



# BSM 2.0 Server Add-ons

## Installation and Administrator's Guide



REFERENCE  
86 A2 59FA 06



# BSM 2.0 Server Add-ons

## Installation and Administrator's Guide

### Software

January 2012

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

**REFERENCE**  
**86 A2 59FA 06**

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 2008-2012

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

<b>Preface</b> .....	<b>ix</b>
Intended Readers.....	ix
Highlighting .....	ix
Related Publications.....	x
<b>Chapter 1.    Bull System Manager Server Add-ons Concepts</b> .....	<b>1</b>
1.1    Bull System Manager Overview .....	1
1.1.1    Monitoring Services.....	2
1.1.2    Event Reception .....	2
1.1.3    Hardware Manager .....	2
1.1.4    Storage Manager .....	2
1.1.5    Virtualization Manager.....	3
1.2    Bull System Manager Server Add-ons .....	3
<b>Chapter 2.    Installing and Configuring BSM Server Add-ons</b> .....	<b>5</b>
2.1    General Installation Requirements .....	5
2.1.1    Restrictions .....	6
2.2    Installing BSM Server Add-ons for Windows .....	7
2.2.1    Installing Management Server Add-ons from the BSM CD-ROM.....	7
2.2.2    Un-installing BSM Server Add-on Components .....	10
2.2.3    Upgrading to a New BSM Server Add-on Version .....	10
2.3    Installing Bull System Manager Server Add-ons for Linux.....	11
2.3.1    Prerequisites .....	11
2.3.2    Installing Management Server Add-ons from the CD-ROM.....	12
2.3.3    Uninstalling BSM Server Add-on Components.....	14
2.3.4    Upgrading to new Bull System Manager Server Add-on Versions.....	15
2.4    Monitoring Configuration.....	16
2.4.1    GUI Configuration.....	16
2.4.2    Categories and Services .....	17
<b>Chapter 3.    BSM Server Add-ons</b> .....	<b>19</b>
3.1    Internal Storage (Free) .....	19
3.1.1    BSM GAMTT for LSI MegaRAID 320-2x Management.....	19
3.1.2    BSMLSICIM for LSI 22320 Chip Management.....	21
3.1.3    BSM MegaRaidSAS (LSI MegaRAID SAS (IR) Management) .....	24
3.2    External Storage Server Add-ons.....	26
3.2.1    BSMStoreWayFDA (StoreWay FDA Management).....	26

3.2.2	BSMEmcClariion (EMC CLARiiON Management).....	28
3.2.3	BSMNetApp (NetApp Management) .....	30
3.2.4	BSMStoreWayDPA (StoreWay DPA Management).....	33
3.2.5	BSM SwitchBrocade (Brocade Fibre Channel Switch Management).....	35
3.3	External Device Server Add-ons .....	38
3.3.1	BSM WaterCooledDoor (Water Cooled Door Management) .....	38
3.3.2	BSM PDU-APC (APC Power Distribution Unit Management) .....	42
3.3.3	BSM iPDU (intelligent Power Distribution Unit Management) .....	45
3.4	Virtualization Server Add-ons.....	49
3.4.1	Overview .....	49
3.4.2	BSMVMwareVS for managing VMware vSphere .....	51
3.4.3	EscalLPAR Add-on.....	72
3.4.4	Bull System Manager Console.....	78
3.5	Bull Products Server Add-ons .....	82
3.5.1	DDFA.....	82
<b>Chapter 4.</b>	<b>Check Commands for Add-on Customizable Services .....</b>	<b>85</b>
4.1	Internal Storage Management Add-ons .....	85
4.1.1	BSMGAMTT Add-on .....	85
4.1.2	BSMLSICIM Add-on .....	88
4.1.3	BSMMegaRaidSAS Add-on .....	89
4.2	External Storage Management.....	92
4.2.1	BSMStoreWayFDA .....	92
4.2.2	BSMEmcClariion .....	93
4.2.3	BSMNetApp .....	94
4.2.4	BSMWaterCooledDoor .....	100
4.2.5	BSMStoreWayDPA .....	101
4.2.6	BSMSwitchBrocade .....	102
4.2.7	BSMPDU-APC .....	103
4.2.8	BSMIPDU .....	105
4.3	Virtualization Management .....	108
4.3.1	BSMVMwareVS .....	108
4.3.2	BSMEscalpar .....	110
4.3.3	BSMDD4A.....	116
<b>Appendix A.</b>	<b>Third Party License Agreement.....</b>	<b>119</b>
<b>Index .....</b>	<b>.....</b>	<b>121</b>

---

## List of figures

Figure 1-1.	Bull System Manager Architecture .....	2
Figure 2-1.	Windows Installation - Bull System Manager Welcome Page .....	7
Figure 2-2.	Windows Installation - Bull System Manager Install Page .....	8
Figure 2-3.	Windows Installation - Selecting Bull System manager Server Add-ons .....	9
Figure 2-4.	Windows Installation - Bull System Manager Server Add-ons Install Page .....	9
Figure 2-5.	Linux Installation - Bull System Manager Welcome Page .....	12
Figure 2-6.	Linux Installation - Selecting Bull System Manager Components .....	13
Figure 2-7.	Linux Installation - Selecting Bull System Manager Server Add-ons .....	13
Figure 2-8.	Linux Installation - Bull System Manager Server Add-ons Install page .....	14
Figure 3-1.	GAM Monitoring Components .....	19
Figure 3-2.	LSI CIM Monitoring Components .....	21
Figure 3-3.	MegaRAID SAS Monitoring Components .....	24
Figure 3-4.	StoreWay FDA Monitoring Components .....	26
Figure 3-5.	EMC CLARiiON Monitoring Components .....	28
Figure 3-6.	NetApp Monitoring Components .....	30
Figure 3-7.	StoreWayDPA Monitoring Components .....	33
Figure 3-8.	Brocade Fibre Channel Switch Monitoring Components .....	35
Figure 3-9.	Water Cooled Door Monitoring Components .....	38
Figure 3-10.	APC Power Distribution Unit Monitoring Components .....	42
Figure 3-11.	intelligent Power Distribution Unit Monitoring Components .....	45
Figure 3-12.	BSM Console Views .....	49
Figure 3-13.	Virtual Managers view .....	50
Figure 3-14.	Virtual Manager Monitoring Window .....	50
Figure 3-15.	ESX Virtual Platforms page .....	52
Figure 3-16.	ESX Platform Properties .....	53
Figure 3-17.	ESX Virtual Machines pane .....	54
Figure 3-18.	Host Topology modification confirmation screen .....	55
Figure 3-19.	VMware DataCenter Platforms page .....	57
Figure 3-20.	Virtual Center Properties .....	57
Figure 3-21.	Datacenters panel .....	59
Figure 3-22.	Topology modification confirmation .....	61
Figure 3-23.	VMwareESX monitoring information .....	69
Figure 3-24.	VMware reporting information .....	70
Figure 3-25.	EscalaLPAR Add-on components for HMC managed systems .....	72
Figure 3-26.	EscalaLPAR Add-on components for IVM managed systems .....	73
Figure 3-27.	VIOS.UsedPool Service Properties pane .....	75
Figure 3-28.	HMC activation from Bull System Manager Console .....	78
Figure 3-29.	IVM activation from Bull System Manager Console .....	79
Figure 3-30.	HMC managed Logical Partition reported Supervision .....	80
Figure 3-31.	HMC Virtualization layer reported supervision .....	80
Figure 3-32.	Escala IVM reported supervision .....	81
Figure 3-33.	DDFA Monitoring Components .....	82

---

## 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 .....	20
Table 3-2.	LSI CIM monitoring services .....	22
Table 3-3.	MegaRaid SAS (IR) monitoring services .....	25
Table 3-4.	StoreWay FDA monitoring services .....	27
Table 3-5.	EmcClariion monitoring services .....	29
Table 3-6.	NetApp monitoring services .....	30
Table 3-7.	StoreWayDPA monitoring services.....	34
Table 3-8.	Default Brocade Fibre Channel Switch monitoring services .....	35
Table 3-9.	Optional Brocade Fibre Channel Switch monitoring services.....	36
Table 3-10.	Default Water Cooled Door monitoring services .....	39
Table 3-11.	Optional Water Cooled Door monitoring services .....	39
Table 3-12.	Default APC Power Distribution Unit monitoring services.....	42
Table 3-13.	Performance Indicators applied to the APC PDU Host.....	43
Table 3-14.	Default intelligent Power Distribution Unit monitoring services.....	45
Table 3-15.	Optional intelligent Power Distribution Unit monitoring services .....	46
Table 3-16.	Performance Indicators applied to the IPDU Host .....	47
Table 3-17.	DDF4 categories and services .....	83



---

## Preface

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

---

**Note** The Bull Support Web site may be consulted for product information, documentation updates and service offers:  
<http://support.bull.com>

---

## Intended Readers

This guide is intended for use by System Administrators.

## Highlighting

The following highlighting conventions are used in this guide:

<b>Bold</b>	Identifies the following: <ul style="list-style-type: none"><li>• Interface objects such as menu names, labels, buttons and icons.</li><li>• File, directory and path names.</li><li>• Keywords to which particular attention must be paid.</li></ul>
<i>Italics</i>	Identifies references such as manuals.
Monospace	Identifies portions of program code, command lines, or messages displayed in command windows.
< >	Identifies parameters to be supplied by the user.

Commands entered by the user

---

System messages displayed on the screen

---



### WARNING

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

## Related Publications

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

- *BSM Installation Guide, 86 A2 54FA*  
explains how to install the Bull System Manager solution for managing Bull systems. This guide is intended for use by System Administrators.
- *BSM Administrator's Guide, 86 A2 56FA*  
explains how to customize Bull System Manager to monitor specific environments. This guide is intended for use by System Administrators.
- *BSM User's Guide, 86 A2 55FA*  
explains how to monitor and manage Bull systems using Bull System Manager, and in particular via the Bull System Manager Console. This guide is intended for use by System Operators.
- *BSM Remote Hardware Management CLI Reference Manual, 86 A2 58FA*  
describes the Hardware Management CLI (Command Line Interface) for Bull systems.
- *BSM Server Add-ons - Installation and Administrator's Guide, 86 A2 59FA*  
Bull System Manager Server Add-ons provide an extension to Bull System Manager for managing specific system devices or tools. This guide is intended for use by System Administrators.
- *Dynamic Domains for Applications User's Guide, 86 A2 63ER*
- *Release Notes, 86 A2 57FA*  
describe the contents, system requirements, installation instructions, and known issues (with workarounds, where applicable) for the current Bull System Manager release.

## Bull System Manager How To guides

The Bull System Manager How To guides, listed below, explains the configuration operations necessary to link BSM with different hardware and software products, so that they are included in BSM monitoring.

- *How To: Link BSM with LSI GAM(TT), 86 A7 00FD*
- *How To: Link BSM with a NovaScale T840 BMC, 86 A7 01FD*
- *How To: Link BSM with an RMC or ARMC (Express5800 BMC), 86 A7 02FD*
- *How To: Link BSM with a NovaScale 30x5 BMC, 86 A7 03FD*
- *How To: Link BSM with a NovaScale R4x0(E1) or T8x0 BMC, 86 A7 04FD*
- *How To: Link BSM with a StoreWay FDA, 86 A7 05FD*
- *How To: Link BSM with a NovaScale 4000 BMC, 86 A7 07FD*
- *How To: Link BSM with a NovaScale R410-E1 or T810-E1 iBMC, 86 A7 09FD*
- *How To: Link BSM with NovaScale R42x AOC-SIMSO(+), 86 A7 10FD*
- *How To: Link BSM with MegaRaid SAS, 86 A7 11FD*
- *How To: Link BSM with StoreWay EMC CLARiiON, 86 A7 13FD*
- *How To: Link BSM with Virtual I/O Server 86 A7 14FD*
- *How To: Link BSM with StoreWay NetApp, 86 A7 15FD*
- *How To: Link BSM with BULL Water Cooled Door, 86 A7 16FD*
- *How To: Link BSM with StoreWay DPA, 86 A7 17FD*
- *How To: Link BSM with HMC for Privilege Line, 86 A7 18FD*
- *How To: Link BSM with a Brocade Switch, 86 A7 20FD*
- *How To: Link BSM with iDRAC (Dell), 86 A7 21FD*
- *How To: Link BSM with APC Power Distribution Unit, 86 A7 22FD*
- *How To: Link BSM with intelligent Power Distribution Unit, 86 A7 23FD*
- *How To: Add new Host Model or OS and associated services, 86 A7 24FD*
- *How To: Link BSM with VMware vSphere, 86 A7 25FD*



---

# Chapter 1. Bull System Manager Server Add-ons Concepts

## 1.1 Bull System Manager Overview

Bull System Manager monitoring is used for the following tasks:

- Monitoring machines: Bull System Manager checks if the hosts are accessible, using the ping command from the System Manager. The machines to be monitored are either specified by the Administrator or detected 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 element monitored. When an anomaly occurs or when there is a return to normal status, **alerts** (in a log file) and **notifications** (by e-mail, by Bull autocall and/or by SNMP traps) 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-on packages.

---

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

---

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

---

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

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

**Note** Management Agent component can also be installed onto AIX systems

---

### Management Server and Server Add-ons

Provides the infrastructure and services responsible for the collection of and treatment of 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 the servers monitored. Management Agent must be installed on each server that is to be monitored.

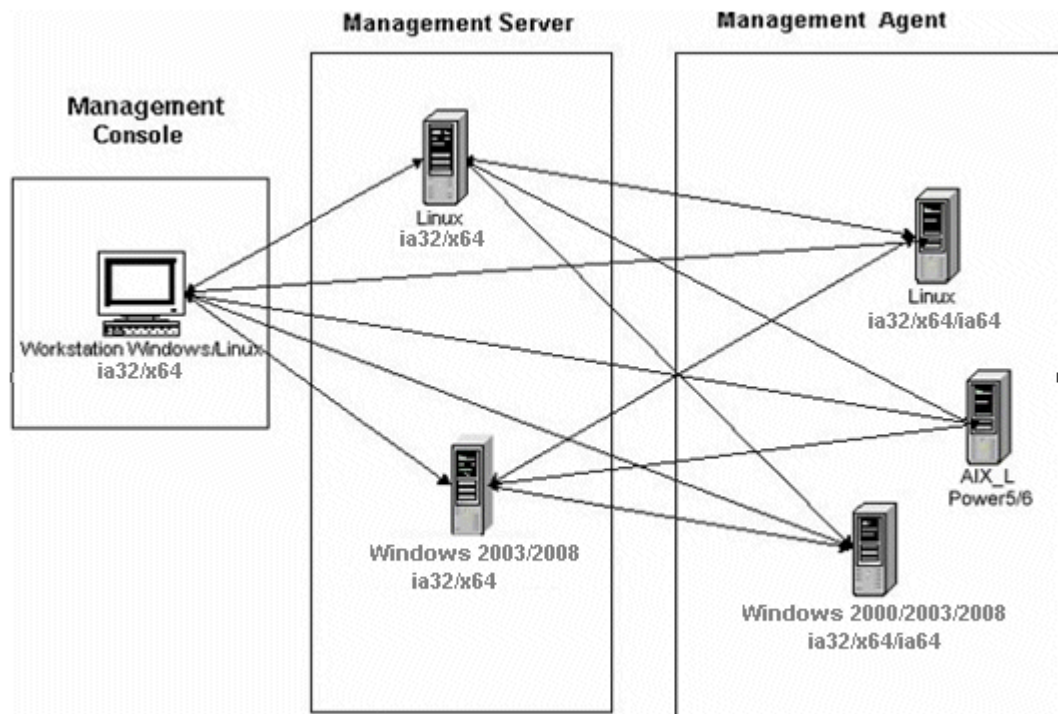


Figure 1-1. Bull System Manager Architecture

---

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

---

### 1.1.1 Monitoring Services

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.

### 1.1.2 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 a SNMP message. SNMP Traps must be defined in a **MIB** (Management Information Base).

### 1.1.3 Hardware Manager

A **Hardware Manager** manages hardware for one or more servers.

### 1.1.4 Storage Manager

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

## 1.1.5 Virtualization Manager

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

## 1.2 Bull System Manager Server Add-ons

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

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

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

---

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

---

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

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

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





---

## Chapter 2. Installing and Configuring BSM Server Add-ons

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

### 2.1 General Installation Requirements

#### Supported Operating Systems

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

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

#### Required Disk Space

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

#### Required Memory

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

Bull System Manager	Memory
Management Server	2 GB

Table 2-1. Bull System Manager - Required Memory

#### BSM Server Add-on Installation Requirements

Server Add-ons	Component
*	BSMServer2.0-x

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

#### BSM Server Add-on Operational Requirements

Server Add-ons	Target Tools
BSMGAMTT	Linux GAM version 6.02.31 or higher. Windows GAM version 6.02.32 or higher. <b>Important:</b> Go to <a href="http://www.lsilogic.com">www.lsilogic.com</a> to download the above versions. If not on-line, contact the Bull support team. <b>Note:</b> For IA32 machines the following earlier versions are supported: Linux GAM version 6.02.21 or higher Windows GAM version 6.02.22 or higher.
BSMLSICIM	LSI CIM provider version 3.06 or higher. <b>Important:</b> Go to <a href="http://www.lsilogic.com">www.lsilogic.com</a> to download the above versions. If not on-

Server Add-ons	Target Tools
	line, contact the Bull support team. <b>Note:</b> Not supported on Linux IA64 systems.
BSMMegaRaidSAS	LSI MegaRaid SAS (IR) SNMP agent version 3.09 or higher. Go to <a href="http://www.lsillogic.com">www.lsillogic.com</a> 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
BSMStoreWayDPA	StoreWay DPA embedded SNMP agent
BSMSwitchBrocade	Switch Brocade embedded SNMP agent
BSMDD4A	DDFA version 2.6.3 or higher
BSMVMwareVSpere	VMware Virtual Center 2.5 or higher VMware ESX 3.0 or higher <b>Important:</b> BSM Add-ons <u>use and include</u> the VI Perl toolkit API. On Windows platforms, the BSM Server uses ActivePerl with the VI Perl toolkit API (see requirements), but on Linux platforms, you have to install the required Perl packages for the VI Perl toolkit API. Go to the VMware documentation site to have the list of requirements <a href="http://www.vmware.com/support/developer/viperltoolkit/">http://www.vmware.com/support/developer/viperltoolkit/</a> . If not on-line, contact the Bull support team.
BSMEscalalPAR	IVM VIOS for Power5 and Power6 (Escala PL or EL Blade servers) or HMC version 6.1 and higher
BSMWaterCooledDoor	Device firmware: EMM release 1.1.0 build14
BSMAPCPDU	APC Switch rack PDU AP7821, AP7921 and AP7922 with firmware release 3 and higher.

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

## 2.1.1 Restrictions

### Windows

N/A

### Linux

N/A

## 2.2 Installing BSM Server Add-ons for Windows

### Prerequisites

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

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

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

Management Server Add-ons, to be installed on the server dedicated to management, require the components indicated in *0 BSM Server Add-on 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 components:

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

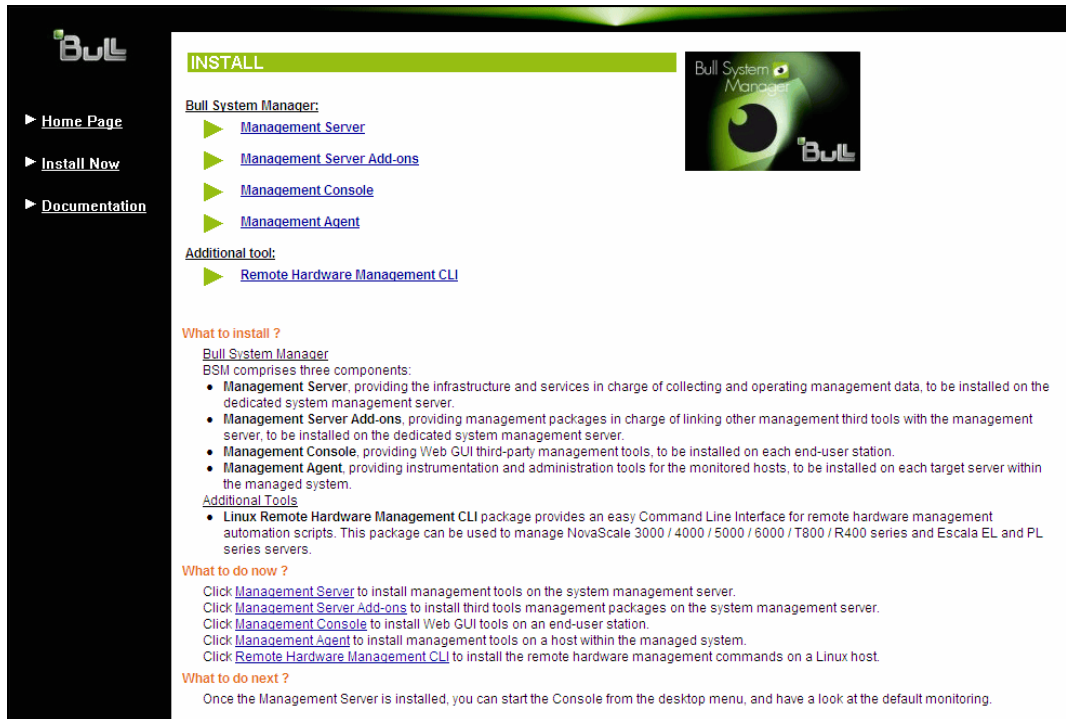


Figure 2-2. Windows Installation - Bull System Manager Install Page

## Select Management Server Add-ons

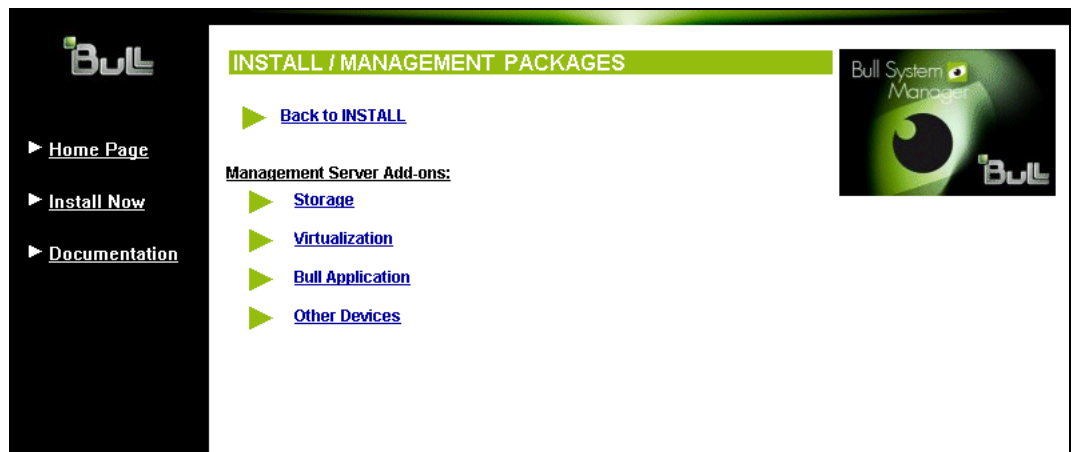


Figure 2-3. Windows Installation - Selecting Bull System manager Server Add-ons

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

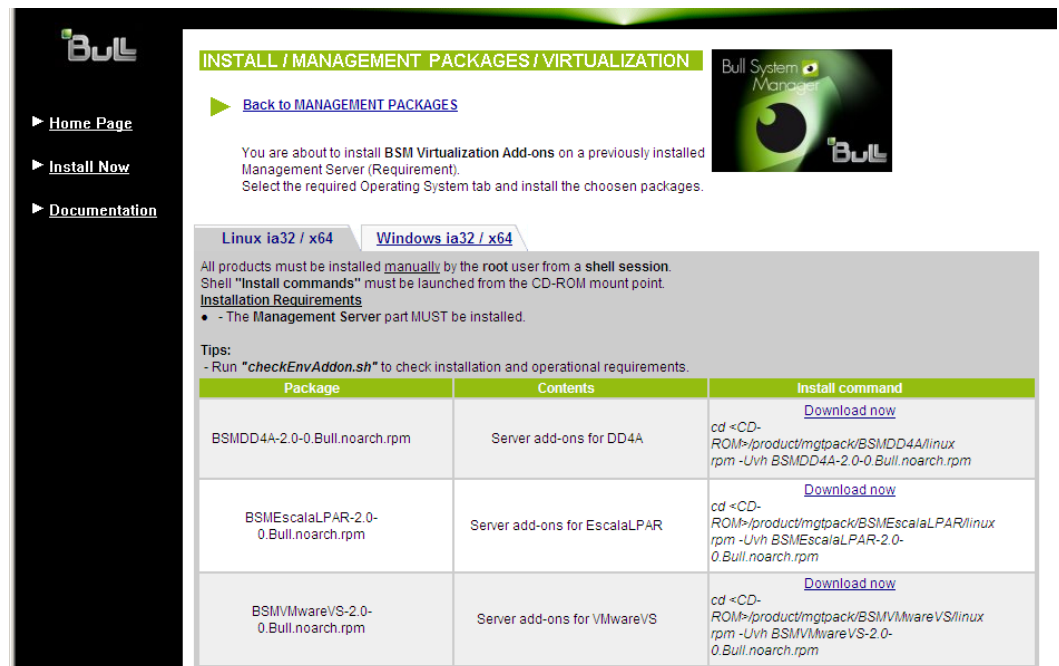


Figure 2-4. Windows Installation - Bull System Manager Server Add-ons Install Page

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

## 2.2.2 Un-installing BSM Server Add-on Components

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

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

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

---

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

---

## 2.2.3 Upgrading to a New BSM Server Add-on Version

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

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

---

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

---

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

## 2.3 Installing Bull System Manager Server Add-ons for Linux

### 2.3.1 Prerequisites

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

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

- 
- Notes**
- You can check if the required packages from a given Add-on are installed by launching.  

```
cd <CD-ROM mount point>  
/checkEnvAddon.sh -a <addOn>
```
  - AddOn is the name of the RPM (BSM<addOnIdent>.<version>.Bull) or the short addOnIdent.
  - The RPM packages listed above may have their own dependencies and require other RPM packages.
  - If the RPM has been installed, the result of the checkEnvAddon is listed in the corresponding installation log (post\_install\_BSM<addOnIdent> log in the <BSM Installation>/engine/tmp/ directory
-

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

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

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

From the dedicated server, launch the installation program.

