



BSM 1.0 Server Add-ons

Installation and Administrator's Guide

NOVASCALÉ
& ESCALÁ



REFERENCE
86 A2 59FA 00

NOVASCALE & ESCALA

BSM 1.0 Server Add-ons Installation and Administrator's Guide

Software

November 2008

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

REFERENCE
86 A2 59FA 00

The following copyright notice protects this book under Copyright laws which prohibit such actions as, but not limited to, copying, distributing, modifying, and making derivative works.

Copyright © Bull SAS 2008

Printed in France

Trademarks and Acknowledgements

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

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

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

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

Table of Contents

Preface	ix
Scope and Audience of this Manual.....	ix
Using this Manual	ix
Related Information	ix
Highlighting.....	x
Chapter 1. Bull System Manager Server Add-ons Concepts	1
1.1 Bull System Manager	1
1.1.1 Overview	1
1.1.2 Monitoring	2
1.1.3 Event Reception	3
1.1.4 Hardware Manager	3
1.1.5 Storage Manager	3
1.1.6 Virtualization Manager.....	3
1.2 Bull System Manager Server Add-ons	4
Chapter 2. Bull System Manager Server Add-ons Installation and Configuration	5
2.1 General Installation Requirements.....	5
2.1.1 Supported Operating Systems	5
2.1.2 Required Disk Space	5
2.1.3 Required Memory	5
2.1.4 Installation Requirements.....	5
2.1.5 Operational Requirements.....	6
2.1.6 Restrictions	6
2.2 Installing Bull System Manager Server Add-ons for Windows	7
2.2.1 Prerequisites	7
2.2.2 Installing Management Server Add-ons from the Bull System Manager CD-ROM.....	7
2.2.3 Installing Management Server Add-ons from the BSM Add-ons CD-ROM	9
2.2.4 Un-installing Bull System Manager Server Add-ons Components	11
2.2.5 Upgrading to a New Bull System Manager Server Add-ons Version.....	12
2.3 Installing Bull System Manager Server Add-ons for Linux	13
2.3.1 Prerequisites	13
2.3.2 Installing Management Server Add-ons from the CD-ROM.....	13
2.3.3 Installing Management Server Add-ons from the BSM Add-ons CD-ROM	15
2.3.4 Uninstalling Bull System Manager Server Add-on Components	17
2.3.5 Upgrading to a new Bull System Manager Server Add-ons Version.....	17
2.4 Monitoring Configuration.....	18
2.4.1 Configuration GUI	18
2.4.2 Categories and Services	18
Chapter 3. Bull System Manager Server Add-ons Description	21
3.1 Internal Storage (Free)	21
3.1.1 BSMGAMTT for LSI MegaRAID 320-2x Management.....	21

3.1.2	BSMLSICIM for LSI 22320 Chip Management	24
3.1.3	BSMMegaRaidSAS (LSI MegaRAID SAS (IR) Management)	27
3.2	External Storage Server Add-ons	29
3.2.1	BSMStoreWayFDA (StoreWay FDA Management)	29
3.2.2	BSMEmcClariion (EMC CLARiiON Management)	31
3.2.3	BSMNetApp (NetApp Management)	33
3.2.4	BSMWaterCooledDoor (Water Cooled Door Management)	37
3.3	Virtualization Server Add-ons	40
3.3.1	Overview	40
3.3.2	BSMVMwareESX for "VMware ESX" Management.....	42
3.3.3	BSMHyperNova for "HyperNova" Management	52
3.3.4	BSMEscalalPAR "EscalalPAR" Management	66
3.4	Bull Products Server Add-ons.....	75
3.4.1	BSMDD4A for Bull "Dynamic Domains For Applications" Management	75
3.4.2	BSMBVS for Bull Video Services Management	76
3.4.3	BSMJOnAS for JOnAS Management	78
Appendix A. Check Commands for Customizable Services of Add_ons		85
Internal Storage Management		85
BSMGAMTT		85
BSMLSICIM		88
BSMMegaRaidSAS		90
External Storage Management		93
BSMStoreWayFDA.....		93
BSMEmcClariion.....		95
BSMNetApp.....		97
BSMWaterCooledDoor.....		105
Virtualization Management.....		107
BSMVMwareESX.....		107
BSMHyperNova.....		110
BSMEscalalpar.....		112
Bull Products Management.....		116
BSMDD4A		116
BSMBVS		118
BSMJOnAS		120
Index.....		123

List of Figures

Figure 1-1.	Bull System Manager Architecture	2
Figure 2-1.	Windows Installation - Bull System Manager Welcome Page.....	8
Figure 2-2.	Windows Installation - Bull System Manager Install Page	8
Figure 2-3.	Windows Installation - Bull System Manager Server Add-ons Install Page	9
Figure 2-4.	Windows Installation - Bull System Manager Add-ons Welcome Page	10
Figure 2-5.	Windows Installation - Bull System Manager Add-ons Install Page.....	10
Figure 2-6.	Windows Installation - Bull System Manager Install/Category Page	11
Figure 2-7.	Linux Installation - Bull System Manager Welcome Page	14
Figure 2-8.	Linux Installation - Selecting Bull System Manager Components	14
Figure 2-9.	Linux Installation - Bull System Manager Server Add-Ons Install page	15
Figure 2-10.	Linux Installation - Bull System Manager Add-ons Welcome Page.....	16
Figure 2-11.	Linux Installation - Selecting Bull System Manager Server Add-ons.....	16
Figure 2-12.	Linux Installation - Bull System Manager Server Add-ons Install Page	17
Figure 3-1.	GAM Monitoring Components.....	21
Figure 3-2.	LSI CIM Monitoring Components.....	24
Figure 3-3.	MegaRAID SAS Monitoring Components	27
Figure 3-4.	StoreWay FDA Monitoring Components	29
Figure 3-5.	EMC CLARiiON Monitoring Components.....	31
Figure 3-6.	NetApp Monitoring Components	33
Figure 3-7.	Water Cooled Door Monitoring Components.....	37
Figure 3-8.	Virtual Managers view.....	41
Figure 3-9.	Virtual Manager information pane.....	41
Figure 3-10.	VMwareESX Add-on components	42
Figure 3-11.	ESX Virtual Platforms page	43
Figure 3-12.	ESX Platform Properties	44
Figure 3-13.	ESX Virtual Machines pane	45
Figure 3-14.	Host Topology modification confirmation.....	46
Figure 3-15.	VMware service properties pane.....	49
Figure 3-16.	VMwareESX monitoring information	51
Figure 3-17.	VMwareESX reporting information	52
Figure 3-18.	HyperNova Add-on components	52
Figure 3-19.	HyperNova Virtualization Platforms page.....	53
Figure 3-20.	HyperNova Platform Properties	53
Figure 3-21.	Virtual Machines display after Discover step	54
Figure 3-22.	Virtual Machines display after Re-iscover step	55
Figure 3-23.	Host Topology modification confirmation.....	56
Figure 3-24.	Virtual Machine Properties pane	59
Figure 3-25.	Categories filter for domain0 Host.....	60
Figure 3-26.	Available categories for domain0 Host	61
Figure 3-27.	Used services for domain0 Host.....	61
Figure 3-28.	Available services for Dom0SystemLoad category	62
Figure 3-29.	Users service for domain0 Host.....	63
Figure 3-30.	Virtual Platform monitoring	65
Figure 3-31.	EscalalPAR Add-on components for HMC managed systems.....	67
Figure 3-32.	EscalalPAR Add-on components for IVM managed systems.....	67
Figure 3-33.	VIOS.UsedPool Service Properties pane	70
Figure 3-34.	Reporting indicators	71
Figure 3-35.	HMC activation from Bull System Manager Console	72

Figure 3-36.	IVM activation from Bull System Manager Console	73
Figure 3-37.	Escala HMC reported Supervision	74
Figure 3-38.	Escala IVM reported supervision	74
Figure 3-39.	DDFA Monitoring Components	75
Figure 3-40.	BVS Web Server Monitoring Components	77
Figure 3-41.	JOnAS Architecture	78
Figure 3-42.	JOnAS configuration	79
Figure 3-43.	JOnAS domains	80
Figure 3-44.	JOnAS properties	80
Figure 3-45.	JOnAS category and services	81
Figure 3-46.	JOnAS indicators	82
Figure 3-47.	JOnAS category view	82
Figure 3-48.	jonasAdmin launching	83

List of Tables

Table 2-1.	Bull System Manager - Required Memory	5
Table 2-2.	Management Server Add-ons Installation Requirements	5
Table 2-3.	Management Server Add-ons Operational Requirements	6
Table 3-1.	GAMTT monitoring services.....	22
Table 3-2.	LSI CIM monitoring services.....	25
Table 3-3.	MegaRaid SAS (IR) monitoring services.....	28
Table 3-4.	StoreWay FDA monitoring services.....	29
Table 3-5.	EmcClariion monitoring services.....	31
Table 3-6.	NetApp monitoring services	33
Table 3-7.	Water Cooled Door monitoring services.....	37
Table 3-8.	DDF4 categories and services.....	76
Table 3-9.	Bull Video Services categories and services	77

Preface

Scope and Audience of this Manual

Bull System Manager Server Add-ons are Bull products, which provide extension to Bull System Manager for managing Bull platform specific devices or tools. Administration environments can include different platforms from the NovaScale Universal or Intensive Series, Express 5800 Series, EvolutiveLine Blade Series or Escala servers

In order to monitor a specific item, Bull System Manager Server Add-ons configuration must be customized. This manual explains also how, as an Administrator you can perform configuration tasks for these Add-ons.

Note Configuration tasks may only be performed by Administrators.

Using this Manual

For a conceptual approach to Bull System Manager Server Add-ons, read **Chapter 1**.

Chapter 2 describes how to install and configure Bull System Manager Server Add-ons.

Chapter 3 describes for each Server Add-on how to configure its elements on the Management server. It provides detailed information about all resource properties as well as concrete examples to help customization of the configuration (Modifying Service Parameters, ...).

This chapter also contains reference information about categories and services of the monitoring server provided by these Bull System Manager Server Add-ons.

Appendix A contains reference information about the check Nagios commands used by Bull System Manager Server Add-ons monitoring services.

Related Information

- *Bull System Manager Installation Guide* (Ref. 86 A2 54FA).
- *Bull System Manager User's Guide* (Ref. 86 A2 55FA). The Bull System Manager GUI (Graphical User Interface) and the way to use are described in this guide.
- *Bull System Manager Administrator's Guide* (Ref. 86 A2 56FA).
- Restrictions and well-known problems are described in the associated *Release Notes* document (Ref. 86 A2 57FA).
- *Dynamic Domains for Applications User's Guide* (Ref. 86 A2 63ER).

Highlighting

The following highlighting conventions are used in this book:

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

Note Important information.

Chapter 1. Bull System Manager Server Add-ons Concepts

1.1 Bull System Manager

1.1.1 Overview

Bull System Manager monitoring ensures the following tasks:

- Monitoring machines: Bull System Manager checks if these hosts are accessible, using the **ping** command from the System Manager. The machines to be monitored are either explicitly specified by the administrator or selected by a discovery mechanism.
- Monitoring specific elements of the hardware, operating system, services and Internet such as **Power Status**, **CPU load**, **memory usage**, **disk usage**, **number of users**, **processes** and **service execution**, **http** and **ftp services**.

The administrator can define status thresholds (OK, WARNING, CRITICAL, UNKNOWN) for each monitoring element. When an anomaly occurs or when normal status is recovered, **alerts** (in a log file) and **notifications** (by e-mail, by Bull autocal and/or by SNMP trap) are generated.

Note Hardware and OS monitoring for Bull Intel-Based platforms are provided by the Bull System Manager Server package, not by the Add-ons packages.

Bull System Manager Server Add-ons extend the Bull System Manager monitoring with more specific links to third-party management tools for specific devices or/and specific system functionalities.

Note These Server Add-ons packages extend generally the management server independently of the platform or/and OS type (storage, network, virtualization, framework, ...).

Bull System Manager consists of three main components that can be deployed on Windows and Linux systems:

- Management Server and Server Add-ons
- Management Console
- Management Agent.

Note Management Agent component can also be installed on AIX systems

Management Server and Server Add-ons

Provides the infrastructure and services in charge of collecting and operating management data. Management Server must be installed on the server dedicated to management.

Management Console

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

Management Agent

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

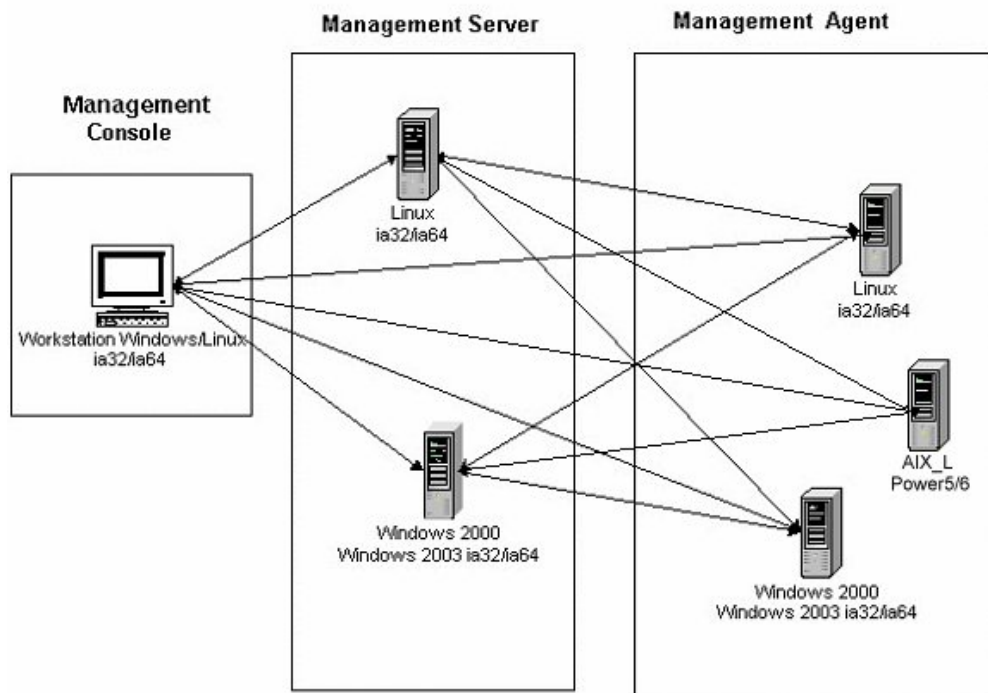


Figure 1-1. Bull System Manager Architecture

Note Bull System Manager for the different operating systems is distributed on the same CD-ROM.

1.1.2 Monitoring

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

Services are organized into monitoring **categories**. For instance, the **SystemLoad** category includes the **CPU** and **Memory** services for a Windows host.

1.1.3 Event Reception

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

1.1.4 Hardware Manager

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

1.1.5 Storage Manager

A **Storage Manager** manages storage for one or a set of servers or/and bays.

1.1.6 Virtualization Manager

A **Virtualization Manager** manages a set of virtual machines, viewed as Virtualization Platform.

1.2 Bull System Manager Server Add-ons

Bull System Manager Server Add-ons deliver optional management packages to extend Bull System Manager Server.

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

Some Server Add-ons are distributed on the *Bull System Manager Server* CD-ROM, while others are on the *Bull System Manager Server Add-ons* CD-ROM.

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

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
External Storage (BSM Server Add-ons CD)	StoreWay FDA Mgt Package
	EMC CLARiiON
	NetApp
External Device (BSM Server Add-ons CD)	Bull Water Cooled Door
Bull Tools Management (BSM Server Add-ons CD)	Dynamic Domains Mgt Package
	Bull Video Service Mgt Package
	JOnAS framework Mgt Package
Virtualization Management (BSM Server Add-ons CD)	Vmware ESX Mgt Package
	Xen HyperNova Master Mgt Package
	Escala LPAR Mgt Package

Each Server Add-on is described in the following chapters.

Chapter 2. Bull System Manager Server Add-ons Installation and Configuration

2.1 General Installation Requirements

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

2.1.1 Supported Operating Systems

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

The principal Requirements are the Bull System Manager Server pre-installation and its own requirements. See *Bull System Manager Installation Guide* for details.

2.1.2 Required Disk Space

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

2.1.3 Required Memory

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

Bull System Manager	Memory
Management Server	512 MB

Table 2-1. Bull System Manager - Required Memory

2.1.4 Installation Requirements

Server Add-ons	Component
*	BSMServer1.0-x

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

2.1.5 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 Web site to download the above versions. If not on-line, contact the Bull support team. Note: For IA32 machines the following previous 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 Web site to download the above versions. If not on-line, contact the Bull support team. Note: Not supported on Linux IA64 system.
BSMMegaRaidSAS	LSI MegaRaid SAS (IR) SNMP agent version 3.09 or higher. Go to www.lsilogic.com Web site to download the above versions. If not on-line, contact the Bull support team.
BSMStoreWayFDA	StoreWay FDA embedded SNMP Agent.
BSMEmcClariion	EMC Navisphere SNMP agent
BSMNetApp	NetApp embedded SNMP agent
BSMDDD4A	DDFA version 2.6.3 and higher
BSMBVS	BVS version 4.0 and higher
BSMJOnAS	JOnAS version 4.8 and higher
BSMVMwareESX	VMware ESX 3.0 and higher
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

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

2.1.6 Restrictions

Windows

N/A

Linux

N/A

2.2 Installing Bull System Manager Server Add-ons for Windows

2.2.1 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 present on the *Bull System Manager* CD-ROM or on the *Bull System Manager Add-ons* CD-ROM.

2.2.2 Installing Management Server Add-ons from the Bull System Manager CD-ROM

Management Server Add-ons, to be installed on the server dedicated to management, require the components indicated in 2.1.4 *Installation Requirements*, 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 component:
 - Management Server Add-ons
 and provides the following information:
 - What to install?
 - What to do now?

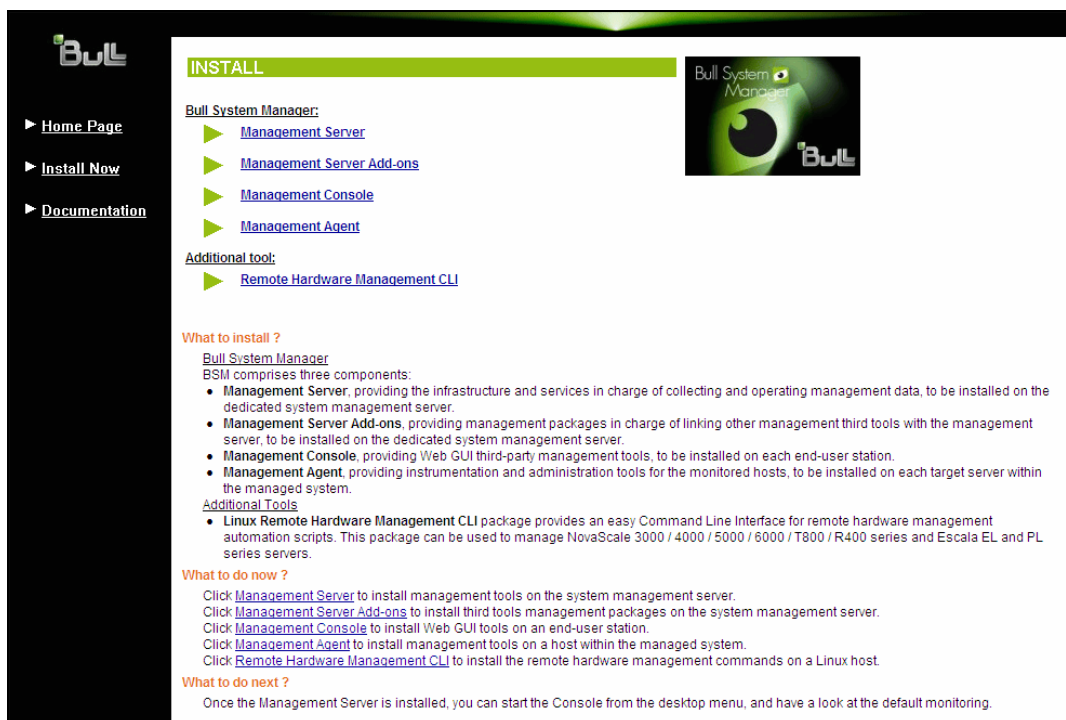


Figure 2-2. Windows Installation - Bull System Manager Install Page

Select **Management Server Add-ons**, then **Windows 32 bits** or **Windows 64 bits** operating system according to server type.

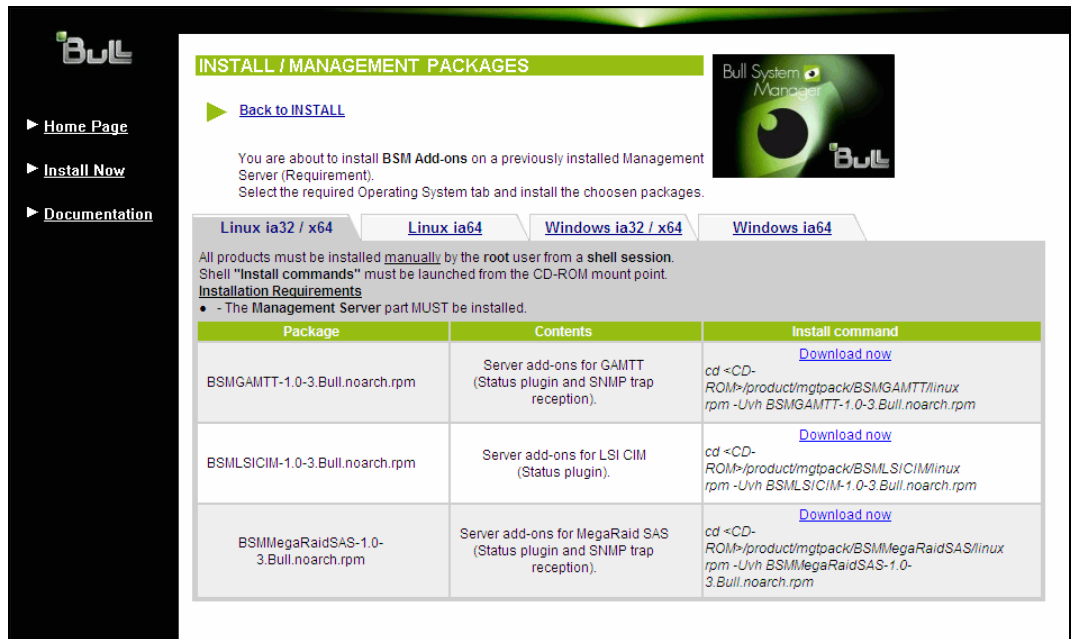


Figure 2-3. Windows Installation - Bull System Manager Server Add-ons Install Page

5. 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, Management Server Add-ons components are automatically operational.

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

Management Server Add-ons require the components indicated in 2.1.4 *Installation Requirements*. They have to be installed from the CD-ROM on the server dedicated to management.

