Bull System Manager

BSM 2.4 Server Add-ons

Installation and Administrator's Guide

REFERENCE
86 A2 59FA 10

Printed in France

Trademarks and Acknowledgements

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

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

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

Software

November 2013

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

Table of Contents

Preface

This guide explains how to configure and customize Bull System Manager Add-ons.

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

Intended Readers

This guide is intended for use by System Administrators.

Highlighting

The following highlighting conventions are used in this guide:

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

```
Commands entered by the user
```

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

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

Related Publications

This list is not exhaustive. Useful documentation is supplied on the Resource & Documentation CD(s) delivered with your system. You are strongly advised to refer carefully to this documentation before proceeding to configure, use, maintain, or update your system.

- *BSM Installation Guide*, 86 A2 54FA
  explains how to install the Bull System Manager solution for monitoring and managing Bull systems. This guide is intended for use by System Administrators.
- *BSM Administrator's Guide*, 86 A2 56FA
  explains how to customize Bull System Manager to monitor specific environments. This guide intended for use by System Administrators.
- *BSM User's Guide*, 86 A2 55FA
  explains how to monitor and manage Bull systems using Bull System Manager, and in particular via the Bull System Manager Console. This guide is intended for use by System Operators.
- *BSM Remote Hardware Management CLI Reference Manual,* 86 A2 58FA
  describes the Hardware Management CLI (Command Line Interface) for Bull systems.
- *BSM Server Add-ons - Installation Guide*, 86 A2 59FA
  Bull System Manager Server Add-ons provide extensions for Bull System Manager to monitor specific system devices or products. This guide is intended for use by System Administrators.
- *Release Notes,* 86 A2 57FA
  describe the contents, system requirements, installation instructions, and known issues (with workarounds, where applicable) for the current Bull System Manager release.

Chapter 1. Bull System Manager Overview

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

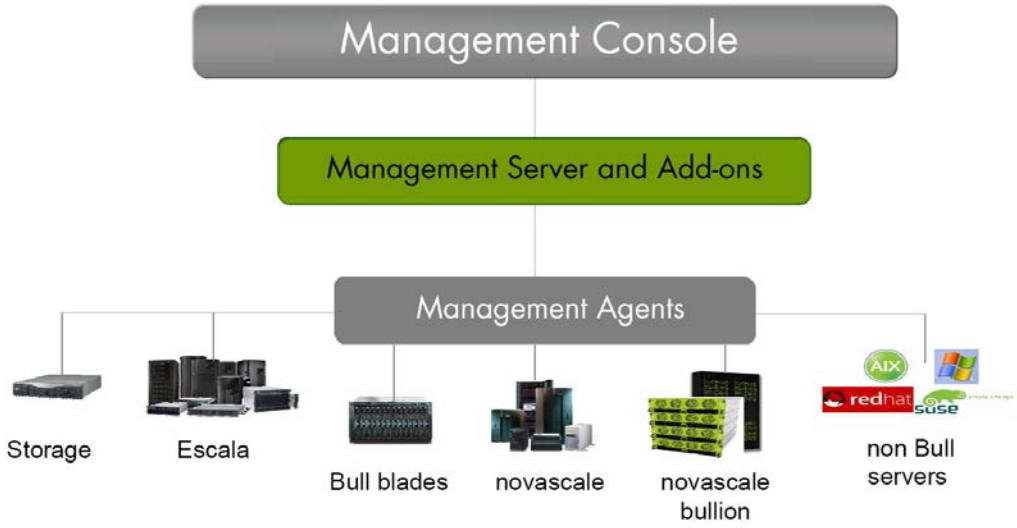
It provides a single point of control for the integrated management of Bull servers and external devices, allowing administrators to see alerts quickly and to take the appropriate actions, thereby enhancing system availability and performance.

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

1.1 Architecture

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

Management Console	installed on each end-user station (Windows or Linux)
Management Server and **Add-ons**	installed on the management server(s) (Windows or Linux)
Management Agents	**installed** on each managed hardware platform (Windows or Linux or AIX)



For large infrastructures, a distributed monitoring solution can be implemented allowing an overall view of managed system status via a Global Management Console. For more information, contact your Bull Customer Representative.

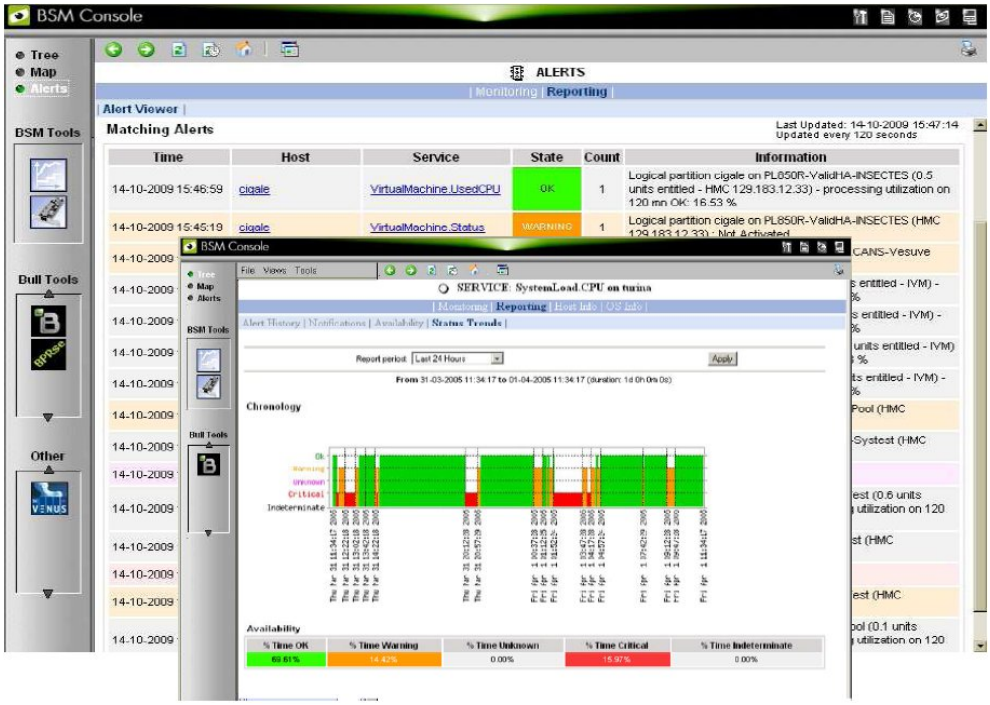
Bull System Manger is also delivered with a Hardware Management CLI package, providing an easy Command Line Interface (CLI) for local or remote hardware management and automation scripts.

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

1.1.1 Management Console

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

If a distributed monitoring solution is implemented, a Global Management Console allows you to graphically view, monitor and manage all the hosts configured for administration on a set of Management Servers.



The Management Console provides access to the **Configuration GUI**, used to configure the monitoring of hosts, and to the **Control GUI**, used to stop and start the Management Server.

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

1.1.2 Management Server

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

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

1.1.3 Management Agent

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

1.1.4 Hardware Management CLIs

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

- Powering on/off
- Obtaining power status details
- Monitoring hardware components
- Inventory purposes for hardware, partition and module details
- Hardware discovery and topological verification
- Configuration and Maintenance
  - Updating firmware
  - Managing CPU allocation
  - Creating and modifying partitions
  - Configuring platform modules
  - Allowing a Support Online connection to be made

1.2 Features

Bull System Manager offers the following features:

- Monitoring
- Reporting
- Alerting
- Remote Operations and Inventory

1.2.1 Monitoring

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

- Specific elements and services such as **Power status**, **CPU load, memory usage, disk usage, number of users, processes** and **service execution, http** and **ftp services** can be monitored. When an anomaly occurs or when normal status is recovered, **alerts** (in a log file) and **notifications** (by e-mail, by Bull auto-call and/or by **SNMP** trap) are generated.
- Status thresholds (**OK**, **WARNING**, **CRITICAL**, **UNKNOWN**) can be defined for each element monitored.
- Monitored hosts and services can be grouped into entities that reflect your environment so that you can easily identify an anomaly for these entities.
- Instantiated services can be grouped into specific functional domains so that you can display monitoring information for that domain only.

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

1.2.2 Reporting

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

1.2.3 Alerting

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

E-mail Notification

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

Bull Autocall Transmission

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

SNMP Trap Alerting

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

1.2.4 Remote Operations

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

1.2.5 Inventory

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

1.3 Bull System Manager Server Add-ons

Bull System Manager Server Add-ons include additional management packages to extend Bull System Manager Server.

A Bull System Manager Server Add-on provides functional links (monitoring, GUI call, reporting, etc.) between a Bull System Manager Server and a third-party management tool.

All the Server Add-ons are distributed on the *Bull System Manager Server* CD-ROM.

Note There is a difference between Server Add-ons and the third-party management tools. Even if the third-party management tool is dedicated to an OS and/or a platform type, its Bull System Manager Server Add-on can be installed on a Bull System Manager Server machine (for example, on Linux and Windows, on IA32 and IA64, etc.).

This release provides several Bull System Manager Server Add-ons. Some of them are free and delivered on the Bull System Manager CD-ROM. The others must be purchased.

System Domain	Server Add-on
Internal Storage (BSM Server CD)	LSI GAMTT Mgt Package
	LSI CIM Mgt Package
	LSI MegaRaid SAS Mgt Package
	Emulex HBA Mgt Package
External Storage (BSM Server CD)	StoreWay FDA Mgt Package
	EMC CLARiiON Mgt Package
	NetApp Mgt Package
	StoreWay DPA Mgt Package
	Switch Brocade Mgt Package
External Device (BSM Server CD)	Bull Water Cooled Door Mgt Package
	APC PDU Mgt Package
	IBM Intelligent PDU Mgt Package
Virtualization Management (BSM Server CD)	VMware vSphere Mgt Package
	Escala LPAR Mgt Package
	Helios Mgt Package
Network Device (BSM Server CD)	Cisco Switch Mgt Package
	IB Switch Mgt Package

Table 1-1. Server Add-Ons

The Server Add-ons are described in the chapters that follow.

Chapter 2. Installing and Configuring BSM Server Add-ons

Before installing Bull System Manager, check that the environment meets the software and hardware requirements, described below.

2.1 General Installation Requirements

Supported Operating Systems

Bull System Manager Server Add-ons operate on **Linux** and **Windows** operating systems.

The principal requirement is the pre-installation of Bull System Manager Server. See *Bull System Manager Installation Guide* for details.

Required Disk Space

In general, each Server Add-on needs between 1 and 2 MB.

Required Memory

The following table indicates the required memory for the Management Server.

Bull System Manager	Memory
Management Server	2 GB

Table 2-1. Bull System Manager - Required Memory

BSM Server Add-on Installation Requirements

Server Add-ons	Component
*	BSMServer2.1-x

Table 2-2. Management Server Add-ons Installation Requirements

BSM Server Add-on Operational Requirements

Server Add-ons	Target Tools
BSMGAMTT	Linux GAM version 6.02.31 or higher. Windows GAM version 6.02-32 or higher. **Important:** Go to www.lsilogic.com to download the above versions. If not on-line, contact the Bull support team. **Note:** For **IA32** machines the following earlier versions are supported: Linux GAM version 6.02-21 or higher Windows GAM version 6.02-22 or higher.
BSMLSICIM	LSI CIM provider version 3.06 or higher. **Important:** Go to www.lsilogic.com to download the above versions. If not on-line, contact the Bull support team. **Note:** Not supported on Linux IA64 systems.
BSMMegaRaidSAS	LSI MegaRaid SAS (IR) SNMP agent version 3.09 or higher. Go to www.lsilogic.com to download the above versions. If not on-line, contact the Bull support team.
BSMEmulexHBA	**On managed ESX hosts:** VMware ESX 5.0 or higher Emulex CIM Provider for VMware ESX 5.0 or higher (http://www.emulex.com/downloads/emulex/vmware/vsphere-50/management.html) **On managed Windows or Linux hosts:** Emulex® OneCommand™ Manager Application version 6.0 or higher or Emulex® OneCommand™ Manager CLI version 6.0 or higher (Windows Server 2003: http://www.emulex.com/downloads/emulex/windows/windows-server-2003/management.html Windows Server 2008 http://www.emulex.com/downloads/emulex/windows/windows-server-2008/management.html Windows Server 2008 R2 http://www.emulex.com/downloads/emulex/windows/windows-server-2008-r2/management.html Windows Server 2012 http://www.emulex.com/downloads/emulex/windows/windows-server-2012/management.html RHEL 5.5 – 5.8 http://www.emulex.com/downloads/emulex/linux/rhel5x/management-and-utilities.html

Server Add-ons	Target Tools
	RHEL 6.0 – 6.3 http://www.emulex.com/downloads/emulex/linux/rhel6x/management-and-utilities.html SUSE 10 SPx http://www.emulex.com/downloads/emulex/linux/sles-10-spx/management-and-utilities.html SUSE 11 SP1 – SP2 http://www.emulex.com/downloads/emulex/linux/sles-11sp1-sp2/management-and-utilities.html) **Important:** On Windows platforms BSM Addons use the Emulex® Core Kit (CLI) (Windows Server 2003 : http://www.emulex.com/downloads/emulex/windows/windows-server-2003/management.html Windows Server 2008 : http://www.emulex.com/downloads/emulex/windows/windows-server-2008/management.html) Windows Server 2008 R2 http://www.emulex.com/downloads/emulex/windows/windows-server-2008-r2/management.html Windows Server 2012 http://www.emulex.com/downloads/emulex/windows/windows-server-2012/management.html) On Linux platforms for managed **ESX** hosts BSM Addons use the WBEM CLI utility. Use *yum install sblim-wbemcli* to install it. On Linux platforms for managed **Windows/Linux** hosts BSM Addons use the Emulex® Core Kit (CLI). (RHEL 5.5 – 5.8 http://www.emulex.com/downloads/emulex/linux/rhel5x/management-and-utilities.html RHEL 6.0 – 6.3 http://www.emulex.com/downloads/emulex/linux/rhel6x/management-and-utilities.html SUSE 10 SPx http://www.emulex.com/downloads/emulex/linux/sles-10-spx/management-and-utilities.html SUSE 11 SP1 – SP2 http://www.emulex.com/downloads/emulex/linux/sles-11sp1-sp2/management-and-utilities.html)
BSMStoreWayFDA	StoreWay FDA embedded SNMP Agent.
BSMEmcClariion	EMC Navisphere SNMP agent
BSMNetApp	NetApp embedded SNMP agent

Server Add-ons	Target Tools
BSMStoreWayDPA	StoreWay DPA embedded SNMP agent
BSMSwitchBrocade	Switch Brocade embedded SNMP agent
BSMVMwareVSphere	VMware Virtual Center 2.5 or higher VMware ESX 3.0 or higher **Important**: BSM Add-ons use and include the VI Perl toolkit API. On Windows platforms, the BSM Server uses ActivePerl with the VI Perl toolkit API (see requirements), but on Linux platforms, you have to install the required Perl packages for the VI Perl toolkit API. Go to the VMware documentation site to have the list of requirements http://www.vmware.com/support/developer/viperltoolkit/. If not on-line, contact the Bull support team.
BSMEscalaLPAR	IVM VIOS for Power5 and Power6 (Escala PL or EL Blade servers) or HMC version 6.1 and higher
BSMWaterCooledDoor	Device firmware: EMM release 1.1.0 build14
BSMAPCPDU	APC Switch rack PDU AP7821, AP7921 and AP7922 with firmware release 3 and higher.
BSMHelios	BSM agents installed on Helios DBSS and Helios Linux targets GCOS8 SNMP Agent
BSMCiscoSwitch	Cisco SNMP Agent
BSMIBSwitch	IB Switch SNMP Agent

Table 2-3. Management Server Add-ons Operational Requirements

2.1.1 Restrictions

Windows

N/A

Linux

N/A

2.2 Installing BSM Server Add-ons for Windows

Prerequisites

To install Bull System Manager Server Add-ons on Windows:

- The user must be a member of an Administrators group. The default administrator login is Administrator.
- The installation program requires the Internet Explorer web browser. Other browsers, such as Netscape or Mozilla, cannot be used to install Bull System Manager on Windows.
- Management Server Add-ons are to be installed on the server dedicated to management.
- Acrobat Reader is required to view PDF versions of the Bull System Manager documentation.
- The Server Add-ons are included on the *Bull System Manager* CD-ROM.

2.2.1 Installing Management Server Add-ons from the BSM CD-ROM

Management Server Add-ons, to be installed on the server dedicated to management, require the components indicated in *General Installation Requirements* in Section 2.1, and must be installed from the CD-ROM.

To install **Management Server Add-ons** from the CD-ROM:

1. From the dedicated server, launch the installation program.
2. Log on as Administrator.
3. Insert the Bull System Manager CD-ROM in the drive.
   The installation program is launched automatically and opens the **Welcome** page.

Note If the installation does not start automatically, double-click **<CD-ROM drive> / setup.exe**.

Figure 2-1. Windows Installation - Bull System Manager Welcome Page

4. Click **Install Now** to open the **Install** page, which allows the selection of the required Bull System Manager components:
   - Management Server Add-ons
     and provides the following information:
   - What to install?
   - What to do now?

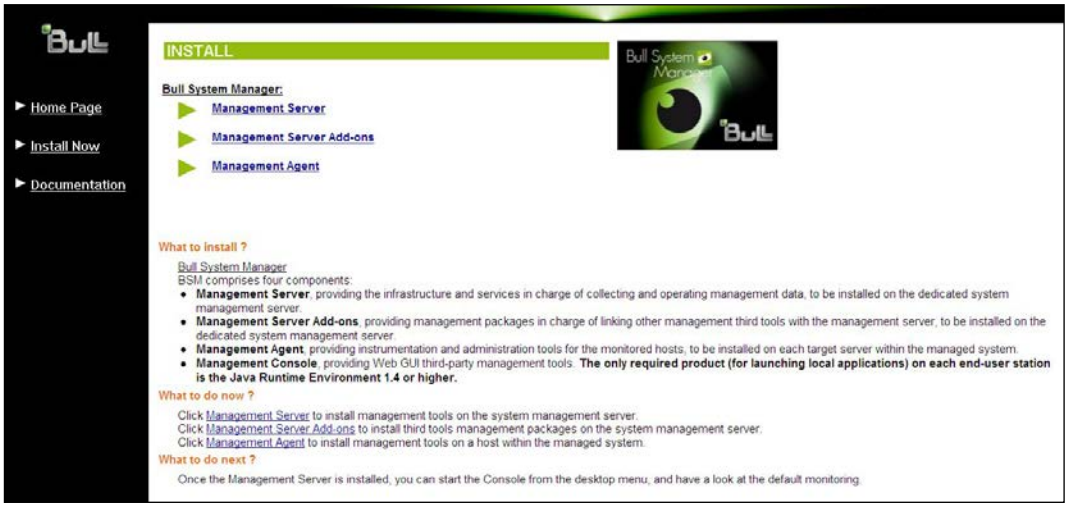


Figure 2-2. Windows Installation - Bull System Manager Install Page

5. Select **Management Server Add-ons**

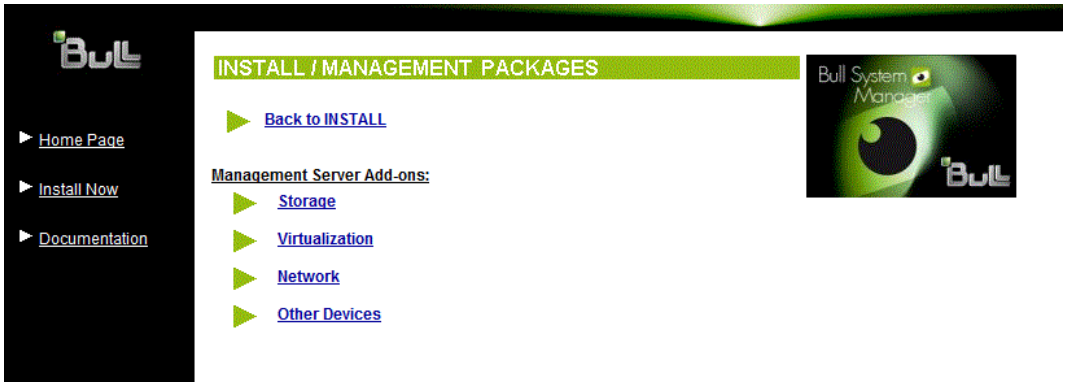


Figure 2-3. Windows Installation - Selecting Bull System manager Server Add-ons

6. Select an Add-ons family **(Storage, Virtualization, Network** or **Other Devices)**, then **Windows 32 bits** operating system.

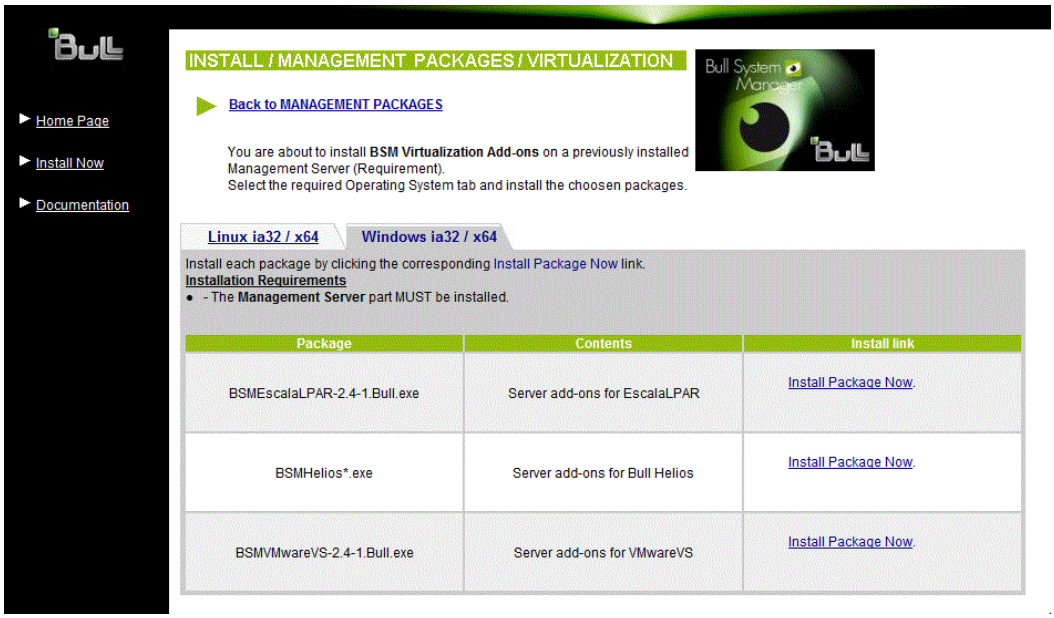


Figure 2-4. Windows Installation - Bull System Manager Server Add-ons Install Page

7. Click the corresponding **Install Package Now** link to install the **Server Add-ons** package. The wizard prompts for a destination folder. The default value can be changed if required.

At the end of the installation process, the Management Server Add-ons components are automatically operational.

2.2.2 Un-installing BSM Server Add-on Components

Un-installation operations must be launched locally. Launching the un-installation program removes all files and folders.

To un-install Bull System Manager Add-ons components:

1. From the Control Panel, launch **Add/Remove Programs**.
2. Select the required Bull System Manager Server Add-ons components and click **Remove**.

Note After un-installation operations, customized categories from previous versions may remain in the configuration. These elements must be removed using the BSM Configuration GUI.

2.2.3 Upgrading to a New BSM Server Add-on Version

When upgrading to a new BSM Server Add-ons version, the existing BSM Server Add-ons environment that may have been customized is maintained.

BSM Server Add-ons are upgraded via the standard installation program.

Note When you upgrade to a new of the BSM Management Server, you must also upgrade BSM Server Add-ons to benefit from new improvements.

See the Release Notes for more details about migrating specific Add-ons, where applicable.

2.3 Installing Bull System Manager Server Add-ons for Linux

This section describes how to install BSM Add-ons for Linux.

2.3.1 Prerequisites

To install Bull System Manager Server Add-ons for Linux:

- The user must be logged as root.
- The installation program requires the **Mozilla** web browser (Version >**1.4.3** or **Firefox**):
  If Mozilla is not installed, launch another web browser and open the file:
  <CD-ROM Mount point>/product /index.html
  It is advised to uninstall the previous version of Mozilla before installing a new version. This operation will not delete bookmarks, histories, cookies and other information stored in the profile directory.
  The Mozilla directory must be set as a root PATH environment variable. If a previous version of Mozilla is still installed, the new Mozilla directory must be set at the beginning of the PATH variable.
- Management Server Add-ons must be installed on the server dedicated to management.
- Acrobat Reader is required to view PDF versions of the Bull System Manager documentation.
- The Server Add-ons are present on the *Bull System Manager* CD-ROM or on the *Bull System Manager Add-ons* CD-ROM.

Notes

- You can check if the required packages from a given Add-on are installed by launching.
  ```
  cd <CD-ROM mount point>
  /checkEnvAddon.sh –a <addOn>
  ```
- AddOn is the name of the RPM (BSM<addOnIdent>.<version>.Bull) or the short addOnIdemt.
- The RPM packages listed above may have their own dependencies and require other RPM packages.
- If the RPM has been installed, the result of the checkEnvAddon is listed in the corresponding installation log (post_install_BSM<addonIdent> log in the `<BSM Installation>/engine/tmp/` directory

2.3.2 Installing Management Server Add-ons from the CD-ROM

Management Server Add-ons to be installed on the server dedicated to management, require the components indicated in *General Installation Requirements* in Section 2.1, and must be installed from the CD-ROM.

To install **Management Server Add-ons** from the CD-ROM:

From the dedicated server, launch the installation program.

Log on as **root**.

1. Insert the Bull System Manager CD-ROM in the drive.
   The CD-ROM file system is automatically mounted as one of the following directories:
   - **/mnt/cdrom** or **/mnt/dvd** (Red Hat and Advanced Server distributions)
   - **/media/cdrom** or **/media/dvd** (SuSE distribution).
2. Launch the following commands:

```
cd <CD-ROM mount point>
./install.sh
```

The **install.sh** script automatically launches the Mozilla or Mozilla Firefox browser and opens the **Welcome** page.

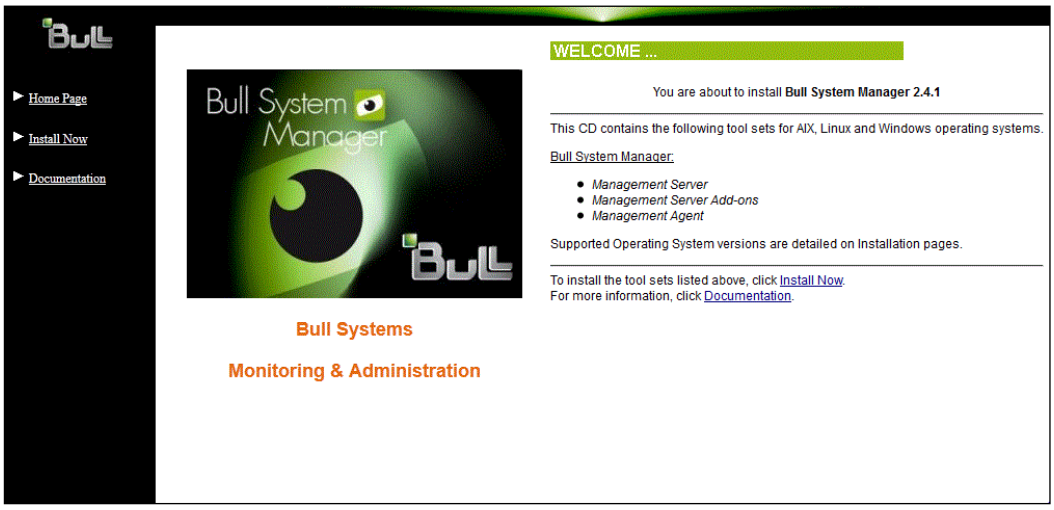


Figure 2-5. Linux Installation - Bull System Manager Welcome Page

3. Click **Install Now** to open the **Install** page, which allows the required Bull System Manager components to be selected:
   - Management Server Add-ons

   and provides the following information:
   - What to install?
   - What to do now?

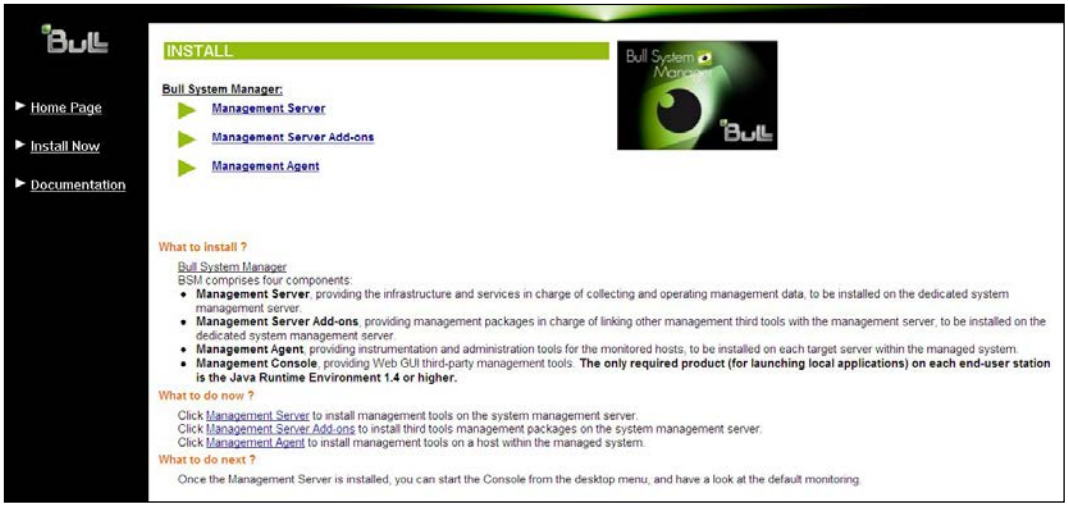


Figure 2-6. Linux Installation - Selecting Bull System Manager Components

4. Select **Management Server Add-ons**.

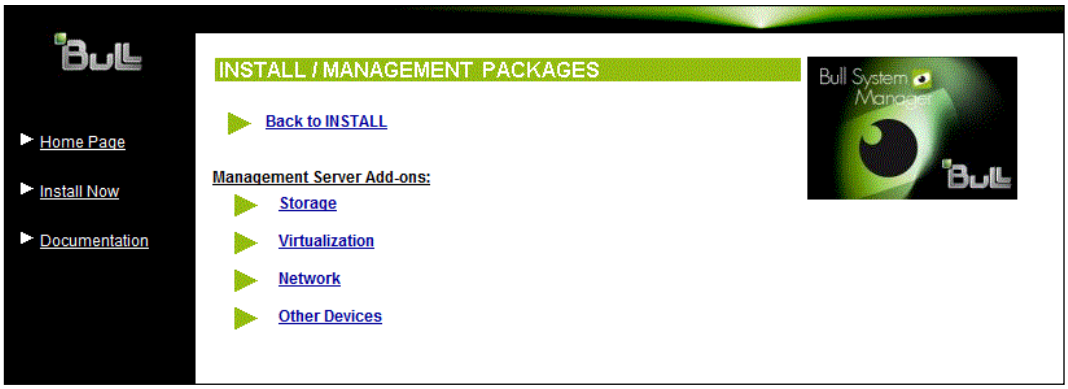


Figure 2-7. Linux Installation - Selecting Bull System Manager Server Add-ons

5. **Select an Add-ons family (Storage, Virtualization or Other Devices),**
   Select the **Linux ia32 / x64** operating system.

Figure 2-8. Linux Installation - Bull System Manager Server Add-ons Install page

6. Install the selected **Bull System Manager Server Add-ons** packages:

```
cd <CD-ROM mount point>/product/mgtpack/BSM<toolname>/linux

rpm –Uhv BSM<toolname>-2.1-x.noarch.rpm
```

2.3.3 Uninstalling BSM Server Add-on Components

1. Log on as **root**.
2. Launch:

```
rpm -e BSM<toolname>-2.1-x.noarch.rpm
```

2.3.4 Upgrading to new Bull System Manager Server Add-on Versions

When upgrading to new Bull System Manager Server Add-on versions, the existing Bull System Manager Add-ons environment that may have been customized is maintained.

Bull System Manager Add-ons are upgraded via the standard rpm installation command:

```
rpm –Uhv BSM<toolname>-2.1-x.noarch.rpm
```

Note When you upgrade the Bull System Manager Management Server, you MUST upgrade the previously installed server Add-ons to benefit from the new improvements.

See the *Release Notes* for more details about migrating specific add-ons, where applicable.

2.4 Monitoring Configuration

Configuring Bull System Manager Monitoring consists mainly in specifying the parameters required for monitoring tasks. Most configuration tasks are performed via the Bull System Manager Configuration GUI (Graphical User Interface).

Bull System Manager Server Add-ons extend the Monitoring configuration default rules that the Administrator can customize. New monitoring categories and services are provided.

2.4.1 GUI Configuration

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

Starting the Configuration GUI

To start the Configuration GUI, 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>/BSM**
- Or, from a web browser, go to the following URL: **http://<Bull System Manager server name>/BSM/config/**

2.4.2 Categories and Services

Bull System Manager Server Add-ons deliver more default monitoring categories and services. These categories and services depend on the Operating System running on the host:

- Services for Windows hosts will be applied to all hosts using a Windows Operating System
- Services for Linux hosts will be applied to all hosts using a Linux Operating System
- Services for hosts, independently of the Operating System, will be applied to all hosts.

The Administrator can change the default monitoring configuration by:

- **Customizing services**, to define specific thresholds and monitoring properties or to modify the list of monitored hosts. A service can be customized 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. For instance, if you do not want to monitor file systems in the same way on all Linux hosts, customize the **All** service in the **FileSystems** category.

Note The Administrator CANNOT modify the OS and/or model type of these monitoring services and categories, as internal tool semantic checks may reject such modifications.

- **Cloning services**, to define new elements monitored. One or more services are created, with different names from the original names. All properties can be edited except the check command. For instance, to monitor a specific logical drive on a Windows system, clone the **C** service and modify the check command parameters.
- **Customizing categories**, to restrict monitoring a whole category to a list of hosts.
- **Creating a category**, to assign a set of cloned services to this category.

See the *Bull System Manager Administrator's Guide* for more details about the configuration.

Chapter 3. BSM Server Add-ons

Bull System Manager Server Add-ons provide different functional items for each Management Package.

3.1 Internal Storage

The following Add-ons are used for monitoring internal storage.

3.1.1 BSM GAMTT for LSI MegaRAID 320-2x Management

GAMTT (or GAM) is the LSI tool used to survey, configure and control RAID provided by LSI MegaRAID Ultra320 SCSI cards.

See http://www.lsilogic.com/products/megaraid/index.html to download the GAMTT install package and for more information.

Note This tool runs on NovaScale machines under Linux or Windows.

The corresponding Bull System Manager Add-on creates monitoring links between Bull System Manager and the GAM SNMP agent.

The following figure shows the different monitoring components:

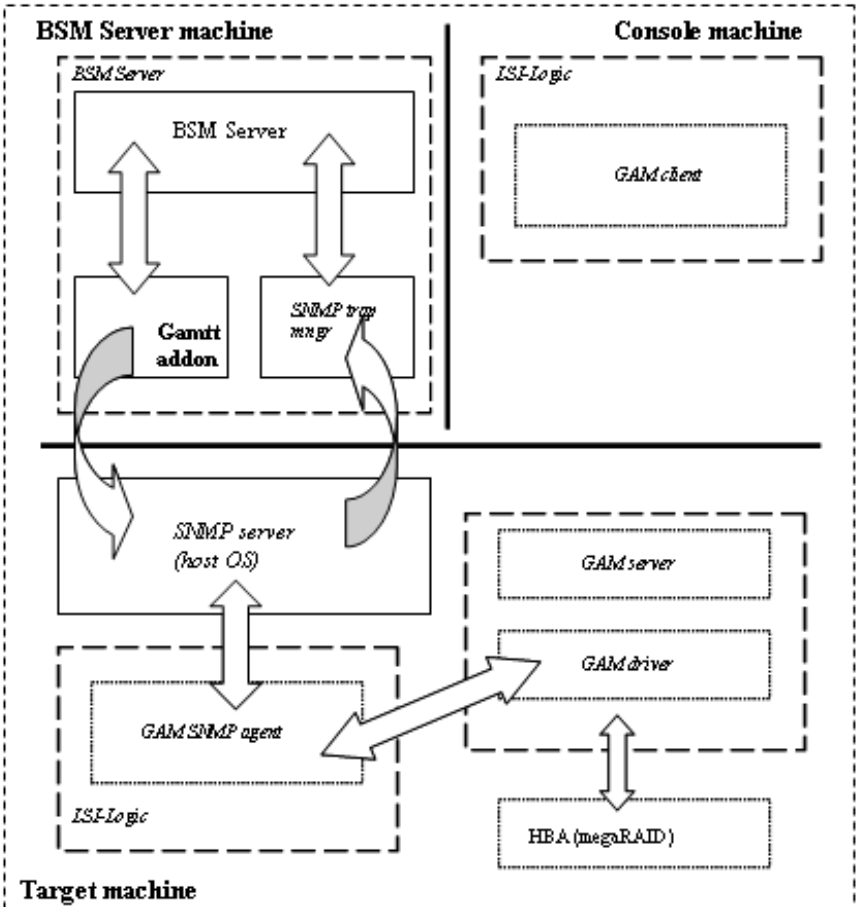


Figure 3-1. GAM Monitoring Components

3.1.1.1 Default Categories & Services (independent of OS type)

Targeted OS	Model	Category	Service	Check command
Any	Any	GAMTTraid	Status	Check_gamttRAID
			Alerts	No check (SNMP trap receiver)

Table 3-1. GAMTT monitoring services

Notes

- This category is based on the **GAMTT** management product from **LSI**. This tool and especially its SNMP interface is a requirement for the **GAMTTraid** monitoring services. Check that this tool works on the targeted OS, if you want to use it for monitoring in Bull System Manager.
- The previous **MegaRAID** category (NovaScale Master release 4.0) is based on the **PowerConsolePlus** management product from LSI. These two management products are functionally redundant but not compatible. So you need to replace the **MegaRAID** category and its services by the **GAMTTraid** category and services, if you replace **PowerConsolePlus** by **GAMTT.**

3.1.1.2 GAMTTraid Category

Status For NovaScale and Express5800 hosts with an LSI (or Mylex) SCSI RAID card managed by GAMTT (or GAM) management tool. This service checks the Host RAID status reported by the associated GAMTT SNMP agent.

Alerts For NovaScale and Express5800 hosts. When an alert is sent from the GAMTT SNMP agent, it is processed by the Bull System Manager server.

Notes

- The **mlxraid.mib** is integrated in the Bull System Manager application
- Do not forget to configure the 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 for this agent.

3.1.1.3 check_gamttRAID (any OS) Nagios command

The configurable Bull System Manager service check command syntax is:

```
check_gamttRAID!<community>!<port>!<timeout>!{ [-A {ALL|<Ct>}] |
[-P {ALL|<Ct>.<Ch>.<Tg>}] | [-L {ALL|<Ct>.<Ldn>}] }
```

Input

<community>	SNMP community string (defaults to ”public”)
<port>	SNMP port (defaults to 161)
<timeout>	Seconds before timing out (defaults to Nagios timeout value)
-A, –adapter ALL | <Ct>	Controller board
-P, –physical ALL | <Ct>.<Ch>.<Tg>	Physical device addr
-L, –logical ALL | <Ct>.<Ldn>	Logical drive addr

Output

See the output of the **check_gamttRAID** command in *Chapter 4*.

Default syntax for **GAMTTraid.Status** (the service name as defined in Nagios configuration based on the category name and service name defined in BSM configuration)

```
check_gamttRAID!public!161!60!-A ALL
```

3.1.2 BSMLSICIM for LSI 22320 Chip Management

LSI CIM is the LSI tool used to survey, configure and control RAID provided by LSI MegaRAID 22320 SCSI cards.

See http://www.lsilogic.com/products/megaraid/index.html for more information or for downloading the LSI CIM install package.

Note This tool runs on NovaScale machines under Linux or Windows.

The corresponding Bull System Manager Add-on creates monitoring links between Bull System Manager and the **LSI CIM** provider.