Log on as **root**.

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

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

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



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

3. Click **Install Now** to open the **Install** page, which allows the required Bull System Manager components to be selected:
  - Management Server Add-onsand provides the following information:
  - What to install?
  - What to do now?



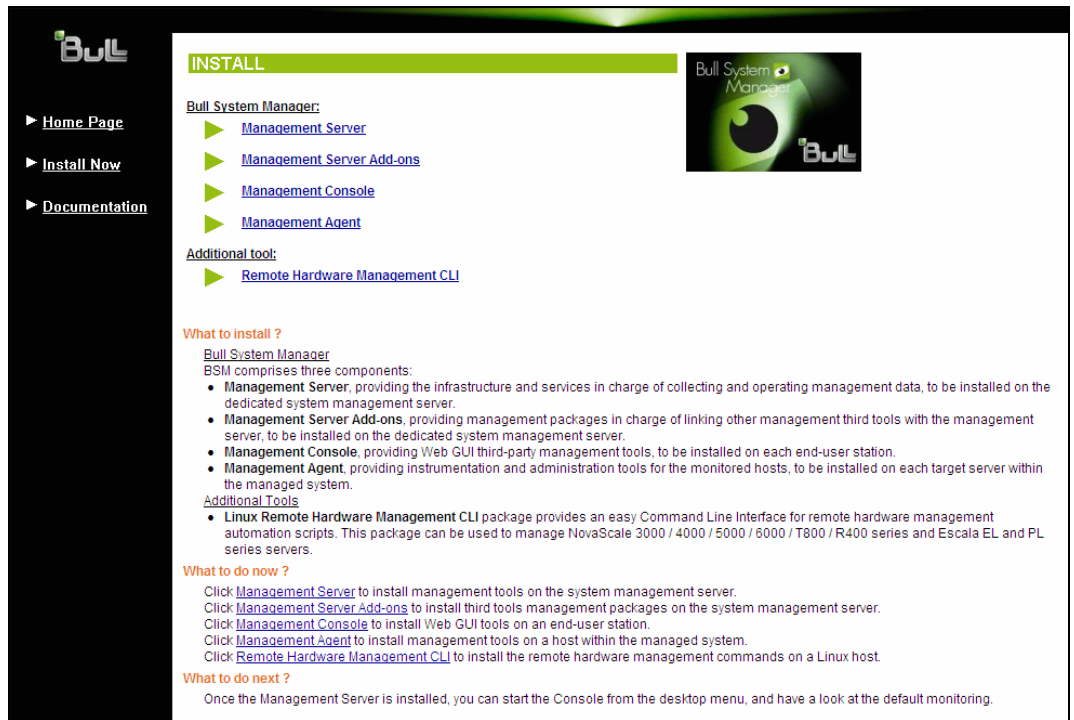


Figure 2-6. Linux Installation - Selecting Bull System Manager Components

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

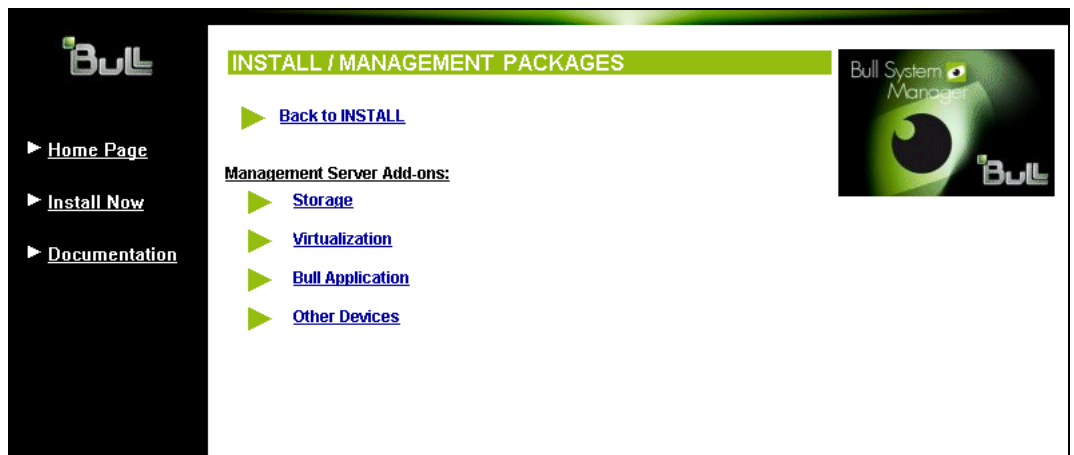


Figure 2-7. Linux Installation - Selecting Bull System Manager Server Add-ons

- Select an Add-ons family (Storage, Virtualization, Bull Application or Other Devices), Select the Linux 32 bits operating system.

Package	Contents	Install command
BSMEmcClariion-2.0-0.Bull.noarch.rpm	Server add-ons for EmcClariion	cd <CD-ROM>/product/mgtpack/BSMEmcClariion/linux rpm -Uvh BSMEmcClariion-2.0-0.Bull.noarch.rpm
BSMGAMTT-2.0-0.Bull.noarch.rpm	Server add-ons for GAMTT (Status plugin and SNMP trap reception)	cd <CD-ROM>/product/mgtpack/BSMGAMTT/linux rpm -Uvh BSMGAMTT-2.0-0.Bull.noarch.rpm
BSMLSICIM-2.0-0.Bull.noarch.rpm	Server add-ons for LSI CIM (Status plugin)	cd <CD-ROM>/product/mgtpack/BSMLSICIM/linux rpm -Uvh BSMLSICIM-2.0-0.Bull.noarch.rpm
BSMMegaRaidSAS-2.0-0.Bull.noarch.rpm	Server add-ons for MegaRaid SAS (Status plugin and SNMP trap reception)	cd <CD-ROM>/product/mgtpack/BSMMegaRaidSAS/linux rpm -Uvh BSMMegaRaidSAS-2.0-0.Bull.noarch.rpm
BSMNetApp-2.0-0.Bull.noarch.rpm	Server add-ons for NetApp	cd <CD-ROM>/product/mgtpack/BSMNetApp/linux rpm -Uvh BSMNetApp-2.0-0.Bull.noarch.rpm
BSMStoreWayDPA-2.0-0.Bull.noarch.rpm	Server add-ons for StoreWayDPA	cd <CD-ROM>/product/mgtpack/BSMStoreWayDPA/linux rpm -Uvh BSMStoreWayDPA-2.0-0.Bull.noarch.rpm

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

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

```
cd <CD-ROM mount point>/product/mgtpack/BSM<toolname>/linux
rpm -Uvh BSM<toolname>-2.0-x.noarch.rpm
```

### 2.3.3 Uninstalling BSM Server Add-on Components

- Log on as root.
- Launch:

```
rpm -e BSM<toolname>-2.0-x.noarch.rpm
```

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

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

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

```
rpm -Uhv BSM<toolname>-2.0-x.noarch.rpm
```

---

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

---

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

## 2.4 Monitoring Configuration

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


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

### 2.4.1 GUI Configuration

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

#### Starting the Configuration GUI

To start the Configuration GUI, either:

- From the Bull System Manager Console, click the  icon representing the Configuration GUI in the Administration zone (top right)
- Or click the **Configuration** link on the Bull System Manager Home Page, URL:  
**`http://<Bull System Manager server name>/BSM`**
- Or, from a web browser, go to the following URL:  
**`http://<Bull System Manager server name>/BSM/config/`**

## 2.4.2 Categories and Services

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

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

The Administrator can change the default monitoring configuration by:

- **Customizing services**, to define specific thresholds and monitoring properties or to modify the list of monitored hosts. A service can be customized to create one or more occurrences of this service with the same name. Each occurrence can have a different host list and different monitoring properties. For instance, if you do not want to monitor file systems in the same way on all Linux hosts, customize the **All** service in the **FileSystems** category.

---

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

---

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

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



## Chapter 3. BSM Server Add-ons

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

### 3.1 Internal Storage (Free)

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

#### 3.1.1 BSM GAMTT for LSI MegaRAID 320-2x Management

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

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

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

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

The following figure shows the different monitoring components:

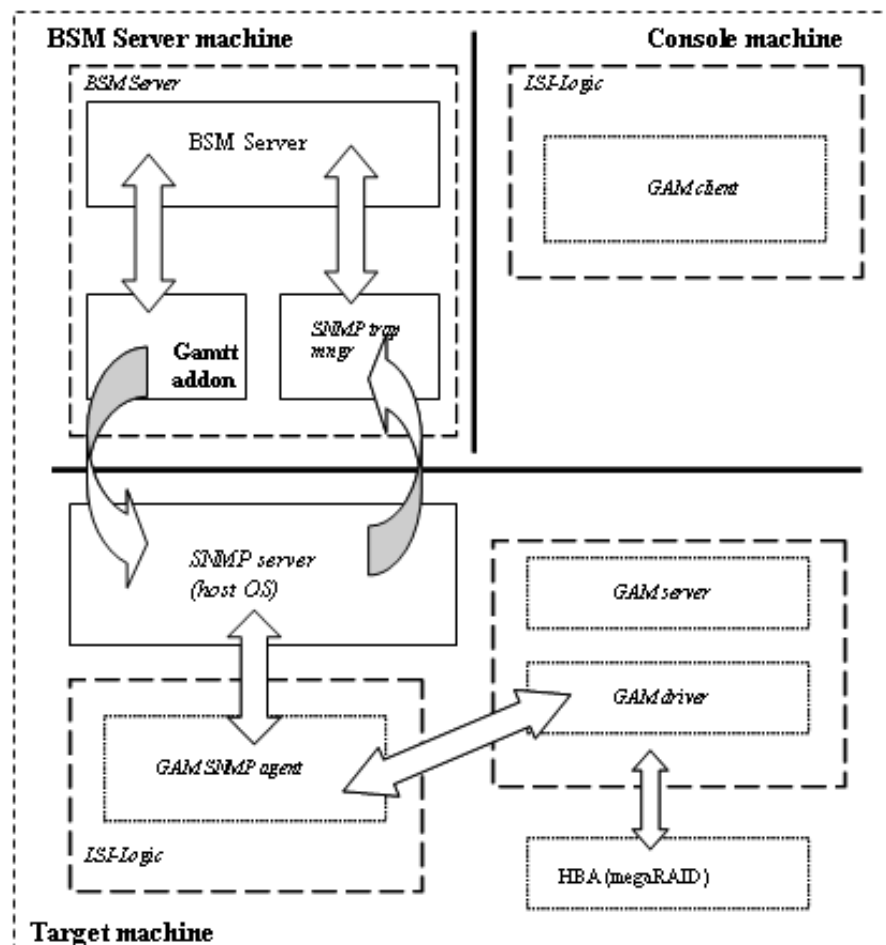


Figure 3-1. GAM Monitoring Components

### 3.1.1.1 Default Categories & Services (independent of OS type)

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

Table 3-1. GAMTT monitoring services

---

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

---

### 3.1.1.2 GAMTTraid Category

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

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

---

**Notes** The **mlxraid.mib** is integrated in the Bull System Manager application. Do not forget to configure the agent to send SNMP traps to the Bull System Manager server by adding the Bull System Manager server host address to the SNMP managers list for this agent.

---

### 3.1.1.3 check\_gamttRAID (any OS) Nagios command

The configurable Bull System Manager service check command syntax is:

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

#### Input

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



### Output

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

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

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

## 3.1.2 BSMLSICIM for LSI 22320 Chip Management

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

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

---

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

---

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

The following figure shows the different monitoring components:

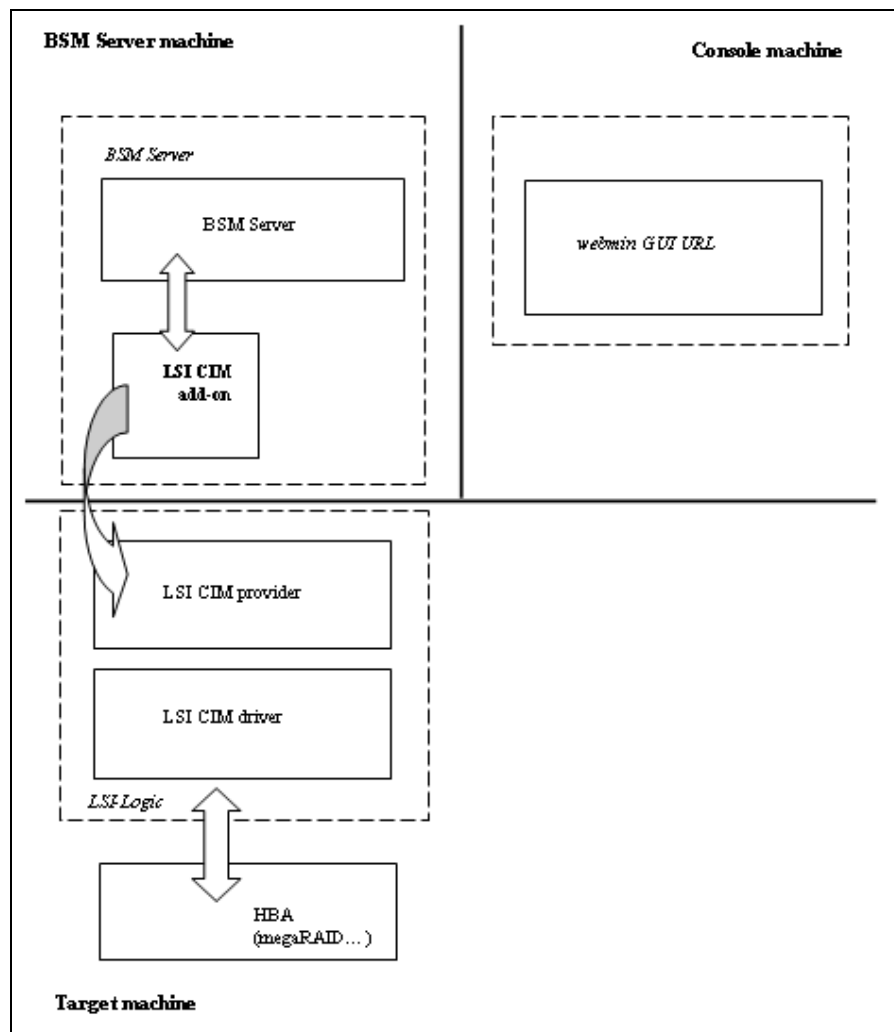


Figure 3-2. LSI CIM Monitoring Components

### 3.1.2.1 Default Categories & Services (independent of OS type)

Targeted OS	Model	Category	Service	Check command
Any	Any	LsiCIM	RAIDStatus	check_LSiCIM
			CTRLstatus	check_LSiCIM_ctrl

Table 3-2. LSI CIM monitoring services

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

#### LsiCIM Category

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

### 3.1.2.2 check\_LSiCIM (any OS) Nagios command

The configurable Bull System Manager service check command syntax is:

```
check_LSiCIM
```

#### Input

N/A

#### Output

See the output of the **check\_LSiCIM** shell command in *Chapter 4*.

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

```
check_LSiCIM
```

### 3.1.2.3 check\_LSiCIM\_ctrl (any OS) Nagios command

The configurable Bull System Manager service check command syntax is:

```
check_LSiCIM_ctrl! [<ctrlname>]
```

#### Input

<ctrlname>            Name of the controller to check

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

#### Output

See the output of the **check\_LSiCIM** shell command in *Chapter 4*.

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

```
check_LSiCIM! 'ctrlname'
```

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

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

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

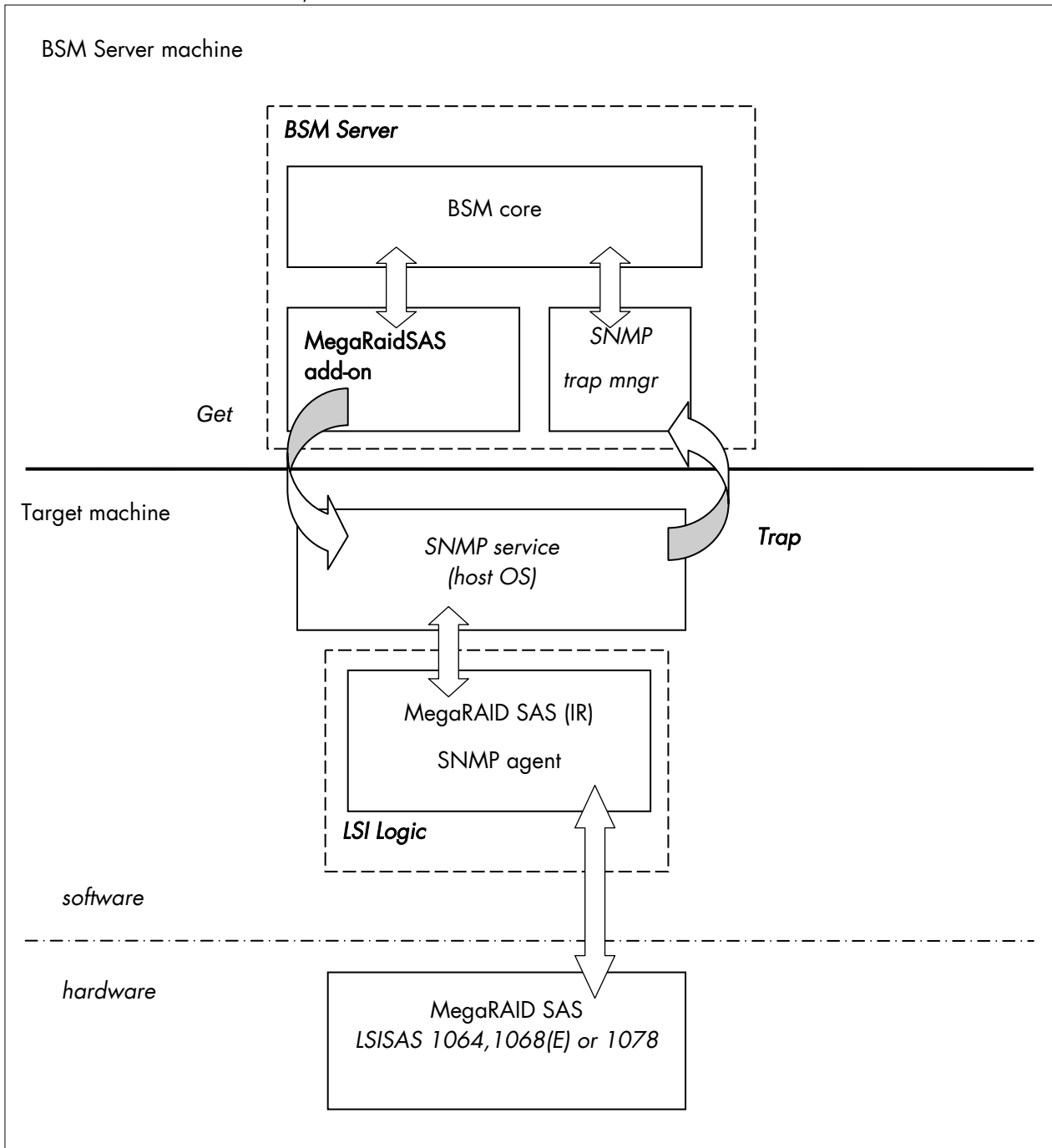


Figure 3-3. MegaRAID SAS Monitoring Components

### 3.1.3.1 Default Categories & Services (independent of OS type)

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

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

---

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

---

### 3.1.3.2 MegaRaidSAS(\_IR) Category

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

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

---

**Notes** The `lsi-.adaptersas(ir).mib` is integrated in the Bull System Manager application.

Do not forget to configure the MegaRAID SAS (IR) SNMP agent to send SNMP traps to the Bull System Manager Server by adding the Bull System Manager Server host address to the agent's SNMP managers list.

---

### 3.1.3.3 check\_MegaRaidSAS(\_IR) (any OS) Nagios command

The configurable Bull System Manager service check command syntax is:

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

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

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

```
check_MegaRaidSAS(_IR)!public!161!60
```

## 3.2 External Storage Server Add-ons

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

### 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.

It supports the StoreWay FDA and StoreWay Optima families.