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

1. Insert the Bull System Manager Add-ons 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`.

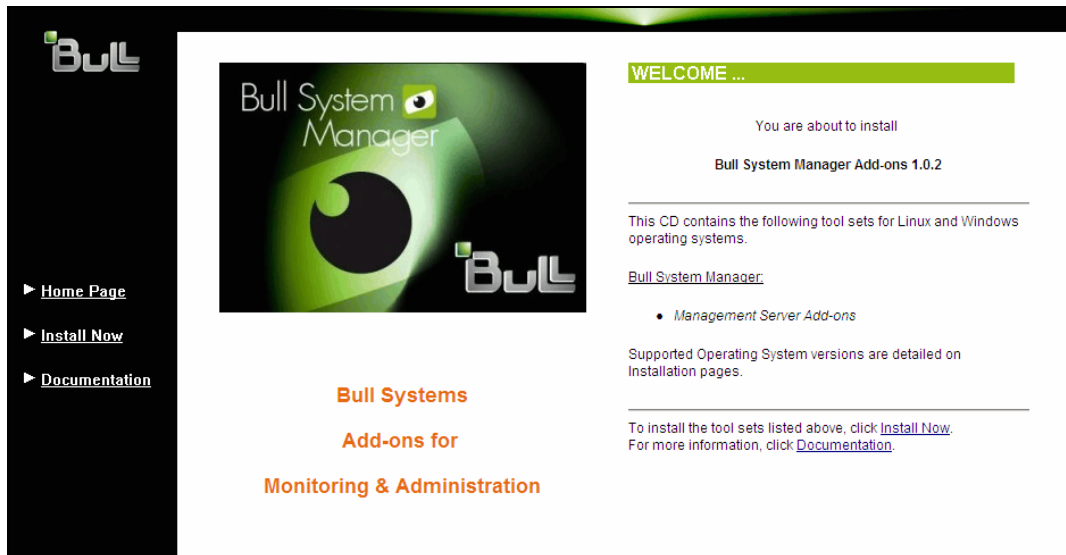


Figure 2-4. Windows Installation - Bull System Manager Add-ons Welcome Page

2. Click **Install Now** to open the **Install** page, which allows the selection of the required Bull System Manager component:

- Management Server Add-ons
- and provides the following information:
- What to install?
 - What to do now?

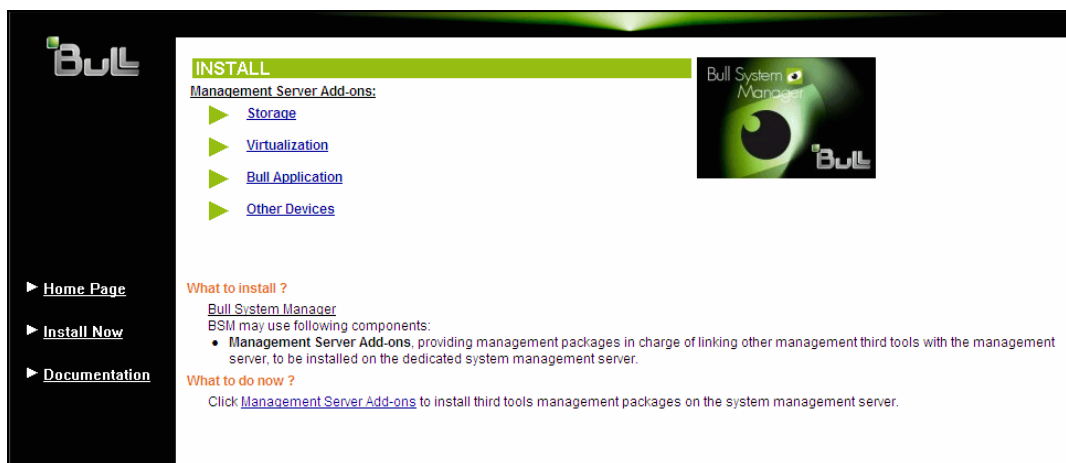


Figure 2-5. Windows Installation - Bull System Manager Add-ons Install Page

3. Select one of the provided categories (Storage, Virtualization, Bull Application or Other Devices) then select **Windows 32 bits** or **Windows 64 bits** operating system according to server type.

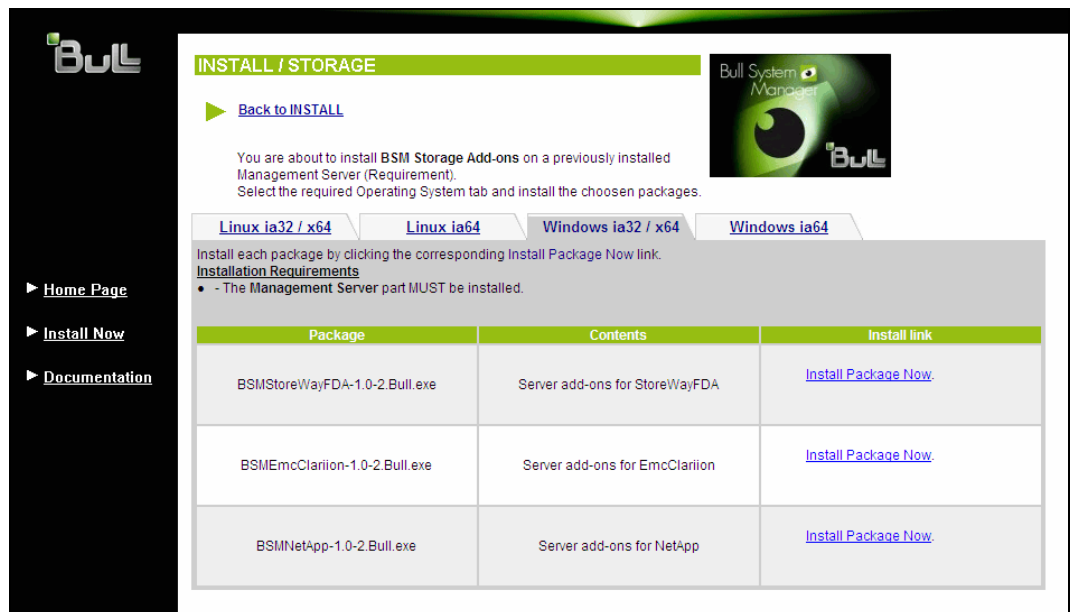


Figure 2-6. Windows Installation - Bull System Manager Install/Category Page

4. 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.

2.2.4 Un-installing Bull System Manager Server Add-ons 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 in previous version can remain in configuration. These elements must be removed using the BSM Configuration GUI.

2.2.5 Upgrading to a New Bull System Manager Server Add-ons 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 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 specific Add-ons migration, where applicable.

2.3 Installing Bull System Manager Server Add-ons for Linux

2.3.1 Prerequisites

To install Bull System Manager Server Add-ons on 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 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 in the root PATH environment variable. If a previous version of Mozilla has not been uninstalled, the Mozilla directory must be set at the beginning of the PATH variable.

- 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 present on the *Bull System Manager* CD-ROM or on the *Bull System Manager Add-ons* CD-ROM.

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 2.1.4 *Installation Requirements*, 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 **root**.
3. Insert the Bull System Manager CD-ROM in the drive.
The CD-ROM filesystem is automatically mounted to one of the following directories:
 - **/mnt/cdrom** or **/mnt/dvd** (Red Hat and Advanced Server distributions)
 - **/media/cdrom** or **/media/dvd** (SuSE distribution).
4. 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 2-7. Linux Installation - Bull System Manager Welcome Page

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

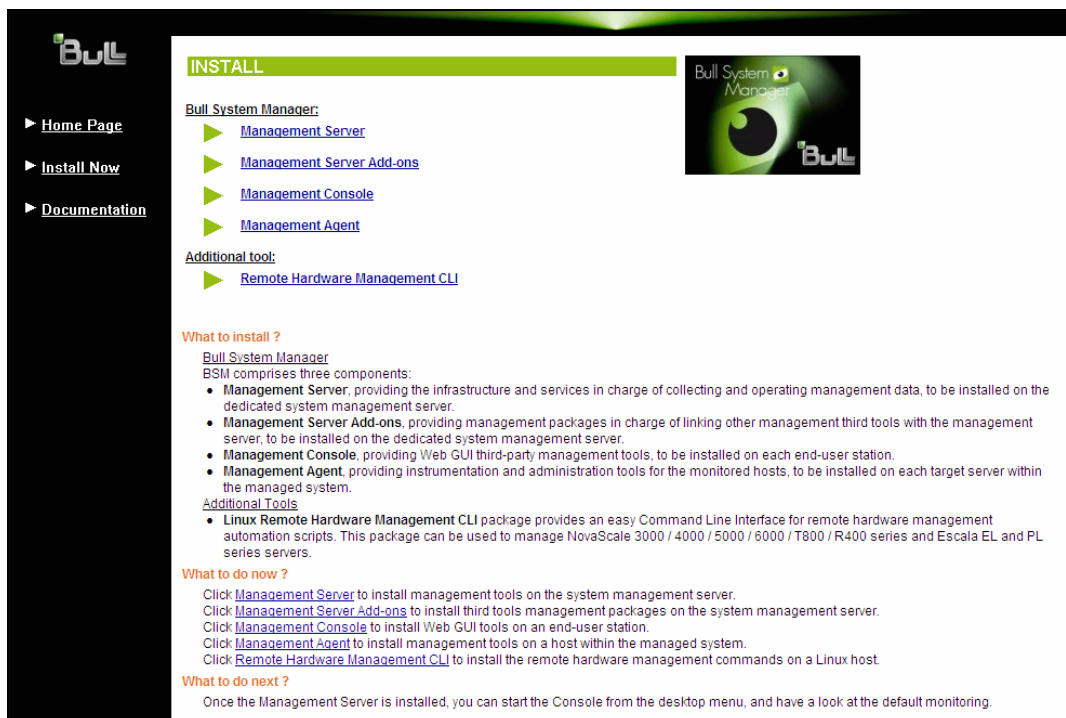


Figure 2-8. Linux Installation - Selecting Bull System Manager Components

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

Select the **Linux 32 bits** or **Linux 64 bits** operating system according to server type.



Figure 2-9. Linux Installation - Bull System Manager Server Add-Ons Install page

7. Install the selected **Bull System Manager Server Add-ons** packages as described below.

```
cd <CD-ROM mount point>/product/mgtpack/BSM<toolname>/linux
rpm -Uvh BSM<toolname>-1.0-x.noarch.rpm
```

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

Management Server Add-ons require the components indicated in 2.1.4 *Installation Requirements*. They have to be installed from the CD-ROM on the server dedicated to management.

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

1. Insert the Bull System Manager Add-ons CD-ROM in the drive.
The CD-ROM filesystem is automatically mounted to 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 2-10. Linux Installation - Bull System Manager Add-ons Welcome Page

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

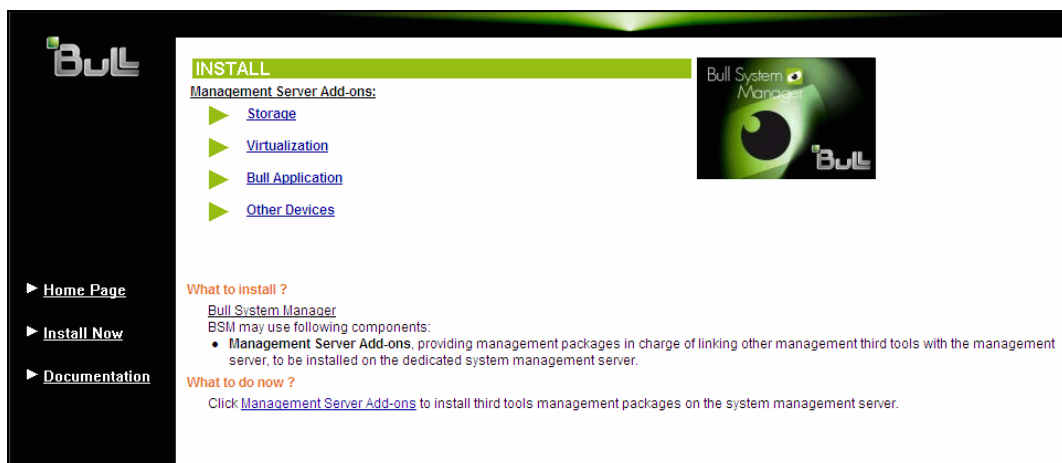


Figure 2-11. Linux Installation - Selecting Bull System Manager Server Add-ons

4. Select one of the provided categories (Storage, Virtualization, Bull Application or Other Devices), then select Linux 32 bits or Linux 64 bits operating system according to server type.

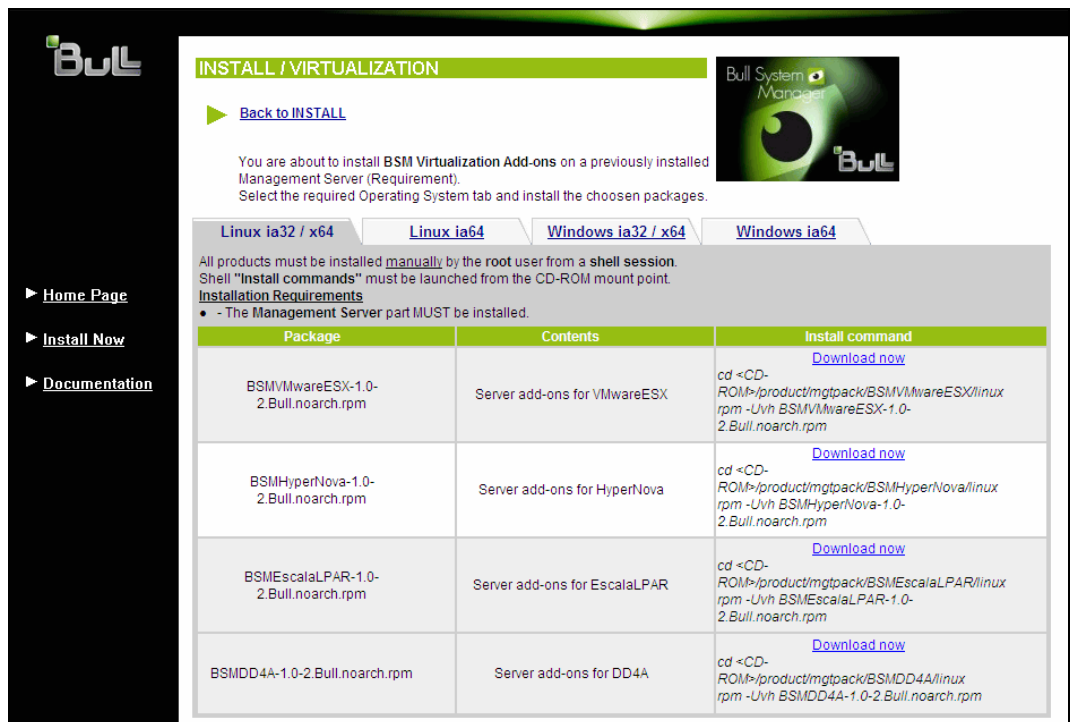


Figure 2-12. Linux Installation - Bull System Manager Server Add-ons Install Page

5. Install the selected **Bull System Manager Server Add-ons** package as follows:

```
cd <CD-ROM mount point>/product/mgtpack/BSM<toolname>/linux
rpm -Uvh BSM<toolname>-1.0-x.noarch.rpm
```

2.3.4 Uninstalling Bull System Manager Server Add-on Components

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

```
rpm -e BSM<toolname>-1.0-x.noarch.rpm
```

2.3.5 Upgrading to a new Bull System Manager Server Add-ons Version

When upgrading to a new Bull System Manager Server Add-ons version, 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 -Uvh BSM<toolname>-1.0-x.noarch.rpm
```

Note When you upgrade the Bull System Manager Management Server, you **MUST** upgrade previous release installed server add-ons to benefit from new improvements.

See the *Release Notes* for more details about specific add-on migration, 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 the Administrator can customize. New monitoring categories and services are provided.

2.4.1 Configuration GUI

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 delivers 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 with a Windows operating system
- Services for Linux hosts will be applied to all hosts with 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 monitored elements. 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 configuration.

Chapter 3. Bull System Manager Server Add-ons Description

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

3.1 Internal Storage (Free)

3.1.1 BSMGAMTT 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.lsiologic.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:

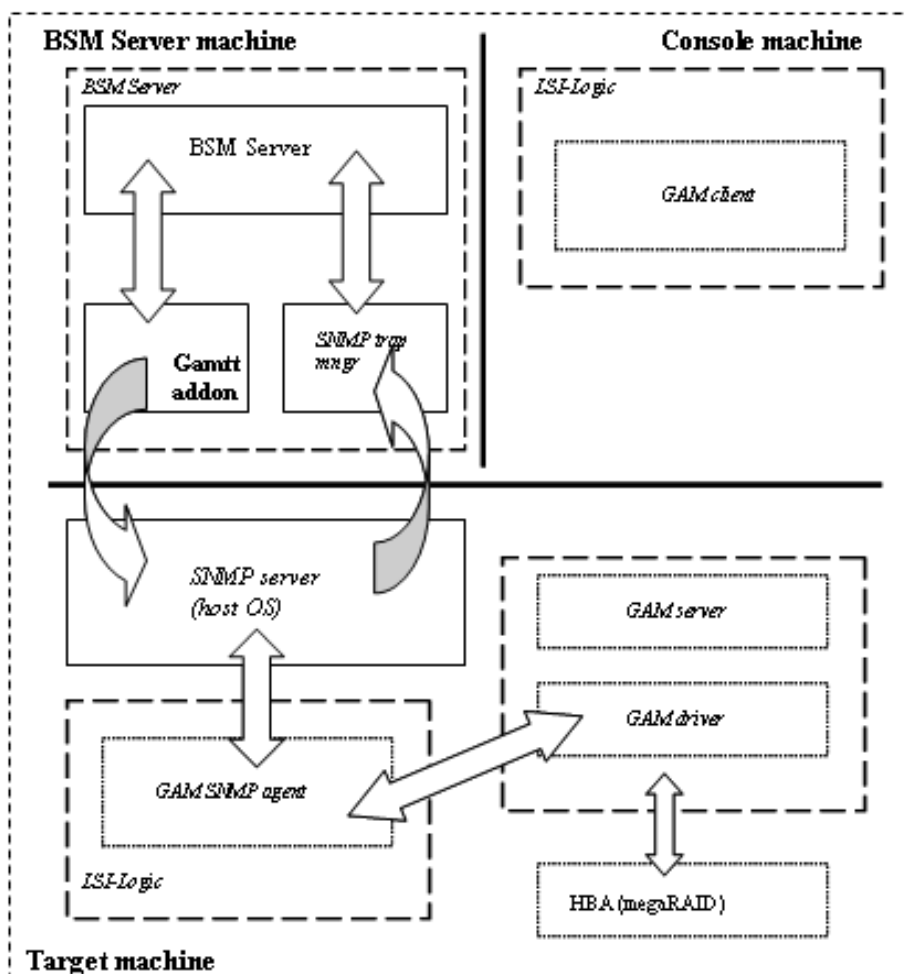


Figure 3-1. GAM Monitoring Components

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 **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 **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** 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 of 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 Appendix A.

Default syntax for "GAMTTraid.Status"

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

3.1.2 BSMLICIM 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:

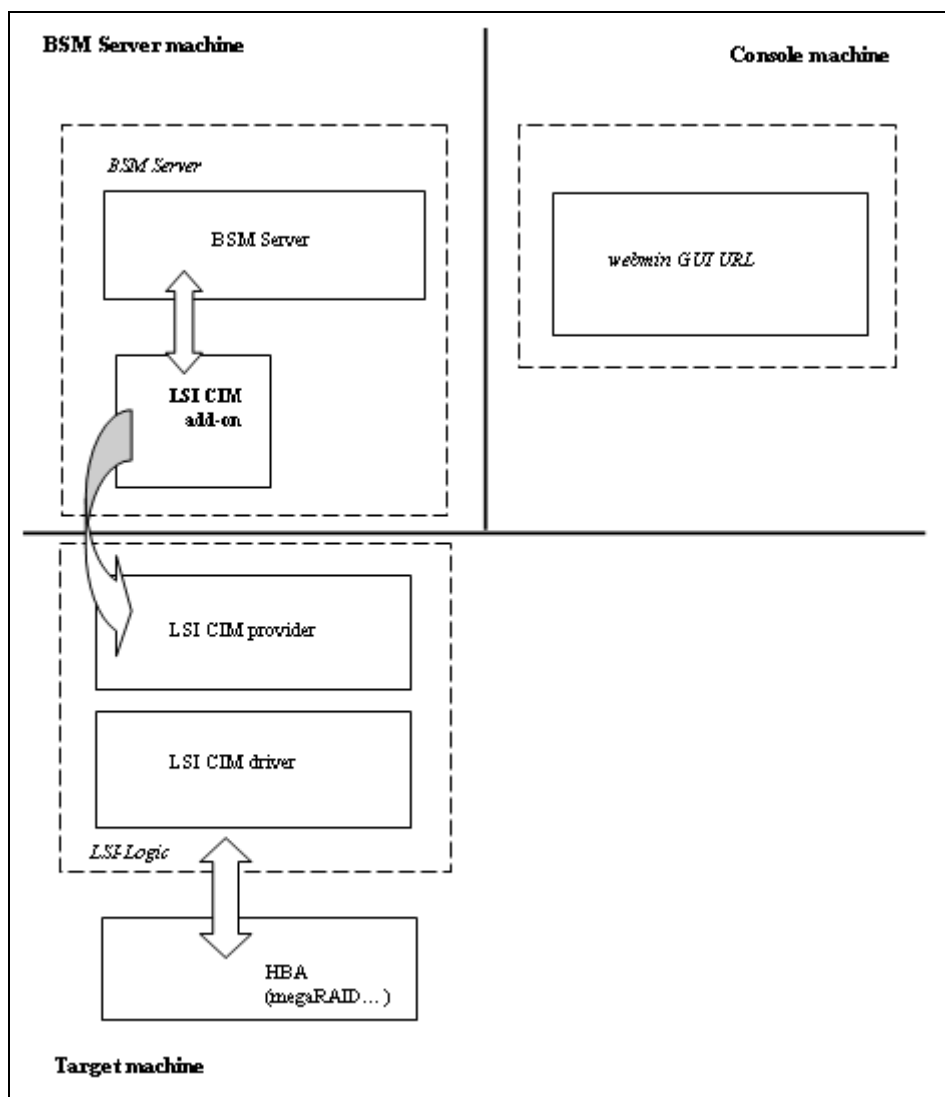


Figure 3-2. LSI CIM Monitoring Components

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 Appendix A.

Default syntax for "LsiCIM.CTRLstatus"

```
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 quote if the name contains blank characters.

Output

See the output of the `check_LSiCIM` shell command in Appendix A.