The following figure shows the different monitoring components:

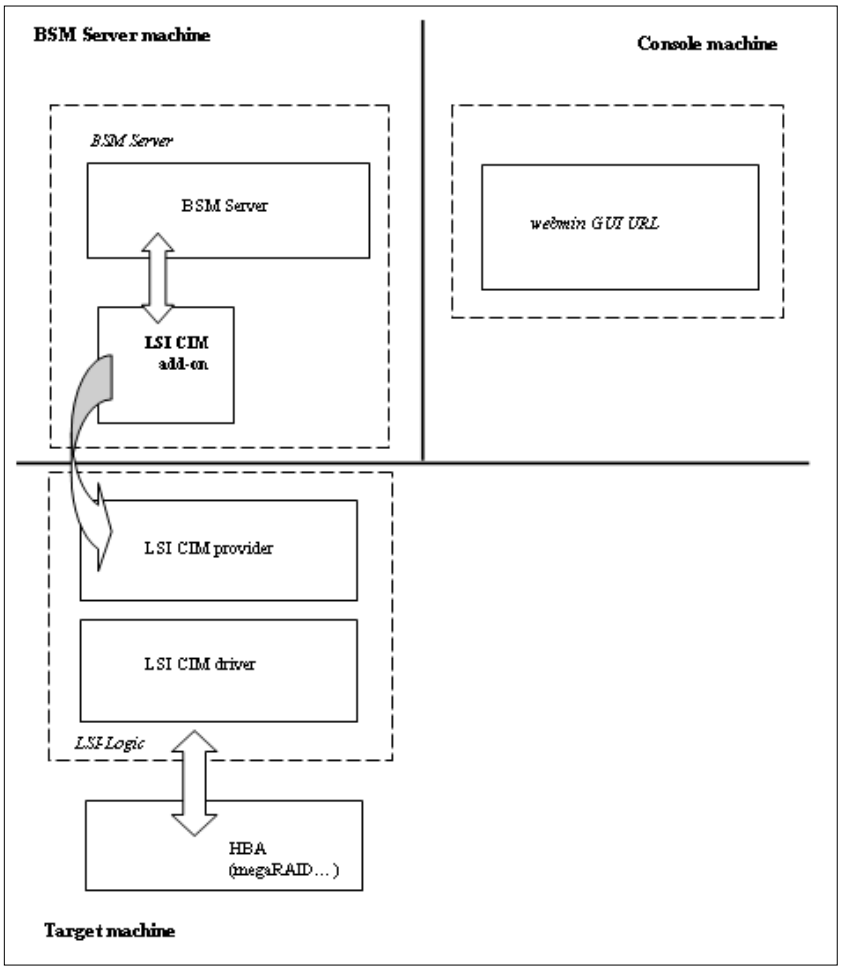


Figure 3-2. LSI CIM Monitoring Components

3.1.2.1 Default Categories & Services (independent of OS type)

Targeted OS	Model	Category	Service	Check command
Any	Any	LsiCIM	RAIDStatus	check_LSICIM
			CTRLstatus	check_LSICIM_ctrl

Table 3-2. LSI CIM monitoring services

Note This category is based on the LSI CIM management product. This tool is a requirement for the following **LsiCIM** monitoring services. Check that this tool works on the targeted OS, if you want to use it for monitoring in Bull System Manager.

LsiCIM Category

RAIDstatus For NovaScale and Express5800 hosts with an LSI SCSI RAID card managed by the LSI CIM management tool. This service checks the Host RAID status reported by the associated LSI CIM provider.

CTRLstatus For NovaScale and Express5800 hosts with an LSI SCSI RAID card managed by the LSI CIM management tool. This service checks the status of a specific RAID SCSI controller reported by the associated LSI CIM provider.

3.1.2.2 check_LSICIM (any OS) Nagios command

The configurable Bull System Manager service check command syntax is:

```
check_LSICIM
```

Input

N/A

Output

See the output of the **check_LSICIM** shell command in *Chapter 4*.

Default syntax for **LsiCIM.CTRL.Status** (the service name as defined in Nagios configuration based on the category name and service name defined in BSM configuration)

```
check_LSICIM
```

3.1.2.3 check_LSICIM_ctrl (any OS) Nagios Command

The configurable Bull System Manager service check command syntax is:

```
check_LSICIM_ctrl![<ctrlname>]
```

Input

<ctrlname> Name of the controller to check

Note The name of the controller must be protected with a quotation mark if the name contains blank characters.

Output

See the output of the **check_LSICIM** shell command in *Chapter 4*.

Default syntax for **LsiCIM.CTRL.Status** (the service name as defined in Nagios configuration based on the category name and service name defined in BSM configuration)

```
check_LSICIM!'ctrlname'
```

3.1.3 BSM MegaRaidSAS (LSI MegaRAID SAS (IR) Management)

The corresponding Bull System Manager Add-on creates monitoring links between Bull System Manager and the LSI MegaRAID SAS(IR) SNMP agent.

It supports the adapters from MegaRAID SAS/SATA Value and Feature Line and the LSI SAS ICs 1064, 1068 and 1078.

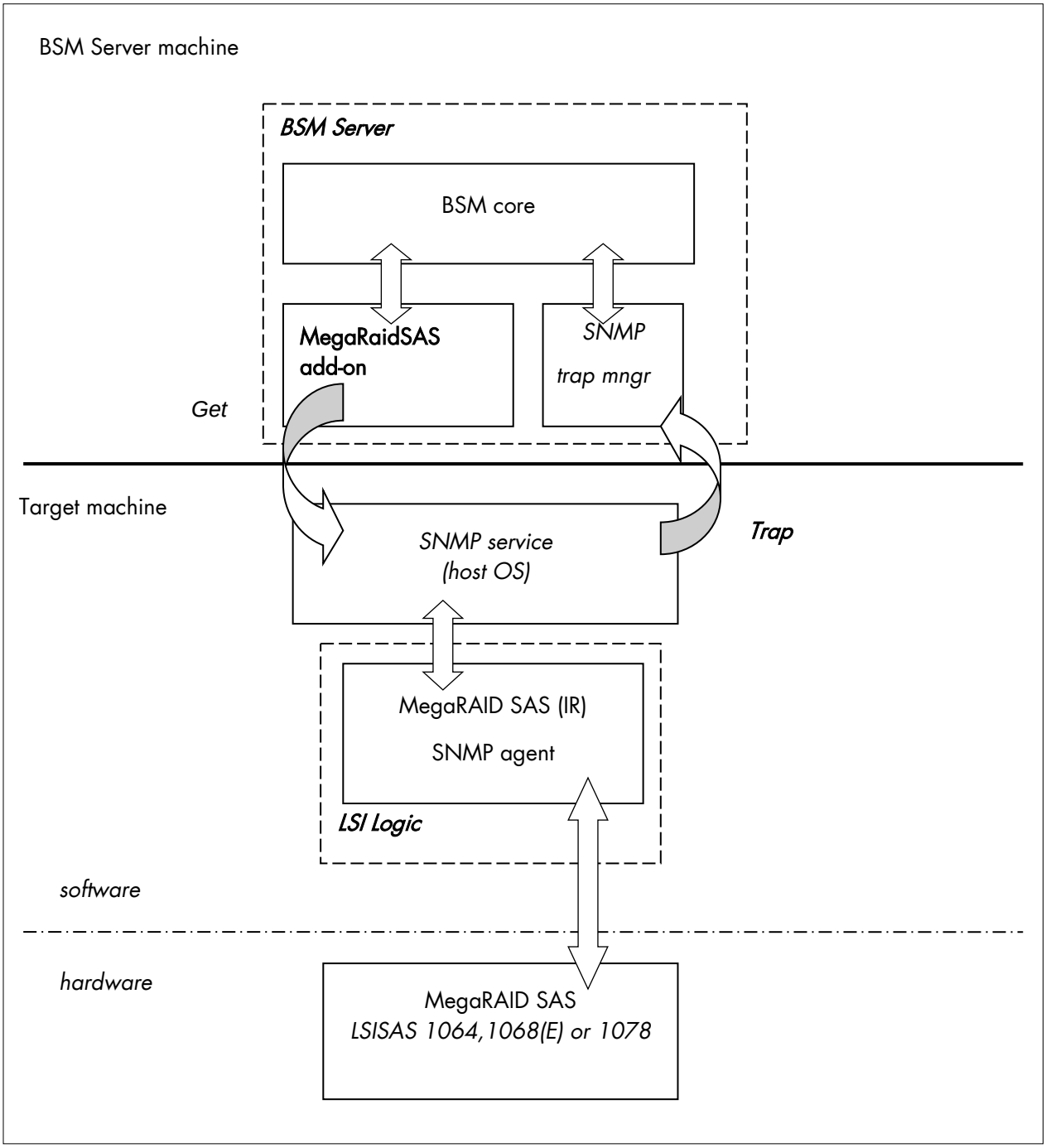


Figure 3-3. MegaRAID SAS Monitoring Components

3.1.3.1 Default Categories & Services (independent of OS type)

Targeted OS	Model	Category	Service	Check command
Any	Any	MegaRaidSAS	Status	check_MegaRAIDSAS
			Alerts	No check (SNMP trap receiver)
Any	Any	MegaRaidSAS_IR	Status	check_MegaRAIDSAS_IR
			Alerts	No check (SNMP trap receiver)

Table 3-3. MegaRaid SAS (IR) monitoring services

Note This category is based on the MegaRAID SAS (IR) SNMP agent. This SNMP interface is a requirement for the following MegaRaidSAS(-IR) monitoring services.

3.1.3.2 MegaRaidSAS(_IR) Category

Status For NovaScale hosts with a MegaRAID SAS card or an integrated LSI SAS chip managed by MegaRAID Storage Management tool. This service checks the MegaRAID SAS (IR) status reported by the MegaRAID SAS (IR) SNMP agent.

Alerts For NovaScale hosts with a MegaRAID SAS card or an integrated LSI SAS chip. When an alert is sent from the MegaRAID SAS (IR) SNMP agent, it is processed by the Bull System Manager Server.

Notes

- The **lsi-adaptersas(ir).mib** is integrated in the Bull System Manager application.
- Do not forget to configure the MegaRAID SAS (IR) SNMP agent to send SNMP traps to the Bull System Manager Server by adding the Bull System Manager Server host address to the agent's SNMP managers list.

3.1.3.3 check_MegaRaidSAS(_IR) (any OS) Nagios command

The configurable Bull System Manager service check command syntax is:

```
check_MegaRaidSAS(_IR)!<community>!<port>!<timeout>
```

See the **check_** `MegaRaidSAS(_IR)` command in *Chapter 4* for parameter details.

Default syntax for **MegaRaidSAS(_IR).Status** (the service name as defined in Nagios configuration based on the category name and service name defined in BSM configuration)

```
check_ MegaRaidSAS(_IR)!public!161!60
```

3.1.4 BSM EmulexHBA (Emulex® HBA Management)

The corresponding Bull System Manager Add-on creates monitoring links between Bull System Manager WEB GUI and the Emulex® LightPulse® Host Bus Adapters (HBAs) via the

- Emulex® CIM provider on servers running VMware ESX operating system (version 5.0 or higher)
- Emulex® OneCommand™ Manager CLI on servers running Windows Server or Linux operating systems.

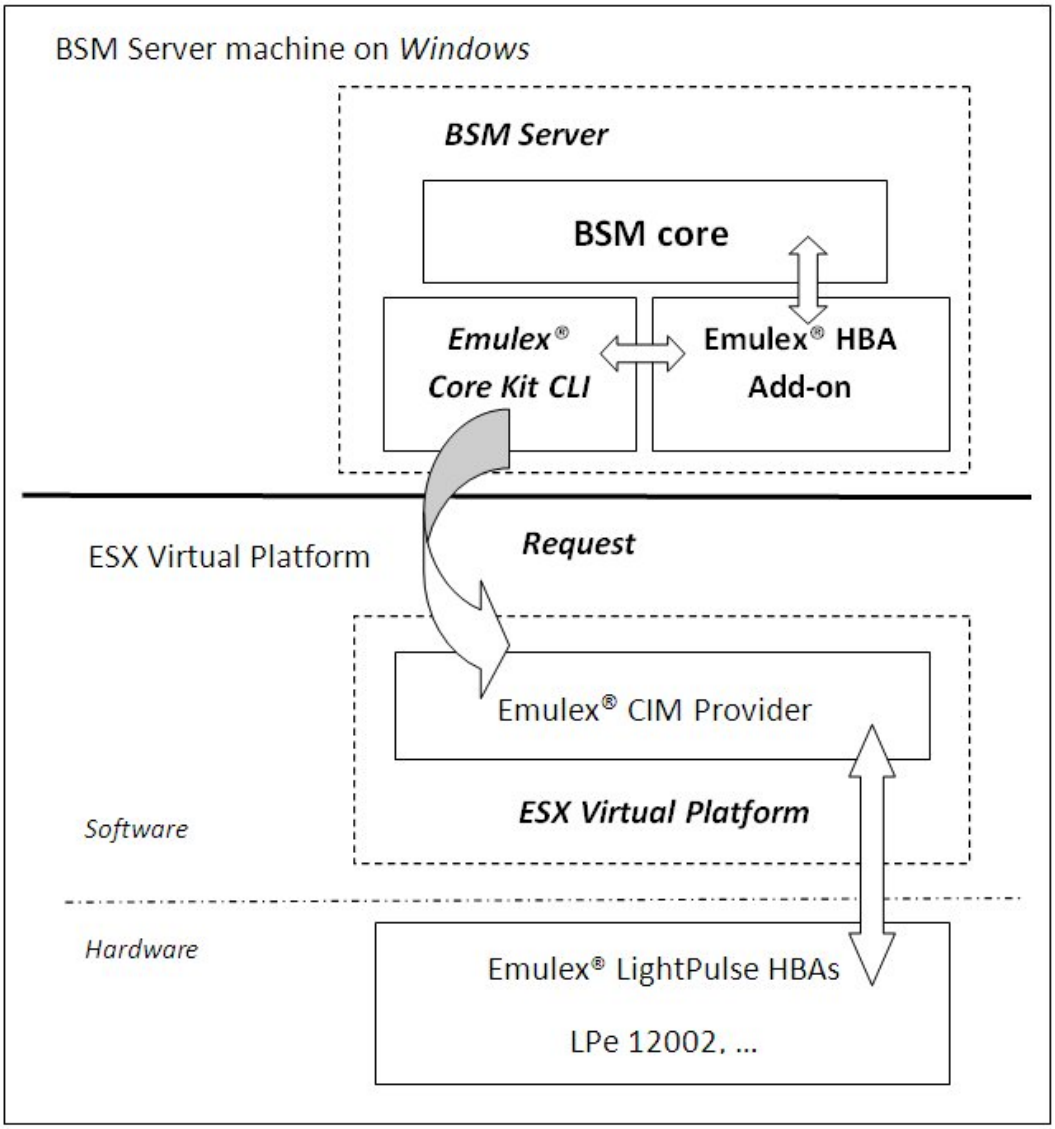


Figure 3-4. ESX Emulex® HBA Monitoring Components and BSM running on Windows

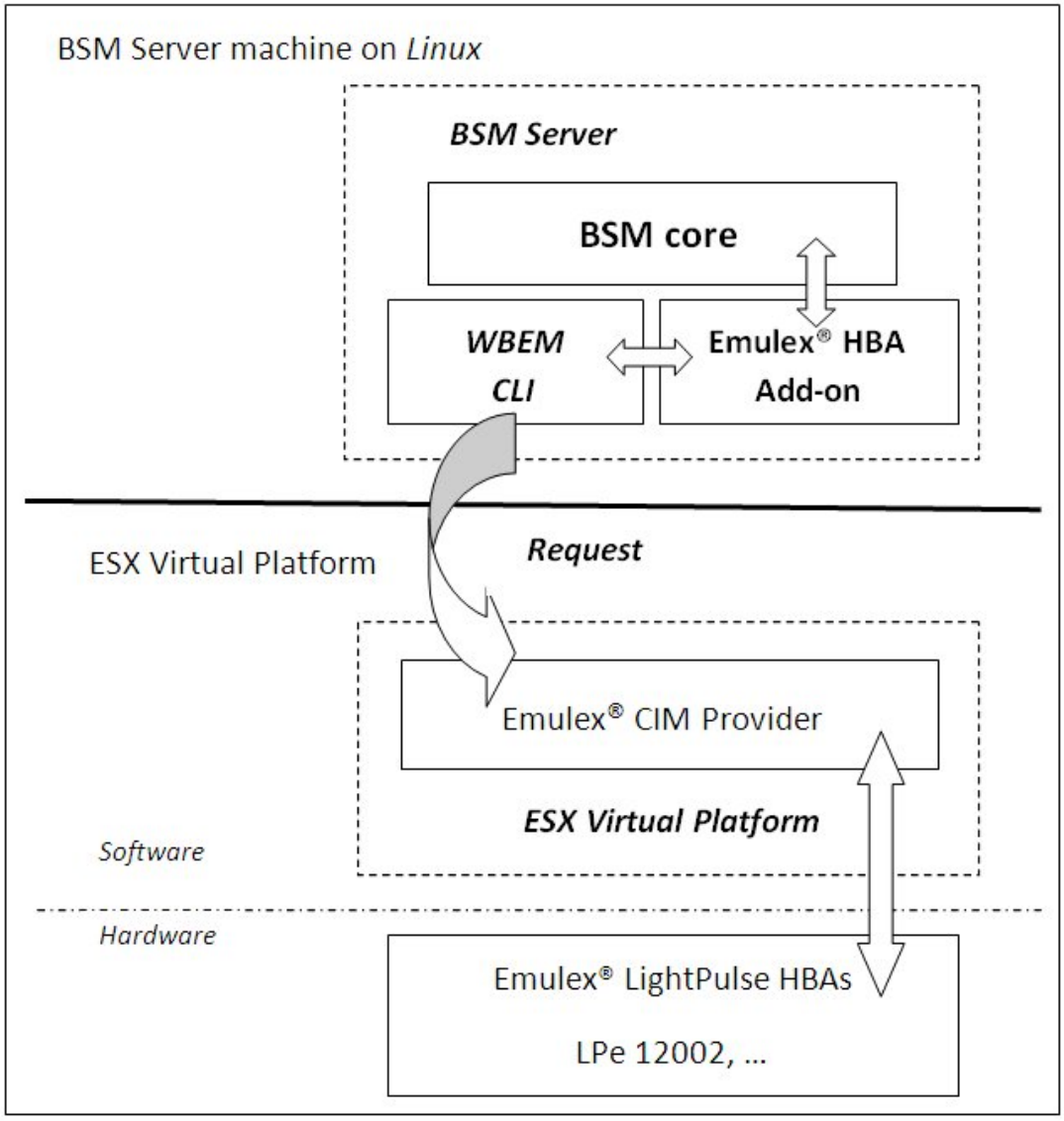


Figure 3-5. ESX Emulex® HBA Monitoring Components and BSM running on Linux

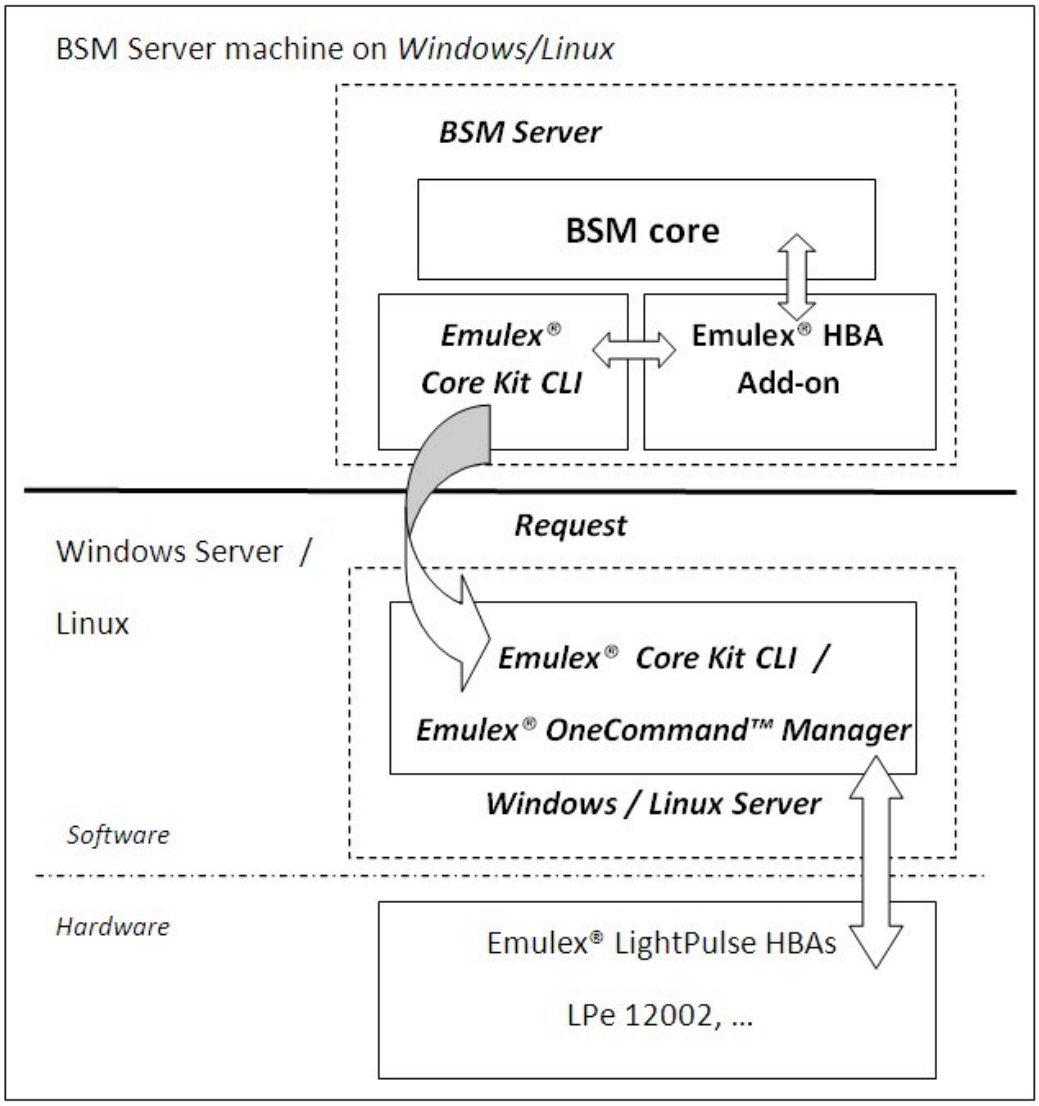


Figure 3-6. Windows/Linux Emulex® HBA Monitoring Components and BSM running on Windows/Linux

3.1.4.1 Default categories & Services

Targeted OS	Model	Category	OS	Service	Check command
ESX	any	EmulexHBA	ESX	Status	check_EmulexHBA
Windows	any	EmulexHBA	Windows	Status	check_EmulexHBA
Linux	any	EmulexHBA	Linux	Status	check_EmulexHBA

Table 3-4. Emulex® HBA Management Monitoring Services

3.1.4.2 EmulexHBA Category for ESX

Status For ESX hosts with Emulex® HBAs installed, managed via Emulex® CIM Provider. This service checks the Emulex® HBA global status reported by the CIM Provider.

3.1.4.3 EmulexHBA Category for Windows Server

Status For hosts running Windows Server (2003, 2008 or 2012) with Emulex® HBAs installed, managed via Emulex® OneCommand™ Manager. This service checks the Emulex® HBA global status reported by the Emulex® OneCommand™ Manager CLI.

3.1.4.4 EmulexHBA Category for Linux Server

Status For hosts running Linux (RHEL 5.5 or higher, SUSE 10 or higher) with Emulex® HBAs installed, managed via Emulex® OneCommand™ Manager. This service checks the Emulex® HBA global status reported by the Emulex® OneCommand™ Manager CLI.

3.1.4.5 check_EmulexHBA command for ESX

The BSM service check_EmulexHBACIM (ESX operating system) check command syntax is:

check_EmulexHBACIM!<action>!<port>!<utility>

Input

<action>	Value available is **Status**
<port>	Value available is **5989**
<utility>	Value available is **CIM**

See *Chapter 4* for details regarding the **check_EmulexHBACIM** command.

3.1.4.6 check_EmulexHBA command for Windows

The BSM service check_EmulexHBAWin (Windows operating system) check command syntax is:

check_EmulexHBAWin!<action>!<utility>

Input

<action>	Value available is **Status**
<utility>	Value available is **SNMP**

See *Chapter 4* for details regarding the **check_EmulexHBAWin** command

3.1.4.7 check_EmulexHBA command for Linux

The BSM service check_EmulexHBALinux (Linux operating system) check command syntax is:

check_EmulexHBALinux!<action>!<utility>

Input

<action>	Value available is **Status**
<utility>	Value available is **SNMP**

See Chapter 4 for details regarding the **check_EmulexHBALinux** command.

3.1.4.8 Configuring EmulexHBA Category

This section describes how to configure EmulexHBA for BSM.

Configuring ESX Virtual Platforms

ESX Virtual Platforms must already be configured on BSM before configuring the EmulexHBA category. To configure an ESX Virtual Platform, refer to *Section 3.4.2.1*

Configuring Windows or Linux Server

Windows or Linux Server must already be configured on BSM before configuring the EmulexHBA category. To configure Hosts, refer to the *BSM Administrator's Guide Section 3.1.*

Configuring EmulexHBA category

To configure EmulexHBA category:

1. From the Supervision tab, select Categories/ Services domain:
2. Click the manage categories link

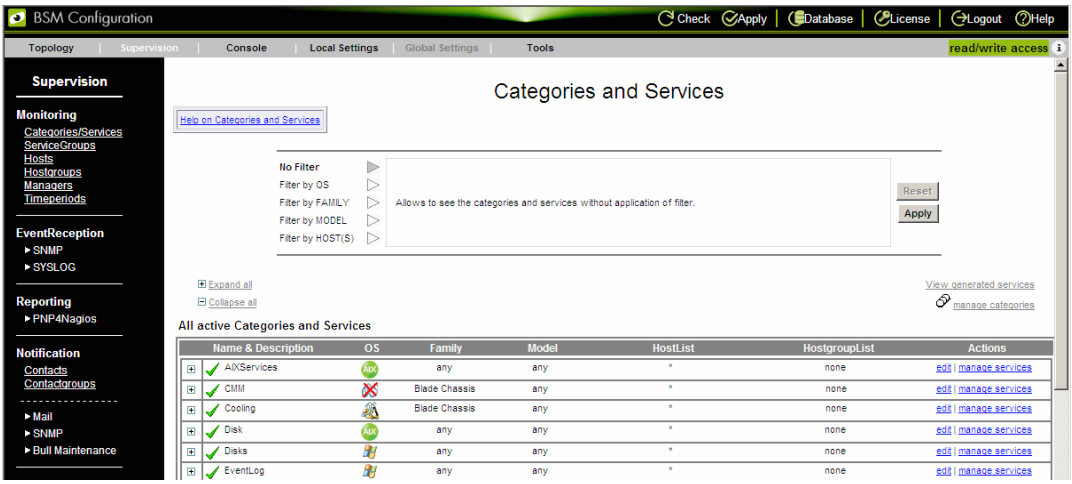


Figure 3-7. Categories and Services Window

3. Click **Add from an unused category template** and select the **EmulexHBA** category corresponding to the host OS.

4. Click on Add from the selected category

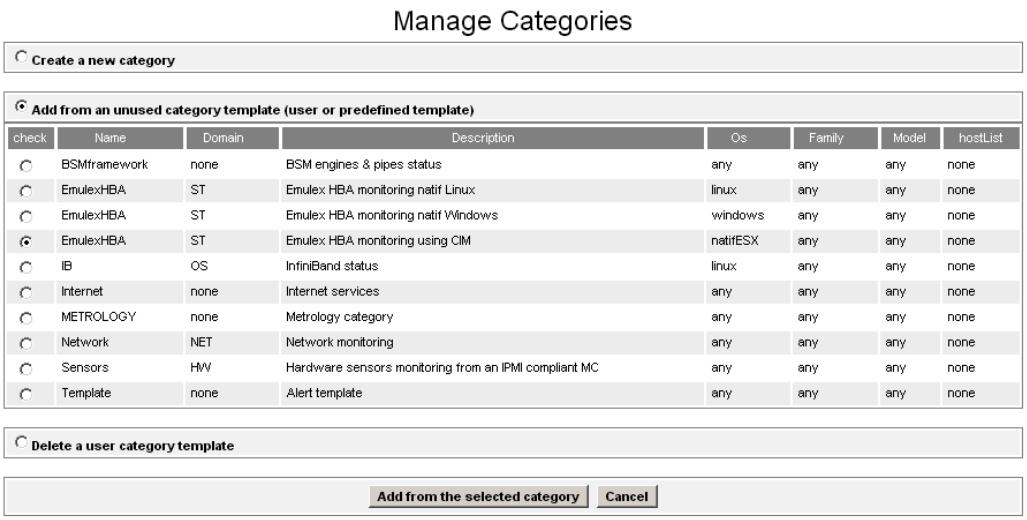


Figure 3-8. Manage Categories Window

5. In the following window, enter the server hostname in the hostlist and click on **OK**.

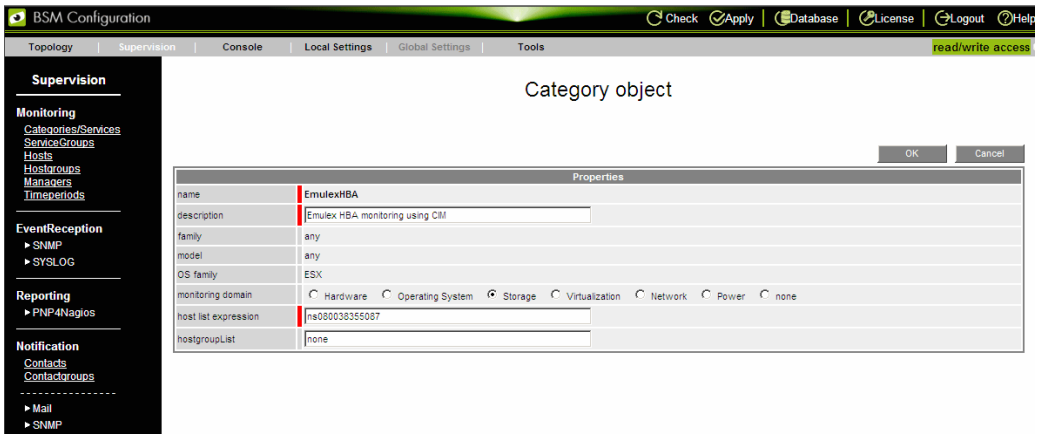


Figure 3-9. Category object Window

6. The **EmulexHBA** category with associated service appears in the list of active categories and services:

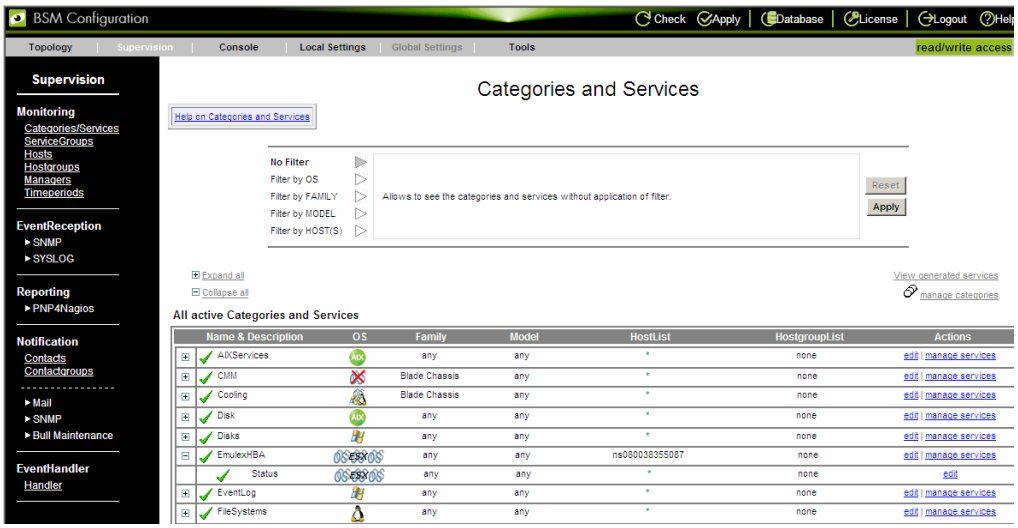


Figure 3-10. Applying Categories and Services

7. Click on **Apply** to validate the configuration.
8. Open the BSM console to display the EmulexHBA.Status service.

Examples

In the example below, Bull System Manager Server is installed on a server running SUSE SLES 11 SP2 operating system. On the managed ESX host named ns080038355087, an Emulex® HBA LPe12002-M8 card is installed.

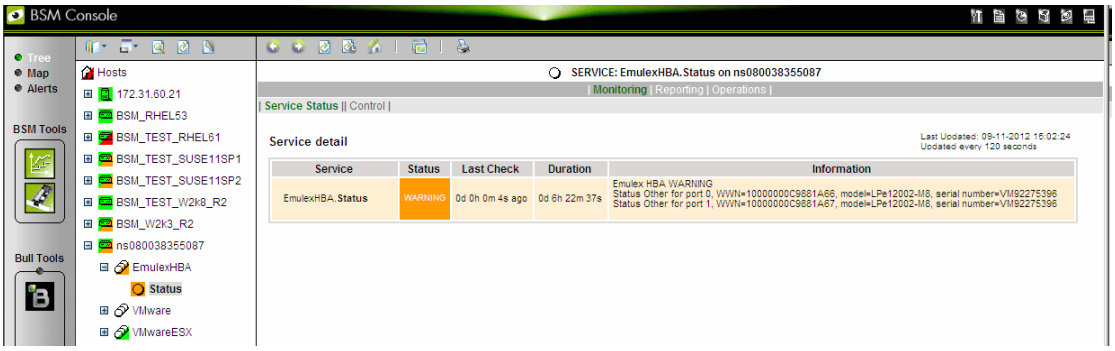


Figure 3-11. Linux example of EmulexHBA.Status service from a managed ESX host.

In the example below, Bull System Manager Server is installed on a server running Windows Server 2003 SP2 operating system and managing the same ESX host named ns080038355087.

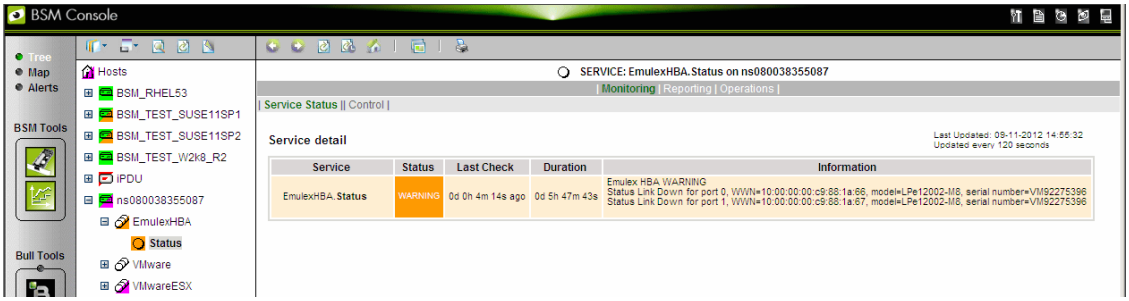


Figure 3-12. Windows example of EmulexHBA.Status service from a managed ESX host.

Note The result of the EmulexHBA.Status service depends of the operating system on which the Bull System Manager Server runs. This is due to the fact, that the Bull System Manager Server running on Windows Server, uses the Emulex® OneCommand Manager Command Line Interface to retrieve information from the managed ESX host, while on Linux (SUSE or RedHat), it uses the WBEM Command Line Interface utility.

In the example below, Bull System Manager Server is installed on a server running Windows Server 2003 SP2 operating system. On the managed RHEL 6.2 host named nsbullion216, an Emulex® HBA LPe12002-M8 card and an Emulex® HBA LPe1250-F8 card are installed.

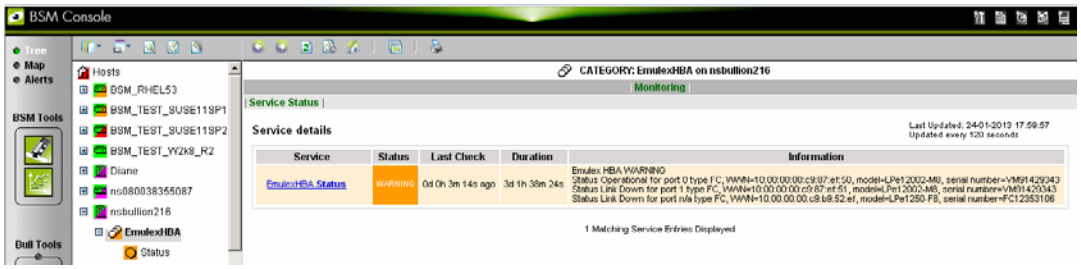


Figure 3-13. Windows example of EmulexHBA.Status service from a managed Linux host.

3.2 External Storage Server Add-ons

The following Add-ons are used for monitoring external storage.

3.2.1 BSMStoreWayFDA

The corresponding Bull System Manager Add-on creates monitoring links between Bull System Manager and the StoreWay FDA SNMP agent and WEB GUI.

It supports the StoreWay FDA and StoreWay Optima families.

Note The access, through the BSM Console/Operations menu, to the administration Web GUI may not be operational for some StoreWay FDA or StoreWay Optima storage systems, due to a bug in their firmware release.

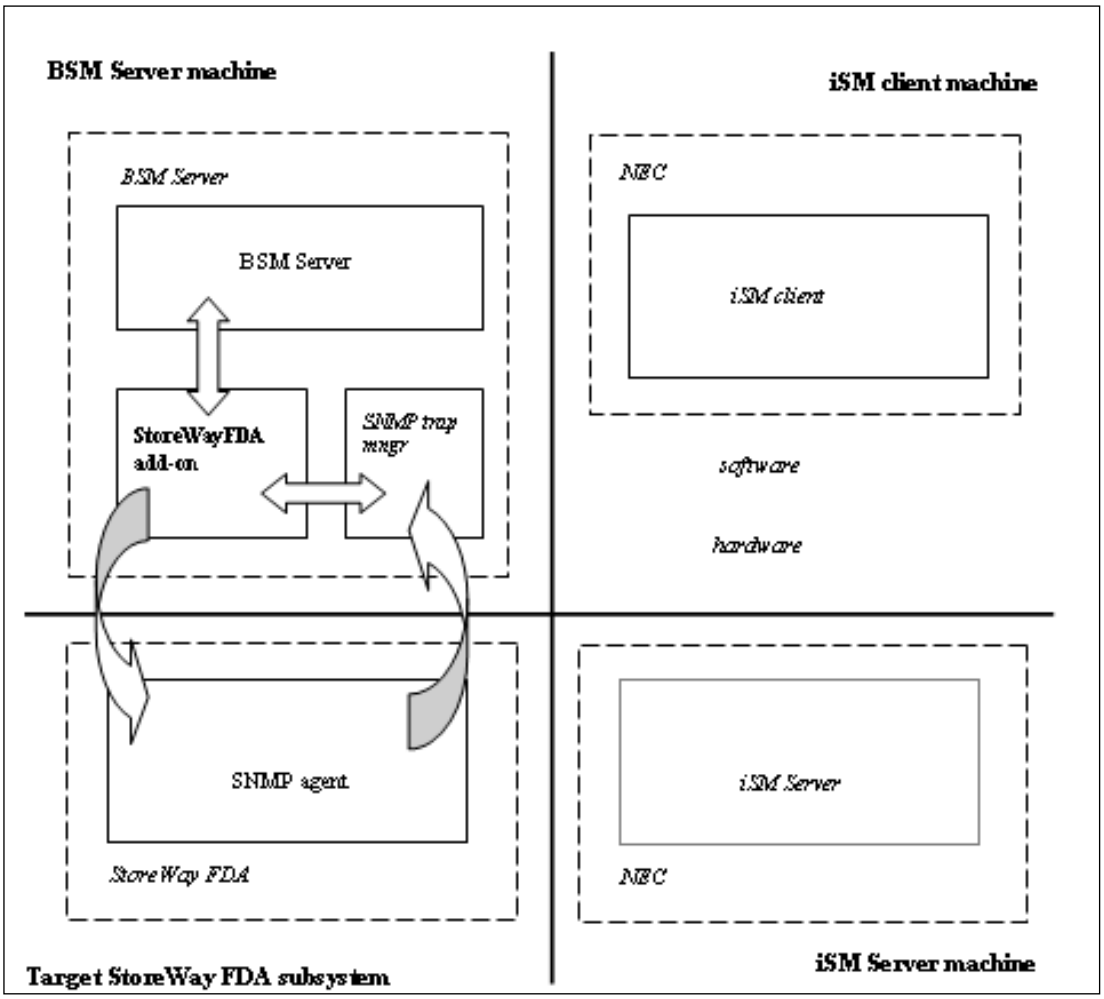


Figure 3-14. StoreWay FDA Monitoring Components

3.2.1.1 Default Categories & Services (independent of OS type)

Targeted OS	Model	Category	Service	Check command
Any	BayStoreWay FDA	StoreWayFDA	Status	check_NECFDA
			Alerts	No check (SNMP trap receiver)

Table 3-5. StoreWay FDA monitoring services

Note This category is based on the StoreWay FDA SNMP agent. This SNMP interface is a requirement for the StoreWayFDA monitoring services.

3.2.1.2 StoreWayFDA Category

Status For StoreWay FDA hosts managed via SNMP agents. This service checks the StoreWay FDA status reported by the SNMP agent.

Alerts For StoreWay FDA hosts. When an alert is sent from the StoreWay FDA SNMP agent, it is processed by the Bull System Manager Server.

Notes

- The **Armg2_4.mib** is integrated in the Bull System Manager application.
- Do not forget to configure the StoreWay FDA agent to send SNMP traps to the Bull System Manager Server by adding the Bull System Manager Server host address to the agent's SNMP managers list.

3.2.1.3 check_NECFDA (any OS) Nagios command

The configurable Bull System Manager service check command syntax is:

```
check_storewayfd!<timeout>
```

See the **check_NECFDA** command in *Chapter 4* for parameter details.

For HOSTADDRESS, SNMP community and SNMP port parameters, the Nagios macros $HOSTADDRESS$, $_HOSTSNMP_COMMUNITY$ and $_HOSTSNMP_PORT$ are used.

Default syntax for **StoreWayFDA.Status** (the service name as defined in Nagios configuration based on the category name and service name defined in BSM configuration)

```
check_necfda!60
```

3.2.1.4 Bull System Manager Configuration

StoreWay FDA configuration for Bull System Manager is available from the configuration GUI by selecting **Topology** → **StoreWay** → **StoreWayFDAs**.

To edit a StoreWay FDA, select **Edit**.

To define a new StoreWay FDA in the Bull System Manager configuration database, click the **New StoreWay FDA** button and initialize the following attributes:

StoreWay FDA name name of the StoreWay FDA

description description

network name bay netname

snmp port number SNMP port number

snmp community SNMP community

3.2.2 BSMEmcClariion (EMC CLARiiON Management)

The corresponding Bull System Manager Add-on creates monitoring links between Bull System Manager and the EMC Navisphere SNMP agent and web GUI.