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

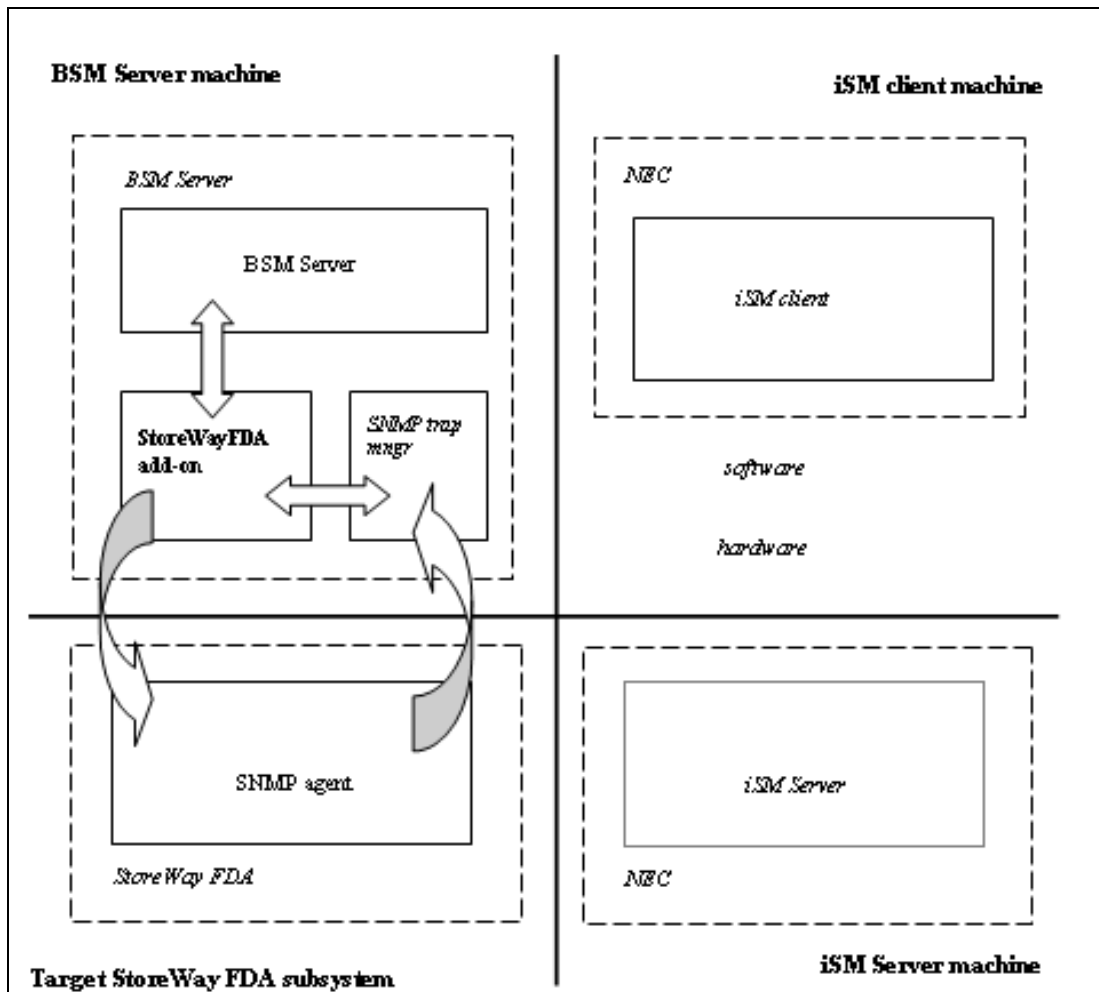


Figure 3-4. StoreWay FDA Monitoring Components

### 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 SNMP agents. This service checks the StoreWay FDA status reported by the SNMP agent.

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

---

**Notes** The **Armg2\_4.mib** is integrated in the Bull System Manager application.

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

---

### 3.2.1.3 check\_NECFDA (any OS) Nagios command

The configurable Bull System Manager service check command syntax is:

```
check_storewayfd!<timeout>
```

See the **check\_NECFDA** command in *Chapter 4* for parameter details.

For HOSTADDRESS, SNMP community and SNMP port parameters, the Nagios macros \$HOSTADDRESS\$, \$\_HOSTSNMP\_COMMUNITY\$ and \$\_HOSTSNMP\_PORT\$ are used.

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

```
check_necfda!60
```

### 3.2.1.4 Bull System Manager Configuration

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

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

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

<b>StoreWay FDA name</b>	name of the StoreWay FDA
<b>description</b>	description
<b>network name</b>	bay netname
<b>snmp port number</b>	SNMP port number
<b>snmp community</b>	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.

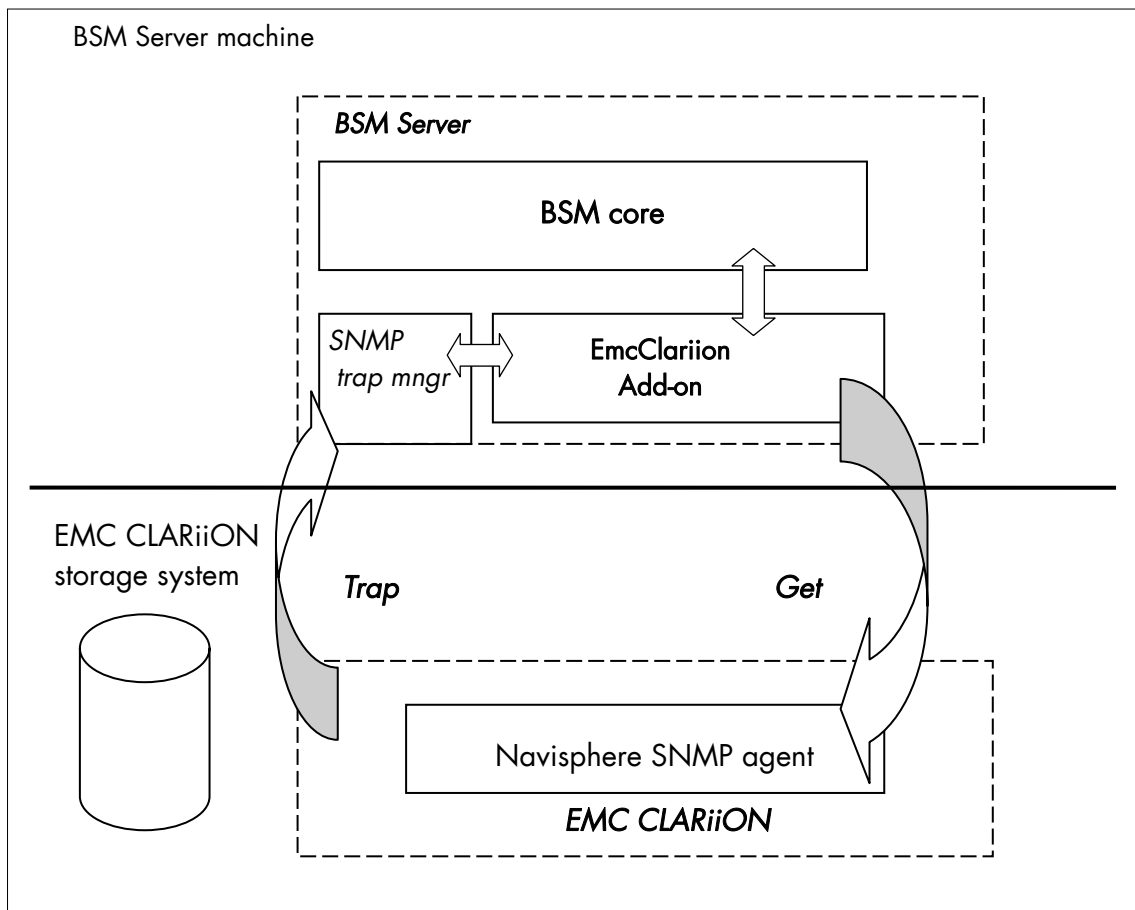


Figure 3-5. EMC CLARiiON Monitoring Components



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

---

### 3.2.2.3 check\_EMCCLARIION (any OS) Nagios command

The configurable Bull System Manager service check command syntax is:

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

See the `check_EMCCLARIION` command in *Chapter 4* for parameter details.

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

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

### 3.2.2.4 Bull System Manager Configuration

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

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

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

<b>StoreWay EMC CLARiiON name</b>	name of the EMC CLARiiON
<b>description</b>	description
<b>network name</b>	bay netname
<b>SNMP port number</b>	SNMP port number

### 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.

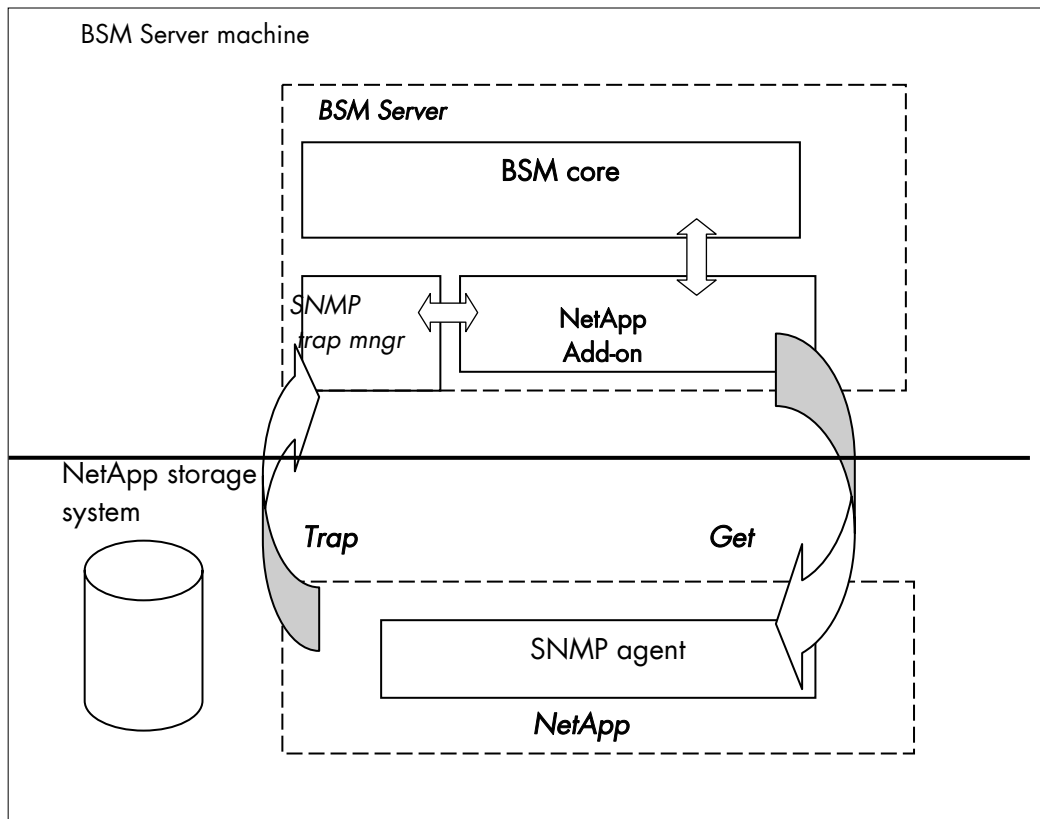


Figure 3-6. NetApp Monitoring Components

#### 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

<b>CPUload</b>	For NetApp hosts managed via SNMP agents. This service checks the NetApp CPU load reported by the SNMP agent.
<b>Disks</b>	For NetApp hosts managed via SNMP agents. This service checks the status of the NetApp disks reported by the SNMP agent.
<b>Fans</b>	For NetApp hosts managed via SNMP agents. This service checks the status of the NetApp fans reported by the SNMP agent.
<b>GlobalStatus</b>	For NetApp hosts managed via SNMP agents. This service checks the NetApp Global Status reported by the SNMP agent.
<b>Power</b>	For NetApp hosts managed via SNMP agents. This service checks the status of the NetApp power supplies reported by the SNMP agent.
<b>RAIDStatus</b>	For NetApp hosts managed via SNMP agents. This service checks the NetApp RAID status reported by the SNMP agent.
<b>VolumeStatus</b>	For NetApp hosts managed via SNMP agents. This service checks the NetApp volume status reported by the SNMP agent.
<b>Alerts</b>	For NetApp hosts. When an alert is sent from the NetApp SNMP agent, it is processed by the Bull System Manager Server.

---

**Notes** The `netapp.mib` is integrated in the Bull System Manager application.

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

---

### 3.2.3.3 Reporting Indicators

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

#### Indicator applied to the NetApp Host

Indicator	Corresponding Service
<NetApp_host>_CPUload	CPUload

### 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 *Chapter 4* for details.

### check-netapp-numdisks (any OS) Nagios command

The Bull System Manager service check command syntax is:

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

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

### check-netapp-failedfans (any OS) Nagios command

The Bull System Manager service check command syntax is:

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

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

### check\_netapp\_globalstatus (any OS) Nagios command

The configurable Bull System Manager service check command syntax is:

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

See the **check\_netapp\_globalstatus** command in *Chapter 4* for parameter details.

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

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

### check-netapp-failedpwr (any OS) Nagios command

The Bull System Manager service check command syntax is:

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

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

### check\_netappraid (any OS) Nagios command

The configurable Bull System Manager service check command syntax is:

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

See the **check\_netappraid** command in *Chapter 4* for parameter details.

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

```
check_ NetAppRaid!public!161!60
```

### check\_netappvol (any OS) Nagios command

The configurable Bull System Manager service check command syntax is:

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

See the **check\_netappvol** command in *Chapter 4* for parameter details.

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

```
check_ NetAppVol!public!161!60
```

### 3.2.3.5 Bull System Manager Configuration

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

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

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

<b>StoreWay NetApp name</b>	name of the NetApp
<b>description</b>	description
<b>network name</b>	bay netname
<b>SNMP port number</b>	SNMP port number
<b>SNMP community</b>	SNMP community

### 3.2.4 BSMStoreWayDPA (StoreWay DPA Management)

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

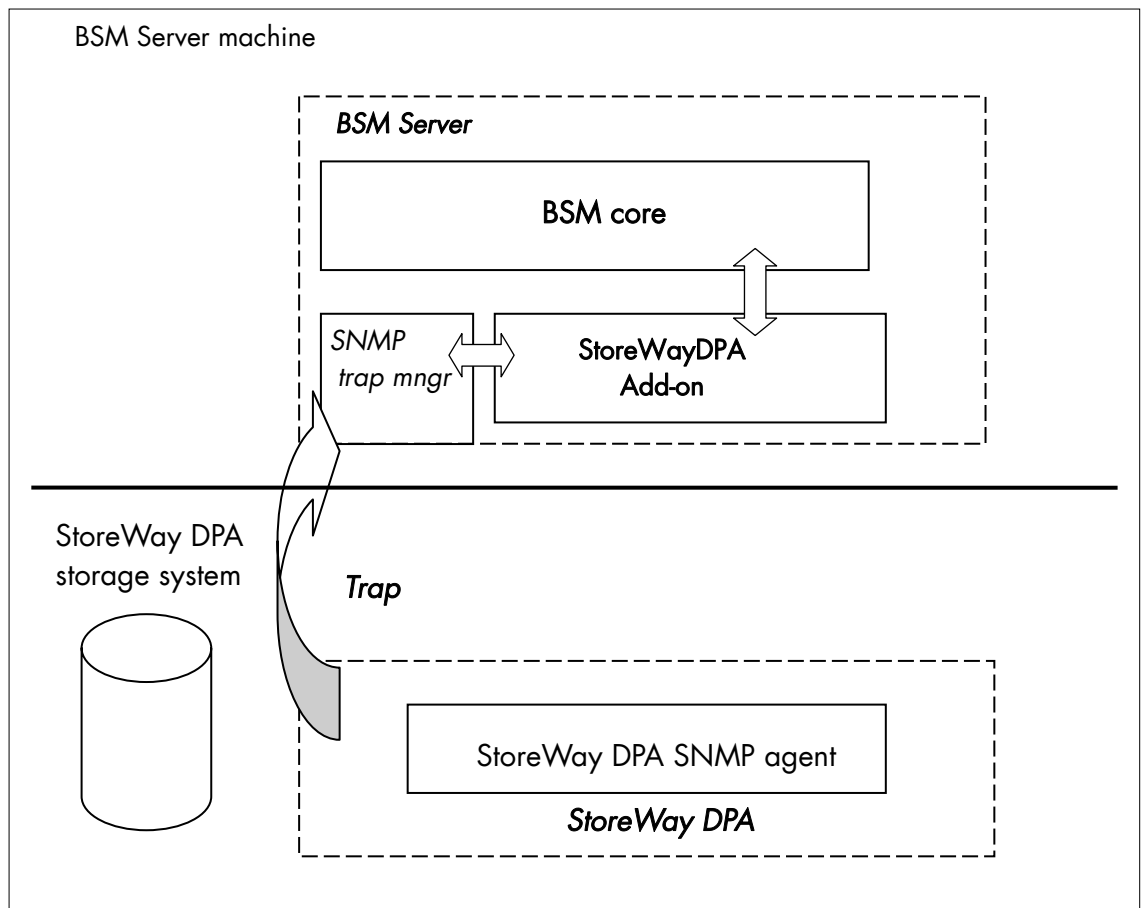


Figure 3-7. StoreWayDPA Monitoring Components

### 3.2.4.1 Default Categories & Services (independent of OS type)

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

Table 3-7. StoreWayDPA monitoring services

---

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

---

### 3.2.4.2 StoreWayDPA Category

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

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

---

**Notes**

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

---

### 3.2.4.3 Nagios check commands

Check\_StoreWayDPA (any OS) Nagios command

The Bull System Manager service check command syntax is:

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

See the `check_StoreWayDPA` command in *Chapter 4* for parameter details.

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

```
check_StoreWayDPA!public!161!60
```

### 3.2.4.4 Bull System Manager Configuration

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

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

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

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

### 3.2.5 BSM SwitchBrocade (Brocade Fibre Channel Switch Management)

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

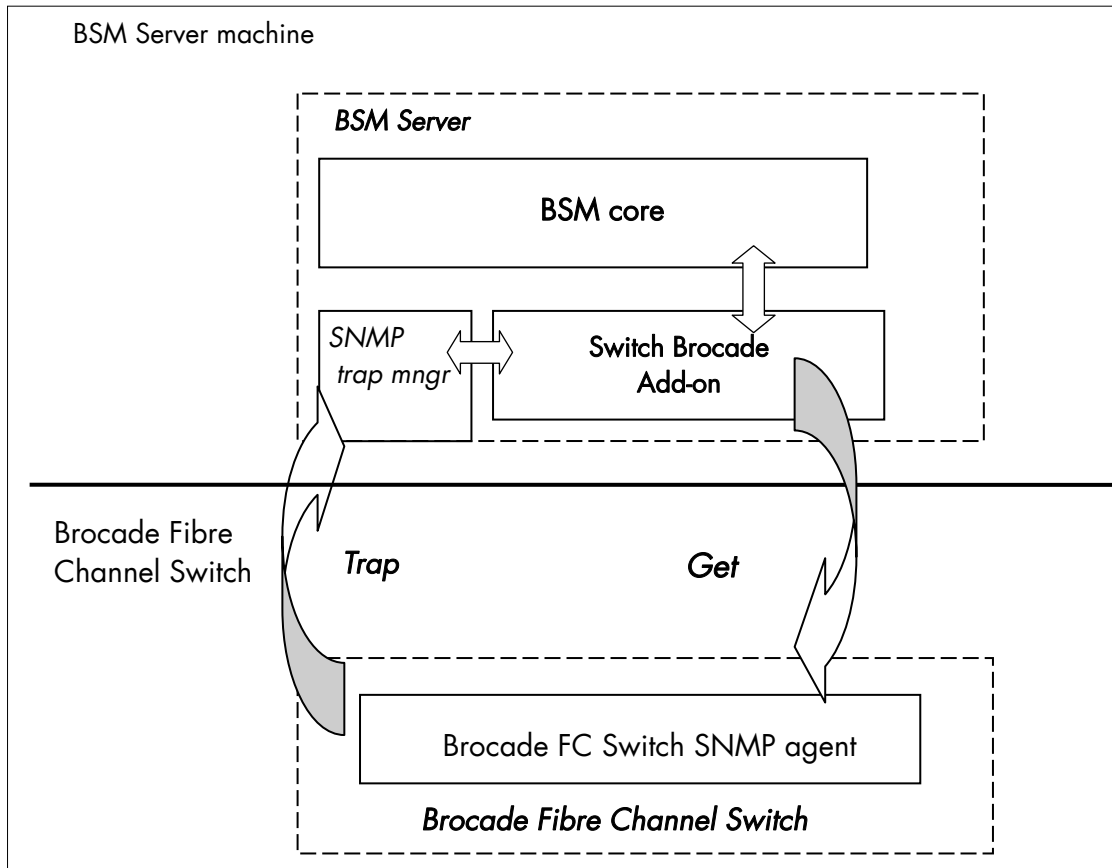


Figure 3-8. Brocade Fibre Channel Switch Monitoring Components

#### 3.2.5.1 Default Categories & Services (independent of OS type)

Targeted OS	Model	Category	Service	Check command
Any	baySwitchBrocade	Brocade	Alerts	No check (SNMP trap receiver)
			Status	check_brocade
			Ports	check_brocade

Table 3-8. Default Brocade Fibre Channel Switch monitoring services

---

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

---

### 3.2.5.2 Optional Categories & Services (independent of OS type)

Targeted OS	Model	Category	Service	Check command
Any	baySwitchBrocade	Brocade_Sensors	Fans	check_brocade
			Temp	check_brocade

Table 3-9. Optional Brocade Fibre Channel Switch monitoring services

---

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

---

### 3.2.5.3 Brocade Category

- Status** For SwitchBrocade hosts managed via its SNMP agent. This service checks the Brocade Fibre Channel Switch global status reported by the SNMP agent.
- Ports** For SwitchBrocade hosts managed via its SNMP agent. This service checks each Brocade Fibre Channel Switch port status reported by the SNMP agent.
- Alerts** For SwitchBrocade hosts. When an alert is sent from the Brocade Fibre Channel Switch SNMP agent, it is processed by the Bull System Manager Server.

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

### 3.2.5.4 Brocade\_Sensors Category

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



### 3.2.5.5 Nagios check commands

check\_brocade (any OS) Nagios command

The Bull System Manager service check command syntax is:

check\_brocade!<sensor>

values available for <sensor> are:

- switch
- port
- fan
- temp

See the **check\_brocade** command in *Chapter 4* for parameter details.

For HOSTADDRESS, SNMP community and SNMP port parameters, the Nagios macros \$HOSTADDRESS\$, \$\_HOSTSNMP\_COMMUNITY\$ and \$\_HOSTSNMP\_PORT\$ are used.

