Bull System Manager

BSM 1.4

Administrator's Guide

NOVASCALE
& ESCALA

REFERENCE
86 A2 56FA 04

NOVASCALE & ESCALA

BSM 1.4

Administrator's Guide

Software

January 2011

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

REFERENCE
86 A2 56FA 04

Printed in France

Trademarks and Acknowledgements

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

Table of Contents

List of Figures

List of Tables

Preface

Scope and Audience of this Manual

Bull System Manager is the Bull product for managing Bull platforms. Administration environments can include different platforms from the **NovaScale Series**, **Express 5800 Series** or **Escala Series** servers.

The Bull System Manager configuration must be customized to monitor specific environments. This manual explains how, as Administrator you can perform various configuration tasks.

Note Configuration tasks may only be performed by Administrators.

Using this Manual

For a conceptual description of Bull System Manager, see **Chapter 1 Introduction**.

If you are configuring Bull System Manager for the first time, see **Chapter 2 Configuration Overview**. This chapter helps identify the configuration tasks that have to be performed, and explains where to find detailed information about these tasks.

Chapter 3 to **Chapter 10** describe how to configure the different Bull System Manager monitoring elements (Hosts, Hostgroups, Hardware Manager, Virtualization Manager, Storage Manager, Supervision, Event Reception, Performance Indicators, Event Handler, Notifications, Views, Maps, Focus Pane).
These chapters provide detailed information about all resource properties, as well as concrete examples to help you customize your environment (Adding Hosts, Creating Hostgroups, Modifying Service Parameters, Organizing Views, Creating Maps, Specifying the Focus Pane, etc.).

Chapter 11 Customizing the Bull System Manager Console describes how to customize the Bull System Manager Console.

Chapter 12 Configuring Local Settings describes how to configure the environment and tasks on the local server.

Chapter 13 Configuring Global Settings describes how to set a distributed solution.

Appendix A Predefined Categories and Services contains reference information about categories and services.

Appendix B Generated Categories and Services lists the generated services with the corresponding host or manager Topology edition page.

Appendix C Check Commands for Customizable Services describes how to use **Nagios** check commands with customizable services.

Appendix D Administration Commands describes some useful commands.

Appendix E SSH Configuration describes the SSH configuration specific to BSM Applications.

Related Information

Bull System Manager Documentation

- In this guide, we assume that Bull System Manager is fully installed. If you need information about installation, refer to the *Bull System Manager Installation Guide* (Ref. 86 A2 54FA).
- The Bull System Manager GUI (Graphical User Interface) is not described in this guide. For information about the GUI and how to use it, refer to the *Bull System Manager User's Guide* (Ref. 86 A2 55FA).
- The Hardware Management CLI provides an easy Command Line Interface (**CLI**) for remote hardware management. For information about the CLI refer to the *Remote Hardware Management CLI Reference Manua*l (Ref. 86 A2 58FA).
- Restrictions and well-known problems are listed in the associated *Release Notes* document (Ref. 86 A2 57FA).

Other documentation

- *NovaScale Blade Chassis Management Module Installation and User's Guide* (Ref. 86 A1 12EM).
- *Getting Started with Intel Server Management (ISM)*.
- *Management Workstation Application (MWA)* guide on the NEC EXPRESSBUILDER CD-ROM (to configure NEC Express 5800 Series Servers).

Highlighting

The following highlighting conventions are used in this book:

Bold Identifies commands, keywords, files, structures, directories, and other items whose names are predefined by the system. Also identifies graphical objects 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 details.

`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.

Chapter 1. Introduction

1.1 Bull System Manager Overview

Bull System Manager (BSM) is the Bull product for managing Bull platforms. Administration environments can include different platforms from the NovaScale series, Express 5800 series, Escala series servers or external devices, including disks bays or switches.

1.1.1 Components

BSM consists of three main components that can be deployed on **Windows** and **Linux** systems:

- **Management Server**
- **Management Console**
- **Management Agent**

Management Server

Provides the infrastructure, and services responsible, for the collection and utilization of operation data. **Management Server** must be installed on the server dedicated to management.

Management Console

Provides third-party management tools for the end-user station running the **Bull System Manager** console web **GUI**.

Management Agent

Provides instrumentation and administration tools for monitored servers. **Management Agent** must be installed on each server that you want to monitor.

Additional extensions are also available to:

- Extend **Bull System Manager** monitoring, with links to third-party management tools for specific devices and/or specific system functionalities.
- Extend server functionalities using **NDOutils** to store all the **Nagios** status information in a **MySQL** database.
- Extend server functionalities using **NSCA** to relay all the **Nagios** status to another Nagios or to receive asynchronous status change via a send_NSCA command.
- Extend server functionalities using **PNP4Nagios** to analyze performance data provided by plugins and store them automatically into RRD-databases.

1.1.2 Distribution

You can implement a distributed solution by joining together multiple Bull System Manager Servers using the database provide by the **NDOutils** extension to allow them to share information, available through a Global Console.

To set a distributed solution, you have to install the **NDOutils** extension on each server, then select a server to be the central node that hosts the centralized database and configures the other secondary nodes to link to the database.

⚠ CAUTION:
A solution with more than one central node is not supported.

There is no global **BSM** configuration tool. Each BSM server node uses its own local **BSM** configuration tool.

Each BSM server node collects the data associated with its configured hosts list and stores them in a centralized repository. The BSM global console uses this repository to show all the data for all the node servers.

1.2 Bull System Manager Concepts

Bull System Manager is a System Management product, which can be used for the following functions: Monitoring, Inventory, Reporting and Remote Operation.

Monitoring

Bull System Manager monitoring ensures the following tasks:

- The monitoring of Bull machines: Bull System Manager checks to see if these hosts are accessible, using the **ping** command from the System Manager. The machines to be monitored are either explicitly specified by the Administrator or selected by a discovery mechanism.
- Monitoring specific elements of the operating system, services and Internet such as **CPU load, memory usage, disk usage, number of users, processes** and **service execution, http and ftp services**.
  You can define status thresholds (**OK**, **WARNING**, **CRITICAL**, **UNKNOWN**) for each element monitored. When an anomaly occurs or when normal status is recovered, **alerts** (in a log file) and **notifications** (by e-mail, by Bull auto-call and/or by **SNMP** trap) are generated.
- Bull System Manager allows you to group monitored hosts into entities that reflect your environment so that you can easily identify an anomaly for these entities.
- Bull System Manager allows you to group instantiated services into specific functional domains so that you can display monitoring information for a functional domain only.

Inventory

Bull System Manager Inventory is used to display hardware and software information for the host. This function requires the installation of the BSM agent on the monitored host.

Reporting

Bull System Manager Reporting allows data to be presented in graph form so that changes for numeric indicators can be seen easily.

Remote Operations

Bull System Manager Remote Operation enables actions to be executed on a host via the OS or via a Hardware Management tool.

1.2.1 Topology Elements

The **Host** is the main resource to be monitored. The Administrator has to define the host properties (**Operating System, Model, Notification properties,** etc.) for all the hosts in the configuration.
See *Configuring Hosts*, on page 27, for a complete description of host properties.

A **Hostgroup** allows you to structure hosts in logical entities reflecting your environment. Hostgroup statistics collect the status for the Hostgroup elements. For each Hostgroup, you can define a **Contactgroup** to be notified of the events which occur on each host in the Hostgroup.
See *Configuring Hostgroups*, on page 71, for a complete description of the Hostgroup properties.

A **Platform** is a particular Hostgroup defined to represent a common set of hosts from the same series. For example, a NovaScale 6xx0 server might contain one or more hosts.
See *Platforms*, on page 72 for details.

A **Virtualization Platform** is a particular Hostgroup defined to represent a set of virtual machines. For example, the Escala servers are commonly represented as a virtualization platform grouping the logical partitions together.
See *Platforms*, on page 72 for details.

Note **NovaScale 5000** & **6000** series hosts are known as **domains**.

1.2.2 Monitoring

A service (or monitoring service) defines how specific host elements are monitored. A service can be defined for all hosts or for a list of hosts, depending on the OS (**Windows**, **Linux**, **AIX** or any) and/or on the model. Notification properties are defined for each service.
Services are organized into monitoring **categories**. For instance, the **SystemLoad** category includes the **CPU** and **Memory** services for a Windows host.

See *Configuring Supervision*, on page 85 and *Predefined Categories and Services*, for a complete description of the services and categories.

1.2.3 Event Reception

Bull System Manager can receive **SNMP traps** from any SNMP agent. SNMP traps enable an agent to notify the Bull System Manager server of significant events via an unsolicited SNMP message. SNMP Traps must be defined in a **MIB** (Management Information Base).

See *Configuring Supervision Event Reception*, on page 153 for details.

1.2.4 Notifications

Bull System Manager can send notifications when events occur on a monitored element (for example alerts or recoveries). Three types of notification are available: by e-mail, by Bull autocall and/or by SNMP trap.

New type of notification can be added by defining a new contact and the corresponding notification commands.

Notification by E-mail

A **Mail server** is needed to relay e-mails. Its configuration is differs for Windows and Linux platforms.
E-mail notifications are sent to all the **Contacts** in a **Contactgroup**.

See *Contacts*, on page 172 and *Contactgroups*, on page 174, for a description of Contact and Contactgroup properties.

Notification by Bull Autocall

Autocall server configuration is required to define the **GTS** server that will relay autocalls to the Bull maintenance site.

Notification by SNMP Trap

SNMP manager configuration is required to define **SNMP** trap receivers.

See *Configuring Notifications*, on page 171, for details about these different notification types.

1.2.5 Event Handling

Bull System Manager can execute commands when the status changes for a monitored element. These commands are executed locally on the Bull System Manager server.

See *Configuring Event Handler*, on page 165, for details about these different notification types.

1.2.6 Hardware Manager

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

See *Configuring a Hardware*, on page 76 for a description of the **Hardware Manager** properties.

1.2.7 Virtualization Manager

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

See *Configuring a Virtualization Manager*, on page 80 for a description of Virtualization Manager properties.

1.2.8 Storage Manager

The **Storage Manager** manages storage for one or a set of servers.

See *Configuring a Storage Manager* on page 78, for a description of Storage Manager properties.

1.2.9 Views

The Management Tree part of the Bull System Manager Console represents monitored hosts through different **views**. Views differ only in the way they display hosts, but their objective is always the same: to present host status and monitoring services.

1.2.10 Maps

As an alternative to Management Tree views, the Bull System Manager Console offers a **map** representation of hostgroups located at specified positions (x,y) and animated according to their status. A zoom on a hostgroup displays the associated hosts with their status.

See *Specifying Maps*, on page 189, for details.

1.2.11 Focus Pane

The Bull System Manager Console allows you to display very important services (with their status) in a separate pane called **Focus Pane**.

See *Specifying the Focus Pane*, on page 192, for details.

1.2.12 Performance Indicators

Performance indicators are used as long-term counters reflecting specific functional qualities. Collection of performance indicators with MRTG tool is deprecated and replaced by PNP4Nagios server extension.

Note: Nevertheless, if MRTG indicators have been defined before the BSM 1.4 migration, or if the BSM integrator or Administrator has enabled the MRTG usage in BSM, you may have both MRTG indicators and PNP4nagios indicators.
You can contact Bull support to get the "BSM MRTG HowTo guide", in order to enable and configure MRTG indicators.

See *Configuring Performance Indicators*, on page 157, for a description of related indicator configuration

An export mechanism is provided for these indicators. A periodic task can be configured to generate a daily repository file for each indicator.
See *Export daily information of a MRTG indicator,* on page 158 for a description of the periodic task properties.
Associated with the generation of daily files is the use of a **Nagios** plugin to send mail notifications regarding the content of these files. See *Monitor and Notify by Mail the indicators daily information,* on page 161 for a description of the plug-in properties.

1.3 Configuration Architecture

The configuration of Bull System Manager is based on a Client-Server architecture:

- A web **GUI** based on **PHP** technologies.
- A common repository on the Bull System Manager server host, which contains two types of configuration information:
  - Predefined resources (default configuration)
  - Customized resources (resources that the Administrator has added or modified).
- Generation tools to check the configuration and to generate configuration data for the Bull System Manager Console Management, monitoring services (**Nagios**) and performance data services (PNP4Nagios).

Note The configuration of Bull System Manager is already performed on BSM server host. For the distributed solution, each server manages its local configuration and publishes it to a centralized database (CMDB), allowing each server to access all data.

The figure below represents this architecture:

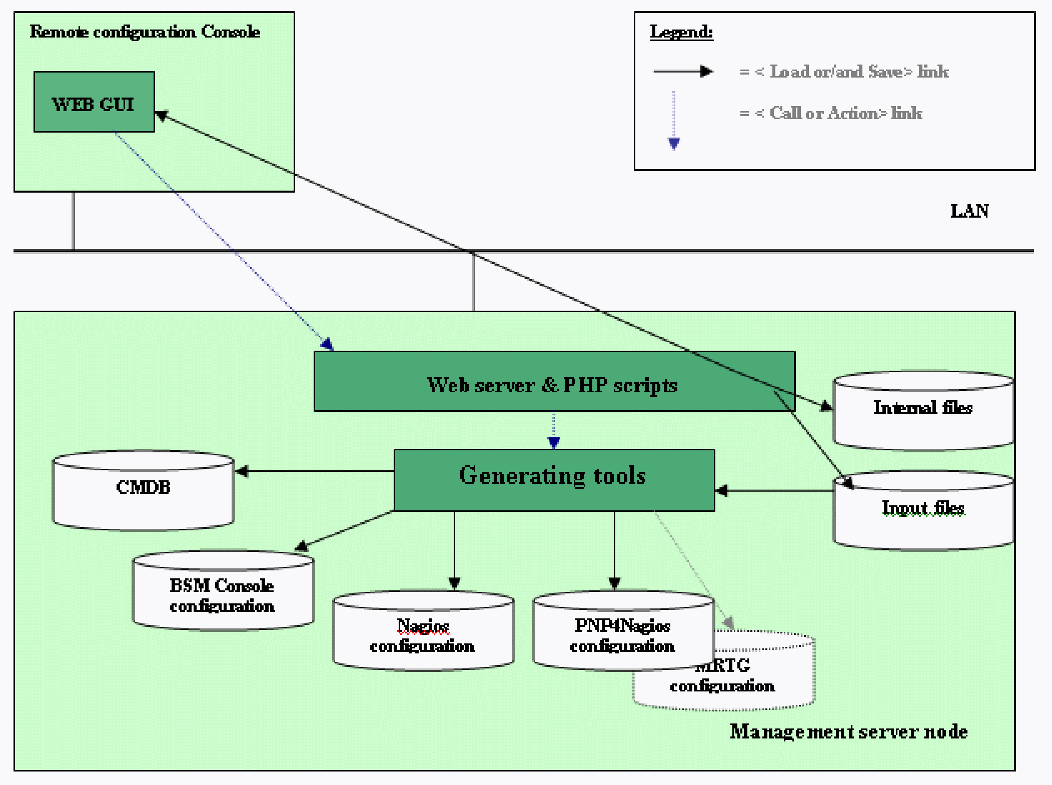


Figure 1-1. Configuration architecture

Note The configuration GUI is based on **PHP** scripts. Consequently, the GUI requires a web server running **PHP**.

Chapter 2. Configuration Overview

Configuring **Bull System Manage**r consists mainly in:

- Specifying the parameters required for monitoring tasks
- Specifying the performance indicators that will be displayed for reporting
- Customizing the Bull System Manager Console to define new applications, the default view, the maps and the focus pane
- Customizing the Bull System Manager functionalities and users
- If needed, specifying the Bull System Manager components for a distributed solution.

Most configuration tasks are performed via the Bull System Manager Configuration GUI (Graphical User Interface).

2.1 Default Configuration

During installation of Bull System Manager, the following configurations are put in place:

- Default categories with their associated monitoring checks (services) are made available.
- The default Reporting indicator is not defined.
- The **mgt-admins** contact group and the **manager** contact are defined for mail notifications.
- The host on which the Bull System Manager server is installed is configured as a host to be monitored. The **BSM** Hostgroup is created, including the Bull System Manager server host.
- The **default_map** map is configured with the **BSM** Hostgroup.

2.2 Configuration Tasks

As the Administrator, you must specify which **hosts** will be monitored. See *Configuring Hosts* on page 27.

If required, you can then modify the default configuration details, by:

- Defining new **Contacts** and **Contactgroups** that will be notified of any anomaly, or recovery, for a monitored element.
  See *Contacts*, on page 172 and *Contactgroups*, on page 174.
- Defining the **hardware managers** that manage host hardware
  See *Configuring a Hardware Manager*, on page 76.
- Defining the **storage managers** that manage host storage.
  See *Configuring a Storage Manager*, on page 78.
- Defining the **virtualization managers** that manage virtual machines. See *Configuring a Virtualization Manager*, on page 80.
- Defining **Hostgroups** (collections of hosts).
  See *Configuring Hostgroups*, on page 71.

- Customizing **categories** and monitoring **services**.
  See *Configuring Supervision*, on page 85, for a description of general monitoring configuration procedures:
  - Restricting monitoring of some services to particular hosts.
    See *Customizing the List of Monitored Hosts*, on page 109.
  - Defining new resources to monitor. For examples see:
    Customizing Windows Services, on page 113
    Customizing Linux or AIX Services, on page 115
    Customizing URL Access, on page 117.
  - Defining of specific monitoring properties (**thresholds, check period, check interval**, etc.) for certain services and for different hosts

    For examples see:

    Customizing the Notification Period, on page 109

    Customizing Thresholds, on page 111.
- Definition of Servicegroups (collections of services).
  See *Configuring Servicegroups*, on page 120 .
- Configuration of the **notification elements**.
  See *Configuring Notifications*, on page 171.
- Creation of important Reporting **performance indicators**.
  See *Configuring Performance Indicators*, on page 157.
- Definition of BSM components for a distributed solution.
  See *Configuring Global Settings*, on page 201.

2.3 Customization Tasks

Customizing the Bull System Manager Console consists in the following tasks:

- Definition of the **users** allowed access to the Bull System Manager Console (name and role/profile, typically Administrator and Operator).
  See *Configuring Users & Roles*, on page 195.
- Specification of the **applications** that can be launched from the Console Application Bar (for example an external web URL or any local command).
  See *Specifying Applications*, on page 186 .
- Choice of the **default view** that will be loaded in the Console Management Tree.
  See *Choosing the Default View*, on page 188 .
- Creation of the **maps** where hostgroups (with their status) are displayed at specified positions on a background image in the Bull System Manager Console.
  See *Specifying Maps*, on page 189.
- Specification of the **focus pane**, to display important services (with their status) in the Bull System Manager Console.
  See *Specifying the Focus Pane*, on page 192.

2.4 Configuration GUI

Bull System Manager provides a GUI to perform the main configuration tasks.

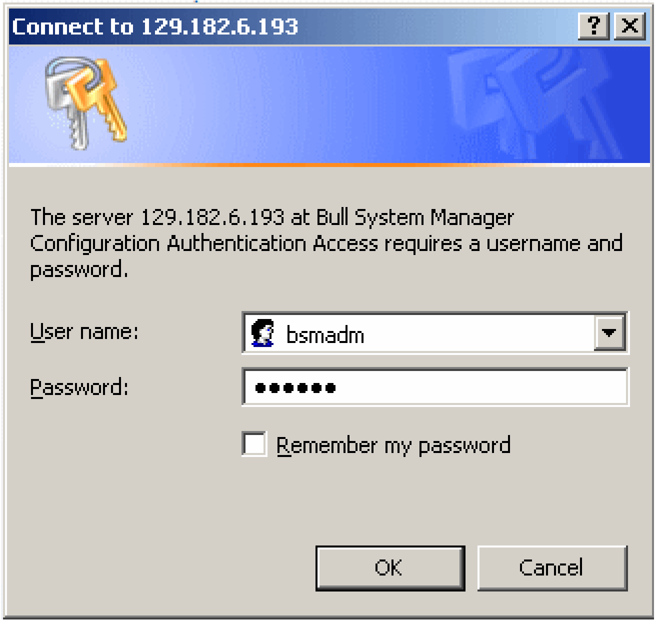
2.4.1 Starting the Configuration GUI

To start the Configuration GUI, you can either:

- From the Bull System Manager Console, click the icon representing the Configuration GUI in the Administration zone (top right).
- Or click the **Configuration** link on the Bull System Manager Home Page, URL: **http://<Bull System Manager server name>:<http_port>/BSM**.

Note The GUI runs with either Internet Explorer (V 6 or later) or Mozilla (V 1.5 or later).

When the GUI is launched, an authentication Window is displayed.



The server 129.182.6.193 at Bull System Manager Configuration Authentication Access requires a username and password.

User name: bsmadm

Password: ••••••

□ Remember my password

Figure 2-1. Authenticating the Bull System Manager configuration user

Authenticated users are specific Apache users (not system users). Users called **bsmadm** (password **bsmadm**), **nagios** (password **nagios**) and **guest** (password **guest**) are created when the Bull System Manager Server is installed.

Each user is associated with a Role: **Administrator** or **Operator**. The Administrator role has write access to the configuration; the Operator role has only read access.

bsmadm and **nagios** users are automatically declared as Bull System Manager **Administrator**. The **guest** user is automatically declared as a Bull System Manager **Operator**.

Note See *Configuring Users & Roles*, on page 195 for details.

Bull System Manager Configuration starts and displays the GUI home page as shown in the following figure:

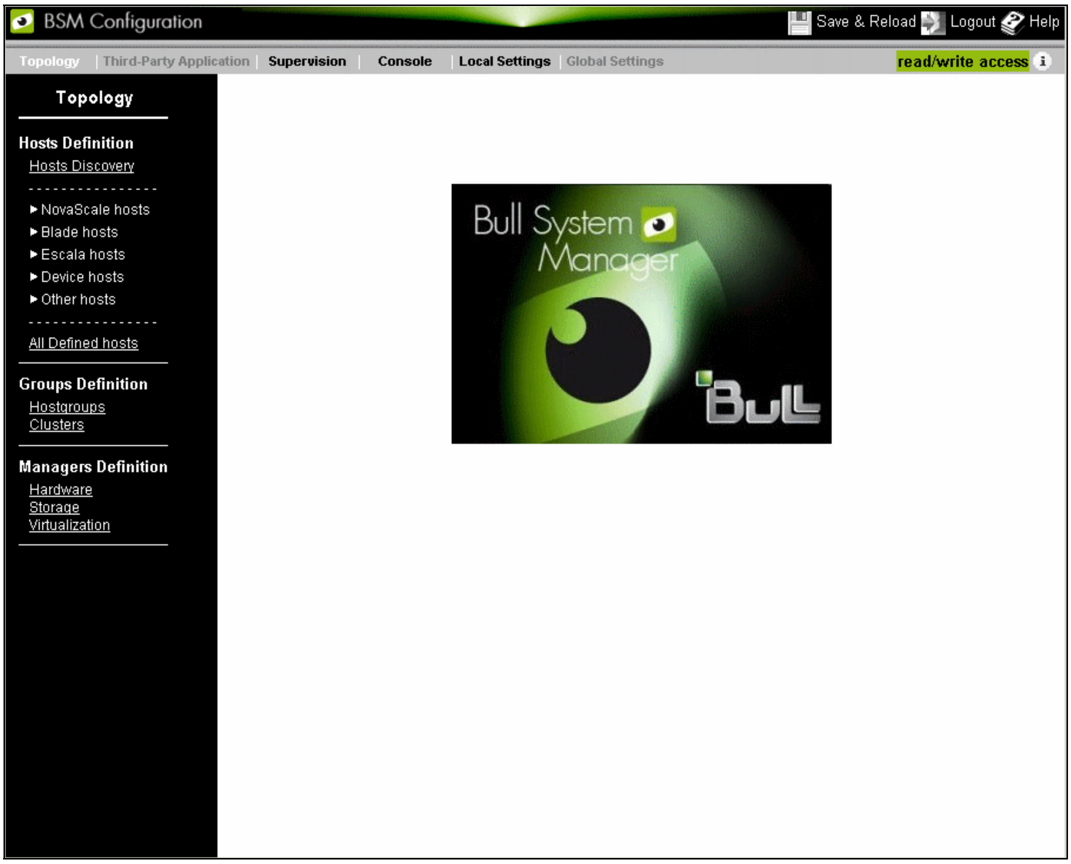


Figure 2-2. Bull System Manager Configuration home page

The **Title Bar** gives access to the following buttons and tabs:

Buttons

Help For access to generic help

Save & Reload To apply current modifications to the Bull System Manager server

Logout To exit from the BSM Configuration GUI

Tabs

Topology For topology configuration (hosts, hostgroups, etc.).

Third-Party Application For the customization of elements related to third party applications like JoNAs. This tab is available only if an application addOn is installed

Supervision For the configuration of supervision elements (services, notification, etc.)

Console For the customization of applications, views, maps, focus pane

LocalSettings For the configuration of features of the local BSM server and users

Global Settings For the configuration of features relative to the distributed solution. This tab is available only if the **NDOutils** server extension is installed.

WARNING:
Launching BSM Configuration GUI by typing the URL or using bookmarked URL is not supported.

2.4.2 Topology Configuration

Select the **Topology tab**. Figure 2-2 is displayed.

To view the **Host Definition** submenu level, click the corresponding item to expand it. The following screen appears:

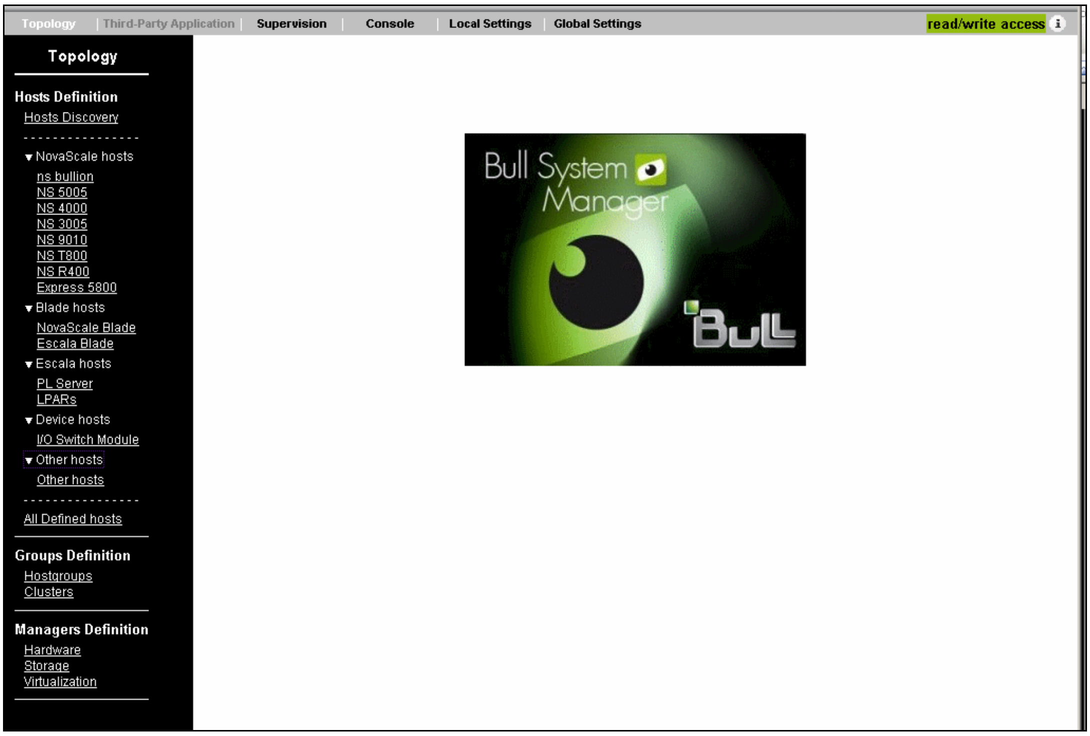


Figure 2-3. Bull System Manager Topology Host Definition submenu

The **Menu Bar** gives access to the following functions:

Hosts Definition To configure Hosts

Groups Definition To configure Hostgroups and Clusters

Managers Definition To configure Hardware, Storage or Virtualization managers

2.4.3 Third-Party Application Configuration

This tab is available only if Add-ons are installed.

2.4.4 Supervision Configuration

Select the **Supervision** tab. The following screen appears:

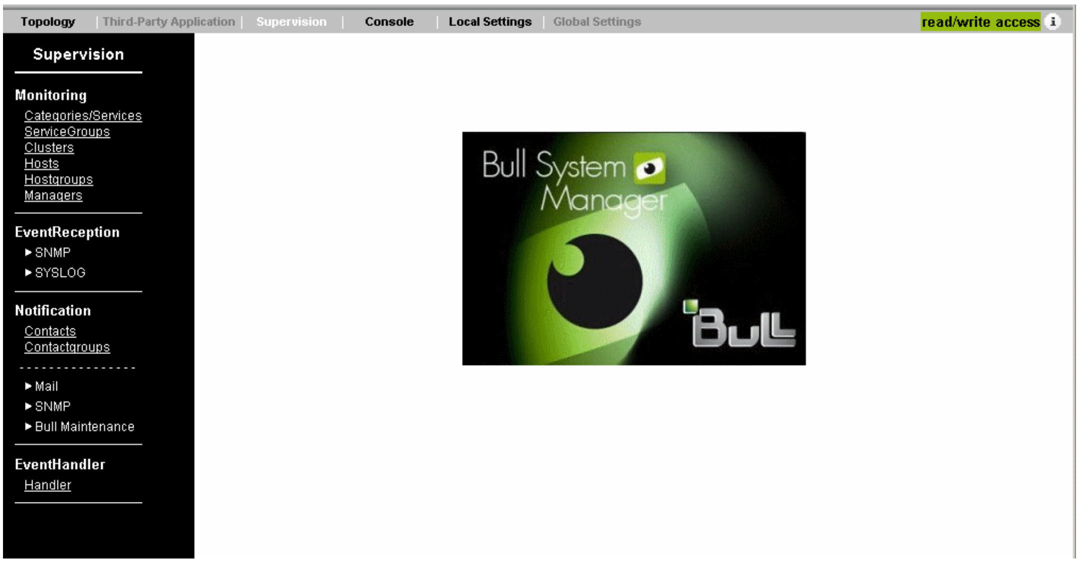


Figure 2-4. Bull System Manager Supervision configuration

The **Menu Bar** gives access to the following functions:

Monitoring To customize categories, services and topology element supervision features (notification, etc).

EventReception To configure the event reception mechanism (SNMP mibs integration, SNMP Trap receiver control).

Reporting To configure performance indicators (PNP4Nagios if the server extension is installed, MRTG if this tool is enabled).

Notification To configure contacts, contactgroups, Mail notifications, SNMP notifications to SNMP applications and autocall notifications for maintenance purposes.

EventHandler To configure the handler.

2.4.5 Console Customization

Select the **Console** tab. The following screen appears:

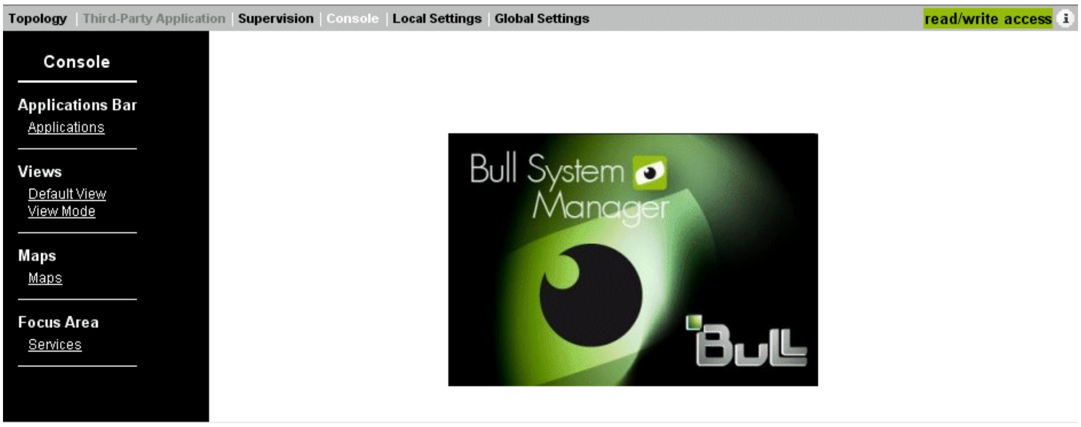


Figure 2-5. Bull System Manager Console customization home page

The **Menu Bar** gives access to the following functions:

Applications Bar To add applications to the left toolbar of the Console

Views To configure the default view and the view mode that is displayed when the Console is started

Maps To configure maps shown in the Bull System Manager Console

Focus Area To specify very important services displayed (with their status) in this area of the Bull System Manager Console

2.4.6 Local Settings Configuration

Select the **Local Settings** tab. The following display appears:

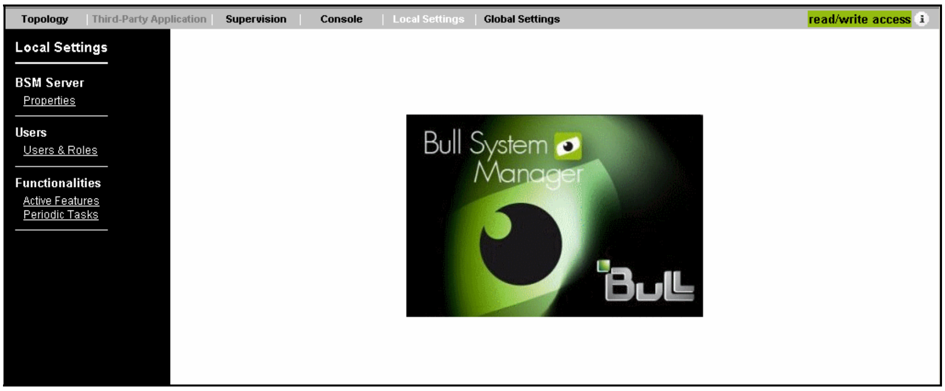


Figure 2-6. Bull System Manager LocalSettings configuration home page

The **Menu Bar** gives access to the following functions:

BSM Server To set BSM server properties used by agent part

Users To configure users and roles (user profiles)

Functionalities To configure BSM functional features

2.4.7 Global Settings

Select the Global Settings tab. The following display appears:

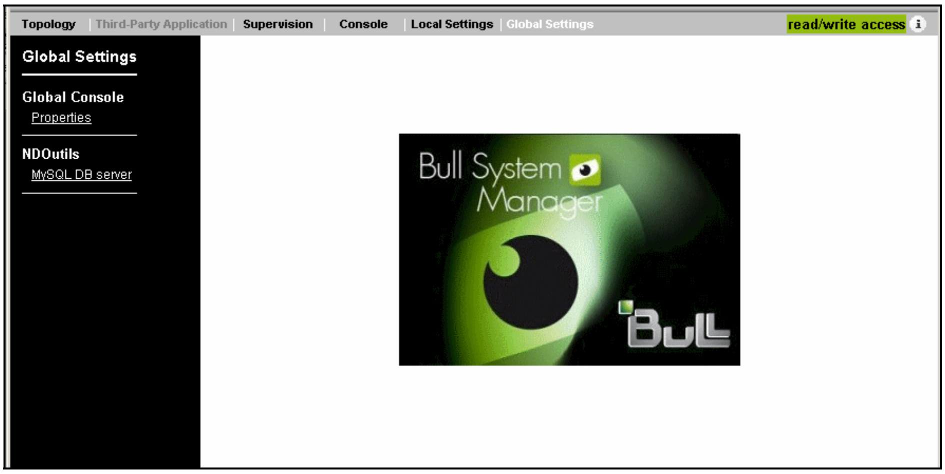


Figure 2-7. Bull System Manager Global Settings configuration home page.

The **Menu bar** gives access to the following functions:

Global Console To set the port number of the global console

NDOutils To set the properties of the server hosting the common **NDOutils** database

Note **Global Setting** domain is available only if the NDOUtils server extension is installed.

2.5 Concurrent Access to the Configuration GUI

Configuration item sharing is based on **read/write access** and **read only access** rules. When the GUI is launched, a test is performed to establish whether you are the first user or not. If you are the first user, you have **read/write access** to the configuration. This means that you will be able to read and modify the configuration details and all buttons are enabled. This status is indicated by a **read/write access** message on the screen and access to the **Save & Reload** in the **Title Bar**.

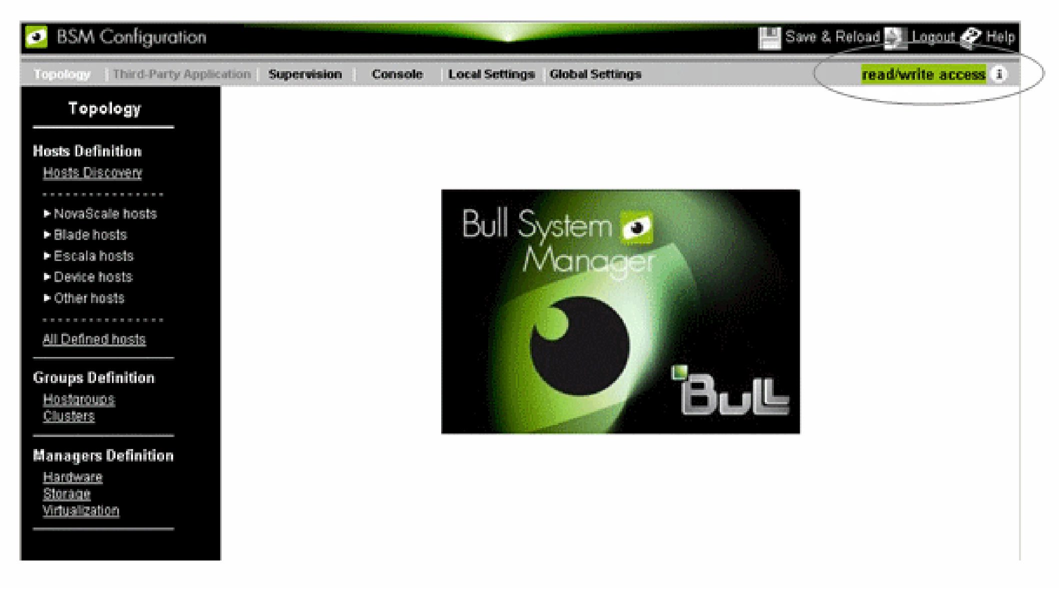
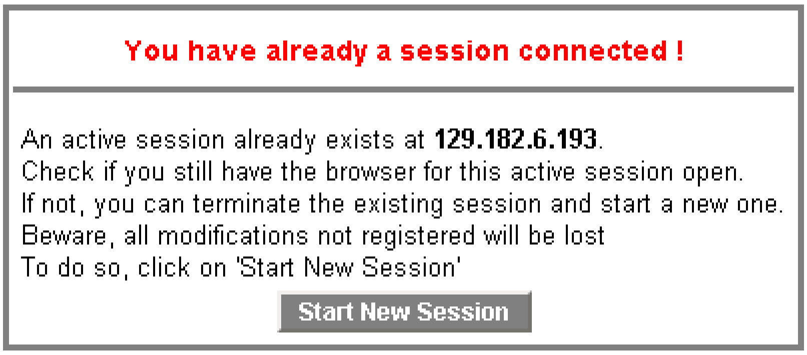


Figure 2-8. GUI with **read/write access**

If your previous session has not been deleted, a message is displayed as shown in the example below:



You have already a session connected !

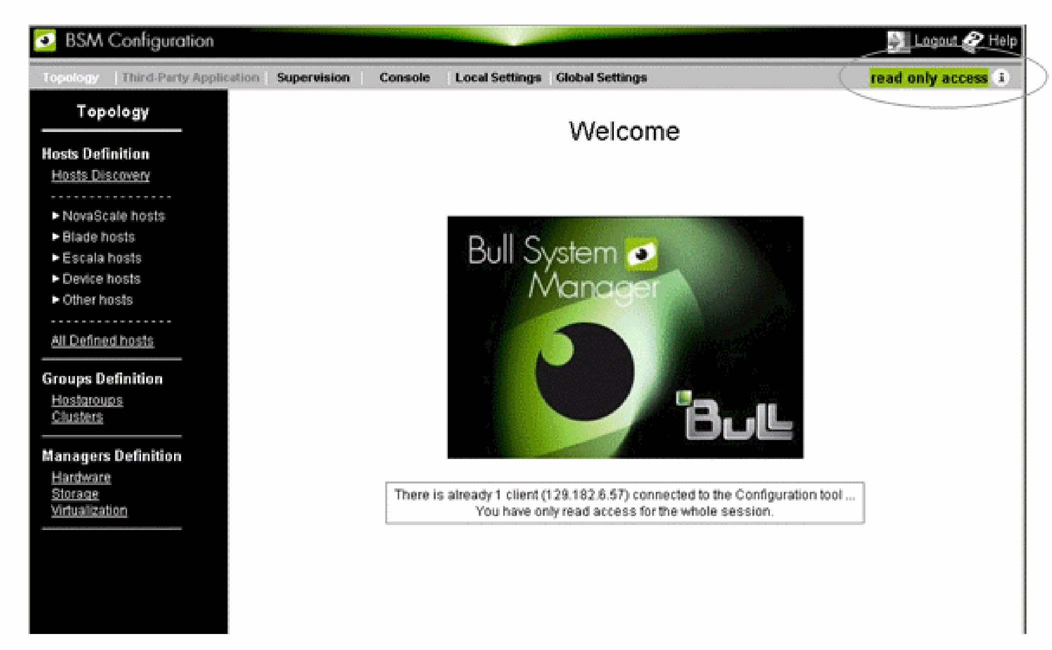
An active session already exists at **129.182.6.193**.
Check if you still have the browser for this active session open.
If not, you can terminate the existing session and start a new one.
Beware, all modifications not registered will be lost
To do so, click on 'Start New Session'

Figure 2-9. Session message

You can remove the previous session and start a new session by clicking the **Start New Session** button, else exit from the browser.

Important:

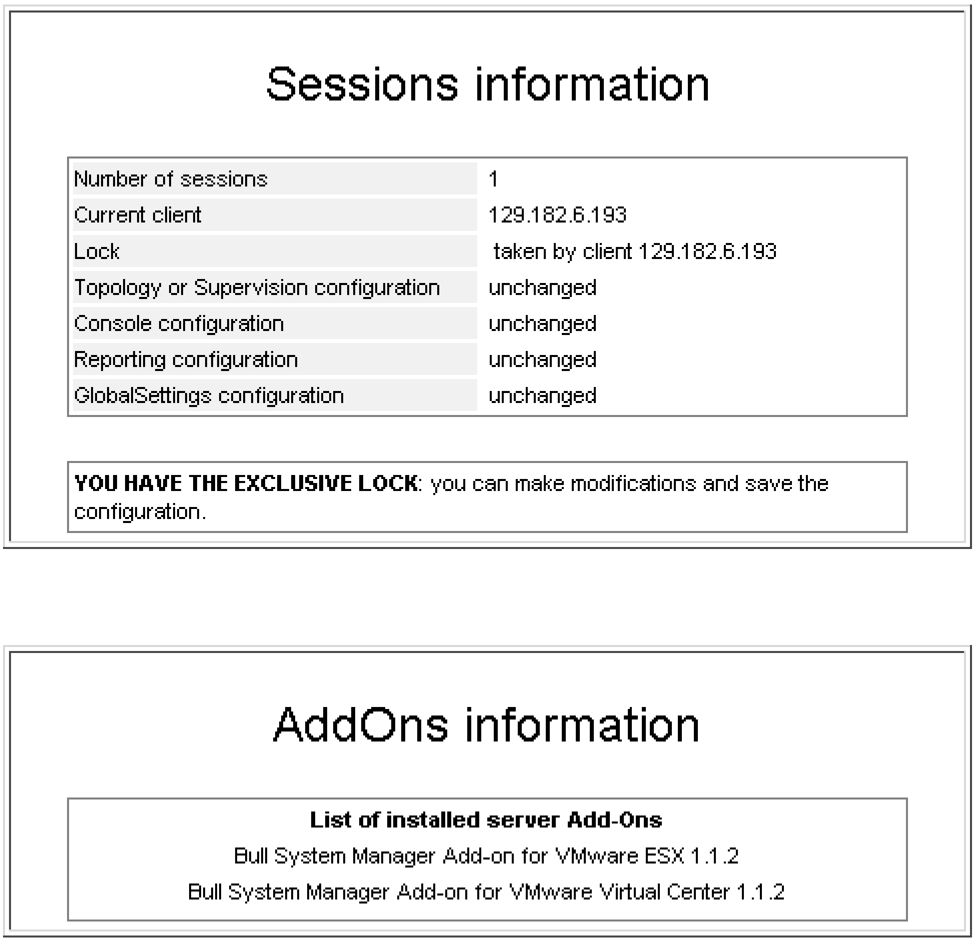
If you are not the first user to launch the GUI, a message indicates that another user is connected (the message gives the user’s IP address) and you have read only access to the configuration. This means that you can only read the configuration, and all editable buttons are disabled. (Note that it is also the case, if you using an Operator role). This status is indicated by a read only access message on the screen and no access to the Save & Reload button.



There is already 1 client (129.182.6.57) connected to the Configuration tool ...
You have only read access for the whole session.

Figure 2-10. GUI with **read only access**

Click the i icon to display information about currently active sessions.



Sessions information

Number of sessions	1
Current client	129.182.6.193
Lock	taken by client 129.182.6.193
Topology or Supervision configuration	unchanged
Console configuration	unchanged
Reporting configuration	unchanged
GlobalSettings configuration	unchanged

YOU HAVE THE EXCLUSIVE LOCK: you can make modifications and save the configuration.

AddOns information

List of installed server Add-Ons

Bull System Manager Add-on for VMware ESX 1.1.2

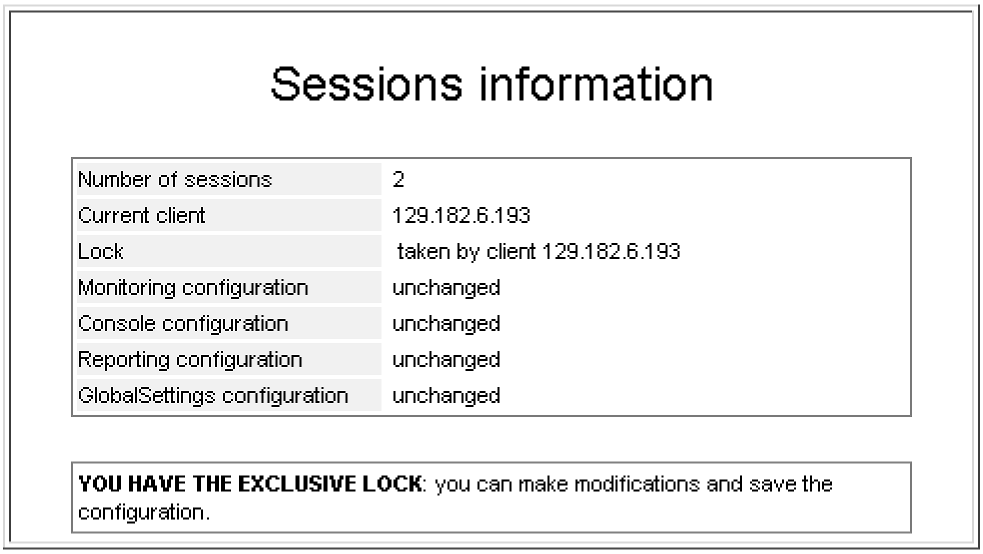
Bull System Manager Add-on for VMware Virtual Center 1.1.2

Figure 2-11. Sessions Information

The **Sessions information** page displays details about the active sessions and the current modifications. Modifications are organized in four domains (**Topology or Supervision**, **Console**, **Reporting** and **GlobalSetting**), however one domain modification can silently trigger a modification in a different domain. For instance, when you configure a complex server, reporting indicators can be automatically generated, activating the Reporting modification flag or change in the **BsmServer** properties that automatically updates the host, leading to a modification in the Topology.

Note **AddOn information** is listed below the **Sessions information**. To get detailed information about **BSM Server Add-ons,** refer to the *BSM Server Add-ons Installation and Administration Guide* (86 A2 59FA).

From the **Sessions information** window, if you have *read only access*, you can obtain read/write access by clicking the **Get Lock** button. After confirmation, you will be authorized to modify the Bull System Manager configuration while other clients will be restricted to read only access.



Sessions information

Number of sessions	2
Current client	129.182.6.193
Lock	taken by client 129.182.6.193
Monitoring configuration	unchanged
Console configuration	unchanged
Reporting configuration	unchanged
GlobalSettings configuration	unchanged

YOU HAVE THE EXCLUSIVE LOCK: you can make modifications and save the configuration.

Figure 2-12. Force Lock information

WARNING
This procedure must be used only when the previous read/write session cannot be closed by the normal procedure.

2.6 Main Configuration Steps

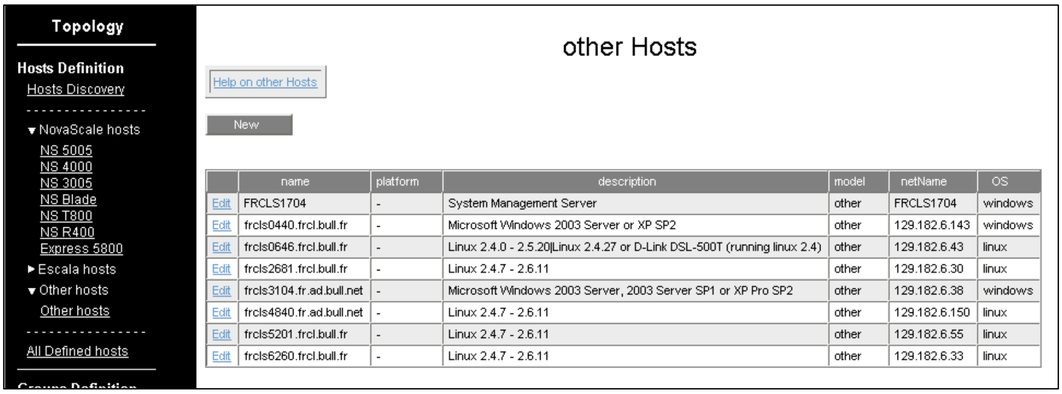
Perform the following steps to modify the default configuration:

1. Start the **BSM Configuration GUI** (see *Starting the Configuration GUI*, on page 11).
2. Select either **Topology**, **Third-Party Application**, **Supervision**, **Console, Local Settings** or **GlobalSettings** tab, according to configuration needs.
3. Click the type of resource you need to configure. Bull System Manager displays all the configured resources of this type.
4. **Create, edit** or **delete** the resources.
5. **Save** and **reload** the configuration on the Bull System Manager server part

This section continues by describing the **Create/Edit/Delete** and **Save & Reload** steps, which are common to all resources. Non-common steps are described in specific chapters.

2.6.1 Create / Edit / Delete Resources

When you click a link in the **Menu bar**, a new display appears, showing all resources of this type with their main properties. For example, when you click the **Other Hosts** link under the **Topology** tab, the following display appears:



other Hosts

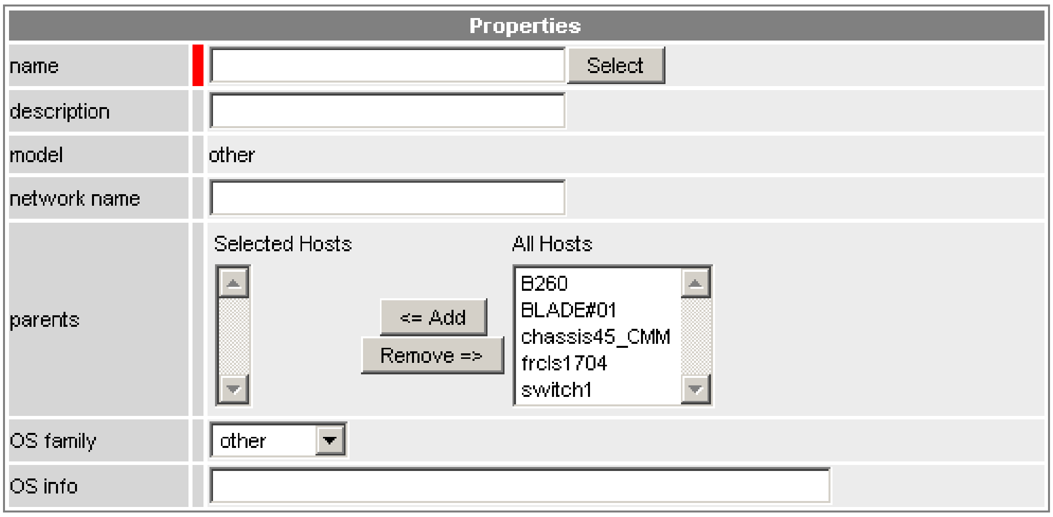
	name	platform	description	model	netName	OS
Edit	FRCLS1704	-	System Management Server	other	FRCLS1704	windows
Edit	frcls0440.frcl.bull.fr	-	Microsoft Windows 2003 Server or XP SP2	other	129.182.6.143	windows
Edit	frcls0646.frcl.bull.fr	-	Linux 2.4.0 - 2.5.20|Linux 2.4.27 or D-Link DSL-500T (running linux 2.4)	other	129.182.6.43	linux
Edit	frcls2681.frcl.bull.fr	-	Linux 2.4.7 - 2.6.11	other	129.182.6.30	linux
Edit	frcls3104.fr.ad.bull.net	-	Microsoft Windows 2003 Server, 2003 Server SP1 or XP Pro SP2	other	129.182.6.38	windows
Edit	frcls4840.fr.ad.bull.net	-	Linux 2.4.7 - 2.6.11	other	129.182.6.150	linux
Edit	frcls5201.frcl.bull.fr	-	Linux 2.4.7 - 2.6.11	other	129.182.6.55	linux
Edit	frcls6260.frcl.bull.fr	-	Linux 2.4.7 - 2.6.11	other	129.182.6.33	linux

Figure 2-13. Hosts page – (example)

For almost all resource types, with read / write access, you can:

- Create a new resource of the same type by clicking the **New** button.
- Edit or delete a resource using the **Edit** link.

When you click the **Edit** link, the following display appears with all the resource properties:



name	
description	
model	other
network name	
parents	All Hosts: B260 BLADE#01 chassis45_CMM frcls1704 switch1
OS family	other
OS info	

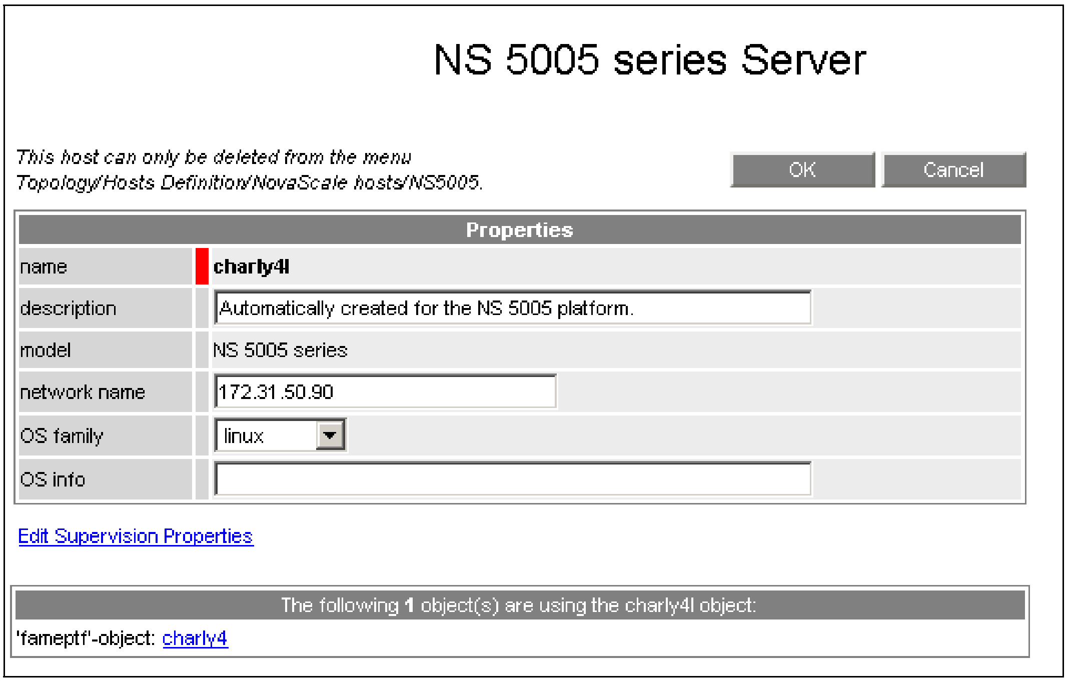
Figure 2-14. Host properties - example

Mandatory properties are identified by a red mark.

Make the changes required, then:

- Click **OK** to validate your change.
- Or click **Cancel** to return to the resources page without changes.
- Or click **Delete** to remove the resource. This operation requires confirmation.

As described in *Chapter 1. Introduction*, system resources are linked. Links are displayed below the form edit, as shown in the following figure:



NS 5005 series Server

This host can only be deleted from the menu Topology/Hosts Definition/NovaScale hosts/NS5005.

Properties

name	🟥	**charly4l**
description		Automatically created for the NS 5005 platform.
model		NS 5005 series
network name		172.31.50.90
OS family		linux
OS info		

The following **1** object(s) are using the charly4l object:

'fameptf'-object: charly4

Figure 2-15. Object links

Notes
- A service defined for all hosts (hostList *) is not displayed in link part.
- An object with links cannot be deleted except if the link is to the platform concerned.
- Some modifications cannot be if linked to another object. For example, the OS of a host with a link to a specific Linux OS service cannot be modified.

2.6.2 Save and Reload

To check and validate the modifications made to the configuration, click **Save & Reload** in the **Title Bar**.

Note The **Save & Reload** operation can be called independently of the configuration context (**Topology** tab, **Supervisions** tab, etc.) and independently of configuration history (for example **Topology** changes then **Console** changes, or only **Topology** changes, or **Console** changes then **Supervision** changes, and so on.

The **Save & Reload** operation requires confirmation.
After confirmation, **Save & Reload** performs the following steps:

1. It verifies which part of the configuration has been modified in order to select the corresponding configuration actions.

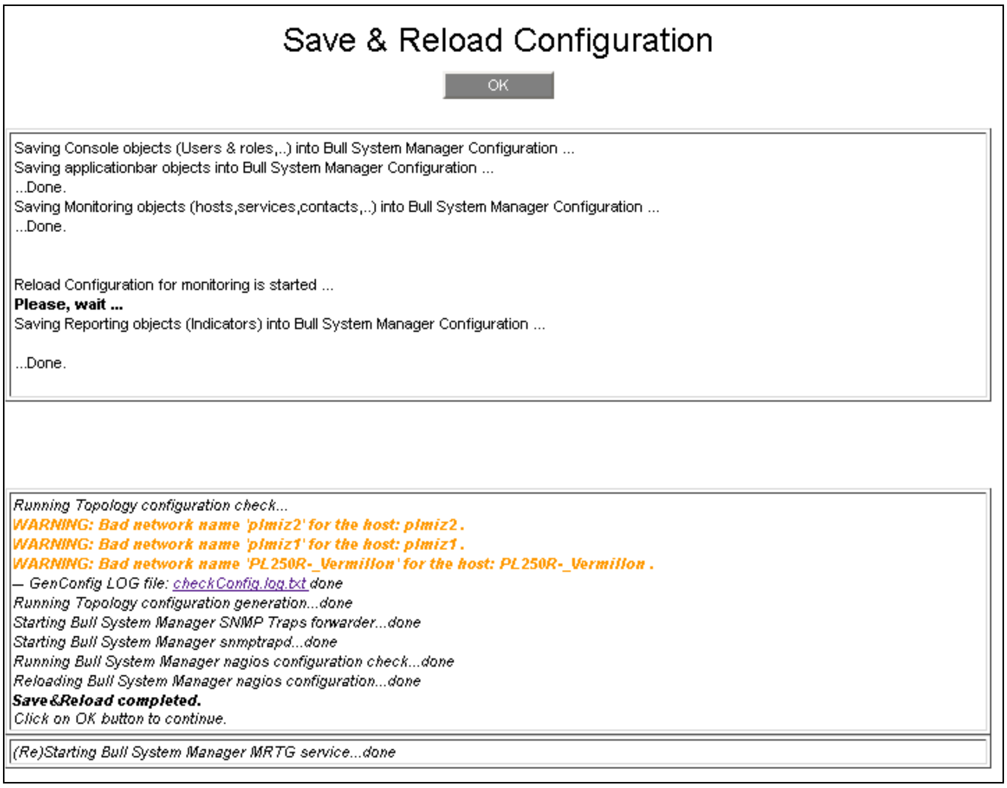
2. It saves the configuration in the files used by the Bull System Manager configuration. These files will be loaded in the next session for the Bull System Manager configuration.

3. It checks the consistency of the new configuration and generates the internal files used for the monitoring and/or reporting and/or the Console.

4. If required, it restarts the monitoring and/or the reporting processes, if no semantic error was found in the previous step.

Note Semantic warnings have consequences for the monitored element list (generally, an incorrectly configured element will be ignored) but they do not prevent the reload process for correctly configured elements.

The result for each step appears in a return window in the web page. Incorrect results for the semantic check phase appear in orange (warnings) and in red (errors), as shown in the following figure:



```
Saving Console objects (Users & roles,..) into Bull System Manager Configuration ...
Saving applicationbar objects into Bull System Manager Configuration ...
...Done.
Saving Monitoring objects (hosts,services,contacts,..) into Bull System Manager Configuration ...
...Done.


Reload Configuration for monitoring is started ...
Please, wait ...
Saving Reporting objects (Indicators) into Bull System Manager Configuration ...

...Done.
```

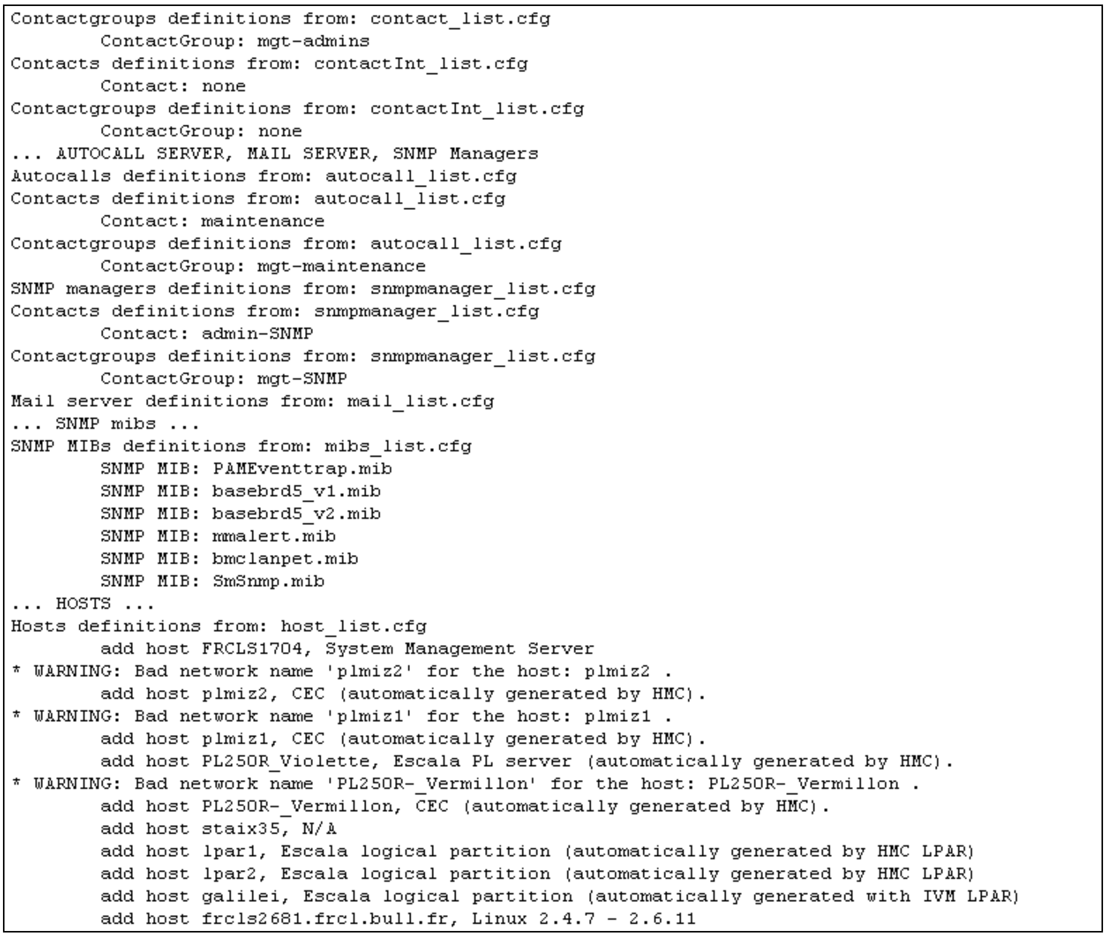
```
Running Topology configuration check...
WARNING: Bad network name 'plmiz2' for the host: plmiz2 .
WARNING: Bad network name 'plmiz1' for the host: plmiz1 .
WARNING: Bad network name 'PL250R-_Vermillon' for the host: PL250R-_Vermillon .
— GenConfig LOG file: checkConfig.log.txt done
Running Topology configuration generation...done
Starting Bull System Manager SNMP Traps forwarder...done
Starting Bull System Manager snmptrapd...done
Running Bull System Manager nagios configuration check...done
Reloading Bull System Manager nagios configuration...done
Save&Reload completed.
Click on OK button to continue.
```

```
(Re)Starting Bull System Manager MRTG service...done
```

Figure 2-16. Save & Reload Configuration report

To return to the home page, click **OK**.

To get details about semantic problems, click the checkConfig.log.txt link. A new display appears showing the checkConfig.log.txt textual file:

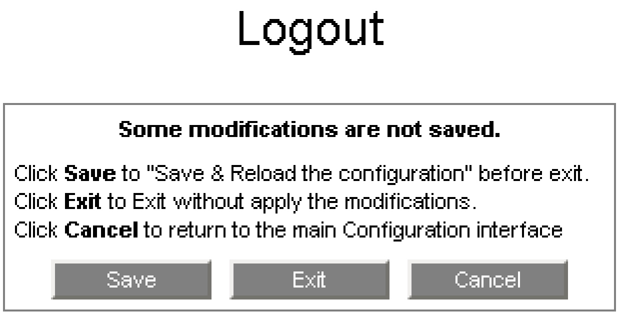


```
Contactgroups definitions from: contact_list.cfg
        ContactGroup: mgt-admins
Contacts definitions from: contactInt_list.cfg
        Contact: none
Contactgroups definitions from: contactInt_list.cfg
        ContactGroup: none
... AUTOCALL SERVER, MAIL SERVER, SNMP Managers
Autocalls definitions from: autocall_list.cfg
Contacts definitions from: autocall_list.cfg
        Contact: maintenance
Contactgroups definitions from: autocall_list.cfg
        ContactGroup: mgt-maintenance
SNMP managers definitions from: snmpmanager_list.cfg
Contacts definitions from: snmpmanager_list.cfg
        Contact: admin-SNMP
Contactgroups definitions from: snmpmanager_list.cfg
        ContactGroup: mgt-SNMP
Mail server definitions from: mail_list.cfg
... SNMP mibs ...
SNMP MIBs definitions from: mibs_list.cfg
        SNMP MIB: PAMEventtrap.mib
        SNMP MIB: basebrd5_v1.mib
        SNMP MIB: basebrd5_v2.mib
        SNMP MIB: mmalert.mib
        SNMP MIB: bmclanpet.mib
        SNMP MIB: SmSnmp.mib
... HOSTS ...
Hosts definitions from: host_list.cfg
        add host FRCLS1704, System Management Server
* WARNING: Bad network name 'plmiz2' for the host: plmiz2 .
        add host plmiz2, CEC (automatically generated by HMC).
* WARNING: Bad network name 'plmiz1' for the host: plmiz1 .
        add host plmiz1, CEC (automatically generated by HMC).
        add host PL250R_Violette, Escala PL server (automatically generated by HMC).
* WARNING: Bad network name 'PL250R-_Vermillon' for the host: PL250R-_Vermillon .
        add host PL250R-_Vermillon, CEC (automatically generated by HMC).
        add host staix35, N/A
        add host lpar1, Escala logical partition (automatically generated by HMC LPAR)
        add host lpar2, Escala logical partition (automatically generated by HMC LPAR)
        add host galilei, Escala logical partition (automatically generated with IVM LPAR)
        add host frcls2681.frcl.bull.fr, Linux 2.4.7 - 2.6.11
```

Figure 2-17. Save & Reload - Configuration detailed report

2.6.3 Logout

To logout from the **BSM** Configuration window, click the **logout** button. The logout action requires confirmation. If some modifications have not been saved, the following page is displayed:

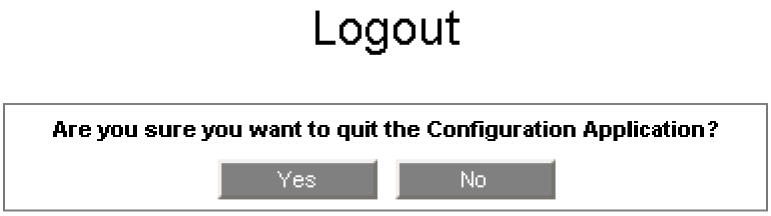

Logout

Some modifications are not saved.

Click **Save** to "Save & Reload the configuration" before exit.
Click **Exit** to Exit without apply the modifications.
Click **Cancel** to return to the main Configuration interface

Figure 2-18. Logout – Unsaved modifications

If all modifications have been saved, the following page is displayed:


Logout

Are you sure you want to quit the Configuration Application?

Figure 2-19. Logout – No modifications

Chapter 3. Configuring Topology

This chapter explains how to define **Hosts**, **Hostgroups** and **Managers** for a **Bull System Manager** configuration.

Notes

- The following characters are not supported in any text fields:

```
[] brackets,
= equal sign,
; semicolon
" commas
   space
```

- The following label names MUST be different from the following strings which are reserved keys or formats:

```
"*<string>",
"none",
"!<string>"
"auto"
"<string>_CMM"
"<string>_PAM"
"<string>_mgr"
"<string>_HNMaster"
```

(where <string> may be any string).

3.1 Configuring Hosts

The **Host** is the main resource monitored in the **Bull System Manager** application. From the **Bull System Manager** console **Hosts view**, all configured Hosts are displayed with their status.

At installation time, the host where Bull System Manager server is installed is configured as a host to be monitored. As Administrator, you must specify the other hosts to monitored.

Bull System Manager can monitor several host models:

- NovaScale Series server hosts (**NovaScale** menu)
- Blade server hosts (**Blade** menu)
- Escala server hosts (**Escala** menu)
- Storage system hosts (**StoreWay** menu)
- Device hosts (**Device** menu)
- Virtual system hosts (**Virtualization** menu)
- Other hosts (**Other hosts** menu).

Notes

- The **StoreWay** and **Virtualization** menus are available only if the corresponding Add-ons are installed. Host configuration for these specific hosts is not described here. Refer to the *Bull System Manager Server Add-ons Installation and Administrator's Guide* (86 A2 59FA).
- Additional models can be defined to allow supervision of server not covered by the BSM scope. You can contact Bull support to get the corresponding HowTo guide,

Host configuration, independently of NovaScale, Escala, Device, StoreWay or Virtualization models, can be performed either by using a **Discovery** mechanism or the **Other Hosts** link. Hosts configured this way are identified only by their OS and IP attributes.

Host configuration with a given model is performed by using the corresponding link in the NovaScale, Blade, Escala, Device, StoreWay or Virtualization menus. Hosts configured this way are also identified by their hardware, storage or virtualization attributes. Once a host is configured with a given model, its name and its model cannot be changed.

Note The configuration of supervision hosts is performed from the Supervision domain.

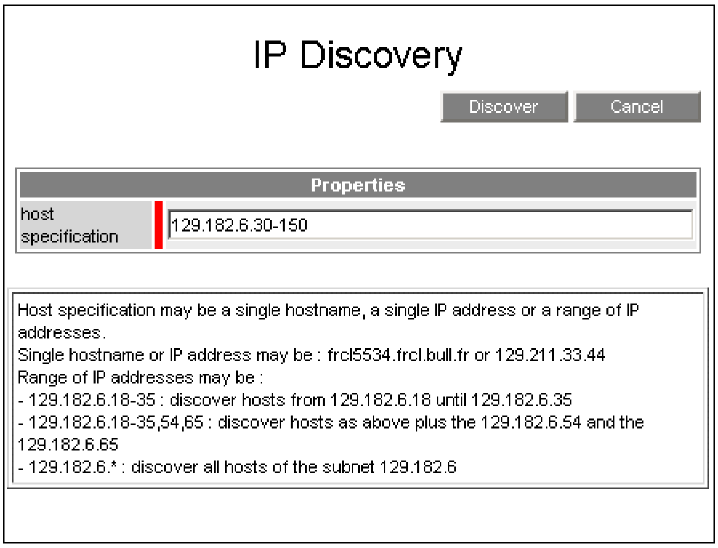
3.1.1 Using Host Discovery

If there are several hosts to be monitored, you can request the automatic discovery of subnet hosts.

Properties such as **name**, **OS info** and **OS family** are set automatically. If required, you can then set other host properties (**model**, **notification**) for certain hosts.

The host discovery mechanism is based on the **NMAP** Open Source product, which is a network exploration tool. When Bull System Manager Server is installed on a Windows server, NMAP software is provided. When Bull System Manager Server is installed on a Linux server, you must install the **NMAP RPM** from the distribution CDs.

Click the **Host Discovery** button to open the **Host Discovery** pane (Figure 3-1).

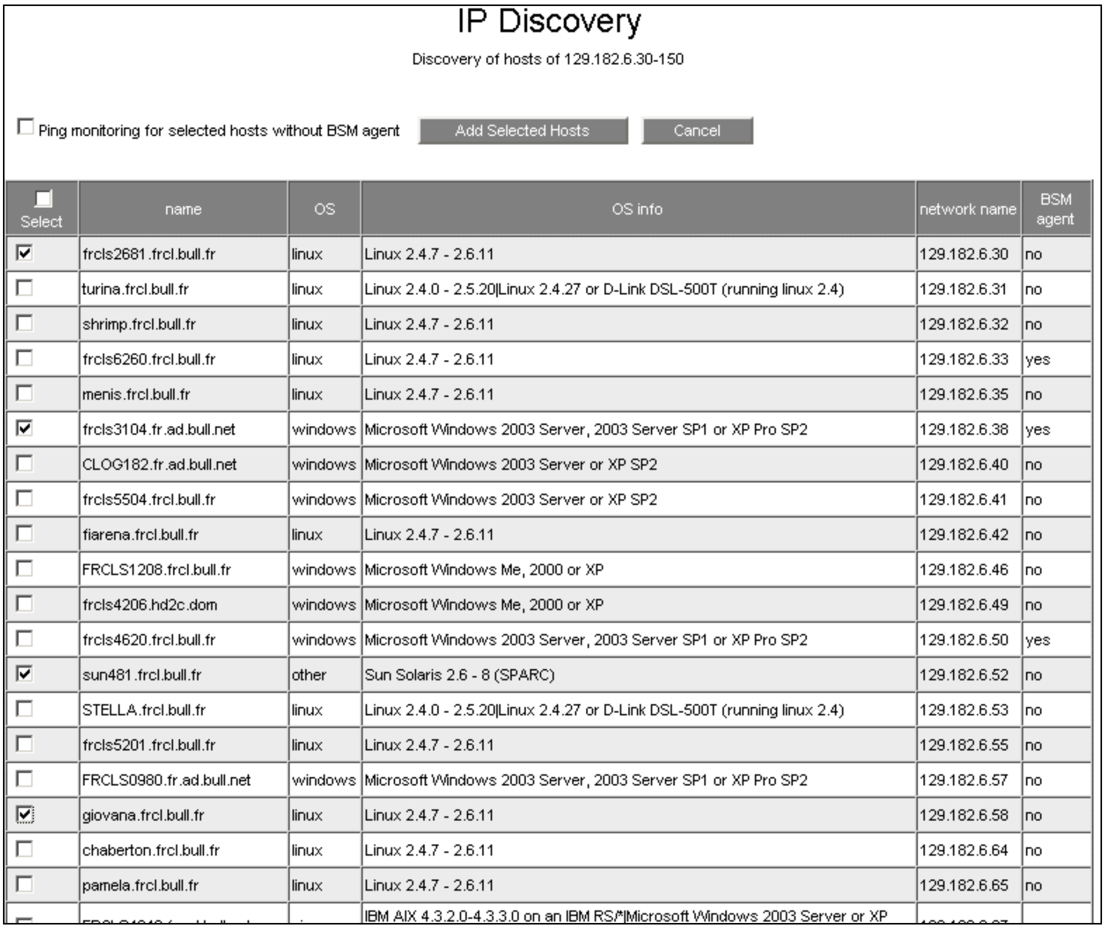


host specification: 129.182.6.30-150

Host specification may be a single hostname, a single IP address or a range of IP addresses.
Single hostname or IP address may be : frcl5534.frcl.bull.fr or 129.211.33.44
Range of IP addresses may be :
- 129.182.6.18-35 : discover hosts from 129.182.6.18 until 129.182.6.35
- 129.182.6.18-35,54,65 : discover hosts as above plus the 129.182.6.54 and the 129.182.6.65
- 129.182.6.* : discover all hosts of the subnet 129.182.6

Figure 3-1. Specification of hosts to be discovered

Set **host specification** properties, which can be a single **hostname**, a single **IP address** or a range of **IP addresses** as explained in the help displayed.
All hosts meeting the specification, which are up and for which **NMAP** has recognized the OS, are discovered and displayed (Figure 3-2). In addition, the discovery mechanism detects whether the Bull System Manager monitoring agent is running on each host.