Default syntax for "LsiCIM.CTRLstatus"

```
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.

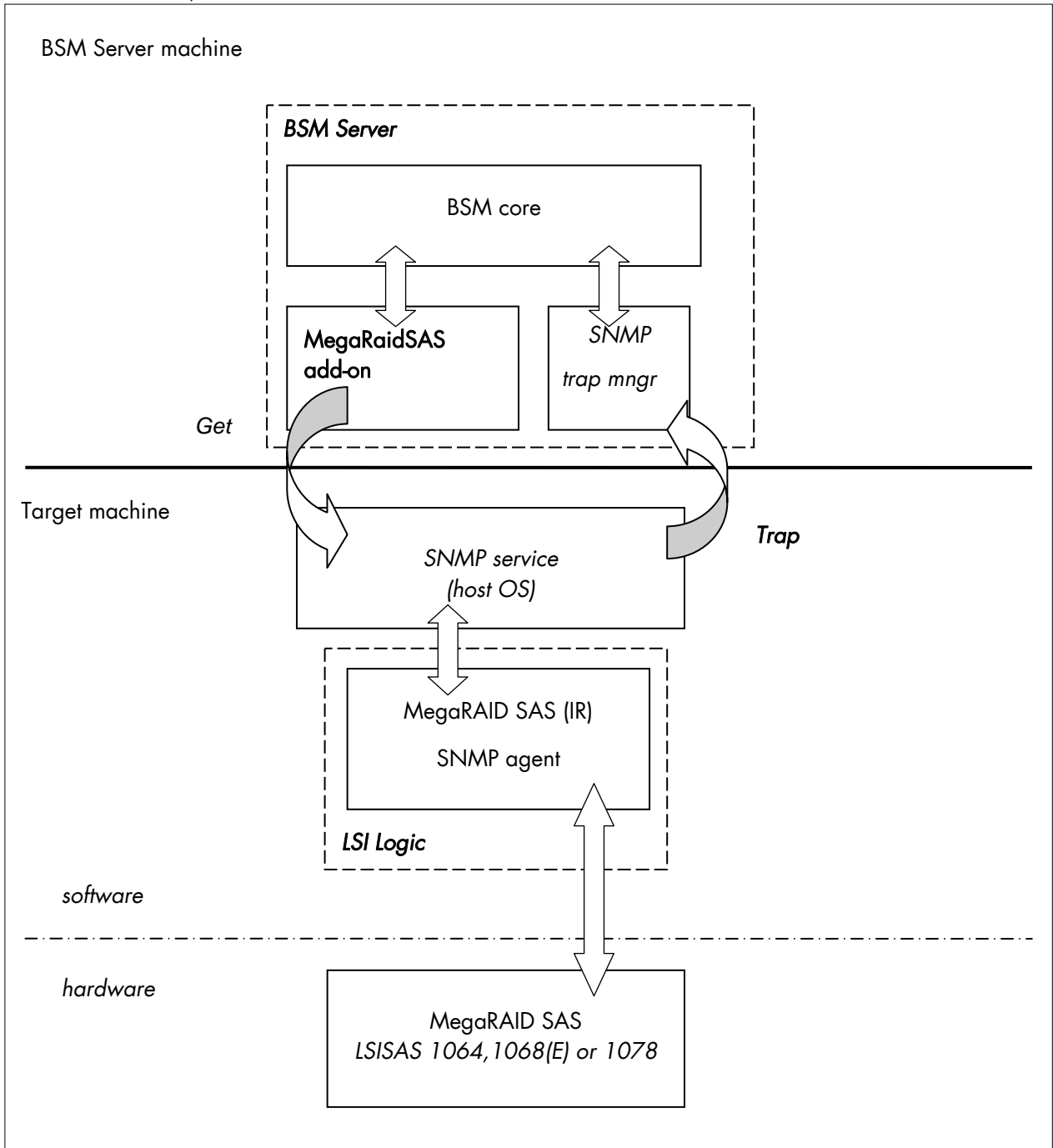


Figure 3-3. MegaRAID SAS Monitoring Components

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` 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 Appendix A for parameters details.

Default syntax for "MegaRaidSAS(_IR).Status"

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

3.2 External Storage Server Add-ons

3.2.1 BSMStoreWayFDA (StoreWay FDA Management)

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

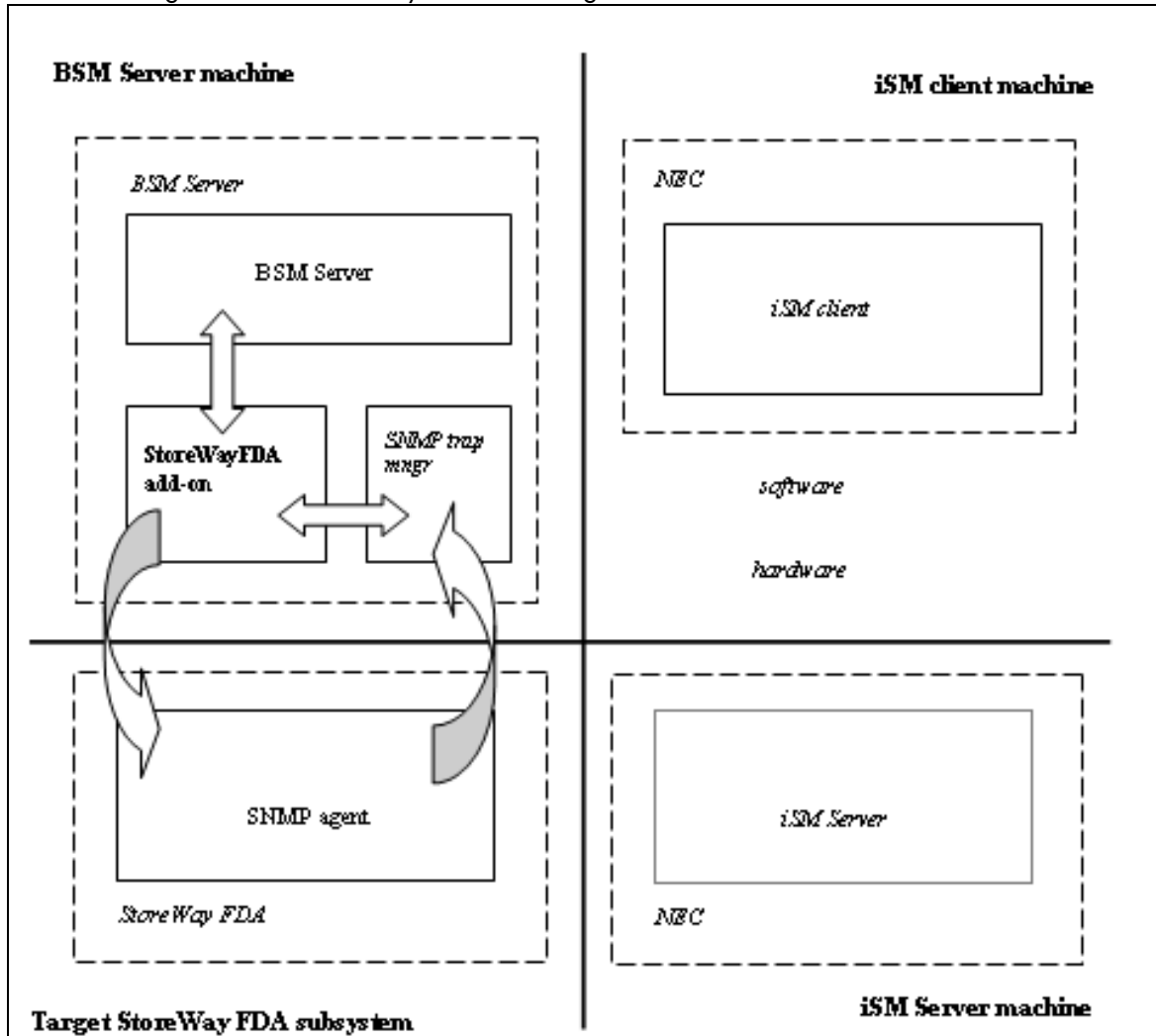


Figure 3-4. StoreWay FDA Monitoring Components

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 3-4. 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 its SNMP agent. 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` 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_storewayfda!<community>!<port>!<timeout>
```

See the `check_NECFDA` command in Appendix A for parameters details.

Default syntax for "StoreWayFDA.Status"

```
check_necfda!public!161!60
```

3.2.1.4 Bull System Manager Configuration

StoreWayFDA 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.

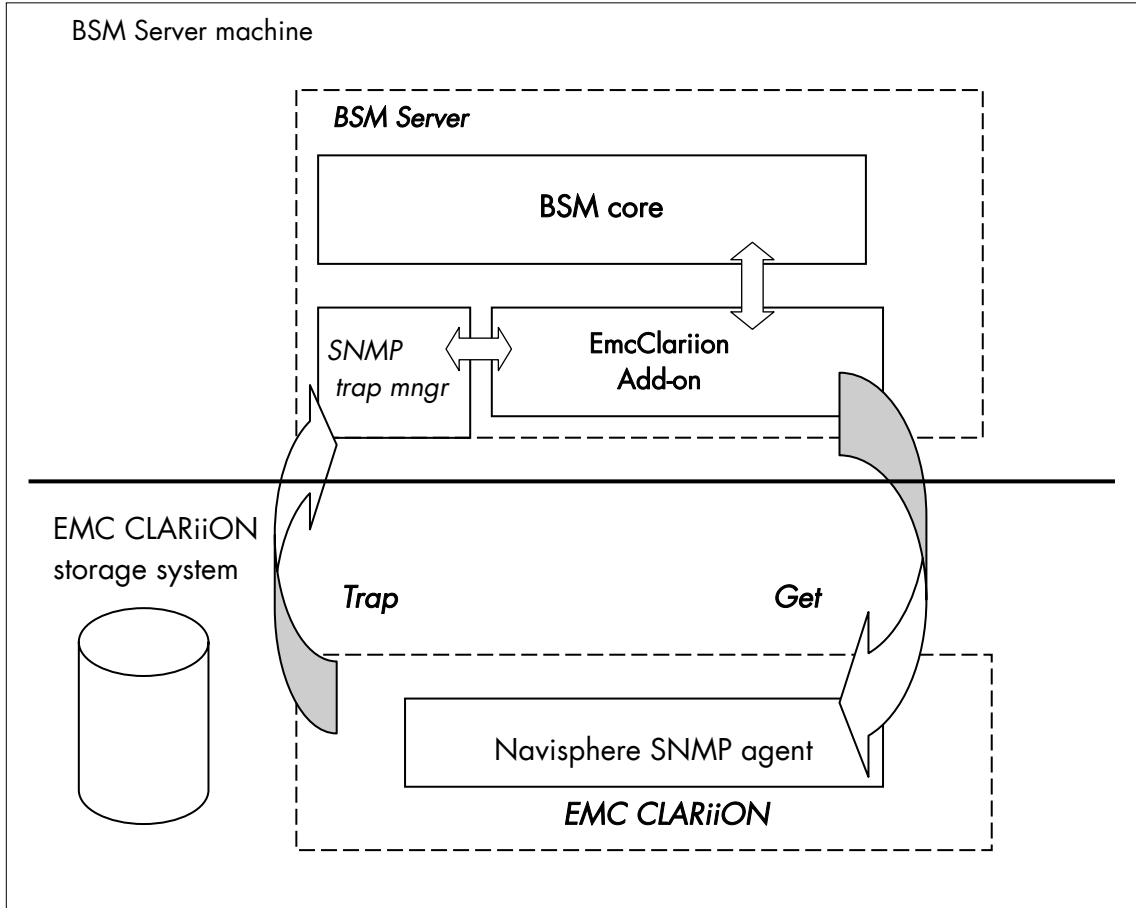


Figure 3-5. EMC CLARiiON Monitoring Components

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 3-5. 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` 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 Appendix A for parameters details.

Default syntax for "EmcClariion.Status"

```
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.

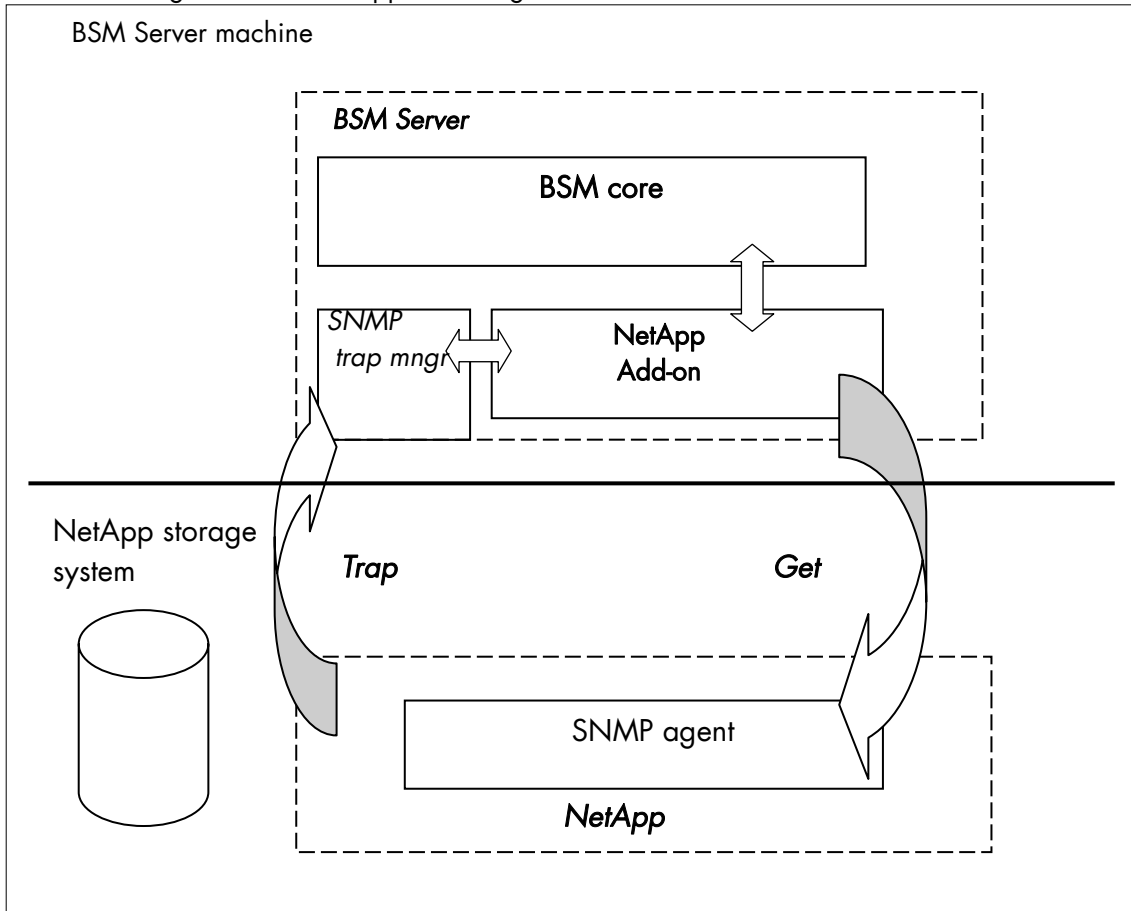


Figure 3-6. NetApp Monitoring Components

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 3-6. 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 its SNMP agent. This service checks the NetApp CPU load reported by the SNMP agent.
- Disks** For NetApp hosts managed via its SNMP agent. This service checks the status of the NetApp disks reported by the SNMP agent.
- Fans** For NetApp hosts managed via its SNMP agent. This service checks the status of the NetApp fans reported by the SNMP agent.
- GlobalStatus** For NetApp hosts managed via its SNMP agent. This service checks the NetApp Global Status reported by the SNMP agent.
- Power** For NetApp hosts managed via its SNMP agent. This service checks the status of the NetApp power supplies reported by the SNMP agent.
- RAIDStatus** For NetApp hosts managed via its SNMP agent. This service checks the NetApp RAID status reported by the SNMP agent.
- VolumeStatus** For NetApp hosts managed via its SNMP agent. 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** 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

3.2.3.4 Nagios check commands

check-netapp-cpload (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-cpload** command in Appendix A 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 Appendix A 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 Appendix A 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 Appendix A for parameters details.

Default syntax for "NetApp.GlobalStatus":

```
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 Appendix A 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 Appendix A for parameters details.

Default syntax for "NetApp.RAIDStatus":

```
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 Appendix A for parameters details.

Default syntax for "NetApp.VolumeStatus":

```
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 BSMWaterCooledDoor (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.

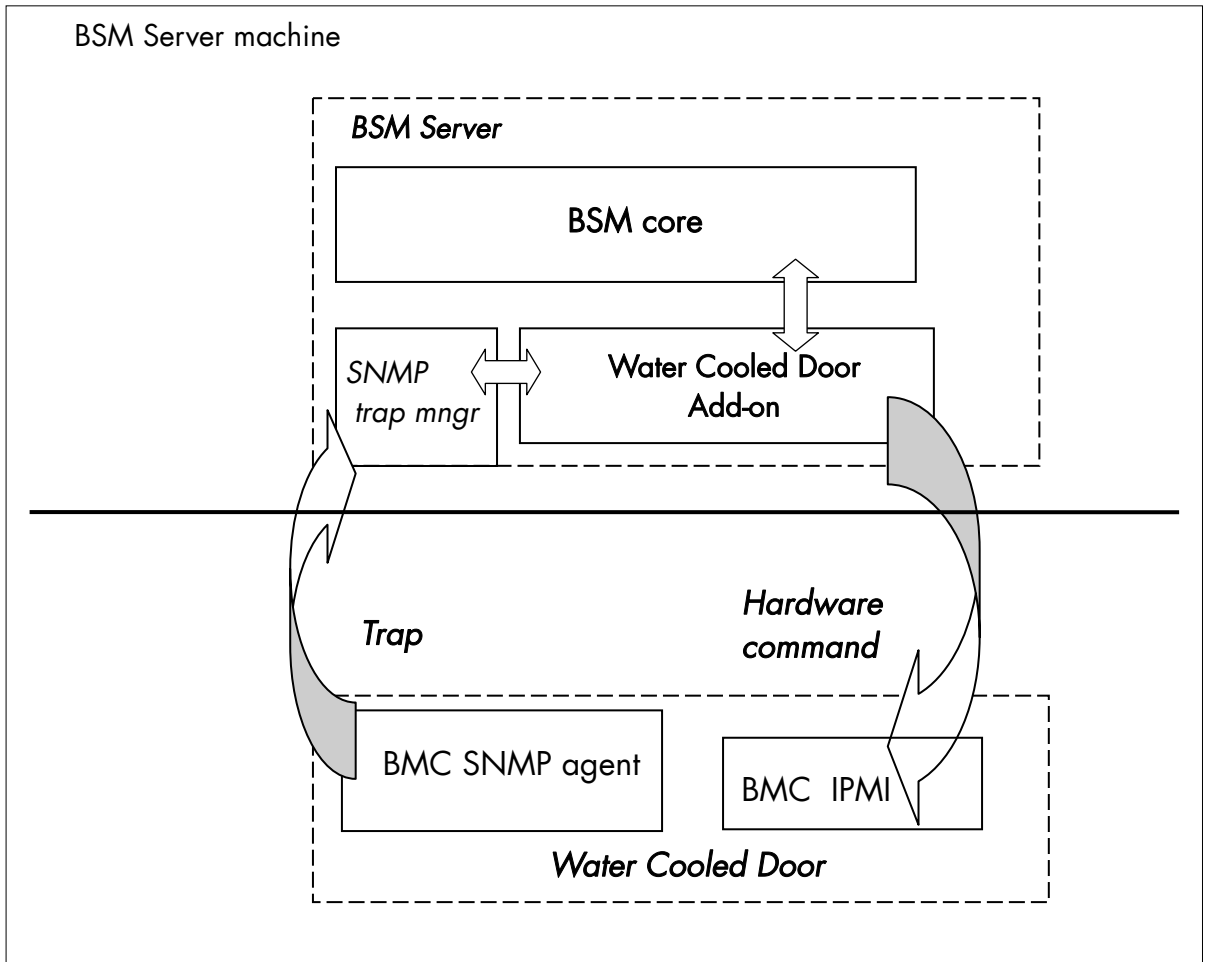


Figure 3-7. Water Cooled Door Monitoring Components

3.2.4.1 Default Categories & Services (independent of OS type)

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

Table 3-7. 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.

3.2.4.2 Hardware Category

PowerStatus For **WaterCooledDoor** hosts managed via IPMI Hardware commands. This service checks the WaterCooledDoor power 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.

3.2.4.3 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.

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.

3.2.4.4 Reporting Indicators

Reporting indicators are defined for the WaterCooledDoor host. They get values from the corresponding monitoring services.

Indicators applied to the WaterCooledDoor Host

Indicator	Corresponding Service
<WaterCooledDoor_host>_CurrentPower	Sensors.CPULoad
<WaterCooledDoor_host>_DeltaPressure	Sensors.DeltaPressure
<WaterCooledDoor_host>_TemperatureAverage	Sensors.TemperatureAverage
<WaterCooledDoor_host>_ValveAperture	Sensors.ValveAperture

3.2.4.5 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 Appendix A 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 Appendix A 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 Appendix A for parameters details.

3.2.4.6 Bull System Manager Configuration

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 Virtualization Server Add-ons

3.3.1 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 them to defined entities,
- Administration features to perform actions on elements.

3.3.1.1 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.

3.3.1.2 Topology Representation

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

To load a specific view, select **File** → **Load** → **SystemMgt** → **view name**

Or, if already loaded, switch from one view to another by selecting **Views** → **view name**

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

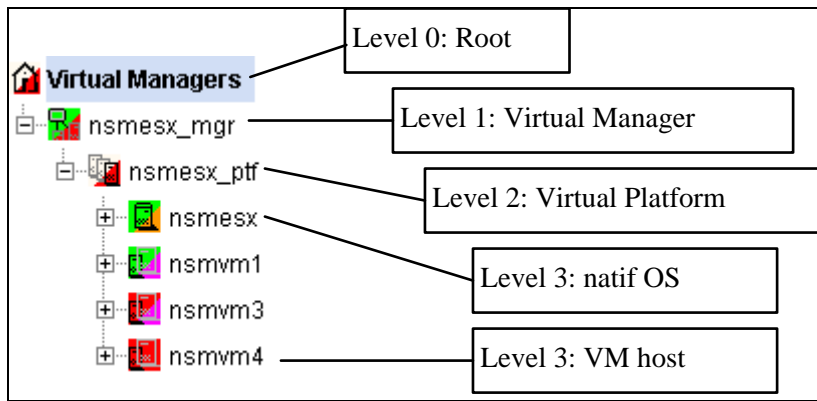


Figure 3-8. Virtual Managers view

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 pane.