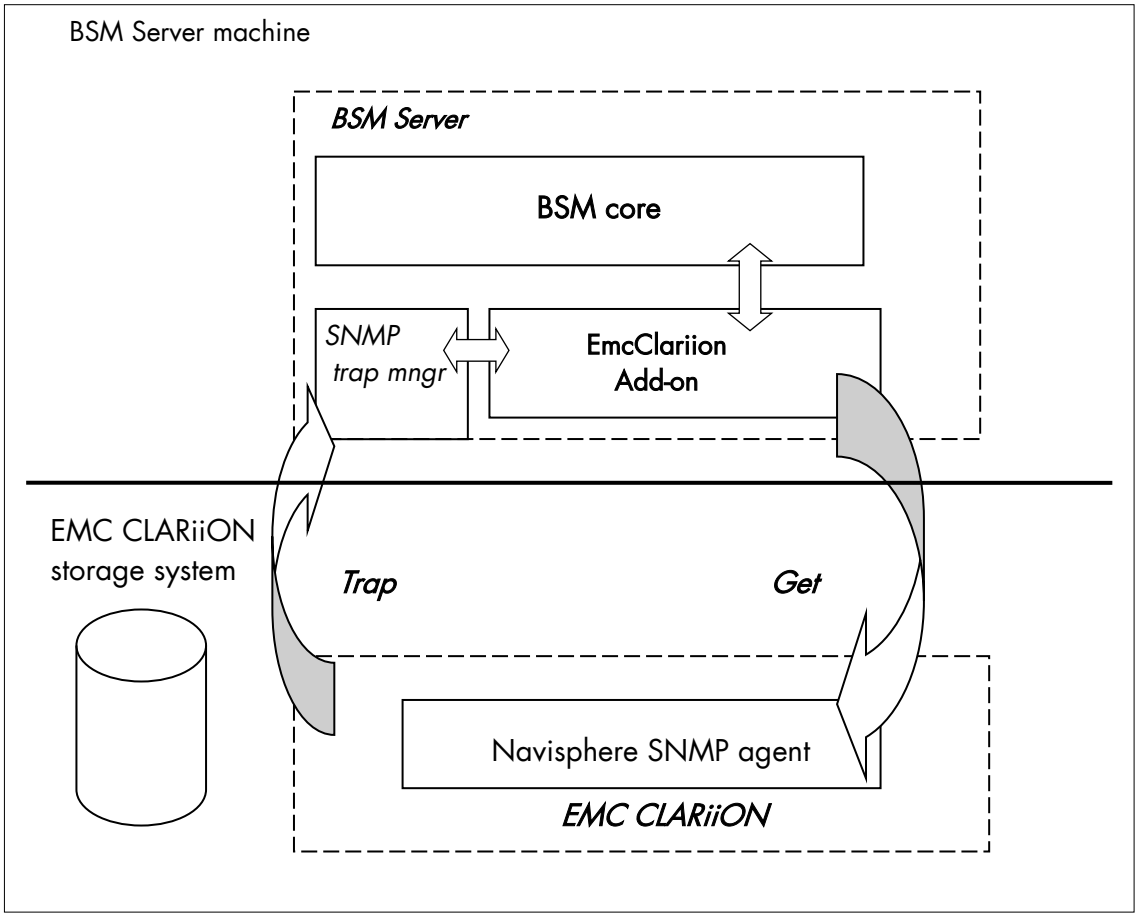


Figure 3-15. EMC CLARiiON Monitoring Components

3.2.2.1 Default Categories & Services (independent of OS type)

Targeted OS	Model	Category	Service	Check command
Any	bayEmcClariion	EmcClariion	Alerts	No check (SNMP trap receiver)
			Status	check_EMCCLARIION

Table 3-6. EmcClariion monitoring services

Note This category is based on the EMC Navisphere SNMP agent. This SNMP interface is a requirement for the EmcClariion monitoring services.

3.2.2.2 EmcClariion Category

Status For EMC CLARiiON hosts managed via Navisphere SNMP agent. This service checks the EMC Clariion status reported by the SNMP agent.

Alerts For EMC CLARiiON hosts. When an alert is sent from the Navisphere SNMP agent, it is processed by the Bull System Manager Server.

Notes

- The **clariion.mib** is integrated in the Bull System Manager application
- Do not forget to configure the Navisphere agent to send SNMP traps to the Bull System Manager Server by adding the Bull System Manager Server host address to the agent's SNMP managers list.

3.2.2.3 check_EMCCLARIION (any OS) Nagios command

The configurable Bull System Manager service check command syntax is:

```
check_EmcClariion!<community>!<port>!<timeout>
```

See the **check_ EMCCLARIION** command in *Chapter 4* for parameter details.

Default syntax for **EmcClariion.Status** (the service name as defined in Nagios configuration based on the category name and service name defined in BSM configuration).

```
check_EmcClariion!public!161!60
```

3.2.2.4 Bull System Manager Configuration

EmcClariion configuration for Bull System Manager is available from the configuration GUI by selecting **Topology** → **StoreWay hosts** → **EmcClariions**.

To edit an EmcClariion, select **Edit**.

To define a new EmcClariion in the Bull System Manager configuration database, click the **New EMC CLARiiON** button and initialize the following attributes:

StoreWay EMC CLARiiON name	name of the EMC CLARiiON
description	description
network name	bay netname
SNMP port number	SNMP port number
SNMP community	SNMP community

3.2.3 BSMNetApp (NetApp Management)

The corresponding Bull System Manager Add-on creates monitoring links between Bull System Manager and the NetApp SNMP agent and WEB GUI.

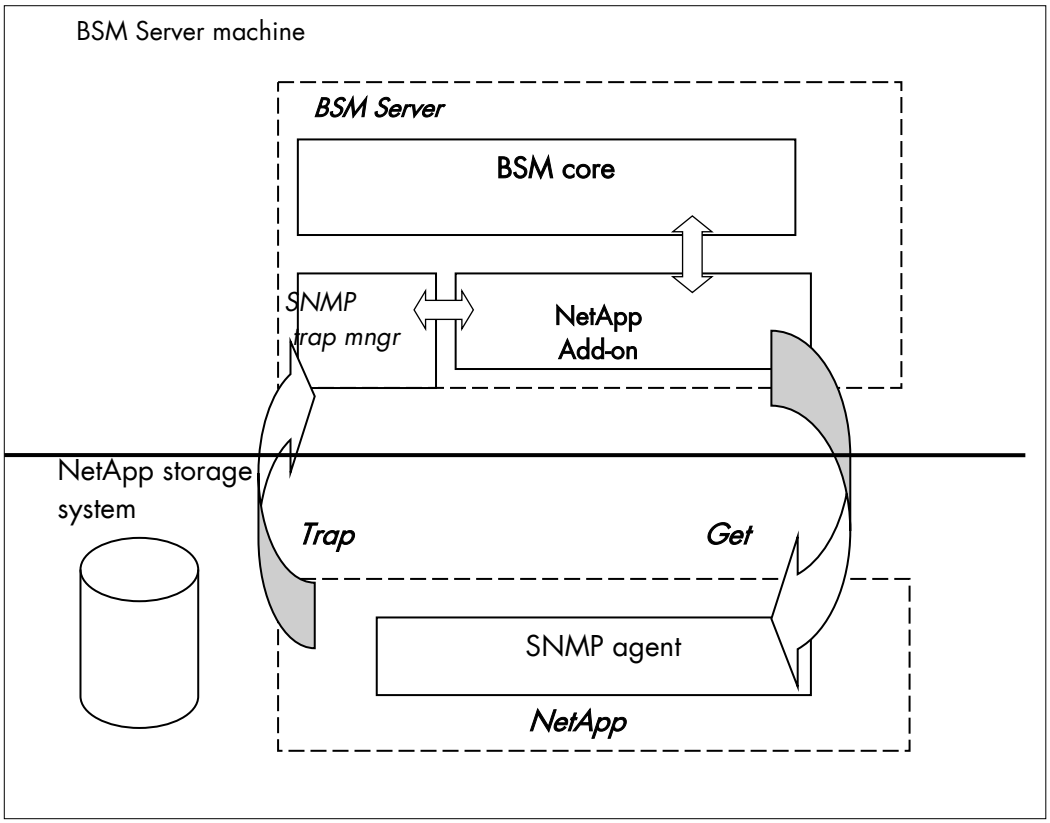


Figure 3-16. NetApp Monitoring Components

3.2.3.1 Default Categories & Services (independent of OS type)

Targeted OS	Model	Category	Service	Check command
any	bayNetApp	NetApp	Alerts	No check (SNMP trap receiver)
			CPULoad	check-netapp-cpuload
			Disks	check-netapp-numdisks
			Fans	check-netapp-failedfans
			GlobalStatus	check_netapp_globalstatus
			Power	check-netapp-failedpwr
			RAIDStatus	check_netappraid
			VolumeStatus	check_netappvol

Table 3-7. NetApp monitoring services

Note This category is based on the NetApp SNMP agent. This SNMP interface is a requirement for the NetApp monitoring services.

3.2.3.2 NetApp Category

CPULoad For NetApp hosts managed via SNMP agents. This service checks the NetApp CPU load reported by the SNMP agent.

Disks For NetApp hosts managed via SNMP agents. This service checks the status of the NetApp disks reported by the SNMP agent.

Fans For NetApp hosts managed via SNMP agents. This service checks the status of the NetApp fans reported by the SNMP agent.

GlobalStatus For NetApp hosts managed via SNMP agents. This service checks the NetApp Global Status reported by the SNMP agent.

Power For NetApp hosts managed via SNMP agents. This service checks the status of the NetApp power supplies reported by the SNMP agent.

RAIDStatus For NetApp hosts managed via SNMP agents. This service checks the NetApp RAID status reported by the SNMP agent.

VolumeStatus For NetApp hosts managed via SNMP agents. This service checks the NetApp volume status reported by the SNMP agent.

Alerts For NetApp hosts. When an alert is sent from the NetApp SNMP agent, it is processed by the Bull System Manager Server.

Notes

- The **netapp.mib** is integrated in the Bull System Manager application.
- Do not forget to configure the NetApp agent to send SNMP traps to the Bull System Manager Server by adding the Bull System Manager Server host address to the agent's SNMP managers list.

3.2.3.3 Reporting Indicators

A reporting indicator is defined for the CPU load of the NetApp storage system. It gets values from the corresponding monitoring service.

Indicator applied to the NetApp Host

Indicator	Corresponding Service
<NetApp_host>_CPULoad	CPULoad

Table 3-8. NetApp Host indicator

3.2.3.4 Nagios check commands

check-netapp-cpuload (any OS) Nagios command

The Bull System Manager service check command syntax is:

```
check_snmp -C public -o .1.3.6.1.4.1.789.1.2.1.3.0 -w 90 -c 95 -u '%' -l
"CPU LOAD"
```

See the **check-netapp-cpuload** command in *Chapter 4* for details.

check-netapp-numdisks (any OS) Nagios command

The Bull System Manager service check command syntax is:

```
check_snmp -C public -o .1.3.6.1.4.1.789.1.6.4.1.0,
.1.3.6.1.4.1.789.1.6.4.2.0, .1.3.6.1.4.1.789.1.6.4.8.0,
.1.3.6.1.4.1.789.1.6.4.7.0 -u 'Total Disks','Active','Spare','Failed' -l
""
```

See the **check-netapp-numdisks** command in *Chapter 4* for details.

check-netapp-failedfans (any OS) Nagios command

The Bull System Manager service check command syntax is:

```
check_snmp -C public -o .1.3.6.1.4.1.789.1.2.4.3.0 -l "Fans"
```

See the **check-netapp-failedfans** command in *Chapter 4* for details.

check_netapp_globalstatus (any OS) Nagios command

The configurable Bull System Manager service check command syntax is:

```
check_NetAppGlobalStatus!<community>!<port>!<timeout>
```

See the **check_netapp_globalstatus** command in *Chapter 4* for parameter details.

Default syntax for **NetApp.GlobalStatus**: (the service name as defined in Nagios configuration based on the category name and service name defined in BSM configuration)

```
check_ NetAppGlobalStatus!public!161!60
```

check-netapp-failedpwr (any OS) Nagios command

The Bull System Manager service check command syntax is:

```
check_snmp -C public -o .1.3.6.1.4.1.789.1.2.4.5.0 -l "Power"
```

See the **check-netapp-failedpwr** command in *Chapter 4* for details.

check_netappraid (any OS) Nagios command

The configurable Bull System Manager service check command syntax is:

```
check_NetAppRaid!<community>!<port>!<timeout>
```

See the **check_netappraid** command in *Chapter 4* for parameter details.

Default syntax for **NetApp.RAIDStatus**: (the service name as defined in Nagios configuration based on the category name and service name defined in BSM configuration)

```
check_NetAppRaid!public!161!60
```

check_netappvol (any OS) Nagios command

The configurable Bull System Manager service check command syntax is:

```
check_NetAppVol!<community>!<port>!<timeout>
```

See the **check_netappvol** command in *Chapter 4* for parameter details.

Default syntax for **NetApp.VolumeStatus**: (the service name as defined in Nagios configuration based on the category name and service name defined in BSM configuration)

```
check_NetAppVol!public!161!60
```

3.2.3.5 Bull System Manager Configuration

NetApp configuration for Bull System Manager is available from the configuration GUI by selecting **Topology** → **StoreWay hosts** → **NetApps**.

To edit a NetApp, select **Edit**.

To define a new NetApp in the Bull System Manager configuration database, click the **New NetApp** button and initialize the following attributes:

StoreWay NetApp name	name of the NetApp
description	description
network name	bay netname
SNMP port number	SNMP port number
SNMP community	SNMP community

3.2.4 BSMStoreWayDPA (StoreWay DPA Management)

The corresponding Bull System Manager Add-on creates monitoring links between Bull System Manager and the StoreWay DPA SNMP agent and WEB GUI.

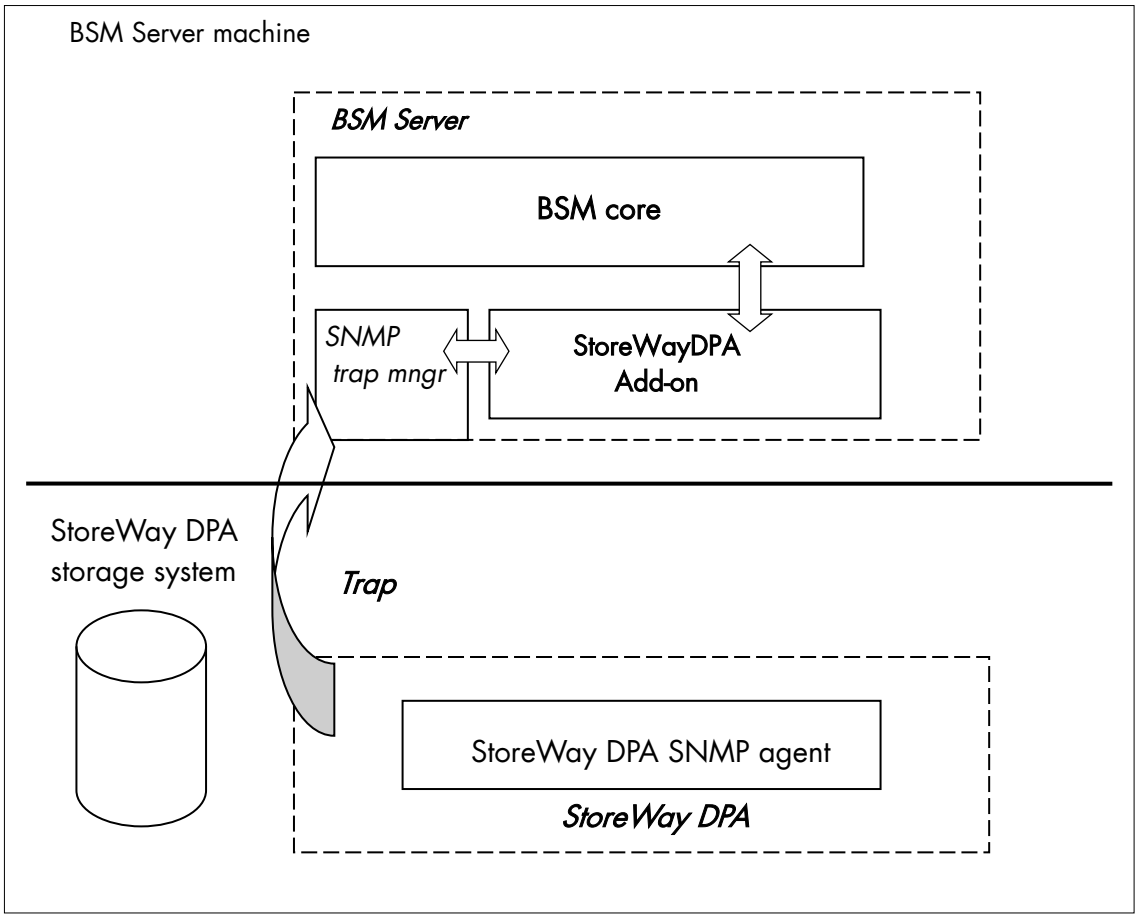


Figure 3-17. StoreWayDPA Monitoring Components

3.2.4.1 Default Categories & Services (independent of OS type)

Targeted OS	Model	Category	Service	Check command
Any	bayStoreWayDPA	StoreWayDPA	Alerts	No check (SNMP trap receiver)
			TaskStatus	check_StoreWayDPA

Table 3-9. StoreWayDPA monitoring services

Note This category is based on the StoreWay DPA SNMP agent. This SNMP interface is a requirement for the StoreWayDPA monitoring services.

3.2.4.2 StoreWayDPA Category

TaskStatus For StoreWay DPA hosts managed via its SNMP agent. This service checks the StoreWay DPA Backup Engine and Task Launcher status reported by the SNMP agent.

Alerts For StoreWay DPA hosts. When an alert is sent from the StoreWay DPA SNMP agent, it is processed by the Bull System Manager Server.

Notes

- The **storewaydpa.mib** is integrated in the Bull System Manager application.
- Do not forget to configure the StoreWay DPA agent to send SNMP traps to the Bull System Manager Server by adding the Bull System Manager Server host address to the agent's SNMP managers list.

3.2.4.3 Nagios check commands

Check_StoreWayDPA (any OS) Nagios command

The Bull System Manager service check command syntax is:

```
check_StoreWayDPA!<community>!<port>!<timeout>
```

See the **check_ StoreWayDPA** command in *Chapter 4* for parameter details.

Default syntax for **StoreWayDPA.TaskStatus** (the service name as defined in Nagios configuration based on the category name and service name defined in BSM configuration)

```
check_ StoreWayDPA!public!161!60
```

3.2.4.4 Bull System Manager Configuration

StoreWayDPA configuration for Bull System Manager is available from the configuration GUI by selecting **Topology** → **StoreWay hosts** → **StoreWayDPAs**.

To edit a StoreWayDPA, select **Edit**.

To define a new StoreWayDPA in the Bull System Manager configuration database, click the **New StoreWay DPA** button and initialize the following attributes:

StoreWay StoreWay DPA name	name of the StoreWay DPA
description	description
network name	bay netname
SNMP port number	SNMP port number
SNMP community	SNMP community

3.2.5 BSM SwitchBrocade (Brocade Fibre Channel Switch Management)

The corresponding Bull System Manager Add-on creates monitoring links between Bull System Manager and the Brocade Fibre Channel Switch SNMP agent and WEB GUI.

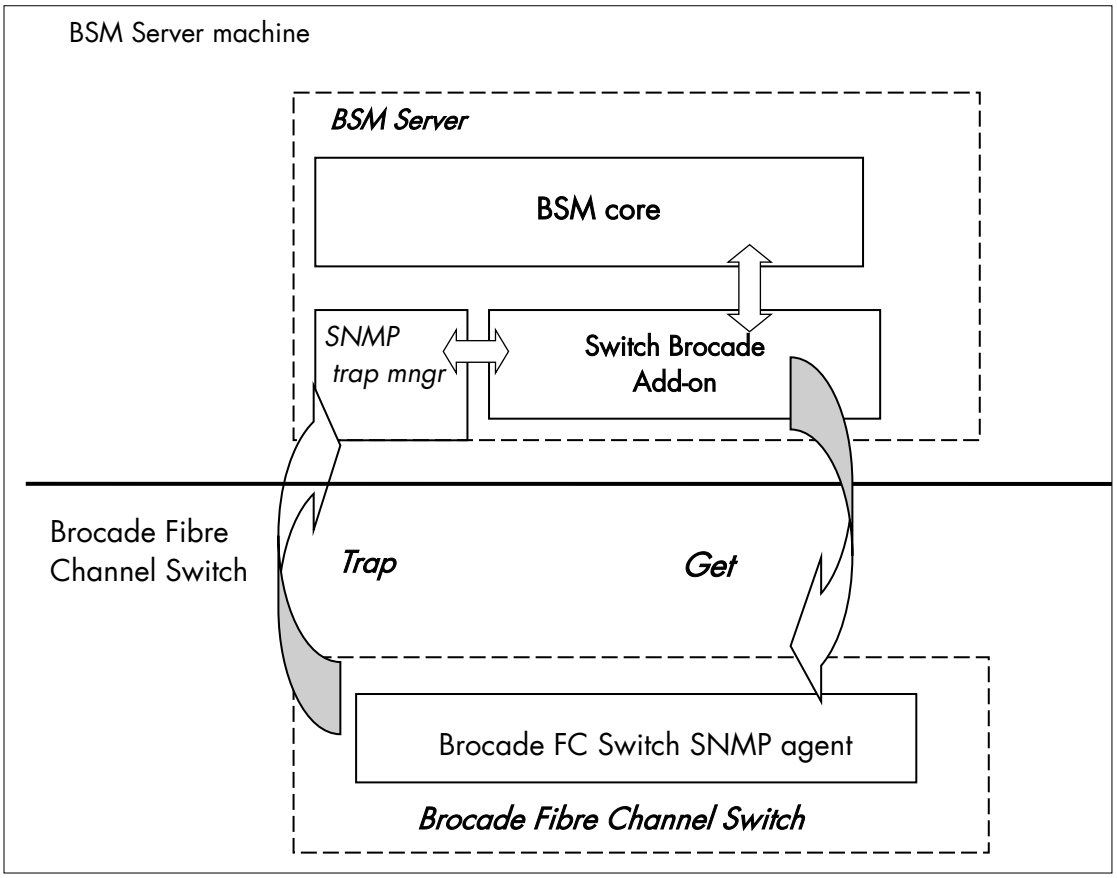


Figure 3-18. Brocade Fibre Channel Switch Monitoring Components

3.2.5.1 Default Categories & Services (independent of OS type)

Targeted OS	Model	Category	Service	Check_command
Any	Any	Brocade	Alerts	No check (SNMP trap receiver)
			FC-Hardware	check_brocade_hw
			Status	check_brocade
			Ports	check_brocade

Table 3-10. Default Brocade Fibre Channel Switch monitoring services

Note This category is based on the Brocade Fibre Channel Switch SNMP agent. This SNMP interface is a requirement for the optional Brocade Fibre Channel Switch monitoring services.

3.2.5.2 Optional Categories & Services (independent of OS type)

Targeted OS	Model	Category	Service	Check_command
Any	Any	Brocade	Portx	check_brocade_port
Any	Any	Brocade_Sensors	Fans	check_brocade
			Temp	check_brocade

Table 3-11. Optional Brocade Fiber Channel Switch monitoring services

Note This category is based on the Brocade Fibre Channel Switch SNMP agent. This SNMP interface is a requirement for the optional Brocade Fibre Channel Switch monitoring services.

3.2.5.3 Brocade Category

Status For Switch Brocade hosts managed via its SNMP agent. This service checks the Brocade Fiber Channel Switch global status reported by the SNMP agent.

Ports For Switch Brocade hosts managed via its SNMP agent. This service checks **all** Brocade Fiber Channel Switch **ports global status** reported by the SNMP agent.

Portx For Switch Brocade hosts managed via its SNMP agent. This service checks **one** Brocade Fiber Channel Switch **port status** reported by the SNMP agent.

FC_Hardware For Switch Brocade hosts managed via its SNMP agent. This service checks the Brocade Fiber Channel Switch **sensors status and values** reported by the SNMP agent.

Alerts For Switch Brocade hosts. When an alert is sent from the Brocade Fibre Channel Switch SNMP agent, it is processed by the Bull System Manager Server.

Notes

- The SW-MIB.mib and SW-TRAP.mib files are integrated in the Bull System Manager application.
- Do not forget to configure the Brocade Fibre Channel Switch SNMP agent to send SNMP traps to the Bull System Manager Server by adding the Bull System Manager host address to the agent's SNMP manager list.

3.2.5.4 Brocade_Sensors Category

Fans For SwitchBrocade hosts managed via SNMP agents. This service checks each Brocade Fibre Channel Switch fan status reported by the SNMP agent.

Temp For SwitchBrocade hosts managed via SNMP agents. This service checks each Brocade Fibre Channel Switch temperature sensor status reported by the SNMP agent.

3.2.5.5 Nagios check commands

check_brocade (any OS) Nagios command

The Bull System Manager service check command syntax is:

check_brocade!<sensor>

Values available for <sensor> are:
- switch
- port
- fan
- temp

See the **check_brocade** command in *Chapter 4* for parameter details.

For HOSTADDRESS, SNMP community and SNMP port parameters, the Nagios macros $HOSTADDRESS$, $_HOSTSNMP_COMMUNITY$ and $_HOSTSNMP_PORT$ are used.

check_brocade_hw (any OS) Nagios command

The Bull System Manager service check command syntax is:

check_brocade_hw

See the **check_brocade_hw** command in *Chapter 4* for parameter details.

For HOSTADDRESS, SNMP community and SNMP port parameters, the Nagios macros $HOSTADDRESS$, $_HOSTSNMP_COMMUNITY$ and $_HOSTSNMP_PORT$ are used.

check_brocade_port (any OS) Nagios command

The Bull System Manager service check command syntax is:

check_brocade!port!<portnb>

Value available for <portnb> is the number of any Brocade Fibre Channel Switch port.

See the **check_brocade_port** command in *Chapter 4* for parameter details.

For HOSTADDRESS, SNMP community and SNMP port parameters, the Nagios macros $HOSTADDRESS$, $_HOSTSNMP_COMMUNITY$ and $_HOSTSNMP_PORT$ are used.

3.2.5.6 Bull System Manager Configuration

SwitchBrocade configuration for Bull System Manager is available from the configuration GUI by selecting **Topology** → **StoreWay hosts** → **SwitchBrocade**.

To edit a SwitchBrocade, select **Edit**.

To define a new SwitchBrocade in the Bull System Manager configuration database, click the **New SwitchBrocade** button and initialize the following attributes:

Switch Brocade name	name of the Brocade Fibre Channel Switch
description	description
network name	bay netname
SNMP port number	SNMP port number
SNMP community	SNMP community

3.2.5.7 Configuration of Optional Brocade_Sensors Category

The configuration of the optional Brocade_Sensors category for SwitchBrocade hosts is available from the configuration GUI by selecting **Supervision** > **Monitoring** > **Categories/Services-> manage categories**.

This opens a new Window. Select **Add from an unused category template** and check the **Brocade_Sensors** category. Then click on **Add from the selected category**.

Add the SwitchBrocade hosts to the hostlist and click on **OK**. Validate the new configuration by clicking on **Save & Reload**.

3.2.5.8 Configuration of Optional Portx Service

The configuration of the optional service Portx from Brocade category for SwitchBrocade hosts is available from the configuration GUI.

1. Select **Supervision > Monitoring > Categories/Services**.

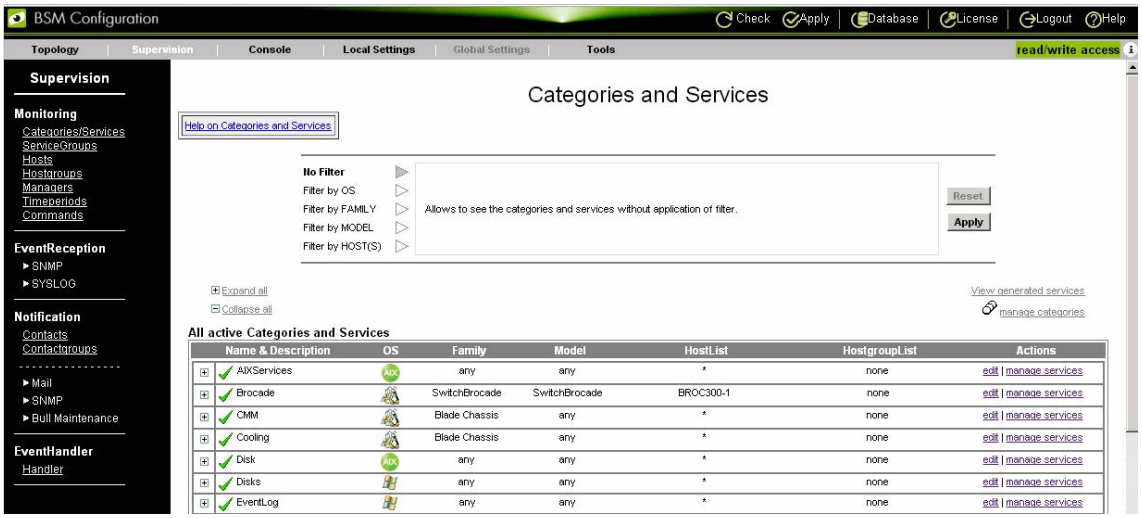


Figure 3-19. Brocade category selection

2. Select **manage services** corresponding to the Brocade category.

This opens a new Window.

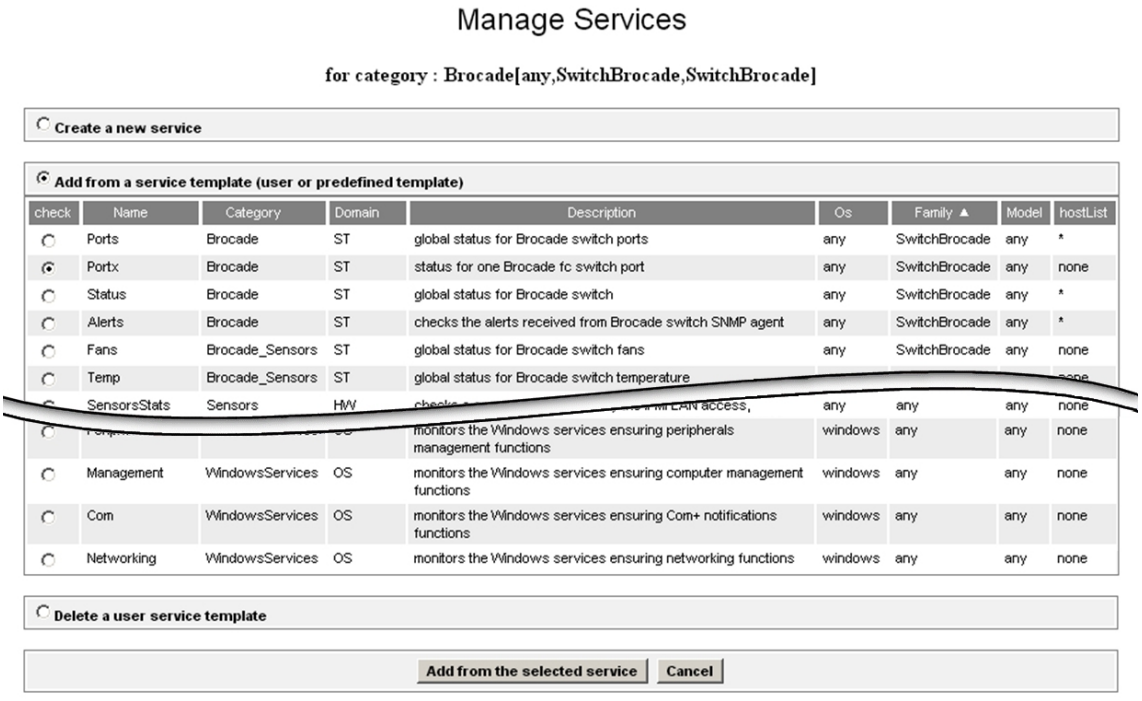


Figure 3-20. Portx service selection

3. Select **Add from an unused service template**.
4. Check the **Portx** service.
5. Click on **Add from the selected service** at the bottom of this window.

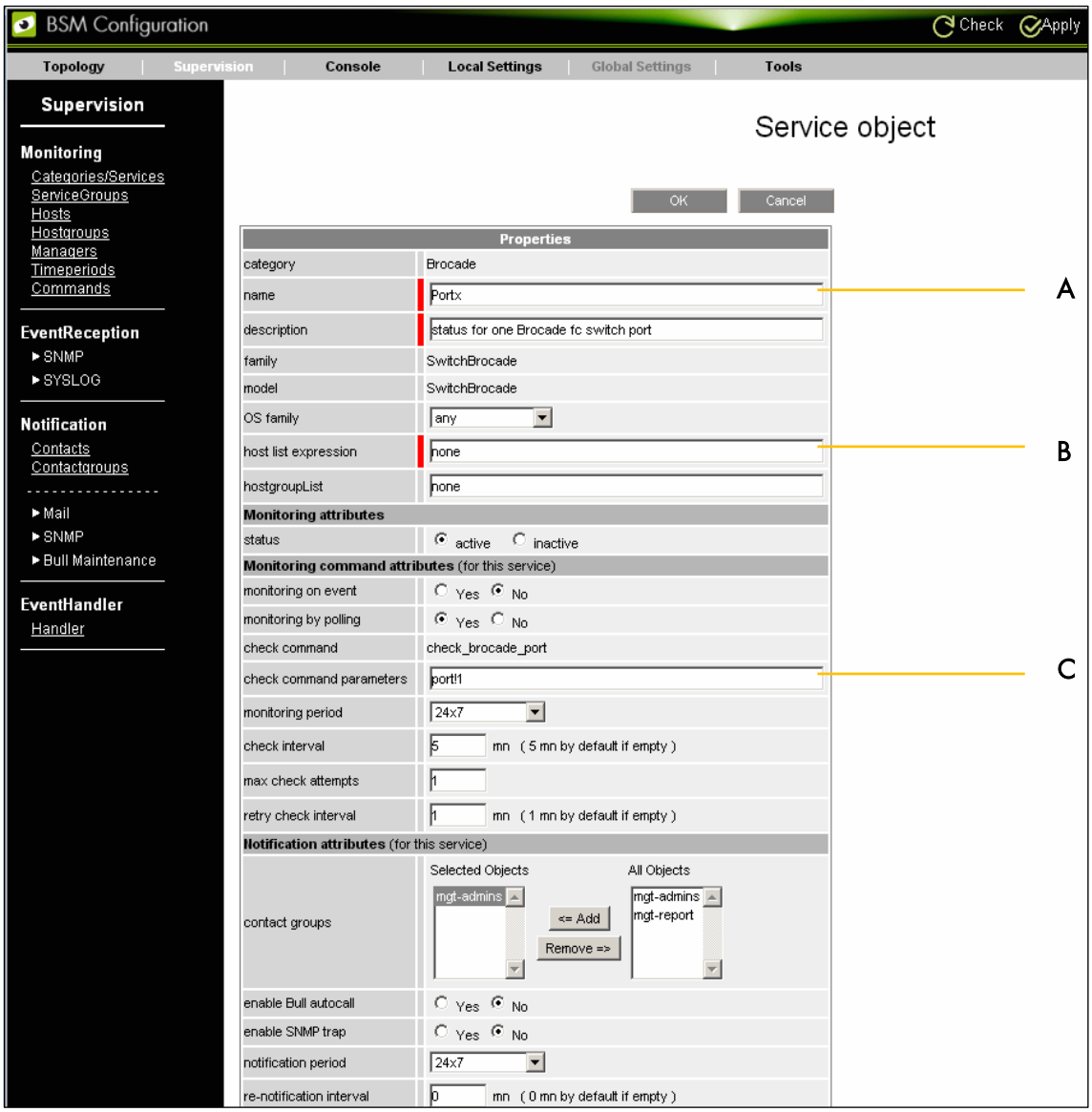


Figure 3-21. Portx service configuration

6. Modify the **service name (A)** by replacing the 'x' by the switch port number to monitor.
7. Add the SwitchBrocade host to the **hostlist (B).**
8. Replace the second **check command parameter (C)** by the switch port number to monitor.
9. Click **OK**.
10. Validate the new configuration by clicking on **Apply.**

3.3 External Device Server Add-ons

The following Add-ons are used for monitoring external devices.

3.3.1 BSM WaterCooledDoor (Water Cooled Door Management)

The corresponding Bull System Manager Add-on creates monitoring links between Bull System Manager and the Baseboard Management Controller of the Bull Water Cooled Door device and its web GUI.

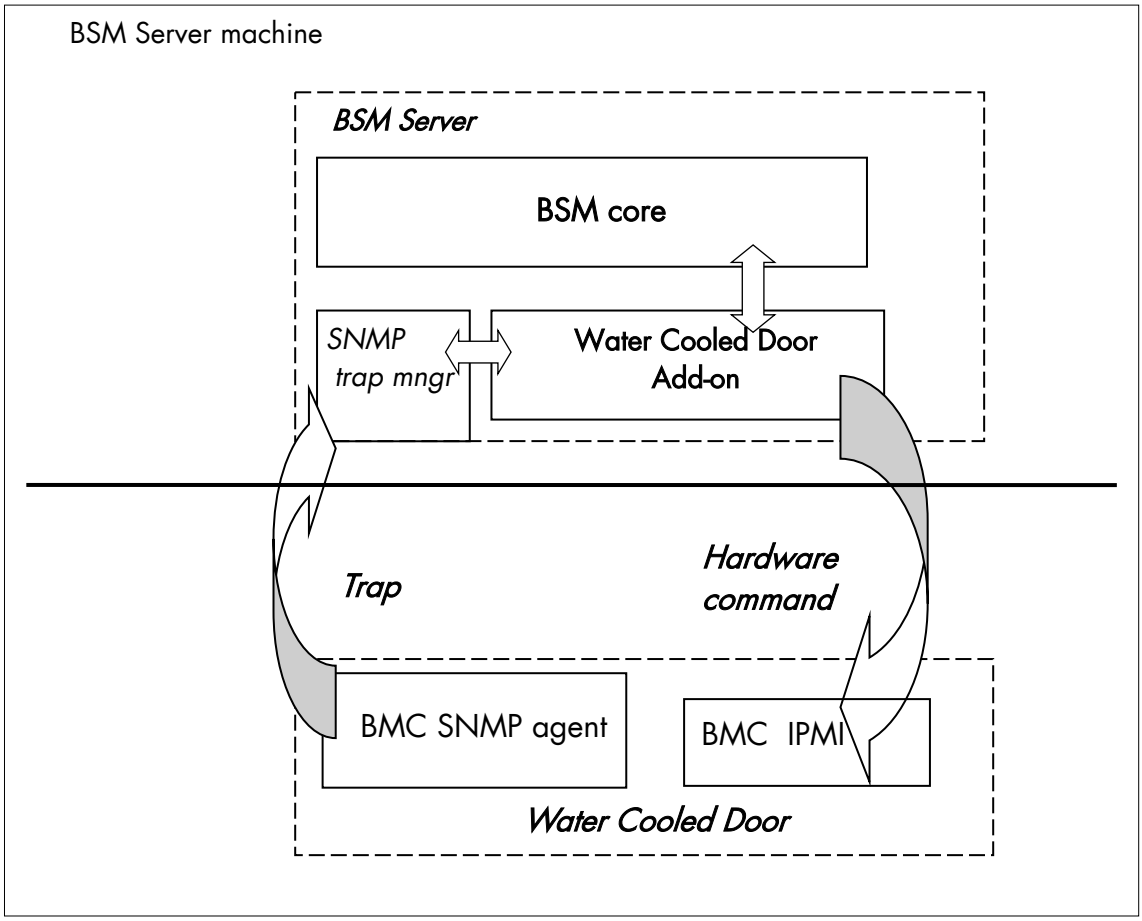


Figure 3-22. Water Cooled Door Monitoring Components

3.3.1.1 Default Categories & Services (independent of OS type)

Targeted OS	Model	Category	Service	Check command
any	devWaterCooledDoor	Hardware	Alerts	No check (SNMP trap receiver)
			CoolingStatus	check_wcd_coolstatus
		Power	PowerStatus	check_IPMI_powerstatus
		Sensors	CurrentPower	check_IPMI_sensor
			DeltaPressure	check_pressure
			TemperatureAverage	check_IPMI_sensor
			ValveAperture	check_IPMI_sensor

Table 3-12. Default Water Cooled Door monitoring services

3.3.1.2 Optional Categories & Services (independent of OS type)

Targeted OS	Model	Category	Service	Check command
any	devWaterCooledDoor	Sensors	OutputTemperature	check_IPMI_sensor
			FanSpeed	check_IPMI_sensor

Table 3-13. Optional Water Cooled Door monitoring services

Note These categories are based on the IPMI Hardware commands. The IPMI interface is a requirement for the WaterCooledDoor monitoring services.

3.3.1.3 Hardware Category

CoolingStatus For WaterCooledDoor hosts managed via IPMI Hardware commands. This service checks the WaterCooledDoor cooling status reported by the BMC.

Alerts For WaterCooledDoor hosts. When an alert is sent from the WaterCooledDoor SNMP agent, it is processed by the Bull System Manager Server.

Note The **WaterCooledDoorMIB.mib** is integrated in the Bull System Manager application. The Alerts service inherits also from the **bmclanpet.mib**, which is also integrated in the Bull System Manager application.

3.3.1.4 Power Category

PowerStatus For WaterCooledDoor hosts managed via **IPMI** hardware commands. This service checks the WaterCooledDoor power status reported by the BMC.

3.3.1.5 Sensors Category

CurrentPower For WaterCooledDoor hosts managed via IPMI Hardware commands. This service checks the power consumption of the WaterCooledDoor reported by the BMC.

