



NOVASCALÉ & ESCALA

BSM 1.3

Administrator's Guide



REFERENCE
86 A2 56FA 03

NOVASCALE & ESCALA

BSM 1.3

Administrator's Guide

Software

August 2010

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

REFERENCE
86 A2 56FA 03

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 2008-2010

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

Table of Contents	iii
List of Figures.....	ix
List of Tables	xiii
Preface.....	xv
Scope and Audience of this Manual.....	xv
Using this Manual	xv
Related Information	xvi
Highlighting.....	xvi
Chapter 1. Introduction	1
1.1 Bull System Manager Overview	1
1.1.1 Components.....	1
1.1.2 Distribution.....	1
1.2 Bull System Manager Concepts.....	2
1.2.1 Topology Elements	3
1.2.2 Monitoring	3
1.2.3 Event Reception	3
1.2.4 Notifications.....	4
1.2.5 Event Handling	4
1.2.6 Hardware Manager	4
1.2.7 Virtualization Manager.....	4
1.2.8 Storage Manager	5
1.2.9 Views	5
1.2.10 Maps.....	5
1.2.11 Focus Pane.....	5
1.2.12 Performance Indicators	5
1.3 Configuration Architecture.....	6
Chapter 2. Configuration Overview	7
2.1 Default Configuration.....	7
2.2 Configuration Tasks	7
2.3 Customization Tasks	8
2.4 Configuration GUI.....	9
2.4.1 Starting the Configuration GUI	9
2.4.2 Topology Configuration	11
2.4.3 Third-Party Application Configuration	11
2.4.4 Supervision Configuration	12
2.4.5 Console Customization	13
2.4.6 LocalSettings Configuration	14

2.4.7	Global Settings	14
2.5	Concurrent Access to the Configuration GUI	15
2.6	Main Configuration Steps	19
2.6.1	Create / Edit / Delete Resources	19
2.6.2	Save and Reload	21
2.6.3	Logout	24
Chapter 3.	Configuring Topology	25
3.1	Configuring Hosts	25
3.1.1	Using Host Discovery	26
3.1.2	Defining NovaScale Hosts	29
3.1.2.1	NS NS5005&6000	29
3.1.2.2	NS R400	33
3.1.2.3	ns bullion, NS 3005, NS 4000, NS 9010, NS T800 and Express 5800	37
3.1.3	Defining Blade Hosts	39
3.1.3.1	NovaScale Blade	39
3.1.3.2	Escala Blade	47
3.1.4	Defining Escala Hosts	48
3.1.4.1	PL Server	48
3.1.4.1.1	HMC Managed PL Servers	49
3.1.4.1.2	IVM Managed PL Server	54
3.1.4.1.3	Non managed PL Server	55
3.1.4.2	LPARs	56
3.1.4.2.1	Platform edition	56
3.1.4.2.2	LPAR edition	60
3.1.5	Defining Device Hosts	64
3.1.5.1	I/O Switch Modules	64
3.1.6	Defining Other Hosts	64
3.1.6.1	Host Properties	65
3.1.6.2	Example: Adding a Host	66
3.2	Configuring Hostgroups	68
3.2.1	Hostgroups	68
3.2.2	Platforms	69
3.3	Configuring Clusters	70
3.4	Configuring a Hardware Manager	73
3.4.1	Editing Properties	73
3.5	Configuring a Storage Manager	75
3.5.1	Editing Properties	75
3.6	Configuring a Virtualization Manager	77
3.6.1	Editing Properties	77
Chapter 4.	Configuring Inventory	79

Chapter 5.	Configuring Supervision	81
5.1	Configuring Categories and Services.....	81
5.1.1	Categories	83
5.1.1.1	Default Categories	83
5.1.1.2	Category Properties	84
5.1.1.3	Creating a new Category	85
5.1.1.4	Customizing a Category.....	86
5.1.1.5	Adding a Category from a Template.....	86
5.1.1.6	Deleting a User Category Template.....	87
5.1.2	Services	88
5.1.2.1	Default Services	88
5.1.2.2	Service Properties	89
5.1.2.3	Creating a New Service	92
5.1.2.4	Customizing a Service.....	94
5.1.2.5	Adding a Service from a Template.....	95
5.1.2.6	Deleting a User Service Template	97
5.1.3	Check Commands.....	98
5.1.4	Examples	100
5.1.4.1	Creating a New Category and Adding a Service	100
5.1.4.2	Creating a New Category and a New Service.....	101
5.1.4.3	Customizing the List of Monitored Hosts	105
5.1.4.4	Customizing the Notification Period	105
5.1.4.5	Customizing Thresholds	107
5.1.4.6	Warning and Critical Thresholds	107
5.1.4.7	Thresholds Related to Windows Event Logs Scanning	109
5.1.4.8	Customizing Windows Services.....	109
5.1.4.9	Customizing Linux or AIX Services	111
5.1.4.10	Customizing URL Access.....	113
5.1.4.11	Creating an Alerts Service	115
5.1.4.12	Using the perf_indic Service Template	115
5.2	Configuring Servicegroups	117
5.2.1	Default Servicegroup	118
5.2.1.1	Default Servicegroup edition	118
5.2.1.2	Default Servicegroup generation.....	118
5.2.2	User Servicegroup.....	119
5.2.2.1	User Servicegroup edition.....	119
5.2.2.2	User Servicegroup Members edition.....	120
5.2.2.3	User Servicegroup checking.....	124
5.3	Configuring Hosts/Hostgroups/Managers monitoring	125
5.3.1	Host Properties	125
5.3.2	Hostgroup Properties	127
5.3.3	Manager Properties.....	127
5.3.4	Example: Monitoring NS 4000 Hardware	128
5.3.4.1	Disabling Hardware Monitoring at Host Level	130
5.3.4.2	Disabling Hardware Monitoring at Manager Level	131
5.4	Syslog Monitoring	133
5.4.1	Host Properties	133
5.4.2	Syslog Filter Properties.....	134

5.4.3	Example: Monitoring Linux Host.....	138
5.4.3.1	Creating Linux Syslog Filter	138
5.4.3.2	Configuring Host.....	140
5.4.4	Example: Monitoring Aix Host.....	142
5.4.4.1	Creating Aix Syslog Filter.....	142
5.4.4.2	Configuring Host.....	147
Chapter 6.	Configuring Supervision Event Reception	149
6.1	Integrating MIBs	149
6.2	Controlling the Trap Receiver	151
Chapter 7.	Configuring Performance Indicators	153
7.1	Configuring Reporting.....	153
7.1.1	Example: Configuring an Indicator from Bull System Manager Monitoring Data	158
7.1.2	Example: Configuring an Indicator from SNMP Protocol	159
7.1.3	Browse Mibs Details	160
7.2	Configuring export	162
7.2.1	Export daily information of a perf_indic	162
7.2.2	Monitor and Notify by Mail the daily information of a perf_indic.....	164
Chapter 8.	Configuring Event Handler	167
8.1	Event Handler Definition.....	167
8.1.1	Host Event Handler.....	167
8.1.2	Service Event Handler.....	168
8.2	Event Handler Command.....	169
8.2.1	Host Event Handler Arguments.....	169
8.2.2	Service Event Handler Arguments.....	169
8.3	Event Handler Templates	170
8.3.1	Host Event Handler.....	170
8.3.2	Service Event Handler.....	170
8.4	Sample Event Handler.....	171
Chapter 9.	Configuring Notifications	173
9.1	Notification by E-mail.....	174
9.1.1	Mail Server	174
9.1.1.1	Mail Server on Linux.....	174
9.1.1.2	Mail Server on Windows	175
9.1.2	Contacts.....	175
9.1.3	Contactgroups	176
9.1.4	Example: Sending E-mail Notifications.....	177
9.1.4.1	Start Bull System Manager Configuration	177
9.1.4.2	Configure the Mail Server	177
9.1.4.3	Specify the Mail Address of the Receiver	178
9.1.4.4	Reload the Server Part	178
9.2	Notification by Autocalls	179

9.3	Notification by SNMP Trap	180
9.3.1	SNMP Manager	180
Chapter 10.	Configuring NSCA	183
Chapter 11.	Customizing the Bull System Manager Console	185
11.1	Specifying Applications	186
11.1.1	Bull System Manager Applications	186
11.1.2	User's Applications	187
11.2	Choosing the Default View	188
11.3	Specifying Maps	189
11.4	Specifying the Focus Pane	192
Chapter 12.	Configuring Local Settings	195
12.1	Configuring BSM Server	195
12.2	Configuring Users & Roles	196
12.3	Configuring Active Features	198
12.4	Configuring Periodic Tasks	199
Chapter 13.	Configuring Global Settings	201
13.1	Configuring Global Console	201
13.2	Configuring NDOutils Db Server	202
13.3	Example	203
13.3.1	Configuration of the Global Console	203
13.3.2	Configuration of the NDOutils Db Server	203
13.3.2.1	Central node, BSM1	203
13.3.2.2	Secondary nodes, BSM2 and BSM3	203
Appendix A.	Predefined Categories and Services	205
A.1	SystemLoad Category	206
A.2	LogicalDisks Category	207
A.3	EventLog Category	207
A.4	WindowsServices Category	207
A.5	FileSystems Category	208
A.6	Syslog Category	208
A.7	LinuxServices Category	208
A.8	Internet Category	209
A.9	Reporting Category	209
A.10	Hardware Category	209
A.11	Power Category	210

A.12	PAM Category	210
A.13	CMM Category.....	210
Appendix B. Generated Categories and Services		211
Appendix C. Check Commands for Customizable Services.....		213
C.1	check_ns_eventlog (Windows)	213
C.2	check_ns_disk (Windows).....	215
C.3	check_ns_load (Windows).....	216
C.4	check_ns_mem (Windows)	217
C.5	check_ns_service (Windows)	218
C.6	check_windisks (Windows).....	219
C.7	check_procs (Linux, AIX).....	220
C.8	check_log2.pl (Linux, AIX)	222
C.9	check_disk (Linux, AIX)	224
C.10	check_disks.pl (Linux, AIX)	225
C.11	check_cpuload (Linux, AIX)	226
C.12	check_lpar_load (AIX)	227
C.13	check_mem.pl (AIX)	228
C.14	check_memory (Linux)	228
C.15	check_swap (Linux, AIX)	229
C.16	check_users (Linux, AIX)	230
C.17	check_httpURL (Windows, Linux and AIX).....	231
C.18	check_mrtg (Windows, AIX and Linux).....	232
C.19	check_PowerStatus (IPMI servers).....	233
C.20	check_IPMI_sensor (IPMI servers).....	233
C.21	check_IPMI_sensor_avg (IPMI servers)	234
C.22	check_pressure (IPMI servers).....	235
Appendix D. Administration Commands		237
Appendix E. SSH Configuration		239
E.1	SSH client configuration on Bull System Manager Server.....	239
E.2	Keys generation on Bull System Manager Server	239
E.3	Use other identity file	240
E.4	Test non-prompted connection	241
Index.....		243

List of Figures

Figure 1-1.	Configuration architecture	6
Figure 2-1.	Authenticating the Bull System Manager configuration user	9
Figure 2-2.	Bull System Manager Configuration home page.....	10
Figure 2-3.	Bull System Manager Topology Host Definition submenu	11
Figure 2-4.	Bull System Manager Supervision configuration	12
Figure 2-5.	Bull System Manager Console customization home page	13
Figure 2-6.	Bull System Manager LocalSettings configuration home page	14
Figure 2-7.	Bull System Manager GlobalSettings configuration home page.....	14
Figure 2-8.	GUI with "read/write access"	15
Figure 2-9.	Session message	15
Figure 2-10.	GUI with "read only access"	16
Figure 2-11.	Sessions Information	17
Figure 2-12.	Force Lock information	18
Figure 2-13.	Hosts page – (example).....	19
Figure 2-14.	Host properties - example	20
Figure 2-15.	Object links	20
Figure 2-16.	Save & Reload Configuration report	22
Figure 2-17.	Save & Reload - Configuration detailed report	23
Figure 2-18.	Logout – Unsaved modifications	24
Figure 2-19.	Logout – No modifications	24
Figure 3-1.	Specification of hosts to be discovered.....	26
Figure 3-2.	Discovery result	27
Figure 3-3.	Replace and confirmation.....	28
Figure 3-4.	List of all hosts (old and new)	28
Figure 3-5.	NovaScale NS5005 Servers main page	29
Figure 3-6.	NS 5005 platform.....	30
Figure 3-7.	NS 5005 domains.....	31
Figure 3-8.	NS R400 hosts.....	33
Figure 3-9.	NS R400 host edition	34
Figure 3-10.	NS R422 edition	35
Figure 3-11.	NS Blade Servers main page	39
Figure 3-12.	Blade Chassis edition.....	40
Figure 3-13.	Blade and I/O Modules Definition with SNMP access	41
Figure 3-14.	Chassis Elements Definition without SNMP access	42
Figure 3-15.	Chassis Elements Re-discovery.....	43
Figure 3-16.	NovaScale Blade confirmation	44
Figure 3-17.	Deleting a Blade Chassis.....	46
Figure 3-18.	NS Blade Servers not linked to a chassis	46
Figure 3-19.	Escala PL Servers.....	48
Figure 3-20.	HMC Edition	49
Figure 3-21.	PL Servers discovery.....	50
Figure 3-22.	PL Servers Re-discovery.....	51
Figure 3-23.	HMC Managed Systems Confirmation	51
Figure 3-24.	IVM Managed PL Server.....	54
Figure 3-25.	Non managed PL Server.....	55
Figure 3-26.	Escala LPARs page	56
Figure 3-27.	HMC managed Escala LPAR platform	56

Figure 3-28.	IVM managed Escala LPAR platform	57
Figure 3-29.	Non managed Escala LPAR platform	57
Figure 3-30.	Host Topology modification confirmation for HMC managed Escala LPAR platform	59
Figure 3-31.	Logical Partitions display after Discover step	61
Figure 3-32.	Logical Partitions display after Discovery failure.....	61
Figure 3-33.	Logical partition display after Re-discover step.....	62
Figure 3-34.	Hosts configuration window	64
Figure 3-35.	Host properties	65
Figure 3-36.	Declaration form for a host	67
Figure 3-37.	Hostgroup properties.....	68
Figure 3-38.	Hostgroups	69
Figure 3-39.	Defining Cluster object	70
Figure 3-40.	Defining Cluster object supervision.....	71
Figure 3-41.	Cluster supervision	72
Figure 3-42.	Hardware manager properties	73
Figure 3-43.	Storage manager properties.....	75
Figure 3-44.	Virtualization Manager properties	77
Figure 4-1.	updateInventory periodic task properties	79
Figure 5-1.	Categories and services page	82
Figure 5-2.	Manage Categories popup.....	85
Figure 5-3.	Category properties edition	85
Figure 5-4.	Customizing a category.....	86
Figure 5-5.	Manage Categories popup.....	86
Figure 5-6.	Add Category from template.....	87
Figure 5-7.	Delete Category template	87
Figure 5-8.	Manage services popup	92
Figure 5-9.	Service properties edition	93
Figure 5-10.	Customize service	94
Figure 5-11.	Manage service popup.....	95
Figure 5-12.	Add service from template	96
Figure 5-13.	Delete service template.....	97
Figure 5-14.	Categories and Services table with a new category.....	100
Figure 5-15.	Categories and services table with a new service	101
Figure 5-16.	my_category creation	102
Figure 5-17.	List of categories for host	103
Figure 5-18.	Categories and Services table with customized services	106
Figure 5-19.	Customized threshold	108
Figure 5-20.	Categories and services table with customized services.....	108
Figure 5-21.	HTTP_BSM customized service.....	114
Figure 5-22.	perf_indic service example.....	116
Figure 5-23.	Service detail – example.....	116
Figure 5-24.	Servicegroups.....	117
Figure 5-25.	Hardware servicegroup edition	118
Figure 5-26.	User Servicegroup edition.....	119
Figure 5-27.	Servicegroup Members edition	120
Figure 5-28.	Servicegroup Members: filtering on monitoring domain.....	121
Figure 5-29.	Servicegroup Members: add of selected services.....	121
Figure 5-30.	Servicegroup members: reset of filter.....	122
Figure 5-31.	Servicegroup Members: filtering on domain and OS.....	122
Figure 5-32.	Servicegroup member: add Windows services	123
Figure 5-33.	User Servicegroup Control	124

Figure 5-34.	Hardware category monitoring domain.....	128
Figure 5-35.	NS4000 Hardware category and services	129
Figure 5-36.	Host hardware monitoring status	130
Figure 5-37.	NS4000 services deactivation	130
Figure 5-38.	NS4000 Alert service status	131
Figure 5-39.	Manager hardware monitoring status	131
Figure 5-40.	NS4000 Health service deactivation	131
Figure 5-41.	NS4000 Health service status.....	132
Figure 5-42.	Syslog Filters configuration window	138
Figure 5-43.	Common Syslog Filter properties	138
Figure 5-44.	Linux Syslog Filter properties.....	139
Figure 5-45.	Hosts configuration window.....	140
Figure 5-46.	Host monitoring properties.....	141
Figure 5-47.	Syslog Filters configuration window	142
Figure 5-48.	Common Syslog Filter properties	142
Figure 5-49.	Aix Syslog Filter common properties	143
Figure 5-50.	Aix Syslog Filter ErrorId properties.....	144
Figure 5-51.	Aix Syslog Filter ErrorLabel properties.....	145
Figure 5-52.	Aix Syslog Filter other properties	146
Figure 5-53.	Hosts configuration window.....	147
Figure 5-54.	Host monitoring properties.....	148
Figure 6-1.	Default SNMP Mibs integration	149
Figure 6-2.	SNMP MIB integration Edition.....	149
Figure 6-3.	SNMP trap customization message.....	150
Figure 6-4.	Control SNMP trap receiver	151
Figure 7-1.	Indicator properties - BSM monitoring collect mode	154
Figure 7-2.	Indicator properties - snmp collect mode.....	155
Figure 7-3.	Indicator properties - example.....	158
Figure 7-4.	Defining a new indicator	159
Figure 7-5.	Indicator graphs	160
Figure 7-6.	Browse Mibs: mibs tree	160
Figure 7-7.	MIB resource.....	161
Figure 7-8.	Select this oid button	161
Figure 7-9.	Getting the oid property	162
Figure 7-10.	Periodic Tasks list	162
Figure 7-11.	exportMRTG periodic task properties	163
Figure 8-1.	Host event handler creation	167
Figure 9-1.	Mail Server properties on Linux	174
Figure 9-2.	Mail Server properties on Windows	175
Figure 9-3.	Contact properties	175
Figure 9-4.	Contactgroup properties.....	176
Figure 9-5.	Autocall properties.....	179
Figure 9-6.	SNMP Manager properties.....	181
Figure 10-1.	Send via NSCA edition	183
Figure 10-2.	Reception via NSCA edition	184
Figure 11-1.	Customized default view and applications bar	185
Figure 11-2.	Bull System Manager Applications.....	186
Figure 11-3.	Bull System Manager Application edition	186
Figure 11-4.	An application as a web URL.....	187
Figure 11-5.	An application as a local command	187
Figure 11-6.	List of all applications.....	188

Figure 11-7.	Choosing the default view.....	188
Figure 11-8.	BSM Focus window.....	192
Figure 11-9.	Focused service properties	192
Figure 11-10.	List of all focused services	193
Figure 12-1.	BSM Server properties.....	195
Figure 12-2.	Users allowed accessing the Bull System Manager Applications	197
Figure 12-3.	Users & Roles properties	197
Figure 12-4.	Default Global Settings.....	198
Figure 12-5.	Disabling Monitoring.....	198
Figure 12-6.	Periodic Tasks	199
Figure 13-1.	Global Console properties	201
Figure 13-2.	NDOutils MySQL server configuration.....	202
Figure 13-3.	NDOutils DB Server BSM2 configuration	203
Figure D-1.	Authenticating the Bull System Manager control user.....	237
Figure D-2.	BSM Server Status.....	238

List of Tables

Table 3-1.	NS R400 menu	36
Table 3-2.	NS R400 objects	36
Table 3-3.	NS 3005, NS 9010, NS 4000, NS T800, Express 5800 menu	38
Table 3-4.	NS 3005, NS 4000, NS 9010, NS T800, Express 5800 objects	38
Table 3-5.	NS Blade Chassis objects	45
Table 3-6.	Host properties	66
Table 3-7.	Cluster properties	71
Table 3-8.	Hardware manager properties	74
Table 3-9.	Storage manager properties	76
Table 3-10.	Virtualization Manager properties	78
Table 5-1.	Service properties	91
Table 5-2.	Category and Service host selection -syntax rules	91
Table 5-3.	Check commands list	99
Table 5-4.	Customizing thresholds	107
Table 5-5.	Service parameters syntax	107
Table 5-6.	Windows services check commands and parameters	109
Table 5-7.	Linux services check commands and parameters	111
Table 5-8.	Customizing URL access	113
Table 5-9.	Syslog Monitoring host properties	133
Table 5-10.	Syslog Filters common properties	134
Table 5-11.	Syslog Filters Linux properties	134
Table 5-12.	Syslog Filters Aix properties	136
Table 5-13.	level values	136
Table 5-14.	facility values	137
Table 5-15.	ErrorClass values	137
Table 5-16.	ErrorType values	137
Table 6-1.	SNMP MIB properties	150
Table 6-2.	SNMP trap properties	151
Table 7-1.	Indicator properties	156
Table 9-1.	Contact properties	176
Table 9-2.	Contactgroup properties	177
Table 9-3.	Autocall properties	180
Table 9-4.	SNMP manager properties	181
Table 10-1.	Send via NSCA properties	183
Table 10-2.	Reception via NSCA properties	184
Table 11-1.	Focused service properties	192
Table 12-1.	Users, Roles and Functions	196
Table A-1.	Predefined categories and services	206
Table B-1.	Generated categories and services	211
Table C-1.	check_ns_eventlog output	214
Table C-2.	check_ns_disk (Windows) output	215
Table C-3.	check_ns_load (Windows) output	216
Table C-4.	check_ns_mem (Windows) output	217
Table C-5.	check_ns_service (Windows) output	218
Table C-6.	check_windisks (Windows) output	219
Table C-7.	check_procs (Linux) output	220

Table C-8.	check_log2.pl (Linux) output.....	222
Table C-9.	check_disk (Linux) command output.....	224
Table C-10.	check_disks.pl (Linux) output.....	225
Table C-11.	check_cpuload (Linux) command output.....	226
Table C-12.	check_lpar_load (AIX) output.....	227
Table C-13.	check_mem.pl (Linux) output.....	228
Table C-14.	check_memory (Linux) output.....	229
Table C-15.	check_swap (Linux)output.....	230
Table C-16.	check_users (Linux) output	230
Table C-17.	check_httpURL (Windows and Linux) output.....	232
Table C-18.	check_IPMI_sensor (IPMI servers) output.....	234
Table C-19.	check_IPMI_sensor_avg (IPMI servers) output.....	235
Table C-20.	check_pressure (IPMI servers) output.....	236
Figure D-1.	Authenticating the Bull System Manager control user.....	237
Figure D-2.	BSM Server Status.....	238

Preface

Scope and Audience of this Manual

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

In order to monitor a specific environment, Bull System Manager configuration must be customized. This manual explains how, as Administrator you can perform configuration tasks.

Note Configuration tasks may only be performed by Administrators.

Using this Manual

For a conceptual approach to Bull System Manager, read **Chapter 1 Introduction**.

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

Chapter 3 to **Chapter 10** describe how to configure Bull System Manager monitoring elements (Hosts, Hostgroups, Hardware Manager, Virtualization Manager, Storage Manager, Supervision, Event Reception, Performance Indicators, Event Handler, Notifications, Views, Maps, Focus Pane).

These chapters provide detailed information about all resource properties as well as concrete examples to help you customize your environment (Adding Hosts, Creating Hostgroups, Modifying Service Parameters, Organizing Views, Creating Maps, Specifying the Focus Pane,).

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

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

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

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

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

Appendix C Check Commands for Customizable Services describes the usage of the Nagios check commands by customizable services.

Appendix D Administration Commands describes some useful commands.

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

Related Information

Bull System Manager Documentation

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

Other documentation

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

Highlighting

The following highlighting conventions are used in this book:

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

Chapter 1. Introduction

1.1 Bull System Manager Overview

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

1.1.1 Components

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

- Management Server
- Management Console
- Management Agent

Management Server

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

Management Console

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

Management Agent

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

Additional extensions are also available in order to;

- extend Bull System Manager monitoring with more specific links to third-party management tools for specific devices and/or specific system functionalities.
- extend server functionalities as NDOutils that allows you to store all the Nagios status information in a MySQL database.

1.1.2 Distribution

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

To set a distributed solution, you have to install the NDOutils extension on each server, then choose one of them, identified as the central node, to host the centralized database and configure the others, the secondary nodes, to link the remote database.



CAUTION:

Solution with more than one central node is not supported.

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

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

1.2 Bull System Manager Concepts

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

Bull System Manager monitoring ensures the following tasks:

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

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

Bull System Manager Reporting offers the ability to draw graphs to follow the evolution of numeric indicators.

Bull System Manager Remote Operation allows to execute actions on host via the OS or via a Hardware Management tool.

1.2.1 Topology Elements

The **Host** is the main resource to be monitored. The administrator has to define host properties (**Operating System**, **Model**, **Notification properties**, etc) for all the hosts in the configuration.

See *Configuring Hosts*, on page 25, for a complete description of host properties.

A **Hostgroup** allows you to structure hosts in logical entities reflecting your environment. Hostgroup statistics collect the Hostgroup element status. For each Hostgroup, you can define a **Contactgroup** that will be notified of events occurring on each host in the Hostgroup.

See *Configuring Hostgroups*, on page 68, for a complete description of Hostgroup properties.

A **Platform** is a particular Hostgroup defined to represent a common set of hosts from the same series. For instance, a NovaScale 6xx0 server might contain one or more hosts. See *Platforms*, on page 69 for details.

A **Virtualization Platform** is a particular Hostgroup defined to represent a set of virtual machines. For instance, the Escala servers are commonly represented as virtualization platform grouping the logical partitions
See *Platforms*, on page 69 for details.

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

1.2.2 Monitoring

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

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

See *Configuring Supervision*, on page 81 and *Predefined Categories and Services*, for a complete description of the services and categories.

1.2.3 Event Reception

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

See *Configuring Supervision Event Reception*, on page 149 for details.

1.2.4 Notifications

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

Notification by E-mail

A **Mail server** is needed to relay e-mails. Its configuration is different on Windows and Linux platforms.

E-mail notifications are sent to all the **Contacts** in a **Contactgroup**.

See *Contacts*, on page 175 and *Contactgroups*, on page 176, for a description of Contact and Contactgroup properties.

Notification by Bull Autocall

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

Notification by SNMP Trap

SNMP manager configuration is required to define SNMP trap receivers.

See *Configuring Notifications*, on page 173, for details about these different types of notification.

1.2.5 Event Handling

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

See *Configuring Event Handler*, on page 167, for details about these different types of notification.

1.2.6 Hardware Manager

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

See *Configuring a Hardware Manager*, on page 73 for a description of Hardware Manager properties.

1.2.7 Virtualization Manager

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

See *Configuring a Virtualization Manager*, on page 77 for a description of Virtualization Manager properties.

1.2.8 Storage Manager

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

See *Configuring a Storage Manager* on page 75, for a description of Storage Manager properties.

1.2.9 Views

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

1.2.10 Maps

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

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

1.2.11 Focus Pane

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

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

1.2.12 Performance Indicators

Performance indicators are used as long-term counters. Counters reflect specific functional qualities. Indicators may be collected either using the SNMP protocol or from Bull System Manager monitoring data.

See *Configuring Performance Indicators*, on page 153, for a description of indicator properties.

An export mechanism is provided for these indicators. A Periodic Task can be configured to generate a daily repository file for each indicator.

See *Export daily information of a perf_indic*, on page 162 for a description of the periodic task properties.

Associated to this daily files generation, a Nagios plugin can be used to notify by mail the content of these files.

See *Monitor and Notify by Mail the daily information of a perf_indic*, on page 164 for a description of the plugin properties.

1.3 Configuration Architecture

The configuration of Bull System Manager is based on a client-server architecture:

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

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

The following figure represents this architecture:

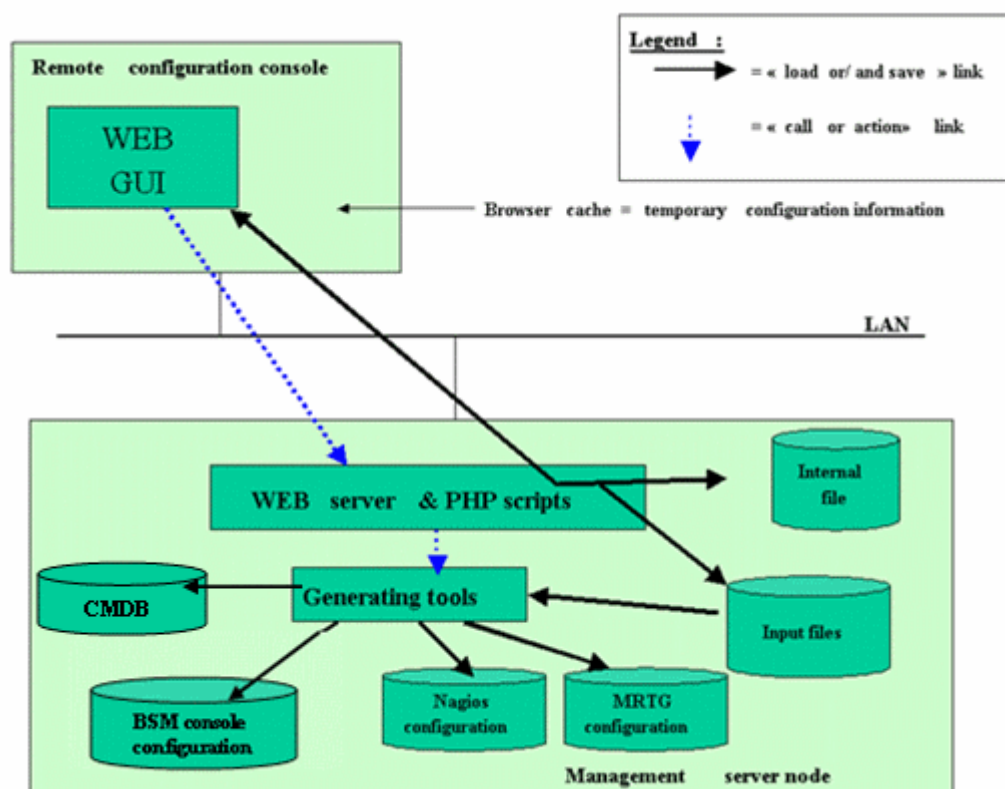


Figure 1-1. Configuration architecture

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

Chapter 2. Configuration Overview

Configuring Bull System Manager consists mainly in:

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

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

2.1 Default Configuration

At installation time, Bull System Manager is configured as follows:

- Default categories and their associated monitoring checks (services) are available.
- No default Reporting indicator is defined.
- The **mgt-admins** Contactgroup and the **manager** Contact are defined for mail notifications.
- The host on which Bull System Manager server is installed is configured as a host to monitor. The **BSM** Hostgroup is created, containing the Bull System Manager server host.
- The **default_map** map is configured with the **BSM** Hostgroup.

2.2 Configuration Tasks

As administrator, you must specify the **hosts** to monitor. See *Configuring Hosts* on page 25.

If required, you can then modify default configuration as follows:

- Definition of new **Contacts** and **Contactgroups** that will be notified of any anomaly or recovery on a monitoring element.
See *Contacts*, on page 175 and *Contactgroups*, on page 176.
- Definition of the **hardware managers** that manage host hardware
See *Configuring a Hardwa*, on page 73.
- Definition of the **storage managers** that manage host storage.
See *Configuring a Storage Manager*, on page 75.
- Definition of the **virtualization managers** that manage virtual machines. See *Configuring a Virtualization Manager*, on page 77.
- Definition of **Hostgroups** (collections of hosts).
See *Configuring Hostgroups*, on page 68.

- Customization of **categories** and monitoring **services**.
See *Configuring Supervision*, on page 81, for a description of general monitoring configuration procedures:
 - Restriction of the monitoring of some services to particular hosts.
See *Customizing the List of Monitored Hosts*, on page 105.
 - Definition of new resources to monitor. For examples see:
Customizing Windows Services, on page 109
Customizing Linux or AIX Services, on page 111
Customizing URL Access, on page 113.
 - Definition of specific monitoring properties (**thresholds, check period, check interval...**) for certain services and for different hosts
For examples see:
Customizing the Notification Period, on page 105
Customizing Thresholds, on page 107.
- Definition of Servigroups (collections of services).
See *Configuring Servicegroups*, on page 117 .
- Configuration of the **notification elements**.
See *Configuring Notifications*, on page 173.
- Creation of important Reporting **performance indicators**.
See *Configuring Performance Indicators*, on page 153.
- Definition of BSM components for distributed solution.
See *Configuring Global Settings*, on page 201.

2.3 Customization Tasks

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


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

2.4 Configuration GUI

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

2.4.1 Starting the Configuration GUI

To start the Configuration GUI, you can either:

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

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

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



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

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

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

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

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

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

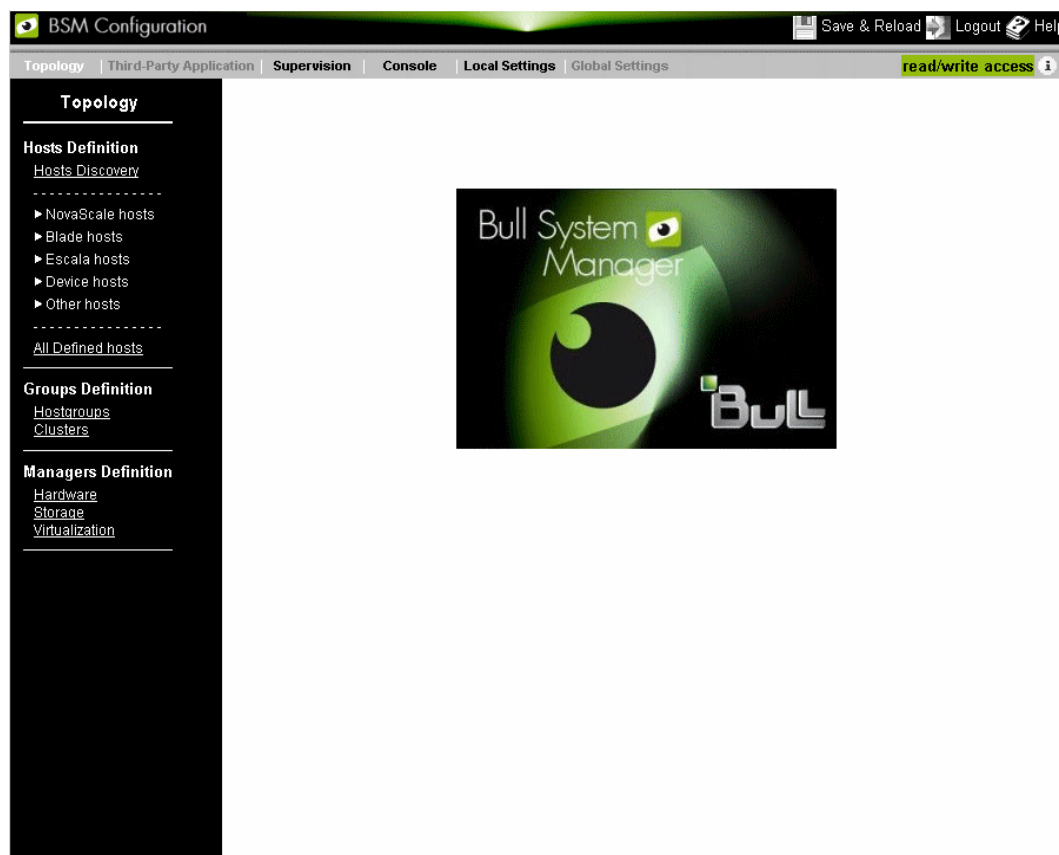


Figure 2-2. Bull System Manager Configuration home page

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

Buttons

Help	For access to generic help.
Save & Reload	To apply current modifications to the Bull System Manager server.
Logout	To exit from the BSM Configuration GUI

Tabs

Topology	For topology configuration (hosts, hostgroups ...).
Third-Party Application	For the customization of elements related to third party applications like JoNAs. This tab is available only if an application addOns is installed.
Supervision	For the configuration of supervision elements (services, notification ...).
Console	For the customization of applications, views, maps, focus pane.
LocalSettings	For the configuration of features of the local BSM server and users.

Global Settings

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



WARNING:

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

2.4.2 Topology Configuration

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

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

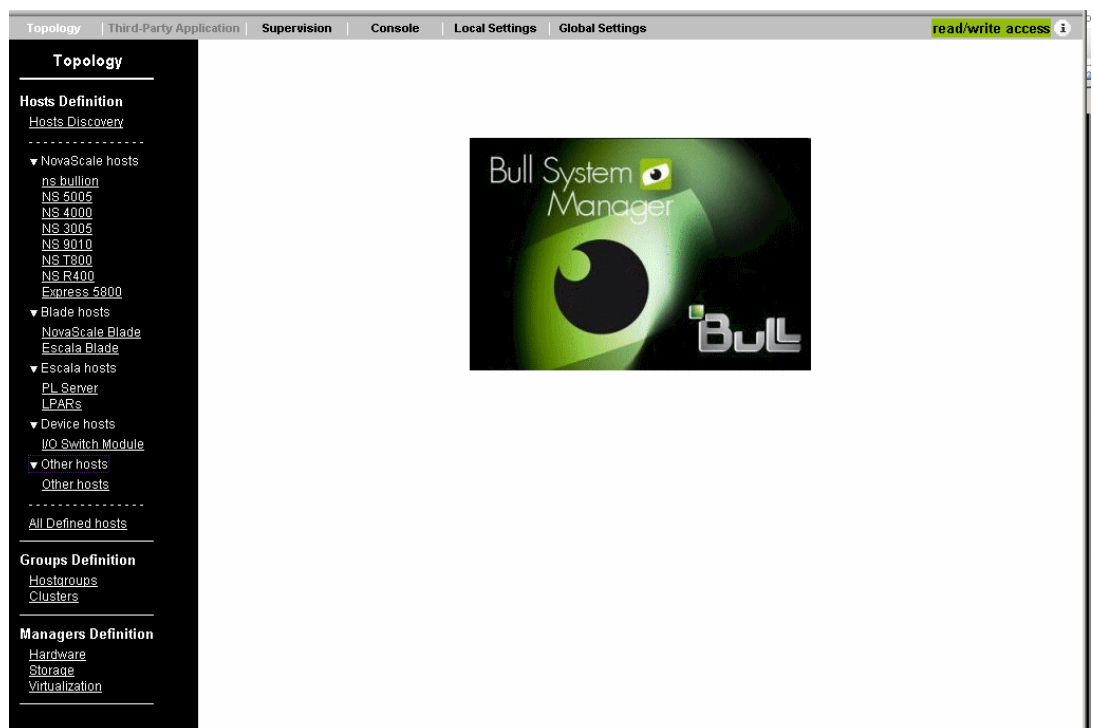


Figure 2-3. Bull System Manager Topology Host Definition submenu

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

Hosts Definition	to configure Hosts.
Groups Definition	to configure Hostgroups and Clusters
Managers Definition	to configure Hardware, Storage or Virtualization managers.