### 3.2.5.6 Bull System Manager Configuration

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

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

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

<b>Switch Brocade name</b>	name of the Brocade Fibre Channel Switch
<b>description</b>	description
<b>network name</b>	bay netname
<b>SNMP port number</b>	SNMP port number
<b>SNMP community</b>	SNMP community

### 3.2.5.7 Configuration of optional Brocade\_Sensors category

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

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

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

### 3.3 External Device Server Add-ons

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

#### 3.3.1 BSM WaterCooledDoor (Water Cooled Door Management)

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

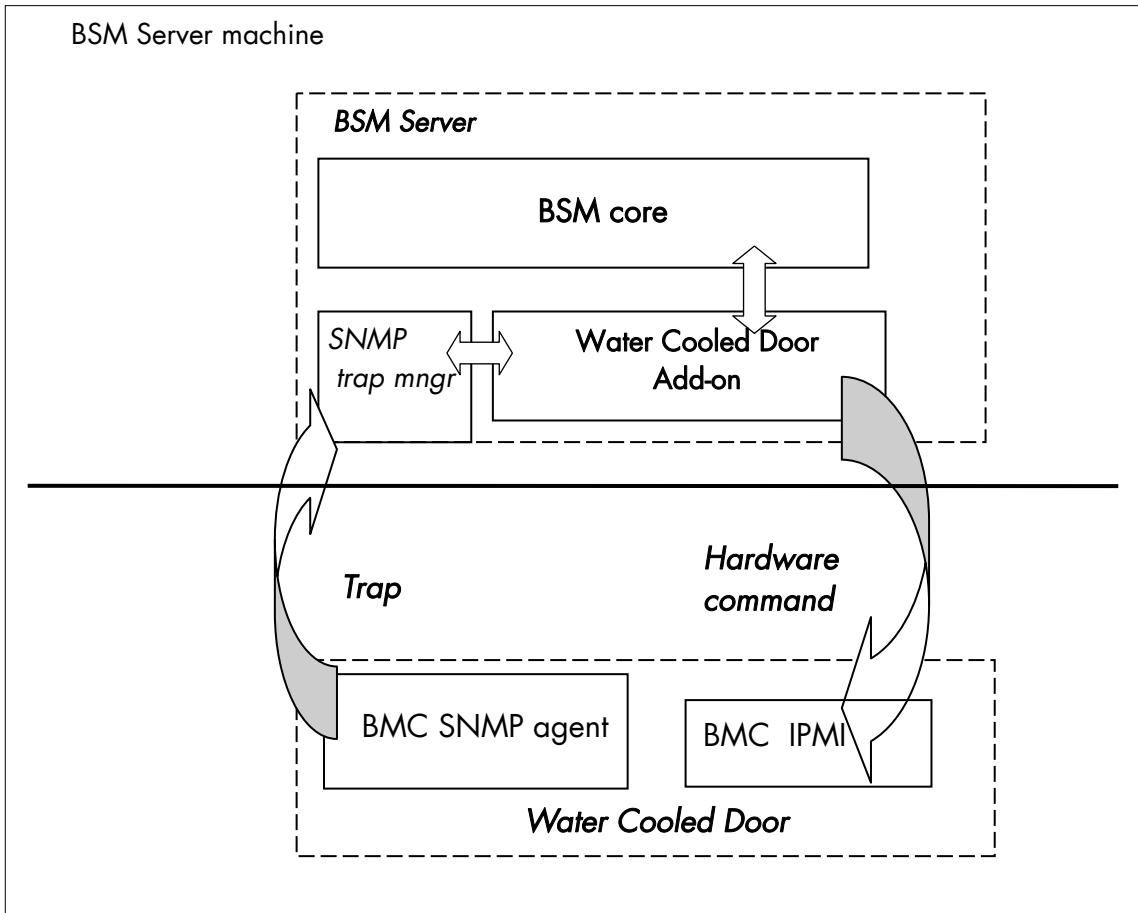


Figure 3-9. Water Cooled Door Monitoring Components

### 3.3.1.1 Default Categories & Services (independent of OS type)

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

Table 3-10. Default Water Cooled Door monitoring services

### 3.3.1.2 Optional Categories & Services (independent of OS type)

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

Table 3-11. Optional Water Cooled Door monitoring services

---

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

---

### 3.3.1.3 Hardware Category

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

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

---

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

---

### 3.3.1.4 Power Category

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

### 3.3.1.5 Sensors Category

- CurrentPower** For WaterCooledDoor hosts managed via IPMI Hardware commands. This service checks the power consumption of the WaterCooledDoor reported by the BMC.
- DeltaPressure** For WaterCooledDoor hosts managed via IPMI Hardware commands. This service checks the in/out pressure difference of the water circuit of the WaterCooledDoor reported by the BMC.
- TemperatureAverage** For WaterCooledDoor hosts managed via IPMI Hardware commands. This service checks the temperature average of the different temperature sensors of the WaterCooledDoor reported by the BMC.
- ValveAperture** For WaterCooledDoor hosts managed via IPMI Hardware commands. This service checks the cooled water circuit valve aperture reported by the BMC.
- OutputTemperature** For WaterCooledDoor hosts managed via IPMI Hardware commands. This service checks one of the external temperature sensors of the WaterCooledDoor reported by the BMC.
- FanSpeed** For WaterCooledDoor hosts managed via IPMI Hardware commands. This service checks the speed of one upon several fans reported by the BMC.

---

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

---

### 3.3.1.6 Reporting Indicators

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

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

#### Indicators applied to the WaterCooledDoor Host

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

### Optional Indicators applied to the WaterCooledDoor Host

Indicator	Corresponding Service
<WaterCooledDoor_host>_FanSpeed (RPM)	Sensors.FanSpeed
<WaterCooledDoor_host>_OutputTemperature (degrees C)	Sensors.OutputTemperature

#### 3.3.1.7 Nagios check commands

##### check\_IPMI\_powerstatus (any OS) Nagios command

The Bull System Manager service check command syntax is:

```
check_IPMILAN_powerstatus
```

See the **check\_IPMI\_powerstatus** command in *Chapter 4* for details.

##### check\_pressure (any OS) Nagios command

The Bull System Manager service check command syntax is:

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

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

##### check\_IPMI\_sensor (any OS) Nagios command

The configurable Bull System Manager service check command syntax is:

```
check_sensor!<sensor>
```

See the **check\_sensor** command in *Chapter 4* for parameter details.

#### 3.3.1.8 Bull System Manager Configuration

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

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

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

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

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

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

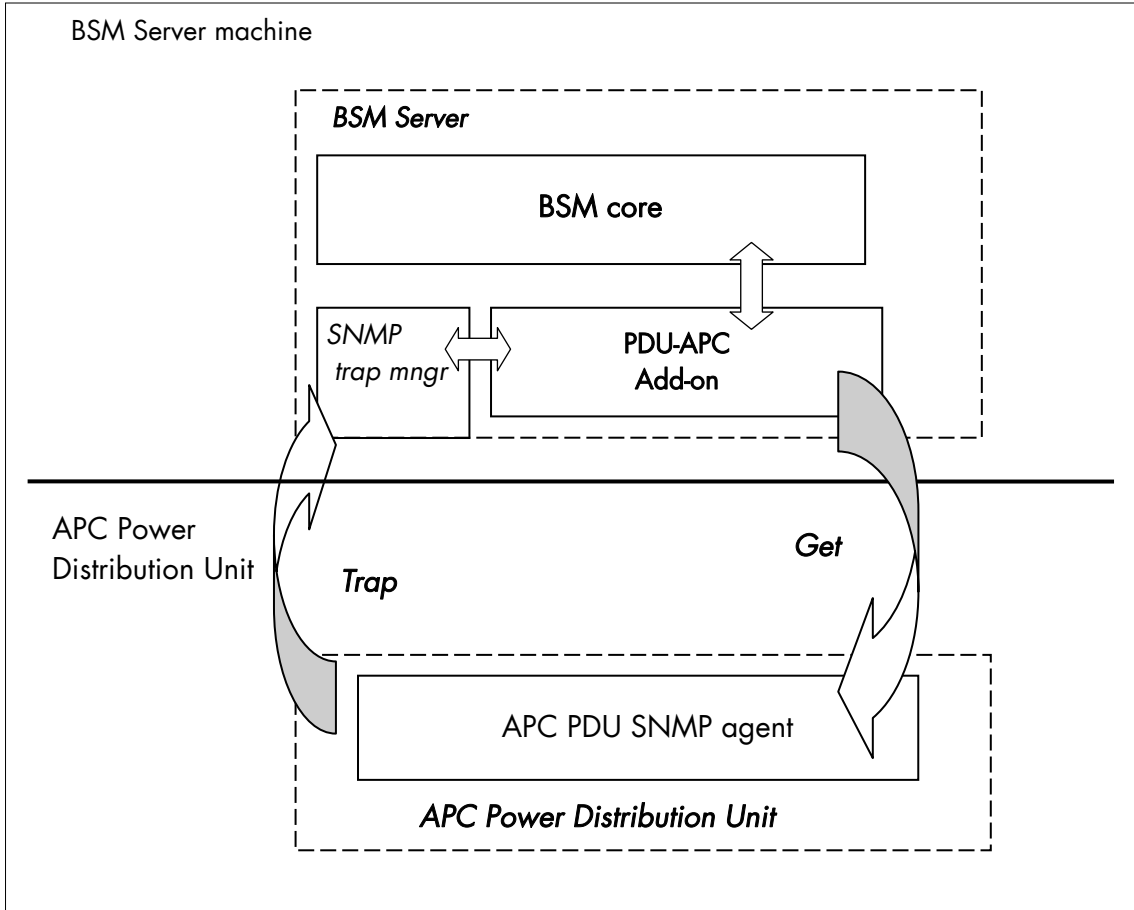


Figure 3-10 APC Power Distribution Unit Monitoring Components

#### 3.3.2.1 Default Categories & Services (independent of OS type)

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

Table 3-12. Default APC Power Distribution Unit monitoring services

---

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

---

### 3.3.2.2 PDUAPC Category

- Alerts** For APC PDU hosts. When an alert is sent from the APC PDU SNMP agent, it is processed by the Bull System Manager Server.
- Status** For APC PDU hosts managed via its SNMP agent. This service checks the APC PDU power supplies status reported by the SNMP agent.

---

**Notes** The **powernet398.mib** file are integrated in the Bull System Manager application. The trap severity SEVERE was changed to CRITICAL

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

---

### 3.3.2.3 Power Category

- Consumption** For APC PDU hosts managed via SNMP agents. This service checks the global power consumption (in Watts) for each APC PDU.
- Outlets** For APC PDU hosts managed via SNMP agents. This service checks each APC PDU outlet status reported by the SNMP agent.

### 3.3.2.4 Performance Indicators

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

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

Indicators	Corresponding Service
watts	Power.Consumption

Table 3-13. Performance Indicators applied to the APC PDU Host

### 3.3.2.5 Nagios check commands

check\_PDUAPC (any OS) Nagios command

The Bull System Manager service check command syntax is:

```
check_PDUAPC!<action>!
```

Values available for <action> are:

- Status
- Consumption
- Outlets

See the **check\_PDUAPC** command in *Chapter 4* for parameter details.

For HOSTADDRESS, SNMP community and SNMP port parameters, the Nagios macros \$HOSTADDRESS\$, \$\_HOSTSNMP\_COMMUNITY\$ and \$\_HOSTSNMP\_PORT\$ are used.

### 3.3.2.6 Bull System Manager Configuration

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

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

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

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



### 3.3.3 BSM iPDU (intelligent Power Distribution Unit Management)

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

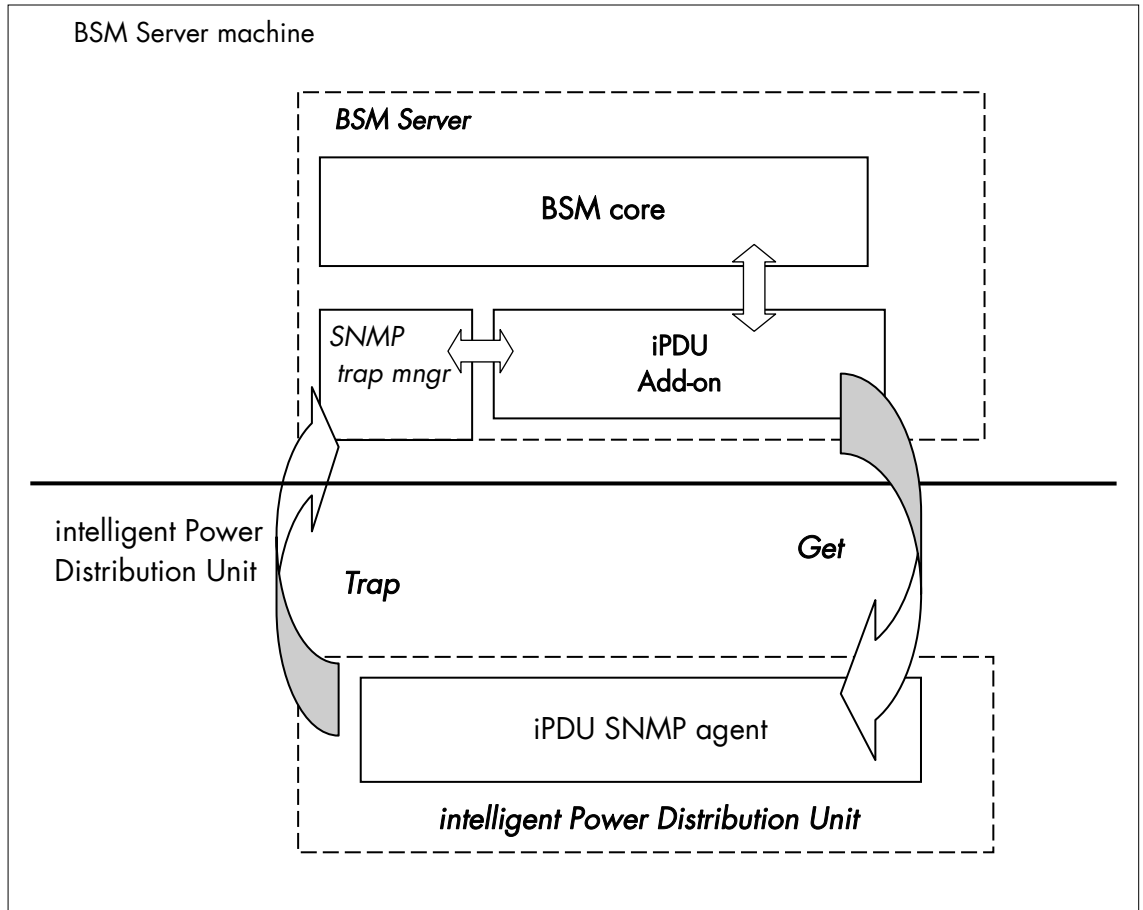


Figure 3-11 intelligent Power Distribution Unit Monitoring Components

#### 3.3.3.1 Default Categories & Services (independent of OS type)

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

Table 3-14. Default intelligent Power Distribution Unit monitoring services

### 3.3.3.2 Optional Services (independent of OS type)

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

Table 3-15. Optional intelligent Power Distribution Unit monitoring services

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

### 3.3.3.3 IPDU Category

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

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

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

### 3.3.3.4 Power Category

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

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

#### Optional services

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

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

### 3.3.3.5 Environment Category

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

### Optional services

#### Humidity

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

### 3.3.3.6 Performance Indicators

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

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

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

Table 3-16. Performance Indicators applied to the IPDU Host

### 3.3.3.7 Nagios check commands

`check_IPDU` (any OS) Nagios command

The Bull System Manager service check command syntax is:

```
check_IPDU!<action>!<timeout>
```

Values available for <action> are:

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

See the `check_IPDU` command in *Chapter 4* for parameter details.

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

### 3.3.3.8 Bull System Manager Configuration

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

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

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

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

## 3.4 Virtualization Server Add-ons

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

### 3.4.1 Overview

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

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


#### 3.4.1.1 Definitions

Virtualization Add-ons use specific topology elements:

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

#### 3.4.1.2 Topology Representation

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

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

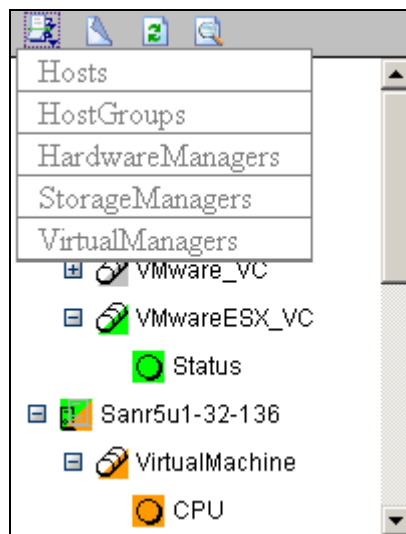



Figure 3-12. BSM Console Views

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

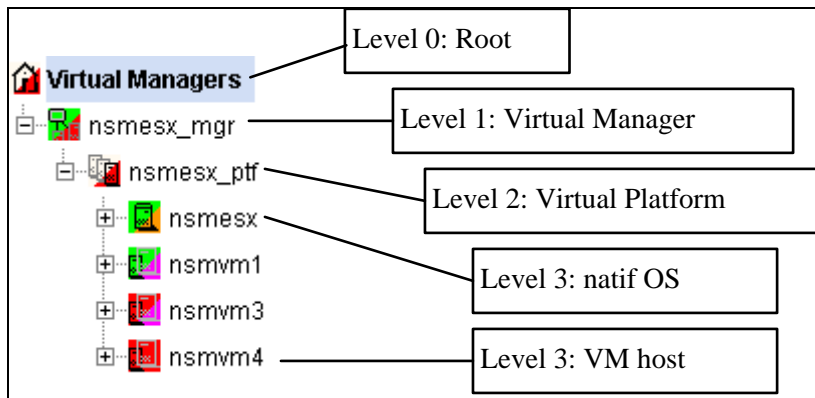


Figure 3-13. Virtual Managers view

Under the root node, the first node is the Virtual Manager that administrates the Virtual Platform. The Virtual Platform contains the native host and the VM hosts.

When you select a node, information about the elements are displayed in the Application Window.

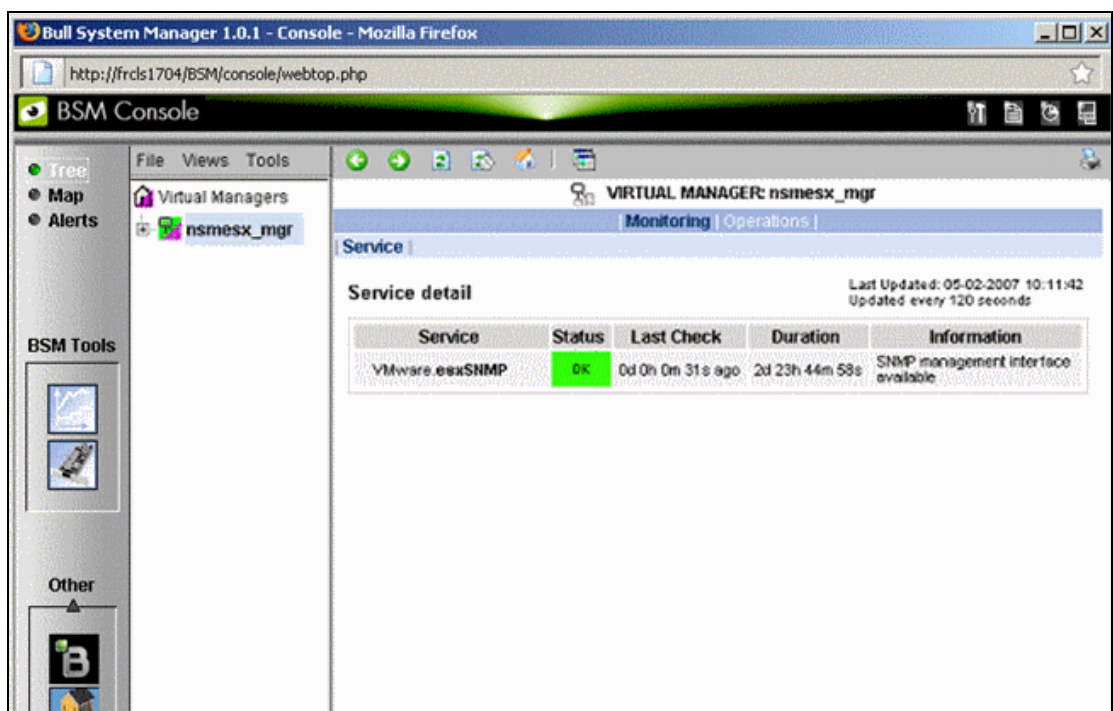


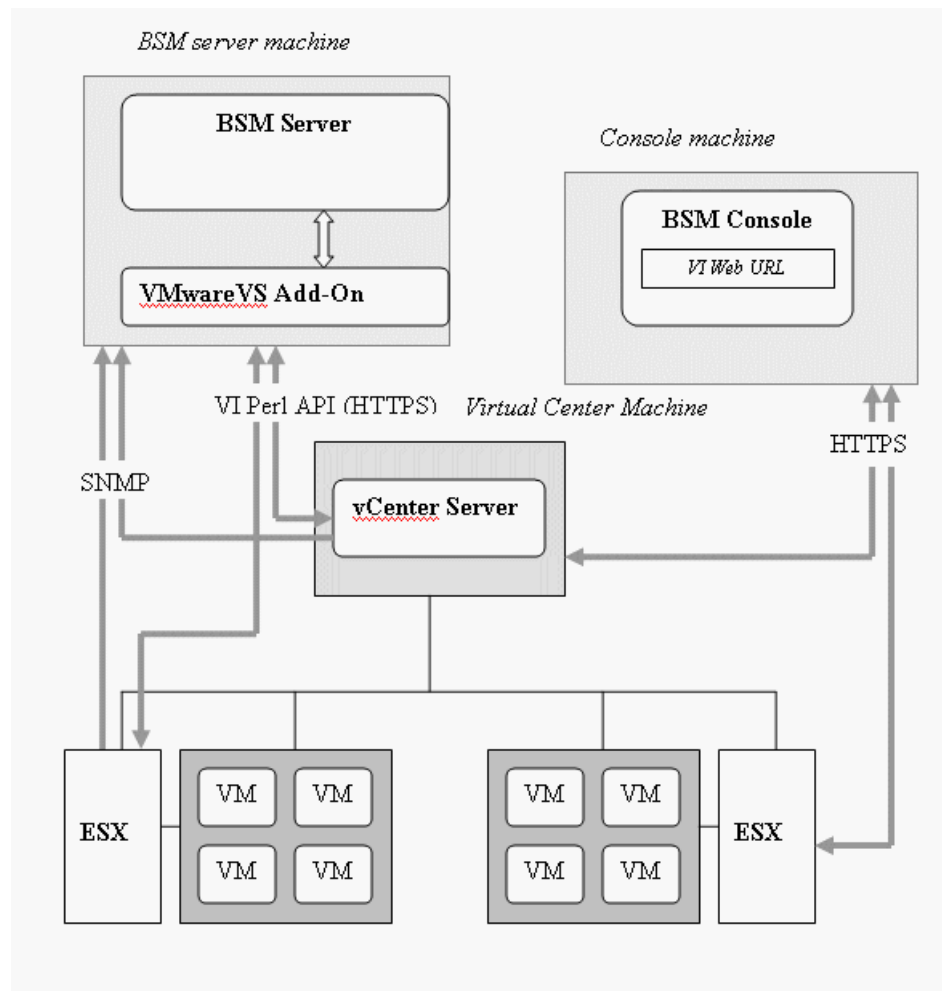
Figure 3-14. Virtual Manager Monitoring Window

### 3.4.2 BSMVMwareVS for managing VMware vSphere

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

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

The following figure shows links between each component:





important

The VMwareVS add-on replaces VMwareESX and VMwareVC Add-ons.

Migration from VMwareVC to VMwareVS can be done automatically with special installation.

Migration from VMwareESX to VMwareVS also requires manual operation.

For details, see section 3.4.2.7 *Migrating VMwareVC or VMwareESX to VMwareVS* on page 70.