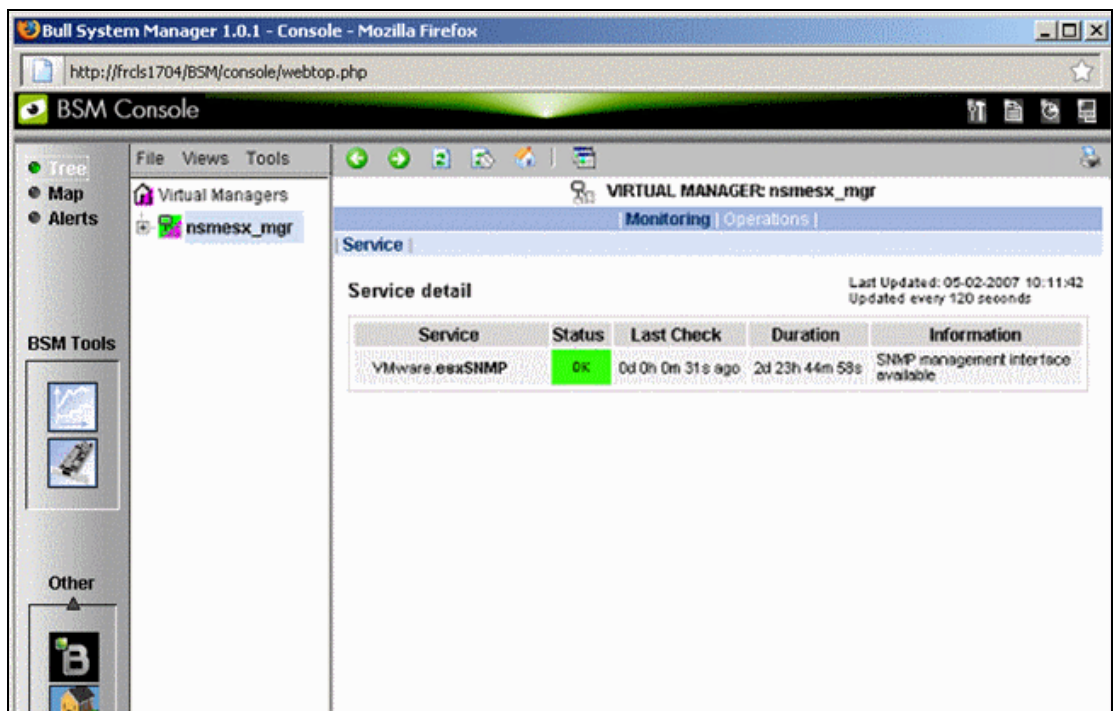


Figure 3-9. Virtual Manager information pane

3.3.2 BSMVMwareESX for "VMware ESX" Management

3.3.2.1 Overview

The **VMware ESX** server is a virtualization layer that abstracts processor, memory, storage and networking resources into multiple virtual machines. The VMwareESX Add-on provides functional links to manage the virtual machines hosted by the ESX server.

Note The link is functional only with the version 3 of the ESX server.

The VMwareESX Add-on retrieves VM and native OS monitoring information via the VMware Service Console SNMP interface and allows the Web Virtual Interface to be launched from the Bull System Manager Console.

The following figure shows the link between each component:

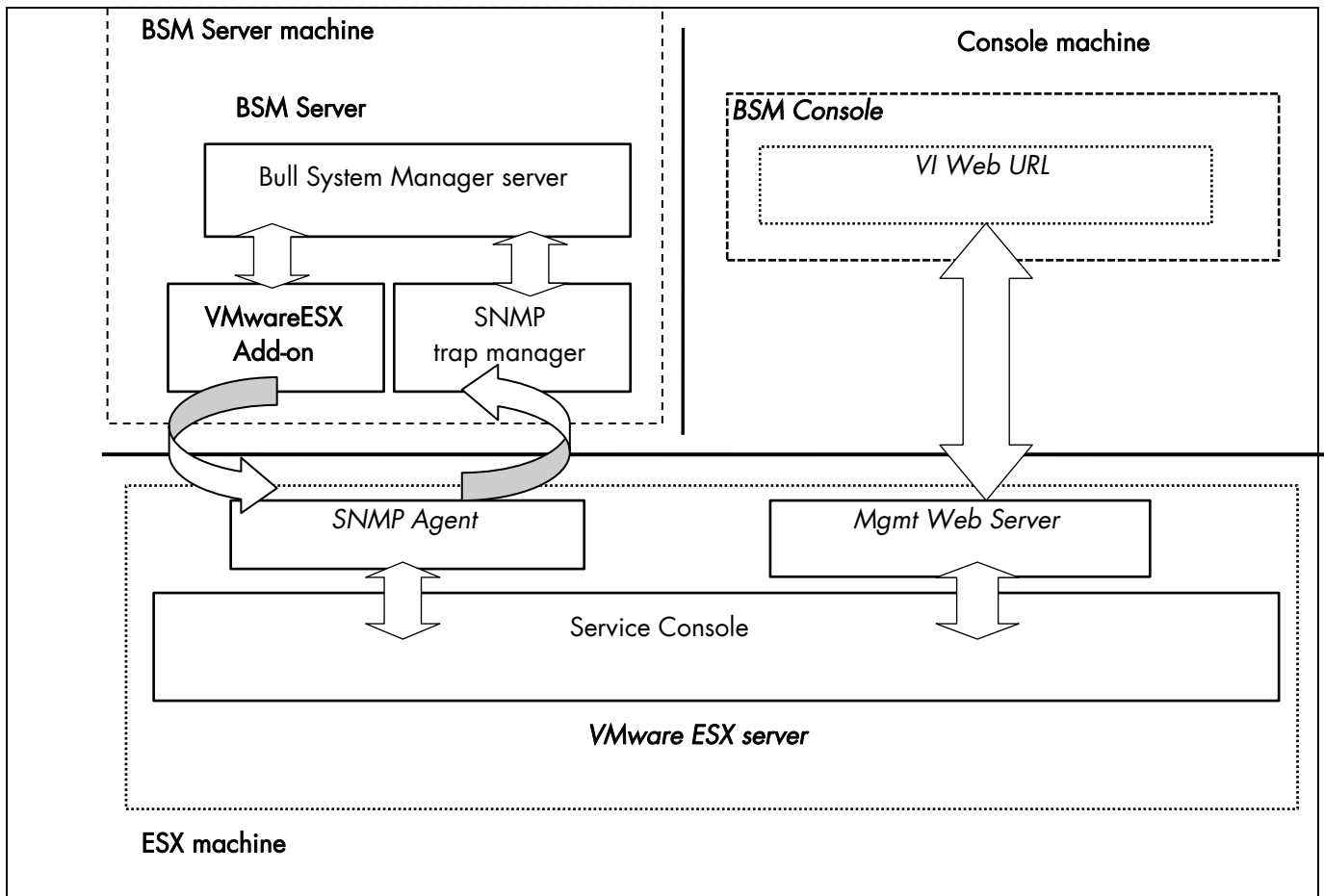


Figure 3-10. VMwareESX Add-on components

Note The SNMP agent of the ESX server must be configured to receive SNMP requests from and to send traps to the Bull System Manager Server. Web access requires specific configuration of the Web client. For detailed information about these procedures, see the VMware Infrastructure documentations available at http://www.vmware.com/support/pubs/vi_pubs.html.

3.3.2.2 Bull System Manager Configuration

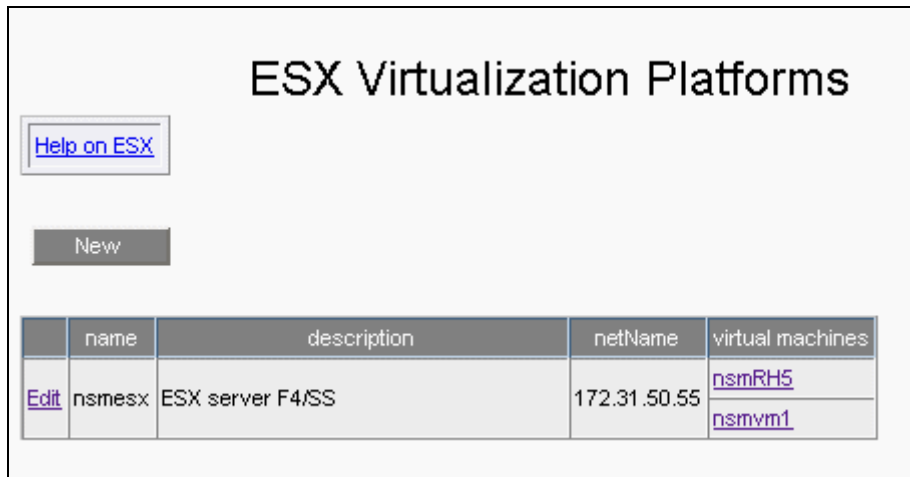
To configure the monitoring elements for the VMware ESX Add-on, you have to define an ESX Virtual Platform from the Bull System Manager Configuration GUI. Native OS, VMs, related monitoring services and reporting indicators are defined in one easy step.

The native OS is represented by a BSM host with the OS: **ESX**.

VMs are represented by a BSM host with the model: **VMware**.

3.3.2.2.1 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 in the following example:



	name	description	netName	virtual machines
Edit	nsmesx	ESX server F4/SS	172.31.50.55	nsmRH5 nsmvm1

Figure 3-11. ESX Virtual Platforms page

It is possible:

- To create a new ESX Virtual Platform using the **New** button
- To edit or delete a resource using the **Edit** link
- To edit a virtual machine using the **<hostname>** link.

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

Properties	
name	<input type="text"/>
description	<input type="text"/>
ESX Server Host	
name	<input type="text"/> <input type="button" value="Select"/>
model	<input type="text" value="other"/> ▼
network name	<input type="text"/>
SNMP Configuration	
SNMP port	<input type="text" value="161"/>
SNMP community	<input type="text" value="public"/>
Virtualization Platform	
Virtual Machines	
<input type="button" value="Discover"/>	To get the list of virtual machine hosted, click the Discover button

Figure 3-12. ESX Platform Properties

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

- **ESX Server Host:** used to define the physical machine and the native OS.
- **SNMP Configuration:** used to configure SNMP interface data.
- **Virtualization Platform:** 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 <i>Bull System Manager Administrator's Guide</i> for values).
network name	ESX host network name (hostname or IP address).

SNMP Configuration Properties

SNMP port	SNMP agent port.
SNMP configuration	SNMP agent community.

Virtualization Platform Properties

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

Virtual Machines Discovery

The result of the discovery is 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 an already defined host by clicking the **Select** button or you can create a host by completing the corresponding fields.

Note When you select an already defined host, you cannot change its network name and OS. But 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.

<input checked="" type="checkbox"/>	ESX Virtual Machines	NS Master Configuration			
	Name	Name	netName	OS	
<input checked="" type="checkbox"/>	nsmvm5	nsmvm5	Select	nsmvm5	other
<input checked="" type="checkbox"/>	nsmvm2	nsmvm2	Select	nsmvm2	other
<input checked="" type="checkbox"/>	White windows	White_windows	Select	White_windows	other
<input checked="" type="checkbox"/>	nsmRH5	nsmRH5	Select	nsmRH5	other
<input checked="" type="checkbox"/>	nsmvm1	nsmvm1	Select	172.31.50.60	other
<input checked="" type="checkbox"/>	nsmvm4	nsmvm4	Select	nsmvm4	other

To update the list of virtual machines, click the Re-discover button

Figure 3-13. ESX Virtual Machines pane

Virtual Machines Re-Discovery

Re-Discovery 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 more defined in the VMware ESX configuration.

During the Re-discovery 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 platform on form validation. New VMs must be explicitly checked for being added in the platform to be linked to the platform on form validation.

Note How to Add, Delete or Modify Virtual Machine is detailed in 3.3.2.2.2 *Virtual Machine Edition*, on page 47.

After edition:

- Click **OK** to validate your edition
- Or click **Cancel** to return to Virtual Platforms pages without changes
- 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 Edition with a **Topology modification** requires confirmation: a page listing all modifications to be applied to the Topology configuration is displayed, as shown in the following figure.

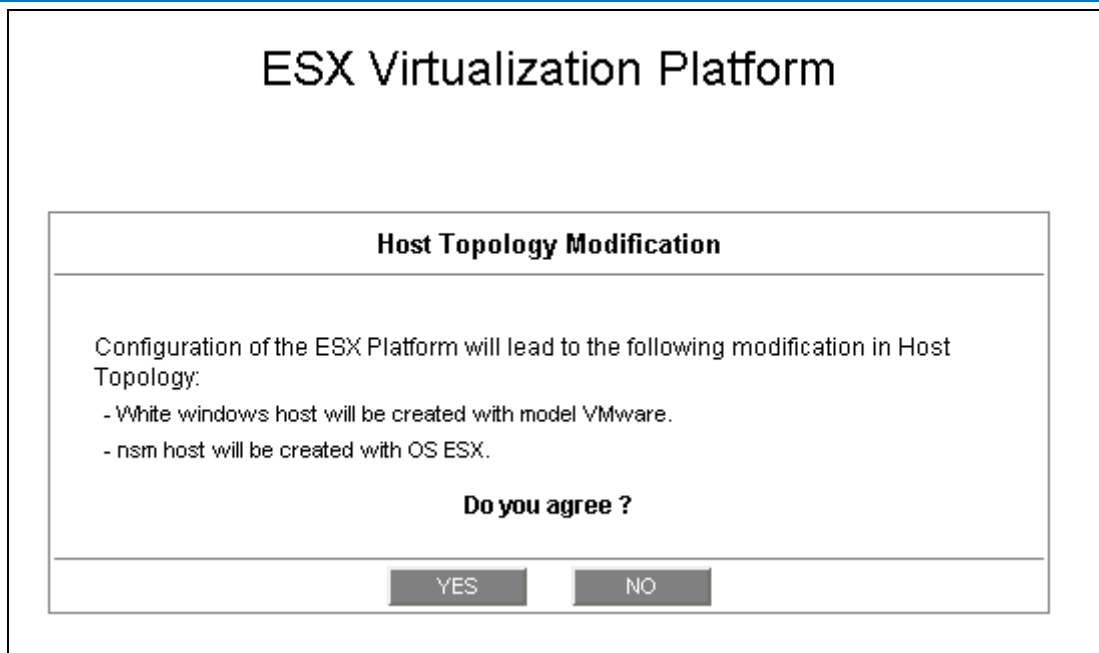


Figure 3-14. Host Topology modification confirmation

If you do not agree, click **NO** to return to the platform edition page, 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 specific Supervision linked to this type of server. The following table 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 VirtualMachine category and related services are instantiated for each VMware host.

3.3.2.2.2 Virtual Machine Edition

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

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

Modification of host properties must be done from the Host edition page.

Add a virtual machine to a platform

Adding a virtual machine is performed by checking the corresponding line in Virtual Machines part of the platform edition form and setting the host characteristics in 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 as part of the Bull System Manager platform are displayed. To add a virtual machine, you must perform a Re-discovery to get the list of all machines defined on the Virtualization Server.

Remove a virtual machine from a platform

Removing a virtual machine is performed by unchecking the corresponding line in the Virtual Machines part of 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.

Modify 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 choose it in the list of already defined hosts in Bull System Manager by clicking the **Select** button.

To modify other characteristics as 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.

Delete all virtual machines and corresponding hosts.

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

3.3.2.2.3 Virtualization Supervision

As specified above, services are instantiated for each 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 Native OS

Service	Description	Check_command
Status	Checks ESX server status	check_esx_server
SNMP	Checks the ESX SNMP interface	check_esx_snmp
Memory	Checks ESX memory availability	check_esx_mem
Alerts	Processes alerts received from the ESX SNMP agent	none (SNMP Trap receiver)

Monitoring services defined for VM hosts are associated with the **VirtualMachine** category.

Services Applied to the VM Host

Service	Description	Check_command
Status	Checks VM status	check_esx_vm
CPU	Checks VM CPU usage	check_esx_vm_cpu
Memory	Checks VM memory availability	check_esx_vm_mem

Monitoring services related to Virtual Platform elements are automatically created during the edition of the ESX Virtual Platform. These services can be displayed and edited from the Services page in the Supervision domain, but only attributes related to monitoring or notification can be edited.

Properties	
category	VMwareESX
name	Status
description	checks the ESX server status (automatically generated)
model	any
OS family	ESX
host list expression	nsmesx
Monitoring attributes	
status	<input checked="" type="radio"/> active <input type="radio"/> inactive
Monitoring command attributes (for this service)	
check command	check_esx_server
check command parameters	public!50%!0%
monitoring period	24x7
polling interval	5 mn (5 mn by default if empty)
Notification attributes (for this service)	
e-mail contact groups	<div style="display: flex; justify-content: space-between;"> <div> <p>Selected Objects</p> <ul style="list-style-type: none"> mgt-admins </div> <div style="text-align: center;"> <p><= Add</p> <p>Remove =></p> </div> <div> <p>All Objects</p> <ul style="list-style-type: none"> mgt-admins </div> </div>
enable Bull autocal	<input type="radio"/> Yes <input checked="" type="radio"/> No
enable SNMP trap	<input checked="" type="radio"/> Yes <input type="radio"/> No
notification period	24x7
re-notification interval	0 mn (0 mn by default if empty)
notify if warning	<input checked="" type="radio"/> Yes <input type="radio"/> No
notify if critical	<input checked="" type="radio"/> Yes <input type="radio"/> No
notify if recovery	<input checked="" type="radio"/> Yes <input type="radio"/> No

Figure 3-15. VMware service properties pane

Note During ESX Platform definition, all services are defined and activated for the ESX server and for each VM. To deactivate the monitoring of one service, set **status** (Monitoring attributes part) to inactive.

3.3.2.3 Nagios Check Commands

check_esx_server

The configurable Bull System Manager service check command syntax is:

```
check_esx_server!<snmp_community>!<wThres>%!<cThres>%
```

See the **check_esx3** command in Appendix A for parameters details.

check_esx_snmp

The configurable Bull System Manager service check command syntax is:

```
check_esx_snmp!<snmp_community>
```

See the **check_esx3** command in Appendix A for parameters details.

check_esx_mem

The configurable Bull System Manager service check command syntax is:

```
check_esx_mem!<snmp_community>!<wThres>!<cThres>
```

See the **check_esx3** command in Appendix A for parameters details.

check_esx_vm

The configurable Bull System Manager service check command syntax is:

```
check_esx_vm!<esx_server>!<snmp_community>!<vmname>
```

See the **check_esx3** command in Appendix A for parameters details.

check_esx_vm_memory

The configurable Bull System Manager service check command syntax is:

```
check_esx_vm!<esx_server>!<snmp_community>!<vmname><wThres>!<cThres>
```

See the **check_esx3** command in Appendix A for parameters details.

check_esx_vm_cpu

The configurable Bull System Manager service check command syntax is:

```
check_esx_cpu!<esx_server>!<snmp_community>!<vmname><wThres>!<cThres>
```

See the **check_esx3** command in Appendix A for parameters details.

3.3.2.4 Reporting Indicators

Reporting indicators are defined for VM hosts and for native OS. They get values from the corresponding monitoring services.

Indicators Applied to the Native OS

Indicator	Corresponding Service
<esx_server>_esxMemory	esxMemory

Indicators Applied to the VM Host

Indicator	Corresponding Service
<vm_host>_vmCPU	vmCPU
<vm_host>_vmMemory	vmMemory

Note During ESX Platform definition, all indicators are defined and activated for the ESX server and for each VM. To deactivate the reporting of one indicator, set it to inactive. Beware, if you deactivate the corresponding service, the indicator will no longer be collected.

3.3.2.5 Bull System Manager Console

VMwareESX 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 VI Web

VMwareESX Monitoring

From the platform or host elements, you can access monitoring information.

From the hosts element, you can display information related to associated services 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:

The screenshot shows the VMwareESX monitoring interface. At the top, there's a navigation bar with 'Monitoring', 'Reporting', and 'Operations'. Below that, a summary table shows the status of hosts and services. The 'Selected Host Services' row shows 13 hosts, 3 problems, 1 OK, 1 Warning, 2 Unknown, 0 Critical, and 1 Pending. Below this is a 'Service details' table with columns for Host, Service, Status, Last Check, Duration, and Information.

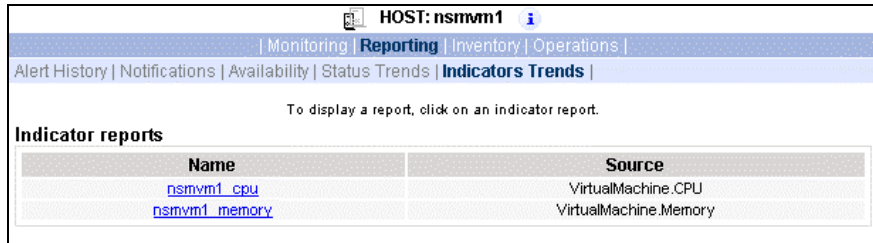
Host	Service	Status	Last Check	Duration	Information
nsmRH5	PING	OK	0d 0h 2m 50s ago	0d 0h 2m 50s	PING OK - Packet loss = 0%, RTA = 0.00 ms
	VirtualMachine.CPU	UNKNOWN	0d 0h 1m 59s ago	0d 0h 1m 59s	No saved state for nsmRH5 CPU time yet - wait for next poll.
	VirtualMachine.Memory	OK	0d 0h 1m 9s ago	0d 0h 1m 9s	Memory free: 225.28Mb (88%) [Total available 256Mb] on vhost nsmRH5
	VirtualMachine.Status	OK	0d 0h 7m 49s ago	0d 0h 9m 30s	Virtual host is up (ID: 192)
nsmesx	PING	OK	0d 0h 4m 30s ago	0d 0h 6m 59s	PING OK - Packet loss = 0%, RTA = 0.00 ms
	VMwareESX.Alerts	PENDING	0d 0h 5m 55s+ ago	0d 0h 5m 55s+	Service is not scheduled to be checked...
	VMwareESX.Memory	OK	0d 0h 3m 39s ago	0d 0h 6m 9s	Memory free: 16111.6Mb (98%) [Total available 16383.6Mb]
	VMwareESX.SNMP	OK	0d 0h 2m 48s ago	0d 0h 2m 48s	SNMP management interface available
	VMwareESX.Status	WARNING	0d 0h 1m 56s ago	0d 0h 1m 56s	VHosts: 2/7 up: nsmvm5(OFF), nsmvm2(OFF), VWhite windows(OFF), nsmRH5(ON), nsmvm1(ON), nsmvm3(OFF), nsmvm4(OFF)
nsmvm1	PING	OK	0d 0h 1m 6s ago	0d 0h 6m 57s	PING OK - Packet loss = 0%, RTA = 0.00 ms
	VirtualMachine.CPU	UNKNOWN	0d 0h 6m 54s ago	0d 0h 6m 54s	No saved state for nsmvm1 CPU time yet - wait for next poll.

Figure 3-16. VMwareESX monitoring information

VMwareESX Reporting

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

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



The screenshot shows the VMware ESX Reporting interface for host 'nsmvm1'. The 'Reporting' menu is active, and the 'Indicators Trends' sub-menu is selected. Below the navigation bar, there is a table titled 'Indicator reports' with two columns: 'Name' and 'Source'. The table contains two entries: 'nsmvm1_cpu' with source 'VirtualMachine.CPU' and 'nsmvm1_memory' with source 'VirtualMachine.Memory'. A message above the table says 'To display a report, click on an indicator report.'

Name	Source
nsmvm1_cpu	VirtualMachine.CPU
nsmvm1_memory	VirtualMachine.Memory

Figure 3-17. VMwareESX reporting information

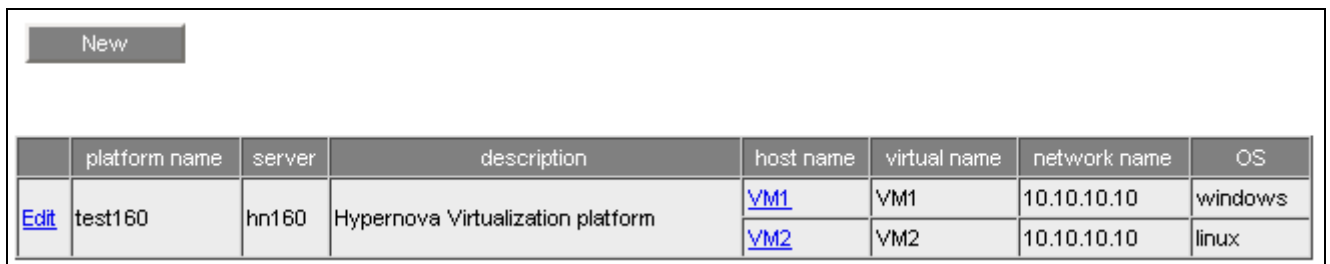
From the platform element, you can display indicators related to all platform elements.