2.4.3 Third-Party Application Configuration

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

2.4.4 Supervision Configuration

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

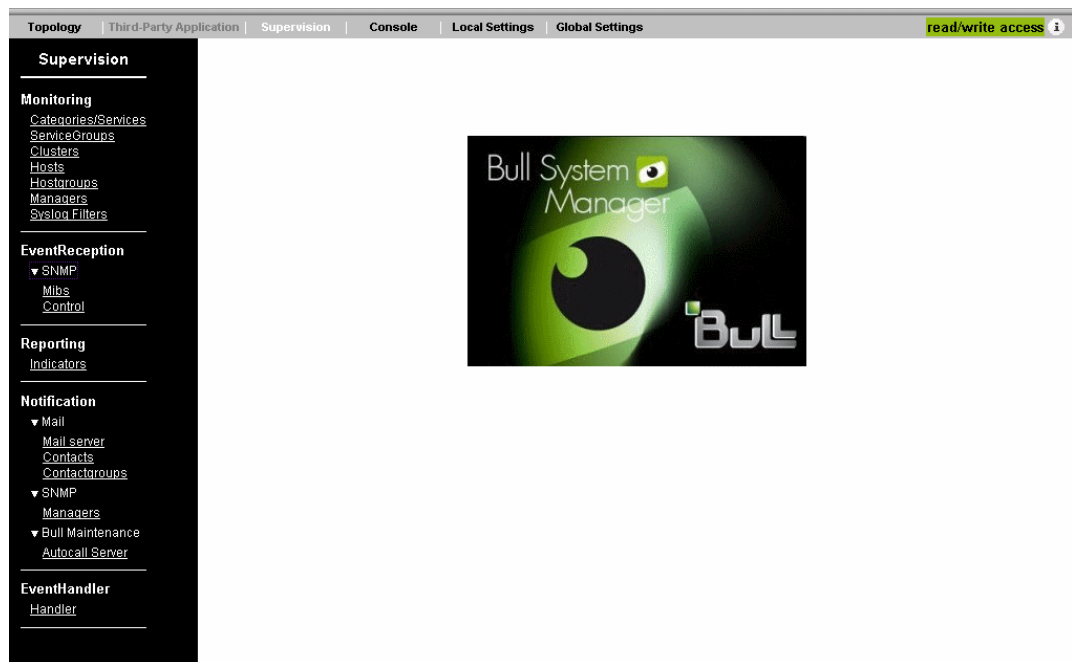


Figure 2-4. Bull System Manager Supervision configuration

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

Monitoring	to customize categories, services and topology element supervision features (notification ...).
EventReception	to configure the event reception mechanism (SNMP mibs integration, SNMP Trap receiver control).
Reporting	to configure performance indicators.
Notification	to configure mail notifications (contacts, Contactgroups and mail server), SNMP notifications to SNMP applications and autocall notifications for maintenance purposes.
EventHandler	to configure the handler.

2.4.5 Console Customization

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

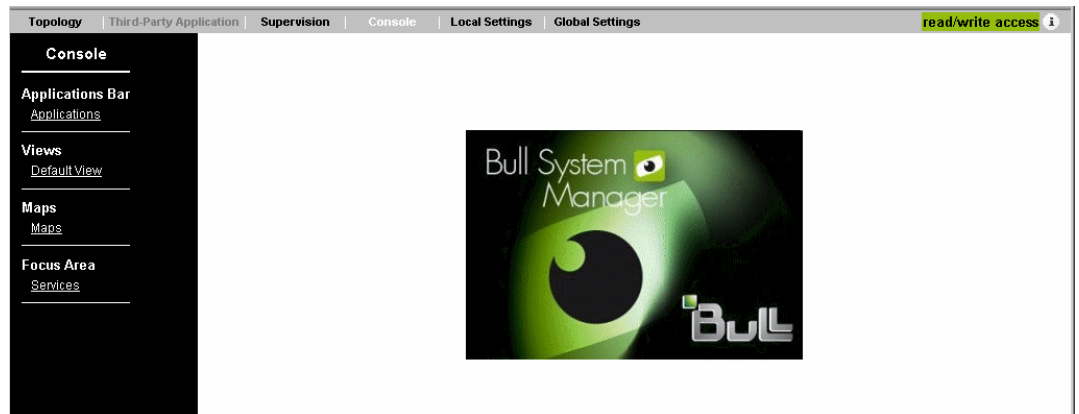


Figure 2-5. Bull System Manager Console customization home page

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

- | | |
|-------------------------|---|
| Applications Bar | to add applications to the left toolbar of the Console. |
| Views | to configure the default view that is displayed when the Console is started. |
| Maps | to configure maps shown in the Bull System Manager Console. |
| Focus Area | to specify very important services displayed (with their status) in this area of the Bull System Manager Console. |

2.4.6 LocalSettings Configuration

Select the **LocalSettings** tab. The following display appears:

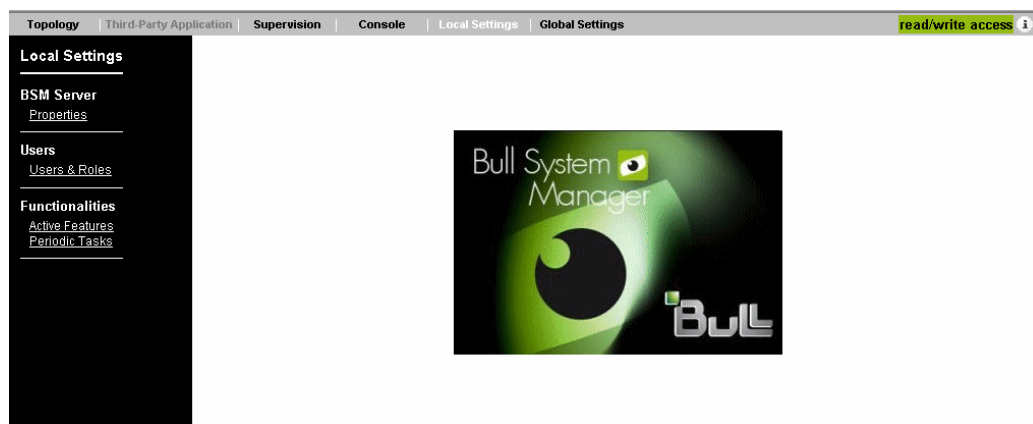


Figure 2-6. Bull System Manager LocalSettings configuration home page

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

- BSM Server** to set BSM server properties used by agent part.
- Users** to configure users and roles (user profiles).
- Functionnalities:** to configure BSM functional features.

2.4.7 Global Settings

Select the **GlobalSettings** tab. The following display appears:

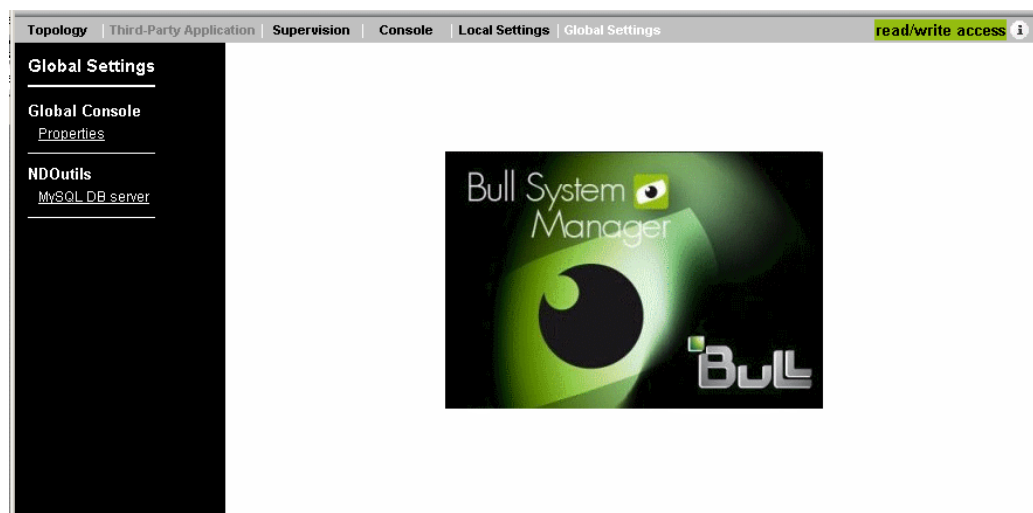


Figure 2-7. Bull System Manager GlobalSettings configuration home page.

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

- Global Console** to set the port number of the global console
- NDOutils** to set the properties of the server hosting the common NDOutils database.

2.5 Concurrent Access to the Configuration GUI

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

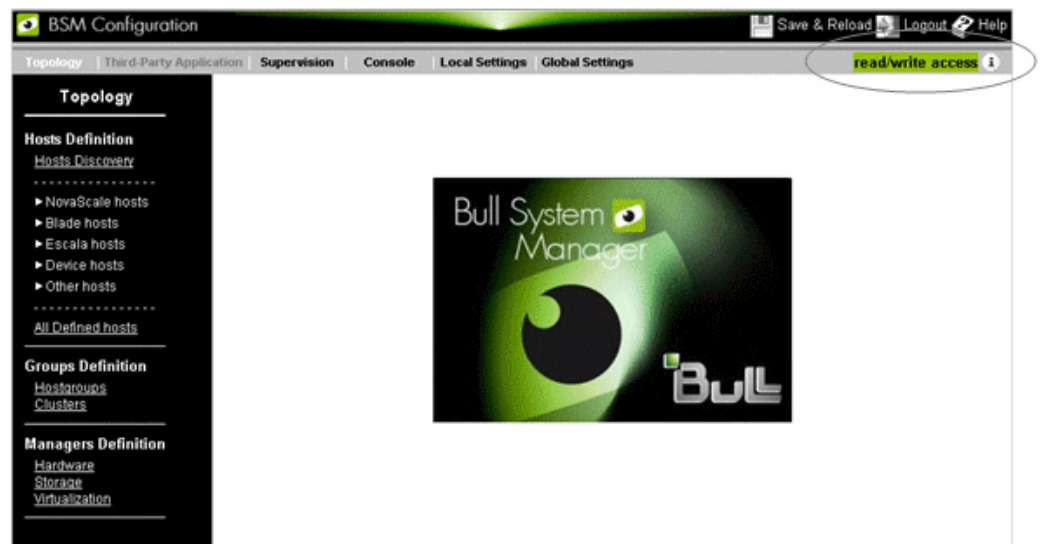


Figure 2-8. GUI with "read/write access"

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

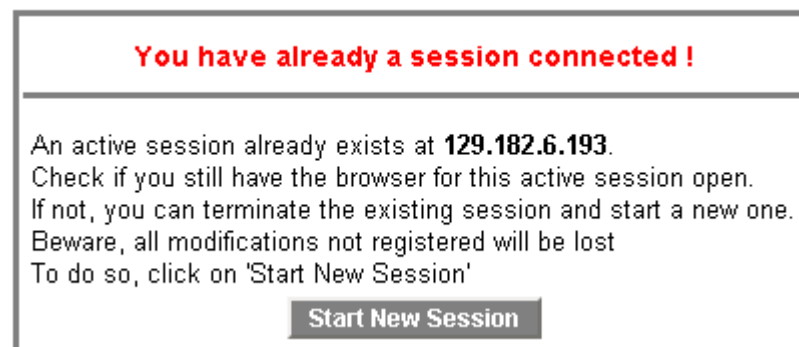


Figure 2-9. Session message

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



important:

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

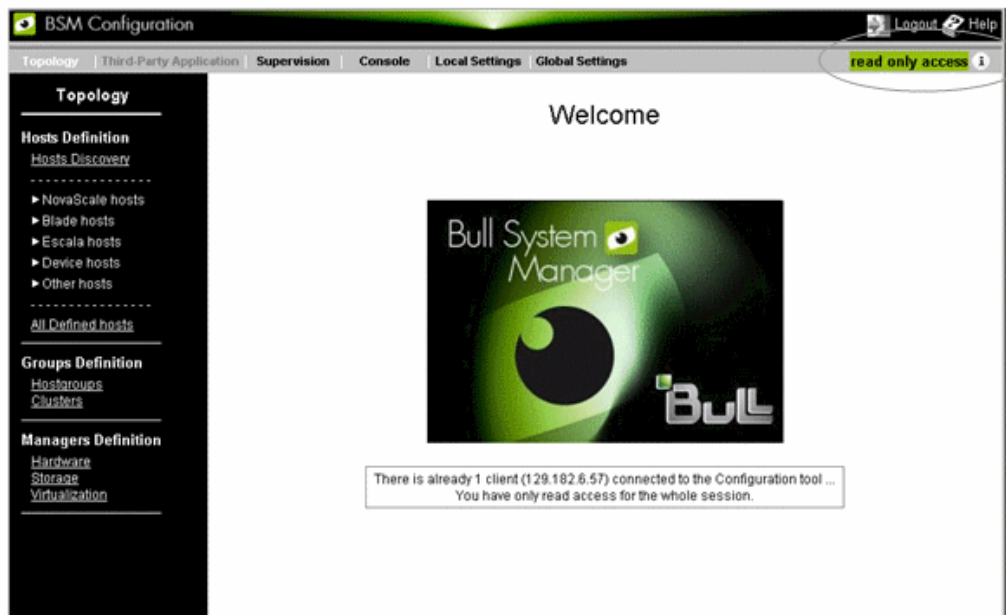



Figure 2-10. GUI with "read only access"

Click the  icon to display information about currently active sessions.

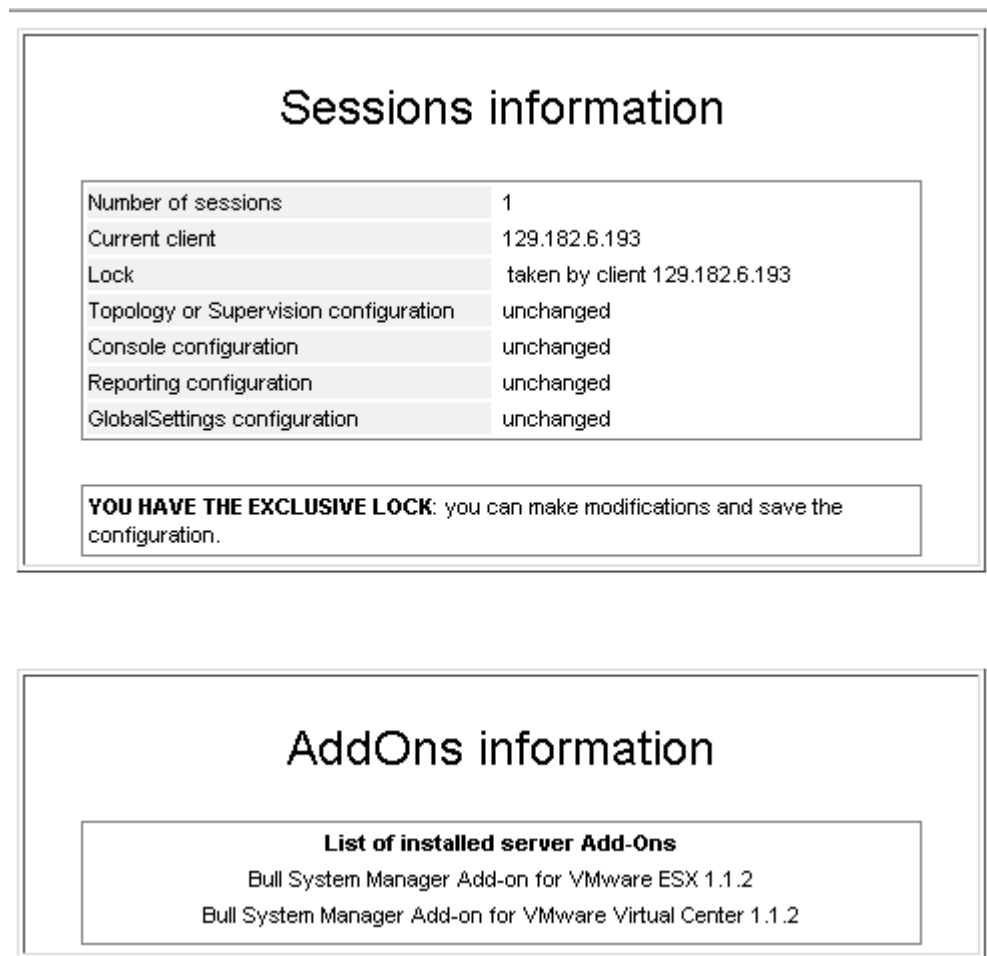


Figure 2-11. Sessions Information

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

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

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

Sessions information

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

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

Figure 2-12. Force Lock information



WARNING

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

2.6 Main Configuration Steps

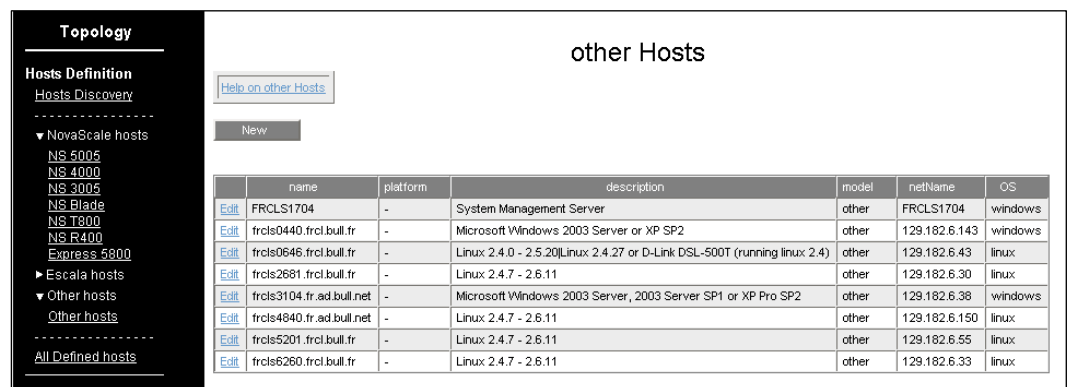
Perform the following steps to modify the default configuration:

1. Start the **BSM Configuration GUI** (see *Starting the Configuration GUI*, on page 9).
2. Select either **Topology**, **Third-Party Application**, **Supervision**, **Console**, **Local Settings** or **GlobalSettings** tab, according to configuration needs.
3. Click the type of resource you need to configure. Bull System Manager displays all the configured resources of this type.
4. **Create**, **edit** or **delete** the resources to configure.
5. **Save** and **reload** the configuration on the Bull System Manager server part

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

2.6.1 Create / Edit / Delete Resources

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



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

Figure 2-13. Hosts page – (example)

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

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

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

Properties	
name	<input type="text"/> <input type="button" value="Select"/>
description	<input type="text"/>
model	other
network name	<input type="text"/>
parents	<div>Selected Hosts: <input type="text"/></div> <div>All Hosts: <div>B260 BLADE#01 chassis45_CMM frcls1704 switch1</div></div> <div><input type="button" value="Add"/> <input type="button" value="Remove"/></div>
OS family	other <input type="button" value="v"/>
OS info	<input type="text"/>

Figure 2-14. Host properties - example

Mandatory properties are identified by a red mark.

Make required changes, then:

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

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

NS 5005 series Server

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

Properties	
name	charly4l
description	Automatically created for the NS 5005 platform.
model	NS 5005 series
network name	172.31.50.90
OS family	linux <input type="button" value="v"/>
OS info	<input type="text"/>

[Edit Supervision Properties](#)

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

'fameptf'-object: [charly4](#)

Figure 2-15. Object links

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

2.6.2 Save and Reload

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

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

The **Save & Reload** operation requires confirmation.

After confirmation, **Save & Reload** performs the following steps:

1. It verifies which part of the configuration has been modified in order to select corresponding configuration actions.
2. It saves the configuration in the files used by Bull System Manager Configuration. These files will be loaded in the next session of Bull System Manager Configuration.
3. It checks the consistency of the new configuration and generates the internal files used for the monitoring and/or reporting and/or the Console.
4. If required, it restarts the monitoring and/or the reporting processes, if no semantic error was found in the previous step.

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

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

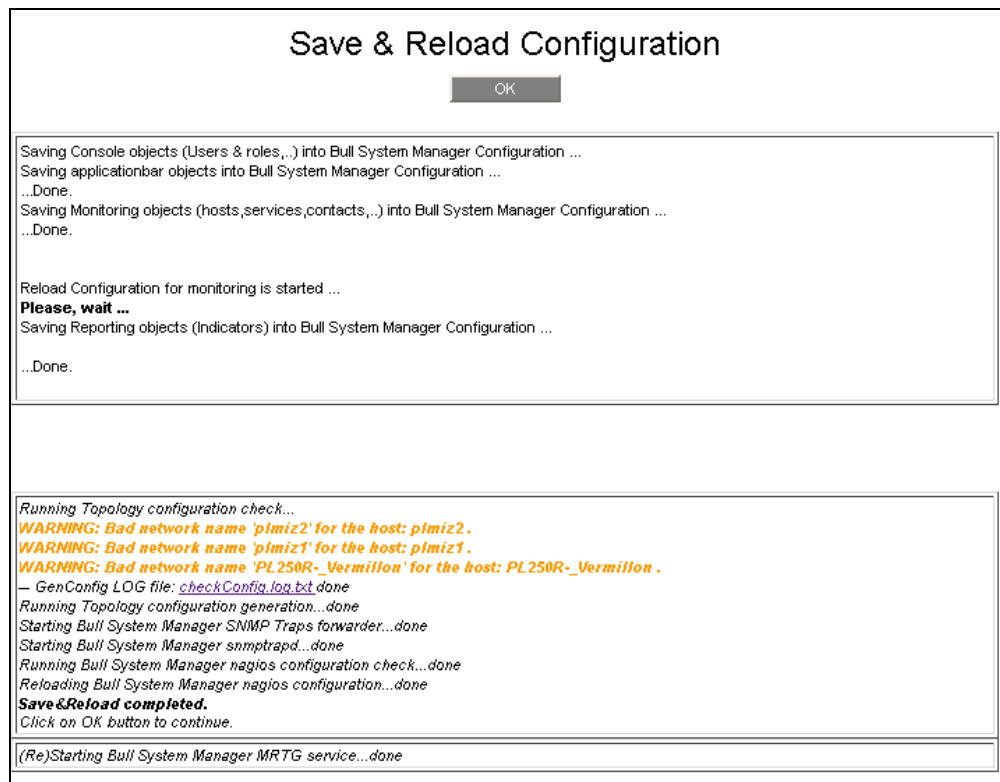


Figure 2-16. Save & Reload Configuration report

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

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

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

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

2.6.3 Logout

To logout from the BSM Configuration, click the logout button .
The logout action requires confirmation:

If some modifications have not been saved, the following page is displayed:

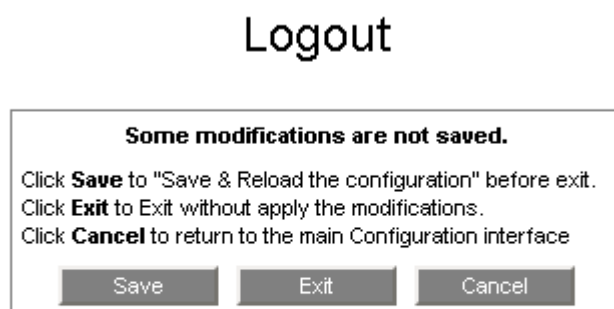


Figure 2-18. Logout – Unsaved modifications

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

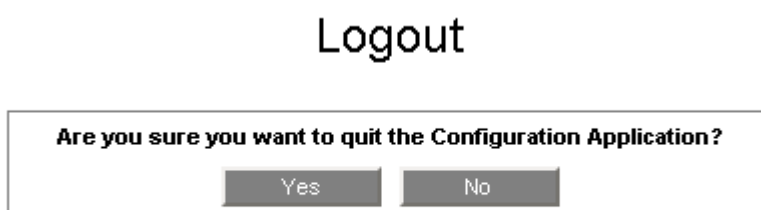


Figure 2-19. Logout – No modifications

Chapter 3. Configuring Topology

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

Notes

- The following characters are not supported in any text fields:
 - [] brackets,
 - = equal sign,
 - ; semicolon
 - " commas
 - space
 - The following label names **MUST** be different from the following strings which are reserved keys or formats:
 - "*<string>",
 - "none",
 - "!<string>"
 - "auto"
 - "<string>_CMM"
 - "<string>_PAM"
 - "<string>_mgr"
 - "<string>_HNMaster"
 - (where <string> may be any string).
-

3.1 Configuring Hosts

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

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

Bull System Manager can monitor several host models:

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

Note The **StoreWay** and **Virtualization** menus are available only if the corresponding Add-ons are installed. Host configuration for these specific hosts is not described here. Refer to the *Bull System Manager Server Add-ons Installation and Administrator's Guide* (86 A2 59FA).

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

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

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

3.1.1 Using Host Discovery

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

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

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

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

IP Discovery

Discover Cancel

Properties

host specification 129.182.6.30-150

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

Figure 3-1. Specification of hosts to be discovered

Set **host specification** properties, which can be a **single hostname**, a **single IP address** or a **range of IP addresses** as explained in the displayed help.

All hosts meeting the specification, which are up and for which NMAP has recognized the OS, are discovered and displayed (Figure 3-2). Moreover, the discovery mechanism detects whether the Bull System Manager monitoring agent is running on each host.

IP Discovery					
Discovery of hosts of 129.182.6.30-150					
<input type="checkbox"/> Ping monitoring for selected hosts without BSM agent <input type="button" value="Add Selected Hosts"/> <input type="button" value="Cancel"/>					
Select	name	OS	OS info	network name	BSM agent
<input checked="" type="checkbox"/>	frcls2681.frcl.bull.fr	linux	Linux 2.4.7 - 2.6.11	129.182.6.30	no
<input type="checkbox"/>	turina.frcl.bull.fr	linux	Linux 2.4.0 - 2.5.20[Linux 2.4.27 or D-Link DSL-500T (running linux 2.4)]	129.182.6.31	no
<input type="checkbox"/>	shrimp.frcl.bull.fr	linux	Linux 2.4.7 - 2.6.11	129.182.6.32	no
<input type="checkbox"/>	frcls6260.frcl.bull.fr	linux	Linux 2.4.7 - 2.6.11	129.182.6.33	yes
<input type="checkbox"/>	menis.frcl.bull.fr	linux	Linux 2.4.7 - 2.6.11	129.182.6.35	no
<input checked="" type="checkbox"/>	frcls3104.fr.ad.bull.net	windows	Microsoft Windows 2003 Server, 2003 Server SP1 or XP Pro SP2	129.182.6.38	yes
<input type="checkbox"/>	CLOG182.fr.ad.bull.net	windows	Microsoft Windows 2003 Server or XP SP2	129.182.6.40	no
<input type="checkbox"/>	frcls5504.frcl.bull.fr	windows	Microsoft Windows 2003 Server or XP SP2	129.182.6.41	no
<input type="checkbox"/>	fiarena.frcl.bull.fr	linux	Linux 2.4.7 - 2.6.11	129.182.6.42	no
<input type="checkbox"/>	FRCLS1208.frcl.bull.fr	windows	Microsoft Windows Me, 2000 or XP	129.182.6.46	no
<input type="checkbox"/>	frcls4206.hd2c.dom	windows	Microsoft Windows Me, 2000 or XP	129.182.6.49	no
<input type="checkbox"/>	frcls4620.frcl.bull.fr	windows	Microsoft Windows 2003 Server, 2003 Server SP1 or XP Pro SP2	129.182.6.50	yes
<input checked="" type="checkbox"/>	sun481.frcl.bull.fr	other	Sun Solaris 2.6 - 8 (SPARC)	129.182.6.52	no
<input type="checkbox"/>	STELLA.frcl.bull.fr	linux	Linux 2.4.0 - 2.5.20[Linux 2.4.27 or D-Link DSL-500T (running linux 2.4)]	129.182.6.53	no
<input type="checkbox"/>	frcls5201.frcl.bull.fr	linux	Linux 2.4.7 - 2.6.11	129.182.6.55	no
<input type="checkbox"/>	FRCLS0980.fr.ad.bull.net	windows	Microsoft Windows 2003 Server, 2003 Server SP1 or XP Pro SP2	129.182.6.57	no
<input checked="" type="checkbox"/>	giovana.frcl.bull.fr	linux	Linux 2.4.7 - 2.6.11	129.182.6.58	no
<input type="checkbox"/>	chaberton.frcl.bull.fr	linux	Linux 2.4.7 - 2.6.11	129.182.6.64	no
<input type="checkbox"/>	pamela.frcl.bull.fr	linux	Linux 2.4.7 - 2.6.11	129.182.6.65	no
<input type="checkbox"/>			IBM AIX 4.3.2.0-4.3.3.0 on an IBM RS/6000		

Figure 3-2. Discovery result

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

Notes

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

IP Discovery

☐ Replace

Confirm Add
Cancel

Use Replace checkbox to replace already existing hosts.

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

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

Host named 'frcls4206.hd2c.dom' will be created.

Host named 'frcls4620.frcl.bull.fr' will be created.

Figure 3-3. Replace and confirmation

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

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

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

other Hosts

[Help on other Hosts](#)

New

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

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

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

3.1.2 Defining NovaScale Hosts

3.1.2.1 NS NS5005&6000

NovaScale 5005 servers are usually housed in a module managed by the Platform & Administration Manager (PAM).

To configure NovaScale 5005 hosts, expand the NovaScale menu under Host Definition and select the NovaScale 5005&6000 item. The following page is displayed:

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

Figure 3-5. NovaScale NS5005 Servers main page

To configure a standalone NovaScale Blade NS5005, click the **New Host** button. This action results in the display of a form edition similar to those of the Other Host edition.

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

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

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



Important:

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

NS 5005 Platform Edition

The following form is used to define a NS 5005 platform:

NS 5005 series Platform

[Help on NS 5005 series Platform](#)

OKCancelDeleteDeleteAll

Properties

NS 5005 platform namecharly4

descriptionNS 5005 platform

PAM manager

network name172.31.50.50

userfru


password...confirm...

NS 5005 Hosts (= PAM domains)

Servers Configuration

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

Figure 3-6. NS 5005 platform

important:

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

Platform Information

NS 5005 platform name	The label used to identify the platform in Bull System Manager, ns5005ptf in the example.
	Note: We advise you to use the "Central Subsystem" Name defined in the PAM tool that contains corresponding domains. Elsewhere, if needed, this defined platform name may contain a set of defined domains that do not correspond to one PAM Central Subsystem but are necessarily managed by the same PAM manager.
description	Short text describing the platform, NS 5005 platform in the example.

PAM Manager

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

NS 5005 Hosts

Lists the servers to be managed by Bull System Manager.

At platform creation, this part of the form is not displayed. An initial discovery request to the PAM application must be performed to get the list of servers in the platform. Click the **Discover** button to get the list of domains configured in the NS 5005 Platform.

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

The screenshot shows a window titled 'Servers Configuration'. Inside, there is a text box with instructions: 'Select ns5005 servers to manage by clicking the corresponding checkbox. Then, update the Bull System Manager Host by directly editing the property fields or by selecting a defined host by clicking the 'Select' button.' Below this is a table with two main sections: 'PAM Domain Servers' and 'Bull System Manager Hosts'.

PAM Domain Servers		Bull System Manager Hosts		
	Domain Name	host Name	netName	OS
<input checked="" type="checkbox"/>	dom0	charly4l	172.31.50.90	linux
<input checked="" type="checkbox"/>	dom1	charly4w	172.31.50.91	windows

At the bottom left is a 'Re-discover' button. To its right is a text box containing the instruction: 'To update the list of ns5005 servers from Management Module, click the Re-discover button'.

Figure 3-7. NS 5005 domains

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

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

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

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

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

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

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

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

After editing:

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

When Topology is modified, confirmation is required. A page is displayed listing all the changes to be applied. If you do not agree, click the **NO** button to return to the NS5005 Platform edition page, otherwise click the **YES** button to create the NovaScale Blade chassis and all related objects.

Related N5005 Platform Objects

When a NS 5005 Platform object is defined, related objects are automatically generated to configure the specific Supervision linked to this type of NovaScale server. The following table describes the objects generated during the creation of a NS5005 Platform.

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

Type	Description
categories and services	<p>The PAM category and related services are instantiated for the PAM host.</p> <p>The Hardware category and related services are instantiated for each NS 5005 host.</p>

Deleting a NS 5005 Platform

They are two ways to delete a NS 5005 Platform:

- Click the **Delete** button to delete the platform but keep the NS 5005 servers
The hostgroup, manager (if not linked by another NS5005 platform) and related services are deleted but the NS 5005 servers remain in the configuration as unlinked host.
- Or click the **DeleteAll** button to delete the platform and all linked NS 5005 servers.

3.1.2.2

NS R400

Nova Scale R400 series are rack-optimized servers used as front-end and applications servers in space constrained environments. They generally fit one server except the R422 model. The NovaScale R422 features an innovative packaging that allows fitting two servers into a single 1U chassis.

To configure a NS R400, click the **NS R400** menu. The current configured R400 are displayed. To define a new R400, click the **New Platform** button for a R422, otherwise click the **New Host** button

NS R400 series						
Help on NS R400 series						
<div>New Platform</div> <div>New Host</div>						
	Platform	Node	Host name	Description	Network name	OS
-	-	-	nsmaster	N/A	129.182.6.150	linux
Edit	rack1	1	frcls6260.frcl.bull.fr	Linux 2.4.7 - 2.6.11	129.182.6.33	linux
		2	frcls0646.frcl.bull.fr	Linux 2.4.0 - 2.5.20 Linux 2.4.27 or D-Link DSL-500T (running linux 2.4)	129.182.6.43	linux

Figure 3-8. NS R400 hosts

NS R400 Edition

The following forms are used to define a NS R400.

NS R400 series Server

OK Cancel

Properties	
name	<input type="text"/> Select
description	<input type="text"/>
model	<input checked="" type="radio"/> NS R400 <input type="radio"/> NS R400 E1 <input type="radio"/> NS R400 E2 <input type="radio"/> NS R400 F2
network name	<input type="text"/>
parents	<div><div>Selected Hosts</div><div><div></div><div></div></div><div><div><= Add</div><div>Remove =></div></div><div>All Hosts</div><div><div>frcls1704</div><div>frcls6260</div><div>nsmesx</div><div>rh54</div><div>sles10</div></div></div>
OS family	<input type="text" value="other"/>
OS info	<input type="text"/>
Out-of-band attributes	
network name	<input type="text"/>
user	<input type="text"/>
password	<input type="text"/> confirm <input type="text"/>
GUI URL	<input type="checkbox"/> <input type="text"/>

Figure 3-9. NS R400 host edition

Figure 3-10. NS R422 edition

Host Properties	Description
Platform name	Platform name (only for NS R422 model).
name	<p>Host short name (label).</p> <p>This name is the one displayed in the Bull System Manager Console views. Generally, this label is the host name.</p> <p>Note: In the configuration, the host name MUST be different from the following reserved keys: "*", "none" and "auto".</p> <p>The host may be selected from the hosts defined without model (discovered by Discovery or created from the Other hosts menu).</p>
description	<p>Description of the host.</p> <p>This description is displayed in an info tip in the Management Tree when you move the mouse over the node associated with this host.</p>
model	<p>Model of the host.</p> <p>You can be more specific by choose a sub-model among NS R400, NS R400 E1, NS R400 E2 or NS R400 F2 .</p>
network name	<p>Host network name (hostname or IP address).</p> <p>Default value: host name (label).</p>
parents	<p>List of hosts that link the host with remote hosts.</p> <p>For instance, a host representing a network equipment (router, switch, ...) is typically a parent host.</p>

Host Properties	Description
OS family	Operating System type (Windows, Linux, aix, none, other). Other OS can be supported if the corresponding Add-on is installed. Default value: <i>other</i> .
OS info	When a host is discovered by Discovery , certain properties are set automatically. This is the case of OS info , which gives information about the OS running on the host. description , if empty, is automatically set to the same value as OS info .
Out-of-band attributes	Description
network name	Out-of-band platform management card address.
user, password	Authentication information (login, password) used by Bull System Manager to access the management card.
GUI URL	Hardware management application URL

Table 3-1. NS R400 menu

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

Related NS R400 Objects

When a R400 object is defined, related objects are automatically generated to configure the specific Supervision linked to this type of NovaScale server. The following table describes the objects generated during the creation of a NS R400.

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

Table 3-2. NS R400 objects

3.1.2.3

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

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

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

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

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

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

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

When this type of host is defined, related objects are automatically generated to configure the specific Supervision linked to this type of NovaScale server. The following table describes the objects generated.

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

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

3.1.3 Defining Blade Hosts

3.1.3.1 NovaScale Blade

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

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

NS Blade series

[Help on NS Blade series](#)

[New Chassis](#)

[New Server](#)

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

Figure 3-11. NS Blade Servers main page

To configure a standalone NS Blade Server, click the **New Host** button. This action results in the display of a form edition similar to those of the Other Host edition.

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

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

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

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



Important:

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

Blade Chassis Edition

The following form is used to define a Blade Chassis:

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

Figure 3-12. Blade Chassis edition

Chassis Information

- chassis name** The label used to identify the chassis in Bull System Manager, `chassis3` in the example.
- description** Short text describing the chassis, `chassis 45 F4/SS` in the example.

Management Module

- network name** IP address used to access the CMM, `192.168.207.45` in the example.
- SNMP port** SNMP agent port used to get information about CMM configuration, `161` in the example.
Default value: `161`.
- SNMP community** SNMP community used in the SNMP request to identify the Bull System Manager server, `public` in the example.
Default value: `public`.

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

Blade Servers

Lists the servers to be managed by Bull System Manager.

I/O Modules

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

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

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

Blades and I/O Modules

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

To update the list of chassis element from Management Module, click the Re-discover button

Blade Configuration

	Blade Servers			Bull System Manager Hosts			
	Bay	Model	Ident	Name		netName	OS
<input checked="" type="checkbox"/>	1	NS Blade	BLADE#01	BLADE#01	<input type="button" value="Select"/>	BLADE#01	other
<input checked="" type="checkbox"/>	2	NS Blade	SN#YK105183N129	SN#YK105183N129	<input type="button" value="Select"/>	SN#YK105183N129	other
<input checked="" type="checkbox"/>	3	NS Blade	SN#ZJ1SHA36G113	SN#ZJ1SHA36G113	<input type="button" value="Select"/>	SN#ZJ1SHA36G113	other
<input checked="" type="checkbox"/>	4	NS Blade	SN#J1S8J34W137	SN#J1S8J34W137	<input type="button" value="Select"/>	SN#J1S8J34W137	other
<input checked="" type="checkbox"/>	5	NS Blade	SN#J1SH936F118	SN#J1SH936F118	<input type="button" value="Select"/>	SN#J1SH936F118	other
<input checked="" type="checkbox"/>	6	NS Blade	SN#ZJ1TRL3AF13F	SN#ZJ1TRL3AF13F	<input type="button" value="Select"/>	SN#ZJ1TRL3AF13F	other
<input type="checkbox"/>	7	N/A	No blade present		<input type="button" value="Select"/>		other
<input checked="" type="checkbox"/>	8	NS Blade	BLADE#03	BLADE#03	<input type="button" value="Select"/>	BLADE#03	other
<input type="checkbox"/>	9	N/A	No blade present		<input type="button" value="Select"/>		other
<input type="checkbox"/>	10	N/A	No blade present		<input type="button" value="Select"/>		other
<input type="checkbox"/>	11	N/A	No blade present		<input type="button" value="Select"/>		other
<input type="checkbox"/>	12	N/A	No blade present		<input type="button" value="Select"/>		other
<input type="checkbox"/>	13	N/A	No blade present		<input type="button" value="Select"/>		other
<input type="checkbox"/>	14	N/A	No blade present		<input type="button" value="Select"/>		other

I/O Modules Configuration

	I/O Modules			Bull System Manager Hosts			
	Bay	Type	MacAddr	Name		netName	OS
<input checked="" type="checkbox"/>	1	ethernet	00:05:5D:7D:37:24	00:05:5D:7D:37:24	<input type="button" value="Select"/>	0.0.0.0	none
<input type="checkbox"/>	2	N/A	No switch present		<input type="button" value="Select"/>		none
<input type="checkbox"/>	3	N/A	No switch present		<input type="button" value="Select"/>		none
<input type="checkbox"/>	4	N/A	No switch present		<input type="button" value="Select"/>		none

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

- The left column allows you to select the bay corresponding to the element defined in the monitored chassis. Only the bay that contains an element can be selected to remain coherent with the CMM configuration.

- The central part displays element configuration as defined in the CMM. The bay number, the blade model (NS Blade or EL Blade) or the type of switch and the element ident are displayed.

The model of blade is setting according to the code of the product type. The mapping is configured in the `bladetype.cfg` file available in the `<BSM Directory>/core/share/bsmConfig..`

Note Element configuration as defined in the CMM cannot be modified.

- 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 bay is checked. You can select an already defined host ("other" model and Blade or I/O Switch modules model depending of the kind of element) by clicking the **Select** button or you can create a host by completing the corresponding field. By default, **Name** and **netName** are set with the ident of the element.