The VM and ESX elements can be monitored from an ESX server or from a vCenter application. When elements are monitored from an ESX server, they are grouped in a single BSM platform (ESX Virtual Platform).

When elements are monitored from a vCenter, they are grouped in several platforms (VMware Datacenter Platform), depending of the VMware Datacenters configuration.

Each ESX server is represented by a BSM host with the OS: **ESX**.

Each VM is represented by a BSM host with the model: **VMware**.

### 3.4.2.1 Configuring ESX Virtual Platform

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

**ESX Virtualization Platforms**

[Help on ESX](#)

**New**

platform	server	description	host name	virtual name	network name	OS
<a href="#">nsmesx_ptf</a>	<a href="#">nsmesx_esx</a>	VMware ESX Virtualization platform	<a href="#">sles10_esx</a>	sles10	172.31.50.61	other
			<a href="#">rh54_esx</a>	rh54	172.31.50.60	other

Figure 3-15. ESX Virtual Platforms page

It is possible:

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

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



Figure 3-16. ESX Platform Properties

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

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

### ESX Server Host Properties

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

### Virtual Machines Properties

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

---

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

---

### Virtual Machines Discovered

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

- The left column allows you to select the VMs to be associated to the platform.
- The center part displays Virtual Machine Configuration as defined on the VMware ESX server.

- The right part allows you to edit the main properties (name, network name and OS) of the corresponding BSM host. The host can be edited only if the corresponding VM is selected. You can select a host, already defined, by clicking the **Select** button or you can create a host by completing the corresponding fields.

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

ESX Virtual Machines		Bull System Manager Configuration		
	Name	Name	netName	OS
<input checked="" type="checkbox"/>	sles10	sles10_esx	172.31.50.61	other
<input checked="" type="checkbox"/>	rh54	rh54_esx	172.31.50.60	other

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

Figure 3-17. ESX Virtual Machines pane

### Virtual Machines Re-Discovered

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

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

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

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

**Note** How to Add, Delete or Modify Virtual Machine is detailed in § 3.4.2.2 *Editing Virtual Machine Set-up*, on page 56.

When the configuration has been edited:

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

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

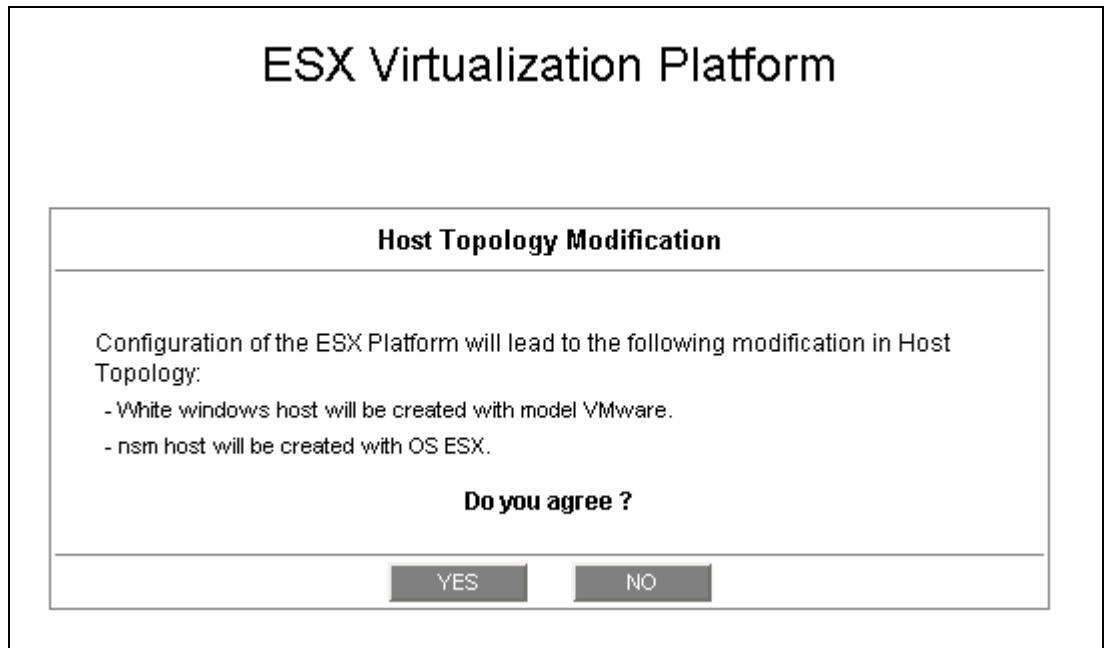


Figure 3-18. Host Topology modification confirmation screen

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

### Related ESX Virtualization platform Objects

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

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

### 3.4.2.2 Editing Virtual Machine Set-up

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

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

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

#### Adding a virtual machine to a platform

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

---

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

---

#### Removing a virtual machine from a platform

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

---

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

---

#### Modifying a virtual machine defined in a platform

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

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

---

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

---

#### Deleting all virtual machines and corresponding hosts.

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

### 3.4.2.3 Configuring vCenter managed Datacenter Platforms

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

## VMware DataCenter Platforms

[Help on DataCenter](#)

New

Datacenter	Type	Host name	description	Manager
DC2	VM	<a href="#">rhel5</a>	VM host (automatically generated with DC2 VMware DataCenter Platform)	VC1
		<a href="#">sles10</a>	VM host (automatically generated with DC2 VMware DataCenter Platform)	
	ESX	<a href="#">vmx</a>	VM host (associated to DC2 VMware DataCenter Platform)	
DC1	VM	<a href="#">rhel6</a>	VM host (automatically generated with DC1 VMware DataCenter Platform)	VC1
		<a href="#">sles9</a>	VM host (automatically generated with DC1 VMware DataCenter Platform)	
	ESX	<a href="#">esx1</a>	ESX server (automatically generated with DC1 VMware DataCenter Platform)	

Figure 3-19. VMware DataCenter Platforms page

It is possible:

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

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

Virtual Center Properties	
name	<input type="text"/>
description	VMware Virtual Center
network name	<input type="text"/>
user	<input type="text"/>
password	<input type="password"/> confirm <input type="password"/>
VMware Datacenters	
<input type="button" value="Discover"/>	To get the list of elements (VM, ESX) for each Datacenters, click the Discover button

Figure 3-20. Virtual Center Properties

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

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

### Virtual Center Properties

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

## Datcenters Properties

### Datcenters

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

See below the complete description of the procedure.

## DatataCenters Discovery

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

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

---

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

---

Virtual Center Properties				
name	VC1			
description	VMware Virtual Center			
network name	129.182.6.105			
user	Administrateur			
password	••••	confirm	••••	
VMware Datacenters				
<p>Expand Datacenter and select elements (VM, ESX) to be supervised in BSM by clicking the corresponding checkbox. Then, map each element to a defined Bull System Manager host or choose to create a new. You can also change the BSM label of the platform corresponding to the Datacenter</p>				
Datacenter DC2				
Platform name		DC2		
<input checked="" type="checkbox"/>	Virtual Center VMs	Bull System Manager Hosts		
	Name	Host name	netName	OS
<input checked="" type="checkbox"/>	rhel5	rhel5 <input type="button" value="Select"/>	rhel5	other ▼
<input checked="" type="checkbox"/>	sles10	sles10 <input type="button" value="Select"/>	sles10	other ▼
<input checked="" type="checkbox"/>	vmx	vmx <input type="button" value="Select"/>	10.10.10.10	other ▼
<input checked="" type="checkbox"/>	Virtual Center ESXs	Bull System Manager Hosts		
	Name	Host name	netName	OS
<input checked="" type="checkbox"/>	172.31.50.55	172.31.50.55 <input type="button" value="Select"/>	172.31.50.55	ESX ▼
Datacenter DC1				
Platform name		DC1		
<input checked="" type="checkbox"/>	Virtual Center VMs	Bull System Manager Hosts		
	Name	Host name	netName	OS
<input checked="" type="checkbox"/>	rhel6	rhel6 <input type="button" value="Select"/>	rhel6	other ▼
<input checked="" type="checkbox"/>	sles9	sles9 <input type="button" value="Select"/>	sles9	other ▼
<input checked="" type="checkbox"/>	Virtual Center ESXs	Bull System Manager Hosts		
	Name	Host name	netName	OS
<input checked="" type="checkbox"/>	esx1	esx1 <input type="button" value="Select"/>	esx1	ESX ▼
<input type="button" value="Re-discover"/>	To update the list of elements( VM, ESX), click the Re-discover button			

Figure 3-21. Datacenters panel

## Datacenters Re-Discovery

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

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

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

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

**VMware Datacenters**

Expand Datacenter and select elements (VM, ESX) to be supervised in BSM by clicking the corresponding checkbox. Then, map each element to a defined Bull System Manager host or choose to create a new. You can also change the BSM label of the platform corresponding to the Datacenter

**Datacenter DC2**

Platform name: DC2

Virtual Center VMs		Bull System Manager Hosts		
	Name	Host name	netName	OS
<input type="checkbox"/>	rhel5	rhel5 <input type="button" value="Select"/>	rhel5	other
<input checked="" type="checkbox"/>	sles10	sles10 <input type="button" value="Select"/>	sles10	other
<input type="checkbox"/>	rhel4	rhel4 <input type="button" value="Select"/>	rhel4	other
<input type="checkbox"/>	vmx	vmx <input type="button" value="Select"/>	10.10.10.10	other

Virtual Center ESXs		Bull System Manager Hosts		
	Name	Host name	netName	OS
<input checked="" type="checkbox"/>	172.31.50.55	172.31.50.55 <input type="button" value="Select"/>	172.31.50.55	ESX

**Datacenter DC1**

To update the list of elements( VM, ESX), click the Re-discover button

**Note** How to Add, Delete or Modify Datacenter elements is detailed in *Configuring Datacenter Element*, on page 62.

When the Datacenter elements have been edited:

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

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



### Host Topology Modification

DC2 platform created, used to represent datacenter DC2.

- rhel5 host created, used to represent rhel5 VM element.
- sles10 host created, used to represent sles10 VM element.
- 172.31.50.55 host created, used to represent 172.31.50.55 ESX element.

DC1 platform elements modified (datacenter DC1).

- rhel6 host created, used to represent rhel6 VM element.

**Do you agree ?**

YES
NO

Figure 3-22. Topology modification confirmation

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

### Related Datacenters platform Objects

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

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

---

**Note** No link between an ESX and a VM machine is configured, due to the vMotion functionality.

---

### 3.4.2.4 Configuring Datacenter Elements

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

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

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

#### Add an element (VM or ESX) to a datacenter

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

---

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

---

#### Remove an element from a datacenter

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

---

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

---

#### Modify an element defined in a datacenter

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

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

---

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

---

#### Delete all elements and corresponding hosts.

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

### 3.4.2.5 Supervising Virtualization

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

## Monitoring Services

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

### Services Applied to the ESX hosts (category VMwareESX)

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

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

### Services Applied to the VM Host (category VirtualMachine)

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

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

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

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

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

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

### 3.4.2.6 Nagios Check Commands

#### check\_esx\_vsphere

The configurable Bull System Manager service check command syntax is:

```
check_esx_vsphere
```

No parameter must be set.

#### check\_esxstat\_vsphere

The configurable Bull System Manager service check command syntax is:

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

See the **check\_vsphere.pl** command examples in *Section 4.3.1* for parameter details.

#### check\_esxcpu\_vsphere

The configurable Bull System Manager service check command syntax is:

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

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

See the **check\_vsphere.pl** command examples in *Section 4.3.1* for parameter details.

#### check\_esxmem\_vsphere

The configurable Bull System Manager service check command syntax is:

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

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

See the **check\_vsphere.pl** command examples in *Section 4.3.1* for parameter details.

#### check\_esxnet\_vsphere

The configurable Bull System Manager service check command syntax is:

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

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

---

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

---

See the **check\_vsphere.pl** command examples in *Section 4.3.1* for parameter details.

#### check\_esxio\_vsphere

The configurable Bull System Manager service check command syntax is:

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

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

---

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

---

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

### `check_vm_vsphere`

The configurable Bull System Manager service check command syntax is:

```
check_vm_vsphere
```

No parameter must be set.

### `check_vmstat_vsphere`

The configurable Bull System Manager service check command syntax is:

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

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

### `check_vmcpu_vsphere`

The configurable Bull System Manager service check command syntax is:

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

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

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

### `check_vmmem_vsphere`

The configurable Bull System Manager service check command syntax is:

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

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

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

### `check_vmnet_vsphere`

The configurable Bull System Manager service check command syntax is:

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

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

---

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

---

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

### `check_vmio_vsphere`

The configurable Bull System Manager service check command syntax is:

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

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

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

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

### Collect task

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

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

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

Properties	
name	collectDataVMware
description	periodic task to collect data from vSphere element (required by vSp
period	*/* * * * *
enable	<input checked="" type="radio"/> Yes <input type="radio"/> No
Command description	
command	/opt/BSMServer/engine/bin/collectVMvSphere.sh

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

### Reporting Indicators

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

### Indicators Applied to the ESX Host

Indicator	Corresponding Service
CPU_usage (%)	VMwareESX.CPU
Memory_usage (%)	VMwareESX.Memory
Memory_Active (Kb)	
Memory_Consumed (Kb)	
Memory_Granted (Kb)	
Memory_Balloon (Kb)	
Memory_Swap_(Kb)	
Used,Memory (Kb)	
Shared Common (Kb)	

Disk_usage (Mb/s)	VMwareESX.Disk
Disk_Read_Rate (Mb/s)	
Disk_Write_Rate (Mb/s)	
Disk_Commands_Issued (cmd/s)	
Disk_Read_Requests (cmd/s)	
Disk_Write_Requests (cmd/s)	
Network_usage (Kb/s)	VMwareESX.Network
Network_Data_Transmit_Rate (Kb/s)	
Network_Data_Received_Rate (Kb/s)	

### Indicators Applied to the VM Host

Indicator	Corresponding Service
CPU_usage (%)	VirtualMachine.CPU
CPU_Used (ms)	
CPU_Ready (ms)	
CPU_Wait (ms)	
CPU_Idle (ms)	
CPU_System (ms)	
Memory_usage (%)	VirtualMachine.Memory
Memory_Active (Kb)	
Memory_Consumed (Kb)	
Memory_Granted (Kb)	
Memory_Balloon (Kb)	

Indicator	Corresponding Service
Disk_usage (Mb/s)	VirtualMachine.Disk
Disk_Read_Rate (Mb/s)	
Disk_Write_Rate (Mb/s)	
Disk_Commands_Issued (cmd/s)	
Disk_Read_Requests (cmd/s)	
Disk_Write_Requests (cmd/s)	
Network_usage (Kb/s)	VirtualMachine.Network
Network_Data_Transmit_Rate (Kb/s)	
Network_Data_Received_Rate (Kb/s)	

---

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

---

### Bull System Manager Console

#### VMware Operation

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

**Operation → Application → VMware Virtual Infrastructure Web Access**

#### VMware Monitoring

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

From the hosts element, you can display information related to the associated service by selecting **Monitoring** menus.

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



Host Selection	All	Problems	Up	Down	Unreachable	Pending	
	2	0	2	0	0	0	
Selected Host Services	All	Problems	Ok	Warning	Unknown	Critical	Pending
	19	1	15	1	0	0	3

Click status links to display the selected hosts and services

### Service details

Last Updated: 25-11-2010 14:23:11  
Updated every 120 seconds

Host	Service	Status	Last Check	Duration	Information
nsmesx_esx	<a href="#">VMware Alerts</a>	PENDING	0d 2h 24m 21s+ ago	0d 2h 24m 21s+	Service is not scheduled to be checked...
	<a href="#">VMwareESX CPU</a>	OK	0d 0h 1m 41s ago	0d 2h 21m 41s	nsmesx.fr.cl.bull.fr: CPU Usage (Average) = 8.96 (sampling period 20 s)
	<a href="#">VMwareESX Disk</a>	OK	0d 0h 1m 12s ago	0d 2h 21m 12s	nsmesx.fr.cl.bull.fr: Disk Usage (Average) = 2.44 (sampling period 20 s)
	<a href="#">VMwareESX Memory</a>	OK	0d 0h 0m 2s ago	0d 2h 20m 2s	nsmesx.fr.cl.bull.fr: Memory Usage (Average) = 36.73 (sampling period 20 s)
	<a href="#">VMwareESX Network</a>	OK	0d 0h 8m 52s ago	0d 2h 18m 52s	nsmesx.fr.cl.bull.fr: Network Usage (Average) = 0.22 (sampling period 20 s)
	<a href="#">VMwareESX Status</a>	OK	0d 0h 7m 42s ago	0d 2h 17m 42s	This host is powered on and has 3 VMs
rh54_esx	<a href="#">FileSystems All</a>	OK	0d 0h 2m 46s ago	0d 3h 38m 19s	DISKS OK: all disks less than 80% utilized.
	<a href="#">HDisks SMARTstatus</a>	OK	0d 0h 7m 14s ago	0d 3h 37m 14s	OK: no SMART errors detected <b>/dev/sda</b> (VMware Virtual disk Version: 1.0) is not a SMART disk.
	<a href="#">LinuxServices syslogd</a>	WARNING	0d 0h 4m 17s ago	0d 3h 44m 38s	PROCS WARNING: 0 processes with command name 'syslogd'
	<a href="#">Syslog Alerts</a>	PENDING	0d 2h 24m 21s+ ago	0d 2h 24m 21s+	Service is not scheduled to be checked...
	<a href="#">Syslog AllEvents</a>	OK	0d 0h 3m 0s ago	0d 0h 13m 0s	OK - No new event found in /var/log/messages
	<a href="#">SystemLoad CPU</a>	OK	0d 0h 4m 51s ago	0d 3h 42m 28s	CPU Utilization: 8% (1mn), 8% (5mn), 8% (15mn)
	<a href="#">SystemLoad Memory</a>	OK	0d 0h 3m 32s ago	0d 3h 41m 24s	Status: OK - (total: 15907Mb) (used: 358Mb, 3%) (free: 15549Mb) (physical: 15907Mb)
	<a href="#">SystemLoad Processes</a>	OK	0d 0h 0m 1s ago	0d 3h 40m 19s	PROCS OK: 116 processes
	<a href="#">SystemLoad Users</a>	OK	0d 0h 4m 45s ago	0d 3h 39m 14s	USERS OK - 3 users currently logged in
	<a href="#">VMware Alerts</a>	PENDING	0d 2h 24m 21s+ ago	0d 2h 24m 21s+	Service is not scheduled to be checked...
	<a href="#">VirtualMachine CPU</a>	OK	0d 0h 6m 32s ago	0d 2h 26m 32s	rh54: CPU Usage (Average) = 7.15 (sampling period 20 s)
	<a href="#">VirtualMachine Memory</a>	OK	0d 0h 5m 22s ago	0d 2h 25m 22s	rh54: Memory Usage (Average) = 1.99 (sampling period 20 s)
	<a href="#">VirtualMachine Status</a>	OK	0d 0h 2m 13s ago	0d 2h 32m 13s	rh54: This virtual machine is powered on and its guest OS is running.

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

Figure 3-23. VMwareESX monitoring information

### VMware Reporting

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

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

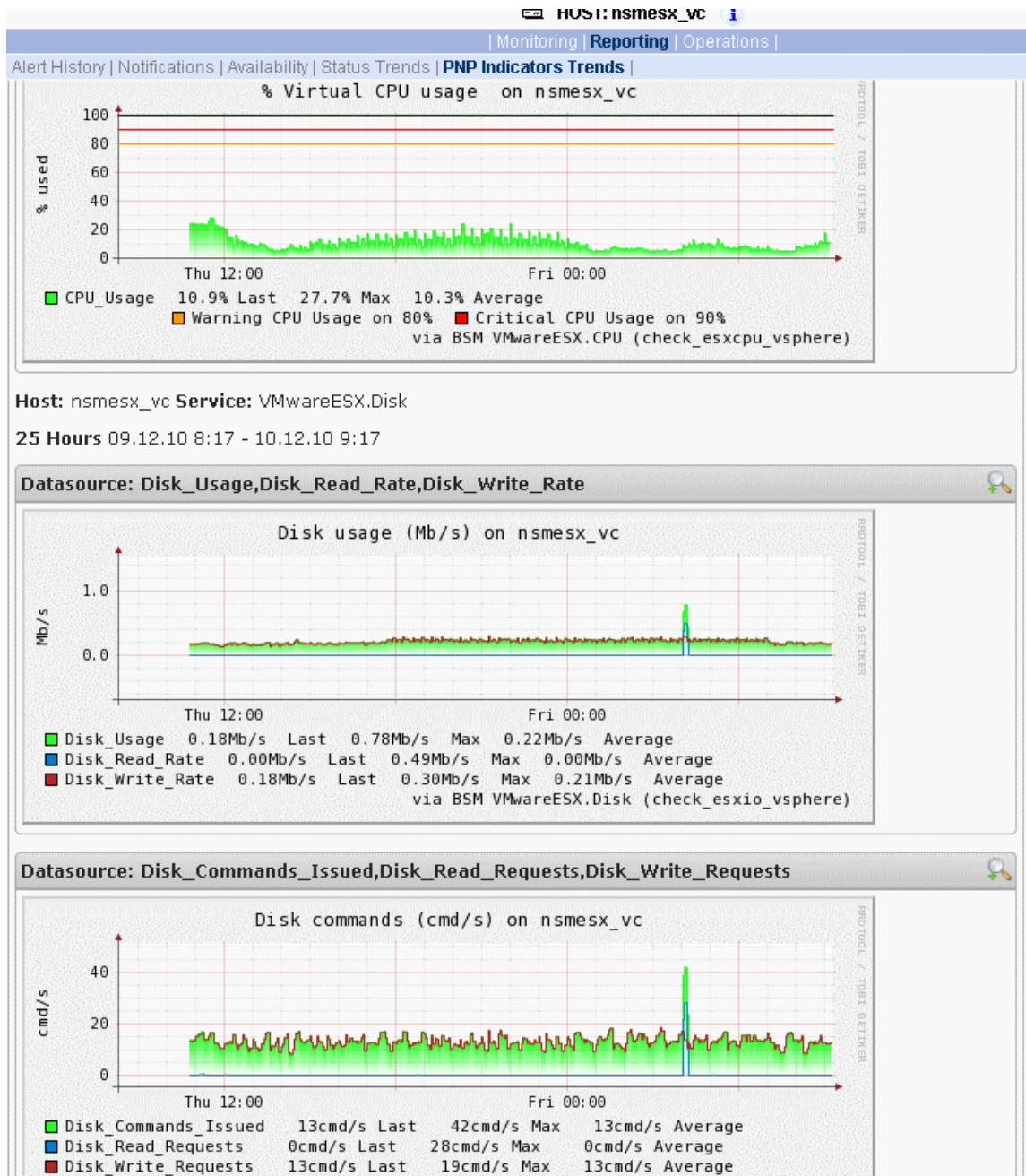


Figure 3-24. VMware reporting information

### 3.4.2.7 Migrating VMwareVC or VMwareESX to VMwareVS

#### Linux Platform installation

The VMwareVS and VMwareVC or VMwareESX Linux package contains similar files. Thus, it is not possible to perform standard installation of the VMwareVS package when the VMwareVC or VMwareESX package is installed. You must use rpm command with `--force` and `--nodeps` options:

After installing the VMwareVS package, you can remove the **VMwareVC** or **VMwareESX** package. All structures must have been preserved by the migration process.