DeltaPressure For WaterCooledDoor hosts managed via IPMI Hardware commands. This service checks the in/out pressure difference of the water circuit of the WaterCooledDoor reported by the BMC.

TemperatureAverage For WaterCooledDoor hosts managed via IPMI Hardware commands. This service checks the temperature average of the different temperature sensors of the WaterCooledDoor reported by the BMC.

ValveAperture For WaterCooledDoor hosts managed via IPMI Hardware commands. This service checks the cooled water circuit valve aperture reported by the BMC.

OutputTemperature For WaterCooledDoor hosts managed via IPMI Hardware commands. This service checks one of the external temperature sensors of the WaterCooledDoor reported by the BMC.

FanSpeed For WaterCooledDoor hosts managed via IPMI Hardware commands. This service checks the speed of one upon several fans reported by the BMC.

Note Do not forget to configure the BMC's SNMP agent to send SNMP traps to the Bull System Manager Server by adding the BSM Server host address to the SNMP managers list.

3.3.1.6 Reporting Indicators

Performance indicators are defined for the monitoring services of APC Power Distribution Unit listed below. They get values from the corresponding monitoring service. Performance indicators are collected by analyzing performance data provided by Nagios plug-in with PNP4Nagios.

PNP4Nagios is delivered as a BSM Server Extension and its installation is optional.

Indicators applied to the WaterCooledDoor Host

Indicator	Corresponding Service
<WaterCooledDoor_host>_CurrentPower (watts)	Sensors.CurrentPower
<WaterCooledDoor_host>_DeltaPressure (Pa)	Sensors.DeltaPressure
<WaterCooledDoor_host>_TemperatureAverage (degrees C)	Sensors.TemperatureAverage
<WaterCooledDoor_host>_ValveAperture (%)	Sensors.ValveAperture
<WaterCooledDoor_host>_FanSpeed (RPM)	Sensors.FanSpeed
<WaterCooledDoor_host>_OutputTemperature (degrees C)	Sensors.OutputTemperature

Table 3-14. Water Cooled Door Host Indicators

3.3.1.7 Nagios check commands

check_IPMI_powerstatus (any OS) Nagios command

The Bull System Manager service check command syntax is:

```
check_IPMILAN_powerstatus
```

See the **check_IPMI_powerstatus** command in *Chapter 4* for details.

check_pressure (any OS) Nagios command

The Bull System Manager service check command syntax is:

```
check_sensor!'Air Pressure'
```

See the **check-sensor** command in *Chapter 4* for details.

check_IPMI_sensor (any OS) Nagios command

The configurable Bull System Manager service check command syntax is:

```
check_sensor!<sensor>
```

See the **check_sensor** command in *Chapter 4* for parameter details.

3.3.1.8 Bull System Manager Configuration

The WaterCooledDoor configuration for Bull System Manager is available from the configuration GUI by selecting **Topology** > **Device hosts** > **WaterCooledDoors**.

To edit a **WaterCooledDoor**, select **Edit**.

To define a new **WaterCooledDoor** in the Bull System Manager configuration database, click the **New Water Cooled Door** button and initialize the following attributes:

Water Cooled Door name	Name of the **Water Cooled Door**
description	Description
network name	Address IP of Water Cooled Door's BMC
user	User name to access the BMC
password	Password associated to the user name

3.3.2 BSM PDU-APC (APC Power Distribution Unit Management)

The corresponding Bull System Manager Add-on creates monitoring links between Bull System Manager and the APC Power Distribution Unit SNMP agent and WEB GUI.

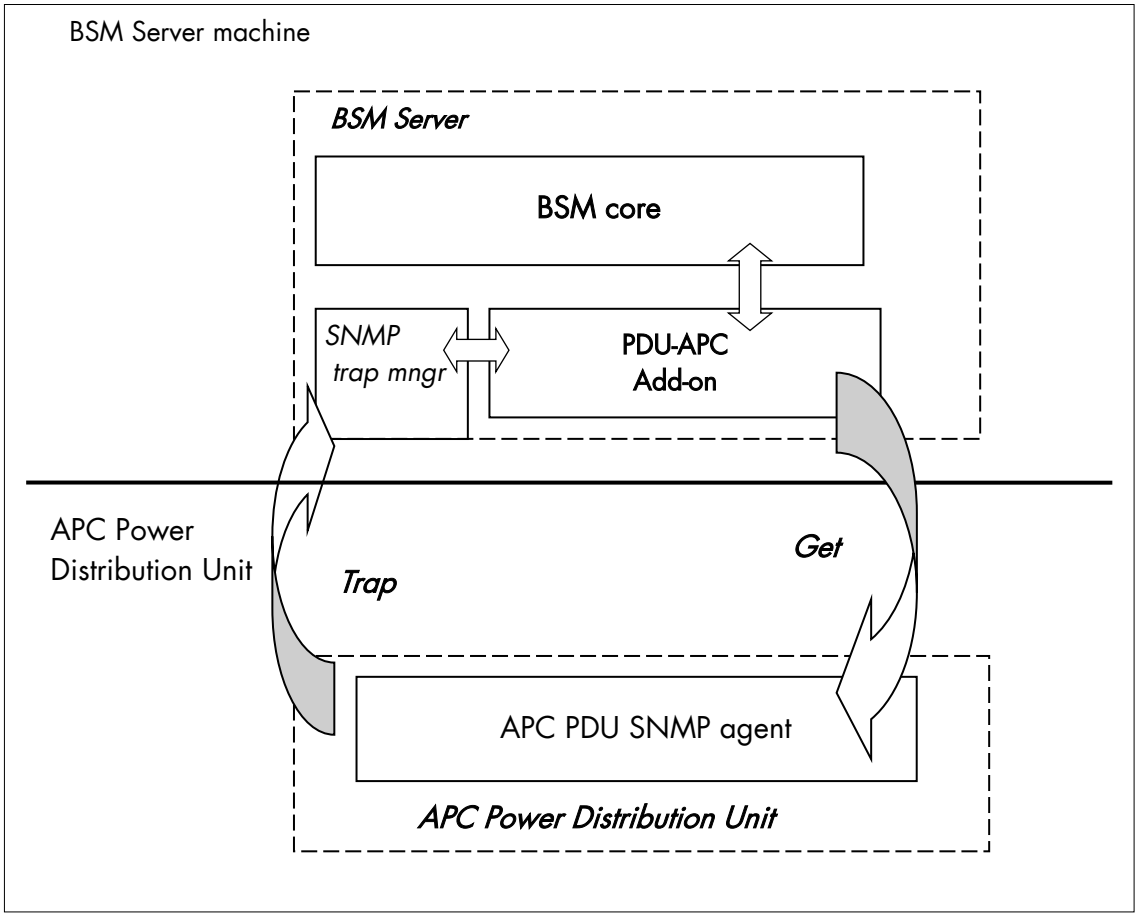


Figure 3-23 APC Power Distribution Unit Monitoring Components

3.3.2.1 Default Categories & Services (independent of OS type)

Targeted OS	Model	Category	Service	Check command
Any	devPDUAPC	PDUAPC	Alerts	No check (SNMP trap receiver)
			Status	check_pduapc_status
		Power	Consumption	check_pduapc_pwr_consumption
			Outlets	check_pduapc_outlets

Table 3-15. Default APC Power Distribution Unit monitoring services

Note This category is based on the APC Power Distribution Unit SNMP agent. This SNMP interface is a requirement for the default APC Power Distribution Unit monitoring services.

3.3.2.2 PDUAPC Category

Alerts For APC PDU hosts. When an alert is sent from the APC PDU SNMP agent, it is processed by the Bull System Manager Server.

Status For APC PDU hosts managed via its SNMP agent. This service checks the APC PDU power supplies status reported by the SNMP agent.

Notes

- The **powernet398.mib** file are integrated in the Bull System Manager application. The trap severity SEVERE was changed to CRITICAL.
- Do not forget to configure the APC PDU SNMP agent to send SNMP traps to the Bull System Manager Server by adding the Bull System Manager Server host address to the agent's SNMP managers list.

3.3.2.3 Power Category

Consumption For APC PDU hosts managed via SNMP agents. This service checks the global power consumption (in Watts) for each APC PDU.

Outlets For APC PDU hosts managed via SNMP agents. This service checks each APC PDU outlet status reported by the SNMP agent.

3.3.2.4 Performance Indicators

Performance indicators are defined for the monitoring services of APC Power Distribution Unit listed below. They get values from the corresponding monitoring service. Performance indicators are collected by analyzing performance data provided by Nagios plug-in with PNP4Nagios.

PNP4Nagios is delivered in as BSM Server Extension and its installation is optional.

Indicators	Corresponding Service
watts	Power.Consumption

Table 3-16. Performance Indicators applied to the APC PDU Host

3.3.2.5 Nagios check commands

check_PDUAPC (any OS) Nagios command

The Bull System Manager service check command syntax is:

`check_PDUAPC!<action>!`

Values available for <action> are:

- Status
- Consumption
- Outlets

See the **check_ PDUAPC** command in *Chapter 4* for parameter details.

For HOSTADDRESS, SNMP community and SNMP port parameters, the Nagios macros $HOSTADDRESS$, $_HOSTSNMP_COMMUNITY$ and $_HOSTSNMP_PORT$ are used.

3.3.2.6 Bull System Manager Configuration

APC PDU configuration for Bull System Manager is available from the configuration GUI by selecting **Topology** → **Device hosts** → **PDUAPC**.

To edit a PDUAPC, select **Edit**.

To define a new PDUAPC in the Bull System Manager configuration database, click the New **PDUAPC** button and initialize the following attributes:

PDUAPC name	name of the APC power Distribution Unit
description	description
network name	bay netname
SNMP port number	SNMP port number
SNMP community	SNMP community

3.3.3 BSM iPDU (intelligent Power Distribution Unit Management)

The corresponding Bull System Manager Add-on creates monitoring links between Bull System Manager and the intelligent Power Distribution Unit SNMP agent and WEB GUI.

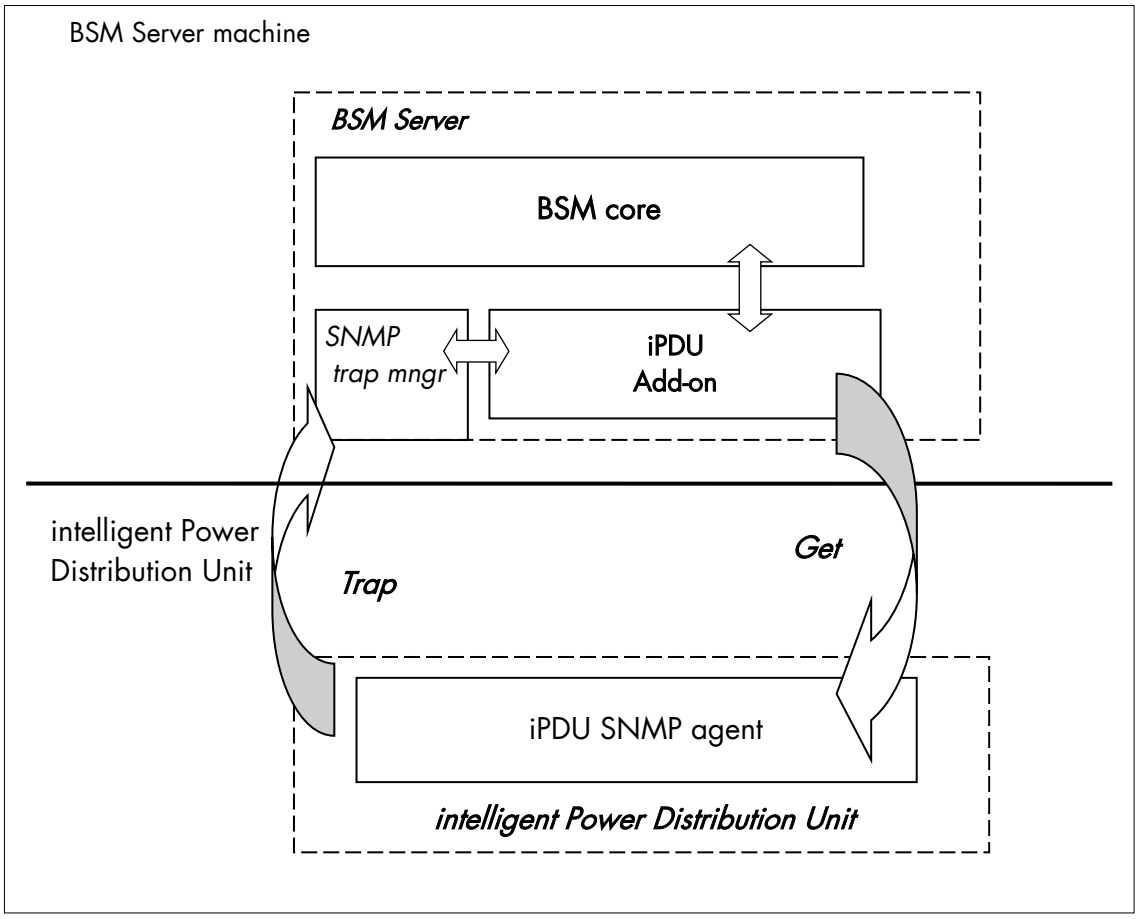


Figure 3-24 intelligent Power Distribution Unit Monitoring Components

3.3.3.1 Default Categories & Services (independent of OS type)

Targeted OS	Model	Category	Service	Check command
Any	IPDU	IPDU	Alerts	No check (SNMP trap receiver)
			Status	check_ipdu_status
		Power	Consumption	check_ipdu_pwr_consumption
			Outlets_Conso	check_ipdu_outlet_conso
		Environment	Temperature	check_ipdu_temperature

Table 3-17. Default intelligent Power Distribution Unit monitoring services

3.3.3.2 Optional Services (independent of OS type)

Targeted OS	Model	Category	Service	Check command
Any	IPDU	Power	Voltage	check_ipdu_voltage)
			Outlets_Voltage	check_ipdu_outlet_volt
		Environment	Humidity	check_ipdu_humidity

Table 3-18. Optional intelligent Power Distribution Unit monitoring services

Note These categories are based on the intelligent Power Distribution Unit SNMP agent. The SNMP interface is a requirement for the default and optional intelligent Power Distribution Unit monitoring services.

3.3.3.3 IPDU Category

Alerts For IPDU hosts. When an alert is sent from the intelligent PDU SNMP agent, it is processed by the Bull System Manager Server.

Status For IPDU hosts managed via its SNMP agent. This service checks the intelligent PDU status reported by the SNMP agent.

Notes

- The **hdpduv0_91_Linux.mib** file is integrated in the Bull System Manager application.
- Do not forget to configure the intelligent PDU SNMP agent to send SNMP traps to the Bull System Manager Server by adding the Bull System Manager Server host address to the agent's SNMP managers list.

3.3.3.4 Power Category

Consumption For intelligent PDU hosts managed via SNMP agents. This service checks the global power consumption (in Watts) for each intelligent PDU.

Outlets_Conso For intelligent PDU hosts managed via SNMP agents. This service checks each intelligent PDU outlet consumption (in Watts) reported by the SNMP agent.

Optional services

Voltage For intelligent PDU hosts managed via SNMP agents. This service checks the input and output voltage and frequency for each intelligent PDU.

Outlets_Voltage For intelligent PDU hosts managed via SNMP agents. This service checks the output voltage of each outlet of an intelligent PDU reported by the SNMP agent.

3.3.3.5 Environment Category

Temperature For intelligent PDU hosts managed via SNMP agents. This service checks the temperature for each intelligent PDU.

Optional services

Humidity For intelligent PDU hosts managed via SNMP agents. This service checks the humidity for each intelligent PDU.

3.3.3.6 Performance Indicators

Performance indicators are defined for the monitoring services of intelligent Power Distribution Unit listed below. These obtain values from the corresponding monitoring services. Performance indicators are collected by analyzing performance data provided by Nagios plug-in with PNP4Nagios.

PNP4Nagios is delivered in as BSM Server Extension and its installation is optional.

Indicators	Corresponding Service
watts, Wh	Power.Consumption
Outlet<n>_watts Outlet<n>_Wh	Power.Outlets_Conso
inputVolt, inputFrequency outputVolt, outputFrequency	Power.Voltage
Outlet<n>_volt, Outlet<n>_frequency	Power.Outlets_Voltage
Temperature	Environment.Temperature
Humidity	Environment.Humidity

Table 3-19. Performance Indicators applied to the IPDU Host

3.3.3.7 Nagios check commands

`check_IPDU` (any OS) Nagios command

The Bull System Manager service check command syntax is:

`check_IPDU!<action>!<timeout>`

Values available for <action> are:

- Status
- Consumption
- OutletsConso
- OutletsVoltage
- Voltage
- Temperature
- Humidity

See the **check_ IPDU** command in *Chapter 4* for parameter details.

For HOSTADDRESS, SNMP community and SNMP port parameters, the Nagios macros $HOSTADDRESS$, $_HOSTSNMP_COMMUNITY$ and $_HOSTSNMP_PORT$ are used.

3.3.3.8 Bull System Manager Configuration

Intelligent PDU configuration for Bull System Manager is available from the configuration GUI by selecting **Topology** → **Device hosts** → **IPDU**.

To edit an IPDU, select **Edit**.

To define a new IPDU in the Bull System Manager configuration database, click the **New IPDU** button and initialize the following attributes:

Intelligent Power Distribution Unit name	name of the intelligent Power Distribution Unit
description	description
network name	IPDU netname
SNMP port number	SNMP port number
SNMP community	SNMP community

3.4 Virtualization Server Add-ons

The following Add-ons are used for monitoring virtual machines.

3.4.1 Overview

The Bull System Manager Server Virtualization Add-ons deliver an optional management package to manage virtual machines. A virtualization Add-on can provide:

- Supervision features to detect abnormalities and notify the corresponding defined entities.
- Administration features to perform actions on elements.

3.4.1.1 Definitions

Virtualization Add-ons use specific topology elements:

- **Native Operating System** (Native OS):
  The virtualization layer installed on a physical machine that hosts virtual machines. It is represented by a Bull System Manager host with a specific OS (specified by the Add-on).
- **Virtual Machine** (VM):
  A machine that is hosted by a native OS. It is represented by a Bull System Manager host with a specific model (specified by the Add-on).
- **Virtual Platform**:
  The set of virtual machines and native OS deployed on a physical machine.
- **Virtual Manager**:
  The interface used to manage the virtual elements.

3.4.1.2 Topology Representation

The elements of a virtual platform are displayed in the Bull System Manager Console views.

To load a specific view, click the  icon at the top of the Tree frame to select a view among available views, as shown below:

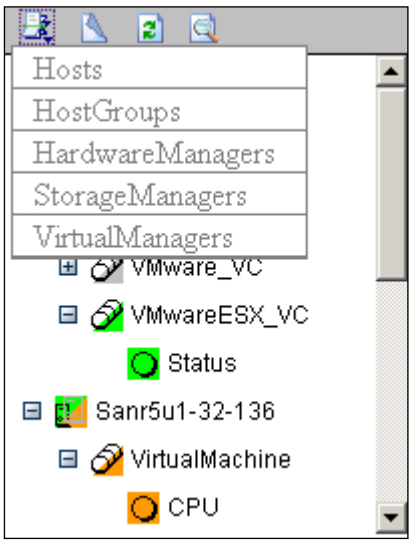


Figure 3-25. BSM Console Views

- Only the native OS and VM hosts are displayed for the **Hosts** view. VM hosts are represented with the specific icon .
- From the **Virtual Managers** view, the virtual platform is displayed as shown in the diagram below:

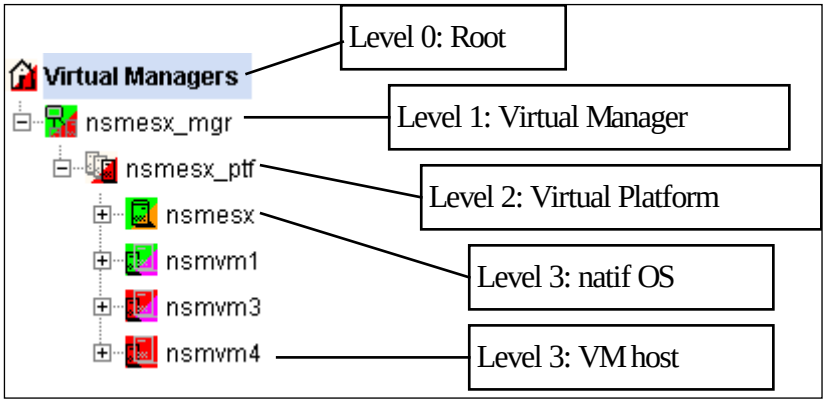


Figure 3-26. Virtual Managers view

Under the root node, the first node is the Virtual Manager that administrates the Virtual Platform. The Virtual Platform contains the native host and the VM hosts.
When you select a node, information about the elements are displayed in the Application Window.

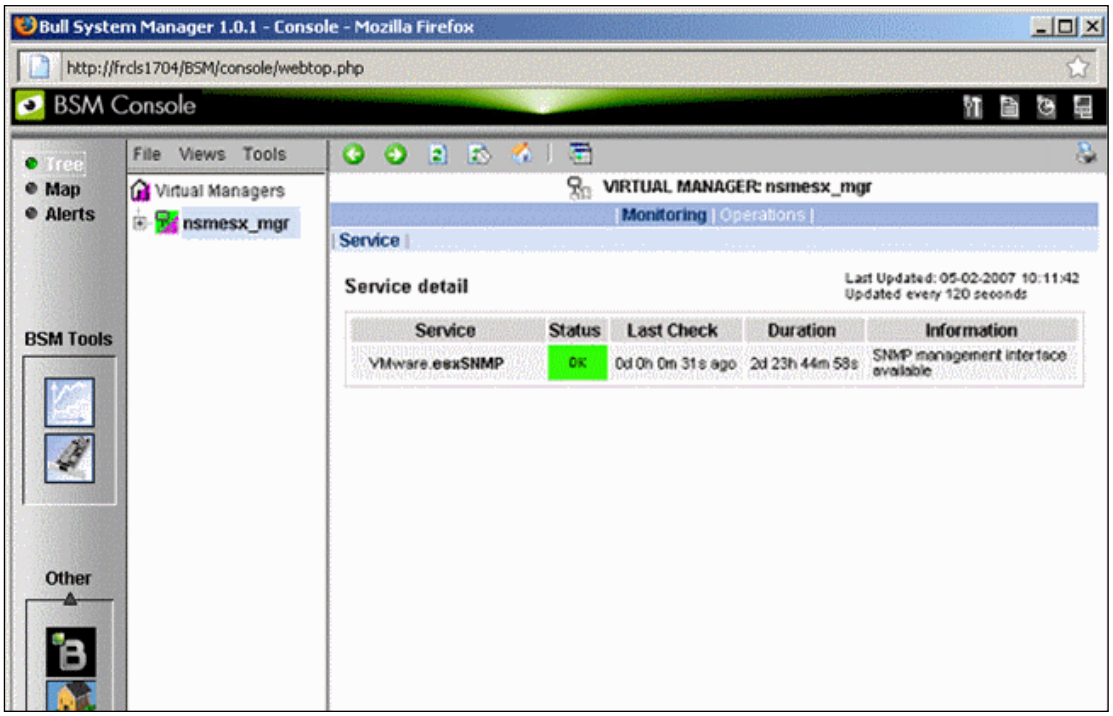


Figure 3-27. Virtual Manager Monitoring Window

3.4.2 BSMVMwareVS for managing VMware vSphere

VMware vSphere allows the management of large pools of virtualized computing infrastructures, including software and hardware. The vSphere includes several components, including the **ESX server (ESX** and **ESXi)**, a virtualization layer that abstracts processor, memory, storage and networking resources into multiple virtual machines, and the **vCenter server** that provides a central point of control for managing, monitoring, provisioning, and migrating virtual machines (VM).

The VMwareVS Add-on retrieves VM and ESX monitoring information from vCenter or ESX via the VI Perl toolkit API and allows the Web Virtual Interface to be launched from the Bull System Manager Console. It can also process trap information sent by vCenter (VirtualCenter) if the vCenter alarms are configured to send this, or by ESX if it is configured to send traps to the Bull System Manager server. For detailed information about these procedures, see the VMware Infrastructure documentations available at http://www.vmware.com/support/pubs/vi_pubs.html (for ESX3) or at http://www.vmware.com/support/pubs/vs_pubs.html. (for ESX4)

The following figure shows links between each component:

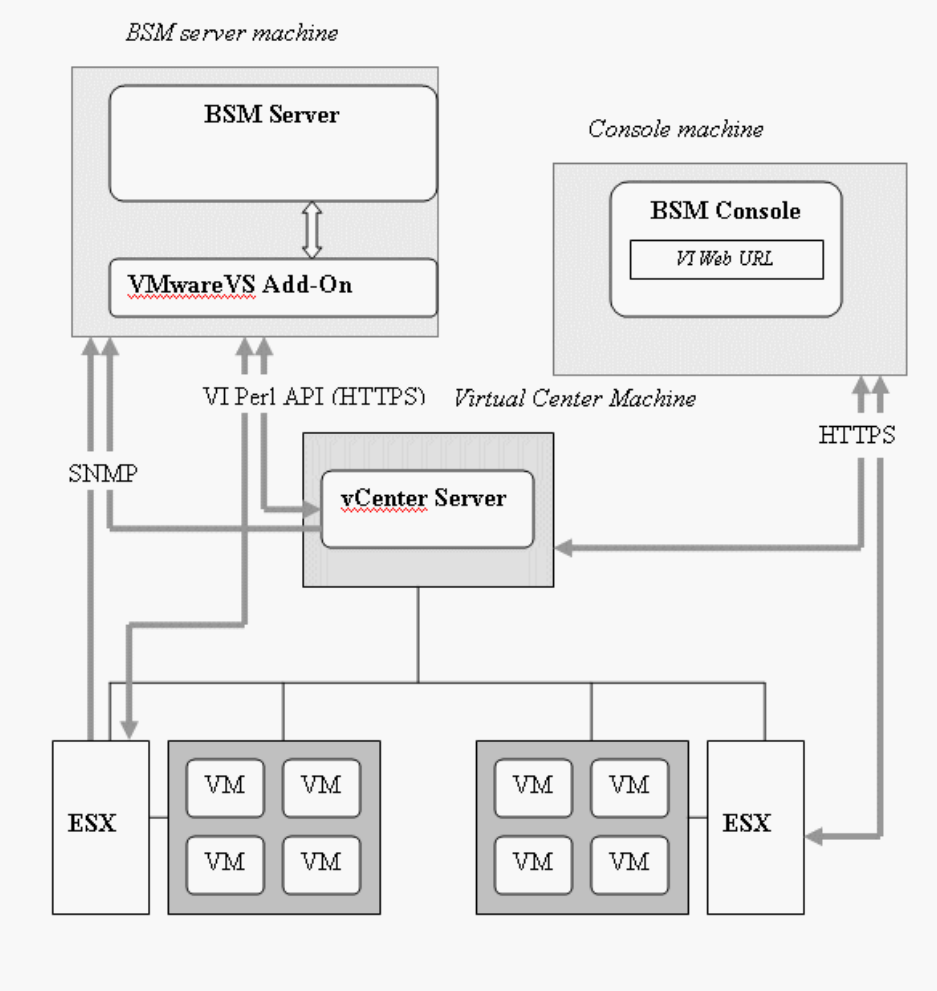


Figure 3-28. VMware Components

Important

The VMwareVS addon replaces VMwareESX and VMwareVC Add-ons.
Migration from VMwareVC to VMwareVS can be done automatically with special installation.
Migration from VMwareESX to VMwareVS also requires manual operation.

The VM and ESX elements can be monitored from an ESX server or from a vCenter application. When elements are monitored from an ESX server, they are grouped in a single BSM platform (ESX Virtual Platform).
When elements are monitored from a vCenter, they are grouped in several platforms (VMware Datacenter Platform), depending of the VMware Datacenters configuration.
Each ESX server is represented by a BSM host with the OS: **ESX**.
Each VM is represented by a BSM host with the model: **VMware**.

3.4.2.1 Configuring ESX Virtual Platform

To configure an ESX Virtual Platform, click the **VMware ESX** link in the Virtualization part of the Topology domain. The list of all configured platforms appears, as shown in the diagram below:

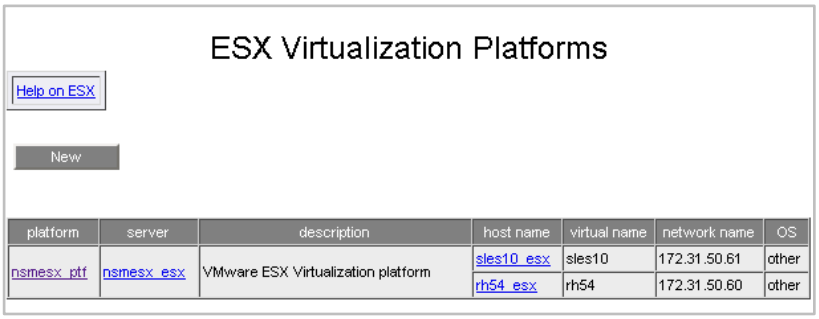


Figure 3-29. ESX Virtual Platforms page

It is possible:
- To create a new ESX Virtual Platform using the **New** button
- To edit or delete a platform using the **<platform>** link
- To edit an ESX host using the **<server>** link.
- To edit a virtual machine using the **<hostname>** link.

When you click the **New** button, the following display appears with all the resource properties:

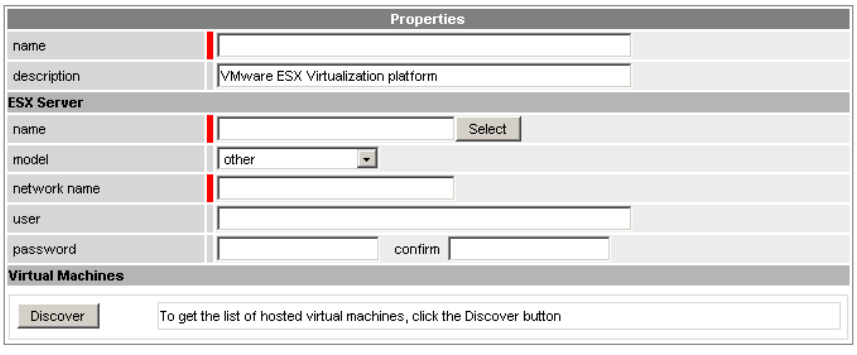


Figure 3-30. ESX Platform Properties

Besides the characteristics (name and description) of the main object, the properties of an ESX virtual platform are divided into two sections:

- **ESX Server Host**: used to define the physical machine and the native OS.
- **Virtual Machines:** used to describe the VMware ESX platform virtual machine.

ESX Server Host Properties

name	ESX host short name. This name is displayed in the Bull System Manager Console views. Click **Select** to choose a defined host from the BSM host list.
model	Host model (see the *Bull System Manager Administrator's Guide* for values).
network name	ESX host network name (hostname or IP address).
user	username used to connect ESX via the VI Perl Toolkit
password	User password

Virtual Machines Properties

Virtual Machines	List of the VMs established by selecting the VMs obtained by requests to the ESX server via the Perl API. The request is performed by clicking the **Discover** button (or **Re-discover** if in edition mode). See the complete description of the procedure below.

Note If VMs are linked to the ESX server, this could not be supervised later with the vCenter server.

Virtual Machines Discovered

Following the use of the Discover tool, the results are displayed as a table composed of three parts:

- The left column allows you to select the VMs to be associated to the platform.
- The center part displays Virtual Machine Configuration as defined on the VMware ESX server.
- 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 VM is selected. You can select a host, already defined, by clicking the **Select** button or you can create a host by completing the corresponding fields.

Note When you select a host, already defined, you cannot change its network name and OS. However, the Select contains a Default Option corresponding to the VM name that can be edited. If the VM name contains space(s), they are replaced by underscore(s) in the host label.

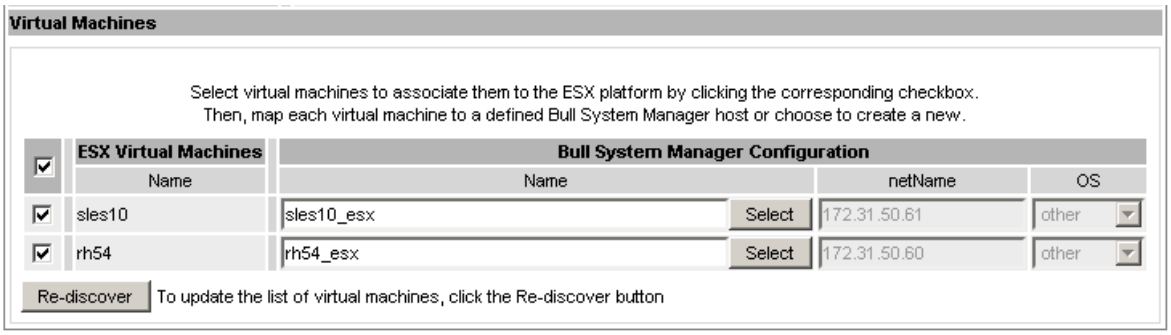


Figure 3-31. ESX Virtual Machines pane

Virtual Machines Re-Discovered

The use of the Re-discover tool is required to check that the current BSM configuration still matches the VMware ESX configuration in order to:

- Add virtual machine not yet registered in the VMware ESX Virtualization Platform
- Remove virtual machine no longer defined in the VMware ESX configuration.

During the Re-discover step, if the current configuration is not compatible with VMware ESX configuration, the invalid VMs are displayed in red and the VMs not referenced in the current BSM configuration are displayed in green.

VMs no longer defined in VMware ESX are automatically unchecked and will be removed from the list shown. New VMs must be explicitly checked to be included.

Note How to Add, Delete or Modify Virtual Machine is detailed in *Table 3-20. Related ESX Virtualization platform Objects* and *Editing Virtual Machine Set-up up*on page 70.

When the configuration has been edited:

- Click **OK** to validate your changes.
- Or click **Cancel** to return to Virtual Platforms pages without any change.
- Or click **Delete** to remove the Virtual Platform and maintain the hosts corresponding to the VMs and the VMware ESX server.
- Or click **DeleteAll** to remove the Virtual Platform and the hosts corresponding to the VMs and the VMwareESX server.

Note **Host Topology modification** require confirmation: a page listing all the modifications to be applied to the Topology configuration is displayed, as shown in the following figure.

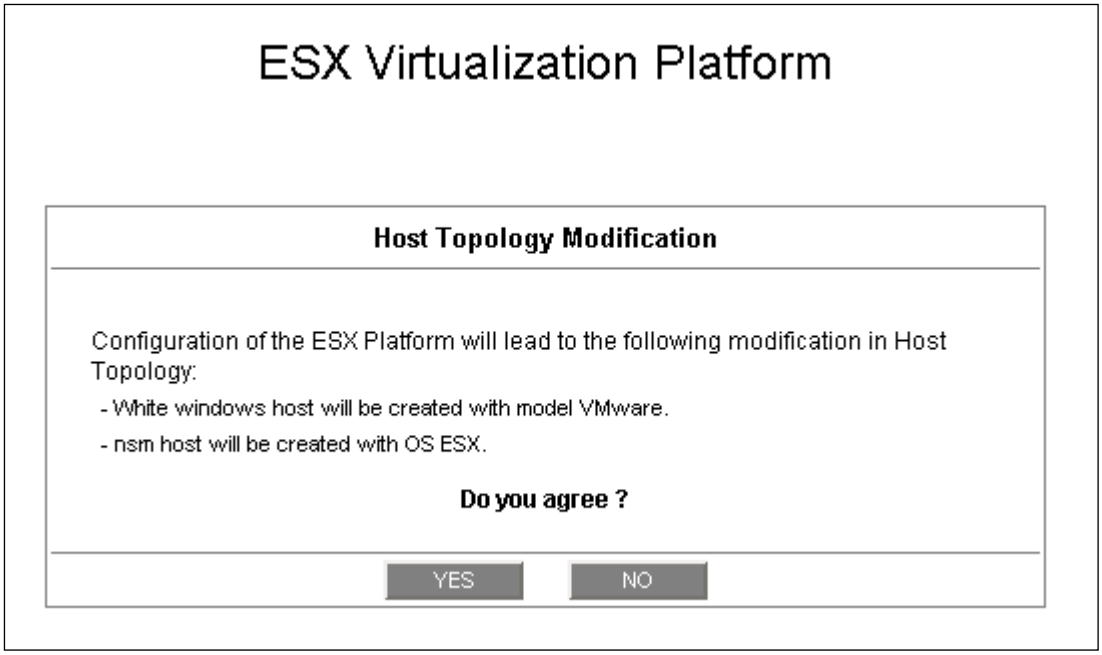


Figure 3-32. Host Topology modification confirmation screen

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

Related ESX Virtualization platform Objects

When an ESX Virtualization platform is defined, related objects are automatically generated to configure the type of Supervision linked to this type of server. The table, below, describes the objects generated during the creation of the platform.

Type	Description
host VMware	As defined in the Virtual Machine configuration part of the edition page.
host ESX	Host corresponding to the virtualization layer, as defined in the ESX server Host configuration part.
hostgroup	hostgroup representing the physical platform, named <platformName>.
manager	Virtualization manager representing the management interface, named < platformName>_mgr.
categories and services	The VMwareESX category and related services are instantiated for the ESX host. The Virtual Machine category and related services are instantiated for each VMware host. The VMware category and related services are instantiated for the ESX and VM hosts.
periodic task	The CollectDataVMware task is activated with a period of 4 minutes (go to LocalSetting domain and click the Periodic Tasks menu to view its properties).

Table 3-20. Related ESX Virtualization platform Objects

3.4.2.2 Editing Virtual Machine Set-up

A virtual machine is represented by a host linked to the VMware ESX Virtualization platform. It has properties linked to the platform, and the properties of a host object.

Adding, removing or modifying properties linked to the platform must be done from the VMware Virtualization platform editing Window.

Modification of host properties must be done from the Host editing Window.

Adding a virtual machine to a platform

Adding a virtual machine is done by checking the corresponding line in Virtual Machines part of the platform editing window, and setting the host characteristics in the BSM Configuration table zone (by filling in the corresponding fields or by selecting an already defined host).

Note When you edit a Virtualization platform, only the Virtual Machines defined for the Bull System Manager platform are displayed. To add a virtual machine, you must perform a Re-discovery to obtain the list of the machines defined for the Virtualization Server.

Removing a virtual machine from a platform

Removing a virtual machine is performed by unchecking the corresponding line in the Virtual Machines section for the platform.

Note The corresponding host remains in the Bull System Manager definition with model set to **other**. To delete it, click the **Other Hosts** link to get the list of all Other Hosts configured, edit the corresponding host and click the **Delete** button.

Modifying a virtual machine defined in a platform

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

To modify other characteristics, for example netName or OS, the Host edition form must be used.

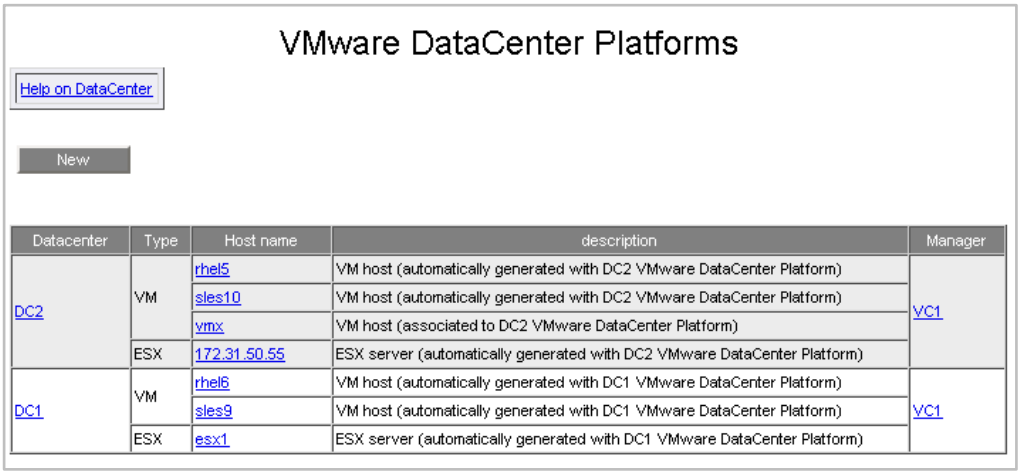
Note To get the Host edition form corresponding to the virtual machine, click the **Hostname** link displayed in the global platforms page.

Deleting all virtual machines and corresponding hosts.

To delete all virtual machines and corresponding hosts, use the **DeleteAll** button of the Virtualization Platform Edition form. Keep in mind the fact that the virtualization server and the platform will also be deleted from the Bull System Manager configuration

3.4.2.3 Configuring vCenter managed Datacenter Platforms

To configure a set of Datacenter Platforms managed by vCenter, click the **VMware vCenter** link in the Virtualization part of the Topology domain. The list of all platforms configured appears, as in the following example:



Datacenter	Type	Host name	description	Manager
DC2	VM	rhel5	VM host (automatically generated with DC2 VMware DataCenter Platform)	VC1
		sles10	VM host (automatically generated with DC2 VMware DataCenter Platform)	
		vmx	VM host (associated to DC2 VMware DataCenter Platform)	
	ESX	172.31.50.55	ESX server (automatically generated with DC2 VMware DataCenter Platform)	
DC1	VM	rhel6	VM host (automatically generated with DC1 VMware DataCenter Platform)	VC1
		sles9	VM host (automatically generated with DC1 VMware DataCenter Platform)	
	ESX	esx1	ESX server (automatically generated with DC1 VMware DataCenter Platform)	

Figure 3-33. VMware DataCenter Platforms page

It is possible:

- To create a new set of platforms managed by vCenter by using the **New** button
- To edit or delete a platform using the **<Datacenter>** link
- To edit or delete a vCenter using the **<Manager>** link
- To edit a virtual machine or ESX using the **<hostname>** link.