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

Blade Configuration							
	Blade Servers			Bull System Manager Hosts			
	Bay	Model	Ident	Name	Select	netName	OS
<input type="checkbox"/>	1	NS Blade	blade1	blade1	Select	blade1	other
<input type="checkbox"/>	2	NS Blade	blade2	blade2	Select	blade2	other
<input type="checkbox"/>	3	NS Blade	blade3	blade3	Select	blade3	other
<input type="checkbox"/>	4	NS Blade	blade4	blade4	Select	blade4	other
<input type="checkbox"/>	5	NS Blade	blade5	blade5	Select	blade5	other
<input type="checkbox"/>	6	NS Blade	blade6	blade6	Select	blade6	other
<input type="checkbox"/>	7	NS Blade	blade7	blade7	Select	blade7	other
<input type="checkbox"/>	8	NS Blade	blade8	blade8	Select	blade8	other
<input type="checkbox"/>	9	NS Blade	blade9	blade9	Select	blade9	other
<input type="checkbox"/>	10	NS Blade	blade10	blade10	Select	blade10	other
<input type="checkbox"/>	11	NS Blade	blade11	blade11	Select	blade11	other
<input type="checkbox"/>	12	NS Blade	blade12	blade12	Select	blade12	other
<input type="checkbox"/>	13	NS Blade	blade13	blade13	Select	blade13	other
<input type="checkbox"/>	14	NS Blade	blade14	blade14	Select	blade14	other

I/O Modules Configuration							
	I/O Modules			Bull System Manager Hosts			
	Bay	Type	MacAddr	Name	Select	netName	OS
<input type="checkbox"/>	1	unknown	switch1	switch1	Select	switch1	none
<input type="checkbox"/>	2	unknown	switch2	switch2	Select	switch2	none
<input type="checkbox"/>	3	unknown	switch3	switch3	Select	switch3	none
<input type="checkbox"/>	4	unknown	switch4	switch4	Select	switch4	none

Figure 3-14. Chassis Elements Definition without SNMP access

Notes

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

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

Blade Configuration							
	Blade Servers			Bull System Manager Hosts			
	Bay	Model	Ident	Name		netName	OS
<input checked="" type="checkbox"/>	1	NS Blade	BLADE#01	blade45_1	Select	192.168.207.41	other
<input checked="" type="checkbox"/>	2	NS Blade	SN#YK105183N129	blade45_2	Select	192.168.207.42	other
<input type="checkbox"/>	3	NS Blade	SN#ZJ1SHA36G113	SN#ZJ1SHA36G113	Select	SN#ZJ1SHA36G113	other
<input type="checkbox"/>	4	NS Blade	SN#J1S8J34W137	SN#J1S8J34W137	Select	SN#J1S8J34W137	other
<input type="checkbox"/>	5	NS Blade	SN#J1SH936F118	SN#J1SH936F118	Select	SN#J1SH936F118	other
<input type="checkbox"/>	6	NS Blade	SN#ZJ1TRL3AF13F	SN#ZJ1TRL3AF13F	Select	SN#ZJ1TRL3AF13F	other
<input type="checkbox"/>	7	N/A	No blade present		Select		other
<input checked="" type="checkbox"/>	8	NS Blade	BLADE#03	blade45_8	Select	192.168.207.48	other
<input type="checkbox"/>	9	N/A	No blade present		Select		other
<input type="checkbox"/>	10	N/A	No blade present		Select		other
<input type="checkbox"/>	11	N/A	No blade present		Select		other
<input type="checkbox"/>	12	N/A	No blade present		Select		other
<input type="checkbox"/>	13	N/A	No blade present		Select		other
<input type="checkbox"/>	14	N/A	No blade present		Select		other

I/O Modules Configuration							
	I/O Modules			Bull System Manager Hosts			
	Bay	Type	MacAddr	Name		netName	OS
<input checked="" type="checkbox"/>	1	ethernet	00:05:5D:7D:37:24	sw24	Select	0.0.0.0	none
<input type="checkbox"/>	2	N/A	No switch present		Select		none
<input type="checkbox"/>	3	N/A	No switch present		Select		none
<input type="checkbox"/>	4	N/A	No switch present		Select		none

Figure 3-15. Chassis Elements Re-discovery

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

After editing:

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

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

Host Topology Modification

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

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

Do you agree ?

YES
NO

Figure 3-16. NovaScale Blade confirmation

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

Related Blade Chassis Objects

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

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

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

Table 3-5. NS Blade Chassis objects

Chassis element edition

A chassis element has properties linked to the Blade Chassis and properties of a host object.

To add, move or modify properties linked to the chassis use the Blade Chassis edition page.

To modify host properties use the Host edition page.

Add an element to a chassis.

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

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

Remove an element from a chassis

To remove an element from a chassis uncheck the corresponding line in the elements Configuration part of the chassis edition form.

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

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

Modify an element linked to a chassis

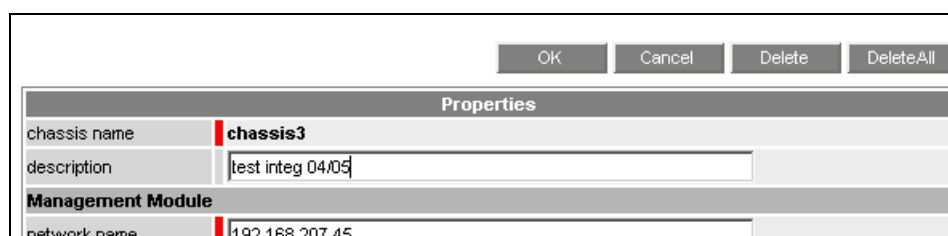
To modify the name of the BSM host corresponding to an element, enter the new name in the corresponding field or choose it in the list of already defined hosts in Bull System Manager by clicking the Select button.

To modify other characteristics (netName, OS...), use the Host edition form.

Notes

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

Deleting a Blade Chassis

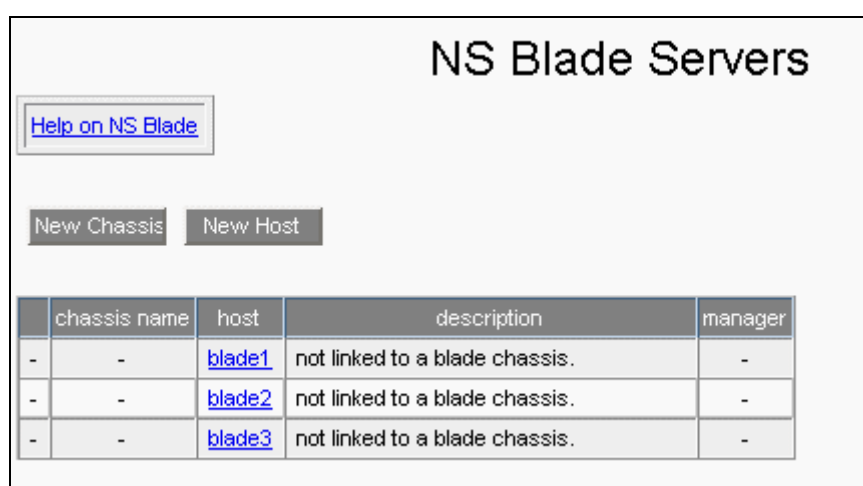


Properties	
chassis name	chassis3
description	test integ 04/05
Management Module	
network name	192.168.207.45

Figure 3-17. Deleting a Blade Chassis

There are two ways of deleting a Blade Chassis:

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



NS Blade Servers				
Help on NS Blade				
New Chassis New Host				
	chassis name	host	description	manager
-	-	blade1	not linked to a blade chassis.	-
-	-	blade2	not linked to a blade chassis.	-
-	-	blade3	not linked to a blade chassis.	-

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

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

3.1.3.2 Escala Blade

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

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

Procedures to create, modify or delete Escala Blade are similar to those described for the NovaScale Blade (see *NovaScale Blade*, on page 39). The main difference is the model of the standalone server, which is set to **EL Blade**.

Note	When the Escala Blade is declared with an OS set to VIOS, the Escala Blade edition is done with the Escala LPAR page, which allows to define the associated logical partitions (see <i>LPARs</i> , on page 56).
-------------	---

3.1.4 Defining Escala Hosts

3.1.4.1 PL Server

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

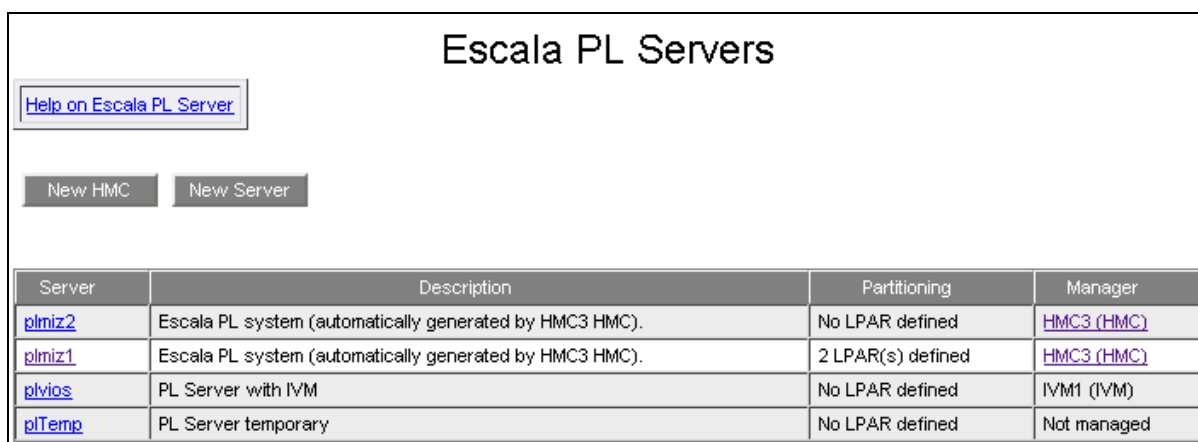
Escala PL Servers can be managed by an **HMC** (Hardware Management Console), a system that provides management tools for controlling one or more Escala PL Servers and associated LPARs. In this case, the platform contains a host representing the Central Electronics Complex (CEC).

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

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

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

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



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

Figure 3-19. Escala PL Servers

To create an HMC and the Escala PL Servers that it manages, click the **New HMC** button.

To create an Escala PL Server managed by IVM or not managed, click the **New Server** button.

To modify or delete an HMC, click the corresponding **HMC** link.

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

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



Important

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

3.1.4.1.1 HMC Managed PL Servers

HMC edition

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

HMC for Escala PL Servers

[Help on HMC](#)

OK Cancel

Properties

name: HMC1

description: Hardware Management Console

SSH Configuration

network name: 172.31.50.12

user: hscroot

identity file: id_dsa

Managed Systems

PL Servers

Discover To get the list of PL Systems from HMC, click the Discover button.

Figure 3-20. HMC Edition

HMC Information

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

description Short text describing the HMC.
"Hardware Management Console" in this example.

SSH Configuration

networkName	IP address used to access the HMC in Bull System Manager. "172.31.50.12" in this example.
user	User for ssh connection, "hscroot" in this example. Default value: <i>hscroot</i> The default value is those commonly used on HMC.
identityFile	File containing the key for ssh connection. "id_dsa" in this example. Default value: <i>id_dsa</i> The default value corresponds to the name of the key file automatically generated by BSM.

Managed Systems

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

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

PL Systems			Bull System Manager Platforms	
	Name	Nb LPARs	Name	
<input checked="" type="checkbox"/>	plmiz2	5	plmiz2	Select
<input checked="" type="checkbox"/>	plmiz1	8	plmiz1	Select

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

Figure 3-21. PL Servers discovery

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

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

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

Managed Systems

PL Servers

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

	PL Systems		Bull System Manager Platforms	
	Name	Nb LPARs	Name	
<input type="checkbox"/>	plmiz2	5	plmiz2	Select
<input checked="" type="checkbox"/>	plmiz1	8	plmiz1	Select
<input type="checkbox"/>	PL260R-Systest	2	PL260R-Systest	Select

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

Figure 3-22. PL Servers Re-discovery

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

After editing:

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

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

HMC for Escala PL Servers

Host Topology Modification

Configuration of the systems managed by **HMC3** will lead to the following modification in Topology:

- PL260R-Systest platform, PL260R-Systest host created and associated to PL260R-Systest partitioned system.
- plmiz2 platform, plmiz2 host no more used to represent HMC managed system.

Do you agree ?

YES **NO**

Figure 3-23. HMC Managed Systems Confirmation

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

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

Related HMC systems Objects

When an HMC system object is defined, related objects are automatically generated to configure the specific Supervision linked to this type of server. The following table describes the topology objects generated during the creation of an HMC system.

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

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

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

HMC managed PL server edition

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

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

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

Add a PL server to HMC Managed Systems

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

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

Remove a PL server from HMC Managed Systems

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

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

Modify a PL server managed by an HMC

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

To modify partitioning characteristics, use the **LPARs** edition form.

Notes

- To get the LPARs edition form corresponding to the PL server, click the **Server** link displayed in the global HMC form.
- When you rename a PL server, the host corresponding to the old name remains as a PL server not managed by an HMC.

Deleting HMC systems

From the HMC edition page, you can only delete the HMC definition by clicking the **Delete** button.

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

3.1.4.1.2 IVM Managed PL Server

The following form is used to define an IVM Managed PL Server.

Escala PL Series

[Help on Escala PL Series](#)

OK Cancel

Properties	
name	plvios
description	Escala PL managed with IVM
model	PL series
partitioning manager	<input type="radio"/> none <input checked="" type="radio"/> IVM

Integrated Virtualization Manager (IVM)	
name	IVM
I/O Server host	staix35_3 <input type="button" value="Select"/>
network name	129.183.12.35
user	padmin
identity file	id_dsa

Figure 3-24. IVM Managed PL Server

Server Information

name	The label used to identify the platform in Bull System Manager. "plvios" in this example.
description	Short text describing the platform. "Escala PL managed with IVM" in the example.
model	Model of the server
partitioning manager	Indicates if the server is managed by IVM or not. Must be set to IVM in this case.

Integrated Virtualization Manager Configuration

name	The label used to identify the manager
I/O Server host	Name of the host with VIOS partition. If the corresponding host is already defined, use the Select to set it.
networkName	IP address used to access the IVM in Bull System Manager. "172.31.50.35" in this example.
user	User for ssh connection, "padmin" in this example. Default value: padmin The default value is those commonly used on IVM.
identityFile	File containing the key for ssh connection. "id_dsa" in this example. Default value: id_dsa The default value corresponds to the name of the key file automatically generated by BSM.

-
- Notes**
- When the server has been initialized by this way, all modifications must be done from the LPAR edition page.
 - It is not possible to modify directly an IVM PL Server to a non managed PL Server. To perform it, first remove the platform, then configure a new PL Server as non managed.
-

3.1.4.1.3 Non managed PL Server

To define a non managed PL Server, use the previous form with the partitioning manager set to none.

Properties	
name	plnone
description	non managed PL Server
model	PL series
partitioning manager	<input checked="" type="radio"/> none <input type="radio"/> IVM

Figure 3-25. Non managed PL Server

To initialize the server, just enter a valid name.

3.1.4.2 LPARs

3.1.4.2.1 Platform edition

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

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

Figure 3-26. Escala LPARs page

It is possible:

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

Note By clicking the **Server** link in PL Server or EL Blade page, you directly access the edition page of the platform.

When you click the **Server** link of an HMC managed system, the following page is displayed:

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

Figure 3-27. HMC managed Escala LPAR platform

When you click the **Server** link of an IVM managed system, the following page is displayed:

Properties	
name	plvios
description	PL Server with IVM
Integrated Virtualization Manager (IVM)	
name	IVM1
I/O Server host	staix35_2
network name	129.183.12.35
user	ipadmin
identity file	id_dsa
Logical Partitions	
<input type="button" value="Discover"/> To get the list of logical partitions, click the Discover button	

Figure 3-28. IVM managed Escala LPAR platform

When you click the Server link of a non managed system, the following page is displayed:

Properties																					
name	plTemp																				
description	PL Server temporary																				
Logical Partitions																					
Platform not linked to managed system. You can define Bull System Manager Hosts for pseudo LPAR: Select LPAR to associate them to the Escala PL platform by clicking the corresponding checkbox. Then, map each LPAR to a defined Bull System Manager host or choose to create a new.																					
<input checked="" type="checkbox"/>	<table border="1"> <thead> <tr> <th colspan="2">Escala PL Logical Partitions</th> <th colspan="3">Bull System Manager Configuration</th> </tr> <tr> <th></th> <th>Name</th> <th>Name</th> <th>netName</th> <th>OS</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/></td> <td>lpar1</td> <td>lpar1</td> <td>lpar1</td> <td>other</td> </tr> <tr> <td><input checked="" type="checkbox"/></td> <td>lpar2</td> <td>lpar2</td> <td>lpar2</td> <td>other</td> </tr> </tbody> </table>	Escala PL Logical Partitions		Bull System Manager Configuration				Name	Name	netName	OS	<input checked="" type="checkbox"/>	lpar1	lpar1	lpar1	other	<input checked="" type="checkbox"/>	lpar2	lpar2	lpar2	other
Escala PL Logical Partitions		Bull System Manager Configuration																			
	Name	Name	netName	OS																	
<input checked="" type="checkbox"/>	lpar1	lpar1	lpar1	other																	
<input checked="" type="checkbox"/>	lpar2	lpar2	lpar2	other																	
VIO Servers No VIO server currently configured.																					
<input type="button" value="Add-LPAR"/> To define new LPAR, click the Add-LPAR button																					

Figure 3-29. Non managed Escala LPAR platform

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

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

Platform Properties

name	Platform short name. This name is displayed in the Bull System Manager Console view.
description	Short text describing the platform. This information is displayed in an info tip in the Management Tree when you move the mouse over the node associated to the platform.
CEC	Name of the system referenced by HMC manager. This property is shown only if the system is managed by an HMC and is not editable (set in HMC edition form).

Hardware Management Console Properties

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

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

Integrated Virtualization Manager properties

name	Manager short name. This property is editable only during the first edition of the platform.
I/O Server host	Name of the Escala server that contains the VIOS partition. This property is not editable (set in Escala Server edition form).
network name	Hostname or IP address of the VIOS partition.
user	Remote user to login. Default value: <i>padmin</i>
identity file	File containing the key for ssh connection. This value cannot be changed. Identity files are generated at BSM installation, with specific rights.

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

Logical Partitions Properties

For managed platform:

List of the partitions established by selecting the partitions obtained by remote command on HMC or IVM.

The request is performed by clicking the **Discover** button (or **Re-discover** if you are in edition mode).

For non managed platform:

The **Discover** button is not available, but a **Add-LPAR** button is available to add as many partition definitions as you want.

All partitions' information must be filled in by the user.

Notes

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

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

The screenshot shows a confirmation dialog titled "HMC managed Escala LPAR Platform". Inside the dialog, there is a section titled "Host Topology Modification". Below this title, the text states: "Configuration of the Escala PL platform will lead to the following modification in Host Topology:" followed by two bullet points: "- brad host created (model Escala LPAR) to represent LPAR brad as element of platform plmiz1_lpars." and "- cervin host created (model Escala LPAR) to represent LPAR cervin as element of platform plmiz1_lpars." Below the text, it asks "Do you agree ?" and provides two buttons: "YES" and "NO".

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

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

After edition:

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

-
- | | |
|--------------|---|
| Notes | <ul style="list-style-type: none">• An HMC managed platform cannot be deleted: you must first remove the platform from the list of managed systems from the HMC page, and then you can delete it.• When platform is deleted, LPARs remain as standalone host.• When IVM platform is deleted, the host representing the VIOS is modified with OS set to other (Delete or DeleteAll action). |
|--------------|---|
-

Related HMC managed platform Objects

When a HMC managed platform is defined, related objects are automatically generated. The following table describes the objects generated during the creation of the platform.

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

Related IVM managed platform Objects

When a IVM managed platform is defined, related objects are automatically generated. The following table describes the objects generated during the creation of the platform.

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

3.1.4.2.2 LPAR edition

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

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

Changing host properties must be done from the Host edition page.

Logical Partitions Discovery

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

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

Logical Partitions

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

<input checked="" type="checkbox"/>	Escala Logical Partition		Bull System Manager Configuration		
	Name	Id	Name	netName	OS
<input checked="" type="checkbox"/>	galilei	2	galilei <input type="button" value="Select"/>	galilei	other ▼
<input checked="" type="checkbox"/>	tyrex	3	tyrex <input type="button" value="Select"/>	tyrex	other ▼
<input checked="" type="checkbox"/>	erale	4	erale <input type="button" value="Select"/>	erale	other ▼
<input checked="" type="checkbox"/>	peg3	5	peg3 <input type="button" value="Select"/>	peg3	other ▼
<input checked="" type="checkbox"/>	essai	6	essai <input type="button" value="Select"/>	essai	other ▼

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

Figure 3-31. Logical Partitions display after Discover step

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

Logical Partitions

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

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

<input type="checkbox"/>	Escala Logical Partition		Bull System Manager Configuration		
	Name	Id	Name	netName	OS
<input type="checkbox"/>	lpar1	1	lpar1 <input type="button" value="Select"/>	lpar1	other ▼
<input type="checkbox"/>	lpar2	2	lpar2 <input type="button" value="Select"/>	lpar2	other ▼

To define new LPAR, click the Add-LPAR button

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

Figure 3-32. Logical Partitions display after Discovery failure

Logical Partitions Re-Discovery

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

- add logical partition not yet registered in the Escala LPAR platform
- remove logical partitions no longer defined in the manager configuration.

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

The screenshot shows a web interface titled "Logical Partitions". It contains a table with two main sections: "Escala Logical Partition" and "Bull System Manager Configuration".

Escala Logical Partition			Bull System Manager Configuration			
	Name	Id	Name	netName	OS	
<input checked="" type="checkbox"/>	galilei	2	galilei	Select	10.10.10.10	aix
<input type="checkbox"/>	tyrex	3	tyrex	Select	10.10.10.10	aix
<input type="checkbox"/>	erable	4	erable	Select	erable	other

Below the table, there is a "Re-discover" button and a note: "To update the list of LPAR, click the Re-discover button".

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

Partitions no longer defined in the manager (in the example above, *tyrex*) are automatically unchecked and will be removed from the platform on form validation.

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

Add a logical partition to a platform

Adding a logical partition is performed by checking the corresponding line in the Logical Partitions part of the platform edition form and setting the host characteristics in the BSM Configuration table zone (by filling in the corresponding fields or by selecting an already defined host).

Remove a logical partition from a platform

Removing a logical partition is performed by unchecking the corresponding line in the Logical Partitions part of the platform.

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

Modify a logical partition defined in a platform

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

To modify other characteristics such as **netName** or **OS**, you must use the Host edition form.

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

Delete all logical partitions and corresponding hosts

To delete all logical partitions and corresponding hosts, use the **DeleteAll** button of the LPAR platform Edition form. Beware: the Vios server and the platform will be also deleted from the Bull System Manager configuration.

Note When the server is managed by an HMC, additional informations like partition type (vioserver or aixlinux) or proc mode (shared, dedicated ...) are displayed for the LPARs.

3.1.5 Defining Device Hosts

3.1.5.1 I/O Switch Modules

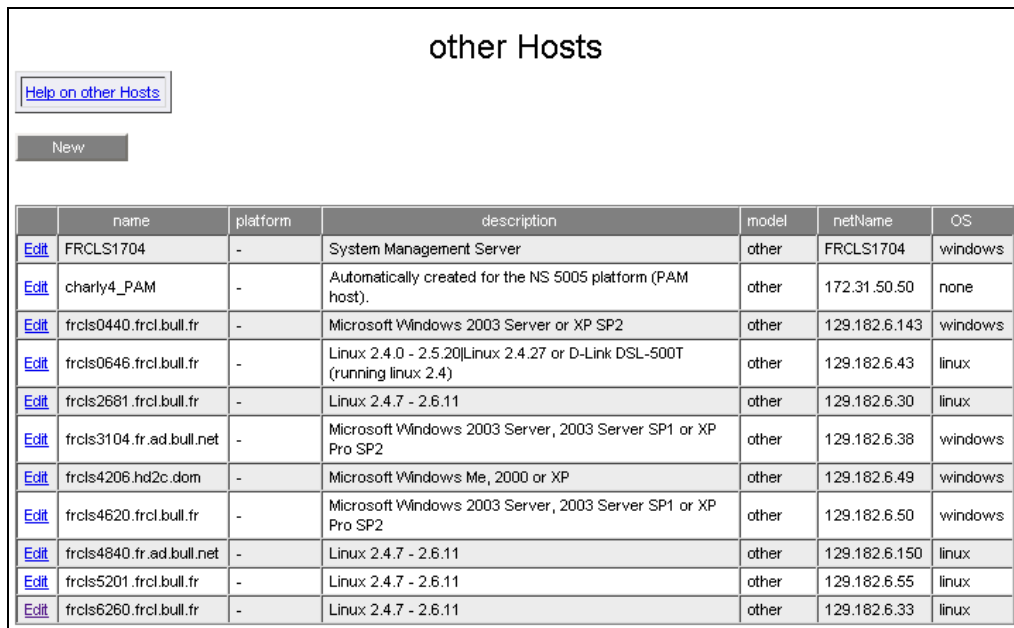
I/O Switch Modules are usually housed in the Blade Chassis and managed with the Chassis Monitoring Module (CMM).

To configure modules, expand the Device Hosts menu and select the I/O Switch Modules menu item.

Procedures to create, modify or delete I/O Switch Modules are similar to those described for the NovaScale Blade (see *NovaScale Blade*, on page 39). The main difference is the model of the standalone server, which is set to **I/O Switch Module**.

3.1.6 Defining Other Hosts

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



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

Figure 3-34. Hosts configuration window

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

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

Note See *Create / Edit / Delete Resources*, on page 19 for details.

3.1.6.1 Host Properties

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

other Host

OKCancelDelete

Properties

name

FRCLS1704

description

System Management Server

model

other

network name

FRCLS1704

parents

Selected Hosts

<= Add

Remove =>

All Hosts

FRCLS1704

HV4

LPAR1

Vermillion

Vesuve

OS family

windows

OS info

[Edit Supervision Properties](#)

The following 1 object(s) are using the FRCLS1704 object:

'hostgroup'-object: [BSM](#)

Figure 3-35. Host properties

Host Properties	Description
name	Host short name (label). This name is the one displayed in the Bull System Manager Console views. Generally, this label is the host name. Note: In the configuration, the host name MUST be different from the following reserved keys: "*", "none" and "auto". The name can be modified once the host is created, except if it is related to another BSM object.
description	Description of the host. This description is displayed in an info tip in the Management Tree when you move the mouse over the node associated with this host.
model	This field is setting according to the menu item (Other) and is not editable. Modification of the model is done by selecting the host during the edition of a specific model.
network name	Host network name (hostname or IP address). Default value: host name (label).
parents	List of hosts that link the host with remote hosts. For instance, a host representing a network equipment (router, switch...) is typically a parent host.
OS family	Operating System type (Windows, Linux, aix, other, none). Default value: <i>other</i> .

Host Properties	Description
OS info	When a host is discovered by Discovery , certain properties are set automatically. This is the case of OS info , which gives information about the OS running on the host. If description is empty, it is automatically set to the same value as OS info .

Table 3-6. Host properties

3.1.6.2 Example: Adding a Host

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

To perform this task, follow these steps:

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

Step 2: Start Bull System Manager Configuration.

Step 3: Declare the new host.

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

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

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

1. Launch the WEB browser with the Bull System Manager home page URL:
`http://<Bull System Manager server>/BSM/`
2. Select **Download** and then follow the instructions.

Step 2: Start Bull System Manager Configuration

See *Starting the Configuration GUI*, on page 9.

Step 3: Declare the New Host

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

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

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

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

- name** A label used to identify the host in Bull System Manager, `FRCLS2681` in the example.
- description** Short text describing the host, `Linux server` in the example.
- network name** Host identification on the LAN (name or IP address), `frcls2681.frcl.bull.fr` in the example.
- OS family** Host Operating System, **Linux** in the example.

Once completed, the form will look as follows:

other Host

OK Cancel Delete

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

[Edit Supervision Properties](#)

Figure 3-36. Declaration form for a host

Click **OK** to validate.

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

Step 4: Save and Reload

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

3.2 Configuring Hostgroups

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

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

The administrator can:

- specify new Hostgroups
- change the properties of an already defined Hostgroup
- delete a Hostgroup that is no longer to be monitored.

3.2.1 Hostgroups

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

The way to create a new Hostgroup and to edit or delete a Hostgroup is described in *Create / Edit / Delete Resources*, on page 19.

The following figure shows the form displayed to edit Hostgroup properties.

The screenshot shows the 'Properties' form for a Hostgroup named 'BSM'. The form is divided into several sections:

- name:** BSM
- description:** Bull System Manager elements
- host members:** A section with two lists: 'Selected Hosts' (containing 'frcls1704') and 'All Hosts' (containing '199.182.250.30', 'BL265', 'Blade#3', 'SN#YL10W727600E', 'blade45_1'). Between the lists are buttons '<= Add' and 'Remove =>'.
- hostgroup members:** A section with two lists: 'Selected Hostgroups' (empty) and 'All Hostgroups' (containing 'charly4', 'chassis3', 'chassis3_blade', 'chassis3_iosm', 'chassis65'). Between the lists are buttons '<= Add' and 'Remove =>'.

At the bottom of the form, a message states: 'The following 1 object(s) are using the BSM object:'. Below this, a list shows: 'map-object: [default](#)'.

Figure 3-37. Hostgroup properties

Hostgroup Properties

Description

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

Note Take care not to select the same resource twice in the **Selected Objects** list. If you do, click the occurrence of this resource and click **Remove**.

3.2.2 Platforms

Particular hostgroups are defined to represent hardware platforms or virtualization platforms. Type of the platform is represented by an additional hostgroup attribute, the 'model' attribute.

They appear in specific table in the Hostgroups page, as displayed in the following figure:

Hostgroups Topology

New Hostgroup

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

Platforms (Edit only)

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

Figure 3-38. Hostgroups

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

3.3 Configuring Clusters

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

Attached to a cluster, you add a monitoring rule:

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

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

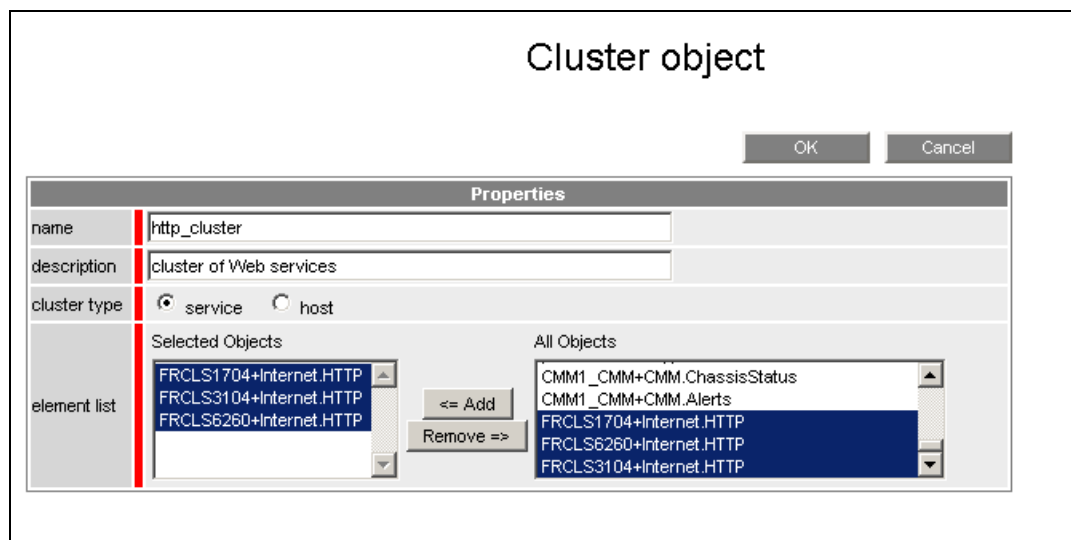


Figure 3-39. Defining Cluster object

Cluster object supervision

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

OK Cancel

Properties	
name	http_cluster
description	cluster of Web services
cluster type	service
element list	FRCLS1704+Internet.HTTP,FRCLS3104+Internet.HTTP,FRCLS6260+Internet.HTTP
Monitoring attributes	
hosted category	FRCLS1704+Internet
status	<input checked="" type="radio"/> active <input type="radio"/> inactive
Monitoring command attributes (for this service)	
warning threshold	2
critical threshold	3
monitoring period	24x7
polling interval	5 mn (5 mn by default if empty)
Notification attributes (for this service)	
e-mail contact groups	<div> <div>Selected Objects</div> <div>mgt-admins</div> <div>All Objects</div> <div>mgt-admins</div> <div><= Add</div> <div>Remove =></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 type="radio"/> Yes <input checked="" 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 3-40. Defining Cluster object supervision

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

Table 3-7. Cluster properties

The result in the console is the following:

○

SERVICE: Internet.http_cluster on FRCLS1704

Monitoring

Reporting

Inventory

Operations

Service Status

Control

Service detail

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

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

Figure 3-41 . Cluster supervision

3.4 Configuring a Hardware Manager

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

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

3.4.1 Editing Properties

To configure the Hardware Manager, click the **Hardware** link in the **Managers View** part of the **Topology** tab. The way to create, edit or delete a manager is described in *Create / Edit / Delete Resources*, on page 19. The following figure shows the form displayed to edit Hardware Manager properties.

The screenshot shows the 'Hardware Manager' dialog box with the 'Properties' tab selected. The dialog has a title bar 'Hardware Manager' and a 'Help on Hardware Manager attributes' link. At the top right are 'OK' and 'Cancel' buttons. The 'Properties' section contains the following fields:

- name:** A text field.
- description:** A text field containing 'platform manager'.
- type:** A section with radio buttons for 'NovaScale' (PAM, CMM, ISM), 'Escala' (HMC), and 'Other' (selected).
- network name:** A text field.

Below the 'Properties' section is the 'Managed hosts' section, which includes:

- element list:** A list box on the left.
- Selected Hosts:** A list box in the middle.
- All Manageable Hosts:** A list box on the right containing the following items: 172.31.50.90, 172.31.50.97, CHARLY4W, FRCLS1704, and FRCLS3104.
- Buttons:** '<= Add' and 'Remove >=' buttons between the 'Selected Hosts' and 'All Manageable Hosts' list boxes.

At the bottom is the 'Application attributes' section with a 'GUI URL' text field.

Figure 3-42. Hardware manager properties

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

Hardware Manager Properties

Description

name	Hardware manager name. This name is seen in the Console Managers view.
description	Description of the resource. This description is displayed in an info tip in the Management Tree when the mouse is hovered over the node associated with this resource.
type	Type of manager (PAM, CMM, ISM, HMC or other).
network name	Manager network name or IP address. Default value: the manager name (label).
element list	Elements that this manager will have to manage. For editable manager (ISM or other), these elements are selected in the All Objects list and moved to the Selected Objects list using the Add button, and vice-versa using the Remove button. Depending on the type of manager, the All Resources list contains: <ul style="list-style-type: none">• all NovaScale 5000 & 6000 series platforms if the manager type is PAM,• all NS Blade Chassis if the manager type is CMM,• all NovaScale 4000 series hosts if the manager type is ISM,• all Escala PL series server if HMC,• all hosts if the manager type is other.

Table 3-8. Hardware manager properties

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

Specific PAM Properties

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

Specific ISM Properties

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

Specific CMM Properties

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

Other Properties

GUI URL	HTTP URL of the manager GUI.
----------------	------------------------------

3.5 Configuring a Storage Manager

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

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

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

3.5.1 Editing Properties

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

The way to create, edit or delete a manager is described in 2.6.1 *Create / Edit / Delete Resources*, on page 19.

The following figure shows the form displayed to edit Storage Manager properties.

Storage Manager object

[Help on Storage Manager attributes](#)

OK Cancel

Properties

name	stmgr1
description	storage manager
type	other
network name	stmgr1

Managed hosts

Selected		All Host Name
Host Name [Storage Id]		
172.31.50.90 [172.31.50.90]	<= Add Remove =>	172.31.50.90
172.31.50.97 [172.31.50.97]		172.31.50.97
		CHARLY4W
		CMM1_CMM
		FRCLS1704

Application attributes

GUI URL	
---------	--

Figure 3-43. Storage manager properties

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

Table 3-9. Storage manager properties

3.6 Configuring a Virtualization Manager

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

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

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

3.6.1 Editing Properties

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

The way to create, edit or delete a manager is described in *Create / Edit / Delete Resources*, on page 19.

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

The screenshot shows a web-based form titled "Properties" for editing a Virtualization Manager. The form is divided into several sections:

- Properties:** This section contains four input fields: "name" (empty), "description" (containing "virtual manager"), "type" (containing "other"), and "network name" (empty).
- Virtualization Platform:** This section contains an "element list" on the left, which is currently empty. To its right are two lists of hosts: "Selected Hosts" (empty) and "All Hosts" (containing "frcls1704"). Between these lists are two buttons: "<= Add" and "Remove =>".
- Application attributes:** This section contains a single input field for "GUI URL" (empty).

Figure 3-44. Virtualization Manager properties

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

Table 3-10. Virtualization Manager properties

Chapter 4. Configuring Inventory

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

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

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

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

To enable `updateInventory` task :

1. Click the **Periodic Tasks** link in the **Functionalities** part of the **GlobalSetting** tab.
2. Click the **Edit** link of the "`updateInventory`" task. The list of its properties appears:

Properties	
name	<code>updateInventory</code>
description	periodic task to update inventory
period	00***
enable	<input type="radio"/> Yes <input checked="" type="radio"/> No
Command description	
command	/bin/update_ALLinventory.sh

Figure 4-1. `updateInventory` periodic task properties

- Modify the period if needed:
the periodicity is defined on five fields as standard cron format: <minute(0-59)> <hour(0-23)> <day of month(0-31)> < month(0-12) or names> <day of week(1-7) or name>".
A field may be an asterisk (*), which always stands for 'first-last': for instance "00 22 * * *" corresponds to a daily execution at 22h.
Range or list of numbers are allowed: for instance "8-11" in hour field specifies execution at hours 8, 9, 10 and 11.
Steps can be used in conjunction with ranges or after asterisk: for instance "*/5" in minute field specifies execution every five minutes.
See *CRON Reference Manual* to get detailed informations.
By default the task is scheduled daily at 00:00.
- Enable the task. By default the task is disabled.
- Click **OK** to validate.

Chapter 5. Configuring Supervision

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

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

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

5.1 Configuring Categories and Services


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

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

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

The administrator can change the default-monitoring configuration by:

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

Note The categories and services related to Hardware or Storage supervision are automatically generated for each concerned host by the BSM Configuration "Hosts Definition" part. There is no template for these categories and services which are represented by the  icon (see *Generated Categories and Services* on page 211).

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

Categories and Services

[Help on Categories and Services](#)

No Filter

Filter by OS ☐


Filter by MODEL ☐

Filter by HOST(S) ☐

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

☒ Expand all

☐ Collapse all

 [manage categories](#)

All active Categories and Services











	Name & Description	OS	Model	HostList	Actions
<input checked="" type="checkbox"/>	EventLog		any	*	edit manage services
<input checked="" type="checkbox"/>	FileSystems		any	*	edit manage services
<input checked="" type="checkbox"/>	LinuxServices		any	*	edit manage services
<input checked="" type="checkbox"/>	LogicalDisks		any	*	edit manage services
<input checked="" type="checkbox"/>	Syslog		any	*	edit manage services
<input checked="" type="checkbox"/>	Syslog		any	*	edit manage services
<input checked="" type="checkbox"/>	SystemLoad		any	*	edit manage services
<input checked="" type="checkbox"/>	SystemLoad		any	*	edit manage services
<input checked="" type="checkbox"/>	SystemLoad		any	*	edit manage services
<input checked="" type="checkbox"/>	WindowsServices		any	*	edit manage services

Figure 5-1. Categories and services page

This page is divided into two parts:

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

5.1.1 Categories

5.1.1.1 Default Categories

Bull System Manager provides the following default categories:

Unused template categories:

- Internet
- Reporting
- Network

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

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

Default categories applied to Windows hosts:

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


Default categories applied to Linux hosts:

- FileSystems
- Syslog
- LinuxServices
- SystemLoad
- HDisks

Default categories applied to AIX hosts:

- FileSystems
- Syslog
- AIXServices
- SystemLoad

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

Automatically generated categories are represented by the  icon (see *Generated Categories and Services* on page 211).