Discovery of hosts of 129.182.6.30-150

□ Ping monitoring for selected hosts without BSM agent

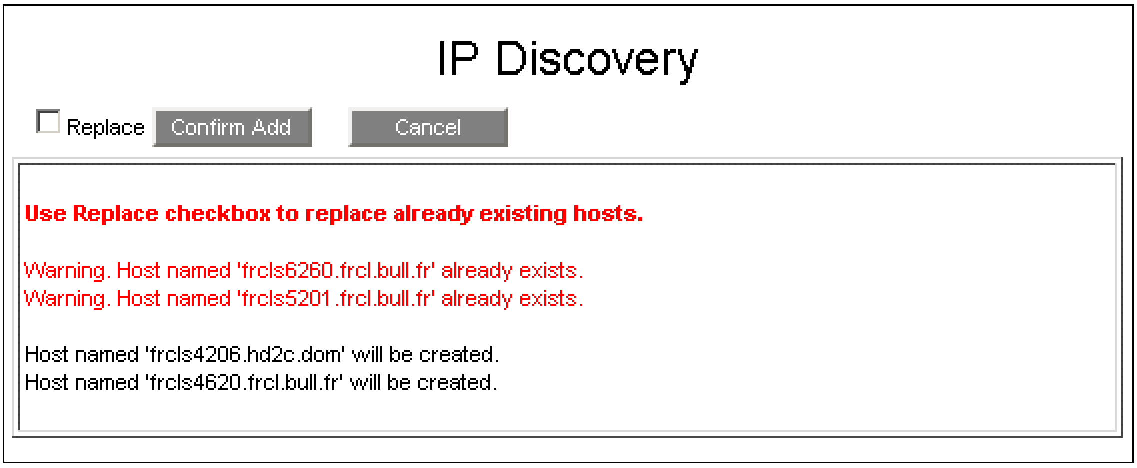
□ Select	name	OS	OS info	network name	BSM agent
☑	frcls2681.frcl.bull.fr	linux	Linux 2.4.7 - 2.6.11	129.182.6.30	no
□	turina.frcl.bull.fr	linux	Linux 2.4.0 - 2.5.20|Linux 2.4.27 or D-Link DSL-500T (running linux 2.4)	129.182.6.31	no
□	shrimp.frcl.bull.fr	linux	Linux 2.4.7 - 2.6.11	129.182.6.32	no
□	frcls6260.frcl.bull.fr	linux	Linux 2.4.7 - 2.6.11	129.182.6.33	yes
□	menis.frcl.bull.fr	linux	Linux 2.4.7 - 2.6.11	129.182.6.35	no
☑	frcls3104.fr.ad.bull.net	windows	Microsoft Windows 2003 Server, 2003 Server SP1 or XP Pro SP2	129.182.6.38	yes
□	CLOG182.fr.ad.bull.net	windows	Microsoft Windows 2003 Server or XP SP2	129.182.6.40	no
□	frcls5504.frcl.bull.fr	windows	Microsoft Windows 2003 Server or XP SP2	129.182.6.41	no
□	fiarena.frcl.bull.fr	linux	Linux 2.4.7 - 2.6.11	129.182.6.42	no
□	FRCLS1208.frcl.bull.fr	windows	Microsoft Windows Me, 2000 or XP	129.182.6.46	no
□	frcls4206.hd2c.dom	windows	Microsoft Windows Me, 2000 or XP	129.182.6.49	no
□	frcls4620.frcl.bull.fr	windows	Microsoft Windows 2003 Server, 2003 Server SP1 or XP Pro SP2	129.182.6.50	yes
☑	sun481.frcl.bull.fr	other	Sun Solaris 2.6 - 8 (SPARC)	129.182.6.52	no
□	STELLA.frcl.bull.fr	linux	Linux 2.4.0 - 2.5.20|Linux 2.4.27 or D-Link DSL-500T (running linux 2.4)	129.182.6.53	no
□	frcls5201.frcl.bull.fr	linux	Linux 2.4.7 - 2.6.11	129.182.6.55	no
□	FRCLS0980.fr.ad.bull.net	windows	Microsoft Windows 2003 Server, 2003 Server SP1 or XP Pro SP2	129.182.6.57	no
☑	giovana.frcl.bull.fr	linux	Linux 2.4.7 - 2.6.11	129.182.6.58	no
□	chaberton.frcl.bull.fr	linux	Linux 2.4.7 - 2.6.11	129.182.6.64	no
□	pamela.frcl.bull.fr	linux	Linux 2.4.7 - 2.6.11	129.182.6.65	no
□			IBM AIX 4.3.2.0-4.3.3.0 on an IBM RS/*|Microsoft Windows 2003 Server or XP		

Figure 3-2. Discovery result

Select all or some hosts to be monitored from the list. Then select **Ping monitoring for the selected hosts without BSM agent** option, if required. Finally, click **Add Selected Hosts**. A new screen appears (*Figure 3-3*).

Notes

- **Ping Monitoring option**
  By default, if a host OS is recognized (**Windows**, **AIX** or **Linux**), Bull System Manager monitors the OS aspects for this host (memory, CPU, logical disks or file systems) using a dialog with the Bull System Manager agent located on the host. If the Bull System Manager agent is not installed, OS monitoring does not work and an **UNKNOWN** status is generated for each corresponding service. When the **Ping monitoring** option is selected, only **ping** monitoring will be performed. OS monitoring will not be performed and Bull System Manager sets the OS to **any**.
- **Windows server**
  If the Configuration GUI is launched from the URL http://localhost;10080/BSM or http://127.0.0.1:10080/BSM/, **IP Discovery** returns no result.



Use Replace checkbox to replace already existing hosts.

Warning. Host named 'frcls6260.frcl.bull.fr' already exists.
Warning. Host named 'frcls5201.frcl.bull.fr' already exists.

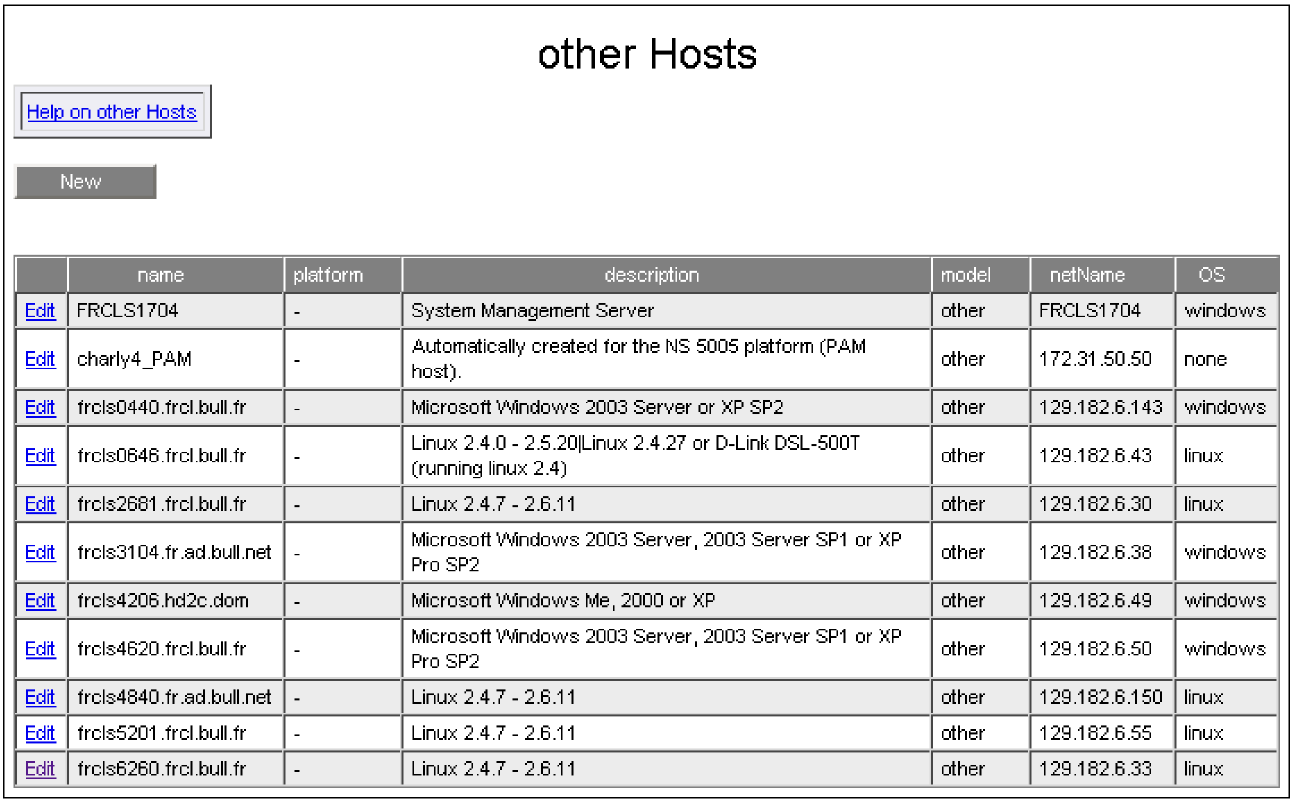
Host named 'frcls4206.hd2c.dom' will be created.
Host named 'frcls4620.frcl.bull.fr' will be created.

Figure 3-3. Replace and confirmation

Among the selected discovered hosts, some hosts may be new to the Bull System Manager configuration, while others may already exist. If the **Replace** option is checked, the discovered hosts replace the existing configured hosts.

In both cases, the newly discovered hosts are added to the Bull System Manager configuration when you click **Confirm Add**.

After **Confirm Add** is executed, the list of all configured hosts is displayed, showing the new hosts (Figure 3-4).



other Hosts

	name	platform	description	model	netName	OS
Edit	FRCLS1704	-	System Management Server	other	FRCLS1704	windows
Edit	charly4_PAM	-	Automatically created for the NS 5005 platform (PAM host).	other	172.31.50.50	none
Edit	frcls0440.frcl.bull.fr	-	Microsoft Windows 2003 Server or XP SP2	other	129.182.6.143	windows
Edit	frcls0646.frcl.bull.fr	-	Linux 2.4.0 - 2.5.20|Linux 2.4.27 or D-Link DSL-500T (running linux 2.4)	other	129.182.6.43	linux
Edit	frcls2681.frcl.bull.fr	-	Linux 2.4.7 - 2.6.11	other	129.182.6.30	linux
Edit	frcls3104.fr.ad.bull.net	-	Microsoft Windows 2003 Server, 2003 Server SP1 or XP Pro SP2	other	129.182.6.38	windows
Edit	frcls4206.hd2c.dom	-	Microsoft Windows Me, 2000 or XP	other	129.182.6.49	windows
Edit	frcls4620.frcl.bull.fr	-	Microsoft Windows 2003 Server, 2003 Server SP1 or XP Pro SP2	other	129.182.6.50	windows
Edit	frcls4840.fr.ad.bull.net	-	Linux 2.4.7 - 2.6.11	other	129.182.6.150	linux
Edit	frcls5201.frcl.bull.fr	-	Linux 2.4.7 - 2.6.11	other	129.182.6.55	linux
Edit	frcls6260.frcl.bull.fr	-	Linux 2.4.7 - 2.6.11	other	129.182.6.33	linux

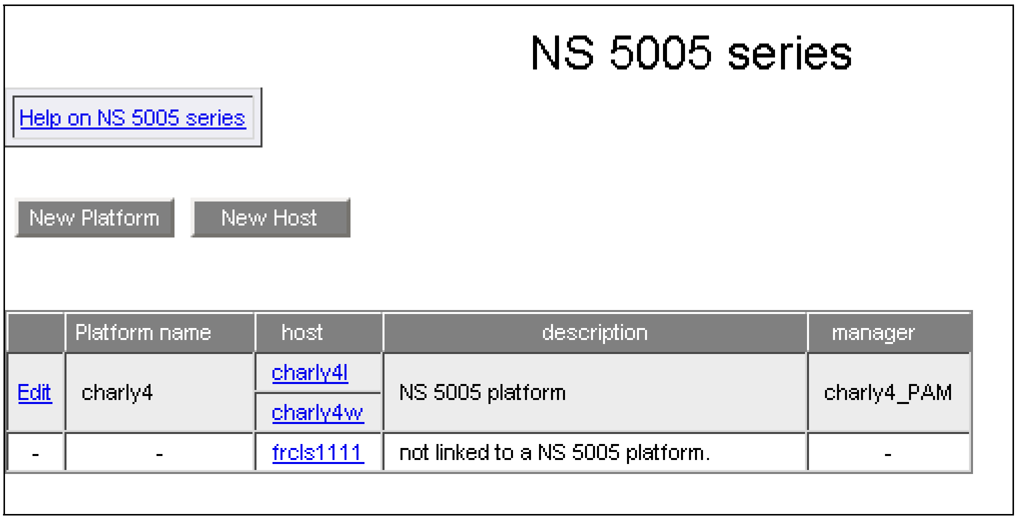
Figure 3-4. List of all hosts (old and new)

You can still set specific properties for some hosts if the default values are not satisfactory, using the **Edit** link for each host. To set model, use the corresponding link in the NovaScale, Blade, Escala, Device, StoreWay or Virtualization menus.

3.1.2 Defining NovaScale Hosts

3.1.2.1 NS NS5005&6000

NovaScale 5005 servers are usually housed in a module managed by the **Platform & Administration Manager (PAM)**.
To configure NovaScale 5005 hosts, expand the NovaScale menu under Host Definition and select the NovaScale 5005 & 6000 items. The following page will be displayed:



NS 5005 series

Help on NS 5005 series

	Platform name	host	description	manager
Edit	charly4	charly4l charly4w	NS 5005 platform	charly4_PAM
-	-	frcls1111	not linked to a NS 5005 platform.	-

Figure 3-5. NovaScale NS5005 Servers main page

To configure a standalone **NovaScale NS5005 host**, click the **New Host** button. This action results in the display of an editable window similar to that for the **Other Hosts**.

To configure a **NovaScale NS5005** platform, click the **New Platform** button.

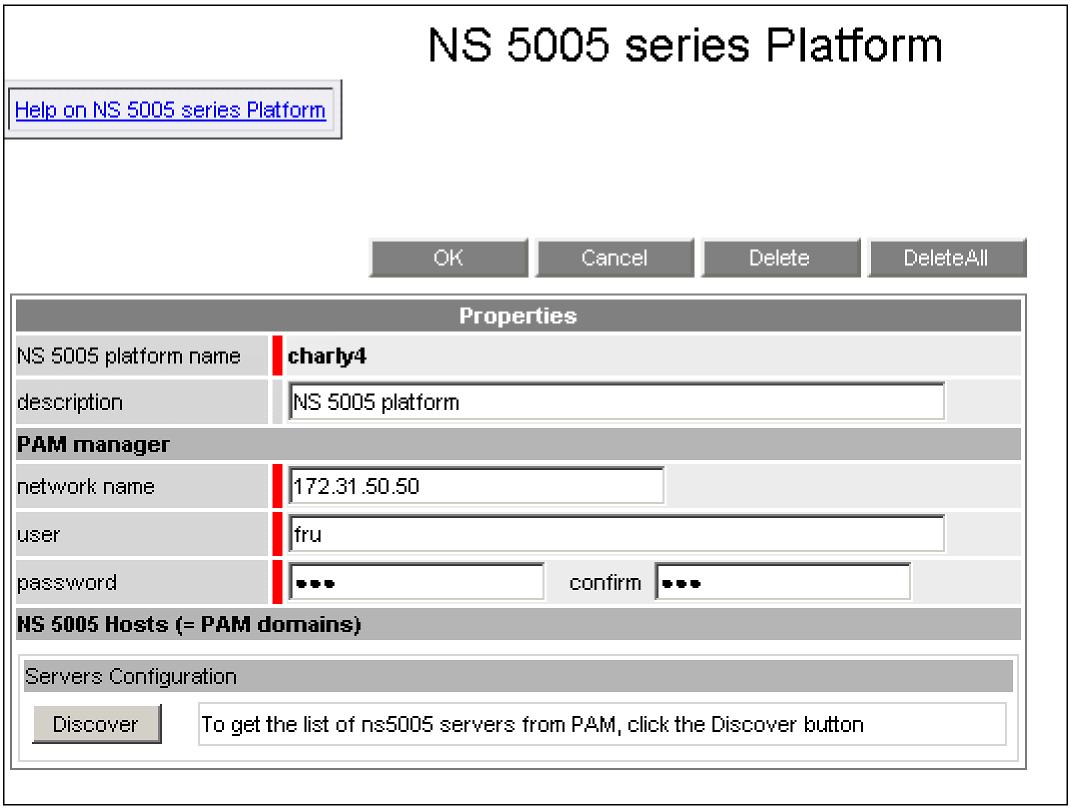
To modify or delete a NovaScale NS5005 platform, click the **Edit** link.

To modify or delete a standalone NovaScale NS5005 platform, click the corresponding link in the **Host** column.

mportant:
A NS 5005 Server linked to a platform cannot be deleted. You must remove it from the platform by editing the NS 5005 Platform object and then, remove the corresponding host.

NS 5005 Platform Edition

The following window is used to change the settings for a NS 5005 platform:



NS 5005 series Platform

Properties			
NS 5005 platform name	charly4		
description	NS 5005 platform		
PAM manager			
network name	172.31.50.50		
user	fru		
password	•••	confirm	•••
NS 5005 Hosts (= PAM domains)			

Servers Configuration

To get the list of ns5005 servers from PAM, click the Discover button

Figure 3-6. NS 5005 platform

mportant:

You can define only one platform for each PAM manager generated. If you define several platforms using the same PAM tool, BSM will generate one PAM manager object per platform. It will create a redundancy for PAM GlobalStatus monitoring.

Platform Information

NS 5005 platform name
The label used to identify the platform in **Bull System Manager**, `ns5005ptf` in the example.

Note:

It is advised to use the **Central Subsystem** name, as defined in the **PAM** tool that contains the corresponding domains. Elsewhere, if needed, this defined platform name may contain a set of defined domains that do not correspond to a single PAM Central Subsystem, but are managed by the same PAM manager.

description
A phrase describing the platform, `NS 5005 platform` in the example above.

PAM Manager

network name — IP address used to access the PAM, `172.31.50.60` in the example.
Note:
If **Bull System Manager** is installed on the same server as the **PAM** manager, the PAM manager network name must be the local default IP address. It may be the private **PAP-PMB** communication address and not the public IP address.

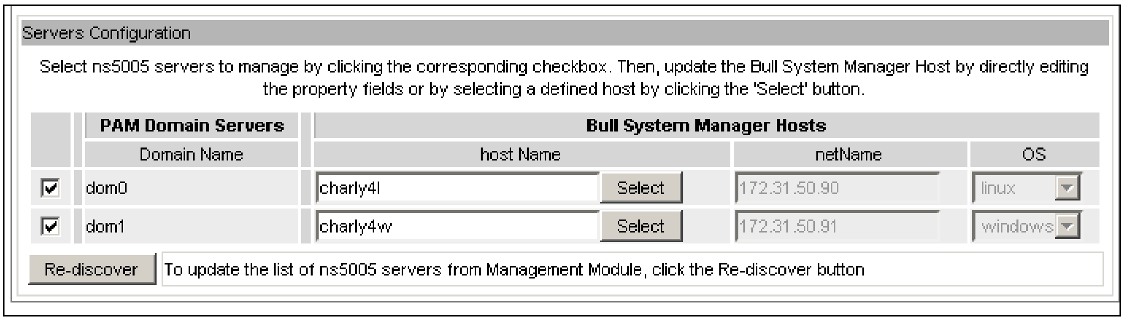
user — Authentication login used by Bull System Manager to access the manager.

password — Authentication password used by Bull System Manager to access the manager.

NS 5005 Hosts

Lists the servers to be managed by **Bull System Manager**.
At platform creation, this part of the window is not displayed. An initial discovery request to the PAM application must be performed to get the list of servers in the platform. Click the **Discover** button to get the list of domains configured for the **NS 5005** Platform.

The following figure shows an NS 5005 platform with two domains:



Servers Configuration

Select ns5005 servers to manage by clicking the corresponding checkbox. Then, update the Bull System Manager Host by directly editing the property fields or by selecting a defined host by clicking the 'Select' button.

	PAM Domain Servers	Bull System Manager Hosts			
	Domain Name	host Name		netName	OS
☑	dom0	charly4l	Select	172.31.50.90	linux
☑	dom1	charly4w	Select	172.31.50.91	windows

Re-discover — To update the list of ns5005 servers from Management Module, click the Re-discover button

Figure 3-7. NS 5005 domains

- The left column allows you to select the domain corresponding to the server defined for the monitored platform. Only configured domains are displayed for consistency with the PAM configuration.
- The central part displays the **Domain Server** configuration as defined in the PAM.

Note Domain Server configuration as defined in the PAM cannot be modified.

- The right column allows you to edit the main properties (name, network name and OS) of the corresponding host. The host can be edited only if the corresponding domain is checked. You can select an already defined host ("other" model or NS 5005 model) by clicking the check box or you can create a host by completing the corresponding field. By default, **Name** and **netName** are set with the ident of the server domain.
If the PAM application is not accessible, two domains are represented without the PAM information and the ident of the domain is set to `domain` suffixed with the domain number. You can select any domain and change the **NS Master Hosts** properties.

Note It is possible to create a platform that does not contain a server.

Once a platform has been created, the Domain Servers part displays the platform topology as registered in **Bull System Manager**. You can only change the **BSM** Host configuration of a previously selected domain. To add a new domain in your configuration, you must perform a **Re-discover** step.

A domain that is not referenced in the current NS Master or that differs from PAM is displayed in orange and is editable.

A domain that is no longer referenced in PAM is displayed in red and is not editable.

Note The **NS 5005 Platform** concept was introduced with **NovaScale Master 5.1** version. The migration process tries to build this object with the previous Bull System Manager configuration (platform and manager) retrieved from PAM. If the application cannot be accessed during migration, the domains are associated with the first domains. When you edit the object and perform a **Re-discover**, there may be a conflict between the NovaScale configuration and the **PAM** configuration.

After editing:

- Click the **OK** button to validate changes
- Or click the **Cancel** button to return to the NS 5005 Servers page without any changes.

When the Topology is modified, confirmation is required. A page is displayed listing all the changes to be applied. If you do not agree, click the **NO** button to return to the NS5005 platform page, otherwise click the **YES** button to add the NovaScale Blade chassis with its properties.

Related N5005 Platform Objects

The following table describes the property details generated when a **NS 5005** platform is created.

Property	Description
ns5005 host	As defined in the **PAM** configuration part of the window.
PAM host	Host representing the PAM, named as <platformName>_PAM **Note:** If the platform was defined in a previous NovaScale Master version, the name used is kept (same as the Manager name, or the Manager name with _mgr suffix).
hostgroup	hostgroup representing the physical platform, named <platformName>.
PAM Manager	Hardware manager representing the PAM, named <platformName>_PAM. **Note:** If the platform was defined in a previous NovaScale Master

Property	Description
	version, the name used is kept.
Categories and services	The **PAM** category and related services are instantiated for the PAM host. The Hardware category and related services are instantiated for each NS 5005 host.

Deleting a NS 5005 Platform

They are two ways to delete a **NS 5005** platform:

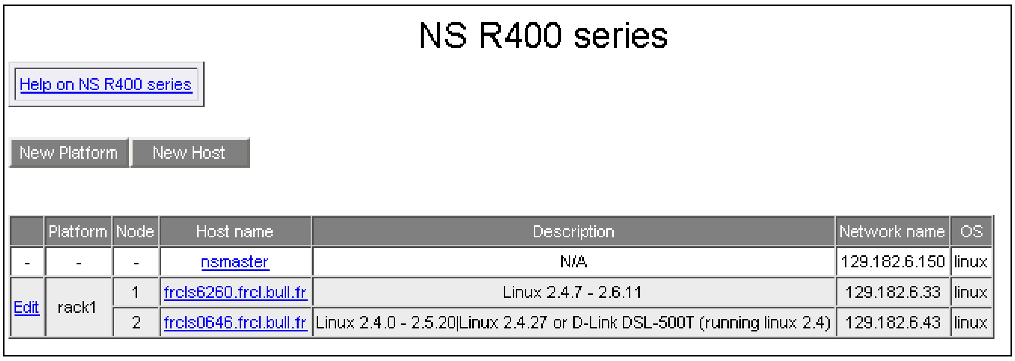
- Click the **Delete** button to delete the platform while keeping the NS 5005 server category.

  The hostgroup, manager (if not linked to another NS5005 platform) and related services are deleted but the NS 5005 server category remains.
- Or click the **DeleteAll** button to delete the platform and all linked NS 5005 servers.

3.1.2.2 NS R400

Nova Scale R400 series servers are rack-optimized servers and are used as front-end/ application servers in space constrained environments. The NovaScale R422 features an innovative design that includes two servers in a single 1U chassis.

To configure a NS R400, click the **NS R400** menu. A list of the existing R400 configured servers is displayed. To define a new R400, click the **New Platform** button for a R422 server, otherwise click the **New Host** button

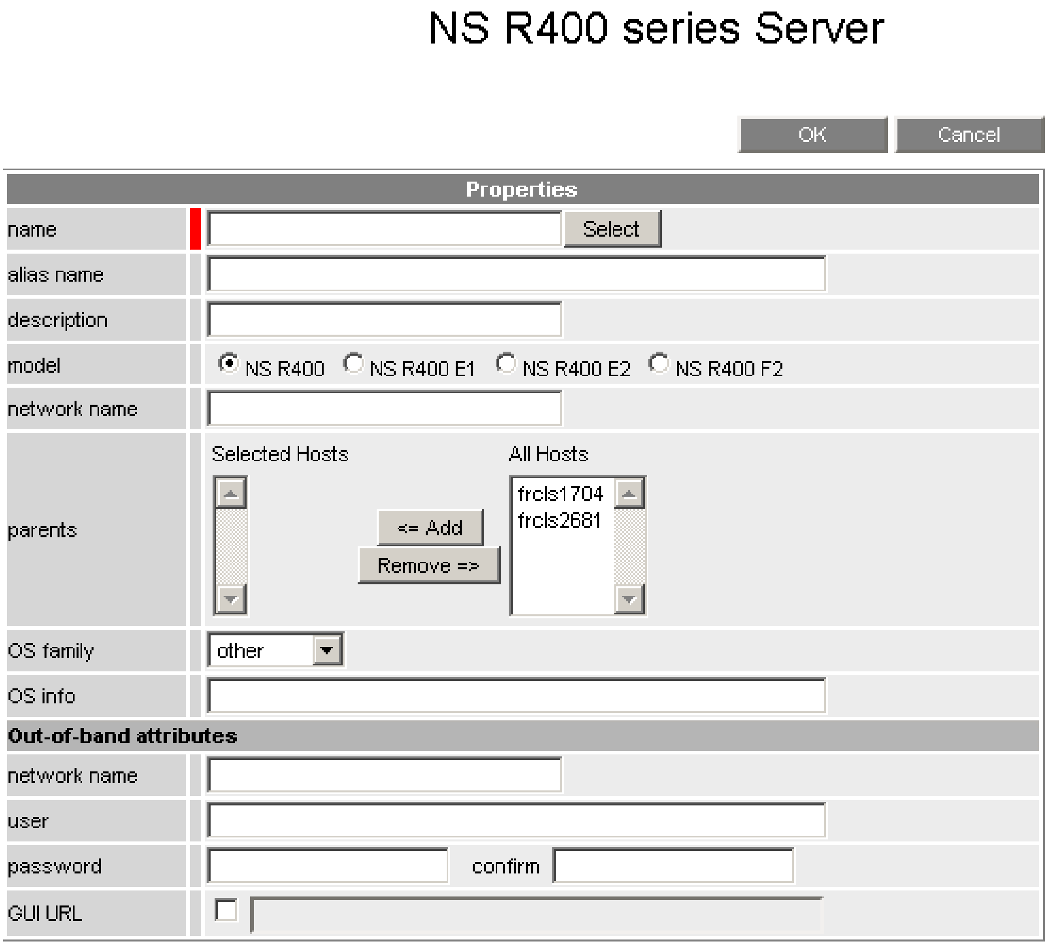


	Platform	Node	Host name	Description	Network name	OS
-	-	-	nsmaster	N/A	129.182.6.150	linux
Edit	rack1	1	frcls6260.frcl.bull.fr	Linux 2.4.7 - 2.6.11	129.182.6.33	linux
		2	frcls0646.frcl.bull.fr	Linux 2.4.0 - 2.5.20|Linux 2.4.27 or D-Link DSL-500T (running linux 2.4)	129.182.6.43	linux

Figure 3-8. NS R400 hosts

NS R400 Edition

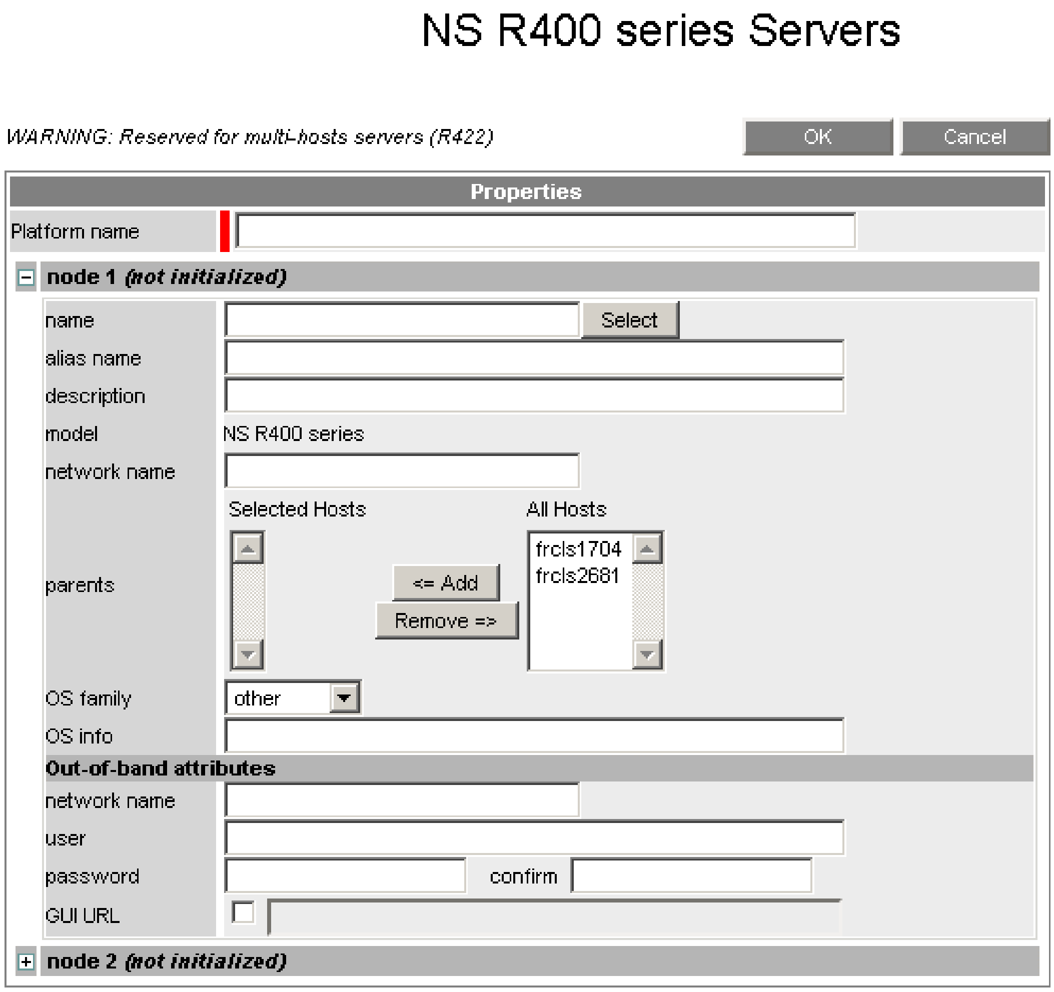
The following windows are used to define a NS R400.



NS R400 series Server

Properties	
name	
alias name	
description	
model	● NS R400 ○ NS R400 E1 ○ NS R400 E2 ○ NS R400 F2
network name	
parents	Selected Hosts All Hosts: frcls1704, frcls2681
OS family	other
OS info	
Out-of-band attributes	
network name	
user	
password	confirm
GUI URL	□

Figure 3-9. NS R400 host edition



NS R400 series Servers

WARNING: Reserved for multi-hosts servers (R422)

OK | Cancel

Properties

Platform name

node 1 *(not initialized)*

name | Select

alias name

description

model: NS R400 series

network name

parents: Selected Hosts | <= Add | Remove => | All Hosts: frcls1704, frcls2681

OS family: other

OS info

Out-of-band attributes

network name

user

password | confirm

GUI URL ☐

node 2 *(not initialized)*

Figure 3-10. NS R422 edition

Host Properties	Description
Platform name	Platform name (only for NS R422 model).
name	Host short name (label). This name is the one displayed in the Bull System Manager console. Generally, this label is the host name. **Note:** In the configuration, the host name MUST be different from the following reserved keys: "*", "none" and "auto". The host may be selected from the hosts defined without a model (discovered by Discovery or created from the **Other hosts** menu).
alias name	Host alias name. This field allows to associate an additional name to the host. (Reserved for future use)
description	Description of the host. This description is displayed in an info tip in the Management Tree when you move the cursor over the node associated with this host.
model	Model of the host. You can be more specific by choosing a sub-model from NS R400, NS R400 E1, NS R400 E2 or NS R400 F2.

Host Properties	Description
network name	Host network name (hostname or IP address). Default value: host name (label).
parents	List of hosts that link the host with remote hosts. For instance, a host representing a network equipment item (router, switch, etc.) is typically a parent host.
OS family	Operating System type (Windows, Linux, AIX, none, other). Other OS can be supported if the corresponding Add-on is installed. Default value: **other**.
OS info	When a host is discovered by **Discovery**, certain properties are set automatically. This is the case of **OS info**, which gives information about the OS running on the host. **description**, if empty, is automatically set to the same value as **OS info**.
Out-of-band attributes	Description
network name	Out-of-band platform management card address.
user, password	Authentication information (login, password) used by Bull System Manager to access the management card.
GUI URL	Hardware management application URL

Table 3-1. NS R400 menu

- To manage **NovaScale R400** series servers using out-of-band over LAN, the **Baseboard Management Controller** (**BMC**) for these servers needs to be configured as present on the **RMC** card. Refer to your Bull Contact.

Related NS R400 Properties

The following table describes the property details generated during the creation of a NS R400 platform.

Type	Description
hostgroup	If the model is R422, a hostgroup representing the physical platform is created.
categories and services	The Hardware category and related services are instantiated for each NS R400 host if the Out-Of-Band attributes are configured. The Power category and related services are instantiated for the host if the Out-Of-Band attributes are configured.

Table 3-2. NS R400 objects

3.1.2.3 ns bullion, NS 3005, NS 4000, NS 9010, NS T800 and Express 5800

To configure **ns bullion, NS 3005, NS 4000, NS 9010, NS T800** or an **Express 5800** server, select the corresponding menu.

Host Properties	Description
name	Host short name (label). This name is the one displayed in the Bull System Manager Console views. Generally, this label is the host name. **Note:** In the configuration, the host name MUST be different from the following reserved keys: "*", "none" and "auto". Once the host is created, the name cannot be modified. You can select from a list of already defined hosts. This will result in the modification of the model of the host, according to the menu options. Only hosts using the other model can be selected.
alias name	Host alias name. This field allows to associate an additional name to the host. (reserved for future use)
description	Host description. This description is displayed in an info tip in the Management Tree when you move the cursor over the node associated with this host.
model	Host model. Supported models are: Express 5800, NovaScale 5000 & 6000 series, NovaScale 4000 series, NovaScale 3005 series, NovaScale T800 and R400 series and NovaScale Blade series. Model is fixed by the menu, except for T800 where you can choose a sub-model from NS T800, NS T800 E1, NS T800 E2 or NS T800 F2. Other models can be supported if the corresponding Add-on is installed. This field is set according to the menu item and is not editable. Once the host is created, the model cannot be modified.
network name	Host network name (hostname or IP address). Default value: host name (label).
parents	List of hosts that link the host with remote hosts. For instance, a host representing a network equipment item (router, switch, etc.) is typically a parent host.
OS family	Operating System type (Windows, Linux, AIX, none, other). Other OS can be supported if the corresponding Add-on is installed. Default value: **other**.
OS info	When a host is discovered by **Discovery**, certain properties are set automatically. This is the case of **OS info**, which gives information about the OS running on the host. **Description**, if empty, is automatically set to the same value as **OS info**.

Out-of-band attributes	Description
network name	Out-of-band platform management card address.
user, password	Authentication information (login, password) used by Bull System Manager to access the management card.
GUI URL	Hardware management application **URL**. Access to application URL can be disabled by unchecking the corresponding checkbox. By default, the URL is enabled if the network name is filled in and set to http://<network name>

Table 3-3. NS 3005, NS 9010, NS 4000, NS T800, Express 5800 menu

- To manage Express 5800 servers using out-of-band over LAN, the **Baseboard Management Controller (BMC)** of these servers needs to be configured as present on the RMC card. Please refer to the *Set Up NEC Express 5800 Series Server* guide included on the NEC EXPRESSBUILDER CD-ROM to set up the LAN configuration parameters (IP address, subnet mask, default gateway).
- To manage NovaScale 4000 series servers using out-of-band over **LAN**, **SMU** user accounts and the LAN channel need to be configured using the System Maintenance Utility (SMU). Please refer to the *Configure the Server Using the System Maintenance Utility* chapter in the *Getting Started with Intel Server Management (ISM)* document to set up these configuration parameters.
- To manage **ns bullion**, **NovaScale 3000 series**, **NovaScale 9010 series**, **T800 series** and **R400 series** servers using out-of-band over LAN, the Baseboard Management Controller (BMC) of these servers needs to be configured as present on the RMC card. Refer to your Bull Contact.

Related NS 3005, NS4000, NS9010, NS T800 and Express5800 Objects

The following table describes the object properties generated when this type of host is defined.

Property	Description
categories and services	The Hardware category and related services are instantiated for the host if the Out-Of-Band attributes are configured. The Power category and related services are instantiated for the host if the Out-Of-Band attributes are configured.

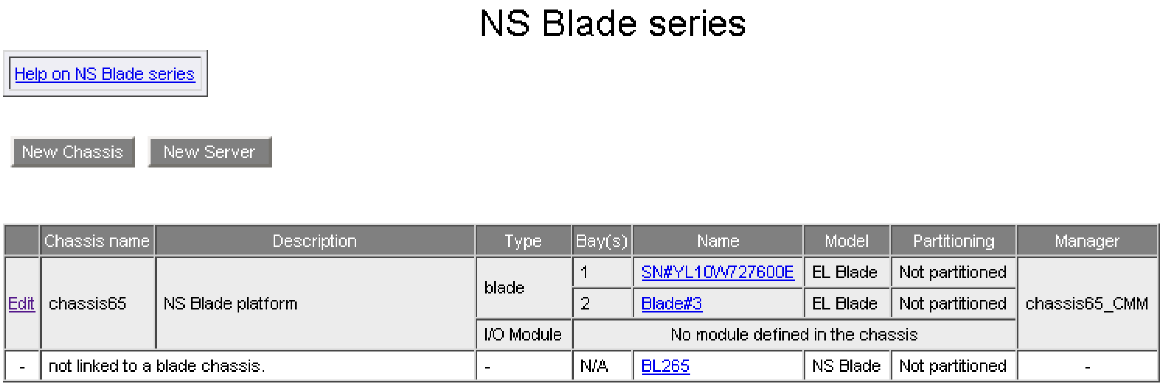
Table 3-4. NS 3005, NS 4000, NS 9010, NS T800, Express 5800 objects

3.1.3 Defining Blade Hosts

3.1.3.1 NovaScale Blade

NovaScale Blade servers are usually housed in the Blade Chassis and managed with the **Chassis Monitoring Module (CMM)**.

To configure Blade hosts, expand the **Blade Hosts** menu from **Host Definition** and select the **NovaScale Blade** item. The following window is displayed:



	Chassis name	Description	Type	Bay(s)	Name	Model	Partitioning	Manager
Edit	chassis65	NS Blade platform	blade	1	SN#YL10W727600E	EL Blade	Not partitioned	chassis65_CMM
				2	Blade#3	EL Blade	Not partitioned	
			I/O Module	No module defined in the chassis				
-	not linked to a blade chassis.		-	N/A	BL265	NS Blade	Not partitioned	-

Figure 3-11. NS Blade Servers main page

To configure a standalone NS Blade Server, click the **New Host** button. This action results in the display of an editable table similar to those for **Other Hosts**.

To configure a Blade Chassis, click the **New Chassis** button.

To modify or delete a Blade Chassis, click the **Edit** link.

To modify or delete a standalone NS Blade Server, click the corresponding link in Host column.

Notes

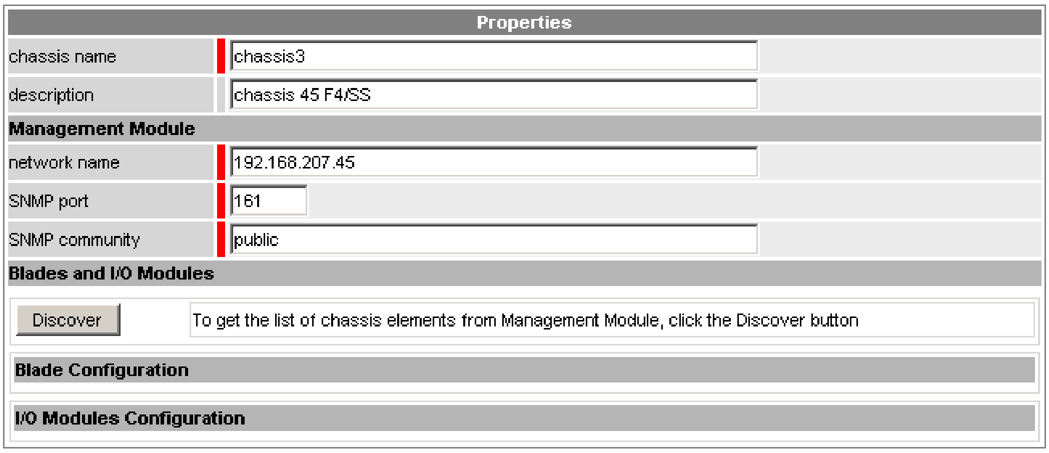
- Blade Chassis can contain two types of blade server: **NS Blade (NovaScale)** or **EL Blade (Enterprise Line)**. Both types can coexist in one chassis. To define a standalone NS Blade, use the **NS Blade** menu. To define a standalone EL Blade, use the **EL Blade** menu.
- Blade Chassis can contain IO Modules. To define a standalone IO module, use the Device hosts / I/O Switch Modules menu.

mportant:

A Blade Server or an I/O Switch linked to a chassis cannot be deleted. You must remove it from the chassis by editing the Blade Chassis object and then, remove the corresponding host.

Blade Chassis Edition

The following form is used to define a Blade Chassis:



Properties	
chassis name	chassis3
description	chassis 45 F4/SS
Management Module	
network name	192.168.207.45
SNMP port	161
SNMP community	public
Blades and I/O Modules	
Discover	To get the list of chassis elements from Management Module, click the Discover button
Blade Configuration	
I/O Modules Configuration	

Figure 3-12. Blade Chassis Edition

Chassis Information

chassis name The label used to identify the chassis in Bull System Manager, `chassis3` in the example.

description Short text description of the chassis, `chassis 45 F4/SS` in the example.

Management Module

network name IP address used to access the CMM, 192.168.207.45 in the example.

SNMP port SNMP agent port used to get information about CMM configuration, `161` in the example.

Default value: *161*.

SNMP community SNMP community used in the SNMP request to identify the Bull System Manager server, `public` in the example.

Default value: *public*.

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

Blade Servers

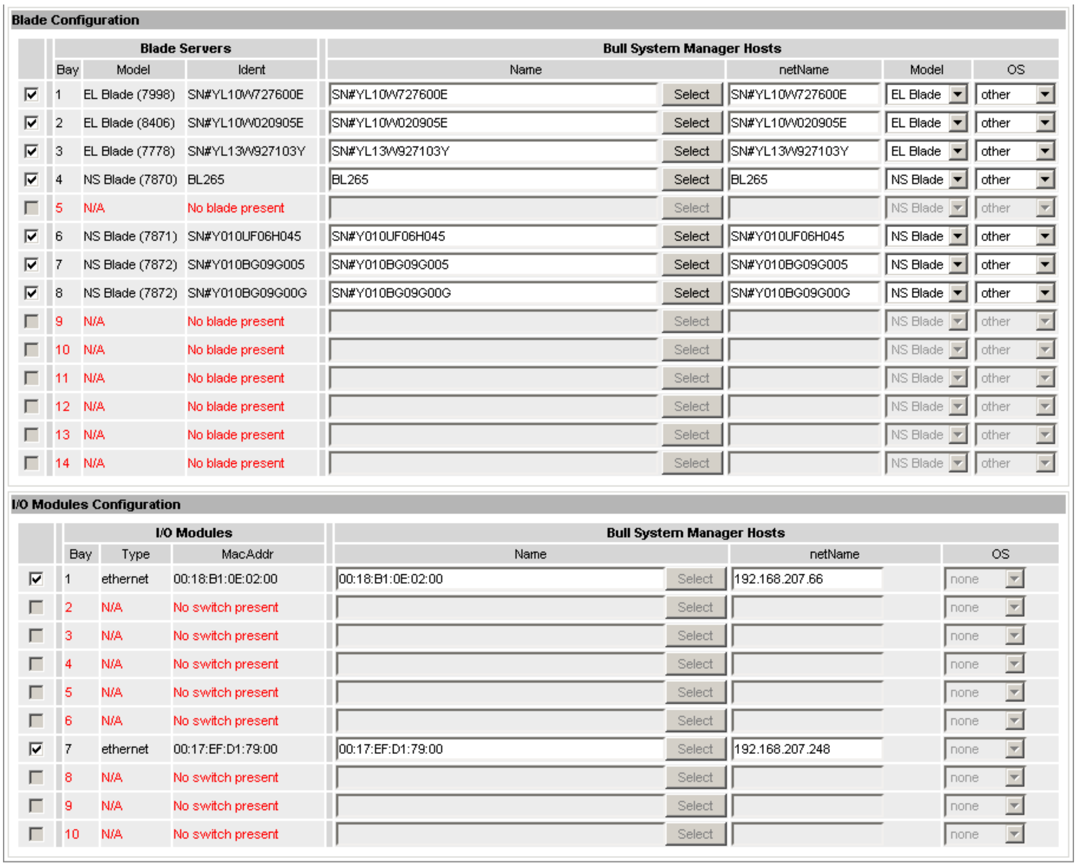
Lists the servers to be managed by Bull System Manager.

I/O Modules

Lists the switch modules to be managed by **Bull System Manager**.

When the chassis is created, this part of the form is not displayed. An initial discovery must be performed to get the list of the servers housed by the chassis, obtained by **SNMP** requests to the **CMM**. Click the **Discover** button to get the list of servers configured in the NS Blade Chassis.

In the following figure, the available bays for blade or I/O module in the chassis are shown with additional details, such as the position of the element in the chassis, and id associated. 14 bays are available for blade servers and 4 for I/O modules



Blade Configuration

	Blade Servers			Bull System Manager Hosts				
	Bay	Model	Ident	Name		netName	Model	OS
☑	1	EL Blade (7998)	SN#YL10W727600E	SN#YL10W727600E	Select	SN#YL10W727600E	EL Blade	other
☑	2	EL Blade (8406)	SN#YL10W020905E	SN#YL10W020905E	Select	SN#YL10W020905E	EL Blade	other
☑	3	EL Blade (7778)	SN#YL13W927103Y	SN#YL13W927103Y	Select	SN#YL13W927103Y	EL Blade	other
☑	4	NS Blade (7870)	BL265	BL265	Select	BL265	NS Blade	other
□	5	N/A	No blade present		Select		NS Blade	other
☑	6	NS Blade (7871)	SN#Y010UF06H045	SN#Y010UF06H045	Select	SN#Y010UF06H045	NS Blade	other
☑	7	NS Blade (7872)	SN#Y010BG09G005	SN#Y010BG09G005	Select	SN#Y010BG09G005	NS Blade	other
☑	8	NS Blade (7872)	SN#Y010BG09G00G	SN#Y010BG09G00G	Select	SN#Y010BG09G00G	NS Blade	other
□	9	N/A	No blade present		Select		NS Blade	other
□	10	N/A	No blade present		Select		NS Blade	other
□	11	N/A	No blade present		Select		NS Blade	other
□	12	N/A	No blade present		Select		NS Blade	other
□	13	N/A	No blade present		Select		NS Blade	other
□	14	N/A	No blade present		Select		NS Blade	other

I/O Modules Configuration

	I/O Modules			Bull System Manager Hosts			
	Bay	Type	MacAddr	Name		netName	OS
☑	1	ethernet	00:18:B1:0E:02:00	00:18:B1:0E:02:00	Select	192.168.207.66	none
□	2	N/A	No switch present		Select		none
□	3	N/A	No switch present		Select		none
□	4	N/A	No switch present		Select		none
□	5	N/A	No switch present		Select		none
□	6	N/A	No switch present		Select		none
☑	7	ethernet	00:17:EF:D1:79:00	00:17:EF:D1:79:00	Select	192.168.207.248	none
□	8	N/A	No switch present		Select		none
□	9	N/A	No switch present		Select		none
□	10	N/A	No switch present		Select		none

Figure 3-13. Blade and I/O Modules Definition with SNMP access

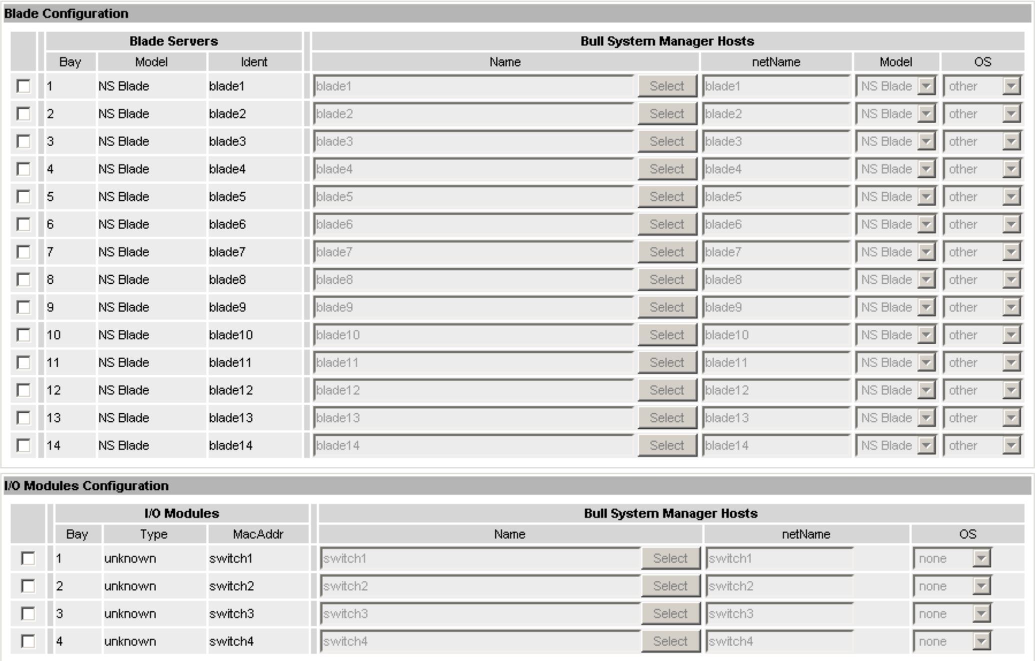
- The left column allows you to select the bay corresponding to the element defined for the monitored chassis. Only the bay that contains an element can be selected to remain coherent with the **CMM** configuration.
- The central section displays the details configured in the CMM. The **bay number**, the **blade model** (NS Blade or EL Blade, followed by the product type in brackets) or the **type of switch** and the **element ident** are displayed.
  The blade model is set according to the code for the product type. The mapping is configured in the `bladetype.cfg` file available in the `<BSM Directory>/core/share/bsmConfig`.

Notes

- The element configuration details in the CMM cannot be modified.
- When the product type information is not available, the model is displayed as N/A
- When the product type is not referenced in the bladetype.cfg file, the model is displayed as unref followed by the product type in brackets.

- The right part allows you to edit the main properties (name, network name, model and OS) of the corresponding BSM host. The host can be edited only if the corresponding bay is checked. You can select an already defined host (**other** model and Blade or I/O Switch modules model depending on the kind of element) by clicking the **Select** button or you can create a host by completing the corresponding field. By default, **Name** and **netName** are set with the ident of the element.

  If the SNMP interface is not accessible, 14 bays are shown for blade servers and 4 bays are shown for I/O modules, without **CMM** information: the **ident** of the Blade server is set to `blade` suffixed with the bay number and the model is set to **NS Blade**, the **ident** of the module is set to `switch` suffixed with the bay number. You can select any bay and fill in the BSM Hosts properties (Figure 3-14).



Blade Configuration

	Blade Servers			Bull System Manager Hosts				
	Bay	Model	Ident	Name		netName	Model	OS
□	1	NS Blade	blade1	blade1	Select	blade1	NS Blade ▾	other ▾
□	2	NS Blade	blade2	blade2	Select	blade2	NS Blade ▾	other ▾
□	3	NS Blade	blade3	blade3	Select	blade3	NS Blade ▾	other ▾
□	4	NS Blade	blade4	blade4	Select	blade4	NS Blade ▾	other ▾
□	5	NS Blade	blade5	blade5	Select	blade5	NS Blade ▾	other ▾
□	6	NS Blade	blade6	blade6	Select	blade6	NS Blade ▾	other ▾
□	7	NS Blade	blade7	blade7	Select	blade7	NS Blade ▾	other ▾
□	8	NS Blade	blade8	blade8	Select	blade8	NS Blade ▾	other ▾
□	9	NS Blade	blade9	blade9	Select	blade9	NS Blade ▾	other ▾
□	10	NS Blade	blade10	blade10	Select	blade10	NS Blade ▾	other ▾
□	11	NS Blade	blade11	blade11	Select	blade11	NS Blade ▾	other ▾
□	12	NS Blade	blade12	blade12	Select	blade12	NS Blade ▾	other ▾
□	13	NS Blade	blade13	blade13	Select	blade13	NS Blade ▾	other ▾
□	14	NS Blade	blade14	blade14	Select	blade14	NS Blade ▾	other ▾

I/O Modules Configuration

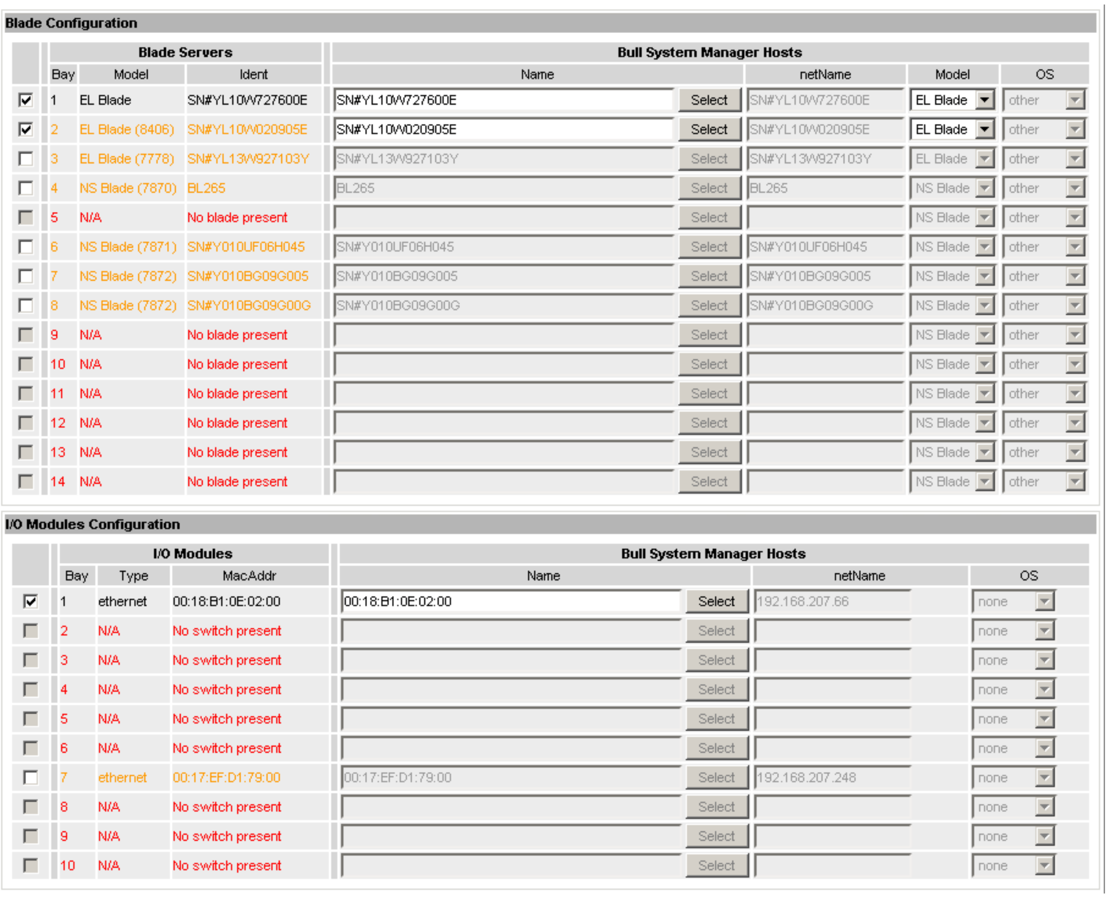
	I/O Modules			Bull System Manager Hosts			
	Bay	Type	MacAddr	Name		netName	OS
□	1	unknown	switch1	switch1	Select	switch1	none ▾
□	2	unknown	switch2	switch2	Select	switch2	none ▾
□	3	unknown	switch3	switch3	Select	switch3	none ▾
□	4	unknown	switch4	switch4	Select	switch4	none ▾

Figure 3-14. Chassis Elements Definition without SNMP access

Notes

- It is possible to create a chassis that contains no elements.
- When you select an already defined host, you cannot change its network name and OS. However, the **Select** box contains a default option corresponding to the element **ident**, which can be edited.

Once a chassis has been created, the elements part displays the chassis topology as registered in **Bull System Manager**. You can only change the **BSM** Host configuration of a previously selected element. To add a new element to your configuration, you must carry out a **Re-discover** step.



Blade Configuration

	Blade Servers			Bull System Manager Hosts				
	Bay	Model	Ident	Name		netName	Model	OS
☑	1	EL Blade	SN#YL10W727600E	SN#YL10W727600E	Select	SN#YL10W727600E	EL Blade	other
☑	2	EL Blade (8406)	SN#YL10W020905E	SN#YL10W020905E	Select	SN#YL10W020905E	EL Blade	other
□	3	EL Blade (7778)	SN#YL13W927103Y	SN#YL13W927103Y	Select	SN#YL13W927103Y	EL Blade	other
□	4	NS Blade (7870)	BL265	BL265	Select	BL265	NS Blade	other
□	5	N/A	No blade present		Select		NS Blade	other
□	6	NS Blade (7871)	SN#Y010UF06H045	SN#Y010UF06H045	Select	SN#Y010UF06H045	NS Blade	other
□	7	NS Blade (7872)	SN#Y010BG09G005	SN#Y010BG09G005	Select	SN#Y010BG09G005	NS Blade	other
□	8	NS Blade (7872)	SN#Y010BG09G00G	SN#Y010BG09G00G	Select	SN#Y010BG09G00G	NS Blade	other
□	9	N/A	No blade present		Select		NS Blade	other
□	10	N/A	No blade present		Select		NS Blade	other
□	11	N/A	No blade present		Select		NS Blade	other
□	12	N/A	No blade present		Select		NS Blade	other
□	13	N/A	No blade present		Select		NS Blade	other
□	14	N/A	No blade present		Select		NS Blade	other

I/O Modules Configuration

	I/O Modules			Bull System Manager Hosts			
	Bay	Type	MacAddr	Name		netName	OS
☑	1	ethernet	00:18:B1:0E:02:00	00:18:B1:0E:02:00	Select	192.168.207.66	none
□	2	N/A	No switch present		Select		none
□	3	N/A	No switch present		Select		none
□	4	N/A	No switch present		Select		none
□	5	N/A	No switch present		Select		none
□	6	N/A	No switch present		Select		none
□	7	ethernet	00:17:EF:D1:79:00	00:17:EF:D1:79:00	Select	192.168.207.248	none
□	8	N/A	No switch present		Select		none
□	9	N/A	No switch present		Select		none
□	10	N/A	No switch present		Select		none

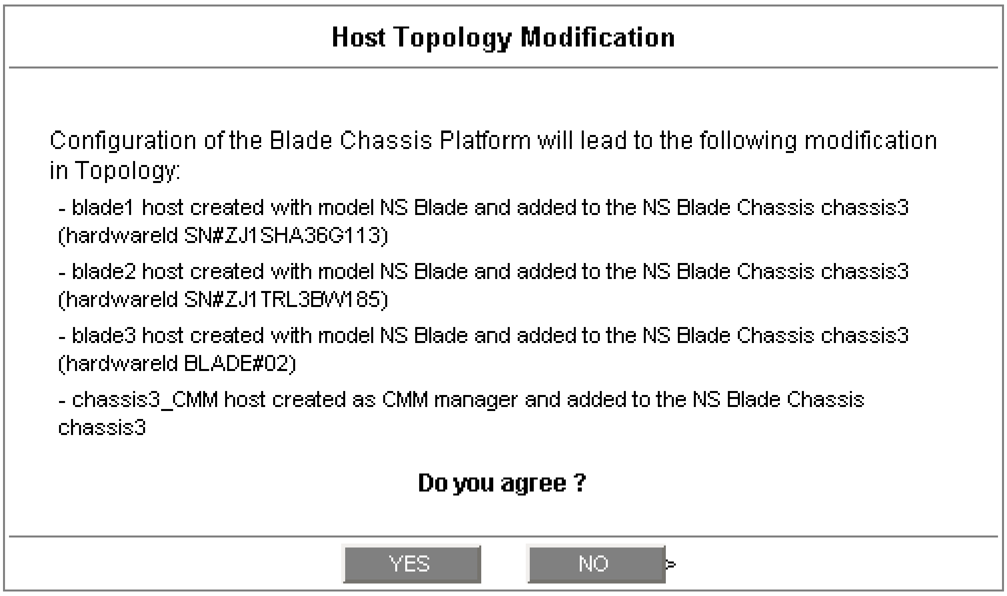
Figure 3-15. Chassis Elements Re-discovery

A bay that is not referenced in the current **BSM** or that differs from **CMM** is displayed in orange and is editable. A bay that is not referenced in **CMM** is displayed in red and is not editable.

After editing:

- Click the **OK** button to validate the changes
- Or click the **Cancel** button to return to the NS Blade Servers page without making any changes.

When the **Topology** is modified, a confirmation is required. A screen is displayed, listing all the changes to be applied, as shown in the following figure:



Host Topology Modification

Configuration of the Blade Chassis Platform will lead to the following modification in Topology:

- blade1 host created with model NS Blade and added to the NS Blade Chassis chassis3 (hardwareId SN#ZJ1SHA36G113)
- blade2 host created with model NS Blade and added to the NS Blade Chassis chassis3 (hardwareId SN#ZJ1TRL3BW185)
- blade3 host created with model NS Blade and added to the NS Blade Chassis chassis3 (hardwareId BLADE#02)
- chassis3_CMM host created as CMM manager and added to the NS Blade Chassis chassis3

Do you agree ?

Figure 3-16. NovaScale Blade confirmation

If you do not agree, click the **NO** button to return to the **NS Blade Chassis** window, otherwise click the **YES** button to create the NS Blade Chassis and all related objects.

Related Blade Chassis Properties

The following table lists the object properties generated when a Blade Chassis is defined.

Property	Description
host blade	As defined in the blade configuration part of the table.
host switch	As defined in the I/O module configuration part of the table.
host CMM	Host representing the CMM, named as <chassisName>_CMM. **Note:** if the chassis was defined in a previous Bull System Manager version, the used name is kept (the same as the Manager name, or the Manager name with _mgr suffix).
hostgroup	hostgroup representing the physical platform, named <chassisName>. This hostgroup is composed of one host representing the manager (see below) and two hostgroups, if needed, one named <chassisName>_blade (for the set of blade server) and the other named <chassisName>_iosm (for the set of I/O switch modules)

Property	Description
manager CMM	Hardware manager representing the CMM, named <chassisName>_CMM. Note: if the chassis was defined in a previous Bull System Manager version, the name used is kept.
categories and services	The **CMM** category and related services are instantiated for the **CMM** host. The Hardware category and related services are instantiated for each **NS Blade** or EL Blade host. The Hardware category and related services are instantiated for each I/O switch host.

Table 3-5. NS Blade Chassis objects

Chassis element

A chassis element has properties linked to the Blade Chassis and properties of a host object. To add, move or modify properties linked to the chassis use the **Blade Chassis** edition page.

To modify host properties use the **Host edition** page.

Add an element to a chassis.

To add an element check the corresponding line in the **Elements Configuration** part of the chassis table and set the host characteristics in the BSM configuration table zone (by filling in the corresponding fields or by selecting a host already defined host).

Note When you edit the details for a chassis, only elements defined as part of the NovaScale platform are displayed. To add elements, you must perform a **Re-discover** step to get the list of all elements as defined in the **CMM** configuration.

Remove an element from a chassis

To remove an element from a chassis, uncheck the corresponding line in the table.

Note The corresponding host remains in the Bull System Manager configuration as an element unlinked to a chassis. To delete it, edit it and click the **Delete** button.

Unlinked switch hosts are displayed in the page corresponding to the menu I/O Switch Module in the Device hosts section.

Modifying an element linked to a chassis

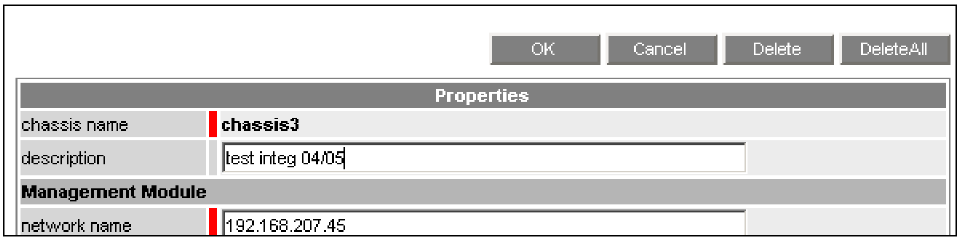
To modify the name of the **BSM host** corresponding to an element, enter the new name in the corresponding field or choose it in the list of already defined hosts in **Bull System Manager** by clicking the Select button.

To modify other characteristics (**netName**, OS, etc.), use the **Host edition** window.

Notes

- To bring up the Host edition window corresponding to the element, click the **Hostname** link displayed in the global chassis window.
- When you rename an element, the host corresponding to the old name remains as an element unlinked to a chassis.

Deleting a Blade Chassis

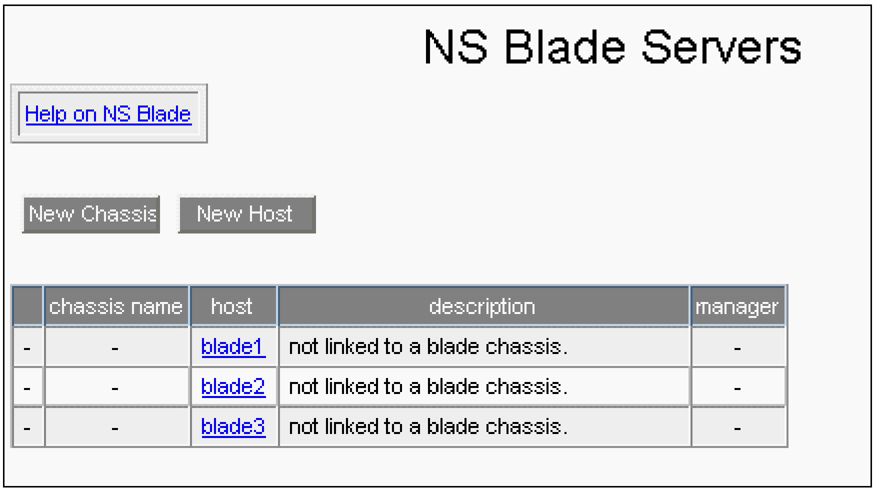


Properties	
chassis name	**chassis3**
description	test integ 04/05
Management Module	
network name	192.168.207.45

Figure 3-17. Deleting a Blade Chassis

There are two ways of deleting a Blade Chassis:

- Click the **Delete** button to delete the chassis but retain its elements.
  The hostgroup, manager and related services are deleted but the elements remain in the **BSM** configuration as unlinked element hosts, as displayed in the figure below:



	chassis name	host	description	manager
-	-	blade1	not linked to a blade chassis.	-
-	-	blade2	not linked to a blade chassis.	-
-	-	blade3	not linked to a blade chassis.	-

Figure 3-18. NS Blade Servers not linked to a chassis

- Or click the **DeleteAll** button to delete the chassis and all its linked elements.

3.1.3.2 Escala Blade

EL Blade servers are usually housed in the Blade Chassis and managed with the **Chassis Monitoring Module (CMM)**.

To configure **EL Blade** hosts, expand the **Blade Hosts** menu under **Host Definition** and select the **Escala Blade** item.

Procedures to create, modify or delete Escala Blade are similar to those described for the NovaScale Blade (see *NovaScale Blade*, on page 42). The main difference is the model of the standalone server, which is set to **EL Blade**.

Note When the Escala Blade is declared with an OS set to **VIOS**, the Escala Blade is configured using the Escala LPAR page, which allows the definition of the associated logical partitions (see *LPARs*, on page 59).

3.1.4 Defining Escala Hosts

3.1.4.1 PL Server

An **Escala PL** Server is represented as a platform grouping logical partitions (**LPAR**).

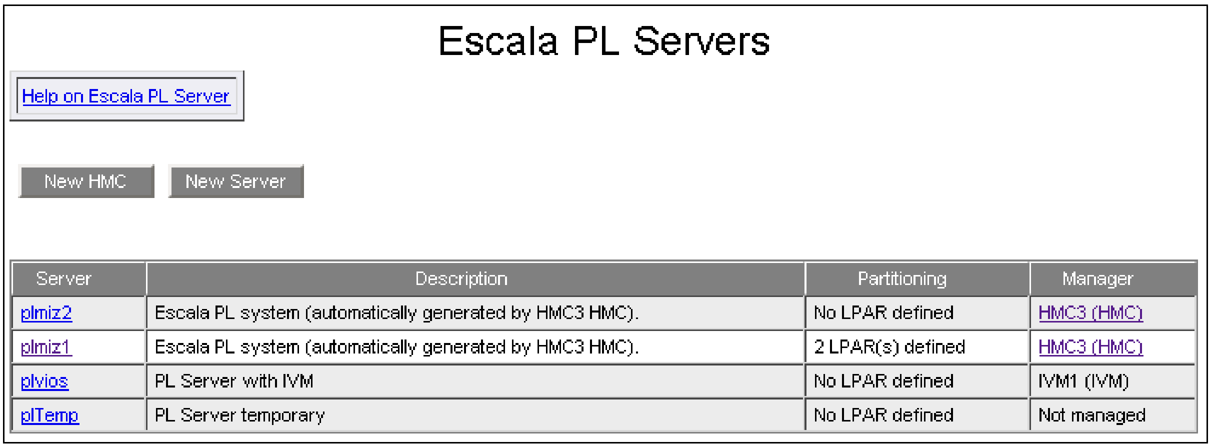
Escala PL Servers can be managed by an **HMC** (Hardware Management Console), a system that provides management tools for controlling one or more **Escala PL** servers and associated **LPAR**s. In this case, the platform contains a host representing the **Central Electronics Complex** (**CEC**).

If no **HMC** system is available, **Escala PL** Servers can be managed with **IVM** (Integrated Virtualization Manager), which is part of the virtual I/O server. In this case, the platform contains a host (with OS set to VIOS) representing the VIO partition.

If no **HMC** or **IVM** is available, the Escala PL Server platform contains only the **LPAR**s.

Note The supervision of the virtualization part of Escala PL platform requires the **EscalaLPAR** Add-on. To obtain information on LPAR supervision, refer to *Bull System Manager Server Add-ons Installation and Administrator's Guide* (86 A2 59FA).

To configure Escala PL Servers, expand the **Escala Hosts** menu under **Hosts Definition** and select the **PL Server** menu. The following page is displayed:



Escala PL Servers

Help on Escala PL Server

Server	Description	Partitioning	Manager
plmiz2	Escala PL system (automatically generated by HMC3 HMC).	No LPAR defined	HMC3 (HMC)
plmiz1	Escala PL system (automatically generated by HMC3 HMC).	2 LPAR(s) defined	HMC3 (HMC)
plvios	PL Server with IVM	No LPAR defined	IVM1 (IVM)
plTemp	PL Server temporary	No LPAR defined	Not managed

Figure 3-19. Escala PL Servers

To create an **HMC** and the **Escala PL** Servers that it manages, click the **New HMC** button. To create an **Escala PL** Server managed by **IVM** or not managed, click the **New Server** button. To modify or delete an **HMC**, click the corresponding **HMC** link.

To modify or delete an **Escala PL** Server, click the corresponding **Platform name link**.

Note An **Escala PL** Server defined as a managed **HMC** system cannot be deleted. You must first remove it from the **HMC** managed systems.

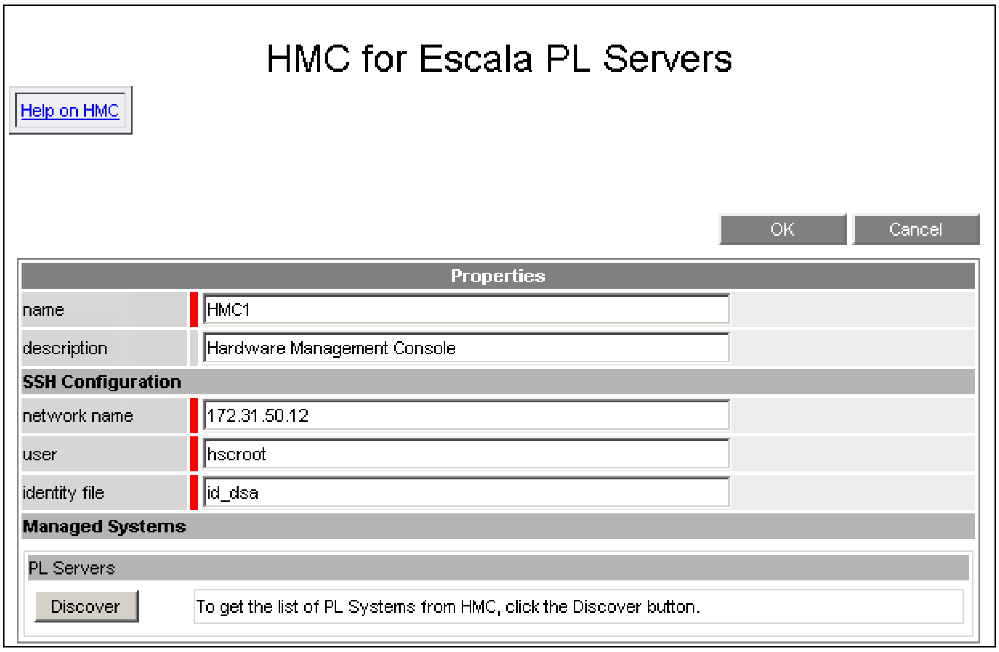
Important

Escala PL Supervision with HMC or IVM requires the setting of a non-prompt ssh connection between the Bull System Manager Server and the manager (HMC or IVM). Private key for the Bull System Manager server is automatically generated at the installation of Bull System Manager server under **`<BSM installation directory>/engine/etc/ssh`** (see Appendix F for detailed information). To allow non-prompt connection between the BSM Server and the manager, the public key must be installed on the manager. Refer to the Escala and AIX documentation for more information.

3.1.4.1.1 HMC Managed PL Servers

HMC edition

The following form is used to define an HMC and its managed systems.



HMC for Escala PL Servers

Properties	
name	HMC1
description	Hardware Management Console
SSH Configuration	
network name	172.31.50.12
user	hscroot
identity file	id_dsa
Managed Systems	
PL Servers	
Discover	To get the list of PL Systems from HMC, click the Discover button.

Figure 3-20. HMC Edition

HMC Information

name
: The label used to identify the HMC in Bull System Manager. **`HMC1`** in this example.

description
: Short text describing the HMC. **`Hardware Management Console`** in this example.

SSH Configuration

networkName
IP address used to access the HMC in Bull System Manager.
`172.31.50.12` in this example.