3.3.3 BSMHyperNova for "HyperNova" Management

3.3.3.1 Overview

The HyperNova server is a virtualization layer that abstracts processor, memory, storage and networking resources into multiple virtual machines. The HyperNova Add-on provides functional links to manage the virtual machines hosted by the HyperNova server, by requesting the administration tool, HyperNova Master (HN Master).

The following figure shows the link between each component:



The screenshot shows a table with a 'New' button at the top left. The table has columns for 'platform name', 'server', 'description', 'host name', 'virtual name', 'network name', and 'OS'. There are two rows of data. The first row has 'test160' as platform name, 'hn160' as server, 'Hypernova Virtualization platform' as description, 'VM1' as host name, 'VM1' as virtual name, '10.10.10.10' as network name, and 'windows' as OS. The second row has 'test160' as platform name, 'hn160' as server, 'Hypernova Virtualization platform' as description, 'VM2' as host name, 'VM2' as virtual name, '10.10.10.10' as network name, and 'linux' as OS. There is an 'Edit' link next to the first row.

	platform name	server	description	host name	virtual name	network name	OS
Edit	test160	hn160	Hypernova Virtualization platform	VM1	VM1	10.10.10.10	windows
				VM2	VM2	10.10.10.10	linux

Figure 3-18. HyperNova Add-on components

3.3.3.2 Bull System Manager Configuration

To configure the monitoring elements for the HyperNova Add-on, you have to define an HyperNova Virtualization Platform from the Bull System Manager Configuration GUI. Native OS, VMs and related monitoring services are defined in one easy step.

The native OS is represented by a BSM host with the OS: **Xen**.

VMs are represented by a BSM host with the model: **HyperNova**.

3.3.3.2.1 HyperNova Virtualization Platform

To configure a HyperNova Virtualization Platform, click the **HyperNova** link in the Virtualization part of the Topology domain. The list of all configured platforms appears, as in the following example:

	platform name	server	description	host name	virtual name	network name	OS
Edit	test160	hn160	Hypernova Virtualization platform	VM1	VM1	10.10.10.10	windows
				VM2	VM2	10.10.10.10	linux

Figure 3-19. HyperNova Virtualization Platforms page

It is possible:

- To create a new HyperNova Virtualization Platform using the **New** button
- To edit or delete a resource using the **Edit** link
- To edit a virtual host using the **<hostname>** link.

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

Properties	
name	<input type="text"/>
description	Hypernova Virtualization platform
Virtualization Server	
name	<input type="text"/> <input type="button" value="Select"/>
model	other <input type="button" value="v"/>
network name	<input type="text"/>
HTTP Configuration	
SSL mode	<input type="radio"/> Yes <input checked="" type="radio"/> No
http port	<input type="text" value="80"/>
Virtual Machines	
<input type="button" value="Discover"/>	To get the list of hosted virtual machines, click the Discover button

Figure 3-20. HyperNova Platform Properties

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

- **Virtualization Server:** used to define the physical machine and the native OS.
- **HTTP Configuration:** used to set the HTTP mode access.
- **Virtual Machines:** used to describe the HyperNova platform virtual machine.

Virtualization Server Properties

- name** Server 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** Server network name (hostname or IP address).

HTTP Configuration

- SSL mode** To enable or disable SSL mode for HTTP
Default value: no

Note:

SSL option is not available on Windows platform. If the HNM Master access is securized, contact the HNM Master administrator to authorized non secure access for the Bull System Manager server.

Virtual Machines Properties

- Virtual Machines** List of the VMs established by selecting the VMs obtained by XML/HTTP requests to HN Master.
The request is performed by clicking the **Discover** button (or **Re-discover** if in edition mode).
See below the complete description of the procedure.

Virtual Machines Discovery

The result of the discovery is 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 virtualization 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 an already defined host by clicking the **Select** button or you can create a host by completing the corresponding fields.

<input checked="" type="checkbox"/>	HyperNova Virtual Machines		NS Master Configuration			
	Name	Type	Name		netName	OS
<input checked="" type="checkbox"/>	Rhel5Para	Para	Rhel5Para	Select	Rhel5Para	other ▾
<input checked="" type="checkbox"/>	Rhel5VT	Full	Rhel5VT	Select	Rhel5VT	other ▾
<input checked="" type="checkbox"/>	win2003	Full	win2003	Select	win2003	other ▾
<input checked="" type="checkbox"/>	Win2003s	Full	Win2003s	Select	Win2003s	other ▾

To update the list of virtual machines, click the Re-discover button

Figure 3-21. Virtual Machines display after Discover step

- Notes**
- When you select an already defined host, you cannot change its network name and OS. But **Select** contains a Default Option that corresponds to the VM name, which can be edited.
 - If the VM name contains space(s), they are replaced by underscore(s) in the host label.

Virtual Machines Re-Discovery

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

- Add virtual machine not yet registered in the HyperNova Virtualization Platform
- Remove virtual machine no more defined in the HyperNova configuration.

During the Re-discovery step, if the current configuration is not compatible with HyperNova configuration the invalid VMs are displayed in red and the VMs not referenced in the current BSM configuration are displayed in green, as shown in the following figure:

<input type="checkbox"/>	HyperNova Virtual Machines		NS Master Configuration			
	Name	Type	Name		netName	OS
<input checked="" type="checkbox"/>	testHNXXA02	Para	testHNXXA02	Select	10.10.10.10	other
<input checked="" type="checkbox"/>	testHNXXA04	Full	testHNXXA04	Select	10.10.10.10	other
<input checked="" type="checkbox"/>	testHNXXA05	Full	testHNXXA05	Select	10.10.10.10	other
<input type="checkbox"/>	testVMrm	Full	testVMrm	Select	10.10.10.10	other
<input checked="" type="checkbox"/>	VM1	Para	VM1	Select	172.31.35.170	other
<input checked="" type="checkbox"/>	VM2	Para	VM2	Select	172.31.35.171	other
<input checked="" type="checkbox"/>	VM3	Para	VM3	Select	172.31.35.172	other
<input checked="" type="checkbox"/>	VM4	Para	VM4	Select	172.31.35.173	other
<input checked="" type="checkbox"/>	VMA	Para	VMA	Select	172.31.35.174	other
<input type="checkbox"/>	shared_para_RHEL5	Para	shared_para_RHEL5	Select	10.10.10.10	other
<input type="checkbox"/>	testHNXX03	Full	testHNXX03	Select	10.10.10.10	other
<input type="checkbox"/>	testVMfullvide	Full	testVMfullvide	Select	10.10.10.10	other
<input type="checkbox"/>	testVMparasansOS	Para	testVMparasansOS	Select	10.10.10.10	other
<input type="checkbox"/>	VMA_BIS	Para	VMA_BIS	Select	VMA_BIS	other
<input type="checkbox"/>	VMA_CR17	Para	VMA_CR17	Select	VMA_CR17	other

Figure 3-22. Virtual Machines display after Re-iscover step

VMs no longer defined in HNmaster are automatically unchecked and will be removed from the platform on form validation. New VMs must be explicitly checked for being added in the platform to be linked to the platform on form validation.

- Note** How to Add, Delete or Modify Virtual Machine is detailed in 3.3.3.2.2 *Virtual Machine Edition*, on page 57.

After edition:

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

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

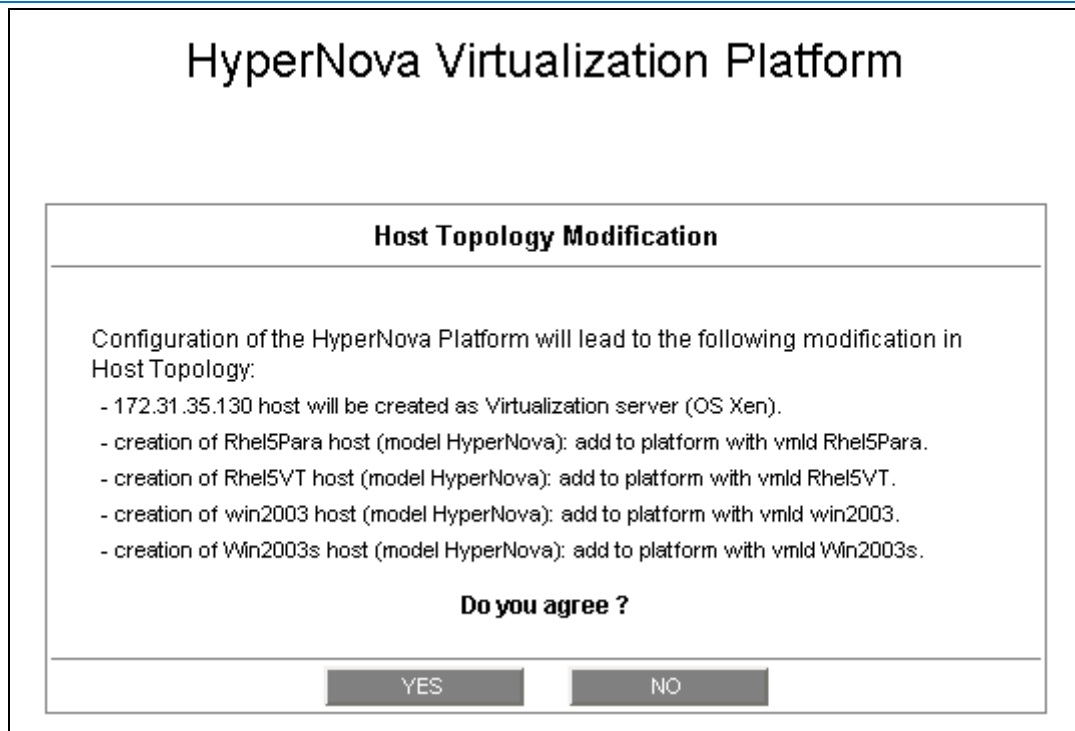


Figure 3-23. Host Topology modification confirmation

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

Related HyperNova Virtualization platform Objects

When a HyperNova Virtualization platform is defined, related objects are automatically generated to configure the specific Supervision linked to this type of NovaScale server. The following table describes the objects generated during the creation the platform.

Type	Description
host HyperNova	As defined in the Virtual Machine configuration part of the edition page.
host HNMmaster	Host corresponding to the virtualization layer and hosting the HNMmaster application, as defined in the Virtualization Server configuration part.
hostgroup	hostgroup representing the physical platform, named <platformName>.
manager	Virtualization manager representing the management interface, named <platformName>_HNMmaster

Type	Description
categories and services	The HyperNova category and related services are instantiated for the HNMaster host. The VirtualMachine category and related services are instantiated for each HyperNova host.

Note A hostgroup representing the virtual platform, a virtualization manager and instances of services for the virtualization server (**HyperNova** category) and for the hosts representing the virtual machine (**VirtualMachine** category) are also created.

3.3.3.2.2 Virtual Machine Edition

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

Adding, removing or modifying properties linked to the platform must be done from the HyperNova Virtualization platform edition page.

Modification of host properties must be done from the Host edition page.

Add a virtual machine to a platform

Adding a virtual machine is performed by checking the corresponding line in Virtual Machines part of the platform edition form and setting the host characteristics in 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 as part of the Bull System Manager platform are displayed. To add virtual machine, you must perform a Re-discovery to get the list of all machines defined on the Virtualization Server.

Remove a virtual machine from a platform

Removing a virtual machine is performed by unchecking the corresponding line in the Virtual Machines part of 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 **Delete**.

Modify 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 choose it in the list of already defined hosts in Bull System Manager by clicking the Select button.

To modify other characteristics as netName or OS, 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.

Delete all virtual machines and corresponding hosts.

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

3.3.3.2.3 Virtualization Supervision

As specified above, services are instantiated for each 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 **HyperNova** category.

Services Applied to the Native OS

Service	Description	Check_command
Status	Checks global status	check_hn_server_status
HTTP	Check availability of supervision page	check_http

Monitoring services defined for VM hosts are associated with the **VirtualMachine** category.

Services Applied to the VM Host

Service	Description	Check_command
Status	Checks VM status	check_hn_vm_status

Monitoring services related to Virtual Platform elements are automatically created during the edition of the HyperNova Virtualization Platform. These services can be displayed and edited from the Services page in the Supervision domain, but only the attributes related to monitoring or notification can be edited.

Properties	
category	VirtualMachine
name	Status
description	checks the virtual machine status (automatically generated)
model	HyperNova
OS family	any
host list expression	VM1
Monitoring attributes	
status	<input checked="" type="radio"/> active <input type="radio"/> inactive
Monitoring command attributes (for this service)	
check command	check_hn_vm_status
check command parameters	172.31.35.160/VM1/0180
monitoring period	24x7
polling interval	5 mn (5 mn by default if empty)
Notification attributes (for this service)	
e-mail contact groups	<div style="display: flex; justify-content: space-between;"> <div style="width: 45%;"> <p>Selected Objects</p> <ul style="list-style-type: none"> mgt-admins </div> <div style="width: 10%; text-align: center;"> <p><= Add</p> <p>Remove =></p> </div> <div style="width: 45%;"> <p>All Objects</p> <ul style="list-style-type: none"> mgt-admins </div> </div>
enable Bull autocall	<input type="radio"/> Yes <input checked="" type="radio"/> No
enable SNMP trap	<input checked="" type="radio"/> Yes <input type="radio"/> No
notification period	24x7
re-notification interval	0 mn (0 mn by default if empty)
notify if warning	<input checked="" type="radio"/> Yes <input type="radio"/> No
notify if critical	<input checked="" type="radio"/> Yes <input type="radio"/> No
notify if recovery	<input checked="" type="radio"/> Yes <input type="radio"/> No

Figure 3-24. Virtual Machine Properties pane

-
- Notes**
- Status is determined by requesting the **HNMaster** application. To avoid overload, the result of the request is stored in a cache on the BSM server. The cache is refreshed each time the **GlobalStatus** service is checked or if the cache is not up-to-date (last update more than 10 minutes).
 - During **HyperNova** Platform definition, all services are defined and activated for the server and for each VM. To deactivate the monitoring of one service, set **status** (Monitoring attributes part) to inactive.
-

3.3.3.2.4 Domain0 Supervision

The monitoring functions to control the resources of the **domain0** are not automatically setup at the platform definition. To enable them, you have to activate the corresponding categories and services.

HyperNova Add-on delivers the following monitoring definitions:

Category	Service
Dom0SystemLoad	CPU(*)
	Memory(*)
	Processes(*)
	Users
	Swap(*)
	Zombies
Dom0FileSystems	All(*)
	/usr
Dom0LinuxServices	syslogd(*)
Dom0Syslog	AuthentFailures
	RootAccess(*)

(*) indicates services that are automatically activated when the corresponding category is instantiated.

Examples

To activate the de **Dom0SystemLoad** related services, do as follows:

1. Click the Categories/Services link in the Supervision tab.
2. Apply a filter (by HOST(s) or by OS) to select only the hosts corresponding to **domain0** of an HyperNova system, as in the following example:

The screenshot shows a web interface for host management. At the top, there's a 'Host List' section with a dropdown menu containing 'staix35 (nativVIDS - EL Blade)', 'tyrex (other - Escala LPAR)', and 'hn160 (nativXen - other)'. The 'hn160' option is selected. To the right, a 'Selected Hosts' box contains 'hn160'. Below this, there are buttons for 'Reset' and 'Apply'. On the left, there are filter options: 'No Filter', 'Filter by OS', 'Filter by MODEL', and 'Filter by HOST(S)'. Below the host list, there are links for 'Expand all', 'Collapse all', and 'manage categories'. A section titled 'Categories and Services found for host(s) : hn160' contains a table with the following data:

Name & Description	OS	Model	HostList	Actions
HyperNova	Xen	any	hn160	edit

Figure 3-25. Categories filter for domain0 Host

- Click the **manage categories** link and choose the **Add from an unused category template (user or predefined)** option to display the categories available for the corresponding hosts.

Manage Categories

for hosts : 172.31.50.55

Create a new category

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

check	Name	Description	Os	Model	hostList
<input type="radio"/>	Cluster	cluster	any	any	*
<input type="radio"/>	Dom0FileSystems	FileSystem services	natifXen	any	none
<input type="radio"/>	Dom0LinuxServices	Linux processes status	natifXen	any	none
<input type="radio"/>	Dom0Syslog	Linux Syslog events	natifXen	any	none
<input checked="" type="radio"/>	Dom0SystemLoad	Load monitoring of this System	natifXen	any	none
<input type="radio"/>	Internet	Internet services	any	any	none
<input type="radio"/>	MegaRAID	MegaRAID monitoring	any	any	none
<input type="radio"/>	reporting	Indicators collected by MRTG	any	any	none

Figure 3-26. Available categories for domain0 Host

- Select the **Dom0SystemLoad** category and click **Add from the selected category**.
- The edition form for the corresponding category is displayed with all fields filled in. Click **OK**.
- The Categories and Services page now displays **Dom0SystemLoad** category in the list of used categories for the selected hosts. Expand the category to display the list of the used services.

[Expand all](#)
 [manage categories](#)

[Collapse all](#)

Categories and Services found for host(s) : 172.31.50.55

	Name & Description	OS	Model	HostList	Actions
[-]	<input checked="" type="checkbox"/> Dom0SystemLoad	Xen	any	172.31.50.55	edit manage services
	<input checked="" type="checkbox"/> CPU	Xen	any	*	edit
	<input checked="" type="checkbox"/> Memory	Xen	any	*	edit
	<input checked="" type="checkbox"/> Processes	Xen	any	*	edit
	<input checked="" type="checkbox"/> Swap	Xen	any	*	edit
[+]	<input checked="" type="checkbox"/> HyperNova	Xen	any	172.31.50.55	edit

Figure 3-27. Used services for domain0 Host

Note The Zombies and Users services are not present. To activate them, you have to associate them explicitly to the hosts (see below).

To activate the Users service, do as follows:

1. Click the **manage services** link of the **Dom0SystemLoad** category and choose the option **Add from a service template (user or predefined)** to display the available services.

Manage Services

for category : Dom0SystemLoad[natifXen,any]


Create a new service

Add from a service template (user or predefined template)

check	Name	Category	Description	Os	Model	hostList
<input type="radio"/>	Ausr	Dom0FileSystems	monitors the percent of free space for the filesystem /usr	natifXen	any	none
<input type="radio"/>	Alerts	MegaRAID	checks the alerts received from the MegaRAID SNMP agent	any	any	*
<input type="radio"/>	All	Dom0FileSystems	monitors the percent of used space for all the mounted filesystems	natifXen	any	*
<input type="radio"/>	AuthentFailures	Dom0Syslog	monitors the authentication failures messages in the messages log	natifXen	any	none
<input type="radio"/>	CPU	Dom0SystemLoad	monitors the CPU load average over three periods of time (1mn, 5mn and 15 mn)	natifXen	any	*
<input type="radio"/>	FTP	Internet	FTP service	any	any	none
<input type="radio"/>	HTTP	Internet	HTTP service	any	any	*
<input type="radio"/>	HTTP_NSMaster	Internet	checks the NSMaster URL	any	any	none
<input type="radio"/>	Memory	Dom0SystemLoad	monitors the percent of used memory (physical and swap) for the domain0	natifXen	any	*
<input type="radio"/>	Processes	Dom0SystemLoad	monitors the number of processes running on the domain0	natifXen	any	*
<input type="radio"/>	RootAccess	Dom0Syslog	monitors the session opened for user root messages in the messages log	natifXen	any	*
<input type="radio"/>	Status	MegaRAID	checks the RAID status	any	any	*
<input type="radio"/>	Swap	Dom0SystemLoad	monitors the percent of swap used by the domain0	natifXen	any	*
<input type="radio"/>	TCP_7	Internet	checks the echo TCP port	any	any	none
<input type="radio"/>	UDP_7	Internet	checks the echo UDP port	any	any	none
<input checked="" type="radio"/>	Users	Dom0SystemLoad	monitors the number of users currently logged in	natifXen	any	none
<input type="radio"/>	Zombies	Dom0SystemLoad	monitors the number of zombie processes running on the domain0	natifXen	any	none
<input type="radio"/>	perf_indic	reporting	monitors one indicator collected by MRTG	any	any	none
<input type="radio"/>	syslogd	Dom0LinuxServices	monitors the presence of a syslogd process running on the system	natifXen	any	*

Figure 3-28. Available services for Dom0SystemLoad category

2. Select the Users service and click **Add from the selected services**. The edition form for the corresponding service is displayed with all fields filled in. Click **OK**.
3. The Categories and Services page now displays the **Users** service in the list of the used **Dom0SystemLoad** services.

Expand all  [manage categories](#)
 Collapse all

Categories and Services found for host(s) : 172.31.50.55


	Name & Description	OS	Model	HostList	Actions
<input type="checkbox"/>	✓ Dom0SystemLoad	Xen	any	172.31.50.55	edit manage services
	✓ Users	Xen	any	172.31.50.55	edit
	✓ CPU	Xen	any	*	edit
	✓ Memory	Xen	any	*	edit
	✓ Processes	Xen	any	*	edit
	✓ Swap	Xen	any	*	edit
<input type="checkbox"/>	 HyperNova	Xen	any	172.31.50.55	edit

Figure 3-29. Users service for domain0 Host

To get detailed information about the Categories and Services configuration, refer to the *Bull System Manager Administrator's Guide*.

3.3.3.3 Nagios Check Commands

[check_hn_server_status](#)

The configurable Bull System Manager service check command syntax is:

```
check_hn_server_status
```

See the **check_NSM_hypervnova_xen** command in Appendix A for parameters details.

[check_hn_vm_status](#)

The configurable Bull System Manager service check command syntax is:

```
check_hn_vm_status!<hypervnova_server>!<vmname>
```

See the **check_NSM_hypervnova_xen** command in Appendix A for parameters details.

[domain0 supervision related commands](#)

The commands used for **domain0** supervision services are those used for Linux supervision. To get detailed information about them, refer to the *Bull System Manager Administrator's Guide*.

The following table lists the commands used by the services.

Category.Service	Command
Dom0SystemLoad.CPU	check_cpuload
Dom0SystemLoad.Memory	check_memory
Dom0SystemLoad.Processes	check_procs
Dom0SystemLoad.Users	check_procs
Dom0SystemLoad.Zombies	
Dom0SystemLoad.Swap	check_swap
Dom0FileSystems.All	check_disks.pl
Dom0FileSystems./usr	
Dom0LinuxServices.syslogd	check_procs
Dom0Syslog.AuthentFailures	check_log2.pl
Dom0Syslog.RootAccess	

3.3.3.4 Bull System Manager Console

Operation

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

Operation → **Application** → **HN Master**

3.3.3.5 HyperNova Monitoring

From the platform or host elements, you can access monitoring information.

