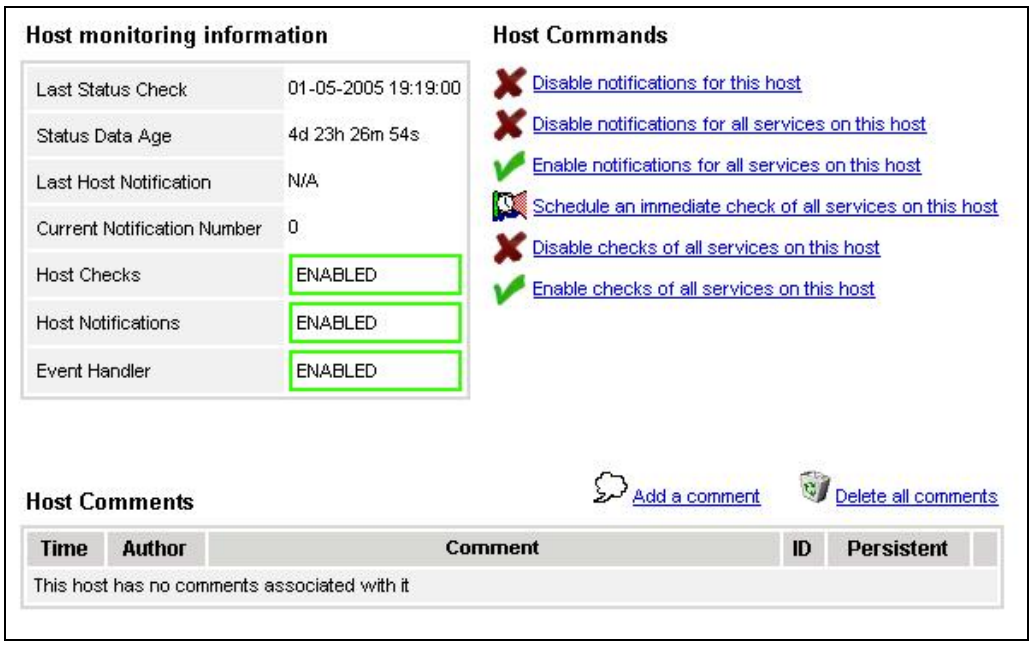


Figure 52. Monitoring Host commands

Host/Service Monitoring Information

Gives general information about host or service monitoring.

Host/Service Comments

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

Host/Service Commands

Enables actions on 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.

Commands require Administrator rights.

Reporting Information

The following table lists the available information types 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.
Avaibility	Root nodes of Hosts and Hostgroups views (Tree), Hostgroup, Host, Service.
Status Trends	Root nodes of Hosts and Hostgroups views (Tree) Host, Service
Indicator Trends	Root nodes of Hosts and Hostgroups views (Tree) Hostgroup, Host, Service.

Alert History

This screen displays host and service alerts according to the selected context. 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 displayed below. Information about Alert History is detailed in chapter 3.3

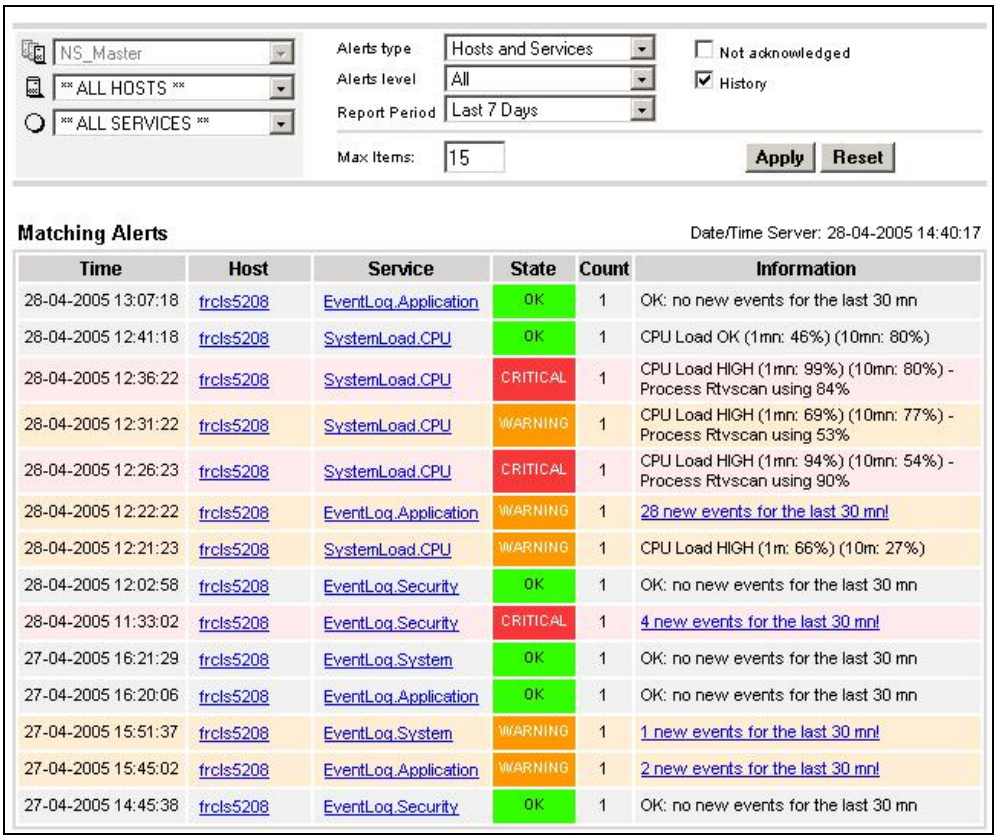


Figure 53. Alert History screen - example

Notifications

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

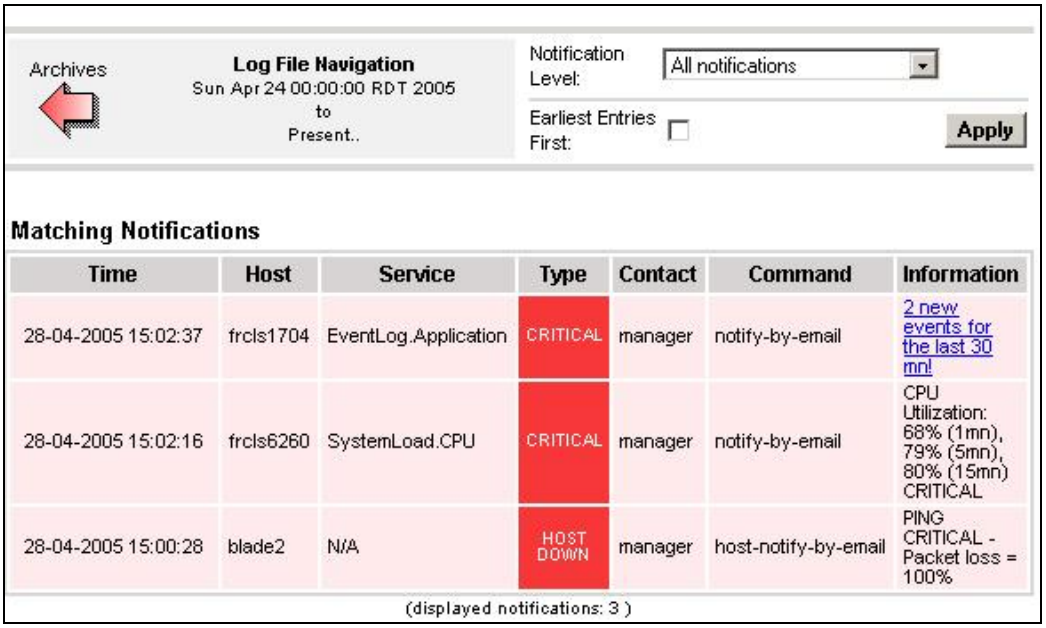


Figure 54. Notifications screen - example

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 Dow, Service Critical,…). By default, all notifications are displayed.
Earliest Entries First	Allows you 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, …**) are displayed according to the criteria previously set. **Type** information reflects the severity of the notification.

Avaibility

This screen reports on the availability of hosts and services over a user-specified period of time. When called from a root node, it will report the avaibility summary for each host declared in the NovaScale Master application. When called from a Host context, the report will be more detailed as displayed below.

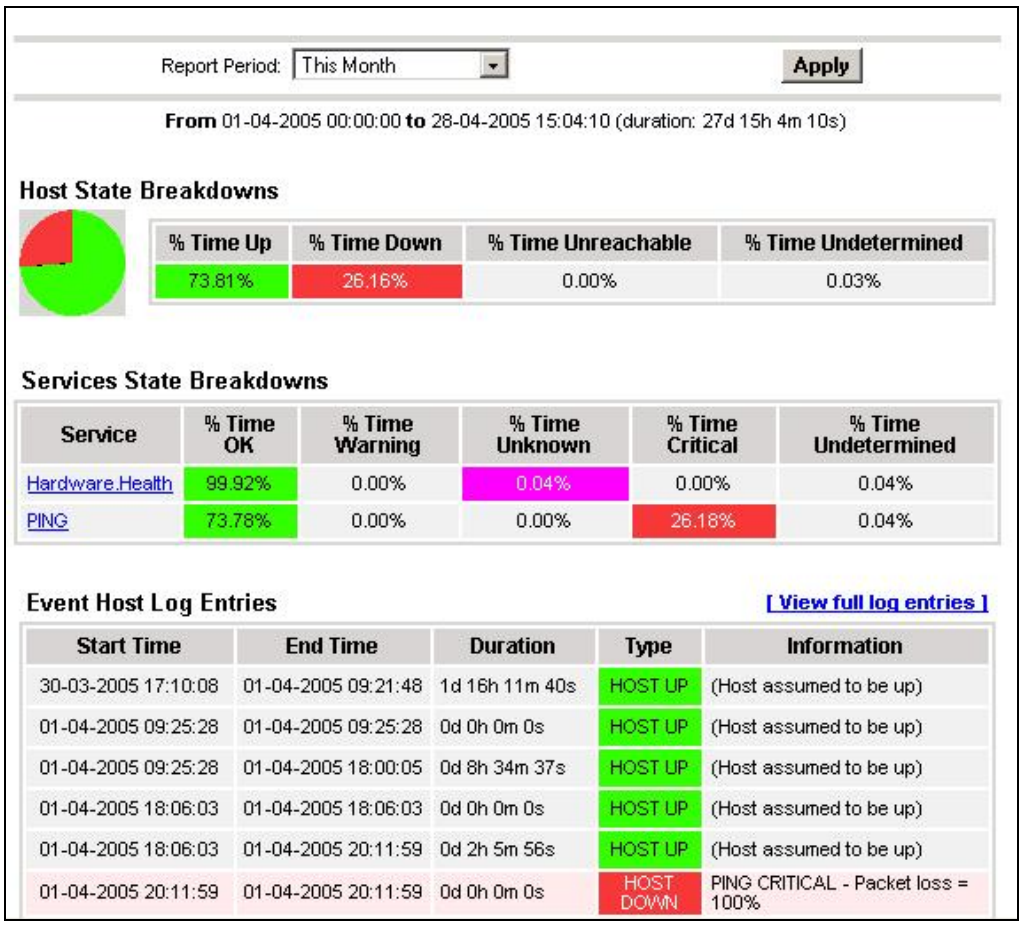


Figure 55. Availability screen - example

The screen is divided into two parts:

- The top part allows you to choose 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 percent 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 if the report is asked 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.