When you click the **New** button, the following display appears for all the resource properties:

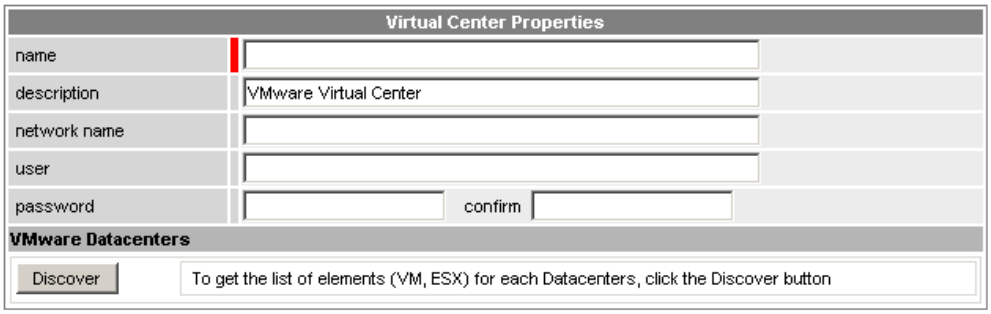


Figure 3-34. Virtual Center Properties

The first part of the form is used to define the characteristics of the VirtualCenter server.

The second part is used to describe the datacenters and the elements to be managed by the Virtual Center.

Virtual Center Properties

name	Virtual Center short name. This name is used to define the Virtualization Manager
network name	Virtual Center network name (hostname or IP address).
user	username used to connect the VirtualCenter via the VI Perl Toolkit
password	User password

Datacenters Properties

Datacenters	List of the datacenters and their elements established by selecting the datacenters obtained by requests to the VirtualCenter server. The request is performed by clicking the **Discover** button (or **Re-discover** if in edition mode). See below the complete description of the procedure.

DatataCenters Discovery

The result of the discovery is displayed as set of tables (one for each datacenter), composed of three parts:

- The left column allows you to select the VMs or the ESX to be associated with the platform.
- The center part displays element Configuration as defined on the VMware Virtual Center server.
- The right part allows you to edit the main properties (name, network name and OS) of the corresponding BSM host. The host can only be edited if the corresponding element is selected. You can select a host already defined by clicking the **Select** button or you can create a host by completing the corresponding fields.

Notes

- When you select a host, previously defined, you cannot change its network name and OS. However, the Select contains a Default Option corresponding to the element name that can be edited. If the name contains space(s), they are replaced by underscore(s) in the host label.
- The OS of ESX server cannot be changed (set to ESX).

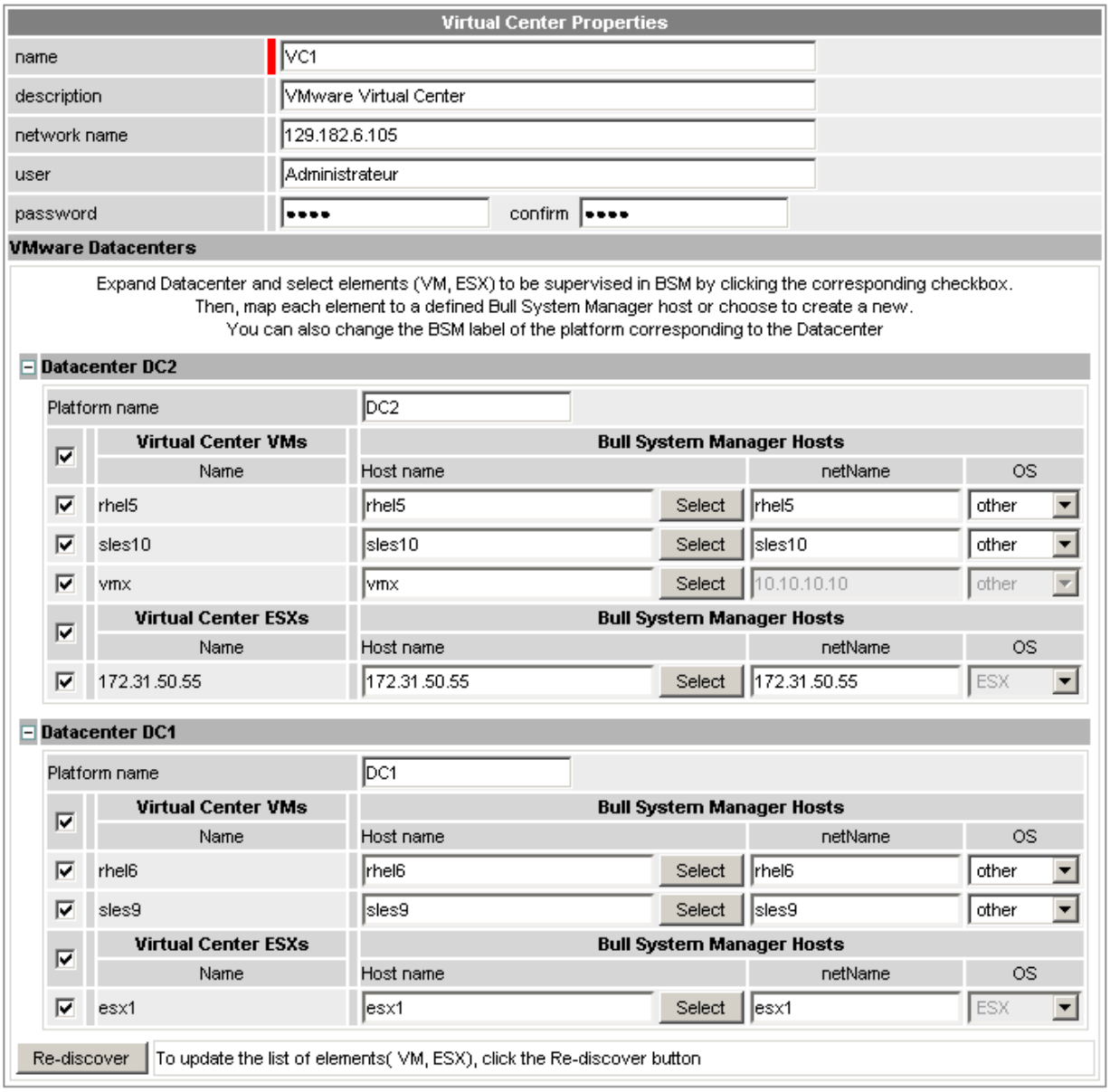


Figure 3-35. Datacenters panel

Datacenters Re-Discovery

Re-Discovery is required to check that the current BSM configuration still matches the Virtual Center configuration in order to:

- Add an element not yet registered in the Datacenter Platform
- Remove an element no longer defined in the Virtual Center configuration.

During the Re-discovery step, if the current configuration is not compatible with Virtual Center configuration, the invalid elements are displayed in red and the elements not referenced in the current BSM configuration are displayed in green.

Elements no longer defined in Virtual Center are automatically unchecked and will be removed from the platform when the form is validated. New elements must be explicitly checked to be added to the platform to be linked to the platform when the form is validated.

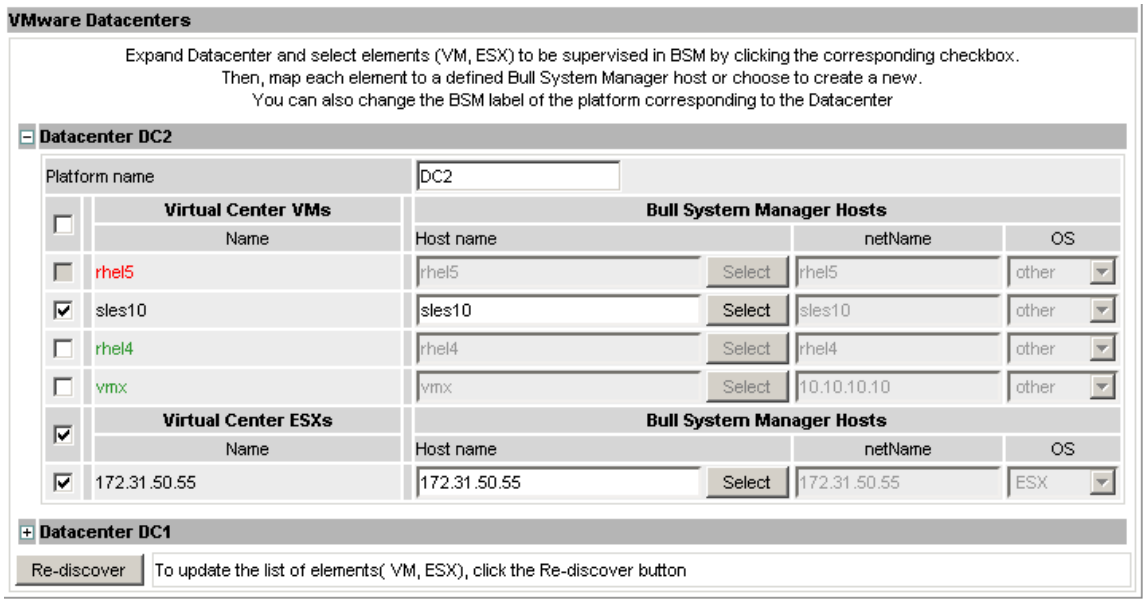


Figure 3-36. Re-discovery Step

Note How to Add, Delete or Modify Datacenter elements is detailed in *Configuring Datacenter Elements*, on page 77.

When the Datacenter elements have been edited:

- Click **OK** to validate your edition
- Or click **Cancel** to return to Datacenter Platform pages without making any changes
- Or click **Delete** to remove the VirtualCenter and Datacenter platforms managed and maintain the hosts corresponding to the VMs and the ESX server
- Or click **DeleteAll** to remove the VirtualCenter, Datacenter platforms managed and the hosts corresponding to the VMs and the VMwareESX server.

Note Any changes made are shown in the **Topology modification** Window and requires confirmation: a page listing all modifications to be applied to the Topology configuration is displayed, as shown in the following figure.

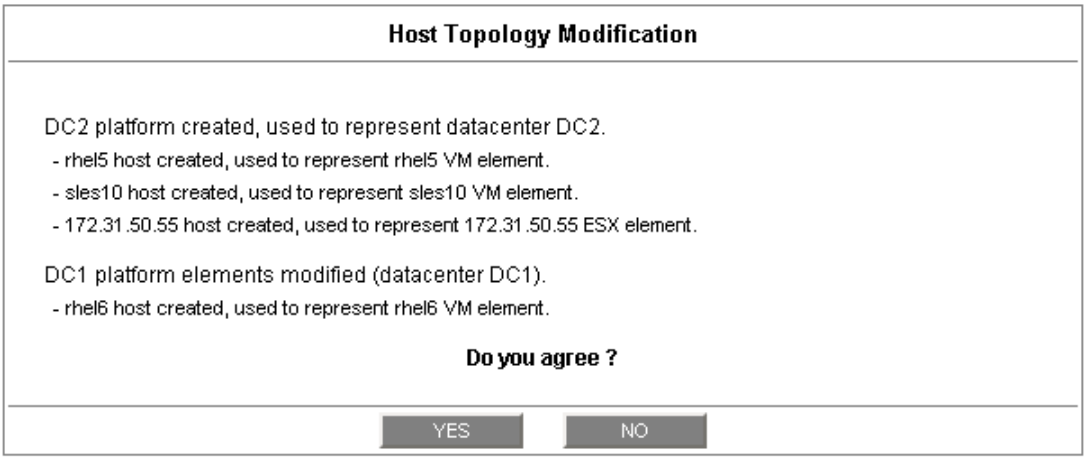


Figure 3-37. Topology modification confirmation

If you do not agree, click **NO** to return to the previous screen, otherwise click **YES** to create the datacenters.

Related Datacenters platform Objects

When a Datacenter platform is defined, related objects are automatically generated or updated to configure the Supervision level linked to this type of server. The following table describes the objects generated when the platform is created.

Type	Description
host VM	As defined in the Virtual Machine configuration section of the edition page.
host ESX	Hosts corresponding to the virtualization layer, as defined in the ESX server Host configuration part.
hostgroup VM	hostgroup representing the datacenter for VM part, named <platformName>.
hostgroup ESX	hostgroup representing the datacenter for ESX part, named <platformName>_ESX.
manager	Virtualization manager representing the management interface, named < platformName>_mgr.
categories and services	The VMwareESX category and related services are instantiated for the ESX host. The Virtual Machine category and related services are instantiated for each VMware host. The VMware category and related services are instantiated for the ESX and VM hosts.
periodic task	The CollectDataVMware task is activated with a period of 4 minutes (go to LocalSetting domain and click the Periodic Tasks menu to view its properties).

Table 3-21. Datacenters platform Objects

Notes
- The link between ESX and VM machines is not modeled by a hostgroup-host relation as in the ESX Configuration platform, due to the non support of vMotion functionality in previous versions. However, the link is symbolized by a parenthost-host relation.
- To allow the dynamic update of the parenthost-host relation, vCenter must be configured to send traps to BSM Server when there are vmBeingRelocatedEvent and VmMigratedEvent events.

3.4.2.4 Configuring Datacenter Elements

A VM or an ESX is represented by a host linked to the Datacenter Virtualization platform. It has properties linked to the platform, and also properties of a host object.

Adding, removing or modifying properties linked to the platform must be done using the VMware Datacenter platform Window.

Modification of host properties must be done using the Host Window.

Add an element (VM or ESX) to a datacenter

An element is added by checking the corresponding line in the platform Window, and by setting the host characteristics in the BSM Configuration table zone (fill in the corresponding fields or select a host that is already defined).

Note When you edit a Datacenter platform, only the elements defined as part of the Bull System Manager platform are displayed. To add an element, you must perform a Re-discovery to get the list of all elements defined in the datacenter.

Remove an element from a datacenter

Removing an element is performed by unchecking the corresponding line in the platform Window.

Notes
- The corresponding host remains in the Bull System Manager definition with the model set to **other**. To delete it, click the **Other Hosts** link to get the list of all the Other Hosts configured, edit the corresponding host and click the **Delete** button.
- If all the elements of a platform are deleted, the platform itself is deleted.

Modify an element defined in a datacenter

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

To modify other characteristics, such as netName or OS, the Host edition form must be used.

Note To view the Host Window for the definition of elements corresponding to the virtual machine, click the **Hostname** link displayed in the global platforms page.

Delete all elements and corresponding hosts

Use the **DeleteAll** button to delete all elements managed by a Virtual Center and corresponding hosts.

3.4.2.5 Supervising Virtualization

As specified above, categories and services are instantiated for the host defined in the Virtualization Platform. You can disable virtualization supervision by editing the hostgroup or manager properties, or by editing each service (refer to the *Bull System Manager Administration Guide* for details).

Monitoring Services

Monitoring services defined for the native OS are associated with the **VMwareESX** category.

Services Applied to the ESX hosts (category VMwareESX)

Service	Description	Check_command
Status	Checks ESX server status	check_esx_vsphere
Memory	Checks ESX memory availability	check_esxmem_vsphere
CPU	Checks ESX CPU availability	check_esxcpu_vsphere
Network	Checks ESX network traffic	check_esxnet_vsphere
Disk	Checks ESX disk traffic	check_esxio_vsphere

Table 3-22. ESX hosts Services

Note To check metrics not defined in delivered services, you can clone the Template service that is based on the **`check_esxstat_vsphere`** command.

Services Applied to the VM host (category VirtualMachine)

Service	Description	Check_command
Status	Checks VM status	check_vm_vsphere
Memory	Checks VM memory availability	check_vmmem_vsphere
CPU	Checks VM CPU availability	check_vmcpu_vsphere
Network	Checks VM network traffic	check_vmnet_vsphere
Disk	Checks VM disk traffic	check_vmio_vsphere

Table 3-23. VM host Services

Note To check metrics not defined in delivered services, you can clone the Template service that is based on the `check_vmstat_vsphere` command.

Services Applied to the ESX and VM hosts (category VMware)

Service	Description	Check_command
Alerts	Processes alerts received from the ESX or vCenter SNMP agent	none (SNMP Trap receiver)

Table 3-24. ESX and VM hosts Services

At installation time, categories are defined with a hostList set to **none** and services are defined with a hostList set to '*'.

When editing the Virtualization Platform, the category's hostList is updated for the ESX and/or VM hosts defined in the platform, leading to the activation of the corresponding services. Theses services can be displayed and edited from the Services page in the Supervision domain

Services Applied to the vCenter host (category vSphere)

Service	Description	Check_command
Connection	Checks the link between the BSM Server and the vCenter machine	check_connect_vsphere

Table 3-25. vCenter host Services

By default, no vCenter host is defined when the vCenter is configured in BSM. To define a service to check the link between the BSM Server and the vCenter machine, you have to:

1. Define an host with the same name that the vCenter object
2. Apply the vSphere category to this host as described below:
   a. Click the **Categories/Services** link in the Monitoring part of the Supervision domain.
   b. Set filters to vCenter host(s)

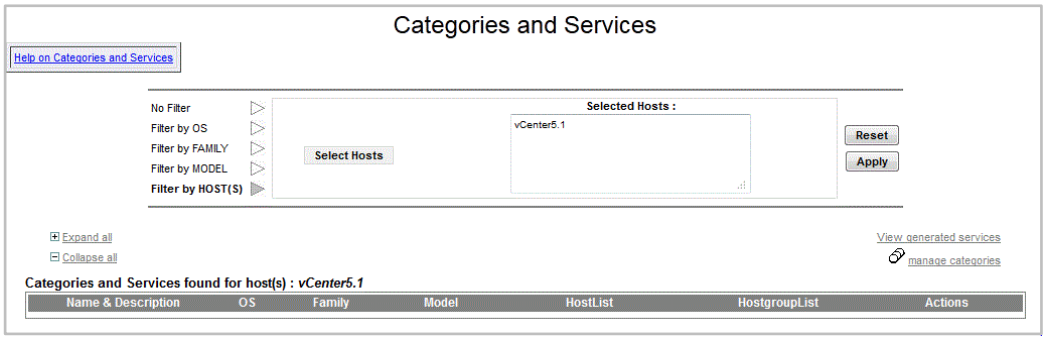


Figure 3-38. vCenter's supervison filtering

   c. Click the **manage categories** link and select **Add from an unused category template (user or predefined template)** and choose the **vSphere** category in the new Windows displayed.

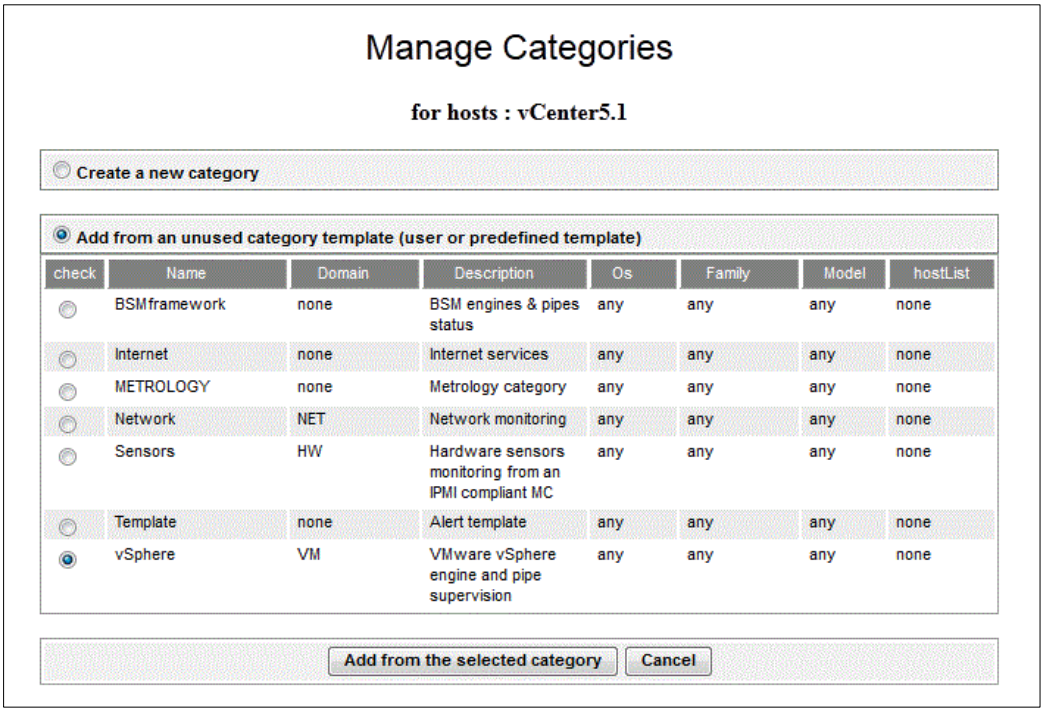


Figure 3-39. Adding the vSphere category

d. After validating the choice by clicking the **Add from the selected category** button, the editing page for the category is displayed with all fields filled in.
Click the **OK** button to instantiate the vSphere category.

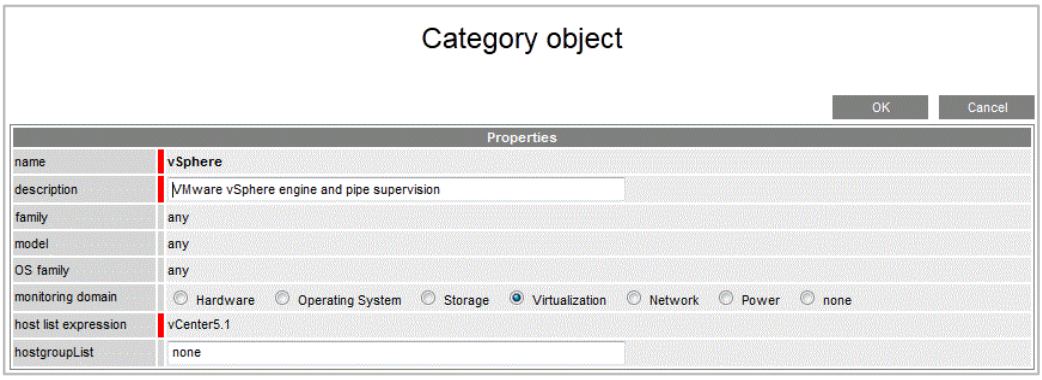


Figure 3-40. vSphere category

e. As shown in the following figure, the Connection service is automatically instantiated

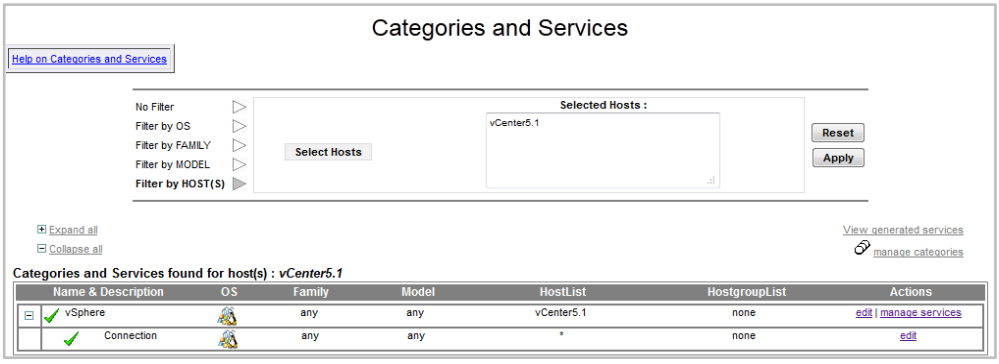


Figure 3-41. vSphere service

3.4.2.6 Configuring vSphere Collect Tasks

Information need to supervise vSphere elements are collected by the BSM server by periodic task. The moment vSphere elements are defined, a collect task is activated and by default, each new vSphere elements added to the BSM Configuration will be associated to this task. In order to dispatch vSphere elements on several tasks and allow different scheduling for some vSphere elements, it is possible to define additional collect task.

To configure an additional task, click the **Collect Tasks** link in the **Functionalities** part of **LocalSetting** domain. The following page is displayed:

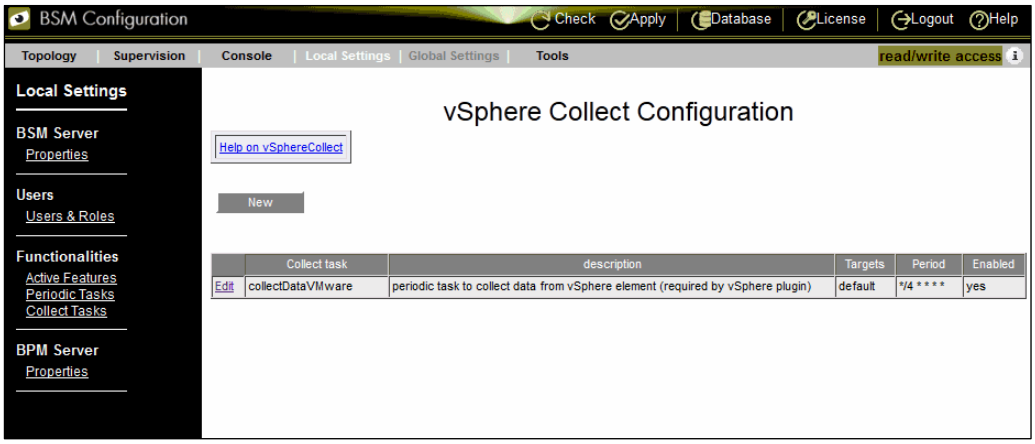


Figure 3-42. vSphere collect configuration main page

The page displays the default object, collectDataVMware, that collect data for all vSphere elements.

It is possible :

- To create a new collect task using the New button,
- To edit or delete a collect task using the Edit link.

When you click the **New** button, the following display appears with all the collect task properties:

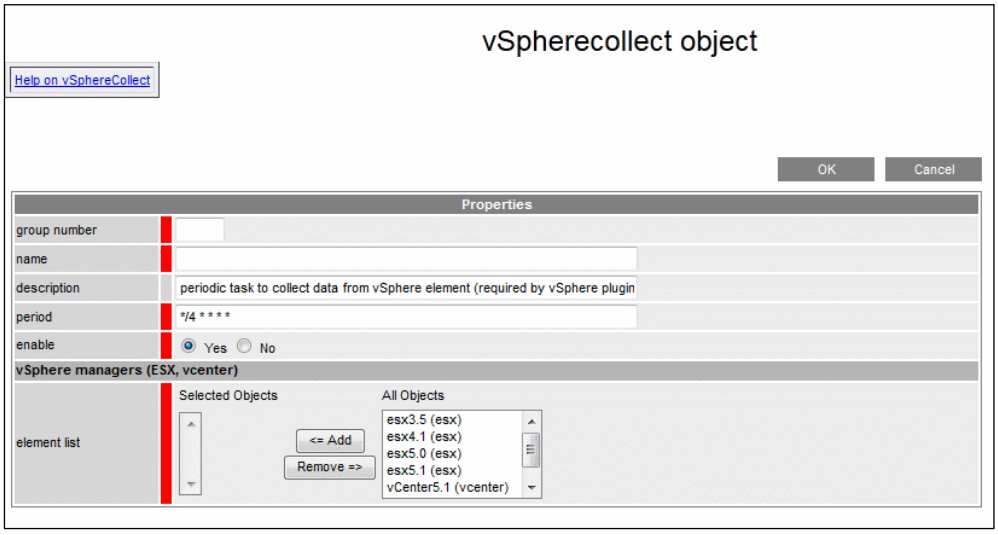


Figure 3-43. vSphere collect object

At least, you have to fill the following attributes:

group number	a number representing the group of vSphere elements linked to the task.
element list	list of vSphere elements that will be collected by the current task.

The other attributes can be filled if you want to change the default values:

name	the default name is the string collectDataVMware followed by the group number (separated by an undderscore)
description	short text decsribing the task
period	this attribute defined the periodicity of the task The periodicity is defined in five fields in the 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 the 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 */10 in the minute field specifies an execution every ten minutes See the *CRON Reference Manual* to get detailed information. By default, the task is scheduled every four minutes
enable	this attribute allows to enable/disable the task. By default, set to 'yes'

When all fields are filled, click the OK button to validate the task edition.

The main page is displayed with the list of all defined tasks, as shown in the following figure:

	Collect task	description	Targets	Period	Enabled
Edit	collectDataVMware	periodic task to collect data from vSphere element (required by vSphere plugin)	default	*/4 * * * *	yes
Edit	collectDataVMware_1	periodic task to collect data from vSphere element (required by vSphere plugin)	esx3.5,esx4.1	*/5 * * * *	yes
Edit	collectDataVMware_2	periodic task to collect data from vSphere element (required by vSphere plugin)	esx5.0,esx5.1	*/11 * * * *	yes

Figure 3-44. vSphere collect tasks

In the upper example, three tasks are defined:

- the default task (collectDataVMware), that collect vSphere elements not affected to other task. The task is scheduled all the 4 minutes.
- the collectDataVMware_1, that collect esx3.5 and sx4.1 elements. This task is scheduled all the 5 minutes
- the collectDataVMware_1, that collect esx5.0 and esx5.1 elements. This task is scheduled all the 11 minutes

3.4.2.7 Nagios Check Commands

check_esx_vsphere

The configurable Bull System Manager service check command syntax is:

```
check_esx_vsphere
```

No parameter must be set.

check_esxstat_vsphere

The configurable Bull System Manager service check command syntax is:

```
check_esxstat_vsphere>!<stat>!<wThres>!<cThres>!<indic>
```

See the **check_vsphere.pl** command examples in *Section 4.3.1* for parameter details.

check_esxcpu_vsphere

The configurable Bull System Manager service check command syntax is:

```
check_esxcpu_vsphere>!<stat>!<wThres>!<cThres>
```

This command checks the `cpu.usage.average metric.`

See the **check_vsphere.pl** command examples in *Section 4.3.1* for parameter details.

check_esxmem_vsphere

The configurable Bull System Manager service check command syntax is:

```
check_esxmem_vsphere>!<stat>!<wThres>!<cThres>
```

This command checks the `mem.usage.average` metric and collects data for additional metrics (see the command to get the list)

See the **check_vsphere.pl** command examples in *Section 4.3.1* for parameter details.

check_esxnet_vsphere

The configurable Bull System Manager service check command syntax is:

```
check_esxnet_vsphere>!<stat>!<wThres>!<cThres>
```

This command checks the `net.usage.average metric` and collects data for additional metrics (see the command to get the list)

Note The **net.usage.average** unit is Kb/s. By default, the threshold are set to 80400 and 102400 in the service definition. Depending on your network capacity, you can change these values.

See the **check_vsphere.pl** command examples in *Section 4.3.1* for parameter details.

check_esxio_vsphere

The configurable Bull System Manager service check command syntax is:

```
check_esxio_vsphere>!<stat>!<wThres>!<cThres>
```

This command checks the `disk.usage.average metric` and collects data for additional metrics (see the command to get the list)

Note The **disk.usage.average** unit is Kb/s. By default, the thresholds are set to 80400 and 102400 in the service definition. Depending on your disk capacity, you can change these values.

See the **check_vsphere.pl** command examples in *Section 4.3.1* for parameter details.

check_vm_vsphere

The configurable Bull System Manager service check command syntax is:

```
check_vm_vsphere
```

No parameter must be set.

check_vmstat_vsphere

The configurable Bull System Manager service check command syntax is:

```
check_statvm_vsphere>!<stat>!<wThres>!<cThres>!<indic>
```

See the **check_vsphere.pl** command examples in *Section 4.3.1* for parameter details.

check_vmcpu_vsphere

The configurable Bull System Manager service check command syntax is:

```
check_vmcpu_vsphere>!<stat>!<wThres>!<cThres>
```

This command checks the `cpu.usage.average metric` and collects data for additional metrics (see the command to get the list)

See the **check_vsphere.pl** command examples in *Section 4.3.1* for parameter details.

check_vmmem_vsphere

The configurable Bull System Manager service check command syntax is:

```
check_vmmem_vsphere>!<stat>!<wThres>!<cThres>
```

This command checks the `mem.usage.average` metric and collects data for additional metrics (see the command to get the list)

See the **check_vsphere.pl** command examples in *Section 4.3.1* for parameter details.

check_vmnet_vsphere

The configurable Bull System Manager service check command syntax is:

```
check_vmnet_vsphere>!<stat>!<wThres>!<cThres>
```

This command checks the `net.usage.average metric` and collects data for additional metrics (see the command to get the list)

Note The net.usage.average unit is Kb/s. By default, the thresholds are set to 80400 and 102400 in the service definition. Depending on your network capacity, you can change these values..

See the **check_vsphere.pl** command examples in *Section 4.3.1* for parameter details.

check_vmio_vsphere

The configurable Bull System Manager service check command syntax is:

`check_vmio_vsphere>!<stat>!<wThres>!<cThres>`

This command checks the `disk.usage.average metric` and collects data for additional metrics (see the command to get the list)

Note The **disk.usage.average** unit is Kb/s. By default, the thresholds are set to 80400 and 102400 in the service definition. Depending on your disk capacity, you can change these values.

See the **check_vsphere.pl** command examples in *Section 4.3.1* for parameter details.

check_connect_vsphere

The check_connect_vsphere Bull System Manager service check command has no parameter. It uses the check_BSM_vsphere_connect.pl system command.

See the **check_vsphere.pl** command examples in *Section 4.3.1* for parameter details.

Collect task

The collect task periodically schedules (each 4 minutes) the script `collectVMvSphere.sh` that requests all the information from the vCenter or ESX needed by the Nagios plug-in, and stores it in a cache file. This task is enabled when at least one virtualization platform is configured in the BSM.

The script is localized in the `<BSM Installation>/engine/bin` directory and its execution is logged in the `<BSM Installation>/engine/tmp/collectVMvSphere.log file.`

To edit task, from LocalSetting domain, click the **Periodic Tasks** menu and edit the **CollectDataVMware** task, the screen below is displayed:

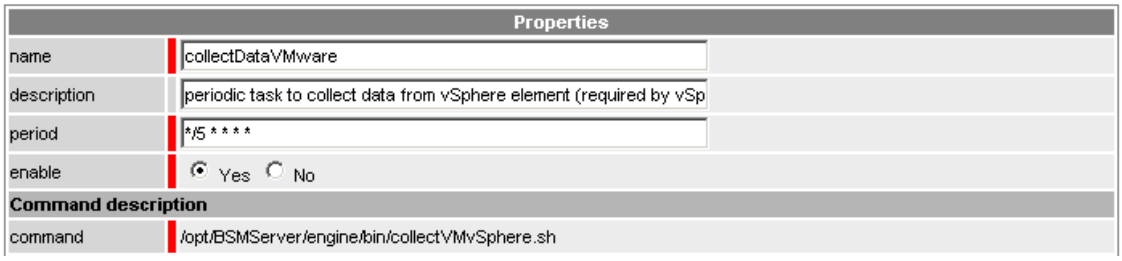


Figure 3-45. CollectDataVMware task properties

Any modification will be taken into account the next time the task is Saved and Reloaded action.

Reporting Indicators

Reporting indicators are collected by analyzing the performance data provided by Nagios plug-in with PNP4Nagios.

Indicators Applied to the ESX Host

Indicator	Corresponding Service
CPU_usage (%)	VMwareESX.CPU
Memory_usage (%)	VMwareESX.Memory
Memory_Active (Kb)	
Memory_Consumed (Kb)	
Memory_Granted (Kb)	
Memory_Balloon (Kb)	
Memory_Swap_(Kb)	
Used,Memory (Kb)	
Shared Common (Kb)	
Disk_usage (Mb/s)	VMwareESX.Disk
Disk_Read_Rate (Mb/s)	
Disk_Write_Rate (Mb/s)	
Disk_Commands_Issued (cmd/s)	
Disk_Read_Requests (cmd/s)	
Disk _Write_Requests (cmd/s)	
Network_usage (Kb/s)	VMwareESX.Network
Network_Data_Transmit_Rate (Kb/s)	
Network_Data_Received_Rate (Kb/s)	

Table 3-26. ESX host Indicators

Indicators Applied to the VM Host

Indicator	Corresponding Service
CPU_usage (%)	VirtualMachine.CPU
CPU_Used (ms)	
CPU_Ready (ms)	
CPU_Wait (ms)	
CPU_Idle (ms)	
CPU_System (ms)	
Memory_usage (%)	VirtualMachine.Memory
Memory_Active (Kb)	
Memory_Consumed (Kb)	
Memory_Granted (Kb)	
Memory_Balloon (Kb)	
Disk_usage (Mb/s)	VirtualMachine.Disk
Disk_Read_Rate (Mb/s)	
Disk_Write_Rate (Mb/s)	
Disk_Commands_Issued (cmd/s)	
Disk_Read_Requests (cmd/s)	
Disk _Write_Requests (cmd/s)	
Network_usage (Kb/s)	VirtualMachine.Network
Network_Data_Transmit_Rate (Kb/s)	
Network_Data_Received_Rate (Kb/s)	

Table 3-27. VM hosts Indicators

Note PNP4Nagios is delivered in as BSM Server Extension and its installation is optional.

Bull System Manager Console

VMware Operation

From the Virtual Manager or from any element of the Virtual Platform, you can launch the **Virtual Infrastructure Web Interface** by selecting the following cascading menu:

Operation → Application → VMware Virtual Infrastructure Web Access

VMware Monitoring

From the platform or host elements, you can access monitoring information.
From the hosts element, you can display information related to the associated service by selecting **Monitoring** menus.
From the platform element, you can display monitoring information related to all elements by selecting **Monitoring** menus. For instance, you can view all services of the hosts in the platform, as shown in the following figure:

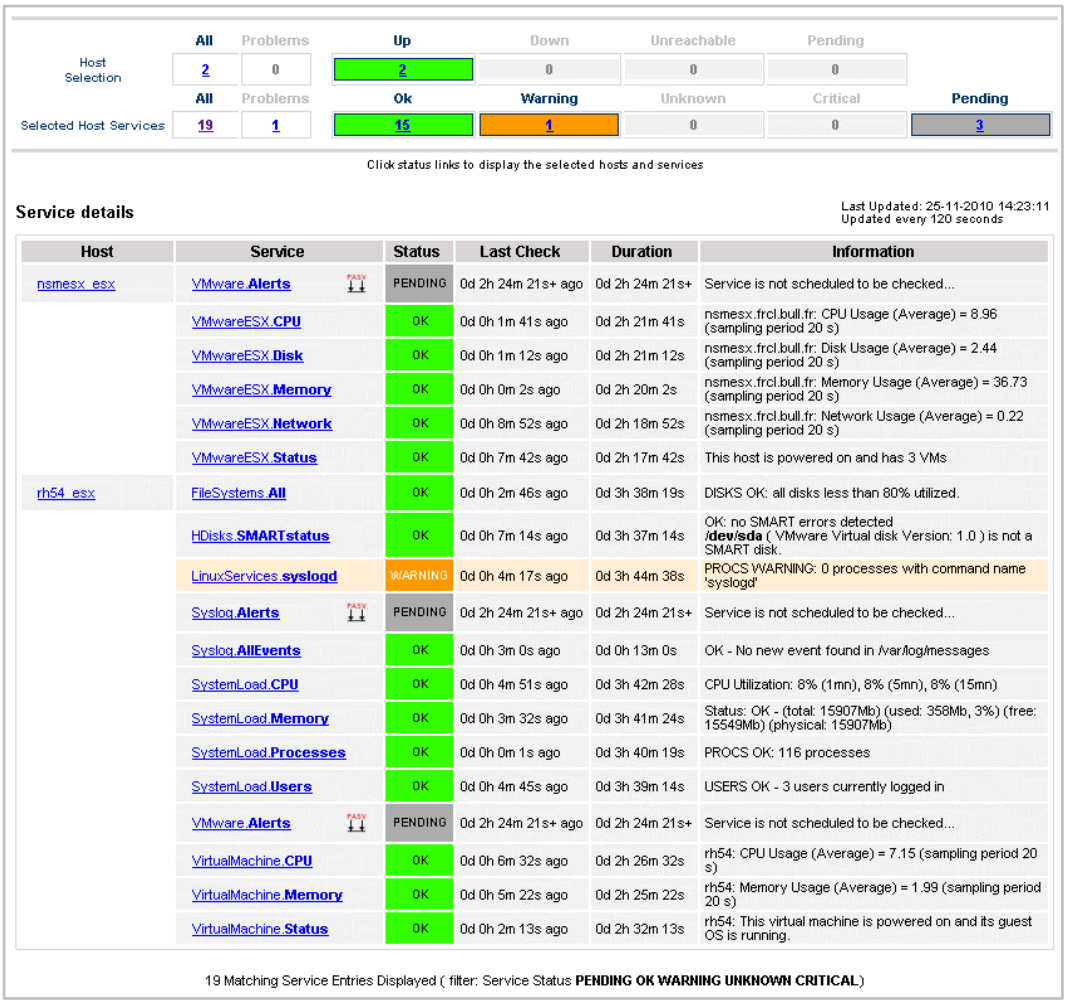


Figure 3-46. VMware ESX monitoring information

VMware Reporting

From host elements, you can access reporting information by selecting **PNP Indicators Trends** from the **Reporting** menu.