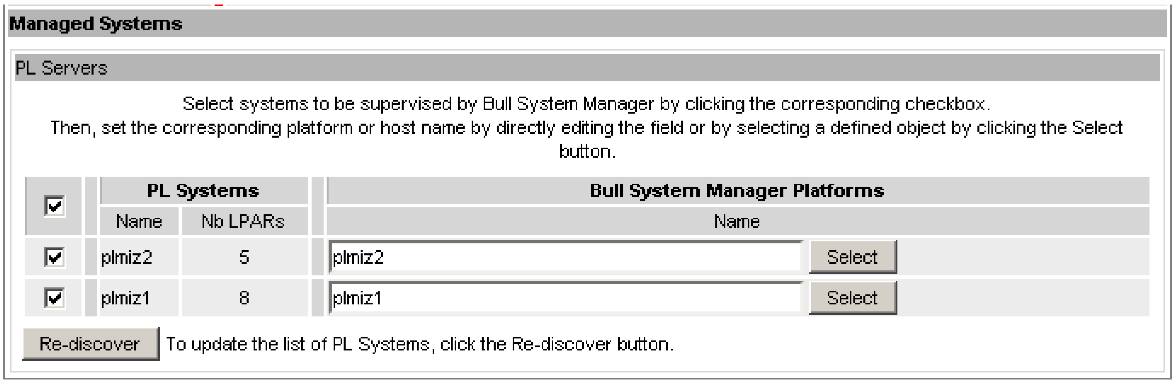
user
User for ssh connection, `hscroot` in this example.
Default value: *hscroot*
The default value is those commonly used on **HMC**.

identityFile
File containing the key for **SSH** connection.
`id_dsa` in this example.
Default value: **id_dsa**
The default value corresponds to the name of the key file automatically generated by BSM.

Managed Systems

Lists the servers to be supervised by **Bull System Manager**.
At **HMC** creation, this part of the form is not displayed. An initial discovery must be performed to get the list of the servers managed by the **HMC**. Click the **Discover** button to get the list of servers configured in the HMC.

In the following figure, the **PL Servers** managed by the current **HMC** are displayed.



Managed Systems

PL Servers

Select systems to be supervised by Bull System Manager by clicking the corresponding checkbox.
Then, set the corresponding platform or host name by directly editing the field or by selecting a defined object by clicking the Select button.

☑	PL Systems		Bull System Manager Platforms	
	Name	Nb LPARs	Name	
☑	plmiz2	5	plmiz2	Select
☑	plmiz1	8	plmiz1	Select

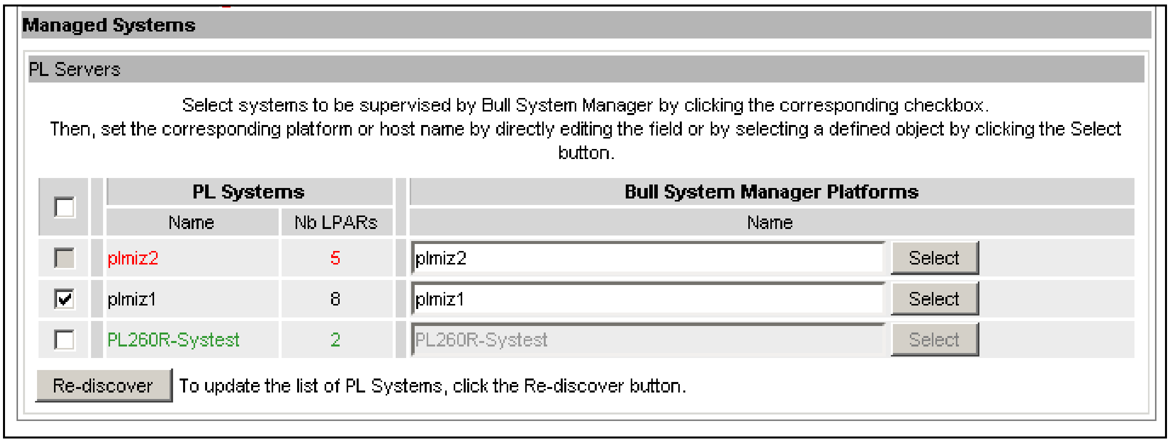
To update the list of PL Systems, click the Re-discover button.

Figure 3-21. PL Servers discovery

- The left column allows you to select the server to be supervised by **Bull System Manager**.
- The central section displays PL Server configuration as defined in the HMC. The number of logical partition configured is displayed.
- The right part allows you to edit the main properties of the corresponding **BSM** platform. The platform can be edited only if the corresponding server is checked. You can select an already defined platform by clicking the **Select** button or you can create a platform by entering its name. By default, **Name** is set with the **ident** defined in the **HMC** configuration.
  If the **ssh** link is not set, you can define your systems, but the supervision will not be correct (lack of system identifier as defined in **HMC**).

Note It is possible to create an **HMC** with no managed system.

Once an **HMC** with managed systems is defined, the **Managed Systems** part displays the server topology as registered in Bull System Manager. You can change only the **BSM** configuration of a previously selected server. To add a new server in your configuration, you must perform a **Re-discover** step.



Managed Systems

PL Servers

Select systems to be supervised by Bull System Manager by clicking the corresponding checkbox.
Then, set the corresponding platform or host name by directly editing the field or by selecting a defined object by clicking the Select button.

□	PL Systems		Bull System Manager Platforms	
	Name	Nb LPARs	Name	
□	plmiz2	5	plmiz2	Select
☑	plmiz1	8	plmiz1	Select
□	PL260R-Systest	2	PL260R-Systest	Select

Re-discover To update the list of PL Systems, click the Re-discover button.

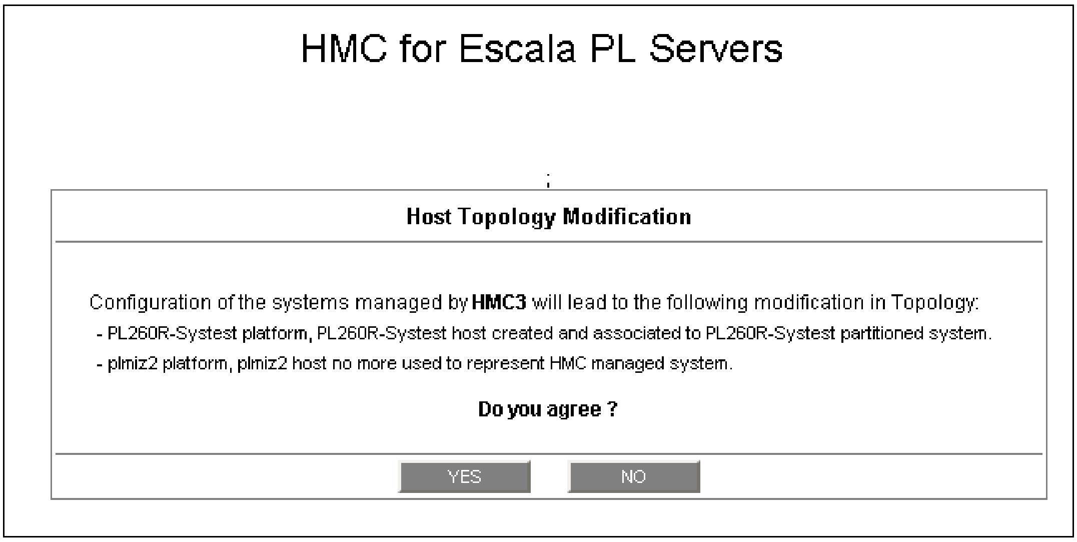
Figure 3-22. PL Servers Re-discovery

A server that is not referenced in the current **BSM** or that differs from **HMC** is displayed in green and is editable. A server that is no longer referenced in **HMC** is displayed in red and is not editable.

After editing:

- Click the **OK** button to validate the changes.
- Or click the **Cancel** button to return to the HMC page without changes.

When the Topology is modified, a confirmation is required. A page is displayed, listing all the changes to be applied, as shown in the following figure:



HMC for Escala PL Servers

Host Topology Modification

Configuration of the systems managed by **HMC3** will lead to the following modification in Topology:
- PL260R-Systest platform, PL260R-Systest host created and associated to PL260R-Systest partitioned system.
- plmiz2 platform, plmiz2 host no more used to represent HMC managed system.

Do you agree ?

Figure 3-23. HMC Managed Systems Confirmation

If you do not agree, click the **NO** button to return to the HMC window, otherwise click the **YES** button to confirm the changes on HMC, managed systems and all related objects.

Notes

- If the **EscalaLPAR** Add-on is not installed, a message is displayed to warn you about the lack of virtualization supervision.
- Installation of the **EscalaLPAR** Add-on automatically generates supervision for all the defined platforms.

Related HMC systems Objects

The following table lists the topology objects generated during the creation of an **HMC** system.

Type	Description
host	As defined in the PL server configuration part of the edition page.
manager HMC	Hardware manager representing the HMC, named <hmc_name>.

The **Hardware** category and related services are automatically generated for each **Escala** PL host declared as a **HMC** managed system. The following table lists the services defined for the **Hardware** category.

Name	Description
CECStatus	This service checks the status of the system reported by the **HMC**.
Events	This service checks if any hardware events have been reported for the given system.

HMC managed PL server edition

A PL server has hardware properties linked to the **HMC** and the properties of a platform object.

To **add**, **move** or **modify** properties linked to the HMC, use the **HMC** edition page.

To modify platform properties use the **LPARs** edition page.

Add a PL server to HMC Managed Systems

To add a PL server check the corresponding line in the **Servers Configuration** part of the **HMC** table and set the platform characteristics in the BSM configuration table zone (by entering the new name or selecting it in the defined non-managed platforms).

Note

When you edit an **HMC**, only the PL servers defined as managed by Bull System Manager are displayed. To add PL servers, you must perform a re-discover step to get the list of all servers as defined in the **HMC** configuration.

Remove a PL server from HMC Managed Systems

To remove a PL server from an **HMC**, uncheck the corresponding line in the **Servers Configuration** part of the HMC properties window.

Note The server representing the CEC is deleted, but the set of LPARs (if defined) remain as a non-managed platform that can be linked to another system.

Modify a PL server managed by an HMC

To modify the name of the **BSM** platform corresponding to a managed PL server, enter the new name in the corresponding field or select it from the list of platforms already defined in Bull System Manager by clicking the **Select** button.

Use the **LPARs** table to modify the partitioning characteristics.

Notes

- To get the **LPAR**s table corresponding to the PL server, click the platform name link displayed in the global **HMC** window.
- When you rename a **PL** server, the host corresponding to the old name remains as a PL server not managed by an HMC.

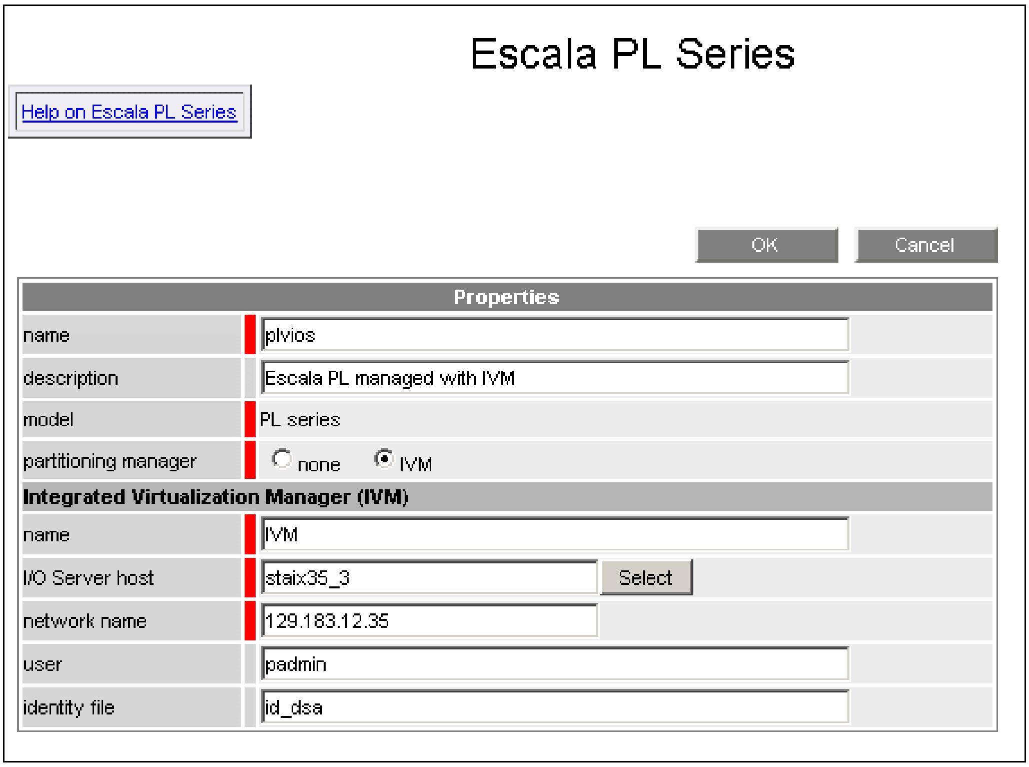
Deleting HMC systems

From the **HMC** window, you can delete the HMC definition by clicking the **Delete** button.

The manager and related services are deleted but the **PL** servers remain in the **BSM** configuration as not managed PL servers.

3.1.4.1.2 IVM Managed PL Server

The following window is used to define an IVM managed PL Server.



Escala PL Series

Properties	
name	plvios
description	Escala PL managed with IVM
model	PL series
partitioning manager	○ none ● IVM
Integrated Virtualization Manager (IVM)	
name	IVM
I/O Server host	staix35_3
network name	129.183.12.35
user	padmin
identity file	id_dsa

Figure 3-24. IVM Managed PL Server

Server Information

name
The label used to identify the platform in Bull System Manager. **`plvios`** in this example.

description
Short text description of the platform. **`Escala PL managed with IVM`** in this example.

model
Server model

partitioning manager
Indicates if the server is managed by IVM or not.
Must be set to **`IVM`** in this example.

Integrated Virtualization Manager Configuration

name
The label used to identify the manager

I/O Server host
Name of the host with the **VIOS** partition. If the corresponding host is already defined, use **Select** to set it.

network name
IP address used to access the **IVM** in Bull System Manager.
`172.31.50.35` in this example.

user
User for **ssh** connection, **`padmin`** in this example.
Default value: `padmin`
The default value is those commonly used on IVM.

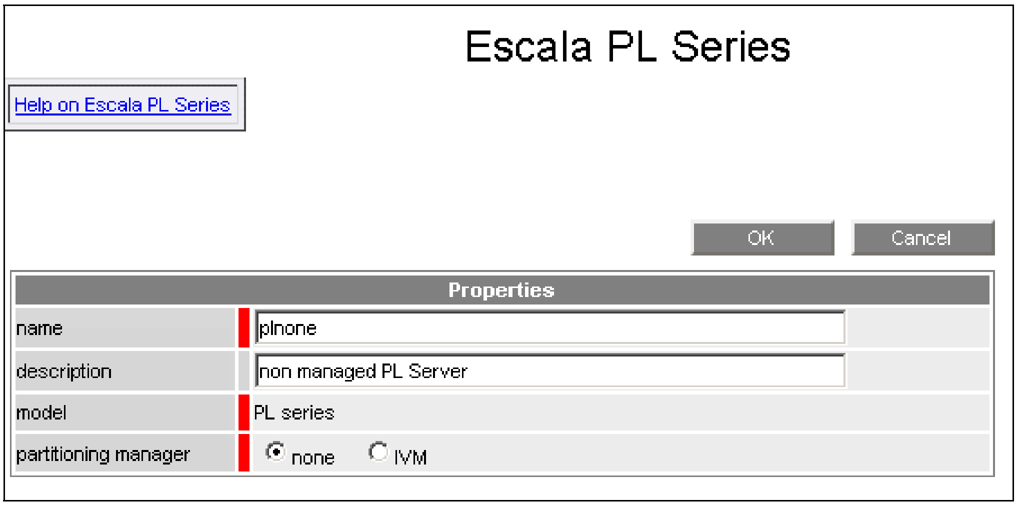
identity file
File containing the key for ssh connection.
`id_dsa` in this example.
Default value: **id_dsa**
The default value corresponds to the name of the key file automatically generated by **BSM**.

Notes

- When the server has been initialized this way, all modifications must be done from the **LPAR** window.
- It is not possible to change IVM PL Server directly to a non-managed PL Server. To do this, first remove the platform, and then configure a new PL Server as non-managed.

3.1.4.1.3 Non-managed PL Server

To define a non-managed PL server, use the previous window with the partitioning manager set to none.



Properties	
name	plnone
description	non managed PL Server
model	PL series
partitioning manager	● none ○ IVM

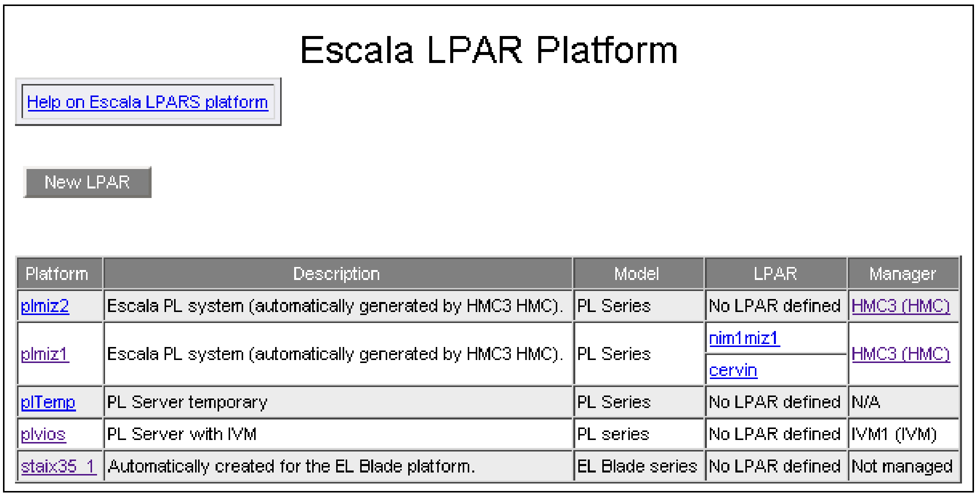
Figure 3-25. Non managed PL Server

To initialize the server, just enter a valid name.

3.1.4.2 LPARs

3.1.4.2.1 Platform edition

To configure partitioning of a PL Server or a EL Blade, click the **LPARs** item. The list of all **Escala** servers appears, as shown below:



Escala LPAR Platform

Platform	Description	Model	LPAR	Manager
plmiz2	Escala PL system (automatically generated by HMC3 HMC).	PL Series	No LPAR defined	HMC3 (HMC)
plmiz1	Escala PL system (automatically generated by HMC3 HMC).	PL Series	nim1miz1 cervin	HMC3 (HMC)
plTemp	PL Server temporary	PL Series	No LPAR defined	N/A
plvios	PL Server with IVM	PL series	No LPAR defined	IVM1 (IVM)
staix35_1	Automatically created for the EL Blade platform.	EL Blade series	No LPAR defined	Not managed

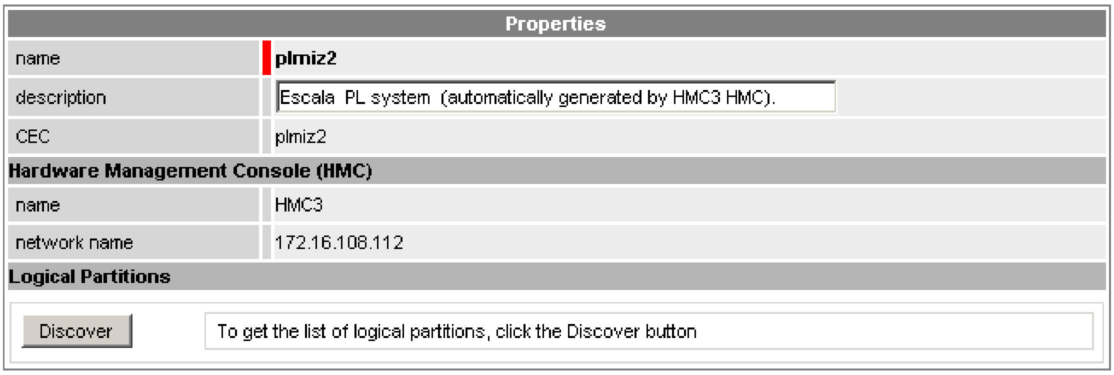
Figure 3-26. Escala LPARs page

It is possible:

- To create a single partition using the **New LPAR** button
- To edit or delete a platform using the **<Platform Name>** link
- To edit a logical partition host using the **<LPAR Name>** link.

Note By clicking the platform name link in PL Server or EL Blade page, you access the **Properties** window directly for the platform.

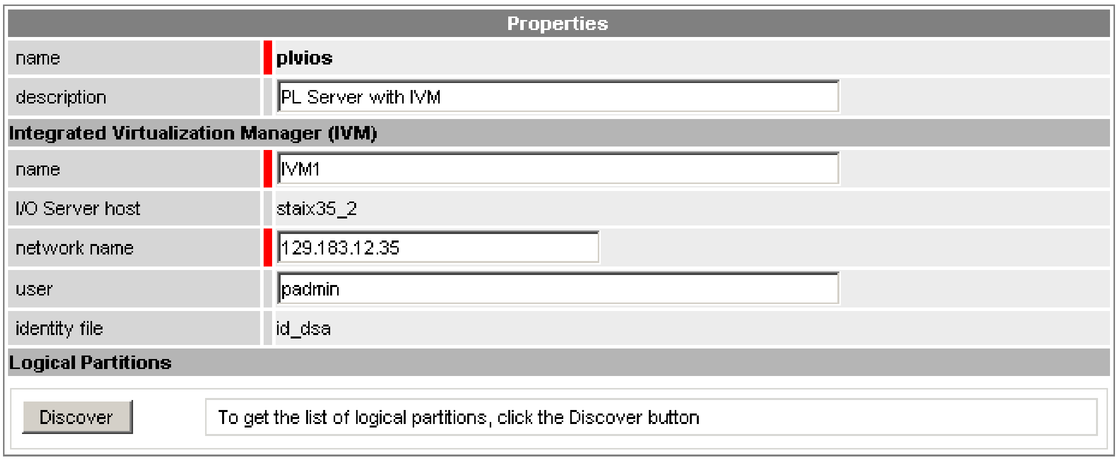
When you click the platform name link of an HMC managed system, the following window is displayed:



Properties	
name	**plmiz2**
description	Escala PL system (automatically generated by HMC3 HMC).
CEC	plmiz2
Hardware Management Console (HMC)	
name	HMC3
network name	172.16.108.112
Logical Partitions	
Discover	To get the list of logical partitions, click the Discover button

Figure 3-27. HMC managed Escala LPAR platform

When you click the platform name link of an IVM managed system, the following window is displayed:

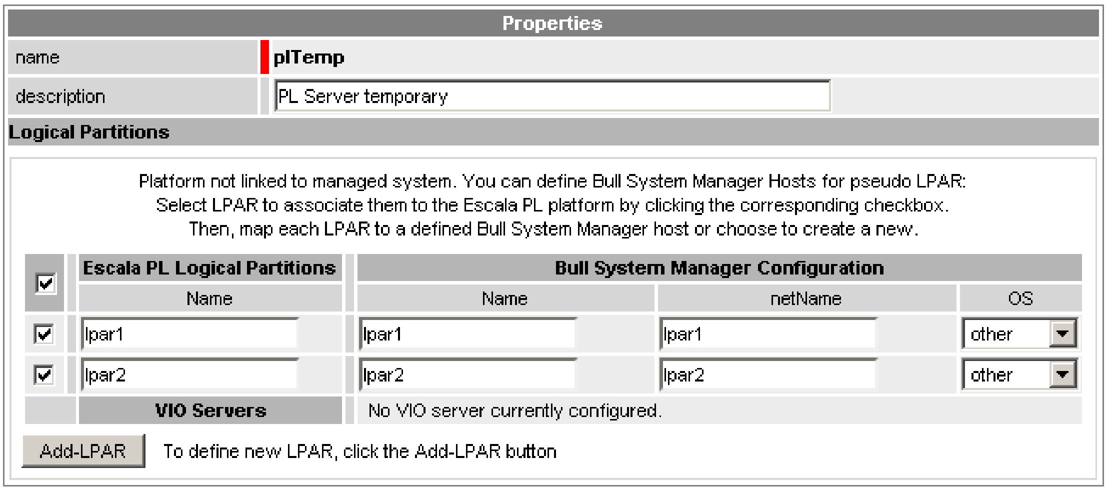


Properties

name	**plvios**
description	PL Server with IVM
Integrated Virtualization Manager (IVM)	
name	IVM1
I/O Server host	staix35_2
network name	129.183.12.35
user	padmin
identity file	id_dsa
Logical Partitions	
Discover	To get the list of logical partitions, click the Discover button

Figure 3-28. IVM managed Escala LPAR platform

When you click the platform name link of a non-managed system, the following window is displayed:



Properties

name	**plTemp**
description	PL Server temporary

Logical Partitions

Platform not linked to managed system. You can define Bull System Manager Hosts for pseudo LPAR:
Select LPAR to associate them to the Escala PL platform by clicking the corresponding checkbox.
Then, map each LPAR to a defined Bull System Manager host or choose to create a new.

☑	**Escala PL Logical Partitions**	**Bull System Manager Configuration**		
	Name	Name	netName	OS
☑	lpar1	lpar1	lpar1	other
☑	lpar2	lpar2	lpar2	other
	VIO Servers	No VIO server currently configured.		

Add-LPAR To define new LPAR, click the Add-LPAR button

Figure 3-29. Non-managed Escala LPAR platform

The properties of Escala LPAR platform are divided into three parts:

- One to identify the platform
- One to identify the manager (HMC or IVM)
- One to configure the LPAR

Platform Properties

name
Short name for the platform.
This name is displayed in the Bull System Manager console view.

description
Short text description of the platform.
When you move the cursor over the node associated with the platform, this information is displayed as an info tip in the Management Tree.

CEC
Name of the system referenced by **HMC** manager.
This property is shown only if the system is managed by an HMC and is not editable (set in HMC properties window).

Hardware Management Console Properties

name
Name of the HMC.
This property is not editable (set in HMC properties window)

network name
Hostname or IP address of the HMC.
This property is not editable in this form (set in HMC Properties window) .

Note CEC and HMC related properties cannot be changed in the LPAR properties window. To change them, you must use the HMC properties window.

Integrated Virtualization Manager properties

name
Manager short name.
This property is editable only during when the platform details are first entered.

I/O Server host
Name of the Escala server that contains the VIOS partition.
This property is not editable (set in Escala Server Properties window).

network name
Hostname or IP address of the **VIOS** partition.

user
Remote user name for login.
Default value: padmin

identity file
File containing the key for ssh connection.
This value cannot be changed. Identity files are generated when BSM is installed with specific rights.

Note Only the network name and user properties can be changed in this window. The other **IVM** properties are defined when the PL Server is initialized and cannot be changed after. To change them, you must delete the server and create it again with new **idents.**

Logical Partitions Properties

For managed platforms:

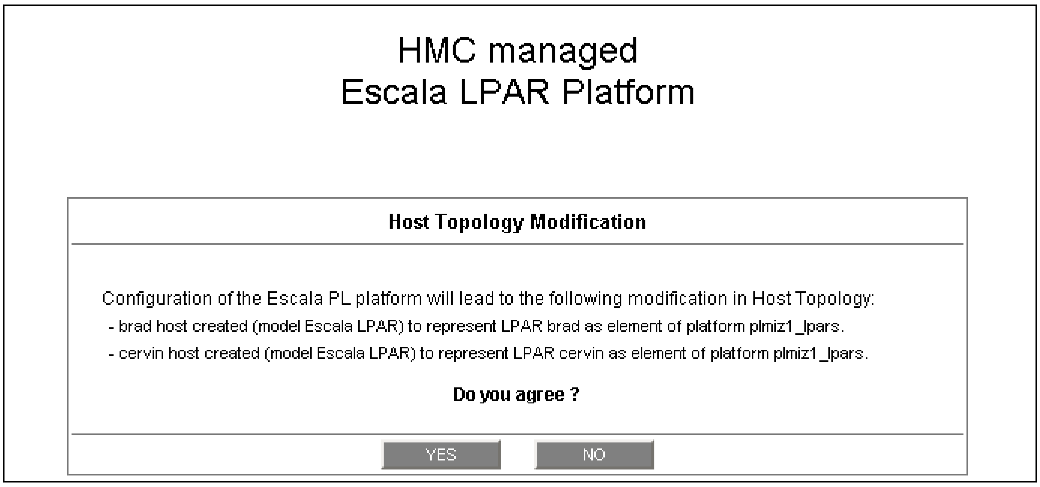
List of the partitions defined by selecting the partitions obtained by remote command on **HMC** or **IVM**.
The request is performed by clicking the **Discover** button (or-**Re-discover** if you are in properties window).

For non managed platforms:

The Discover button is not available, but an Add-LPAR button is used to add as many partition definitions as required.

Notes
- Discover requires that a non-prompt connection can be established between the BSM server and the manager (HMC or IVM) (see **identityFile** property above).
- If the manager is not reachable, a procedure similar to that for non-managed platforms is used.

Topology modifications require confirmation: a page listing all modifications to be applied to the Topology configuration is displayed, as shown below:



HMC managed
Escala LPAR Platform

Host Topology Modification

Configuration of the Escala PL platform will lead to the following modification in Host Topology:
- brad host created (model Escala LPAR) to represent LPAR brad as element of platform plmiz1_lpars.
- cervin host created (model Escala LPAR) to represent LPAR cervin as element of platform plmiz1_lpars.

Do you agree ?

Figure 3-30. Host Topology modification confirmation for HMC managed Escala LPAR platform

If you do not agree, click **NO** to return to the platform Properties window, otherwise click **YES** to create the LPAR platform.

After making the changes:

- Click **OK** to validate your changes
- Or click **Cancel** to return to **Escala** LPAR Platforms pages without changes
- Or click **Delete** to remove the Escala Platform and maintain the hosts corresponding to the partitions
- Or click **DeleteAll** to remove the Escala Platform and the hosts corresponding to partitions.

Notes

- **HMC** managed platforms cannot be deleted: you must first remove the platform from the list of managed systems included in the HMC window, and then delete it.
- When a platform is deleted, the **LPAR**s remain as standalone hosts.
- When an IVM platform is deleted, the host representing the VIOS is modified with the OS set to **other** (**Delete** or **DeleteAll** action).

Related HMC managed platform Objects

The following table describes the objects generated during the creation of a HMC managed platform.

Type	Description
host LPAR	As defined in the Logical Partition configuration part of the properties window.
hostgroup	hostgroup representing the platform, named <platformName>.
manager	Virtualization manager representing the management interface, as defined in HMC part of the window.

Related IVM managed platform Objects

The following table describes the objects generated during the creation of an **IVM** managed platform.

Type	Description
host LPAR	As defined in the Logical Partition configuration part of the Properties window
hostgroup	hostgroup representing the platform, named <platformName>.
manager	Virtualization manager representing the management interface, as defined in the IVM part of the Properties window.

3.1.4.2.2 LPAR edition

A logical partition is represented by a host linked to the Escala LPAR platform. It has properties linked to the platform and properties of a host object.

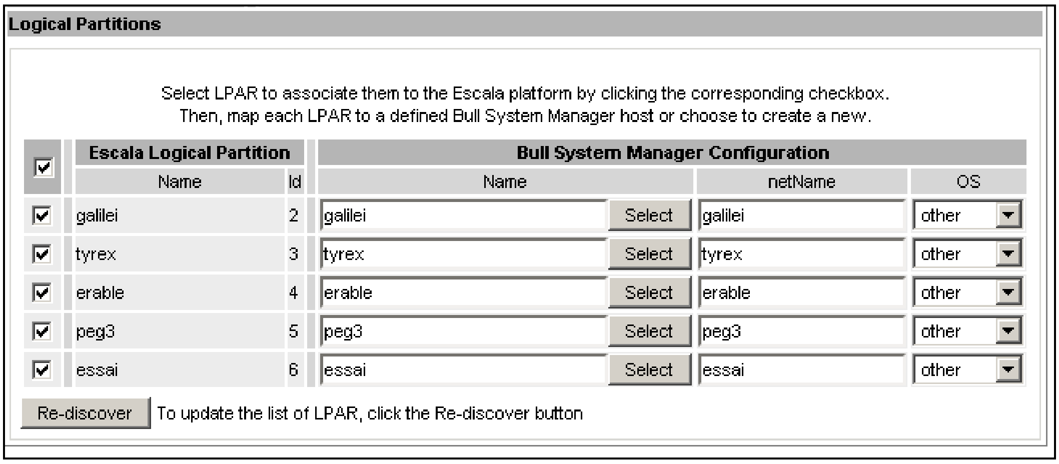
Adding, removing or changing properties linked to the platform must be done from the Escala LPAR platform properties window.

Changing host properties must be done from the Host properties window.

Logical Partitions Discovery

The list of partitions defined for the Escala Server can be obtained from the manager by clicking the **Discovery** button. The result of the discovery is displayed as a table composed of three parts:

- The left column allows you to select the partitions to be associated with the platform.
- The center part displays Partitions properties as configured in the manager (HMC or IVM).
- The right part allows you to edit the main properties (name, network name and OS) of the corresponding BSM host. The host can be edited only if the corresponding partition is selected. You can select an host that is already defined by clicking the **Select** button or you can create a host by completing the corresponding fields.



Logical Partitions

Select LPAR to associate them to the Escala platform by clicking the corresponding checkbox.
Then, map each LPAR to a defined Bull System Manager host or choose to create a new.

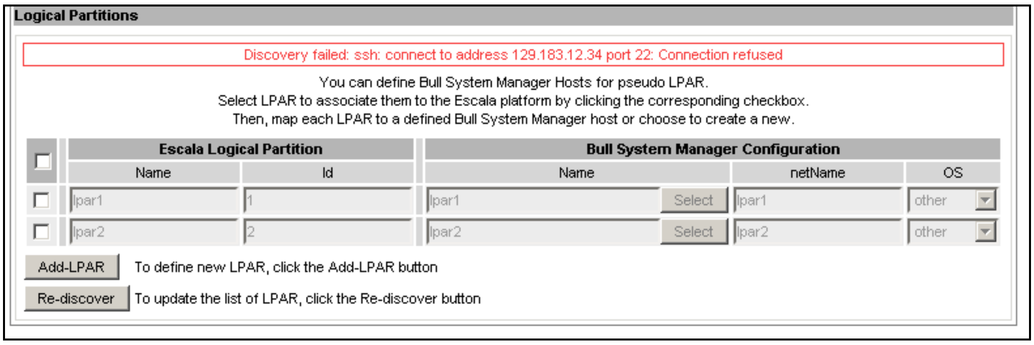
☑	Escala Logical Partition		Bull System Manager Configuration			
	Name	Id	Name		netName	OS
☑	galilei	2	galilei	Select	galilei	other
☑	tyrex	3	tyrex	Select	tyrex	other
☑	erable	4	erable	Select	erable	other
☑	peg3	5	peg3	Select	peg3	other
☑	essai	6	essai	Select	essai	other

To update the list of LPAR, click the Re-discover button

Figure 3-31. Logical Partitions display after Discover step

Notes

- When you select an already defined host, you cannot change its network name and OS. However, the **Select** option contains a Default option corresponding to the partition name, which can be edited.
- Only Linux and AIX Operating Systems are supported by logical partitions.
- If the partition name contains space(s), they are replaced by underscore(s) in the host label.
- If the remote access is not available, you can edit the Escala Logical Partition manually, as shown in the figure below. Beware, if remote access is not available, the supervision process will fail.
- If there is a discovery failure, look at the following messages:
  - `Permission denied (publickey,password,keyboard-interactive)`
    This message indicates an authentication problem. Verify that the public key is installed on the **Vio** Server or that the rights on the private key are correctly set.
  - `ssh: connect to host 192.168.207.50 port 22: Connection refused`
    This message means that **ssh** is not installed on the system hosting the manager.
  - `ssh:<host>: no address associated with name`
    This message indicates that the **netName** of the system hosting the manager is unknown.
  - `Discovery failed: Warning: Identity file .. not accessible`
    This message means that the identity file is not found. Check the contents of the **<BSM Installation Directory>/engine/etc/ssh** directory.



Logical Partitions

Discovery failed: ssh: connect to address 129.183.12.34 port 22: Connection refused

You can define Bull System Manager Hosts for pseudo LPAR.
Select LPAR to associate them to the Escala platform by clicking the corresponding checkbox.
Then, map each LPAR to a defined Bull System Manager host or choose to create a new.

□	Escala Logical Partition		Bull System Manager Configuration			
	Name	Id	Name		netName	OS
□	lpar1	1	lpar1	Select	lpar1	other
□	lpar2	2	lpar2	Select	lpar2	other

Add-LPAR To define new LPAR, click the Add-LPAR button

Re-discover To update the list of LPAR, click the Re-discover button

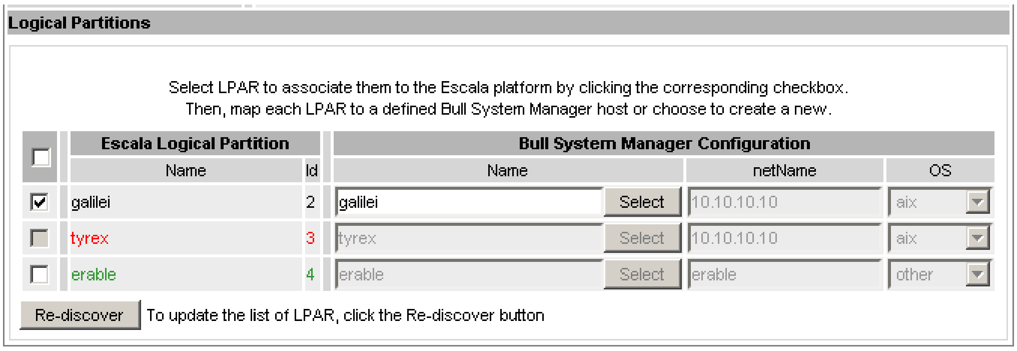
Figure 3-32. Logical Partitions displayed after Discovery failure

Logical Partitions Re-Discovery

Re-discovery is required to check that the Bull System Manager configuration still matches the manager configuration, in order to:

- Add a logical partition not yet registered in the Escala LPAR platform
- Remove logical partitions no longer defined in the manager configuration.

During the Re-discovery step, if the current configuration is not compatible with the manager configuration the invalid partitions are displayed in red, and the partitions not referenced in the current Bull System Manager configuration are displayed in green, as shown in the following figure:



Logical Partitions

Select LPAR to associate them to the Escala platform by clicking the corresponding checkbox.
Then, map each LPAR to a defined Bull System Manager host or choose to create a new.

□	Escala Logical Partition		Bull System Manager Configuration			
	Name	Id	Name		netName	OS
☑	galilei	2	galilei	Select	10.10.10.10	aix
□	tyrex	3	tyrex	Select	10.10.10.10	aix
□	erable	4	erable	Select	erable	other

Re-discover To update the list of LPAR, click the Re-discover button

Figure 3-33. Logical partition display after Re-discover step

Partitions no longer defined in the manager (in the example above, **`tyrex`**) are automatically unchecked and will be removed from the platform when the data is validated.

To add new partitions to the platform (**`erable`** in the example above), you must explicitly check it (see below).

Adding a logical partition to a platform

A logical partition is added by checking the corresponding line in the **Logical Partitions** part of the platform property window and setting the host characteristics in the BSM Configuration table (by filling in the corresponding fields or by selecting a host that is already defined).

Removing a logical partition from a platform

A logical partition is removed by unchecking the corresponding line in the Logical Partitions column for the platform.

Note Removing a logical partition does not delete the corresponding host object. It remains as a standalone LPAR. To delete it, edit the host by clicking the **LPAR** link.

Modify a logical partition defined in a platform

To modify the name of the BSM host corresponding to a logical partition, enter the new name in the corresponding field or select it from the list of hosts, already defined in Bull System Manager by clicking the **Select** button.
To modify other characteristics such as **netName** or **OS**, you must use the Host properties window.

Note To get the **Host** properties window corresponding to the logical partition, click the **Hostname** link displayed in the global platforms window.

Delete all logical partitions and corresponding hosts

To delete all logical partitions and corresponding hosts, use the **DeleteAll** button of the LPAR platform properties window. It is important to bear in mind that the Vios server and the platform will be also deleted from the Bull System Manager configuration.

Note When the server is managed by an HMC, additional information, such as partition type (**vioserver** or **aixlinux**) or proc mode (shared, dedicated, etc.) are displayed for the LPARs.

3.1.5 Defining Device Hosts

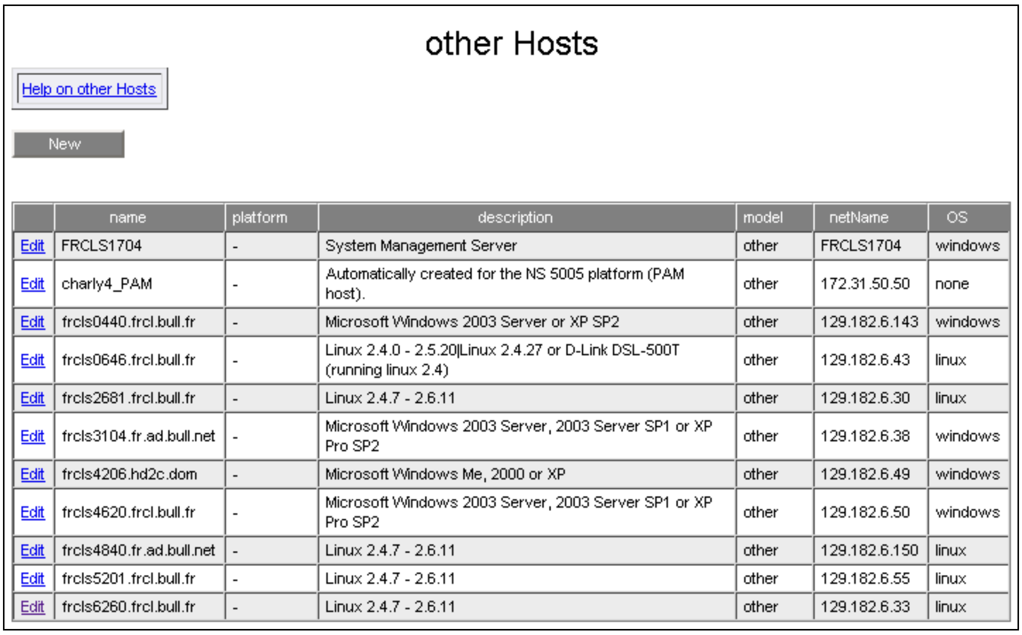
3.1.5.1 I/O Switch Modules

I/O Switch Modules are usually housed in the Blade Chassis and managed with the Chassis Monitoring Module (**CMM**). To configure modules, expand the **Device Hosts** menu and select the I/O Switch Modules menu item.

Procedures to create, modify or delete I/O Switch Modules are similar to those described for the NovaScale Blade (see *NovaScale Blade*, on page 42). The main difference is the model of the standalone server, which is set to **I/O Switch Module**.

3.1.6 Defining Other Hosts

To configure Hosts independently of the model, click the **Other Host** item. The list of configured hosts appears, as in the following example:



other Hosts

	name	platform	description	model	netName	OS
Edit	FRCLS1704	-	System Management Server	other	FRCLS1704	windows
Edit	charly4_PAM	-	Automatically created for the NS 5005 platform (PAM host).	other	172.31.50.50	none
Edit	frcls0440.frcl.bull.fr	-	Microsoft Windows 2003 Server or XP SP2	other	129.182.6.143	windows
Edit	frcls0646.frcl.bull.fr	-	Linux 2.4.0 - 2.5.20|Linux 2.4.27 or D-Link DSL-500T (running linux 2.4)	other	129.182.6.43	linux
Edit	frcls2681.frcl.bull.fr	-	Linux 2.4.7 - 2.6.11	other	129.182.6.30	linux
Edit	frcls3104.fr.ad.bull.net	-	Microsoft Windows 2003 Server, 2003 Server SP1 or XP Pro SP2	other	129.182.6.38	windows
Edit	frcls4206.hd2c.dom	-	Microsoft Windows Me, 2000 or XP	other	129.182.6.49	windows
Edit	frcls4620.frcl.bull.fr	-	Microsoft Windows 2003 Server, 2003 Server SP1 or XP Pro SP2	other	129.182.6.50	windows
Edit	frcls4840.fr.ad.bull.net	-	Linux 2.4.7 - 2.6.11	other	129.182.6.150	linux
Edit	frcls5201.frcl.bull.fr	-	Linux 2.4.7 - 2.6.11	other	129.182.6.55	linux
Edit	frcls6260.frcl.bull.fr	-	Linux 2.4.7 - 2.6.11	other	129.182.6.33	linux

Figure 3-34. Hosts configuration window

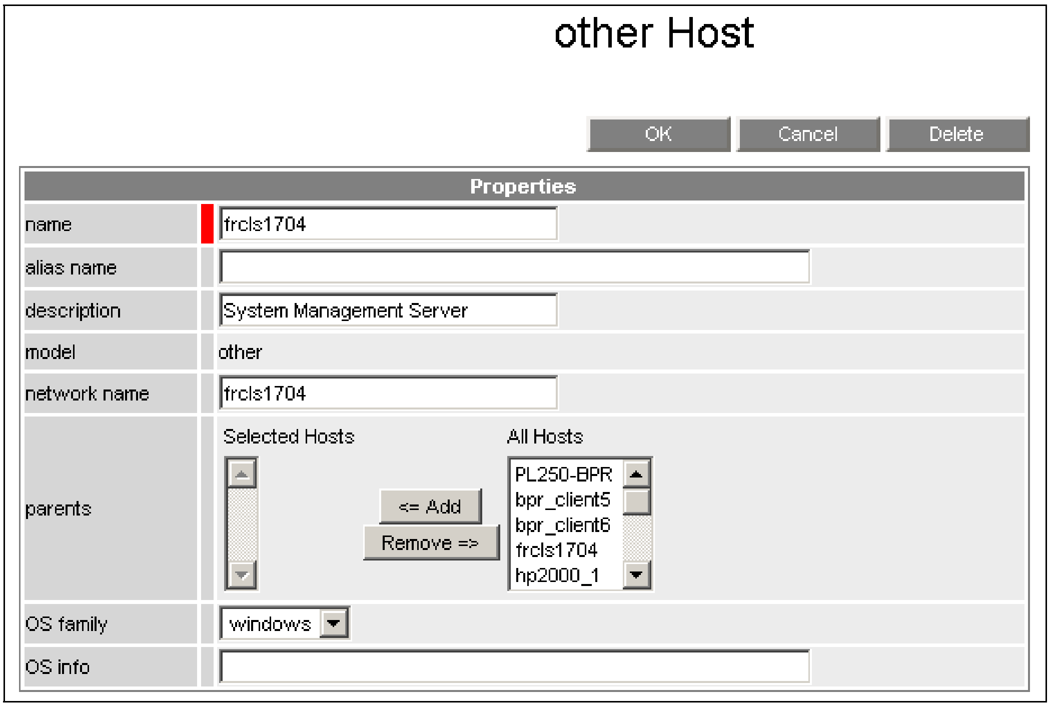
The table can be sorted by **name, netName, OS, model** or **description** properties by clicking the corresponding header. When a header is selected, an arrow indicates that the sort is made on this column. When you click the header again, the table is sorted in reverse order. If another header is selected, the entries are sorted by this property. Only one column can be selected as a sort criterion.

You can change host properties or delete hosts that are no longer to be monitored.

Note See *Create / Edit / Delete Resources*, on page 21 for details.

3.1.6.1 Host Properties

The following figure shows the window used to edit host properties.



name	frcls1704
alias name	
description	System Management Server
model	other
network name	frcls1704
parents	Selected Hosts: All Hosts: PL250-BPR, bpr_client5, bpr_client6, frcls1704, hp2000_1
OS family	windows
OS info	

Figure 3-35. Host properties

Host Properties	Description
name	Host short name (label). This name is the one displayed in the Bull System Manager Console views. Generally, this label is the host name. **Note:** In the configuration, the host name MUST be different from the following reserved keys: *****, **none** and **auto**. The name can be modified once the host is created, except if it is related to another BSM object.
alias name	Host alias name. This field allows to associate an additional name to the host. (reserved for future use)

Host Properties	Description
description	Description of the host. This description is displayed in an info tip in the Management Tree when you move the cursor over the node associated with the host.
model	This field is set according to the menu item (Other) and is not editable. The modification of the model is done by selecting the host when the details are edited for a specific model.
network name	Host network name (hostname or IP address). Default value: host name (label).
parents	List of hosts that link the host with remote hosts. For instance, a host representing a network equipment item(router, switch, etc.) is typically a parent host.
OS family	Operating System type (Windows, Linux, AIX, other, none). Default value: **other**.
OS info	When a host is discovered by **Discovery**, certain properties are set automatically. This is the case of **OS info**, which gives information about the OS running on the host. If **description** is empty, it is automatically set to the same value as **OS info**.

Table 3-6. Host properties

3.1.6.2 Example: Adding a Host

A frequent operation for a Bull System Manager user is to add new hosts to be monitored.

To perform this task, follow these steps:

Step 1: Install the Bull System Manager agent on the host that you want to monitor.

Step 2: Start Bull System Manager configuration window.

Step 3: Declare the new host.

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

Step 1: Install the Management Agent on the New Host to Monitor

Follow the same procedure as the one used to install the Monitoring Agent on the Bull System Manager server. You can either use the CD-ROM or download the software by connecting to the Bull System Manager server home page, as follows:

1. Launch the web browser with the Bull System Manager home page URL:
   `http://<Bull System Manager server>/BSM/`

2. Select **Download** and then follow the instructions.

Step 2: Start Bull System Manager Configuration

See *Starting the Configuration GUI*, on page 11.

Step 3: Declare the New Host

By default, the **Topology** tab is selected in the banner. If not, click **Topology**.

Expand the **Other series** menu under Host Definition, select the **Other Hosts** item and click the **New** button to display the form for declaring a host.

Note You can also let Bull System Manager Configuration discover hosts by specifying an IP address range.

Let us suppose that you want to add a Linux host named`frcls2681.frcl.bull.fr`. Enter the following parameters:

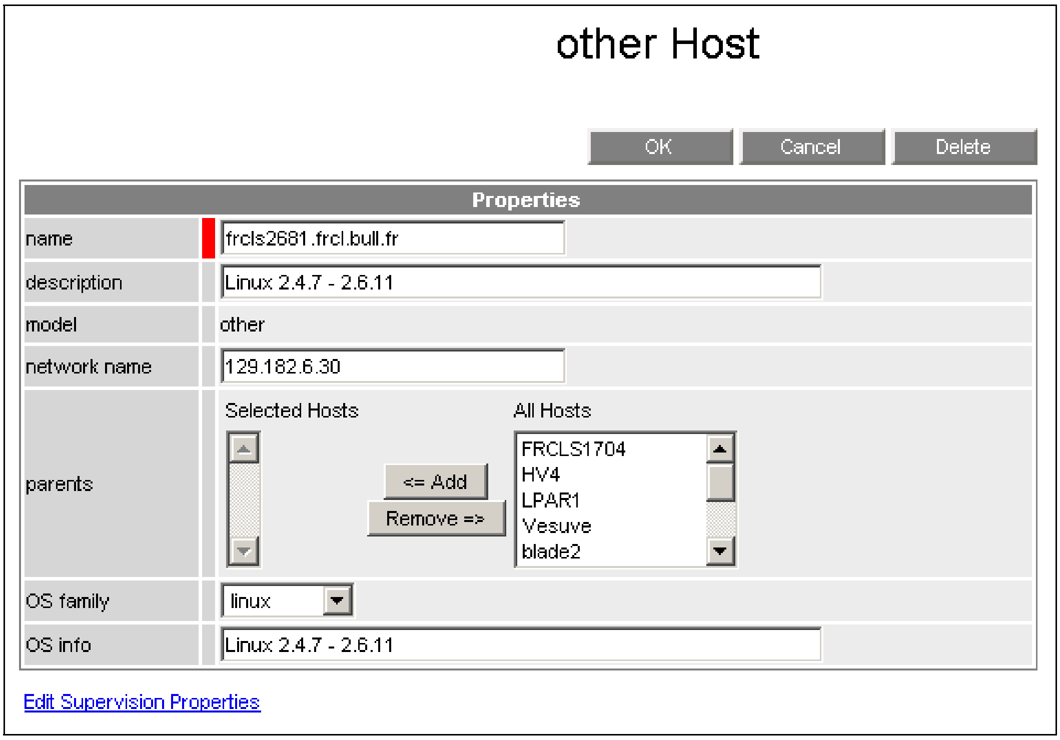
name A label used to identify the host in Bull System Manager, `FRCLS2681` in the example.

description Short text describing the host, `Linux server` in the example.

network name Host identification on the LAN (name or IP address), `frcls2681.frcl.bull.fr` in the example.

OS family Host Operating System, **Linux** in the example.

Once completed, the window will appear as below:



other Host

Properties	
name	frcls2681.frcl.bull.fr
description	Linux 2.4.7 - 2.6.11
model	other
network name	129.182.6.30
parents	Selected Hosts: All Hosts: FRCLS1704, HV4, LPAR1, Vesuve, blade2
OS family	linux
OS info	Linux 2.4.7 - 2.6.11

Figure 3-36. Window for declaring a host

Click **OK** to validate.

The `frcls2681.frcl.bull.fr` host is now in the Hosts list.

Step 4: Save and Reload

Click the **Save & Reload** button to apply the modification to the server part.

3.2 Configuring Hostgroups

The Hostgroup allows you to structure a set of hosts (**host members**) and/or hostgroups (hostgroups member). This set can be displayed in the **Hostgroups** view in the Bull System Manager console.

the **BSM** Hostgroup, containing the Bull System Manager server, is created at installation time.

The Administrator can:

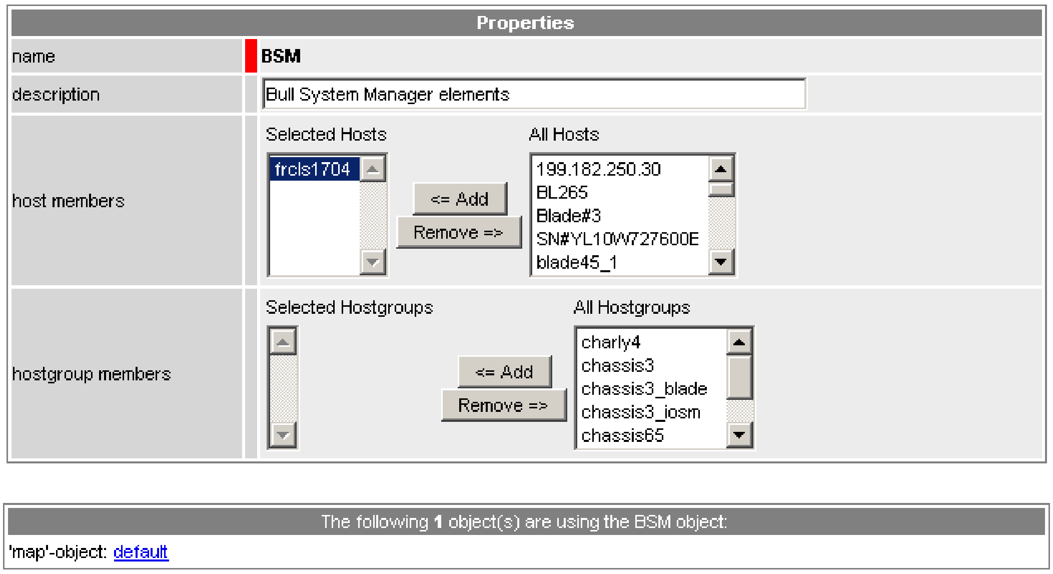
- Specify new Hostgroups
- Change the properties of an already defined Hostgroup
- Delete a Hostgroup that is no longer to be monitored.

3.2.1 Hostgroups

To configure Hostgroups, click the **Hostgroups** link in the **Groups Definition** part of the **Topology** tab.

The way to create a new Hostgroup and to edit or delete a Hostgroup is described in *Create / Edit / Delete Resources*, on page 21.

The following figure shows the Hostgroup properties editing window.



Properties

name	**BSM**
description	Bull System Manager elements
host members	Selected Hosts: frcls1704 All Hosts: 199.182.250.30, BL265, Blade#3, SN#YL10W727600E, blade45_1
hostgroup members	Selected Hostgroups: All Hostgroups: charly4, chassis3, chassis3_blade, chassis3_iosm, chassis65

The following **1** object(s) are using the BSM object:

'map'-object: default

Figure 3-37. Hostgroup properties

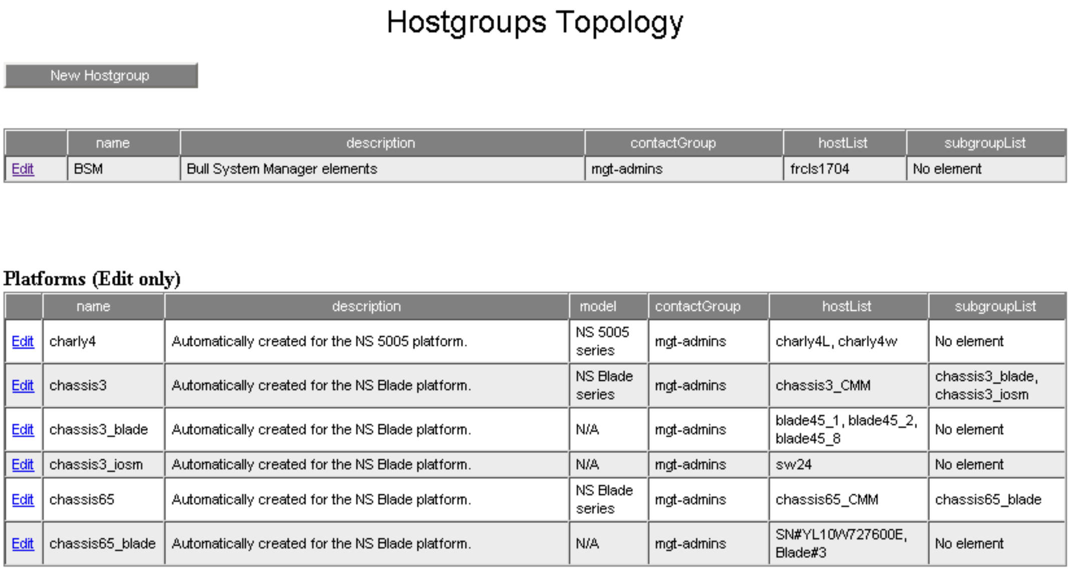
Hostgroup Properties	Description
name	Hostgroup name. This name is seen in the Hostgroups view.
description	Resource description. This description is displayed in an info tip in the Management Tree when you move the cursor over the node associated with this resource.
host members	List of hosts associated with this hostgroup. Hosts are selected in the **All Hosts** list and moved to the **Selected Hosts** list using the **Add** button, and removed using the **Remove** button.
hostgroup members	List of hostgroups associated with this hostgroup. Hostgroups are selected in the **All Hostgroups** list and moved to the **Selected Hostgroups** list using the **Add** button, and removed using the **Remove** button.

Note Ensure that the same resource is not selected twice in the **Selected Objects** list. If so, select one occurrence of the resource and click **Remove**.

3.2.2 Platforms

Particular hostgroups are defined to represent hardware platforms or virtualization platforms. The platform type is represented by an additional hostgroup attribute, the `model` attribute.

They appear in a specific table in the Hostgroups window, as shown below:



Hostgroups Topology

	name	description	contactGroup	hostList	subgroupList
Edit	BSM	Bull System Manager elements	mgt-admins	frcls1704	No element

Platforms (Edit only)

	name	description	model	contactGroup	hostList	subgroupList
Edit	charly4	Automatically created for the NS 5005 platform.	NS 5005 series	mgt-admins	charly4L, charly4w	No element
Edit	chassis3	Automatically created for the NS Blade platform.	NS Blade series	mgt-admins	chassis3_CMM	chassis3_blade, chassis3_iosm
Edit	chassis3_blade	Automatically created for the NS Blade platform.	N/A	mgt-admins	blade45_1, blade45_2, blade45_8	No element
Edit	chassis3_iosm	Automatically created for the NS Blade platform.	N/A	mgt-admins	sw24	No element
Edit	chassis65	Automatically created for the NS Blade platform.	NS Blade series	mgt-admins	chassis65_CMM	chassis65_blade
Edit	chassis65_blade	Automatically created for the NS Blade platform.	N/A	mgt-admins	SN#YL10W727600E, Blade#3	No element

Figure 3-38. Hostgroups

Note The platform cannot be created from the Hostgroup page. It can only be created from **Host Definition** when the selected item corresponds to a host associated with a physical or virtualization platform.

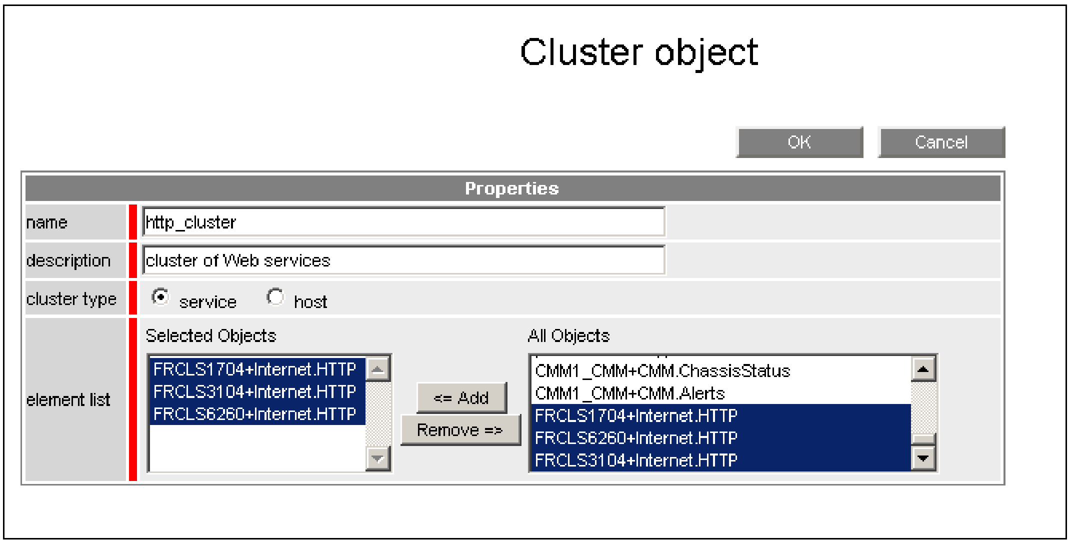
3.3 Configuring Clusters

A cluster is either a set of hosts or a set of services. This cluster object generates a **Nagios** service inside a category. It is used to manage the global status of redundant objects such as web services. If a certain number of objects have an OK status, the global function has an OK status.

A monitoring rule is attached to a cluster:

- If the number of non-OK elements is greater than a warning threshold, the cluster status is **WARNING**
- If the number of non-OK elements is greater than a critical threshold, the cluster status is **CRITICAL**
- Else, the cluster status is **OK**.

The configuration of a cluster is divided into two operations: first you specify the cluster in the **Topology** context (Figure 3-39), then you add monitoring attributes (for example thresholds and the hosted category where this cluster service is displayed) in the **Supervision** context (Figure 3-40).

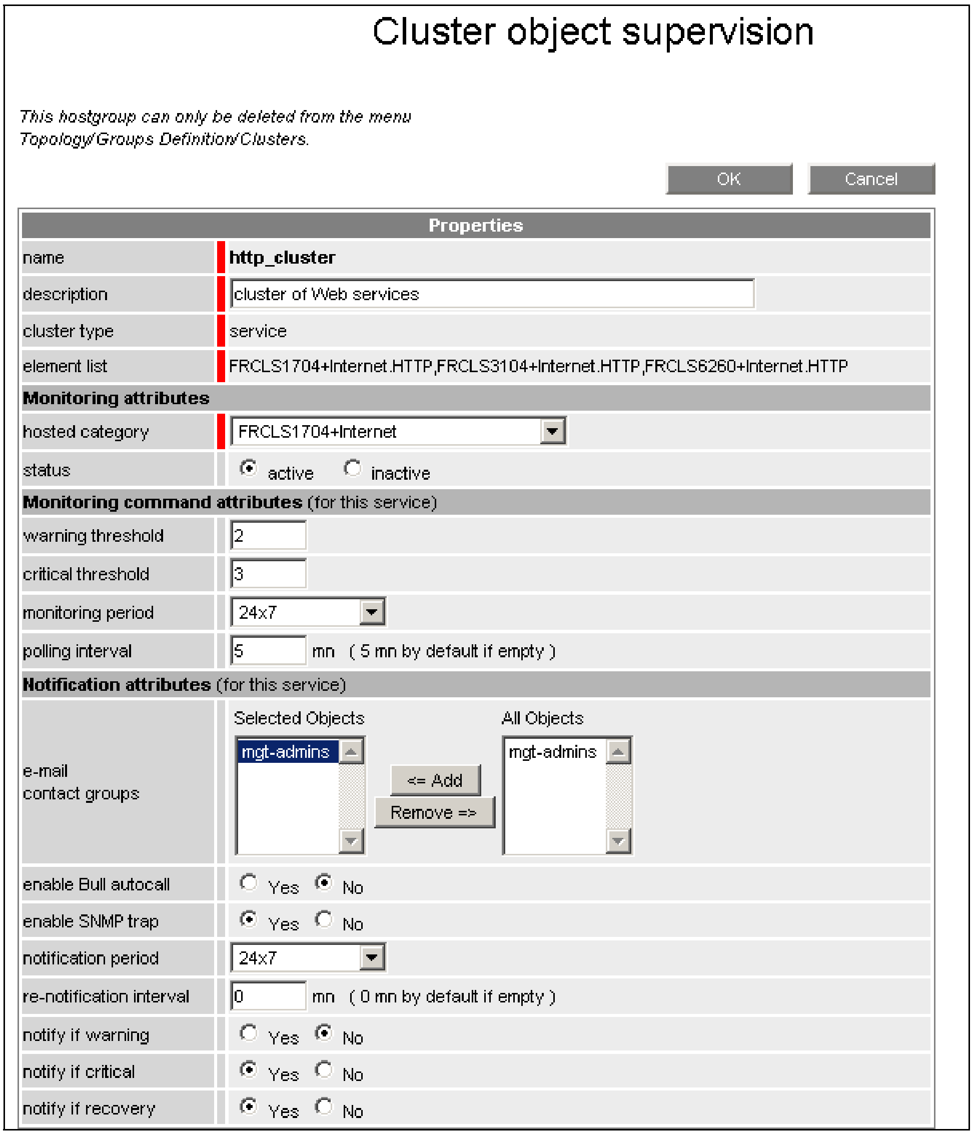


Cluster object

Properties

name	http_cluster
description	cluster of Web services
cluster type	● service ○ host
element list	Selected Objects: FRCLS1704+Internet.HTTP FRCLS3104+Internet.HTTP FRCLS6260+Internet.HTTP All Objects: CMM1_CMM+CMM.ChassisStatus CMM1_CMM+CMM.Alerts FRCLS1704+Internet.HTTP FRCLS6260+Internet.HTTP FRCLS3104+Internet.HTTP

Figure 3-39. Defining Cluster object



Cluster object supervision

This hostgroup can only be deleted from the menu Topology/Groups Definition/Clusters.

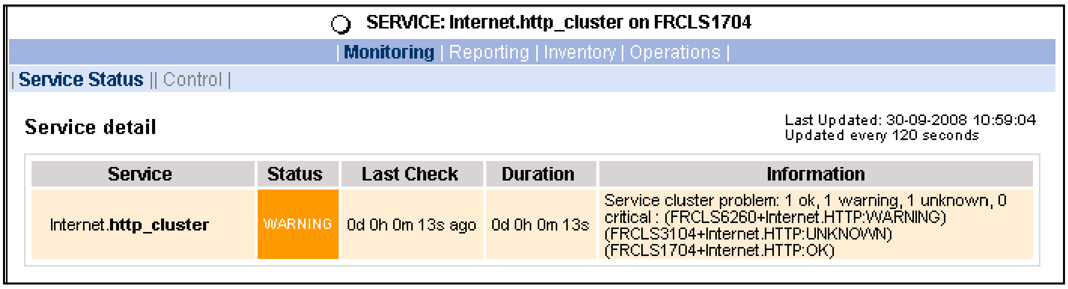
Properties	
name	**http_cluster**
description	cluster of Web services
cluster type	service
element list	FRCLS1704+Internet.HTTP,FRCLS3104+Internet.HTTP,FRCLS6260+Internet.HTTP
Monitoring attributes	
hosted category	FRCLS1704+Internet
status	● active ○ inactive
Monitoring command attributes (for this service)	
warning threshold	2
critical threshold	3
monitoring period	24x7
polling interval	5 mn (5 mn by default if empty)
Notification attributes (for this service)	
e-mail contact groups	Selected Objects: mgt-admins All Objects: mgt-admins
enable Bull autocall	○ Yes ● No
enable SNMP trap	● Yes ○ No
notification period	24x7
re-notification interval	0 mn (0 mn by default if empty)
notify if warning	○ Yes ● No
notify if critical	● Yes ○ No
notify if recovery	● Yes ○ No

Figure 3-40. Defining Cluster object supervision

Cluster Properties	Description
name	Cluster name.
description	Description of the resource. This description is displayed in an info tip in the Management Tree when you move the cursor over the node associated with this resource.
element list	List of the host or service elements. The resources are selected in the **All Objects** list and moved to the **Selected Objects** list using the **Add** button, and removed using the **Remove** button.
hosted_category	The category and the host where the cluster is managed.
warning_threshold	If the number of non-OK elements is greater or equal to this threshold, the cluster status is WARNING
critical_threshold	If the number of non-OK elements is greater or equal to this threshold, the cluster status is CRITICAL

Table 3-7. Cluster properties

The following appears in the cluster:



SERVICE: Internet.http_cluster on FRCLS1704

| Monitoring | Reporting | Inventory | Operations |
| Service Status || Control |

Service detail

Last Updated: 30-09-2008 10:59:04
Updated every 120 seconds

Service	Status	Last Check	Duration	Information
Internet.**http_cluster**	WARNING	0d 0h 0m 13s ago	0d 0h 0m 13s	Service cluster problem: 1 ok, 1 warning, 1 unknown, 0 critical : (FRCLS6260+Internet.HTTP:WARNING) (FRCLS3104+Internet.HTTP:UNKNOWN) (FRCLS1704+Internet.HTTP:OK)

Figure 3-41. Cluster supervision

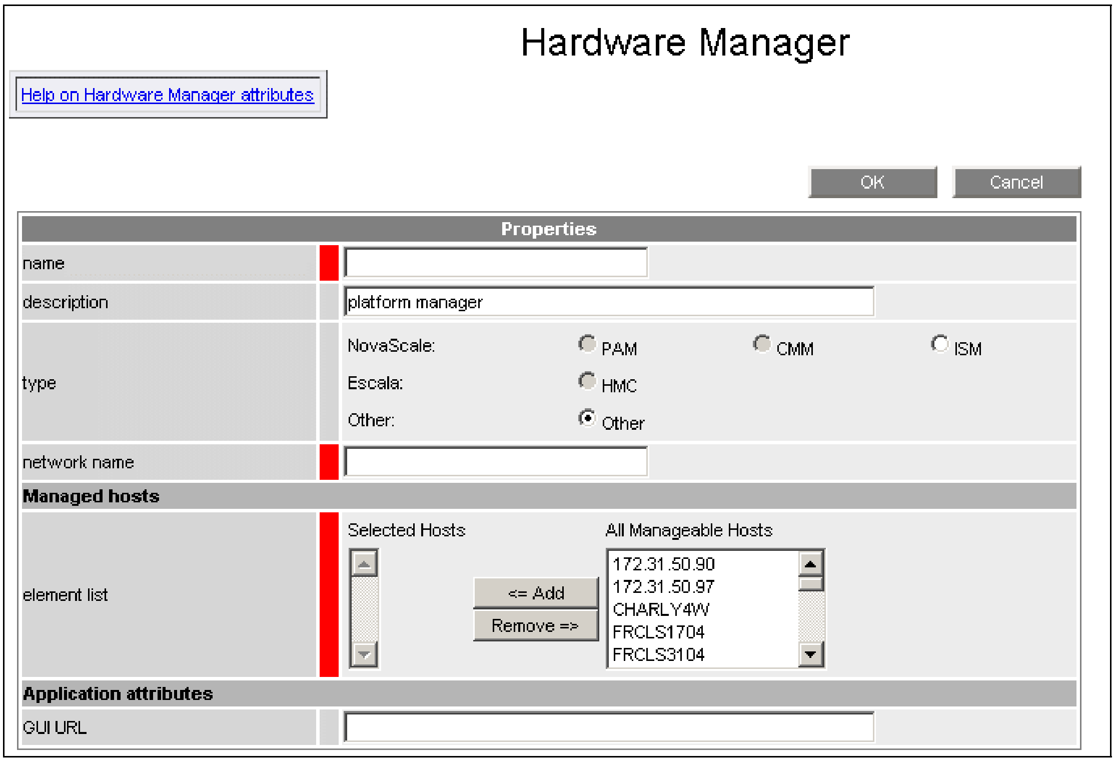
3.4 Configuring a Hardware Manager

This chapter explains how to define a hardware manager for a Bull System Manager configuration. A hardware manager is an application that manages host and platform hardware.

As administrator, you can specify hardware managers for the hosts and platforms defined in the configuration, change their properties, or delete them if the hardware is no longer to be monitored.

3.4.1 Editing Properties

To configure the Hardware Manager, click the **Hardware** link in the **Managers View** part of the **Topology** tab. The way to create, edit or delete a manager is described in *Create / Edit / Delete Resources*, on page 21. The following figure shows the edit window for Hardware Manager properties.



Properties	
name	
description	platform manager
type	NovaScale: ○ PAM ○ CMM ○ ISM Escala: ○ HMC Other: ● Other
network name	
Managed hosts	
element list	Selected Hosts All Manageable Hosts: 172.31.50.90, 172.31.50.97, CHARLY4W, FRCLS1704, FRCLS3104
Application attributes	
GUI URL	

Figure 3-42. Hardware manager properties

Note The platform hardware manager (PAM, CMM) and the Escala hardware manager (HMC) cannot be created from the Hardware Manager properties window. It can be edited only from the **Host Definition** when the selected item corresponds to a host associated with the corresponding model.

Hardware Manager Properties	Description
name	Hardware manager name. This name is seen in the Console Managers view.
description	Description of the resource. This description is displayed in an info tip in the Management Tree when the cursor is moved over the node associated with this resource.
type	Type of manager (PAM, CMM, ISM, HMC or other).
network name	Manager network name or IP address. Default value: the manager name (label).
element list	Elements that this manager will have to manage. For editable manager (ISM or other), these elements are selected in the All Objects list and moved to the Selected Objects list using the **Add** button, and removed using the **Remove** button. Depending on the type of manager, the All Resources list contains: • All NovaScale 5000 & 6000 series platforms if the manager type is **PAM**, • All NS Blade Chassis if the manager type is **CMM**, • All NovaScale 4000 series hosts if the manager type is **ISM**, • All Escala PL series server if **HMC**, • All hosts if the manager type is **other**.

Table 3-8. Hardware manager properties

Note Properties differ according to the selected hardware manager. Consequently, the window displayed will differ.

Specific PAM Properties

user, password	Authentication information (login, password) used by Bull System Manager to access the manager.

Specific ISM Properties

OS family	Operating System type (Windows, Linux,) of the host on which the Hardware manager is running. Default value: **linux**.
user, password	Authentication information (login, password) used by Bull System Manager to access the manager.

Specific CMM Properties

SNMP port	Port of the SNMP agent used to get information about the CMM configuration. Default value: *161.*
SNMP community	SNMP Community used in the SNMP request to identify the Bull System Manager server. Default value: *public.*

Other Properties

GUI URL	HTTP URL of the manager GUI.

3.5 Configuring a Storage Manager

This section explains how to define a storage manager in a Bull System Manager configuration. A storage manager is an application that manages storage for a single host or storage shared by a set of hosts as a SAN.

As administrator, you can specify storage managers for the hosts defined in the configuration, change their properties, or delete them if the storage is no longer to be monitored.

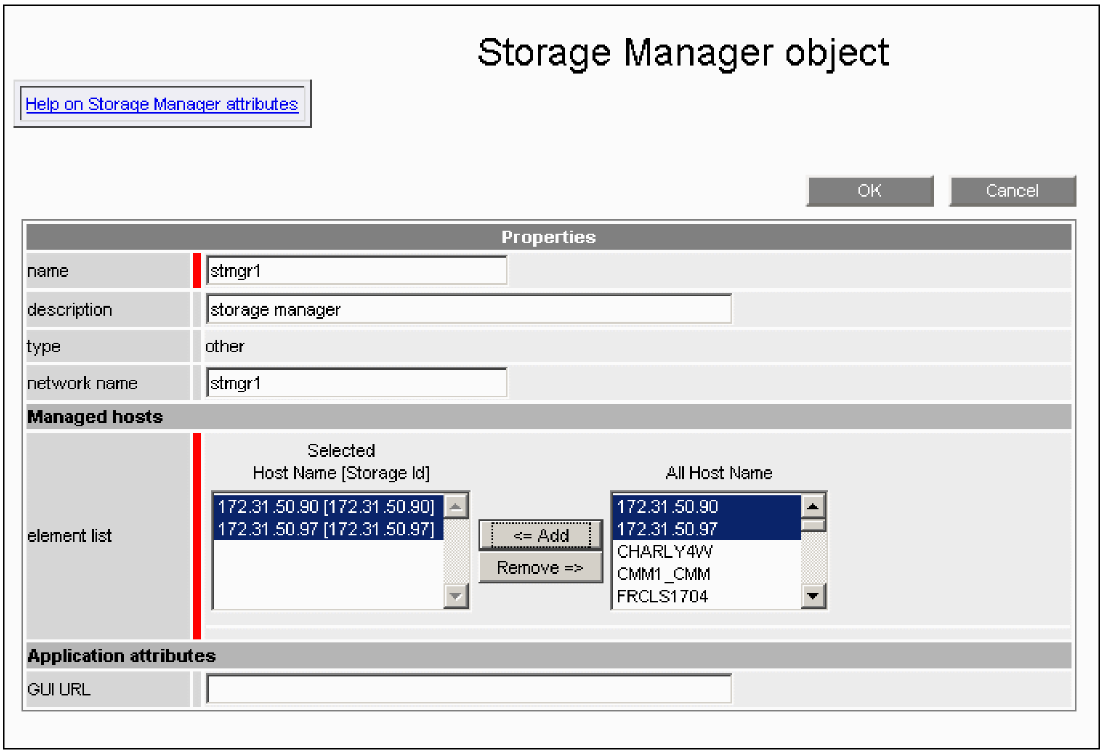
In the current release, no storage system is fully supported by Bull System Manager Server. It is possible to configure other storage managers with limited functions. To extend storage supervision, you must install specific storage Add-ons (see the *Server Add-ons Administration and Installation Guide* to get detailed information).