Status Trends

This screen displays a graph of host or service states over an arbitrary period of time, as displayed below.

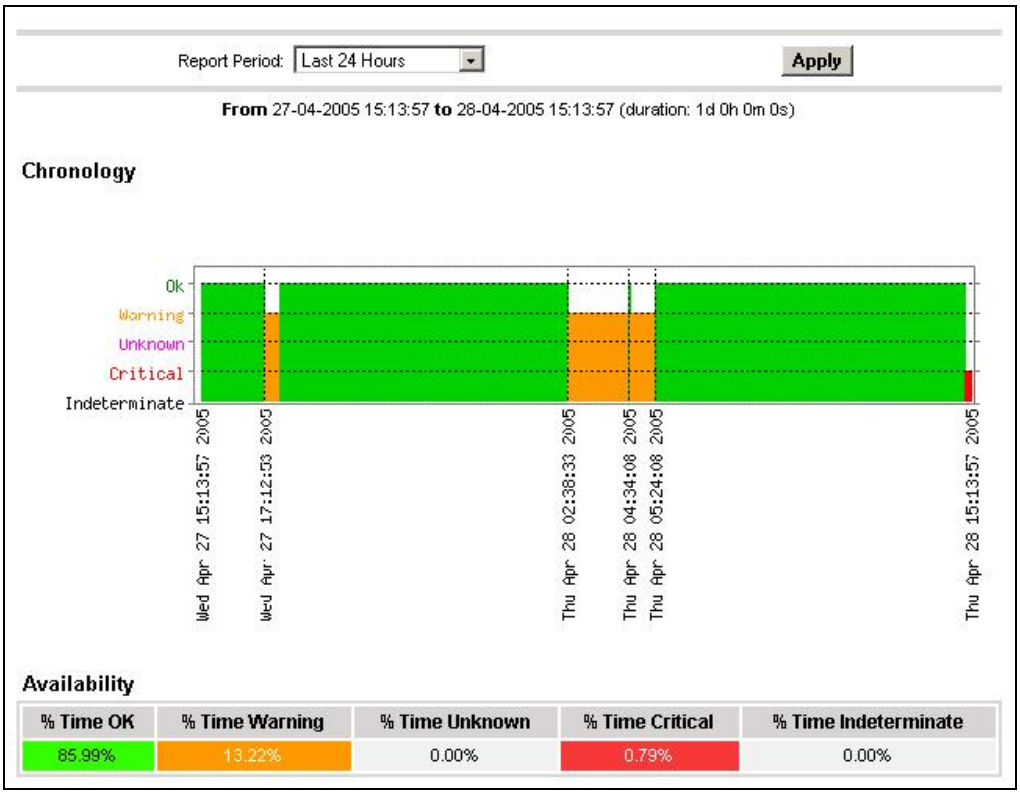


Figure 56. Status Trends on a Service

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 selected report period.

The following information is reported:

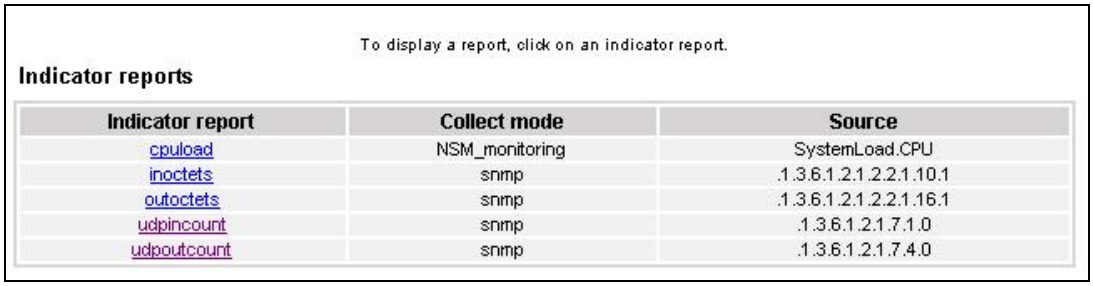
Chronology	Represents the evolution of the host or service status over the selected time period.
Availability	Represents the percent of time spent in each state for the host or service.

Table Status trends information

Indicator Trends

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

Informations about how to vizualize reports associated with these indicators are detailed in the Chapter *Reports,* on page 4-7.


To display a report, click on an indicator report.

Indicator reports

Indicator report	Collect mode	Source
cpuload	NSM_monitoring	SystemLoad.CPU
inoctets	snmp	.1.3.6.1.2.1.2.2.1.10.1
outoctets	snmp	.1.3.6.1.2.1.2.2.1.16.1
udpincount	snmp	.1.3.6.1.2.1.7.1.0
udpoutcount	snmp	.1.3.6.1.2.1.7.4.0

Figure 57. Indicator Trends on a Host

Hardware Information

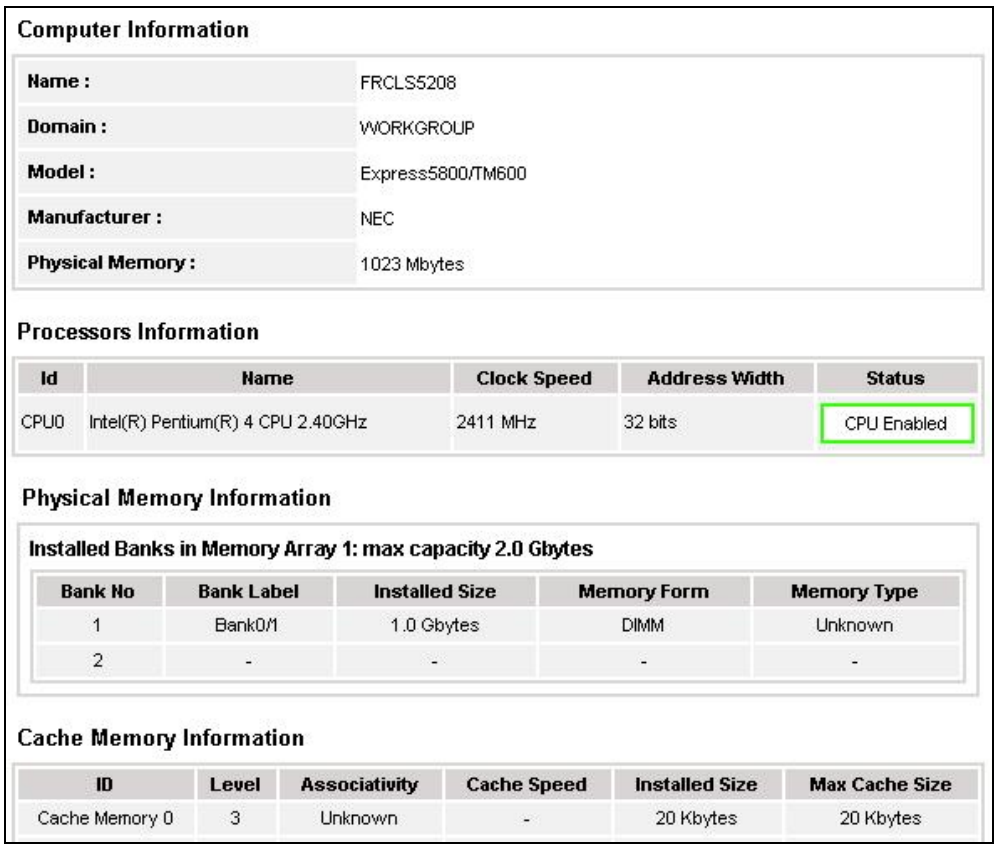
These screens are available for Host or Service supervision. Information levels vary to OS and host type.

Inventory Information

This information is OS-dependent and is only available for hosts with Windows or Linux Operating Systems.