From the host element, you can display indicators related to this host as shown in the following figure:

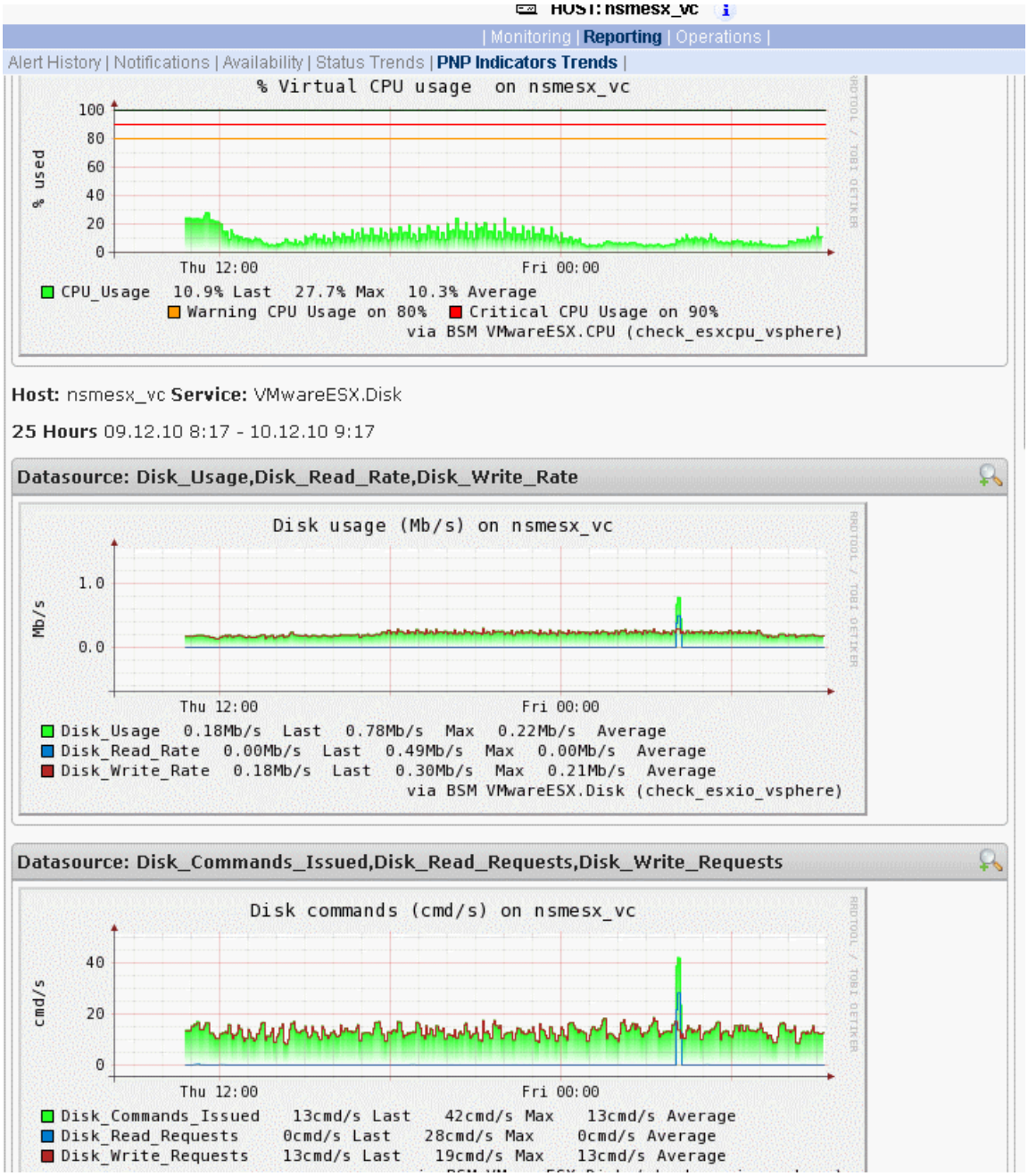


Figure 3-47. VMware reporting information

3.4.3 EscalaLPAR Add-on

Dynamic logical partitioning (LPAR) is a system architecture delivered on Escala systems that is used to divide a single server into several completely independent virtual servers or logical partitions.

The **HMC (Hardware Management Console)** is a special-purpose system that provides management tools for controlling one or more servers and associated logical partitions (LPARs). Management can be performed either through the HMC GUI or through the command-line interface (using a SSH connection to the HMC).

For system not managed by an HMC, **Integrated Virtualization Manager (IVM)** provides a local management of the partitions. IVM, which is part of the Virtual I/O Server, is a special purpose partition that provides virtual I/O resources for the other partitions.

The **EscalaLPAR** Add-on provides functional links to supervise the logical partitions by requesting the HMC system or the IVM component.

Important

Escala Supervision with HMC or IVM requires the setting of a non-prompt SSH connection between the Bull System Manager Server and the manager. 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 a non-prompt connection between the BSM Server and the HMC, the public key must be installed on the HMC or IVM hosting server. Refer to the HMC or IVM documentation to see how to install the key.

The following figure shows the link between each component, for systems managed with HMC:

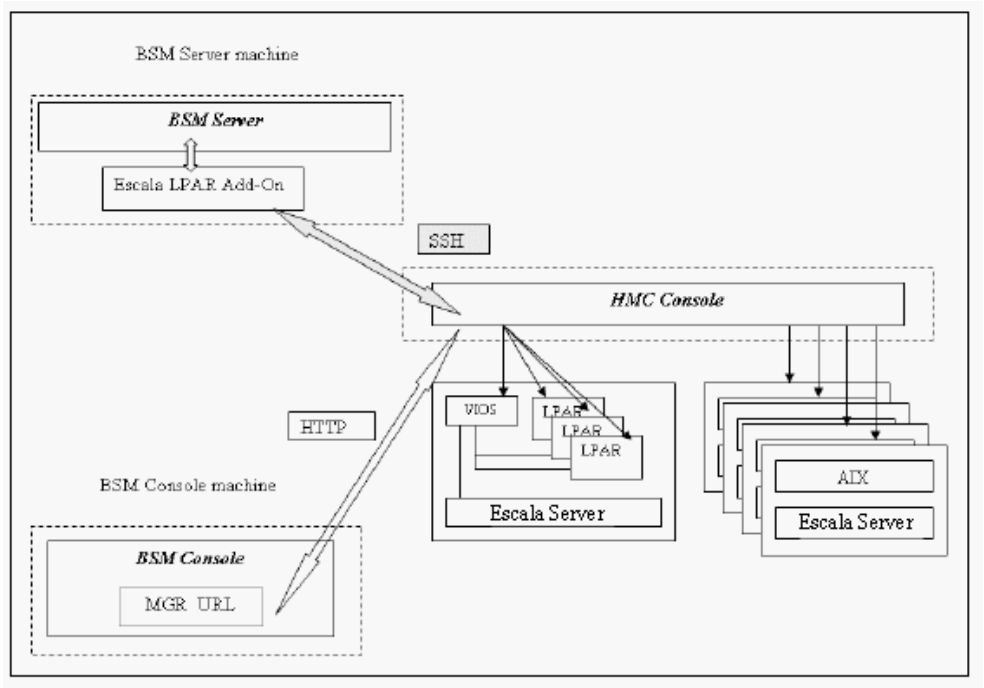


Figure 3-48. EscalaLPAR Add-on components for HMC managed systems

The following figure shows the link between each component, for system managed with IVM:

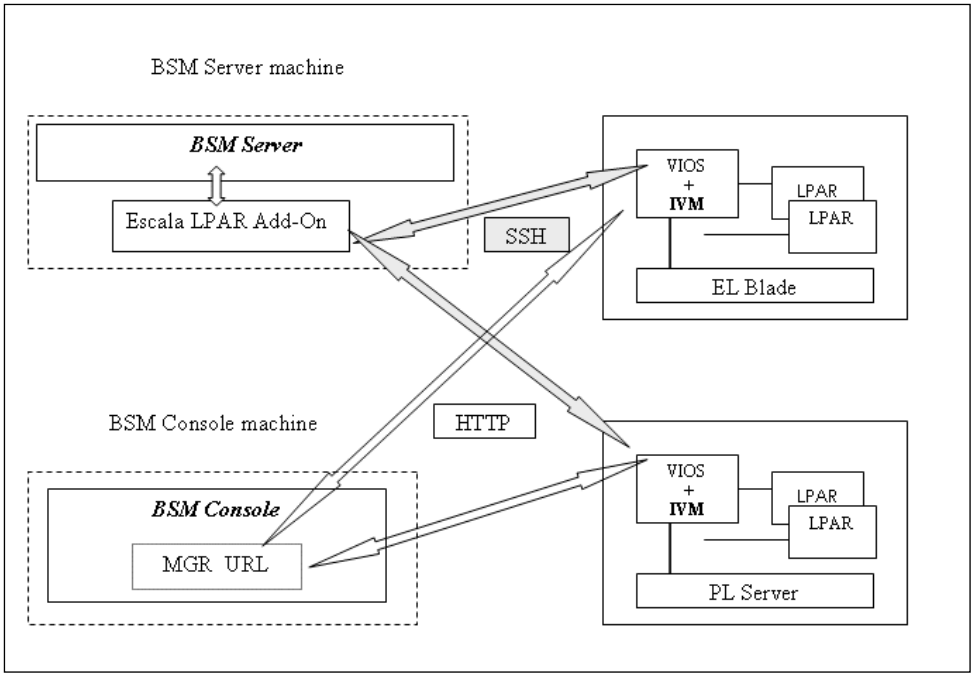


Figure 3-49. EscalaLPAR Add-on components for IVM managed systems

3.4.3.1 Configuring Bull System Manager

To configure the monitoring elements for the EscalaLPAR Add-on, you have to define an Escala Platform from the Bull System Manager Configuration GUI.
The definition of an Escala Platform is done in two steps:

- initialization of the Escala Server
- definition of the partitioning (LPARs)
- configuration of the EscalaMobilityEvent if Live Partition Mobility feature must be supported

HMC managed Escala Server

The initialization of an HMC managed system is done through the **Escala Server** link under Hosts Definition/Escala hosts menu of the **Topology** domain.

IVM managed Escala Server

The initialization of an IVM managed Escala Server requires that this server contains a VIOS partition. This is done through the **Escala Blade** or **Escala Server** links under the Hosts Definition/Blade hosts or Hosts Definition/Escala hosts menu of the **Topology** domain.

Non managed Escala Server

The initialization of a non managed Escala Server is done through the **PL Server** links under the Hosts Definition/Escala hosts menu of the **Topology** domain.

Escala Server Partitioning

The definition of the partitioning is done through the LPARs links To get detailed information about How to Define Escala Hosts, see the *Bull System Manager Administrator's Guide*.

3.4.3.2 Virtualization Supervision

Services and associated performance indicators are applied to each host defined in the Escala LPAR platform.

You can disable virtualization supervision by editing the hostgroup or manager properties, or by editing each service (refer to the *Bull System Manager Administration Guide* for details).

Monitoring Services applied to the VIO server layer

Monitoring services defined for the VIO server are associated with the **VIOSActivity** and **SSP** categories.

Service	Description	Check_command
VIOSActivity.UsedNPIV	Checks the utilization of NPIV on Virtual I/O Server	check_vios_used_npiv
VIOSActivity.UsedSEA	Checks the utilization of SEA on Virtual I/O Server	check_vios_used_sea
SSP.Status	Checks the status of the cluster	check_vios_ssp_status
SSP.NodesStatus	Checks the status of the nodes in the cluster	check_vios_ssp_nodes_status
SSP.PoolDisks	Checks the use of storage space in the cluster	check_vios_ssp_pool_disks
SSP.PoolStatus	Checks the status of the pools in the cluster	check_vios_ssp_pools
SSP.DisksStatus	Checks the status of the disks in the cluster	check_vios_ssp_disks_status

Table 3-28. Vio server layer – Monitoring Services

Monitoring Services applied to the PowerHypervisor layer

Monitoring services defined for the PowerHypervisor layer of an Escala host are associated with the **ProcessorPool** category.

Service	Description	Check_command
UsedPool	Checks the utilization of processor pool on Escala Blade managed by IVM	check_vios_used_pool
DefaultPool	Checks the utilization of the Default Processor Pool on Escala Server managed by HMC	ceck_cec_used_pool
SharedPool	Checks the utilization of a processor pool on Escala Server managed by HMC [(a)]	check_used_configured_pool

Table 3-29. PowerHypervisor layer – Monitoring Services

[(a)] The number and the name of the SharedPool services is deduced from the user defined shared pool.

Monitoring Services Applied to the Partition Host

Monitoring services defined for partition hosts are associated with the **VirtualMachine** and **LPM** categories.

Service	Description	Check_command
VirtualMachineStatus	Checks LPAR status	check lpar_status
VirtualMachineUsedCPU	Checks the utilization of the entitled CPU by the partition	check_lpar_used_cpu
LPM.Status	Check the Logical Partition Manager status	check_lpm.pl (via check_nrpe)

Table 3-30. Partition host – Monitoring Services

Monitoring services related to Escala Platform elements are automatically applied when the platform details are edited. Theses services can be displayed and edited from the **Services** page in the Supervision domain.

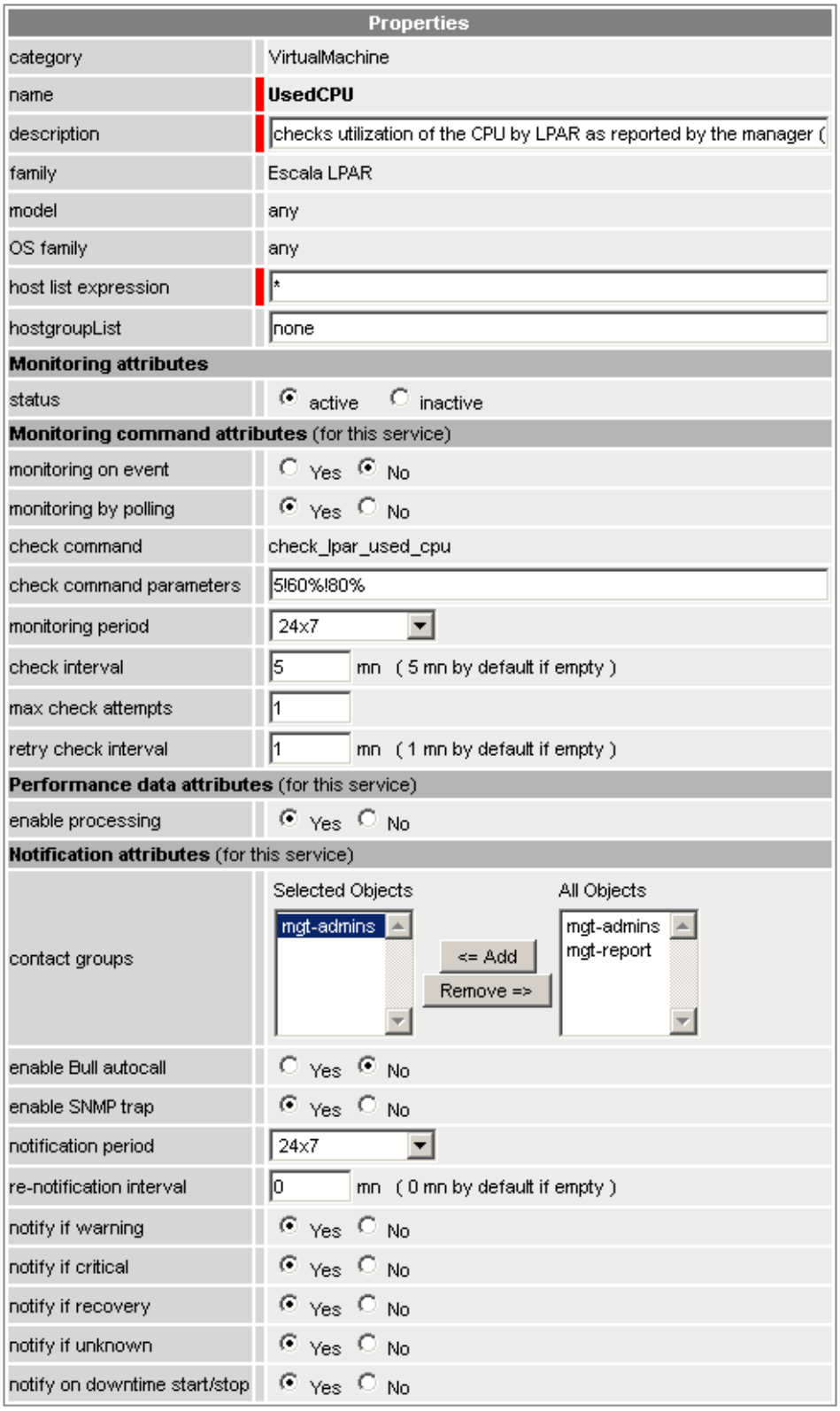


Figure 3-50. VirtualMachine. UsedCPU Service Properties pane

Note During Platform definition, all services are applied to each component of the server (VIOs, PowerHypervisor and partition). To deactivate the monitoring of a service, edit it and set its status (Monitoring attributes part) to inactive.

Reporting indicators

Reporting indicators are collected by analyzing performance data provided by Nagios plug-in with PNP4Nagios.

Indicators applied to the server managed by HMC

Indicator	Corresponding Service
PoolUsage	ProcessorPool.<poolname>
PoolSize	ProcessorPool.<poolname>
<lparname>	ProcessorPool.<poolname>

Table 3-31. Server managed Indicators

Indicators applied to the VIOs host

Indicator	Corresponding Service
CPU_usage	VirtualMachine.UsedCPU
NPIV Usage	VIOSActivity.UsedNPIV
NPIV In for <ident>	VIOSActivity.UsedNPIV
NPIV Out for <ident>	VIOSActivity.UsedNPIV
SEA Usage	VIOSActivity.UsedSEA
SEA In for <ident>	VIOSActivity.UsedSEA
SEA Out for <ident>	VIOSActivity.UsedSEA
Space Used in pool (%)	SSP.PoolDisks
Overcommit in pool (%)	SSP.PoolDisks

Table 3-32. VIOs host Indicators

Indicators applied to the LPAR host

Indicator	Corresponding Service
CPU_usage	VirtualMachine.UsedCPU

Table 3-33. LPAR host Indicators

Configuring escalaMobilityEvent EventHandler

The escalaMobilityEvent is defined by the Add-on, it is not enabled by default. To enable it, perform the following actions:

Click the **Event** link in the EventHandler part of Supervision domain. A page appears with events, defined as shown below:

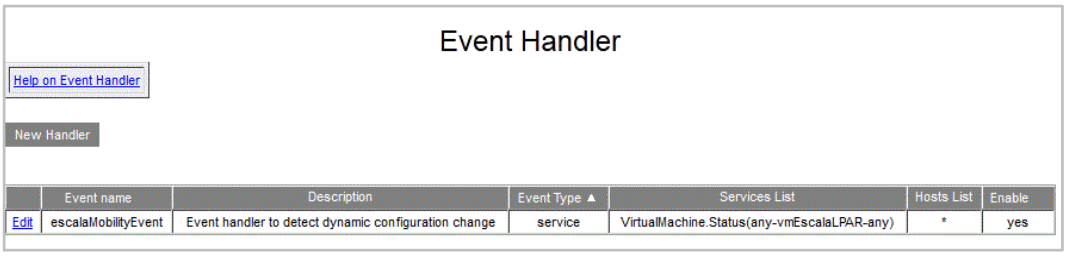


Figure 3-51. Escala Event Handler

To edit the event handler, click the **Edit** link of the escalaMobilityEvent. The Properties page is displayed:

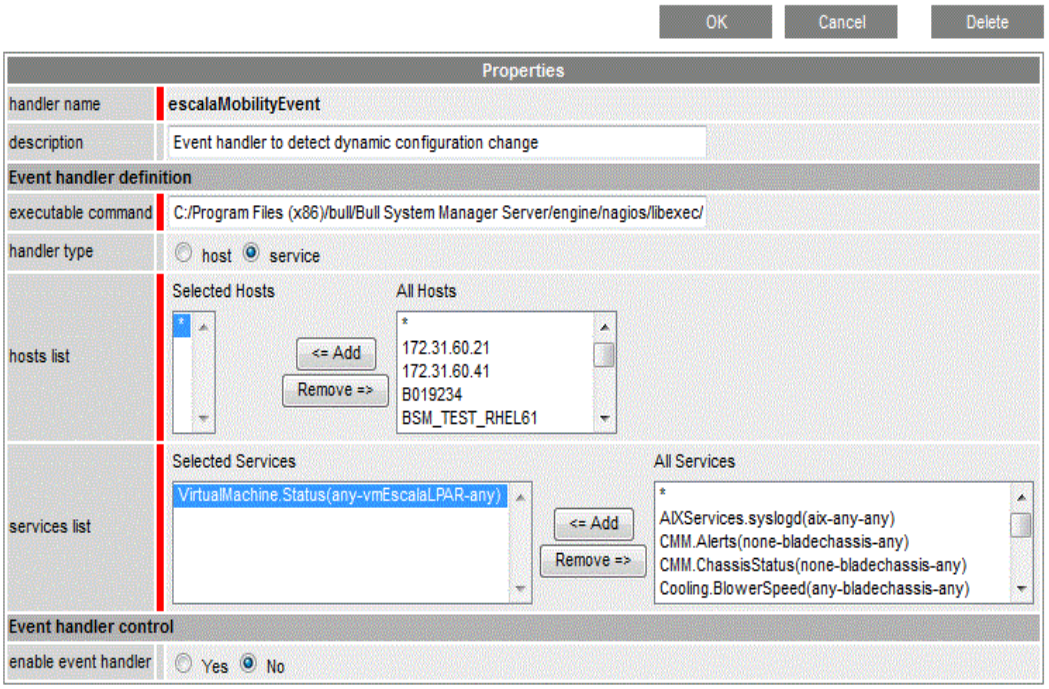


Figure 3-52. Escala Event Handler parameters

Set **enable event handler** to **Yes** and click **OK** to validate the changes. The event handler will be taken into account at next BSM Configuration Apply.

3.4.3.3 Nagios Check Commands

check_vios_status

The configurable BSM service check command syntax is:

```
check_vios_status!<ssh_user>!<identity_file>
```

See the **check_NSM_escala_lpar** command examples in *Section 4.3.2* for parameter details.

check_vios_used_pool

The configurable BSM service check command syntax is:

```
check_vios_used_pool!<ssh_user>!<identity_file>!<sample_time>!<warning_th
reshold>!<critical_threshold>
```

See the **check_NSM_escala_lpar** command examples in *Section 4.3.2* for parameter details.

check_vios_used_sea

The configurable BSM service check command syntax is:

```
check_vios_used_sea!<sample_time>!<warning_threshold>!<critical_threshold>
```

See the **check_NSM_escala_lpar** command examples in *Section 4.3.2* for parameter details.

Note The ssh user and identity file properties are now defined contextually at the host level and are automatically set for the check command by Nagios.

check_vios_used_npiv

The configurable BSM service check command syntax is:

```
check_vios_used_npiv!<sample_time>!<warning_threshold>!<critical_threshold>
```

See the **check_NSM_escala_lpar** command examples in *Section 4.3.2* for parameter details.

Note The ssh user and identity file properties are now defined contextually at the host level and are automatically set for the check command by Nagios.

check_vios_ssp _status

The configurable BSM service check command syntax is:

```
check_vios_ssp _status!<sample_time>
```

See the **check_NSM_escala_vios_ssp** command examples in *Section 4.3.2* for parameter details.

check_vios_ssp _pools

The configurable BSM service check command syntax is:

```
check_vios_ssp _pools!<sample_time>
```

See the **check_NSM_escala_vios_ssp** command examples in *Section 4.3.2* for parameter details.

check_vios_ssp _disks_status

The configurable BSM service check command syntax is:

```
check_vios_ssp _disks_status!<sample_time>
```

See the **check_NSM_escala_vios_ssp** command examples in *Section 4.3.2* for parameter details.

check_vios_ssp_nodes_status

The configurable BSM service check command syntax is:

```
check_vios_ssp_nodes_status!<sample_time>
```

See the **check_NSM_escala_vios_ssp** command examples in *Section 4.3.2* for parameter details.

check_vios_ssp_pool_disks

The configurable BSM service check command syntax is:

```
check_vios_ssp_pool_disks!<sample_time>
```

See the **check_NSM_escala_vios_ssp** command examples in *Section 4.3.2* for parameter details.

check_cec_used_pool

The configurable BSM service check command syntax is:

```
check_cec_used_pool!<hmc_netname>!<ssh_user>!<identity_file>!<cec_name>!<
sample_time>!<warning_threshold>!<critical_threshold>
```

See the **check_NSM_escala_lpar** command examples in *Section 4.3.2* for parameter details.

check_used_configured_pool

The configurable BSM service check command syntax is:

```
check_used_configured_pool!<sharedPoolName>!<sample_time>!<warning_thresh
old>!<critical_threshold>
```

See the **check_NSM_escala_lpar** command examples in *Section 4.3.2* for parameter details.

check_lpar_status

The configurable BSM service check command syntax is:

```
check_lpar_status!<mgr_type>!<mgr_netName>!<ssh_user>!<identity_file>!<sy
stem_name>!<lpar_name>
```

See the **check_NSM_escala_lpar** command examples in *Section 4.3.2* for parameter details.

check_lpar_used_cpu

The configurable BSM service check command syntax is:

```
check_vios_lpar_used_cpu!<mgr_type>!<mgr_netName>!<ssh_user>!<identity_file>!
<system_name>!<lpar_name>!<sample_time>!<warning_threshold>!<critical_threshold>
```

See the **check_NSM_escala_lpar** command examples in *Section 4.3.2* for parameter details.

3.4.3.4 Bull System Manager Console

Escala Operation

From the Virtual Manager or from any element of the Escala Platform:

If the system is managed by HMC, you can launch the **HMC Web Interface** by selecting the cascading menu below:

Operation > Virtualization > HMC

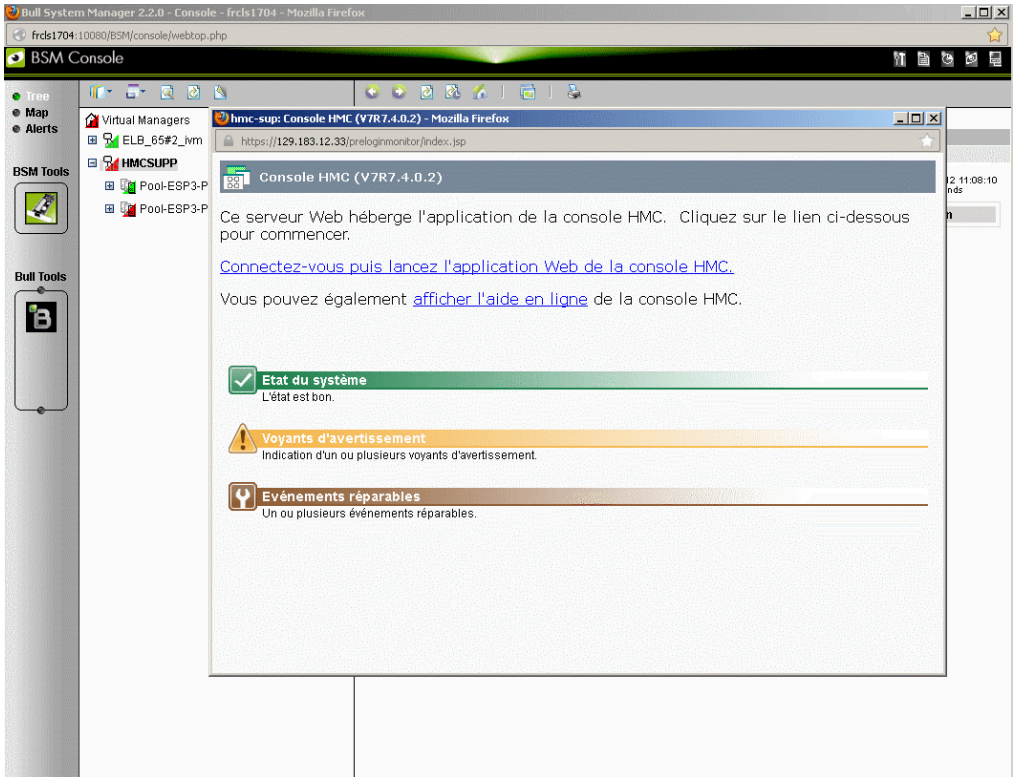


Figure 3-53. HMC activation from Bull System Manager Console

If the system is managed by IVM, you can launch the **IVM Web Interface** by selecting the cascading menu below:

Operation > Virtualization > IVM

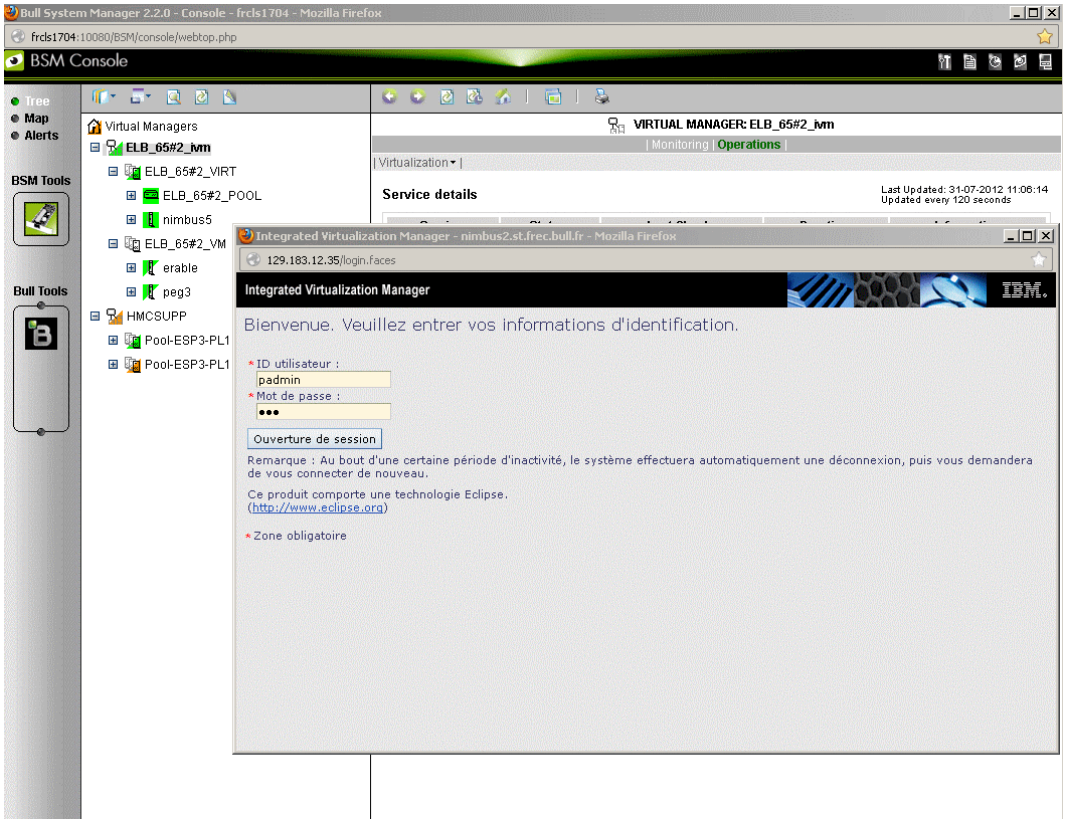


Figure 3-54. IVM activation from Bull System Manager Console

Escala Supervision

To see all the services related to an HMC managed Escala logical partition, use the **Virtual Managers** view, click the corresponding platform node (suffixed with VM) and select Monitoring/Status detail menu. The following page is displayed:

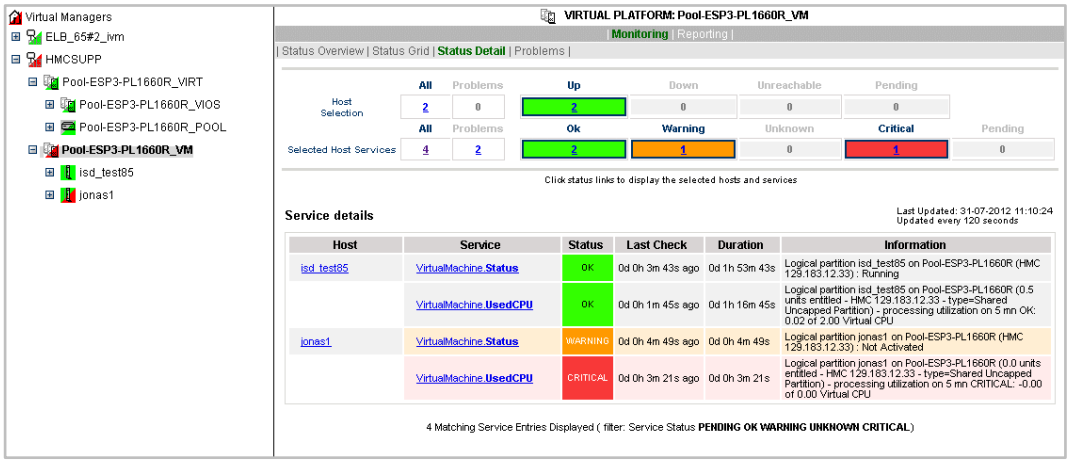


Figure 3-55. HMC managed Logical Partition reported Supervision

To see all the services related to an HMC managed virtualization layers, use the **Virtual Managers** view, click the corresponding platform node (suffixed with VIRT) and select Monitoring/Status detail menu. The following page is displayed:

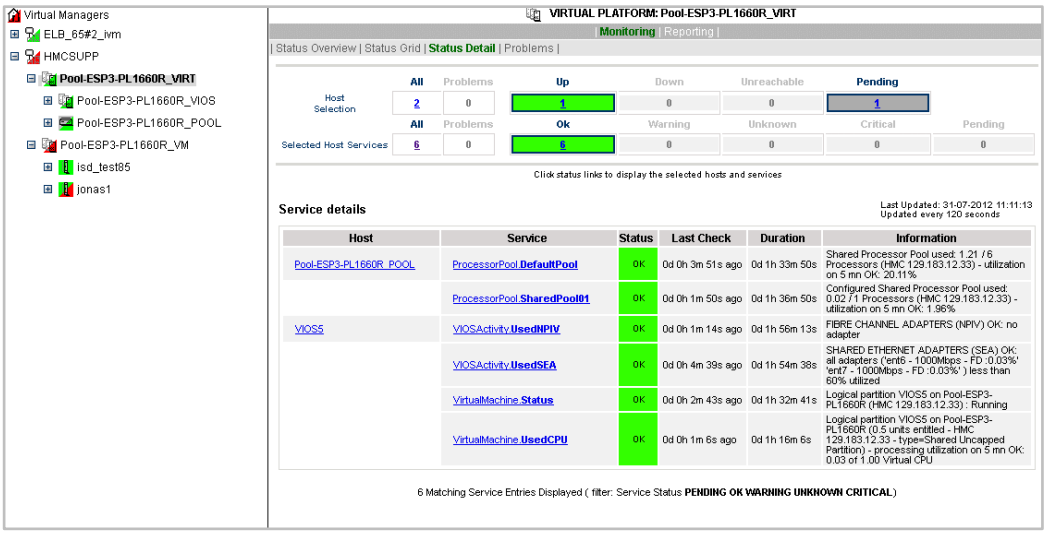


Figure 3-56. HMC Virtualization layer reported supervision

To see all services related to an IVM managed Escala logical partition, use the Virtual Managers view, click the platform node (suffixed by VM) and select Monitoring/Status detail menu. The following page is displayed:

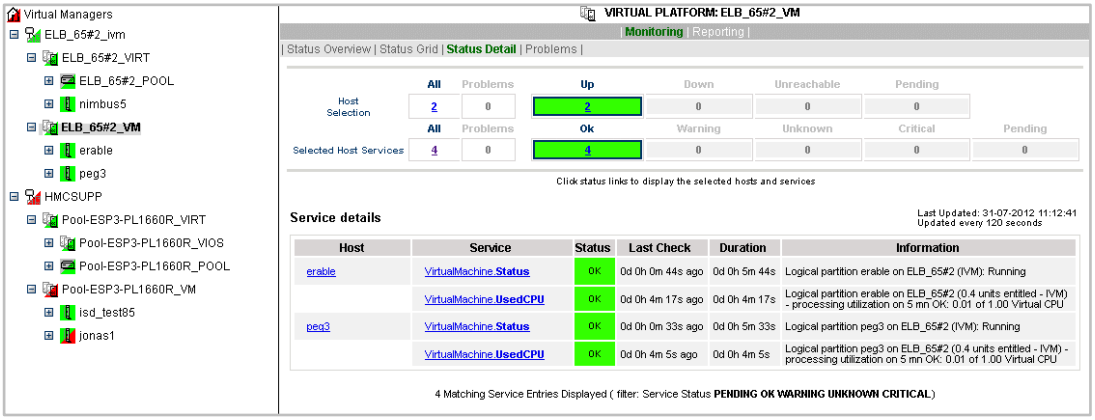


Figure 3-57. Escala IVM reported supervision

To see all services related to an IVM managed virtualization layer, use the Virtual Managers view, click the corresponding platform node (suffixed by VIRT) and select the Monitoring/Status detail menu. The following page is displayed:

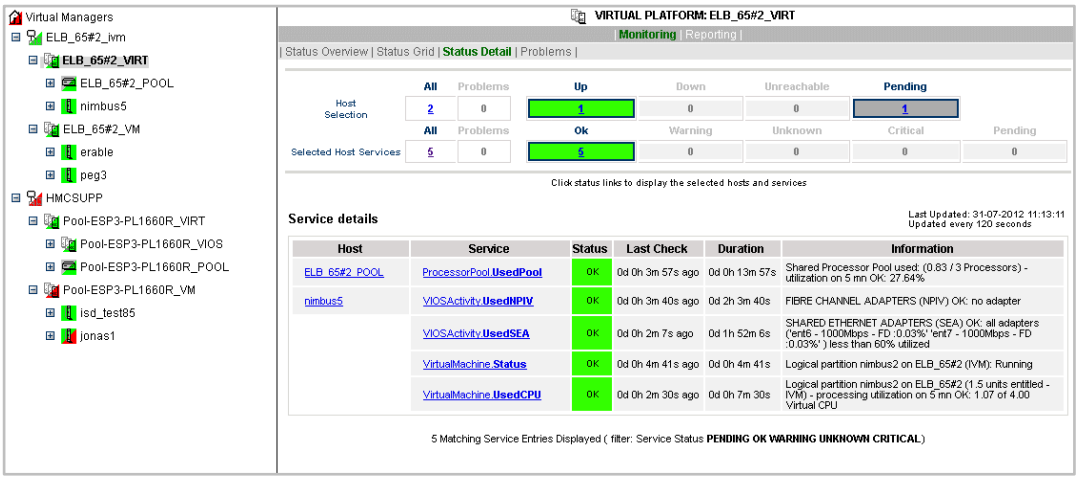


Figure 3-58. IVM Service Details

Escala Reporting

From the host hosting the Vios partition or from host representing the PowerHypervisor layer of HMC managed PL Escala, you can display reporting indicators to see the changes for the utilization of the processing pool.

From any LPAR host, you can display reporting indicators to see the changes in use for the partition CPU

3.4.4 Helios Add-on

The Helios solution consists of a MESCA platform running Linux BAS which emulates the GCOS8 HW. This innovative architecture enables physical partitioning on a single server: GCOS 8, Microsoft® Windows® and Linux® (Red Hat or SuSE) that share system resources through InfiniBand and/or Ethernet fast links. It provides powerful dedicated processors for fast I/O, high telecommunication throughput, and rapid access to large relational databases.

The Helios Add-on retrieves Linux and RDMBS monitoring information from BSM Agent via the NRPE (Nagios Remote Plugin Executor) and GCOS8 monitoring information from SNMP Agent.

The following figure shows links between each component:

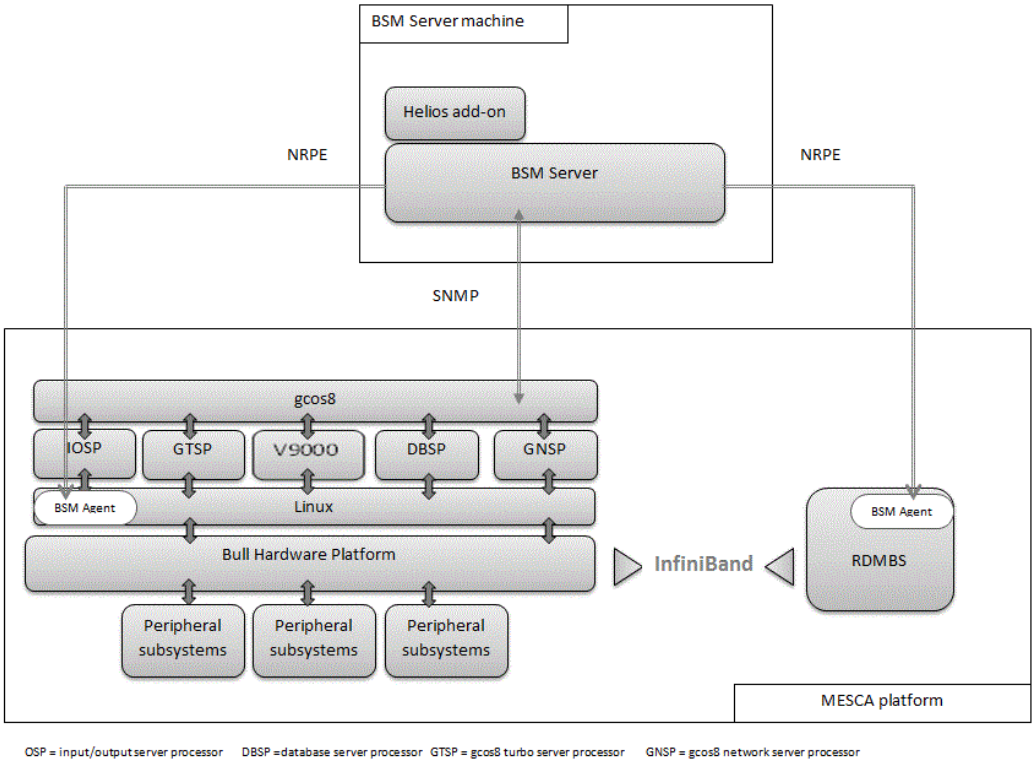


Figure 3-59. Helios Add-on components

Note Monitoring of the Helios solution can be completed with the IBSwitch and CiscoSwitch Add-ons defined in the Network Devices Add-ons part.