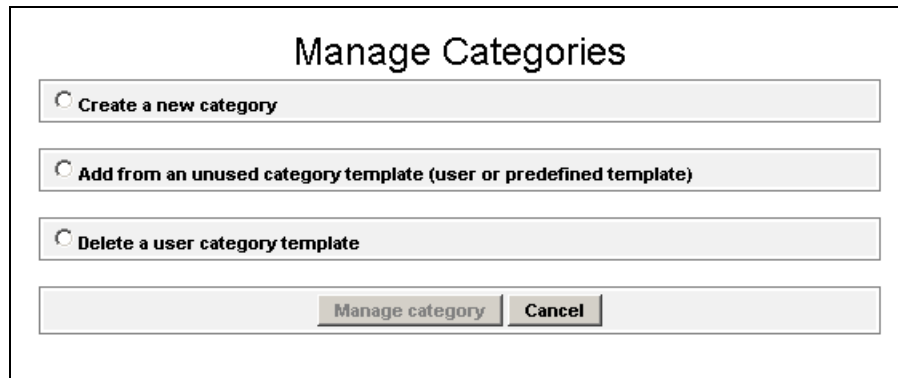
Category Properties	Description
Name	Category name.
description	Category description.
Model	Supported host model to which the category can apply. Default value: any .
OS family	Operating system type (Windows, Linux, AIX, any) Default value: any .
Monitoring domain	The monitoring domain of the category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

Notes

- The host list expression of a category is always a subset of the configured hosts. A host list **MUST NOT** mix the **not (!) hosts** list with other types of expressions (**hosts list, none** or *****). For instance, the expression `!h1, h2, h3` is ambiguous and is forbidden.
 - The categories linked to hardware or storage management are automatically generated and cannot be edited with the category form.
 - The category Monitoring domain property is used when you want to disable a monitoring domain for a host or a Hostgroup (see *Example: Monitoring NS 4000 Hardware* on page 128).
-

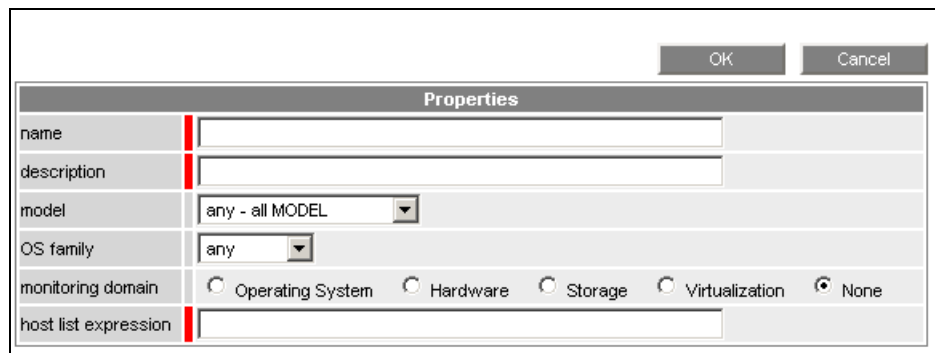
5.1.1.3 Creating a new Category

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



The 'Manage Categories' popup window has a title bar with the text 'Manage Categories'. Below the title bar, there are three radio button options: 'Create a new category', 'Add from an unused category template (user or predefined template)', and 'Delete a user category template'. At the bottom of the window, there are two buttons: 'Manage category' and 'Cancel'.

Figure 5-2. Manage Categories popup



The 'Category properties edition' window has a title bar with 'OK' and 'Cancel' buttons. Below the title bar, there is a 'Properties' section with the following fields: 'name' (text field), 'description' (text field), 'model' (dropdown menu with 'any - all MODEL' selected), 'OS family' (dropdown menu with 'any' selected), 'monitoring domain' (radio buttons for 'Operating System', 'Hardware', 'Storage', 'Virtualization', and 'None', with 'None' selected), and 'host list expression' (text field).

Figure 5-3. Category properties edition

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

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

5.1.1.4 Customizing a Category

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

Properties	
name	EventLog
description	Windows services
model	any
OS family	Windows family
monitoring domain	<input checked="" type="radio"/> Operating System <input type="radio"/> Hardware <input type="radio"/> Storage <input type="radio"/> Virtualization <input type="radio"/> None
host list expression	*

Figure 5-4. Customizing a category

Click **OK** to validate your customization.

5.1.1.5 Adding a Category from a Template

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

Manage Categories					
<input type="radio"/> Create a new category					
<input checked="" type="radio"/> Add from an unused category template (user or predefined template)					
check	Name	Description	Os	Model	hostList
<input type="radio"/>	AIXServices	Linux processes status	aix	any	*
<input type="radio"/>	FileSystems	FileSystem services	aix	any	*
<input checked="" type="radio"/>	Internet	Internet services	any	any	none
<input type="radio"/>	Network	Network monitoring	any	any	none
<input type="radio"/>	Template	Alert template	any	any	none
<input type="radio"/>	reporting	Indicators collected by MRTG	any	any	none
<input type="radio"/> Delete a user category template					
<input checked="" type="button" value="Add from the selected category"/> <input type="button" value="Cancel"/>					

Figure 5-5. Manage Categories popup

Properties	
name	Internet
description	Internet services
model	any
OS family	any
monitoring domain	<input type="radio"/> Operating System <input type="radio"/> Hardware <input type="radio"/> Storage <input type="radio"/> Virtualization <input checked="" type="radio"/> None
host list expression	none

Figure 5-6. Add Category from template

Click OK to add this category.

5.1.1.6 Deleting a User Category Template

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

☐ Create a new category

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

☒ Delete a user category template

check	Name	Description	Os	Model	hostList
<input checked="" type="radio"/>	NS4000_category	NS 4000 specific supervision	any	NS 4000	*

Delete the selected category **Cancel**

Figure 5-7. Delete Category template

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

5.1.2 Services

5.1.2.1 Default Services

Bull System Manager provides the following services:

Default services applied to Windows host:

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

Unused services for a Windows host:

- **C**, which monitors the percent of used space for the local disk C
- **Com**, which monitors the Windows services ensuring Com+ notifications functions
- **Networking**, which monitors the Windows services ensuring networking functions
- **Peripherals**, which monitors the Windows services ensuring peripherals management functions.

Default services applied to Linux host:

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

Unused services for a Linux host:

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

Default services applied to AIX host:


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

Unused services for a AIX host:

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

Unused services for Windows, AIX and Linux hosts:

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

Note Automatically generated services are represented by the  icon, (see *Generated Categories and Services* on page 211).

5.1.2.2 Service Properties

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

Service Properties	Description
status	<p>Monitoring status (active, inactive). Default value: active.</p> <p>Active status means that the service is checked. The service is visible as a node of the host in the Management Tree.</p> <p>Inactive status means that the service is not checked. It is not visible in the Management Tree. This field may be used to activate/deactivate temporarily the service check.</p>
monitoring on event	<p>Indicates if the service check is initiated and performed by external applications, as SNMP Traps, for instance. Default value: 0</p>
monitoring by polling	<p>Indicates if the service check is initiated by the BSM server and performed on a regular manner. Default value: 1</p> <p>When this option is set, the check command, monitoring period and polling interval must be filled in (see below)</p>
check command	<p>The Check box contains the check command. The Parameters box contains check command parameters.</p> <p>Linux Check Commands: All Linux check commands are launched by the check_nrpe command. The check command is the first parameter of the command: <code>/opt /BSMAgent/nrpe/libexec/check_nrpe</code> It must not be modified.</p> <p>This parameter is available only if the 'monitoring by polling' attribute is set to 1.</p>
monitoring period	<p>Time during which the service must be checked. Default value: 24x7. This parameter is available only if the 'monitoring by polling' attribute is set to 1.</p>
polling interval	<p>Number of minutes to wait between regular service checks. Default value: 5 min.</p> <p>This parameter is available only if the 'monitoring by polling' attribute is set to 1.</p>
e-mail contact groups	<p>Name of the contact groups that must be notified if a problem is reported by this service. Default value: mgt-admins.</p>
enable Bull autocall	<p>Enable the autocall mechanism. Default value: No.</p>
enable SNMP trap	<p>Enable SNMP trap notification. Default value: Yes.</p>
notification period	<p>Time during which service notifications must be sent out. Default value: 24x7.</p>
re-notification interval	<p>Number of minutes to wait before re-notifying a contact that service status is still WARNING or CRITICAL (after the notification made immediately after the problem occurred). Default value: 0 (no re-notification).</p>

Service Properties	Description
notify if warning	Notify contacts when service status is at WARNING level.
notify if critical	Notify contacts when service status is at CRITICAL level.
notify if recovery	Notify contacts when service status is at RECOVERY level.

Table 5-1. Service properties

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

Notes

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

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

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

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

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

5.1.2.3 Creating a New Service

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

The image shows a 'Manage Services' popup window. At the top, it says 'Manage Services' and 'for category : EventLog[windows,any]'. Below this, there are three radio button options: 'Create a new service', 'Add from a service template (user or predefined template)', and 'Delete a user service template'. At the bottom, there are two buttons: 'Manage service' and 'Cancel'.

Figure 5-8. Manage services popup

Properties	
category	EventLog
name	<input type="text"/>
description	<input type="text"/>
model	any
OS family	Windows family
host list expression	<input type="text"/>
Monitoring attributes	
status	<input checked="" type="radio"/> active <input type="radio"/> inactive
Monitoring command attributes (for this service)	
monitoring on event	<input type="radio"/> Yes <input checked="" type="radio"/> No
monitoring by polling	<input checked="" type="radio"/> Yes <input type="radio"/> No
check command	<input type="text"/>
check command parameters	<input type="text"/>
monitoring period	24x7
polling interval	5 mn (5 mn by default if empty)
Notification attributes (for this service)	
e-mail contact groups	<div> <div>Selected Objects</div> <div> <input type="text" value="mgt-admins"/> </div> </div> <div> <input type="button" value="Add"/> <input type="button" value="Remove"/> </div> <div> <div>All Objects</div> <div> <input type="text" value="mgt-admins"/> <input type="text" value="mgt-report"/> </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 type="radio"/> Yes <input checked="" 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 5-9. Service properties edition

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

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

See Example *Creating a New Category and a New Service* on page 101 to get a detailed description.

5.1.2.4

Customizing a Service

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

Properties	
category	EventLog
name	Security
description	monitors the Security Event Log for Audit Success, Audit Failure, W
model	any
OS family	Windows family
host list expression	*
Monitoring attributes	
status	<input checked="" type="radio"/> active <input type="radio"/> inactive
Monitoring command attributes (for this service)	
monitoring on event	<input type="radio"/> Yes <input checked="" type="radio"/> No
monitoring by polling	<input checked="" type="radio"/> Yes <input type="radio"/> No
check command	check_ns_eventlog
check command parameters	!0!strlog='Security'!wWWarn=1!eAudF=1!eErr=1
monitoring period	24x7
polling interval	5 mn (5 mn by default if empty)
Notification attributes (for this service)	
e-mail contact groups	<div> <div>Selected Objects</div> <div> mgt-admins </div> </div> <div> <div>All Objects</div> <div> mgt-admins mgt-report </div> </div> <div> <div><= Add</div> <div>Remove =></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 type="radio"/> Yes <input checked="" 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 5-10. Customize service

5.1.2.5 Adding a Service from a Template

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

for category : NS4000_category[any,NS 4000]

☐ Create a new service

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

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

☐ Delete a user service template

Figure 5-11. Manage service popup

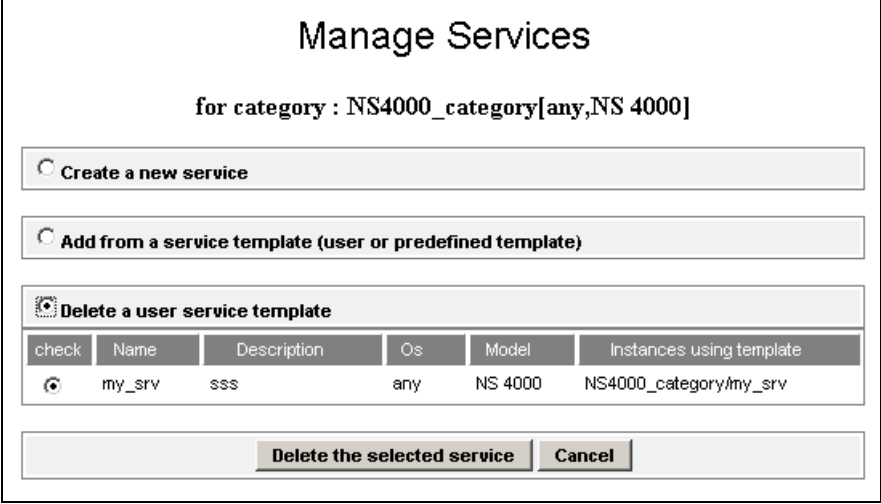
Properties	
category	NS4000-category
name	Sensor2Status
description	checks the sensor (Watt,Percentage,Pressure) reported by the IPM
model	any
OS family	any
host list expression	none
Monitoring attributes	
status	<input checked="" type="radio"/> active <input type="radio"/> inactive
Monitoring command attributes (for this service)	
monitoring on event	<input type="radio"/> Yes <input checked="" type="radio"/> No
monitoring by polling	<input checked="" type="radio"/> Yes <input type="radio"/> No
check command	check_IPMI_sensor
check command parameters	'sensor name'-m lanplus
monitoring period	24x7
polling interval	5 mn (5 mn by default if empty)
Notification attributes (for this service)	
e-mail contact groups	<div> <div>Selected Objects</div> <div> mgt-admins </div> </div> <div> <div>All Objects</div> <div> mgt-admins mgt-report </div> </div> <div> <= Add Remove => </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 5-12. Add service from template

Click OK to add the service in the selected category.

5.1.2.6 Deleting a User Service Template

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



Manage Services

for category : NS4000_category[any,NS 4000]

☐ Create a new service

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

☒ **Delete a user service template**

check	Name	Description	Os	Model	Instances using template
<input checked="" type="radio"/>	my_srv	sss	any	NS 4000	NS4000_category/my_srv

Delete the selected service **Cancel**

Figure 5-13. Delete service template

This will delete this service template with all its instances.

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

5.1.3 Check Commands

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

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

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

Table 5-3. Check commands list

5.1.4 Examples

5.1.4.1 Creating a New Category and Adding a Service

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

1. Click the **Categories/Services** link in the **Supervision** tab.
2. From the **Categories/Services** page, click **Filter by OS** and select **Windows**.
3. Click **manage category**.
4. In the **Manage Category** popup window, check **Create a new category** and click **create a new category**.
 - Enter the name of the category: `my_category`.
 - Enter its description.
 - The **OS family** text field is already filled in with Windows. It is not editable because of the used filter (if you choose **no filter** this text field becomes editable).
 - Choose the monitoring domain.
 - Set **host list expression** to `"*"`
5. Click **OK** to validate. The new category is now displayed in the Categories and Services list:












Categories and Services found for : <i>Windows</i>					
	Name & Description	OS	Model	HostList	Actions
	✓ my_category		any	*	edit manage services
	✓ EventLog		any	*	edit manage services
	✓ LogicalDisks		any	*	edit manage services
	✓ SystemLoad		any	*	edit manage services
	✓ WindowsServices		any	*	edit manage services

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

Note The  icon means that there is no service in the category.

6. To create a new service in `my_category`, click the **manage service** link of `my_category`.
 - In the **Manage Service** popup window, check **Add from service template** and select the service `"C"`. Then click **add from the selected service**.
 - Change the name into `"D"` and change the description.
 - Change the host list into `"*"`.
 - Change the others fields if necessary.
7. Click **OK** to validate. The new service is now displayed in the Categories and Services list:

Categories and Services found for : <i>Windows</i>					
	Name & Description	OS	Model	HostList	Actions
	✓ my_category		any	*	edit manage services
	✓ D		any	FRCLS1704	edit
	✓ EventLog		any	*	edit manage services
	✓ LogicalDisks		any	*	edit manage services
	✓ SystemLoad		any	*	edit manage services
	✓ WindowsServices		any	*	edit manage services