For **Windows** hosts, this screen displays the following information:

- Computer Information
- Processors Information
- Physical Memory Information
- Cache Memory Information
- Non-Storage Devices Information



Computer Information

Name :	FRCLS5208
Domain :	WORKGROUP
Model :	Express5800/TM600
Manufacturer :	NEC
Physical Memory :	1023 Mbytes

Processors Information

Id	Name	Clock Speed	Address Width	Status
CPU0	Intel(R) Pentium(R) 4 CPU 2.40GHz	2411 MHz	32 bits	CPU Enabled

Physical Memory Information

Installed Banks in Memory Array 1: max capacity 2.0 Gbytes

Bank No	Bank Label	Installed Size	Memory Form	Memory Type
1	Bank0/1	1.0 Gbytes	DIMM	Unknown
2	-	-	-	-

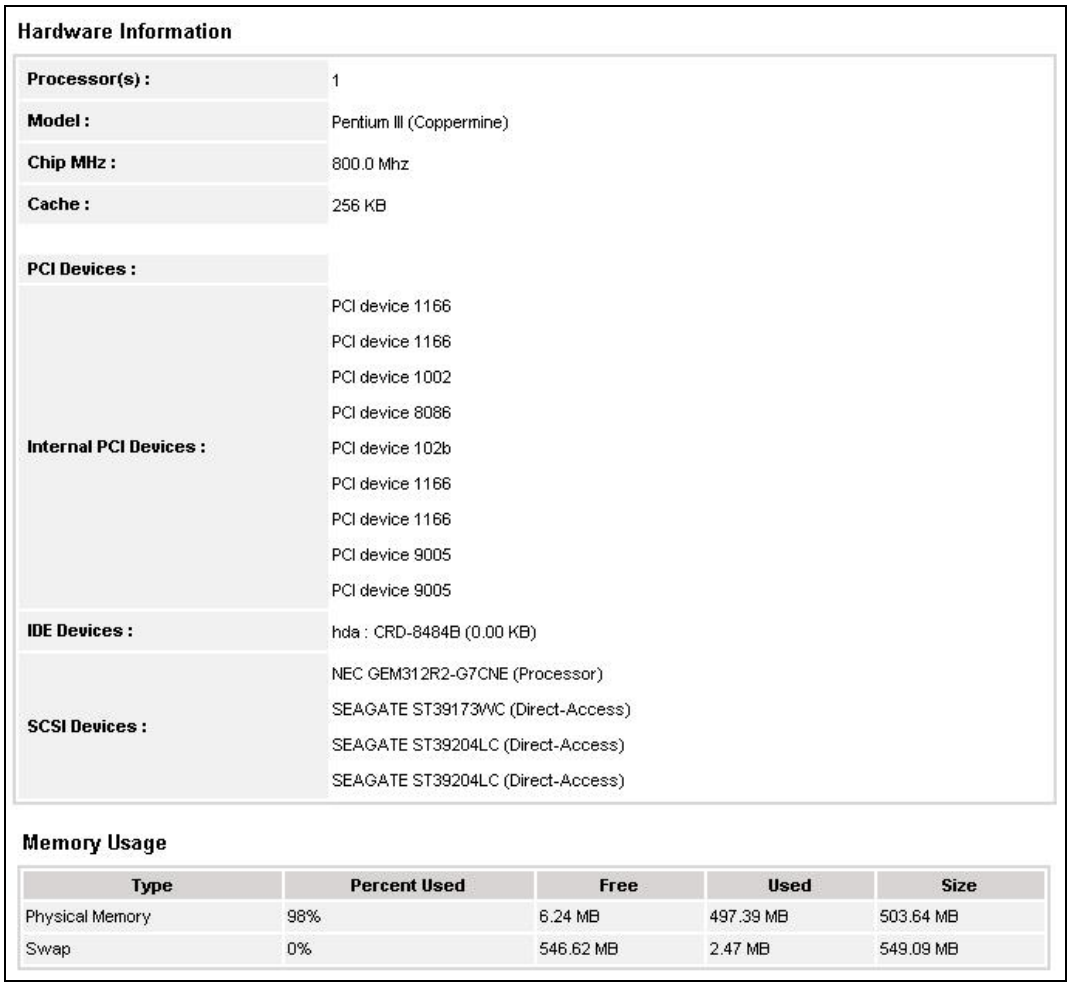
Cache Memory Information

ID	Level	Associativity	Cache Speed	Installed Size	Max Cache Size
Cache Memory 0	3	Unknown	-	20 Kbytes	20 Kbytes

Figure 58. Windows Inventory information - example

For **Linux** hosts, this screen displays the following information:

- Hardware Information
- Memory Usage



Hardware Information

Processor(s) :	1
Model :	Pentium III (Coppermine)
Chip MHz :	800.0 Mhz
Cache :	256 KB
PCI Devices :	
Internal PCI Devices :	PCI device 1166 PCI device 1166 PCI device 1002 PCI device 8086 PCI device 102b PCI device 1166 PCI device 1166 PCI device 9005 PCI device 9005
IDE Devices :	hda : CRD-8484B (0.00 KB)
SCSI Devices :	NEC GEM312R2-G7CNE (Processor) SEAGATE ST39173WC (Direct-Access) SEAGATE ST39204LC (Direct-Access) SEAGATE ST39204LC (Direct-Access)

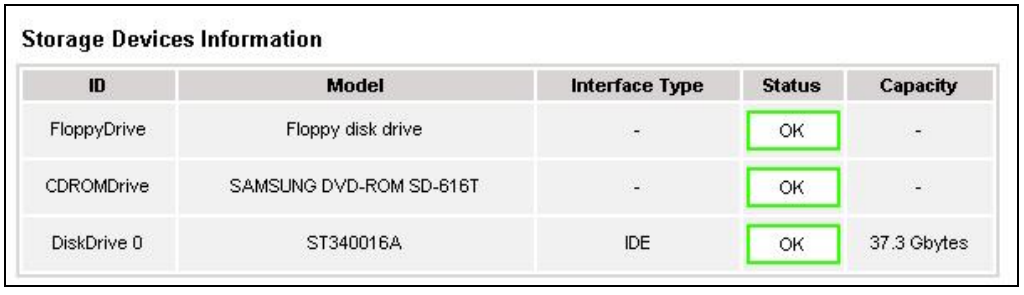
Memory Usage

Type	Percent Used	Free	Used	Size
Physical Memory	98%	6.24 MB	497.39 MB	503.64 MB
Swap	0%	546.62 MB	2.47 MB	549.09 MB

Figure 59. Linux Inventory information - example

Storage Information

This information is OS-dependent and is only available for hosts with Windows or Linux Operating Systems.



Storage Devices Information

ID	Model	Interface Type	Status	Capacity
FloppyDrive	Floppy disk drive	-	OK	-
CDROMDrive	SAMSUNG DVD-ROM SD-616T	-	OK	-
DiskDrive 0	ST340016A	IDE	OK	37.3 Gbytes

Figure 60. Windows Storage information - example

FRU Information

This information is only available for Express 5800 and NovaScale 4000, 5000 or 6000 series hosts.

For details about the information displayed, refer to Chapter *4.1*

Sensor Information

This information is only available for Express 5800 and NovaScale 4000 series hosts.

For details about the information displayed, refer to Chapter *4.1*

SEL Information

This information is only available for Express 5800 and NovaScale 4000, 5000 or 6000 series hosts.

For details about the information displayed, refer to Chapter *4.1*

Software Information

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

Windows Information

The **Windows System** screen displays the following information:

- OS Version Information
- OS Computer Information
- OS Installation Information

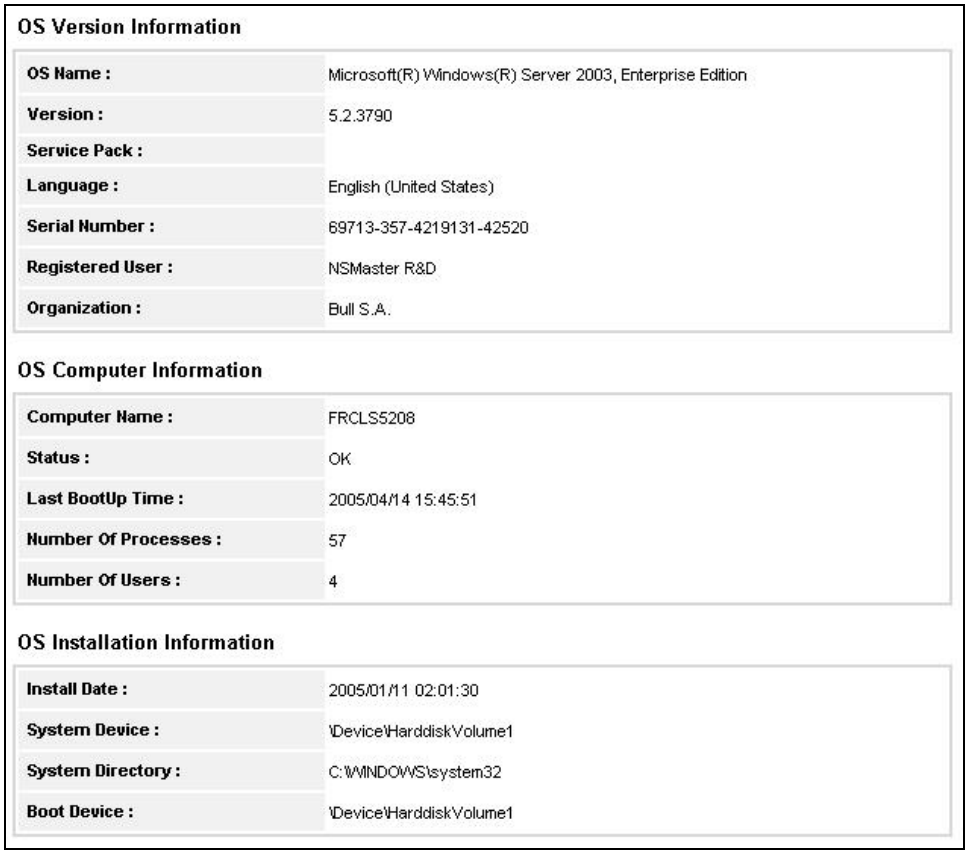
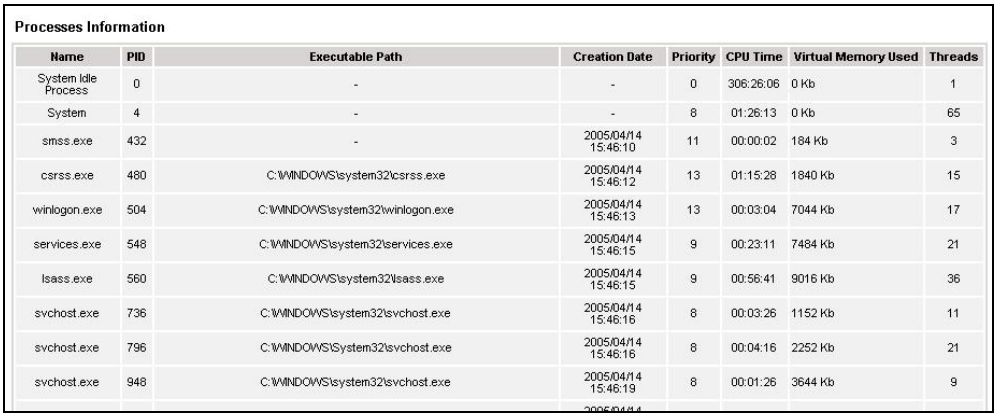