To upgrade a **BSMVMwareESX** or **VMwareVC** Add-on to **VMwareVS**, perform the following step:

- Install the VMwareVS Add-on

```
rpm -i BSMVMwareVS-1.4-1.Bull.noarch.rpm --force --nodeps
```

- De-install VMwareESX or VMwareVC Add-ons

```
rpm -e BSMVMwareVC
```

### Windows installation

On Windows platforms, conflicts between Add-ons may occur following the installation of **VMwareVS** when **VMwareVC** or **VMwareESX** is already installed, however uninstalling VMwareVC or VMwareESX will remove files of VMwareVS add-on. Thus, after uninstalling the VMwareVC or VMwareESX Add-on, you must reinstall the VMwareVS package.

To upgrade a BSMVMwareESX or VMwareVC Add-on to VMwareVS, perform the following steps:

- Install VMwareVS Add-on
- De-install VMwareESX or VMwareVC Add-on
- Re-install VMwareVS Add-on

### Migrating VMwareVC to VMwareVS

The installation of the **VMwareVS** package keeps the topological configuration of **VMwareVC** and automatically performs the following actions:

- Remove categories and services depending from the VMwareVC Add-on
- Update categories and services depending of the VMwareVS Add-on
- Updates the collect task

### Migrating VMwareESX to VMwareVS

The installation of the **VMwareVS** package keeps the topological configuration of VMwareESX and automatically performs the following actions:

- Remove categories and services depending from the VMwareVC add-on

Due to interface evolution between ESX and the add-on, you must complete the configuration by setting complementary information for the ESX server:

- User and password must be filled in
- A re-discovery must be performed to check the user/password and to get internal information related to the ESX server.

### 3.4.3 EscalaLPAR Add-on

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

The **HMC (Hardware Management Console)** is a special-purpose system that provides management tools for controlling one or more 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 for the other partitions.

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



**Important**

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

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

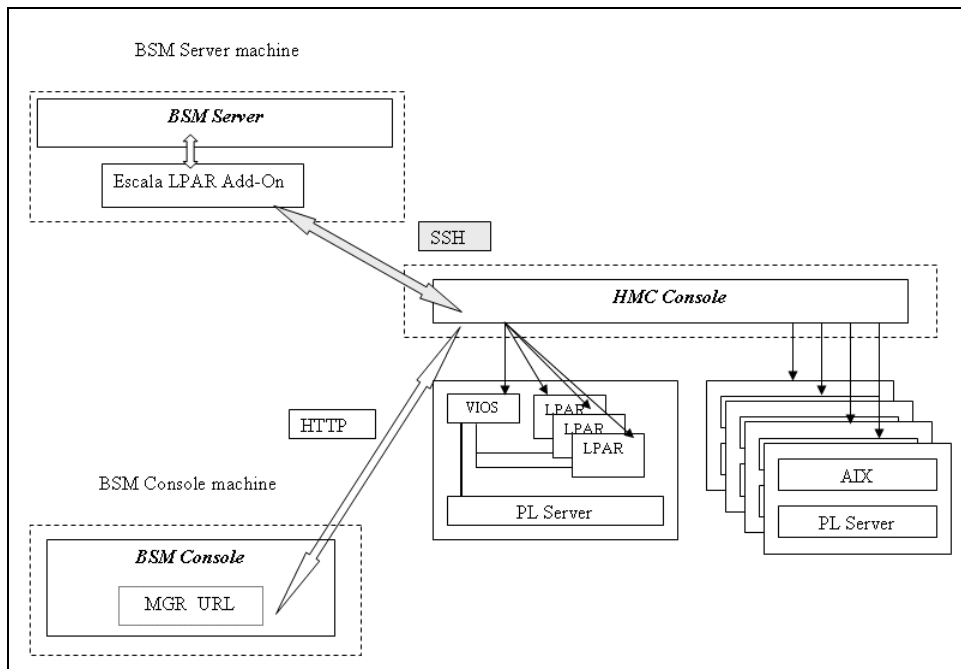


Figure 3-25. EscalaLPAR Add-on components for HMC managed systems

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

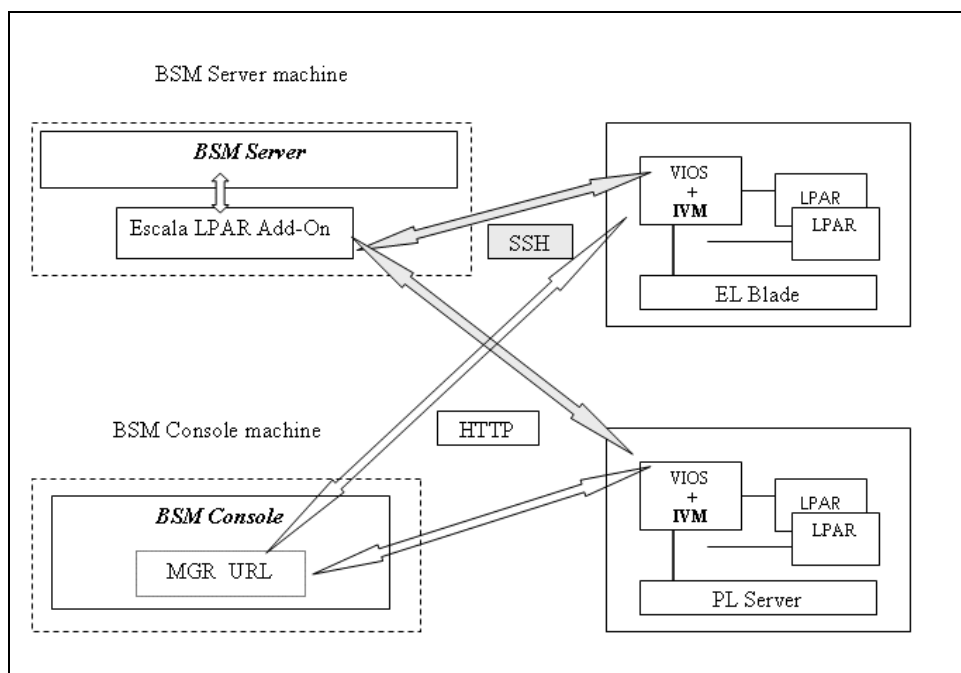


Figure 3-26. EscalaLPAR Add-on components for IVM managed systems

### 3.4.3.1 Configuring Bull System Manager

To configure the monitoring elements for the EscalaLPAR Add-on, you have to define an Escala Platform from the Bull System Manager Configuration GUI.

The definition of an Escala Platform is done in two steps:

- initialization of the Escala Server
- definition of the partitioning (LPARs)

#### 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*.

### 3.4.3.2 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** and **VIOSActivity** categories.

Service	Description	Check_command
VIOS.Status	Checks the status of the Virtual I/O server	check_vios_status
VIOS.UsedPool	Checks the utilization of the processing pool on server	check_vios_pool
VIOSActivity.UsedNPIV	Checks the utilization of NPIV on Virtual I/O Server	check_vios_used_npiv
VIOSActivity.UsedSEA	Checks the utilization of SEA on Virtual I/O Server	check_vios_used_sea

#### Monitoring Services applied to the server managed by HMC

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

Service	Description	Check_command
DefaultPool	Checks the utilization of the Default Processor Pool	ceck_cec_used_pool
SharedPool	Checks the utilization of a processor pool <sup>(a)</sup>	check_used_configured_pool

<sup>(a)</sup> The number and the name of the SharedPool services is deduced from the user defined shared 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 when the platform details are edited. 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	VIOS
name	<b>UsedPool</b>
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"> <li>mgt-admins</li> </ul> </div> <div style="text-align: center;"> <p>&lt;= Add</p> <p>Remove =&gt;</p> </div> <div> <p>All Objects</p> <ul style="list-style-type: none"> <li>mgt-admins</li> </ul> </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 3-27. 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 a service, edit it and set its **status** (Monitoring attributes part) to **inactive**.

### Reporting indicators

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

### Indicators applied to the server managed by HMC

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



### Indicators applied to the VIOs host

Indicator	Corresponding Service
CPU_usage	VirtualMachine.UsedCPU
NPIV Usage	VIOService.UsedNPIV
NPIV In for <ident>	VIOService.UsedNPIV
NPIV Out for <ident>	VIOService.UsedNPIV
SEA Usage	VIOService.UsedSEA
SEA In for <ident>	VIOService.UsedSEA
SEA Out for <ident>	VIOService.UsedSEA

### Indicators applied to the LPAR host

Indicator	Corresponding Service
CPU_usage	VirtualMachine.UsedCPU

## 3.4.3.3 Nagios Check Commands

### check\_vios\_status

The configurable BSM service check command syntax is:

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

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

### check\_vios\_used\_pool

The configurable BSM service check command syntax is:

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

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

### check\_vios\_used\_sea

The configurable BSM service check command syntax is:

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

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

---

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

---

### check\_vios\_used\_npiv

The configurable BSM service check command syntax is:

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



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

---

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

---

### `check_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 examples in *Section 4.3.2* for parameter details.

### `check_used_configured_pool`

The configurable BSM service check command syntax is:

```
check_used_configured_pool!<sharedPoolName>!<sample_time>!<warning_threshold>!<critical_threshold>
```

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

### `check_lpar_status`

The configurable BSM service check command syntax is:

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

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

### `check_lpar_used_cpu`

The configurable BSM service check command syntax is:

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

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

### 3.4.4 Bull System Manager Console

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

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

Operation → Virtualization → HMC

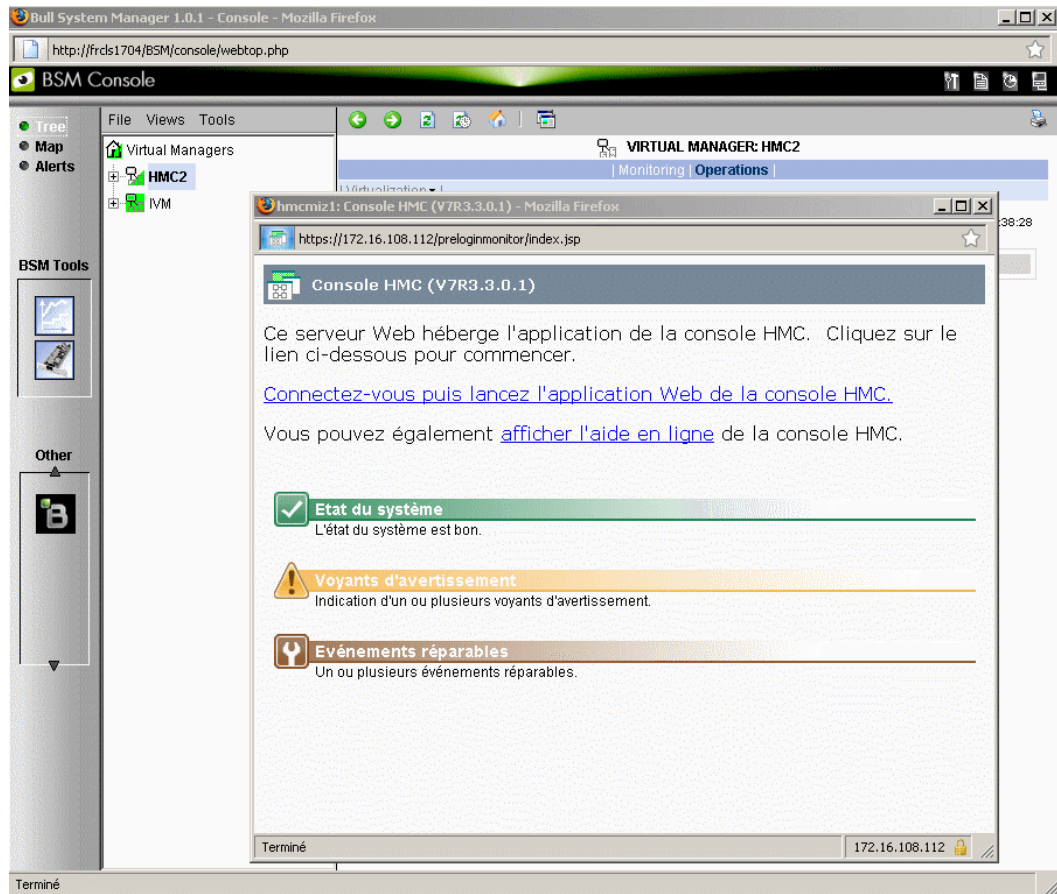


Figure 3-28. HMC activation from Bull System Manager Console

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

Operation → Virtualization → IVM

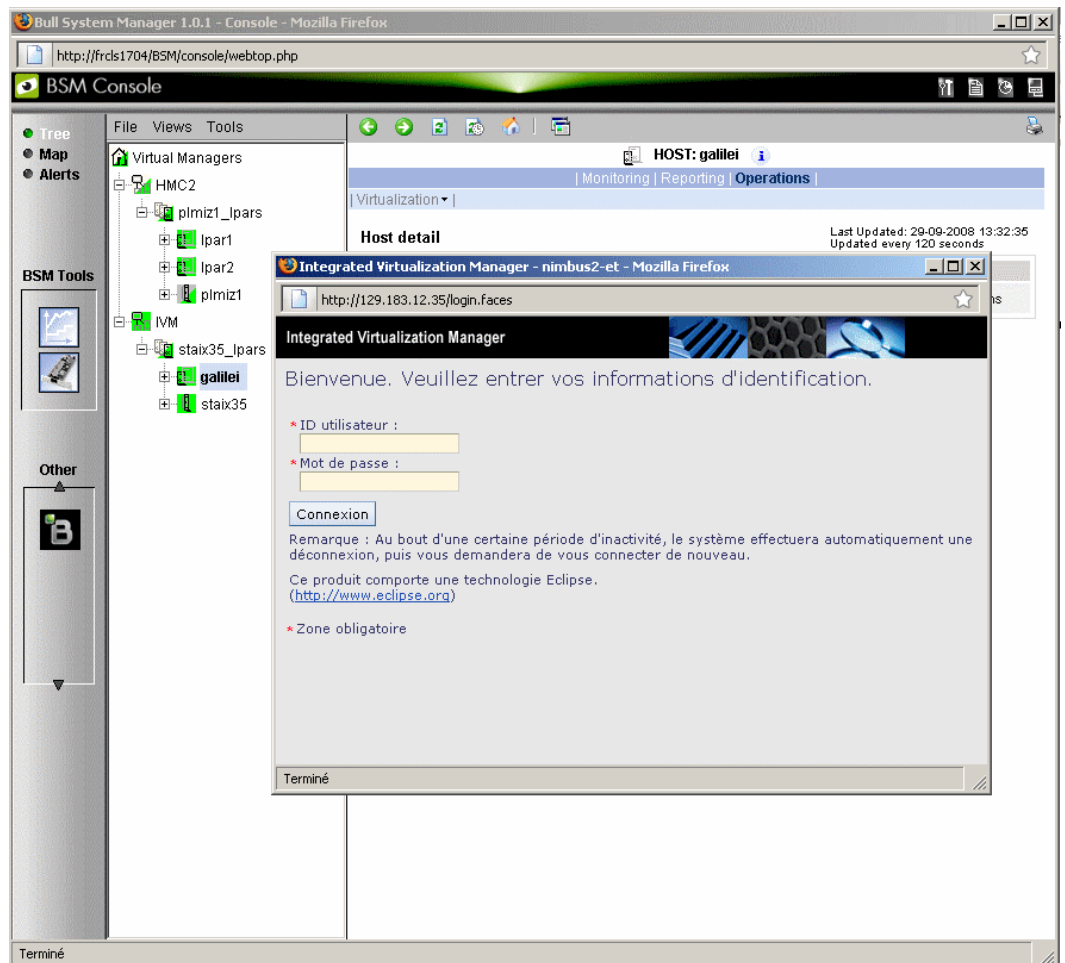


Figure 3-29. IVM activation from Bull System Manager Console

### 3.4.4.1 Escala Supervision

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

- Virtual Managers
- bsmR430F2\_mgr
- HMC SUPP
- Pool-ESP4-PL1660R\_VIRT
- Pool-ESP4-PL1660R\_VM**
- Systest-E1-700\_VIRT
- Systest-E1-700\_VM
- IVM

**VIRTUAL PLATFORM: Pool-ESP4-PL1660R\_VM**

Monitoring | Reporting

Status Overview | Status Grid | **Status Detail** | Problems

	All	Problems	Up	Down	Unreachable	Pending
Host Selection	2	0	2	0	0	0
Selected Host Services	4	0	4	0	0	0

Click status links to display the selected hosts and services

Last Updated: 10-11-2011 15:22:00  
Updated every 120 seconds

**Service details**

Host	Service	Status	Last Check	Duration	Information
sap1	VirtualMachine.Status	OK	0d 0h 2m 9s ago	2d 22h 53m 31s	Logical partition sap1 on Pool-ESP4-PL1660R (HMC 129.183.12.32) : Running
	VirtualMachine.UsedCPU	OK	0d 0h 1m 39s ago	2d 3h 39m 7s	Logical partition sap1 on Pool-ESP4-PL1660R (0.0 units entitled - HMC 129.183.12.32 - type=Shared Uncapped Partition) - processing utilization on 5 mn OK: 0.01
sap2	VirtualMachine.Status	OK	0d 0h 2m 7s ago	2d 23h 4m 24s	Logical partition sap2 on Pool-ESP4-PL1660R (HMC 129.183.12.32) : Running
	VirtualMachine.UsedCPU	OK	0d 0h 0m 45s ago	2d 3h 38m 20s	Logical partition sap2 on Pool-ESP4-PL1660R (0.0 units entitled - HMC 129.183.12.32 - type=Shared Uncapped Partition) - processing utilization on 5 mn OK: 0.01

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

Figure 3-30. HMC managed Logical Partition reported Supervision

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

- Virtual Managers
- bsmR430F2\_mgr
- HMC SUPP
- Pool-ESP4-PL1660R\_VIRT**
- Pool-ESP4-PL1660R\_VM
- Systest-E1-700\_VIRT
- Systest-E1-700\_VM
- IVM

**VIRTUAL PLATFORM: Pool-ESP4-PL1660R\_VIRT**

Monitoring | Reporting

Status Overview | Status Grid | **Status Detail** | Problems

	All	Problems	Up	Down	Unreachable	Pending
Host Selection	2	0	1	0	0	1
Selected Host Services	6	0	6	0	0	0

Click status links to display the selected hosts and services

Last Updated: 10-11-2011 15:24:14  
Updated every 120 seconds

**Service details**

Host	Service	Status	Last Check	Duration	Information
Pool-ESP4-PL1660R_POOL	ProcessorPool.DefaultPool	OK	0d 0h 3m 58s ago	2d 22h 58m 58s	Shared Processor Pool used: 0.26 / 3 Processors (HMC 129.183.12.32) - utilization on 5 mn OK: 8.52 %
	ProcessorPool.SharedPool01	OK	0d 0h 4m 27s ago	2d 22h 54m 27s	Configured Shared Processor Pool used: 0.01 / 2 Processors (HMC 129.183.12.32) - utilization on 5 mn OK: 0.32 %
VIOS4	VIOSActivity.UsedNPIV	OK	0d 0h 1m 23s ago	2d 21h 51m 9s	FIBER CHANNEL ADAPTERS (NPIV) OK: all adapters ('fcs2 - 8Gbps :0.00%' 'fcs3 - 8Gbps :0.00%') less than 70% utilized
	VIOSActivity.UsedSEA	OK	0d 0h 4m 51s ago	2d 21h 54m 51s	SHARED ETHERNET ADAPTERS (SEA) OK: all adapters ('ent4 - 100Mbps - FD:0.13%' 'ent5 - 100Mbps - FD:0.03%') less than 60% utilized
	VirtualMachine.Status	OK	0d 0h 4m 4s ago	2d 22h 59m 4s	Logical partition VIOS4 on Pool-ESP4-PL1660R (HMC 129.183.12.32) : Running
	VirtualMachine.UsedCPU	OK	0d 0h 0m 29s ago	0d 19h 16m 52s	Logical partition VIOS4 on Pool-ESP4-PL1660R (0.0 units entitled - HMC 129.183.12.32 - type=Shared Uncapped Partition) - processing utilization on 5 mn OK: 0.02

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

Figure 3-31. HMC Virtualization layer 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:

The screenshot shows the BSM Console interface for monitoring a VIRTUAL PLATFORM: staix35\_lpars. The interface includes a navigation tree on the left, a status summary table, and a detailed service table.

**Host Selection Summary:**

All	Problems	Up	Down	Unreachable	Pending
2	0	2	0	0	0

**Selected Host Services Summary:**

All	Problems	Ok	Warning	Unknown	Critical	Pending
4	0	4	0	0	0	0

**Service details** (Last Updated: 29-09-2008 13:49:25, Updated every 120 seconds)

Host	Service	Status	Last Check	Duration	Information
gallei	VirtualMachine Status	OK	0d 0h 2m 10s ago	0d 0h 37m 7s	Logical partition gallei on staix35 (IVM): Running
	VirtualMachine UsedCPU	OK	0d 0h 0m 23s ago	0d 0h 35m 26s	Logical partition gallei on staix35 (0.4 units entitled - IVM) - processing utilization on 120 min OK: 43.19 %
staix35	VIOS Status	OK	0d 0h 5m 6s ago	0d 0h 35m 1s	Virtual I/O Server state: Operating
	VIOS UsedPool	OK	0d 0h 3m 11s ago	0d 0h 38m 9s	Processing pool (1.7 / 3 units entitled) - utilization on 120 min OK: 20.67 %

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

Figure 3-32. Escala IVM reported supervision

### 3.4.4.2 Escala Reporting

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

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

## 3.5 Bull Products Server Add-ons

The following Add-ons are used for monitoring Bull Products.

### 3.5.1 DDFA

**Dynamic Domains For Applications (DDFA)** software is a tool that can be used on the Linux operating system to simulate 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>

**WARNING:** You have to verify the URL (`http://<hostname>:10000/ddomains/xml.cgi`) used by BSM nagios plug-in is trusted by the targeted webmin.