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

5.1.4.2 Creating a New Category and a New Service

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

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

```
#!/bin/bash

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

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

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

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

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

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



Important

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

1. Click the **Categories/Services** link in the Supervision tab.
2. From the **Categories/Services** page, click **Filter by Host** and select your host and click the **Apply** button.
3. When the table is ready, click **manage category**.
4. In the **Manage Category** popup window, check **Create a new category** and click **create a new category**.
 - Enter the name of the category: `my_category`.
 - Enter its description.
 - The **OS family** and **Model**, and **host list expression** text fields are already filled (with the values of the selected Host). It is not editable because of the used filter (if you choose **no filter** this text field becomes editable).
 - Choose the monitoring domain.

Properties	
name	<input type="text" value="my_category"/>
description	<input type="text" value="Demo new service"/>
model	other
OS family	Windows family
monitoring domain	<input type="radio"/> Hardware <input type="radio"/> Operating System <input type="radio"/> Storage <input type="radio"/> Virtualization <input type="radio"/> Network <input checked="" type="radio"/> none
host list expression	<input type="text" value="frcls1704"/>

Figure 5-16. my_category creation

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

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














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

Figure 5-17. List of categories for host

Note The  icon means that there is no service in the category.

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

Properties	
category	my_category
name	demo
description	Demo service
model	any
OS family	Windows family
host list expression	frcls1704
Monitoring attributes	
status	<input checked="" type="radio"/> active <input type="radio"/> inactive
Monitoring command attributes (for this service)	
monitoring on event	<input type="radio"/> Yes <input checked="" type="radio"/> No
monitoring by polling	<input checked="" type="radio"/> Yes <input type="radio"/> No
check command	check_demo
check command parameters	20!25
monitoring period	24x7
polling interval	5 mn (5 mn by default if empty)
Notification attributes (for this service)	
e-mail contact groups	<div> <div>Selected Objects</div> <div> mgt-admins </div> </div> <div> <div>All Objects</div> <div> mgt-admins mgt-report </div> </div> <div> <= Add Remove => </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 type="radio"/> Yes <input checked="" 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

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

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

5.1.4.3 Customizing the List of Monitored Hosts

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

Examples of application:

- To disable monitoring of the **Processes** service, on all hosts:
 - a. Edit the **Processes** service.
 - b. Set the host list to **none**.
- To disable monitoring of the **All** service in **FileSystems** category on the `sysman` host, there are two possibilities:
 1. Using the **filter by HOST** filter:
 - a. Select the `sysman` host and click **Apply**.
 - b. Edit the **All** service in the **FileSystem** category.
 - c. Click the **delete for this host list** button.
 2. Or using another filter:
 - a. Edit the **All** service in the **FileSystem** category.
 - b. Set the host list is to **"!sysman"**, that means that the **All** service does apply to all hosts, except the `sysman` host.

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

5.1.4.4 Customizing the Notification Period

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

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

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

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

Using the filter by HOST filter:

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

Using another filter:

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

All active Categories and Services					
	Name & Description	OS	Model	HostList	Actions
	AIXServices		any	*	edit manage services
	EventLog		any	*	edit manage services
	FileSystems		any	*	edit manage services
	FileSystems		any	*	edit manage services
	All		any	frcls6260, nsmaster	edit
	All		any	!frcls6260, !nsmaster	edit
	LinuxServices		any	*	edit manage services

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

5.1.4.5 Customizing Thresholds

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

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

Table 5-4. Customizing thresholds

5.1.4.6 Warning and Critical Thresholds

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

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

Table 5-5. Service parameters syntax

Example:

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

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

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

Figure 5-19. Customized threshold

- 5. Click **OK** to validate

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

+	✓	SystemLoad		any	*	edit manage services
-	✓	SystemLoad		any	*	edit manage services
	✓	CPU		any	*	edit
	✓	Memory		any	*	edit
	✓	Processes		any	*	edit
	✓	Users		any	frcls6260.frcl.bull.fr, nsmaster	edit
	✓	Users		any	!frcls6260.frcl.bull.fr, !nsmaster	edit

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

5.1.4.7

Thresholds Related to Windows Event Logs Scanning

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

Example:

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

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

1. Edit the **Application** service in the **EventLog** category.
2. To change **check command** thresholds, modify the line displayed in the **Parameters** box as follows:
`60!strlog='Application'!wWarn=1!eErr=5`
3. Click **OK** to validate the modifications, and return to the Categories and Services page.

5.1.4.8

Customizing Windows Services

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

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

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

Table 5-6. Windows services check commands and parameters

Note Some of these services can be used as templates.

Examples of application:

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

Example:

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

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

Note

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

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

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

5.1.4.9 Customizing Linux or AIX Services

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

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

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

Table 5-7. Linux services check commands and parameters

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

Example 1:

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

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

Example 2:

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

1. Click the **manage service** link of the **LinuxServices** category (or another Linux category).
2. In the **Manage Service** popup window, check **Add from service template** and select the **syslogd** service. Then click the **add from the selected service** button.
3. Set **service_name** to **xinetd** (or **inetd**).
4. Modify its description.
5. Under **check Parameters**, replace **syslogd** by **xinetd** (or **inetd**) and if needed, modify thresholds and other monitoring properties.
6. Click **OK** to validate the cloning operation.
7. Repeat this operation to create services for monitoring other services or processes.

Example 3:

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

1. From the **filter by HOST** option select **host1**, and click **Apply**.
2. Click the **manage service** link of the **Syslog** category (or another Linux category).
3. In the **Manage Service** popup window, check **Add from service template** and select the **RootAccess** service. Then click the **add from the selected service** button.
4. Set **service_name**.
5. Modify its description.
6. If you do not use the **filter by HOST** option, change the host list to **host1**.
7. Modify **check Parameters** as follows:
 - Do not pay attention to the **#** character at the beginning and at the end of the parameters command.
 - **-l** parameter: replace the **/var/log/messages** file pathname by the pathname of the new file to check.
 - **-s** parameter: replace **rootsess.seek** by a new string (that must be unique).
 - **-p** parameter: replace the string session opened for user root by the new string to search.
8. Click **OK** to validate the cloning operation.
9. Repeat this operation to create a service to scan any file.

5.1.4.10 Customizing URL Access

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

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

Table 5-8. Customizing URL access

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

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

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

Example 1:

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

1. From the **filter by HOST** option select `frcls6260`, and click **Apply**.
2. Click the **manage service** link of the category in which you want to put this service.
3. In the **Manage Service** popup window, check **Add from service template** and select the **HTTP_BSM** service. Then click the **add from the selected service** button.
4. If you do not use the **filter by HOST** option, change the **host list** with the name of the Bull System Manager server (`frcls6260`).
5. Let the check parameters unchanged.
6. Click **OK** to validate the customization operation.

Example 2:

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

Note We assume that the bull (www.bull.com) host has been defined and that the new category my_category has been created with a host list containing www.bull.com. See the example, *Creating a New Category and Adding a Service*, on page 100. Click the **manage service** link of the my_category category.

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

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

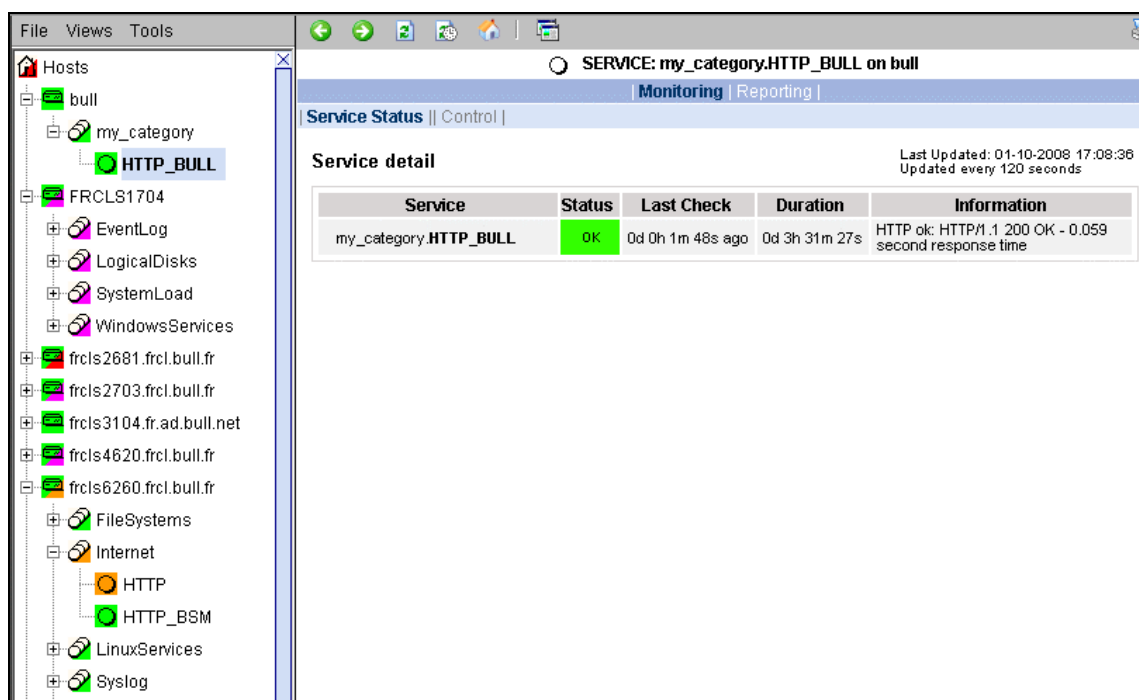


Figure 5-21. HTTP_BSM customized service

5.1.4.11 Creating an Alerts Service

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

Example:

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

Note We assume that the new category `my_category` has been created with a host list containing the corresponding SNMP trap agent.
See *Creating a new Category* example, on page 85.

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

Then follow the next steps described in *Integrating MIBs*, on page 149.

5.1.4.12 Using the perf_indic Service Template

The monitoring of this service gets, and then checks the last value of a reporting indicator, from a reporting log file located in `<install_dir>/core/share/reporting/var`.

This service uses the `check_mrtg` check command.

Note The reporting log file contains the name of the host associated to the reporting indicator. Therefore, the monitoring service cloned from `reporting.perf_indic` must have a `hostlist` containing only one host. By default, `hostlist=none` for the `Perf_indic` service and the `reporting` category.

The monitoring service configuration looks as follows:

Properties	
category	my_category
name	perf_indic
description	monitors one indicator collected by MRTG
model	any
OS family	any
host list expression	none
Monitoring attributes	
status	<input checked="" type="radio"/> active <input type="radio"/> inactive
Monitoring command attributes (for this service)	
monitoring on event	<input type="radio"/> Yes <input checked="" type="radio"/> No
monitoring by polling	<input checked="" type="radio"/> Yes <input type="radio"/> No
check command	check_mrtg
check command parameters	-F 'F:/PROGRA~1/Bull/BULLSY~1/core/share/reporting/var/xx.log!-s
monitoring period	24x7
polling interval	5 mn (5 mn by default if empty)
Notification attributes (for this service)	
e-mail contact groups	<div> <div>Selected Objects</div> <div>mgt-admins</div> <div><= Add</div> <div>Remove =></div> <div>All Objects</div> <div>mgt-admins mgt-report</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	240 mn (0 mn by default if empty)
notify if warning	<input type="radio"/> Yes <input checked="" 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 5-22. perf_indic service example

The monitoring service status looks as follows:

Service detail				
Service ↑↓	Status ↑↓	Last Check ↑↓	Duration ↑↓	Information
reporting.2703 memory	WARNING	0d 0h 3m 4s ago	0d 0h 27m 52s	Load = 28 %

Figure 5-23. Service detail – example

5.2 Configuring Servicegroups

Servicegroup allows to organize services into functional domains, in order to filter topological views or map in BSM Console.

Default servicegroups definitions are automatically generated, containing instantiated services which belong to category defined with a given monitoring domain (see Category Properties on page84).



WARNING:

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

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

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

The following page is displayed:

	name	description	services list	active	auto
Edit	Hardware	Servicegroup for domain Hardware (automatically generated)	list generated during Save&reload step	yes	yes
Edit	Network	Servicegroup for domain Network (automatically generated)	list generated during Save&reload step	yes	yes
Edit	OperatingSystem	Servicegroup for domain OperatingSystem (automatically generated)	list generated during Save&reload step	yes	yes
Edit	Power	Servicegroup for domain Power (automatically generated)	list generated during Save&reload step	yes	yes
Edit	Storage	Servicegroup for domain Storage (automatically generated)	list generated during Save&reload step	yes	yes
Edit	Virtualization	Servicegroup for domain Virtualization (automatically generated)	list generated during Save&reload step	yes	yes
Edit	vcenter	vcenter managed elements	VMwareESX_VC.CPU(nsmesx), VMwareESX_VC.Memory(nsmesx), VMwareESX_VC.Status(nsmesx), VMware_VC.Alerts(nsmesx), VMware_VC.Alerts(rh54_al), ...	yes	no

Figure 5-24. Servicegroups

The servicegroup with flag 'auto' set to 'yes' correspond to the default servicegroup when the others are user defined servicegroups. In the example, six default servicegroups are defined (**Hardware**, **Network**, **OperatingSystem**, **Power**, **Virtualizarion** and **Storage**) and one user servicegroup (**vcenter**).

For default servicegroup, the list of members is not displayed because it will be generated during the Save&Reload step, in order to include all services matching the functional domain.

5.2.1 Default Servicegroup

5.2.1.1 Default Servicegroup edition

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

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

Properties	
name	Hardware
description	<input type="text" value="Servicegroup for domain Hardware (automatically generated)"/>
active	<input checked="" type="radio"/> Yes <input type="radio"/> No
Services	
Rules generation : (monitoring domain = Hardware) <input type="button" value="Modify"/>	

Figure 5-25. Hardware servicegroup edition

After editing:

- click **OK** button to validate changes
- or click **Cancel** button to return to the Servicegroups page without change

5.2.1.2 Default Servicegroup generation

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



WARNING

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

5.2.2 User Servicegroup

5.2.2.1 User Servicegroup edition

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

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

Servicegroup

[Help on Servicegroup](#)

OK Cancel

Properties	
name	<input style="width: 80%;" type="text"/>
description	<input style="width: 80%;" type="text"/>
active	<input checked="" type="radio"/> Yes <input type="radio"/> No
Services	
Services list	
Modify	

Figure 5-26. User Servicegroup edition

The edition of a servicegroup contains two parts:

- definition of general properties of the servicegroup (name, description)
- definition of the list of services. This is done by clicking the 'Modify' button in the bottom part of the window. A new page will appear to facilitate the filling of the service members (see detailed procedure below).

After fill in all the required fields

- click **OK** button to validate edition
- Or click **Cancel** button to return to the Servicegroups page without change

After having completed the member edition:

- click the **OK** button to validate changes
- Or click the **Cancel** button to return to the Servicegroup edition page without change

Example:

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

The following page is displayed.

The screenshot shows the 'Servicegroup Members' page. On the left, under 'Selection filter', the 'monitoring domain' is set to 'is Operating System'. Below it are dropdowns for 'category', 'service', 'OS family', and 'model'. A '>>' button is to the right of the 'service' dropdown. On the right, under 'Filtered services (14 found)', a list of services is shown with checkboxes: SystemLoad.CPU (frcls1704), SystemLoad.CPU (frcls8004), SystemLoad.Memory (frcls1704), SystemLoad.Memory (frcls8004), EventLog.Application (frcls1704), EventLog.Application (frcls8004), and EventLog.Security (frcls1704). To the right of this list are 'Reset' and 'Add' buttons. Below the filtered services is a section titled 'Servicegroup Members' which currently shows 'No member defined' and 'Clear not selected' and 'Clear All' buttons.

Figure 5-28. Servicegroup Members: filtering on monitoring domain

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

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

This screenshot is identical to Figure 5-28, showing the same filters and filtered services. However, the 'Servicegroup Members' section now contains a list of 14 services with checkboxes: EventLog.Application (frcls1704), EventLog.Application (frcls8004), EventLog.Security (frcls1704), EventLog.Security (frcls8004), EventLog.System (frcls1704), EventLog.System (frcls8004), LogicalDisks.All (frcls1704), LogicalDisks.All (frcls8004), LogicalDisks.All (frcls8004), SystemLoad.CPU (frcls1704), SystemLoad.CPU (frcls8004), SystemLoad.Memory (frcls1704), SystemLoad.Memory (frcls8004), and WindowsServices.EventLog (frcls8004). The 'Clear not selected' and 'Clear All' buttons are still present at the bottom.

Figure 5-29. Servicegroup Members: add of selected services

2. Reset filter

- Click the **'Reset'** button

The selection result part of the filter is empty.

The Servicegroup Members part contains the previously selected service.

The screenshot shows the 'Servicegroup Members' interface. The 'Selection filter' section on the left has several dropdown menus: 'monitoring domain' (set to 'is'), 'category' (set to 'Select ...'), 'service' (set to 'Select ...'), 'OS family' (set to 'is'), and 'model' (set to 'is'). A '>>' button is next to the 'service' dropdown. To the right, the 'Filtered services' section is empty, displaying 'No selection done'. On the far right, there are 'Reset' and 'Add' buttons. Below the filter section, the 'Servicegroup Members' section displays a list of services with checkboxes, organized in two columns. The services listed are: EventLog.Application (frcls1704), EventLog.Application (frcls8004), EventLog.System (frcls1704), EventLog.System (frcls8004), LogicalDisks.All (frcls1704), LogicalDisks.All (frcls8004), SystemLoad.CPU (frcls1704), SystemLoad.CPU (frcls8004), SystemLoad.Memory (frcls1704), SystemLoad.Memory (frcls8004), WindowsServices.EventLog (frcls1704), and WindowsServices.EventLog (frcls8004). At the bottom of this section are 'Clear not selected' and 'Clear All' buttons.

Figure 5-30. Servicegroup members: reset of filter

3. Apply second filter: monitoring domain set to 'Network' and OS family set to 'Windows'.

- set criteria
- click the >> button

The following page is displayed:

The screenshot shows the 'Servicegroup Members' interface with the filter applied. In the 'Selection filter' section, 'monitoring domain' is set to 'Network' and 'OS family' is set to 'windows'. The '>>' button is still present. The 'Filtered services' section now contains two items: 'NetworkAdaptors.NIC_Status (frcls1704)' and 'NetworkAdaptors.NIC_Status (frcls8004)', both with checked checkboxes. The 'Reset' and 'Add' buttons remain on the right. The 'Servicegroup Members' section below still displays the same list of services as in Figure 5-30, with 'Clear not selected' and 'Clear All' buttons at the bottom.

Figure 5-31. Servicegroup Members: filtering on domain and OS

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

Servicegroup Members edition

Selection filter
 monitoring domain:
 category:
 service: >>
 OS family:
 model:

Filtered services (2 found)

☒ NetworkAdaptors.NIC_Status (frcls1704)
☒ NetworkAdaptors.NIC_Status (frcls8004)

Servicegroup Members

<input checked="" type="checkbox"/> EventLog.Application (frcls1704) <input checked="" type="checkbox"/> EventLog.Application (frcls8004) <input checked="" type="checkbox"/> EventLog.Security (frcls1704) <input checked="" type="checkbox"/> EventLog.Security (frcls8004) <input checked="" type="checkbox"/> EventLog.System (frcls1704) <input checked="" type="checkbox"/> EventLog.System (frcls8004) <input checked="" type="checkbox"/> LogicalDisks.All (frcls1704) <input checked="" type="checkbox"/> LogicalDisks.All (frcls8004)	<input checked="" type="checkbox"/> NetworkAdaptors.NIC_Status (frcls1704) <input checked="" type="checkbox"/> NetworkAdaptors.NIC_Status (frcls8004) <input checked="" type="checkbox"/> SystemLoad.CPU (frcls1704) <input checked="" type="checkbox"/> SystemLoad.CPU (frcls8004) <input checked="" type="checkbox"/> SystemLoad.Memory (frcls1704) <input checked="" type="checkbox"/> SystemLoad.Memory (frcls8004) <input checked="" type="checkbox"/> WindowsServices.EventLog (frcls1704) <input checked="" type="checkbox"/> WindowsServices.EventLog (frcls8004)
--	--

Figure 5-32. Servicegroup member: add Windows services

4. Click the **OK** button to validate the servicegroup members edition and return to the servicegroup edition page:

Servicegroup

[Help on Servicegroup](#)

Properties

name	Windows	
description	<input type="text" value="Servicegroup for windows supervision"/>	
active	<input checked="" type="radio"/> Yes <input type="radio"/> No	

Services

Services list

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

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

5.2.2.3

User Servicegroup checking

User servicegroups are checked during the Save&Reload to avoid inconsistent definition, that can occur if one of the members of the servicegroup is inactivated (service directly inactivated or host) after the servicegroup edition.

During the check, if such service is found, it is removed from the final servicegroup object. The Administrator is warned by messages, as shown in the following figure:

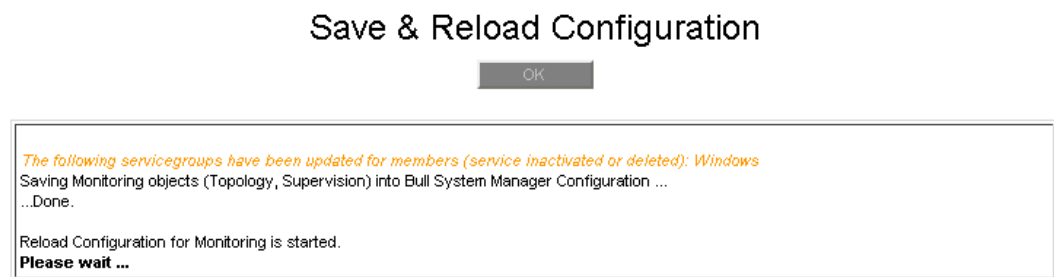


Figure 5-33. User Servicegroup Control

5.3 Configuring Hosts/Hostgroups/Managers monitoring

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

5.3.1 Host Properties

Host Properties	Description
host management	<p>Monitoring status (active, inactive). Default value: active.</p> <p>Active status means that the host is monitored with its associated services. Its node is animated in the Management Tree and in all corresponding menus.</p> <p>Inactive status means that the host is not monitored. It is visible in the Management Tree but its node is not animated and only the Platform menu is available (for NovaScale 5000 & 6000 and NovaScale Blade series hosts). In the Bull System Manager Console Applications pane the host appears with the PENDING monitoring status.</p> <p>This field may be used to temporarily activate/deactivate monitoring on a given host.</p>
Ping checking	<p>To enable host checking with ping command. Default = yes</p> <p>Note: if disable, check of the host is only made with the services defined for this host. It is useful when the host is unreachable by ping.</p>
OS monitoring	<p>To enable or disable OS services monitoring. Default = yes</p>
Hardware monitoring	<p>To enable or disable hardware services monitoring. Default = yes</p>
Virtualization monitoring	<p>To enable or disable virtualization monitoring. Default = yes</p>
Storage monitoring	<p>To enable or disable storage monitoring. Default = yes</p>
Network monitoring	<p>To enable or disable network monitoring. Default = yes</p>
Power Monitoring	<p>To enable or disable power monitoring. Default = yes</p>
Syslog Monitoring	<p>Syslog Monitoring status (see <i>Syslog Monitoring host properties</i> on page 133). Default value: yes</p>
Syslog Filter	<p>Short name of a Syslog Filter (see <i>Syslog Monitoring host properties</i> on page 133). Default = none</p>
Notification enabled	<p>To enable or disable all the notifications. Default = yes</p>
Enable SNMP	<p>To enable notifications by SNMP trap.</p>

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

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

5.3.2 Hostgroup Properties

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

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

5.3.3 Manager Properties

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

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

5.3.4 Example: Monitoring NS 4000 Hardware

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

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

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

Figure 5-34. Hardware category monitoring domain

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

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

There are two ways of monitoring NS 4000 server hardware:

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

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

Categories and Services

[Help on Categories and Services](#)

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

Models :

NS 4000

Reset
Apply

Expand all
Collapse all

manage categories

Categories and Services found for : *NS 4000*

	Name & Description	OS	Model	HostList	Actions
	Hardware		NS 4000	ns4000	edit
	Alerts		NS 4000	ns4000	edit
	Health		NS 4000	ns4000	edit
	PowerStatus		NS 4000	ns4000	edit

Figure 5-35. NS4000 Hardware category and services

5.3.4.1

Disabling Hardware Monitoring at Host Level

Setting the **hardware monitoring** attribute to **No**, as shown in the following figure, will result in the deactivation of all hardware categories and associated services for this ns4000 host.

Host object

*This host can only be deleted from the menu
Topology/Hosts Definition/NovaScale hosts/NS 4000.* OK Cancel

Properties	
name	ns4000
model	NS 4000 series
OS family	other OS
Management attributes	
host management	<input checked="" type="radio"/> active <input type="radio"/> inactive
ping checking	<input checked="" type="radio"/> Yes <input type="radio"/> No
hardware monitoring	<input type="radio"/> Yes <input checked="" type="radio"/> No
storage monitoring	<input checked="" type="radio"/> Yes <input type="radio"/> No
Notification attributes	
notifications enabled	<input checked="" type="radio"/> Yes <input type="radio"/> No
enable SNMP trap	<input checked="" type="radio"/> Yes <input type="radio"/> No
notification period	24x7
re-notification interval	<input type="text"/> mn (0 mn by default if empty)
notify if down	<input checked="" type="radio"/> Yes <input type="radio"/> No
notify if unreachable	<input checked="" type="radio"/> Yes <input type="radio"/> No
notify if recovery	<input checked="" type="radio"/> Yes <input type="radio"/> No
e-mail contact groups	<div> <div>Selected Objects</div> <div>mgt-admins</div> </div> <div> <div>All Objects</div> <div>mgt-admins</div> </div> <div> <div><= Add</div> <div>Remove =></div> </div>

[Edit Topology Properties](#)

Figure 5-36. Host hardware monitoring status

All Hardware services linked to the ns4000 host appear deactivated, as illustrated by the following figure:

Categories and Services found for : NS 4000					
	Name & Description	OS	Model	HostList	Actions
<input checked="" type="checkbox"/>	Hardware		NS 4000	ns4000	edit
	Alerts		NS 4000	ns4000	edit
	Health		NS 4000	ns4000	edit
	PowerStatus		NS 4000	ns4000	edit

Figure 5-37. NS4000 services deactivation

The services are deactivated because the "monitoring domain" of the Hardware category is "Hardware" and the "hardware monitoring status" of the host is set to "No". The status of the service is always set to active as display in the following figure:

Properties	
category	Hardware
name	Alerts
description	checks the alerts received from the BMC of this host (automatically
model	NS 4000 series
OS family	any
host list expression	ns4000
Monitoring attributes	
status	<input checked="" type="radio"/> active <input type="radio"/> inactive
Monitoring command attributes (for this service)	
receives SNMP traps	yes
Notification attributes (for this service)	
	Selected Objects All Objects

Figure 5-38. NS4000 Alert service status

In the Management Tree, categories hardware and associated services are no longer visible.

5.3.4.2 Disabling Hardware Monitoring at Manager Level

Setting the **hardware monitoring** attribute to **No**, as shown in the following figure, will result in the deactivation of the Health service associated to the ns4000 host.

Properties	
name	ISM1
type	ISM
element list	ns4000
Management attributes	
hardware monitoring	<input type="radio"/> Yes <input checked="" type="radio"/> No

Figure 5-39. Manager hardware monitoring status

Only the Health service dependent on the ISM manager is deactivated, as illustrated in the following figure:









Categories and Services found for : NS 4000					
	Name & Description	OS	Model	HostList	Actions
<input checked="" type="checkbox"/>	 Hardware		NS 4000	ns4000	edit
	 Alerts		NS 4000	ns4000	edit
	 Health		NS 4000	ns4000	edit
	 PowerStatus		NS 4000	ns4000	edit

Figure 5-40. NS4000 Health service deactivation

The service is deactivated now because the status has been set to Inactive during manager edition as displayed in the following figure. The monitoring status of the corresponding host is always set to 'Yes'.

Properties	
category	Hardware
name	Health
description	checks the hardware status for the platform of this host from a Plat
model	NS 4000 series
OS family	any
host list expression	ns4000
Monitoring attributes	
status	<input type="radio"/> active <input checked="" type="radio"/> inactive
Monitoring command attributes (for this service)	
check command	check_healthism
check command parameters	!!5988
monitoring period	24x7
polling interval	1 min. (5 min by default if empty)

Figure 5-41. NS4000 Health service status

In the Management Tree, the **Hardware** category is visible but the **Health** service is not displayed. If the **Health** service is the only service associated to the **Hardware** category, no child is displayed for this category.

5.4 Syslog Monitoring

Syslog events are collected on BSMAgent hosts and are sent to the BSMServer as SNMP traps. On Linux hosts, the syslog events are collected with syslog-ng; **syslog-ng application is exclusive with syslogd**. On AIX hosts, the syslog events are collected with syslogAixErr. The syslog event collection and sending SNMP traps can be stopped or started on demand. The events can be filtered at source at the collection time. To do this, filters are prepared on the BSMServer and sent to the BSMAgent hosts to be applied to the event collection.

When several BSMServer manage a same BSMAgent, it is the last filter sent to the BSMAgent that is running.

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

5.4.1 Host Properties

Host Properties	Description
Syslog Monitoring	Syslog Monitoring status. Default value: yes . Yes: means that collection events and sending traps to this server will be started. No: means that collection events and sending traps to this server will be stopped. This field may be used to temporarily start/stop monitoring on a given host.
Syslog Filter	Short name of a Syslog Filter. Default = none Note: Linux hosts: only Syslog Filters of type LINUX-syslogng will be proposed. Aix hosts: only Syslog Filters of type AIX-errpt will be proposed.

Table 5-9. Syslog Monitoring host properties

5.4.2 Syslog Filter Properties

The filters have a common part and a specific part for each type of filter.

Common Syslog Filters part

Syslog Filter Properties	Description
Syslog filter type	Type of the Syslog Filter, depends of the OS of the host. Default value: none . LINUX-syslogng : can be assigned to agents Linux. AIX-errpt : can be assigned to agents Aix. Each type of filter has its own properties.

Table 5-10. Syslog Filters common properties

Note	When the syslog filter type is not set, only the common properties are displayed.
-------------	--

Linux Syslog Filters part

Syslog Filter Properties	Description
Level list	Match messages having one of the listed level code. Default value: empty . A list of levels taken in the mib "BSM-SYSLOG-MIB" (see level values) If empty , messages are not filtered on level code.
Facility list	Match messages having one of the listed facility code. Default value: empty . A list of facilities taken in the mib "BSM-SYSLOG-MIB" (see facility values) If empty , messages are not filtered on facility code.

Table 5-11. Syslog Filters Linux properties

Note	When the syslog filter type is set to LINUX-syslogng , the common properties and the Linux properties are displayed.
-------------	--

Aix Syslog Filters part

Syslog Filter Properties	Description
Class / facility mapping	<p>To translate ErrorClass from errpt into facility of BSM-SYSLOG-MSG mib.</p> <p>A list of four pairs (ErrorClass, facility) (see ErrorClass values and facility values).</p>
Type / level mapping	<p>To translate ErrorType from errpt into level of BSM-SYSLOG-MSG mib.</p> <p>A list of six pairs (ErrorType, level) (see ErrorType values and level values).</p>
Filter scope	<p>Scope of the AIX-errpt syslog filter</p> <p>Default value: none.</p> <p>ErrorId: messages are filtered on the errorID.</p> <p>ErrorLabel: messages are filtered on the errorID.</p> <p>other: messages are filtered on the errorClass and/or the ErrorType and/or the ResourceName.</p> <p>none: messages are not filtered.</p> <p>Mapping properties are always applied.</p>
ErrorClass list	<p>Match messages having one of the listed ErrorClass.</p> <p>Default value: empty (idem no filter).</p> <p>A list of ErrorClass values (see ErrorClass values).</p> <p>If empty, messages are not filtered on ErrorClass attribut.</p>
ErrorType list	<p>Match messages having one of the listed ErrorType.</p> <p>Default value: empty (idem no filter).</p> <p>A list of ErrorType values (see ErrorType values).</p> <p>If empty, messages are not filtered on ErrorType attribut.</p>
ResourceName list	<p>Match messages having one of the listed ResourceName.</p> <p>Default value: empty (idem no filter).</p> <p>A list of ResourceName values (see the Aix errpt documentation).</p> <p>If empty, messages are not filtered on ResourceName attribut.</p>
ErrorId list	<p>Match messages having / not having one of the listed ErrorId depending on Include / exclude the list property.</p> <p>Default value: empty (idem no filter).</p> <p>A list of ErrorId values (see Aix the errpt documentation).</p> <p>If empty, messages are not filtered on ErrorId attribut.</p>
ErrorLabel list	<p>Match messages having / not having one of the listed ErrorLabel depending on Include / exclude the list property.</p> <p>Default value: empty (idem no filter).</p> <p>A list of ErrorLabel values (see the Aix errpt documentation).</p> <p>If empty, messages are not filtered on ErrorLabel attribut.</p>

Syslog Filter Properties	Description
Include / exclude the list	<p>Include / exclude matching messages.</p> <p>Default value: <i>include</i></p> <p><i>include</i>: only the events whose attribute value is in the corresponding list will be forwarded</p> <p><i>exclude</i>: only the events whose attribute value is not in the corresponding list will be forwarded</p>

Table 5-12. Syslog Filters Aix properties

Note	<p>When the syslog filter type is set to AIX-errpt, the common properties and the Aix properties are displayed.</p> <p>Depending on the filter scope, only the corresponding properties are displayed.</p>
-------------	---

Values of level in "BSM-SYSLOG-MIB" mib:

Level	Description
Emerg	emergency; system is unusable
Alert	action must be taken immediately
Crit	critical condition
Err	error condition
warning	warning condition
Notice	normal but significant condition
Info	informational message
Debug	debug-level messages

Table 5-13. level values

Values of facility in "BSM-SYSLOG-MIB" mib:

facility	Description
kern	kernel messages
user	user-level messages
mail	mail system messages
daemon	system daemons messages
auth	authorization messages
syslog	syslogd messages
lpr	line printer subsystem messages
news	network news subsystem messages
uucp	UUCP subsystem messages
cron	clock daemon messages
authpriv	security / authorization messages
ftp	ftp daemon messages
local0	

facility	Description
local1	
local2	
local3	
local4	
local5	
local	
local7	

Table 5-14. facility values

Values of errpt ErrorClass:

ErrorClass	Description
H	hardware
S	Software
O	informational / errlogger
U	Undetermined

Table 5-15. ErrorClass values

Values of errpt ErrorType:

ErrorType	Description
PEND	Pending
PERF	Performance
PERM	Permanent
UNKN	Unknown
TEMP	Temporary
INFO	Informational

Table 5-16. ErrorType values

5.4.3 Example: Monitoring Linux Host

5.4.3.1 Creating Linux Syslog Filter

To edit syslog filters, click the Syslog Filters item in the Monitoring part of the Supervision tab. The list of configured syslog filters appears, as in the following example:

Syslog Filters

New Filter

	filter name	description	filter type
Edit	syslogfilter_aix	syslog filter for aix with errpt	aixerrpt
Edit	syslogfilter_aix1	syslog filter aix on ErrorClass:H,S	aixerrpt
Edit	syslogfilter_aix_ErrorId	syslog filter aix on ErrorId	aixerrpt
Edit	syslogfilter_aix_ErrorLabel	syslog filter aix on ErrorLabel	aixerrpt
Edit	syslogfilter_aix_def	syslog filter aix default	aixerrpt
Edit	syslogfilter_aix_def_plus_ErrorClass	syslog filter aix default plus ErrorClass	aixerrpt
Edit	syslogfilter_aix_mapping	syslog filter aix mapping seul	aixerrpt
Edit	syslogfilter_linux	syslog filter for linux with syslog-ng	linuxsyslogng
Edit	syslogfilter_linux_def	syslog filter linux default	linuxsyslogng
Edit	syslogfilter_linux_def_plus_facility	syslog filter linux default plus facility	linuxsyslogng
Edit	syslogfilter_linux_vide	syslog filter linux vide	linuxsyslogng

Figure 5-42. Syslog Filters configuration window

Note See *Create / Edit / Delete Resources*, on page 19 for details.

To create a syslog filter, click the **New Filter** button, the following page is displayed:

Syslog Filter object

OK Cancel

Properties	
name	<input type="text" value="syslogfilter"/>
description	<input type="text" value="syslog filter"/>
Syslog filter attributes	
syslog filter type	<input type="radio"/> LINUX-syslogng <input type="radio"/> AIX-errpt

Figure 5-43. Common Syslog Filter properties

Set the **syslog filter type** attribute to **LINUX-syslogng**.

As shown in the following example, the Linux Syslog Filter properties are displayed:

Syslog Filter object

Properties	
name	syslogfilter_linux
description	syslog filter for linux with syslog-ng
Syslog filter attributes	
syslog filter type	<input checked="" type="radio"/> LINUX-syslogng <input type="radio"/> AIX-errpt
LINUX-syslog-ng Filter	
level	<input checked="" type="checkbox"/> emergency <input checked="" type="checkbox"/> alert <input checked="" type="checkbox"/> critical <input type="checkbox"/> error <input type="checkbox"/> warning <input type="checkbox"/> notice <input type="checkbox"/> informational <input type="checkbox"/> debug
facility	<input checked="" type="checkbox"/> kernel <input type="checkbox"/> user-level <input type="checkbox"/> mail <input checked="" type="checkbox"/> system daemons <input checked="" type="checkbox"/> authorization <input type="checkbox"/> syslog <input type="checkbox"/> line printer <input checked="" type="checkbox"/> network news <input type="checkbox"/> uucp <input type="checkbox"/> cron <input type="checkbox"/> security/authorization <input type="checkbox"/> ftp <input type="checkbox"/> ntp <input type="checkbox"/> audit <input type="checkbox"/> console <input type="checkbox"/> clock <input type="checkbox"/> local0 <input type="checkbox"/> local1 <input type="checkbox"/> local2 <input type="checkbox"/> local3 <input type="checkbox"/> local4 <input type="checkbox"/> local5 <input type="checkbox"/> local6 <input type="checkbox"/> local7

Figure 5-44. Linux Syslog Filter properties

Set the **level** list by checking the buttons.

If no level button is checked, no filter is applied on level attribute.

Set the **facility** list by checking the buttons.

If no facility button is checked, no filter is applied on facility attribute.

5.4.3.2 Configuring Host

To configure hosts, click the hosts item in the Monitoring part of the Supervision tab. The list of configured hosts appears, as in the following example:

Hosts Supervision

Search

	name	platform	description	model	netName	OS
Edit	FRCLS3105	-	System Management Server	other	FRCLS3105	windows
Edit	aixHv4	-	N/A	other	172.31.50.97	aix
Edit	frcls6260	-	SystemManagement Agent	other	129.182.6.33	linux
Edit	hv453nsm	-	SystemManagement Server	other	172.31.50.97	aix
Edit	linuxRedHat	-	N/A	other	172.31.50.60	linux
Edit	rh54.frcl.bull.fr	-	SystemManagement Server	other	172.31.50.60	linux

Figure 5-45. Hosts configuration window

Note See *Create / Edit / Delete Resources*, on page 19 for details.

As shown in the following example, edit a linux host.

Set the **Syslog Monitoring** attribute to **Yes** or **No**.

Select a **Syslog Filter** in the list: only Syslog Filters of **LINUX-syslogng** type will be proposed.
If no **Syslog Filter** is selected, no filter is applied.

Host object

*This host can only be deleted from the menu
Topology/Hosts Definition/Other hosts.*

OK

Cancel

Properties	
name	linuxRedHat
model	other
OS family	Linux family
Management attributes	
host management	<input checked="" type="radio"/> active <input type="radio"/> inactive
ping checking	<input checked="" type="radio"/> Yes <input type="radio"/> No
Hardware monitoring	<input checked="" type="radio"/> Yes <input type="radio"/> No
Operating System monitoring	<input checked="" type="radio"/> Yes <input type="radio"/> No
Storage monitoring	<input checked="" type="radio"/> Yes <input type="radio"/> No
Virtualization monitoring	<input checked="" type="radio"/> Yes <input type="radio"/> No
Network monitoring	<input checked="" type="radio"/> Yes <input type="radio"/> No
Power monitoring	<input checked="" type="radio"/> Yes <input type="radio"/> No
Syslog monitoring attributes	
Syslog Monitoring	<input checked="" type="radio"/> Yes <input type="radio"/> No
Syslog Filter	syslogfilter_linux
Notification attributes	
notifications enabled	<input checked="" type="radio"/> Yes <input type="radio"/> No
enable SNMP trap	<input checked="" type="radio"/> Yes <input type="radio"/> No
notification period	24x7
re-notification interval	<input type="text"/> mn (0 mn by default if empty)
notify if down	<input checked="" type="radio"/> Yes <input type="radio"/> No
notify if unreachable	<input checked="" type="radio"/> Yes <input type="radio"/> No
notify if recovery	<input checked="" type="radio"/> Yes <input type="radio"/> No
e-mail contact groups	<div><div>Selected Objects</div><div>mgt-admins</div><div>All Objects</div><div>mgt-admins mgt-report</div><div><= Add Remove =></div></div>

Figure 5-46. Host monitoring properties

5.4.4 Example: Monitoring Aix Host

5.4.4.1 Creating Aix Syslog Filter

To edit syslog filters, click the Syslog Filters item in the Monitoring part of the Supervision tab. The list of configured syslog filters appears, as in the following example:

Syslog Filters			
New Filter			
	filter name	description	filter type
Edit	syslogfilter_aix	syslog filter for aix with errpt	aixerrpt
Edit	syslogfilter_aix1	syslog filter aix on ErrorClass:H,S	aixerrpt
Edit	syslogfilter_aix_ErrorId	syslog filter aix on ErrorId	aixerrpt
Edit	syslogfilter_aix_ErrorLabel	syslog filter aix on ErrorLabel	aixerrpt
Edit	syslogfilter_aix_def	syslog filter aix default	aixerrpt
Edit	syslogfilter_aix_def_plus_ErrorClass	syslog filter aix default plus ErrorClass	aixerrpt
Edit	syslogfilter_aix_mapping	syslog filter aix mapping seul	aixerrpt
Edit	syslogfilter_linux	syslog filter for linux with syslog-ng	linuxsyslogng
Edit	syslogfilter_linux_def	syslog filter linux default	linuxsyslogng
Edit	syslogfilter_linux_def_plus_facility	syslog filter linux default plus facility	linuxsyslogng
Edit	syslogfilter_linux_vide	syslog filter linux vide	linuxsyslogng

Figure 5-47. Syslog Filters configuration window

Note See *Create / Edit / Delete Resources*, on page 19 for details.

To create a syslog filter, click the **New Filter** button, the following page is displayed:

		OK	Cancel
Properties			
name		syslogfilter	
description		syslog filter	
Syslog filter attributes			
syslog filter type		<input type="radio"/> LINUX-syslogng	<input type="radio"/> AIX-errpt

Figure 5-48. Common Syslog Filter properties

Set the **syslog filter type** attribute to **AIX-errpt**.

As shown in the following example, three AIX Syslog Filter properties are displayed:

Syslog Filter object

OK Cancel

Properties	
name	syslogfilter_aix
description	syslog filter for aix with errpt
Syslog filter attributes	
syslog filter type	<input type="radio"/> LINUX-syslogng <input checked="" type="radio"/> AIX-errpt
AIX-errpt Filter	
errpt / syslog mapping	
class / facility mapping	Hardware local0
	Software local1
	Informational local2
	Undetermined local3
type / level mapping	Pending alert
	Performance critical
	Permanent error
	Unknown error
	Temporary warning
	Informational informational
errpt filter	
filter scope	<input type="radio"/> ErrorId <input type="radio"/> ErrorLab

emergency

alert

critical

error

warning

notice

informational

debug

Figure 5-49. AIX Syslog Filter common properties

The **class/facility mapping** and **type/level mapping** properties are displayed with a default value. Each mapping can be modified by selecting a value in the proposed list.

Set the **filter scope** by checking a button to select one of the three values. If no button is checked, no filter is applied, only mapping.

If **Filter scope** is set to **Errorld**, two more properties are displayed, as in the following example:

Syslog Filter object

Properties		
name	<input style="width: 90%;" type="text" value="syslogfilter_aix"/>	
description	<input style="width: 90%;" type="text" value="syslog filter for aix with errpt"/>	
Syslog filter attributes		
syslog filter type	<input type="radio"/> LINUX-syslogng <input checked="" type="radio"/> AIX-errpt	
AIX-errpt Filter		
errpt / syslog mapping		
class / facility mapping	Hardware	<input style="width: 80%;" type="text" value="local0"/>
	Software	<input style="width: 80%;" type="text" value="local1"/>
	Informational	<input style="width: 80%;" type="text" value="local2"/>
	Undetermined	<input style="width: 80%;" type="text" value="local3"/>
type / level mapping	Pending	<input style="width: 80%;" type="text" value="alert"/>
	Performance	<input style="width: 80%;" type="text" value="critical"/>
	Permanent	<input style="width: 80%;" type="text" value="error"/>
	Unknown	<input style="width: 80%;" type="text" value="error"/>
	Temporary	<input style="width: 80%;" type="text" value="warning"/>
	Informational	<input style="width: 80%;" type="text" value="informational"/>
errpt filter		
filter scope	<input checked="" type="radio"/> Errorld <input type="radio"/> ErrorLabel <input type="radio"/> Other	
filtered Errorld list	<input style="width: 90%;" type="text" value="F89FB899,F7FA22C9"/> <small>Liste of Errorld values separated with comma and without any space</small>	
include / exclude the list	<input checked="" type="radio"/> include <input type="radio"/> exclude	

Figure 5-50. Aix Syslog Filter Errorld properties

Set the **filtered Errorld list** with a list of Errorld separated with comma and without space.

If the Errorld list is empty, no filter is applied on Errorld attribute.

Set the **include/exclude the list** property by checking a button to select one of the values:

- **include**: only the events whose Errorld value is in the **filtered Errorld list** will be forwarded,
- **exclude**: only the events whose Errorld value is not in the **filtered Errorld list** will be forwarded.

If **Filter scope** is set to **Errorlabel**, two more properties are displayed, as in the following example:

Syslog Filter object

Properties	
name	syslogfilter_aix
description	syslog filter for aix with errpt
Syslog filter attributes	
syslog filter type	<input type="radio"/> LINUX-syslogng <input checked="" type="radio"/> AIX-errpt
AIX-errpt Filter	
errpt / syslog mapping	
class / facility mapping	<div>Hardware local0 ▾</div> <div>Software local1 ▾</div> <div>Informational local2 ▾</div> <div>Undetermined local3 ▾</div>
type / level mapping	<div>Pending alert ▾</div> <div>Performance critical ▾</div> <div>Permanent error ▾</div> <div>Unknown error ▾</div> <div>Temporary warning ▾</div> <div>Informational informational ▾</div>
errpt filter	
filter scope	<input type="radio"/> ErrorId <input checked="" type="radio"/> ErrorLabel <input type="radio"/> Other
filtered ErrorLabel list	<div>DMPCHK_NOSPACE,J2_FS_FULL</div> <div>Liste of ErrorLabel values separated with comma and without any space</div>
include / exclude the list	<input type="radio"/> include <input checked="" type="radio"/> exclude

Figure 5-51. Aix Syslog Filter ErrorLabel properties

Set the **filtered Errorlabel list** with a list of Errorlabel separated with comma and without space.

If the ErrorLabel list is empty, no filter is applied on ErrorLabel attribute.

Set the **include/exclude the list** property by checking a button to select one of the values.

- **include**: only the events whose Errorlabel value is in the **filtered Errorlabel list** will be forwarded,
- **exclude**: only the events whose Errorlabel value is not in the **filtered Errorlabel list** will be forwarded.

If **Filter scope** is set to **other**, three more properties are displayed, as in the following example:

Syslog Filter object

OK Cancel

Properties

name

syslogfilter_aix

description

syslog filter for aix with errpt

Syslog filter attributes

syslog filter type

☐ LINUX-syslogng ☒ AIX-errpt

AIX-errpt Filter

errpt / syslog mapping

class / facility mapping

Hardware

local0

Software

local1

Informational

local2

Undetermined

local3

type / level mapping

Pending

alert

Performance

critical

Permanent

error

Unknown

error

Temporary

warning

Informational

informational

errpt filter

filter scope

☐ ErrorId ☐ ErrorLabel ☒ Other

ErrorClass

☒ Hardware

☒ Software

☐ Informational

☐ Undetermined

ErrorType

☒ Pending

☒ Performance

☐ Permanent

☐ Unknown

☐ Temporary

☐ Informational

ResourceName list

dumpcheck,SYSJ2

Liste of ResourceName values separated with comma and without any space

Figure 5-52. Aix Syslog Filter other properties

Set the **ErrorClass** list by checking the boxes.

If no ErrorClass button is checked, no filter is applied on ErrorClass attribute.

Set the **ErrorType** list by checking the boxes.

If no ErrorType button is checked, no filter is applied on ErrorType attribute.

Set the **ResourceName** list with a list of ResourceName separated with comma and without space.

If the ResourceName list is empty, no filter is applied on ResourceName attribute.

5.4.4.2 Configuring Host

To configure hosts, click the hosts item in the Monitoring part of the Supervision tab. The list of configured hosts appears, as in the following example:

Hosts Supervision

	name	platform	description	model	netName	OS
Edit	FRCLS3105	-	System Management Server	other	FRCLS3105	windows
Edit	aixHv4	-	N/A	other	172.31.50.97	aix
Edit	frcls6260	-	SystemManagement Agent	other	129.182.6.33	linux
Edit	hv453nsm	-	SystemManagement Server	other	172.31.50.97	aix
Edit	linuxRedHat	-	N/A	other	172.31.50.60	linux
Edit	rh54.frcl.bull.fr	-	SystemManagement Server	other	172.31.50.60	linux

Figure 5-53. Hosts configuration window

Note See *Create / Edit / Delete Resources* on page 19 for details.

As shown in the following example, edit an Aix host.

Set the **Syslog Monitoring** attribute to **Yes** or **No**.

Select a **Syslog Filter** in the list: only Syslog Filters of **AIX-errpt** type will be proposed. If no **Syslog Filter** is selected, no filter is applied.

Host object

*This host can only be deleted from the menu
Topology/Hosts Definition/Other hosts.*

OK

Cancel

Properties	
name	aixHv4
model	other
OS family	AIX family
Management attributes	
host management	<input checked="" type="radio"/> active <input type="radio"/> inactive
ping checking	<input checked="" type="radio"/> Yes <input type="radio"/> No
Hardware monitoring	<input checked="" type="radio"/> Yes <input type="radio"/> No
Operating System monitoring	<input checked="" type="radio"/> Yes <input type="radio"/> No
Storage monitoring	<input checked="" type="radio"/> Yes <input type="radio"/> No
Virtualization monitoring	<input checked="" type="radio"/> Yes <input type="radio"/> No
Network monitoring	<input checked="" type="radio"/> Yes <input type="radio"/> No
Power monitoring	<input checked="" type="radio"/> Yes <input type="radio"/> No
Syslog monitoring attributes	
Syslog Monitoring	<input checked="" type="radio"/> Yes <input type="radio"/> No
Syslog Filter	syslogfilter_aix
Notification attributes	
notifications enabled	
enable SNMP trap	
notification period	
re-notification interval	
notify if down	<input checked="" type="radio"/> Yes <input type="radio"/> No
notify if unreachable	<input checked="" type="radio"/> Yes <input type="radio"/> No
notify if recovery	<input checked="" type="radio"/> Yes <input type="radio"/> No
e-mail contact groups	<div><div>Selected Objects</div><div>mgt-admins</div><div>All Objects</div><div>mgt-admins mgt-report</div><div><= Add Remove =></div></div>

Figure 5-54. Host monitoring properties

Chapter 6. Configuring Supervision Event Reception

Bull System Manager can receive SNMP traps from any SNMP agent. This chapter explains how to configure Event reception. This configuration consists in integrating a MIB and enabling or disabling the SNMP trap receiver service.

6.1 Integrating MIBs

To receive the SNMP traps from specific equipment, the equipment MIB must be integrated into Bull System Manager.

By default, some MIBs are integrated in the Bull System Manager solution.

To display SNMP MIBs, click the **Mibs** link under **Event reception** function in the Bull System Manager Console. The following display appears:

SNMP MIBs integration			
Help on SNMP MIBs integration			
New MIB			
	MIB file	description	Monitoring Service
Edit	PAMEventtrap.mib	MIB PAM NovaScale 5000 and 6000 series	PAM.Alerts
Edit	SmSnmp.mib	MIB NovaScale 3000 series	Hardware.Alerts
Edit	basebrd5_v1.mib	MIB SNMP V1 NovaScale 4000 series	Hardware.Alerts
Edit	basebrd5_v2.mib	MIB SNMP V2 NovaScale 4000 series	Hardware.Alerts
Edit	bmclanpet.mib	MIB for PET events	Hardware.Alerts
Edit	mmalert.mib	MIB CMM NovaScale Blade series	CMM.Alerts

Figure 6-1. Default SNMP Mibs integration

To display and change the SNMP MIB properties click the **Edit** link:

SNMP MIBs integration	
OK	Cancel Delete
Properties	
MIB file	PAMEventtrap.mib
description	MIB PAM NovaScale 5000 and 6000 series
Monitoring Service	PAM.Alerts
SNMP traps customization	
Trap name	Trap severity
bullPamCriticalTrap	critical
bullPamVarningTrap	minor
bullPamSuccessTrap	normal
bullPamInfoTrap	normal
Enter the required data and click OK. This may take a few minutes.	

Figure 6-2. SNMP MIB integration Edition

MIB Properties	Description
MIB file	MIB file name. This name must be suffixed by .mib .
description	MIB description.
Monitoring Service	Monitoring category and service (e.g. in PAM SNMP traps will be visible in the BSM Console Management tree under PAM Alerts).
Trap name	SNMP trap name as defined in the MIB.
Trap severity	<p>TRAP severity as defined in the MIB or customized by the Administrator. If not specified in the MIB, severity is set to normal by default.</p> <p>Note: Trap customization consists in modifying the displayed trap severity value if this value is not pertinent. Select a value in the select box (normal, cleared, critical, indeterminate, major, minor, warning or informational).</p>

Table 6-1. SNMP MIB properties

Click **OK** to validate the changes, **Delete** to remove the MIB, or **Cancel** to leave the integration unchanged.

Trap customization may be not effective if the following message appears:

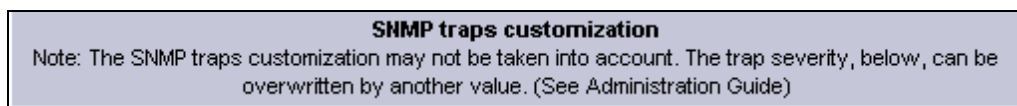


Figure 6-3. SNMP trap customization message

In some cases, the severity of the trap is determined by a specific independent procedure (for instance, it may be extracted from an attribute of the trap).

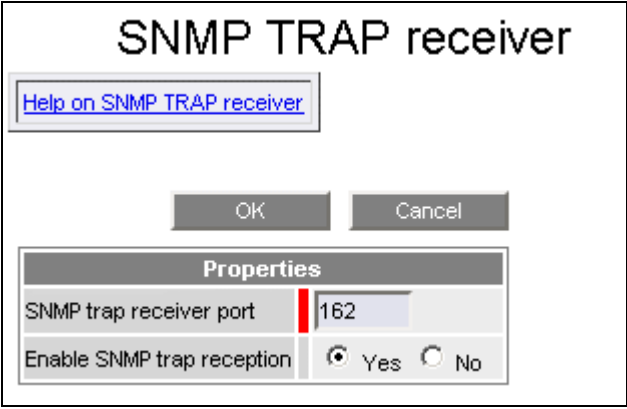
To integrate a new MIB, click **New MIB** and initialize the name of the MIB file, the description and the Monitoring service.

Please note that:

- the MIB file must be installed in the following directory:
<Bull System Manager server Installation Directory>/engine/etc/snmp/mibs
- the Monitoring service (category and service) must be created before MIB integration. See *Creating an Alerts Service*, on page 115, for details about creating a new Alert Service.

6.2 Controlling the Trap Receiver

To control the SNMP trap receiver process, click the **Control** link under **Event reception** in the Bull System Manager Console. The following display appears:

A screenshot of a Windows-style dialog box titled "SNMP TRAP receiver". At the top left is a button labeled "Help on SNMP TRAP receiver". Below it are "OK" and "Cancel" buttons. A "Properties" section contains two settings: "SNMP trap receiver port" with a text box showing "162" and a red vertical bar on the left, and "Enable SNMP trap reception" with two radio buttons, "Yes" (selected) and "No".

SNMP TRAP receiver	
Help on SNMP TRAP receiver	
<div>OK Cancel</div>	
Properties	
SNMP trap receiver port	162
Enable SNMP trap reception	<input checked="" type="radio"/> Yes <input type="radio"/> No

Figure 6-4. Control SNMP trap receiver

SNMP Trap Properties	Description
SNMP trap receiver port	Port used to receive SNMP traps. Linux: the SNMP trap receiver is the snmptrapd process. Default value: <i>162</i> . Windows: the SNMP trap service receives SNMP traps on port <i>162</i> and forwards them to the Bull System Manager snmptrapd on port <i>1620</i> . Default value: <i>1620</i> . This value may be changed to avoid conflicts with other applications
Enable SNMP trap reception	Enable or disable SNMP trap reception. Default value: Yes.

Table 6-2. SNMP trap properties

Chapter 7. Configuring Performance Indicators

This chapter explains how to define a performance indicator in the Bull System Manager configuration.

7.1 Configuring Reporting

A **performance indicator** is collected regularly, every 5 minutes, from Bull System Manager monitoring data or from the SNMP protocol.

Bull System Manager **Reporting** creates an HTML page (every 5 minutes) representing the evolution of the indicator on four graphs: **daily**, **weekly**, **monthly** and **yearly**.

Indicators can be displayed by clicking the **Reports** button on the Bull System Manager home page.

Bull System Manager Monitoring checks that Bull System Manager service (**used memory**, **used cpu**, **number of users**) values are limited to specific thresholds. This information is used to get certain service values at regular intervals for Reporting functions.

BSM monitoring information, associated to a service, may contain more than one value inside the returned string. Each of these values (up to three) can be a filter associated to a performance indicator.

As administrator, you can specify the target host and service (and filter name when the service is a BSM monitoring service) for which values are to be retrieved. Note that it is possible, using BSM monitoring collect, to select several hosts for a given report indicator.

On a **Windows** host, the services that can be used to create performance indicators are:

- **SystemLoad.CPU**: total CPU load percent over 10 minutes. This service has only one filter, named **"used"**.
- **SystemLoad.Memory**: memory usage percent (i.e. the sum of physical and virtual memory, also known as commit charge). This service has only one filter, named **"used"**.
- **LogicalDisks.C**: the percent of used space for the local disk C. This service has only one filter, named **"used"**.
- **LogicalDisks.X**: the percent of used space for any logical disk (named here X) associated with the LogicalDisks.X service (clone of the LogicalDisks.C predefined service).

On a **Linux** host, the services that can be used to create performance indicators are:

- **SystemLoad.CPU**: total CPU load percent over 5 minutes. This service has three filters named **"cpu5mn"**, **"cpu15mn"** and **"cpu1mn"** corresponding to cpu percent over 5 min, 15 min and 1 min.
- **SystemLoad.Memory**: memory usage percent (i.e. the sum of physical and virtual memory). This service has two filters named **"used"** and **"freeMB"**.
- **SystemLoad.Users**: the number of currently logged users. This service has only one filter named **"users"**.

- **SystemLoad.Processes**: the number of running processes. This service has only one filter named "processes".
- **FileSystems./usr**: the percent of free (and not used) space for the /usr FileSystem. This service has only one filter named "free".
- **FileSystems.X**: the percent of free space for any FileSystem (named here X) associated with the FileSystems.X service (clone of the FileSystems./usr predefined service).

An indicator may also be collected using the SNMP dialog between the Bull System Manager server and the remote host. As administrator, you can specify the target host, the **oid** for which the value is to be retrieved, the port and community used to dialog between the Bull System Manager server and the target host.

Linux Requirements:

On the Bull System Manager server:

- the **PHP-SNMP** RPM must be installed.

On the remote host:

- the SNMP agent must be running
- SNMP configuration allows the Bull System Manager server to get data using SNMP dialog.

For more details about requirements, please refer to the NovaScale Performance Indicator Module in the *Bull System Manager Installation Guide* (86 A2 54FA). See also the *Bull System Manager User's Guide* (86 A2 55FA).

The following figure shows the page used to create a Performance indicator. Two collect modes are available: **Bull System Manager monitoring** and **snmp**. The form differs according to the selected collect mode (see the following figures).

The screenshot shows a 'Properties' dialog box with the following sections:

- name**: A text input field.
- host**: A section with two columns: 'Selected Hosts' (empty) and 'All Hosts' (containing a list: *, AIX_HV4, FRCLS8004, LPAR1, NST820). Between the columns are buttons '<= Add' and 'Remove =>'.
- status**: Radio buttons for 'active' (selected) and 'inactive'.
- collect mode**: Radio buttons for 'BSM monitoring' (selected) and 'snmp'.
- BSM monitoring collect (Source)**: A section with a 'service' dropdown menu and a 'filter' dropdown menu.
- Graph information**: A section with 'graph title' and 'graph legend' text input fields.

Figure 7-1. Indicator properties - BSM monitoring collect mode

Properties	
name	<input type="text"/>
host	<div> <div>Selected Hosts</div> <div> <input type="text"/> <input type="text"/> <input type="text"/> </div> <div> <input type="button" value="Add"/> <input type="button" value="Remove"/> </div> </div> <div> <div>All Hosts</div> <div> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> </div> </div>
status	<input checked="" type="radio"/> active <input type="radio"/> inactive
collect mode	<input type="radio"/> BSM monitoring <input checked="" type="radio"/> snmp
Snmp collect (Source)	
relative	<input type="radio"/> Yes <input checked="" type="radio"/> No
port	<input type="text" value="161"/>
community	<input type="text" value="public"/>
oid	<input type="text"/> <input type="button" value="Browse Mibs .."/> <input type="button" value="Get value"/>
result filter (in unix shell syntax)	<input type="text" value="cut -d '=' -f 2 cut -d ':' -f 2"/> <input type="button" value="Test filter"/>
Graph information	
graph title	<input type="text"/>
graph legend	<input type="text"/>

Figure 7-2. Indicator properties - snmp collect mode

Indicator Properties	Description
name	Performance indicator name. All indicator names are displayed when, as administrator, you select Reports from the Bull System Manager home page. When you a given indicator name, you display the associated graphs.
host	Name of the host in the Bull System Manager configuration. Note that it is possible, using BSM monitoring collect, to select several hosts for a given report indicator.
status	Reporting status (active or inactive) Active status means that the collect of the indicator is started. Inactive status means that the collect of the indicator is not performed. Default: active
collect mode	If the collect mode is Bull System Manager monitoring , a service parameter is required. Bull System Manager will retrieve the value from information collected by the Bull System Manager monitoring associated with this service. If the collect mode is snmp , the port, community, oid and result filter parameters are required. Default value: Bull System Manager monitoring .
service	Available if the collect mode is Bull System Manager monitoring . A select box lists all available services for the specified host (it takes into account the host list of each service).
relative	yes means that Bull System Manager Reporting reports a value calculated as follows: the difference between the current and the previous value, divided by the elapsed time between the two last readings (300 seconds). "no" means that Bull System Manager Reporting reports the current value. Default value: no.
port	The port used to communicate with the remote snmp agent located on the specified host. Default value: 161 .

Indicator Properties	Description
community	The community used to communicate with the remote snmp agent located on the specified host. Default value: public .
oid	The oid for which the value is to be retrieved with snmp protocol. The oid must begin with a . character and must be in numerical form as .1.3.6.1.2.1.25.3.3.1.2.2. The oid designates an instance. Examples: uptime oid is: .1.3.6.1.2.1.1.3.0, oid for load of a specific processor is: .1.3.6.1.2.1.25.3.3.1.2.2 To check that you have specified a correct oid, click Get value to see the value of this oid, retrieved from the snmp protocol. You can also click Browse Mibs to find the correct numerical oid. Then click Select this oid to automatically set the oid field in the form.
result filter	Defines a filter to extract the value of interest from the result returned by the snmp request (which can be in text format). Click Get value for the result of the snmp request, then specify the appropriate filter. Test the filter by clicking Test filter . The filter expression uses Unix command syntax. It can be a series of piped cut -d commands. Example: to extract the uptime value from the Timeticks text: (26036090) 3 days, 0:19:20.90, specify <code>cut -d '=' -f 2 cut -d ')' -f 2 cut -d 'd' -f 1</code>
graph title	Title of the graph. Example: <code>SystemLoad.Memory on frcl180</code> .
graph legend	Data unit (%used, days ...) as displayed on the vertical axis of the graph.

Table 7-1. Indicator properties

Note for Bull System Manager server on Windows

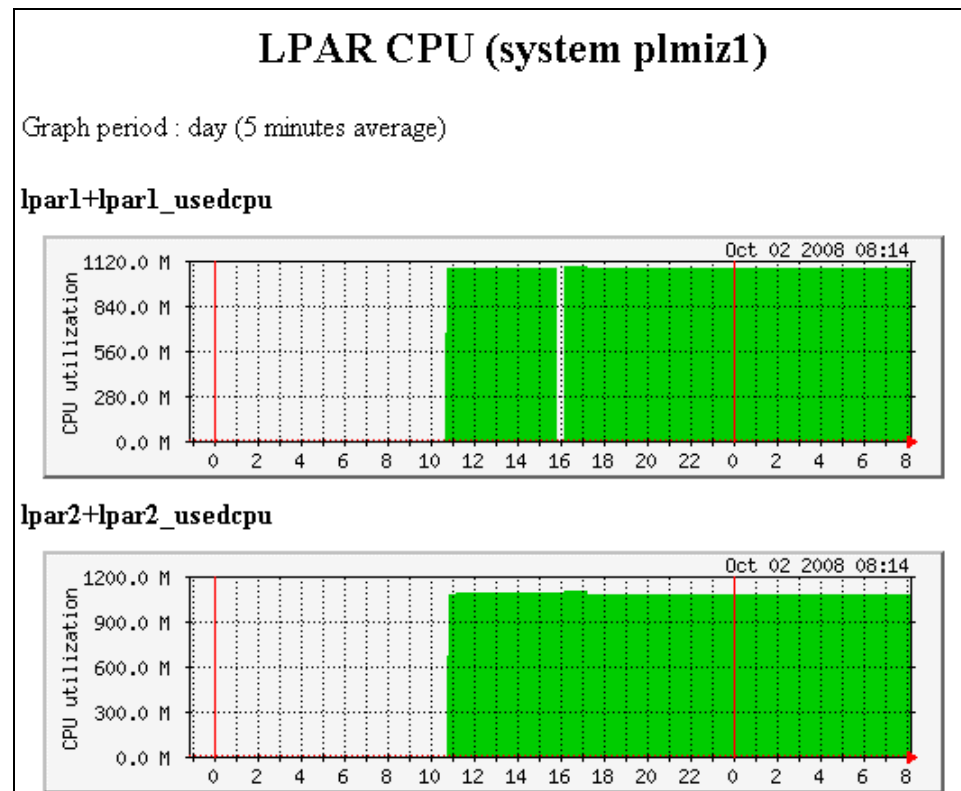
The names of hosts and indicators listed by Bull System Manager Console Report are displayed in lowercase in the Bull System Manager console even if they contain uppercase characters in Bull System Manager configuration.

The internal files generated for reporting (for MRTG) have their name in lowercase characters. This is due to the MRTG product on Windows, used by Bull System Manager server to generate reports. Take care of not create two indicators with same string, one in uppercase characters and the second in lowercase characters: an indicator will be replaced by the other.

You may specify a graph of several indicators, of same or different hosts:

Properties		
graph_indic_name	plmiz1_lpar_cpu	
indicList	<div>Selected Indicators</div> <div>lpar1+lpar1_UsedCPU lpar2+lpar2_UsedCPU</div> <div><div><= Add</div><div>Remove =></div></div>	<div>All Indicators</div> <div>* galilei+galilei_UsedCPU lpar1+lpar1_UsedCPU lpar2+lpar2_UsedCPU plmiz1+plmiz1_UsedPool</div>
	period	day
title	LPAR CPU (system plmiz1)	

The result in the console is the following:



7.1.1 Example: Configuring an Indicator from Bull System Manager Monitoring Data

In this example, we assume that the service associated with the indicator is already defined (explicitly or by default).

1. Click **Reporting > Indicators**: the defined indicators are listed with details.
2. From the **Indicators** page, click **New** to edit a new indicator.
 - Enter the name, for example `2703_cpuload`.
 - Select the host on which the indicator will be measured, for example `FRCLS2703`.
 - Select the **Bull System Manager Monitoring** collect mode.
 - Select the **SystemLoad.CPU** service. Select a filter (here `used`). The graph title automatically displays **SystemLoad.CPU (windows)** and the graph legend displays `used`.
 - Click **OK** to validate the definition.
3. When all indicators are defined, click **Save & Reload** to save and launch the new reporting configuration.

The screenshot shows a 'Properties' dialog box for an indicator. The 'name' field is '2703_cpuload'. The 'host' field is 'FRCLS2703', selected from a list of 'All Hosts' which includes '*', 'AIX_HV4', 'FRCLS2703', 'FRCLS8004', and 'LPAR1'. The 'status' is set to 'active'. The 'collect mode' is 'BSM monitoring'. Under 'BSM monitoring collect (Source)', the 'service' is 'SystemLoad.CPU (windows)' and the 'filter' is 'used'. The 'graph title' is 'SystemLoad.CPU (windows)' and the 'graph legend' is 'used'.

Properties	
name	2703_cpuload
host	<div>Selected Hosts: FRCLS2703</div> <div>All Hosts: *, AIX_HV4, FRCLS2703, FRCLS8004, LPAR1</div> <div><= Add, Remove =></div>
status	<input checked="" type="radio"/> active <input type="radio"/> inactive
collect mode	<input checked="" type="radio"/> BSM monitoring <input type="radio"/> snmp
BSM monitoring collect (Source)	
service	SystemLoad.CPU (windows)
filter	used
Graph information	
graph title	SystemLoad.CPU (windows)
graph legend	used

Figure 7-3. Indicator properties - example

7.1.2

Example: Configuring an Indicator from SNMP Protocol

In this example, we assume that SNMP dialog is available between Bull System Manager server and the remote host.

1. Click **Reporting -> Indicators**: the defined indicators are listed with details.
2. From the Indicators page, click **New** to edit a new indicator.
 - Enter the name, for example `2703_uptime`.
 - Select the host on which the indicator will be measured, for example `FRCLS2703`.
 - Select the **snmp** collect mode.
 - Choose **yes** for **relative** because the value of interest to be reported is the **number of input bytes per second**.
 - Maintain the default **port** and **community** values, which are `161` and `public`.
 - Click **Browse Mibs** to find the **oid** corresponding to `sysUptime`. When the oid is found, click **Select this oid** to complete automatically the oid field. See details in *Browse Mibs Details*, on page 160.
 - Click **Test filter** to check that the default filter is correct for extracting the value of interest from the returned text. If not, append piped cut commands and test again.
 - Complete the graph title with `Uptime frcls2703`.
 - Complete the graph legend with `days`.
 - Click **OK** to validate the definition.
3. When all indicators are defined, click **Save & Reload** to save and launch the new reporting configuration

Properties	
name	2703_uptime
host	<div>Selected Hosts frcls2703.frcl.bull.fr</div> <div>All Hosts frcls2681.frcl.bull.fr frcls2703.frcl.bull.fr frcls3104.fr.ad.bull.net frcls4620.frcl.bull.fr frcls6260.frcl.bull.fr</div> <div><= Add Remove =></div>
status	<input checked="" type="radio"/> active <input type="radio"/> inactive
collect mode	<input type="radio"/> BSM monitoring <input checked="" type="radio"/> snmp
Snmp collect (Source)	
relative	<input checked="" type="radio"/> Yes <input type="radio"/> No
port	161
community	public
oid	1.3.6.1.2.1.1.3 Browse Mibs ... Get value
result filter (in unix shell syntax)	cut -d '=' -f 2 cut -d ':' -f 2 Test filter
Graph information	
graph title	Uptime frcls2703
graph legend	days

Figure 7-4. Defining a new indicator

The report associated with this indicator is similar to the following:

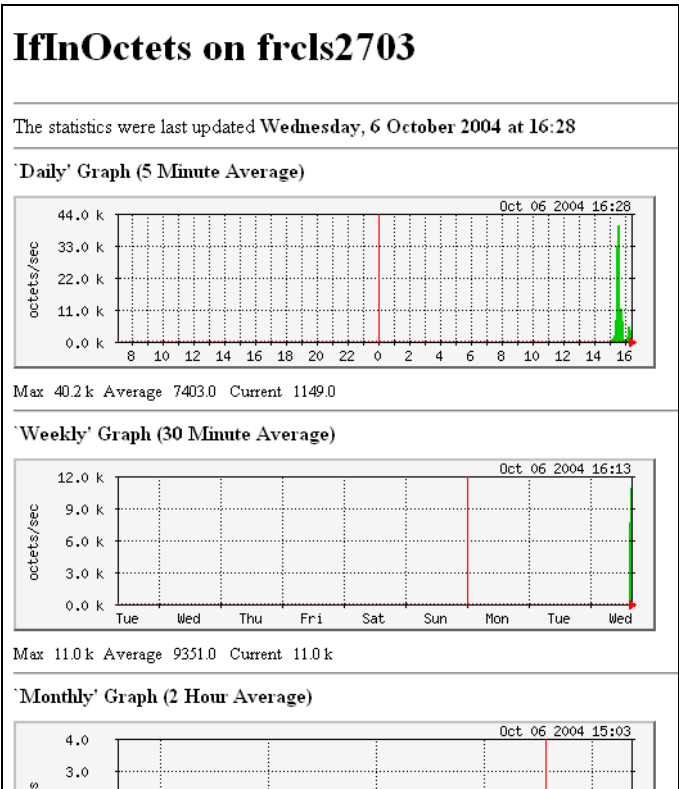


Figure 7-5. Indicator graphs

7.1.3 Browse Mibs Details

The **Browse Mibs** function allows you to navigate in the **mibs tree**. The entry point is **.iso.org.dod.internet (.1.3.6.1)**.

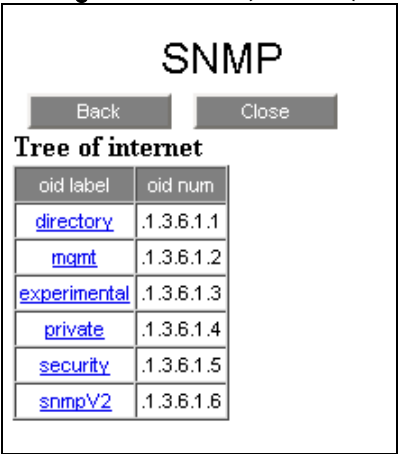
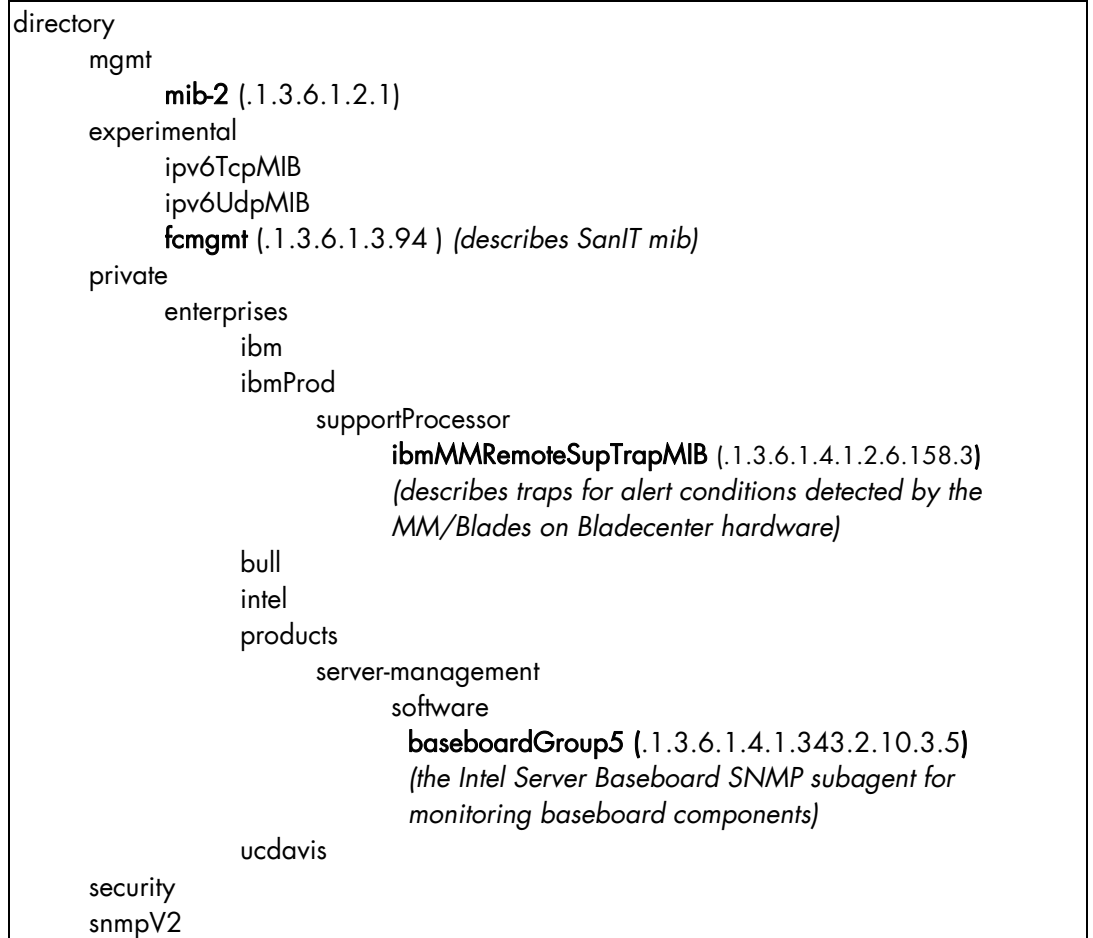


Figure 7-6. Browse Mibs: mibs tree

To define a new mib, enter the definition under the following directory:

- Linux: `/usr/share/snmp/mibs`
- Windows: `<Bull System Manager install dir>\engine\usr\share\snmp\mibs`

The **mibs tree** is similar to the following:



Currently, mib browsing reaches instances of mib resources (on a given host):

Tree of .1.3.6.1.2.1.2.2.1.10

oid label	oid num
interfaces.ifTable.ifEntry.ifInOctets.1	.1.3.6.1.2.1.2.2.1.10.1
interfaces.ifTable.ifEntry.ifInOctets.65539	.1.3.6.1.2.1.2.2.1.10.65539
interfaces.ifTable.ifEntry.ifInOctets.262148	.1.3.6.1.2.1.2.2.1.10.262148

Figure 7-7. MIB resource

When you click one of this instance, you get the value. Click **Select this oid** to complete automatically the **oid** field in the indicator page.

The value of interfaces.ifTable.ifEntry.ifInOctets.65539 (.1.3.6.1.2.1.2.2.1.10.65539) on is :

Counter32: 1448841114

Select this oid

Figure 7-8. Select this oid button

Figure 7-9. Getting the oid property

7.2 Configuring export

7.2.1 Export daily information of a perf_indic

A Periodic Task can be configured to generate a daily repository file for each indicator. Bull System Manager uses a CRON engine to schedule this task. The files are stored in a WEB shared directory:

"http://<BSM URL>/reporting/var/export2send".

NB: the CRON task delete all files 30 days years older.

At installation, this specific task is always disabled. To enable it, proceed as follows: Click the **Periodic Tasks** link in the **Functionalities** part of the **GlobalSetting** tab. The "exportMrtg" task is listed, as displayed in the following page:

	Name	Description	Period	Enabled
Edit	exportMrtg	periodic task to export MRTG metrics	00 22 * * *	no
Edit	updateInventory	periodic task to update inventory	0 0 * * *	no

Figure 7-10. Periodic Tasks list

To configure this task, proceed as follows:

1. Click the **Edit** link of the "exportMRTG" task. The list of its properties appears:

The screenshot shows the BSM Configuration web interface. The top navigation bar includes 'Topology', 'Third-Party Application', 'Supervision', 'Console', and 'GlobalSettings'. The 'GlobalSettings' section is active, showing a sidebar with 'Users', 'Functionalities', and 'BSM Server'. The main content area is titled 'Periodic task' and contains a 'Help on Task' link, 'OK' and 'Cancel' buttons, and a 'Properties' table.

Properties	
name	exportMrtg
description	periodic task to export MRTG metrics
period	00 22 * * *
enable	<input type="radio"/> Yes <input checked="" type="radio"/> No
Command description	
command	/bin/exportMRTG_All.sh
command parameters	DEFAULT_PERIOD 24

Figure 7-11. exportMRTG periodic task properties

2. Modify the period if needed: the periodicity is defined on five fields as standard cron format: <minute(0-59)> <hour(0-23)> <day of month(0-31)> < month(0-12) or names> <day of week(1-7) or name>".
A field may be an asterisk (*), which always stands for 'first-last': for instance "00 22 * * *" corresponds to a daily execution at 22h.
Range or list of numbers are allowed: for instance "8-11" in hour field specifies execution at hours 8, 9, 10 and 11.
Steps can be used in conjunction with ranges or after asterisk: for instance "* */5" in minute field specifies execution every five minutes.
See *CRON Reference Manual* to get detailed informations. By default the task is scheduled daily at 22:00.
3. Enable the task. By default the task is disabled.
4. Choose the historical period for each file 24 hours or 48 hours. By default the value is 24.
5. Click **OK** to validate.

7.2.2 Monitor and Notify by Mail the daily information of a perf_indic

Associated to this daily files generation, a Nagios plugin can be used to notify by mail the content of these files. Indeed, the "METROLOGY.exportToNotify" monitoring service takes each file present in the export2send directory, notify its content and move the file in another WEB shared directory "http://<BSM URL>/reporting/var/exportsent".

To check monitor and notify export files, Bull System Manager provides the **METROLOGY.exportToNotify** service template.

category	service	check_command	check parameters
METROLOGY	exportToNotify	check_exportMRTG	None

The **METROLOGY.exportToNotify** service template can be used as described in the following example.

Example :

To apply the **METROLOGY.exportToNotify** service to a set of hosts, proceed as follows:

6. From the **filter by HOST** option select `frcls6260`, and click **Apply**.
7. Click the **manage service** link of the category in which you want to put this service.
8. In the **Manage Service** popup window, check **Add from service template** and select the **METROLOGY.exportToNotify** service. Then click the **add from the selected service** button.
9. If you do not use the **filter by HOST** option, change the **host list** with the name of the Bull System Manager server (`frcls6260`).
10. You can change this service parameter:

Properties	
category	METROLOGY
name	exportToNotify
description	verify files to export to notify them
model	any
OS family	any
host list expression	*
Monitoring attributes	
status	<input checked="" type="radio"/> active <input type="radio"/> inactive
Monitoring command attributes (for this service)	
monitoring on event	<input type="radio"/> Yes <input checked="" type="radio"/> No
monitoring by polling	<input checked="" type="radio"/> Yes <input type="radio"/> No
check command	check_exportMRTG
monitoring period	exporthours
polling interval	5 mn (5 mn by default if empty)
Notification attributes (for this service)	
e-mail contact groups	<div> <div>Selected Objects</div> <div> mgt-report </div> </div> <div> <div>All Objects</div> <div> mgt-admins mgt-report </div> </div> <div> <div><= Add</div> <div>Remove =></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 type="radio"/> Yes <input checked="" type="radio"/> No

The specific properties of this service are:

- The monitoring period: "exporthours" corresponding to 00:00 until 06:00 AM period
- The contact group: "mgt-report" which contains the contact "report" by default.

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

The monitoring service status looks as follows:

Service	Status	Last Check	Duration	Information
METROLOGY.exportToNotify	WARNING	0d 0h 0m 5s ago	0d 0h 0m 5s	2 files to export found for frcls0564. The first is 1237140902.METROLOGY_of_frcls0564_cpu_on_frcls0564.txt to notify

The notification mail looks as follows:

```

"
***** Bull System Manager (nagios 3.0) *****

Notification Type: PROBLEM

Service: METROLOGY.exportToNotify
Host: frcls0564 Description: System Management Server
Address: frcls0564
State: WARNING

Date/Time: Thu Mar 12 18:12:04      2009

Information:

15 files to export found for frcls0564. The first is
1236875702.METROLOGY_of_memoryused_frcls0564_on_frcls0564.txt to notify

Additional Info:

DATE: 1236875702 (2009-03-12 17:35:02 +01:00)

HOST: frcls0564
INDICATOR: memoryused_frcls0564
LEGEND: used

Last 48 hours metrology (every 5mn)
#####
1236875100 54
1236874800 54
1236874500 54
1236874200 53
1236873900 53
1236873600 53
1236873300 53
1236873000 53
...

1236702900 0
1236702600 0

BSM link for this host:
http://<BSM\_netname>:10080/BSM/console/heading-
php/wrapper.php?panel=Services\_status&host=frcls0564&nodetype=host
"

```


Chapter 8. Configuring Event Handler

This chapter explains how to define an event handler in a Bull System Manager configuration. Event handlers are optional commands that are executed, on Bull System Manager server, whenever a host or service state change occurs:

- UP, DOWN and UNREACHABLE states for a host
- OK, WARNING, UNKNOWN and CRITICAL states for a service.

The PENDING service state is an initial state. A service state cannot change into a PENDING state.

Two main types of event handlers can be defined:
service event handlers and host event handlers.

8.1 Event Handler Definition

To configure Event Handlers click the **Handler** link in the **EventHandler** part of the **Supervision** tab.

8.1.1 Host Event Handler

The following figure shows the form displayed to create a new event handler for a host.

The screenshot shows a web form titled "Properties" for creating a new event handler. It is divided into three main sections: "Properties", "Event handler definition", and "Event handler control".

- Properties:** Contains two text input fields: "handler name" and "description".
- Event handler definition:** Contains an "executable command" text input field, a "handler type" section with radio buttons for "host" (selected) and "service", and a "hosts list" section. The "hosts list" section includes two lists: "Selected Hosts" (empty) and "All Hosts" (containing "bull", "frcls2681.frcl.bull.fr", "frcls2703.frcl.bull.fr", "frcls3104.fr.ad.bull.net", and "frcls4620.frcl.bull.fr"). Between the lists are buttons for "<= Add" and "Remove =>".
- Event handler control:** Contains a section "enable event handler" with radio buttons for "Yes" (selected) and "No".

Figure 8-1. Host event handler creation

handler name	event handler name.
description	event handler description.

Event handler definition

executable command	full pathname of the command. The file must exist.
system command	specifies if the command must be executed being root user. This attribute is only displayed if Bull System Manager server is running on Linux.
handler type	handler type (host).
hosts list	list of the hosts on which the event handler will be applied.

Event Handler control

enable event handler	controls (enable/disable) the event handler.
-----------------------------	--

Note Several event handlers can be specified for a given host, in which case, commands will be launched sequentially.

8.1.2 Service Event Handler

The following figure shows the form displayed to create a new event handler for a service.

The screenshot shows a 'Properties' dialog box for configuring an event handler. It includes fields for 'handler name' and 'description'. The 'Event handler definition' section contains an 'executable command' field, a 'handler type' section with radio buttons for 'host' and 'service' (where 'service' is selected), and two list management sections: 'services list' and 'hosts list'. Each list section has a 'Selected' list, an 'All' list, and buttons for '<= Add' and 'Remove =>'. The 'services list' 'All' list contains: '*', 'AIXServices.syslogd(aix-any)', 'EventLog.Application(windows-any)', 'EventLog.Security(windows-any)', and 'EventLog.System(windows-any)'. The 'hosts list' 'All' list contains: 'bull', 'frcls2681.frcl.bull.fr', 'frcls2703.frcl.bull.fr', 'frcls3104.fr.ad.bull.net', and 'frcls4620.frcl.bull.fr'. The 'Event handler control' section at the bottom has a radio button for 'enable event handler' with 'Yes' selected.

handler name	event handler name.
description	event handler description.

Event handler definition

executable command	full pathname of the command. The file must exist on the Bull System Manager server.
system command	specifies if the command must be executed being root user. This attribute is only displayed if Bull System Manager server is running on Linux.
handler type	handler type (host).
services list	list of the services on which the event handler will be applied only for the hosts specified below.
hosts list	list of the hosts on which the event handler will be applied.

Event Handler control

enable event handler	controls (enable/disable) the event handler.
-----------------------------	--

Note Only one event handler can be specified for a service.

8.2 Event Handler Command

Event handler commands are shell or perl scripts. They can be bat files on Windows.

8.2.1 Host Event Handler Arguments

The script for a host event handler requires the following arguments:

<event-handler command> HOSTSTATE HOSTADDRESS	
HOSTSTATE	state of the host (UP, DOWN, UNREACHABLE)
HOSTADDRESS	network address of the host

8.2.2 Service Event Handler Arguments

The script for a service event handler requires the following arguments:

<event-handler command> SERVICESTATE HOSTADDRESS SERVICEDESC	
SERVICESTATE	state of the service (OK, WARNING, CRITICAL, UNKNOWN)
HOSTADDRESS	network address of the host
SERVICEDESC	service description (<category name>.<service name>)

8.3 Event Handler Templates

8.3.1 Host Event Handler

```
#!/bin/bash
# HOST EVENT handler
# arguments: $HOSTSTATE $HOSTADDRESS
# $1=state(UP,DOWN,UNREACHABLE)
# $2=host netname

case "$1" in
UP)
    # action on UP state
    ;;
DOWN)
    # action on DOWN state
    ;;
UNREACHABLE)
    # action on UNREACHABLE state
    ;;
esac
exit 0
```

8.3.2 Service Event Handler

```
#!/bin/bash
# Event handler template

# SERVICE EVENT handler
# arguments: $SERVICESTATE $HOSTADDRESS $SERVICEDESC
# $1=state(OK,WARNING,UNKNOWN,CRITICAL)
# $2=host netname
# $3=service name

# service state

case "$1" in
OK)
    # action on OK state
    ;;
WARNING)
    # action on WARNING state
    ;;
UNKNOWN)
    # action on UNKNOWN state
    ;;
CRITICAL)
    # action on CRITICAL state
    ;;
esac
exit 0
```

8.4 Sample Event Handler