Figure 61. Windows System screen - example

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

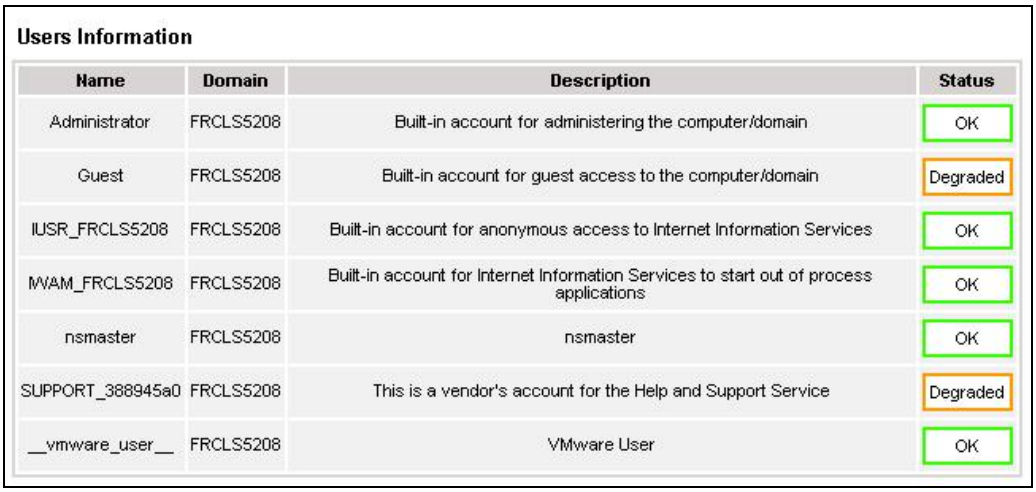


Processes Information

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

Figure 62. Windows Process screen - example

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

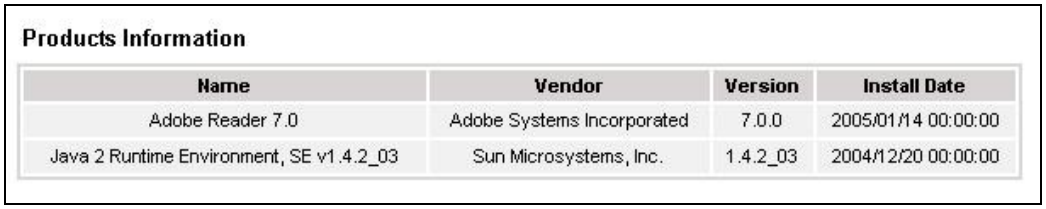


Users Information

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 63. Windows Users screen - example

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



Products Information

Name	Vendor	Version	Install Date
Adobe Reader 7.0	Adobe Systems Incorporated	7.0.0	2005/01/14 00:00:00
Java 2 Runtime Environment, SE v1.4.2_03	Sun Microsystems, Inc.	1.4.2_03	2004/12/20 00:00:00

Figure 64. Windows Products screen - example

Note: On servers running Windows Operating System, only products installed using a .MSI file are displayed.

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

Logical Disks Information

Drive	Description	Volume Name	Provider Name	Capacity	Used Space	Free Space
A:	3 1/2 Inch Floppy Drive	-	-	-	-	-
C:	Local Fixed Disk		-	19.5 Gbytes	67 %	6.5 Gbytes
D:	CD-ROM Disc	-	-	-	-	-
X:	Network Connection	livraison	\\frcls2681\livraison	9.4 Gbytes	88 %	1.2 Gbytes
Y:	Network Connection	PamLife : 8.9 GB	\\Pamweb\Security	8.9 Gbytes	35 %	5.9 Gbytes
Z:	Network Connection	Factory	\\hortalix\factory	17.0 Gbytes	46 %	9.2 Gbytes

Figure 65. Windows Logical Disks screen - example

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

Services Information

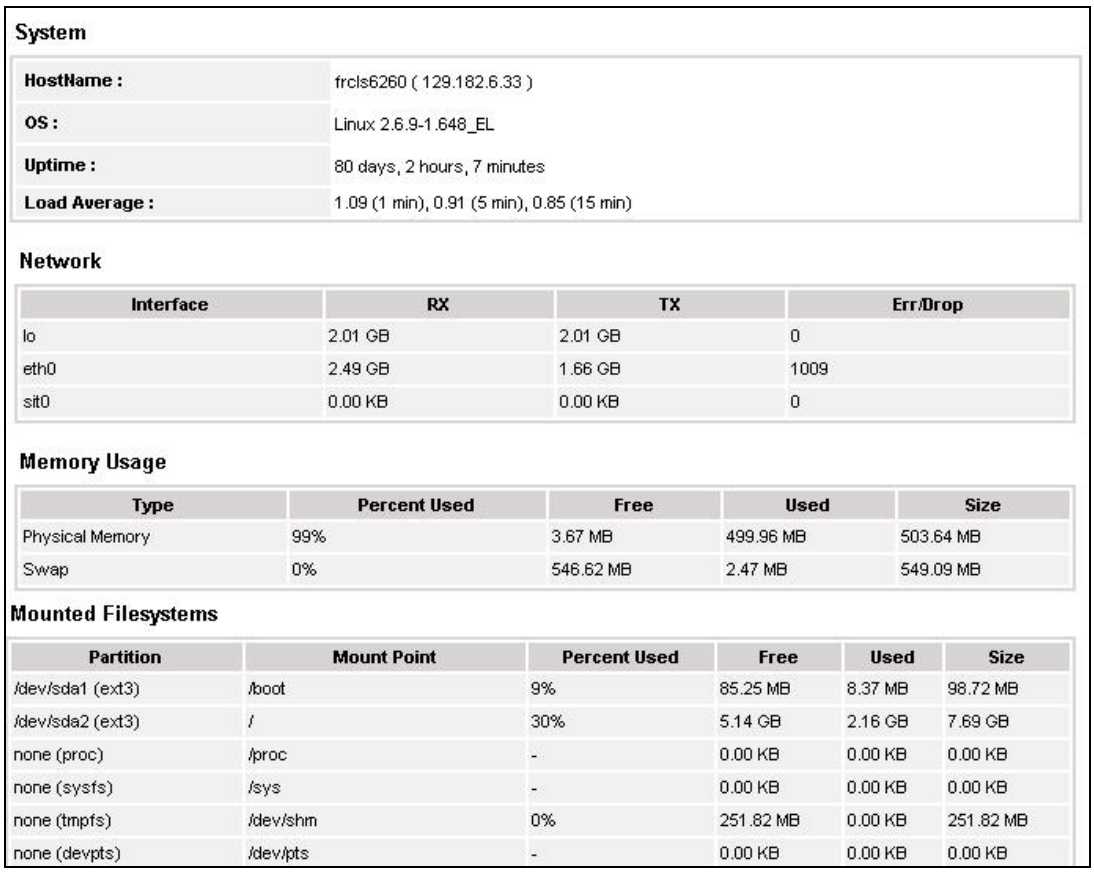
Display Name	State	Has Been Started ?	Start Mode	Executable Path	Action if Startup Failure	Account
Alerter	Stopped	FALSE	Disabled	C:\WINDOWS\system32\svchost.exe -k LocalService	Normal	NT AUTHORITY\LocalService
Application Layer Gateway Service	Stopped	FALSE	Manual	C:\WINDOWS\System32\alg.exe	Normal	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 66. Windows Services screen - example

Linux Information

The **Linux System**screen displays the following information:

- System Information
- Network Information
- Memory Usage Information
- Mounted Filesystems Information



System

HostName :	frcls6260 (129.182.6.33)
OS :	Linux 2.6.9-1.648_EL
Uptime :	80 days, 2 hours, 7 minutes
Load Average :	1.09 (1 min), 0.91 (5 min), 0.85 (15 min)

Network

Interface	RX	TX	Err/Drop
lo	2.01 GB	2.01 GB	0
eth0	2.49 GB	1.66 GB	1009
sit0	0.00 KB	0.00 KB	0

Memory Usage

Type	Percent Used	Free	Used	Size
Physical Memory	99%	3.67 MB	499.96 MB	503.64 MB
Swap	0%	546.62 MB	2.47 MB	549.09 MB

Mounted Filesystems

Partition	Mount Point	Percent Used	Free	Used	Size
/dev/sda1 (ext3)	/boot	9%	85.25 MB	8.37 MB	98.72 MB
/dev/sda2 (ext3)	/	30%	5.14 GB	2.16 GB	7.69 GB
none (proc)	/proc	-	0.00 KB	0.00 KB	0.00 KB
none (sysfs)	/sys	-	0.00 KB	0.00 KB	0.00 KB
none (tmpfs)	/dev/shm	0%	251.82 MB	0.00 KB	251.82 MB
none (devpts)	/dev/pts	-	0.00 KB	0.00 KB	0.00 KB

Figure 67. Linux System 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 select the required sort option by clicking the corresponding link.