3.5.1 Editing Properties

To configure the Storage Manager click the **Storage** link in the **Managers** part of the **Topology** tab.

The way to create, edit or delete a manager is described in 2.6.1 *Create / Edit / Delete Resources*, on page 21.

The following figure shows the Storage Manager properties window.



Storage Manager object

Help on Storage Manager attributes

Properties	
name	stmgr1
description	storage manager
type	other
network name	stmgr1
Managed hosts	
element list	Selected Host Name [Storage Id]: 172.31.50.90 [172.31.50.90] 172.31.50.97 [172.31.50.97] All Host Name: 172.31.50.90 172.31.50.97 CHARLY4W CMM1_CMM FRCLS1704
Application attributes	
GUI URL	

Figure 3-43. Storage manager properties

Storage Manager Properties	Description
name	Storage manager name. This name is seen in the Console Managers view.
description	Description of the resource. This description is displayed in an info tip in the Management Tree when the cursor is moved over the node associated with this resource.
type	Type of manager (other).
network name	Manager network name or IP address. Default value: the manager name (label).
element list	Elements that this manager will manage. These elements are selected in the All Host Name list and moved to the Selected Host Name list using the Add button, and removed using the Remove button. Note: Any Host declared in the Bull System Manager configuration can be managed by a storage manager, but a single host can only be managed by one manager.
GUI URL	HTTP URL of the manager GUI.

Table 3-9. Storage manager properties

3.6 Configuring a Virtualization Manager

This section explains how to define a virtualization manager in a Bull System Manager configuration. A virtualization manager is an element that manages virtual machine.

As administrator, you can specify virtualization managers for the hosts defined in the configuration, change their properties, or delete them if virtualization is no longer to be monitored.

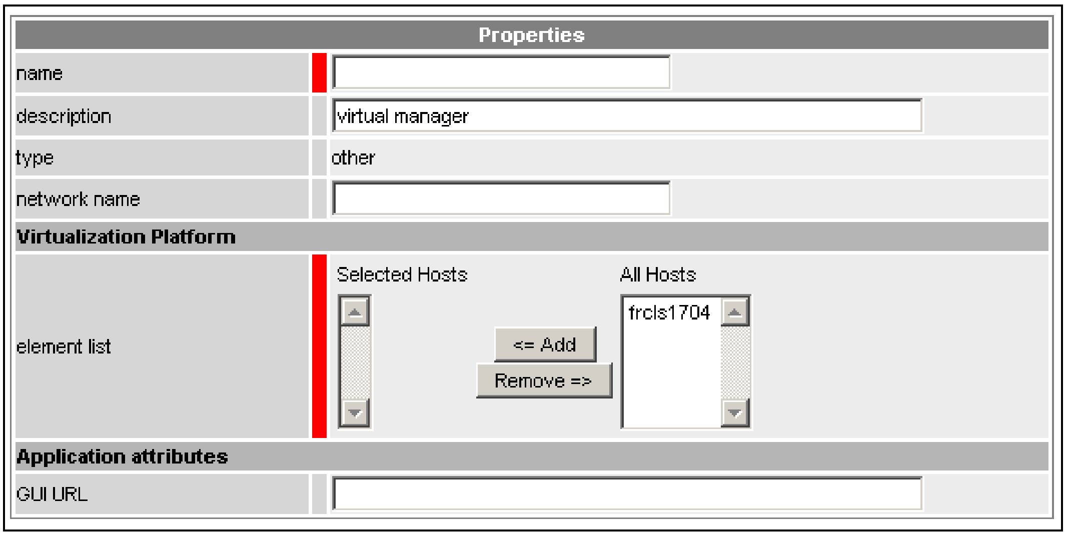
In the current release, no virtualization system is fully supported by Bull System Manager Server. It is possible to configure other virtualization managers with limited functions. To extend virtualization supervision, you must install specific virtualization Add-ons (see the *Server Add-ons Administration and Installation Guide* to get detailed information).

3.6.1 Editing Properties

To configure the Virtualization Manager, click the **Virtualization** link in the **Managers** part of the **Topology** tab.

The way to create, edit or delete a manager is described in *Create / Edit / Delete Resources*, on page 21.

The following figure shows the window displayed to edit Virtualization Manager properties.



Properties

name	
description	virtual manager
type	other
network name	

Virtualization Platform

element list	Selected Hosts	All Hosts frcls1704

Application attributes

GUI URL	

Figure 3-44. Virtualization Manager properties

Virtualization Manager Properties	Description
name	Manager name. This name is seen in the Console Managers view.
description	Description of the resource. This description is displayed in an info tip in the Management Tree when the cursor is moved over the node associated with this resource.
type	Type of manager (other).
network name	Manager network name or IP address. Default value: the manager name (label).
element list	Elements that this manager will manage. These elements are selected in the All Host Name list and moved to the Selected Host Name list using the Add button, and removed using the Remove button. **Note:** Any Host declared in the Bull System Manager configuration can be managed by a virtualization manager, but a single host can only be managed by one manager.
GUI URL	HTTP URL of the manager GUI.

Table 3-10. Virtualization Manager properties

Chapter 4. Configuring Inventory

This chapter explains how to setup the **Inventory** functions in the Bull System Manager configuration.

For the host, no specific configuration is required for the Inventory but:

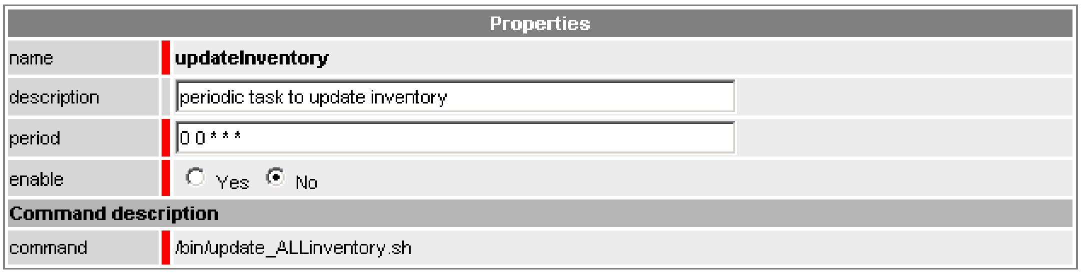
- the host must be defined with a supported Operating System (AIX, Linux or Windows)
- a BSM agent must be installed on the host
- the host must be able to contact the BSM Server. For this feature, see *Configuring BSM Server* on page 195.

The Host inventory is updated when the host is defined in the **BSM** configuration and when the host reboots. To schedule a regular update of the inventory, you can enable the **updateInventory** task.

To enable **updateInventory**:

1. Click the **Periodic Tasks** link in the **Functionalities** part of the **GlobalSetting** tab.

2. Click the **Edit** link of the **updateInventory** task. Its list of properties appear:



Properties

name	**updateInventory**
description	periodic task to update inventory
period	0 0 * * *
enable	○ Yes ● No

Command description

command	/bin/update_ALLinventory.sh

Figure 4-1. updateInventory periodic task properties

- – Modify the period if needed:
  - The periodicity is defined in five fields as standard **cron** format: <minute(0-59)> <hour(0-23)> <day of month(0-31)> < month(0-12) or names> <day of week(1-7) or name>".
  - A field may be an asterisk (*), which always stands for **first-last**: for instance **00 22 * * *** corresponds to a daily execution at 22 h.
  - A range or a list of numbers is allowed: for instance **8-11** in hour field specifies execution at 8, 9, 10 and 11 hours.
  - Steps can be used in conjunction with ranges or after an asterisk: for instance ***/5** in the minute field specifies an execution every five minutes.

  See *CRON Reference Manual* to get detailed information.

  By default, the task is scheduled daily at 00:00.
- – Enable the task. By default, the task is disabled.
- – Click **OK** to validate.

Chapter 5. Configuring Supervision

This chapter explains how to setup the monitoring functions that will control the resources in the Bull System Manager configuration.

Note The following characters are not supported in any text field:

```
[] brackets,
= equal sign,
; semicolon
“ commas (only accepted in the check parameters of a Service Object)
```

5.1 Configuring Categories and Services

Bull System Manager delivers default monitoring categories and services. These categories and services depend on the Operating System running on the host or on its model:

- Services for Windows hosts will be applied to all hosts with a Windows operating system
- Services for Linux hosts will be applied to all hosts with a Linux operating system
- Services for AIX hosts will be applied to all hosts with an AIX operating system
- Services for hosts, independent of the operating system, will be applied to all hosts
- Services for hardware elements will be applied to all hosts with managed hardware
- Services for storage elements will be applied to all hosts with managed storage.

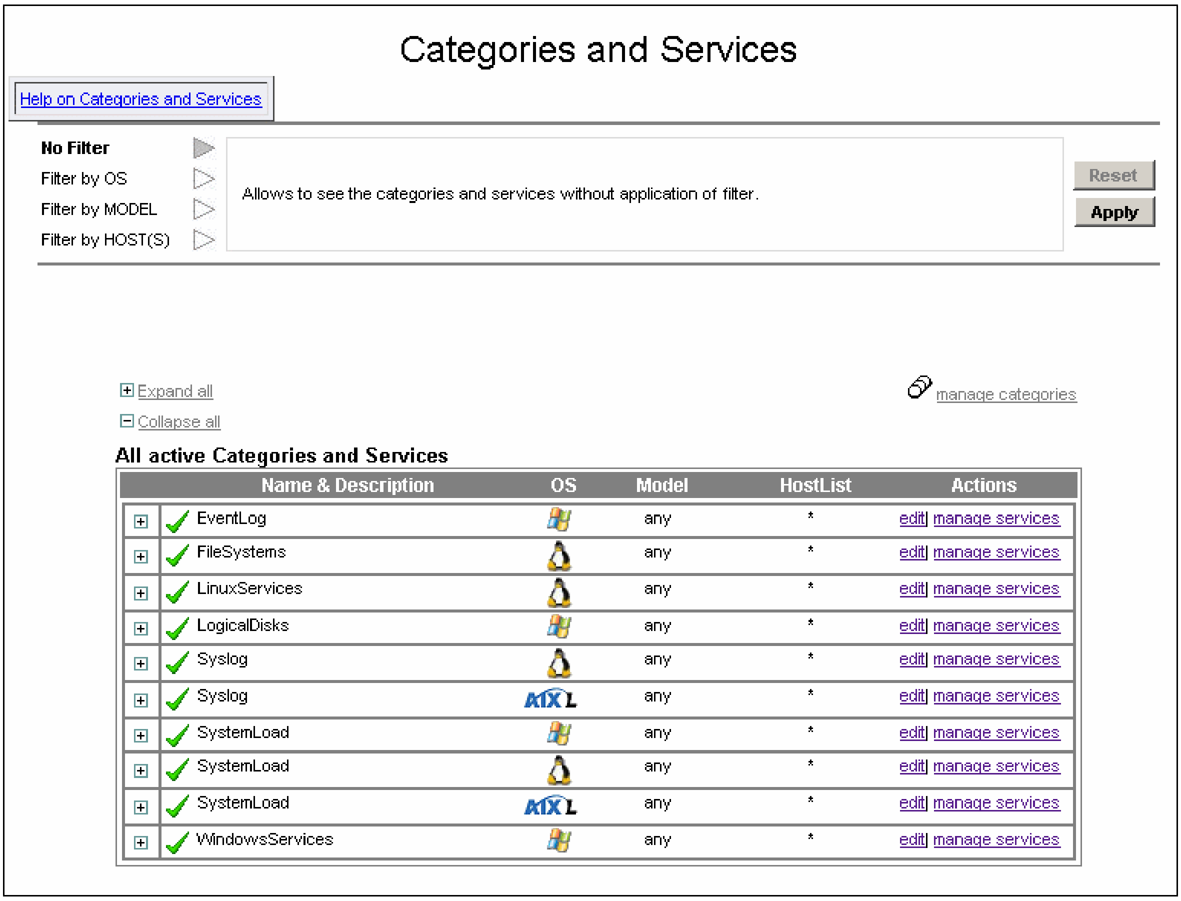
Besides these default categories and services, Bull System Manager provides some templates of categories and services that, as administrator, you may customize to monitor other host elements.

The administrator can change the default-monitoring configuration by:

- **Customizing services**, to modify thresholds and monitoring properties, or to modify the list of monitored hosts.
- **Customizing categories,** to restrict monitoring of a whole category to a list of hosts.
- **Adding a service from a service template**, to define new monitored elements (for instance, to monitor a specific logical drive on a Windows system, you can clone the C service and modify the check command parameters), or if you want to create one or more occurrences of this service with the same name. Each occurrence can have a different host list and different monitoring properties.
- **Adding a category from an unused category template**, to activate some unused category templates with their services.
- **Creating a new service,** if no service template meets your requirement.
- **Creating a category,** to assign a set of cloned services to this category.

Note The categories and services related to Hardware or Storage supervision are automatically generated for each host concerned by the BSM Configuration **Hosts Definition** part. There is no template for these categories and services, which are represented by the ⚙ icon (see *Generated Categories and Services* on page 213*)*.

To display the set of used categories and services click the **Categories/Services** link in the **Supervision** tab. The following page is displayed:



Categories and Services

Help on Categories and Services

No Filter ▶
Filter by OS ▷
Filter by MODEL ▷
Filter by HOST(S) ▷

Allows to see the categories and services without application of filter.

Reset

Apply

⊞ Expand all

⊟ Collapse all

manage categories

All active Categories and Services

		Name & Description	OS	Model	HostList	Actions
⊞	✓	EventLog	🪟	any	*	edit| manage services
⊞	✓	FileSystems	🐧	any	*	edit| manage services
⊞	✓	LinuxServices	🐧	any	*	edit| manage services
⊞	✓	LogicalDisks	🪟	any	*	edit| manage services
⊞	✓	Syslog	🐧	any	*	edit| manage services
⊞	✓	Syslog	AIX L	any	*	edit| manage services
⊞	✓	SystemLoad	🪟	any	*	edit| manage services
⊞	✓	SystemLoad	🐧	any	*	edit| manage services
⊞	✓	SystemLoad	AIX L	any	*	edit| manage services
⊞	✓	WindowsServices	🪟	any	*	edit| manage services

Figure 5-1. Categories and services page

This page is divided into two parts:

- The **filter** part, allows the user to refine the configuration according to three different criteria: the OS, the model, and the host list:
  - **No filter** : no filter is applied.
  - **Filter by OS** : filters the Categories and Services according to the Operating System.
  - **Filter by MODEL** : filters the Categories and Services according to the models.
  - **Filter by HOST(S)**: filters the Categories and Services according to the names of the machines.
- The **All active Categories and Services** table allows you to visualize and manage (customize, add and create) categories and services.

5.1.1 Categories

5.1.1.1 Default Categories

Bull System Manager provides the following default categories:

Unused template categories

- Internet
- Reporting
- Network

Categories related to hardware or software supervision (automatically generated if needed)

- Hardware
- PAM (for PAM manager)
- CMM (for CMM manager)
- Storage
- Power

Default categories applied to Windows hosts

- LogicalDisks
- EventLog
- WindowsServices
- SystemLoad
- Disks
- NetworkAdaptors

Default categories applied to Linux hosts

- FileSystems
- Syslog
- LinuxServices
- SystemLoad
- HDisks

Default categories applied to AIX hosts

- FileSystems
- Syslog
- AIXServices
- SystemLoad

Note A category can be present in all Operating Systems (example of the **SystemLoad** category) but it actually represents three distinct categories.

Automatically generated categories are represented by the ⚙ icon (see *Generated Categories and Services* on page 213).

5.1.1.2 Category Properties

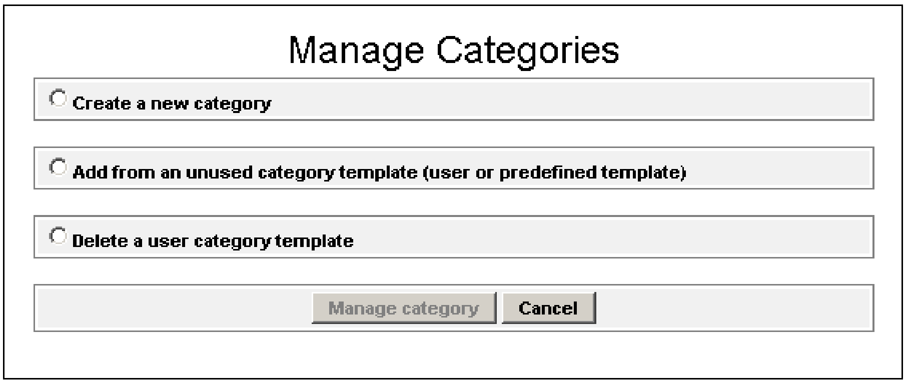
Category Properties	Description
Name	Category name
description	Category description
Model	Supported host model to which the category can apply. Default value: **any**.
OS family	Operating system type (Windows, Linux, AIX, any) Default value: **any**.
Monitoring domain	The monitoring domain of the category (Operating System, Hardware, Storage, Virtualization, etc., none). Default value: **none**. NB: The value **none** means that the category does not belong to a specific domain. BSM will not generate service group none that would contain the category.
host list expression	List of hosts to which the category will apply. The host list expression can be defined as follows: • *: all configured hosts with an Operating System corresponding to the **OS family** or **model** categories. • **none:** no host. • a list of host names separated by a comma to exclude other configured hosts. Example: `host1,host2,host3`. • a list of host names separated by a comma and prefixed by "!" to exclude these hosts. Example: `!host1,!host2,!host3`.

Notes

- The host list expression of a category is always a subset of the configured hosts. A host list MUST NOT mix the **not (!) hosts** list with other types of expressions (**hosts list, none** or *). For instance, the expression `!h1,h2,h3` is ambiguous and is forbidden.
- The categories linked to hardware or storage management are automatically generated and cannot be edited with the category form.
- The **Monitoring** category domain property is used when you want to disable a monitoring domain for a host or a Hostgroup (see *Example: Monitoring NS 4000 Hardware* on page 131).

5.1.1.3 Creating a new Category

To create a new category, click the **manage categories** link. Then, in the **Manage Categories** popup window (Figure 5-2), check **Create a new category** and click the **Create a new category** button. A new window is used to edit the category properties (Figure 5-3).



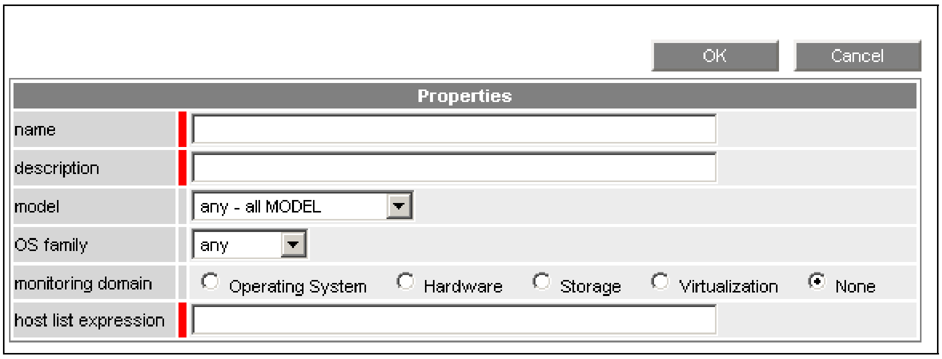
Manage Categories

○ Create a new category

○ Add from an unused category template (user or predefined template)

○ Delete a user category template

Figure 5-2. Manage Categories popup



name	
description	
model	any - all MODEL
OS family	any
monitoring domain	○ Operating System ○ Hardware ○ Storage ○ Virtualization ● None
host list expression	

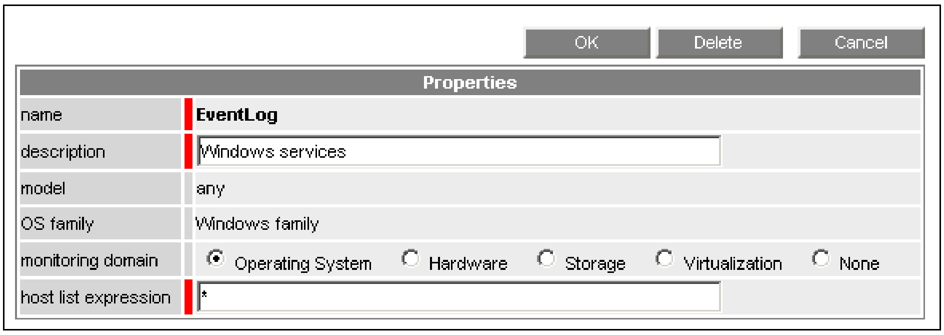
Figure 5-3. Category properties window

Note According to the filter, some text fields are already filled in and are not editable. For example, if filter by OS has been selected, the **OS family** field is filled in and is not editable.

Click **OK** to validate. This will create a new category with its model.

5.1.1.4 Customizing a Category

To customize a category, click the **edit** link for this category. A new window allows you to customize the description, the monitoring domain and the host list. The other text fields are not editable because these attributes are used for category identification.



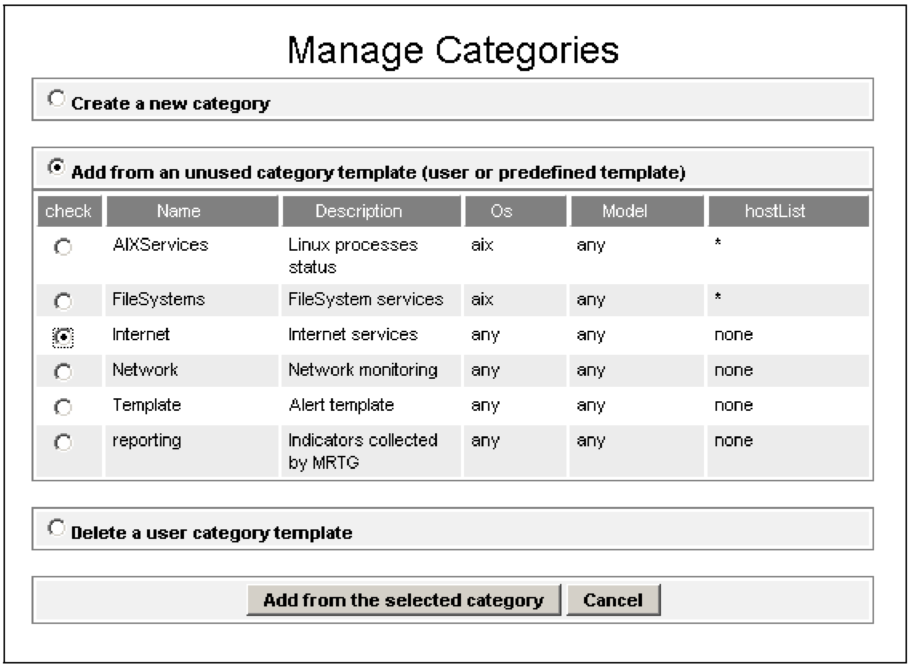
Properties	
name	**EventLog**
description	Windows services
model	any
OS family	Windows family
monitoring domain	● Operating System ○ Hardware ○ Storage ○ Virtualization ○ None
host list expression	*

Figure 5-4. Customizing a category

Click **OK** to validate the changes.

5.1.1.5 Adding a Category from a Template

To add a category from a category template, click the **manage category** link. In the **Manage Categories** popup window (Figure 5-5), check **Add from an unused category template**, choose a template and click the **Add from the selected category** button. A new window allows you to edit this category's properties (Figure 5-6).



Manage Categories

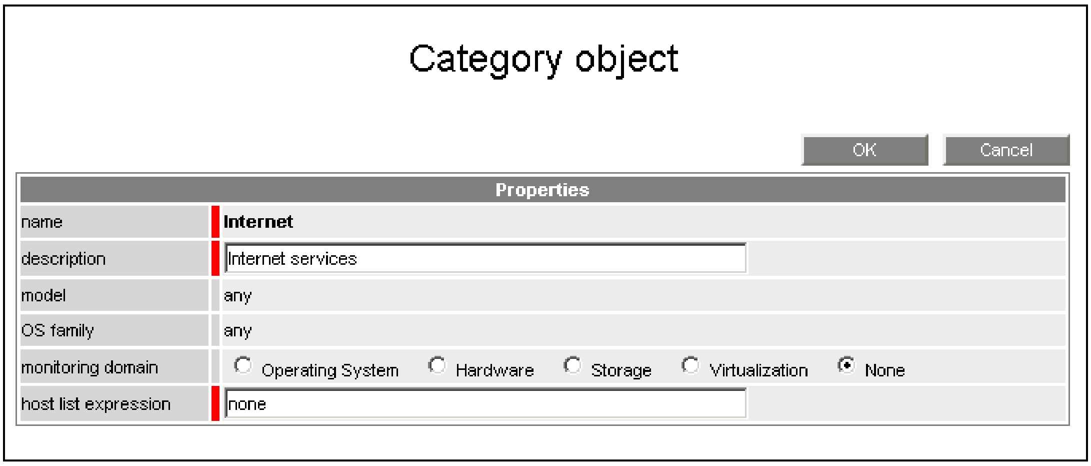
○ **Create a new category**

● **Add from an unused category template (user or predefined template)**

check	Name	Description	Os	Model	hostList
○	AIXServices	Linux processes status	aix	any	*
○	FileSystems	FileSystem services	aix	any	*
●	Internet	Internet services	any	any	none
○	Network	Network monitoring	any	any	none
○	Template	Alert template	any	any	none
○	reporting	Indicators collected by MRTG	any	any	none

○ **Delete a user category template**

Figure 5-5. Manage Categories popup



Category object

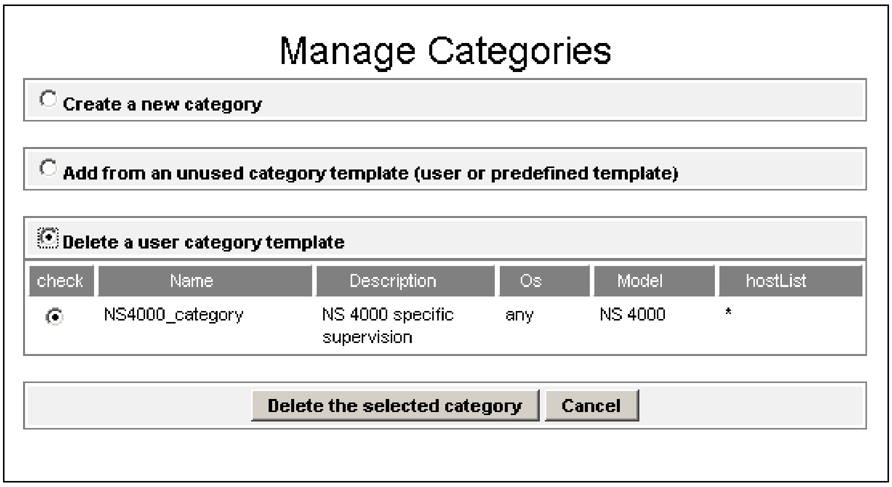
Properties	
name	**Internet**
description	Internet services
model	any
OS family	any
monitoring domain	○ Operating System ○ Hardware ○ Storage ○ Virtualization ● None
host list expression	none

Figure 5-6. Add Category from template

Click **OK** to add this category.

5.1.1.6 Deleting a User Category Template

To delete a user category template, click the **manage category** link. Then in the **Manage Categories** popup window (Figure 5-7), check **Delete a user category template**, choose the template and click the **Delete the selected category** button.



Manage Categories

○ **Create a new category**

○ **Add from an unused category template (user or predefined template)**

● **Delete a user category template**

check	Name	Description	Os	Model	hostList
●	NS4000_category	NS 4000 specific supervision	any	NS 4000	*

Figure 5-7. Delete Category template

This will delete this category template and its instance with its services.

5.1.2 Services

5.1.2.1 Default Services

Bull System Manager provides the following services:

Default services applied to Windows host

- **CPU** and **Memory** services (in the SystemLoad category)
- **All** services (in the **LogicalDisks** category)
- **System**, **Application** and **Security** services (in the **EventLog** category)
- **EventLog** services (in the **WindowsServices** category).

Unused services for a Windows host

- **C** monitors the percentage of used space for the local disk C
- **Com** monitors the Windows services ensuring Com+ notifications functions
- **Networking** monitors the Windows services ensuring networking functions
- **Peripherals** monitors the Windows services ensuring peripheral management functions.

Default services applied to Linux host

- **CPU**, **Memory**, **Users** and **Processes** services (in the **SystemLoad** category)
- **All** services (in the **FileSystems** category)
- **AuthentFailures** services (in the **Syslog** category)
- **syslogd** services (in the **LinuxServices** category).

Unused services for a Linux host

- **/usr** monitors the percent of free space for the file system **/usr**
- **RootAccess** monitors the '*session opened for user* root' messages in the messages log.

Default services applied to AIX host

- **CPU**, **PagingSpace** and **Swap** services (in the **SystemLoad** category)
- **All** service (in the **FileSystems** category)
- **Errors** service (in the **Syslog** category)
- **syslogd** service (in the **AIXServices** category).

Unused services for a AIX host

- **/usr** monitors the percentage of free space for the **/usr** file system.
- **LoadAverage** monitors the CPU and IOWAIT load average over three periods of time (1 min, 5 min and 15 min)
- **Memory** monitors the percentage of used memory (physical and swap) for the system
- **Processes** monitors the number of processes running on the system
- **users** monitors the number of users currently logged in
- **zombies** monitors the number of zombie processes running on the system

Unused services for Windows, AIX and Linux hosts

- **FTP**, FTP service
- **HTTP**, HTTP service
- **HTTP_BSM**, which checks the BSM URL
- **TCP_7**, which checks the echo TCP port
- **UDP_7**, which checks the echo UDP port
- **Perf_indic** service (in the **Reporting** category), which monitors reporting indicators from their log files; this service must be cloned.

Note Automatically generated services are represented by the ⚙ icon, (see *Generated Categories and Services* on page 213).

5.1.2.2 Service Properties

Service Properties	Description
category	Service category
name	Service name
description	Description of the service
model	Supported host model(s) to which the service can apply (multiple choice is allowed)
OS family	Operating system supported for the service
host list expression	List of hosts to which the service will apply. The host list expression can be defined as follows: • *: all configured hosts with an Operating System corresponding to the service OS family and the service model • **none:** no host. • a list of host names separated by a comma to exclude other configured hosts. Example: `host1,host2,host3`. • a list of host names separated by a comma and prefixed by "!" to exclude these hosts. Example: `!host1,!host2,!host3`.

Service Properties	Description
status	Monitoring status (active, inactive). Default value: **active**. Active status means that the service is checked. The service is visible as a node of the host in the Management Tree. Inactive status means that the service is not checked. It is not visible in the Management Tree. This field may be used to activate/deactivate temporarily the service check.
monitoring on event	Indicates if the service check is initiated and performed by external applications, for instance SNMP Traps. Default value: 0
monitoring by polling	Indicates if the service check is initiated by the BSM server and performed on a regular manner. Default value: 1 When this option is set, the check command, monitoring period and polling interval must be filled in (see below)
check command	The **Check** box contains the check command. The **Parameters** box contains check command parameters. Linux Check Commands: All Linux check commands are launched by the **check_nrpe** command. The check command is the first parameter of the command: **/opt /BSMAgent/nrpe/libexec/check_nrpe** It must not be modified. This parameter is available only if the **monitoring by polling** attribute is set to 1.
monitoring period	Time during which the service must be checked. Default value: **24x7**. This parameter is available only if the 'monitoring by polling' attribute is set to 1.
polling interval	Number of minutes to wait between regular service checks. Default value: **5 min**. This parameter is available only if the 'monitoring by polling' attribute is set to 1.
enable processing	Performance data processing. Default value: **No** **Yes**: means that performance data are processed. **No**: means that performance data are not processed. For BSM defined services, this attribute is displayed only if performance data is available for the service. For user defined services, this attribute is always displayed and no control is done on the availability of performance data.
contact groups	Name of the contact groups that must be notified if a problem is reported by this service. Default value: **mgt-admins**.
enable Bull autocall	Enable the autocall mechanism. Default value: **No**.

Service Properties	Description
enable SNMP trap	Enable SNMP trap notification. Default value: **Yes**.
notification period	Time during which service notifications must be sent out. Default value: **24x7**.
re-notification interval	Number of minutes to wait before re-notifying a contact that service status is still **WARNING** or **CRITICAL** (after the notification made immediately after the problem occurred). Default value: ***0*** **(no re-notification)**.
notify if warning	Notify contacts when service status is at **WARNING** level.
notify if critical	Notify contacts when service status is at **CRITICAL** level.
notify if recovery	Notify contacts when service status is at **RECOVERY** level.
notify if unknown	Notify contacts when service status is at **UNKNOWN** level.
notify on downtime start/stop	Notify contacts when scheduled downtime is started or stopped for this service.

Table 5-1. Service properties

The host list for a service is always a subset of the category host list.

Notes

- A host list MUST NOT mix the **not (!) hosts** list with other types of expression (**hosts list**, **none** or *). For instance, the expression `!h1,h2,h3` is ambiguous and is forbidden.
- The host list of services linked to hardware or storage management is automatically generated and cannot be edited with the service form.

The following table gives examples of host selection results, according to the category and service host list values.

Category host list	Service host list	Host selection result
*	*	This service monitors all configured hosts.
*	none	This service does not apply to a host.
*	h1,h2	This service applies to `h1` and `h2` hosts only.
*	!h1,!h2	This service applies to all configured hosts except `h1` and `h2`.
none	any value	No services of this category are applied to a host.
h1,h2,h3	*	This service applies to `h1`, `h2` and `h3` hosts.
h1,h2,h3	none	This service does not apply to a host.
h1,h2,h3	!h3	This service applies to `h1` and `h2` hosts, but not to `h3`.

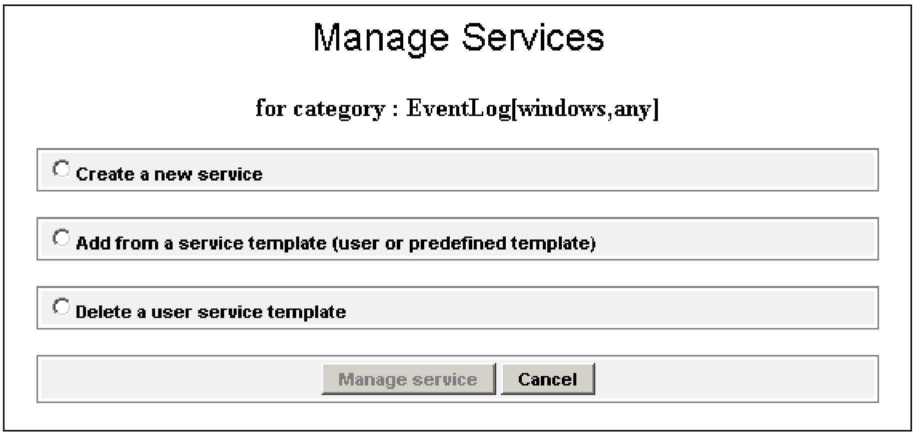
Table 5-2. Category and Service host selection -syntax rules

Note

When you customize a service, the **Category** name, **model** and **OS family** are not editable because these attributes are used for service identification. To change them, you MUST inhibit the existing predefined service (with **hostList = none**) and create a new service with or without the same name.

5.1.2.3 Creating a New Service

To create a new service in a category, click the **manage service** link of this category. Then, in the **Manage Services** popup window (Figure 5-8), check **Create a new service** and click the **Create a new service** button. A new window allows you to edit the service properties (Figure 5-9).



Manage Services

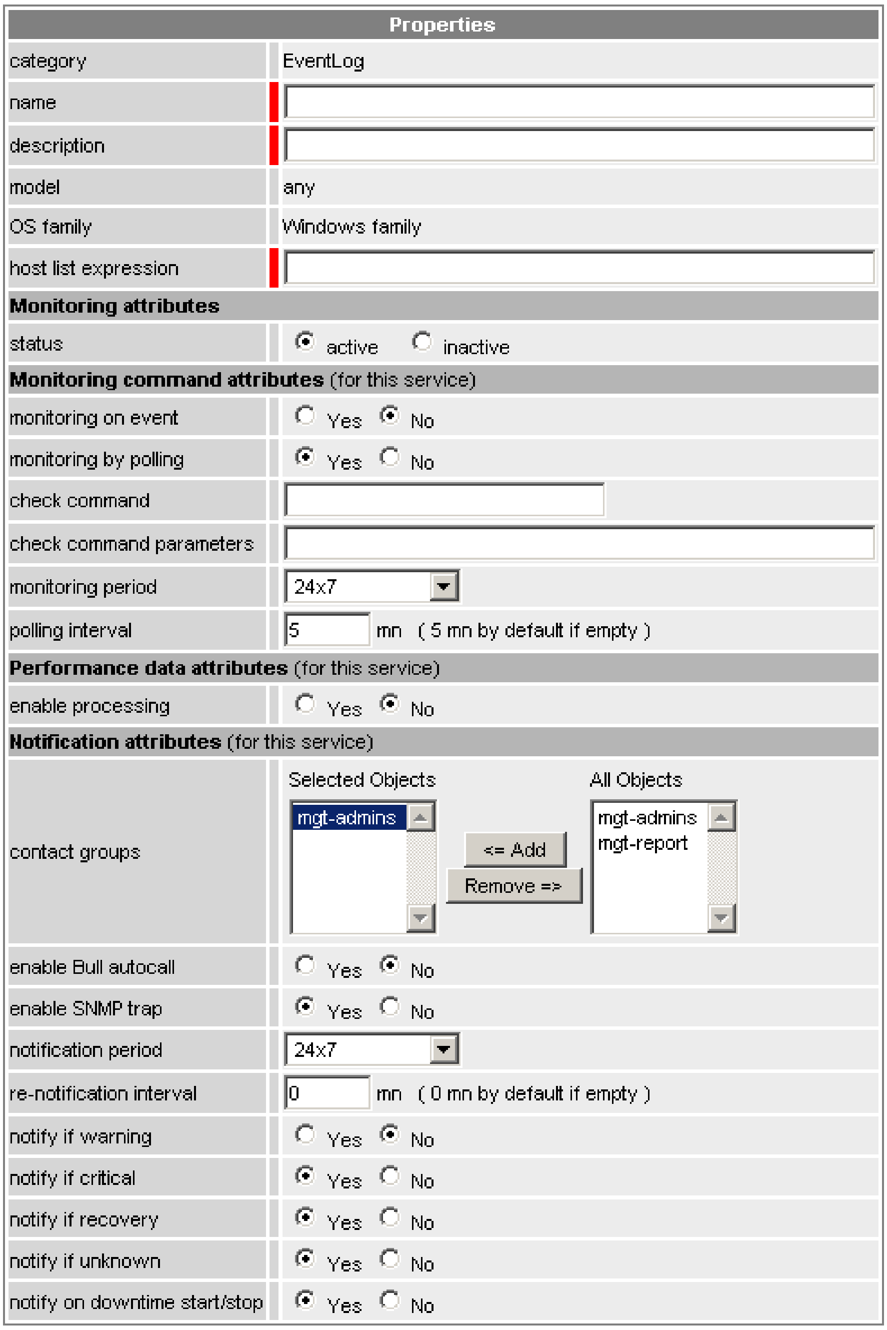
for category : EventLog[windows,any]

○ Create a new service

○ Add from a service template (user or predefined template)

○ Delete a user service template

Figure 5-8. Manage services popup



Properties	
category	EventLog
name	
description	
model	any
OS family	Windows family
host list expression	
Monitoring attributes	
status	● active ○ inactive
Monitoring command attributes (for this service)	
monitoring on event	○ Yes ● No
monitoring by polling	● Yes ○ No
check command	
check command parameters	
monitoring period	24x7
polling interval	5 mn (5 mn by default if empty)
Performance data attributes (for this service)	
enable processing	○ Yes ● No
Notification attributes (for this service)	
contact groups	Selected Objects: mgt-admins All Objects: mgt-admins, mgt-report
enable Bull autocall	○ Yes ● No
enable SNMP trap	● Yes ○ No
notification period	24x7
re-notification interval	0 mn (0 mn by default if empty)
notify if warning	○ Yes ● No
notify if critical	● Yes ○ No
notify if recovery	● Yes ○ No
notify if unknown	● Yes ○ No
notify on downtime start/stop	● Yes ○ No

Figure 5-9. Service properties edition

Click **OK** to create this service in the selected category.

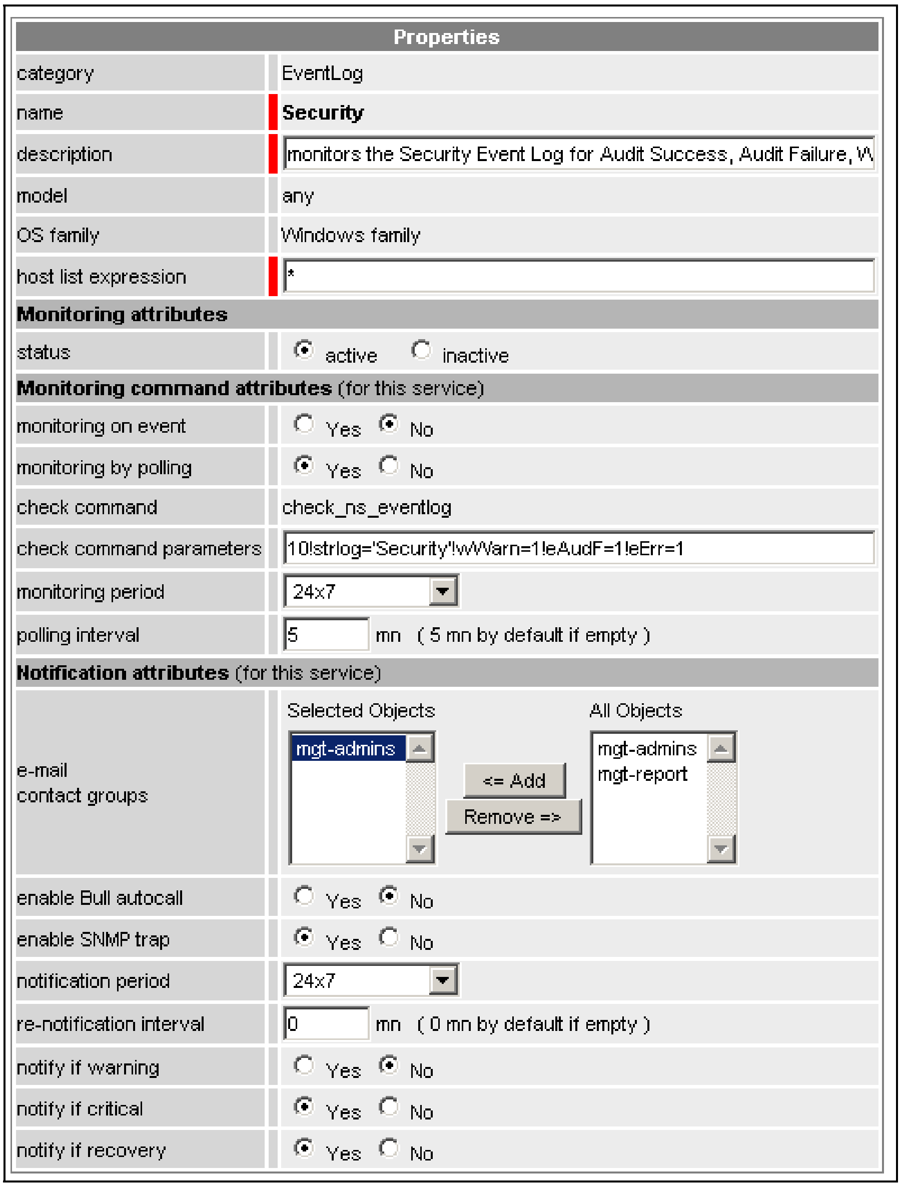
Notes

- The **check**_command must be defined in a Nagios configuration file (*.cfg) installed under the directory **<BSM Directory>/engine/nagios/etc/NSM**
- The corresponding Nagios plugin must be installed in the directory**<BSM Directory>/engine/nagios/libexec**

See *Creating a New Category and a New Service* on page 105 to get a detailed description.

5.1.2.4 Customizing a Service

To customize a service, click the **edit** link for the service. A new window allows you to customize threshold and monitoring properties or to modify the host list. Some text fields (**category**, **service name**, **model**, OS, **check command**) are not editable.

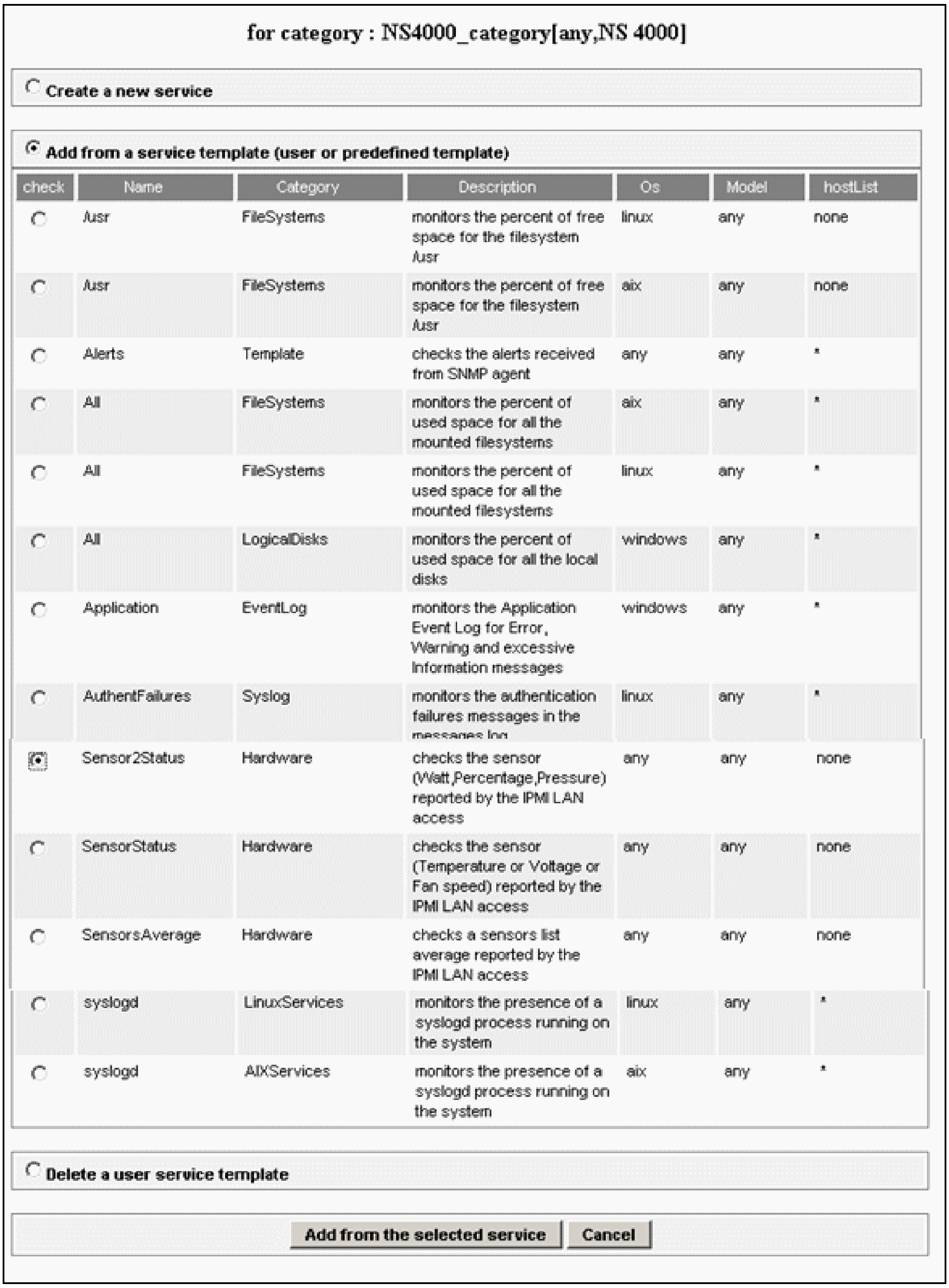


Properties	
category	EventLog
name	**Security**
description	monitors the Security Event Log for Audit Success, Audit Failure, W
model	any
OS family	Windows family
host list expression	*
Monitoring attributes	
status	● active ○ inactive
Monitoring command attributes (for this service)	
monitoring on event	○ Yes ● No
monitoring by polling	● Yes ○ No
check command	check_ns_eventlog
check command parameters	10!strlog='Security'!wWarn=1!eAudF=1!eErr=1
monitoring period	24x7
polling interval	5 mn (5 mn by default if empty)
Notification attributes (for this service)	
e-mail contact groups	Selected Objects: mgt-admins All Objects: mgt-admins, mgt-report
enable Bull autocall	○ Yes ● No
enable SNMP trap	● Yes ○ No
notification period	24x7
re-notification interval	0 mn (0 mn by default if empty)
notify if warning	○ Yes ● No
notify if critical	● Yes ○ No
notify if recovery	● Yes ○ No

Figure 5-10. Customize service

5.1.2.5 Adding a Service from a Template

To add a service in a category from a category template, click the **manage service** link for the category. In the **Manage Service** popup window (Figure 5-11), check **Add from a service template**, choose your template and click the **Add from the selected service** button. A new window allows you to modify the properties for this service if necessary (Figure 5-12).



for category : NS4000_category[any,NS 4000]

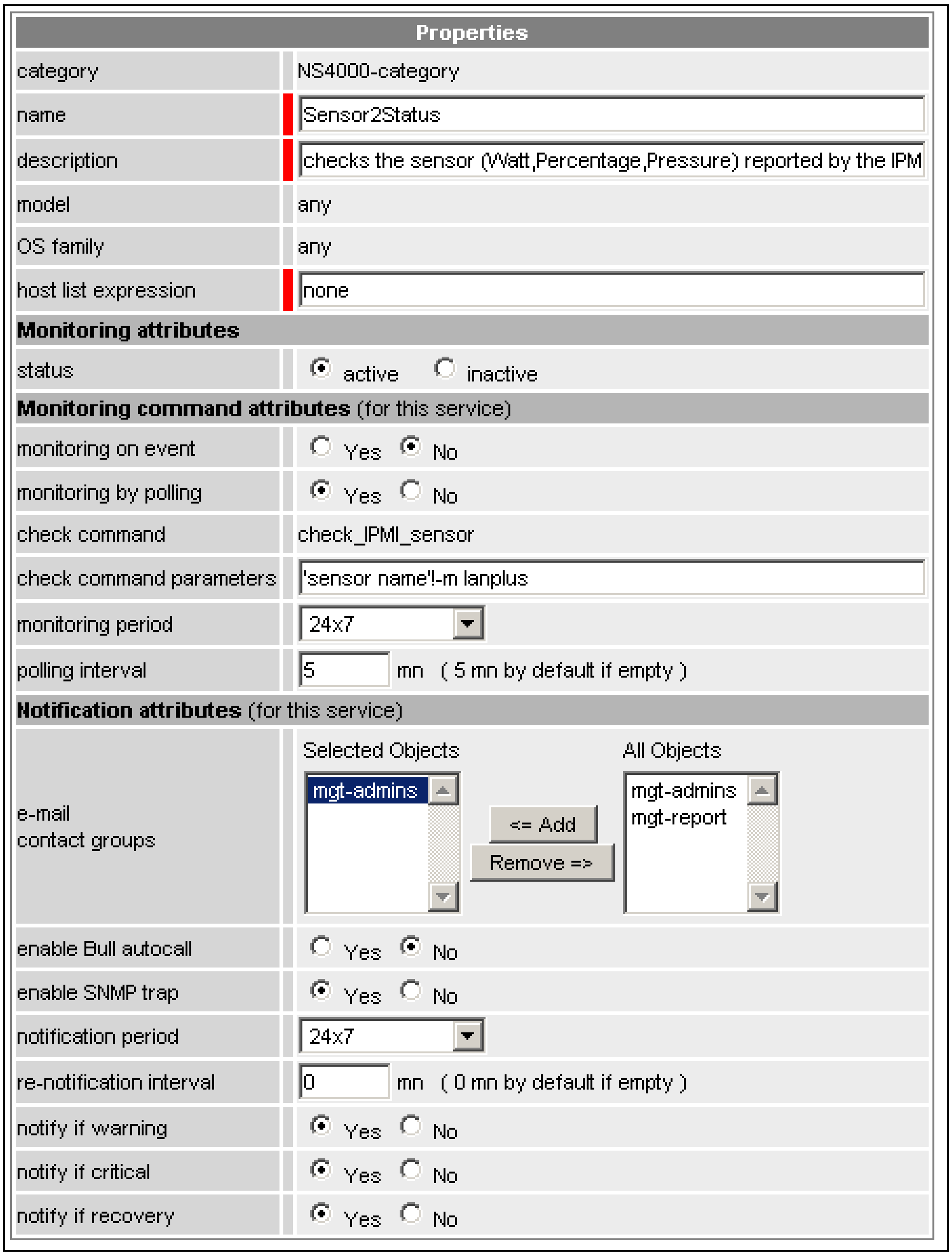
○ **Create a new service**

● **Add from a service template (user or predefined template)**

check	Name	Category	Description	Os	Model	hostList
○	/usr	FileSystems	monitors the percent of free space for the filesystem /usr	linux	any	none
○	/usr	FileSystems	monitors the percent of free space for the filesystem /usr	aix	any	none
○	Alerts	Template	checks the alerts received from SNMP agent	any	any	*
○	All	FileSystems	monitors the percent of used space for all the mounted filesystems	aix	any	*
○	All	FileSystems	monitors the percent of used space for all the mounted filesystems	linux	any	*
○	All	LogicalDisks	monitors the percent of used space for all the local disks	windows	any	*
○	Application	EventLog	monitors the Application Event Log for Error, Warning and excessive Information messages	windows	any	*
○	AuthentFailures	Syslog	monitors the authentication failures messages in the messages log	linux	any	*
●	Sensor2Status	Hardware	checks the sensor (Watt,Percentage,Pressure) reported by the IPMI LAN access	any	any	none
○	SensorStatus	Hardware	checks the sensor (Temperature or Voltage or Fan speed) reported by the IPMI LAN access	any	any	none
○	SensorsAverage	Hardware	checks a sensors list average reported by the IPMI LAN access	any	any	none
○	syslogd	LinuxServices	monitors the presence of a syslogd process running on the system	linux	any	*
○	syslogd	AIXServices	monitors the presence of a syslogd process running on the system	aix	any	*

○ **Delete a user service template**

Figure 5-11. Manage service popup



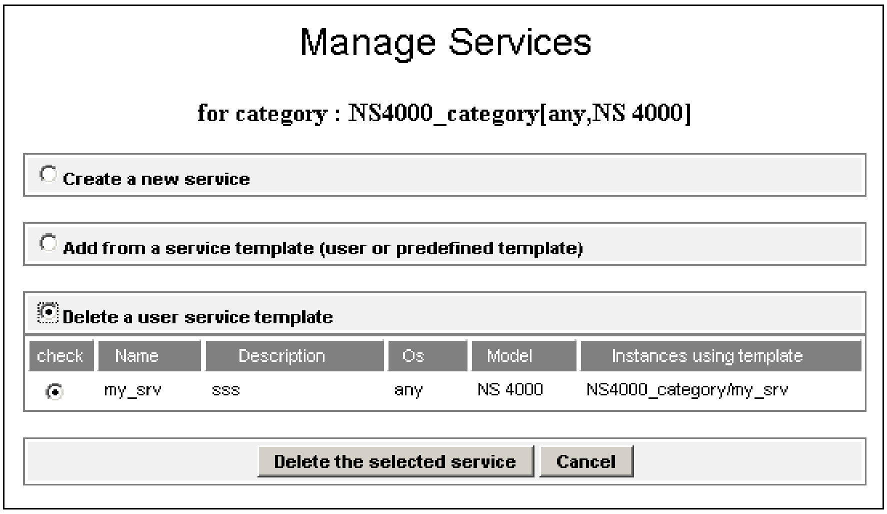
Properties	
category	NS4000-category
name	Sensor2Status
description	checks the sensor (Watt,Percentage,Pressure) reported by the IPM
model	any
OS family	any
host list expression	none
Monitoring attributes	
status	● active ○ inactive
Monitoring command attributes (for this service)	
monitoring on event	○ Yes ● No
monitoring by polling	● Yes ○ No
check command	check_IPMI_sensor
check command parameters	'sensor name'!-m lanplus
monitoring period	24x7
polling interval	5 mn (5 mn by default if empty)
Notification attributes (for this service)	
e-mail contact groups	Selected Objects: mgt-admins All Objects: mgt-admins, mgt-report
enable Bull autocall	○ Yes ● No
enable SNMP trap	● Yes ○ No
notification period	24x7
re-notification interval	0 mn (0 mn by default if empty)
notify if warning	● Yes ○ No
notify if critical	● Yes ○ No
notify if recovery	● Yes ○ No

Figure 5-12. Add service from template

Click **OK** to add the service to the selected category.

5.1.2.6 Deleting a User Service Template

To delete a user service template, click the **manage service** link of the category that uses this template. In the **Manage Services** popup (Figure 5-13), check **Delete a user service template**, choose a template and click the **Delete the selected service** button.



Manage Services

for category : NS4000_category[any,NS 4000]

○ Create a new service

○ Add from a service template (user or predefined template)

● Delete a user service template

check	Name	Description	Os	Model	Instances using template
●	my_srv	sss	any	NS 4000	NS4000_category/my_srv

Figure 5-13. Delete service template

This will delete this service template with all its instances.

Note You cannot manage services (add service, create service) from an automatically generated category.

5.1.3 Check Commands

The following table lists the **check commands** used by the predefined activated services. See also *Appendix B - Check Commands for Customizable Services*, which describes the syntax of the check commands associated with the services that can be customized.

Operating System	Model	Category	Service	Check Command
Windows	any	WindowsServices	Peripherals	check_ns_service
			Management	
			EventLog	
			Networking	
			Com	
		EventLog	Application	check_ns_eventlog
			Security	
			System	
		LogicalDisks	All	check_windisks
			C	
		SystemLoad	CPU	check_ns_load
			Memory	check_ns_mem
Linux	any	LinuxServices	syslogd	check_procs
		Syslog	Alert	No check (SNMP trap receiver)
		Syslog	AuthentFailures	check_log2.pl
			RootAccess	
		SystemLoad	CPU	check_cpuload
			Users	check_users
			Processes	check_procs
			Zombies	
			Memory	check_memory
			Swap	check_swap
		FileSystems	All	check_disks.pl
AIX	any	AIXServices	syslogd	check_procs
		Syslog	Alert	No check (SNMP trap receiver)
		Syslog	Errors	check_errpt.sh
		SystemLoad	CPU	check_lpar_load
			PagingSpace	check_pgsp
			Swap	check_swap
			LoadAverage	check_load
			Memory	check_mem.pl
			Prccesses	check_procs
			zombies	
			Users	check_users
		FileSystems	All	check_disks.pl
any	I/O Switch Module	Hardware	Health	Internal generated check (not editable)

Operating System	Model	Category	Service	Check Command
any	NovaScale 4000, Blade series	Hardware	Health	Internal generated check (not editable)
any	ns bullion, NovaScale 3005, 4000, 5005, T800, R400 &9019 series, Express5800		Alerts	No check (SNMP trap receiver)
any	Escala PL series	Hardware	CECStatus	check_hmc_cec_status
			Events	check_hmc_hw_event
Windows	any	PAM	Alerts	No check (SNMP trap receiver)
			GlobalStatus	Internal generated check (not editable)
any	any	CMM	Alerts	No check (SNMP trap receiver)
			ChassisStatus	Internal generated check (not editable)
any	Novascale 4000, 3005, 9010, T800, R400, Express5800, ns bullion	Power	Status	Internal generated check (not editable)
any	ns bullion	Power	Consumption	Internal generated check (not editable)
any	any	Reporting	Perf_indic	check_mrtg
any	any	Internet	FTP	check_ftp
			HTTP	check_http
			UDP_7	check_udp
			HTTP_BSM	check_httpURL
			TCP_7	check_tcp
any	any	MegaRAID	Alerts	No check
			Status	check_megaraid

Table 5-3. Check commands list

5.1.4 Examples

5.1.4.1 Creating a New Category and Adding a Service

This example shows how to create a new category (`my_category`) for Windows hosts and add a new service aimed at monitoring the percentage of used space for the local disk D.

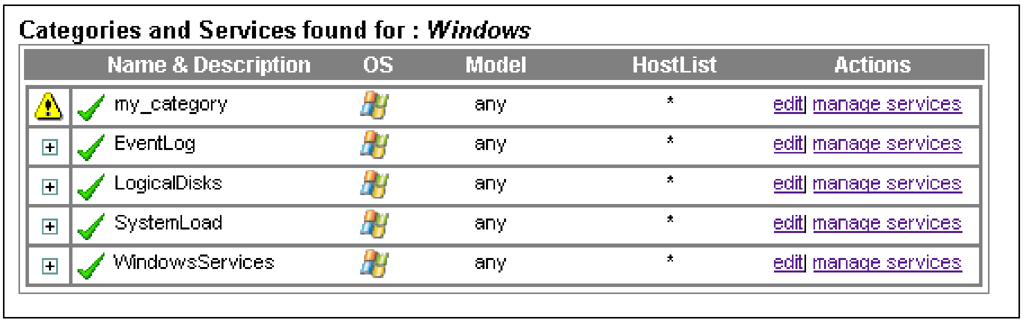
1. Click the **Categories/Services** link in the **Supervision** tab.

2. From the **Categories/Services** page, click **Filter by OS** and select **Windows**.

3. Click **manage category**.

4. In the **Manage Category** popup window, check **Create a new category** and click **create a new category**.
   – Enter the name of the category: `my_category.`
   – Enter its description.
   – The **OS family** text field is already filled in with Windows. It is not editable because of the filter used (if you choose **no filter** this text field becomes editable).
   – Choose the monitoring domain.
   – Set **host list expression** to "*"

5. Click **OK** to validate. The new category is now displayed in the Categories and Services list:



Categories and Services found for : ***Windows***

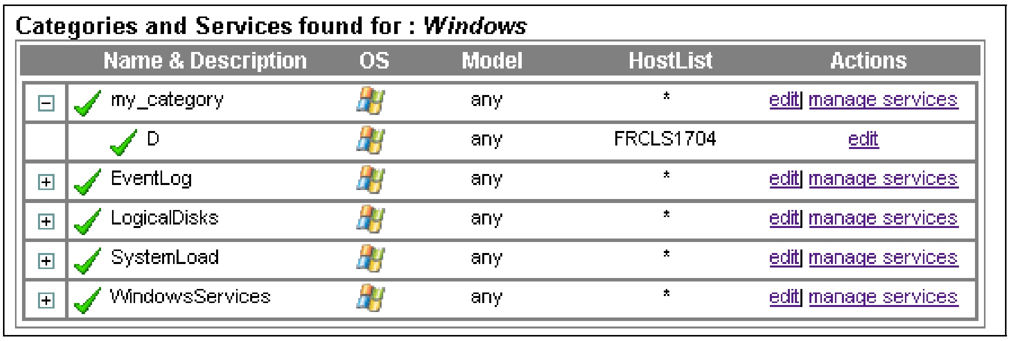
		Name & Description	OS	Model	HostList	Actions
⚠	✓	my_category	🪟	any	*	edit| manage services
⊞	✓	EventLog	🪟	any	*	edit| manage services
⊞	✓	LogicalDisks	🪟	any	*	edit| manage services
⊞	✓	SystemLoad	🪟	any	*	edit| manage services
⊞	✓	WindowsServices	🪟	any	*	edit| manage services

Figure 5-14. Categories and Services table with a new category

Note The ⚠ icon means that there is no service for this category.

6. To create a new service in `my_category`, click the **manage service** link of `my_category`
   – In the **Manage Service** popup window, check **Add from service template** and select the service C. Then click **add from the selected service**.
   – Change the name into D and change the description.
   – Change the host list into *.
   – Change the others fields if necessary.

7. Click **OK** to validate. The new service is now displayed in the Categories and Services list:



Categories and Services found for : *Windows*

	Name & Description	OS	Model	HostList	Actions
⊟	✓ my_category		any	*	edit| manage services
	✓ D		any	FRCLS1704	edit
⊞	✓ EventLog		any	*	edit| manage services
⊞	✓ LogicalDisks		any	*	edit| manage services
⊞	✓ SystemLoad		any	*	edit| manage services
⊞	✓ WindowsServices		any	*	edit| manage services

Figure 5-15. Categories and services table with a new service

5.1.4.2 Creating a New Category and a New Service

This example shows how to create a new category (`my_category`) for a host and to create a new service based on a new Nagios plugin (check_demo.sh).

The Nagios plugin is the following shell script (check_demo.sh):

```
#!/bin/bash

usage() {
echo "Usage:  check_demo.sh -h HOSTNAME -c CRIT_TRESHOLD -w
WARN__TRESHOLD"
exit 255
}

while getopts h:w:c: option
do
        case $option in
        h) HOSTNAME=${OPTARG};continue;;
        c) CRIT=${OPTARG};continue;;
        w) WARN=${OPTARG};continue;;
        ?) usage;;
        esac

done


echo "Demo service on ${HOSTNAME}: critical threshold set to $WARN
warning threshold set to $CRIT"
exit 0
```

The check command is defined in the **demo_command.cfg** file:

```
# check_demo command definition
define command {
 command_name   check_demo
 command_line   $USER1$/check_demo.sh -h $HOSTADDRESS$ -w $ARG2$ -c
$ARG2$
}
```

Note

The **check**_command can reference information from the host configuration as a parameter by using Nagios macro (HOSTADDRESS in this example), that will be automatically substituted by Nagios before the command executes. Other parameters must be set in the service definition. To get detailed information about the Nagios plugin and command definition, refer to the standard Nagios documentation on http://www.nagios.org/

Important

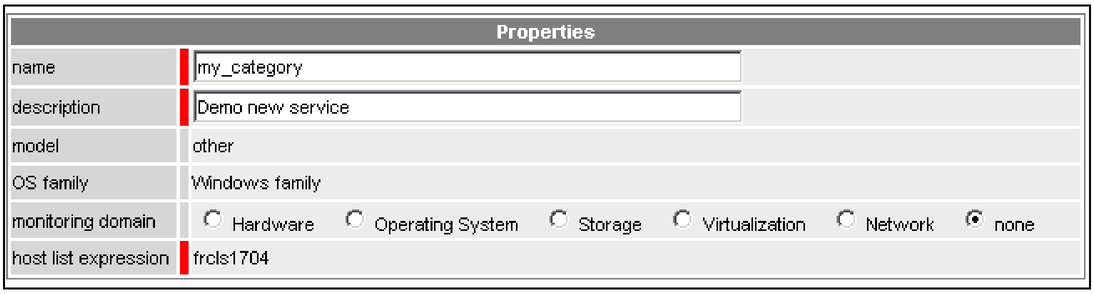
Before configuring your service in BSM, you have to install the Nagios plugin (check_demo.sh) in the <BSM Directory>/engine/nagios/libexec directory and the command definition file (demo_command.cfg) in the directory <BSM Directory>/engine/nagios/etc/NSM.

1. Click the **Categories/Services** link in the Supervision tab.

2. From the **Categories/Services** page, click **Filter by Host** , select your host and click the **Apply** button.

3. When the table is ready, click **manage category**.

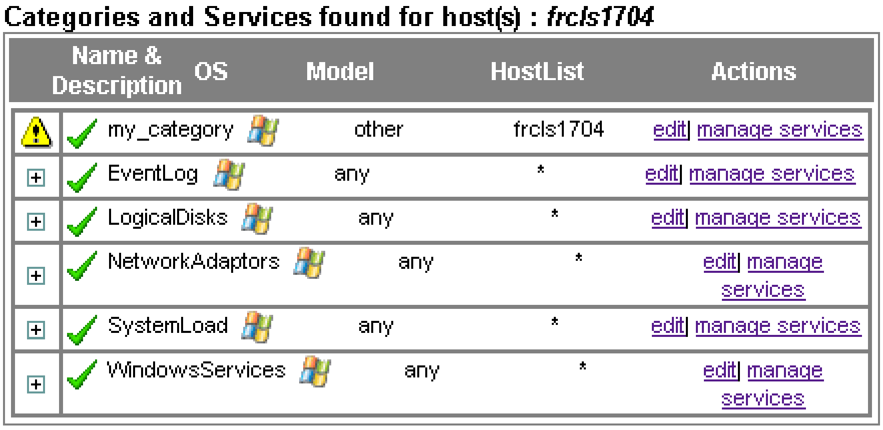
4. In the **Manage Category** popup window, check **Create a new category** and click **create a new category**.
   - Enter the name of the category: `my_category`.
   - Enter its description.
   - The **OS family** and **Model**, and **host list expression** text fields are already filled (with the values of the selected Host). It is not editable because of the used filter (if you choose **no filter** this text field becomes editable).
   - Choose the monitoring domain.



Properties	
name	my_category
description	Demo new service
model	other
OS family	Windows family
monitoring domain	○ Hardware ○ Operating System ○ Storage ○ Virtualization ○ Network ● none
host list expression	frcls1704

Figure 5-16. my_category creation

5. Click **OK** to validate. The new category is now displayed in the Categories and Services list:



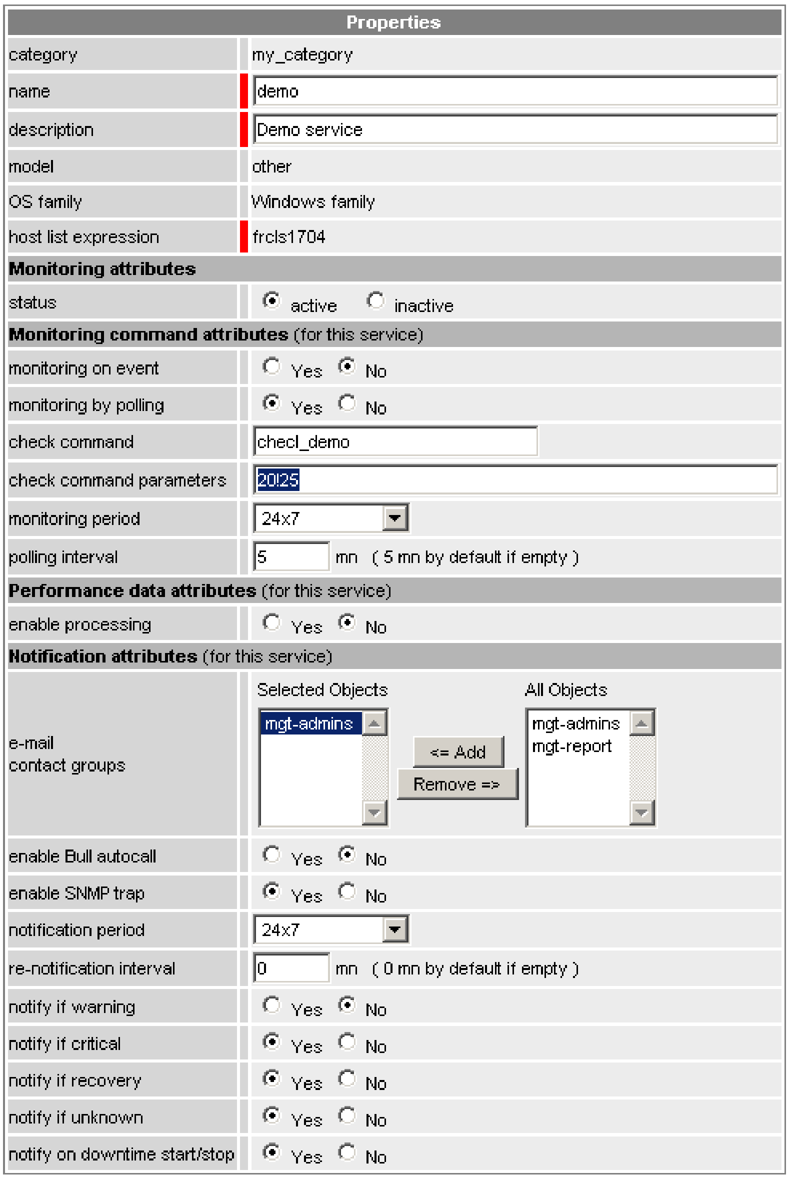
Categories and Services found for host(s) : *frcls1704*

		Name & Description	OS	Model	HostList	Actions
⚠	✓	my_category		other	frcls1704	edit| manage services
⊞	✓	EventLog		any	*	edit| manage services
⊞	✓	LogicalDisks		any	*	edit| manage services
⊞	✓	NetworkAdaptors		any	*	edit| manage services
⊞	✓	SystemLoad		any	*	edit| manage services
⊞	✓	WindowsServices		any	*	edit| manage services

Figure 5-17. List of categories for host

Note The ⚠ icon means that there is no service for this category.

6. To create a new service in `my_category`, click the **manage service** link of `my_category`
   - In the **Manage Service** popup window, check **Create a new service** and click the button with same label.
   - In the **Service Object** window write a name `demo` and the description.
   - Write the check Nagios command name and its parameters : values corresponding to ARG1 and ARG2 must be entered, separated by '!'
   - Change the others fields if necessary.



Properties	
category	my_category
name	demo
description	Demo service
model	other
OS family	Windows family
host list expression	frcls1704
Monitoring attributes	
status	● active ○ inactive
Monitoring command attributes (for this service)	
monitoring on event	○ Yes ● No
monitoring by polling	● Yes ○ No
check command	checl_demo
check command parameters	20!25
monitoring period	24x7
polling interval	5 mn (5 mn by default if empty)
Performance data attributes (for this service)	
enable processing	○ Yes ● No
Notification attributes (for this service)	
e-mail contact groups	Selected Objects: mgt-admins All Objects: mgt-admins, mgt-report
enable Bull autocall	○ Yes ● No
enable SNMP trap	● Yes ○ No
notification period	24x7
re-notification interval	0 mn (0 mn by default if empty)
notify if warning	○ Yes ● No
notify if critical	● Yes ○ No
notify if recovery	● Yes ○ No
notify if unknown	● Yes ○ No
notify on downtime start/stop	● Yes ○ No

7. Click OK to validate. The new service is now displayed in the Categories and Services list.

After saving and reloading your configuration, the new service will be scheduled by Nagios and be available in BSM Console.

Important

If the plugin provides performance data, set the enable processing attribute to 1 to allow the collection of corresponding indicators. To get detailed informations on how to write plugin with performance data, see documentation on: http://nagiosplug.sourceforge.net/developer-guidelines.html

5.1.4.3 Customizing the List of Monitored Hosts

By default, a service is monitored on all the hosts specified in the corresponding category host list. You may also define a specific host list for a service.

Examples of application:

- To disable monitoring of the **Processes** service on all hosts:
  a. Edit the **Processes** service.
  b. Set the host list to **`none`**.
- To disable monitoring of the **All** service in **FileSystems** category on the `sysman` host, there are two possibilities:

1. Using the **filter by HOST** filter:
   a. Select the `sysman` host and click **Apply**.
   b. Edit the **All** service in the **FileSystem** category.
   c. Click the **delete for this host list** button.
2. Or using another filter:
   a. Edit the **All** service in the **FileSystem** category.
   b. Set the host list is to **`"!sysman",`** that means that the **All** service does apply to all hosts, except the `sysman` host.

Note For manager Categories (PAM, CMM, etc.) the **hostList** attribute must be a list of managers. All referenced hosts that are not a manager of the required type, will be automatically excluded from the host list.

5.1.4.4 Customizing the Notification Period

You can define specific monitoring or notification properties for a service. You can even create several identical services for different host lists with different properties.

In the following example, the administrator has customized two occurrences of the **All** service in the **FileSystems** category.

- In the first occurrence the host list is `host1, host2` (only `host1` and `host2`) and notification is not active (`none`) for this host list.
- In the second occurrence, the host list is `!host1,!host2` (all hosts except `host1` and `host2`) and notification is active (default: `24x7`) for this host list.

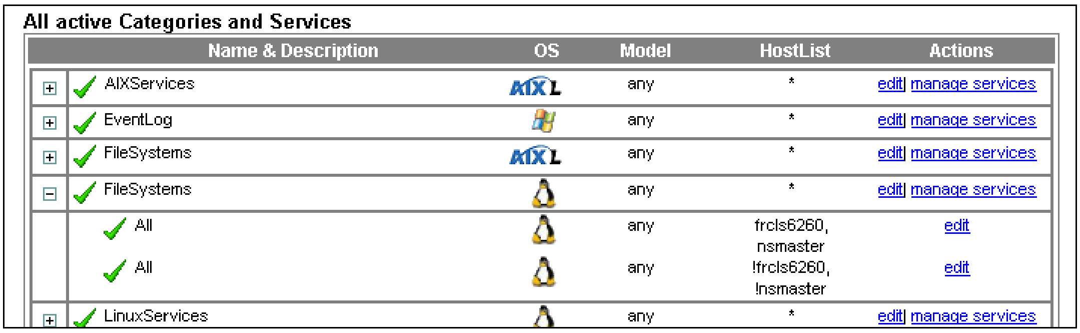
Note The contact groups associated with the service must be configured to allow the reception of notifications.