3.4.4.1 Configuring Helios Elements

To configure the monitoring elements for the Helios Add-on, you have to define hosts with specific Operating Systems, as detailed in the table below:

Helios element	OS
Linux host	Helios Linux
RDMBS host	DBSS Linux
gcos8 host	GCOS8

Table 3-34. Helios elements

3.4.4.2 Supervising Helios Elements

Services and associated performance indicators are automatically applied to the Helios defined elements.

You can disable Helios supervision by editing each category or service or by disabling Operating System supervision for each host (refer to the *Bull System Manager Administration Guide* for details).

Monitoring Services applied to the Helios Linux layer

Monitoring services defined for the Helios Linux Layer are associated with categories that have name beginning with Helios.

Category	Service	Check_command
HeliosLinuxDisks	AvailableSpace	check_disks.pl [(a)]
	MDCheck	md_check[(b)]
	SMARTstatus	check_smart.sh[(a)]
HeliosLinuxServices	MSMAgent	check_procs[(a)]
	crond	check_procs[(a)]
	klogd	check_procs[(a)]
	macd	check_procs[(a)]
	ntpd	check_procs[(a)]
	syslogd	check_procs[(a)]
	mdmonitor	check_procs[(a)]
	xinetd	check_procs[(a)]
HeliosSystemLoad	CPUuse	check_cpu.sh[(a)]
	Memory	check_memory[(a)]
	Processes	check_procs[(a)]
	CPULoad2	check_cpuload2.sh
HeliosNetwork	Bonding	check_linux_bonding
HeliosStorage	Infiniband	check_ib.sh
	IB_Errors_Port1	check_iberrors
	IB_Errors_Port2	check_iberrors
	EmulexHBA	check_log2.pl[(a)]

Table 3-35. Helios Linux layer – Monitoring Services

(a): command executed on BSM Agent via NRPE protocol
(b): command available only in Helios Appliance

The description of the **check_command** is detailed in 3.4.4.3

Reporting indicators applying to the Helios Linux Layer

Indicator (unit)	Service
<filesystem> (%use)	HeliosLinuxDisks.AvailableSpace
DisksGood (nb unit)	HeliosLinuxDisks.SMARTstatus
DisksBad (nb unit)	
DisksWarn (nb unit)	
DisksUnkn (nb unit)	
Cpu_user (%use)	HeliosSystemLoad.CPUuse
Cpu_sys (%use)	
Cpu_iowait (%use)	
Cpu_idle (%use)	
Load1avg (no Unit)	HeliosSystemLoad.CPULoad2
Load5avg (no Unit)	
Load15avg (no Unit)	
Emulcpu (no Unit)	
setOcpu(no Unit)	
MemPercentUsed (%use)	HeliosSystemLoad.Memory
MemFreeRest (MB Free)	
TotalProcesses (no Unit)	HeliosSystemLoad.Process
Ib0 (nb unit)	HeliosStorage.InfinBand
Ib1 (nb unit)	
Receiving (errors/day)	HeliosStorage.IB_Errors_Port1
Symbolerrors (errors/day)	
Xmtdiscards (errors/day)	
Receiving (errors/day)	HeliosStorage.IB_Errors_Port2
Symbolerrors (errors/day)	
Xmtdiscards (errors/day)	

Table 3-36. Helios Linux layer – Reporting Indicators

Monitoring services applying to GCOS8 host

Category	Service	Check_command
GCOS8_console_msgs	diskDeviceEvent	none
	jobAbortEvent	none
	jobFlowEvent	none
	printerDeviceEvent	none
	tapeDeviceEvent	none
	standardGCOS8Trap	none
GCOS8Stats	g8SystemName	check_snmp
	Processors	check_snmp
	Memory	check_snmp
	g8SystemCpuIdleTime	check_snmp
	g8SystemCpuOverheadTime	check_snmp

Table 3-37. GCOS8 host – Monitoring Services

The description of the **check_command** is detailed in 3.4.4.3.

Reporting indicators applying to GCOS8 host.

Indicator (unit)	Service
g8SystemCpuIdleTime.0 (ms)	GCOS8Stats.g8SystemCpuIdleTime
g8SystemCpuOverheadTime.0 (ms)	GCOS8Stats.g8SystemCpuOverheadTime
g8MemoryPhysical.0 (1024 36-bit words)	GCOS8Stats.Memory
g8MemoryAvailable.0 (1024 36-bit words)	
g8MemoryUsed.0 (1024 36-bit words)	
g8SystemCpuConfigured.0 (nb unit)	GCOS8Stats.Processors
g8SystemCpuAvailable.0 (nb unit)	

Table 3-38. GCOS8 host – Reporting Indicators

Monitoring services applying to RDBMS host

Category	Service	Check_command
DBSSLinuxDisks	AvailableSpace	check_disks.pl (a)
DBSSLinuxDisks	Smartstatus	check_smart.sh (a)
DBSSLinuxServices	DB_MAN	check_procs(a)
DBSSLinuxServices	crond	check_procs (a)
DBSSLinuxServices	rsyslogd	check_procs (a)
DBSSLinuxServices	xinetd	check_procs (a)
DBSSLinuxServices	ntpd	check_procs (a)
DBSSSystemLoad	CPULoad	check_cpuload.sh (a)
DBSSSystemLoad	CPUuse	check_cpu.sh (a)
DBSSSystemLoad	Memory	check_memory (a)
DBSSSystemLoad	Processes	check_procs (a)
DBSSNetwork	Bonding	check_linux_bonding
DBSSStorage	Infiniband	check_ib.sh
DBSSStorage	IB_Errors_Port1	check_iberrors
DBSSStorage	IB_Errors_Port2	check_iberror
DBSSStorage	EmulexHBA	check_log2.pl (a)
DBSSRemoteConnection	A-Authentication	check_log2.pl (a)
DBSSRemoteConnection	B-OpenSession	check_log2.pl (a)
DBSSRemoteConnection	C-SwitchToSupervisor	check_log2.pl (a)
DBSSRemoteConnection	D-CloseSession	check_log2. (a)
DBSSPowerpath	check_dead	check_pp_dead.sh
DBSSMegaRaidCLI	checkmegaraidsas	check_megaraid_sas.pl

Table 3-39. RDBMS host – Monitoring Services

(a): command executed on BSM Agent via NRPE protocol

The description of the check_command is detailed in 3.4.4.3.

Reporting indicators applying to RDBMS Host

Indicator (unit)	Service
<filesystem> (%use)	DBSSLinuxDisks.AvailableSpace
DisksGood (nb unit)	DBSSLinuxDisks.SMARTstatus
DisksBad (nb unit)	
DisksWarn (nb unit)	
DisksUnkn (nb unit)	
Cpu_user (%use)	DBSSSystemLoad.CPUuse
Cpu_sys (%use)	
Cpu_iowait (%use)	
Cpu_idle (%use)	
Load1avg (no Unit)	DBSSSystemLoad.CPULoad
Load5avg (no Unit)	
Load15avg (no Unit)	
Emulcpu (no Unit)	
setOcpu(no Unit)	
MemPercentUsed (%use)	DBSSSystemLoad.Memory
MemFreeRest (MB Free)	
TotalProcesses (no Unit)	DBSSSystemLoad.Process
Ib0 (nb unit)	DBSSStorage.InfiniBand
Ib1 (nb unit)	
Receiving (errors/day)	DBSSStorage.IB_Errors_Port1
Symbolerrors (errors/day)	
Xmtdiscards (errors/day)	
Receiving (errors/day)	DBSSStorage.IB_Errors_Port2
Symbolerrors (errors/day)	
Xmtdiscards (errors/day)	

Table 3-40. RDBMS host – Reporting Indicators

3.4.4.3 Nagios Check Commands

Helios Add-on executes two kinds of check_command:

1. **check_nrpe** to execute system command on BSM Agent. To see details about the system commands used, see the command example in Section 4.3.3.
2. **check_snmp** to execute request on SNMP Agent with the check_snmp plugin. To see details about the plugin check_snmp, see usage in the *BSM Administrator's Guide*, 86 A2 56FA.

3.5 Network Devices Add-ons

The following add-ons are used to monitoring network devices.

3.5.1 CiscoSwitch Add-on

The CiscoSwitch add-on allows to monitor Cisco switch add-on with informations obtained from the SNMP Agent.The following figure shows links between each component:

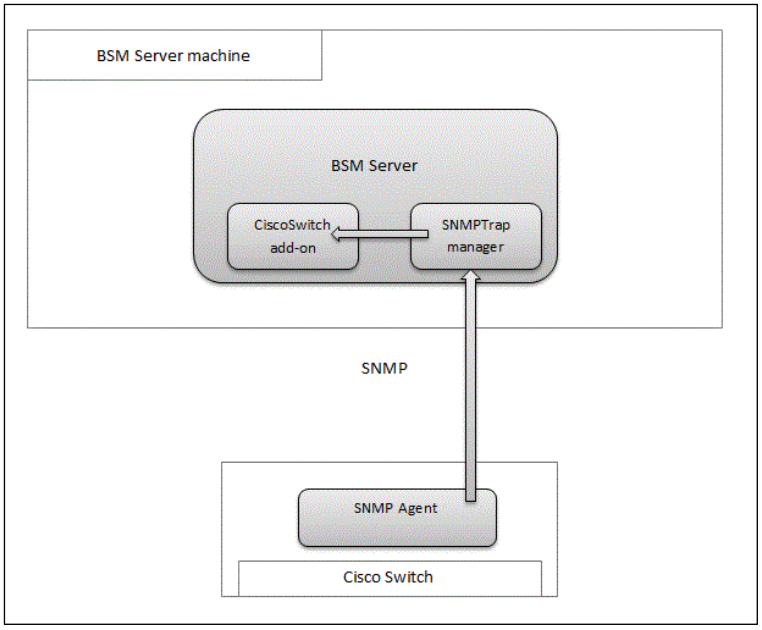


Figure 3-60. CiscoSwitch add-on components

The SNMP Agents must implemented the following MIBs:

- SNMPv2-MIB
- CISCO-CONFIG-MAN-MIB
- CISCO-IPSEC-FLOW-MONITOR-MIB
- CISCO-VTP-MIB
- CISCOTRAP-MIB
- CISCOSB-CDP-MIB
- CISCOSB-COPY-MIB
- CISCOSB-LLDP-MIB
- CISCOSB-RLBRGMULTICAST-MIB
- CISCOSB-PHYSDESCRIPTION-MIB
- CISCOSB-TRAPS-MIB
- DISMAN-PING-MIB
- DISMAN-TRACEROUTE-MIB
- DISMAN-NSLOOKUP-MIB
- LLDP-MIB
- LLDP-EXT-MED-MIB

3.5.1.1 Configuring CiscoSwitch Elements

To configure the monitoring elements for the CiscoSwitch, you have to define host with CiscoSwitch family with the Topology/HostsDefinition/Device hosts/Cisco Switch menu.

Note In this version, only one model is defined in the CiscoSwitches family, the Cisco 300 Series Switches model.

3.5.1.2 Supervising CiscoSwitch Elements

Services are automatically applied to CiscoSwitch defined elements.

You can disable CiscoSwitch supervision by editing each categories or services or by disabling the Network supervision for each hosts (refer to the *Bull System Manager Administration Guide* for details).

Monitoring services applying to CiscoSwitch hosts

All services defined for the CiscoSwitch hosts is based on SNMP Traps emitted by the SNMP Agent. No check_command is associated.

Two categories are defined:

- Cisco category, which applies to any host defined with the CiscoSwitch family
- CiscoSB category, which applies only to host of Cisco 300 Series Swicth model

Category	Service
Cisco	Alerts
	ConfigManAlerts
	IPsecFlow Alerts
	SNMPv2Alerts
CiscoSB	Alerts
	VTPAlerts
	CDPAlerts
	copyAlerts
	macMulticastAlerts
	physdescAlerts
	pingAlerts
	LLDPAlerts
	LLDPstdAlerts
	LLDPMedAlerts

Table 3-41. Cisco Switch monitoring services

3.5.2 IBSwitch Add-on

The IBSwitch add-on allows to monitor InfinBand switch with informations obtained from the SNMP Agent.

The following figure shows links between each component:

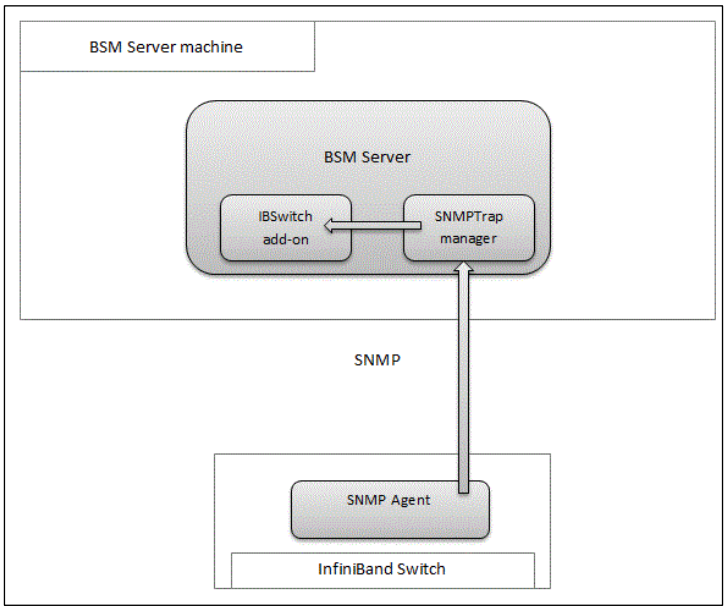


Figure 3-61. IBSwitch add-on components

The SNMP Agents must implemented the SMA-MIB MIB.

3.5.2.1 Configuring IBSwitch Elements

To configure the monitoring elements for the IBSwitch Add-on, you have to define host with InfiniBandSwitch family with the Topology/HostsDefinition/Device hosts/InfiniBand Switch menu.

Note In this version, only one model is defined in the CiscoSwitches family, the Voltaire InfinBand Switches model.

3.5.2.2 Supervising IBSwitch Elements

Services are automatically applied to IBSwitch defined elements.

You can disable IBSwitch supervision by editing each categories or services or by disabling the Network supervision for each hosts (refer to the *Bull System Manager Administration Guide* for details).

Monitoring services applying to IBSwitch hosts

All services defined for the IBSwitch hosts is based on SNMP Traps emitted by the SNMP Agent. No check_command is associated.

Category	Service
IBVoltaire	Alerts

Table 3-42. InfiniBand Switch monitoring service

Chapter 4. Check Commands for Add-on Customizable Services

This chapter describes the usage of the check commands for the customizable services. These Linux commands run only under CYGWIN on Windows.

4.1 Internal Storage Management Add-ons

The following check commands apply to the internal storage management Add-ons.

4.1.1 BSMGAMTT Add-on

The **check_gamttraid** check command applies to the **BSMGAMTT** Add-on and uses the following shell (PERL) command options.

Usage

```
check_gamttraid -H <host> [-C <community>] [-p <port>] [-t <timeout>]
{ [-A {ALL|<Ct>}] | [-P {ALL|<Ct>.<Ch>.<Tg>}] | [-L {ALL|<Ct>.<Ldn>}] }
[-v <vl>] [-f <f>]
```

-H, –hostname <host>	Hostname or IP address of target to check
-C, –community <community>	SNMP community string (defaults to **public**)
-p, –port <port>	SNMP port (defaults to 161)
-t, –timeout <timeout>	Seconds before timing out (defaults to **Nagios** timeout value)
-A, –adapter ALL | <Ct>	Controller board
-P, –physical ALL | <Ct>.<Ch>.<Tg>	Physical device addr
-L, –logical ALL | <Ct>.<Ldn>	Logical drive addr
-v, —verbosity <vl>	Verbosity level: **0** None **1** Adds the <CtrlModel> and the status of all controller boards filtered
-f, –format <f>	**0** Carriage Return in ASCII mode (\n) **1** Carriage Return in HTML mode ( )

Return code

OK (0), WARNING (1), CRITICAL (2), UNKNOWN (3)

- OK
  All logical drives and all physical devices run normally.
- WARNING
  At least one logical drive or one physical device is in a WARNING state.
- CRITICAL
  At least one logical drive or one physical device is in a CRITICAL state.
- UNKNOWN
  All other types of processing errors (bad parameter, no response, and so on).

Note In the case of multiple errors, the global state will be the most severe one; CRITICAL > WARNING > OK.

Output

A string composed with a global state descriptor followed, if they exist, by error states of the components concerned (controller, Logical Device, Physical Device).

global state descriptor

The first line shows the global state. The syntax is:

```
GAMTT RAID [CT |PD |LD ]<GlobalStatus>
```

"CT " if "-A".

"PD " if "-P".

"LD " if "-L".

state descriptor by controller

These may be present after the global state descriptor if an error exists.

The syntax is:

```
[ CT(Ct<Ct>) <CtrlModel> <CtrlStatus>
[{LD(Ct<Ct> Nu<Ldn>) <LDType> <LDStatus>[, ] …}]
[{PD(Ct<Ct> Ch<Ch> Tg<Tg>) <PDType> <PDStatus>[, ] …}]
…]
```

<GlobalStatus>	most severe status detected
<CtrlModel>	controller model
<CtrlStatus>	most severe state detected for an element of this controller (LD and PD)
<Ct>	controller number
<Ldn>	logical drive number
<LDType>	logical drive type: RAIDx or JBOD
<LDStatus>	logical drive status
<Ct>	controller number
<Ch>	channel number
<Tg>	target number
<PDType>	physical device type: Disk, Processor, Ctrl Channel, □
<PDStatus>	physical device status

Examples

If global state is **OK**:

```
> check_gamttraid -H <host>
GAMTT RAID OK
>

> check_gamttraid -H <host> -P 0.0.1
GAMTT RAID PD OK
>

> check_gamttraid -H <host> -L 0.0
GAMTT RAID LD OK
>

> check_gamttraid -H <host> –v 1
GAMTT RAID OK
CT(Ct0) MegaRAID Ultra320-2x OK
CT(Ct1) DAC960FFX2 OK
CT(Ct2) MegaRAID Ultra320-2x OK
>

> check_gamttraid -H <host> -A 1 –v 1
GAMTT RAID CT OK
CT(Ct1) DAC960FFX2 OK
>
```

If global state is **CRITICAL** or **WARNING**, only the elements concerned are displayed:

```
> check_gamttraid -H <host>
GAMTT RAID CRITICAL
CT(Ct0) MegaRAID Ultra320-2x CRITICAL
PD(Ct0 Ch0 Tg1) Disk Dead
>

> check_gamttraid -H <host> -L 0.1
GAMTT RAID LD CRITICAL
CT(Ct0) MegaRAID Ultra320-2x CRITICAL
LD(Ct0 Nu1) RAID5 Critical
>
```

If return code is **UNKNOWN**:

```
> check_gamttraid -H <host>
GAMTT RAID UNKNOWN - snmp query timed out
>
```

4.1.2 BSMLSICIM Add-on

The **check_LSICIM** check command applies to the **BSMLSICIM** Add-on and uses the following shell (PERL) command options:

Usage

```
check_LSICIM –H <host> [-C <ctrlname>]
```

-H, –hostname <host> Hostname or IP address of target to check

-C, –ctrlname <ctrlname> Name of the controller to check

Note The name of the controller must be protected with a quotation mark if the name contains blank characters.

Return code

OK (0), WARNING (1), CRITICAL (2), UNKNOWN (3)

- OK
  All controllers run normally.
- WARNING
  At least one controller is in a WARNING state.
- CRITICAL
  At least one controller is in a CRITICAL state.
- UNKNOWN
  All other types of processing errors (bad parameter, no response, etc.).

Note In the case of multiple errors, the global state will be the most severe one; CRITICAL > WARNING > OK.

Output

A string indicates the state of mirroring followed, where applicable, by the component error states (controller, Logical Device, Physical Device) concerned.

If the GlobalStatus determined by the most severe status of components is not OK, the state of the component is reported with the following format:

```
[CT(Ct<Ct>) <CtrlName> <CtrlStatus>
[{> LD(Ct<Ct> Nu<Ldn>) <LDType> <LDStatus>[, ] …}]
[{  - PD(Ct<Ct> Ch<Ch> Tg<Tg>) <PDManufacturer> <PDModel> <PDStatus>[,
[{> PD(Ct<Ct> Ch<Ch> Tg<Tg>) <PDManufacturer> <PDModel> <PDStatus>[, ] …}]
```

<Ct>	controller number
<CtrlModel>	controller model
<CtrlStatus>	worst state detected for an element of this controller (LD and PD)
<Ldn>	logical drive number
<LDType>	logical drive type: IM
<LDStatus>	logical drive status as reported by the LSI CIM provider
<Ch>	channel number
<Tg>	target number
<PDManufacturer>	physical device manufacturer
<PDModel>	physical device model
<PDStatus>	physical device status as reported by the LSI CIM provider

Examples

```
$ ./check_LSICIM -H 172.31.50.71
: LSI SCSI storage - Integrated Mirroring not available –

LSI SCSI storage - Integrated Mirrored available -
CT(0) LSI 53C1030 CRITICAL
> LD(Ct0 Ch2 Tg0) IMVolume: Degraded Redundancy
  - PD(Ct0 Ch3 Tg0) SEAGATE ST373454LC: Error


$ ./check_LSICIM –H 172.31.50.71 -C 'LSI SCSI1030 – 0'

> CT(0) LSI 53C1030 OK

$ ./check_LSICIM -H 172.31.50.71 -C 'LSI SCSI1030 - 0'
> CT(0) LSI 53C1030 CRITICAL
  - PD(Ct0 Ch0 Tg0) MAXTOR ATLAS10K4_36SCA CRITICAL
```

4.1.3 BSMMegaRaidSAS Add-on

The **check_MegaRaidSAS(_IR** check command applies to the **BSMMegaRaidSAS** Add-on and uses the following shell (PERL) command options.

Usage

check_MegaRaidSAS(_IR) `-H <host> [-C <community>] [-p <port>] [-t <timeout>] { [-A {ALL|<Ct>}] | [-P {ALL|<Ct.Pdn>}] | [-L {ALL|<Ct.Ldn>}] } [-f <f>]`

-H, –hostname <host>	Hostname or IP address of target to check
-C, –community <community>	SNMP community string (defaults to **public**)
-p, –port <port>	SNMP port (defaults to 161)
-t, –timeout <timeout>	Seconds before timing out (defaults to **Nagios** timeout value)
-A, –adapter ALL | <Ct>	Controller board
-P, –physical ALL | <Ct.Pdn>	Physical device identifier
-L, –logical ALL | <Ct.Ldn>	Virtual drive identifier
-f, –format <f>	**0** Carriage Return in HTML mode ( ) **1** Carriage Return in ASCII mode (\n)

Return code

OK (0), WARNING (1), CRITICAL (2), UNKNOWN (3)

- OK
  All logical drives and all physical devices run normally.
- WARNING
  At least one logical drive or one physical device is in a WARNING state.
- CRITICAL
  At least one logical drive or one physical device is in a CRITICAL state.
- UNKNOWN
  All other types of processing errors (bad parameter, no response, and so on).

Note In the case of multiple errors, the global state will be the most severe one; CRITICAL > WARNING > OK.

Output

A string composed of a global state descriptor followed, if they exist, by error states of the component (controller, Logical Device, Physical Device) concerned.

Global state descriptor

The first line shows the global state. The syntax is:

```
MegaRAID SAS [CT |PD |LD ]<GlobalStatus>
```

"CT " if "-A".

"PD " if "-P".

"VD " if "-L".

state descriptor by controller

These may be present after the global state descriptor if an error exists.

The syntax is:

```
[ CT(Ct<Ct>) <CtrlModel> <CtrlStatus>
[PD(CT<id> DEV<id> ENC<id> SLOT<id> SN<number>) <PDType>
<PDStatus> …]
[VD(CT<id> DEV<id>) <RAIDLevel> <VDStatus> …]
…]
```

<CtrlModel>	controller model
<CtrlStatus>	most severe state detected for a controller
<id>	controller or Drive or Logical drive index
<RAIDLevel>	RAID level (0,1,5,10,50,60)
<VDStatus>	logical drive status
<PDType>	physical device type: Disk, Processor, Ctrl Channel,
<PDStatus>	physical device status
<SN>	serial number of physical drive

Examples

If the global state is OK:

```
> check_MegaRaidSAS -H <hostname>
MegaRAID SAS CT OK
CT0 MegaRAID SAS 8408E OK
PD: 4
VD: 2 ( RAID0, 1 RAID1)
>

> check_MegaRaidSAS -H < hostname > -A ALL
MegaRAID SAS CT OK
CT0 MegaRAID SAS 8408E OK
PD: 4
VD: 2 ( RAID0, 1 RAID1)
>

> check_MegaRaidSAS-H < hostname > -L ALL
MegaRAID SAS VD OK
>

> check_MegaRaidSAS-H < hostname > -P  ALL
MegaRAID SAS PD OK
>

> check_MegaRaidSAS-H < hostname > -P 0.2
MegaRAID SAS PD OK
>

> check_MegaRaidSAS-H < hostname > -L 0.1
MegaRAID SAS VD OK
>
```

If the global state is CRITICAL or WARNING, only the elements concerned are displayed:

```
> check_MegaRaidSAS -H <hostname> -L ALL
MegaRAID SAS VD WARNING
VD(CT0 DEV0) RAID1 degraded
VD(CT0 DEV2) RAID1 degraded>
>

> check_MegaRaidSAS -H <hostname>
MegaRAID SAS CT CRITICAL
CT0 MegaRAID SAS 8408E CRITICAL
PD: 4
VD: 2 ( RAID0, 1 RAID1)
PD(CT0 DEV0 ENC1 SLOT0 SN50010b90000972e2) DISK offline>
VD(CT0 DEV0) RAID1 degraded
VD(CT0 DEV1) RAID0 offline>
>
```

If the return code is UNKNOWN:

```
> check_MegaRaidSAS-H <hostname>
MegaRAID SAS UNKNOWN - no MegaRAID SAS Adapter present

>
```

4.1.4 BSMEmulexHBA Add-on

The check_EmulexHBA check command applies to the BSMEmulexHBA Add-on and uses the following shell (PERL) command options.

Usage

```
check_EmulexHBA -H <host> -a <action> [-p <port>] -u <utility>
[-t <timeout>] [-P <hbacmdpath>] [-f <f>]
```

-H, –hostname <host>	Hostname or IP address of target to check
-a, –action <action>	Action on Emulex HBA, value: Status
-p, –port <port>	CIM port (defaults to 5989)
-u, –utility<utility>	Tool used by action, values: CIM, SNMP
	CIM: for managed ESX hosts
	SNMP: for managed Windows or Linux hosts
-t, –timeout <timeout>	Seconds before timing out (defaults to Nagios timeout value)
-P, –hbacmdpath	Path to hbacmd.exe (only used on Windows), defaults to C:\ Program Files\Emulex\Util\OCManager\HbaCmd.exe
-f, –format <f>	0 Carriage Return in HTML mode ( ) (default value) 1 Carriage Return in ASCII mode (\n)

Return code

OK (0), WARNING (1), CRITICAL (2), UNKNOWN (3)

- OK
  All logical drives and all physical devices run normally.
- WARNING
  At least one logical drive or one physical device is in a WARNING state.
- CRITICAL
  At least one logical drive or one physical device is in a CRITICAL state.
- UNKNOWN
  All other types of processing errors (bad parameter, no response, and so on).

Note In the case of multiple errors, the global state will be the most severe one; CRITICAL > WARNING > OK.

Output

A string composed of a global state descriptor followed by an state descriptor for each component (HBA port).

Global state descriptor

The first line shows the global state. The syntax is:

```
Emulex HBA <GlobalStatus>
```

State descriptor by HBA port

The syntax is:

```
Status  <status> for port <HbaPortNb>, WWN=<HbaWwn>, model=<HbaModel>,
serial nb=<HbaSerialnb>
```

< status >	Status of HBA port
< HbaPortNb >	HBA port number
< HbaWwn >	HBA World Wide Name
< HbaModel >	HBA model
< HbaSerialnb >	HBA serial number

Examples

If the global state is OK (on Windows for managed Windows or Linux hosts):

```
> check_EmulexHBA -H <hostname> -a <action> -u <utility>

Emulex HBA OK

Status Link Up for port 0, WWN=10:00:00:00:c9:88:1a:66, model=LPe12002-
M8, serial number=VM92275396

Status Link UP for port 1, WWN=10:00:00:00:c9:88:1a:67, model=LPe12002-
M8, serial number=VM92275396

>
```

If the global state is WARNING (on Windows for managed ESX hosts):

```
> check_EmulexHBA -H <hostname> -a <action> -u <utility>

Emulex HBA WARNING

Status Link Down for port 0, WWN=10:00:00:00:c9:88:1a:66, model=LPe12002-
M8, serial number=VM92275396

Status Link DOWN for port 1, WWN=10:00:00:00:c9:88:1a:67, model=LPe12002-
M8, serial number=VM92275396

>
```

If the global state is WARNING (on Linux for managed ESX hosts):

```
> check_EmulexHBA -H <hostname> -a <action> -u <utility>

Emulex HBA WARNING

Status Other for port 0, WWN=10:00:00:00:c9:88:1a:66, model=LPe12002-M8,
serial number=VM92275396

Status Other for port 1, WWN=10:00:00:00:c9:88:1a:67, model=LPe12002-M8,
serial number=VM92275396

>
```

Note In the example above, for the same state, Emulex Core Kit CLI on Windows returns **Link Down**, while WBEM CLI on Linux returns **Other**.

4.2 External Storage Management

The following check commands apply to the external storage management Add-ons.

4.2.1 BSMStoreWayFDA

The **check_necfda** command applies to the **BSMStoreWayFDA** Add-on and uses the following shell (PERL) command options:

Usage

```
check_necfda -H <host> [-C <community>] [-p <port>] [-t <timeout>] [-f
<f>]
```

-H, –hostname <host>	Hostname or IP address of the target to check
-C, –community <community>	SNMP community string (defaults to **public**)
-p, –port <port>	SNMP port (defaults to 161)
-t, –timeout <timeout>	Seconds before timing out (defaults to Nagios timeout value)
-f, –format <f>	**0** Carriage Return in ASCII mode (\n) **1** Carriage Return in HTML mode ( )

```
check_necfda –help
```

-h, –help Display help

```
check_necfda –version
```

-V, –version Display version

Return code

OK (0), WARNING (1), CRITICAL (2), UNKNOWN (3)

Output

The first line shows the global state in the following format:

```
necfda <GlobalStatus>
```

<GlobalStatus> Most severe state detected for a controller.

Examples

If the global state is OK

```
> check_necfda -H <host>
necfda OK
>
```

If the global state is CRITICAL or WARNING, only the errors are displayed.

When the return code is UNKNOWN:

```
> check_necfda -H <host>
necfda CRITICAL
>

> check_necfda -H <host>
necfda WARNING
>

> check_necfda -H <host>
necfda UNKNOWN - snmp query timed out
>

> check_necfda -H <host>
necfda UNKNOWN - no data received
>
```

4.2.2 BSMEmcClariion

The **check_EmcClariion** command applies to the **EmcClariion** Add-on and uses the following shell (PERL) command options:

Usage

```
check_EmcClariion -H <host> [-C <community>] [-p <port>] [-t <timeout>]
[-f <f>]
```

-H, –hostname <host>	Hostname or IP address of the target to check
-C, –community <community>	SNMP community string (defaults to **public**)
-p, –port <port>	SNMP port (defaults to 161)
-t, –timeout <timeout>	Seconds before timing out (defaults to Nagios timeout value)
-f, –format <f>	**0** Carriage Return in HTML mode ( ) **1** Carriage Return in ASCII mode (\n)

```
check_EmcClariion –help
```

-h, –help Display help

```
check_EmcClariion –version
```

-V, –version Display version

Return code

OK (0), WARNING (1), CRITICAL (2), UNKNOWN (3)

Output

The first line shows the global state in the following format:

```
EmcClariion <GlobalStatus>
```

<GlobalStatus> Most severe state detected for a controller.

Examples:

If the global state is OK:

```
> check_EmcClariion -H <host>
EmcClariion CX200 B-APM00024600159 OK
>
```

If the global state is CRITICAL or WARNING, only the errors are displayed :

```
> check_EmcClariion -H <host>
EmcClariion CX200 B-APM00024600159 CRITICAL
>

> check_EmcClariion -H <host>
EmcClariion CX200 B-APM00024600159 WARNING
>
```

When the return code is UNKNOWN:

```
> check_EmcClariion -H <host>
EmcClariion UNKNOWN - snmp query timed out
>

> check_EmcClariion -H <host>
EmcClariion UNKNOWN - no data received
>
```

4.2.3 BSMNetApp

The **BSMNetApp** Add-on uses the following check commands:

4.2.3.1 check-netapp-cpuload

check-netapp-cpuload uses the following shell (PERL) command options:

Usage

```
check_snmp -H <host> -C <community> -o <OID> -w <warning range>]
-c <critical range> -u <unit label>  -l <label>
```

-H, –hostname <host>	Hostname or IP address of the target to check
-C, –community <community>	SNMP community string (defaults to public)
-o, –oid <OID>	object identifier to query
-w, –warning <int>	range which will not result in a WARNING status
-c, –critical <int>	range which will not result in a CRITICAL status
-u, –units <string>	units label for output data (e.g., 'sec.', '%')
-l, –label <string>	prefix label for output data from plugin (default: –s 'SNMP')

Return code

OK (0), WARNING (1), CRITICAL (2), UNKNOWN (3)

Output

The output shows the state in the following format:

```
CPU LOAD <Status> - <int> %
```

<Status>	status of the command
<int>	CPU load.

Examples

If the state is OK:

```
> check_snmp -H $HOSTADDRESS$ -C public -o .1.3.6.1.4.1.789.1.2.1.3.0 -w
90 -c 95 -u '%' -l "CPU LOAD"
CPU LOAD OK – 8%
>
```

If the global state is CRITICAL or WARNING:

```
> check_snmp -H $HOSTADDRESS$ -C public -o .1.3.6.1.4.1.789.1.2.1.3.0 -w
90 -c 95 -u '%' -l "CPU LOAD"
CPU LOAD WARNING – 92%
```

```
> check_snmp -H $HOSTADDRESS$ -C public -o .1.3.6.1.4.1.789.1.2.1.3.0 -w
90 -c 95 -u '%' -l "CPU LOAD"
CPU LOAD CRITICAL – 99%
```

4.2.3.2 check-netapp-numdisks

check-netapp-numdisks uses the following shell (PERL) command options:

Usage

```
check_snmp -H <host> -C <community> -o <OID1,OID2,OID3,OID4>
-u <unit label>  -l <label>
```

-H, –hostname <host>	Hostname or IP address of the target to check
-C, –community <community>	SNMP community string (defaults to ”public”)
-o, –oid <OID>	object identifiers to query
-u, –units <string>	units label for output data (e.g., ‘sec.’, ‘%’)
-l, –label <string>	prefix label for output data from plugin (default: –s ‘SNMP’)

Return code

OK (0), WARNING (1), CRITICAL (2), UNKNOWN (3)

Output

The output shows the state in the following format:

```
<Status> - <int> Total Disks <int> Active <int> Spare <int> Failed
```

<Status>	status of the command
<int>	number of disks.

Examples

If the state is OK

```
> check_snmp -H $HOSTADDRESS$ -C public -o
.1.3.6.1.4.1.789.1.6.4.1.0,.1.3.6.1.4.1.789.1.6.4.2.0,.1.3.6.1.4.1.789.1.
6.4.8.0,.1.3.6.1.4.1.789.1.6.4.7.0 –u 'Total
Disks','Active','Spare','Failed' -l ""
OK – 8 Total Disks 7 Active 1 Spare 0 Failed
>
```

If the state is WARNING

```
> check_snmp -H $HOSTADDRESS$ -C public -o
.1.3.6.1.4.1.789.1.6.4.1.0,.1.3.6.1.4.1.789.1.6.4.2.0,.1.3.6.1.4.1.789.1.
6.4.8.0,.1.3.6.1.4.1.789.1.6.4.7.0 –u 'Total
Disks','Active','Spare','Failed' -l ""
WARNING – 8 Total Disks 6 Active 1 Spare 1 Failed
>
```

4.2.3.3 check-netapp-failedfans

check-netapp-failedfans uses the following shell (PERL) command options:

Usage

```
check_snmp -H <host> -C <community> -o <OID> -l <label>
```

-H, –hostname <host>	Hostname or IP address of the target to check
-C, –community <community>	SNMP community string (defaults to ”public”)
-o, –oid <OID>	object identifiers to query
-l, –label <string>	prefix label for output data from plug-in (default: –s ‘SNMP’)

Return code

OK (0), WARNING (1), CRITICAL (2), UNKNOWN (3)

Output

The output shows the state in the following format:

```
Fans <Status> - < msg>
```

<Status>	status of the command
<msg>	msg concerning failed fans

Examples

If the state is OK:

```
> check_snmp -H $HOSTADDRESS$ -C public -o .1.3.6.1.4.1.789.1.2.4.3.0 -l
"Fans"

Fans OK – There are no failed fans.
>
```

If the state is WARNING:

```
> check_snmp -H $HOSTADDRESS$ -C public -o .1.3.6.1.4.1.789.1.2.4.3.0 -l
"Fans"

Fans WARNING – There are 2 failed fans.
>
```

4.2.3.4 check-netapp-failedpwr

check-netapp-failedpwr uses the following shell (PERL) command options:

Usage

```
check_snmp -H <host> -C <community> -o <OID> -l <label>
```

-H, –hostname <host>	Hostname or IP address of the target to check
-C, –community <community>	SNMP community string (defaults to "public")
-o, –oid <OID>	object identifiers to query
-l, –label <string>	prefix label for output data from plugin (default: –s 'SNMP')

Return code

OK (0), WARNING (1), CRITICAL (2), UNKNOWN (3)

Output

The output shows the state in the following format:

```
Power <Status> - < msg>
```

<Status>	status of the command
<msg>	msg concerning failed power supplies.

Examples

If the state is OK:

```
> check_snmp -H $HOSTADDRESS$ -C public -o .1.3.6.1.4.1.789.1.2.4.5.0 -l
"Power"

Power OK – There are no failed power supplies.
>
```

If the state is WARNING:

```
> check_snmp -H $HOSTADDRESS$ -C public -o .1.3.6.1.4.1.789.1.2.4.5.0 -l
"Power"


Power WARNING – There are 2 failed power supplies.
>
```

4.2.3.5 check_netapp_globalstatus

check_netapp_globalstatus uses the following shell (PERL) command options:

Usage

```
check_NetAppGlobalStatus -H <host> [-C <community>] [-p <port>]
[-t <timeout>] [-f <f>]
```

-H, –hostname <host>	Hostname or IP address of the target to check
-C, –community <community>	SNMP community string (defaults to **public**)
-p, –port <port>	SNMP port (defaults to 161)
-t, –timeout <timeout>	Seconds before timing out (defaults to Nagios timeout value)
-f, –format <f>	**0** Carriage Return in HTML mode ( ) **1** Carriage Return in ASCII mode (\n)

```
check_NetAppGlobalStatus –help
```

-h, –help	Display help

```
check_NetAppGlobalStatus –version
```

-V, –version	Display version

Return code

OK (0), WARNING (1), CRITICAL (2), UNKNOWN (3)

Output

The output shows the global state in the following format:

```
<GlobalStatus> - <msg>
```

<GlobalStatus>	Global state of the NetApp storage system.
<msg>	message explaining the global state

Examples

If the global state is OK :

```
> check_NetAppGlobalStatus -H <host>
OK – The system’s global status is normal
>
```

If the global state is CRITICAL or WARNING:

```
> check_NetAppGlobalStatus -H <host>
WARNING - /vol/luns is full (using or reserving 100% of space and 0% of
inodes, using 63% of reserve).
>
```

4.2.3.6 check_netappvol

check_netappvol uses the following shell (PERL) command options:

Usage

```
check_NetAppVol -H <host> [-C <community>] [-p <port>] [-t <timeout>]
[-f <f>]
```

-H, –hostname <host>	Hostname or IP address of the target to check
-C, –community <community>	SNMP community string (defaults to public)
-p, –port <port>	SNMP port (defaults to 161)
-t, –timeout <timeout>	Seconds before timing out (defaults to Nagios timeout value)
-f, –format <f>	0 Carriage Return in HTML mode ( ) 1 Carriage Return in ASCII mode (\n)

```
check_NetAppGlobalVol –help
```

-h, –help	Display help

```
check_NetAppGlobalVol –version
```

-V, –version	Display version

Return code

OK (0), WARNING (1), CRITICAL (2), UNKNOWN (3)

Output

The first line shows the global volume state in the following format:

```
NetApp <model> <GlobalVolumeStatus>
```

<GlobalVolumeStatus>	Global state of all volumes of the NetApp storage system.
<model>	model of NetApp storage system

The following lines show the status of each volume

```
Volume <name>, <status> (<raidtype, <voltype>, <aggregateName>)
```

Examples

If the global state is OK:

```
> check_NetAppGlobalStatus -H <host>
NetApp FAS3020 RAID OK
Volume vol0, online (raid_dp, flexible, aggr0)
Volume BULL_TRAVAIL, online (raid_dp, flexible, BULL)
Volume luns, online (raid_dp, flexible, BULL)
Volume GORKI, online (raid_dp, flexible, aggr1)
>
```

If the global state is CRITICAL or WARNING:

```
> check_NetAppGlobalStatus -H <host>
NetApp FAS3020 RAID WARNING
Volume vol0, online (raid_dp, flexible, aggr0)
Volume BULL_TRAVAIL, online (raid_dp, flexible, BULL)
Volume luns, online (raid_dp, flexible, BULL)
Volume GORKI, offline (raid_dp, flexible, aggr1)
>
```

4.2.3.7 check_netappraid

check_netappraid uses the following shell (PERL) command options:

Usage

```
check_NetAppGlobalRaid -H <host> [-C <community>] [-p <port>] [-t
<timeout>] [-f <f>]
```

-H, –hostname <host>	Hostname or IP address of the target to check
-C, –community <community>	SNMP community string (defaults to **public**)
-p, –port <port>	SNMP port (defaults to 161)
-t, –timeout <timeout>	Seconds before timing out (defaults to Nagios timeout value)
-f, –format <f>	0 Carriage Return in HTML mode ( ) 1 Carriage Return in ASCII mode (\n)

```
check_NetAppRaid –help
```

-h, –help	Display help

```
check_NetAppRaid –version
```

-V, –version	Display version

Return code

OK (0), WARNING (1), CRITICAL (2), UNKNOWN (3)

Output

The first line shows the global state of all RAID groups in the following format:

```
NetApp <model> <GlobalRgStatus>
```

<GlobalRgStatus>	Global state of all raid groups of the NetApp storage system.
<model>	model of NetApp storage system

The following lines show the status of each RAID group

```
RAID group <name> <status>
```

Examples

If the global Raid group state is OK:

```
> check_NetAppRaid -H <host>
NetApp FAS3020 RAID OK
RAID group /aggr0/plex0/rg0 active
RAID group /BULL/plex0/rg0 active
RAID group /aggr1/plex0/rg0 active
>
```

If the global Raid group state is CRITICAL or WARNING:

```
> check_NetAppRaid -H <host>
NetApp FAS3020 RAID WARNING
RAID group /aggr0/plex0/rg0 active
RAID group /BULL/plex0/rg0 active
RAID group /aggr1/plex0/rg0 reconstructionInProgress
>
```

4.2.4 BSMWaterCooledDoor

The **BSMWaterCooledDoor** Add-on uses the **check_sensor** check command that uses the following shell (PERL) command options:

Usage

```
check_sensor [-h] -m model [-H host] [-u user] [-p password] -s sensorid
[-F factor] [-c lowercrit] [-w lowerwarn] [-W upperwarn] [-C uppercrit]
```

-h	Help
-m model	Remote host model: ipmilan
-H host	Remote host name or ipaddr
-u user	Remote SMU username
-p password	Remote SMU or MWA password
-s sensorid	Specify the sensor id string
-F factor	Specify the factor to apply to the reading value
-c lowercrit	Specify the sensor lower critical level
-w lowerwarn	Specify the sensor lower warning level
-C uppercrit	Specify the sensor upper critical level
-W upperwarn	Specify the sensor upper warning level

Return code

OK(0), WARNING(1), CRITICAL(2), UNKNOWN(3).