Display : PID User **Memory** CPU Search

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

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

Figure 68. Linux Process screen - example

The **Linux Users** screen displays user information:

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 69. Linux Users screen - example

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

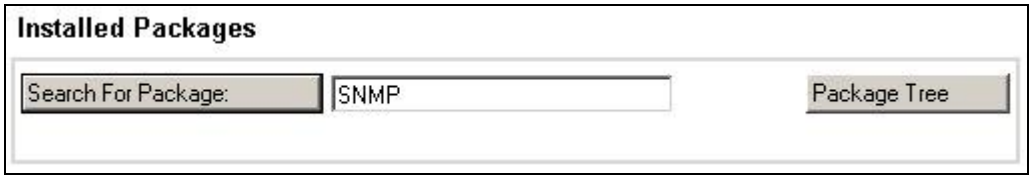


Figure 70. Linux RMP Products search screen - example

For example, if you enter **SNMP** in the search field and then click **Search For Package**, the following display appears:

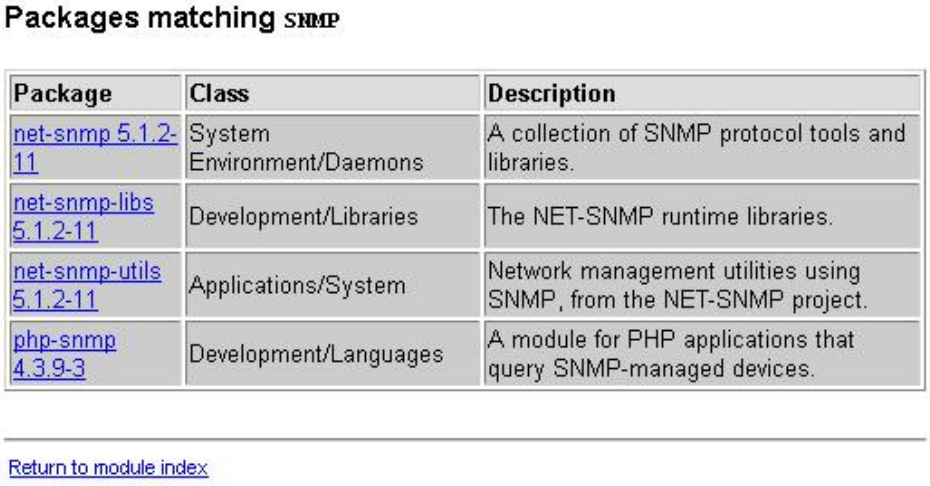


Figure 71. Linux RPM Products - example

The **Linux System Logs** screen displays available logs and allows you to view them.

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 72. Linux System Logs screen - example

Chapter 4. Using NovaScale Master Console Applications

NovaScale Master Hardware Management Application

The **NovaScale Master 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 Log**s for Express 5800 and NovaScale 4000, 5000 or 6000 series servers.

There are two ways to start the application:

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

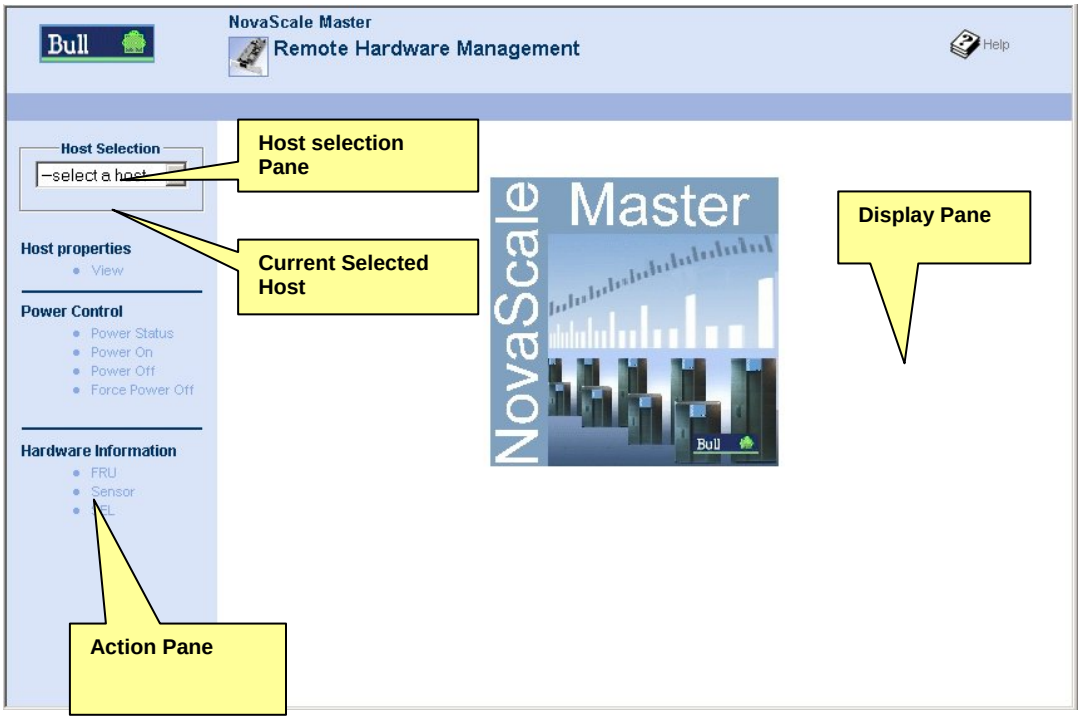


Figure 73. Remote Hardware Management screen

NovaScale Master Remote Hardware Management comprises three functional parts:

Host Selection Pane & Current Selected Host Pane Allows you to select the current host from all the Express 5800 and NovaScale 4000, 5000 or 6000 servers declared in the NovaScale Master configuration and displays it.

Action Pane Displays the hardware operations that can be executed.

Display Pane Displays parameter forms, messages and command results.

Host Selection

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

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 Pane**.

When a host is selected, the application reads NovaScale Master **configuration files** to get host properties.

Host Properties

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

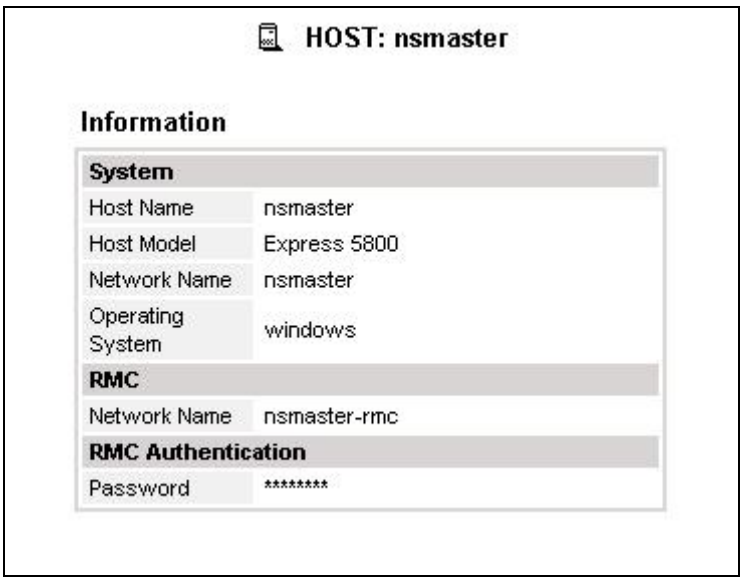


Figure 74. NovaScale 5000 Server host properties - example

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

Name	Name of the current selected host to which commands are applied.
Model	Host model.
Network Name	Current selected host local network name or IP address.
Operating System	Operating system type (Windows, Linux or any).
User	SMU authentication user. This user must be configured using ISM (Intel System Management) and is specific to the managed host. Therefore, this field is different from the **User** field required as **Authentication for Monitoring** when declaring an ISM Manager in NovaScale Master Configuration.
Password	SMU authentication password.

Table 16. NovaScale 4000 Server host properties

Name	Name of the current selected host to which commands are applied.
Model	Host model.
Domain	Current selected host domain name.
Operating System	Operating system type (Windows, Linux or any)
Platform	Platform name.
Manager Name	PAM Manager name.
Manager Network Name	Local network name or IP address of the PAP server managing the current selected host.
User	PAM authentication user (valid PAP server user).
Password	PAM authentication password.

Table 17. NovaScale 5000 or 6000 Server host properties

Name	Name of the current selected host to which commands are applied..
Model	Host model.
Network Name	Current selected host local network name or IP address.
Operating System	Operating system type (Windows, Linux or any).
RMC Netname	RMC network name.
RMC password	RMC password.

Table 18. Express 5800 Server host properties

Note:
These values always correspond with those found in the NovaScale Master Configuration.

Commands

Note:
All commands are applicable to the **Current Selected Host**.

Prerequisites

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. Uuser authentication must be declared in the NovaScale Master Configuration.

NovaScale 5000 and 6000 Servers

NovaScale Master 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 NovaScale Master server.

Express5800 Servers

The BMC (Baseboard Management Controller) on the managed host must be configured for remote-control over LAN. This is done using the MWA (Management Workstation Application) or DOS configuration tool available on the NEC EXPRESSBUILDER CD-ROM delivered with EXPRESS5800 Series servers.

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.

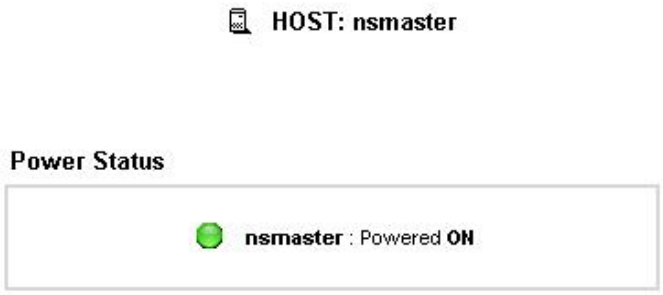


Figure 75. Power Status output - example

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).

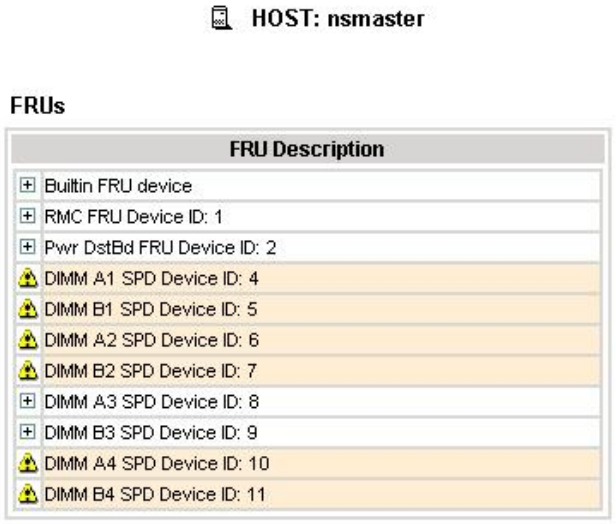


Figure 76. FRU output - example

SENSOR

Click **Sensor** to display sensors.