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:

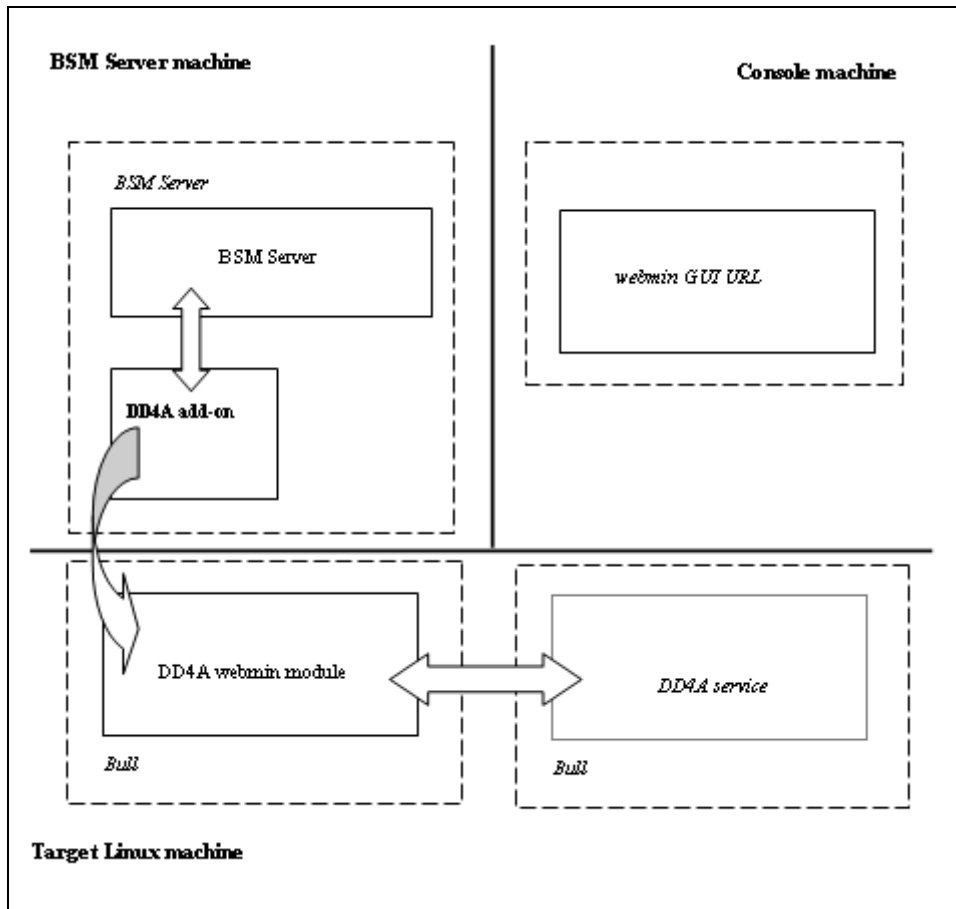


Figure 3-33. DDFA Monitoring Components

Bull System Manager Server Add-ons provide the default Bull product categories, as below.

### 3.5.1.1 Default Categories & Services Proposed for Linux Hosts

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

Table 3-17. DDF4 categories and services

### 3.5.1.2 DynamicDomains Category

#### All Services

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

---

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

---

#### default Service

For 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.

---

### 3.5.1.3 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** (the service name as defined in Nagios configuration based on the category name and service name defined in BSM configuration):

```
check_DynamicDomains!ALL
```

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

```
check_DynamicDomains!default
```





---

## Chapter 4. Check Commands for Add-on Customizable Services

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

### 4.1 Internal Storage Management Add-ons

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

#### 4.1.1 BSMGAMTT Add-on

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

##### Usage

```
check_gamtraid -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 <b>public</b> )
-p, -port <port>	SNMP port (defaults to 161)
-t, -timeout <timeout>	Seconds before timing out (defaults to <b>Nagios</b> timeout value)
-A, -adapter ALL   <Ct>	Controller board
-P, -physical ALL   <Ct>.<Ch>.<Tg>	Physical device addr
-L, -logical ALL   <Ct>.<Ldn>	Logical drive addr
-v, --verbosity <vl>	Verbosity level: 0 None 1 Adds the <CtrlModel> and the status of all controller boards filtered
-f, -format <f>	0 Carriage Return in ASCII mode (\n) 1 Carriage Return in HTML mode ( )

##### Return code

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

- OK  
All logical drives and all physical devices run normally.
- WARNING  
At least one logical drive or one physical device is in a WARNING state.
- CRITICAL  
At least one logical drive or one physical device is in a CRITICAL state.

- UNKNOWN  
All other types of processing errors (bad parameter, no response, and so on).

---

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

---

## Output

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

### global state descriptor

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

```
GAMTT RAID [CT |PD |LD ]<GlobalStatus>
"CT " if "-A".
"PD " if "-P".
"LD " if "-L".
```

### state descriptor by controller

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

The syntax is:

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

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

## Examples

- If global state is **OK**:

```
> check_gamttraid -H <host>
GAMTT RAID OK
>
> check_gamttraid -H <host> -P 0.0.1
GAMTT RAID PD OK
>
> check_gamttraid -H <host> -L 0.0
GAMTT RAID LD OK
>
> check_gamttraid -H <host> -v 1
GAMTT RAID OK
CT(Ct0) MegaRAID Ultra320-2x OK
CT(Ct1) DAC960FFX2 OK
CT(Ct2) MegaRAID Ultra320-2x OK
>
> check_gamttraid -H <host> -A 1 -v 1
GAMTT RAID CT OK
CT(Ct1) DAC960FFX2 OK
>
```
- If global state is **CRITICAL** or **WARNING**, only the elements concerned are displayed:

```
> check_gamttraid -H <host>
GAMTT RAID CRITICAL
CT(Ct0) MegaRAID Ultra320-2x CRITICAL
PD(Ct0 Ch0 Tg1) Disk Dead
>
> check_gamttraid -H <host> -L 0.1
GAMTT RAID LD CRITICAL
CT(Ct0) MegaRAID Ultra320-2x CRITICAL
LD(Ct0 Nul) RAID5 Critical
>
```
- If return code is **UNKNOWN**:

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

## 4.1.2 BSMLSICIM Add-on

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

### Usage

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

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

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

---

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

---

### Return code

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

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

---

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

---

### Output

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

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

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

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

### Examples

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

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

$ ./check_LSICIM -H 172.31.50.71 -C 'LSI SCSI1030 - 0'
> CT(0) LSI 53C1030 OK

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

## 4.1.3 BSM MegaRaidSAS Add-on

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

### Usage

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

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

## Return code

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

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

---

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

---

## Output

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

### Global state descriptor

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

```
MegaRAID SAS [CT |PD |LD ]<GlobalStatus>
"CT " if "-A".
"PD " if "-P".
"VD " if "-L".
```

### state descriptor by controller

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

The syntax is:

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

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

## Examples:

- If the global state is OK:

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

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

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

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

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

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

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

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

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

- If the return code is UNKNOWN:

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

## 4.2 External Storage Management

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

### 4.2.1 BSMStoreWayFDA

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

#### Usage

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

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

```
check_necfda -help
```

`-h, -help` Display help

```
check_necfda -version
```

`-V, -version` Display version

#### Return code

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

#### Output

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

```
necfda <GlobalStatus>
```

<GlobalStatus> Most severe state detected for a controller.

#### Examples:

- If the global state is OK

```
> check_necfda -H <host>
necfda OK
>
```
- If the global state is CRITICAL or WARNING, only the errors are displayed.
- When the return code is UNKNOWN:

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



```

> check_necfda -H <host>
necfda UNKNOWN - snmp query timed out
>
> check_necfda -H <host>
necfda UNKNOWN - no data received
>

```

## 4.2.2 BSMEmcClariion

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

### Usage

```

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

```

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

```

check_EmcClariion -help

```

```

-h, -help          Display help

```

```

check_EmcClariion -version

```

```

-V, -version       Display version

```

### Return code

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

### Output

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

```

EmcClariion <GlobalStatus>

```

<GlobalStatus> Most severe state detected for a controller.

### Examples:

- If the global state is OK
 

```

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

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

```

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

```

- When the return code is UNKNOWN:
 

```
> check_EmcClariion -H <host>
EmcClariion UNKNOWN - snmp query timed out
>
> check_EmcClariion -H <host>
EmcClariion UNKNOWN - no data received
>
```

## 4.2.3 BSMNetApp

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

### 4.2.3.1 check-netapp-cpuload

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

#### Usage

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

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

#### Return code

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

#### Output

The output shows the state in the following format:

```
CPU LOAD <Status> - <int> %
<Status>    status of the command
<int>       CPU load.
```

#### Examples:

- If the state is OK
 

```
> check_snmp -H $HOSTADDRESS$ -C public -o .1.3.6.1.4.1.789.1.2.1.3.0
-w 90 -c 95 -u '%' -l "CPU LOAD"
CPU LOAD OK - 8%
>
```
- If the global state is CRITICAL or WARNING:
 

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

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

### 4.2.3.2 check-netapp-numdisks

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

#### Usage

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

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

#### Return code

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

#### Output

The output shows the state in the following format:

```
<Status> - <int> Total Disks <int> Active <int> Spare <int> Failed
<Status>      status of the command
<int>         number of disks.
```

#### Examples:

- If the state is OK
 

```
> check_snmp -H $HOSTADDRESS$ -C public -o
.1.3.6.1.4.1.789.1.6.4.1.0,.1.3.6.1.4.1.789.1.6.4.2.0,.1.3.6.1.4.1.78
9.1.6.4.8.0,.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,.1.3.6.1.4.1.78
9.1.6.4.8.0,.1.3.6.1.4.1.789.1.6.4.7.0 -u 'Total
Disks','Active','Spare','Failed' -l ""
WARNING - 8 Total Disks 6 Active 1 Spare 1 Failed
>
```

### 4.2.3.3 check-netapp-failedfans

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

#### Usage

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

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

-C, -community <community> SNMP community string (defaults to "public")  
 -o, -oid <OID> object identifiers to query  
 -l, -label <string> prefix label for output data from plug-in  
 (default: -s 'SNMP' )

### Return code

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

### Output

The output shows the state in the following format:

Fans <Status> - < msg>

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

### Examples:

- If the state is OK
 

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

Fans OK - There are no failed fans.
>
```
- If the state is WARNING
 

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

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

## 4.2.3.4 check-netapp-failedpwr

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

### Usage

check\_snmp -H <host> -C <community> -o <OID> -l <label>

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

### Return code

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

### Output

The output shows the state in the following format:

Power <Status> - < msg>

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

### Examples:

- If the state is OK

```
> check_snmp -H $HOSTADDRESS$ -C public -o .1.3.6.1.4.1.789.1.2.4.5.0
-l "Power"
Power OK - There are no failed power supplies.
>
```
- If the state is WARNING

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

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

## 4.2.3.5      **check\_netapp\_globalstatus**

**check\_netapp\_globalstatus** uses the following shell (PERL) command options:

### Usage

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

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

```
check_NetAppGlobalStatus -help
```

```
-h, -help            Display help
```

```
check_NetAppGlobalStatus -version
```

```
-V, -version         Display version
```

### Return code

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

### Output

The output shows the global state in the following format:

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

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

## Examples

- If the global state is OK

```
> check_NetAppGlobalStatus -H <host>
OK - The system's global status is normal
>
```
- If the global state is CRITICAL or WARNING:

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

### 4.2.3.6 check\_netappvol

**check\_netappvol** uses the following shell (PERL) command options:

#### Usage

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

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

```
check_NetAppGlobalVol -help
```

```
-h, -help          Display help
```

```
check_NetAppGlobalVol -version
```

```
-V, -version       Display version
```

#### Return code

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

#### Output

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

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

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

```
<model>                  model of NetApp storage system
```

The following lines show the status of each volume

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

### Examples:

- If the global state is OK

```
> check_NetAppGlobalStatus -H <host>
NetApp FAS3020 RAID OK
Volume vol0, online (raid_dp, flexible, aggr0)
Volume BULL_TRAVAIL, online (raid_dp, flexible, BULL)
Volume luns, online (raid_dp, flexible, BULL)
Volume GORKI, online (raid_dp, flexible, aggr1)
>
```
- If the global state is CRITICAL or WARNING:

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

### 4.2.3.7 check\_netappraid

`check_netappraid` uses the following shell (PERL) command options:

#### Usage

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

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

```
check_NetAppRaid -help
```

```
-h, -help          Display help
```

```
check_NetAppRaid -version
```

```
-V, -version       Display version
```

#### Return code

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

#### Output

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

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

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

The following lines show the status of each RAID group

```
RAID group <name> <status>
```

## Examples

- If the global Raid group state is OK

```
> check_NetAppRaid -H <host>
NetApp FAS3020 RAID OK
RAID group /aggr0/plex0/rg0 active
RAID group /BULL/plex0/rg0 active
RAID group /aggr1/plex0/rg0 active
>
```
- If the global Raid group state is CRITICAL or WARNING:

```
> check_NetAppRaid -H <host>
NetApp FAS3020 RAID WARNING
RAID group /aggr0/plex0/rg0 active
RAID group /BULL/plex0/rg0 active
RAID group /aggr1/plex0/rg0 reconstructionInProgress
>
```

## 4.2.4 BSMWaterCooledDoor

The **BSMWaterCooledDoor** Add-on uses the `check_sensor` check command that uses the following shell (PERL) command options:

### Usage

```
check_sensor [-h] -m model [-H host] [-u user] [-p password] -s sensorid
[-F factor] [-c lowercrit] [-w lowerwarn] [-W upperwarn] [-C uppercrit]
```

-h	Help
-m model	Remote host model: ipmilan
-H host	Remote host name or ipaddr
-u user	Remote SMU username
-p password	Remote SMU or MWA password
-s sensorid	Specify the sensor id string
-F factor	Specify the factor to apply to the reading value
-c lowercrit	Specify the sensor lower critical level
-w lowerwarn	Specify the sensor lower warning level
-C uppercrit	Specify the sensor upper critical level
-W upperwarn	Specify the sensor upper warning level

### Return code

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

### Output

The output shows the state and the value of the sensor in the following format:

```
<sensor status> : <value>
```

### Examples

```
> check_sensor -m ipmilan -H 172.31.50.71 -u super -p pass -s 'Pwr
Consumption'
OK : 142.480 Watts
>
```



```

> check_sensor -m ipmilan -H 172.31.50.71 -u super -p pass -s 'Valve
Vperture'
OK : 21.750 %
>
> check_sensor -m ipmilan -H 172.31.50.71 -u super -p pass -s 'Air
Pressure' -F 1000
OK : 19 Pa
>

check_sensor -m ipmilan -H 172.31.50.71 -u super -p pass -s 'Average
Temp.'

OK : 18.3 degrees C
>

```

## 4.2.5 BSMStoreWayDPA

The **BSMStoreWayDPA** Add-on uses the **check\_StoreWayDPA** check command that uses the following shell (PERL) command options:

### Usage

```

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

```

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

```

check_StoreWayDPA -help

```

```

-h, -help          Display help

```

```

check_StoreWayDPA -version

```

```

-V, -version       Display version

```

### Return code

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

### Output

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

```

StoreWay DPA <TaskStatus>

```

```

<TaskStatus>      Most severe task state detected on a StoreWay DPA system.

```

## Examples

- If the task state is OK

```
> check_StoreWayDPA -H <host>
StoreWay DPA OK
>
```
- If the global state is CRITICAL, only the tasks with state stopped are displayed :

```
> check_StoreWayDPA -H <host>
StoreWay DPA CRITICAL
Backup Engine stopped
>
> check_StoreWayDPA -H <host>
StoreWay DPA CRITICAL
Task Launcher stopped
>

> check_StoreWayDPA -H <host>
StoreWay DPA CRITICAL
Backup Engine and Task Launcher stopped
>
```
- When the return code is UNKNOWN:

```
> check_StoreWayDPA -H <host>
StoreWay DPA UNKNOWN - snmp query timed out
>
> check_StoreWayDPA -H <host>
StoreWay DPA UNKNOWN - no data received
>
```

## 4.2.6 BSMSwitchBrocade

The **BSMSwitchBrocade** Add-on uses the **check\_brocade** check command with the following shell (PERL) command options:

### Usage

```
check_fcsww.pl -H <host IP address> -c <command>
```

- |              |   |
|--------------|---|
| -H <host>    | Hostname or IP address of the target to check               |
| -c <command> | specifies the type of element to be monitored               |
|              | switch : gets the monitoring state of the FC switch itself  |
|              | port : gets the monitoring state of the FC ports            |
|              | fan : gets the monitoring state of the fans                 |
|              | temp : gets the monitoring state of the temperature sensors |
| -h, -help    | displays help   |

### Return code

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

### Output

The output displays the state of the sensor.

### Examples:

- If the task state is OK

```
> check_fcsw.pl -H <host> -c switch
Global switch status is OK
>
> check_fcsw.pl -H <host> -c port
All 16 FC ports are OK
>
> check_fcsw.pl -H <host> -c temp
All 4 Temperature Sensors are OK
>
> check_fcsw.pl -H <host> -c fan
All 4 Fans are OK
>
```
- When the return code is UNKNOWN:

```
> check_fcsw.pl -H <host> -c switch
Cannot access to Switch status, Cannot access to Switch name
>
> check_fcsw.pl -H <host> -c temp
Cannot access to sensors states
>
> check_fcsw.pl -H <host> -c port
Cannot access to FC port states
>
```

## 4.2.7 BSMPDU-APC

The **BSMPDU-APC** Add-on uses the **check\_PDUAPC** check command with the following shell (PERL) command options:

### Usage

```
check_PDUAPC -H <host IP address> -s <action> [-p <port>] [-C
<community>] [-T <snmp timeout>]
```

-H <host>	Hostname or IP address of the target to check
-c <action>	Status: gets the APC PDU power supply(ies) status Consumption: gets the APC PDU power consumption (in Watts) Outlets: gets the APC PDU outlets status
-p <port>	snmp port number (default value: 161)
-C <community>	snmp community (default value: public)
-T <timeout>	snmp timeout (default value: 30 seconds)
-h, -help	displays help

### Return code

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

### Output

The output displays the APC PDU power supply(ies) state, the APC PDU global power consumption or the APC PDU outlets state.

## Examples:

- **Action Status**
  - **Return code OK:**

```
> check_PDUAPC -H 129.182.6.174 -a Status
Power Distribution Unit: 129.182.6.174, MODEL: "AP7922", Serial Nb:
"ZA0909003404", Firm Rev: "v3.5.7"
All Power Supplies OK
>
```
  - **Return code WARNING:**

```
> check_PDUAPC -H 129.182.6.174 -a Status
Power Distribution Unit: 129.182.6.174, MODEL: "AP7922", Serial Nb:
"ZA0909003404", Firm Rev: "v3.5.7"
Power Supply 1 OK, Power Supply 2 FAILED
>
```
  - **Return code CRITICAL:**

```
> check_PDUAPC -H 129.182.6.174 -a Status
Power Distribution Unit: 129.182.6.174, MODEL: "AP7922", Serial Nb:
"ZA0909003404", Firm Rev: "v3.5.7"
All Power Supplies FAILED
>
```
- **Action Consumption:**
  - **Return code OK:**

```
> check_PDUAPC -H 129.182.6.174 -a Consumption
Power OK: Reading 0 Watts
```
  - **Return code WARNING:**

```
> check_PDUAPC -H 129.182.6.174 -a Consumption
Power WARNING: Reading 6000 > Threshold 5520 Watts>
```
  - **Return code CRITICAL:**

```
> check_PDUAPC -H 129.182.6.174 -a Consumption
Power CRITICAL: Reading 8000 > Threshold 7360 Watts
>
```
- **Action Outlets:**
  - **Return code OK:**

```
> check_PDUAPC -H 129.182.6.174 -a Outlets
Power Distribution Unit: 129.182.6.174, MODEL: "AP7922", Serial Nb:
"ZA0909003404", Firm Rev: "v3.5.7"
Outlets(1 - 16) power: On(1)
>
```

```
> check_PDUAPC -H 129.182.6.174 -a Outlets
Power Distribution Unit: 129.182.6.174, MODEL: "AP7922", Serial Nb:
"ZA0909003404", Firm Rev: "v3.5.7"
Outlets(1,3,5,7,9,11,12,14,16) power: On(1)
Outlets(2,4,6,8,10,13,15) power: Off(2)
>
```
  - **Return code WARNING:**

```
> check_PDUAPC -H 129.182.6.174 -a Outlets
Power Distribution Unit: 129.182.6.174, MODEL: "AP7922", Serial Nb:
"ZA0909003404", Firm Rev: "v3.5.7"
Outlets(1 - 16) power: Off(2)
>
```

## 4.2.8 BSMIPDU

The **BSMIPDU** Add-on uses the **check\_IPDU** check command with the following shell (PERL) command options:

### Usage

```
check_IPDU -H <host IP address> -a <action> [-p <port>] [-C <community>]
[-t <snmp timeout>] [-o <outlet>]
```

-H <host>	Hostname or IP address of the target to check
-a <action>	Status : gets the IPDU global status Consumption : gets the global IPDU power consumption (in Watts) OutletsConso : gets the power consumption for one or all IPDU outlets OutletsVoltage: gets the output voltage for one or all IPDU outlets Voltage: gets the input and output voltage and frequency of the IPDU Temperature: gets the temperature of the IPDU Humidity: gets the humidity for the IPDU
-p <port>	snmp port number (default value: 161)
-C <community>	snmp community (default value: public)
-t <timeout>	snmp timeout (default value: 50 seconds)
-o <outlet>	outlet number (default value: all); available only for actions OutletsConso and OutletsVoltage
-h, -help	displays help

### Return code

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

### Output

The output displays for action Status the IPDU global state and additional information about the IPDU host, for action Consumption the IPDU global power consumption and additional metrics as performance data, for action OutletsConso the power consumption per outlet and additional metrics as performance data, for action OutletsVoltage the output voltage per outlet and additional metrics as performance data, for action Voltage the input and output voltage and frequency and additional metrics as performance data, for action Temperature the temperature of the IPDU and additional metrics as performance data and for action Humidity the humidity of the IPDU and additional metrics as performance data.

## Examples:

- **Action Status**

```
$ check_IPDU -H 172.16.113.41 -a Status
Status OK - MODEL: "IBM DPI C13 BULK", Device Firmware Version:
"0202.0008", Agent Firmware Versio: "IBM DPI V0210.0001"
INPUT Frequency: 50 Hz, Voltage: 240.4 volts, Current: 6.2 amp.
OUTPUT VA rating: 14950, frequency: 50 Hz, total power: 1352 watts,
VA: 1493 volt-amps.
>
```

- **Action Consumption:**

```
> check_IPDU -H 172.16.113.41 -a Consumption
Consumption OK - OVERALL OUTPUT: 1341 watts|totalpower=
1341watts;;;547;1782 wattshours=1346Wh;;;0;1466
>
```

- **Action OutletsConso:**

```
> check_IPDU -H 172.16.113.41 -a OutletsConso
Outlet1 ("[13] ESP4 - PL1660R") : 198 watts
Outlet2 ("[09] ESP3 - PL1660R base") : 527 watts
Outlet3 ("[19] Power7 - M6-700 base") : 529 watts
Outlet4 : 0 watts
Outlet5 ("[18] FC sta/st6") : 42 watts
Outlet6 ("[01] Citrix VDI") : 52 watts
|Outlet1-watts=198;;;0;615 Outlet1-wattshours=198;;;0;457 Outl
et2-watts=527;;;0;637 Outlet2-wattshours=527;;;0;556 Outlet3-
watts=529;;;0;958 Outlet3-wattshours=531;;;0;648 Outlet4-
watts=0;;;0;581 Outlet4-wattshours=0;;;0;146 Outlet5-watts=42;;;38;44
Outlet5-wattshours=42;;;0;43 Outlet6-watts=52;;;0;95 Outlet6-
wattshours=51;;;0;52
>
> check_IPDU -H 172.16.113.41 -a OutletsConso -o 3
Outlet3 ("[19] Power7 - M6-700 base") : 533 watts|watts=533;;;0;958
wattshours=532;;;0;648
>
```

- **Action OutletsVoltage:**