From the hosts element, you can display information related to associated services 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:

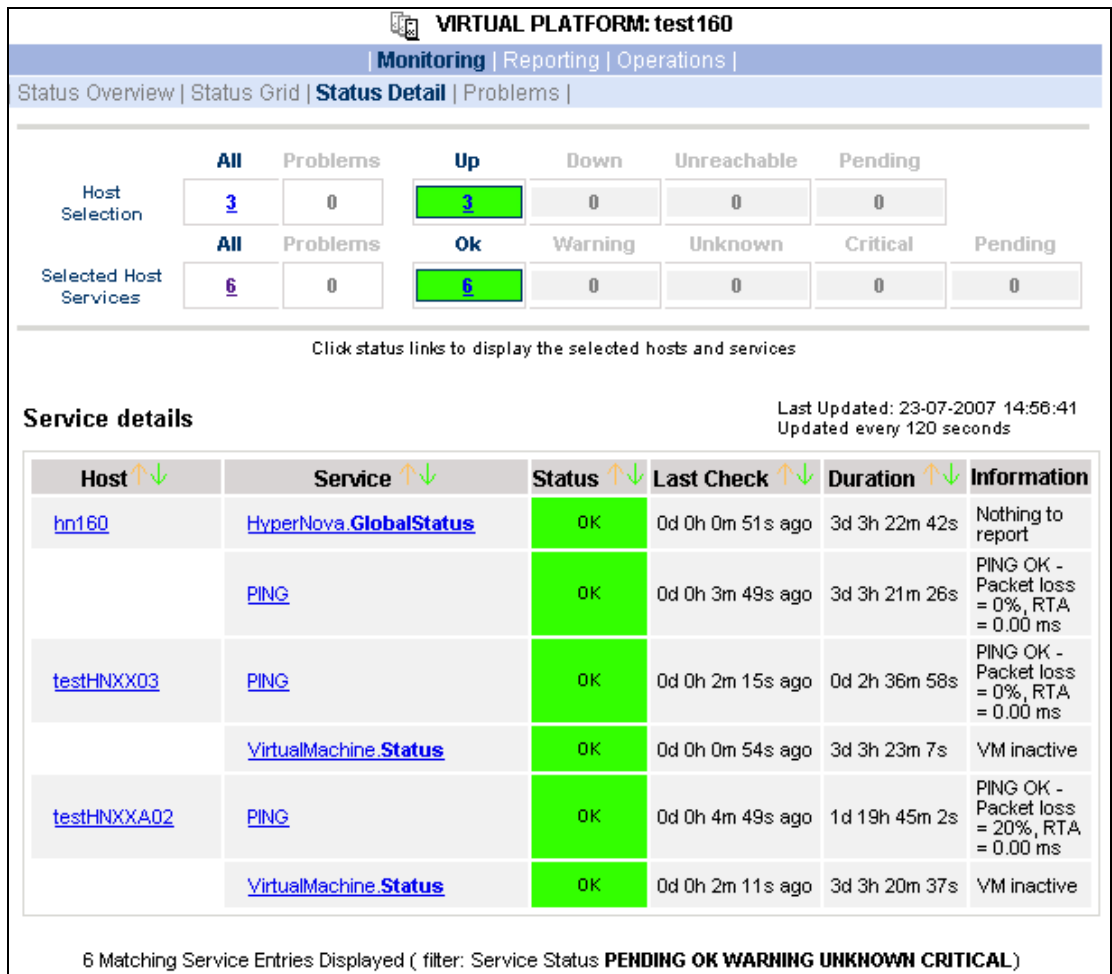


Figure 3-30. Virtual Platform monitoring

3.3.4 BSMEscalaLPAR "EscalaLPAR" Management

3.3.4.1 Overview

Dynamic logical partitioning (LPAR) is a system architecture delivered on Escala systems that allows the division of 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 Escala Privilege Line 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 to other partitions.

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



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 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 system managed with HMC:

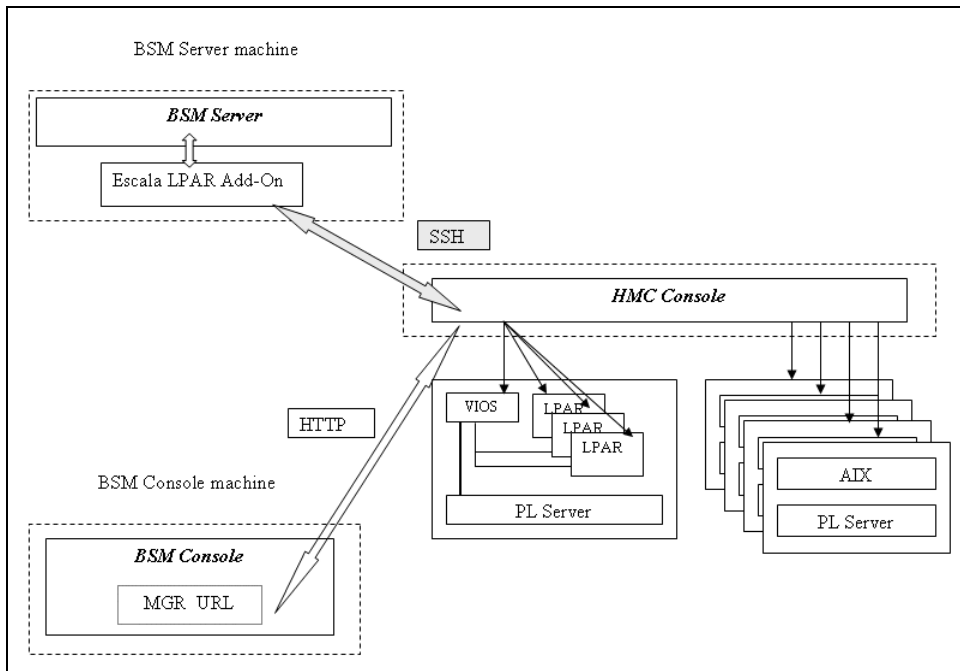


Figure 3-31. EscalalPAR Add-on components for HMC managed systems

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

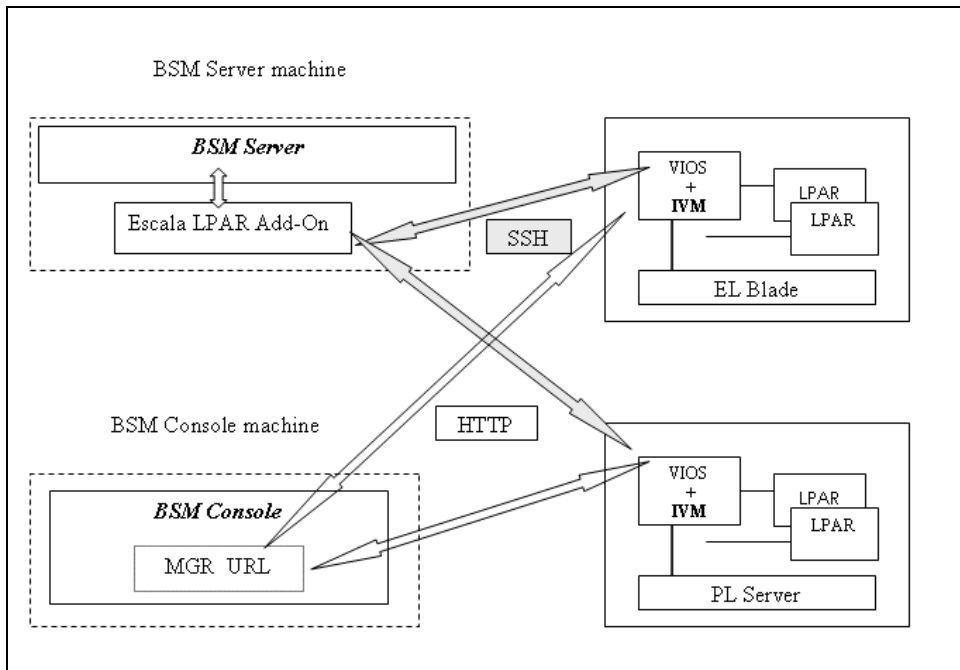


Figure 3-32. EscalalPAR Add-on components for IVM managed systems

3.3.4.2 Bull System Manager Configuration

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).

HMC managed Escala Server

The initialization of an HMC managed system is done through the **PL 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 **EL Blade** or **PL Server** links under the 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*.

3.3.4.2.1 Virtualization Supervision

Services and associated performance indicators are instantiated for 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 server managed by IVM

Monitoring services defined for the server managed by IVM (hosting the VIOS partition) are associated with the **VIOS** category.

Service	Description	Check_command
Status	Checks the status of the Virtual I/O server	check_vios_status
UsedPool	Checks the utilization of the processing pool on server	check_vios_pool

Monitoring Services applied to the server managed by HMC

Monitoring services defined for the PL server managed by an HMC are associated with the **PowerHypervisor** category.

Service	Description	Check_command
UsedPool	Checks the utilization of the processing pool on the server	ceck_cec_used_pool

Monitoring Services Applied to the LPAR Host

Monitoring services defined for LPAR hosts are associated with the **VirtualMachine** category.

Service	Description	Check_command
Status	Checks LPAR status	check_lpar_status
UsedCPU	Checks the utilization of the entitled CPU by the partition	check_lpar_used_cpu

Monitoring services related to Escala Platform elements are automatically created during the edition of the Platform. Theses services can be displayed and edited from the **Services** page in the Supervision domain, but only the attributes related to monitoring or notification can be edited.

Properties	
category	VIOS
name	UsedPool
description	checks the utilization of the processing pool on Virtual I/O Server (a
model	any
OS family	VIOS
host list expression	staix35
Monitoring attributes	
status	<input checked="" type="radio"/> active <input type="radio"/> inactive
Monitoring command attributes (for this service)	
check command	check_vios_used_pool
check command parameters	padminlid_dsa.nsm!120!70%!80%!
monitoring period	24x7
polling interval	5 mn (5 mn by default if empty)
Notification attributes (for this service)	
e-mail contact groups	<div style="display: flex; justify-content: space-between;"> <div> <p>Selected Objects</p> <ul style="list-style-type: none"> mgt-admins </div> <div style="text-align: center;"> <p><= Add</p> <p>Remove =></p> </div> <div> <p>All Objects</p> <ul style="list-style-type: none"> mgt-admins </div> </div>
enable Bull autocall	<input type="radio"/> Yes <input checked="" type="radio"/> No
enable SNMP trap	<input checked="" type="radio"/> Yes <input type="radio"/> No
notification period	24x7
re-notification interval	0 mn (0 mn by default if empty)
notify if warning	<input checked="" type="radio"/> Yes <input type="radio"/> No
notify if critical	<input checked="" type="radio"/> Yes <input type="radio"/> No
notify if recovery	<input checked="" type="radio"/> Yes <input type="radio"/> No

Figure 3-33. VIOS.UsedPool Service Properties pane

Note During Platform definition, all services are defined and activated for the server and for each LPAR. To deactivate the monitoring of one service, edit it and set its **status** (Monitoring attributes part) to **inactive**.

Reporting indicators

A performance indicator is defined for the Escala server to describe the utilization of the processing pool. This indicator is identified as **<escaleServer>_UsedPool**.

A reporting indicator is defined for each LPAR to describe the utilization of the entitled CPU of a given LPAR. This indicator is identified as **<lpár_host>_UsedCPU**.

Indicators

Indicators

New

	host	name	collect mode	source	status
Edit	galilei	galilei_UsedCPU	NSM_monitoring	VirtualMachine.UsedCPU	active
Edit	lpar1	lpar1_UsedCPU	NSM_monitoring	VirtualMachine.UsedCPU (any)	active
Edit	lpar2	lpar2_UsedCPU	NSM_monitoring	VirtualMachine.UsedCPU (any)	active
Edit	plmiz1	plmiz1_UsedPool	NSM_monitoring	PowerHypervisor.UsedPool (none)	active
Edit	staix35	staix35_UsedPool	NSM_monitoring	VIOS.UsedPool	active

Figure 3-34. Reporting indicators

Note The collection of all these indicators is activated during the Platform definition. To deactivate some of them, edit the indicator and set its **status** to **inactive**.

3.3.4.3 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_escalalpar** command in Appendix A for parameters details.

[check_vios_used_pool](#)

The configurable BSM service check command syntax is:

```
check_vios_used_pool!<ssh_user>!<identity_file>!<sample_time>!<warning_threshold>!<critical_threshold>
```

See the **check_NSM_escalalpar** command in Appendix A for parameters 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_escalalpar** command in Appendix A for parameters details.

[check_lpar_status](#)

The configurable BSM service check command syntax is:

```
check_lpar_status!<mgr_type>!<mgr_netName>!<ssh_user>!<identity_file>!<system_name>!<lpar_name>
```

See the **check_NSM_escalalpar** command in Appendix A for parameters 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 in Appendix A for parameters details.

3.3.4.4 Bull System Manager Console

3.3.4.4.1 Operation

From the Virtual Manager or from any element of the Escala Platform, do as follows:

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

Operation → Virtualization → HMC

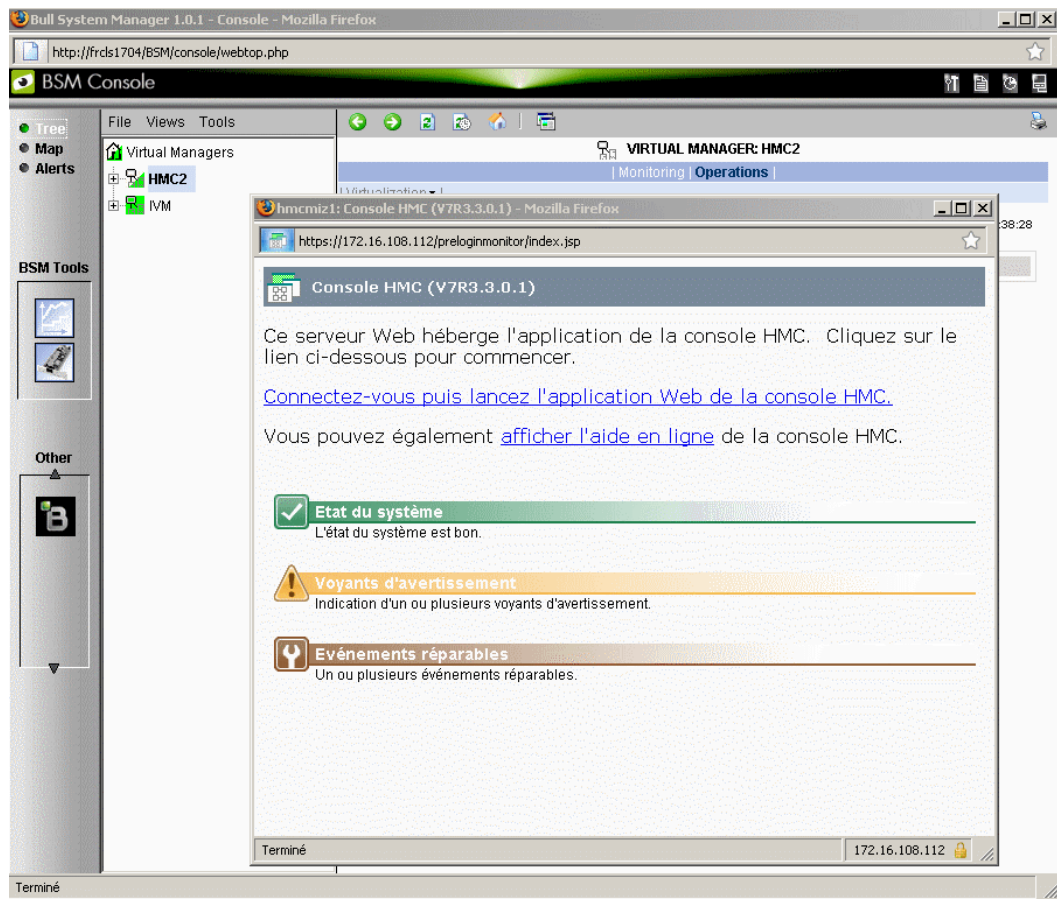


Figure 3-35. HMC activation from Bull System Manager Console

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

Operation → Virtualization → IVM

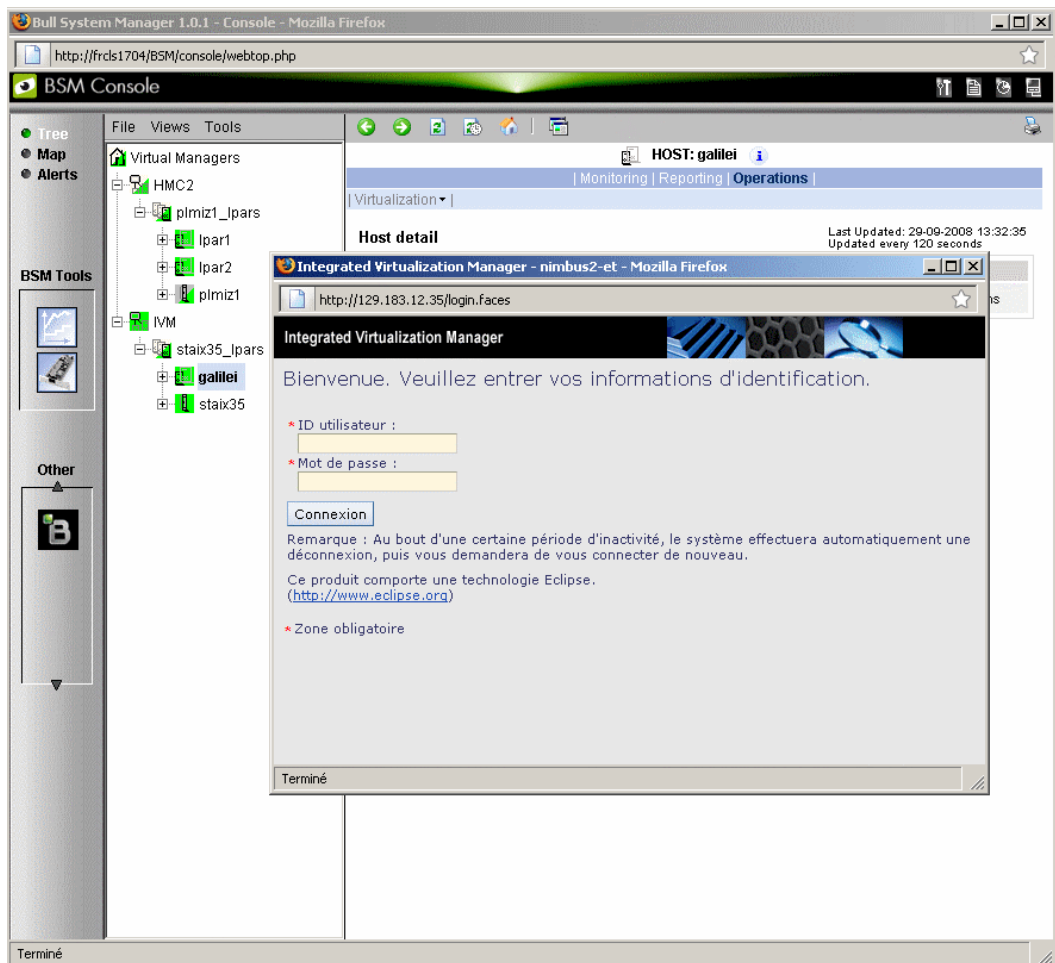


Figure 3-36. IVM activation from Bull System Manager Console

3.3.4.4.2 Escala Supervision

To see all services related to an HMC managed Escala server, use the **Virtual Managers** view, click the platform node and select Monitoring/Status detail menu. The following page is displayed:

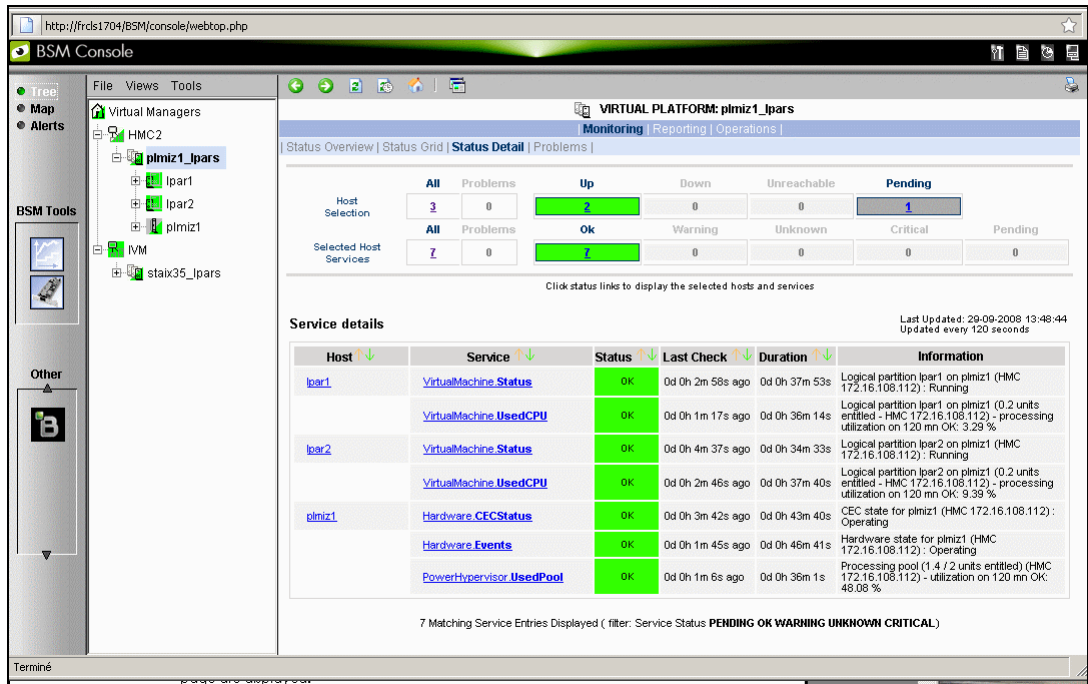


Figure 3-37. Escala HMC reported Supervision

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

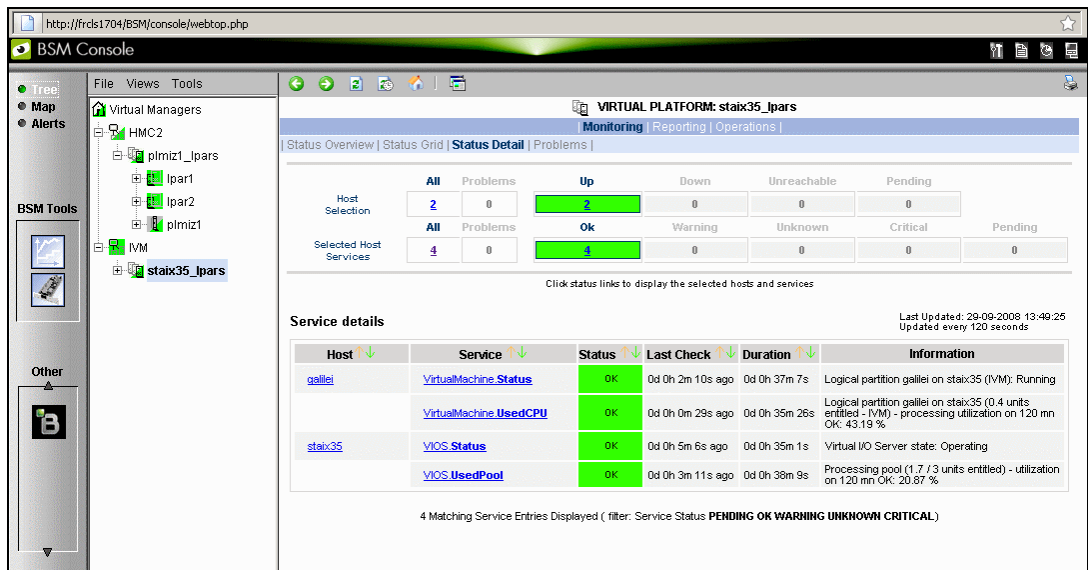


Figure 3-38. Escala IVM reported supervision

3.3.4.4.3 Escala Reporting

From the host hosting the Vios partition or from host representing the hardware of HMC managed PL Escala, you can display reporting indicators to get evolution of the processing pool utilization.