Using the filter by HOST filter:

1. Select `host1` and `host2`, and click **Apply**.
2. Edit the **All** service in **FileSystems** category.
3. Change the notification period to none.
4. Click **OK** to validate.

Using another filter:

1. Edit the **All** service in the **FileSystems** category.
2. Change the host list to `!host1, !host2`.
3. Leave the notification period (set by default to **24x7**) unchanged
4. Click **OK** to validate.
5. Click the **manage service** link of the **FileSystems** category.
6. In the **Manage Service** popup window, check **Add from service template** and select the **All** service. Then click the **add from the selected service** button.
7. Change the host list to `host1,host2`.
8. Change the notification period to **none**.
9. Click **OK** to validate.



All active Categories and Services

	Name & Description	OS	Model	HostList	Actions
⊞	✓ AIXServices	AIXL	any	*	edit| manage services
⊞	✓ EventLog		any	*	edit| manage services
⊞	✓ FileSystems	AIXL	any	*	edit| manage services
⊟	✓ FileSystems		any	*	edit| manage services
	✓ All		any	frcls6260, nsmaster	edit
	✓ All		any	!frcls6260, !nsmaster	edit
⊞	✓ LinuxServices		any	*	edit| manage services

Figure 5-18. Categories and Services table with customized services

5.1.4.5 Customizing Thresholds

This section explains how, as administrator, you can modify service thresholds for all hosts or for different host lists. Thresholds can be modified for the following services:

Category	Services with customizable thresholds
SystemLoad	CPU (Windows, Linux, Aix), Memory (Windows, Linux),), Swap (Linux), Users (Linux), Processes (Linux), Zombies (Linux), PagingSpace (Aix)
EventLog	Application, Security, System.
LogicalDisks	All
FileSystems	All (Linux, Aix)

Table 5-4. Customizing thresholds

5.1.4.6 Warning and Critical Thresholds

Thresholds are defined in the command used by Bull System Manager to check the service. Service **Parameters** displays this command (see the following table for syntax). Customizable names and character strings are in **bold** type.

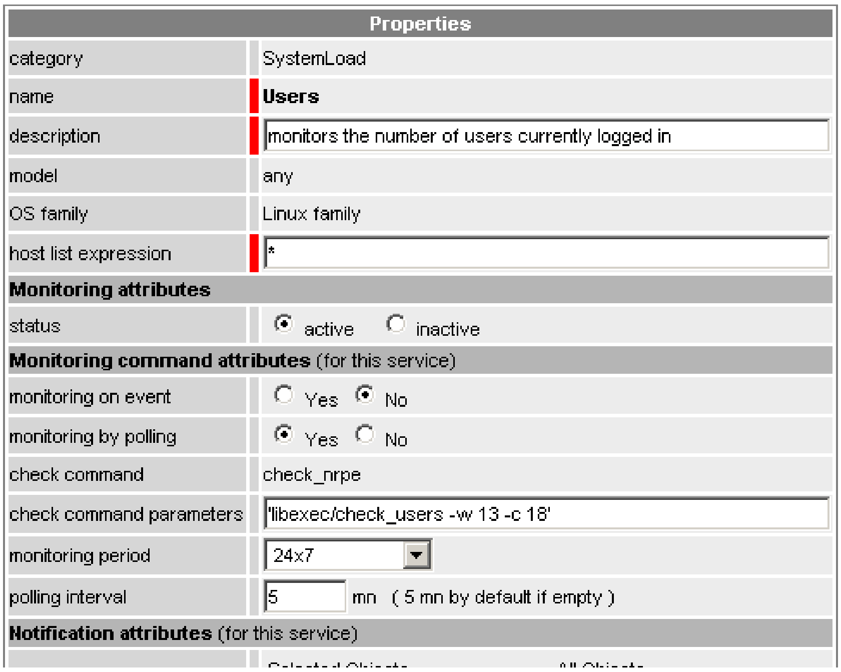
Category	Service	Check command[1]	check parameters
SystemLoad (Windows)	CPU	check_ns_load	1!**80**!**90**!10!**60**!**80**
	Memory	check_ns_mem	PERCENT!70!90
EventLog	Application	check_ns_eventlog	30!applog=1!wInf=**10**!wWarn=1!eErr=1
	Security		30!seclog=1!wAudS=**10**!wWarn=1!eAudF=1!eErr=1
	System		30!syslog=1!wInf=**10**!wWarn=1!eErr=1
LogicalDisks	All	check_windisks	-w **80**!-c **90**
SystemLoad (Linux)	CPU	check_cpuload	-w 80,70,60 -c 90,80,70
	Memory	check_memory	70 90
	Swap	check_swap	-w **50%** -c **80%**
	Users	check_users	-w **15** -c **20**
	Processes	check_procs	-w **150** -c **200**
	Zombies	check_procs	-w **5** -c **10** -s Z
FileSystems	All	check_disks.pl	-w **80** -c **90** -e /mnt/cdrom -e /mnt/floppy
[1] On Linux services, the check command given in the table is the first parameter of the command: /opt/BSMAgent/nrpe/libexec/check_nrpe. DO NOT MODIFY THIS STRING.			

Table 5-5. Service parameters syntax

Example

In the following example the **Users** Linux service is configured with specific thresholds (`13,18`) for `frcls6260.frcl.bull.fr` and `nsmaster`. The other hosts are monitored with the default thresholds (`15, 20`). From the filter by host, proceed as follows:

1. Select `frcls6260.frcl.bull.fr` and `nsmaster`, and click **Apply**.
2. Edit the **Users** service in **SystemLoad** category.
3. To change the **check command** thresholds, modify the **check_users** command displayed in the **Parameters** box as follows:
4. Change string `15` (default warning threshold) to the new warning threshold (`13`), and the string `20` (default critical threshold) to the new critical threshold (`18`).

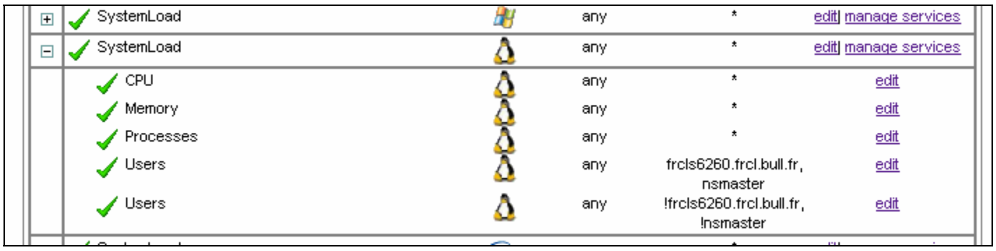


Properties	
category	SystemLoad
name	**Users**
description	monitors the number of users currently logged in
model	any
OS family	Linux family
host list expression	*
Monitoring attributes	
status	● active ○ inactive
Monitoring command attributes (for this service)	
monitoring on event	○ Yes ● No
monitoring by polling	● Yes ○ No
check command	check_nrpe
check command parameters	'libexec/check_users -w 13 -c 18'
monitoring period	24x7
polling interval	5 mn (5 mn by default if empty)
Notification attributes (for this service)	
	Selected Objects All Objects

Figure 5-19. Customized threshold

5. Click **OK** to validate

This will create the two occurrences of the All service. In one occurrence the hostlist is `frcls6260.frcl.bull.fr, nsmaster`, in the other occurrence the hostlist is `!frcls6260.frcl.bull.fr, !nsmaster`, as shown in the following figure (No filter set)



⊞ ✓ SystemLoad		any	*	edit| manage services
⊟ ✓ SystemLoad		any	*	edit| manage services
✓ CPU		any	*	edit
✓ Memory		any	*	edit
✓ Processes		any	*	edit
✓ Users		any	frcls6260.frcl.bull.fr, nsmaster	edit
✓ Users		any	!frcls6260.frcl.bull.fr, !nsmaster	edit

Figure 5-20. Categories and services table with customized services

5.1.4.7 Thresholds Related to Windows Event Logs Scanning

Bull System Manager uses the **check_ns_eventlog** command to monitor the number of event types in the Windows event logs (**Application**, **Security** and **System**) during a given period starting immediately.

Example:

Proceed as follows to configure the **Application** service of the **EventLog** category (Windows system) in order to:

- Check the number of error messages in the Application Event Log over the last 60 min
- Set a critical state if there are at least 5 error messages
- Set a warning state if there is at least 1 error message

1. Edit the **Application** service in the **EventLog** category.

2. To change the **check command** thresholds, modify the line displayed in the **Parameters** box as follows:
   ```
   60!strlog='Application'!wWarn=1!eErr=5
   ```

3. Click **OK** to validate the modifications, and return to the Categories and Services page.

5.1.4.8 Customizing Windows Services

Bull System Manager provides predefined services to monitor certain Windows OS elements.

The following table displays the commands and parameters used by Bull System Manager to check the services. Customizable names and character strings are in **bold** type.

Category	Service	check command	check parameters
Windows Services	Networking	check_ns_service	showall!RpcSs!TrkWks!Dhcp!Dnscache!Netman
	EventLog	check_ns_service	showall!**Eventlog**
	Peripherals	check_ns_service	showall!NtmsSvc!PlugPlay
	Com	check_ns_service	showall!SENS!EventSystem
	Management	check_ns_service	showall!Wmi!WinMgmt!dmserver
LogicalDisks	C	check_ns_disk	PERCENT!C:!80!90

Table 5-6. Windows services check commands and parameters

Note Some of these services can be used as templates.

Examples

- To monitor any Windows logical disk (F:, G: etc.) the Administrator can use and customize the **C** service template with specific thresholds.
- To check the presence of one or more specific Windows services running on the system, the administrator can use and customize one of the services defined for the Windows services (**Networking**, **EventLog**, **Peripherals**, **Com**, **Management**), by modifying the list of checked Windows services set in the **showall** command.

Example:

To remove, for all hosts, the **Wmi** service from the list of Windows services to be checked by the **Management** service, proceed as follows:

1. Click the **manage service** link of the **WindowsServices** category (or another Windows category)
2. In the Manage Service popup window, check **Add from service template** and select the Management service. Then click the **add** button from the selected service.
3. Change the host list to `*`.
4. Remove the `Wmi!` string in the check Parameters. If required, change the other monitoring properties.
5. Click **OK** to validate the modifications.

Note The names of the Windows services specified as check parameters are the short names displayed by one of the following Windows operations:

- Menu **Start -> Parameters -> Control Panel -> Administrative Tools -> Services**.
- Right click selected service -> Properties -> General.

The Service name field gives the short name of the service. For example, the short name for the **DHCP Client** service is **Dhcp**.

5.1.4.9 Customizing Linux or AIX Services

Bull System Manager provides predefined services to monitor certain **Linux** or **AIX OS** elements.

The following table displays the commands and parameters used by Bull System Manager to check services. Customizable names and character strings are in bold type.

category	service	check command	check parameters
LinuxServices **AIXServices**	syslogd	check_procs	-w 1:1 -C syslogd
Syslog	AuthentFailures (linux)	check_log2.pl	-l /var/log/messages -s authfail.seek -p 'authentication failure|FAILED LOGIN|Permission denied' -n 'login.*authentication failure'
	RootAccess (linux)	check_log2.pl	-l /var/log/messages -s rootsess.seek -p 'session opened for user root'
FileSystems	/usr	check_disk	-w **20%** -c **10%** -p **/usr**
SystemLoad	**PagingSpace**	check_pgsp.pl	-w 80 -c 90 -W 5 -C 10';

Table 5-7. Linux services check commands and parameters

Note On Linux or AIX services, the check command given in the table is the first parameter of the command: **/opt/BSMAgent/nrpe/libexec/check_nrpe**.
DO NOT MODIFY THIS STRING.

Example 1

To monitor the Linux or AIX **/home** FileSystem for `host1` with specific thresholds, use the **/usr** service template as follows:

1. From the **filter by host** select `host1`, and click **Apply**.
2. Click the **manage service** link of the **FileSystems** category (or another Linux category)
3. In the **Manage Service** popup window, check **Add from service template** and select the **/usr** service. Then click the **add from the selected service** button.
4. Set **service_name** to `/home`.
5. Modify its description.
6. If you do not use the **filter by HOST** option, change the host list to `host1`.
7. Under **check Parameters**, replace `/usr` by `/home` and if needed, modify thresholds and other monitoring properties.
8. Click **OK** to validate the cloning operation.
9. Repeat this operation to create services for monitoring other specific FileSystems.

Example 2

To check the presence of the **xinetd** (or **inetd**) Linux or AIX service, use the **syslogd** service template as follows:

1. Click the **manage service** link of the **LinuxServices** category (or another Linux category).

2. In the **Manage Service** popup window, check **Add from service template** and select the **syslogd** service. Then click the **add from the selected service** button.

3. Set **service_name** to `xinetd` (or `inetd`).

4. Modify its description.

5. Under **check Parameters**, replace `syslogd` by `xinetd` (or `inetd`) and if needed, modify thresholds and other monitoring properties.

6. Click **OK** to validate the cloning operation.

7. Repeat this operation to create services for monitoring other services or processes.

Example 3

To check, for the `host1` Linux host, the presence of specific character strings in a given file, use the **RootAccess** service template as follows:

1. From the **filter by HOST** option select `host1`, and click **Apply**.

2. Click the **manage service** link of the **Syslog** category (or another Linux category).

3. In the **Manage Service** popup window, check **Add from service template** and select the **RootAccess** service. Then click the **add from the selected service** button.

4. Set service_name.

5. Modify its description.

6. If you do not use the **filter by HOST** option, change the host list to `host1` .

7. Modify **check Parameters** as follows:
   - Do not pay attention to the **#** character at the beginning and at the end of the parameters command.
   - **-l** parameter: replace the **/var/log/messages** file pathname by the pathname of the new file to check.
   - **-s** parameter: replace **rootsess.seek** by a new string (that must be unique).
   - **-p** parameter: replace the string session opened for user root by the new string to search.

8. Click **OK** to validate the cloning operation.

9. Repeat this operation to create a service to scan any file.

5.1.4.10 Customizing URL Access

To check a specific URL on a given port with specific contents, Bull System Manager provides the **HTTP_BSM** service template.

category	service	check_command	check parameters
Internet	HTTP_BSM	check_http	10080!/BSM'HTTP/1.1 200 OK'!'Bull System Manager

Table 5-8. Customizing URL access

By default, the service checks that the Bull System Manager web site is accessible.

Check parameter syntax is: *<port>!<url>!'<response_substring>'!'<content_response>'*

The **HTTP_BSM** service template can be used as described in the following examples.

Example 1

To apply the **HTTP_BSM** service to a set of hosts, proceed as follows:

1. From the **filter by HOST** option select `frcls6260`, and click **Apply**.

2. Click the **manage service** link of the category in which you want to put this service.

3. In the **Manage Service** popup window, check **Add from service template** and select the **HTTP_BSM** service. Then click the **add from the selected service** button.

4. If you do not use the **filter by HOST** option, change the **host list** with the name of the Bull System Manager server (`frcls6260`).

5. Leave the check parameters unchanged.

6. Click **OK** to validate the customization operation.

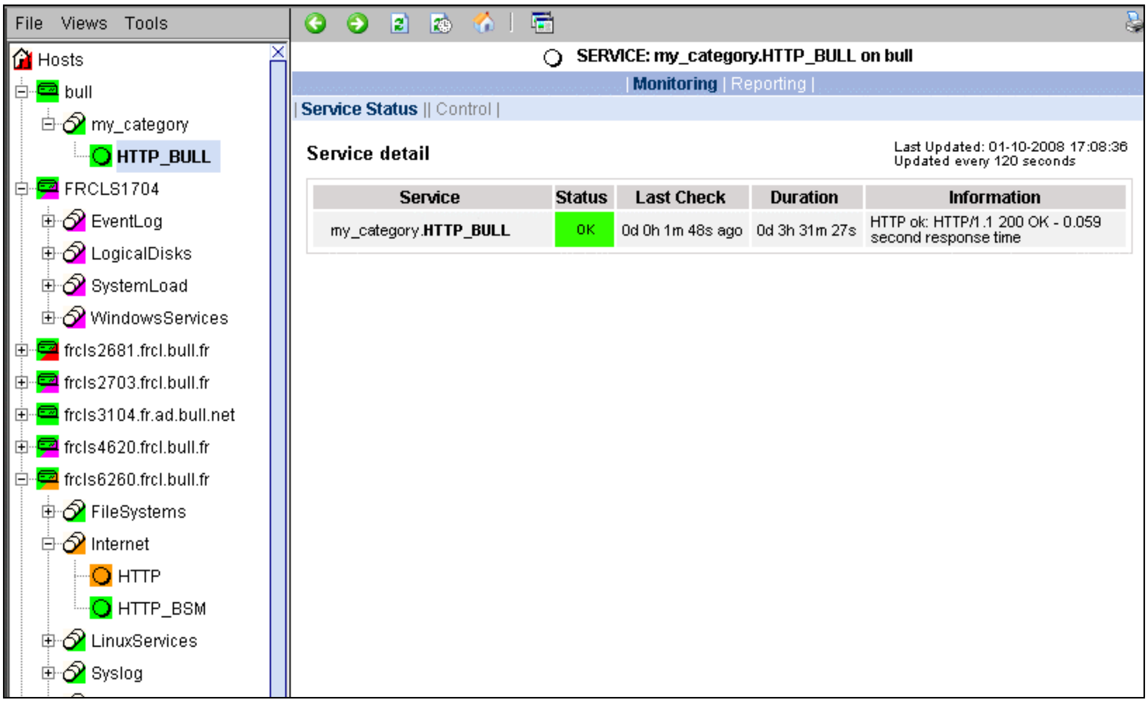
Example 2:

To create a service that monitors http access to the Bull web site (www.bull.com), proceed as follows:

Note We assume that the `bull` (`www.bull.com`) `host` has been defined and that the new category `my_category` has been created with a host list containing `www.bull.com` See the example, *Creating a New Category and Adding a Service*, on page 104. Click the **manage service** link of the `my_category` category.

1. In the **Manage Service** popup window, check **Add from service** template and select the **HTTP_BSM** service. Then click **add from the selected service**.
2. Set the service_name to `HTTP_BULL`.
3. Modify its description.
4. Assign this service to `my_category` category.
5. Specify check parameters as follows:
   `80!/contact.html!'HTTP/1.1 200 OK'!'ABOUT BULL'`
   The `/contact.html` URL is checked on port `80`. The HTTP response must contain the substring `HTTP/1.1 200 OK` and the returned page must contain the substring `ABOUT BULL` .

The following figure shows the `HTTP_BSM` customized service for the `Bull System Manager frcls6260` host, under the Internet category. It also displays the `HTTP_BULL` cloned service, for the `bull` host.



SERVICE: my_category.HTTP_BULL on bull

Service detail

Last Updated: 01-10-2008 17:08:36
Updated every 120 seconds

Service	Status	Last Check	Duration	Information
my_category.**HTTP_BULL**	OK	0d 0h 1m 48s ago	0d 3h 31m 27s	HTTP ok: HTTP/1.1 200 OK - 0.059 second response time

Figure 5-21. HTTP_BSM customized service

5.1.4.11 Creating an Alerts Service

To receive SNMP traps from specific equipment, the corresponding monitoring service MUST exist in the Bull System Manager monitoring services list. If needed, you can create it.

Example

To create a service that receives **SNMP** traps from a remote SNMP agent, proceed as follows.

Note We assume that the new category `my_category` has been created with a host list containing the corresponding SNMP trap agent.
See *Creating a new Category* example, on page 89.

---

1. Click the **manage service** link of the `my_category` category.
2. In the **Manage Service** popup window, check **Create a new service**. Then click the **Create a new service** button.
3. Set the service_name to Traps.
4. Modify its description.
5. Set the monitoring on event parameter to **Yes**.

Then follow the steps described in *Integrating MIBs*, on page 153.

5.2 Configuring Servicegroups

Servicegroups organize services into functional domains, in order to filter topological views or for mapping in the BSM Console.

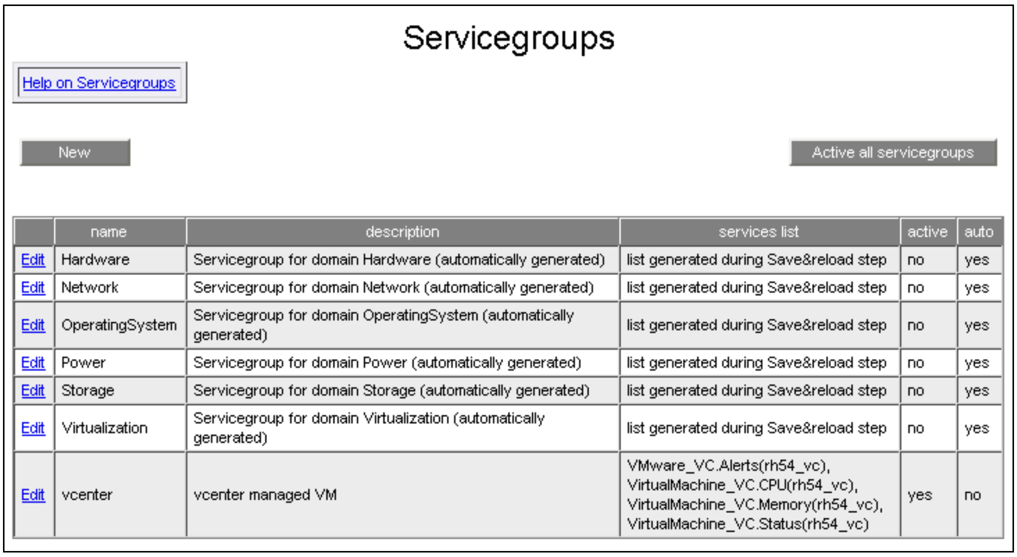
Default servicegroups definitions are automatically generated, containing instantiated services which belong to a category defined with a given monitoring domain (see Category Properties on page88).

WARNING:
Default servicegroups are defined as inactive and thus, not available in the BSM Console. The user must edit them with BSM Configuration tool to change the value of the **active** parameter .

User defined servicegroups can be defined, by selecting the services constituting the servicegroup.

To view servicegroups, click the **Servicegroups** link in the **Monitoring** part of the **Supervision** domain.

The screen below appears:



	name	description	services list	active	auto
Edit	Hardware	Servicegroup for domain Hardware (automatically generated)	list generated during Save&reload step	no	yes
Edit	Network	Servicegroup for domain Network (automatically generated)	list generated during Save&reload step	no	yes
Edit	OperatingSystem	Servicegroup for domain OperatingSystem (automatically generated)	list generated during Save&reload step	no	yes
Edit	Power	Servicegroup for domain Power (automatically generated)	list generated during Save&reload step	no	yes
Edit	Storage	Servicegroup for domain Storage (automatically generated)	list generated during Save&reload step	no	yes
Edit	Virtualization	Servicegroup for domain Virtualization (automatically generated)	list generated during Save&reload step	no	yes
Edit	vcenter	vcenter managed VM	VMware_VC.Alerts(rh54_vc), VirtualMachine_VC.CPU(rh54_vc), VirtualMachine_VC.Memory(rh54_vc), VirtualMachine_VC.Status(rh54_vc)	yes	no

Figure 5-22. Servicegroups

The table lists defined servicegroups. The servicegroup with the **auto** flag set to **yes** correspond to the default servicegroup when the others are user defined servicegroups. In the example, six default servicegroups are defined (**Hardware**, **Network**, **OperatingSystem**, **Power**, **Virtualizarion** and **Storage**) and one user servicegroup (**vcenter**). For the default servicegroups, the list of members is not displayed because it will be generated during the Save & Reload step, and includes all services matching the functional domain.

To create a user servicegroup, click the **New** button.

To edit a servicegroup, click the corresponding link.

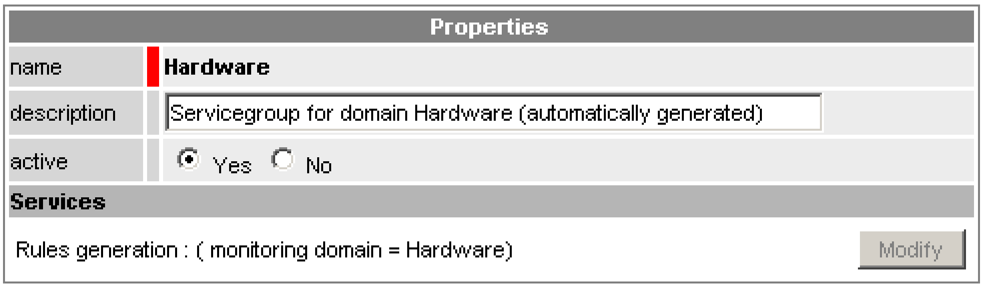
To activate all the servicegroups in one step, click the **Activate all servicegroups** button.

5.2.1 Default Servicegroup

5.2.1.1 Default Servicegroup edition

To edit a default servicegroup, click the **Edit** link for this servicegroup. A new window allows you to customize the description of the servicegroup or to enable/disable it. The list of member services cannot be modified, as it is generated when you save your configuration (Save & Reload action).

By default, the servicegroup is generated as an inactive servicegroup. To enable it, set **active** to **Yes**.



Properties

name	**Hardware**
description	Servicegroup for domain Hardware (automatically generated)
active	● Yes ○ No

Services

Rules generation : (monitoring domain = Hardware)

Figure 5-23. Hardware servicegroup edition

After editing:

- Click **OK** button to validate changes
- Or click **Cancel** button to return to the Servicegroups page without making any changes

5.2.1.2 Default Servicegroup generation

The default **Servicegroup** is generated during the **Save & Reload** phase by selecting the instantiated services corresponding to the monitoring domain.

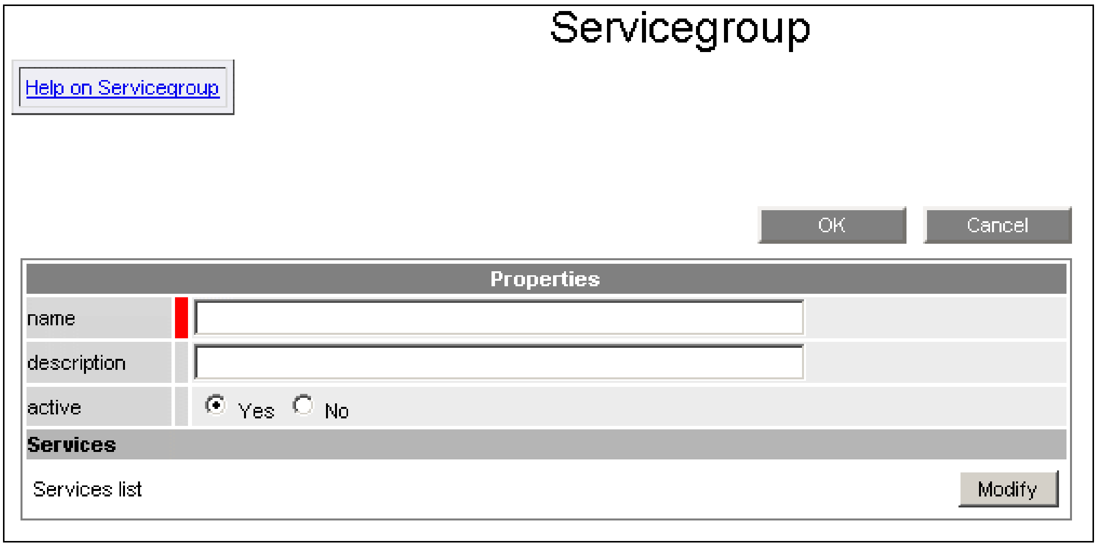
WARNING
All the services defined in the Bull System Manager Configuration do not correspond to the instantiated services. A service, for which the host is inactive for monitoring or for a specific monitoring domain (if monitoring domain matches the servicegroup rule) will not be used as servicegroup members.

5.2.2 User Servicegroup

5.2.2.1 Editing a User Servicegroup

To edit a user servicegroup, click the **Edit** link for this servicegroup.

To create a user servicegroup, click the **New** button in the **Servicegroups** page. The following window is displayed:



name	
description	
active	● Yes ○ No

Figure 5-24. User Servicegroup edition

The edition of a servicegroup contains two parts:

- Definition of general properties of the servicegroup (name, description)
- Definition of the list of services. This is done by clicking the **Modify** button in the bottom part of the window. A new page appears and is used to add service members (see detailed procedure below).

Once all the required fields have been updated

- Click **OK** button to validate the changes made
- Or click the **Cancel** button to return to the Servicegroups page without making the changes

5.2.2.2 Editing User Servicegroup Members

A separate window is used to edit the servicegroup members. It is divided into two parts, as shown below:

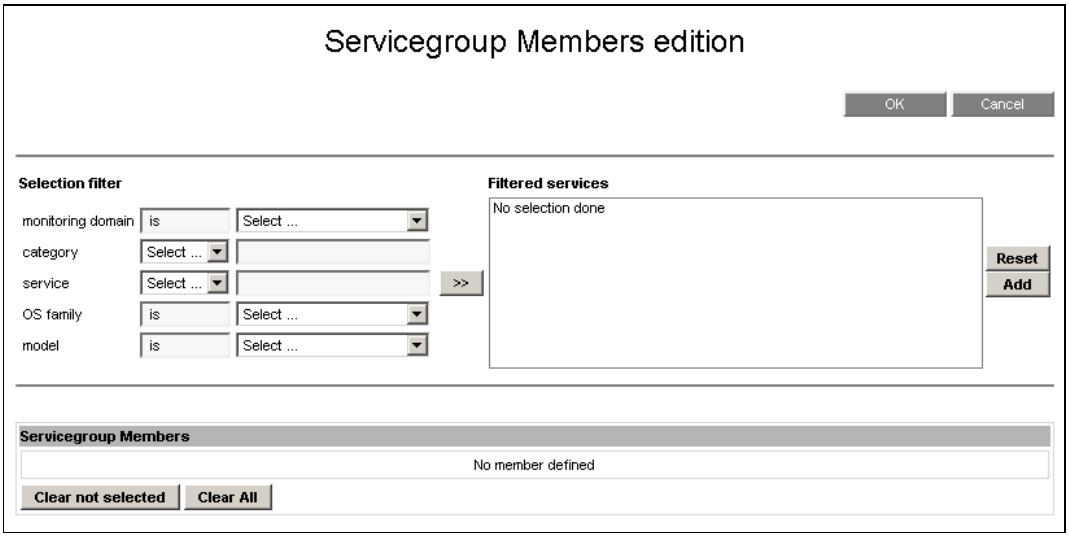


Figure 5-25. Editing Servicegroup Members

- The **Selection filter** part, which allows the user to select services according to five criteria: the monitoring domain, the name of the category, the name of the service, the OS or the model of the host.
  - First, choose the criteria. Several can be used:
    - For monitoring domain, OS and model, items are selected from the drop down lists.
    - For category and service, a string must be provided, after having selected the level of comparison (**is** for a complete match, **contains** for a partial match)
  - Then, click the **>>** button to see the corresponding selected services. In the **Filtered services** list, you can unselect some services.
  - Click the **Add** button to add the selected services to the list of members or click the **Reset** button to cancel the selection.
- The **Servicegroup members** part, is used to visualize and manage the list of services.
  - After adding selected services, you can:
    - Unselect some of them and clear them from the members list by clicking the **Clear not selected** button.
    - Remove all by clicking the **Clear all** button.

Note You can use different filters successively to combine services with unrelated criteria.

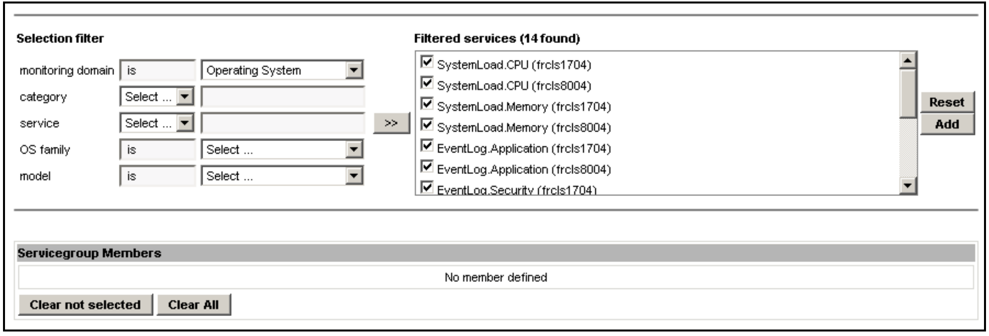
After editing the Servicegroup member details:

- Click the **OK** button to validate the changes
- Or click he **Cancel** button to return to the Servicegroup editing window without making the changes

Example:

1. Apply first filter: monitoring domain set to **'OperatingSystem'**
   - Set criteria,
   - Click the **>>** button.

   The following window is displayed.



Selection filter

monitoring domain: is — Operating System
category: Select ...
service: Select ...
OS family: is — Select ...
model: is — Select ...

Filtered services (14 found)

☑ SystemLoad.CPU (frcls1704)
☑ SystemLoad.CPU (frcls8004)
☑ SystemLoad.Memory (frcls1704)
☑ SystemLoad.Memory (frcls8004)
☑ EventLog.Application (frcls1704)
☑ EventLog.Application (frcls8004)
☑ EventLog.Security (frcls1704)

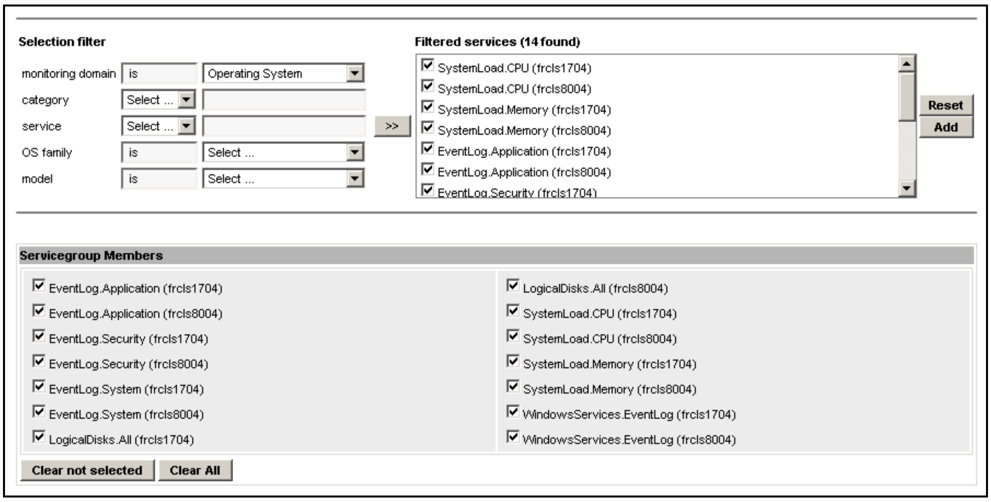
Servicegroup Members

No member defined

Figure 5-26. Servicegroup Members: filtering on monitoring domain

   - Click the **Add** button to add the selected services to the list of members

   The selected services appear in the **Servicegroup Members** section, as shown below.



Selection filter

monitoring domain: is — Operating System
category: Select ...
service: Select ...
OS family: is — Select ...
model: is — Select ...

Filtered services (14 found)

☑ SystemLoad.CPU (frcls1704)
☑ SystemLoad.CPU (frcls8004)
☑ SystemLoad.Memory (frcls1704)
☑ SystemLoad.Memory (frcls8004)
☑ EventLog.Application (frcls1704)
☑ EventLog.Application (frcls8004)
☑ EventLog.Security (frcls1704)

Servicegroup Members

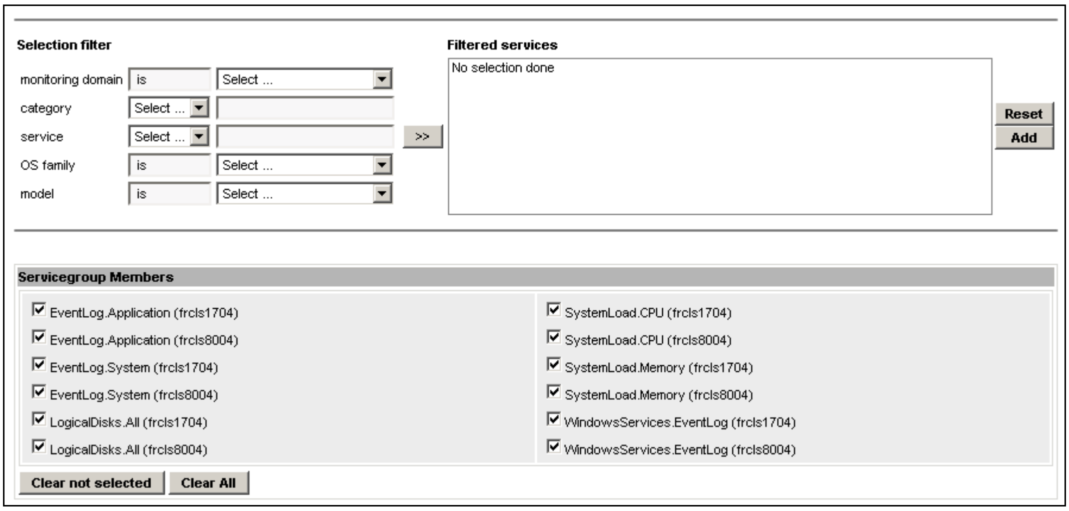
☑ EventLog.Application (frcls1704)
☑ EventLog.Application (frcls8004)
☑ EventLog.Security (frcls1704)
☑ EventLog.Security (frcls8004)
☑ EventLog.System (frcls1704)
☑ EventLog.System (frcls8004)
☑ LogicalDisks.All (frcls1704)
☑ LogicalDisks.All (frcls8004)
☑ SystemLoad.CPU (frcls1704)
☑ SystemLoad.CPU (frcls8004)
☑ SystemLoad.Memory (frcls1704)
☑ SystemLoad.Memory (frcls8004)
☑ WindowsServices.EventLog (frcls1704)
☑ WindowsServices.EventLog (frcls8004)

Figure 5-27. Servicegroup Members: add of selected services

2. Reset filter

   – Click the **Reset** button

   The Filtered services selection box is empty.
   The **Servicegroup Members** section contains the services previously selected.



Selection filter

monitoring domain: is — Select ...
category: Select ...
service: Select ...
OS family: is — Select ...
model: is — Select ...

Filtered services

No selection done

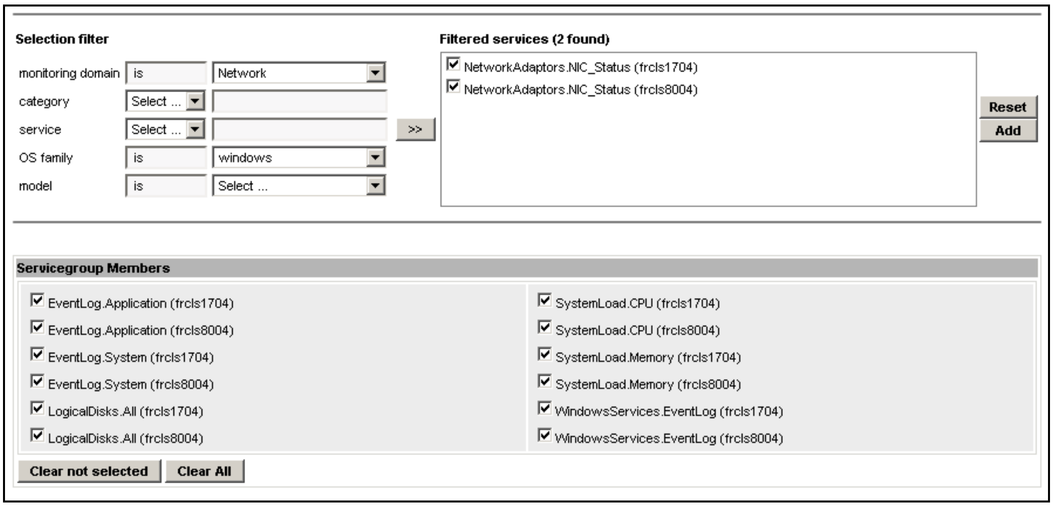
Servicegroup Members

☑ EventLog.Application (frcls1704)
☑ EventLog.Application (frcls8004)
☑ EventLog.System (frcls1704)
☑ EventLog.System (frcls8004)
☑ LogicalDisks.All (frcls1704)
☑ LogicalDisks.All (frcls8004)
☑ SystemLoad.CPU (frcls1704)
☑ SystemLoad.CPU (frcls8004)
☑ SystemLoad.Memory (frcls1704)
☑ SystemLoad.Memory (frcls8004)
☑ WindowsServices.EventLog (frcls1704)
☑ WindowsServices.EventLog (frcls8004)

Figure 5-28. Servicegroup members: filter reset

3. Apply a second filter: monitoring domain set to **Network** and **OS** family set to **Windows**.
   – Set criteria
   – Click the **>>** button

The following window is displayed:



Selection filter

monitoring domain: is — Network
category: Select ...
service: Select ...
OS family: is — windows
model: is — Select ...

Filtered services (2 found)

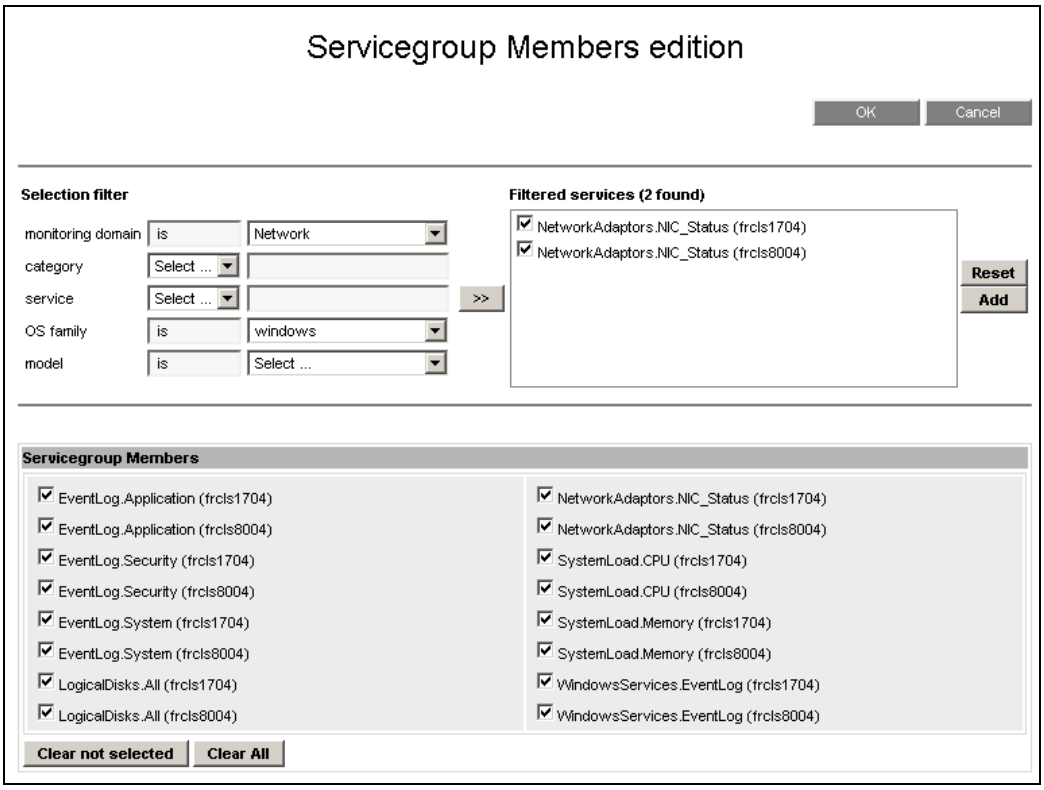
☑ NetworkAdaptors.NIC_Status (frcls1704)
☑ NetworkAdaptors.NIC_Status (frcls8004)

Servicegroup Members

☑ EventLog.Application (frcls1704)
☑ EventLog.Application (frcls8004)
☑ EventLog.System (frcls1704)
☑ EventLog.System (frcls8004)
☑ LogicalDisks.All (frcls1704)
☑ LogicalDisks.All (frcls8004)
☑ SystemLoad.CPU (frcls1704)
☑ SystemLoad.CPU (frcls8004)
☑ SystemLoad.Memory (frcls1704)
☑ SystemLoad.Memory (frcls8004)
☑ WindowsServices.EventLog (frcls1704)
☑ WindowsServices.EventLog (frcls8004)

Figure 5-29. Servicegroup Members: filter section on for monitoring domain and OS family

– Click the **Add** button to add the selected services to the list of members:



Servicegroup Members edition

Selection filter

monitoring domain	is	Network
category	Select ...	
service	Select ...	
OS family	is	windows
model	is	Select ...

Filtered services (2 found)

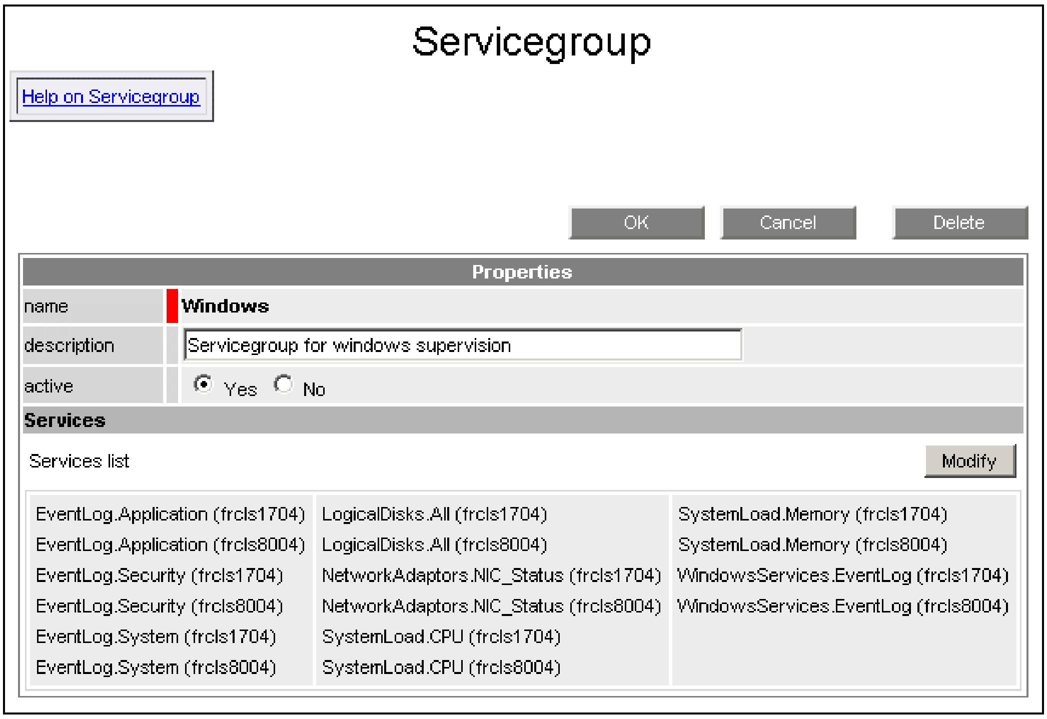
- ☑ NetworkAdaptors.NIC_Status (frcls1704)
- ☑ NetworkAdaptors.NIC_Status (frcls8004)

Servicegroup Members

- ☑ EventLog.Application (frcls1704)
- ☑ EventLog.Application (frcls8004)
- ☑ EventLog.Security (frcls1704)
- ☑ EventLog.Security (frcls8004)
- ☑ EventLog.System (frcls1704)
- ☑ EventLog.System (frcls8004)
- ☑ LogicalDisks.All (frcls1704)
- ☑ LogicalDisks.All (frcls8004)
- ☑ NetworkAdaptors.NIC_Status (frcls1704)
- ☑ NetworkAdaptors.NIC_Status (frcls8004)
- ☑ SystemLoad.CPU (frcls1704)
- ☑ SystemLoad.CPU (frcls8004)
- ☑ SystemLoad.Memory (frcls1704)
- ☑ SystemLoad.Memory (frcls8004)
- ☑ WindowsServices.EventLog (frcls1704)
- ☑ WindowsServices.EventLog (frcls8004)

Figure 5-30. Servicegroup member: Add Windows services

4. Click the **OK** button to validate the Servicegroup members changes and return to the servicegroup window:



Servicegroup

Properties

name	**Windows**
description	Servicegroup for windows supervision
active	● Yes ○ No

Services

Services list

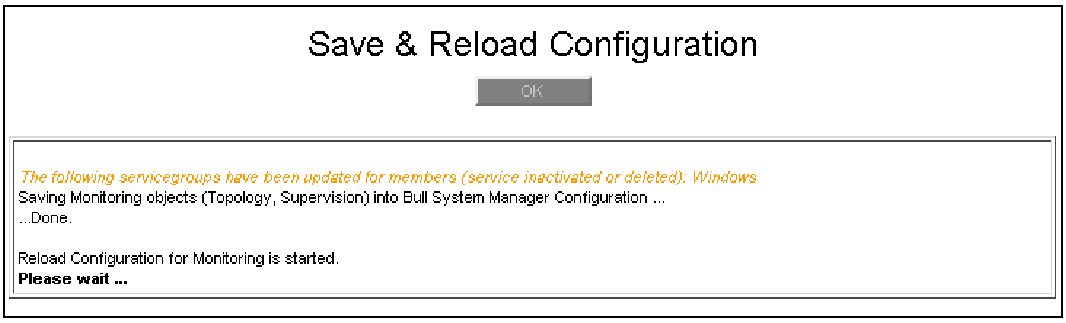
EventLog.Application (frcls1704)
EventLog.Application (frcls8004)
EventLog.Security (frcls1704)
EventLog.Security (frcls8004)
EventLog.System (frcls1704)
EventLog.System (frcls8004)
LogicalDisks.All (frcls1704)
LogicalDisks.All (frcls8004)
NetworkAdaptors.NIC_Status (frcls1704)
NetworkAdaptors.NIC_Status (frcls8004)
SystemLoad.CPU (frcls1704)
SystemLoad.CPU (frcls8004)
SystemLoad.Memory (frcls1704)
SystemLoad.Memory (frcls8004)
WindowsServices.EventLog (frcls1704)
WindowsServices.EventLog (frcls8004)

5. Click the **OK** button to apply changes for the Windows servicegroup.

5.2.2.3 User Servicegroup checking

User Servicegroups are checked during the **Save & Reload** phase to avoid inconsistent definitions, that can occur if one of the members of the servicegroup is inactivated (service directly inactivated or host) after the servicegroup configuration has been changed.

During the check, if such a service is found, it is removed from the final servicegroup object. The Administrator is warned by an message, as shown in the example below:


Save & Reload Configuration

The following servicegroups have been updated for members (service inactivated or deleted): Windows
Saving Monitoring objects (Topology, Supervision) into Bull System Manager Configuration ...
...Done.

Reload Configuration for Monitoring is started.
Please wait ...

Figure 5-31. User Servicegroup Control

5.3 Configuring the Monitoring of Hosts/Hostgroups/Managers

To configure the monitoring of hosts, hostgroups and managers, click the corresponding link menu in the Monitoring part of the Supervision tab and modify the properties.

5.3.1 Host Properties

Host Properties	Description
host management	Monitoring status (active, inactive). Default value: **active**. **Active** status means that the host is monitored with its associated services. Its node is animated in the Management Tree and in all corresponding menus. **Inactive** status means that the host is not monitored. It is visible in the Management Tree but its node is not animated and only the Platform menu is available (for NovaScale 5000 & 6000 and NovaScale Blade series hosts). In the Bull System Manager Console Applications pane the host appears with the PENDING monitoring status. This field may be used to activate/deactivate monitoring on a given host temporarily.
Ping checking	To enable host checking with ping command. Default = **yes** **Note**: if disabled, check of the host is only made with the services defined for this host. This is useful when the host is unreachable by ping.
OS monitoring	To enable or disable OS services monitoring. Default = **yes**
Hardware monitoring	To enable or disable hardware services monitoring. Default = **yes**
Virtualization monitoring	To enable or disable virtualization monitoring. Default = **yes**
Storage monitoring	To enable or disable storage monitoring. Default = **yes**
Network monitoring	To enable or disable network monitoring. Default = ***yes***
Power Monitoring	To enable or disable power monitoring. Default = **yes**
Syslog Monitoring	Syslog Monitoring status (see *Syslog Monitoring host properties* on page 136). Default value: **yes**
Syslog Filter	Short name of a Syslog Filter (see *Syslog Monitoring host properties* on page 136). Default = **none**

Host Properties	Description
Notification enabled	To enable or disable all the notifications. Default = **yes**
Enable SNMP trap	To enable notifications by **SNMP** trap. Default = **yes**
notification period	Short name of the time that determines when notifications about this host must be sent out (**24x7**, **work hours**, **non-work hours** and **none**). Default value: **24x7**, which means **all the time**. **work hours** means from Monday to Friday between 09:00 and 17:00. **non-work hours** means all day Saturday and Sunday and from 00:00 to 09:00 and from 17:00 to 24:00 on other days. **none** means no time is a good time.
re-notification interval	Number of minutes to wait before re-notifying the contact that the host is still down. Default value: **240**.
notify if down	Notify contacts when this host is down? Default value: **yes**.
notify if unreachable	Notify contacts when this host is unreachable? Default value: **yes**.
notify if recovery	Notify contacts when this host is recovering? Default value: **yes**.
notify on downtime start/stop	Notify contacts when scheduled downtime is started or stopped for this host
contactGroup	contact groups Default value: **mgt-admins** **Note**: contact group is also defined at the Hostgroup level. Thus, the contact group for a host is the set of contacts defined at the host level and those defined at the hostgroup level.

Note When a given type of host monitoring is disabled, all categories that have set their **monitoring_domain** to that domain are deactivated.
If host monitoring is disabled, all the properties are disabled.
Categories and associated services are not visible in the Management Tree.

5.3.2 Hostgroup Properties

Hostgroup Properties	Description
Hardware monitoring	To enable or disable hardware services monitoring (only for hardware platforms).
Operating System monitoring	To enable or disable OS services monitoring.
Network monitoring	To enable or disable network services monitoring.
Storage monitoring	To enable or disable storage services monitoring.
Virtualization monitoring	To enable or disable virtualization monitoring.
Hardware monitoring	To enable or disable hardware monitoring.
Power monitoring	To enable or disable power monitoring
contactGroup	contact groups

Note Disabling a given type of monitoring for a hostgroup results in the disabling of all corresponding categories for each host of the hostgroup. Categories and associated services are not visible in the Management Tree.

5.3.3 Manager Properties

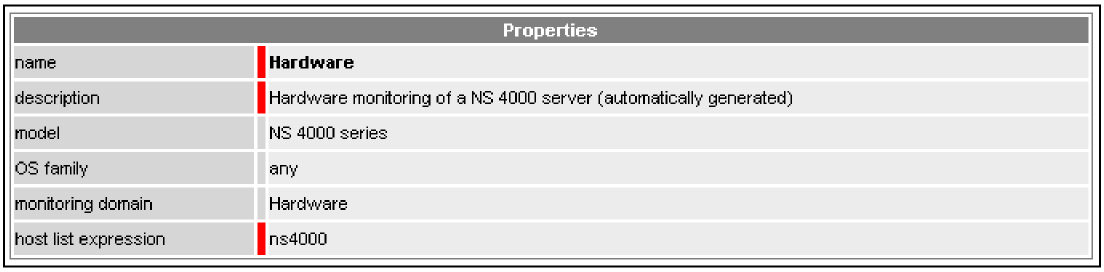
Manager Properties	Description
Hardware monitoring	To enable or disable hardware services monitoring related to the manager.
Virtualization monitoring	To enable or disable virtualization monitoring.

Note The **Hardware monitoring** and **Virtualization monitoring** properties are displayed only if the corresponding manager is a Hardware or Virtualization manager.
Disabling a given type of monitoring for a manager results in the disabling of all services dependent on it, by setting the **monitoring_status** attribute to inactive. The corresponding categories are always activated; some services could be independent of the manager. Associated services are no longer visible in the Management Tree.

5.3.4 Example: Monitoring NS 4000 Hardware

As described above, the host, hostgroup and manager have supervision attributes that affect service behavior.

- Disabling hardware monitoring at host level will result in deactivation of all hardware categories specified for this host, i.e. all categories for which the monitoring domain is set to **Hardware**, as shown in the following figure. Deactivation of these categories results in the deactivation of all associated services.



Properties	
name	**Hardware**
description	Hardware monitoring of a NS 4000 server (automatically generated)
model	NS 4000 series
OS family	any
monitoring domain	Hardware
host list expression	ns4000

Figure 5-32. Hardware category monitoring domain

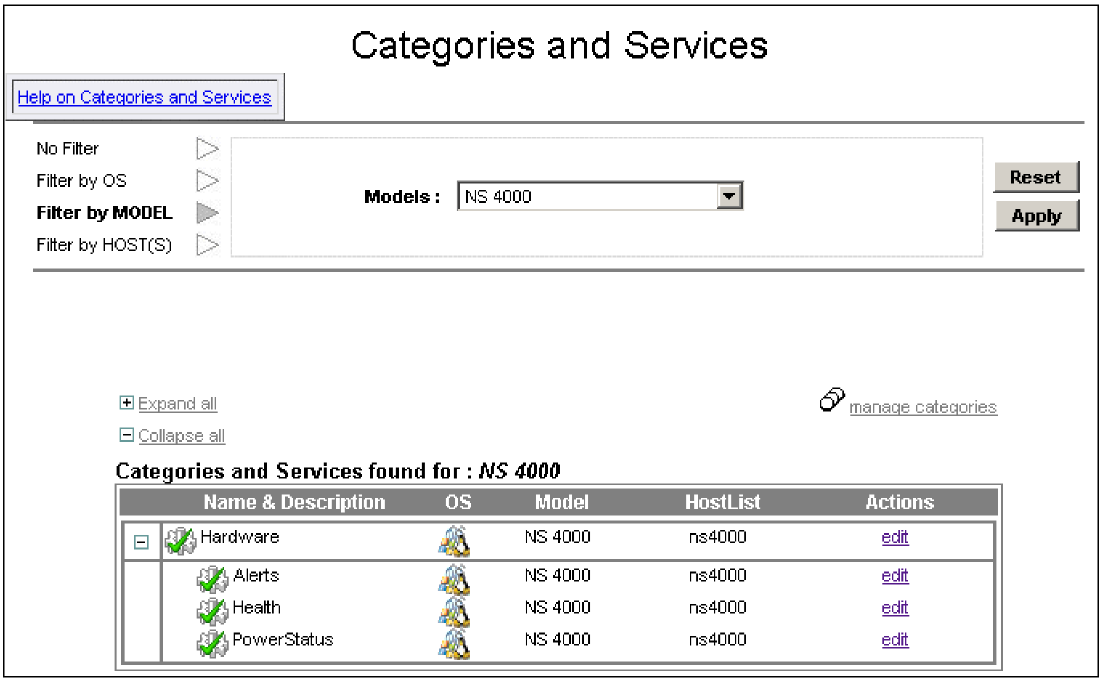
- Disabling hardware monitoring at hostgroup level will result in the deactivation of all hardware services specified for all hosts for this hostgroup, using the same mechanism as described above;
- Disabling hardware monitoring at manager level will result in deactivation of all hardware services dependent on this manager. Setting hardware monitoring of a manager to **no** is equivalent to setting the status of all corresponding services to **no**.

The following example explains how to enable/disable hardware monitoring for a NS4000 server at topology object level.

There are two ways of monitoring NS 4000 server hardware:

- By setting Out-of-Band attributes for the host: this will lead to automatic instantiation of the **Alert** and **PowerStatus** services (category Hardware);
- Or by configuring an **ISM** type hardware manager, managing the **NS 4000** server: this will lead to the automatic instantiation of the Health service (category Hardware);

The following figure shows the services applied to the **ns4000** host, managed by the **ISM** manager admism:



Categories and Services

Help on Categories and Services

- No Filter ▷
- Filter by OS ▷
- **Filter by MODEL** ▶
- Filter by HOST(S) ▷

Models : NS 4000

Reset **Apply**

⊞ Expand all

⊟ Collapse all

manage categories

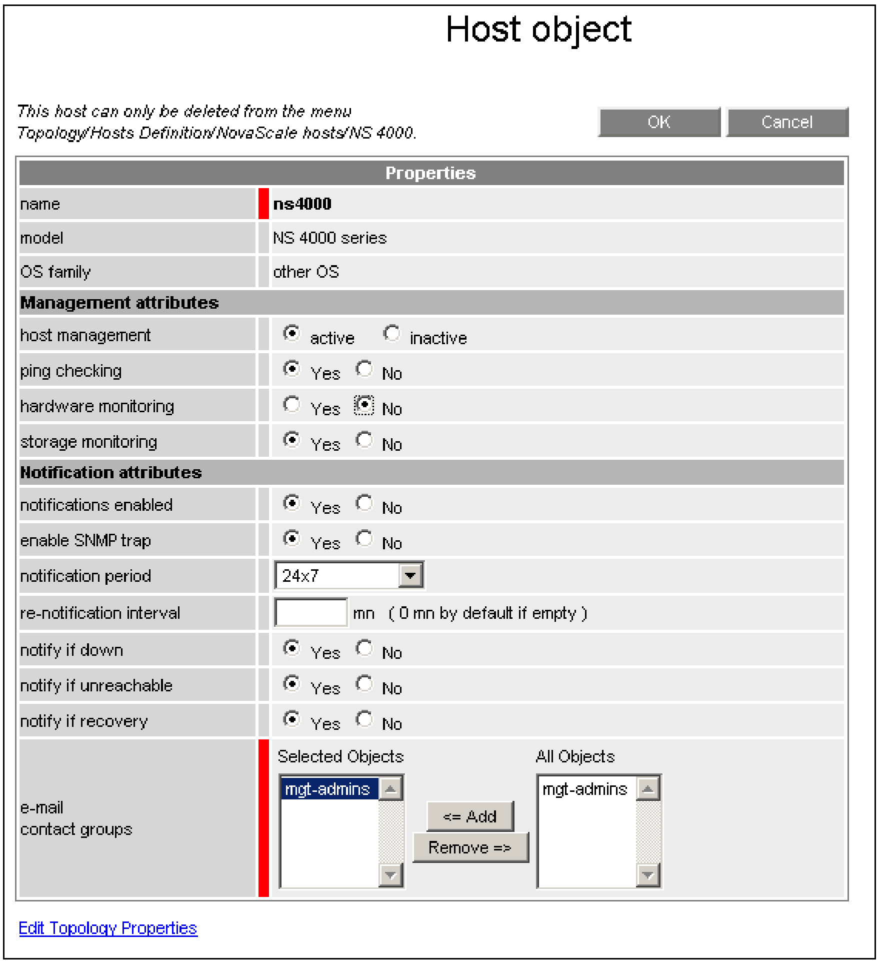
Categories and Services found for : *NS 4000*

	Name & Description	OS	Model	HostList	Actions
⊟	Hardware		NS 4000	ns4000	edit
	Alerts		NS 4000	ns4000	edit
	Health		NS 4000	ns4000	edit
	PowerStatus		NS 4000	ns4000	edit

Figure 5-33. NS4000 Hardware category and services

5.3.4.1 Disabling Hardware Monitoring at Host Level

Setting the **hardware monitoring** attribute to **No**, as shown in the following figure, will result in the deactivation of all hardware categories and associated services for this **ns4000** host.



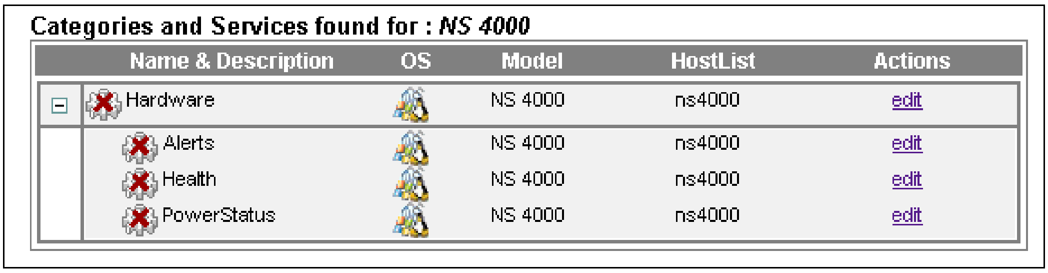
Host object

This host can only be deleted from the menu Topology/Hosts Definition/NovaScale hosts/NS 4000.

Properties	
name	**ns4000**
model	NS 4000 series
OS family	other OS
Management attributes	
host management	● active ○ inactive
ping checking	● Yes ○ No
hardware monitoring	○ Yes ● No
storage monitoring	● Yes ○ No
Notification attributes	
notifications enabled	● Yes ○ No
enable SNMP trap	● Yes ○ No
notification period	24x7
re-notification interval	mn (0 mn by default if empty)
notify if down	● Yes ○ No
notify if unreachable	● Yes ○ No
notify if recovery	● Yes ○ No
e-mail contact groups	Selected Objects: mgt-admins All Objects: mgt-admins

Figure 5-34. Host hardware monitoring status

All Hardware services linked to the **ns4000** host appear deactivated, as shown by the following figure:

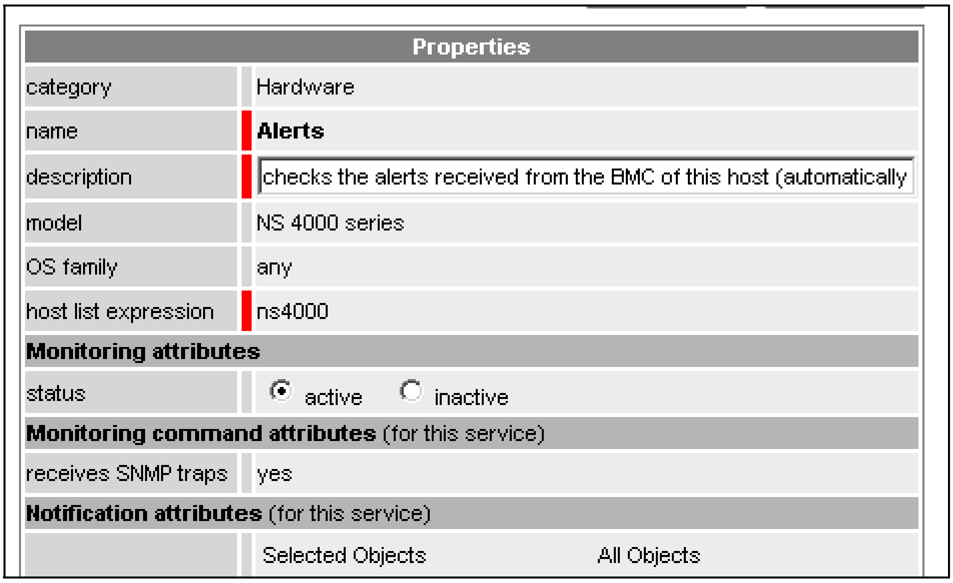


Categories and Services found for : *NS 4000*

Name & Description	OS	Model	HostList	Actions
Hardware		NS 4000	ns4000	edit
Alerts		NS 4000	ns4000	edit
Health		NS 4000	ns4000	edit
PowerStatus		NS 4000	ns4000	edit

Figure 5-35. NS4000 services deactivation

The services are deactivated because the **monitoring domain** of the Hardware category is **Hardware** and the **hardware monitoring status** of the host is set to **No**. The status of the service is always set to active as shown in the following figure:



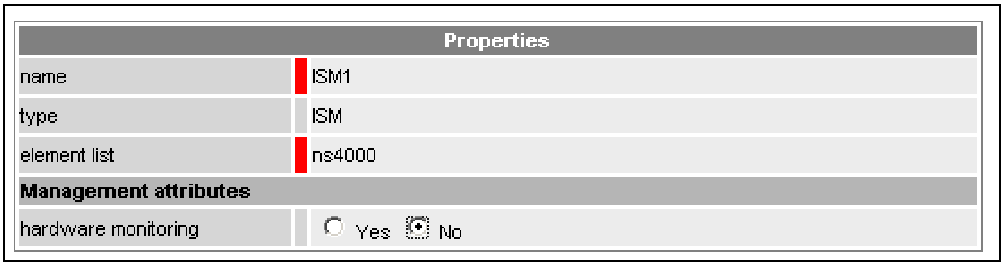
Properties	
category	Hardware
name	**Alerts**
description	checks the alerts received from the BMC of this host (automatically
model	NS 4000 series
OS family	any
host list expression	ns4000
Monitoring attributes	
status	● active ○ inactive
Monitoring command attributes (for this service)	
receives SNMP traps	yes
Notification attributes (for this service)	
	Selected Objects All Objects

Figure 5-36. NS4000 Alert service status

In the Management Tree, the hardware categories and associated services are no longer visible.

5.3.4.2 Disabling Hardware Monitoring at Manager Level

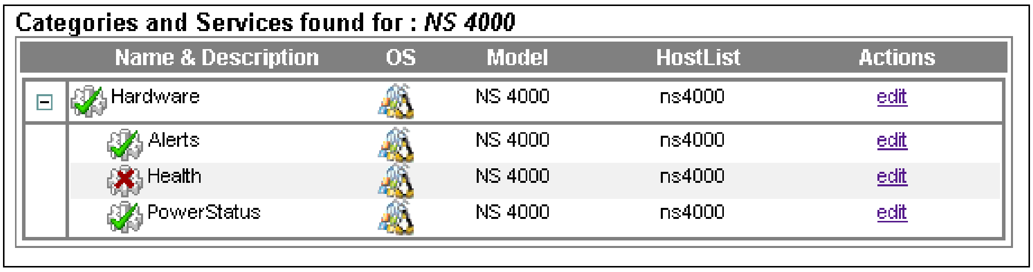
Setting the **hardware monitoring** attribute to **No**, as shown in the following figure, will result in the deactivation of the Health service associated with the ns4000 host.



Properties	
name	ISM1
type	ISM
element list	ns4000
Management attributes	
hardware monitoring	○ Yes ● No

Figure 5-37. Manager hardware monitoring status

Only the Health service dependent on the ISM manager is deactivated, as illustrated in the following figure:

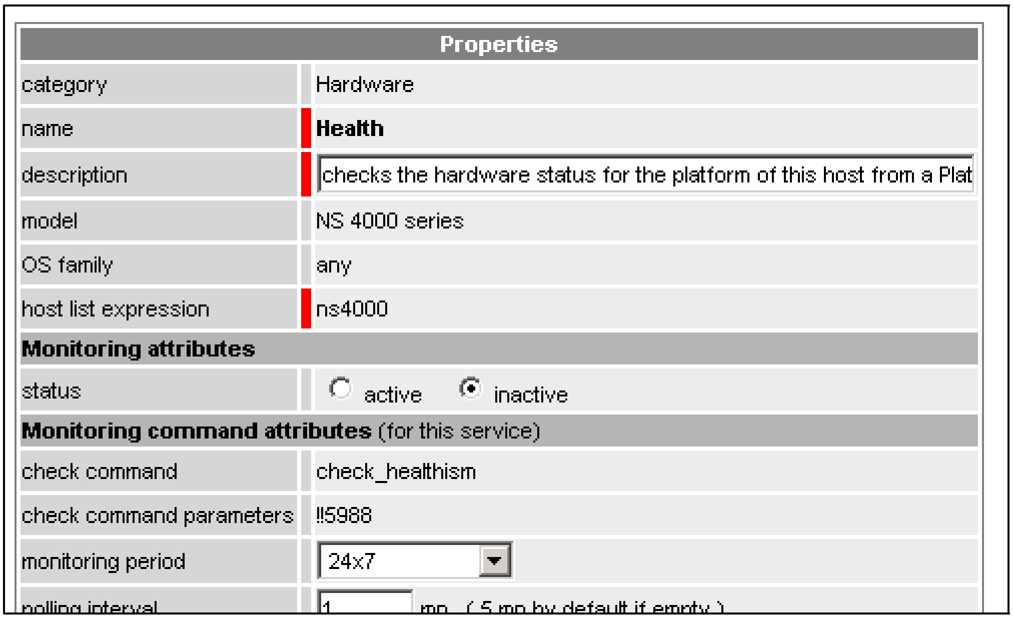


Categories and Services found for : *NS 4000*

Name & Description	OS	Model	HostList	Actions
⊟ ✓ Hardware		NS 4000	ns4000	edit
✓ Alerts		NS 4000	ns4000	edit
✗ Health		NS 4000	ns4000	edit
✓ PowerStatus		NS 4000	ns4000	edit

Figure 5-38. NS4000 Health service deactivation

The service is deactivated now because the status has been set to **Inactive** when the Hardware manager properties were edited, as displayed in the following figure. The monitoring status of the corresponding host is always set to **Yes**.



Properties	
category	Hardware
name	**Health**
description	checks the hardware status for the platform of this host from a Plat
model	NS 4000 series
OS family	any
host list expression	ns4000
Monitoring attributes	
status	○ active ● inactive
Monitoring command attributes (for this service)	
check command	check_healthism
check command parameters	!!5988
monitoring period	24x7
polling interval	1 mn (5 mn by default if empty)

Figure 5-39. NS4000 Health service status

In the Management Tree, the **Hardware** category is visible but the **Health** service is not displayed. If the **Health** service is the only service associated with the **Hardware** category, no child is displayed for this category.

5.4 Syslog Monitoring

Syslog events are collected on BSMAgent hosts and are sent to the BSMServer as SNMP traps. On Linux hosts, the syslog events are collected with syslog-ng; **syslog-ng application is exclusive with syslogd**. On AIX hosts, the syslog events are collected with **syslogAixErr**. The syslog event collection and the sending of SNMP traps can be stopped or started on demand. The events can be filtered at source during collection time. To do this, filters are prepared on the BSMServer and sent to the BSMAgent hosts to be applied to the event collection.

When several BSMServers manage the same BSMAgent, it is the last filter sent to the BSMAgent that runs.

To configure hosts monitoring and syslog filters, click the corresponding link menu in the **Monitoring** part of the **Supervision** tab and modify the properties.

5.4.1 Host Properties

Host Properties	Description
Syslog Monitoring	Syslog Monitoring status. Default value: **yes**. **Yes***:* means that collection events and sending traps to this server will be started. **No***:* means that collection events and sending of traps to this server will be stopped. This field may be used to start/stop monitoring on a given host temporarily.
Syslog Filter	Short name for a Syslog Filter. Default = **none** **Note**: Linux hosts: only **Syslog** Filters of type **LINUX-syslogng** will be available. Aix hosts: only **Syslog** Filters of type **AIX-errpt** will be available.

Table 5-9. Syslog Monitoring host properties

5.4.2 Syslog Filter Properties

The filters have a common part and a specific part for each type of filter.

Common Syslog Filter Properties

Syslog Filter Properties	Description
Syslog filter type	Type of the Syslog Filter, depends on the OS of the host. Default value: *none*. **LINUX-syslogng**: can be assigned to Linux agents. **AIX-errpt**: can be assigned to Aix agents. Each type of filter has its own properties.

Table 5-10. Syslog Filters common properties

Note When the **syslog filter type** is not set, only the common properties are displayed.

Linux Syslog Filter Properties

Syslog Filter Properties	Description
Level list	Match messages having one of the listed level codes. Default value: **empty**. A list of levels taken in the **BSM-SYSLOG-MIB** mib (see Level values) **If empty**, messages are not filtered on level code.
Facility list	Match messages having one of the listed facility codes. Default value: **empty**. A list of facilities taken in the **BSM-SYSLOG-MIB** mib (see Facility values) **If empty**, messages are not filtered on the facility code.

Table 5-11. Linux Syslog Filters properties

Note When the **syslog filter type** is set to **LINUX-syslogng**, the common properties and the Linux properties are displayed.

Aix Syslog Filter Properties

Syslog Filter Properties	Description
Class / facility mapping	To translate ErrorClass from errpt into a facility of **BSM-SYSLOG-MSG mib**. A list of four pairs (ErrorClass, facility) (see ErrorClass values and Facility values).
Type / level mapping	To translate ErrorType from errpt into **BSM-SYSLOG-MSG** mib level. A list of six pairs (ErrorType, level) (see ErrorType values and Level values).
Filter scope	Scope of the AIX-errpt syslog filter Default value: **none**. **ErrorId**: messages are filtered on the errorID. **ErrorLabel**: messages are filtered on the errorID. **other**: messages are filtered on the errorClass and/or the ErrorType and/or the ResourceName. **none**: messages are not filtered. Mapping properties are always applied.
ErrorClass list	Match messages having one of the listed ErrorClass values. Default value: **empty** (idem no filter). A list of ErrorClass values (see ErrorClass values). **If empty**, messages are not filtered on ErrorClass attribut.
ErrorType list	Match messages having one of the listed ErrorType values. Default value: **empty** (idem no filter). A list of ErrorType values (see ErrorType values). **If empty**, messages are not filtered on ErrorType attribut.
ResourceName list	Match messages having one of listed ResourceName values. Default value: **empty** (idem no filter). A list of ResourceName values (see the Aix errpt documentation). **If empty**, messages are not filtered using ResourceName attribut.
ErrorId list	Match messages having/not having one of the listed ErrorId values depending on **Include / exclude the list** property. Default value: **empty** (idem no filter). A list of ErrorId values (see Aix the errpt documentation). **If empty**, messages are not filtered on ErrorId attribut.
ErrorLabel list	Match messages having/not having one of the listed ErrorLabel values depending on **Include / exclude the list** property. Default value: **empty** (idem no filter). A list of ErrorLabel values (see the Aix errpt documentation). **If empty**, messages are not filtered on ErrorLabel attribut.