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

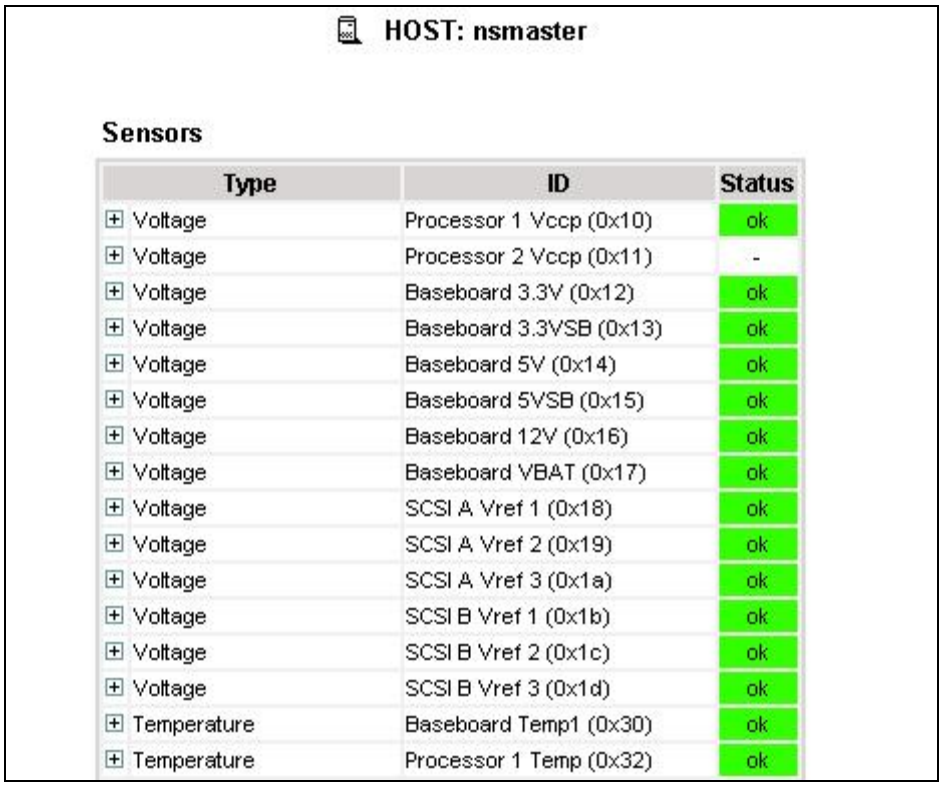


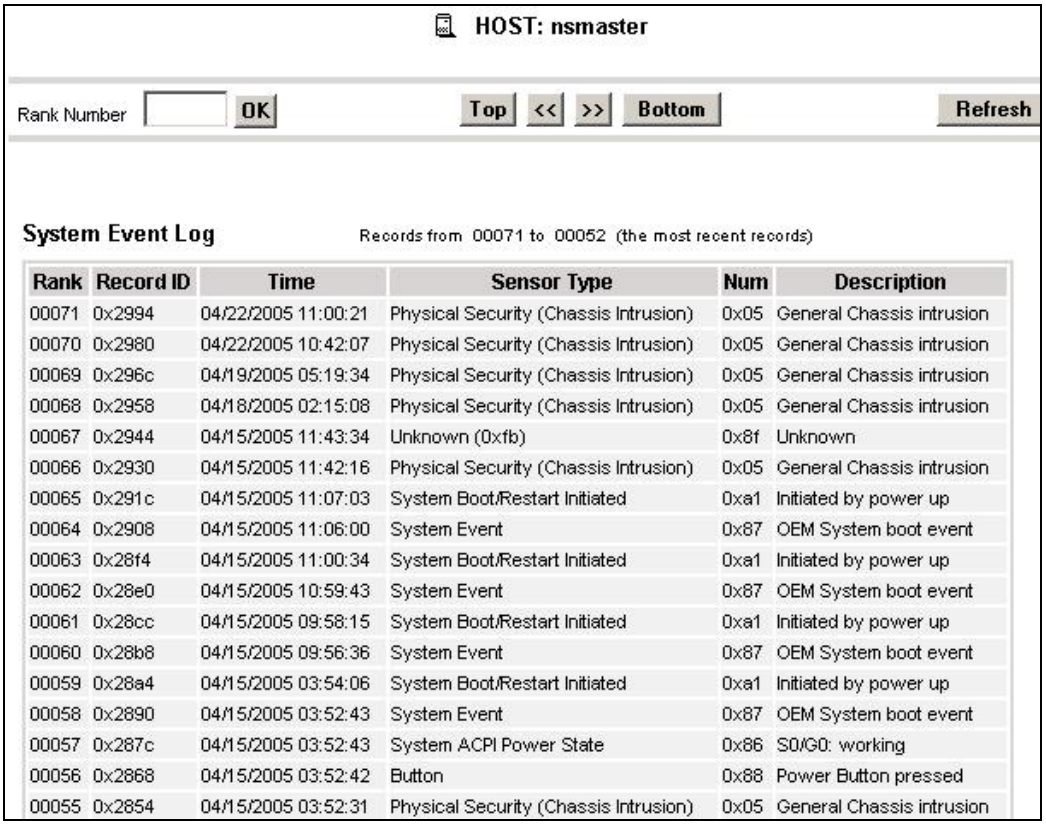
Figure 77. SENSOR output - example

SEL/PAM History

Click **SEL** (Express 5800 and Nova Scale 4000 Series) or **PAM History** (Nova Scale 5000 and 6000 Series) to display the 20 most recent records of the System Event Log.

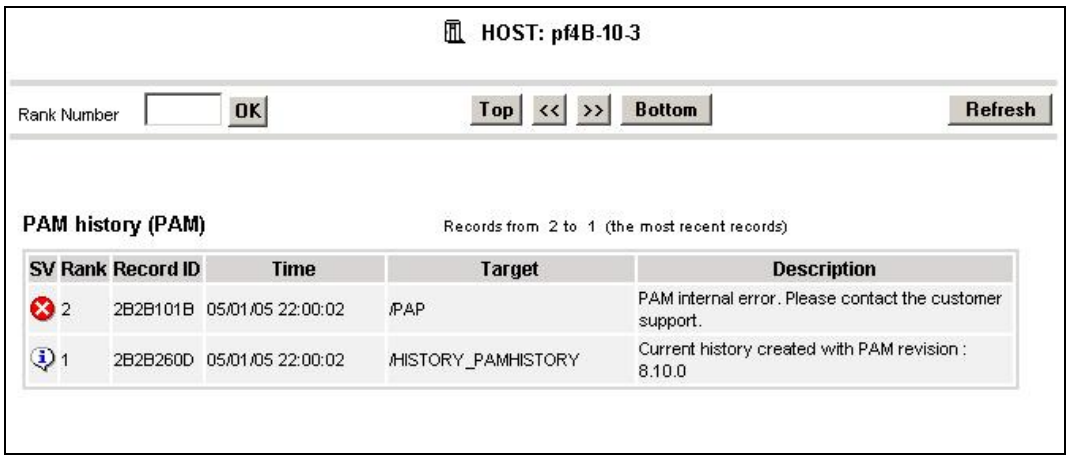
You can view records according to rank, to naviagate to next or previous records and to view the oldest records.

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



Rank	Record ID	Time	Sensor Type	Num	Description
00071	0x2994	04/22/2005 11:00:21	Physical Security (Chassis Intrusion)	0x05	General Chassis intrusion
00070	0x2980	04/22/2005 10:42:07	Physical Security (Chassis Intrusion)	0x05	General Chassis intrusion
00069	0x296c	04/19/2005 05:19:34	Physical Security (Chassis Intrusion)	0x05	General Chassis intrusion
00068	0x2958	04/18/2005 02:15:08	Physical Security (Chassis Intrusion)	0x05	General Chassis intrusion
00067	0x2944	04/15/2005 11:43:34	Unknown (0xfb)	0x8f	Unknown
00066	0x2930	04/15/2005 11:42:16	Physical Security (Chassis Intrusion)	0x05	General Chassis intrusion
00065	0x291c	04/15/2005 11:07:03	System Boot/Restart Initiated	0xa1	Initiated by power up
00064	0x2908	04/15/2005 11:06:00	System Event	0x87	OEM System boot event
00063	0x28f4	04/15/2005 11:00:34	System Boot/Restart Initiated	0xa1	Initiated by power up
00062	0x28e0	04/15/2005 10:59:43	System Event	0x87	OEM System boot event
00061	0x28cc	04/15/2005 09:58:15	System Boot/Restart Initiated	0xa1	Initiated by power up
00060	0x28b8	04/15/2005 09:56:36	System Event	0x87	OEM System boot event
00059	0x28a4	04/15/2005 03:54:06	System Boot/Restart Initiated	0xa1	Initiated by power up
00058	0x2890	04/15/2005 03:52:43	System Event	0x87	OEM System boot event
00057	0x287c	04/15/2005 03:52:43	System ACPI Power State	0x86	S0/G0: working
00056	0x2868	04/15/2005 03:52:42	Button	0x88	Power Button pressed
00055	0x2854	04/15/2005 03:52:31	Physical Security (Chassis Intrusion)	0x05	General Chassis intrusion

Figure 78. SEL output - example



SV	Rank	Record ID	Time	Target	Description
	2	2B2B101B	05/01/05 22:00:02	/PAP	PAM internal error. Please contact the customer support.
	1	2B2B260D	05/01/05 22:00:02	/HISTORY_PAMHISTORY	Current history created with PAM revision : 8.10.0

Figure 79. PAM History output - example

Reports

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

1. Launch the NovaScale Master Console and click **Reports** button to display available reports.
2. Click the required report.