From any LPAR host, you can display reporting indicators to get evolution of the utilization of the CPU entitled to the partition.

3.4 Bull Products Server Add-ons

3.4.1 BSMDD4A for Bull “Dynamic Domains For Applications” Management

The **Dynamic Domains For Applications** (DDFA) software is a tool that can be used on the Linux operating system for simulating the partitioning of a multi-CPU machine at application level. Dynamic Domains for Applications can be used with standard Linux distributions and can be managed using the Webmin standard administration tool. See the *Dynamic Domains for Applications User’s Guide* (ref 86 A2 63ER) for more information. You can install DDFA from the *Bull Extension Pack for RedHat CD*.

Note DDFA runs only on Linux machines and uses a Webmin module for its management. You can download the prerequisite Webmin package from the web site: <http://www.webmin.com>

This Add-on creates monitoring links between Bull System Manager and the **DDFA** management webmin module.

The following figure shows the different components used for monitoring:

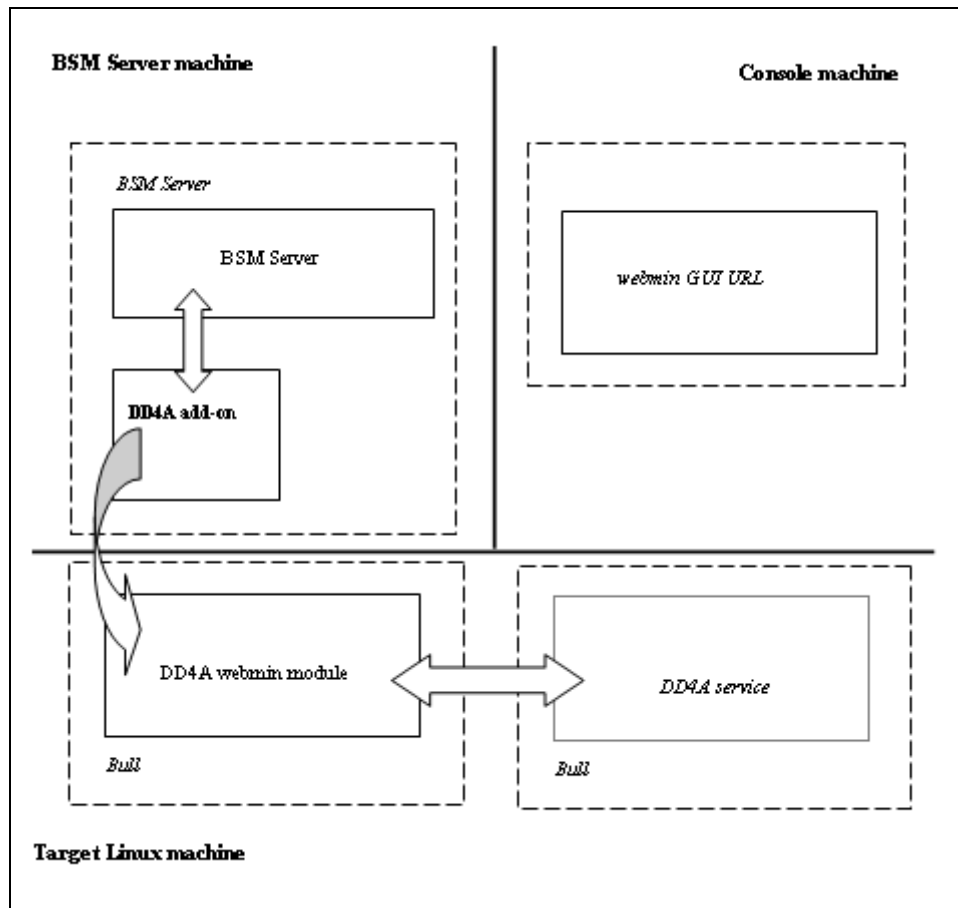


Figure 3-39. DDFA Monitoring Components

Bull System Manager Server Add-ons provides the default Bull product categories by Management Package described below.

3.4.1.1 Default Categories & Services Proposed for Linux Hosts

Targeted OS	Model	Category	Service	Check command
Linux	Any	DynamicDomains	All	check_dd4a
			Default	

Table 3-8. DDF4 categories and services

3.4.1.2 DynamicDomains Category

All Service

For NovaScale and Express5800 Linux hosts with the Dynamic Domains management tool. This service dynamically checks global status reported by the associated webmin module for all defined Dynamic Domains.

Note There is no need to reconfigure the tool to survey new defined Dynamic Domains.

default Service

For NovaScale and Express5800 Linux hosts with the Dynamic Domains management tool. This service checks the status of the default Dynamic Domain.

Note When creating a new Dynamic Domain, statically clone the default monitoring service to survey the new dynamic domain.

3.4.1.3 check_DynamicDomains (Linux OS) Nagios Command

The configurable Bull System Manager service check command syntax is:

```
check_DynamicDomains!<{ALL|<DomainName>}
```

Default syntax for **DynamicDomains.All**:

```
check_DynamicDomains!ALL
```

Default syntax for **DynamicDomains.default**:

```
check_DynamicDomains!default
```

3.4.2 BSMBVS for Bull Video Services Management

Bull Video Services (BVS) software is a tool that can be used with standard Linux distributions and Windows and can be managed using Web server.

See the *Bull Video Services User's Guide* for more information.

You can install BVS from the Bull Video Services CD (ref 36673900-xxx).

Note BVS 4.1 runs on Linux and Windows machines and uses an integrated Web server for management.

This Add-on creates monitoring links between Bull System Manager and the **BVS** management Web server module.

The following figure shows the different monitoring components:

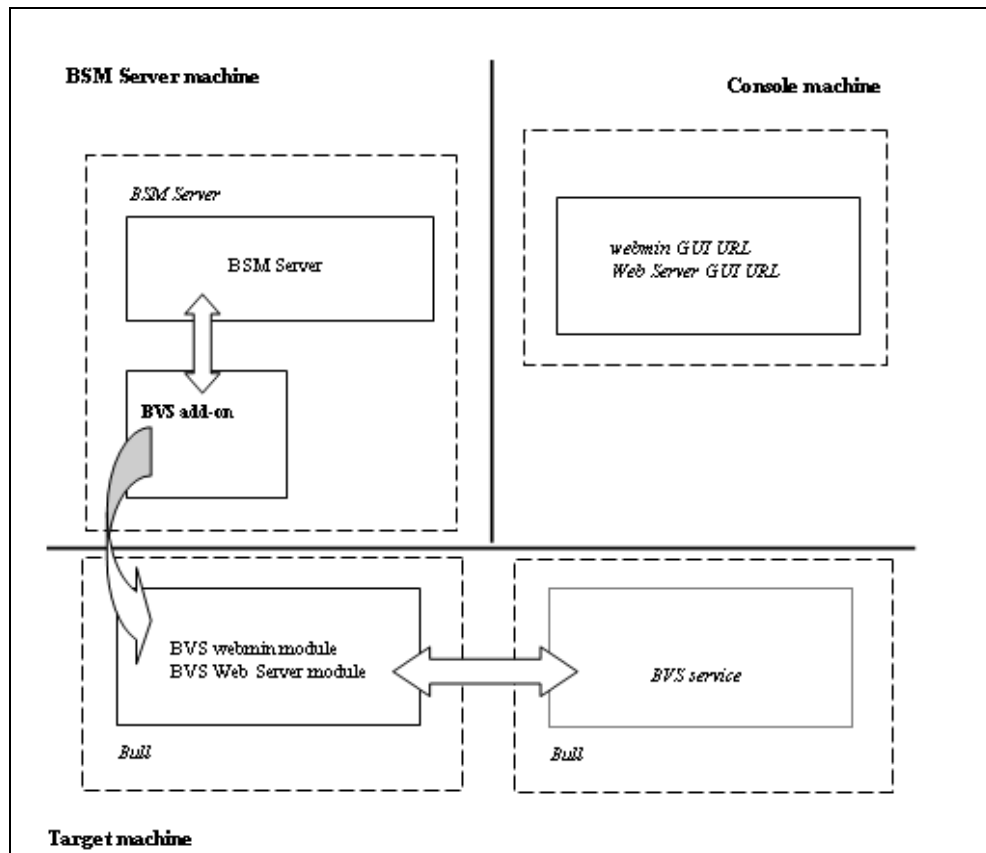


Figure 3-40. BVS Web Server Monitoring Components

Targeted OS	Model	Category	Services	Check command
linux Windows	any	BullVideoServices	Streaming Recording Datagrams	check_BullVideoServices

Table 3-9. Bull Video Services categories and services

3.4.2.1 BullVideoServices Category

- Streaming** For NovaScale hosts acting as Bull video server. This service checks the status of the video streaming service.
- Recording** For NovaScale hosts acting as Bull video server. This service checks the status of the video recording service.
- Datagrams** For NovaScale hosts acting as Bull video server. This service checks the status of the video datagram errors.

3.4.2.2 check_BVS Nagios Command

The configurable Bull System Manager service check command syntax is:

```
check_BVS!<serviceName>
```

See the **check_BVS** command, in Appendix A for parameters details.

For instance, Default syntax for **BullVideoService.Streaming** is:

```
check_BVS!Streaming
```

3.4.3 BSMJOnAS for JOnAS Management

3.4.3.1 JOnAS Overview

JOnAS is a pure Java, open source application server. Its high modularity allows it to be used as:

- A J2EE server, for deploying and running EAR applications (i.e. applications composed of both web and ejb components)
- An EJB container, for deploying and running EJB components (e.g. for applications without web interfaces or when using JSP/Servlet engines that are not integrated as a JOnAS container)
- A WEB container, for deploying and running JSPs and Servlets (e.g. for applications without EJB components).

The JOnAS architecture is illustrated in the following figure, showing WEB and EJB containers relying on JOnAS services.

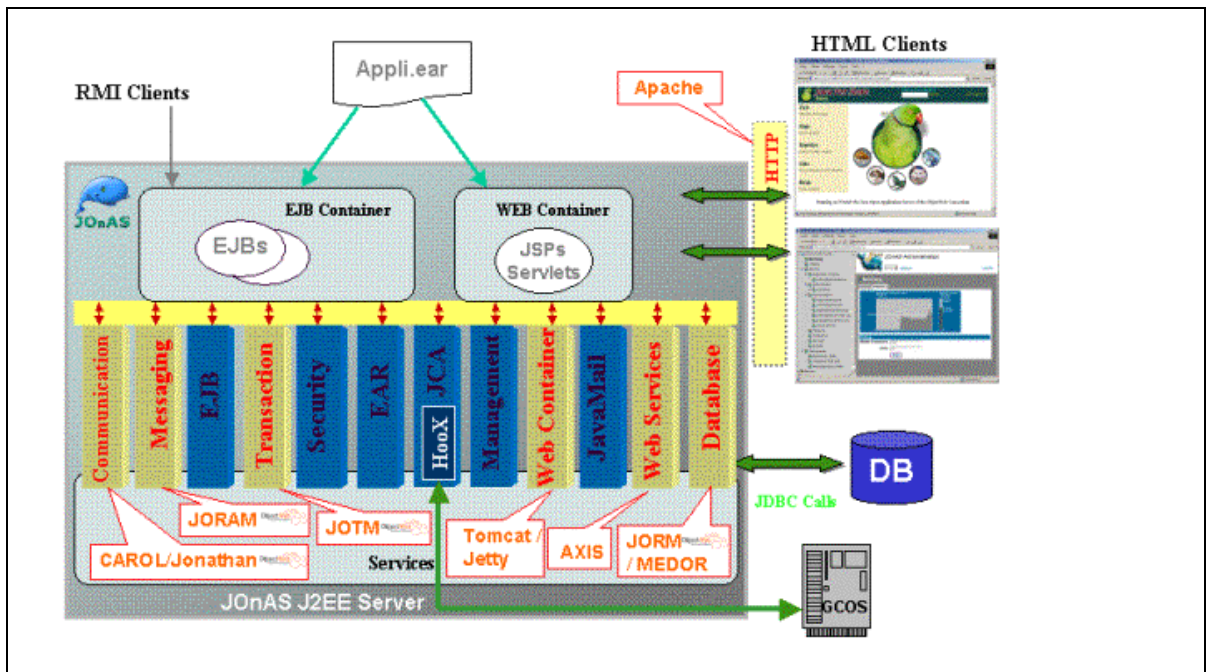


Figure 3-41. JOnAS Architecture

See <http://jonas.objectweb.org/doc/index.html> for more information.

3.4.3.2 JOnAS Domain Topology

A JOnAS management domain is composed of a set of JOnAS servers that are running under the same management authority. All the servers in the domain must have a distinct **server name** and a common **domain name**.

The servers in a domain can be administered by a management application running on a server playing the role of **administrator** or **master**. The managed servers play the role of **slaves**.

A default domain configuration is provided in `$JONAS_ROOT/conf/domain.xml`. This configuration corresponds to a domain named `jonas` managed by a server also named `jonas`.

JOnAS administrators are responsible for the configuration and administration of JOnAS servers running within a management domain.

3.4.3.3 JOnAS Monitoring Information

Bull System Manager retrieves domain and server monitoring information from JOnAS (administrator or master) server via the WEB services.

Note WEB services are operational only if the `conf/server.xml` file on JOnAS (administrator or master) server is correctly configured as follows:
The `localhost` value must be replaced by the **DNS host name**.

3.4.3.4 Bull System Manager Configuration

JOnAS configuration for Bull System Manager is available from the configuration GUI by selecting **Third-Party Application** → **JOnAS**.

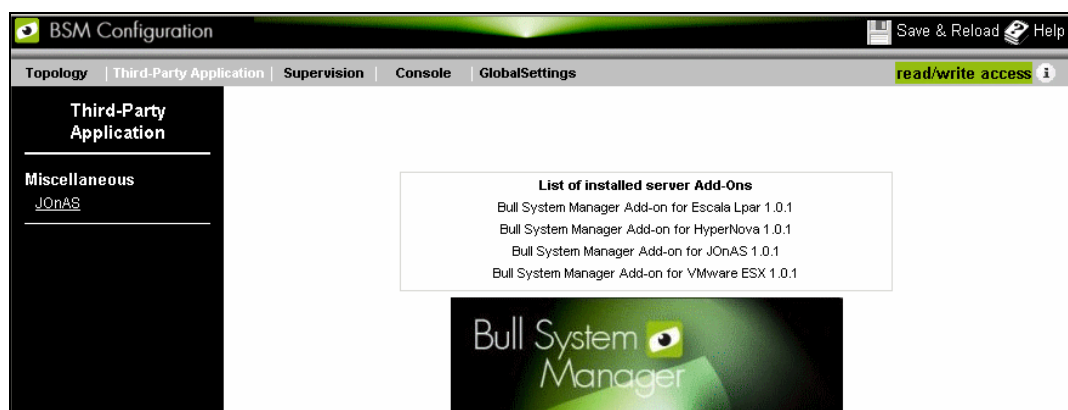


Figure 3-42. JOnAS configuration

JOnAS Domain Definition

To display the JOnAS domains already defined, click **Third-Party Application** → **JOnAS**.

New Domain					
	Domain name	Description	Host name	Admin server	Other servers
Edit	jonas	N/A	charly4L	jonas	none
Edit	jonas	N/A	frcls6260	instance1	instance2,instance3
Edit	jonas	N/A	nsmaster	jonas	none

Figure 3-43. JOnAS domains

To edit a domain, click **Edit**.

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

JOnAS Domain Attributes

[Help on JOnAS Domain attributes](#)

OK Cancel

Properties

domain name

description

Domain information access

host name

port number

Authentication

user name

password confirm

Domain monitored Servers

admin server name

master server Yes No

Figure 3-44. JOnAS properties

domain name name of JOnAS domain

description description of the domain

Domain information access

host name name of the host

port number port number

user name name of the user

password password

Domain monitored Servers

admin server name name of JOnAS administrator or master server

master server master server flag

If the master server flag is set to **Yes**, the **Get Servers** button is displayed:

master server	<input checked="" type="radio"/> Yes <input type="radio"/> No
other servers	<input type="button" value="Get servers"/> Click on "Get servers" to get the servers managed in the domain

Click the **Get Servers** button to list all the servers belonging to the specified domain:

Domain monitored Servers							
admin server name	instance1						
master server	<input checked="" type="radio"/> Yes <input type="radio"/> No						
other servers	<table border="0"> <tr> <td>Selected Servers</td> <td></td> <td>All Servers</td> </tr> <tr> <td>instance2 instance3</td> <td> <input type="button" value="=< Add"/> <input type="button" value="Remove =>"/> </td> <td>instance2 instance3</td> </tr> </table>	Selected Servers		All Servers	instance2 instance3	<input type="button" value="=< Add"/> <input type="button" value="Remove =>"/>	instance2 instance3
Selected Servers		All Servers					
instance2 instance3	<input type="button" value="=< Add"/> <input type="button" value="Remove =>"/>	instance2 instance3					

other servers the selected servers will be monitored by Bull System Manager.

3.4.3.5 JOnAS Category and Service

The definition of a domain creates or updates a **JOnAS** category and creates one service by JOnAS server identified by the JOnAS server name.







<input type="checkbox"/>	JOnAS : JOnAS monitoring (automatically generated)	 any	charly4L, nsmaster, frcls6260	<input type="checkbox"/>
			clone modify withdraw	All <input type="checkbox"/>
	instance2	 any	frcls6260	<input type="checkbox"/>
	instance3	 any	frcls6260	<input type="checkbox"/>
	instance1	 any	frcls6260	<input type="checkbox"/>
	jonas	 any	nsmaster	<input type="checkbox"/>
	jonas	 any	charly4L	<input type="checkbox"/>

Figure 3-45. JOnAS category and services

The `check_NSM_JOnAS` command defined for the service returns the state of the server (**RUNNING**, **STOPPED**, **FAILED**, **UNREACHABLE**). If the server is running, the following attributes are returned:

- Threads count
- Memory allocated and used
- HTTP requests count
- Committed transactions count

3.4.3.6 JOnAS Reporting Indicators

Threads and **MemoryUsed** indicators are created for each JOnAS service.

- The **Threads** indicator returns the current threads count.
- The **MemoryUsed** indicator returns the current memory used.

	host	name	collect mode	source	status
Edit	charly4L	JOnASjonas.MemoryUsed	NSM_monitoring	JOnAS.jonas	active
Edit	charly4L	JOnASjonas.Threads	NSM_monitoring	JOnAS.jonas	active

Figure 3-46. JOnAS indicators

3.4.3.7 Bull System Manager Console

JOnAS Monitoring Representation

The JOnAS category groups services monitoring for all the servers in the domain.

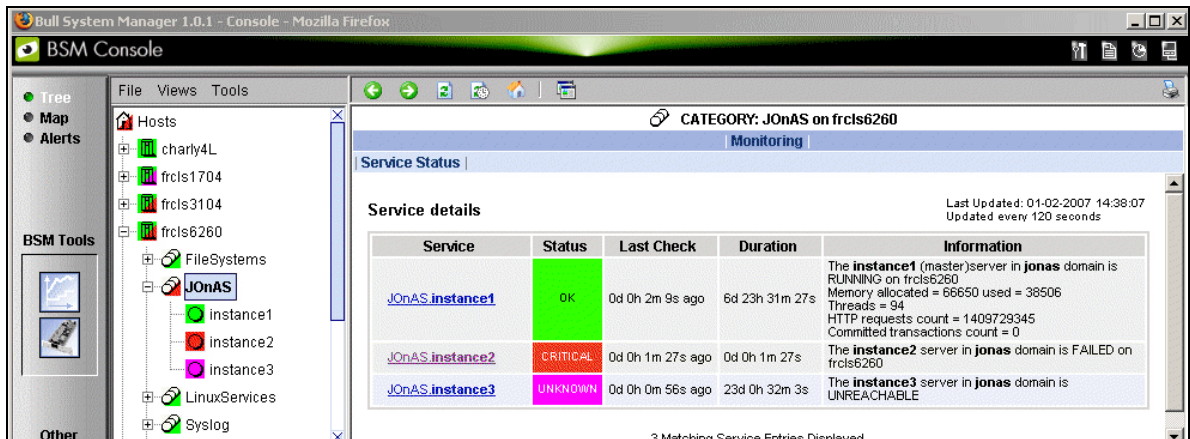


Figure 3-47. JOnAS category view

Launching the jonasAdmin Application

The JOnAS administration tool, **jonasAdmin**, can be contextually launched from a service node on the Bull System Manager console by clicking:

Operations → **Application** → **jonasAdmin**

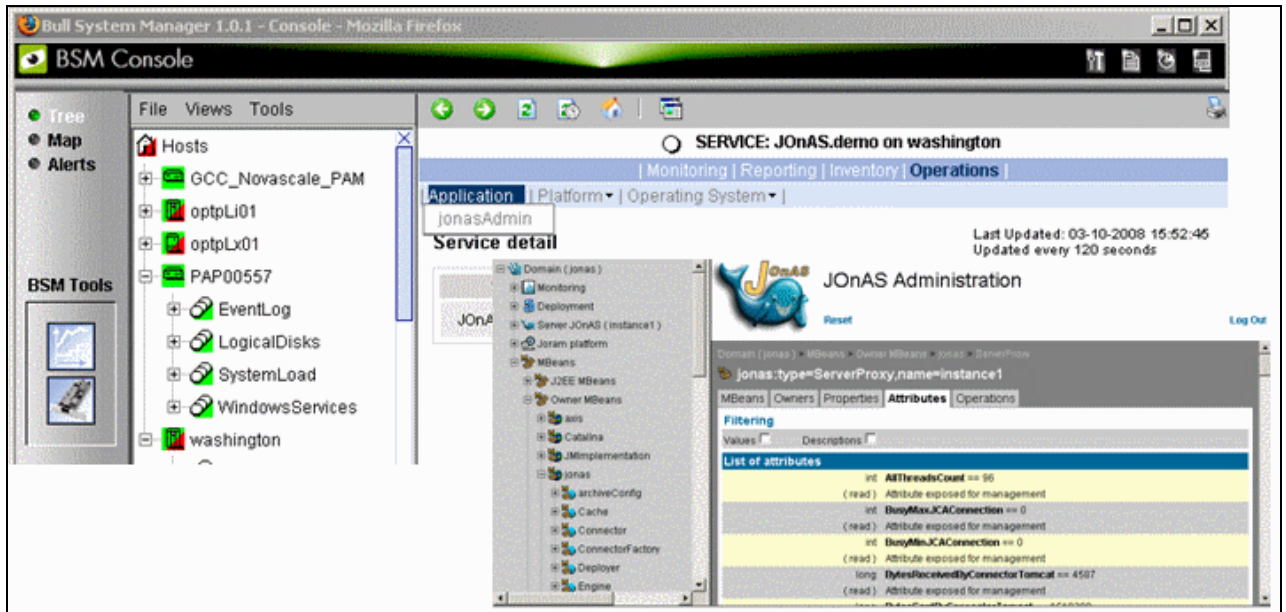


Figure 3-48. jonasAdmin launching

Appendix A. Check Commands for Customizable Services of Add_ons

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

Internal Storage Management

BSMGAMTT

check_gamttRAID

check_gamttRAID uses the following shell (PERL) command:

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 worst one;
CRITICAL > WARNING > OK.