Syslog Filter Properties	Description
Include / exclude the list	Include / exclude matching messages. Default value: **include** **include**: only the events whose attribute value is in the corresponding list will be forwarded **exclude**: only the events whose attribute value is not in the corresponding list will be forwarded

Table 5-12. Syslog Filters Aix properties

Note When the **syslog filter type** is set to **AIX-errp**t, the common properties and the Aix properties are displayed.
Depending on the **filter scope**, only the corresponding properties are displayed.

Values of level in BSM-SYSLOG-MIB mib

Level	Description
Emerg	Emergency; system is unusable
Alert	Action must be taken immediately
Crit	Critical condition
Err	Error condition
warning	Warning condition
Notice	Normal but significant condition
Info	Informational message
Debug	Debug-level messages

Table 5-13. Level values

Values of facility in BSM-SYSLOG-MIB mib

facility	Description
kern	Kernel messages
user	User-level messages
mail	Mail system messages
daemon	System daemons messages
auth	Authorization messages
syslog	Syslogd messages
lpr	Line printer subsystem messages
news	Network news subsystem messages
uucp	UUCP subsystem messages
cron	Clock daemon messages
authpriv	Security / authorization messages
ftp	Ftp daemon messages
local0	

facility	Description
local1	
local2	
local3	
local4	
local5	
local	
local7	

Table 5-14. Facility values

Values of errpt ErrorClass

ErrorClass	Description
H	Hardware
S	Software
O	Iinformational / errlogger
U	Undetermined

Table 5-15. ErrorClass values

Values of errpt ErrorType

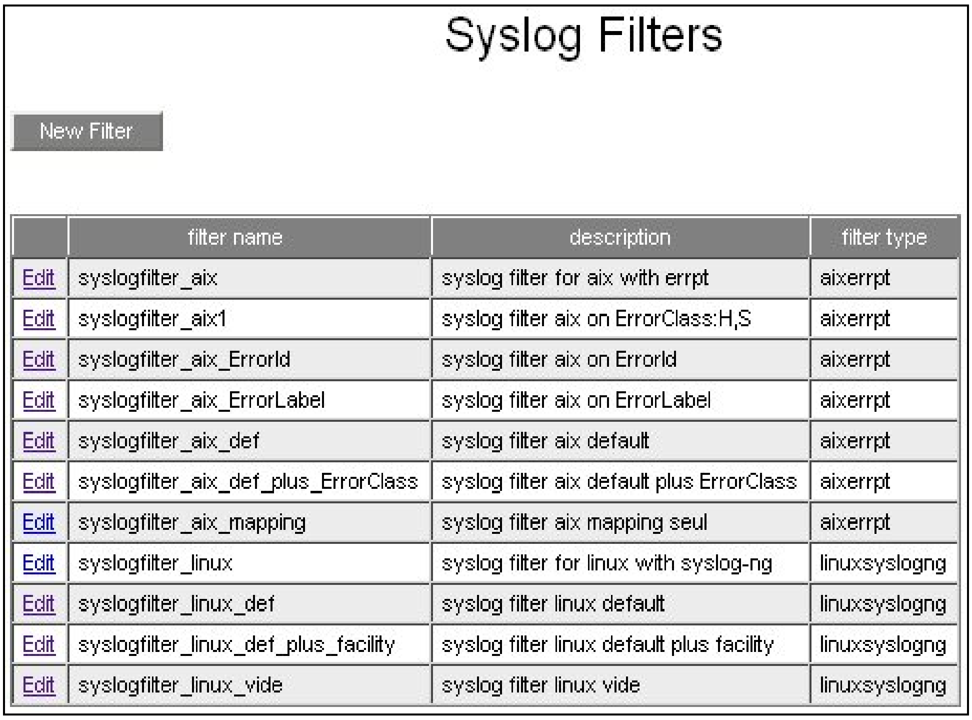
ErrorType	Description
PEND	Pending
PERF	Performance
PERM	Permanent
UNKN	Unknown
TEMP	Temporary
INFO	Informational

Table 5-16. ErrorType values

5.4.3 Example: Monitoring Linux Host

5.4.3.1 Creating Linux Syslog Filter

To edit syslog filters, click the Syslog Filters item in the Monitoring part of the Supervision tab. The list of configured syslog filters appears, as in the following example:



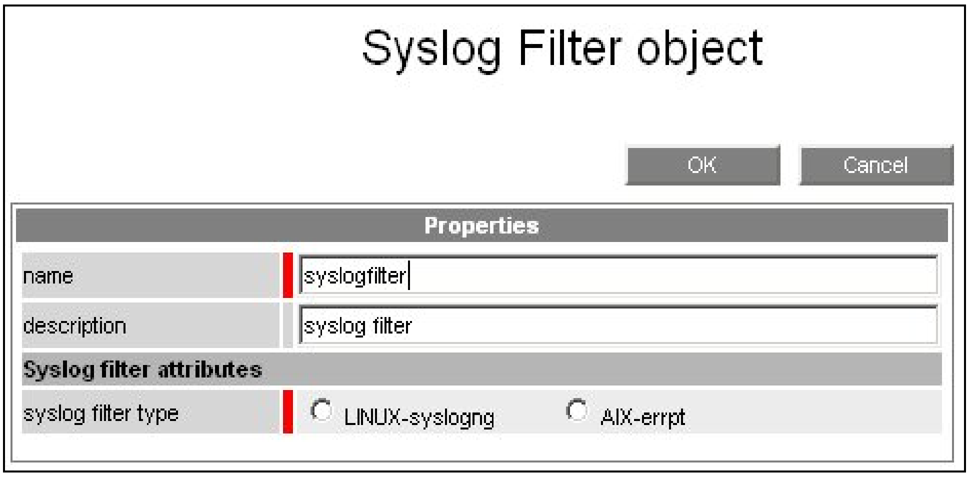
Syslog Filters

	filter name	description	filter type
Edit	syslogfilter_aix	syslog filter for aix with errpt	aixerrpt
Edit	syslogfilter_aix1	syslog filter aix on ErrorClass:H,S	aixerrpt
Edit	syslogfilter_aix_ErrorId	syslog filter aix on ErrorId	aixerrpt
Edit	syslogfilter_aix_ErrorLabel	syslog filter aix on ErrorLabel	aixerrpt
Edit	syslogfilter_aix_def	syslog filter aix default	aixerrpt
Edit	syslogfilter_aix_def_plus_ErrorClass	syslog filter aix default plus ErrorClass	aixerrpt
Edit	syslogfilter_aix_mapping	syslog filter aix mapping seul	aixerrpt
Edit	syslogfilter_linux	syslog filter for linux with syslog-ng	linuxsyslogng
Edit	syslogfilter_linux_def	syslog filter linux default	linuxsyslogng
Edit	syslogfilter_linux_def_plus_facility	syslog filter linux default plus facility	linuxsyslogng
Edit	syslogfilter_linux_vide	syslog filter linux vide	linuxsyslogng

Figure 5-40. Syslog Filters configuration window

Note See *Create / Edit / Delete Resources*, on page 21 for details.

To create a syslog filter, click the **New Filter** button, the following window appears:



Syslog Filter object

Properties

name	syslogfilter
description	syslog filter

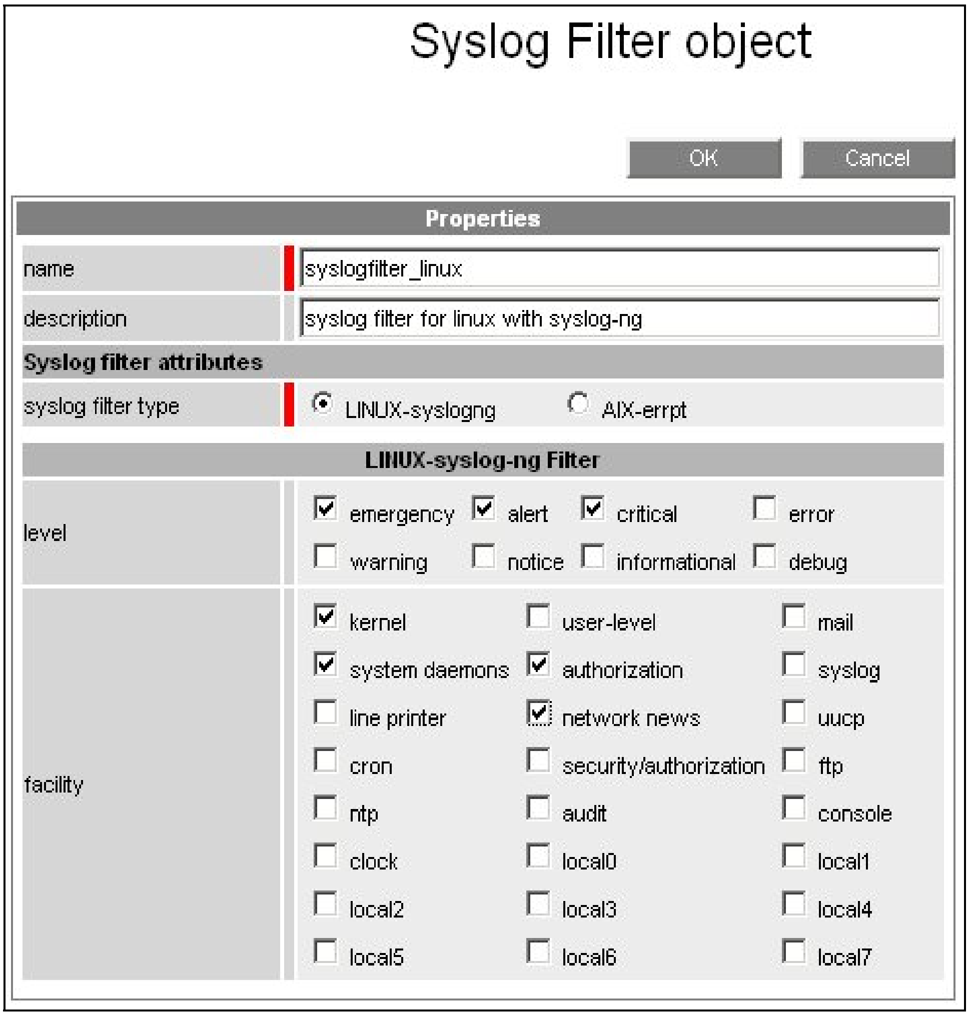
Syslog filter attributes

syslog filter type ○ LINUX-syslogng ○ AIX-errpt

Figure 5-41. Common Syslog Filter properties

Set the **syslog filter type** attribute to **LINUX-syslogng**.

As shown in the following example, the Linux Syslog Filter properties are displayed:



Properties

name	syslogfilter_linux
description	syslog filter for linux with syslog-ng

Syslog filter attributes

syslog filter type: ● LINUX-syslogng ○ AIX-errpt

LINUX-syslog-ng Filter

level:

☑ emergency	☑ alert	☑ critical	□ error
□ warning	□ notice	□ informational	□ debug

facility:

☑ kernel	□ user-level	□ mail
☑ system daemons	☑ authorization	□ syslog
□ line printer	☑ network news	□ uucp
□ cron	□ security/authorization	□ ftp
□ ntp	□ audit	□ console
□ clock	□ local0	□ local1
□ local2	□ local3	□ local4
□ local5	□ local6	□ local7

Figure 5-42. Linux Syslog Filter properties

Set the **level** list by checking the buttons.

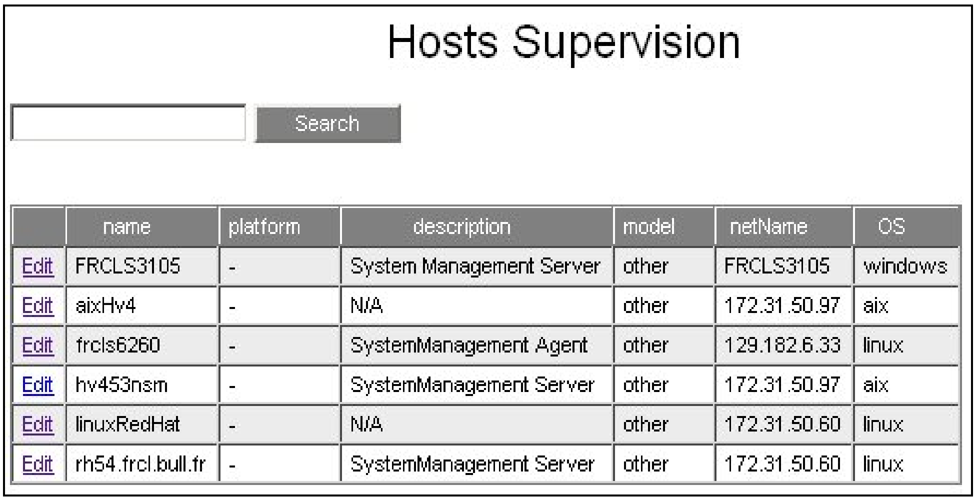
If no level button is checked, no filter is applied for the level attribute.

Set the **facility** list by checking the buttons.

If no facility button is checked, no filter is applied for the facility attribute.

5.4.3.2 Configuring Host

To configure hosts, click the **hosts** item in the Monitoring part of the Supervision tab. The list of configured hosts appears, as shown in the following example:



	name	platform	description	model	netName	OS
Edit	FRCLS3105	-	System Management Server	other	FRCLS3105	windows
Edit	aixHv4	-	N/A	other	172.31.50.97	aix
Edit	frcls6260	-	SystemManagement Agent	other	129.182.6.33	linux
Edit	hv453nsm	-	SystemManagement Server	other	172.31.50.97	aix
Edit	linuxRedHat	-	N/A	other	172.31.50.60	linux
Edit	rh54.frcl.bull.fr	-	SystemManagement Server	other	172.31.50.60	linux

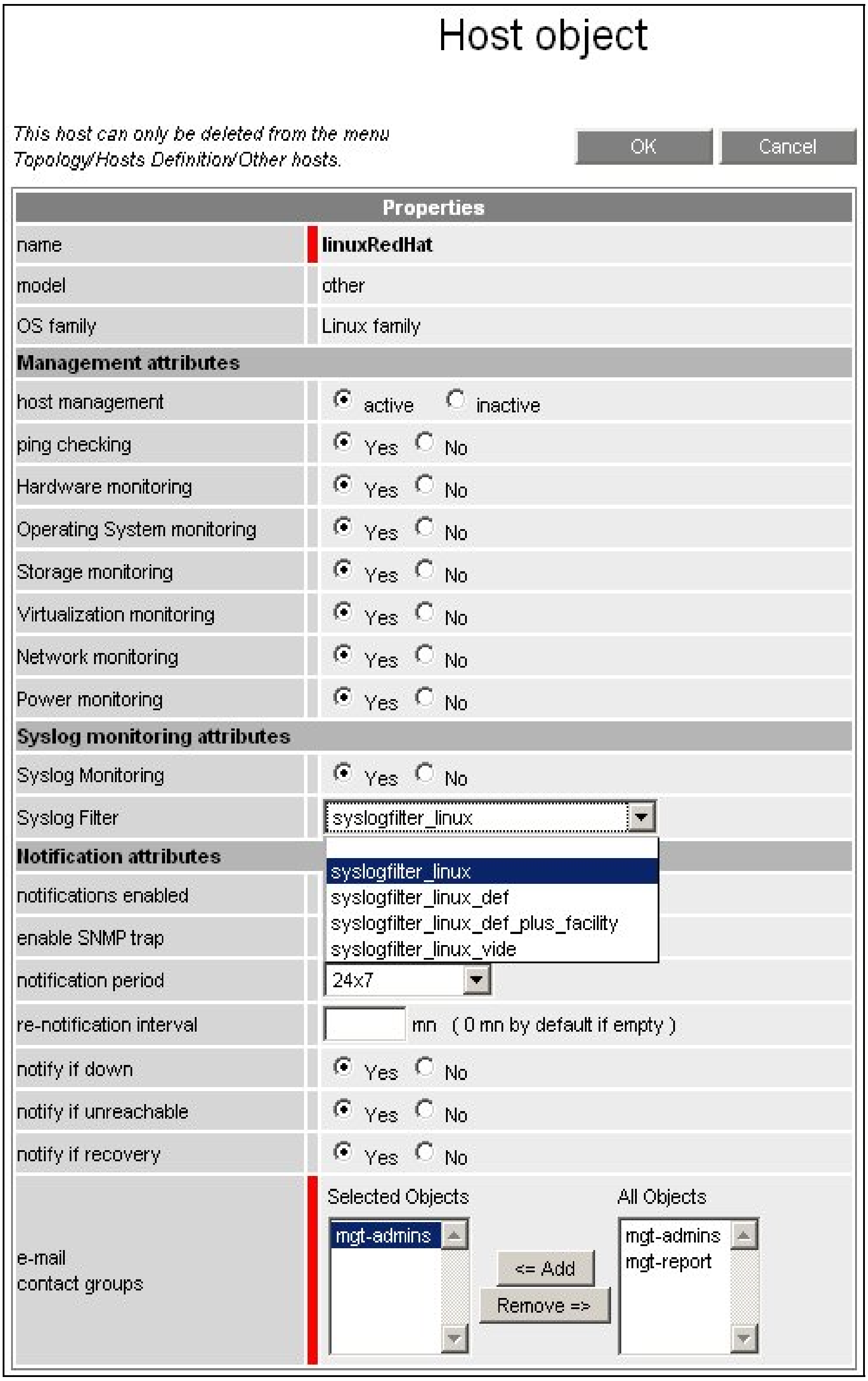
Figure 5-43. Hosts configuration window

Note See *Create / Edit / Delete Resources*, on page 21 for details.

The following example shows how to edit a Linux host.

Set the **Syslog Monitoring** attribute to **Yes** or **No**.

Select a **Syslog Filter** in the list: only Syslog Filters of **LINUX-syslogng** type will appear. If no **Syslog Filter** is selected, no filter is applied.



Host object

This host can only be deleted from the menu Topology/Hosts Definition/Other hosts.

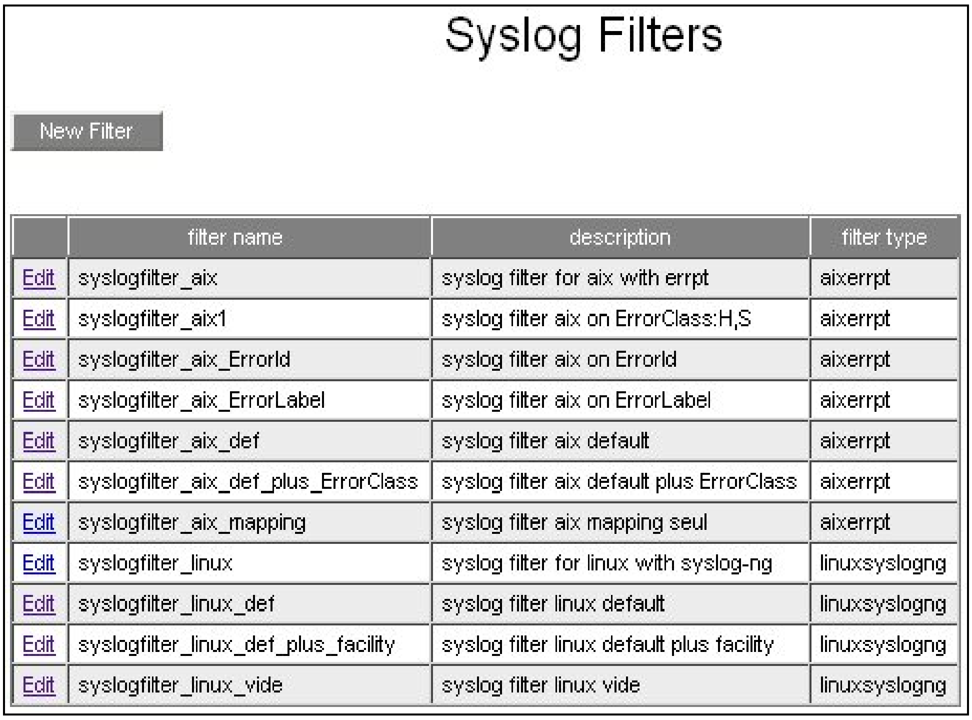
Properties	
name	**linuxRedHat**
model	other
OS family	Linux family
Management attributes	
host management	● active ○ inactive
ping checking	● Yes ○ No
Hardware monitoring	● Yes ○ No
Operating System monitoring	● Yes ○ No
Storage monitoring	● Yes ○ No
Virtualization monitoring	● Yes ○ No
Network monitoring	● Yes ○ No
Power monitoring	● Yes ○ No
Syslog monitoring attributes	
Syslog Monitoring	● Yes ○ No
Syslog Filter	syslogfilter_linux
Notification attributes	
notifications enabled	
enable SNMP trap	
notification period	24x7
re-notification interval	mn (0 mn by default if empty)
notify if down	● Yes ○ No
notify if unreachable	● Yes ○ No
notify if recovery	● Yes ○ No
e-mail contact groups	Selected Objects: mgt-admins All Objects: mgt-admins, mgt-report

Figure 5-44. Host monitoring properties

5.4.4 Example: Monitoring Aix Host

5.4.4.1 Creating Aix Syslog Filters

To edit syslog filters, click the Syslog Filters item in the Monitoring part of the Supervision tab. The list of configured syslog filters appears, as in the following example:



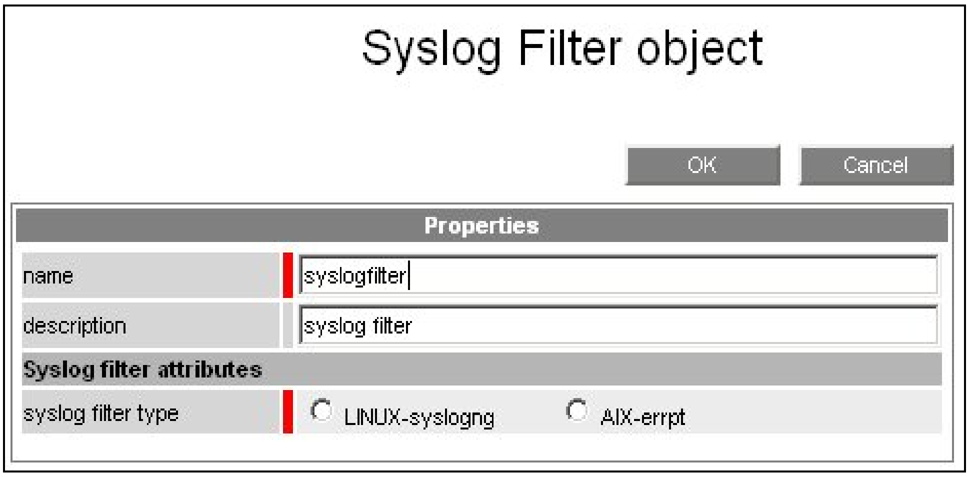
Syslog Filters

	filter name	description	filter type
Edit	syslogfilter_aix	syslog filter for aix with errpt	aixerrpt
Edit	syslogfilter_aix1	syslog filter aix on ErrorClass:H,S	aixerrpt
Edit	syslogfilter_aix_ErrorId	syslog filter aix on ErrorId	aixerrpt
Edit	syslogfilter_aix_ErrorLabel	syslog filter aix on ErrorLabel	aixerrpt
Edit	syslogfilter_aix_def	syslog filter aix default	aixerrpt
Edit	syslogfilter_aix_def_plus_ErrorClass	syslog filter aix default plus ErrorClass	aixerrpt
Edit	syslogfilter_aix_mapping	syslog filter aix mapping seul	aixerrpt
Edit	syslogfilter_linux	syslog filter for linux with syslog-ng	linuxsyslogng
Edit	syslogfilter_linux_def	syslog filter linux default	linuxsyslogng
Edit	syslogfilter_linux_def_plus_facility	syslog filter linux default plus facility	linuxsyslogng
Edit	syslogfilter_linux_vide	syslog filter linux vide	linuxsyslogng

Figure 5-45. Syslog Filters configuration window

Note See *Create / Edit / Delete Resources*, on page 21 for details.

To create a syslog filter, click the **New Filter** button, the following page appears:



Syslog Filter object

Properties

name: syslogfilter

description: syslog filter

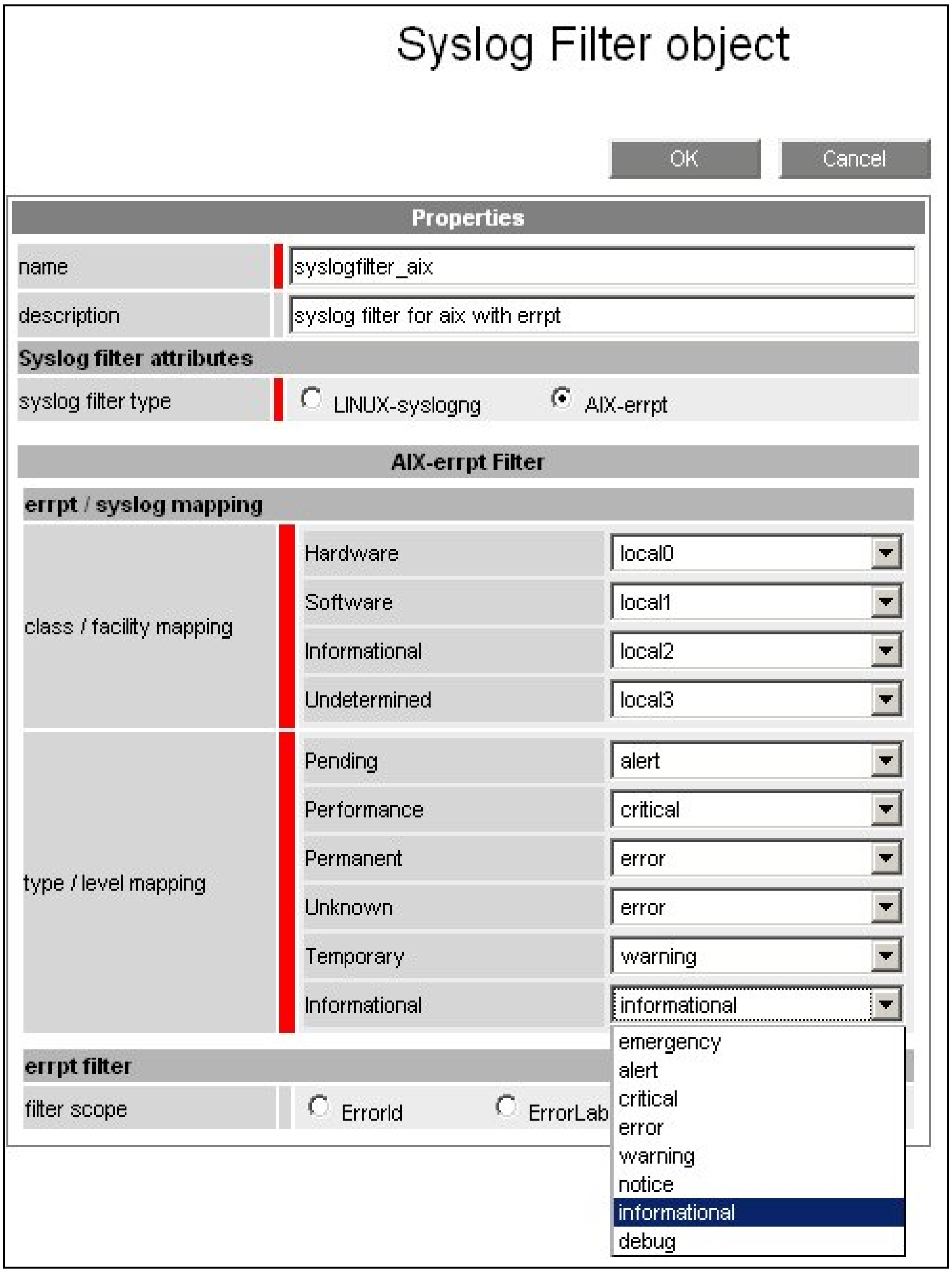
Syslog filter attributes

syslog filter type: ○ LINUX-syslogng ○ AIX-errpt

Figure 5-46. Common Syslog Filter properties

Set the **syslog filter type** attribute to **AIX-errpt**.

As shown in the following example, three Aix Syslog Filter properties are displayed:



Properties

name	syslogfilter_aix
description	syslog filter for aix with errpt
Syslog filter attributes	
syslog filter type	○ LINUX-syslogng ● AIX-errpt

AIX-errpt Filter

errpt / syslog mapping

class / facility mapping	Hardware	local0
	Software	local1
	Informational	local2
	Undetermined	local3
type / level mapping	Pending	alert
	Performance	critical
	Permanent	error
	Unknown	error
	Temporary	warning
	Informational	informational

errpt filter

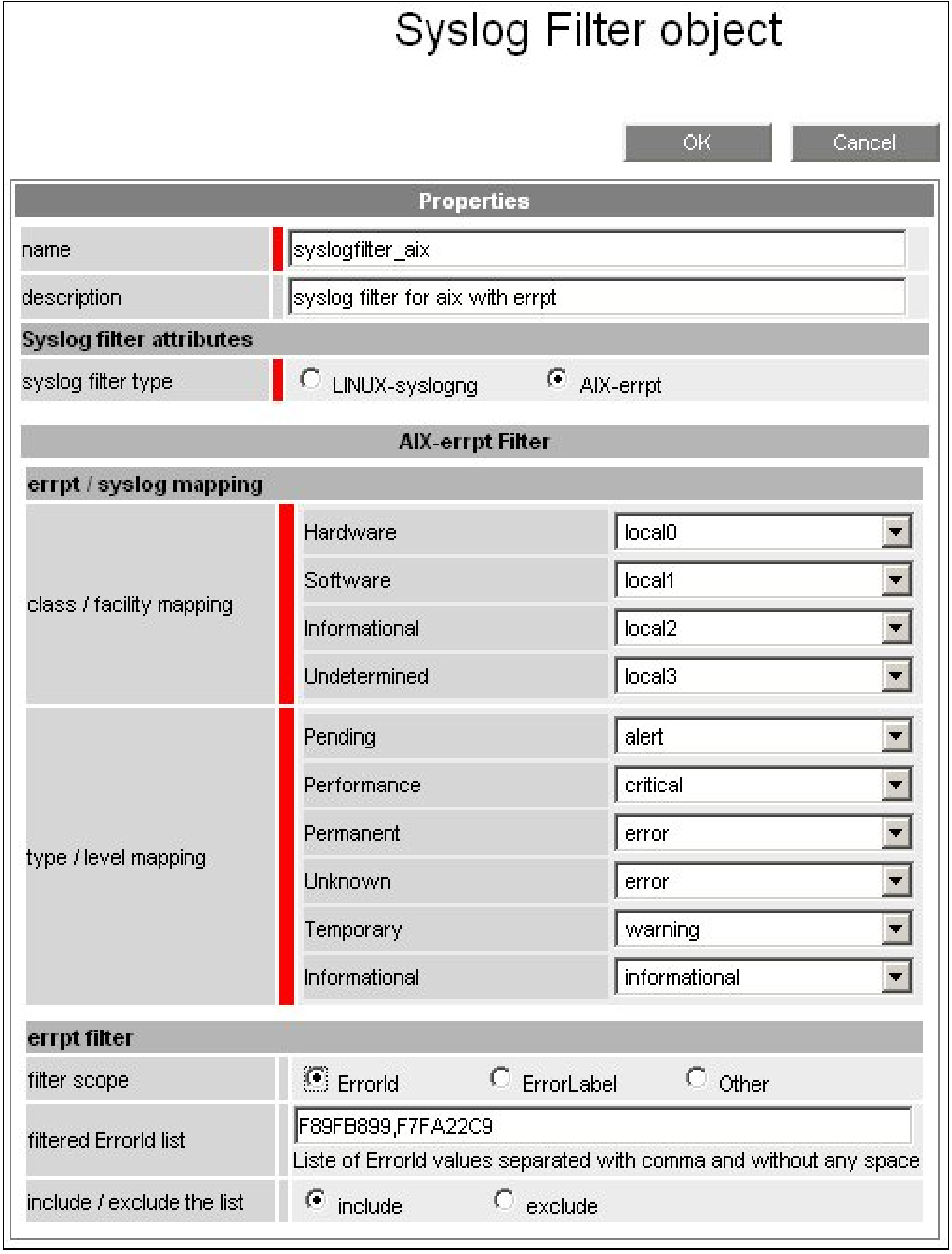
filter scope	○ ErrorId ○ ErrorLab

Figure 5-47. Aix Syslog Filter common properties

The **class/facility mapping** and **type/level mapping** properties are displayed with a default value. Each mapping can be modified by selecting a value from the list that appears.

Set the **filter scope** by checking a button to select one of the three values. If no button is checked, no filter is applied, only mapping.

If **Filter scope** is set to **ErrorId**, two more properties are displayed, as shown in the following example:



Syslog Filter object

Properties		
name	syslogfilter_aix	
description	syslog filter for aix with errpt	
Syslog filter attributes		
syslog filter type	○ LINUX-syslogng ● AIX-errpt	

AIX-errpt Filter

errpt / syslog mapping		
class / facility mapping	Hardware	local0
	Software	local1
	Informational	local2
	Undetermined	local3
type / level mapping	Pending	alert
	Performance	critical
	Permanent	error
	Unknown	error
	Temporary	warning
	Informational	informational

errpt filter	
filter scope	● ErrorId ○ ErrorLabel ○ Other
filtered ErrorId list	F89FB899,F7FA22C9 Liste of ErrorId values separated with comma and without any space
include / exclude the list	● include ○ exclude

Figure 5-48. Aix Syslog Filter ErrorId properties

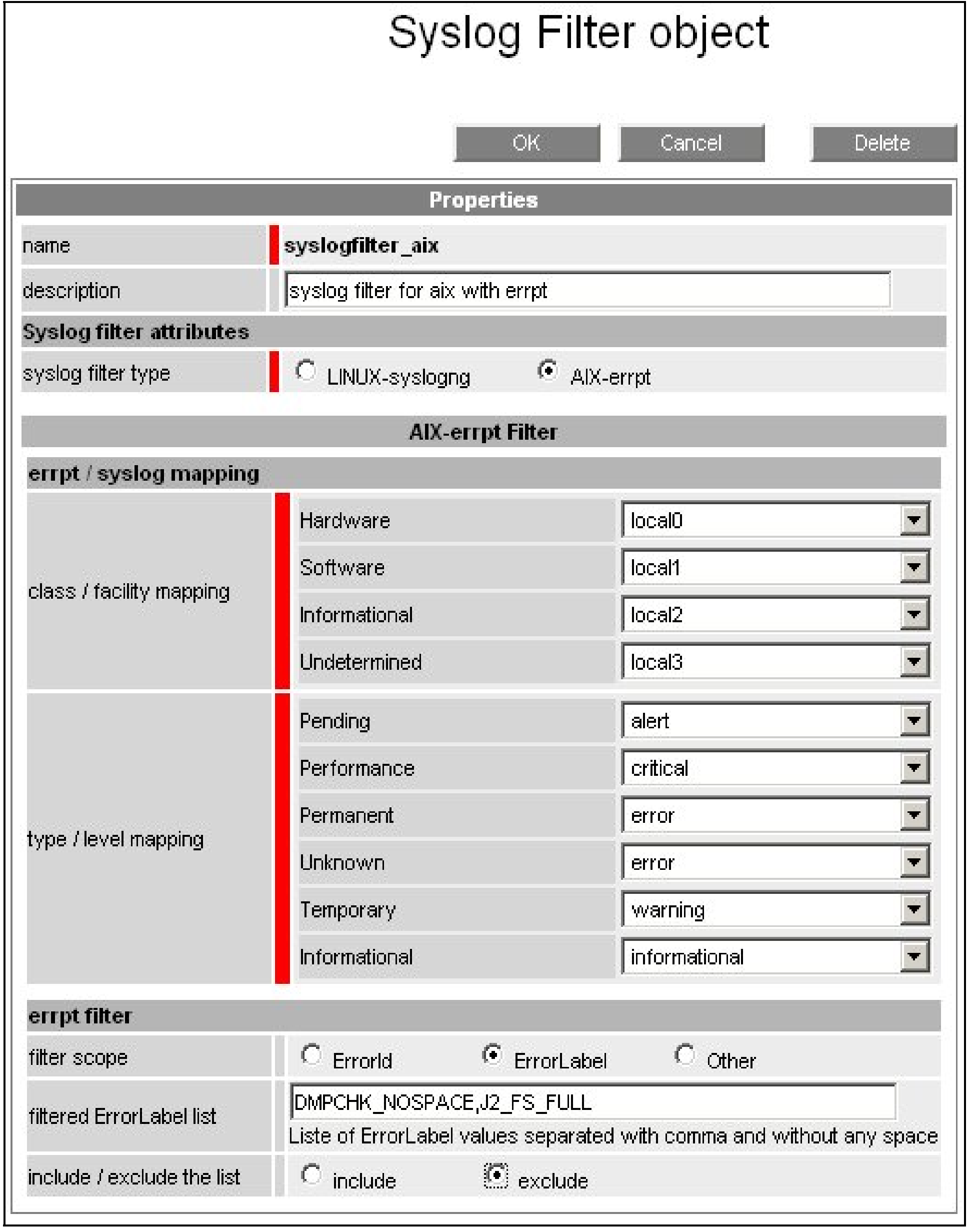
Set the **filtered ErrorId list** with a list of ErrorId separated with commas and without spaces.

If the ErrorId list is empty, no filter is applied for the ErrorId attribute.

Set the **include/exclude the list** property by checking a button to select one of the values:

- **include**: only the events whose ErrorId value is in the **filtered ErrorId list** will be forwarded.
- **exclude**: only the events whose ErrorId value is not in the **filtered ErrorId list** will be forwarded.

If Filter scope is set to Errorlabel, two more properties are displayed, as in the following example:



Properties

name	**syslogfilter_aix**	
description	syslog filter for aix with errpt	
Syslog filter attributes		
syslog filter type	○ LINUX-syslogng ● AIX-errpt	
AIX-errpt Filter		
errpt / syslog mapping		
class / facility mapping	Hardware	local0
	Software	local1
	Informational	local2
	Undetermined	local3
type / level mapping	Pending	alert
	Performance	critical
	Permanent	error
	Unknown	error
	Temporary	warning
	Informational	informational
errpt filter		
filter scope	○ ErrorId ● ErrorLabel ○ Other	
filtered ErrorLabel list	DMPCHK_NOSPACE,J2_FS_FULL Liste of ErrorLabel values separated with comma and without any space	
include / exclude the list	○ include ● exclude	

Figure 5-49. Aix Syslog Filter ErrorLabel properties

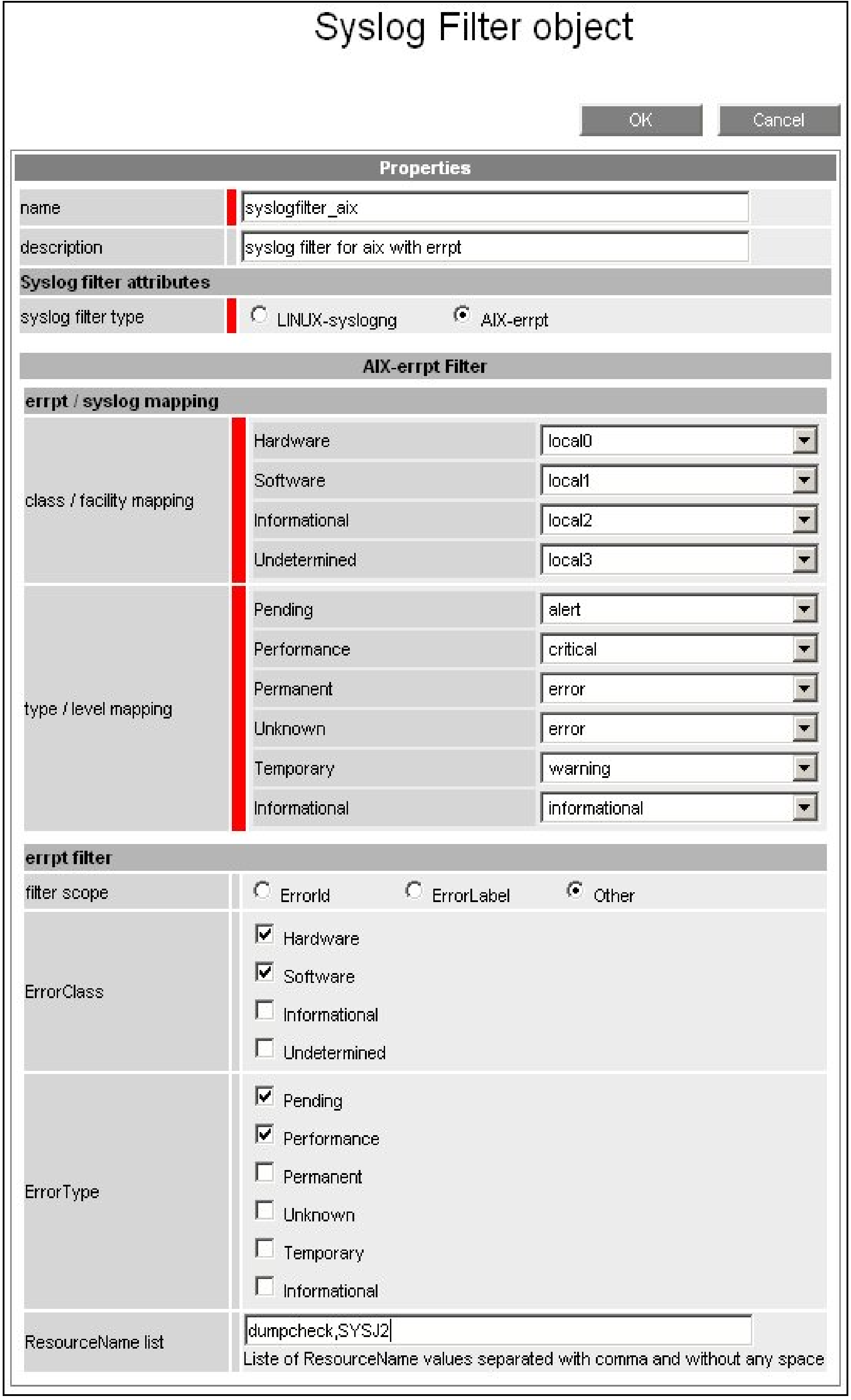
Set the **filtered Errorlabel list** with a list of Errorlabel separated with commas and without spaces.

If the ErrorLabel list is empty, no filter is applied to the ErrorLabel attribute.

Set the **include/exclude the list** property by checking a button to select one of the values.

- **include**: only the events whose Errorlabel value is in the **filtered Errorlabel list** will be forwarded.
- **exclude**: only the events whose Errorlabel value is not in the **filtered Errorlabel list** will be forwarded.

If **Filter scope** is set to **other**, three more properties are displayed, as shown in the following example:



Syslog Filter object

Properties

name	syslogfilter_aix
description	syslog filter for aix with errpt

Syslog filter attributes

syslog filter type: ○ LINUX-syslogng ● AIX-errpt

AIX-errpt Filter

errpt / syslog mapping

class / facility mapping	Hardware	local0
	Software	local1
	Informational	local2
	Undetermined	local3
type / level mapping	Pending	alert
	Performance	critical
	Permanent	error
	Unknown	error
	Temporary	warning
	Informational	informational

errpt filter

filter scope: ○ ErrorId ○ ErrorLabel ● Other

ErrorClass:
☑ Hardware
☑ Software
☐ Informational
☐ Undetermined

ErrorType:
☑ Pending
☑ Performance
☐ Permanent
☐ Unknown
☐ Temporary
☐ Informational

ResourceName list: dumpcheck,SYSJ2
Liste of ResourceName values separated with comma and without any space

Figure 5-50. Aix Syslog Filter other properties

Set the **ErrorClass** list by checking the boxes.

If no ErrorClass button is checked, no filter is applied to the ErrorClass attribute.

Set the **ErrorType** list by checking the boxes.

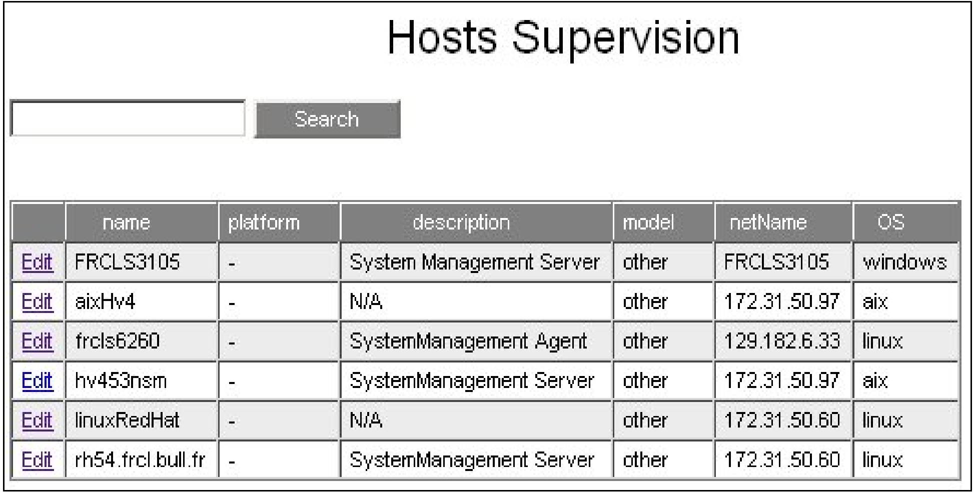
If no ErrorType button is checked, no filter is applied to the ErrorType attribute.

Set the **ResourceName list** with a list of ResourceNames separated with commas and without spaces.

If the ResourceName list is empty, no filter is applied to the ResourceName attribute.

5.4.4.2 Configuring Host

To configure hosts, click the hosts item in the Monitoring part of the Supervision tab. The list of configured hosts appears, as shown in the following example:



	name	platform	description	model	netName	OS
Edit	FRCLS3105	-	System Management Server	other	FRCLS3105	windows
Edit	aixHv4	-	N/A	other	172.31.50.97	aix
Edit	frcls6260	-	SystemManagement Agent	other	129.182.6.33	linux
Edit	hv453nsm	-	SystemManagement Server	other	172.31.50.97	aix
Edit	linuxRedHat	-	N/A	other	172.31.50.60	linux
Edit	rh54.frcl.bull.fr	-	SystemManagement Server	other	172.31.50.60	linux

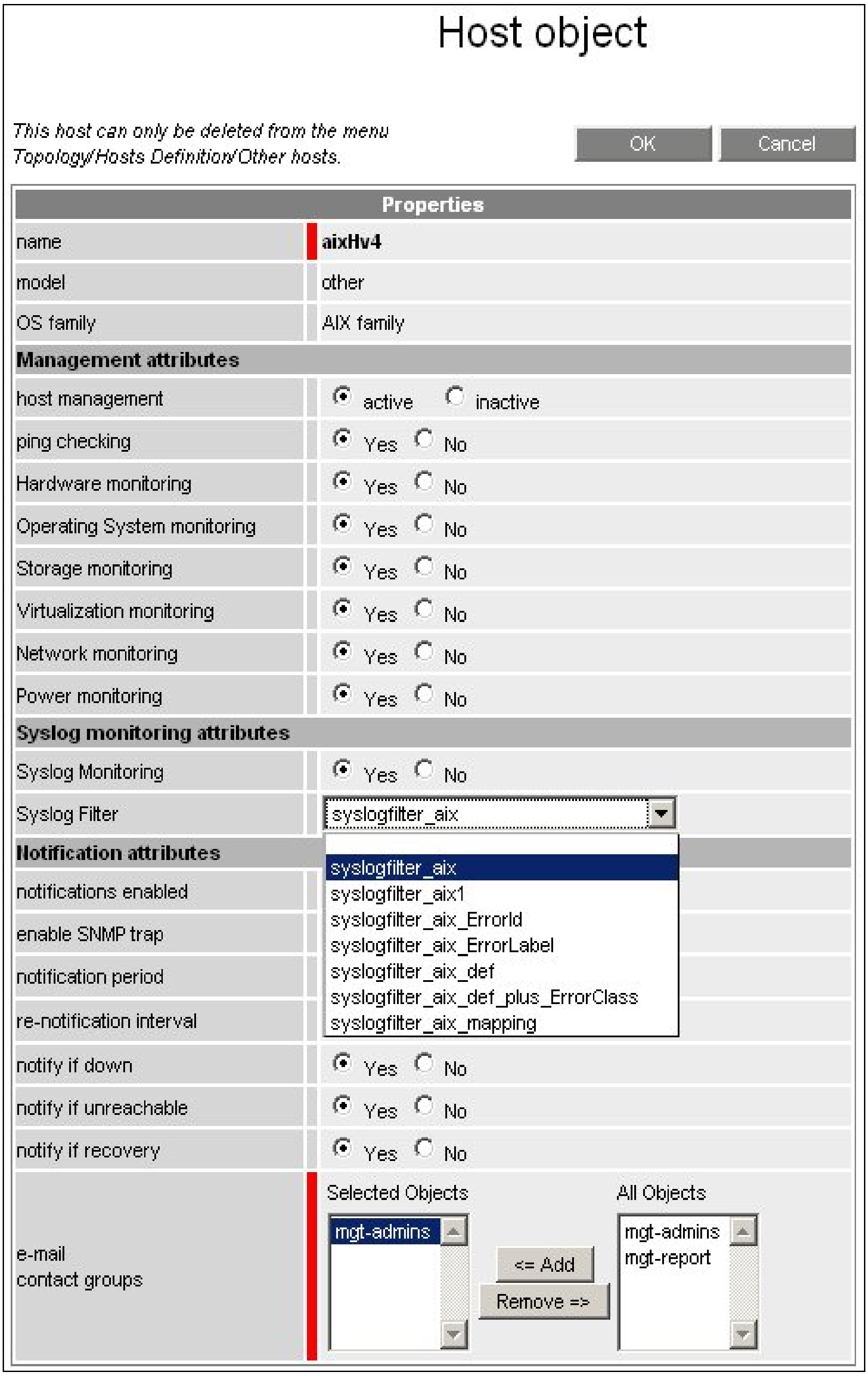
Figure 5-51. Hosts configuration window

Note See *Create / Edit / Delete Resources* on page 21 for details.

As shown in the following example, edit an Aix host.

Set the **Syslog Monitoring** attribute to **Yes** or **No**.

Select a **Syslog Filter** in the list: only Syslog Filters of **AIX-errpt** type will appear. If no **Syslog Filter** is selected, no filter is applied.



Host object

This host can only be deleted from the menu Topology/Hosts Definition/Other hosts.

OK | Cancel

Properties	
name	**aixHv4**
model	other
OS family	AIX family
Management attributes	
host management	● active ○ inactive
ping checking	● Yes ○ No
Hardware monitoring	● Yes ○ No
Operating System monitoring	● Yes ○ No
Storage monitoring	● Yes ○ No
Virtualization monitoring	● Yes ○ No
Network monitoring	● Yes ○ No
Power monitoring	● Yes ○ No
Syslog monitoring attributes	
Syslog Monitoring	● Yes ○ No
Syslog Filter	syslogfilter_aix
Notification attributes	
notifications enabled	
enable SNMP trap	
notification period	
re-notification interval	
notify if down	● Yes ○ No
notify if unreachable	● Yes ○ No
notify if recovery	● Yes ○ No
e-mail contact groups	Selected Objects: mgt-admins All Objects: mgt-admins, mgt-report

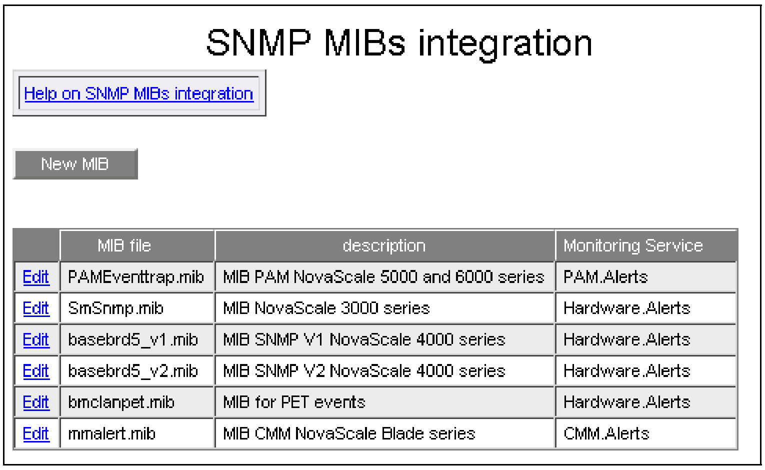
Figure 5-52. Host monitoring properties

Chapter 6. Configuring Supervision Event Reception

Bull System Manager can receive **SNMP** traps from any SNMP agent. This chapter explains how to configure Event reception. This configuration consists in integrating a MIB and enabling or disabling the SNMP trap receiver service.

6.1 Integrating MIBs

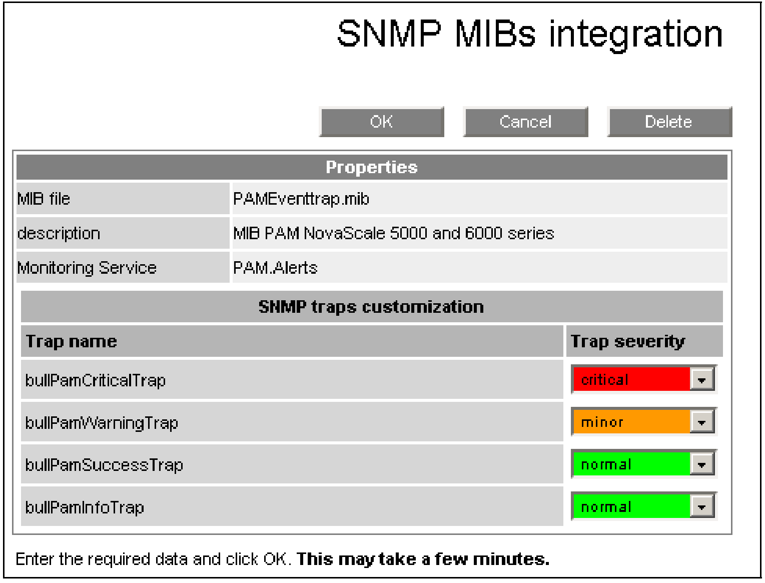
To receive the SNMP traps from specific equipment, the equipment MIB must be integrated into Bull System Manager. By default, some MIBs are integrated in the Bull System Manager solution.
To display SNMP MIBs, click the **Mibs** link under **Event reception** function in the Bull System Manager Console. The following display appears:



	MIB file	description	Monitoring Service
Edit	PAMEventtrap.mib	MIB PAM NovaScale 5000 and 6000 series	PAM.Alerts
Edit	SmSnmp.mib	MIB NovaScale 3000 series	Hardware.Alerts
Edit	basebrd5_v1.mib	MIB SNMP V1 NovaScale 4000 series	Hardware.Alerts
Edit	basebrd5_v2.mib	MIB SNMP V2 NovaScale 4000 series	Hardware.Alerts
Edit	bmclanpet.mib	MIB for PET events	Hardware.Alerts
Edit	mmalert.mib	MIB CMM NovaScale Blade series	CMM.Alerts

Figure 6-1. Default SNMP Mibs integration

To display and change the SNMP MIB properties click the **Edit** link:



Properties	
MIB file	PAMEventtrap.mib
description	MIB PAM NovaScale 5000 and 6000 series
Monitoring Service	PAM.Alerts

SNMP traps customization

Trap name	**Trap severity**
bullPamCriticalTrap	critical
bullPamWarningTrap	minor
bullPamSuccessTrap	normal
bullPamInfoTrap	normal

Enter the required data and click OK. **This may take a few minutes.**

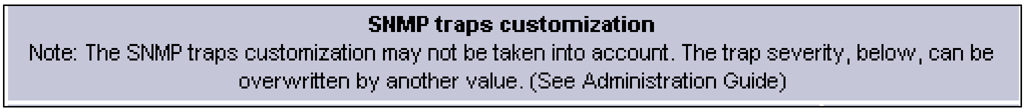
Figure 6-2. Changing SNMP MIBs integration Properties

MIB Properties	Description
MIB file	MIB file name. This name must be suffixed by **.mib**.
description	MIB description.
Monitoring Service	Monitoring category and service (e.g. in PAM SNMP traps will be visible in the BSM Console Management tree under PAM **Alerts**.
Trap name	SNMP trap name as defined in the MIB.
Trap severity	TRAP severity as defined in the MIB or customized by the Administrator. If not specified in the MIB, severity is set to normal by default. **Note:** Trap customization consists in modifying the displayed trap severity value if this value is not pertinent. Select a value listed in the select box (normal, cleared, critical, indeterminate, major, minor, warning or informational).

Table 6-1. SNMP MIB properties

Click **OK** to validate the changes, **Delete** to remove the MIB, or **Cancel** to leave the integration unchanged.

Trap customization may be not effective if the following message appears:



SNMP traps customization

Note: The SNMP traps customization may not be taken into account. The trap severity, below, can be overwritten by another value. (See Administration Guide)

Figure 6-3. SNMP trap customization message

In some cases, the severity of the trap is determined by an independent procedure (for instance, it may be extracted from a trap attribute).

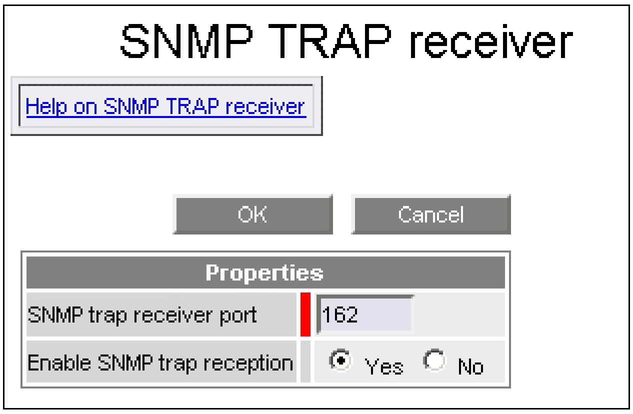
To integrate a new MIB, click **New MIB** and initialize the name of the MIB file, the description and the Monitoring service.

Please note that:

- The MIB file must be installed in the following directory:
  <Bull System Manager server Installation Directory>/engine/etc/snmp/mibs
- The Monitoring service (category and service) must be created before MIB integration. See *Creating an Alerts Service*, on page 119, for details about creating a new Alert Service.

6.2 Controlling the Trap Receiver

To control the SNMP trap receiver process, click the **Control** link under **Event reception** in the Bull System Manager Console. The following display appears:



Properties	
SNMP trap receiver port	162
Enable SNMP trap reception	● Yes ○ No

Figure 6-4. Control SNMP trap receiver

SNMP Trap Properties	Description
SNMP trap receiver port	Port used to receive SNMP traps. Linux: the SNMP trap receiver is the **snmptrapd** process. Default value: 162. Windows: the SNMP trap service receives SNMP traps on port 162 and forwards them to the Bull System Manager **snmptrapd** on port **1620**. Default value: **1620**. This value may be changed to avoid conflicts with other applications
Enable SNMP trap reception	Enable or disable **SNMP** trap reception. Default value: **Yes**.

Table 6-2. SNMP trap properties

Chapter 7. Configuring Performance Indicators

The collection of indicator with MRTG tool is deprecated in Bull System Manager 1.4 and higher. It is replaced with the Nagios extension, PNP4Nagios. Thus, indicator configuration is now dependant with Nagios plugins.

Note Nevertheless, if MRTG indicators has been defined before the BSM 1.4 migration, or if the BSM integrator or Administrator has enabled the MRTG usage in BSM, you may have both: MRTG indicators and PNP4nagios indicators.

You can contact Bull support to get the BSM MRTG HowTo guide, in order to enable and configure MRTG indicators.

Installation of the PNP4Nagios server extension triggers automatically the collection of all indicators processed in the active Nagios plugin.

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

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

Configuration tasks consist mainly in:

- Enabling/disabling performance indicator for a given service. See *Service Properties*, on page 93
- Globaly enabling/disabling performance indicator. See *Indicators generation Control (Nagios perfdata and RRD files generation),* on page 164
- Configuring export if needed.

7.1 Configuring export

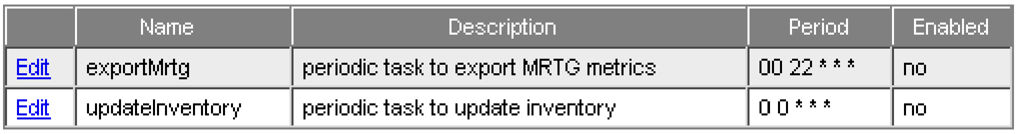
7.1.1 Export daily information of a MRTG indicator

In the case where MRTG is enabled.

A Periodic Task can be configured to generate a daily repository file for each indicator. Bull System Manager uses a CRON engine to schedule this task. The files are stored in a web shared directory:
http:/<BSM URL>/reporting/var/export2send.

NB: The CRON task deletes all files older than 30 days.

When first installation, this specific task is always disabled. To enable it, proceed as follows:
Click the **Periodic Tasks** link in the **Functionalities** part of the **GlobalSetting** tab. The **exportMrtg** task is listed, as shown below:

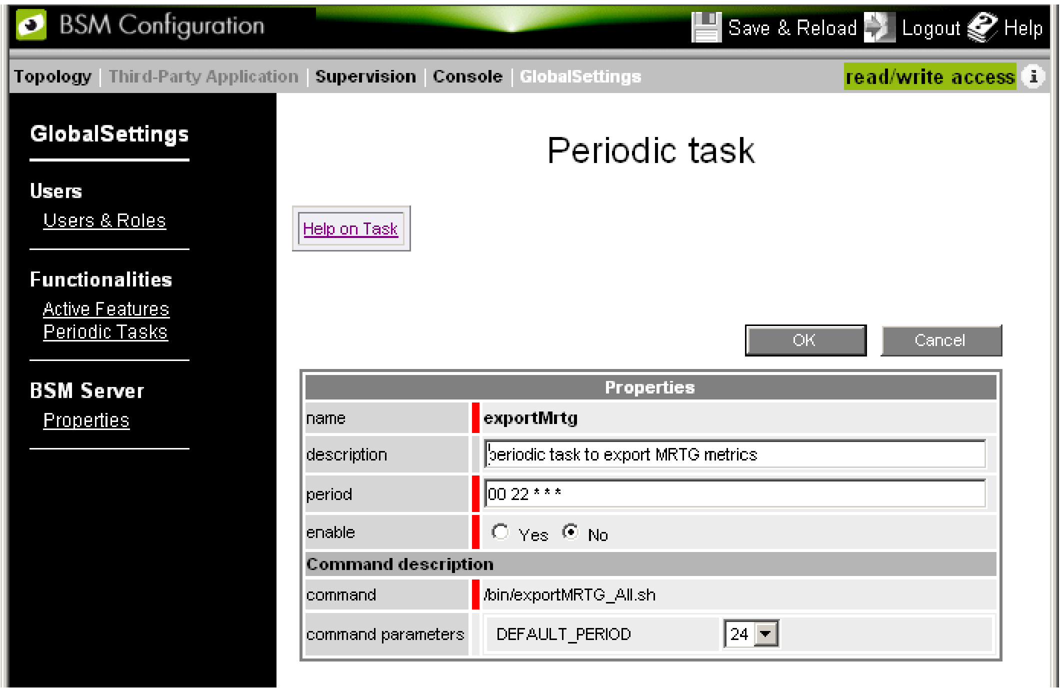


	Name	Description	Period	Enabled
Edit	exportMrtg	periodic task to export MRTG metrics	00 22 * * *	no
Edit	updateInventory	periodic task to update inventory	0 0 * * *	no

Figure 7-1. Periodic Tasks list

To configure this task, proceed as follows:

1. Click the **Edit** link of the **exportMRTG** task. The list of its properties appears:



Properties	
name	exportMrtg
description	periodic task to export MRTG metrics
period	00 22 * * *
enable	○ Yes ● No
Command description	
command	/bin/exportMRTG_All.sh
command parameters	DEFAULT_PERIOD 24

Figure 7-2. exportMRTG periodic task properties

2. Modify the period as needed: the periodicity is defined in the five fields in a standard cron format: <minute(0-59)> <hour(0-23)> <day of month(0-31)> < month(0-12) or names> <day of week(1-7) or name>".
   A field may be an asterisk (*), which always stands for 'first-last': for instance **00 22 * * *** corresponds to a daily execution at 22h.
   A range or a list of numbers is allowed: for instance, 8-11 in the hour field specifies execution at 8, 9, 10 and 11 hours.
   Steps can be used in conjunction with ranges or after asterisk: for instance ***/5** in the minute field specifies an execution every five minutes.
   See the *CRON Reference Manual* to get detailed information. By default, the task is scheduled daily at 22:00.

3. Enable the task. By default, the task is disabled.

4. Choose the time period for each file, 24 hours or 48 hours. By default, the value is 24.

5. Click **OK** to validate.

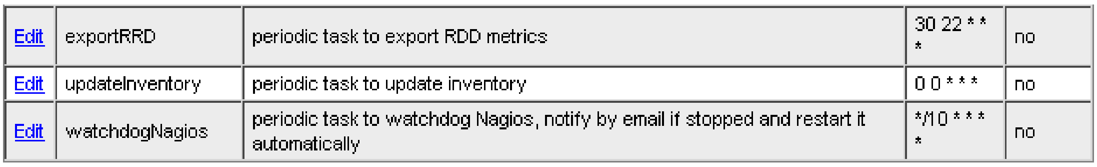
7.1.2 Export daily information of RRD indicators (perfdata)

In the case of PNP4nagios extension is installed.

A Periodic Task can be configured to generate a daily repository file for each indicator. Bull System Manager uses a CRON engine to schedule this task. The files are stored in a web shared directory:
http:/<BSM URL>/reporting/var/export2send.

Note The CRON task deletes all files older than 30 days.

After the first installation, this specific task is always disabled. To enable it, proceed as follows:
Click the **Periodic Tasks** link in the **Functionalities** part of the **GlobalSetting** tab. The **exportRRD** task is listed, as shown below:

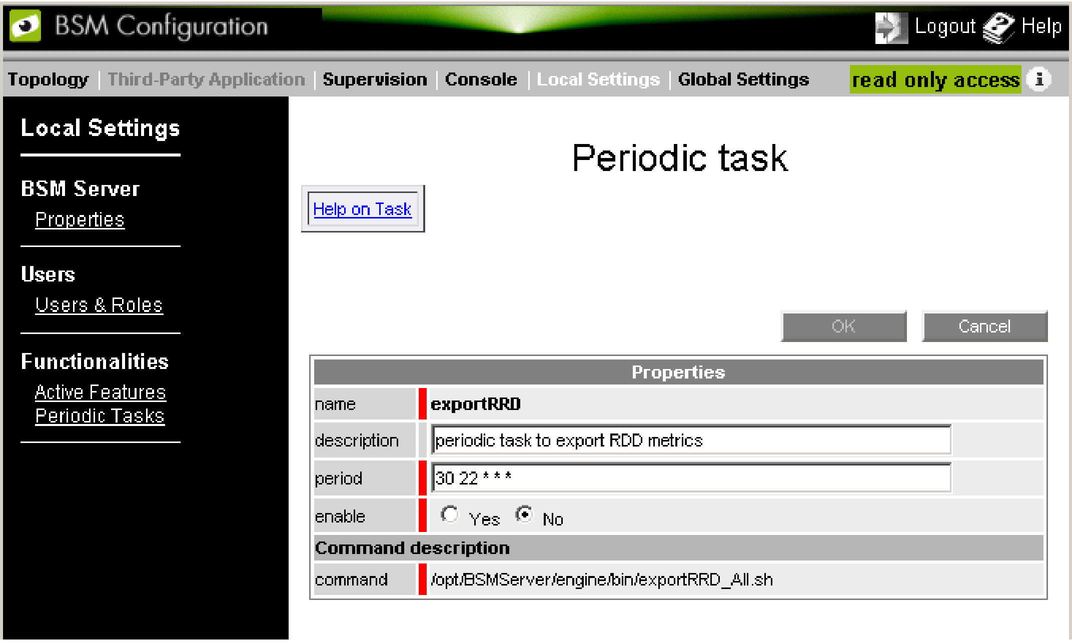


Edit	exportRRD	periodic task to export RDD metrics	30 22 * * *	no
Edit	updateInventory	periodic task to update inventory	0 0 * * *	no
Edit	watchdogNagios	periodic task to watchdog Nagios, notify by email if stopped and restart it automatically	*/10 * * * *	no

Figure 7-3. Periodic Tasks list

To configure this task, proceed as follows:

1. Click the **Edit** link of the **exportRRD** task. The list of its properties appears:



Periodic task

Properties	
name	**exportRRD**
description	periodic task to export RDD metrics
period	30 22 * * *
enable	○ Yes ● No
Command description	
command	/opt/BSMServer/engine/bin/exportRRD_All.sh

Figure 7-4. exportRRD periodic task properties

2. Modify the period as needed: the periodicity is defined in the five fields in a standard cron format: <minute(0-59)> <hour(0-23)> <day of month(0-31)> < month(0-12) or names> <day of week(1-7) or name>".
   A field may be an asterisk (*), which always stands for 'first-last': for instance **30 22 * * *** corresponds to a daily execution at 22h30.
   A range or a list of numbers is allowed: for instance, 8-11 in the hour field specifies execution at 8, 9, 10 and 11 hours.
   Steps can be used in conjunction with ranges or after asterisk: for instance ***/5** in the minute field specifies an execution every five minutes.
   See the *CRON Reference Manual* to get detailed information. By default, the task is scheduled daily at 22:30.

3. Enable the task. By default, the task is disabled.

4. Click **OK** to validate.

7.1.3 Monitor and Notify by Mail the indicators daily information

Associated with this daily files generation, a Nagios plug-in can be used to notify by mail the content of these files. The **METROLOGY.exportToNotify** monitoring service takes each file present in the **export2send** directory, notifies the details of its content, and moves the file to the **http:/<BSM URL>/reporting/var/exportsent**. web shared directory

To check, monitor and notify export files, Bull System Manager provides the **METROLOGY.exportToNotify** service template.

category	service	check_command	check parameters
METROLOGY	exportToNotify	check_exportMRTG	None

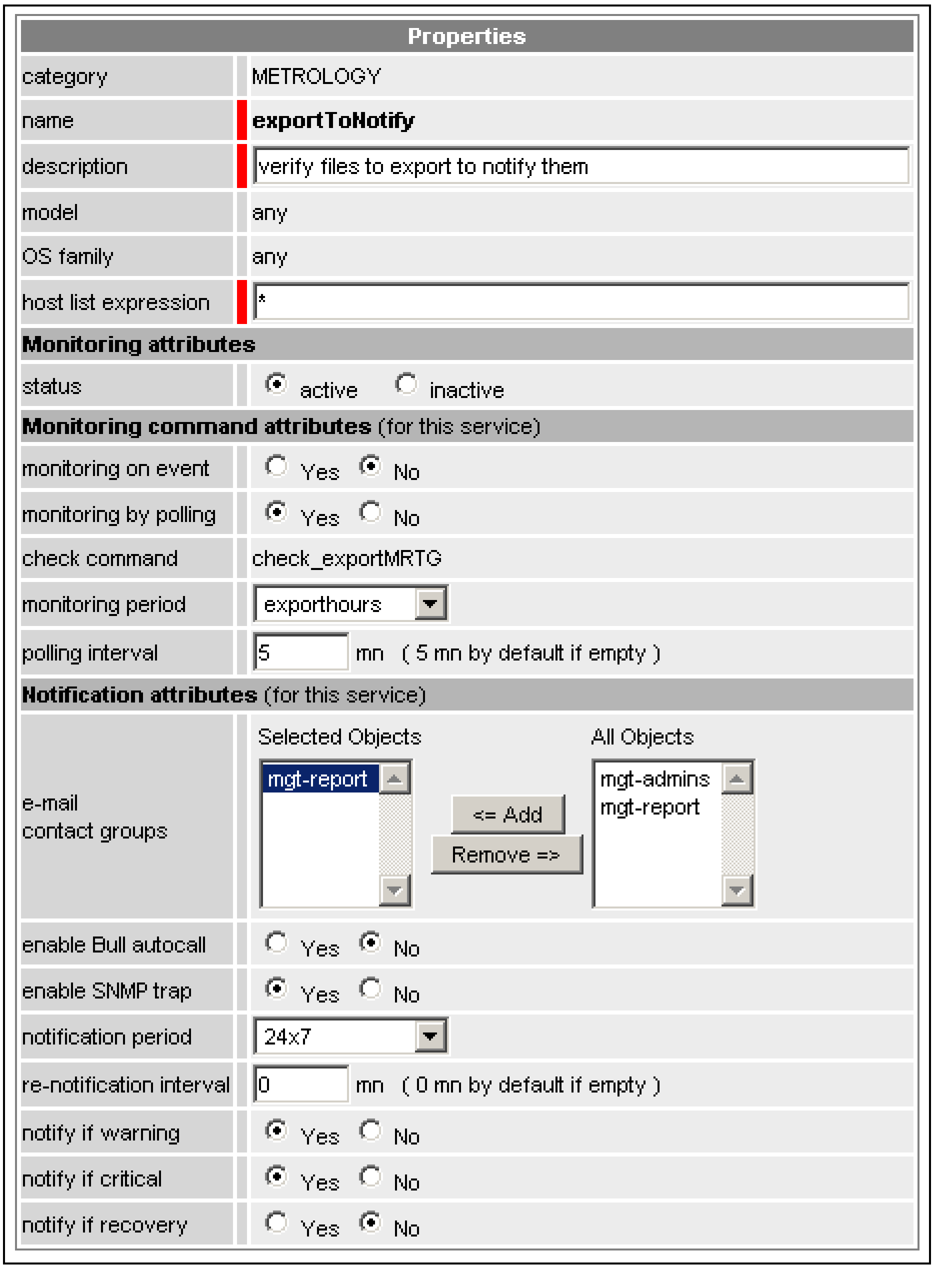
Note The check command name is historic. This service template works also with data files created by **exportRRD** periodic task.

The **METROLOGY.exportToNotify** service template can be used as illustrated in the following example.

Example

To apply the **METROLOGY.exportToNotify** service to a set of hosts, proceed as follows:

1. From the **filter by HOST** option select `frcls6260`, and click **Apply**.
2. Click the **manage service** link of the category where you want to put this service.
3. In the **Manage Service** popup window, check **Add from service template** and select the **METROLOGY.exportToNotify** service. Then click the **add from the selected service** button.
4. If you do not use the **filter by HOST** option, change the **host list** with the name of the Bull System Manager server (`frcls6260`).
5. You can change the service parameters as shown in the following diagram:



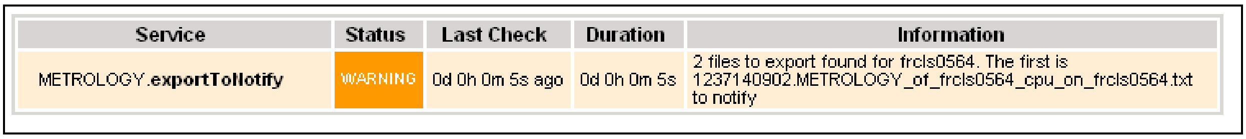
Properties	
category	METROLOGY
name	**exportToNotify**
description	verify files to export to notify them
model	any
OS family	any
host list expression	*
Monitoring attributes	
status	● active ○ inactive
Monitoring command attributes (for this service)	
monitoring on event	○ Yes ● No
monitoring by polling	● Yes ○ No
check command	check_exportMRTG
monitoring period	exporthours
polling interval	5 mn (5 mn by default if empty)
Notification attributes (for this service)	
e-mail contact groups	Selected Objects: mgt-report <= Add Remove => All Objects: mgt-admins, mgt-report
enable Bull autocall	○ Yes ● No
enable SNMP trap	● Yes ○ No
notification period	24x7
re-notification interval	0 mn (0 mn by default if empty)
notify if warning	● Yes ○ No
notify if critical	● Yes ○ No
notify if recovery	○ Yes ● No

The specific properties for this service are:

- The monitoring period: **exporthours** corresponding with 00:00 until 06:00 AM period
- The contact group: **mgt-report** which contains the contact **report** by default.