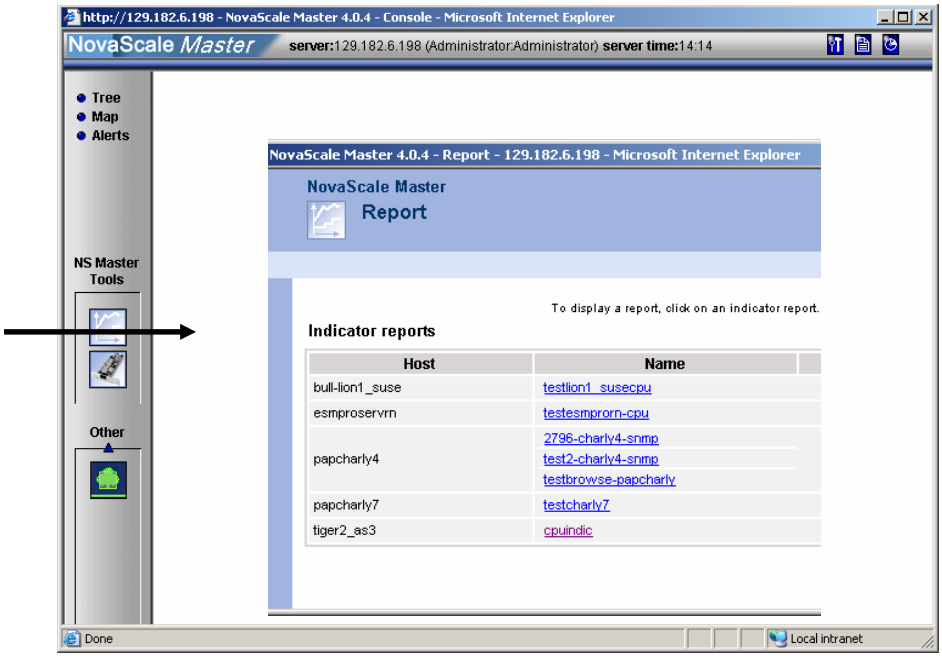


Figure 80. Indicator Reports

Each report comprises four graphs:

- Daily
- Weekly
- Monthly
- Yearly

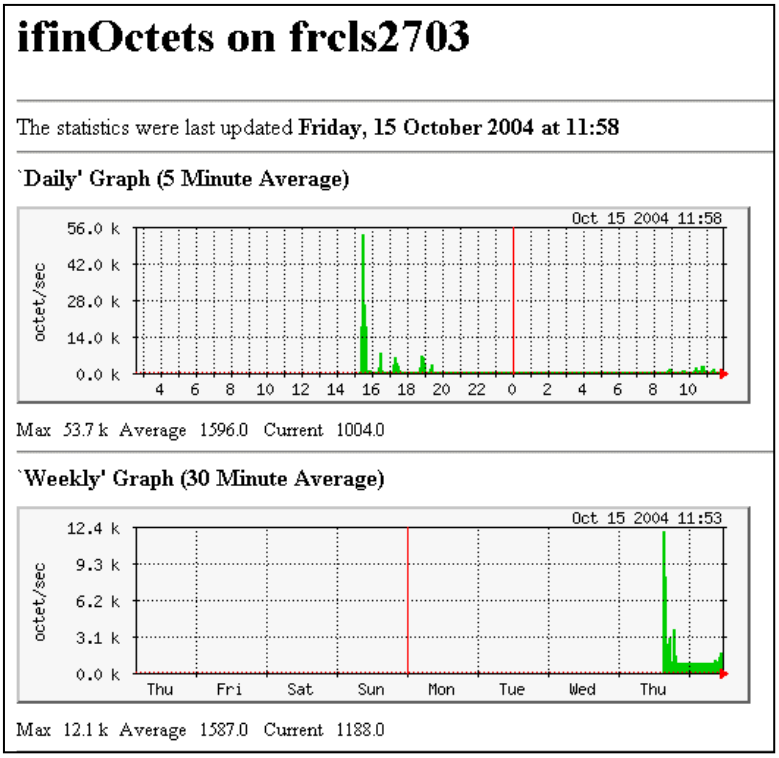


Figure 81. Daily and Weekly Report Graphs - example

Other Applications

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

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

Figure 82. Other applications

Chapter 5. Categories and Services Reference List

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

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

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 Pane (Monitoring Status Details).

Monitoring Hosts

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

Internet Category

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

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 **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.

HTTP_NSMaster

The **Internet.HTTP_NSMaster** service monitors the presence and status of the NS Master URL.

FTP

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

- Status is set to **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.

TCP_n

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

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

UDP_n

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

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

Reporting Category

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

Perf_indic

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

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

Monitoring Linux Systems

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

FileSystems Category

This category contains all the services for monitoring file systems.

All Service

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

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

Status Information

If status is set to **WARNING** or **CRITICAL**, **Status Information** lists the filesystems 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 Pane, click **System** (**Detailed Information** box) to get information about host filesystem size.
- From the Tree Pane, display the host pop-up menu and select:
  Remote Operation -> Actions -> FileSystems.
  You now have access to the host and you can investigate and correct the problem.

LinuxServices Category

This category contains all the services for checking the presence of a **Linux daemon**.

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 is different 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.

Examples:

OK – 1 processes running with command name syslogd

Correcting Status

- From the Applications Pane, click **Processes** (**Detailed Information** box) to get the list of processes currently running on the system.
- From the Tree Pane, display the host pop-up menu and select:
  Remote Operation -> Actions -> Processes or **Remote Operation -> Telnet**.
  You now have access to the host and you can investigate and correct the problem.

Syslog Category

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

AuthentFailures Service

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 than a FAILED LOGIN line, already detected).

Note:
Only new lines (if any) are checked each time. If the file has been truncated or rotated since the last check, 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:
WARNING status can be very fugitive 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 regularly consult service history.

Note:
The **notify_recovery** field is set to **0** because it is not applicable to this service.

Status Information

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

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…) is the last matching line detected.

Correcting Status

- From the Applications Pane, click **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 Tree Pane, display the host pop-up menu and select:
  Remote Operation -> Actions or Telnet.
  You have now access to the host and you can investigate and correct the problem.

SystemLoad Category

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

CPU Service

The **CPU** service monitors total CPU load over three periods of time:

- 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. 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 respectively the last **1** minute, the last **5** minutes and the last **15** minutes.

Examples:

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

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

Correcting Status

- From the Applications Pane, click **Processes** (**Detailed Information** box) to get process CPU consumption.
- From the Tree Pane, display the host pop-up menu and select:
  Remote Operation -> Actions -> Processes
  You have now access to the host and you can investigate and correct the problem.

Memory Service

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

You have now access to the host and you can investigate and correct the problem.

Processes Service

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 Pane, click **Processes** (**Detailed Information** box) to get the list of the processes.
- From the Tree Pane, display the host pop-up menu and select:
  Remote Operation -> Actions -> Processes.
  You have now access to the host and you can investigate and correct the problem.

Users Service

The **Users** service monitors the number of **users currently logged** in 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 to the system.

Examples:

USERS OK – 2 users currently logged in

USERS WARNING - 16 users currently logged in

Correcting Status

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

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.

Note:
The Windows monitoring agent part is based on two windows services:

NovaScale Master Management agent.

Its main function is giving OS and HW information, but it provides the **“LogicalDisk.All”** monitoring service too.

NovaScale Master Monitoring agent.

It provides all Windows monitored services, except “LogicalDisk.All”.

EventLog Category

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

Application Service

The **EventLog.Application** service monitors the number of **Error, Warning** and **Information** events generated in the Application Event log for the last **30** 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 status is set to **WARNING** or **CRITICAL**, gives the number of events responsible. This message is also a link to an html file containing the following detailed information:

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

Examples:

OK: no new events for the last 30 mn

WARNING: 1 new events for the last 30 mn!

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

Correcting Status

- From the Applications Pane, click **Events** (**Detailed Information** box) for more information.
- From the Tree Pane, display the host pop-up menu and select:
  Remote Operation -> VNC Viewer or **Remote Operation -> Telnet**.
  You have now access to the host and you can correct the problem.

Security Service

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

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

Status Information

If status is set to **WARNING** or **CRITICAL**, gives the total number of events responsible. This message is also a link to an html file containing the following detailed information:

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

Examples:

OK: no new events for the last 30 mn

WARNING: 4 new events for the last 30 mn!

Correcting Status

- From the Applications Pane, click **Events** (**Detailed Information** box) for more information.
- From the Tree Pane, display the host pop-up menu and select:
  Remote Operation -> VNC Viewer or **Remote Operation -> Telnet**.
  You have now access to the host and you can correct the problem.

System Service

The **EventLog.System** service monitors the number of **Error, Warning** and **Information** events generated in the System event log over the last **30** 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 status is set to **WARNING** or **CRITICAL**, gives the total number of events responsible This message is also a link to an html file containing the following detailed information:

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

Examples:

OK: no new events for the last 30 mn

CRITICAL: 8 new events for the last 30 mn!

Correcting Status

- From the Applications Pane, click **Events** (**Detailed Information** box) for more information.
- From the Tree Pane, display the host pop-up menu and select:
  Remote Operation -> VNC Viewer or **Remote Operation -> Telnet**.
  You have now access to the host and you can investigate and correct the problem.

LogicalDisks Category

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

All Service

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

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

Status Information

Gives the list of 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 Pane, 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 Tree Pane, display the host pop-up menu and select:
  Remote Operation -> VNC Viewer or **Remote Operation -> Telnet**.
  You have now access to the host and you can investigate and correct the problem.

SystemLoad Category

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

CPU Service

The **CPU** service monitors the total CPU load over two periods of time: 1min and 10 min

- 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 percentage of average CPU load for respectively the last **1** minute and the last **10** minutes. If status is **WARNING or** CRITICAL**,** it displays the most consuming process, and its percentage of CPU consumption, at check time.