Output

A string composed with a global state descriptor followed, if they exist, by error states of concerned component (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

They 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>	worst detected status
<CtrlModel>	controller model
<CtrlStatus>	worst 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 concerned elements 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 Nul) RAID5 Critical
>

```

- If return code is UNKNOWN:

```

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

```

BSMLSICIM

check_LSICIM

check_LSICIM uses the following shell (PERL) command:

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 quote 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 "Controllers" is in a WARNING state.
- CRITICAL:
At least one "Controllers" 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 worst one; CRITICAL > WARNING > OK.

Output

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

If the GlobalStatus determined by the worst 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
```

BSMMegaRaidSAS

check_MegaRaidSAS(_IR)

check_MegaRaidSAS(_IR) uses the following shell (PERL) command:

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 worst one;
CRITICAL > WARNING > OK.

Output

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

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

They 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>	worst state detected for an element of this 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 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 global state is CRITICAL or WARNING, only concerned elements 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 return code is UNKNOWN:

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

External Storage Management

BSMStoreWayFDA

check_NECFDA

check_NECFDA uses the following shell (PERL) command:

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 with the following format:

```
necfda <GlobalStatus>
```

<GlobalStatus> Most severe state detected on a controller.

Examples:

- If the global state is « OK »

```
> check_necfda -H <host>
necfda OK
>
```
- If the global state is CRITICAL or WARNING, only 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
>
```


BSMEmcClariion

check_EMCCLARIION

check_EMCCLARIION uses the following shell (PERL) command:

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 with the following format:

```
EmcClariion <GlobalStatus>
```

<GlobalStatus> Most severe state detected on 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 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
>

BSMNetApp

check-netapp-cpload

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

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 with 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%
```

check-netapp-umdisks

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

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 with 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
>
```

check-netapp-failedfans

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

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 with 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.  
>
```

check-netapp-failedpwr

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

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 with 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.
```

```
>
```

check_netapp_globalstatus

check_netapp_globalstatus uses the following shell (PERL) command:

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 with 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).
>
```

check_netappvol

check_netappvol uses the following shell (PERL) command:

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 with 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)
>
```

check_netappraid

check_netappraid uses the following shell (PERL) command:

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 with 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  
>
```

BSMWaterCooledDoor

check_sensor

check_sensor uses the following shell (PERL) command:

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
```

```
>
```

Virtualization Management

BSMVMwareESX

check_esx3

The Nagios check commands used by NMasterVMwareESX Add-on uses the shell (PERL) command `check_esx3`.

Usage

```
check_esx3 -H esxname [-N|-M|-B] [-C community] [-v virtualhost]
[-l thing [-w warn -c crit]] [-t timeout]
```

- H <esxname> Hostname or IP address of the ESX server to check
- N, -M, -B Set context for check execution
 - N for Nagios mode,
 - M for MRTG mode,
 - B for BSM mode.
- C <community> SNMP community string (defaults to "public")
- v <virtualhost> Name of the virtual host to check
- l <thing> Specify what to check
 - Available **thing** values: CPU, MEM, SNMP, STATE, LIST, LISTNET.
- 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 calling Nagios command. See detailed cases below.

check_esx_server case

The `check_esx3` shell is called with the following syntax:

```
check_esx3 -B -H <esxname> -C <community> -l LIST -w <warn>% -c <crit>%
```

Output:

```
VHosts: <nb-up>/<nb-all> up: <VMname> (<status>), .
```

Example:

```
check_esx3 -H esx -C public -w 50% -c 0%
VHosts: 2/4 up: nsmvm5(OFF), nsmvm1(ON), nsmvm3(ON), nsmvm4(OFF)
```

Status is set to **WARNING** if more than 50% of VMs are down.
 Status is set to **CRITICAL** if all VMs are down.

Note The list of VMs used to establish ESX server status corresponds to all the VMs declared on the ESX server and not only to those declared on the Bull System Manager ESX platform. The VMname is that declared on the VMware ESX server (this name can be different from the BSM hostname).

check_esx_snmp case

The check_esx3 shell is called with the following syntax:

```
check_esx3 -B -H <esxname> -C <community> -l SNMP
```

Output:

```
OK          SNMP management interface available
CRITICAL    SNMP management interface not available
```

check_esx_mem case

The check_esx3 shell is called with the following syntax:

```
check_esx3 -B -H <esxname> -C <community> -l MEM -w <warn>% -c <crit>%
```

Output:

```
Memory free: <free>Mb (<percent_free>) [Total available <total>Mb]
```

Example:

```
check_esx3 -H esx -C public -l MEM -w 20% -c 10%
Memory free: 16111.6Mb (98%) [Total available 16383.6Mb]
```

Status is set to **WARNING** if less than 20% of memory is available.
 Status is set to **CRITICAL** if less than 10% of memory is available.

check_esx_vm

The check_esx3 shell is called with the following syntax:

```
check_esx3 -B -H <esxname> -C <community> -v <virtualHost> -l STATE
```

Output:

```
OK          VHost <VMname>is up (ID: <id>)
CRITICAL    VHost <VMname>is down (ID: <id>)
```

Example:

```
check_esx_vm -H esx -C public -v nsmvm1 -l STATE
VHost nsmvm1 is up (ID: 48)
```

Status is set to OK if the VM is up.
Status is set to CRITICAL if the VMs are down.

Note The VMname is that declared on the ESX server (this name can be different from the BSM hostname).

check_esx_vm_memory

The check_esx3 shell is called with the following syntax:

```
check_esx3 -B -H <esxname> -C <community> -v <virtualHost> -l MEM
-w <warn>% -c <crit>%
```

Output:

```
Memory free: <free>Mb (<percent_free>) [Total available <total>Mb] on
vhost <VMname>
```

Example:

```
check_esx_vm_mem -B -H esx -C public -v nsmvm1 -w 20% -c 10%
Memory free: 460.8Mb (90%) [Total available 512Mb] on vhost smvm1
```

Status is set to **WARNING** if less than 20% of memory is available.
Status is set to **CRITICAL** if less than 10% of memory is available.

Note The VMname is that declared on the ESX server (this name can be different from the BSM hostname).

check_esx_vm_cpu

The check_esx3 shell is called with the following syntax:

```
check_esx3 -B -H <esxname> -C <community> -v <virtualHost> -l CPU
-w <warn>% -c <crit>%
```

Output:

```
CPU usage is <percent_used> on <VMname> nsmvm1 (<time>average)
```

Example:

```
check_esx_vm_cpu -B -H esx -C public -v nsmvm1 -w 80% -c 90%
CPU usage is 3% on nsmvm1 (301s average)
```

Status is set to WARNING if more than 80% of CPU is used.
Status is set to CRITICAL if more than 90% of CPU is used.

Note The VMname is that declared on the ESX server (this name can be different from the BSM hostname).

BSMHyperNova

check_NSM_hypervnova_xen

The Nagios check commands used by NMasterHyperNova Add-ons uses the shell (PERL) command `check_NSM_hypervnova_xen`.

Usage

```
check_NSM_hypervnova_xen -H <hnname> [-m <virtualhost>][-t timeout]
```

-H <hnname>	Hostname or IP address of the HyperNova server to check
-v <virtualhost>	name of the virtual host to check
-h, -help	Display help

Return code

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

Output

The output is the StatusText as setting by HNMaste. For the list of values, refer to the HyperNova documentation

Examples:

Check_hn_server_status

The `check_NSM_hypervnova_xen` shell is called with the following syntax:

```
check_NSM_hypervnova_xen -H <hnserver>
```

Output:

StatusText as returned by HNMaste

Example:

```
check_NSM_hypervnova_xen -H hnserver
```

Nothing to report

Status is set to OK.

Check_hn_vm_status

The `check_NSM_hypervnova_xen` shell is called with the following syntax:

```
check_NSM_hypervnova_xen -H <hnserver> -m <virtualhost>
```


Output:

<virtualHost>: StatusText as returned by HNMaster

Example:

```
check_NSM_hypernova_xen -H hnserver -m VM1
```

```
VM1: VM inactive
```

Status is set to WARNING.

Note The VMname is those declared on the HyperNova Server (this name can be different from the BSM hostname).

BSMEscalalpar

check_NSM_escalalpar

The Nagios check commands used by BSMEscalalPAR Add-on uses the shell (PERL) command `check_NSM_escalalpar`.

Usage

```
check_NSM_escalalpar -M manager [HMC|IVM] -H <netname> -U <remote_user>
-I <identity_file> [-l <lpar_name>] [-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
-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. See below to get detailed information.

check_vios_status case

The check_NSM_escalalpar shell is called with the following syntax:

```
check_NSM_escalalpar -M IVM -H <vios_netName> -N <server_name> -U <user>
-I <identity_file>
```

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 based on the state given by the **lssyscfg** IVM command to obtain the state of the Vios system.

Example:

```
check_NSM_escalalpar -H ivml -U padmin -I id_dsa_nsm
```

Output: Virtual I/O Server state: Operating

Return code: OK.

check_vios_used_pool case

The check_NSM_escalalpar shell is called with the following syntax:

```
check_NSM_escalalpar -M IVM -H <vios_netName> -U <user>
-I <identity_file> -N <server_name> -i POOL -e <sample_time> -w <warn>%
-c <crit>%
```

Output:

```
Processing pool (nbCPU / CPUTotal units entitled) - utilization on
<sampleTime> mn <check_status>: <utilization percent>%
```

Note The check_vios_used_pool command is based on pool_cycle metrics (total_pool_cycle, utilized_pool_cycle) obtained by the **lslparutil** IVM command.

It requires that data collection is activated by the **chlparutil** command:

```
chlparutil -r config -s 30
```

Example:

```
check_NSM_escalalpar -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) - utilization on 5 mn OK: 2.16 %
```

Return code: OK

check_cec_used_pool case

The check_NSM_escalalpar shell is called with the following syntax:

```
check_NSM_escalalpar -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_escalalpar -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_lpar_status case

The check_NSM_escalalpar shell is called with the following syntax:

```
check_NSM_escalalpar -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_vios_lpar_status command is based on Lpar state obtained by the **lssyscfg** IVM command.

Examples:

```
check_NSM_escalalpar -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_escalalpar -H 192.168.207.60 -U padmin -I id_dsa_nsm
-N ivml 1 part2
```

Output:

```
Logical partition tyrex on staix35 (IVM): Not Available
Return code: CRITICAL.
```

check_lpar_used_cpu case

The check_NSM_escalalpar shell is called with the following syntax:

```
check_NSM_escalalpar -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>%
```

Output:

```
Logical partition <lpar_name> on <server_name> (<nbCPU> units entitled -
IVM or HMC) - 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 **lsparutil** command (see above how to activate data collection on HMC or IVM).

Example:

```
check_NSM_escalalpar -H 192.168.207.60 -U padmin -I id_dsa_nsm -N ivml -
l part1 -I CPU-e 5 -w 10% -c 20%
```

Output:

```
Logical partition part1 on blade_js21 (0.4 units entitled - IVM) -
processing utilization on 5 mn WARNING: 17.77 %
```

Return code: WARNING

Bull Products Management

BSMDD4A

check_DynamicDomains

check_DynamicDomains uses the check_DD4A shell (PERL) command:

Usage

```
check_DD4A -H <host> [-w ] [-D <domainName>]
```

-H, --hostname <host> Hostname or IP address of target to check
-D, --domain ALL | <domainName> ALL domains or a specific one: <domainName>
-w, --web WEB HTML output format

Return code

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

- OK:
All "Dynamic Domains" run normally.
- WARNING:
At least one "Dynamic Domain" is in a WARNING state.
- CRITICAL:
At least one " Dynamic Domain " 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 worst one;
CRITICAL > WARNING > OK.

Output

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

If `-D ALL` or without `-D` parameter is used, the first line displays the defined Dynamic Domains number. Then, only Dynamic Domains with issues are displayed with their status, their number of used CPUs, their CPU load (and the associated threshold) and their number of tasks.

Note The global state is not displayed textually, only the command return code contains this status information.

If `-D <domainName>` is used, the command output displays the defined Dynamic Domain name with its number of used CPUs, its CPU load (and the associated threshold) and its number of tasks.

Examples:

- `check_DD4A -H <host>`
- `check_DD4A -H <host> -D ALL`
4 Dyn.Domains.
- domain2 : WARNING
CPUs: 4 / 4, tasks: 70
load: 80% (> 75%)
- domain3 : CRITICAL
CPUs: 4 / 4, tasks: 110
load: 100% (> 75%)
- `check_DD4A -H <host> -D default`
default : OK
CPUs: 7 / 8, tasks: 37
load: 0.56% (< 75%)

BSMBVS

check_BVS

check_BullVideoServices uses the check_BVS shell (PERL) command:

Usage

```
check_BVS -H <host> -S {Streaming|Recording|Datagrams}
[{-p <period>} | { -l <begin> -t <end> }] [-w]
```

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

-S, -service Streaming | Recording | Datagrams

-p, -period <period> | -l <begin> -t <end>
indicates to the Bull Video Server the period in seconds to calculate the average values

-w, -web WEB HTML output format

Return code

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

- OK:
"Bull Video Server" runs normally.
- WARNING:
"Bull Video Server" is in WARNING state.
- CRITICAL:
"Bull Video Server" is in CRITICAL state.
- UNKNOWN
All other type of processing errors (bad parameter, and so on...).

The BVS state "UNREACHABLE" (*Bull Video Server* is in " UNREACHABLE " state (daemon not started, communication timeout, ...)).will be transformed to Nagios "UNKNOWN" status.

The status values (OK, WARNING, CRITICAL) are fixed by the video server itself according to criteria's indicated by a Bull Video Server administrator.

Output

The following information is displayed. Average values are calculated using the value specified by the 'polling interval' textbox from the service configuration screen. The default value is 1 min. A modification of this value will be automatically taken into account by the check_BVS plugin.

'Streaming' service

Status	global status of 'Streaming' service
Channels	number of channels used for streaming (average)
Rate	average rate in MB/s
Load	percentage of disk rate in relation to a value declared on BVS server

Example:

```
check_BVS -H <host> -S Streaming
  Status: OK
  channels: 17.00,
  rate (MB/s): 38.84,
  load: 12.69 %
```

'Recording' service

Status	global status of 'Recording' service
Channels	number of channels used for recording (average)
Rate	average rate in MB/s
Load	percentage of disk rate in relation to a value declared on BVS server.

Example:

```
check_BVS -H <host> -S Recording
  Status: OK
  channels: 7.00,
  rate (MB/s): 3.84,
  load: 7.69 %
```

'Datagrams' service

Status	global status of 'Datagram' service
Nb of late dg	number of UDP datagram's sent late per second (average)
Avg late value	average delay value in ms. A delay value between 0 and 10 ms is considered as a normal value.
Nb of deleted dg	number of deleted UDP datagrams per second (average).

Example:

```
check_BVS -H <host> -S Datagrams
  Status: OK
  nb of late dg: 128.67,
  avg late value: 1.03 ms,
  nb of deleted dg: 3.08
```

Service Inaccessible

In case of inaccessible service only the RC will be displayed.

Example:

```
check_BVS -H <host> -S <service>
  Status: UNREACHABLE
```

BSMJOnAS

Check_JOnAS

Check_JOnAS uses the following shell (PERL) command:

Usage

```
check_JOnAS -H <host> -N <network name> -a <jonas master> -d <domain>  
-s <server> -p <port number> [-u <user> -p <password> ] [ -m ] -w
```

-H host	host name
-N network name	network name
-a <jonas master>	JOnAS server name Administrator or master
-d <domain>	domain name
-s <server>	target server name
-p <port number>	port number
-u <user name>	user name(mandatory if called outside BSM)
-p <password>	password (mandatory if called outside BSM)
-m	set if JOnAS server is master
-w	command output in HTML

Return Code

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

- OK:
JOnAS server runs normally.
- WARNING:
JonAS server is in "STOPPED" state.
- CRITICAL:
JOnAS server is in "FAILED" state.
- UNKNOWN:
JOnAS server is in "UNREACHABLE" state.

Example:

```
check_JOnAS -H nasmaster -N BSM.frcl.bull.fr -a jonas -d jonas -s jonas -p 9000
```

```
The jonas server in jonas domain is RUNNING on BSM.frcl.bull.fr  
Memory allocated = 57700 used = 39949  
Threads = 95  
HTTP requests count = 0  
Committed transactions count = 0  
check_JOnAS -H frcls6260 -N frcls6260.frcl.bull.fr -a instance1 -d  
jonas -s instance1 -p 9000 -m
```

```
The instance1 (master)server in jonas domain is RUNNING on frcls6260
Memory allocated = 64315 used = 36359
Threads = 98
HTTP requests count = 478157905
Committed transactions count = 0
```

Index

A

Alerts, 1
Alerts Service, 22, 28, 30
All Service, 76
Armg2_4.mib, 30

B

BSMEscalaLPAR, 66
BSMGAMTT, 21
BSMHyperNova, 52
BSMLSICIM, 24
BSMMegaRaidSAS, 27
Bull Video Services Management, 76
BullVideoServices Category, 77
BVS, 76

C

check command
 syntax, 85
check_EMCCLARIION, 32
check_JOnAS, 120
check_BVS, 78, 118
check_DynamicDomains, 76, 116
check_EMCCLARIION, 95
check_esx_mem, 50, 108
check_esx_server, 49, 107
check_esx_snmp, 50, 108
check_esx_vm, 50, 108
check_esx_vm_cpu, 50, 109
check_esx_vm_memory, 50, 109
check_esx3, 107

check_gamttRAID, 22, 85
check_hn_server_status, 63
check_hn_vm_status, 63
check_LSICIM, 25, 88
check_LSICIM_ctrl, 25
check_MegaRaidSAS(_IR), 28
check_MegaRaidSAS(_IR), 90
check_NECFDA, 30, 93
check_netapp_globalstatus, 101
check_netapp_globalstatus, 35
check_netapp_numdisks, 98
check_netappraid, 36, 103
check_netappvol, 36, 102
check_NSM_escalalpar, 112
check_NSM_hypernova_xen, 110
check_NSM_JOnAS, 81
check_sensor, 105
check-netapp-cpload, 35
check-netapp-cpload, 97
check-netapp-failedfans, 35, 99
check-netapp-failedpwr, 35, 100
check-netapp-numdisks, 35
CIM, 24
clariion.mib, 32
Commands
 check_JOnAS S, 120
 check_BVS, 78, 118
 check_DynamicDomains, 116
 check_EMCCLARIION, 95
 check_esx_mem, 50
 check_esx_server, 49
 check_esx_snmp, 50
 check_esx_vm, 50
 check_esx_vm_cpu, 50
 check_esx_vm_memory, 50
 check_esx3, 107
 check_gamttRAID, 22, 85
 check_LSICIM, 25, 88

- check_LSICIM_ctrl, 25
- check_MegaRaidSAS(_IR), 28, 90
- check_NECFDA, 93
- check_netapp_globalstatus, 101
- check_netapp_numdisks, 98
- check_netappraid, 103
- check_netappvol, 102
- check_NSM_escalalpar, 112
- check_NSM_hypervnova_xen, 110
- check_NSM_JOnAS, 81
- check_sensor, 105
- check-netapp-cpload, 97
- check-netapp-failedfans, 99
- check-netapp-failedpwr, 100
- ping, 1

CPUload, 34

CTRLstatus Service, 25

CurrentPower, 38

D

Datagrams Service, 77

DDFA, 75

DeltaPressure, 38

Disk Space
Requirements, 5

Disks, 34

Domain0 Supervision, 60

Dynamic Domains For Applications, 75

DynamicDomains Category, 76

E

EMC CLARiiON Management, 31

EmcClariion Category, 32

EscalalPAR, 66

ESX Virtual Platform, 43

F

Fans, 34

G

GAM, 21

GAMTT, 21

GAMTTraid Category, 22

GlobalStatus, 34

GUI, 18

- configuration tasks, 18
- starting, 18

H

Hardware Management Console (HMC), 66

Hardware Manager, 3

HMC (Hardware Management Console), 66

Host

- ESX, 46
- HNMaster, 56
- HyperNova, 56
- VMware, 46

HyperNova, 52

I

Installation

- Requirements, 5
- Windows, 7

Installation (Linux), 13

Integrated Virtualization Manager (IVM), 66

IVM (Integrated Virtualization Manager), 66

J

JOnAS, 78

jonasAdmin, 82

L

Logical partitioning (LPAR), 66

LPAR (logical partitioning), 66

LSI 22320 chip, 24
LSI CIM, 24
LSI MegaRAID, 21
LSI MegaRAID SAS (IR), 27
lsi-adaptersas(ir).mib, 28
LsiCIM Category, 25

M

MegaRAID, 21
megaraid.mib, 22
MegaRaidSAS(_IR) Category, 28
Memory
 Requirements, 5
MIB, 3
Monitoring Configuration, 18

N

NetApp Category, 34
NetApp Management, 33
netapp.mib, 34
Notifications, 1

O

Operating Systems, 5

P

Partitioning, 66
ping command, 1
Power, 34
PowerStatus, 38

R

RAIDStatus, 34

RAIDstatus Service, 25
Recording Service, 77
Restrictions, 6

S

Server Add-On, 4
Service
 Cloning, 19
 Creating, 19
 Customization, 18
 Customizing, 19
 definition, 2
ServiceStatus, 22, 28, 30
SNMP traps, 3
Storage Manager, 3
Storage Server, 29
StoreWay FDA Management, 29
StoreWayFDA Category, 30
Streaming Service, 77

T

TemperatureAverage, 38
Thresholds, 1

U

Uninstallation (Linux), 17
Uninstallation (Windows), 11
Upgrading (Linux), 17
Upgrading (Windows), 12
URL
 Bull System Manager main page, 18

V

ValveAperture, 38
Virtualization Manager, 3

Virtualization platform, 52

Virtualization Server, 40

Vmware ESX, 42

VolumeStatus, 34

W

Water Cooled Door Management, 37

WaterCooledDoorMIB.mib, 38

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

REFERENCE
86 A2 59FA 00