6. Click **OK** to validate the customization operation.

The monitoring service status looks as follows:



Service	Status	Last Check	Duration	Information
METROLOGY.**exportToNotify**	WARNING	0d 0h 0m 5s ago	0d 0h 0m 5s	2 files to export found for frcls0564. The first is 1237140902.METROLOGY_of_frcls0564_cpu_on_frcls0564.txt to notify

The notification mail appears as shown in the example below:

```
"
***** Bull System Manager (nagios 3.0) *****

Notification Type: PROBLEM

Service: METROLOGY.exportToNotify
Host: frcls0564 Description: System Management Server
Address: frcls0564
State: WARNING

Date/Time: Thu Mar 12 18:12:04     2009

Information:

15 files to export found for frcls0564. The first is
1236875702.METROLOGY_of_memoryused_frcls0564_on_frcls0564.txt to notify

Additional Info:

DATE: 1236875702 (2009-03-12 17:35:02 +01:00)

HOST: frcls0564
INDICATOR: memoryused_frcls0564
LEGEND: used

Last 48 hours metrology (every 5mn)
###########################################
1236875100 54
1236874800 54
1236874500 54
1236874200 53
1236873900 53
1236873600 53
1236873300 53
1236873000 53
…

1236702900 0
1236702600 0



BSM link for this host:
http://<BSM netname>:10080/BSM/console/heading-
php/wrapper.php?panel=Services_status&host=frcls0564&nodetype=host

"
```

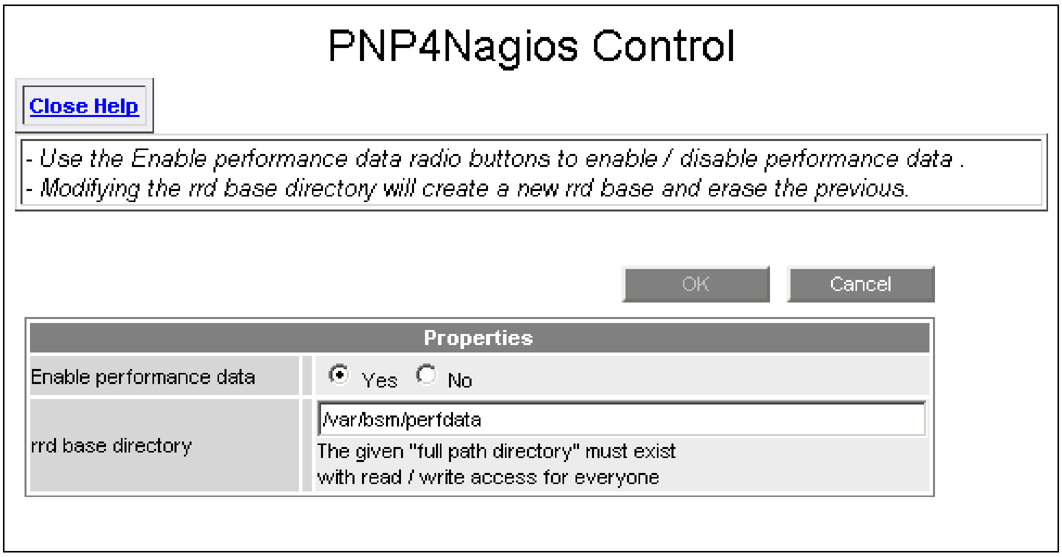
7.2 Manage RRD Indicator (nagios perfdata)

Note If MRTG indicators have been defined before the BSM 1.4 migration, or if the BSM integrator or administrator has enabled the MRTG usage in BSM, you may have both MRTG indicators and PNP4nagios indicators.

You can contact Bull support to get the “BSM MRTG HowTo guide”, in order to enable and configure MRTG indicators.

7.2.1 Indicators generation Control (Nagios perfdata and RRD files generation)

To control performance indicators, click the PNP4nagios/Control item in the Reporting menu from the Supervision domain. The following window is displayed:



PNP4Nagios Control

- Use the Enable performance data radio buttons to enable / disable performance data .
- Modifying the rrd base directory will create a new rrd base and erase the previous.

Properties	
Enable performance data	● Yes ○ No
rrd base directory	/var/bsm/perfdata The given "full path directory" must exist with read / write access for everyone

Figure 7-5. RRD generation control

You can enable/disable the performance data generation (enabled by default)

You can change the RRD repository directory, where RRD files will be generated.

WARNING
You CANNOT change the RRD repository on a Windows BSM server.

Note It can be usefull to use a shared directory to centralize all RRD files in the case of a distributed BSM solution.

Chapter 8. Configuring Event Handler

This chapter explains how to define an event handler for a Bull System Manager configuration. Event handlers are optional commands that are executed, on Bull System Manager servers, whenever a host or service state change occurs:

- UP, DOWN and UNREACHABLE states for a host
- OK, WARNING, UNKNOWN and CRITICAL states for a service.

The PENDING service state is the initial state. A service state cannot change into the PENDING state.

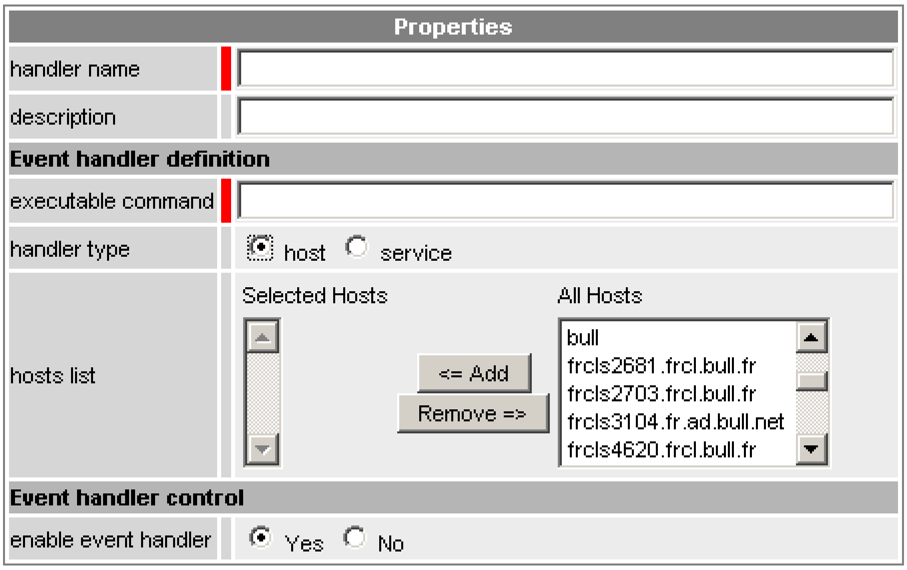
Two main types of event handlers can be defined: **service** event handlers and **host** event handlers.

8.1 Event Handler Definition

To configure Event Handlers, click the **Handler** link in the **EventHandler** part of the **Supervision** tab.

8.1.1 Host Event Handler

The following window appears for the creation of a new event handler for a host.



Properties

handler name	
description	

Event handler definition

executable command	
handler type	● host ○ service
hosts list	Selected Hosts All Hosts: bull, frcls2681.frcl.bull.fr, frcls2703.frcl.bull.fr, frcls3104.fr.ad.bull.net, frcls4620.frcl.bull.fr

Event handler control

enable event handler	● Yes ○ No

Figure 8-1. Host event handler creation window

handler name event handler name.

description event handler description.

Event handler definition

executable command Full pathname of the command. The file must exist.

system command Specifies if the command must be executed as root user. This attribute is only displayed if Bull System Manager server is running on Linux.

handler type Handler type (host).

hosts list List of the hosts on which the event handler will be applied.

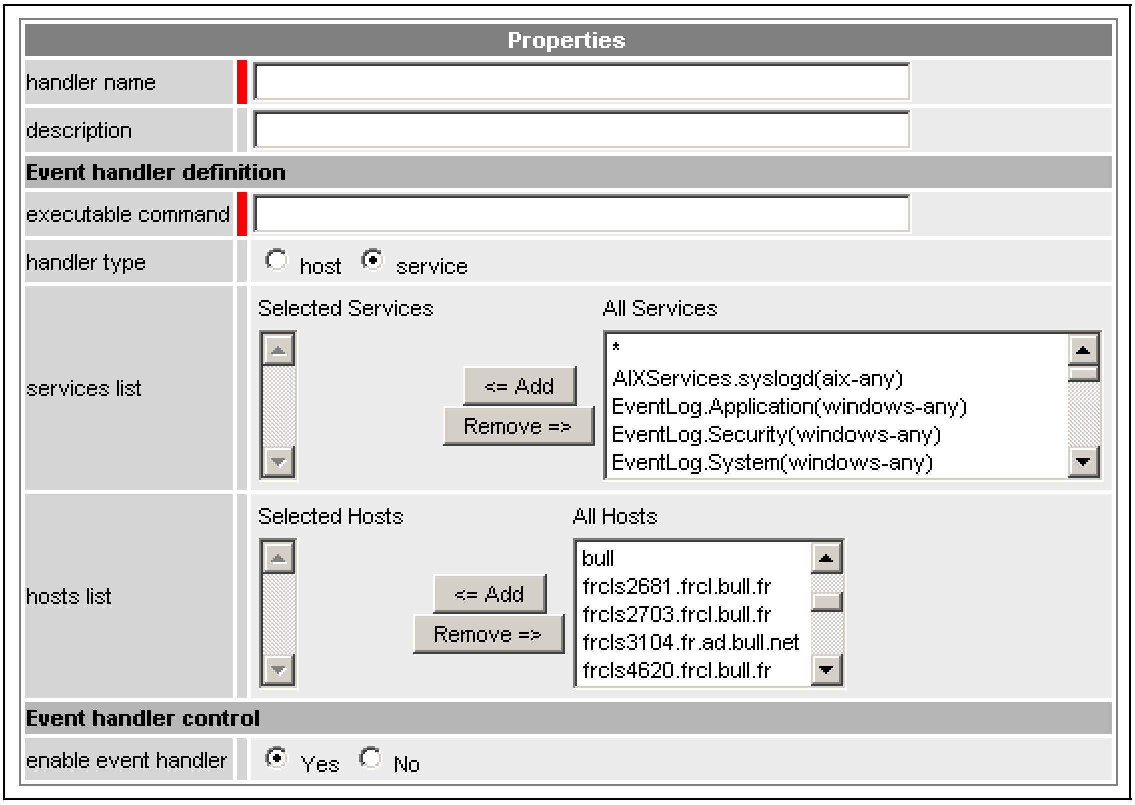
Event Handler control

enable event handler Controls (enable/disable) the event handler.

Note Several event handlers can be specified for a given host, in which case, the commands will be launched sequentially.

8.1.2 Service Event Handler

The following figure shows the window for the creation of a new event handler for a service.



Properties	
handler name	
description	
Event handler definition	
executable command	
handler type	○ host ● service

services list	Selected Services
	All Services
	*
	AIXServices.syslogd(aix-any)
	EventLog.Application(windows-any)
	EventLog.Security(windows-any)
	EventLog.System(windows-any)

hosts list	Selected Hosts All Hosts bull frcls2681.frcl.bull.fr frcls2703.frcl.bull.fr frcls3104.fr.ad.bull.net frcls4620.frcl.bull.fr
Event handler control	
enable event handler	● Yes ○ No

handler name Event handler name.

description Event handler description.

Event handler definition

executable command Full pathname of the command. The file must exist on the Bull System Manager server.

system command Specifies if the command must be executed as root user. This attribute is only displayed if Bull System Manager server is running on Linux.

handler type Handler type (host).

services list List of the services on which the event handler will be applied only for the hosts specified in the hosts list below.

hosts list List of the hosts on which the event handler will be applied.

Event Handler control

enable event handler Controls (enable/disable) the event handler.

Note Only one event handler can be specified for a service.

8.2 Event Handler Command

Event handler commands are shell or PERL scripts. They can be **bat** files on Windows.

8.2.1 Host Event Handler Arguments

The script for a host event handler requires the following arguments:

<event-handler command> HOSTSTATE HOSTADDRESS

HOSTSTATE	State of the host (UP, DOWN, UNREACHABLE)
HOSTADDRESS	Network address of the host

8.2.2 Service Event Handler Arguments

The script for a service event handler requires the following arguments:

<event-handler command> SERVICESTATE HOSTADDRESS SERVICEDESC

SERVICESTATE	State of the service (OK, WARNING, CRITICAL, UNKNOWN)
HOSTADDRESS	Network address of the host
SERVICEDESC	Service description (<category name>.<service name)

8.3 Event Handler Templates

8.3.1 Host Event Handler

```
#!/bin/bash
# HOST EVENT handler
# arguments: $HOSTSTATE $HOSTADDRESS
# $1=state(UP,DOWN,UNREACHABLE)
# $2=host netname

case "$1" in
UP)
     # action on UP state
     ;;
DOWN)
     # action on DOWN state
     ;;
UNREACHABLE)
     # action on UNREACHABLE state
     ;;
esac
exit 0
```

8.3.2 Service Event Handler

```
#!/bin/bash
# Event handler template

# SERVICE EVENT handler
# arguments: $SERVICESTATE $HOSTADDRESS $SERVICEDESC
# $1=state(OK,WARNING,UNKNOWN,CRITICAL)
# $2=host netname
# $3=service name

# service state

case "$1" in
OK)
     # action on OK state
     ;;
WARNING)
     # action on WARNING state
     ;;
UNKNOWN)
     # action on UNKNOWN state
     ;;
CRITICAL)
     # action on CRITICAL state
     ;;
esac
exit 0
```

8.4 Sample Event Handler

```
#!/bin/sh
#
# Event handler script for restarting the web server on the local
machine
#
# What state is the HTTP service in?
case "$1" in
OK)
     # The service just came back up, so don't do anything...
     ;;
WARNING)
     # We don't really care about warning states, since the
service is probably still running...
     ;;
UNKNOWN)
     # We don't know what might be causing an unknown error, so
don't do anything...
     ;;
CRITICAL)
     # The HTTP service appears to have a problem - perhaps we
should restart the server...
     echo -n "Restarting HTTP service..."
     # Call the init script to restart the HTTPD server
     /etc/rc.d/init.d/httpd restart
     ;;
esac
exit 0
```

Chapter 9. Configuring Notifications

This chapter describes how to configure contacts, contactgroups and notifications sent by e-mails, autocalls or **SNMP** traps. The decision to send out notifications is made at the service and host monitoring level. Host and service notifications are sent out when an anomaly or a recovery is detected.

Notification periods are specified at different levels according to requirements: **24x7**, **workhours**, **nonworkhours**, **none** (**none** disables notifications).

- **Host and service notification period:** Defines when a notification is to be sent.
- **Contact notification period for host alerts:** Defines when a notification about host problems and recoveries is to be sent.
- **Contact notification period for service alerts:** Defines when a notification about service problems and recoveries is to be sent.

The **notification period for service alerts** and **notification period for host alerts** define an **on call** period for each contact.

It may be helpful to specify different times for host and service notifications. For example, for a given contact, you can specify:

- No host notifications on weekdays
- Service notifications on weekdays.

Notification periods should cover *any time* that the contact can be notified.
You can control notification times for specific services and hosts on a one-by-one basis as described below:
The **host notification period** controls when Bull System Manager should send out notifications regarding problems or recoveries for that host. When a **host notification** is about to be sent out, Bull System Manager checks that the current time is within the valid **notification period** range. If the time is valid, Bull System Manager attempts to notify each contact of the host problem.

Note Some contacts may not receive the host notification if their **notification period for host alerts** does not allow host notifications at that time.
If the time is not valid, Bull System Manager does not send out the notification.

mportant

Time period settings allow you to have greater control of how Bull System Manager performs monitoring and notification functions, but can lead to problems. If you are not sure of the times to implement, or if you are having problems with your current settings, we suggest the use of the 24x7 time: all times, every day of the week.

The **host and service re-notification interval** defines the time between two notifications for the same resource.
The **notify if** ... options specify the type of event for which a notification is sent:

- **Host**: **down**, **unreachable**, or when a **recovery** occurs.
- **Service**: **warning** or **critical** status, or when a **recovery** occurs.

9.1 Contacts and contactgroups

A **Contact** identifies the target of the notifications sent by Bull System Manager.

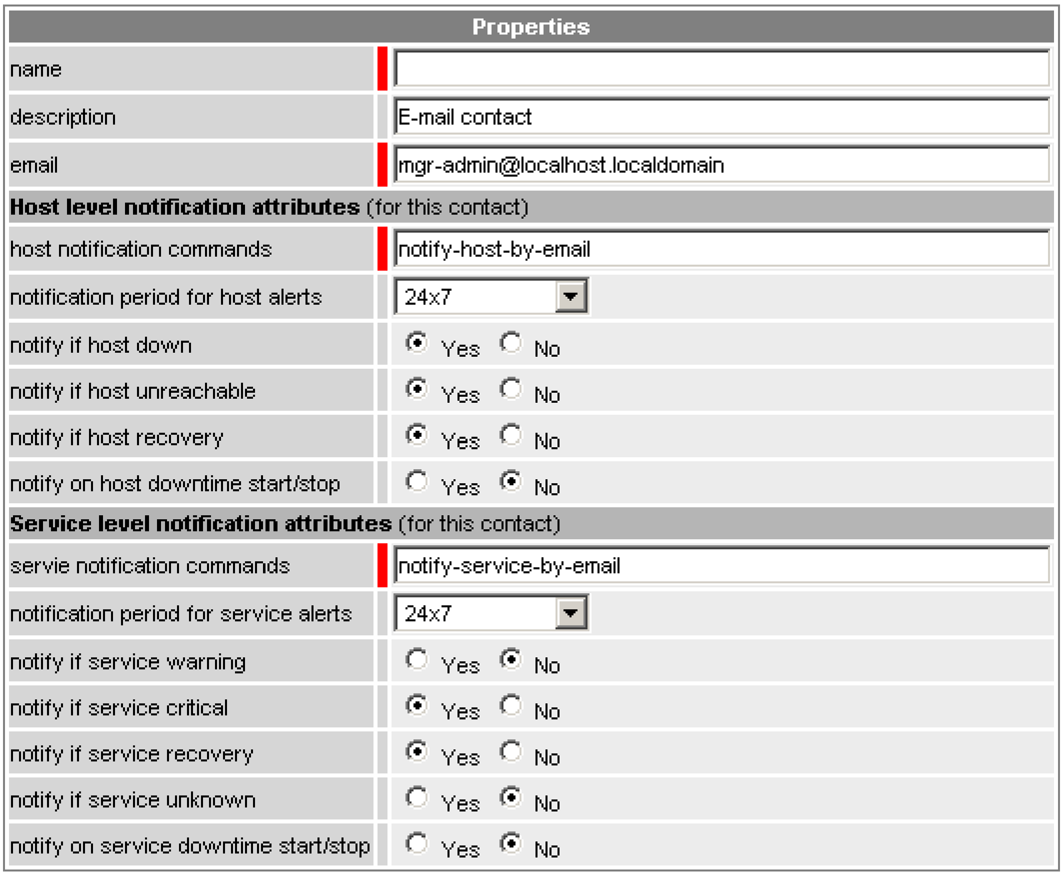
A **Contactgroup** groups one or more contacts together in order to send out alert/recovery notifications. When a host or service has a problem or recovers from a problem, Bull System Manager notifies all the contacts in the contact groups concerned by the event.

For each service, a **Contactgroup** specifies which contact group will receive notifications for that service. Each Contactgroup can contain one or more individual contacts.

Each host may belong to one or more host groups. For each host group a **Contactgroup** specifies which contact group will receive notifications for hosts in that host group. If a host does not belong to a host group, notifications will not be sent for the host.

9.1.1 Contacts

To configure a Contact, click the **Contacts** link in the **Notification** part of the **Monitoring** tab.
The way to create, edit or delete a Mail server is described in *Create / Edit / Delete Resources*, on page 21.
The following figure shows the setting window displayed for **Contact** resource.



Properties	
name	
description	E-mail contact
email	mgr-admin@localhost.localdomain
Host level notification attributes (for this contact)	
host notification commands	notify-host-by-email
notification period for host alerts	24x7
notify if host down	● Yes ○ No
notify if host unreachable	● Yes ○ No
notify if host recovery	● Yes ○ No
notify on host downtime start/stop	○ Yes ● No
Service level notification attributes (for this contact)	
servie notification commands	notify-service-by-email
notification period for service alerts	24x7
notify if service warning	○ Yes ● No
notify if service critical	● Yes ○ No
notify if service recovery	● Yes ○ No
notify if service unknown	○ Yes ● No
notify on service downtime start/stop	○ Yes ● No

Figure 9-1. Contact properties

Contact Properties	Description
name	Short name used to identify the contact (user name).
description	Contact full name and/or description.
email	Contact e-mail address or any information required by the notification command.
host notification commands	Commands used to notifify the contact on host change. Default value; **host-notify-by-email**
notification period for host alerts	Period during which host notifications must be sent to this contact. Possible values: **24x7**, **workhours**, **nonworkhours**, **none**. Default value: **24x7**.
notify if host down	Notify contact when hosts are down? Default value: **yes**.
notify if host unreachable	Notify contact when hosts are unreachable? Default value: **yes**.
notify if host recovery	Notify contact on host recovery? Default value: **yes**.
notify on host downtime start/stop	Notify contact when scheduled downtime is started or stopped for a host ? Default value: **yes**
service notification commands	Commands used to notifify the contact on service change. Default value; **service-notify-by-email**
notification period for service alerts	Time during which service notifications must be sent to this contact. Possible values: **24x7**, **workhours**, **nonworkhours**, **none**. Default value: **24x7**.
notify if service warning	Notify contact for warning service status? Default value: no.
notify if service critical	Notify contact for critical service status? Default value: **yes**.
notify if service recovery	Notify contact for service recovery? Default value: **yes**.
notify if service unknown	Notify contact for unknown service status ? Default value: **yes**
notify on service downtime start/stop	Notify contact when scheduled downtime is started or stopped for a service ? Default value: **yes**

Table 9-1. Contact properties

Notes

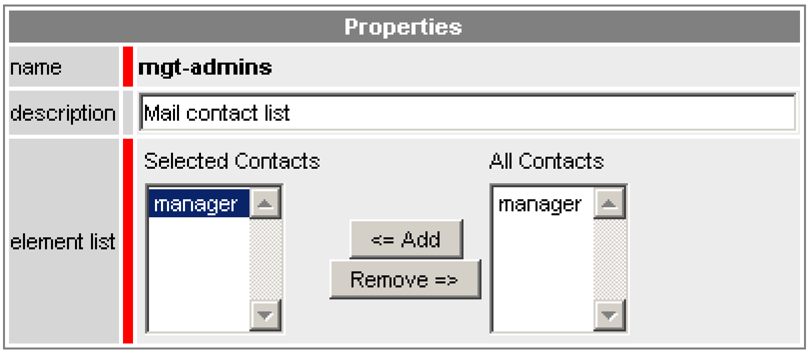
- The notification command must be defined in a Nagios configuration file (*.cfg) installed under the directory <BSM directory>/engine/nagios/etc/NSM
- The corresponding system command must be installed under the directory <BSM directory>/engine/nagios/libexec
- The notification command can reference informations from the contact and the host or service configuration as a parameter by using Nagios macro (for example, EMAIL for contact) that will be automatically substituted by Nagios before the command executes. To get detailed information about the notification command definition, refer to the standard Nagios documentation on http://www.nagios.org/

9.1.2 Contactgroups

To configure a contactgroup, click the **Contactgroups** link in the **Notification** part of the **Monitoring** tab.

The way to create, edit or delete a Mail server is described in *Create / Edit / Delete Resources*, on page 21.

The following figure shows the settings window displayed for a **Contactgroup** resource.



Properties

name: mgt-admins

description: Mail contact list

element list:
Selected Contacts: manager
All Contacts: manager

Figure 9-2. Contactgroup properties

Contactgroup Properties	Description
name	Name of the contact group containing contacts.
description	Description of the resource. This description is only for information and is not visible from the Bull System Manager Console.
element list	List of contacts belonging to this contactgroup. The resources are selected in the **All Resources** list, moved to the **Selected Resources** list using the **Add** button, and removed using the **Remove** button.

Table 9-2. Contactgroup properties

Note The **mgt-admins** contact group is defined by default. It contains the manager contact. It is used as the main contact for all services and hosts and consequently, cannot be removed.

9.2 Notification by E-mail

Sending notifications by e-mail requires:

- Access to a mail server
- **enable e-mail notification** set to `Yes` under Mail server
- Contact groups defined with a list of contacts
- Contacts defined with a valid e-mail address
- Valid and coherent notification periods at host/service, contact levels.

9.2.1 Mail Server

To access the mail server configuration, click the **Mail server** link in the **Notification** part of the **Monitoring** tab.

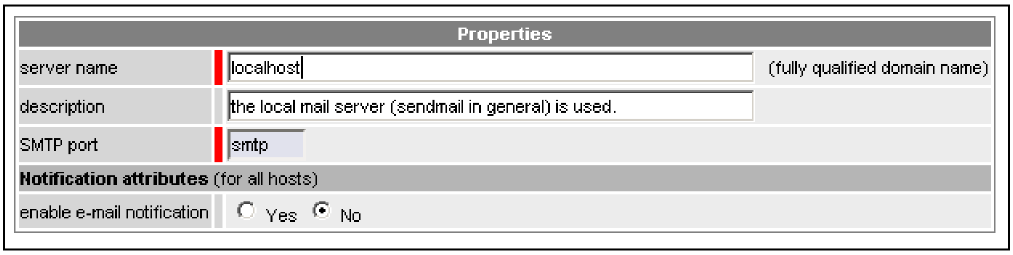
The way to create, edit or delete a Mail server is described in *Create / Edit / Delete Resources*, on page 21.

Mail server configuration is different on Linux and Windows platforms.

9.2.1.1 Mail Server on Linux

On **Linux** platforms, the Bull System Manager server host is normally configured as a Mail server. You have to check that mail sending is operational from the Bull System Manager server host.

The following figure shows the window displayed to edit **Mail Server** settings on Linux.



Properties		
server name	localhost	(fully qualified domain name)
description	the local mail server (sendmail in general) is used.	
SMTP port	smtp	
Notification attributes (for all hosts)		
enable e-mail notification	○ Yes ● No	

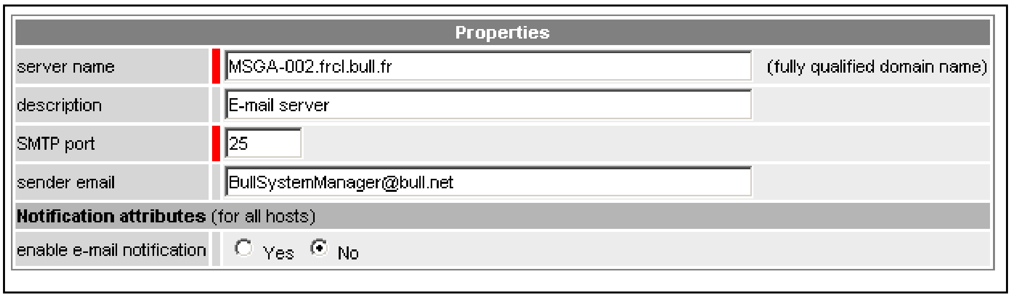
Figure 9-3. Mail Server properties on Linux

The **enable e-mail notification** setting may be changed to enable or disable e-mail) notification by mail (Default value: **No**).

Note On a Linux Bull System Manager server, the **server name** and **SMTP port** properties are not used and are therefore not editable. Only default information is displayed, which can be different from the local sendmail configuration values.

9.2.1.2 Mail Server on Windows

On **Windows** platforms, a mail server must be defined. Click **New** to create it.
The following figure shows the window displayed to edit Mail Server settings on Windows



Properties		
server name	MSGA-002.frcl.bull.fr	(fully qualified domain name)
description	E-mail server	
SMTP port	25	
sender email	BullSystemManager@bull.net	
Notification attributes (for all hosts)		
enable e-mail notification	○ Yes ● No	

Figure 9-4. Mail Server properties on Windows

Enter the name of the Mail Server (**server name**), this must be a fully qualified domain name. Enter a short description.

The **SMTP port** property is left unchanged. Default value: **25**.

The **enable e-mail notification** setting may be changed to enable or disable the e-mail notification. (Default value: **No**.)

A valid **sender email** must be specified in some secured network configurations. Otherwise, email sending will fail.

9.2.2 Example: Sending E-mail Notifications

To configure the notification by e-mail:

Step 1: Start Bull System Manager Configuration.

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

Step 3: Specify the mail address of the receiver.

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

9.2.2.1 Start Bull System Manager Configuration

See *Starting the Configuration GUI*, on page 11.

9.2.2.2 Configure the Mail Server

This step is only required if Bull System Manager Server runs on a Windows system.

1. From the **Notification** part of the **Monitoring** tab, click **Mail server**. The list of defined mail servers is displayed. If no server has been yet defined, this list is empty.

2. Click **New**. The mail server form appears.

3. Enter the host mail server, e.g. `clmail001.frcl.bull.fr`.The **smtp_port** used is the default port for outgoing mail: `25`.

4. Set the **enable e-mail notification** field to **Yes**.

5. Click **OK** to validate.

9.2.2.3 Specify the Mail Address of the Receiver

When a problem occurs on a host or service, Bull System Manager sends a notification to the contact groups, and not directly to contacts.

Note A contact group is a set of contacts, each contact represented by a mail address.

By default, Bull System Manager defines a contact group named **mgt-admins**, which contains a contact named **manager**. As the Administrator, you can set up the email address of the **manager** contact and/or add new contact groups and new contacts, according to requirements.

1. From the **Notification** part of the **Monitoring** tab, click **Contacts**: the contacts list is displayed.

2. Click **Edit to** modify the default contact properties.

3. Complete the **email** field with the mail address where notifications will be sent. The contact form is displayed.

4. Set the **notification period for host alerts** to **24x7** so that you are always notified of host events.

5. Set the **notification period for service alerts** to **24x7** so that you are always notified of the monitored service events.

6. By default, you will be notified of all events: host down, **host unreachable**, **host recovery (return to normal status)**, **service warning**, **service critical and service recovery**.

7. By default, you will receive notifications for all services. If you want to receive notifications only for some services, or for some hosts, you must edit the definition of the services or hosts.

8. To receive notifications for a second mail address, define another contact for this address and add it to the **mgt-admins** group.

9.2.2.4 Reload the Server Part

Click the **Save & Reload** Button to apply modifications to the server part.

9.3 Notification by Autocalls

Autocalls are **XML** files transferred to the Bull Remote Maintenance Center (GTS server). Sending notifications by Autocalls requires:

- An access to a GTS server name (Bull Remote Maintenance Center)
- **enable Bull autocall** set to **Yes** under Autocall

Important

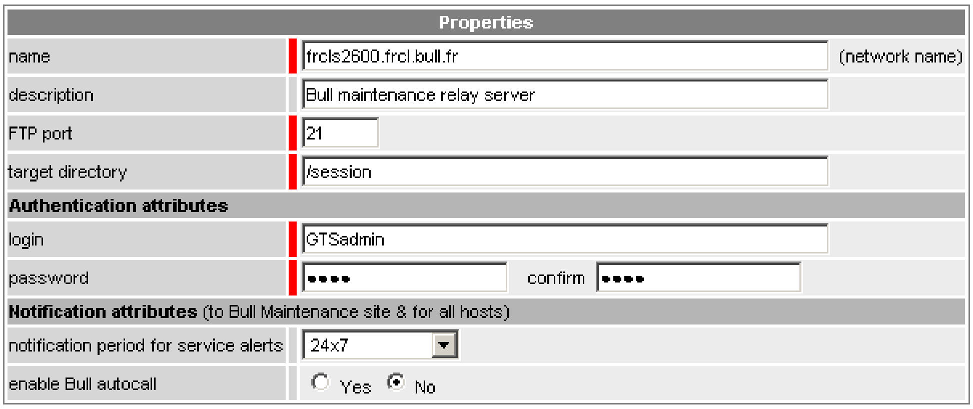
Each service has an enable Bull autocall option that specifies if the notification may be sent by Autocall or not. The notification will only be sent if enable Bull autocall is set to Yes under Autocall.

By default, **enable Bull autocall** is set to **Yes** only for the **Alerts** service. The **Alerts** service receives **SNMP** traps from the NovaScale host.

Autocall Server

The Autocall server specifies the FTP parameters for the server that will receive the autocalls. Autocalls are sent automatically by FTP without user interaction (silent mode). To configure the Autocall server, click the Autocall Platform name in the Notification part of the Monitoring tab.
The way to create, edit or delete a Mail server is described in *Create / Edit / Delete Resources* section, on page 21.

The following figure shows the window used to change the settings for an Autocall resource.



Properties		
name	frcls2600.frcl.bull.fr	(network name)
description	Bull maintenance relay server	
FTP port	21	
target directory	/session	
Authentication attributes		
login	GTSadmin	
password	••••	confirm ••••
Notification attributes (to Bull Maintenance site & for all hosts)		
notification period for service alerts	24x7 ▾	
enable Bull autocall	○ Yes ● No	

Figure 9-5. Autocall properties

Autocall Properties	Description
name	Host name of the server that will receive autocalls
description	Server description
FTP port	The port on which this server will receive autocalls. Default value: **21**
target directory	Directory pathname where autocalls are stored. Default value: **/session**
login	User name used by ftp to transmit autocalls
password	Password used by ftp to transmit autocalls
notification period for service alerts	Time during which service notifications must be sent to this contact. Possible values: **24x7**, **workhours**, **nonworkhours**, **none**. Default value: *24x7*.
enable Bull autocall	Enable the autocall mechanism? Default value: **no**.

Table 9-3. Autocall properties

9.4 Notification by SNMP Trap

Notification by SNMP trap allows the integration of Bull System Manager within a global management solution. Sending notifications by SNMP Trap requires:

- The definition of at least one target of the **SNMP** trap packet (SNMP Manager),
- **enable SNMP trap** set to **Yes** under SNMP Manager,

Important:

Each service has an enable SNMP trap option indicating whether SNMP Trap notification may be used or not. The trap will only be sent if at least one manager has the enable SNMP trap option set to Yes. The trap is sent by the Bull System Manager server on behalf of the managed host.

By default, all services allow **SNMP Trap** notification. To disable this feature on selected services, you must set the enable **SNMP trap** option to **No**.
You can configure detailed notification options by editing the corresponding contact, **admin-snmp**.

Note SNMP Trap PDU format is **SNMPv1**. The **mib** (BSM-TRAP-MIB) text file is delivered under **<BSM installation directory>/engine/etc/snmp/mibs**.

9.4.1 SNMP Manager

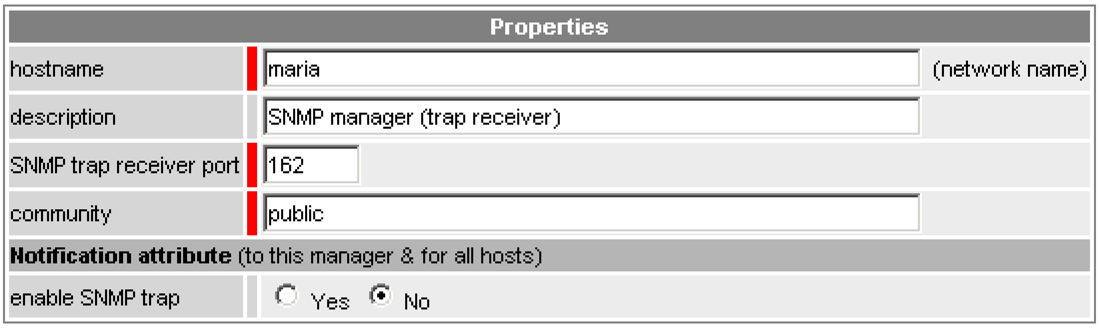
SNMP Manager defines a management platform that will receive the SNMP traps sent by the Bull System Manager server.

Note It is advised NOT to define the Bull System Manager host as the SNMP manager. This configuration can lead to loops in trap emission.

To configure an SNMP Manager, click the **Managers** link in the **SNMP** part of the **Monitoring** tab.

The way to create, edit or delete a Mail server is described in *Create / Edit / Delete Resources*, on page 21.

The following figure shows the window used to edit **SNMP** Manager settings.



Properties

hostname	maria	(network name)
description	SNMP manager (trap receiver)	
SNMP trap receiver port	162	
community	public	
Notification attribute (to this manager & for all hosts)		
enable SNMP trap	○ Yes ● No	

Figure 9-6. SNMP Manager properties

SNMP Manager Properties	Description
name	Host name of the management platform that will receive the traps.
description	Short description of the SNMP Manager.
snmptrapd port	Port used to receive SNMP traps. Default value: *162*.
community	SNMP community name. Default value: **public**.
enable SNMP trap	Enable SNMP Trap notification for this SNMP Manager. Default value: **No** . This value must be changed to **Yes** to allow SNMP Trap notification.

Table 9-4. SNMP manager properties

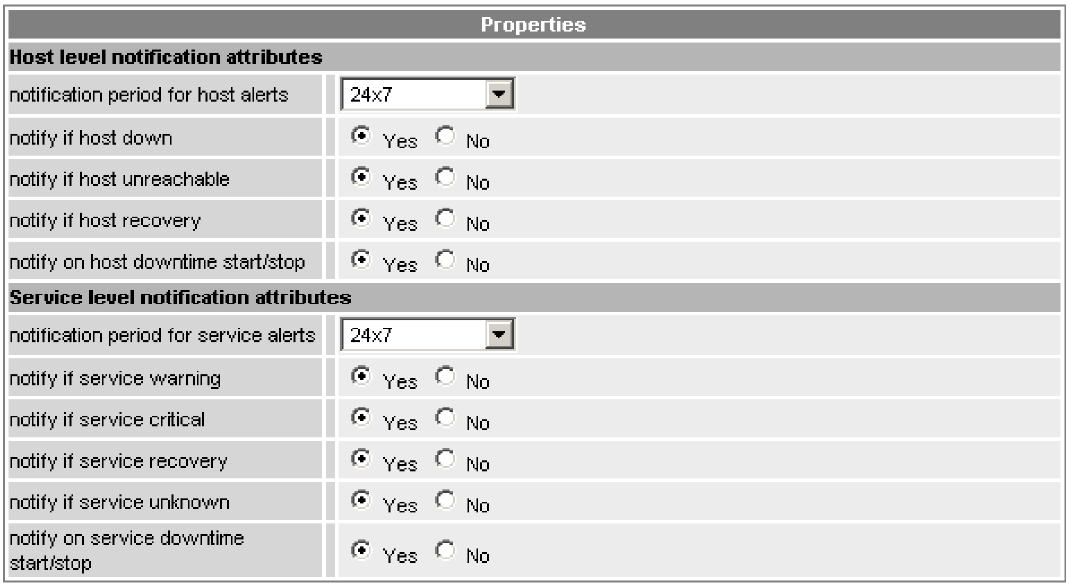
Notes

- You can define as many SNMP managers as you want. They will be all notified.
- If the message `WARNING: snmptrap command not found` is displayed during **Save and Reload**, you must install the appropriate package to provide the **snmptrap** command (refer to the *Bull System Manager Installation Guide,* 86 A2 54FA). The SNMP Manager configuration is not taken into account.

9.4.2 SNMP Notification Filter

To configure a SNMP Filter click the **Filter** link under the **SNMP** item in the **Notification** part of the **Monitoring** tab.

The following figure shows the window displayed for **Filter** settings:



Properties	
Host level notification attributes	
notification period for host alerts	24x7
notify if host down	● Yes ○ No
notify if host unreachable	● Yes ○ No
notify if host recovery	● Yes ○ No
notify on host downtime start/stop	● Yes ○ No
Service level notification attributes	
notification period for service alerts	24x7
notify if service warning	● Yes ○ No
notify if service critical	● Yes ○ No
notify if service recovery	● Yes ○ No
notify if service unknown	● Yes ○ No
notify on service downtime start/stop	● Yes ○ No

Figure 9-7. SNMP Filter properties

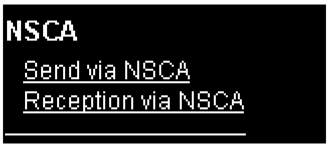
Filter Properties	Description
notification period for host alerts	Period during which host notifications must be sent to this contact. Possible values: **24x7**, **workhours**, **nonworkhours**, **none**. Default value: **24x7**.
notify if host down	Notify contact when hosts are down? Default value: **yes**.
notify if host unreachable	Notify contact when hosts are unreachable? Default value: **yes**.
notify if host recovery	Notify contact on host recovery? Default value: **yes**.
notify on host downtime start/stop	Notify contact when scheduled downtime is started or stopped for a host ? Default value: **yes**

Filter Properties	Description
notification period for service alerts	Time during which service notifications must be sent to this contact. Possible values: 24x7, workhours, nonworkhours, none. Default value: 24x7.
notify if service warning	Notify contact for warning service status? Default value: no.
notify if service critical	Notify contact for critical service status? Default value: yes.
notify if service recovery	Notify contact for service recovery? Default value: yes.
notify if service unknown	Notify contact for unknown service status ? Default value: yes
notify on service downtime start/stop	Notify contact when scheduled downtime is started or stopped for a service ? Default value: yes

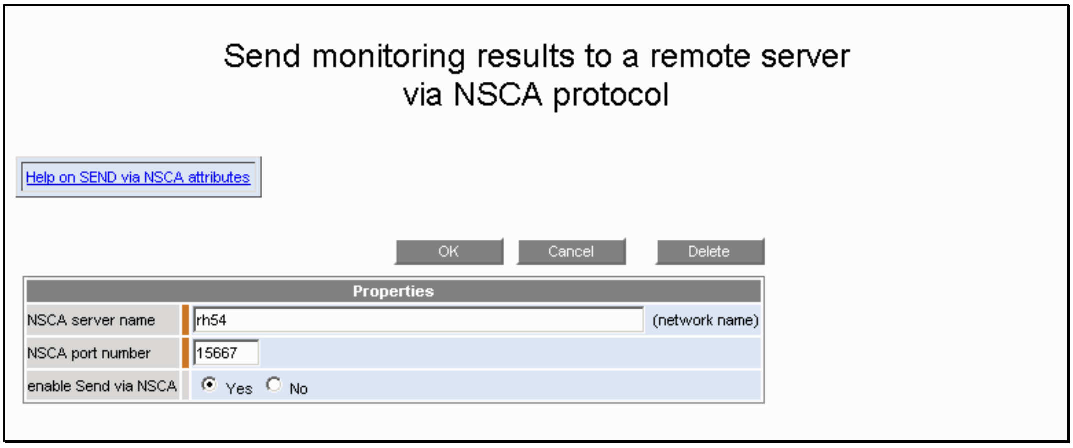
Table 9-5. SNMP Filter properties

Chapter 10. Configuring the NSCA Protocol

This chapter explains how to configure **NSCA**. NSCA functionalities (**send_nsca** and NSCA daemon) are delivered by NSCA server extension package.



Send via NSCA is used to configure the sending of check results to a remote monitoring server (a **BSM** server or a central **Nagios** one) via the **NSCA** protocol. The NSCA daemon must be running on the remote server. The monitoring services must be defined as passive (**monitoring on event** attribute set) on the remote server configuration.



Send monitoring results to a remote server via NSCA protocol

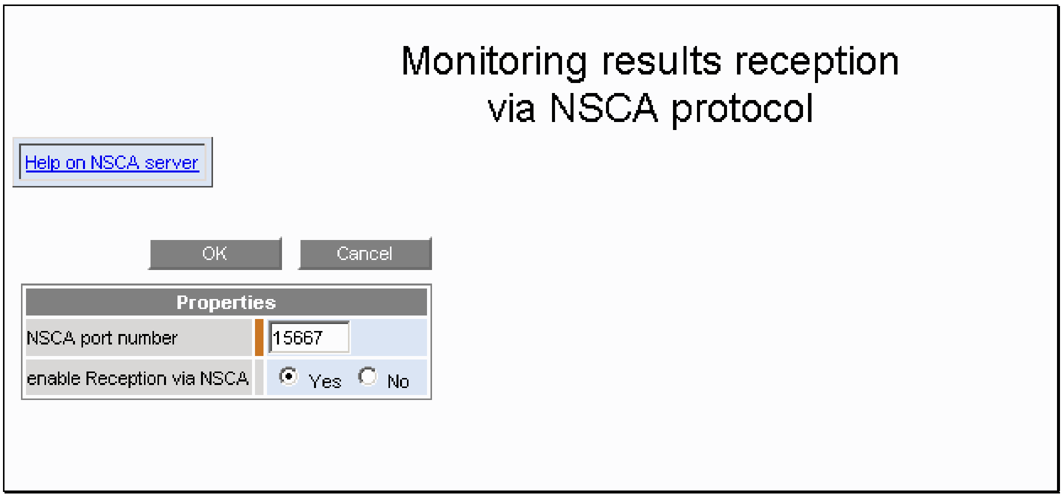
Properties		
NSCA server name	rh54	(network name)
NSCA port number	15667	
enable Send via NSCA	● Yes ○ No	

Figure 10-1 Send via NSCA edition

SEND NSCA Properties	Description
NSCA server name	Remote server netname, which will receive the monitoring results. The NSCA daemon must be running on this remote host
NSCA port number	NSCA daemon port number
Enable send via NSCA	Enable send NSCA mechanism. Default is no

Table 10-1 Send via NSCA properties

Reception via NSCA is used to configure the NSCA daemon listening for host and service check results from remote hosts. The monitoring services must be defined as passive services in the BSM configuration.



Monitoring results reception via NSCA protocol

Properties	
NSCA port number	15667
enable Reception via NSCA	● Yes ○ No

Figure 10-2 Reception via NSCA edition

NSCA Reception Properties	Description
NSCA port number	NSCA daemon port number
Enable reception via NSCA	Enable NSCA reception mechanism. Default is **no**. If it is set to yes, the NSCA daemon will be launched.

Table 10-2 Reception via NSCA properties

Chapter 11. Customizing the Bull System Manager Console

This chapter explains how to customize the Bull System Manager Console. The following customization tasks are described:

- Choosing the BSM applications that can be launched from the **Bull Tools** Bar.
- Specifying the **user's applications** that can be launched from the **Other** Bar. These applications may be any external web URL or any local command for the station on which the Bull System Manager Console is running.
- Choosing the **default view** that will be loaded in the Console Management Tree.
- Specifying the **maps** that will be displayed in the Bull System Manager Console.
- Specifying very important monitoring services that will be displayed with their status in the Bull System Manager Console **Focus** Pane.

The following figure shows a default view example of customization of the applications bar.

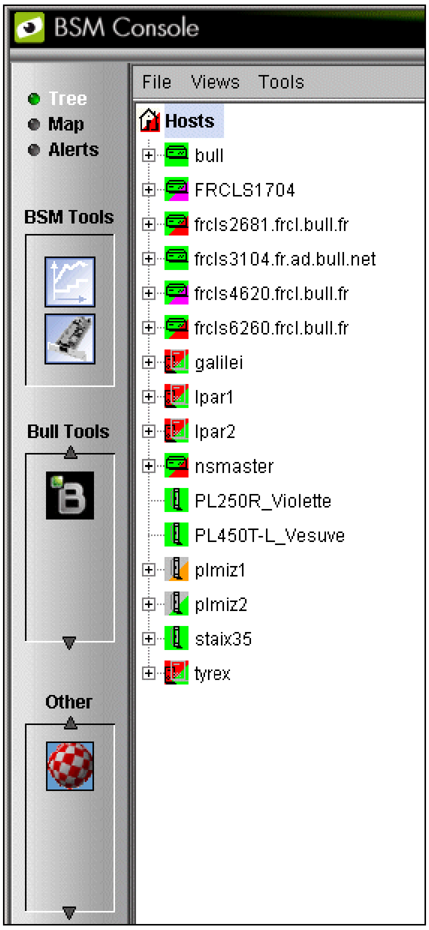


Figure 11-1. Customized default view and applications bar

To access the Console customization functions, click **Console** under the domain tab.

Then click the corresponding link to activate one of the following functions: **Applications, Default view, Maps and Focus services**.

11.1 Specifying Applications

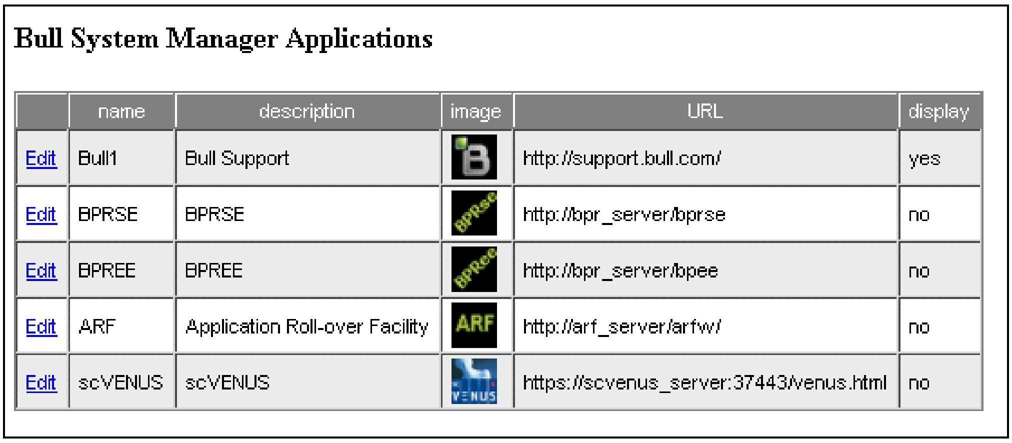
11.1.1 Bull System Manager Applications

Bull System Manager provides six Bull applications that can be displayed in the **Bull Tools** Bar:

- **Bull Support** (displayed by default)
- **ScVenusBPRSE** (Bull Performance Report Server Edition)
- **BPREE** (Bull Performance Report Enterprise Edition)
- **Application Roll-over Facility (ARF)**

To display these Bull applications, proceed as follows:

1. Click the **Applications** link under the **Console** tab. The list of the available applications is displayed:

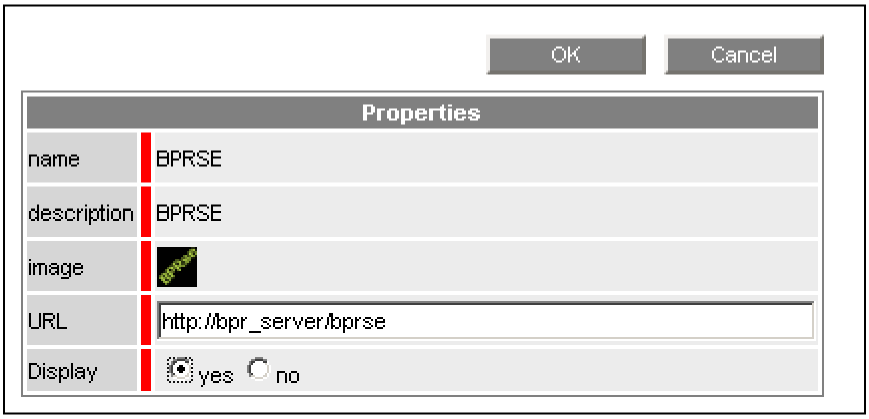


Bull System Manager Applications

	name	description	image	URL	display
Edit	Bull1	Bull Support	B	http://support.bull.com/	yes
Edit	BPRSE	BPRSE	BPRSE	http://bpr_server/bprse	no
Edit	BPREE	BPREE	BPREE	http://bpr_server/bpee	no
Edit	ARF	Application Roll-over Facility	ARF	http://arf_server/arfw/	no
Edit	scVENUS	scVENUS	VENUS	https://scvenus_server:37443/venus.html	no

Figure 11-2. Bull System Manager Applications

2. Click **Edit** for the Bull System Manager Application you want to display. The following **Properties** form appears:



Properties

name	BPRSE
description	BPRSE
image	BPRSE
URL	http://bpr_server/bprse
Display	● yes ○ no

Figure 11-3. Bull System Manager Application edition

3. Specify the URL if needed.

4. Check **Display** : **yes**.

5. Click **OK**.

11.1.2 User's Applications

Other applications can be defined with either access to a web URL or the activation of a command on the station where Bull System Manager Console is running.

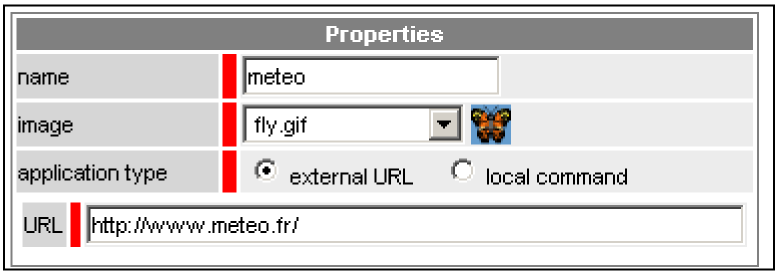
To configure a new application, proceed as follows:

1. Click the **Applications** link under the **Console** tab.

2. From the **Applications** page, click **New** to edit a new application.

   – Specify a name and select an image from those that are displayed (this image will be used as the application icon in the Applications bar).

   – For a web URL application: select **external URL** as application type and specify the full external URL (Figure 11-4).

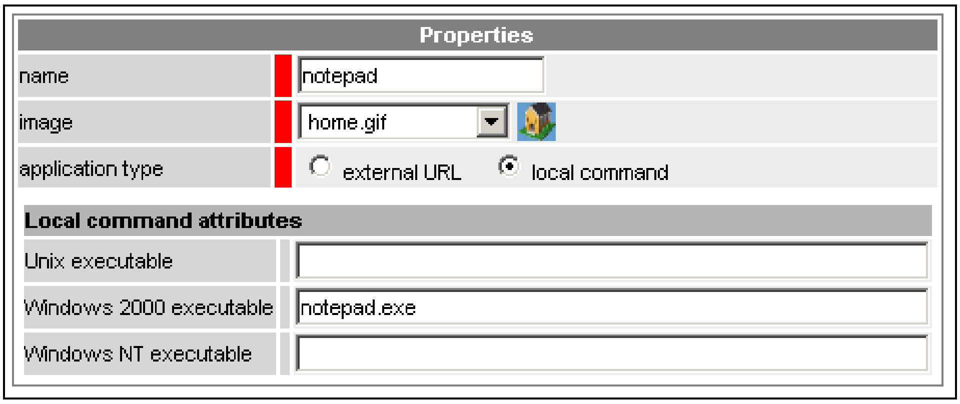


Properties

name	meteo
image	fly.gif
application type	● external URL ○ local command
URL	http://www.meteo.fr/

Figure 11-4. An application as a web URL

   – For a local command application: select **local command** as the application type and specify the command or executable that will be launched for each OS (Figure 11-5).



Properties

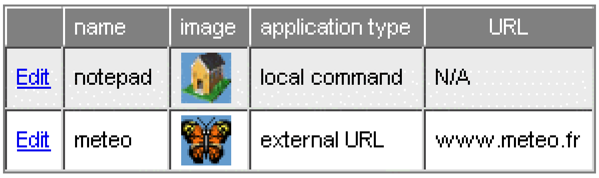
name	notepad
image	home.gif
application type	○ external URL ● local command

Local command attributes

Unix executable	
Windows 2000 executable	notepad.exe
Windows NT executable	

Figure 11-5. An application as a local command

3. Click **OK**. The list of the customized applications is displayed.



	name	image	application type	URL
Edit	notepad		local command	N/A
Edit	meteo		external URL	www.meteo.fr

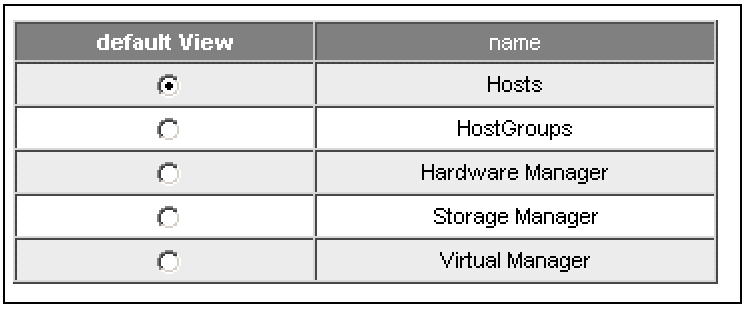
Figure 11-6. List of all applications

4. Do not forget to run **Save & Reload**.

11.2 Choosing the Default View

When Bull System Manager Console is started, the default view is displayed in the Management Tree section. You can then load another view from the **Load** menu. At installation time, the default view is the **Hosts** view. To change this default view, proceed as follows:

1. Click the **Default view** link under the Console tab. The following display appears:



default View	name
●	Hosts
○	HostGroups
○	Hardware Manager
○	Storage Manager
○	Virtual Manager

Figure 11-7. Choosing the default view

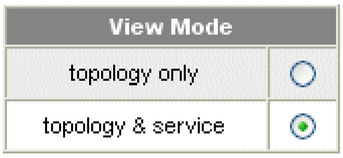
2. Select the required view and click OK.

3. Do not forget to **Save & Reload** in order to register your choice.

11.3 Choosing the View Mode

At instrallation time, when Bull System Manager Console is started, the views are displayed with the “topology & service” mode. In this mode all hosts with their services are displayed. You can choose the mode “topology” which allows to display only hosts. To change the view mode, proceed as follows:

1. Click the **view Mode** link under the Console tab. The following display appears:



View Mode	
topology only	○
topology & service	●

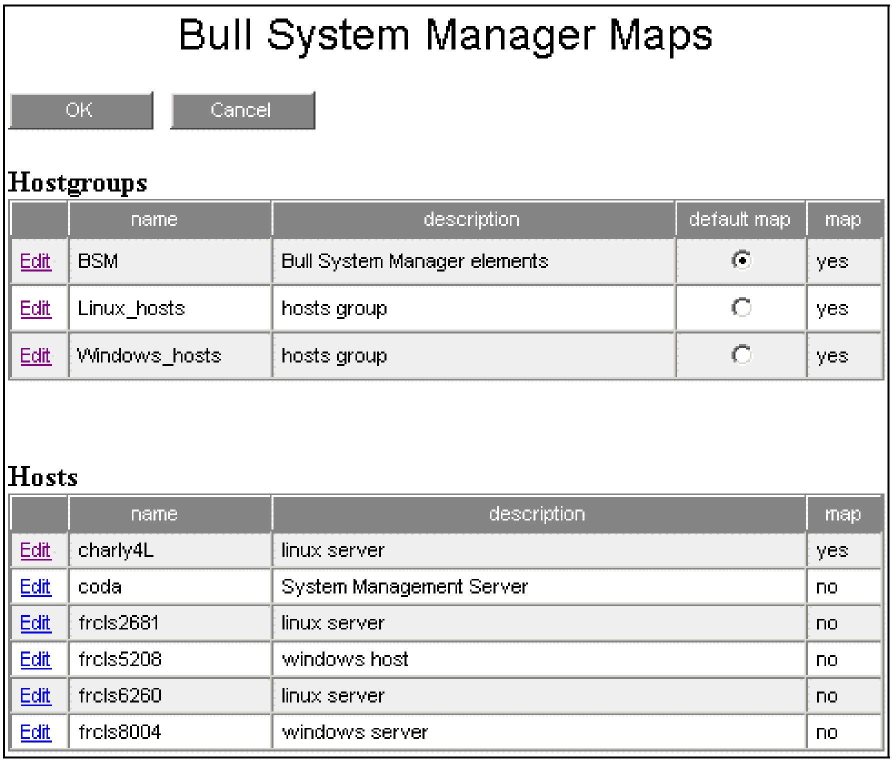
2. Select the required mode and click OK.

3. Do not forget to **Save & Reload** in order to register your choice.

11.4 Specifying Maps

Each hostgroup, platform and host can be represented as a map. A hostgroup (or platform) map is used to display their objects (hosts or hostgroups), animated with their status, at specified positions on the map. A host map is usually used to display an image of this host. In a map, each object can be represented by an icon or a rectangle (with or without a label).

To create or modify a map, click on the **Maps** link in the **Console** tab. The following window is displayed:



Bull System Manager Maps

Hostgroups

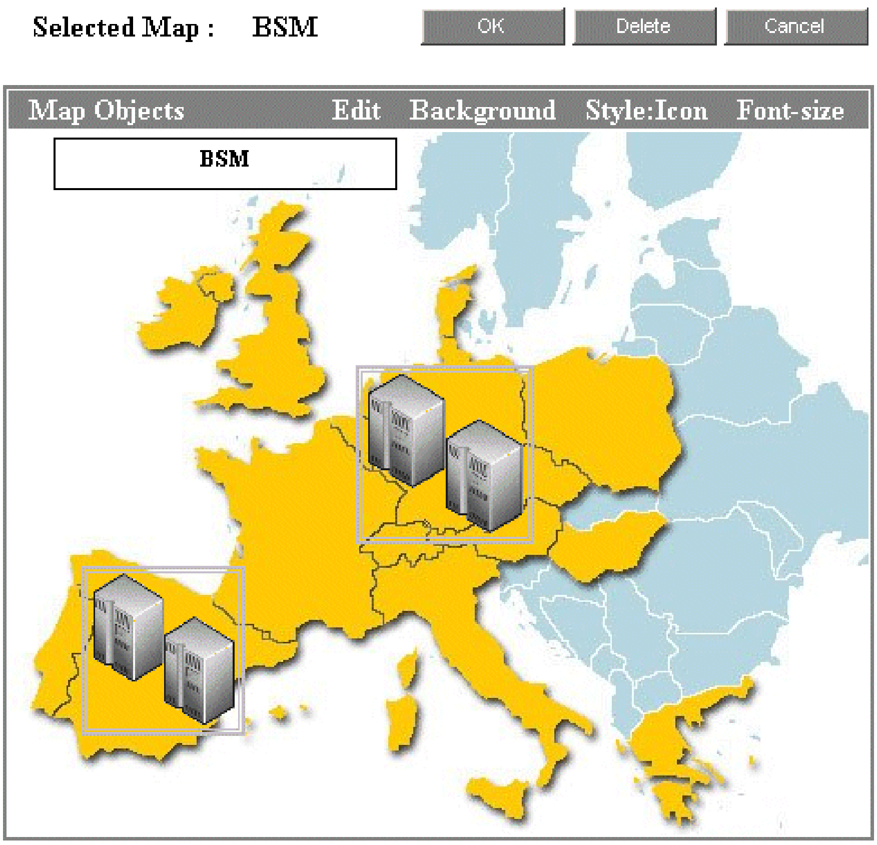
	name	description	default map	map
Edit	BSM	Bull System Manager elements	●	yes
Edit	Linux_hosts	hosts group	○	yes
Edit	Windows_hosts	hosts group	○	yes

Hosts

	name	description	map
Edit	charly4L	linux server	yes
Edit	coda	System Management Server	no
Edit	frcls2681	linux server	no
Edit	frcls5208	windows host	no
Edit	frcls6260	linux server	no
Edit	frcls8004	windows server	no

This window displays all the objects that can have a map. It allows you to edit a specific map and to specify which map is the default map.

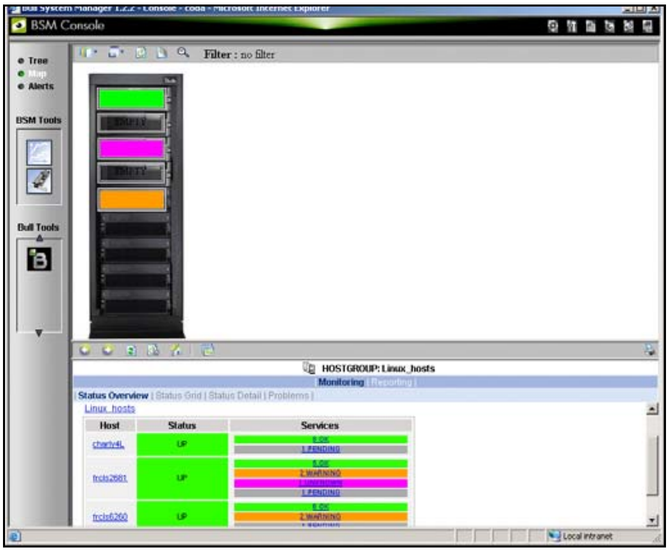
To edit a map, just click the **Edit** link of the chosen object (for example the hostgroup BSM). The following map editor is displayed:



From this editor you can display each object belonging to the chosen hostgroup, you can specify a background image (geographical image, machine image, etc.), you can move or resize each object with the mouse.

Commands	Description
Map Objects	Displays all the objects of the chosen hostgroup, a map title object and an empty object.
	Allows you to choose the object you want to display.
Edit	Allows you to remove a selected object from the map.
Background	Allows you to choose the background image.
Style	Allows you to choose the representation style of an object.
	Three styles are available: Icon, Rectangle, No label (rectangle without label).
FontSize	Allows you to change the font size of a label

Some examples of maps displayed in the Bull System Manager Console:



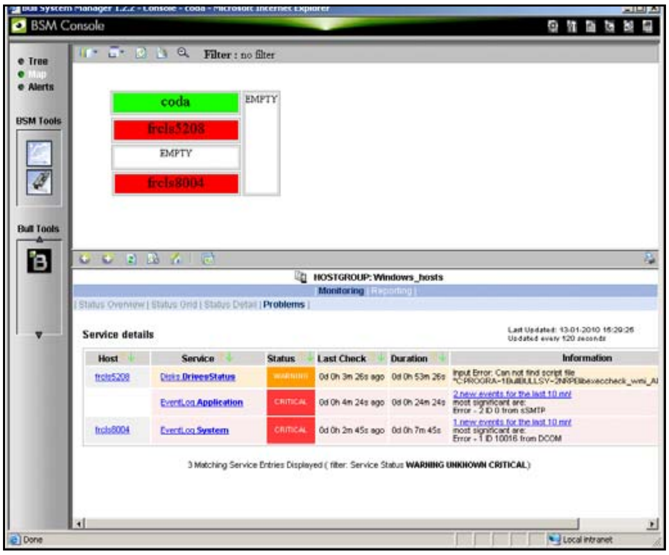
HOSTGROUP: Linux_hosts

| Monitoring | Reporting |

| Status Overview | Status Grid | Status Detail | Problems |

Linux_hosts

Host	Status	Services
charly4L	UP	8 OK 1 PENDING
frcls2681	UP	5 OK 2 WARNING 1 UNKNOWN 1 PENDING
frcls6260	UP	6 OK 2 WARNING



HOSTGROUP: Windows_hosts

| Monitoring | Reporting |

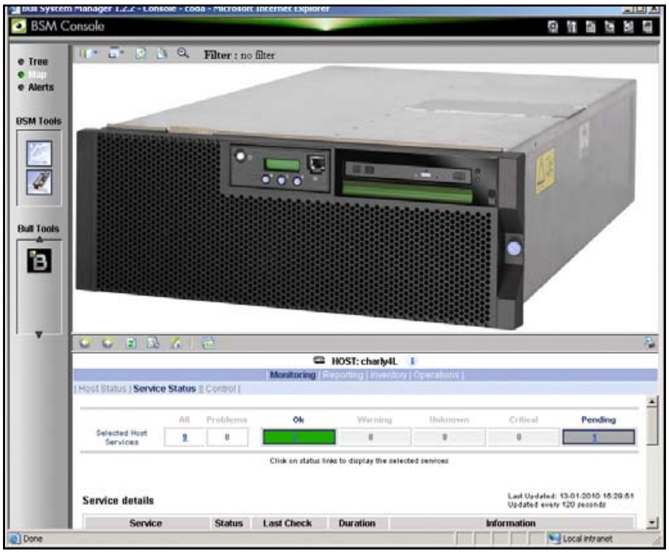
| Status Overview | Status Grid | Status Detail | Problems |

Service details

Last Updated: 13-01-2010 16:29:26
Updated every 120 seconds

Host	Service	Status	Last Check	Duration	Information
frcls5208	Disks DrivesStatus	WARNING	0d 0h 3m 26s ago	0d 0h 53m 26s	Input Error: Can not find script file "C:PROGRA~1BullBULLSY~2NRPElibexeccheck_wmi_Al
	EventLog Application	CRITICAL	0d 0h 4m 24s ago	0d 0h 24m 24s	2 new events for the last 10 mn! most significant are: Error - 2 ID 0 from sSMTP
frcls8004	EventLog System	CRITICAL	0d 0h 2m 45s ago	0d 0h 7m 45s	1 new events for the last 10 mn! most significant are: Error - 1 ID 10016 from DCOM

3 Matching Service Entries Displayed (filter: Service Status **WARNING UNKHOWN CRITICAL**)



HOST: charly4L

| Monitoring | Reporting | Inventory | Operations |

| Host Status | Service Status || Control |

	All	Problems	Ok	Warning	Unknown	Critical	Pending
Selected Host Services	9	0	8	0	0	0	1

Click on status links to display the selected services

Service details

Last Updated: 13-01-2010 16:29:51
Updated every 120 seconds

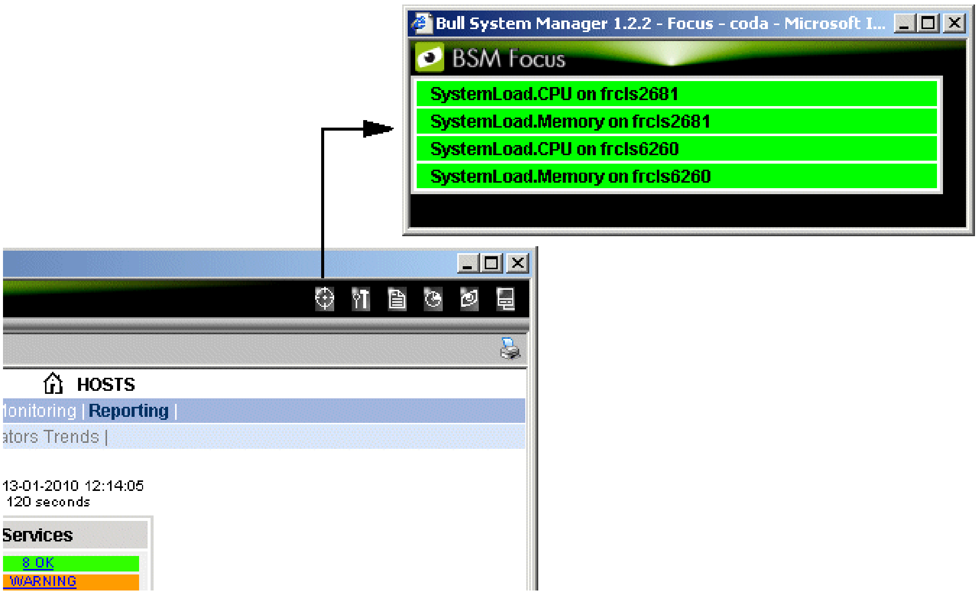
Service	Status	Last Check	Duration	Information

11.5 Specifying the Focus Pane

It may be useful to survey the status of the very important monitoring services. The **Bull System Manager Focus Windows**, displaying the status of defined focused services, allows you to do so.

To display the Bull System Manager Focus window, you have just to click on this icon from the Bull System Manager Console.

The following figure shows an example of a Bull System Manager Focus window.



Bull System Manager 1.2.2 - Focus - coda - Microsoft I...

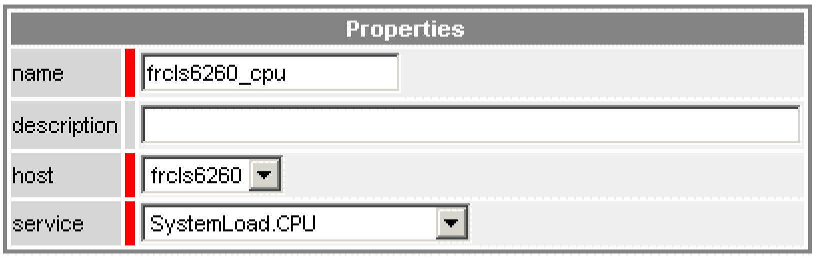
BSM Focus

SystemLoad.CPU on frcls2681
SystemLoad.Memory on frcls2681
SystemLoad.CPU on frcls6260
SystemLoad.Memory on frcls6260

13-01-2010 12:14:05
120 seconds

Figure 11-8. BSM Focus window

The following figure shows the settings window for focused services.



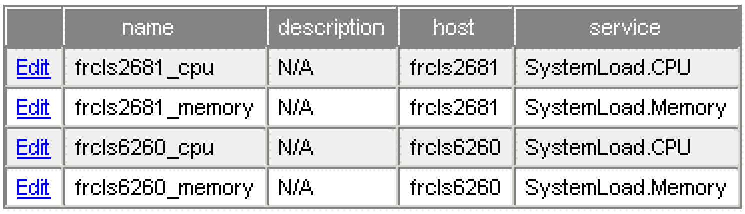
Properties	
name	frcls6260_cpu
description	
host	frcls6260
service	SystemLoad.CPU

Figure 11-9. Focused service properties

Focused Service Properties	Description
name	Focused service name
description	Short description of the focused service
host	Host associated with the focused service.
service	Monitoring service (already configured) associated with the focused service.

Table 11-1. Focused service properties

Click **OK** to display the list of all focused services.



	name	description	host	service
Edit	frcls2681_cpu	N/A	frcls2681	SystemLoad.CPU
Edit	frcls2681_memory	N/A	frcls2681	SystemLoad.Memory
Edit	frcls6260_cpu	N/A	frcls6260	SystemLoad.CPU
Edit	frcls6260_memory	N/A	frcls6260	SystemLoad.Memory

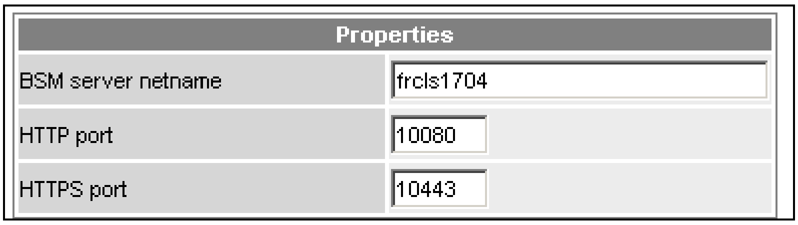
Figure 11-10. List of all focused services

Chapter 12. Configuring Local Settings

This chapter explains how to configure access to the Bull System Manager applications or to configure functional features for Bull System Manager.

12.1 Configuring BSM Server

To modify BSM Server characteristics, click the **Properties** link under the **BSM Server** item. The following form is displayed:



Properties	
BSM server netname	frcls1704
HTTP port	10080
HTTPS port	10443

Figure 12-1. BSM Server properties

Properties	Description
BSM Server netName	Resolved network name used to reach the Bull System Manager server. This value is used by the BSM Agent to send its Inventory information, and also for the notifications sent by mail that contains the BSM console URL to access more information.
HTTP port	Port used to reach the Bull System Manager server with non-secured HTTP protocol.
HTTPS port	Port used to reach the Bull System Manager server with secured HTTP protocol.

Notes

- When the ports number (HTTP, HTTPS) are modified, the Apache service must be restarted to take the new values into account.
- To use secured HTTP protocol (if your Apache server is not already secured with SSL), you have to edit the file **<Bull System Manager_install_dir>/core/etc/sysmgt-httpd.conf** and uncomment this line:

  ```
  # Include "<Bull System Manager_install_dir>/core/etc/sysmgt-ssl.conf
  ```

  The **sysmgt-ssl.conf** file uses a private key and a self-signed certificate, which are automatically installed for Apache during the installation of Bull System Manager.

12.2 Configuring Users & Roles

Bull System Manager applications must be authenticated, with an Apache user defined on the server part. The authenticated user is used to apply a user profile or role defined by the Role Base Management system.

Notes

- This **User** configuration is used not only by the BSM local console, but also by the BSM global console.
- For the distributed BSM solution, the different BSM servers MUST be configured in the same way with the same User and role.

Four roles, with distinct rights, are defined in Bull System Manager Server, as described below:

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

Table 12-1. Users, Roles and Functions

At installation time, three users are created and registered in the Role Based Management:

User	Password	Role
bsmadm	bsmadm	Administrator
nagios	nagios	Administrator
guest	guest	Operator

The administrator then can modify or register the other users of the Bull System Manager Applications.

mportant:

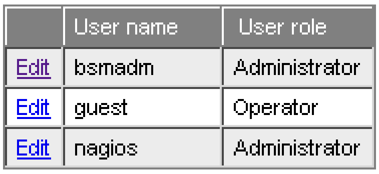
At least one user MUST always be defined with the Administrator role, to be able to configure Bull System Manager.

Notes

- The **Users & Roles** function is applicable to all Bull System Manager Windows and Linux platforms, except on Linux platforms with a PHP lower than 4.2.2 (Red Hat 7.3). In this case, use Administration commands to add/update Bull System Manager users.
- From NovaScale Master Release 4.0, the roles are exclusive to users.

To configure a user, proceed as follows:

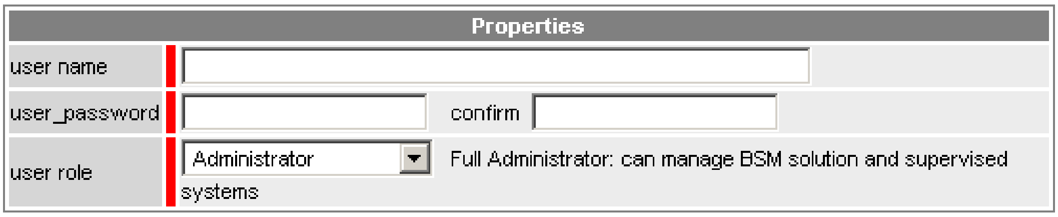
1. Click the **Users & Roles** link of the **Local Setting** tab. The list of the configured users appears:



	User name	User role
Edit	bsmadm	Administrator
Edit	guest	Operator
Edit	nagios	Administrator

Figure 12-2. Users allowed to access the Bull System Manager Applications

2. From the **Users & Roles** page, click **New** to edit a new user. This menu appears:



Properties

user name			
user_password		confirm	
user role	Administrator	Full Administrator: can manage BSM solution and supervised systems	

Figure 12-3. Users & Roles properties

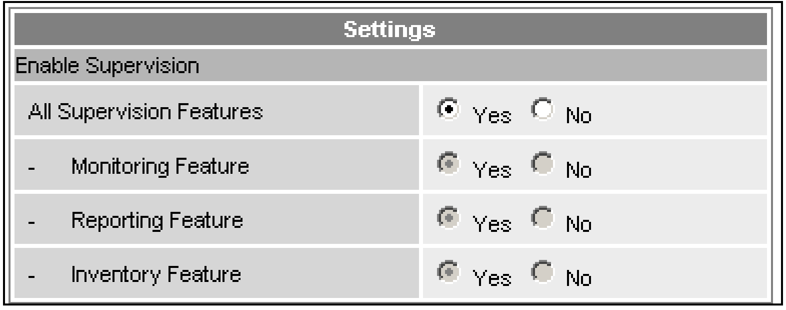
   – Enter the user name.
   – Enter the password
   – Select the exclusive role associated with this user.
   – Click **OK** to validate.

3. Repeat step 2 for each user to be created. Newly created users are now displayed in the **Users & Roles** page.

Note Check that the user has not opened a Bull System Manager session before you **Save & Reload** role modifications, as the user’s current session may become unstable.