Output

The output shows the state and the value of the sensor in the following format:

```
<sensor status> : <value>
```

Examples

```
> check_sensor -m ipmilan -H 172.31.50.71 -u super -p pass -s 'Pwr
Consumption'

OK : 142.480 Watts

>

> check_sensor -m ipmilan -H 172.31.50.71 -u super -p pass -s 'Valve
Vperture'

OK : 21.750 %

>

> check_sensor -m ipmilan -H 172.31.50.71 -u super -p pass -s 'Air
Pressure' –F 1000

OK : 19 Pa

>

check_sensor -m ipmilan -H 172.31.50.71 -u super -p pass -s ’Average
Temp.’


OK : 18.3 degrees C

>
```

4.2.5 BSMStoreWayDPA

The **BSMStoreWayDPA** Add-on uses the **check_StoreWayDPA** check command that uses the following shell (PERL) command options:

Usage

```
check_StoreWayDPA -H <host> [-C <community>] [-p <port>] [-t <timeout>]
[-f <f>]
```

-H, –hostname <host>	Hostname or IP address of the target to check
-C, –community <community>	SNMP community string (defaults to **public**)
-p, –port <port>	SNMP port (defaults to 161)
-t, –timeout <timeout>	Seconds before timing out (defaults to Nagios timeout value)
-f, –format <f>	0 Carriage Return in HTML mode ( ) 1 Carriage Return in ASCII mode (\n)

```
check_StoreWayDPA –help
```

-h, –help	Display help

```
check_StoreWayDPA –version
```

-V, –version	Display version

Return code

OK (0), WARNING (1), CRITICAL (2), UNKNOWN (3)

Output

The first line shows the task state in the following format:

```
StoreWay DPA <TaskStatus>
```

<TaskStatus>	Most severe task state detected on a StoreWay DPA system.

Examples

If the task state is OK:

```
> check_StoreWayDPA -H <host>
StoreWay DPA OK
>
```

If the global state is CRITICAL, only the tasks with state stopped are displayed :

```
> check_StoreWayDPA -H <host>
StoreWay DPA  CRITICAL

Backup Engine stopped
>

> check_StoreWayDPA -H <host>
StoreWay DPA CRITICAL

Task Launcher stopped
>

> check_StoreWayDPA -H <host>
StoreWay DPA CRITICAL

Backup Engine and Task Launcher stopped
>
```

When the return code is UNKNOWN:

```
> check_StoreWayDPA -H <host>
StoreWay DPA UNKNOWN - snmp query timed out
>

> check_StoreWayDPA -H <host>
StoreWay DPA UNKNOWN - no data received
>
```

4.2.6 BSMSwitchBrocade

The **BSMSwitchBrocade** Add-on uses the **check_brocade, check_brocade_port** and **check_brocade_hw** check commands with the following shell (PERL) command options:

check_brocade_hw check command

Usage

check_FCBrocade_hardware.sh `-H <host IP address> -c <community>`

-H <host>	Hostname or IP address of the target to check
-c <community>	specifies the snmp community.
-h, –help	displays help

Return code

OK (0), WARNING (1), CRITICAL (2), UNKNOWN (3)

Output

The output displays the state and the values of the sensors.

Examples

If the task state is OK:

```
> check_FCBrocade_hardware.sh -H <host> -c public
HARDWARE OK : SLOT#0TEMP#1=27C, SLOT#0TEMP#2=27C, SLOT#0TEMP#3=28C,
FAN#1=6136RPM, FAN#2=5921RPM, FAN#3=5921RPM, PowerSupply#1=1
```

check_brocade check command

Usage

`check_fcsw.pl -H <host IP address> -c <command> [-p <port number>]`

-H <host>	Hostname or IP address of the target to check
-c <command>	specifies the type of element to be monitored
	switch : gets the monitoring state of the FC switch itself
	port : gets the monitoring state of the FC ports
	fan : gets the monitoring state of the fans
	temp : gets the monitoring state of the temperature sensors
-p <port number>	gets the monitoring state of the specified FC port
	This option can only be used when **–c port** is specified
-h, –help	displays help

Return code

OK (0), WARNING (1), CRITICAL (2), UNKNOWN (3)

Output

The output displays the state of the sensor.

Examples

If the task state is OK:

```
> check_fcsw.pl -H <host> -c switch
Global switch status is OK
>

> check_fcsw.pl -H <host> -c port
All 16 FC ports are OK
>

> check_fcsw.pl -H <host> -c temp
All 4 Temperature Sensors are OK
>

> check_fcsw.pl -H <host> -c fan
All 4 Fans are OK
>

> check_fcsw.pl -H <host> -c port –p 16
Status: OK
FC port 16 – OK [inSync]
```

When the return code is UNKNOWN:

```
> check_fcsw.pl -H <host> -c switch
Cannot access to Switch status, Cannot acces to Switch name
>

> check_fcsw.pl -H <host> -c temp
Cannot access to sensors states
>

> check_fcsw.pl -H <host> -c port
Cannot access to FC port states
>

> check_fcsw.pl -H <host> -c port –p 26
Status UNKNOWN
FC port 26 – UNKNOWN [port number out of range (24)]
```

4.2.7 BSMPDU-APC

The **BSMPDU-APC** Add-on uses the **check_PDUAPC** check command with the following shell (PERL) command options:

Usage

```
check_PDUAPC -H <host IP address> -s <action> [-p <port>] [-C
<community>] [-T <snmp timeout>]
```

-H <host>	Hostname or IP address of the target to check
-c <action>	Status: gets the APC PDU power supply(ies) status
	Consumption: gets the APC PDU power consumption (in Watts)
	Outlets: gets the APC PDU outlets status
-p <port>	snmp port number (default value: 161)
-C <community>	snmp community (default value: public)

-T <timeout> snmp timeout (default value: 30 seconds)

-h, –help displays help

Return code

OK (0), WARNING (1), CRITICAL (2), UNKNOWN (3)

Output

The output displays the APC PDU power supply(ies) state, the APC PDU global power consumption or the APC PDU outlets state.

Examples

- Action Status
  - Return code OK:

```
> check_PDUAPC -H 129.182.6.174 -a Status
Power Distribution Unit: 129.182.6.174, MODEL: "AP7922", Serial Nb:
"ZA0909003404", Firm Rev: "v3.5.7"
All Power Supplies OK
>
```

  - Return code WARNING:

```
> check_PDUAPC -H 129.182.6.174 -a Status
Power Distribution Unit: 129.182.6.174, MODEL: "AP7922", Serial Nb:
"ZA0909003404", Firm Rev: "v3.5.7"
Power Supply 1 OK, Power Supply 2 FAILED
>
```

  - Return code CRITICAL:

```
> check_PDUAPC -H 129.182.6.174 -a Status
Power Distribution Unit: 129.182.6.174, MODEL: "AP7922", Serial Nb:
"ZA0909003404", Firm Rev: "v3.5.7"
All Power Supplies FAILED
>
```

- Action Consumption:
  - Return code OK:

```
> check_PDUAPC -H 129.182.6.174 -a Consumption
Power OK: Reading 0 Watts
```

  - Return code WARNING:

```
> check_PDUAPC -H 129.182.6.174 -a Consumption
Power WARNING: Reading 6000 > Threshold 5520 Watts>
```

  - Return code CRITICAL:

```
> check_PDUAPC -H 129.182.6.174 -a Consumption
Power CRITICAL: Reading 8000 > Threshold 7360 Watts
>
```

- Action Outlets:
  - Return code OK:

```
> check_PDUAPC -H 129.182.6.174 -a Outlets
```

```
Power Distribution Unit: 129.182.6.174, MODEL: "AP7922", Serial Nb:
"ZA0909003404", Firm Rev: "v3.5.7"

Outlets(1 - 16) power: On(1)

>


> check_PDUAPC -H 129.182.6.174 -a Outlets

Power Distribution Unit: 129.182.6.174, MODEL: "AP7922", Serial Nb:
"ZA0909003404", Firm Rev: "v3.5.7"

Outlets(1,3,5,7,9,11,12,14,16) power: On(1)

Outlets(2,4,6,8,10,13,15) power: Off(2)

>
```

- Return code WARNING:

```
> check_PDUAPC -H 129.182.6.174 -a Outlets

Power Distribution Unit: 129.182.6.174, MODEL: "AP7922", Serial Nb:
"ZA0909003404", Firm Rev: "v3.5.7"

Outlets(1 - 16) power: Off(2)

>
```

4.2.8 BSMIPDU

The **BSMIPDU** Add-on uses the **check_IPDU** check command with the following shell (PERL) command options:

Usage

```
check_IPDU -H <host IP address> -a <action> [-p <port>] [-C <community>]
[-t <snmp timeout>] [-o <outlet>]
```

-H <host>	Hostname or IP address of the target to check
-a <action>	Status : gets the IPDU global status
	Consumption : gets the global IPDU power consumption (in Watts)
	OutletsConso : gets the power consumption for one or all IPDU outlets
	OutletsVoltage: gets the output voltage for one or all IPDU outlets
	Voltage: gets the input and output voltage and frequency of the IPDU
	Temperature: gets the temperature of the IPDU
	Humidity: gets the humidity for the IPDU
-p <port>	snmp port number (default value: 161)
-C <community>	snmp community (default value: public)
-t <timeout>	snmp timeout (default value: 50 seconds)
-o <outlet>	outlet number (default value: all); available only for actions OutletsConso and OutletsVoltage
-h, –help	displays help

Return code

OK (0), WARNING (1), CRITICAL (2), UNKNOWN (3)

Output

The output displays for action Status the IPDU global state and additional information about the IPDU host, for action Consumption the IPDU global power consumption and additional metrics as performance data, for action OutletsConso the power consumption per outlet and additional metrics as performance data, for action OutletsVoltage the output voltage per outlet and additional metrics as performance data, for action Voltage the input and output voltage and frequency and additional metrics as performance data, for action Temperature the temperature of the IPDU and additional metrics as performance data and for action Humidity the humidity of the IPDU and additional metrics as performance data.

Examples

- Action Status:

```
$ check_IPDU -H 172.16.113.41 -a Status

Status OK -  MODEL: "IBM DPI C13 BULK", Device Firmware Version:
"0202.0008", Agent Firmware Versio: "IBM DPI V0210.0001"

 INPUT Frequency: 50 Hz, Voltage: 240.4 volts, Current: 6.2 amp.

 OUTPUT VA rating: 14950, frequency: 50 Hz, total power: 1352 watts, VA:
1493 volt-amps.

>
```

- Action Consumption:

```
> check_IPDU -H 172.16.113.41 -a Consumption

Consumption OK - OVERALL OUTPUT: 1341 watts|totalpower=
1341watts;;;547;1782 wattshours=1346Wh;;;0;1466

>
```

- Action OutletsConso:

```
> check_IPDU -H 172.16.113.41 -a OutletsConso

Outlet1 ("[13] ESP4 - PL1660R") : 198 watts

Outlet2 ("[09] ESP3 - PL1660R base") : 527 watts

Outlet3 ("[19] Power7 - M6-700 base") : 529 watts

Outlet4 : 0 watts

Outlet5 ("[18] FC sta/st6") : 42 watts

Outlet6 ("[01] Citrix VDI") : 52 watts

|Outlet1-watts=198;;;0;615 Outlet1-wattshours=198;;;0;457 Outl

et2-watts=527;;;0;637 Outlet2-wattshours=527;;;0;556 Outlet3-
watts=529;;;0;958 Outlet3-wattshours=531;;;0;648 Outlet4-watts=0;;;0;581
Outlet4-wattshours=0;;;0;146 Outlet5-watts=42;;;38;44 Outlet5-
wattshours=42;;;0;43 Outlet6-watts=52;;;0;95 Outlet6-wattshours=51;;;0;52

>

> check_IPDU -H 172.16.113.41 -a OutletsConso -o 3

Outlet3 ("[19] Power7 - M6-700 base") : 533 watts|watts=533;;;0;958
wattshours=532;;;0;648

>
```

- Action OutletsVoltage:

```
> check_IPDU -H 172.16.113.41 -a OutletsVoltage

Outlet1 ("[13] ESP4 - PL1660R") : 241 volts

Outlet2 ("[09] ESP3 - PL1660R base") : 241 volts

Outlet3 ("[19] Power7 - M6-700 base") : 238.8 volts

Outlet4 : 238.7 volts

Outlet5 ("[18] FC sta/st6") : 237.7 volts

Outlet6 ("[01] Citrix VDI") : 237.6 volts

|Outlet1-voltage=241;;;226.5;247.3 Outlet2-voltage=241;;;226.5;247.3
Outlet3-voltage=238.8;;;231.9;244.8 Outlet4-voltage=238.7;;;232;244.8
Outlet5-voltage=237.7;;;231;243.8 Outlet6-voltage=237.6;;;231;243.8

>

> check_IPDU -H 172.16.113.41 -a OutletsVoltage -o 3
```

```
Outlet3 ("[19] Power7 - M6-700 base") : 239.6volts

|voltage=239.6;;;231.9;244.8
>
```

- Action Voltage:

```
> check_IPDU -H 172.16.113.41 -a Voltage

Input Voltage: 240 volts

Input frequency: 50 Hz

Output voltage: 240 volts

Output frequency: 50 Hz

|inputVoltage=240volts;;;; inputFrequency=50Hz;;;;
outputVoltage=240volts;;;; outputFrequency=50Hz;;;;

>
```

- Action Humidity

```
> check_IPDU -H 172.16.113.41 -a Humidity
Humidity CRITICAL - 11%|humidity=11%;22:78;20:80;10;44
>
```

- Action Temperature

```
> check_IPDU -H 172.16.113.41 -a Temperature
Temperature OK - 30°C|Temperature=30C;16:32;16:32;23;42
AmbientTemperature=37C;;;29;46
>
```

4.3 Virtualization Management

The following check commands apply to the virtualization management Add-ons.

4.3.1 BSMVMwareVS

The Nagios check commands used by **BSMVMwareVC** Add-on use the shell (PERL) **check_virtualcenter.pl** command.

Usage

```
check_virtualcenter.pl --–server <vCenter>
                       --vmname <VM_id>
                       --hostname <ESX_id>
                       --stat <metric>
                       --crit <nb>
                       --warn <nb>
                       --indics <list of metrics>
```

where:

–server <vCenter>	Hostname or IP address of the vCenter
–vmname <VM_id>	Name of the VM (in vCenter context)
–hostname <ESX_id>	Name of the ESX host (in vCenter context)
–stat <tmetric>	Type of performance metric to check. See below for valid VMware metrics
–warn <nb>	Warning threshold for performance statistics
–crit <nb>	Critical threshold for performance statistics
–indic <metric list>	Additional performance metrics to use as reporting indicator. See below for valid VMware metrics
–help	Display help

Supported host's metrics:

- cpu.usage.average
- sys.resourceCpuUsage.average
- mem.usage.average
- mem.consumed.average
- mem.granted.average
- mem.vmmemctl.average
- mem.active.average
- mem.swapused.average
- mem.sharedcommon.average
- net.usage.average
- net.transmitted.average
- net.received.average
- net.droppedRx.summation
- net.packetsRx.summation
- net.droppedTx.summation
- net.packetsTx.summation
- disk.usage.average
- disk.commands.summation
- disk.numberRead.summation
- disk.numberWrite.summation

- disk.read.average
- disk.write.average
- disk.deviceLatency.average
- disk.kernelLatency.average
- disk.totalLatency.average
- disk.queueLatency.average

Supported VM's metrics:

- cpu.usage.average
- cpu.used.summation
- cpu.ready.summation
- mem.usage.average
- mem.consumed.average
- mem.granted.average
- mem.vmmemctl.average
- mem.active.average
- net.usage.average
- net.transmitted.average
- net.received.average
- net.droppedRx.summation
- net.packetsRx.summation
- net.droppedTx.summation
- net.packetsTx.summation
- disk.usage.average
- disk.commands.summation
- disk.numberRead.summation
- disk.numberWrite.summation
- disk.read.average
- disk.write.average

Return code

OK(0), WARNING(1), CRITICAL(2), UNKNOWN(3).

Output

The output has the following format:

```
<VMware name>: <metric label> (<counter type>) = <value> (sampling
period <period>
```

The VMware name is the name of the host or VM as set in vCenter or ESX

The metric label is those defined in VMware.

Examples

Example 1

```
check_vsphere.pl –server 129.182.6.57 –hostname 172.31.50.55
172.31.50.55: Nothing to report about this host.
```

The ESX status returned is determined by the vCenter server.

Example 2

```
check_vsphere.pl –-server 129.182.6.57 –hostname 172.31.50.55 –stat
mem.usage.average –crit 80 –warn 70
```

```
172.31.50.55: Memory Usage (Average) = 36.65 (sampling period 20 s)
```

The status returned is dependant on the threshold setting. In this example, the status returned is good.

Example 3

```
$ ./check_vsphere.pl --server 129.182.6.57 --hostname 172.31.50.55 --stat
mem.usage.average --crit 90 --warn 80 --indics mem.consumed.aver>
```

```
172.31.50.55: Memory Usage (Average) = 36.65 (sampling period 20
s)|Memory_Usage=36.65%;80;90;0;100 Memory_Consumed=61493.32kb;;;;
Memory_Granted=62800.12kb;;;;
```

Output returns also additional metrics as performance data.

Failure case

Example 1

```
172.16.115.100 : information status for this host is not available
(/opt/BSMServer/engine/tmp/VCcache1721611358.pm not found)has
```

This output indicates that the collect task has not started or has failed to collect information from vCenter.

Check the following:

- The task has been enabled in BSM
- The task is scheduled to run periodically (see the collectVMvCenter.log log file)
- If the failure has occurred during the collect process (see the log file vcenter.err)

Example 2

```
vmx: out-of-date status information (Wed Nov 4 14:35:11 2009) - vmx: This
virtual machine is powered off or suspended.
```

This output indicates that the collect task has not been scheduled recently, or has failed to collect information from vCenter.

Check the following:

- The task is still enabled in BSM
- The task has been scheduled recently (see the collectVMvCenter.log log file)
- If the failure has occurred during the collect process (see the vcenter.err log file)

4.3.2 BSMEscalaLpar

The **Nagios** check commands used by **BSMEscalaLPAR** Add-on use the shell (PERL) **check_NSM_escala_lpar** or **check_NSM_escala_vios_ssp** commands on BSM server and the **check_lpm.pl** command launched on the AIX agent via the NRPE protocol.

4.3.2.1 check_NSM_escala_lpar

Usage

```
check_NSM_escala_lpar –M manager [HMC|IVM] -H <netname> -U <remote_user>
-I <identity_file> [-l <lpar_name>] [-p <poolname>] [-S <hoststate>]
[-i <STATUS|CPU|POOL>] [-e sample_time] [-w <warn>%] [-c <crit>%]
[–N < name>] [-t timeout]
```

-M <manager>	Type of manager used to retrieve plugin information. Available value are: IVM, when the Escala is managed by an IVM installed on Vios partition, HMC, when the Escala is managed by a remote station.
-H < netname>	Hostname or IP address of the manager used for checking
-U <remote_user>	User for remote connection
-I <identity_file>	Name of the file from which the identity (private key) for RSA or DSA authentication is read. The file must be localized into the directory <BSM Installation Directory>/engine/etc/ssh. To use it as authentication file for Vios platform, you have to install the corresponding public key on the VIO server.
-N < name>	Name of the CEC or Vios LPAR (used in output of the plugin related to a given logical partition).
-l <lpar_name>	Name of the logical partition to check.
-p <poolname>	Name of the processing pool.
-S <hoststate>	Nagios status of the lpar or pool host. The status is passed by Nagios. If the status is not UP, the info is not checked.
-i <check information>	Available values are: STATUS (to check the status of the VIO server or of a logical partition), POOL (to check the utilization of the processing pool), CPU (to check the utilization of the CPU entitled to a partition). Default value is STATUS
-e <sample time>	Sample time in minutes used to perform calculation on utilization. Default value is 5.
-w <warnThreshold>	Warning threshold
-c <criticalThreshold>	Critical threshold.
-h, –help	Display help

Return code

OK(0), WARNING(1), CRITICAL(2), UNKNOWN(3).

Output

The output depends on the type of check performed, as shown in the examples below.

check_vios _status

The check_NSM_escala_lpar shell is called using the following syntax:

```
check_NSM_escala_lpar –M IVM –H <vios_netName> -N <server_name> -U <user>
-I <identity_file> -i status
```

Output

Only two states are possible for Vios status: OK or UNKNOWN:

- for OK state, the output is "`Virtual I/O Server state: Operating`"
- for UNKNOWN state, the output is "`Unable to determine Virtual I/O Server state`", following the reason.

Note The check_vios_status command is dependent on the state of the Vios system given by the **lssyscfg** IVM command.

Example

```
check_NSM_escala_lpar –H ivm1 –U padmin –I id_dsa_nsm –I status
```

Output

```
Virtual I/O Server state: Operating
```

Return code: `OK`.

check_vios_used_pool case

The check_NSM_escala_lpar shell is called using the following syntax:

```
check_NSM_escala_lpar –M IVM –H <vios_netName> -U <user>
-I <identity_file> -N <server_name> -i POOL -e <sample_time> -w <warn>%
-c <crit>%
```

Output

```
Shared Procesor Pool Used (nbCPU / CPUTotal units entitled) - utilization
on <sampleTime> mn <check_status>: <utilization percent>%
```

Note The check_vios_used_pool command is based on the pool_cycle metrics (total_pool_cycle, utilized_pool_cycle) obtained by the **lslparutil** IVM command.

It requires that the data collection is activated by the **chlparutil** command:
`chlparutil –r config –s 30`

Example

```
check_NSM_escala_lpar –H 192.168.207.60 –U padmin –I id_dsa_nsm -i POOL
–e 5 –w 70% –c 80%
```

Output

```
Shared Procesor Pool Used (1.40 / 2 units entitled) - utilization on 5 mn
OK: 2.16 %
```

Return code: OK

check_cec_used_pool case

The check_NSM_escala_lpar shell is called using the following syntax:

```
check_NSM_escala_lpar –M HMC –H <hmc_netName> -U <user>
-I <identity_file> -N <cecname>-i POOL -e <sample_time> -w <warn>%
-c <crit>%
```

Output

```
Processing pool (nbCPU / CPUTotal units entitled) (HMC <hmc_netname>
- utilization on <sampleTime> mn <check_status>: <utilization percent>%
```

Note The check_cec_used_pool command is based on pool_cycle metrics (total_pool_cycle, utilized_pool_cycle) obtained by the **lslparutil** HMC command.

It requires that data collection is activated for the system by the **chlparutil** command:
`chlparutil –r config –s 3600 [–m <systemName>]`

If the **systemName** parameter is not specified, the data collection is activated for all managed systems.

Example

```
check_NSM_escala_lpar –H 192.168.207.60 –U padmin –I id_dsa_nsm -i POOL –
e 5 –w 70% –c 80%
```

Output

Processing pool (1.4 / 2 units entitled) (HMC 172.16.108.112) - utilization on 120 mn OK: 52.83 %

Return code: OK

check _used_configured_pool case

The check_NSM_escala_lpar shell is called using the following syntax:

```
check_NSM_escala_lpar –M HMC –H <hmc_netName> -U <user>
-I <identity_file> -N <cecname> -p <poolname> -i POOL -e <sample_time>
-w <warn>% -c <crit>%
```

Output

```
Configured Shared Processing pool (nbCPU / CPUTotal units entitled) (HMC
<hmc_netname>
- utilization on <sampleTime> mn <check_status>: <utilization percent>%
```

Note The check_used_configured_pool command is based on pool_cycle metrics (total_pool_cycle, utilized_pool_cycle) obtained by the **lslparutil** HMC command.

It requires that data collection is activated for the system by the **chlparutil** command:
`chlparutil –r config –s 3600 [–m <systemName>]`

If the systemName parameter is not specified, the data collection is activated for all managed systems.

Example

```
check_NSM_escala_lpar –H 192.168.207.60 –U padmin –I id_dsa_nsm -i POOL
-p SharedPool01 –e 5 –w 70% –c 80%
```

Output

```
Configured Shared Processor Pool used: 0.03 / 2 Processors (HMC hmc-
squad) - utilization on 5 mn OK: 1.69 %
```

Return code: OK

check_lpar_status case

The **check_NSM_escala_lpar** shell is called using the following syntax:

```
check_NSM_escala_lpar –M [IVM|HMC] –H <netName> -U <user>
-I <identity_file> -l <lpar_name> -N <name>
```

Output

```
Logical partition <lpar_name> on <server_name> (HMC or IVM):
<lpar_status>
```

Note The check _lpar_status command is based on the Lpar state obtained by the **lssyscfg** IVM command.

Examples

```
check_NSM_escala_lpar –H 192.168.207.60 –U padmin –I id_dsa_nsm
–N ivm1 l part1
```

Output

```
Logical partition galilei on staix35 (IVM): Running
```

Return code: OK.

```
check_NSM_escala_lpar –H 192.168.207.60 –U padmin –I id_dsa_nsm
–N ivm1 l part2
```

Output

```
Logical partition tyrex on staix35 (IVM): Not Available
```

Return code: CRITICAL.

check_lpar_used_cpu example

The **check_NSM_escala_lpar** shell is called using the following syntax:

```
check_NSM_escala_lpar –M [IVM|HMC] –H <mgr_netName> -U <user>
-I <identity_file> -N <server_name> -l <lpar_name> -i CPU
-e <sample_time> -w <warn>% -c <crit>% -S <status>
```

Output

```
Logical partition <lpar_name> on <server_name> (<nbCPU> units entitled –
IVM or HMC - type=<partition type>) - processing utilization on
<sample_time>mn <check_status>: <utilization percent>%
```

Note The check_lpar_used_CPU command is based on cycles metrics (entitled_cycles, capped_cycles, uncapped_cycles) obtained by the **lslparutil** command (see above how to activate data collection on HMC or IVM).

Example

```
check_NSM_escala_lpar –H 192.168.207.60 –U hscroot –I id_dsa_nsm -N Pool-
ESP3-PL1660R –l Coop-IBM -I CPU–e 5 –w 10% –c 20%
```

Output

```
Logical partition Coop-IBM on Pool-ESP3-PL1660R (1.0 units entitled - HMC
129.183.12.32 - type=Shared Uncapped Partition) - processing utilization
on 5 mn OK: 0.04
```

Return code: `WARNING`

```
Shared Processor Pool used (nbCPU / CPUTotal units entitled) (HMC
<hmc_netname>
- utilization on <sampleTime> mn <check_status>: <utilization percent>%
```

4.3.2.2 check_NSM_escala_vios

The Nagios check commands used by BSMEscalaLPAR Add-on use the shell (PERL) check_NSM_escala_vios command.

Usage

```
check_NSM_escala_vios -H <hostname> -S <hoststate> -U <remote_user> -I
<identity_file> -i <STATUS|CPU|POOL>] [-e sample_time] [-w <warn>%] [-c
<crit>%]
```

-H < hostname>	Hostname or IP address of the VIO server to check
-U <remote_user>	User for remote connection
-I <identity_file>	Name of the file from which the identity (private key) for RSA or DSA authentication is read. The file must be localized into the directory <BSM Installation Directory>/engine/etc/ssh. To use it as authentication file for Vios platform, you have to install the corresponding public key on the VIO server.
-S < hoststate>	Nagios status of the VIO server host. The status is passed by Nagios. If the status is not UP, the info is not checked.
-i <check information>	Available values are: SEA (to check the utilization of the shared Ethernet adapters), NPIV (to check the utilization of the fibre channel adapter)
-e <sample time>	Sample time in minutes used to perform calculation on utilization. Default value is 5.
-w <warnThreshold>	Warning threshold
-c <criticalThreshold>	Critical threshold.
-h, –help	Display help

Return code

OK(0), WARNING(1), CRITICAL(2), UNKNOWN(3).

Output

The output depends on the type of check performed, as shown in the examples below.

check_vios _used_sea

The check_NSM_escala_vios shell is called using the following syntax:

```
check_NSM_escala_vios –H <vios_netName> -U <user> -I <identity_file>
-e <sample_time> –w <warning_threshold>% –c <critical_threshold>% -i SEA
–S <hoststate>
```

Output

```
SHARED ETHERNET ADAPTERS (SEA) <check_status>: all adapters
(['<adaptater_name> - <freq>Mbps - FD :<percent_use>%' ],…) less than
<threshold>% utilized
```

Example

```
SHARED ETHERNET ADAPTERS (SEA) OK: all adapters ('ent4 - 100Mbps - FD
:0.14%' 'ent5 - 1000Mbps - FD :0.00%' ) less than 60% utilized
Return code: OK.
```

check_vios _used_npiv

The check_NSM_escala_vios shell is called using the following syntax:

```
check_NSM_escala_vios –H <vios_netName> -U <user> -I <identity_file>
-e <sample_time> –w <warning_threshold>% –c <critical_threshold>% -i NPIV
–S <hoststate>
```

Output

```
FIBER CHANNEL ADAPTERS (NPIV) <check_status>: all adapters
((['<adaptater_name> - <freq>Gbps -:<percent_use>%' ],…) less than
<threshold>% utilized
```

Example

```
FIBER CHANNEL ADAPTERS (NPIV) OK: all adapters ('fcs0 - 8Gbps :0.00%'
'fcs1 - 8Gbps :0.00%') less than 70% utilized

Return code: OK.
```

4.3.3 BSMHelios

The Nagios check commands, used by the BSMHelios Add-on, use the standard Nagios check_snmp command documented in in the *BSM Administrator's Guide*, 86 A2 56FA or commands launched on the BSM agent via the NRPE protocol, most of them documented in the *BSM Administrator's Guide*, 86 A2 56FA.

In this section, only Helios specific commands are documented.

4.3.3.1 check_cpuload2.sh

Usage

```
check_cpuload2.sh -w <WLOAD1,WLOAD5,WLOAD15> -c <CLOAD1,CLOAD5,CLOAD15>
```

-w	list of warning thresholds for average number of processes ready to run or running over three time frames, 1 minute, 5 minutes and 15 minutes
-c	list of critical thresholds for average number of processes ready to run or running over three time frames, 1 minute, 5 minutes and 15 minutes

Note The always-busy dedicated CPUs are subtracted from the average and the number of CPUs actually available are used to convert the percent value.

Return code

OK(0), WARNING(1), CRITICAL(2), UNKNOWN(3).

Output

The output has the following format:

CPU Load <return label>: <avgload1>% (1min), <avgload5>% (5min), <avgload15>% (15min), (emulcpu,set0cpu)

emulcpu: number of CPUs dedicated to running Helios CPU emulation.

set0cpu: number of CPUs assigned to cpuset set_0. These are the number of CPUs available to run Linux and Helios I/O emulation.

Loadavg: the numbers reported by Linux in /proc/loadavg are a running average of the number of tasks in the scheduler queue that are ready to run.

Example

The check_cpuload3.sh command is launched on BSM Agent with the check_nrpe script.

```
check_nrpe -H W.X.Y.Z -c 'libexec/check_cpuload2.sh -w 100,100,100 -c
120,120,120'
```

Output

```
CPU Load OK: 0% (1min), 0% (5min), 0% (15min), (800 8) | load1avg=8.02
load5avg=8.03 load15avg=8.00 emulcpu=8 set0cpu=8
```

The string after the pipe correspond to perfdata information

4.3.3.2 check_linux_bonding

Usage

```
check_linux_bonding [OPTION]
```

OPTIONS:

-t, –timeout	Plugin timeout in seconds [5]
-s, –state	Prefix alerts with alert state
-S, –short-state	Prefix alerts with alert state abbreviated
-n, –no-bonding	Alert level if no bonding interfaces found [ok]
–slave-down	Alert level if a slave is down [warning]
–disable-sysfs	Don't use sysfs (default), use procfs
-b, –blacklist	Blacklist failed interfaces
-d, –debug	Debug output, reports everything
-h, –help	Display this help text
-V, –version	Display version info

For more information and advanced options, see the manual page or URL:

http://folk.uio.no/trondham/software/check_linux_bonding.html

Return code

OK(0), WARNING(1), CRITICAL(2), UNKNOWN(3).

Output

The output contains one line per interface which has the following format:

Interface <interface> is <up|down>

Output examples

- ```
  Interface bond0 is up: mode=0 (balance-rr), 2 slaves: eth1, eth5
  Interface bond1 is up: mode=0 (balance-rr), 2 slaves: eth3, eth7
  Interface rma is up: mode=5 (balance-tlb), 2 slaves: eth0!, eth2
  ```
- ```
  Bonding interface bond0 [mode=1 (active-backup)]: Slave eth3 is down
  Interface rma is up: mode=5 (balance-tlb), 2 slaves: eth0!, eth2
  ```

Example

The command is launched on BSM Agent with the check_nrpe script.

```
check_nrpe -H W.X.Y.Z -c 'libexec/check_linux_bonding -v'
```

Output

```
Interface bond0 is up: mode=0 (balance-rr), 2 slaves: eth1, eth5
Interface bond1 is up: mode=0 (balance-rr), 2 slaves: eth3, eth7
Interface rma is up: mode=5 (balance-tlb), 2 slaves: eth0!, eth2
```

4.3.3.3 check_ib.sh

Usage

```
check_ib.sh: check_ib.sh [-h] [--rate 40]
```

Check state of all Infiniband interfaces configured as IP interfaces with ONBOOT=yes.

–rate	threshold for interface rate default value set 40 Gb/s
-h, –help	Display this help text

Return code

OK(0), WARNING(1), CRITICAL(2), UNKNOWN(3).

OK state returns if IBn is "up" and have a carrier signal to be good.
WARNING if IB rate is less than the expected rate.
CRITICAL if any non-up or carrier-down interfaces is reported.

Output

The output has the following format:

```
<Status> : <nb interface>, ibn=<rate>,…,ibm=<rate>
```

Examples

The command is launched on BSM Agent with the check_nrpe script.

```
check_nrpe -H W.X.Y.Z -c 'libexec/check_ib.sh'
```

Output

```
CRITICAL: 1 bad, 0 degraded, 1 good, ib0=40, ib1=0|ib0=40, ib1=0
```

```
check_nrpe -H W.X.Y.Z -c 'libexec/check_ib.sh'
```

Output

```
OK: 2 Infiniband, ib0=40, ib1=40|ib0=40, ib1=40OK: 2 Infiniband, ib0=40,
ib1=40
```

The string after the pipe correspond to perfdata information.

4.3.3.4 check_iberrors

Usage

```
check_iberrors -w <Rcv errors warning value> -c <Rcv errors critical
value> -x <Symbol errors warning value> -d <Symbol errors critical value>
-y <Xmt Discards warning value> -e <Xmt Discards critical value> -p
<port> [-h] [-V]
```

-w	Rcv Errors Warning trigger level
-c	Rcv Errors Critical trigger level
-x	Symbol Errors Warning trigger level
-d	Symbol Errors Critical trigger level
-y	Xmt Discards Warning trigger level
-e	Xmt Discards Critical trigger level
-p	port number
-h	Show this page
-V	Version of the plugin

Return code

OK(0), WARNING(1), CRITICAL(2), UNKNOWN(3).

NB : For the 3 folowing errors : RCV, Symbol et Xmt Discards, the severity (WARNING or CRITICAL) depend on the warning criteria given with options –w, -x or –y and the critical criteria given with options –c, -d or –e.

Output

See Example

Example

The command is launched on BSM Agent with the check_nrpe script.

```
check_nrpe -H W.X.Y.Z -c 'libexec/check_iberrors -w 65534 -c 65535 -x
65536 -d 65537 -y 65536 -e 65537 -p 1'
```

Output

```
OK - Pt0 RCVErrors/day<br>OK - 0 SYMBErrors/day<br>OK - 0
XMTDiscards/day|Receiving=Pt0errors/day;65534;65535
symbolerrors=0errors/day;65536;65537 xmtdiscards=0errors/day;65536;65537;
```

The string after the pipe correspond to perfdata information.

4.3.3.5 check_pp_dead.sh

Usage

```
check_pp_dead.sh
```

Return code

OK(0), WARNING(1), CRITICAL(2), UNKNOWN(3).

NB: Warning means one port of the 2 HBA cards is in “devices dead” state.

Output

See Example

Example

The command is launched on BSM Agent with the check_nrpe script.

```
check_nrpe -H W.X.Y.Z -c 'libexec/check_pp_dead.sh'
```

Output

```
No dead path
```

or

```
112 device(s) dead on the 1st port/1st board <=> FA 4bA DMX4 5052
```

4.3.3.6 check_megaraid_sas.pl

Usage

```
Usage: ./check_megaraid_sas.pl [-s number] [-m number] [-o number]
```

-s	is how many hotspares are attached to the controller
-m	is the number of media errors to ignore
-p	is the predictive error count to ignore
-o	is the number of other disk errors to ignore

Return code

OK(0), WARNING(1), CRITICAL(2), UNKNOWN(3).

NB : Warning : If one of two disks of the mirror is not present or if an error (predefined media or others) occurs ona disk.

Output

See Example.

Example

The command is launched on BSM Agent with the check_nrpe script.

Output

```
WARNING: 0:0:RAID-1:2 drives:558.375GB:Optimal Drives:2 (3 Errors)
```

Appendix A. Third Party License Agreements

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

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

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

Glossary

A

Add-on

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

Alert

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

Alert Mode

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

Autocall Server

Used to relay notifications to Bull support.

B

BMC

Baseboard Management Controller. See Embedded Management Controller.

BSM

Bull System Manager.

BSM Console

See Management Console

C

Category

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

CIM

Common Information Model.

CLI

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

CMM

Chassis Management Module.

Configuration GUI

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

Contact

Defines the target for BSM notifications

Contactgroup

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

Control GUI

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

D

DHCP

Dynamic Host Configuration Protocol.

Distributed Solution

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

Domain

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

E

EMM

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

Event Handler

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

Event Reception

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

F

Focus Pane

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

FRU

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

G

Global Console

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

GTS

Global Transaction Server

GUI

Graphical User Interface

H

Hardware Manager

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

Hardware Partition

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

HMC

Hardware Management Controller.

Host

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

Hostgroup

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

Hostlist

List of hosts associated with a host group.

Hosts view

Window that displays all configured hosts with their status.

I

IPMI

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

IPMItool

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

J

No entries

K

No entries

L

LDAP

Lightweight Directory Access Protocol.

M

Management Agent

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

Management Console

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

Management Server

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

Management Tree

A hierarchal representation of the resources defined in the Bull System Manager configuration. Each resource displayed in the tree is represented by a node that may have sub-nodes.

Map Mode

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

MIB

Management Information Base.

Monitoring Service

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

MySQL

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

N

Nagios

Open Source monitoring tool.

NDOutils

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

NIC

Network Interface Controller.

NSCA

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

O

OCS Inventory Ng

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

P

PAM

Platform Administration and Maintenance Software

Performance Indicators

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

PDU

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

PHP

PHP: Hypertext Preprocessor. A server side scripting language.

Platform

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

PNP4Nagios

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

Q

No entries

R

RRD

Round-robin database.

RRD Indicators

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

S

Service

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

Service group

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

SNMP

Simple Network Management Protocol.

Storage Manager

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

Supervision Mode

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

T

Timeperiod

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

Topology

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

Tree mode

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

U

UltraVNC Server

For remote operation on **Windows** hosts.

V

View

A **view** is a tree structure that can display:

- the entire host list

- managers and the hosts they manage

- host groups

From each tree node, the user can display detailed information about a host or a service, according to their User role (Administrator or Operator).

Virtualization Platform

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

Virtualization Manager

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

W

WBEM

Web-Based Enterprise Management.

Webmin

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

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