Examples:

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

CPU Load HIGH (1mn: 92%) (10mn: 56%) – Process cputest.exe using 100%

Correcting Status

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

MemoryUsage Service

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

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

Status Information

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

Examples:

Memory Usage OK - (total: 1480Mb) (used: 193Mb, 13%) (free: 1287Mb) (physical: 511Mb)

Memory Usage WARNING - (total: 2462Mb) (used: 1773Mb, 72%) (free: 689Mb) (physical: 1023Mb)

Correcting Status

- From the Applications Pane, click **Memory** (**Detailed Information** box) to get detailed memory consumption.
  Then click **Processes** to get memory consumption spent per process.
  Then click **General (Host Information** box**)** to get information about the physical memory configuration and layout.
- From the Tree Pane, display the host pop-up menu and select:
  Remote Operation -> VNC Viewer or **Remote Operation -> Telnet**.
  You have now access to the host and you can investigate and correct the problem.

WindowsServices Category

EventLog Service

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

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

- Status is set to **WARNING** at least one of these services is **paused** and the others are **running**.

- Status is set to **CRITICAL** if at least one of these services **does not exist** or is **not running**.

Status Information
Displays service name and status.

Examples:

OK: ‘EventLog’

NotActive: ‘EventLog’

Correcting Status
- From the Applications Pane, click **Memory** (**Detailed Information** box) to get detailed information about services.
- From the Tree Pane, display the host pop-up menu and select:
  Remote Operation -> VNC Viewer or **Remote Operation -> Telnet**.
  You have now access to the host and you can investigate and correct the problem.

Hardware Monitoring

Hardware Category for NovaScale Blade Series

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 identified the host in the NovaScale Blade Chassis) must be provided during NovaScale Master configuration. 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 can't be retrieved from the CMM manager due to connection timeout. This issue can result from a bad declaration of the SNMP Manager in the CMM configuration.

Correcting Status

- From the Tree Pane, display the host pop-up menu and select:
  HW Manager GUI to launch the CMM tool and investigate and correct the problem.

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

Hardware Category for NovaScale 4000 Series

Alerts Service

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

To enable this service, the **mib basebrd5** must be integrated in the NovaScale Master application and **SNMP trap reception** must be enabled.

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

Traps are previously filtered and only the traps emitted by the Hardware Management card are used to animate this service. The Hardware Management card must be properly configured with the Intel SMU tool to send traps to the NovaScale Master_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 status information

Example:

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

Correcting Status

- From the Tree Pane, display the host pop-up menu and select:
  HW Manager GUI to launch the ISM tool and investigate and correct the problem.

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

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 ISM.

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

Correcting Status

- From the Tree Pane, display the host pop-up menu and select:
  HW Manager GUI to launch the ISM tool and investigate and correct the problem.

Hardware Category for NovaScale 5000 & 6000 Series

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.

Examples:

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 Pane, display the host pop-up menu and select:
  PAM to launch the PAM tool and investigate and correct the problem.

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

Other Monitoring

PAM Category

GlobalStatus Service

The **GlobalStatus** service reflects global functional status, as returned by the PAM manager. This comprises the hardware status of the whole configuration managed by this instance of PAM, as well as the status of the PAM manager itself.

This service only exists on a host declared as a NovaScale 5000 / 6000 manager (see the *Administrator's Guide* for details about how, as Administrator, you can declare a manager).

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

Status Information

Status information is set by PAM and represents the global functional state for the managed hosts and for the PAM manager tool.

Examples:

The PAM manager global status is WARNING

Correcting Status

- From the Tree Pane, display the host pop-up menu and select:
  PAM to launch the PAM tool and investigate and correct the problem.

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

Alerts Service

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

To enable this service, the **mib PAMEventtrap** must be integrated in the NovaScale Master 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 have been correctly configured to send traps to the NovaScale Master_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.

CMM Category

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 Pane, display the host pop-up menu and select:
  CMM to launch the CMM tool and investigate and correct the problem.

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

Alerts Service

The **Alerts** Service is used to collect the hardware SNMP traps emitted by the manager. To enable this service, the **mib mmalert** must be integrated in the NovaScale Master 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 NovaScale Master_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.

RMC Category

PowerStatus Service

The **PowerStatus** service reflects the power status of an Express5800, as returned by the RMC management card.

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

- Status is set to **CRITICAL** if RMC has assigned a **power** status **off**.
- Status is set to **UNKNOWN** if RMC is not accessible or if RMC has not been able to compute power status.

Correcting Status

- From the Tree Pane, display the host pop-up menu and select:
  RMC to launch the CMM tool and investigate and correct the problem.

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

Alerts Service

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

To enable this service, the **mib bmclanpet** must be integrated in the NovaScale Master 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 NovaScale Master_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.

Storage Monitoring

Storage Category

SanitStatus Service

The **SanitStatus** service monitors the state of the storage, returned by the S@N.IT! application, for any host managed in the SAN.

To enable this service, a SANIT manager must be declared for the host.

- Status is set to **OK** if S@N.IT! has assigned a **NORMAL** status to the host.
- Status is set to **CRITICAL** if S@N.IT! has assigned a **FAULTY** status to the host.
- Status is set to **UNKNOWN** if S@N.IT! has assigned an **UNKNOWN** or **NOT MONITORED** status to the host OR if the storage identifier provided during the NovaScale Master configuration is not valid. Please refer to the *Administrator's Guide* for details.

Correcting Status

- From the Tree Pane, display the host pop-up menu and select:
  S@N.IT to launch the client part of the application (Web or local mode) and investigate and correct the problem.

SANIT Category

Alerts Service

The **Alerts** Service is used to collect the SNMP traps emitted by the S@N.IT! application.

To enable this service, the **mib fcmgmt3** must be integrated in the NovaScale Master application and **SNMP trap reception** must be enabled.

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

The S@N.IT! application must be correctly configured to send traps to the NovaScale Master_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..

MegaRAID Category

Status Service

The **Status** service monitors the state of the storage, returned by the MegaRAID SNMP agent.

To enable this service, **MegaRAID** category and **Status** service must be configured for the host.

- Status is set to **OK** if agent has assigned a **NORMAL** status to the host.
- Status is set to **CRITICAL** if agent has assigned a **FAULTY** status to the host.
- Status is set to **UNKNOWN** if agent has assigned an **UNKNOWN** or **NOT MONITORED** status to the host. Please refer to the *Administrator's Guide* for details.

Alerts Service

The **Alerts** Service is used to collect the SNMP traps emitted by the MegaRAID SNMP agent.

To enable this service, the **mib megaraid** must be integrated in the NovaScale Master application and **SNMP trap reception** must be enabled.

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

The MegaRAID SNMP agent must be correctly configured to send traps to the NovaScale Master_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.

Index

Vos remarques sur ce document / Technical publication remark form

Titre / Title : Bull NovaScale Master User's Guide

Nº Reférence / Reference Nº : 86 A2 49EG 04

Daté / Dated : July 2005

ERREURS DETECTEES / ERRORS IN PUBLICATION

AMELIORATIONS SUGGEREES / SUGGESTIONS FOR IMPROVEMENT TO PUBLICATION

Vos remarques et suggestions seront examinées attentivement.
Si vous désirez une réponse écrite, veuillez indiquer ci-après votre adresse postale complète.

Your comments will be promptly investigated by qualified technical personnel and action will be taken as required.
If you require a written reply, please furnish your complete mailing address below.

NOM / NAME : _____ Date : _____

SOCIETE / COMPANY : _____

ADRESSE / ADDRESS : _____

_____

Remettez cet imprimé à un responsable BULL ou envoyez-le directement à :

Please give this technical publication remark form to your BULL representative or mail to:

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

Technical Publications Ordering Form

Bon de Commande de Documents Techniques

To order additional publications, please fill up a copy of this form and send it via mail to:
Pour commander des documents techniques, remplissez une copie de ce formulaire et envoyez-la à :

BULL CEDOC
ATTN / Mr. L. CHERUBIN
357 AVENUE PATTON
B.P.20845
49008 ANGERS CEDEX 01
FRANCE

Phone / Téléphone : +33 (0) 2 41 73 63 96
FAX / Télécopie +33 (0) 2 41 73 60 19
E–Mail / Courrier Electronique : srv.Cedoc@franp.bull.fr

Or visit our web sites at: / Ou visitez nos sites web à:

http://www.logistics.bull.net/cedoc

`http://www-frec.bull.com` `http://www.bull.com`

CEDOC Reference # Nº Référence CEDOC	**Qty** Qté	**CEDOC Reference #** Nº Référence CEDOC	**Qty** Qté	**CEDOC Reference #** Nº Référence CEDOC	**Qty** Qté
__ __ ____ _ [__]		__ __ ____ _ [__]		__ __ ____ _ [__]	
__ __ ____ _ [__]		__ __ ____ _ [__]		__ __ ____ _ [__]	
__ __ ____ _ [__]		__ __ ____ _ [__]		__ __ ____ _ [__]	
__ __ ____ _ [__]		__ __ ____ _ [__]		__ __ ____ _ [__]	
__ __ ____ _ [__]		__ __ ____ _ [__]		__ __ ____ _ [__]	
__ __ ____ _ [__]		__ __ ____ _ [__]		__ __ ____ _ [__]	
__ __ ____ _ [__]		__ __ ____ _ [__]		__ __ ____ _ [__]	
[_ _] : **no revision number means latest revision** / pas de numéro de révision signifie révision la plus récente					

NOM / NAME : ______________________________ Date : __________

SOCIETE / COMPANY : ______________________________

ADRESSE / ADDRESS : ______________________________

____

PHONE / TELEPHONE : ____________________ FAX : ____________________

E–MAIL : ______________________________

For Bull Subsidiaries / Pour les Filiales Bull :

Identification: ______________________________

For Bull Affiliated Customers / Pour les Clients Affiliés Bull :

Customer Code / Code Client : ______________________________

For Bull Internal Customers / Pour les Clients Internes Bull :

Budgetary Section / Section Budgétaire : ______________________________

For Others / Pour les Autres :

Please ask your Bull representative. / Merci de demander à votre contact Bull.

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

ORDER REFERENCE
86 A2 49EG 04

Utiliser les marques de découpe pour obtenir les étiquettes.
Use the cut marks to get the labels.

NovaScale
Master
User's Guide

86 A2 49EG 04

NovaScale
Master
User's Guide

86 A2 49EG 04

NovaScale
Master
User's Guide

86 A2 49EG 04