12.3 Configuring Active Features

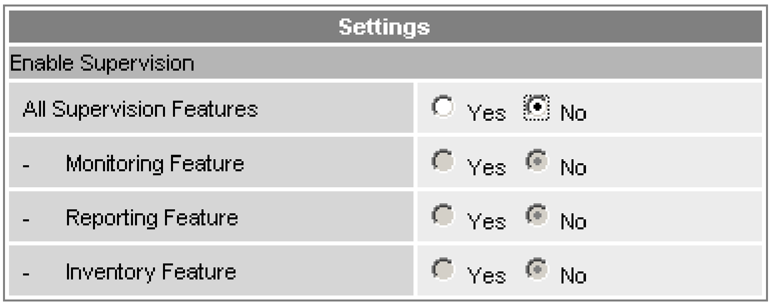
At installation time, the **Monitoring feature** is always enabled.
To disable the Monitoring feature, click the **Active features** link in the **Functionalities** part of the **Local Setting** tab. The features, grouped in two parts (Supervision and Remote Operation) are listed, as displayed in the following page:



Settings	
Enable Supervision	
All Supervision Features	● Yes ○ No
- Monitoring Feature	● Yes ○ No
- Reporting Feature	● Yes ○ No
- Inventory Feature	● Yes ○ No

Figure 12-4. Default Global Settings

To disable Monitoring (and associated Reporting and Inventory features), click the **No** check box corresponding to the **All Supervision Features** item.



Settings	
Enable Supervision	
All Supervision Features	○ Yes ● No
- Monitoring Feature	○ Yes ● No
- Reporting Feature	○ Yes ● No
- Inventory Feature	○ Yes ● No

Figure 12-5. Disabling Monitoring

Notes

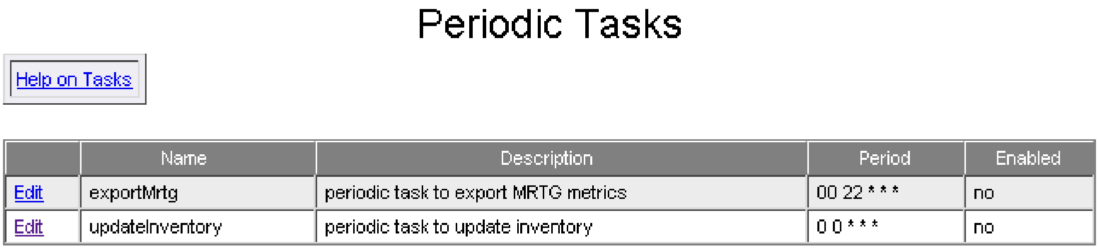
- As the **Reporting** and **Information** features are strongly linked to the **Monitoring** feature, when you enable or disable the Monitoring feature you also activate or deactivate the Reporting and Information features.
- The **Remote Operation** feature cannot be disabled in this version. However, if you do not want to use this feature, connect to the console using the Operator Role.
- When you disable / enable the Monitoring feature, you also affect the availability of applications in the Bull System Manager Console. **Any open Bull System Manager Console must be restarted subsequent to modifications in the Global Setting configuration.**

12.4 Configuring Periodic Tasks

BSM Server allows tasks to be launched automatically for various operations.

To activate or configure a task (period), click the **Periodic Tasks** link under the **Functionalities** item.

A page is displayed with all predefined tasks. In this version, only one task is available as displayed in the following window:



Periodic Tasks

	Name	Description	Period	Enabled
Edit	exportMrtg	periodic task to export MRTG metrics	00 22 * * *	no
Edit	updateInventory	periodic task to update inventory	0 0 * * *	no

Figure 12-6. Periodic Tasks

To get detailed information about the **exportMrtg** task, see *Export daily information of a MRTG* indicator, on page 158.

To get detailed information about updateInventory, see *Configuring Inventory*, on page 83.

Chapter 13. Configuring Global Settings

This chapter explains how to configure distributed Bull System Manager solutions, consisting of several servers, each one of them managing a set of hosts and providing a global console allowing all elements to be viewed.

Each server manages its local configuration and publishes it to a central database (CMDB) accessible for the whole server. By default, the database is hosted on the local server. In order to set a distributed solution, you have to define a BSM server that hosts the CMDB and to configure other servers to fill the central CMDB.

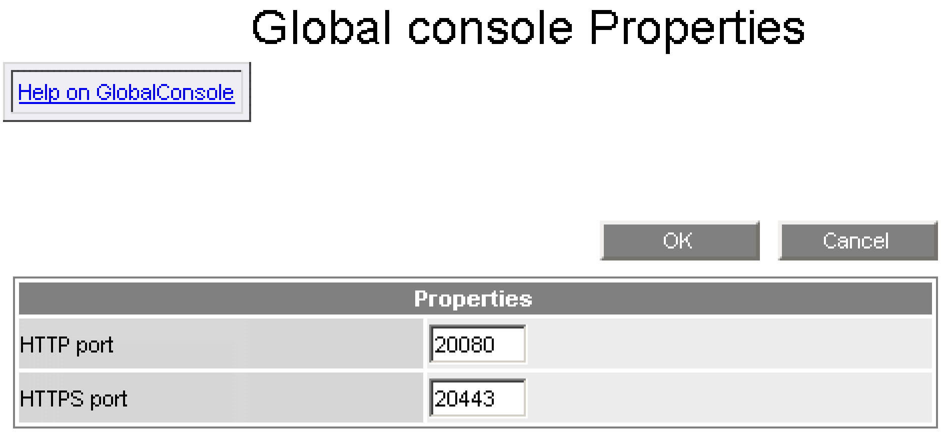
In this part, you can configure the port to access the Global Console or to redefine the server that hosted the central database.

Important:
The distributed solution requires that the **NDOutils** extension is installed on all **BSM** server nodes.

13.1 Configuring Global Console

To change the Global Console properties, click the **Properties** link under the **Global Console** item.

The following window allows you to change the HTTP port numbers used to access the global console:



Properties	
HTTP port	20080
HTTPS port	20443

Figure 13-1. Global Console properties

Click the **OK** button to apply your changes.

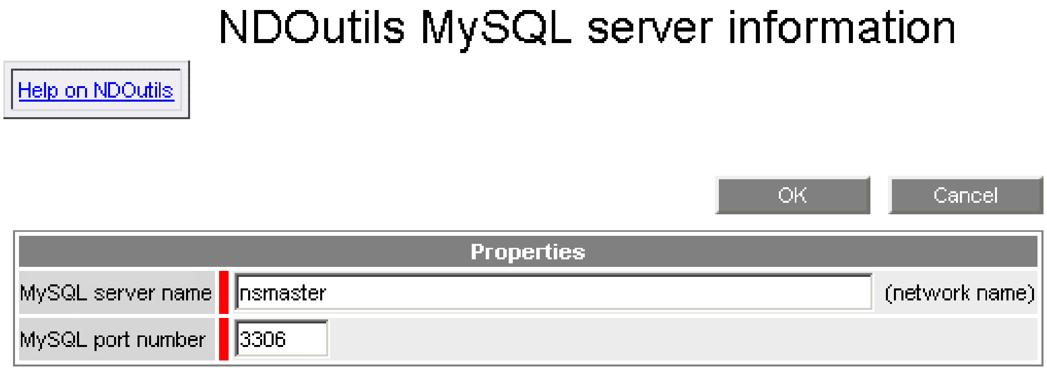
Notes

- When the ports number (HTTP, HTTPS) are modified, the Apache service must be restarted to take into account the new values.
- The port number used for the Global Console must be different from those set for the Local Console (see *Configuring BSM Server*, on page 195).

13.2 Configuring NDOutils Db Server

To change the MySQL server properties, click the **MySQL DB server** link under the **NDOutils** item.

The following page allows you to change the hostname and the port used to access the MySQL database:



NDOutils MySQL server information

Properties		
MySQL server name	nsmaster	(network name)
MySQL port number	3306	

Figure 13-2. NDOutils MySQL server configuration

Properties	Description
MySQL Server netName	Resolved network name used to reach the MySQL server This value is used by the NDOutils part to determine which server hosted the central database. Must correspond to a BSM server with the NDOutils extension installed. This value is initialized with the hostname of the BSM server.
MySQL port number	Port used to reach to reach the MySQL server The value is initialized to **13306** for a Windows server and to **3306** for a Linux server.

Click the **OK** button to apply your changes.

Important:

The MySQL port number differs for Linux and Windows systems. If a distributed solution contains heterogeneous servers, then do not forget to modify the port in with regard to the BSM server OS.

13.3 Example

The following example shows how to set a distributed solution with three BSM Servers: BSM1, BSM2 and BSM3. The central database is hosted by BSM1.

13.3.1 Configuration of the Global Console

By default, the **http** and **https** ports for the Global Console are set to 20080 and 20443, respectively.

If you want to change these values, it must be done on all BSM server nodes involved in the distributed solution.

13.3.2 Configuration of the NDOutils Db Server

13.3.2.1 Central node, BSM1

By default, the **NDOutils** Db server is defined with the BSM server as server and default MySQL port. So, nothing has to be done on the central node, except if you have changed the MySQL port.

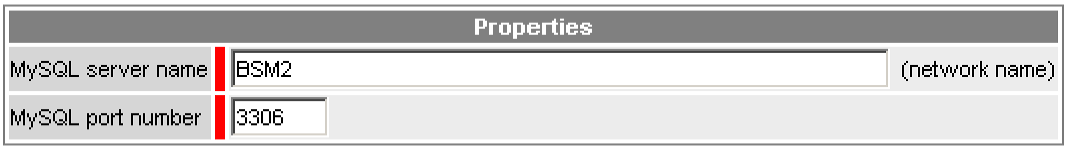
13.3.2.2 Secondary nodes, BSM2 and BSM3

The **NDOutils MySQL** server must be changed on the secondary nodes, to refer to the central node, BSM3.

For each secondary node:

1. Launch the GUI Configuration
2. Click the Global Setting tab
3. Click the NDOutils DB Server

The following page is displayed:



Properties		
MySQL server name	BSM2	(network name)
MySQL port number	3306	

Figure 13-3. NDOutils DB Server BSM2 configuration

4. Replace BSM2 with BSM1
5. Click the OK button to apply your change
6. Perform **Save & Reload** to populate the BSM1 CMDB with the configured objects of the secondary node.

Appendix A. Predefined Categories and Services

The following table lists categories and services, with their default values. It also indicates if the **Clone** function is available. Services in **bold** text are the default services in place for all hosts, following the installation of Bull System Manager.

Category	OS	Category hostList	Hardware model	Service	Service hostList	Clone function	Perfdata (PNP4Nagios)
SystemLoad	Windows	*	Any	**CPU**	*		CPU_1mn CPU_10mn
				Memory	*		MemoryUsed
SystemLoad	Linux	*	Any	**CPU**	*		CPU_1mn CPU_5Mn CPU_15mn
				Memory	*		MemoryUsed
				Users	*		
				Processes	*		NbProc
				Swap	None		swap
				Zombies	None		
SystemLoad	AIX			**CPU**	*		cpuLoad cpuUser cpuSys cpuWait cpuIdle
				PagingSpace	*		Paging_space Paging-out Paging-in
				Swap	*		swap
				LoadAverage	None		
				Memory	None		MemoryUsed
				Processes	None		NbProc
				Users	None		
				Zombies	None		
LogicalDisks	Windows	*	Any	**All**	*		
				C	None	x	C_DiskUsed
EventLog	Windows	*	Any	**System**	*		
				Application	*		
				Security	*		
Windows Services	Windows	*	Any	**EventLog**	*	x	
				Networking	None	x	
				Com	None	x	
				Peripherals	None	x	
				Management	None	x	
FileSystems	Linux	*	Any	**All**	*		FileSystem name list
				/usr	None	x	/usr
FileSystems	AIX	*	Any	**All**	*		FileSystem name list
				/usr	None		/usr
Syslog	Linux	*	Any	**AuthentFailures**	*	x	
				RootAccess	None	x	
				Alerts	*		
Syslog	AIX	*	Any	**Errors**	*		nbErr
				Alerts	*		
Linux Services	Linux	*	Any	**syslogd**	*	x	
AIX	AIX	*	Any	**syslogd**	*		

Category	OS	Category hostList	Hardware model	Service	Service hostList	Clone function	Perfdata (PNP4Nagios)
Services							
Internet	Any (W/L)	None	Any	http	*		
				FTP	None		
				http_BSM	None	x	
				TCP_7	None	x	
				UDP_7	None	x	
Hardware	Any		I/O Switch Module	Health	host		
Hardware	Any (W/L)	*	NS 4000, 5000, 6000 NS Blade, EL Blade	Health	host (1)		
			NSR400,T800, 3000,4000 Express 5800 , ns bullion	Alerts	host (1)	x	
Hardware			Escala PL	CecStatus	host (1)	x	
			Escala PL	Events	host (1)	x	
Power	Any		NS 4000, NS 3000, Express 5008, NS T800, NS R400, ns bullion	Status	host (1)		
			NS 9019, ns bullion	Consumption	host(1)		<consumption sensor name>
PAM	Any (W/L)	*	Any	GlobalStatus	* (1)		
				Alerts	* (1)		
CMM	Any (W/L)	*	Any	ChassisStatus	* (1)		
				Alerts	* (1)		

Table A–1. Predefined categories and services

*W means Windows, L means Linux and W/L means both.
(1) The host list is generated automatically during the definition of the host, depending on semantic checks and links between hosts and managers (see *Configuring Hosts*, on page 27).

A.1 SystemLoad Category

CPU (Windows)

Monitors total CPU load percentages over two periods of time (1 and 10 min). The final status is the worst status for the two periods. If status is not OK, the service indicates the process with the highest consumption (if any) at request time. By default, **warning** thresholds are **80** (over 1 min) and **60** (over 10 min) and **critical** thresholds are **90** (over 1 min) and **80** (over 10 min).

Memory (Windows)

Monitors memory usage percentage (i.e. the sum of physical and virtual memory, also known as **commit charge**), in terms of percentage or size. By default, the **warning** threshold is **70** and the **critical** threshold is **90**.

CPU (Linux)

Monitors total CPU load percentage over three periods of time (1 min, 5 min and 15 min). Final status is the worst status for the three periods. By default, **warning** thresholds are **80** (over 1 min), **70** (over 5 min) and **60** (over 15 min) and **critical** thresholds are **90** (over 1 min), **80** (over 5 min) and **70** (over 15 min).

Memory (Linux)

Monitors total memory usage percent (i.e. the sum of physical memory and virtual memory). By default, the **warning** threshold is **70** and the **critical** threshold is **90**.

Swap (Linux)

Monitors system swap percentage. By default, the **warning** threshold is **50** and the **critical** threshold is **80**.

Users (Linux)

Monitors the number of users currently logged on. By default, the **warning** threshold is **15** and the **critical** threshold is **20**.

Processes (Linux)

Monitors the number of processes running on the system. By default, the **warning** threshold is **150** and the **critical** threshold is **200**.

Zombies (Linux)

Monitors the number of zombie processes (state = Z) running on the system. By default, the **warning** threshold is **5** and the **critical** threshold is **10**.

A.2 LogicalDisks Category

All

Monitors the percentage of used space for all the local disks. By default, the **warning** threshold is **80** and the **critical** threshold is **90**.

C

Monitors the percentage of used space for the local disk C: By default, the **warning** threshold is **80** and the **critical** threshold is **90**.

A.3 EventLog Category

Application

Monitors the number of Error, Warning and Information events generated in the Application event log over the last 30 minutes. By default, the **warning** threshold is **10 Information events** or at least **1 Warning event** and the **critical** threshold is at least **1 Error event**.

System

Monitors the number of Error, Warning and Information events generated in the System event log over the last 30 minutes. By default, the **warning** threshold is **10 Information events** or at least **1 Warning event** and the **critical** threshold is at least **1 Error event.**

Security

Monitors the number of Audit Success, Audit Failures, Error and Warning events generated in the Security event log over the last 30 minutes. By default, the **warning** threshold is **10 Audit Success events** or at least **1 Warning event** and the **critical** threshold is at least **1 Audit Failure** or **1 Error event**.

A.4 WindowsServices Category

EventLog

Monitors the Windows services ensuring event-logging functions. Status is set to **warning** at least 1 **service is paused** and the **others are running**. Status is set to **critical** if at least 1 **service does not exist** or 1 **service is not running**.

EventLog (Event Log): logs event messages issued by programs and Windows. Event Log reports contain information that can be useful in diagnosing problems. Reports are viewed in the Event Viewer.

Networking

Monitors the Windows services ensuring networking functions. Status is set to **warning** if at least 1 **service is paused** and the **others are running**. Status is set to **critical** if at least 1 **service does not exist** or 1 **service is not running**.

RpcSs (Remote Procedure Call (RPC)): provides the endpoint mapper and other miscellaneous RPC services.

TrkWks (Distributed Link Tracking Client): sends notifications of file moving between NTFS volumes in a network domain.

Dhcp (DHCP Client): manages network configuration by registering and updating IP addresses and DNS names.

Dnscache (DNS Client): resolves and caches Domain Name System (DNS) names.

Netman (Network Connections): manages resources in the Network and Dial-Up Connections folder, in which you can view both local area network and remote connections.

Com

Monitors the Windows services ensuring **Com+** notification functions. Status is set to **warning** if at least 1 **service is paused** and the **others are running**. Status is set to **critical** if at least 1 **service does not exist** or 1 **service is not running**.

SENS (System Event Notification): tracks system events such as Windows login, network, and power events. Notifies COM+ Event System subscribers of these events.

EventSystem (COM+ Event System): provides automatic distribution of events to subscribing COM components.

Peripherals

Monitors the Windows services ensuring peripheral management functions. Status is set to **warning** if at least 1 **service is paused** and the **others are running**. Status is set to **critical** if at least 1 **service does not exist** or 1 **service is not running**.

NtmsSvc (Removable Storage): manages removable media, drives, and libraries.

PlugPlay (Plug and Play): manages device installation and configuration and notifies programs of device changes.

Management

Monitors the Windows services ensuring computer management functions. Status is set to **warning** if at least 1 **service is paused** and the **others are running**. Status is set to **critical** if at least 1 **service does not exist** or 1 **service is not running**.

Wmi (Windows Management Instrumentation Driver Extensions): provides systems management information to and from drivers.

WinMgmt (Windows Management Instrumentation): provides system management information.

dmserver (Logical Disk Manager): Logical Disk Manager Watchdog Service.

A.5 FileSystems Category

All

Monitors the percentage of used space for all the mounted FileSystems except CD-ROM and floppy. By default, the warning threshold is 80 and the critical threshold is 90.

/usr

Monitors the percentage of free space for the /usr FileSystem. By default, the warning threshold is 80 and the critical threshold is 90.

A.6 Syslog Category

AuthentFailures

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** (such a line traps the same error as a **FAILED LOGIN** line, already detected).

Status is set to **warning** if there is at least **1 new matching line since the last check**. Status is only set to **critical** state if a processing error occurs.

Note: **warning status** may be transitory in the Console. When a new matching line appears in the log file, the service sets status to warning only during the interval between the check that detects the error and the next one (if no new error appears). You are therefore advised to activate notification and to consult the service history regularly to see if any errors have been detected.

The **notifyRecovery** field is set to **no** for this service, as it is not applicable for this type of service.

RootAccess

Monitors the /var/log/messages file for the detection of a session opened with the root user. It searches for lines containing **session opened for user root**.

Status is set to **warning** if there is at least **1 new matching line since the last check**. Status is only set to **critical** state if a processing error occurs.

Note: **warning status** may be transitory in the Console. When a new matching line appears in the log file, the service sets status to warning only during the interval between the check that detects the error and the next one (if no new error appears). You are therefore advised to activate notification and to consult the service history regularly to see if any errors have been detected.

The **notifyRecovery** field is set to **no** for this service, as it is not applicable for this type of service.

Alerts
(Linux, AIX)

Linux and AIX hosts:
When an alert is sent from the Bull System Manager agent, it is processed by the Bull System Manager server.

Note: The **BSM-SYSLOG-MSG.mib** mib must be integrated in the Bull System Manager application (see *Integrating MIBs*, on page 121).

A.7 LinuxServices Category

syslogd

Monitors that there is one, and only one, syslogd process running on the system. syslogd is a system utility daemon that provides support for system logging. Status is set to **warning** if the number of syslogd processes is **not 1**. Status is only set to **critical** state if a processing error occurs.

A.8 Internet Category

FTP

Checks the accessibility of FTP on its standard port **21**. Status is set to **warning** if the **connection is successful**, but **incorrect response messages** are issued from the host and to **critical** if **response time exceeds 10 seconds** or if the **connection with the server is impossible**.

HTTP

Monitors the HTTP access of the hosts on port **80** on the '/' URL (i.e. **http://host:80/**). The **timeout value** is **10 seconds**. Status is set to **warning** for **HTTP errors: 400, 401, 402, 403 or 404** such as **unauthorized access** and to **critical** if **response time exceeds 10 seconds** or for **HTTP errors 500, 501, 502 or 503**, or if the **connection with the server is impossible**.

TCP 7

Monitors the TCP 7 port (echo) access of the hosts. Status is set to **critical** if the **connection with the server is impossible**.

UDP

Monitors the UDP 7 port (echo) access of the hosts. Status is set to **critical** if the **connection with the server is impossible**.

A.9 Reporting Category

perf_indic

Checks the status of a component based on the value collected by MRTG.

A.10 Hardware Category

Health
For NovaScale 4000 series hosts managed by ISM or for NovaScale 5000 & 6000 series hosts managed by PAM or for NovaScale Blade series hosts or Enterprise Line Blade series hosts or I/O Switch Module host managed by CMM. This service checks the host hardware status reported by the associated ISM, PAM or CMM.

Alerts
NovaScale 4000 series hosts:
When an alert is sent from the NovaScale host, it is processed by the Bull System Manager server.

Note: The **basebrd5.mib** mib must be integrated in the Bull System Manager application (see *Integrating MIBs*, on page 153).

NovaScale 4000, 3000, T800, R400 series and Express 5800 hosts:
When an alert is sent from the host management card, it is processed by the Bull System Manager server.

Note: The **bmclanpet.MIB** mib must be integrated in the Bull System Manager application (see *Integrating MIBs*, on page 153).

Do not forget to configure the Hardware manager or agent to send SNMP traps to the Bull System Manager server by adding the Bull System Manager server host address to the SNMP managers list. This configuration is explained in the corresponding Hardware Manager documentation.

CECStatus
For Escala PL series servers managed by an HMC. This service checks the CEC status, as reported by the HMC.

Events
For Escala PL series servers managed by an HMC. This service checks the hardware status, based on the presence of hardware events, as reported by the HMC.

Note These services are automatically applied to the specified targets, when they are configured.

PowerStatus
For IPMI compliant server hosts (NS R400, NS T800, NS 3005, etc.). This service may check the power status of the server (ON or OFF).

Sensor
For IPMI compliant server hosts (NS R400, NS T800, NS 3005, etc.). This service can check a sensor (Volt, Temperature, FanSpeed, etc.) and get the current numeric value.

SensorAvg
For IPMI compliant server hosts (NS R400, NS T800, NS 3005, etc.). This service may check a set of sensors (Volt, Temperature, FanSpeed, etc.) and get current numeric values and finally return an average value.

A.11 Power Category

Status
For IPMI compliant server hosts (NS R400, NS T800, NS 3005, etc.). This service may check the power status of the server (ON or OFF).

Consumption
For IPMI compliant server hosts (NS R400, NS T800, NS 3005, etc.). This service can check a sensor (Volt, Temperature, FanSpeed, etc.) and get the current numeric value.

A.12 PAM Category

GlobalStatus

For hosts running PAM (these hosts are also named PAP). This service checks global hardware status for all NovaScale 5000 & 6000 series platforms managed by a PAM manager.

For information about PAM, refer to the *Bull NovaScale 5000 & 6000 Series User's Guide*.

Alerts

When an alert is sent from PAM, it is processed by the Bull System Manager server.

Note: The **PAMeventtrap.MIB** mib must be integrated in the Bull System Manager application (see *Integrating MIBs*, on page 153).

Do not forget to configure the Hardware manager to send SNMP traps to the Bull System Manager server by adding the Bull System Manager server host address to the SNMP managers list. This configuration is explained in the *NovaScale 5000 or 6000 Series User's Guide*.

Note These services are automatically applied to the specified targets, when they are configured.

A.13 CMM Category

ChassisStatus

For hosts running CMM (these hosts are management cards in the chassis). This service checks global hardware status for all common resources shared by NovaScale Blade series hosts managed by a CMM manager.

Alerts

For NovaScale Blade series hosts managed by CMM. When an alert is sent from the NovaScale manager, it is processed by the Bull System Manager server and forwarded to the remote maintenance center (if specified).

Note: The **mmalert.mib** mib must be integrated in the Bull System Manager application (see *Integrating MIBs*, on page 153).

Note These services are automatically applied to the specified targets, when they are configured. Correct service processing requires that Bull System Manager server is declared as SNMP Manager in the CMM configuration. For details, please refer to the *NovaScale Blade Chassis Management Module Installation and User's Guide*.

Appendix B. Generated Categories and Services

The following table lists the generated services with the corresponding host.

Category	Service	Model	Conditions	Reference
Power	Status	NS 4000	out-of-band attributes set	NS4000
Hardware	Alerts	NS 4000	out-of-band attributes set	NS4000
Hardware	Health	NS 4000	managed by ISM	Hardware Manager
Hardware	Health	NS blade	managed by CMM	NS Blade
Hardware	Health	EL BLade	managed by CMM	EL Blade
Hardware	Health	I/O Switch Module	managed by CMM	I/O Switch Module
Hardware	Health	NS 5005	managed by PAM	NS 5005
Power	Status	Express 5800	out-of-band attributes set	Express 5800
Hardware	Alerts	Express 5800	out-of-band attributes set	Express 5800
Hardware	PowerStatus	NS 3005	out-of-band attributes set	NS 3005
Hardware	Alerts	NS 3005	out-of-band attributes set	NS 3005
Power	Status	NS 9010	out-of-band attributes set	NS 9010
Power	Consumption	N 9010	out-of-band attributes set	NS 9010
Hardware	Alerts	NS 9010	out-of-band attributes set	NS 9010
Power	Status	ns bullion	out-of-band attributes set	ns bullion
Power	Consumption	ns bullion	out-of-band attributes set	ns bullion
Hardware	Alerts	ns bullion	out-of-band attributes set	ns bullion
Power	Status	NS T800	out-of-band attributes set	NS T800
Hardware	Alerts	NS T800	out-of-band attributes set	NS T800
Power	Status	NS R400	out-of-band attributes set	NS R400
Hardware	Alerts	NS R400	out-of-band attributes set	NS R400
Hardware	CECStatus	Escala PL	managed by HMC	PL Server
Hardware	Events	Escala PL	managed by HMC	PL Server
PAM	GlobalStatus	-	manager PAM	NS 5005
PAM	Alerts	-	manager PAM	NS 5005
CMM	ChassisStatus	-	manager CMM	NS Blade
CMM	Alerts	-	manager CMM	NS Blade

Table B–1. Generated categories and services

Appendix C. Check Commands for Customizable Services

This chapter describes the usage of the **Nagios** check commands by customizable services. See *Check Commands*, on page 102, for the list of the check commands used by the predefined services.

Note The **!** character must be used to separate the check command parameters in the service definition.

Launching Linux Check Commands

All Linux check commands for Nagios are launched by the **check_nrpe** command. For instance, the check command associated to the **SystemLoad.Users** service is:

```
check_nrpe!’/opt/BSMAgent/nrpe/libexec/check_users -w 15 -c
```

The check always invokes the **/opt/BSMAgent/nrpe/libexec/check_nrpe** executable with a unique parameter corresponding to the check command launched on the target system. In the following sections, the usage given for the check command corresponds to this parameter. The name of the command launched by **check_nrpe** must not be modified.

C.1 check_ns_eventlog (Windows)

Usage

check_ns_eventlog <period> strlog=<LogName> [filtersrc=<SrcList>] [excludesrc=<SrcList>] [eInf=<nb>] [wWarn=<nb>] [eWarn=<nb>] [wErr=<nb>] [eErr=<nb>] [wAudS=<nb>] [eAudS=<nb>] [wAudF=<nb>] [eAudF=<nb>]

<period>	Time (in minutes) going backwards from the present moment for the period used for event checking. Events before this period are ignored.
strlog=<LogName>	Defines the event log (Application, Security, System, DNS Server, etc.) from which events must be retrieved.
filtersrc=<SrcList>	Only events logged by sources from this list must be retrieved from the Log defined with the strlog=<LogName>.
excludesrc=<SrcList>	Events logged by sources from this list are excluded from the events retrieved from the log defined with strlog=<LogName>.
wInf=<nb>	Number of Information events that result in a WARNING message.
eInf=<nb>	Number of Information events that result in a CRITICAL message.
wWarn=<nb>	Number of Warning events that result in a WARNING message.
eWarn=<nb>	Number of Warning events that result in a CRITICAL message.
wErr=<nb>	Number of Error events that result in a WARNING message.
eErr=<nb>	Number of Error events that result in a CRITICAL message.
wAudS=<nb>	Number of Audit Success events that result in a WARNING message.
eAudS=<nb>	Number of Audit Success events that result in a CRITICAL message.
wAudF=<nb>	Number of Audit Failure events that result in a WARNING message.
eAudF=<nb>	Number of Audit Failure events that result in a CRITICAL message.

The **<period>** parameter and the **<strlog>** parameter are required.

<LogName> argument containing a blank space must be enclosed by double quotes.

The optional **[filtersrc=<SrcList>]** and **[excludesrc=<SrcList>]** parameters are exclusive

If several sources must be defined in the **<SrcList>** argument, they must be separated by the "," character.

If at least one source defined in the <SrcList> argument contains a blank space, the complete <srcList> must be enclosed by double quotes.

Events that are out of date regarding the period parameter are discarded.
Checking conditions apply to this final set.

All condition combinations are allowed. Each condition is tested against the events set issued from the specified log files and the out-of-date condition. The final status is the most severe status for each condition result.

Only threshold conditions specified as parameters are taken into account. Non-specified conditions are ignored.

Notes

- The <period> parameter must be the first parameter.
- The Application, Security, and System event logs previously defined using the parameters "applog=1", "seclog=1", and "syslog=1", are now defined using the parameter "strlog=<LogName>".

Output

OK state	OK: no new messages for the last <period> min
WARNING or CRITICAL state	`<nb_msg> new messages for the last <period> min!` The message gives the total number of events that are responsible for a status that has degraded. This message is also a link to an html file giving event details. The following information is provided: **Event type** Error, Warning, Information, Audit Success or Audit Failure **Last Time** Last time an event of 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 **Note:** Only the events that have exceeded any of the specified limits are listed here (and not all the new events, nor the entire log file).

Table C-1. check_ns_eventlog output

In the event of a status that has degraded, a new file is created for each *<period>* of time, or when something changes in the output. Otherwise, the file is overwritten.

Examples

Below are two examples of parameters for the **check_ns_eventlog** command used in service definition, and their corresponding output.

-
  ```
  60!strlog=Application!wErr=1!eErr=5
  ```

  ```
  OK: no new events for the last 60 min
  ```
  Checks the number of error messages in the Application Event Log for the last 60 min. Status is set to **critical** if there are at least **five error messages**, and to **warning** if there is at least **one error message**.

-
  ```
  60!strlog=”DNS Server”!wErr=1!eErr=5
  ```

  ```
  OK: no new events for the last 60 min
  ```
  Checks the number of error messages in the DNS Server Event Log for the last 60 min.

-
  ```
  30!strlog=Application!filtersrc=”Bull System Manager
  snmptrapd”!wInf=10!wWarn=1!eErr=1
  ```

  ```
  2 new events for the last 30 min!
  A html file is generated
  ```
  Checks in Application Event Log only events for the last 30 minutes logged by the **Bull System Manager snmptrad** software.

-
  ```
  30!strlog=Application!excludesrc=Perflib,snmptrapd!wInf=10!wWa
  rn=1!eErr=1
  ```

  ```
  50 new events for the last 30 min!
  A html file is generated
  ```
  Checks all events logged for the last 30 minutes in the Application Event Log, except the events logged by **snmptrad** and **Perflib** software.

C.2 check_ns_disk (Windows)

Usage

check_ns_disk PERCENT | SIZE <path> <wThresh> <cThresh>

PERCENT | SIZE	unit for limits, percentage or size in Mbytes.
<path>	full path to local disk to monitor.
<wThresh>	value of used space resulting in a WARNING message.
<cThresh>	value of used space resulting in a CRITICAL message.

All arguments are required.

Output

OK state	`Disk <disk name> (total: <total size>Mb) (used: <used size>Mb, <used percent>%) (free: <free size>Mb)`
WARNING or CRITICAL state	`Problem on disk <disk name>: (total: <total size>Mb) (used: <used size>Mb, <used percent>%) (free: <free size>Mb)`

Table C-2. check_ns_disk (Windows) output

Example

```
check_ns_disk!PERCENT!C:!80!90
Disk C: (total: 2996Mb) (used: 2062Mb, 68%) (free: 934Mb)
```

This command checks the used space for disk C: .
If the used space is more than or equal to 80% to the total disk space, the status is set to **warning**.
If used space is more than or equal to 90% of the total disk space, the status is set to **critical**.

C.3 check_ns_load (Windows)

Usage

check_ns_load <interval1> <wload1> <cload1> <interval2> <wload2> <cload2>

<interval1>	First time interval, in minutes, used to measure the cpu load average. It must be a number between 0 and 15 minutes.
<wload1>	CPU load limit that results in a WARNING message for the first time interval. This must be a number between 0 and 100.
<cload1>	CPU load limit that results in a CRITICAL message for the first time interval. This must be a number between 0 and 100.
<interval2>	Second time interval, in minutes, used to measure the CPU load average. It must be a number between 0 and 15 minutes.
<wload2>	CPU load limit that results in a WARNING message for the second time interval. This must be a number between 0 and 100.
<cload2>	CPU load that results in a CRITICAL message for the second time interval. It must be a number between 0 and 100.

All the arguments are required.

This command checks the CPU average load during the two time intervals. It is possible to set a **warning** and a **critical** limit for each time interval. Returned status is the most severe status. The agent collects the total CPU load and stores it in a table every second. It also stores the CPU process with the highest consumption. When it is queried by the command, it computes the average load for the two requested periods, and returns the process with the highest consumption, if any.

Note The CPU process with the highest consumption at the time the request was issued does not necessarily match the process with the highest consumption during the time interval when the average CPU load was computed.

Output

OK state	CPU Load OK (<interval1>mn:< load1>%) (<interval2>mn: <load2%>)
WARNING or CRITICAL state	If the load of the process with the highest consumption, at the time the check is done, is more than zero: CPU Load HIGH (<interval1>mn:< load1>%) (<interval2>mn: <load2%>) - Process <pname> using <pload>% If it is zero: CPU Load HIGH (<interval1>mn:< load11>%) (<interval2>mn: <load2%>)

Table C--3. check_ns_load (Windows) output

Example

```
check_ns_load!1!80!90!10!60!80
```

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

Status is set to **warning** if load is more than 80% over the last minute, or more than 60% over the last ten minutes.
Status is set to **critical** if load is more than 90% over the last minute, or more than 80% over the last ten minutes.

C.4 check_ns_mem (Windows)

Usage

check_ns_mem PERCENT | SIZE <wThresh> <cThresh>

<table>
<tr><td>PERCENT | SIZE</td><td>unit for the limits, percentage or size in Mbytes.</td></tr>
<tr><td>&lt;wThresh&gt;</td><td>value of used memory that result in a WARNING message.</td></tr>
<tr><td>&lt;cThresh&gt;</td><td>value of used memory that result in a CRITICAL message.</td></tr>
</table>

All the arguments are required.

The memory measured is the total memory used by the system (physical memory + virtual memory). It is equivalent to the **Commit Charge** displayed in the Window Task Manager.

Output

OK state	Memory Usage OK (total: <total_mb>Mb) (used: <used_mb>Mb, <used pct>%) (free: <free mb>Mb) (physical: <phys_mb>Mb)
WARNING or CRITICAL state	Memory Usage HIGH (total: <total mb>Mb) (used: <used mb>Mb, <used_pct>%) (free: <free_mb>Mb) (physical: <phys_mb>Mb)

Table C–4. check_ns_mem (Windows) output

The output also contains the amount of the physical memory for the system.

Example

```
check_ns_mem!PERCENT!70!90
```

```
Memory Usage OK (total: 302Mb) (used: 208Mb, 68%) (free: 94Mb)
(physical: 127Mb)
```

Status is set to **warning** if the memory used is more than or equal to 70% of the total memory.
Status is set to **critical** if the memory used is more than or equal to 90% of the total memory.
The total memory for this host is 302 Mb, while the physical memory is 127 Mb.

C.5 check_ns_service (Windows)

Usage

check_ns_service showall | showfail <ServiceName1> [ServiceName2]

showall | showfail	specifies if all services, or only the services that are not running will be shown in the output.
<ServiceNameN>	name of the services to monitor (key name or display name are both accepted).

At least one service to be monitored must be specified. Up to eight services can be specified. If more than one service is specified, status returned is the most severe service status

Service names containing a blank space must be enclosed by double quotes.

Services can be given with either their display name or their key name. The display name is the name that appears in the Service Management Window, and depends on the OS language. For instance: "`Fax Service`", or "`Service de télécopie`"

The key name of a service can be found in the registry, under the key:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
For instance: `Fax`

Output

OK state	If showall is set: OK: `'<ServiceName1>' '<ServiceName2>' 0` If showfail is set: All OK

WARNING state	If showall is set:
	`<state1>:'<ServiceName1>' <state2>:'<ServiceName2>'`
	where `<stateN>` is one of the following state:
	`OK:` the service is started
	`Paused:` the service is suspended
	If showfail is set:
	`<state1>:'<ServiceName1>' <state2>:'<ServiceName2>' 0`
	where <stateN> is Paused (OK services are not listed).

CRITICAL state	If showall is set (depending on the problem):
	`<state1>:'<ServiceName1>' <state2>:'<ServiceName2>'`
	where `<stateN>` is one of the following state:
	`OK` the service is started
	`NotActive:` the service is stopped
	`NotExist:` the service does not exist
	`Timeout:` the service did not respond to the request
	`CheckError` something went wrong in the checking mechanism
	If showfail is set:
	`<state1>:'<ServiceName1>' <state2>:'<ServiceName2>' 0`
	where `<stateN>` is one of the following state: NotActive, NotExist, Timeout, CheckError (OK services are not listed)

Table C–5. check_ns_service (Windows) output

Example

```
check_ns_service!showall!”Client DHCP”!”Client DNS”!Telnet
```

```
OK:’Client DHCP’ OK:’Client DNS’ NotActive:’Telnet’
```

This command checks that the Client DHCP, Client DNS and Telnet services are running. Final status is critical because the Telnet service is not active on the machine. With the **showall** option, all the services are listed in the output, even the services that are running.

C.6 check_windisks (Windows)

Usage

check_windisk -w <warning_limit> -c <critical_limit> [-i <drive to include>] [-e <drive_to exclude>]

-w <warning_limit>	Amount of space used that results in a WARNING message.
-c <critical_limit>	Amount of space used that results in a CRITICAL message.
-i <drive to include>	DRIVE letter to include in the check.
-e <drive_to exclude>	DRIVE letter to exclude from the check

Output

OK state	DISKS OK: All disks (drives list) below the <warning limit> utilized
WARNING or CRITICAL state	DISKS <STATE>: (drives list) above the <state limit> utilized

Table C–6. check_windisks (Windows) output

Examples

- `check_windisk!-w 80!-c 90`
  This command checks the space used for all the disks.

If the space used is more than or equal to 80%, the status is set to **warning** as in the output below:

```
DISKS WARNING: (C:, D:, E:, F:, G:, I:) more than 80% utilized
```

If the space used is more than or equal to 90%, the status is set to **critical** as in the output below:

```
DISKS CRITICAL: (C:, D:, E:, F:, G:, I:) more than 90% utilized
```

- `check_windisk!-w 80!-c 90!-e G`

  This command checks the space used for all the disks, except the `G` drive.

  ```
  DISKS OK: all disks (C:, D:, E:, F:, I:) less than 80% utilized
  ```

C.7 check_procs (Linux, AIX)

Usage

check_procs -w <w_range> -c <c_range> [-s <states>] [-p <ppid>] [-u <user>] [-a <args>] [-C <command>]

<w_ range> Generates **warning** status if process count is outside this range.
<c_ range> Generates **critical** status if process count is outside this range.
Ranges are specified as follows: 'min:max' or 'min:' or ':max' (or 'max'). A warning or critical status will be generated if the count is inside the specified range ('max:min'), lower than min ('min:'), or more than max (':max' or 'max').
<states> Only scans the processes for which the status (resulting from by the **ps** command) corresponds to a specified status.
<ppid> Only scans children for which the parent process ID is this **ppid**.
<user> Only scans processes with this user name or ID.
<args> Only scans processes with a full command (with arguments) beginning with the specified string.
<command> Only scans processes with a command equal to the one specified.

This command checks the number of processes currently running and sets status to **WARNING** or **CRITICAL** if the process count is outside the specified threshold ranges. The process count can be filtered by process owner, parent process PID, current status (for example 'Z'), or it may be the total number of processes running.

Output

OK, WARNING or CRITICAL state	`<status> - <nb_procs> processes running`
	`<filter_conditions>`
	`<status>` service state (OK, WARNING or CRITICAL)
	`<nb_procs>` number of running processes matching the filter conditions
	`<filter_conditions>` applied filters conditions.

Table C–7. check_procs (Linux) output

Example

With the assumptino that the `/bin/ps -axo 'stat uid ppid comm args'` command returns the following lines:

```
STAT   UID  PPID COMMAND      COMMAND
S       0    0 init        init
SW      0    1 keventd      [keventd]
```

```
SWN    0    0 ksoftirqd_CPU0  [ksoftirqd_CPU0]
SWN    0    0 ksoftirqd_CPU1  [ksoftirqd_CPU1]
SW     0    0 kswapd      [kswapd]
SW     0    0 kreclaimd    [kreclaimd]
SW     0    0 bdflush     [bdflush]
SW     0    0 kupdated     [kupdated]
SW<    0    1 mdrecoveryd   [mdrecoveryd]
SW     0    1 kjournald    [kjournald]
SW     0    1 khubd      [khubd]
SW     0    1 kjournald    [kjournald]
SW     0    1 kjournald    [kjournald]
SW     0    1 kjournald    [kjournald]
SW     0    1 kjournald    [kjournald]
S     0   1 dhcpcd      /sbin/dhcpcd -n -H -R eth0

S     0   1 syslogd     syslogd -m 0
S     0   1 klogd      klogd -2
S     32   1 portmap     portmap
S     29   1 rpc.statd    rpc.statd
S     0   1 sshd       /usr/sbin/sshd
S     4   1 lpd       lpd Waiting
S     0   1 sendmail     sendmail: accepting connections
S     0   1 gpm       gpm -t ps/2 -m /dev/mouse
```

Examples using the check_procs command and the corresponding output include:

- `check_procs -w 100 -c 150`

  `OK - 24 processes running`

  This command checks the number of processes running on the local host.
  Status is set to warning if the number of processes is more than 100.
  Status is set to critical if the number of processes is more than 150.

- `check_procs -w 1: -C lpd`

  `OK - 1 processes running with command name lpd`

  This command checks that there is at least one lpd process running on the local host.
  Status is set to warning if the lpd process is not running. '1:' means that the result is OK if the number of processes is in the range from 1 (included) to the maximum integer value.

- `check_procs -w 3:1 -c 1: -C kjournald`

  `OK - 5 processes running with command name kjournald`

  This command checks the number of kjournald processes.
  Status is set to warning if this number is 1, 2 or 3, to critical if it is 0, and to OK otherwise.

- `check_procs -w:10 -s W`

  `WARNING - 14 processes running with STATE = W`

  This command checks the number of processes that have a W state (this includes SW and SWN).
  Status is set to warning if this number is more than 10.

- `check_procs -w:2 -s 'N<'`

  `WARNING - 3 processes running with STATE = N<`

  This command checks the number of processes that have a N or < state (this includes SWN and SW<).
  Status is set to warning if this number is more than 2.

- `check_procs -w 1: -a "sendmail: accepting"`

  ```
  OK - 1 processes running with args sendmail: accepting
  ```
  This command checks that there is at least one process with the full command starting with **sendmail: accepting** running on the local host.

- `check_procs -w 1: -a "accepting connections"`

  ```
  WARNING - 0 processes running with args accepting connections
  ```
  No process with a full command starting with **accepting connections** was found. Although the **sendmail: accepting connections** command matches the **-a** string, it does not match at position 0 and is not counted as a matching process.

C.8 check_log2.pl (Linux, AIX)

Usage

check_log2.pl -l <log_file> -s <seek_file> -p <pattern> [-n <negpattern>]

<log_file>	Text file to scan for patterns.
<seek_file>	Temporary file used to store the seek byte position of the last scan. The name must be composed of alphanumeric characters (/ not allowed). If the file size is smaller than the seek position (the file has been truncated or rotated since the last check), the scan is started from the beginning.
<pattern>	Pattern to be searched. It can be any Regular Expression pattern that PERL's syntax accepts.
<negpattern>	Negative pattern. Lines containing this pattern are discarded from the search.

This command scans arbitrary text files for regular expression matches.

This script runs with the root setuid bit in order to scan log files that are accessible by the root user. This is why the seek file location is forced in a safe directory.

Notes

- The **notify_recovery** value for the service should be set to **0**, so that Bull System Manager does not notify recoveries for the check. Since pattern matches in the log file will only be reported once and not the next time, there will still be unmeaningful recoveries.
- The **notificationPeriod** must be **different from none** so that someone is alerted that the pattern was found once and eventually not found again since the last scan.
- A different **<seek_file>** must be supplied for each service that will use this command script - even if the different services check the same <log_file> for pattern matches. This is necessary for the way the script operates.

Output

OK	a file is successfully scanned and no pattern matches are found. `OK - No matches found`
WARNING	one or more patterns are found along with the pattern count and the line of the last pattern matched.
CRITICAL	an error occurred, such as 'file not found'.

Table C–8. check_log2.pl (Linux) output

WARNING or CRITICAL status output:

`<nb-matching-line> <last-matching-line-in-file>`

`<nb-matching-line>` Number of lines matching the pattern (and not matching the optional negative pattern)

`<last-matching-line-in-file>` the last matching line found in the log file.

Examples

Assuming that the **/var/log/messages** file contains the following lines:

```
Nov 26 15:30:44 horus pam_rhosts_auth[4790]: allowed to
Administrator@osiris as integ
Nov 26 15:30:44 horus rsh(pam_unix)[4790]: session opened for user integ
by (uid=0)
Nov 26 15:30:49 horus login(pam_unix)[4786]: authentication failure;
logname= uid=0 euid=0 tty=pts/1 ruser= rhost=isis user=root
Nov 26 15:30:51 horus login[4786]: FAILED LOGIN 1 FROM isis FOR root,
Authentication failure
Nov 26 15:31:11 horus login(pam_unix)[4786]: check pass; user unknown
Nov 26 15:31:11 horus login(pam_unix)[4786]: authentication failure;
logname= uid=0 euid=0 tty=pts/1 ruser= rhost=isis
Nov 26 15:31:13 horus login[4786]: FAILED LOGIN 2 FROM isis FOR admin,
Authentication failure
Nov 26 15:31:24 horus rsh(pam_unix)[4790]: session closed for user integ
Nov 26 15:31:29 horus login(pam_unix)[4786]: check pass; user unknown
Nov 26 15:31:32 horus login[4786]: FAILED LOGIN 3 FROM isis FOR admin,
Authentication failure
Nov 26 15:33:14 horus login(pam_unix)[4853]: session opened for user
netsaint by (uid=0)
Nov 26 15:33:14 horus -- netsaint[4853]: LOGIN ON pts/1 BY netsaint FROM
isis
Nov 26 15:33:22 horus login(pam_unix)[4853]: session closed for user
netsaint
Nov 26 15:33:37 horus ftpd[4916]: FTP session closed
Nov 26 15:34:11 horus su(pam_unix)[4931]: session opened for user root by
root(uid=503)
```

Examples using the **check_log2.pl** command and corresponding output include.

- `check_log2.pl -l /var/log/messages -s t2.seek - p 'FAILED'`

  ```
  (3): Nov 26 15:31:32 horus login[4786]: FAILED LOGIN 3 FROM
  isis FOR admin, Authentication failure
  ```

  This command searches for lines containing the string **FAILED** in the **/var/log/messages** file. Three lines were found and the last one is displayed.

- `check_log2.pl -l /var/log/messages -s t3.seek - p 'session opened'`

  ```
  (3): Nov 26 15:34:11 horus su(pam_unix)[4931]: session opened
  for user root by root(uid=503)
  ```
  This command searches for lines containing the string **`session opened`** in the /var/log/messages file. Three lines were found and the last one is displayed.

- `check_log2.pl -l /var/log/messages -s t4.seek -p 'LOGIN.*isis' -n netsaint`

  ```
  (3): Nov 26 15:31:32 horus login[4786]: FAILED LOGIN 3 FROM
  isis FOR admin, Authentication failure
  ```
  This command searches for all LOGINs from the host `isis`, except ones with `netsaint` user, in the /var/log/messages file. Three lines were found and the last one is displayed.

C.9 check_disk (Linux, AIX)

Usage

check_disk -w <wlimit>[%] -c <climit>[%] [-p <path>]

<wlimit>	minimum value of free space that result in a WARNING message the value in expressed in Kbytes, unless '%' is specified.
<climit>	minimum value of free space that result in a CRITICAL message the value is expressed in Kbytes, unless '%' is specified
<path>	filesystem to be checked (checks all mounted filesystems if unspecified). the name can be given either as the mounting point (ex: /usr) or as the device name (ex: /dev/sda2). If a directory name that does not match a filesystem is given, the command tries to determine the corresponding filesystem. If successful, it checks that filesystem.

Note The warning limit must be above the critical limit.

This command checks the free space left on FileSystems. It uses the **df** command. Limits can be given either in percentage, or in Kbytes.

Output

OK, WARNING or CRITICAL state	DISK <status> - [<free kb> kB (<free percent>%) free on <device name>] <status> service state (OK, WARNING or CRITICAL) <free Kb> free space in Kbytes left on filesystem <free percent> percentage of free space left on filesystem <device name> device name of the filesystem. This information is repeated for each filesystem, if all the mounted filesystems are monitored.

Table C-9. check_disk (Linux) command output

Example

```
check_disk -w 20% -c 10% -p /usr
```

```
DISK OK - [7068772 kB (75%) free on /dev/sda2]
```

This command checks the free space percentage for the FileSystem /usr (/dev/sda2) on the local host.
Status is set to **warning** if the free space left on FileSystem /usr is **less than 20%**.
Status is set to **critical** if the free space left on FileSystem /usr is **less than 10%**.

C.10 check_disks.pl (Linux, AIX)

Usage

```
check_disks.pl -w <warn%> -c <crit%> [-i <include-fs>]* [-e <exclude-fs>]*
```

<warn%> Percentage of space used that result in a WARNING message.
<crit%> Percentage of space used that result in a CRITICAL message.
<include-fs> filesystem to be checked (checks all mounted filesystems if unspecified). This option can be repeated to specify more than one filesystem to be checked.
The name must be given as the mount point (ex: /usr).
<excluded-fs> filesystem to be excluded from the check. This option can be repeated for specifying more than one filesystem to exclude
The name must be given as the mount point (ex: /usr).

This command checks the space used for FileSystems, and allows the exclusion of some FileSystems from the check. It uses the **df** command. Limits are given in percentages.

Output

OK state	DISKS OK: all disks less than 70% utilized
WARNING or CRITICAL state	DISK <status>: (<filesystems>) more than <limit>% utilized. <status> service state (WARNING or CRITICAL). <filesystems> list of filesystems whose used space percentage is over the limit. <limit> limit value defined for the status.

Table C-10. check_disks.pl (Linux) output

If there are FileSystems with **WARNING** and **CRITICAL** status, this information is repeated to indicate all the FileSystems with a non-OK status.

Unlike **check_disk**, this command does not give full information (capacity and space used) for the FileSystems, but reports synthetically the FileSystems with problems. It can be used for a global vision of FileSystems status, while **check_disk** can be used for specific FileSystems details.

Example

```
check_disks.pl -w 60 -c 75 -e /mnt/cdrom
```

```
DISK CRITICAL: ( / ) more than 75% utilized - DISKS WARNING: ( /usr /var
) more than 60% utilized
```

This command checks the used space for the **all** the mounted FileSystems, except **/mnt/cdrom**.
If the used space is **more than or equal to 60%**, status is set to **warning.**
If the used space is **more than or equal to 75%**, status is set to **critical**.
Here, status is **CRITICAL** because **/** has more than 75% space used. **/usr** and **/var** are also set to **warning** because they have more than 60% space used.

C.11 check_cpuload (Linux, AIX)

Usage

check_cpuload -w WLOAD1,WLOAD5,WLOAD15 -c CLOAD1,CLOAD5,CLOAD15

<wload1> Utilization average limit results in a WARNING message during the last minute, must be a number between 0 and 100.

<wload5> Utilization average limit results in a WARNING message during the last 5 minutes, must be a number between 0 and 100.

<wload15> Utilization average limit results in a WARNING message during the last 15 minutes, must be a number between 0 and 100.

<cload1> Utilization average limit results in a CRITICAL message during the last minute, must be a number between 0 and 100.

<cload5> Utilization average limit results in a CRITICAL message during the last 5 minutes, must be a number between 0 and 100.

<cload15> Utilization average limit results in a CRITICAL message during the last 15 minutes, must be a number between 0 and 100.

All the arguments are required.

This command checks average CPU utilization during three predefined time intervals. It is possible to set a **warning** and a **critical** limit for each time interval.

CPU utilization is defined as: (load average / number of processors) * 100

Load average is given by **uptime** and **w**.

The status returned is the most severe status.

Output

OK state	CPU Utilization: <load1> (1mn), <load5> (5mn), <load15> (15mn)
WARNING or CRITICAL state	CPU Utilization: <load1> (1mn), <load5> (5mn), <load15> (15mn) <status>
<load1> <load5> <load15> percentage of average CPU load for respectively the last minute, the last 5 minutes and the last 15 minutes. <status> either WARNING or CRITICAL.	

Table C–11. check_cpuload (Linux) command output

Example

```
check_cpuload -w 80,70,60 -c 90,80,70
```

This command checks the CPU load for the local host.

Status is set to **warning** if load is more than 80% during the last minute, or more than 70% during the last 5 minutes or more than 60% during the last 15 minutes, as in the following result:

```
CPU Utilization: 87% (1mn), 52% (5mn), 29% (15mn) WARNING
```

Status is set to **critical** if load is more than 90% during the last minute, or more than 80% during the last 5 minutes or more than 70% during the last 15 minutes, as in the following result:

```
CPU Utilization: 100% (1mn), 64% (5mn), 37% (15mn) CRITICAL
```

Status is set to **OK** if no limit is raised, as in the following result

```
CPU Utilization: 23% (1mn), 29% (5mn), 24% (15mn)
```

C.12 check_lpar_load (AIX)

Usage

check_lpar_load –w <wlimit> -c <climit>

<wlimit>	percent of load CPU that result in a WARNING message
<climit>	percent of load CPU that result in a CRITICAL message.

All the arguments are required.

This command gets the CPU load of an AIX system or partition. The warning limit must be lower than the critical limit.

Output

The output depends on the type of partition: shared capped, shared uncapped, dedicated.

WARNING, CRITICAL or OK state	Shared capped	<status> - Phys CPU load is load_cpu% entc=entitled_capacity% (idle:idle_cpu% wait:wait_cpu%) - type=Shared Capped partition
	Shared uncapped	<status> - Phys CPU load is load_cpu% of max_cpu CPU (idle:idle_cpu% wait:wait_cpu%) - max_vp=maximum_virtual_cpu type=Shared Uncapped partition
	dedicated	<status> - CPU load is load_cpu (idle:idle_cpu% wait:wait_cpu%) - type=Dedicated partition

Table C–12. check_lpar_load (AIX) output

Example

```
check_lpar_load -w 80 -c 90
```

```
OK - Phys CPU load is 0.00 0% of 1 CPU (idle:99.2% wait:0%) -
max_vp=2 type=Shared Uncapped partition
```

C.13 check_mem.pl (AIX)

Usage

check_mem.pl –w <wlimit> -c <climit>

<wlimit>	percent of used memory that result in a WARNING message
<climit>	percent of used memory that result in a CRITICAL message.

All the arguments are required.

This command measures memory used, so the warning limit must be lower than the critical limit. The measured memory is the total memory used by the system (physical memory + swap).

Output

OK, WARNING or CRITICAL state	Memory: WARNING - Total: <total_mb> (pgsize: 4K) (used: <used_mb>, <used_pct>%) (free: <free_mb>)

Table C–13. check_mem.pl (Linux) output

Example

```
check_mem.pl -w 95 -c 99
```

```
Memory: WARNING - Total: 131072 (pgsize: 4K)
(used: 126284, 96.3%) (free: 4788)
```

C.14 check_memory (Linux)

Usage

check_memory <wlimit> <climit>

<wlimit>	percent of used memory that result in a WARNING message
<climit>	percent of used memory that result in a CRITICAL message.

All the arguments are required.

This command measures used memory, so the warning limit must be lower than the critical limit. The measured memory is the total memory used by the system (physical memory + swap).

Output

OK, WARNING or CRITICAL state	Status: <status> - (total: <total_mb>Mb) (used: <used_mb>Mb, <used_pct>%) (free: <free_mb>Mb) (physical: <phys_mb>Mb)	
	<status>	service status (OK, WARNING or CRITICAL)
	<total_mb>	total memory size (physical memory + swap)
	<used_mb>	total memory used
	<used_pct>	percentage of total memory used by the system
	<free_mb>	memory (physical or swap) left free
	<phys_mb>	size of the physical memory.
All values are expressed in Mbytes.		

Table C–14. check_memory (Linux) output

Example

```
check_memory 70 90
```

```
Status: OK - (total: 2996Mb) (used: 863Mb, 29%) (free: 2132Mb)
(physical: 1004Mb)
```

This command checks the free memory percentage for the local host.

Status is set to **warning** if the memory used is **more than 70%**.
Status is set to **critical** if the memory used is **more than 90%**.

The total memory for this host is 2996 MB, while the physical memory is 1004 MB.

C.15 check_swap (Linux, AIX)

Usage

check_swap -w <w_usedpercent>% -c <c_usedpercent>%

<w_usedpercent>	percent of used swap that result in a WARNING message.
<c_usedpercent>	percent of used swap that result in a CRITICAL message.

Or:

check_swap -w <w_freebytes> -c <c_freebytes>

<w_ freebytes>	lowest free swap space that result in a WARNING message.
<c_ freebytes>	lowest free swap space that result in a CRITICAL message.

All the arguments are required.

This command can measure either the percentage of swap space used, or the value of free swap space in bytes. This depends on the presence or not of the %'sign.

If % is specified, the measure is the percentage of space **used**, so the critical limit must be more than the warning limit.
If % is not specified, the measure is the **free** space left in bytes, so the warning limit must be more than the critical limit.

Output

OK, WARNING or CRITICAL state	<status> - Swap used: <used-percent>% (<used-mbytes> Mb out of <swap-mbytes>)	
	<status>	service state ("Swap ok", WARNING or CRITICAL)
	<used-percent>	percentage of used swap space
	<used-mbytes>	used swap space in Mbytes
	<swap-mbytes>	size of the swap in Mbytes.

Table C–15. check_swap (Linux)output

Example

```
check_swap -w 50% -c 80%
```

```
Swap ok - Swap used: 0% (0 Mb out of 1992)
```

This command checks the swap percentage used for the local host.
Status is set to **warning** if the used swap is **more than** 50%.
Status is set to **critical** if the used swap is **more than** 80%.
The size of the swap is 1992 Mbytes.

C.16 check_users (Linux, AIX)

Usage

check_users -w <wlimit> -c <climit>

<wlimit>	number of logged in users that result in a WARNING message.
<climit>	number of logged in users that result in a CRITICAL message.

All the arguments are required.

This command checks the number of users currently logged on to the local system.

Output

OK, WARNING or CRITICAL state	`USERS <status> - <nb-users> users currently logged in` <status> service state (OK, WARNING or CRITICAL) <nb-users> number of users currently logged in.

Table C-16. check_users (Linux) output

Example

```
check_users -w 10 -c 20
```

```
USERS WARNING - 18 users currently logged in
```

Status is set to **warning** if there are **10 or more users** logged in.
Status is set to **critical** if there are **20 or more users** logged in.

C.17 check_httpURL (Windows, Linux and AIX)

Usage

check_httpURL <port>!<url>!'<response_substring>'!'<content_response>'

<port>	port on which URL is to be tested.
<url>	URL to be tested. Do not forget the character '/'.
<response_substring>	search this substring in the first line of the HTTP response.
<content_substring>	search this substring in the content of the returned page.

response_substring and **contents_substring** must be surrounded by single quotes.

To know which substring to check in the HTTP response (**response_substring**), you may launch the following command if Bull System Manager Server is installed on a Linux operating system:

```
<Bull System Manager server install dir>/engine/nagios/libexec/check_httpURL
 -H <hostname> -p <port> -u <url>
```

The output of this command is the HTTP response, in which you can choose a substring to be checked. If the output indicates an error, correct the port or the **URL** parameters.

Status is set to **warning** for HTTP errors: 400, 401, 402, 403 or 404 such as unauthorized access.

Status is set to **critical** if:

- The substring <response_substring> is not found in the first line of the HTTP response. The error message is: "Invalid HTTP response received from host on port xx"
- The substring <contents_substring> is not found in the returned page. The error message is **string not found**.
- The response time exceeds 10 seconds
- There is an HTTP error 500, 501, 502 or 503
- The connection with the server is impossible.

Output:

OK state	HTTP ok: HTTP/1.0 200 Document follows - 0 second response time
WARNING state	HTTP WARNING: HTTP/1.0 401 Unauthorized
CRITICAL state	Invalid HTTP response received from host on port HTTP CRITICAL: string not found Connection refused by host Socket timeout after 10 seconds

Table C–17. check_httpURL (Windows and Linux) output

C.18 check_mrtg (Windows, AIX and Linux)

Usage

check_mrtg -F <reporting_logfile> -a AVG -v 1 -e 10 -w <warning_threshold> -c <critical_threshold> -l <status_info_label> -u <status_info_unit>

<reporting_logfile>	Each reporting indicator, associated to a host, has its values logged in a log file named "<host_name>+<indicator_name>.log". This log file is located in <install_dir>/core/share/reporting/var.
<warning_threshold>	Minimum value of free space that result in a WARNING message. The default value is 80.
<critical_threshold>	Minimum value of free space that result in a CRITICAL message. The default value is 90.
<status_info_label>	The status information of the monitoring service looks like "<status_info_label>: <last value> <status_info_unit>". The default value for status_info_label is "Load". This parameter is only displayed in the status information in the console.
<status_info_unit>	The status information of the monitoring service looks like "<status_info_label>: <last value> <status_info_unit>". The default value for status_info_unit is "%".This parameter is only displayed in the status information in the console.

This command gets, then checks the last value for a reporting indicator, from a reporting log file located in **<install_dir>/core/share/reporting/var**.

Notes

- The reporting log file contains the name of the host associated with the reporting indicator. Therefore, the monitoring service cloned from **reporting.perf_indic** must have a **hostlist** containing only one host. By default, **hostlist=none** for the **Perf_indic** service and the **reporting** category.
- The warning limit must be greater than the critical limit.

Example

```
check_mrtg -F ' c:/PROGRA~1/Bull/BULLSY~1/core/share/reporting/var/
frcls2703+2703_memory.log' -a AVG -v 1 -e 10 -w 10 -c 90 -l Load -u %
```

C.19 check_PowerStatus (IPMI servers)

Usage

check_PowerStatus [[!user]!password]

<user>	The IPMI user name if it exists
<password>	The IPMI password associated to the user if this last one exists, or the IPMI authentification key.

This command gets, then checks the power status via the IPMIoverLAN protocol for the BMC of the server.

Example

```
check_PowerStatus!user!pass
```

C.20 check_IPMI_sensor (IPMI servers)

Usage

check_IPMI_sensor!<sensor_name>[!<-c lower_critical>][!<-w lower_non-critical>][!<-W upper_non-critical>][!<-C upper_critical>]

<sensor name>	The name of a numeric sensor listed in the SDR.
<lower_critical>	Lower critical threshold value that results in a CRITICAL state.
<lower_non-critical>	Lower non-critical threshold value that results in a WARNING state.
<upper_non-critical>	Upper non-critical threshold value that results in a WARNING state.
<upper_ critical>	Upper critical threshold value that results in a CRITICAL state.

sensor name must be surrounded by single or double quotes.

This command gets a numeric sensor value, then checks it with the threshold values defined in the SDR or to the thresholds values passed in arguments if any.

Note The unit (V, degrees C, rpm etc.) is automatically extracted from the sensor information.

Output

OK state	The current sensor value is in the NORMAL area (lower non-critical threshold < current value < upper non-critical threshold)
WARNING state	The current value is in the WARNING area (lower critical threshold < current value < lower non-critical threshold or upper non-critical threshold < current value < upper critical threshold)
CRITICAL state	The current value is in the CRITICAL area (current value < lower critical threshold or current value > upper critical threshold)
UNKNOWN state	The current value cannot be retrieved (sensor not found, unable to establish LAN session)

Table C–18. check_IPMI_sensor (IPMI servers) output

Example

```
check_IPMI_sensor!”Valve Aperture”
```

```
OK : 55.380 %
```

C.21 check_IPMI_sensor_avg (IPMI servers)

Usage

check_IPMI_sensor_avg!<sensor name list>[!<-c lower_critical>][!<-w lower_non-critical>][!<-W upper_non-critical>][!<-C upper_critical>]

<sensor name list>	A list of names of numeric sensors (listed in the SDR) separated with a comma.
<lower_critical>	Lower critical threshold value that results in a CRITICAL state.
<lower_non-critical>	Lower non-critical threshold value that results in a WARNING state.
<upper_non-critical>	Upper non-critical threshold value that results in a WARNING state.
<upper_ critical>	Upper critical threshold value that results in a CRITICAL state.

Each **sensor name** must be surrounded by single quotes.

This command gets the current value of a list of numeric sensors, then calculates the average value, and checks it with the contextual thresholds if any.

Note The unit (V, degrees C, rpm, etc.) must be the same for all the sensors, and is automatically extracted from the sensor information.

Output:

OK state	The average of the sensors values is in the NORMAL area (lower non-critical threshold < average value < upper non-critical threshold)
WARNING state	The average of the sensors values is in the WARNING area (lower critical threshold < average value < lower non-critical threshold or upper non-critical threshold < average value < upper critical threshold)
CRITICAL state	The average of the sensors values is in the WARNING area (average value < lower critical threshold or average value > upper critical threshold)
UNKNOWN state	The average value cannot be calculated (sensor not found, unable to establish LAN session, sensors types are differents …)

Table C–19. check_IPMI_sensor_avg (IPMI servers) output

Example

```
check_IPMI_sensor_avg!”TH_0 Temp.”,”TH_1 Temp.”,”TH_3 Temp.”
```

```
OK : 23.100 degrees C
```

C.22 check_pressure (IPMI servers)

Usage

check_pressure!<sensor name>[!<-c lower_critical>][!<-w lower_non-critical>][!<-W upper_non-critical>][!<-C upper_critical>]

<sensor name>	The name of a numeric sensor listed in the SDR.
<lower_critical>	Lower critical threshold value that result in a CRITICAL state.
<lower_non-critical>	Lower non-critical threshold value that result in a WARNING state.
<upper_non-critical>	Upper non-critical threshold value that result in a WARNING state.
<upper_ critical>	Upper critical threshold value that result in a CRITICAL state.

sensor name must be surrounded by single or double quotes.

This command, dedicated to pressure sensor, is similar to check_IPMI_sensor but, if the sensor unit is **kPa**, it multiplies the current value by 1000 and changes the unit to **Pa**.

Note The unit (kPa) is automatically extracted from the sensor information.

Output:

OK state	The current sensor value is in the NORMAL area (lower non-critical threshold < current value < upper non-critical threshold)
WARNING state	The current value is in the WARNING area (lower critical threshold < current value < lower non-critical threshold or upper non-critical threshold < current value < upper critical threshold)
CRITICAL state	The current value is in the CRITICAL area (current value < lower critical threshold or current value > upper critical threshold)
UNKNOWN state	The current value cannot be got (sensor not found, unable to establish LAN session ...)

Table C–20. check_pressure (IPMI servers) output

Example

```
check_pressure!”Air Pressure”
```

```
OK : 18 Pa
```

Appendix D. Administration Commands

Bull System Manager Server menus allow you, as administrator, to perform the most frequently used operations.

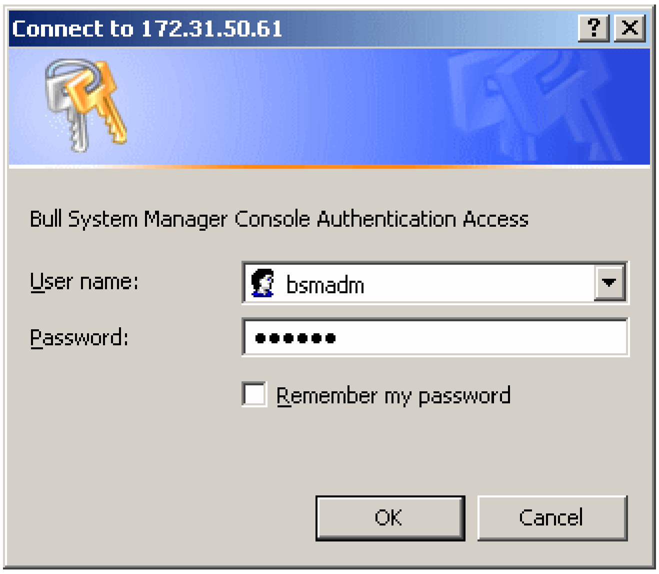
To display these menus, from the Bull System Manager Console:

- Click the icon representing the BSM Control GUI in the Administration zone (top right),

or

- Click the Control link on the Bull System Manager Home Page.

When the GUI is launched, an authentication dialog is displayed:



Connect to 172.31.50.61

Bull System Manager Console Authentication Access

User name: bsmadm

Password: ••••••

□ Remember my password

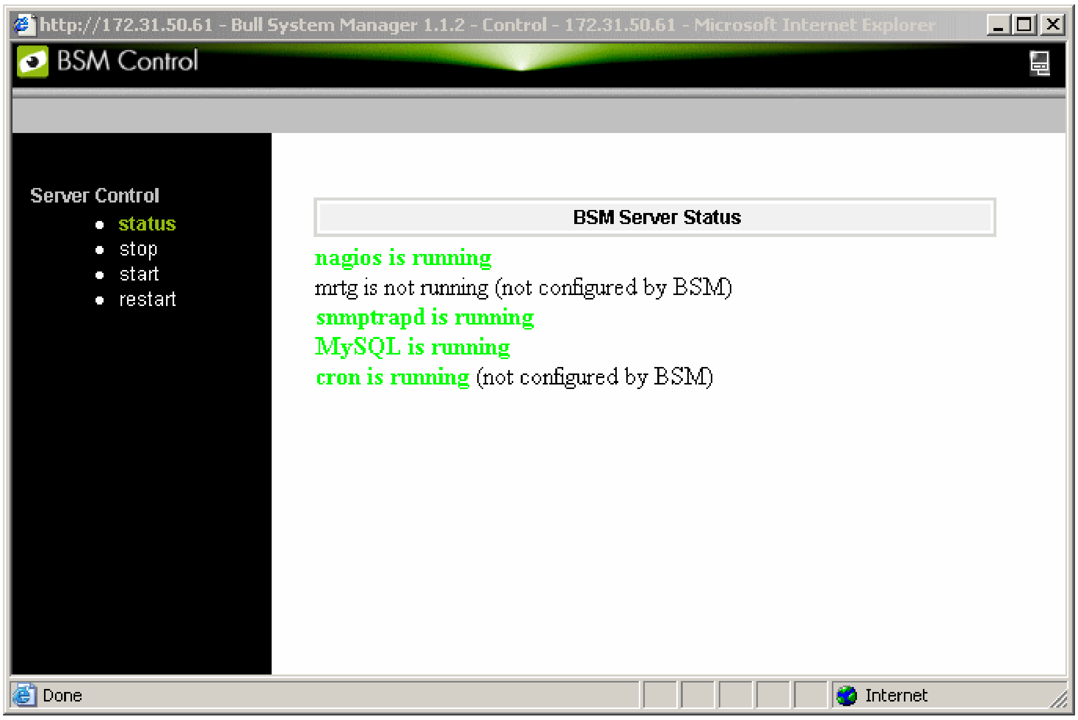
Figure D–1. Authenticating the Bull System Manager control user

- On Windows, Authenticated users are users declared in the Windows users database. The user name must be entered in the following format: **DOMAINNAME\Username**
- On Linux, enter **bsmadm** / **bsmadm**.

This user is associated with a Role: **Administrator** or **Operator**. The Administrator role has write access to the configuration; the Operator role has only read access. The execution of the BSM Control requires the Administrator role.

Note This user (and role) is created during the installation process. Refer to the *Bull System Manager Installation Guide* (86 A2 54FA) to learn how to configure the Bull System Manager Configuration tool authentication feature.

The Bull System Manager ServerControl GUI allows you to start, stop, or restart the BSM Server, according to your requirements. When the BSM Control GUI is launched, the current status of the server is displayed, as shown in the following figure:


http://172.31.50.61 - Bull System Manager 1.1.2 - Control - 172.31.50.61 - Microsoft Internet Explorer
BSM Control
Server Control
status
stop
start
restart
Done
Internet

BSM Server Status

nagios is running
mrtg is not running (not configured by BSM)
snmptrapd is running
MySQL is running
cron is running (not configured by BSM)

Figure D–2. BSM Server Status

Appendix E. SSH Configuration

The SSH configuration specific to the BSM Applications is in the **<BSM installation directory>/engine/etc/ssh/** directory.

E.1 SSH client configuration on Bull System Manager Server

The **<BSM installation directory>/engine/etc/ssh/config_bsm** file delivered by Bull System Manager, contains SSH configuration parameters. It can be used to perform non-prompt connection when executing SSH.

Parameters setting in config_bsm (Linux case):

```
PasswordAuthentication     no
NumberOfPasswordPrompts    0
StrictHostKeyChecking      no
UserKnownHostsFile
          /opt/BSMServer/engine/etc/ssh/known_hosts_bsm
```

E.2 Keys generation on Bull System Manager Server

Private key generation for the Bull System Manager Server is automatically performed during the post-installation of a Bull System Manager Server, to allow BSM servers to perform non-prompted connection on a remote machine, from the configuration GUI (as Web user) or from the **nagios** service (as nagios user). One key is generated and is copied in multiple files to respect the restricted permissions required for identity files.

The following table display the key files delivered by Bull System Manager and their characteristics:

Linux platform

File	Owner/Group	Right	Usage
id_dsa.bsm	bsmuser/bsmgroup	600	Private key used in Nagios plugin. Note: another filename can be used (can be specified during the configuration of the Vios in Bull System Manager).
id_dsa.www	apache*/bsmgroup	600	Private key used by the configuration GUI. Note: this name must not be changed
id_dsa.pub	bsmuser/bsmgroup	664	Corresponding public key.

* the name of the Apache user can differ among Linux distribution.

Windows platform

File	Owner	Right	Usage
id_dsa.bsm	SYSTEM	600	Private key used in Nagios plugin. Note: another filename can be used (it can be specified during the configuration of the Vios in Bull System Manager).
id_dsa.iis	administrator	600	Private key used by the configuration GUI when using IIS http server. Note: this name must not be changed.
id_dsa.apache	administrator	666	Private key used by the configuration GUI when using Apache http server. Note: this name must not be changed.
id_dsa.pub	bsmuser/bsmgroup	664	Corresponding public key.

The corresponding public key (id_dsa.pub) must be installed on the remote machine:

1. Copy the public key on the remote machine (use available protocole as ftp or scp)
2. Edit the file **<user home>/.ssh/authorized_keys2** to add the key.

E.3 Use other identity file

You can use your own identity file, if you install it in the **BSM SSH** configuration directory and execute the **set-ssh-key** script to generate the files used by **BSM** application.

1. Copy your key files (private and public key) into the BSM SSH Configuration directory.

2. Run the **set-ssh-key** file.

– On the Linux platform:

```
cd <BSM_install_directory>/core/bin
./set-ssh-key.sh –f <private_identity_file_name>
```

This script will generate the following files under the <BSM_install_directory>/engine/etc/ssh directory:

<private_identity_file_name>.www

<private_identity_file_name>.bsm

– On the Windows platform:

```
cd <BSM_install_directory>/core/bin
./set-ssh-key.bat  <private_identity_file_name>
```

This script will generate the following files under the **<BSM_install_directory>/engine/etc/ssh** directory:

<private_identity_file_name>.apache

<private_identity_file_name>.iis

<private_identity_file_name>.bsm

E.4 Test non-prompted connection

After installing the keys, the SSH connection can be tested:

- On Linux platforms, execute the **ssh** command with the –i and **–F** parameters to use the BSM SSH configuration:

```
cd <BSM_install_directory>/engine/etc/ssh
ssh <remote_machine> -l <remote_user> -i id_dsa –F config_bsm <remote_command>
```

- On Windows platform, run the **test-ssh.bat** command delivered in the <BSM_install_directory>/core/bin/directory:

```
cd <BSM_install_directory>/core/bin
test-ssh.bat <remote_machine> <remote_user> <id_file_name><remote_command>
```

Index

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

REFERENCE
86 A2 56FA 04