```
> check_IPDU -H 172.16.113.41 -a OutletsVoltage
Outlet1 ("[13] ESP4 - PL1660R") : 241 volts
Outlet2 ("[09] ESP3 - PL1660R base") : 241 volts
Outlet3 ("[19] Power7 - M6-700 base") : 238.8 volts
Outlet4 : 238.7 volts
Outlet5 ("[18] FC sta/st6") : 237.7 volts
Outlet6 ("[01] Citrix VDI") : 237.6 volts
|Outlet1-voltage=241;;;226.5;247.3 Outlet2-voltage=241;;;226.5;247.3
Outlet3-voltage=238.8;;;231.9;244.8 Outlet4-voltage=238.7;;;232;244.8
Outlet5-voltage=237.7;;;231;243.8 Outlet6-voltage=237.6;;;231;243.8
>
> check_IPDU -H 172.16.113.41 -a OutletsVoltage -o 3
Outlet3 ("[19] Power7 - M6-700 base") : 239.6volts
|voltage=239.6;;;231.9;244.8
>
```

- **Action Voltage:**

```
> check_IPDU -H 172.16.113.41 -a Voltage
Input Voltage: 240 volts
Input frequency: 50 Hz
Output voltage: 240 volts
Output frequency: 50 Hz
|inputVoltage=240volts;;; inputFrequency=50Hz;;;
outputVoltage=240volts;;; outputFrequency=50Hz;;;
>
```
- **Action Humidity**

```
> check_IPDU -H 172.16.113.41 -a Humidity
Humidity CRITICAL - 11%|humidity=11%;22:78;20:80;10:44
>
```
- **Action Temperature**

```
> check_IPDU -H 172.16.113.41 -a Temperature
Temperature OK - 30°C|Temperature=30C;16:32;16:32;23:42
AmbientTemperature=37C;;;29;46
>
```

## 4.3 Virtualization Management

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

### 4.3.1 BSMVMwareVS

The Nagios check commands used by **BSMVMwareVC** Add-on use the shell (PERL) `check_virtualcenter.pl` command.

#### Usage

```
check_virtualcenter.pl --server <vCenter>
                      --vmname <VM_id>
                      --hostname <ESX_id>
                      --stat <metric>
                      --crit <nb>
                      --warn <nb>
                      --indics <list of metrics>
```

where:

<code>-server &lt;vCenter&gt;</code>	Hostname or IP address of the vCenter
<code>-vmname &lt;VM_id&gt;</code>	Name of the VM (in vCenter context)
<code>-hostname &lt;ESX_id&gt;</code>	Name of the ESX host (in vCenter context)
<code>-stat &lt;tmetric&gt;</code>	Type of performance metric to check. See below for valid VMware metrics
<code>-warn &lt;nb&gt;</code>	Warning threshold for performance statistics
<code>-crit &lt;nb&gt;</code>	Critical threshold for performance statistics
<code>-indic &lt;metric list&gt;</code>	Additional performance metrics to use as reporting indicator. See below for valid VMware metrics
<code>-help</code>	Display help

Supported host's metrics:

- cpu.usage.average
- sys.resourceCpuUsage.average
- mem.usage.average
- mem.consumed.average
- mem.granted.average
- mem.vmmemctl.average
- mem.active.average
- mem.swapused.average
- mem.sharedcommon.average
- net.usage.average
- net.transmitted.average
- net.received.average
- net.droppedRx.summation
- net.packetsRx.summation
- net.droppedTx.summation
- net.packetsTx.summation
- disk.usage.average
- disk.commands.summation
- disk.numberRead.summation
- disk.numberWrite.summation



- disk.read.average
- disk.write.average
- disk.deviceLatency.average
- disk.kernellatency.average
- disk.totalLatency.average
- disk.queueLatency.average

Supported VM's metrics:

- cpu.usage.average
- cpu.used.summation
- cpu.ready.summation
- mem.usage.average
- mem.consumed.average
- mem.granted.average
- mem.vmmemctl.average
- mem.active.average
- net.usage.average
- net.transmitted.average
- net.received.average
- net.droppedRx.summation
- net.packetsRx.summation
- net.droppedTx.summation
- net.packetsTx.summation
- disk.usage.average
- disk.commands.summation
- disk.numberRead.summation
- disk.numberWrite.summation
- disk.read.average
- disk.write.average

### Return code

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

### Output

The output has the following format:

```
<VMware name>: <metric label> (<counter type>) = <value> (sampling
period <period>)
```

The VMware name is the name of the host or VM as set in vCenter or ESX

The metric label is those defined in VMware.

### Examples

#### Example 1:

```
check_vsphere.pl -server 129.182.6.57 -hostname 172.31.50.55
172.31.50.55: Nothing to report about this host.
```

The ESX status returned is determined by the vCenter server.

### Example 2:

```
check_vsphere.pl --server 129.182.6.57 -hostname 172.31.50.55 -stat mem.usage.average -crit 80 -warn 70
```

```
172.31.50.55: Memory Usage (Average) = 36.65 (sampling period 20 s)
```

The status returned is dependant on the threshold setting. In this example, the status returned is good.

### Example 3:

```
$ ./check_vsphere.pl --server 129.182.6.57 --hostname 172.31.50.55 --stat mem.usage.average --crit 90 --warn 80 --indics mem.consumed.aver>
```

```
172.31.50.55: Memory Usage (Average) = 36.65 (sampling period 20 s)|Memory_Usage=36.65%;80;90;0;100 Memory_Consumed=61493.32kb;;; Memory_Granted=62800.12kb;;;
```

Output returns also additional metrics as performance data.

## Failure case

### Example 1:

```
172.16.115.100 : information status for this host is not available (/opt/BSMServer/engine/tmp/VCcache1721611358.pm not found)has
```

This output indicates that the collect task has not started or has failed to collect information from vCenter.

Check the following:

- The task has been enabled in BSM
- The task is scheduled to run periodically (see the collectVMvCenter.log log file)
- If the failure has occurred during the collect process (see the log file vcenter.err)

### Example 2:

```
vmx: out-of-date status information (Wed Nov 4 14:35:11 2009) - vmx: This virtual machine is powered off or suspended.
```

This output indicates that the collect task has not been scheduled recently, or has failed to collect information from vCenter.

Check the following:

- The task is still enabled in BSM
- The task has been scheduled recently (see the collectVMvCenter.log log file)
- If the failure has occurred during the collect process (see the vcenter.err log file)

## 4.3.2 BSMEscalalpar

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

### Usage

```
check_NSM_escalalpar -M manager [HMC|IVM] -H <netname> -U <remote_user> -I <identity_file> [-l <lpar_name>] [-p <poolname>] [-S <hoststate>] [-i <STATUS|CPU|POOL>] [-e sample_time] [-w <warn>%] [-c <crit>%] [-N < name>] [-t timeout]
```

-M <manager>	Type of manager used to retrieve plugin information. Available value are: IVM, when the Escala is managed by an IVM installed on Vios partition, HMC, when the Escala is managed by a remote station.
-H <netname>	Hostname or IP address of the manager used for checking
-U <remote_user>	User for remote connection
-I <identity_file>	Name of the file from which the identity (private key) for RSA or DSA authentication is read. The file must be localized into the directory <BSM Installation Directory>/engine/etc/ssh. To use it as authentication file for Vios platform, you have to install the corresponding public key on the VIO server.
-N <name>	Name of the CEC or Vios LPAR (used in output of the plugin related to a given logical partition).
-l <lpar_name>	Name of the logical partition to check.
-p <poolname>	Name of the processing pool.
-S <hoststate>	Nagios status of the lpar or pool host. The status is passed by Nagios. If the status is not UP, the info is not checked.
-i <check information>	Available values are: STATUS (to check the status of the VIO server or of a logical partition), POOL (to check the utilization of the processing pool), CPU (to check the utilization of the CPU entitled to a partition). Default value is STATUS
-e <sample time>	Sample time in minutes used to perform calculation on utilization. Default value is 5.
-w <warnThreshold>	Warning threshold
-c <criticalThreshold>	Critical threshold.
-h, -help	Display help

### Return code

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

### Output

The output depends on the type of check performed, as shown in the examples below.

### check\_vios\_status

The check\_NSM\_escalalpar shell is called using the following syntax:

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

### Output

Only two states are possible for Vios status: OK or UNKNOWN:

- for OK state, the output is "Virtual I/O Server state: Operating"

- for UNKNOWN state, the output is "Unable to determine Virtual I/O Server state", following the reason.

---

**Note** The `check_vios_status` command is dependent on the state of the Vios system given by the `lssyscfg` IVM command.

---

### Example

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

---

```
Output: Virtual I/O Server state: Operating
```

---

Return code: OK.

### check\_vios\_used\_pool case

The `check_NSM_escalalpar` shell is called using 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

---

```
Shared Processor Pool Used (nbCPU / CPUTotal units entitled) -
utilization on <sampleTime> mn <check_status>: <utilization percent>%
```

---

---

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

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

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

### Example

```
check_NSM_escalalpar -H 192.168.207.60 -U padmin -I id_dsa_nsm -i
POOL
-e 5 -w 70% -c 80%
```

### Output

---

```
Shared Processor Pool Used (1.40 / 2 units entitled) - utilization on 5
mn OK: 2.16 %
```

---

Return code: OK

### check\_cec\_used\_pool case

The `check_NSM_escalalpar` shell is called using 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\_used\_configured\_pool case

The `check_NSM_escalalpar` shell is called using the following syntax:

```
check_NSM_escalalpar -M HMC -H <hmc_netName> -U <user>
-I <identity_file> -N <cecname> -p <poolname> -i POOL -e <sample_time>
-w <warn>% -c <crit>%
```

### Output

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

---

**Note** The `check_used_configured_pool` command is based on `pool_cycle` metrics (`total_pool_cycle`, `utilized_pool_cycle`) obtained by the `lslparutil` HMC command.

It requires that data collection is activated for the system by the `chlparutil` command:  
`chlparutil -r config -s 3600 [-m <systemName>]`

If the `systemName` parameter is not specified, the data collection is activated for all managed systems.

---

### Example

```
check_NSM_escalalpar -H 192.168.207.60 -U padmin -I id_dsa_nsm -i
POOL
-p SharedPool01 -e 5 -w 70% -c 80%
```

### Output

```
Configured Shared Processor Pool used: 0.03 / 2 Processors (HMC hmc-
squad) - utilization on 5 mn OK: 1.69 %
```

---

Return code: OK

### check\_lpar\_status case

The `check_NSM_escalalpar` shell is called using 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_lpar_status` command is based on the 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 ivm1 l part2
```

#### Output

```
-----
Logical partition tyrex on staix35 (IVM): Not Available
-----
```

Return code: CRITICAL.

### check\_lpar\_used\_cpu example

The `check_NSM_escalalpar` shell is called using 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>% -S <status>
```

#### Output

```
Logical partition <lpar_name> on <server_name> (<nbCPU> units entitled -
IVM or HMC - type=<partition type>) - processing utilization on
<sample_time>mn <check_status>: <utilization percent>%
```

---

**Note** The `check_lpar_used_CPU` command is based on cycles metrics (`entitled_cycles`, `capped_cycles`, `uncapped_cycles`) obtained by the `lslparutil` command (see above how to activate data collection on HMC or IVM).

---

#### Example

```
check_NSM_escalalpar -H 192.168.207.60 -U hscroot -I id_dsa_nsm -N
Pool1-ESP3-PL1660R -l Coop-IBM -I CPU-e 5 -w 10% -c 20%
```

## Output

```
-----  
Logical partition Coop-IBM on Pool-ESP3-PL1660R (1.0 units entitled -  
HMC 129.183.12.32 - type=Shared Uncapped Partition) - processing  
utilization on 5 mn OK: 0.04  
-----
```

Return code: WARNING

```
Shared Processor Pool used (nbCPU / CPUTotal units entitled) (HMC  
<hmc_netname>  
- utilization on <sampleTime> mn <check_status>: <utilization percent>%
```

### 4.3.2.1 check\_NSM\_escalavios

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

#### Usage

```
check_NSM_escalavios -H <hostname> -S <hoststate> -U <remote_user> -I  
<identity_file> -i <STATUS|CPU|POOL> [-e sample_time] [-w <warn>%] [-c  
<crit>%]
```

- |                        |  |
|------------------------|--|
| -H <hostname>          | Hostname or IP address of the VIO server to check  |
| -U <remote_user>       | User for remote connection   |
| -I <identity_file>     | Name of the file from which the identity (private key) for RSA or DSA authentication is read. The file must be localized into the directory <BSM Installation Directory>/engine/etc/ssh. To use it as authentication file for Vios platform, you have to install the corresponding public key on the VIO server. |
| -S <hoststate>         | Nagios status of the VIO server host.<br>The status is passed by Nagios. If the status is not UP, the info is not checked.   |
| -i <check information> | Available values are:<br>SEA (to check the utilization of the shared Ethernet adapters),<br>NPIV (to check the utilization of the fiber channer adapter)   |
| -e <sample time>       | Sample time in minutes used to perform calculation on utilization.<br>Default value is 5.  |
| -w <warnThreshold>     | Warning threshold  |
| -c <criticalThreshold> | Critical threshold.  |
| -h, -help              | Display help   |

#### Return code

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

#### Output

The output depends on the type of check performed, as shown in the examples below.

#### check\_vios\_used\_sea

The `check_NSM_escalavios` shell is called using the following syntax:

```
check_NSM_escalavios -H <vios_netName> -U <user> -I <identity_file>
-e <sample_time> -w <warning_threshold>% -c <critical_threshold>% -i SEA
-S <hoststate>
```

### Output

```
SHARED ETHERNET ADAPTERS (SEA) <check_status>: all adapters
(['<adapater_name> - <freq>Mbps - FD :<percent_use>%' ],...) less than
<threshold>% utilized
```

### Example

```
SHARED ETHERNET ADAPTERS (SEA) OK: all adapters ('ent4 - 100Mbps - FD
:0.14%' 'ent5 - 100Mbps - FD :0.00%' ) less than 60% utilized
Return code: OK.
```

## check\_vios\_used\_npiv

The check\_NSM\_escalavios shell is called using the following syntax:

```
check_NSM_escalavios -H <vios_netName> -U <user> -I <identity_file>
-e <sample_time> -w <warning_threshold>% -c <critical_threshold>% -i NPIV
-S <hoststate>
```

### Output

```
FIBER CHANNEL ADAPTERS (NPIV) <check_status>: all adapters
(['<adapater_name> - <freq>Gbps - :<percent_use>%' ],...) less than
<threshold>% utilized
```

### Example

```
FIBER CHANNEL ADAPTERS (NPIV) OK: all adapters ('fcs0 - 8Gbps :0.00%'
'fcs1 - 8Gbps :0.00%') less than 70% utilized
Return code: OK.
```

## 4.3.3 BSMDD4A

The BSMDD4A Add-on uses the following check command:

### 4.3.3.1 check\_DynamicDomains

check\_DynamicDomains uses the check\_DD4A shell (PERL) command options:

#### 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 most severe one; CRITICAL > WARNING > OK.

---

### Output

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

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, the number of CPUs used, their CPU load (and 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 number of CPUs it uses, its CPU load (and 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% )



---

## Appendix A. Third Party License Agreement

### VMware(R) Infrastructure Perl Toolkit Agreement

VMware, Inc. ("VMware") provides the VMware Infrastructure Perl Toolkit ("Toolkit") to you subject to the following terms and conditions. If you disagree with any of the following terms, then do not use this Toolkit.

1. This Toolkit contains a variety of materials, including but not limited to, interface definitions, documentation, sample utility applications and sample code regarding programming interfaces to one or more VMware products as referenced in such materials ("VMware Software"). This Toolkit is intended to be used to execute supplied sample utilities or to serve as a guide for writing programs to interact with the VMware Software.
2. Subject to the restrictions below, you may download and make a reasonable number of copies of the Toolkit contents for your personal use solely for the purpose of creating software that communicates with VMware Software ("Developer Software"). You agree to defend, indemnify and hold harmless VMware, and any of its directors, officers, employees, affiliates or agents, from and against any and all claims, losses, damages, liabilities and other expenses (including reasonable attorneys' fees), arising from your modification and distribution of the utility applications or sample code or breach of this Toolkit Terms and Conditions.
3. Restrictions: You may not (1) use the Toolkit to design or develop anything other than Developer Software; (2) make any more copies of the Toolkit than are reasonably necessary for the authorized use and backup and archival purposes; (3) modify, create derivative works of, reverse engineer, reverse compile, or disassemble the Toolkit, except that you may modify and create derivative works of the utility applications and sample code and distribute the modified utility applications and sample code in connection with Developer Software; (4) distribute, sell, lease, rent, lend, or sublicense any part of the Toolkit to any third party except as provided herein; (5) use the Toolkit to (a) design or develop programs to circumvent or over-ride the display of any VMware End User License Agreements to end customers and (b) design or develop software to upload or otherwise transmit any material containing software viruses or other computer code, files or programs designed to interrupt, destroy, or limit the functionality of any software or hardware.
4. VMware retains ownership of the Toolkit, including without limitation all copyrights and other intellectual property rights therein.
5. You may not represent that the programs you develop using the Toolkit are certified or otherwise endorsed by VMware. You may not use the VMware name or any other trademarks or service marks of VMware in connection with programs that you develop using the Toolkit.
6. If you are currently entitled to support from VMware, you may submit a support request for installation assistance of this Toolkit and assistance in executing unmodified utility applications provided with this Toolkit. Except as provided herein, you are not entitled any VMware support for this Toolkit or any other services from VMware in connection with this Toolkit.

7. Term, Termination and Changes: This Agreement shall continue as long as you are in compliance with the terms specified herein or until otherwise terminated. You and or VMware each may terminate this Agreement for any reason at any time. You agree, upon termination, to destroy all copies of the Toolkit within your possession or control. The Confidential Information, Limitations of Warranties, Liability and Indemnification sections set out in this Agreement shall survive any termination or expiration of this Agreement.

8. Limitations of Warranties and Liability: THE TOOLKIT IS PROVIDED "AS IS" WITHOUT ANY WARRANTIES OF ANY KIND. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, VMWARE DISCLAIMS ANY IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT WILL VMWARE BE LIABLE FOR ANY LOST PROFITS OR BUSINESS OPPORTUNITIES, LOSS OF USE, BUSINESS INTERRUPTION, LOSS OF DATA, OR ANY OTHER INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE TOOLKIT OR YOUR USE OF THE TOOLKIT, UNDER ANY THEORY OF LIABILITY, WHETHER BASED IN CONTRACT, TORT, NEGLIGENCE, PRODUCT LIABILITY, OR OTHERWISE. BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE PRECEDING LIMITATION MAY NOT APPLY TO YOU.

VMWARE'S LIABILITY ARISING OUT OF THE TOOLKIT PROVIDED HEREUNDER WILL NOT, IN ANY EVENT, EXCEED US\$5.00.

THE FOREGOING LIMITATIONS SHALL APPLY TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, REGARDLESS OF WHETHER VMWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND REGARDLESS OF WHETHER ANY REMEDY FAILS OF ITS ESSENTIAL PURPOSE.

9. These terms are governed by the laws of the State of California and the United States of America without regard to conflict of laws principles. You may not assign any part of this Agreement without the prior written consent of VMware. Any attempted assignment without consent shall be void. These terms constitute the entire agreement between you and VMware with respect to the Toolkit, and supersede all prior written or oral communications, understandings and agreements. Any waiver of these terms must be in writing to be effective. If any provision of these terms is found to be invalid or unenforceable, the remaining terms will continue to be valid and enforceable to the fullest extent permitted by law.

---

# Index

## A

Alerts, 1  
Alerts Service, 20, 25, 27  
All Service, 83  
Armg2\_4.mib, 27

## B

BSMGAMTT, 19  
BSMLSICIM, 21  
BSMMegaRaidSAS, 24

## C

check command  
    syntax, 85  
check\_EMCCLARIION, 29  
check\_DynamicDomains, 83, 116  
check\_esx\_server, 64  
check\_esx\_snmp, 64, 65  
check\_esx\_vm, 65  
check\_gamttRAID, 20  
check\_LSICIM, 22  
check\_LSICIM\_ctrl, 22  
check\_MegaRaidSAS(\_IR), 25  
check\_NECFDA, 27  
check\_netapp\_globalstatus, 97  
check\_netapp\_globalstatus, 32  
check\_netapp\_numdisks, 95  
check\_netappraid, 32, 99  
check\_netappvol, 32, 98  
check\_NSM\_escalalpar, 115  
check-netapp-cpload, 31  
check-netapp-cpload, 94  
check-netapp-failedfans, 32, 95  
check-netapp-failedpwr, 32, 96  
check-netapp-numdisks, 32  
CIM, 21

clariion.mib, 29, 34, 36, 43

## Commands

check\_DynamicDomains, 116  
check\_esx\_server, 64  
check\_esx\_snmp, 64, 65  
check\_esx\_vm, 65  
check\_gamttRAID, 20  
check\_LSICIM, 22  
check\_LSICIM\_ctrl, 22  
check\_MegaRaidSAS(\_IR), 25  
check\_netapp\_globalstatus, 97  
check\_netapp\_numdisks, 95  
check\_netappraid, 99  
check\_netappvol, 98  
check\_NSM\_escalalpar, 115  
check-netapp-cpload, 94  
check-netapp-failedfans, 95  
check-netapp-failedpwr, 96  
ping, 1

CPUload, 31

CTRLstatus Service, 22

CurrentPower, 40

## D

DDFA, 82

DeltaPressure, 40

Disk Space  
    Requirements, 5

Disks, 31

DynamicDomains Category, 83

## E

EMC CLARiiON Management, 28, 33, 35, 42, 45

EmcClariion Category, 29, 34, 36, 43, 46

EscalalPAR, 72

## F

Fans, 31

## G

GAM, 19

GAMTT, 19

GAMTTraid Category, 20

GlobalStatus, 31

GUI, 16

configuration tasks, 16

starting, 16

## H

Hardware Management Console (HMC), 72

Hardware Manager, 2

HMC (Hardware Management Console), 72

Host

ESX, 55, 61

VMware, 55, 61

## I

Installation

Requirements, 5

Windows, 7

Installation (Linux), 11

Integrated Virtualization Manager (IVM), 72

IVM (Integrated Virtualization Manager), 72

## L

Logical partitioning (LPAR), 72

LPAR (logical partitioning), 72

LSI 22320 chip, 21

LSI CIM, 21

LSI MegaRAID, 19

LSI MegaRAID SAS (IR), 24

lsi-adaptersas(ir).mib, 25

LsiCIM Category, 22

## M

MegaRAID, 19

megaraid.mib, 20

MegaRaidSAS(\_IR) Category, 25

Memory

Requirements, 5

MIB, 2

Monitoring Configuration, 16

## N

NetApp Category, 31

NetApp Management, 30

netapp.mib, 31

Notifications, 1

## O

Operating Systems, 5

## P

**Partitioning**, 72

ping command, 1

Power, 31

PowerStatus, 39

## R

RAIDStatus, 31

RAIDstatus Service, 22

Restrictions, 6

## S

Server Add-On, 3

Service

Cloning, 17

Creating, 17

Customization, 17

Customizing, 17

definition, 2

ServiceStatus, 20, 25, 27

SNMP traps, 2

Storage Manager, 2

Storage Server, 26

StoreWay FDA Management, 26

StoreWayFDA Category, 27

## T

TemperatureAverage, 40

Thresholds, 1

## U

Uninstallation (Linux), 14

Uninstallation (Windows), 10

Upgrading (Linux), 15

Upgrading (Windows), 10

URL

Bull System Manager main page, 16

## V

ValveAperture, 40

Virtualization Manager, 3

Virtualization Server, 38, 49

VolumeStatus, 31

## W

Water Cooled Door Management, 38

WaterCooledDoorMIB.mib, 39







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

REFERENCE  
86 A2 59FA 06