```
#!/bin/sh
#
# Event handler script for restarting the web server on the local
machine
#
# What state is the HTTP service in?
case "$1" in
OK)
    # The service just came back up, so don't do anything...
    ;;
WARNING)
    # We don't really care about warning states, since the
service is probably still running...
    ;;
UNKNOWN)
    # We don't know what might be causing an unknown error, so
don't do anything...
    ;;
CRITICAL)
    # The HTTP service appears to have a problem - perhaps we
should restart the server...
    echo -n "Restarting HTTP service..."
    # Call the init script to restart the HTTPD server
/etc/rc.d/init.d/httpd restart
    ;;
esac
exit 0
```

Chapter 9. Configuring Notifications

This chapter describes notifications sent by e-mails, autocalls or SNMP traps. The decision to send out notifications is made at service and host monitoring level. Host and service notifications are sent out when an anomaly or a recovery is detected.

Notification periods are specified at different levels according to requirements: **24x7**, **workhours**, **nonworkhours**, **none** (**none** disables notifications).

- **Host and service notification period:** defines when a notification is to be sent.
- **Contact notification period for host alerts:** defines when a notification about host problems and recoveries is to be sent.
- **Contact notification period for service alerts:** defines when a notification about service problems and recoveries is to be sent.

The **notification period for service alerts** and **notification period for host alerts** define an **on call** period for each contact.

It may be helpful to specify different times for host and service notifications. For example, for a given contact, you can specify:

- no host notifications on weekdays
- service notifications on weekdays.

Notification periods should cover *any time* that the contact can be notified.

You can control notification times for specific services and hosts on a one-by-one basis as described below:

The **host notification period** controls when Bull System Manager should send out notifications regarding problems or recoveries for that host. When a **host notification** is about to be sent out, Bull System Manager checks that the current time is within the valid **notification period** range. If the time is valid, Bull System Manager attempts to notify each contact of the host problem.

Note Some contacts may not receive the host notification if their **notification period for host alerts** does not allow host notifications at that time.
If the time is not valid, Bull System Manager does not send out the notification.



Important:

Time period settings allow you to have greater control of how Bull System Manager performs monitoring and notification functions, but can lead to problems. If you are not sure of the times to implement, or if you are having problems with your current settings, we suggest the use of the 24x7 time: all times, every day of the week.

The **host and service re-notification interval** defines the time between two notifications about the same resource.

The “**notify if ...**” options specify in which event a notification is to be sent:

- **Host:** **down**, **unreachable**, or when a **recovery** occurs.
- **Service:** **warning** or **critical** status, or when a **recovery** occurs.

9.1 Notification by E-mail

Sending notifications by e-mail requires:

- access to a mail server
- **enable e-mail notification** set to Yes under Mail server
- contact groups defined with a list of contacts
- contacts defined with a valid e-mail address
- valid and coherent notification periods at host/service, contact levels.

For each service, a **Contactgroup** specifies which contact group will receive notifications for that service. Each Contactgroup can contain one or more individual contacts.

Each host may belong to one or more host groups. For each host group a **Contactgroup** specifies which contact group will receive notifications for hosts in that host group. If a host does not belong to a host group, notifications will not be sent for this host.

9.1.1 Mail Server

To access mail server configuration, click the **Mail server** link in the **Notification** part of the **Monitoring** tab.

The way to create, edit or delete a Mail server is described in *Create / Edit / Delete Resources*, on page 19.

Mail server configuration is different on Linux and Windows platforms.

9.1.1.1 Mail Server on Linux

On Linux platforms, the Bull System Manager server host is normally configured as a Mail server. You have to check that sending mail is operational from the Bull System Manager server host.

The following figure shows the form displayed to edit a **Mail Server** on Linux.

The screenshot shows a 'Properties' window for a Mail Server. It contains the following fields and options:

Properties	
server name	localhost (fully qualified domain name)
description	the local mail server (sendmail in general) is used.
SMTP port	smtp
Notification attributes (for all hosts)	
enable e-mail notification	<input type="radio"/> Yes <input checked="" type="radio"/> No

Figure 9-1. Mail Server properties on Linux

The **enable e-mail notification** property may be changed to enable or disable notification by mail (default value: No).

Note On a Linux Bull System Manager server, the **server name** and **SMTP port** properties are not used and are therefore not editable. Only default information is displayed, which can be different from the local sendmail configuration values.

9.1.1.2 Mail Server on Windows

On Windows platforms, a mail server must be defined. Click **New** to create it.
The following figure shows the form displayed to edit a Mail Server resource on Windows

Properties	
server name	MSG-A-002.frcl.bull.fr (fully qualified domain name)
description	E-mail server
SMTP port	25
sender email	BullSystemManager@bull.net
Notification attributes (for all hosts)	
enable e-mail notification	<input type="radio"/> Yes <input checked="" type="radio"/> No

Figure 9-2. Mail Server properties on Windows

Enter the name of the Mail Server (**server name**), which must be a fully qualified domain name, and type a short description.

The **SMTP port** property is left unchanged. Default value: **25**.

The **enable e-mail notification** property may be changed to enable or disable the notification by mails Default value: **No**.

A valid **sender email** must be specified in some secured network configurations. Otherwise, the sending of an email will fail.

9.1.2 Contacts

A contact identifies the target of the notifications sent by Bull System Manager.
To configure a Contact click the **Contacts** link in the **Notification** part of the **Monitoring** tab.
The following figure shows the form displayed to edit a **Contact**.

Properties	
name	manager
description	System Manager mail contact
email	mgr-admin@localhost.localdomain
Host level notification attributes (for this contact)	
notification period for host alerts	24x7
notify if host down	<input checked="" type="radio"/> Yes <input type="radio"/> No
notify if host unreachable	<input checked="" type="radio"/> Yes <input type="radio"/> No
notify if host recovery	<input checked="" type="radio"/> Yes <input type="radio"/> No
Service level notification attributes (for this contact)	
notification period for service alerts	24x7
notify if service warning	<input checked="" type="radio"/> Yes <input type="radio"/> No
notify if service critical	<input checked="" type="radio"/> Yes <input type="radio"/> No
notify if service recovery	<input checked="" type="radio"/> Yes <input type="radio"/> No

Figure 9-3. Contact properties

Contact Properties	Description
name	Short name used to identify the contact (user name).
description	Contact full name and/or description.
email	Contact e-mail address.
notification period for host alerts	Time during which host notifications must be sent to this contact. Possible values: 24x7, workhours, nonworkhours, none. Default value: 24x7.
notify if host down	Notify contact when hosts are down? Default value: yes.
notify if host unreachable	Notify contact when hosts are unreachable? Default value: yes.
notify if host recovery	Notify contact on host recovery? Default value: yes.
notification period for service alerts	Time during which service notifications must be sent to this contact. Possible values: 24x7, workhours, nonworkhours, none. Default value: 24x7.
notify if service warning	Notify contact on warning service status? Default value: no.
notify if service critical	Notify contact on critical service status? Default value: yes.
notify if service recovery	Notify contact on service recovery? Default value: yes.

Table 9-1. Contact properties

Note The **manager** contact is defined by default. In Figure 9-3, the e-mail address given is only an example.

9.1.3 Contactgroups

A **Contactgroup** groups one or more contacts together in order to send out alert/recovery notifications. When a host or service has a problem or recovers from a problem, Bull System Manager notifies all the contacts in the contact groups concerned by the event.

To configure a ontactgroup, click the **Contactgroups** link in the **Notification** part of the **Monitoring** tab.

The way to create, edit or delete a Mail server is described in *Create / Edit / Delete Resources*, on page 19.

The following figure shows the form displayed to edit a **Contactgroup** resource.

The screenshot shows a 'Properties' dialog box for a Contactgroup. The 'name' field is 'mgt-admins' and the 'description' field is 'Mail contact list'. Below these is the 'element list' section, which contains two lists: 'Selected Contacts' and 'All Contacts'. Both lists contain the 'manager' contact. Between the lists are buttons for '<= Add' and 'Remove =>'.

Figure 9-4. Contactgroup properties

Contactgroup Properties	Description
name	Name of the contact group containing contacts.
description	Description of the resource. This description is just for information and is not visible from the Bull System Manager Console.
element list	List of contacts belonging to this contactgroup. The resources are selected in the All Resources list and moved to the Selected Resources list using the Add button, and vice-versa using the Remove button.

Table 9-2. Contactgroup properties

Note The **mgt-admins** contact group is defined by default. It contains the manager contact. It is used as main contact for all services and hosts and consequently, cannot be removed.

9.1.4 Example: Sending E-mail Notifications

To configure the e-mail notification mechanism, follow these steps:

Step 1: Start Bull System Manager Configuration.

Step 2: Configure the Mail Server (only if Bull System Manager Server runs on a Windows system).

Step 3: Specify the mail address of the receiver.

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

9.1.4.1 Start Bull System Manager Configuration

See *Starting the Configuration GUI*, on page 9.

9.1.4.2 Configure the Mail Server

This step is required only if Bull System Manager Server runs on a Windows system.

1. From the **Notification** part of the **Monitoring** tab, click **Mail server**. The list of defined mail servers is displayed. If no server has been yet defined, this list is empty.
2. Click **New**. The mail server form appears.
3. Enter the host mail server, e.g. `clmail001.frc1.bull.fr`. The **smtp_port** used is the default port for outgoing mail: 25.
4. Set the **enable e-mail notification** field to **Yes**.
5. Click **OK** to validate.

9.1.4.3 Specify the Mail Address of the Receiver

When a problem occurs on a host or service, Bull System Manager sends a notification to contact groups, and not directly to contacts.

Note A contact group is a set of contacts, each contact represented by a mail address.

By default, Bull System Manager defines a contact group named **mgt-admins**, which contains a contact named **manager**. As administrator, you can set up the email address of the **manager** contact and/or add new contact groups and new contacts, according to requirements.

1. From the **Notification** part of the **Monitoring** tab, click **Contacts**: the contacts list is displayed.
2. Click **Edit** to modify default contact properties.
3. Complete the **email** field with the mail address where notifications will be sent. The contact form is displayed.
4. Set the **notification period for host alerts** to **24x7** so that you are permanently notified of host events.
5. Set the **notification period for service alerts** to **24x7** so that you are permanently notified of the monitored service events.
6. By default, you will be notified of all events: host down, host unreachable, host recovery (return to normal status), service warning, service critical and service recovery.
7. By default, you will receive notifications for all services. If you want to receive notifications only for some services, or for some hosts, you must edit the services or hosts definition.
8. To receive notifications at a second mail address, define another contact for this address and add it in the **mgt-admins** group.

9.1.4.4 Reload the Server Part

Click the **Save&Reload** Button to apply modifications to the server part.

9.2 Notification by Autocalls

Autocalls are XML files transferred to the Bull Remote Maintenance Center (GTS server). Sending notifications by Autocalls requires:

- an access to a GTS server name (Bull Remote Maintenance Center)
- **enable Bull autocall** set to **Yes** under Autocall



Important:

Each service has an **enable Bull autocall** option that specifies if the notification may be sent by Autocall or not. The notification will only be sent if **enable Bull autocall** is set to **Yes** under Autocall.

By default, **enable Bull autocall** is set to **Yes** only for the **Alerts** service. The **Alerts** service receives SNMP traps from the NovaScale host.

Autocall Server

The Autocall server specifies the FTP parameters for the server that will receive the autocalls. Autocalls are sent automatically by FTP without user interaction (silent mode). To configure the Autocall server, click the Autocall Server link in the Notification part of the Monitoring tab.

The way to create, edit or delete a Mail server is described in *Create / Edit / Delete Resources*, on page 19.

The following figure shows the form displayed to edit an Autocall resource.

Properties	
name	<input type="text" value="frcls2600.frcl.bull.fr"/> (network name)
description	<input type="text" value="Bull maintenance relay server"/>
FTP port	<input type="text" value="21"/>
target directory	<input type="text" value="/session"/>
Authentication attributes	
login	<input type="text" value="GTSadmin"/>
password	<input type="password" value="...."/> confirm <input type="password" value="...."/>
Notification attributes (to Bull Maintenance site & for all hosts)	
notification period for service alerts	<input type="text" value="24x7"/>
enable Bull autocall	<input type="radio"/> Yes <input checked="" type="radio"/> No

Figure 9-5. Autocall properties

Autocall Properties	Description
name	Host name of the server that will receive autocalls.
description	Server description.
FTP port	The port on which this server will receive autocalls. Default value: 21.
target directory	Directory pathname where autocalls are stored. Default value: /session.
login	User name used by ftp to transmit autocalls.
password	Password used by ftp to transmit autocalls.

Autocall Properties	Description
notification period for service alerts	Time during which service notifications must be sent to this contact. Possible values: 24x7, workhours, nonworkhours, none. Default value: 24x7.
enable Bull autocall	Enable the autocall mechanism? Default value: <i>no</i> .

Table 9-3. Autocall properties

9.3 Notification by SNMP Trap

Notification by SNMP trap allows the integration of Bull System Manager within a global management solution.

Sending notifications by SNMP Trap requires:

- the definition of at least one target of the SNMP trap packet (SNMP Manager),
- **enable SNMP trap** set to **Yes** under SNMP Manager,
- the availability of the **snmptrap** command on the Bull System Manager server:
 - **Linux:** this command is installed along with snmp tools (refer to the *Bull System Manager Installation Guide*, 86 A2 54FA, for the package name).
 - **Windows:** this command is packaged with the Bull System Manager Server delivery.



Important:

Each service has an **enable SNMP trap** option indicating whether SNMP Trap notification may be used or not. The trap will only be sent if at least one manager has the **enable SNMP trap** option set to **Yes**. The trap is sent by the Bull System Manager server on behalf of the managed host.

By default, all services allow SNMP Trap notification. To disable this feature on selected services, you must set the **enable SNMP trap** option to **No**.

Note SNMP Trap PDU format is **SNMPv1**. The **mib** (BSM-TRAP-MIB) text file is delivered under **<BSM installation directory>/engine/etc/snmp/mibs**.

9.3.1 SNMP Manager

SNMP Manager defines a management platform that will receive the SNMP traps sent by the Bull System Manager server.

Note You are advised NOT to define the Bull System Manager host as the SNMP manager. This configuration can lead to an unexpected situation with a loop in trap emission.

To configure an SNMP Manager, click the **Managers** link in the **SNMP** part of the **Monitoring** tab.

The way to create, edit or delete a Mail server is described in *Create / Edit / Delete Resources*, on page 19.

The following figure shows the form displayed to edit an SNMP Manager.

Properties	
hostname	maria (network name)
description	SNMP manager (trap receiver)
SNMP trap receiver port	162
community	public
Notification attribute (to this manager & for all hosts)	
enable SNMP trap	<input type="radio"/> Yes <input checked="" type="radio"/> No

Figure 9-6. SNMP Manager properties

SNMP Manager Properties	Description
name	Host name of the management platform that will receive the traps.
description	Short description of the SNMP Manager.
snmptrapd port	Port used to receive SNMP traps. Default value: 162.
community	SNMP community name. Default value: public.
enable SNMP trap	Enable SNMP Trap notification for this SNMP Manager. Default value: No. This value must be changed to Yes to allow SNMP Trap notification.

Table 9-4. SNMP manager properties

Notes

- You can define as many SNMP managers as you want. They will be all notified.
- If the message `WARNING: snmptrap command not found` is displayed during **Save and Reload**, you must install the appropriate package to provide the **snmptrap** command (refer to the *Bull System Manager Installation Guide*, 86 A2 54FA). SNMP Manager configuration is not taken into account.

Chapter 10. Configuring NSCA

This chapter explains how to configure NSCA. NSCA functionalities (send_nsca and NSCA daemon) are brought by NSCA server extension package.



Send via NSCA is used to configure sending of checks results to a remote monitoring server (a BSM server or a central Nagios) via NSCA protocol. The NSCA daemon must be running on the remote server. The monitoring services must be defined as passive (attribute 'monitoring on event' set) on the remote server configuration .

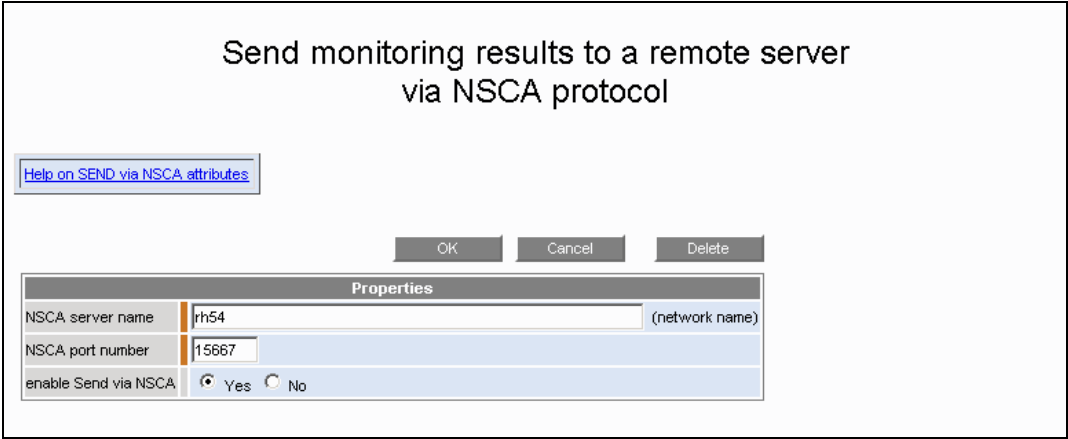


Figure 10-1 Send via NSCA edition

SEND NSCA Properties	Description
NSCA server name	Remote server netname which will receive monitoring results. The NSCA daemon must be running on this remote host
NSCA port number	NSCA daemon port number
Enable send via NSCA	Enable send nsca mechanism. Default is no

Table 10-1 Send via NSCA properties

Reception via NSCA is used to configure the NSCA daemon listening for host and services checks results from remote hosts. The monitoring services must be defined as passive services in the BSM configuration

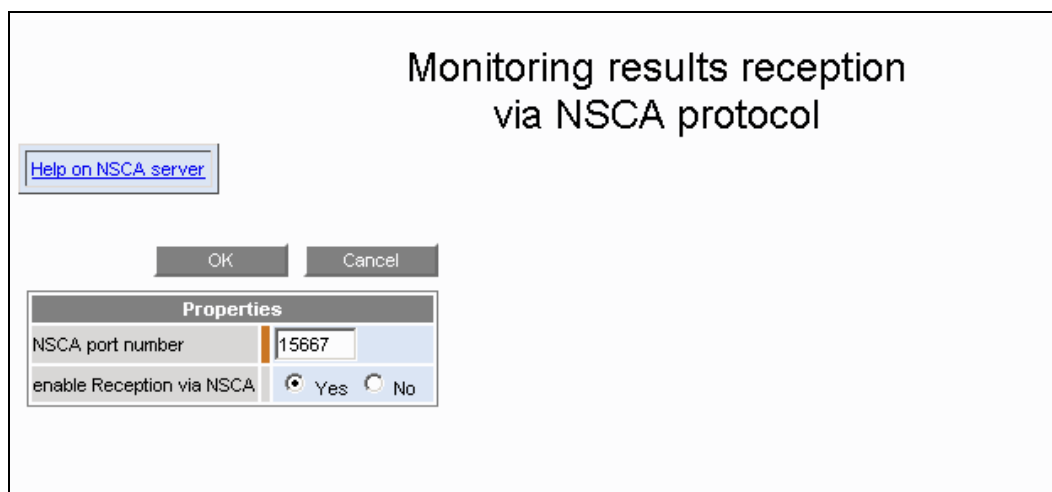


Figure 10-2 Reception via NSCA edition

NSCA Reception Properties	Description
NSCA port number	NSCA daemon port number
Enable reception via NSCA	Enable reception nsca mechanism. Default is no. If it is set to yes, the NSCA daemon will be launched.

Table 10-2 Reception via NSCA properties

Chapter 11. Customizing the Bull System Manager Console

This chapter explains how to customize the Bull System Manager Console. The following customization tasks are described:

- Choosing the BSM applications that can be launched from the **Bull Tools** Bar.
- Specifying the **user's applications** that can be launched from the **Other** Bar. These applications may be any external web URL or any local command to the station on which Bull System Manager Console is running.
- Choosing the **default view** that will be loaded in the Console Management Tree.
- Specifying the **maps** that will be displayed in the Bull System Manager Console.
- Specifying very important monitoring services that will be displayed with their status in the Bull System Manager Console **Focus** Pane.

The following figure shows an example of default view and applications bar customization.

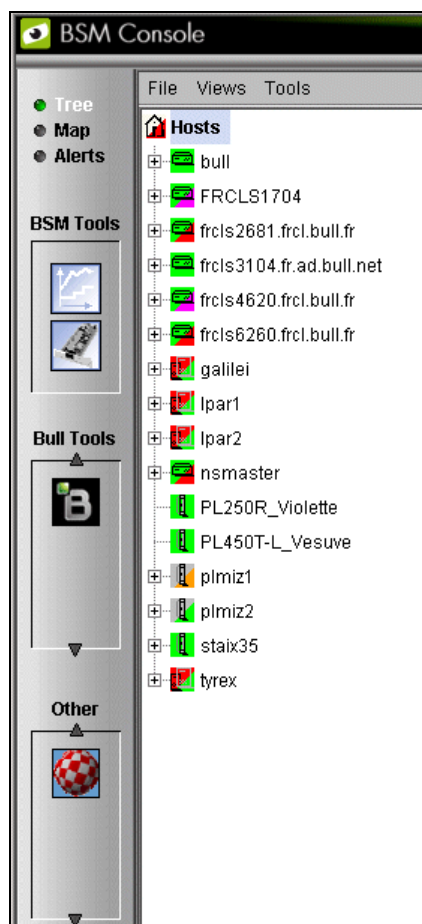


Figure 11-1. Customized default view and applications bar

To access Console customization functions, click **Console** under the domain tab.

Then click the corresponding link to activate one of the following functions: **Applications**, **Default view**, **Maps** and **Focus services**.

11.1 Specifying Applications

11.1.1 Bull System Manager Applications

Bull System Manager provides six Bull applications that can be displayed into the **Bull Tools** Bar:

- **Bull Support** (displayed by default)
- **ScVenusBPRSE** (Bull Performance Report Server Edition)
- **BPREE** (Bull Performance Report Enterprise Edition)
- **Application Roll-over Facility (ARF)**

To display these Bull applications, proceed as follows:

1. Click the **Applications** link under the **Console** tab. The list of the available applications is displayed:

Bull System Manager Applications






	name	description	image	URL	display
Edit	Bull1	Bull Support		http://support.bull.com/	yes
Edit	BPRSE	BPRSE		http://bpr_server/bprse	no
Edit	BPREE	BPREE		http://bpr_server/bpee	no
Edit	ARF	Application Roll-over Facility		http://arf_server/arfsw/	no
Edit	scVENUS	scVENUS		https://scvenus_server:37443/venus.html	no

Figure 11-2. Bull System Manager Applications

2. Click **Edit** for the Bull System Manager Application you want to display. The following **Properties** form appears:

OKCancel

Properties


name	BPRSE
description	BPRSE
image	
URL	<input type="text" value="http://bpr_server/bprse"/>
Display	<input checked="" type="radio"/> yes <input type="radio"/> no

Figure 11-3. Bull System Manager Application edition


3. Specify the URL if needed.
4. Check **Display : yes**.
5. Click **OK**.

11.1.2 User's Applications

Other applications can be defined with either access to a web URL or the activation of a command on the station where Bull System Manager Console is running.

To configure a new application, proceed as follows:

1. Click the **Applications** link under the **Console** tab.
2. From the **Applications** page, click **New** to edit a new application.
 - Specify a name and select an image from those proposed (this image will be used as the application icon in the Applications bar).
 - For a web URL application: select **external URL** as application type and specify the full external URL (Figure 11-4).

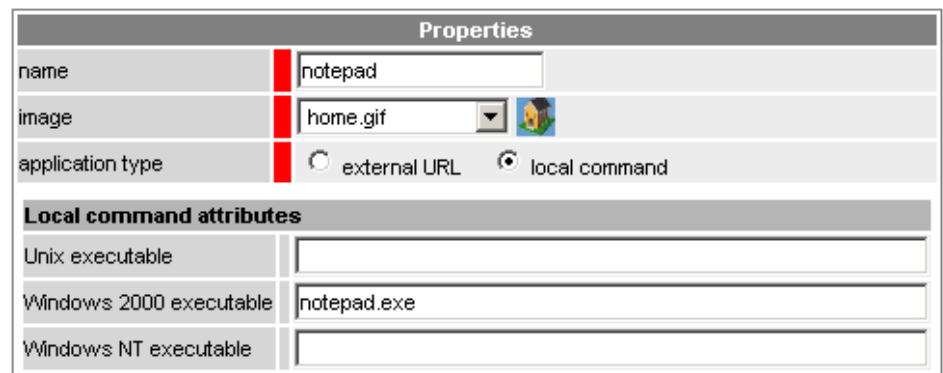


The screenshot shows a 'Properties' dialog box for configuring an application. It has four main sections: 'name' with the value 'meteo', 'image' with a dropdown set to 'fly.gif' and a butterfly icon, 'application type' with radio buttons for 'external URL' (selected) and 'local command', and 'URL' with the text 'http://www.meteo.fr/'.

Properties	
name	meteo
image	fly.gif 
application type	<input checked="" type="radio"/> external URL <input type="radio"/> local command
URL	http://www.meteo.fr/

Figure 11-4. An application as a web URL

- For a local command application: select **local command** as application type and specify the command or executable that will be launched for each OS (Figure 11-5).



The screenshot shows a 'Properties' dialog box for configuring a local command application. It has four main sections: 'name' with the value 'notepad', 'image' with a dropdown set to 'home.gif' and a person icon, 'application type' with radio buttons for 'external URL' and 'local command' (selected), and a 'Local command attributes' section with three rows: 'Unix executable' (empty), 'Windows 2000 executable' with the value 'notepad.exe', and 'Windows NT executable' (empty).


Properties	
name	notepad
image	home.gif 
application type	<input type="radio"/> external URL <input checked="" type="radio"/> local command
Local command attributes	
Unix executable	
Windows 2000 executable	notepad.exe
Windows NT executable	

Figure 11-5. An application as a local command

3. Click **OK**. The list of all customized applications is displayed.



	name	image	application type	URL
Edit	notepad		local command	N/A
Edit	meteo		external URL	www.meteo.fr

Figure 11-6. List of all applications

4. Do not forget to run **Save & Reload**.

11.2 Choosing the Default View

When Bull System Manager Console is started, the default view is displayed in the Management Tree part. You can then load another view from the **Load** menu. At installation time, the default view is the **Hosts** view. To change this default view, proceed as follows:

1. Click the **Default view** link under the Console tab. The following display appears:

default View	name
<input checked="" type="radio"/>	Hosts
<input type="radio"/>	HostGroups
<input type="radio"/>	Hardware Manager
<input type="radio"/>	Storage Manager
<input type="radio"/>	Virtual Manager

Figure 11-7. Choosing the default view

2. Select the required view and click **OK**.
3. Do not forget to **Save & Reload** in order to register your choice.

11.3 Specifying Maps

Each hostgroup, platform and host can have a map representation. A hostgroup (or platform) map is used to display their objects (hosts or hostgroups), animated with their status, at specified positions on the map. A host map is usually used to display an image of this host. In a map, each object can be represented by an icon or a rectangle (with or without a label).

To create or modify a map, click on the **Maps** link in the **Console** tab. The following page is displayed:

Bull System Manager Maps

Hostgroups

	name	description	default map	map
Edit	BSM	Bull System Manager elements	<input checked="" type="radio"/>	yes
Edit	Linux_hosts	hosts group	<input type="radio"/>	yes
Edit	Windows_hosts	hosts group	<input type="radio"/>	yes

Hosts

	name	description	map
Edit	charly4L	linux server	yes
Edit	coda	System Management Server	no
Edit	frcls2681	linux server	no
Edit	frcls5208	windows host	no
Edit	frcls6260	linux server	no
Edit	frcls8004	windows server	no

This page displays all the objects which can have a map. It allows you to edit a specific map and to specify which map is the default map.

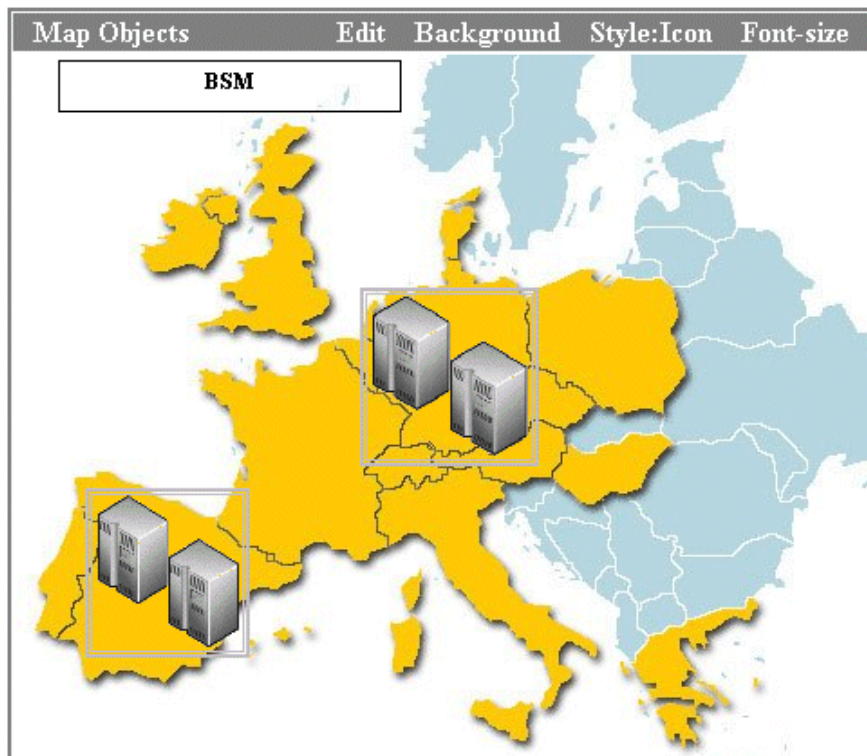
To edit a map, just click the **Edit** link of the chosen object (for example the hostgroup BSM). The following map editor is displayed:

Selected Map : BSM

OK

Delete

Cancel



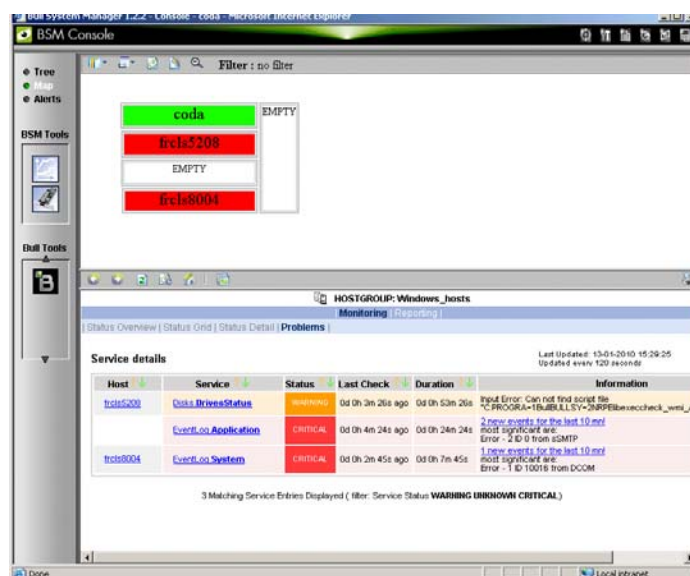
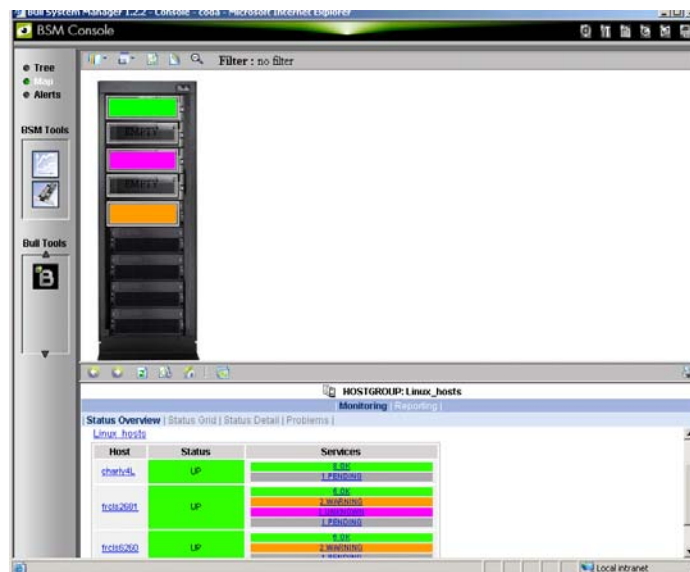
From this editor you can display each object belonging to the chosen hostgroup, you can specify a background image (geographical image, machine image ...), you can move or resize each object with the mouse.

Commands

Description


Map Objects	Displays all the objects of the chosen hostgroup, a map title object and an empty object. Allows you to choose the object you want to display.
Edit	Allows you to remove a selected object from the map.
Background	Allows you to choose the background image.
Style	Allows you to choose the representation style of an object. Three styles are available: Icon, Rectangle, No label (rectangle without label).
FontSize	Allows you to change the font size of a label

Some examples of map displayed in the Bull System Manager Console:



11.4 Specifying the Focus Pane

It may be useful to survey the status of very important monitoring services. The **Bull System Manager Focus Windows**, displaying the status of defined focused services, allows you to do so.

To display the Bull System Manager Focus window, you have just to click on this icon  from the Bull System Manager Console.

The following figure shows an example of a Bull System Manager Focus window.

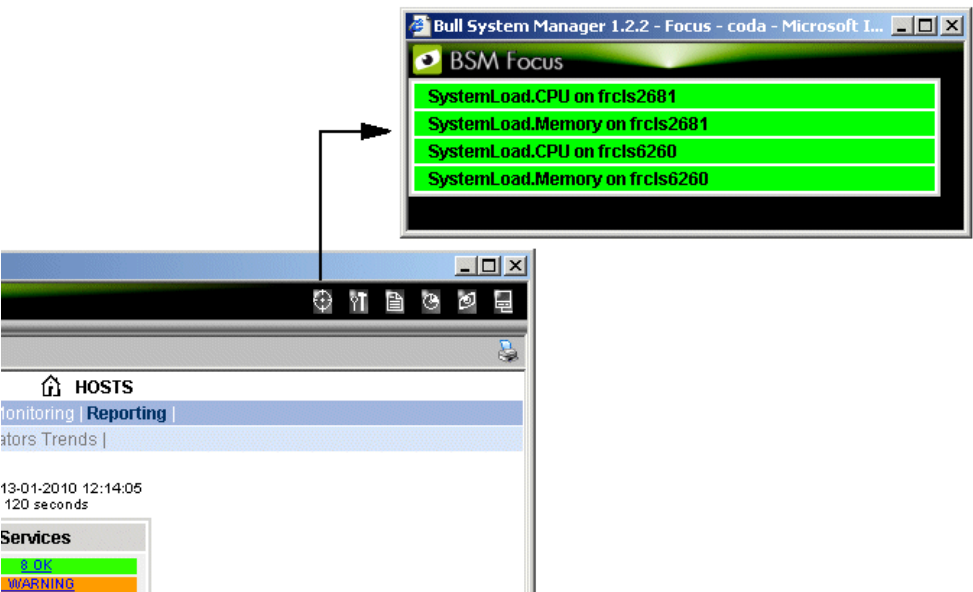


Figure 11-8. BSM Focus window

The following figure shows the form displayed to edit a focused service.

Properties	
name	<input type="text" value="frcls6260_cpu"/>
description	<input type="text"/>
host	<input type="text" value="frcls6260"/>
service	<input type="text" value="SystemLoad.CPU"/>

Figure 11-9. Focused service properties

Focused Service Properties	Description
name	Focused service name.
description	Short description of the focused service
host	Host associated with the focused service.
service	Monitoring service (already configured) associated with the focused service.

Table 11-1. Focused service properties

Click **OK** to display the list of all focused services.

	name	description	host	service
Edit	frcls2681_cpu	N/A	frcls2681	SystemLoad.CPU
Edit	frcls2681_memory	N/A	frcls2681	SystemLoad.Memory
Edit	frcls6260_cpu	N/A	frcls6260	SystemLoad.CPU
Edit	frcls6260_memory	N/A	frcls6260	SystemLoad.Memory

Figure 11-10. List of all focused services

Chapter 12. Configuring Local Settings

This chapter explains how to configure access to the Bull System Manager applications or to configure functional features of Bull System Manager.

12.1 Configuring BSM Server

To modify BSM Server characteristics, click the **Properties** link under the **BSM Server** item. The following form is displayed:

Properties	
BSM server netname	<input type="text" value="frcls1704"/>
HTTP port	<input type="text" value="10080"/>
HTTPS port	<input type="text" value="10443"/>

Figure 12-1. BSM Server properties

Properties	Description
BSM Server netName	Resolved network name used to reach the Bull System Manager server. This value is used by the BSM Agent to send its Inventory information, and also in the notifications sent by mail which contain the BSM console URL to access more information.
HTTP port	Port used to reach the Bull System Manager server with non secured HTTP protocol.
HTTPS port	Port used to reach the Bull System Manager server with secured HTTP protocol.

Notes

- When the ports number (HTTP, HTTPS) are modified, the Apache service must be restarted to take the new values into account.
- To use secured HTTP protocol (if your Apache server is not already secured with SSL), you have to edit the file **<Bull System Manager_install_dir>/core/etc/sysmgt-httpd.conf** and uncomment this line:

```
# Include "<Bull System Manager_install_dir>/core/etc/sysmgt-ssl.conf"
```


The **sysmgt-ssl.conf** file uses a private key and a self-signed certificate, which are automatically installed for apache during the installation of Bull System Manager.

12.2 Configuring Users & Roles

Bull System Manager applications must be authenticated, with an Apache user defined on the server part. The authenticated user is used to apply a user profile or role defined by the Role Base Management system.

-
- Notes**
- This **User** configuration is used not only by the BSM local console, but also by the BSM global console.
 - Moreover, in the case of a distributed BSM solution, the different BSM servers **MUST** be configured uniformly with the same User and role.
-

Four roles, with distinct rights, are defined in Bull System Manager Server, as described below:

Role	BSM Configuration	BSM Control	BSM Console		
			global monitoring control menu (at the tree root)	Host Monitoring control menu	Host Remote Operation menu
Administrator	Write	Yes	Yes	Yes	Yes
BSM-Administrator	Write	Yes	Yes	Yes	No
System-Administrator	ReadOnly	No	No	Yes	Yes
Operator	ReadOnly	No	No	Yes	No

Table 12-1. Users, Roles and Functions

At installation time, three users are created and registered in the Role Based Management::

User	Password	Role
bsmadm	bsmadm	Administrator
nagios	nagios	Administrator
guest	guest	Operator

The administrator then can modify or register the other users of the Bull System Manager Applications.



Important:

At least one user **MUST** always be defined with the Administrator role, to be able to configure Bull System Manager.

Notes

- The **Users & Roles** function is applicable to all Bull System Manager server Windows and Linux platforms, except on Linux platforms with a PHP lower than 4.2.2 (Red Hat 7.3).
In this case, use Administration commands to add/update Bull System Manager users.
 - From NovaScale Master Release 4.0, roles are exclusive to users.
-

To configure a user, proceed as follows:

1. Click the **Users & Roles** link of the **LocalSetting** tab. The list of the configured users appears:

	User name	User role
Edit	bsmadm	Administrator
Edit	guest	Operator
Edit	nagios	Administrator

Figure 12-2. Users allowed accessing the Bull System Manager Applications

2. From the **Users & Roles** page, click **New** to edit a new user. This menu appears:

Properties		
user name	<input type="text"/>	
user_password	<input type="password"/>	confirm <input type="password"/>
user role	<div>Administrator <input type="button" value="v"/></div> <div>Full Administrator: can manage BSM solution and supervised systems</div>	

Figure 12-3. Users & Roles properties

- Enter the user name.
 - Enter the password,
 - Select the exclusive role associated with this user.
 - Click **OK** to validate.
3. Repeat step 2 for each user to be configured. New configured users are now displayed in the **Users & Roles** page.

Note Check that the user has not opened a Bull System Manager session before you **Save & Reload** role modifications as the user's current session may become unstable.

12.3 Configuring Active Features

At installation, the Monitoring feature is always enabled. To disable it, proceed as follows: To disable the Monitoring feature, click the **Active features** link in the **Functionalities** part of the **LocalSetting** tab. The features, grouped in two parts (Supervision and Remote Operation) are listed, as displayed in the following page:

Settings	
Enable Supervision	
All Supervision Features	<input checked="" type="radio"/> Yes <input type="radio"/> No
- Monitoring Feature	<input checked="" type="radio"/> Yes <input type="radio"/> No
- Reporting Feature	<input checked="" type="radio"/> Yes <input type="radio"/> No
- Inventory Feature	<input checked="" type="radio"/> Yes <input type="radio"/> No

Figure 12-4. Default Global Settings

To disable Monitoring (and associated Reporting and Inventory features), click the "No" check box corresponding to the **All Supervision Features** item.

Settings	
Enable Supervision	
All Supervision Features	<input type="radio"/> Yes <input checked="" type="radio"/> No
- Monitoring Feature	<input type="radio"/> Yes <input checked="" type="radio"/> No
- Reporting Feature	<input type="radio"/> Yes <input checked="" type="radio"/> No
- Inventory Feature	<input type="radio"/> Yes <input checked="" type="radio"/> No

Figure 12-5. Disabling Monitoring

Notes

- As the **Reporting** and **Information** features are strongly linked to the **Monitoring** feature, when you enable or disable the Monitoring feature you also activate or deactivate the Reporting and Information features.
 - The **Remote Operation** feature cannot be disabled in this version. However, if you do not want to use this feature, connect to the console with the Operator Role.
 - When you disable / enable the Monitoring feature, you also affect the availability of applications in the Bull System Manager Console. **Any open Bull System Manager Console must be restarted subsequent to modifications in the GlobalSetting configuration.**
-

12.4 Configuring Periodic Tasks

BSM Server offers to automatically launch tasks to perform various operations.

To activate or configure a task (period), click the **Periodic Tasks** link under the **Functionalities** item.

A page is displayed with all predefined tasks. In this version, only one task is available as displayed on the following page:

Periodic Tasks				
Help on Tasks				
	Name	Description	Period	Enabled
Edit	exportMrtg	periodic task to export MRTG metrics	00 22 * * *	no
Edit	updateInventory	periodic task to update inventory	0 0 * * *	no

Figure 12-6. Periodic Tasks

To get detailed information about exportMrtg task, see *Export daily information of a perf_indic*, on page 162.

To get detailed information about updateInventory, see *Configuring Inventory*, on page 79

Chapter 13. Configuring Global Settings

This chapter explains how to configure distributed Bull System Manager solutions, constituted by several servers, each of them managing a set of hosts and offering a global console allowing to view all elements.

Each server manages its local configuration and publishes it to a central database (CMDB) accessible by all server. By default, the database is hosted on the local server. In order to set a distributed solution, you have to define a BSM server which hosts the CMDB and to configure other servers to fill the central CMDB.

In this part, you can configure the port to access Global Console or redefine the server that hosted the central database.



Important:

Distributed solution requires that the NDOutils extension is installed on all BSM server nodes.

13.1 Configuring Global Console

To change the Global Console properties, click the **Properties** link under the **Global Console** item.

The following page allows you to change the HTTP port numbers used to access the global console:

Global console Properties

[Help on GlobalConsole](#)

OKCancel

Properties	
HTTP port	<input type="text" value="20080"/>
HTTPS port	<input type="text" value="20443"/>

Figure 13-1. Global Console properties

To apply your changes, do not forget to click the **OK** button.

- Notes

- When the ports number (HTTP, HTTPS) are modified, the Apache service must be restarted to take into account the new values.
 - The port number used for the Global Console must be different from those set for the Local Console (see *Configuring BSM Server*, on page 195).

13.2 Configuring NDOutils Db Server

To change the MySQL server properties, click the **MySQL DB server** link under the **NDOutils** item.

The following page allows you to change the hostname and the port used to access the MySQL database:

NDOutils MySQL server information

[Help on NDOutils](#)

OKCancel

Properties	
MySQL server name	<input type="text" value="nsmaster"/> (network name)
MySQL port number	<input type="text" value="3306"/>

Figure 13-2. NDOutils MySQL server configuration

Properties	Description
MySQL Server netName	<div>Resolved network name used to reach the MySQL server</div> <div>This value is used by the NDOutils part to determine which server hosted the central database.</div> <div>Must correspond to a BSM server with the NDOutils extension installed.</div> <div>This value is initialized with the hostname of the BSM server.</div>
MySQL port number	<div>Port used to reach to reach the MySQL server</div> <div>The value is initialized to 13306 for a Windows server and to 3306 for a Linux server.</div>

To apply your changes, don't forget to click the **OK** button.



Important:

MySQL port number differs between Linux and Windows. If distributed solution contains heterogeneous server, don't forget to modify the port in regard of the BSM server OS.

13.3 Example

The following example shows how to set a distributed solution with three BSM Servers: BSM1, BSM2 and BSM3. The central database is hosted by BSM1.

13.3.1 Configuration of the Global Console

By default, the http and https ports for the Global Console are set to 20080 and 20443, respectively.

If you want to change these values, it must be done on all BSM server nodes involved in the distributed solution.

13.3.2 Configuration of the NDOutils Db Server

13.3.2.1 Central node, BSM1

By default, the NDOutils Db server is defined with the BSM server as server and default MySQL port. So, nothing have to be done on the central node, except if you have changed the MySQL port.

13.3.2.2 Secondary nodes, BSM2 and BSM3

The NDOutils MySQL server must be changed on secondary nodes, to refer to the central node, BSM3.

For each secondary node:

1. Launch the Configuration GUI.
2. Click the GlobalSetting tab
3. Click the NDOutils DB Server

The following page is displayed:

Properties	
MySQL server name	<input type="text" value="BSM2"/> (network name)
MySQL port number	<input type="text" value="3306"/>

Figure 13-3. NDOutils DB Server BSM2 configuration

4. Change BSM2 by BSM1
5. Click the OK button to apply your change
6. Perform Save&Reload to populate the BSM1 CMDB with the configured objects of the secondary node.

Appendix A. Predefined Categories and Services

The following table lists categories and services, with their default values. It also indicates if the **Clone** function is available. Services in **bold** characters are the default services effective just after Bull System Manager installation, for all hosts.

Category	OS	Category hostList	Hardware model	Service	Service hostList	Clone function
SystemLoad	Windows	*	Any	CPU	*	
				Memory	*	
SystemLoad	Linux	*	Any	CPU	*	
				Memory	*	
				Users	*	
				Processes	*	
				Swap	None	
				Zombies	None	
SystemLoad	AIX			CPU	*	
				PagingSpace	*	
				Swap	*	
				LoadAverage	None	
				Memory	None	
				Processes	None	
				Users	None	
				Zombies	None	
LogicalDisks	Windows	*	Any	All	*	
				C	None	x
EventLog	Windows	*	Any	System	*	
				Application	*	
				Security	*	
Windows Services	Windows	*	Any	EventLog	*	x
				Networking	None	x
				Com	None	x
				Peripherals	None	x
				Management	None	x
FileSystems	Linux	*	Any	All	*	
				/usr	None	x
FileSystems	AIX	*	Any	All	*	
				/usr	None	
Syslog	Linux	*	Any	AuthentFailures	*	x
				RootAccess	None	x
				Alerts	*	
Syslog	AIX	*	Any	Errors	*	
				Alerts	*	
Linux Services	Linux	*	Any	syslogd	*	x
AIX Services	AIX	*	Any	syslogd	*	
Internet	Any (W/L)	None	Any	http	*	
				FTP	None	
				http_BSM	None	x
				TCP_7	None	x
				UDP_7	None	x
Hardware	Any		I/O Switch Module	Health	host	
Hardware	Any (W/L)	*	NS 4000, 5000, 6000 NS Blade, EL Blade	Health	host (1)	

Category	OS	Category hostList	Hardware model	Service	Service hostList	Clone function
			NSR400,T800,3000,4000 Express 5800, ns bullion	Alerts	host (1)	x
Hardware			Escala PL	CecStatus	host (1)	x
			Escala PL	Events	host (1)	x
Power	Any		NS 4000, NS 3000, Expres 5008, NS T800, NS R400, ns bullion NS 9019, ns bullion	Status	host (1)	
				Consumption	host(1)	
PAM	Any (W/L)	*	Any	GlobalStatus	* (1)	
				Alerts	* (1)	
CMM	Any (W/L)	*	Any	ChassisStatus	* (1)	
				Alerts	* (1)	
reporting	Any (W/L)	None	Any	Perf_indic	None	x

Table A-1. Predefined categories and services

*W means Windows, L means Linux and W/L means both.

(1) The host list is automatically generated during the definition of the host (, depending on semantic checks and links between hosts and managers (see *Configuring Hosts*, on page 25).

A.1 SystemLoad Category

CPU (Windows)	Monitors total CPU load percent over two periods of time (1 and 10 min). Final status is the worst status for the two periods. If status is not OK, the service returns the most consuming process (if any) at request time. By default, warning thresholds are 80 (over 1 min) and 60 (over 10 min) and critical thresholds are 90 (over 1 min) and 80 (over 10 min).
Memory (Windows)	Monitors memory usage percent (i.e. the sum of physical and virtual memory, also known as commit charge), in terms of percent or size. By default, the warning threshold is 70 and the critical threshold is 90 .
CPU (Linux)	Monitors total CPU load percent over three periods of time (1 min, 5 min and 15 min). Final status is the worst status for the three periods. By default, warning thresholds are 80 (over 1 min), 70 (over 5 min) and 60 (over 15 min) and critical thresholds are 90 (over 1 min), 80 (over 5 min) and 70 (over 15 min).
Memory (Linux)	Monitors total memory usage percent (i.e. the sum of physical memory and virtual memory). By default, the warning threshold is 70 and the critical threshold is 90 .
Swap (Linux)	Monitors system swap percent. By default, the warning threshold is 50 and the critical threshold is 80 .
Users (Linux)	Monitors the number of users currently logged in. By default, the warning threshold is 15 and the critical threshold is 20 .
Processes (Linux)	Monitors the number of processes running on the system. By default, the warning threshold is 150 and the critical threshold is 200 .
Zombies (Linux)	Monitors the number of zombie processes (state = Z) running on the system. By default, the warning threshold is 5 and the critical threshold is 10 .

A.2 LogicalDisks Category

All	Monitors the percent of used space for all the local disks. By default, the warning threshold is 80 and the critical threshold is 90 .
C	Monitors the percent of used space for the local disk C: By default, the warning threshold is 80 and the critical threshold is 90 .

A.3 EventLog Category

Application	Monitors the number of Error, Warning and Information events generated in the Application event log over the last 30 minutes. By default, the warning threshold is 10 Information events or at least 1 Warning event and the critical threshold is at least 1 Error event .
System	Monitors the number of Error, Warning and Information events generated in the System event log over the last 30 minutes. By default, the warning threshold is 10 Information events or at least 1 Warning event and the critical threshold is at least 1 Error event .
Security	Monitors the number of Audit Success, Audit Failures, Error and Warning events generated in the Security event log over the last 30 minutes. By default, the warning threshold is 10 Audit Success events or at least 1 Warning event and the critical threshold is at least 1 Audit Failure or 1 Error event .

A.4 WindowsServices Category

EventLog	<p>Monitors the Windows services ensuring event-logging functions. Status is set to warning at least 1 service is paused and the others are running. Status is set to critical if at least 1 service does not exist or 1 service is not running.</p> <p>EventLog (Event Log): logs event messages issued by programs and Windows. Event Log reports contain information that can be useful in diagnosing problems. Reports are viewed in the Event Viewer.</p>
Networking	<p>Monitors the Windows services ensuring networking functions. Status is set to warning if at least 1 service is paused and the others are running. Status is set to critical if at least 1 service does not exist or 1 service is not running.</p> <p>RpcSs (Remote Procedure Call (RPC)): provides the endpoint mapper and other miscellaneous RPC services.</p> <p>TrkWks (Distributed Link Tracking Client): sends notifications of file moving between NTFS volumes in a network domain.</p> <p>Dhcp (DHCP Client): manages network configuration by registering and updating IP addresses and DNS names.</p> <p>Dnscache (DNS Client): resolves and caches Domain Name System (DNS) names.</p> <p>Netman (Network Connections): manages resources in the Network and Dial-Up Connections folder, in which you can view both local area network and remote connections.</p>
Com	<p>Monitors the Windows services ensuring Com+ notification functions. Status is set to warning if at least 1 service is paused and the others are running. Status is set to critical if at least 1 service does not exist or 1 service is not running.</p> <p>SENS (System Event Notification): tracks system events such as Windows login, network, and power events. Notifies COM+ Event System subscribers of these events.</p> <p>EventSystem (COM+ Event System): provides automatic distribution of events to subscribing COM components.</p>
Peripherals	<p>Monitors the Windows services ensuring peripherals management functions. Status is set to warning if at least 1 service is paused and the others are running. Status is set to critical if at least 1 service does not exist or 1 service is not running.</p> <p>NtmsSvc (Removable Storage): manages removable media, drives, and libraries.</p> <p>PlugPlay (Plug and Play): manages device installation and configuration and notifies programs of device changes.</p>
Management	<p>Monitors the Windows services ensuring computer management functions. Status is set to warning if at least 1 service is paused and the others are running. Status is set to critical if at least 1 service does not exist or 1 service is not running.</p> <p>Wmi (Windows Management Instrumentation Driver Extensions): provides systems management information to and from drivers.</p> <p>WinMgmt (Windows Management Instrumentation): provides system management information.</p> <p>dmserver (Logical Disk Manager): Logical Disk Manager Watchdog Service.</p>

A.5 FileSystems Category

All	Monitors the percent of used space for all the mounted FileSystems except CD-ROM and floppy. By default, the warning threshold is 80 and the critical threshold is 90.
/usr	Monitors the percent of free space for the /usr FileSystem. By default, the warning threshold is 80 and the critical threshold is 90.

A.6 Syslog Category

AuthentFailures	<p>Monitors the /var/log/messages file for the detection of authentication failure messages. It searches for the lines containing authentication failure or FAILED LOGIN or Permission denied, but not containing login.*authentication failure (such a line traps the same error as a FAILED LOGIN line, already detected).</p> <p>Status is set to warning if there is at least 1 new matching line since the last check. Status is only set to critical state if a processing error occurs.</p> <p>Note: warning status can be very fugitive in the Console. When a new matching line appears in the log file, the service sets status to warning only during the interval between the check that detects the error and the next one (if no new error appears). You are therefore advised to activate notification and to consult the service history regularly to see if any errors have been detected.</p> <p>The notifyRecovery field is set to no for this service, as it is not applicable to this type of service.</p>
RootAccess	<p>Monitors the /var/log/messages file for the detection of a session opened with the root user. It searches for lines containing session opened for user root.</p> <p>Status is set to warning if there is at least 1 new matching line since the last check. Status is only set to critical state if a processing error occurs.</p> <p>Note: warning status can be very fugitive in the Console. When a new matching line appears in the log file, the service sets status to warning only during the interval between the check that detects the error and the next one (if no new error appears). You are therefore advised to activate notification and to consult the service history regularly to see if any errors have been detected.</p> <p>The notifyRecovery field is set to no for this service, as it is not applicable to this type of service.</p>
Alerts (Linux, AIX)	<p>Linux and AIX hosts:</p> <p>When an alert is sent from the Bull System Manager agent, it is processed by the Bull System Manager server.</p> <p>Note: The BSM-SYSLOG-MSG.mib mib must be integrated in the Bull System Manager application (see <i>Integrating MIBs</i>, on page 121).</p>

A.7 LinuxServices Category

syslogd	Monitors that there is one and only one syslogd process running on the system. syslogd is a system utility daemon that provides support for system logging. Status is set to warning if the number of syslogd processes is not 1 . Status is only set to critical state if a processing error occurs.
----------------	--

A.8 Internet Category

FTP	Checks the accessibility of FTP on its standard port 21. Status is set to warning if the connection is successful , but incorrect response messages are issued from the host and to critical if response time exceeds 10 seconds or if the connection with the server is impossible .
HTTP	Monitors the HTTP access of the hosts on port 80 on the '/' URL (i.e. <code>http://host:80/</code>). The timeout value is 10 seconds . Status is set to warning for HTTP errors: 400, 401, 402, 403 or 404 such as unauthorized access and to critical if response time exceeds 10 seconds or for HTTP errors 500, 501, 502 or 503 , or if the connection with the server is impossible .
TCP 7	Monitors the TCP 7 port (echo) access of the hosts. Status is set to critical if the connection with the server is impossible .
UDP	Monitors the UDP 7 port (echo) access of the hosts. Status is set to critical if the connection with the server is impossible .

A.9 Reporting Category

perf_indic	Checks the status of a component based on the value collected by MRTG.
------------	--

A.10 Hardware Category

Health	For NovaScale 4000 series hosts managed by ISM or for NovaScale 5000 & 6000 series hosts managed by PAM or for NovaScale Blade series hosts or Enterprise Line Blade series hosts or I/O Switch Module host managed by CMM. This service checks the host hardware status reported by the associated ISM, PAM or CMM.
Alerts	<p>NovaScale 4000 series hosts: When an alert is sent from the NovaScale host, it is processed by the Bull System Manager server.</p> <p>Note: The basebrd5.mib mib must be integrated in the Bull System Manager application (see <i>Integrating MIBs</i>, on page 149).</p> <p>NovaScale 4000, 3000, T800, R400 series and Express 5800 hosts: When an alert is sent from the host management card, it is processed by the Bull System Manager server.</p> <p>Note: The bmclanpet.MIB mib must be integrated in the Bull System Manager application (see <i>Integrating MIBs</i>, on page 149).</p> <p>Do not forget to configure the Hardware manager or agent to send SNMP traps to the Bull System Manager server by adding the Bull System Manager server host address to the SNMP managers list. This configuration is explained in the corresponding Hardware Manager documentation.</p>
CECStatus	For Escala PL series servers managed by an HMC. This service checks the CEC status, as reported by the HMC.
Events	For Escala PL series servers managed by an HMC. This service checks the hardware status, based on the presence of hardware events, as reported by the HMC.

Note These services are automatically applied to the specified targets, when they are configured.

PowerStatus	For IPMI compliant server hosts (NS R400, NS T800, NS 3005 ...). This service may check the power status of the server (ON or OFF).
Sensor	For IPMI compliant server hosts (NS R400, NS T800, NS 3005 ...). This service can check a sensor (Volt, Temperature, FanSpeed ...) and get the current numeric value.
SensorAvg	For IPMI compliant server hosts (NS R400, NS T800, NS 3005 ...). This service may check a set of sensors (Volt, Temperature, FanSpeed ...) and get current numeric values and finally return a average value.

A.11 Power Category

Status	For IPMI compliant server hosts (NS R400, NS T800, NS 3005 ...). This service may check the power status of the server (ON or OFF).
Consumption	For IPMI compliant server hosts (NS R400, NS T800, NS 3005 ...). This service can check a sensor (Volt, Temperature, FanSpeed ...) and get the current numeric value.

A.12 PAM Category

GlobalStatus	<p>For hosts running PAM (these hosts are also named PAP). This service checks global hardware status for all NovaScale 5000 & 6000 series platforms managed by a PAM manager.</p> <p>For information about PAM, refer to the <i>Bull NovaScale 5000 & 6000 Series User's Guide</i>.</p>
Alerts	<p>When an alert is sent from PAM, it is processed by the Bull System Manager server.</p> <p>Note: The PAMeventtrap.MIB mib must be integrated in the Bull System Manager application (see <i>Integrating MIBs</i>, on page 149).</p> <p>Do not forget to configure the Hardware manager to send SNMP traps to the Bull System Manager server by adding the Bull System Manager server host address to the SNMP managers list. This configuration is explained in the <i>NovaScale 5000 or 6000 Series User's Guide</i>.</p>

Note These services are automatically applied to the specified targets, when they are configured.

A.13 CMM Category

ChassisStatus	For hosts running CMM (these hosts are management cards in the chassis). This service checks global hardware status for all common resources shared by NovaScale Blade series hosts managed by a CMM manager.
Alerts	<p>For NovaScale Blade series hosts managed by CMM. When an alert is sent from the NovaScale manager, it is processed by the Bull System Manager server and forwarded to the remote maintenance center (if specified).</p> <p>Note: The mmalert.mib mib must be integrated in the Bull System Manager application (see <i>Integrating MIBs</i>, on page 149).</p>

Note These services are automatically applied to the specified targets, when they are configured. Correct service processing requires that Bull System Manager server is declared as SNMP Manager in the CMM configuration. For details, please refer to the *NovaScale Blade Chassis Management Module Installation and User's Guide*.

Appendix B. Generated Categories and Services

The following table lists the generated services with corresponding host or manager edition page the in Topology part.

Category	Service	Model	Conditions	Reference
Power	Status	NS 4000	out-of-band attributes set	NS4000
Hardware	Alerts	NS 4000	out-of-band attributes set	NS4000
Hardware	Health	NS 4000	managed by ISM	Hardware Manager
Hardware	Health	NS blade	managed by CMM	NS Blade
Hardware	Health	EL Blade	managed by CMM	EL Blade
Hardware	Health	I/O Switch Module	managed by CMM	I/O Switch Module
Hardware	Health	NS 5005	managed by PAM	NS 5005
Power	tatus	Express 5800	out-of-band attributes set	Express 5800
Hardware	Alerts	Express 5800	out-of-band attributes set	Express 5800
Hardware	PowerStatus	NS 3005	out-of-band attributes set	NS 3005
Hardware	Alerts	NS 3005	out-of-band attributes set	NS 3005
Power	Status	NS 9010	out-of-band attributes set	NS 9010
Power	Consumption	N 9010	out-of-band attributes set	NS 9010
Hardware	Alerts	NS 9010	out-of-band attributes set	NS 9010
Power	Status	ns bullion	out-of-band attributes set	ns bullion
Power	Consumption	ns bullion	out-of-band attributes set	ns bullion
Hardware	Alerts	ns bullion	out-of-band attributes set	ns bullion
Power	Status	NS T800	out-of-band attributes set	NS T800
Hardware	Alerts	NS T800	out-of-band attributes set	NS T800
Power	tatus	NS R400	out-of-band attributes set	NS R400
Hardware	Alerts	NS R400	out-of-band attributes set	NS R400
Hardware	CECStatus	Escala PL	managed by HMC	PL Server
Hardware	Events	Escala PL	managed by HMC	PL Server
PAM	GlobalStatus	-	manager PAM	NS 5005
PAM	Alerts	-	manager PAM	NS 5005
CMM	ChassisStatus	-	manager CMM	NS Blade
CMM	Alerts	-	manager CMM	NS Blade

Table B-1. Generated categories and services

Appendix C. Check Commands for Customizable Services

This chapter describes the usage of the Nagios check commands by customizable services. See *Check Commands*, on page 98, for the list of the check commands used by predefined services.

Note The ! character must be used to separate the check command parameters in the service definition.

Launching Linux Check Commands

All Linux check commands for Nagios are launched by the **check_nrpe** command. For instance, the check command associated to the **SystemLoad.Users** service is:

```
check_nrpe!'/opt/BSMAgent/nrpe/libexec/check_users -w 15 -c
```

The check invokes always the **/opt/BSMAgent/nrpe/libexec/check_nrpe** executable with a unique parameter corresponding to the check command launched on the target system. In the following sections, the usage given for the check command corresponds to this parameter. The name of the command launched by **check_nrpe** must not be modified.

C.1 check_ns_eventlog (Windows)

Usage

```
check_ns_eventlog <period> strlog=<LogName> [filtersrc=<SrcList>] [excludesrc=<SrcList>]
[elnf=<nb>] [wWarn=<nb>] [eWarn=<nb>] [wErr=<nb>] [eErr=<nb>] [wAudS=<nb>]
[eAudS=<nb>] [wAudF=<nb>] [eAudF=<nb>]
```

<period>	Time (in minutes) back from now, used for event checking. Events older than this period are ignored.
strlog=<LogName>	Defines the event log (Application, Security, System, DNS Server, ...) from which events must be retrieved.
filtersrc=<SrcList>	Only events logged by Sources from this List must be retrieved from the Log defined with strlog=<LogName>.
excludesrc=<SrcList>	Events logged by Sources from this List are excluded from the events retrieved from the Log defined with strlog=<LogName>.
wInf=<nb>	Number of Information events that result in a WARNING message.
eInf=<nb>	Number of Information events that result in a CRITICAL message.
wWarn=<nb>	Number of Warning events that result in a WARNING message.
eWarn=<nb>	Number of Warning events that result in a CRITICAL message.
wErr=<nb>	Number of Error events that result in a WARNING message.
eErr=<nb>	Number of Error events that result in a CRITICAL message.
wAudS=<nb>	Number of Audit Success events that result in a WARNING message.
eAudS=<nb>	Number of Audit Success events that result in a CRITICAL message.
wAudF=<nb>	Number of Audit Failure events that result in a WARNING message.
eAudF=<nb>	Number of Audit Failure events that result in a CRITICAL message.

The <period> parameter and the <strlog> parameter are required.

<LogName> argument containing a blank space must be enclosed by double quotes.

The optional [filtersrc=<SrcList>] and [excludesrc=<SrcList>] parameters are exclusive

If several Sources must be defined in the <SrcList> argument, they must be separated with the “,” character.

If at least one Source defined in the <SrcList> argument contains a blank space, the complete <srcList> must be enclosed by double quotes.

Events that are out of date regarding the period parameter are discarded.
Checking conditions apply to this final set.

All condition combinations are allowed. Each condition is tested against the events set issued from the specified log files and the out-of-date condition.

Final status is the most severe status of each condition result.

Only threshold conditions specified as parameters are taken into account. Non-specified conditions are ignored.

Notes

- The <period> parameter must be the first parameter.
 - The Application, Security, and System event logs previously defined using the parameters “applog=1”, “seclog=1”, and “syslog=1”, are now defined using the parameter “strlog=<LogName>”.
-

Output

OK state	OK: no new messages for the last <period> min
WARNING or CRITICAL state	<nb_msg> new messages for the last <period> min! The message gives the total number of events that are responsible for degraded status. This message is also a link to an html file giving event details. The following information is provided: Event type Error, Warning, Information, Audit Success or Audit Failure Last Time Last time an event of the same type, source and id occurred Count Number of events with the same type, source and id Source Event source Id Event id Description Event message Note: Only the events that have exceeded any of the specified limits are listed here (and not all the new events, nor the entire log file).

Table C-1. check_ns_eventlog output

In the event of degraded status, a new file is created for each <period> of time, or when something changes in the output. Otherwise, the file is overwritten.

Examples

Following are two examples of parameters for the `check_ns_eventlog` command used in service definition, and their corresponding output.

- `60!strlog=Application!wErr=1!eErr=5`
OK: no new events for the last 60 min
Checks the number of error messages in the Application Event Log for the last 60 min. Status is set to **critical** if there are at least **five error messages**, and to **warning** if there is at least **one error message**.
- `60!strlog="DNS Server"!wErr=1!eErr=5`
OK: no new events for the last 60 min
Checks the number of error messages in the DNS Server Event Log for the last 60 min.
- `30!strlog=Application!filtersrc="Bull System Manager snmptrapd"!wInf=10!wWarn=1!eErr=1`
2 new events for the last 30 min!
A html file is generated
Checks in Application Event Log only events for the last 30 minutes logged by the "Bull System Manager snmptrad" software.
- `30!strlog=Application!excludesrc=Perflib,snmptrapd!wInf=10!wWarn=1!eErr=1`
50 new events for the last 30 min!
A html file is generated
Checks in Application Event Log all events logged for the last 30 minutes except the events logged by snmptrad and Perflib software.

C.2 check_ns_disk (Windows)

Usage

`check_ns_disk PERCENT | SIZE <path> <wThresh> <cThresh>`

PERCENT | SIZE unit for limits, percentage or size in Mbytes.
<path> full path to local disk to monitor.
<wThresh> value of used space resulting in a WARNING message.
<cThresh> value of used space resulting in a CRITICAL message.
All arguments are required.

Output

OK state	Disk <disk name> (total: <total size>Mb) (used: <used size>Mb, <used percent>%) (free: <free size>Mb)
WARNING or CRITICAL state	Problem on disk <disk name>: (total: <total size>Mb) (used: <used size>Mb, <used percent>%) (free: <free size>Mb)

Table C-2. `check_ns_disk` (Windows) output

Example

```
check_ns_disk!PERCENT!C:!80!90
```

```
Disk C: (total: 2996Mb) (used: 2062Mb, 68%) (free: 934Mb)
```

This command checks the used space for disk C: .

If the used space is more than or equal to 80%, status is set to **warning**.

If used space is more than or equal to 90%, status is set to **critical**.

C.3 check_ns_load (Windows)

Usage

```
check_ns_load <interval1> <wload1> <cload1> <interval2> <wload2> <cload2>
```

- <interval1> first time interval, in minutes, used to measure the cpu load average.
It must be a number between 0 and 15 minutes.
- <wload1> cpu load limit to result in a WARNING message during the first time interval.
It must be a number between 0 and 100.
- <cload1> cpu load limit to result in a CRITICAL message during the first time interval.
It must be a number between 0 and 100.
- <interval2> second time interval, in minutes, used to measure the cpu load average.
It must be a number between 0 and 15 minutes.
- <wload2> cpu load limit to result in a WARNING message during the second time interval.
It must be a number between 0 and 100.
- <cload2> cpu load limit to result in a CRITICAL message during the second time interval.
It must be a number between 0 and 100.

All arguments are required.

This command checks the average of CPU load during two time intervals. It is possible to set a warning and a critical limit for each time interval. Returned status is the most severe status. Every second, the agent collects the total CPU load and stores it in a table. It also stores the most CPU consuming process. When it is queried by the command, it computes the average load for the two requested periods, and returns the most consuming process, if any.

Note	The most consuming process at the time the request was issued does not necessarily match the most consuming process during the interval of time where the average CPU load was computed.
-------------	--

Output

OK state	CPU Load OK (<interval1>mn:< load1>%) (<interval2>mn: <load2%>)
WARNING or CRITICAL state	If the load of the most consuming process, at the time the check is done, is more than zero: CPU Load HIGH (<interval1>mn:< load1>%) (<interval2>mn: <load2%>) - Process <pname> using <pload>% If it is zero: CPU Load HIGH (<interval1>mn:< load1>%) (<interval2>mn: <load2%>)

Table C-3. check_ns_load (Windows) output

Example

```
check_ns_load!1!80!90!10!60!80
```

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

Status is set to **warning** if load is more than 80% over the last minute, or more than 60% over the last ten minutes.

Status is set to **critical** if load is more than 90% over the last minute, or more than 80% over the last ten minutes.

C.4 check_ns_mem (Windows)

Usage

```
check_ns_mem PERCENT | SIZE <wThresh> <cThresh>
```

PERCENT | SIZE unit for the limits, percentage or size in Mbytes.

<wThresh> value of used memory that result in a WARNING message.

<cThresh> value of used memory that result in a CRITICAL message.

All arguments are required.

The memory measured is the total memory used by the system (physical memory + virtual memory). It is equivalent to the **Commit Charge** displayed in the Window Task Manager.

Output

OK state	Memory Usage OK (total: <total_mb>Mb) (used: <used_mb>Mb, <used_pct>%) (free: <free_mb>Mb) (physical: <phys_mb>Mb)
WARNING or CRITICAL state	Memory Usage HIGH (total: <total_mb>Mb) (used: <used_mb>Mb, <used_pct>%) (free: <free_mb>Mb) (physical: <phys_mb>Mb)

Table C-4. check_ns_mem (Windows) output

The output also contains the value of the physical memory for the system.

Example

```
check_ns_mem!PERCENT!70!90
```

```
Memory Usage OK (total: 302Mb) (used: 208Mb, 68%) (free: 94Mb)
(physical: 127Mb)
```

Status is set to **warning** if used space is more than or equal to 70%.

Status is set to **critical** if used space is more than or equal to 90%.

The total memory for this host is 302 Mb, while physical memory is 127 Mb.

C.5 check_ns_service (Windows)

Usage

check_ns_service showall | showfail <ServiceName1> [ServiceName2]

showall showfail	specifies if all services, or only the services that are not running will be shown in the output.
<ServiceNameN>	name of the services to monitor (key name or display name are both accepted).

At least one service to monitor must be specified. Up to eight services can be specified. If more than one service is specified, returned status is the most severe service status

Service names containing a blank space must be enclosed by double quotes.

Services can be given with either their display name or their key name. The display name is the name that appears in the Service Management Window, and depends on the OS language. For instance: "Fax Service", or "Service de télécopie"

The key name of a service can be found in the registry, under the key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services

For instance: Fax

Output

OK state	If showall is set: OK: '<ServiceName1>' '<ServiceName2>' 0 If showfail is set: All OK
WARNING state	If showall is set: <state1>: '<ServiceName1>' <state2>: '<ServiceName2>' where <stateN> is one of the following state: OK: the service is started Paused: the service is suspended If showfail is set: <state1>: '<ServiceName1>' <state2>: '<ServiceName2>' 0 where <stateN> is Paused (OK services are not listed).
CRITICAL state	If showall is set (depending on the problem): <state1>: '<ServiceName1>' <state2>: '<ServiceName2>' where <stateN> is one of the following state: OK the service is started NotActive: the service is stopped NotExist: the service does not exist Timeout: the service did not respond to the request CheckError something went wrong in the checking mechanism If showfail is set: <state1>: '<ServiceName1>' <state2>: '<ServiceName2>' 0 where <stateN> is one of the following state: NotActive, NotExist, Timeout, CheckError (OK services are not listed)

Table C-5. check_ns_service (Windows) output

Example

```
check_ns_service!showall!"Client DHCP"! "Client DNS"!Telnet  
OK:'Client DHCP' OK:'Client DNS' NotActive:'Telnet'
```

This command checks that the Client DHCP, Client DNS and Telnet services are running. Final status is critical because the Telnet service is not active on the machine. With the **showall** option, all services are listed in the output, even running services.

C.6 check_windisks (Windows)

Usage

```
check_windisk -w <warning_limit> -c <critical_limit> [-i <drive to include>] [-e <drive_to  
exclude>]
```

-w <warning_limit> value of used space that result in a WARNING message.
-c <critical_limit> value of used space that result in a CRITICAL.
-i <drive to include> DRIVE letter to include in the check.
-e <drive_to exclude> DRIVE letter to exclude from the check

Output

OK state	DISKS OK: all disks (drives list) less than <warning limit> utilized
WARNING or CRITICAL state	DISKS <STATE>: (drives list) more than <state limit> utilized

Table C-6. check_windisks (Windows) output

Examples

- `check_windisk!-w 80!-c 90`
This command checks the used space for all the disks.
If used space is more than or equal to 80%, status is set to **warning** as in the following output:
DISKS WARNING: (C:, D:, E:, F:, G:, I:) more than 80% utilized
If used space is more than or equal to 90%, status is set to **critical** as in the following output:
DISKS CRITICAL: (C:, D:, E:, F:, G:, I:) more than 90% utilized
- `check_windisk!-w 80!-c 90!-e G`
This command checks used space for all the disks, except the G drive.
DISKS OK: all disks (C:, D:, E:, F:, I:) less than 80% utilized

C.7 check_procs (Linux, AIX)

Usage

check_procs -w <w_range> -c <c_range> [-s <states>] [-p <ppid>] [-u <user>] [-a <args>]
[-C <command>]

- <w_range> generates warning status if process count is outside this range.
- <c_range> generates critical status if process count is outside this range.
- Ranges are specified as follows: 'min:max' or 'min:' or ':max' (or 'max'). A warning or critical status will be generated if the count is inside the specified range ('max:min'), lower than min ('min:'), or more than max (':max' or 'max').
- <states> scans only the processes for which status (issued by the ps command) corresponds to a specified status.
- <ppid> scans only children for which the parent process ID is this ppid.
- <user> scans only processes with this user name or ID.
- <args> scans only processes with a full command (with arguments) beginning with the specified string.
- <command> scans only processes with a command equal to the one specified.

This command checks the number of currently running processes and sets status to **WARNING** or **CRITICAL** if the process count is outside the specified threshold ranges. The process count can be filtered by process owner, parent process PID, current status (for example 'Z'), or it may be the total number of running processes.

Output

OK, WARNING or CRITICAL state	<status> - <nb_procs> processes running
	<filter_conditions>
	<status> service state (OK, WARNING or CRITICAL)
	<nb_procs> number of running processes matching the filter conditions
	<filter_conditions> applied filters conditions.

Table C-7. check_procs (Linux) output

Example

Let's suppose that the `/bin/ps -axo 'stat uid ppid comm args'` command returns the following lines:

```
STAT  UID  PPID  COMMAND      COMMAND
S      0    0  init         init
SW     0    1  keventd      [keventd]
SWN    0    0  ksoftirqd_CPU0 [ksoftirqd_CPU0]
SWN    0    0  ksoftirqd_CPU1 [ksoftirqd_CPU1]
SW     0    0  kswapd       [kswapd]
SW     0    0  kreclaimd    [kreclaimd]
SW     0    0  bdflush      [bdflush]
SW     0    0  kupdated     [kupdated]
SW<    0    1  mdrecoveryd  [mdrecoveryd]
SW     0    1  kjournald    [kjournald]
SW     0    1  khubd        [khubd]
SW     0    1  kjournald    [kjournald]
SW     0    1  kjournald    [kjournald]
SW     0    1  kjournald    [kjournald]
SW     0    1  kjournald    [kjournald]
S      0    1  dhcpcd       /sbin/dhcpcd -n -H -R eth0
```

```

S    0    1 syslogd      syslogd -m 0
S    0    1 klogd       klogd -2
S    32    1 portmap     portmap
S    29    1 rpc.statd    rpc.statd
S    0    1 sshd          /usr/sbin/sshd
S    4    1 lpd          lpd Waiting
S    0    1 sendmail      sendmail: accepting connections
S    0    1 gpm          gpm -t ps/2 -m /dev/mouse

```

Following are examples using the **check_procs** command and the corresponding output.

- `check_procs -w 100 -c 150`
OK - 24 processes running
This command checks the number of processes running on the local host.
Status is set to **warning** if the number of processes is more than 100.
Status is set to **critical** if the number of processes is more than 150.
- `check_procs -w 1: -C lpd`
OK - 1 processes running with command name lpd
This command checks that there is at least one lpd process running on the local host.
Status is set to **warning** if the lpd process is not running. '1:' means that the result is OK if the number of processes is in the range from 1 (included) to the maximum integer value.
- `check_procs -w 3:1 -c 1: -C kjournald`
OK - 5 processes running with command name kjournald
This command checks the number of kjournald processes.
Status is set to **warning** if this number is 1, 2 or 3, to critical if it is 0, and to OK otherwise.
- `check_procs -w:10 -s W`
WARNING - 14 processes running with STATE = W
This command checks the number of processes that have a W state (this includes SW and SWN).
Status is set to **warning** if this number is more than 10.
- `check_procs -w:2 -s 'N<'`
WARNING - 3 processes running with STATE = N<
This command checks the number of processes that have a N or < state (this includes SWN and SW<).
Status is set to **warning** if this number is more than 2.
- `check_procs -w 1: -a "sendmail: accepting"`
OK - 1 processes running with args sendmail: accepting
This command checks that there is at least one process with the full command starting with "sendmail: accepting" running on the local host.
- `check_procs -w 1: -a "accepting connections"`
WARNING - 0 processes running with args accepting connections
No process with a full command starting with "accepting connections" was found.
Although the command "sendmail: accepting connections" matches the -a string, it does not match at position 0 and is not counted as a matching process.

C.8 check_log2.pl (Linux, AIX)

Usage

check_log2.pl -l <log_file> -s <seek_file> -p <pattern> [-n <negpattern>]

<log_file> text file to scan for patterns.
<seek_file> temporary file used to store the seek byte position of the last scan. The name must be composed of alphanumeric characters (/ not allowed). If the file size is smaller than the seek position (the file has been truncated or rotated since the last check), the scan is started from the beginning.
<pattern> pattern to be searched. It can be any Regular Expression pattern that perl's syntax accepts.
<negpattern> negative pattern. Lines containing this pattern are discarded from the search.

This command scans arbitrary text files for regular expression matches.

This script runs with the root setuid bit in order to scan log files that are accessible only by root user. This is why the seek file location is forced in a safe directory.

Notes

- The **notify_recovery** value for the service should be set to **0**, so that Bull System Manager does not notify recoveries for the check. Since pattern matches in the log file will only be reported once and not the next time, there will still be unmeaningful recoveries.
- The **notificationPeriod** must be **different from none** so that someone is alerted that the pattern was found once and eventually not found again since the last scan.
- A different **<seek_file>** must be supplied for each service that will use this command script - even if the different services check the same **<log_file>** for pattern matches. This is necessary for the way the script operates.

Output

OK	a file is successfully scanned and no pattern matches are found. OK - No matches found
WARNING	one or more patterns are found along with the pattern count and the line of the last pattern matched.
CRITICAL	an error occurred, such as 'file not found'.

Table C-8. check_log2.pl (Linux) output

WARNING or CRITICAL status output:

<nb-matching-line> <last-matching-line-in-file>
<nb-matching-line> number of lines matching the pattern (and not matching the optional negative pattern)
<last-matching-line-in-file> the last matching line found in the log file.

Examples

Let's suppose that the `/var/log/messages` file contains the following lines:

```
Nov 26 15:30:44 horus pam_rhosts_auth[4790]: allowed to
Administrator@osiris as integ
Nov 26 15:30:44 horus rsh(pam_unix)[4790]: session opened for user integ
by (uid=0)
Nov 26 15:30:49 horus login(pam_unix)[4786]: authentication failure;
logname= uid=0 euid=0 tty=pts/1 ruser= rhost=isis user=root
Nov 26 15:30:51 horus login[4786]: FAILED LOGIN 1 FROM isis FOR root,
Authentication failure
Nov 26 15:31:11 horus login(pam_unix)[4786]: check pass; user unknown
Nov 26 15:31:11 horus login(pam_unix)[4786]: authentication failure;
logname= uid=0 euid=0 tty=pts/1 ruser= rhost=isis
Nov 26 15:31:13 horus login[4786]: FAILED LOGIN 2 FROM isis FOR admin,
Authentication failure
Nov 26 15:31:24 horus rsh(pam_unix)[4790]: session closed for user integ
Nov 26 15:31:29 horus login(pam_unix)[4786]: check pass; user unknown
Nov 26 15:31:32 horus login[4786]: FAILED LOGIN 3 FROM isis FOR admin,
Authentication failure
Nov 26 15:33:14 horus login(pam_unix)[4853]: session opened for user
netsaint by (uid=0)
Nov 26 15:33:14 horus -- netsaint[4853]: LOGIN ON pts/1 BY netsaint FROM
isis
Nov 26 15:33:22 horus login(pam_unix)[4853]: session closed for user
netsaint
Nov 26 15:33:37 horus ftpd[4916]: FTP session closed
Nov 26 15:34:11 horus su(pam_unix)[4931]: session opened for user root by
root(uid=503)
```

Following are examples using the `check_log2.pl` command and the corresponding output.

- `check_log2.pl -l /var/log/messages -s t2.seek -p 'FAILED'`

(3): Nov 26 15:31:32 horus login[4786]: FAILED LOGIN 3 FROM
isis FOR admin, Authentication failure
This command searches for lines containing the string **FAILED** in the
`/var/log/messages` file. Three lines were found and the last one is displayed.
- `check_log2.pl -l /var/log/messages -s t3.seek -p 'session
opened'`

(3): Nov 26 15:34:11 horus su(pam_unix)[4931]: session opened
for user root by root(uid=503)
This command searches for lines containing the string "session opened" in the
`/var/log/messages` file. Three lines were found and the last one is displayed.
- `check_log2.pl -l /var/log/messages -s t4.seek -p 'LOGIN.*isis'
-n netsaint`

(3): Nov 26 15:31:32 horus login[4786]: FAILED LOGIN 3 FROM
isis FOR admin, Authentication failure
This command searches for all **LOGIN** from the host `isis`, except the ones with
`netsaint` user, in the `/var/log/messages` file. Three lines were found and the last
one is displayed.

C.9 check_disk (Linux, AIX)

Usage

check_disk -w <wlimit>[%] -c <climit>[%] [-p <path>]

- <wlimit> minimum value of free space that result in a WARNING message
the value in expressed in Kbytes, unless '%' is specified.
- <climit> minimum value of free space that result in a CRITICAL message
the value is expressed in Kbytes, unless '%' is specified
- <path> filesystem to be checked (checks all mounted filesystems if unspecified).
the name can be given either as the mounting point (ex: /usr) or as the device name (ex: /dev/sda2). If a directory name that does not match a filesystem is given, the command tries to determine the corresponding filesystem. If successful, it checks that filesystem.

Note The warning limit must be more than the critical limit.

This command checks the free space left on FileSystems. It uses the **df** command. Limits can be given either in percentage, or in Kbytes.

Output

OK, WARNING or CRITICAL state	DISK <status> - [<free kb> kB (<free percent>%) free on <device name>]
	<status> service state (OK, WARNING or CRITICAL)
	<free Kb> free space in Kbytes left on filesystem
	<free percent> percentage of free space left on filesystem
	<device name> device name of the filesystem.
	This information is repeated for each filesystem, if all the mounted filesystems are monitored.

Table C-9. check_disk (Linux) command output

Example

```
check_disk -w 20% -c 10% -p /usr
```

```
DISK OK - [7068772 kB (75%) free on /dev/sda2]
```

This command checks the free space percentage for the FileSystem /usr (/dev/sda2) on the local host.

Status is set to **warning** if the free space left on FileSystem /usr is **less than 20%**.

Status is set to **critical** if the free space left on FileSystem /usr is **less than 10%**.

C.10 check_disks.pl (Linux, AIX)

Usage

```
check_disks.pl -w <warn%> -c <crit%> [-i <include-fs>]* [-e <exclude-fs>]*
```

<warn%> percentage of space used that result in a WARNING message.
<crit%> percentage of space used that result in a CRITICAL message.
<include-fs> filesystem to be checked (checks all mounted filesystems if unspecified). This option
 can be repeated for specifying more than one filesystem to check.
 the name must be given as the mounting point (ex: /usr).
<excluded-fs> filesystem to be excluded from the check. This option can be repeated for specifying
 more than one filesystem to exclude
 the name must be given as the mounting point (ex: /usr).

This command checks the space used for FileSystems, and allows the exclusion of some FileSystems from the check. It uses the **df** command. Limits are given in percentage.

Output

OK state	DISKS OK: all disks less than 70% utilized
WARNING or CRITICAL state	DISK <status>: (<filesystems>) more than <limit>% utilized. <status> service state (WARNING or CRITICAL). <filesystems> list of filesystems whose used space percentage is over the limit. <limit> limit value defined for the status.

Table C-10. check_disks.pl (Linux) output

If there are FileSystems with WARNING and CRITICAL status, this information is repeated to indicate all the FileSystems with a non-OK status.

Unlike **check_disk**, this command does not give full information (capacity and space used) for the FileSystems, but reports synthetically the FileSystems with problems. It can be used for a global vision of FileSystems status, while **check_disk** can be used for specific FileSystems details.

Example

```
check_disks.pl -w 60 -c 75 -e /mnt/cdrom
```

```
DISK CRITICAL: ( / ) more than 75% utilized - DISKS WARNING: ( /usr /var  
) more than 60% utilized
```

This command checks the used space for the all the mounted FileSystems, except **/mnt/cdrom**.

If used space is **more than or equal to 60%**, status is set to **warning**.

If used space is **more than or equal to 75%**, status is set to **critical**.

Here, status is **CRITICAL** because **/** has more than 75% used space. **/usr** and **/var** are also set to **warning** because they have more than 60% used space.

C.11 check_cpuload (Linux, AIX)

Usage

```
check_cpuload -w WLOAD1,WLOAD5,WLOAD15 -c CLOAD1,CLOAD5,CLOAD15
```

<wload1>	utilization average limit to result in a WARNING message during the last minute, must be a number between 0 and 100.
<wload5>	utilization average limit to result in a WARNING message during the last 5 minutes, must be a number between 0 and 100.
<wload15>	utilization average limit to result in a WARNING message during the last 15 minutes, must be a number between 0 and 100.
<cload1>	utilization average limit to result in a CRITICAL message during the last minute, must be a number between 0 and 100.
<cload5>	utilization average limit to result in a CRITICAL message during the last 5 minutes, must be a number between 0 and 100.
<cload15>	utilization average limit to result in a CRITICAL message during the last 15 minutes, must be a number between 0 and 100.

All arguments are required.

This command checks average CPU utilization during three predefined time intervals. It is possible to set a **warning** and a **critical** limit for each time interval.

CPU utilization is defined as: (load average / number of processors) * 100

Load average is given by **uptime** and **w**.

Returned status is the most severe status.

Output

OK state	CPU Utilization: <load1> (1mn), <load5> (5mn), <load15> (15mn)
WARNING or CRITICAL state	CPU Utilization: <load1> (1mn), <load5> (5mn), <load15> (15mn) <status>
<load1> <load5> <load15> percentage of average CPU load for respectively the last minute, the last 5 minutes and the last 15 minutes.	
<status> either WARNING or CRITICAL.	

Table C-11. check_cpuload (Linux) command output

Example

```
check_cpuload -w 80,70,60 -c 90,80,70
```

This command checks the CPU load for the local host.

Status is set to **warning** if load is more than 80% during the last minute, or more than 70% during the last 5 minutes or more than 60% during the last 15 minutes, as in the following result:

CPU Utilization: 87% (1mn), 52% (5mn), 29% (15mn) WARNING

Status is set to **critical** if load is more than 90% during the last minute, or more than 80% during the last 5 minutes or more than 70% during the last 15 minutes, as in the following result:

CPU Utilization: 100% (1mn), 64% (5mn), 37% (15mn) CRITICAL

Status is set to **OK** if no limit is raised, as in the following result

CPU Utilization: 23% (1mn), 29% (5mn), 24% (15mn)

C.12 check_lpar_load (AIX)

Usage

```
check_lpar_load -w <wlimit> -c <climit>
```

<wlimit> percent of load CPU that result in a WARNING message
<climit> percent of load CPU that result in a CRITICAL message.

All the arguments are required.

This command gets the cpu load of an AIX system or partition. The warning limit must be lower than the critical limit.

Output

The output depends on the type of partition: shared capped, shared uncapped, dedicated.

WARNING, CRITICAL or OK state	Shared capped	<status> - Phys CPU load is load_cpu% entc=entitled_capacity% (idle:idle_cpu% wait:wait_cpu%) - type=Shared Capped partition
	Shared uncapped	<status> - Phys CPU load is load_cpu% of max_cpu CPU (idle:idle_cpu% wait:wait_cpu%) - max_vp=maximum_virtual_cpu type=Shared Uncapped partition
	dedicated	<status> - CPU load is load_cpu (idle:idle_cpu% wait:wait_cpu%) - type=Dedicated partition

Table C-12. check_lpar_load (AIX) output

Example

```
check_lpar_load -w 80 -c 90
```

```
OK - Phys CPU load is 0.00 0% of 1 CPU (idle:99.2% wait:0%) -  
max_vp=2 type=Shared Uncapped partition
```

C.13 check_mem.pl (AIX)

Usage

```
check_mem.pl -w <wlimit> -c <climit>
```

- <wlimit> percent of used memory that result in a WARNING message
- <climit> percent of used memory that result in a CRITICAL message.

All the arguments are required.

This command measures used memory, so the warning limit must be lower than the critical limit. The measured memory is the total memory used by the system (physical memory + swap).

Output

OK, WARNING or CRITICAL state	Memory: WARNING - Total: <total_mb> (pgsize: 4K) (used: <used_mb>, <used_pct>%) (free: <free_mb>)
-------------------------------------	--

Table C-13. check_mem.pl (Linux) output

Example

```
check_mem.pl -w 95 -c 99
```

```
Memory: WARNING - Total: 131072 (pgsize: 4K)  
(used: 126284, 96.3%) (free: 4788)
```

C.14 check_memory (Linux)

Usage

```
check_memory <wlimit> <climit>
```

- <wlimit> percent of used memory that result in a WARNING message
- <climit> percent of used memory that result in a CRITICAL message.

All the arguments are required.

This command measures used memory, so the warning limit must be lower than the critical limit. The measured memory is the total memory used by the system (physical memory + swap).

Output

OK, WARNING or CRITICAL state	Status: <status> - (total: <total_mb>Mb) (used: <used_mb>Mb, <used_pct>%) (free: <free_mb>Mb) (physical: <phys_mb>Mb)
	<status> service status (OK, WARNING or CRITICAL)
	<total_mb> total memory size (physical memory + swap)
	<used_mb> total memory used
	<used_pct> percentage of total memory used by the system
	<free_mb> memory (physical or swap) left free
	<phys_mb> size of the physical memory.
All values are expressed in Mbytes.	

Table C-14. check_memory (Linux) output

Example

```
check_memory 70 90
```

```
Status: OK - (total: 2996Mb) (used: 863Mb, 29%) (free: 2132Mb)
(physical: 1004Mb)
```

This command checks the free memory percentage for the local host.

Status is set to **warning** if the memory used is **more than 70%**.

Status is set to **critical** if the memory used is **more than 90%**.

The total memory for this host is 2996 MB, while the physical memory is 1004 MB.

C.15 check_swap (Linux, AIX)

Usage

```
check_swap -w <w_usedpercent>% -c <c_usedpercent>%
```

<w_usedpercent> percent of used swap that result in a WARNING message.

<c_usedpercent> percent of used swap that result in a CRITICAL message.

Or:

```
check_swap -w <w_freebytes> -c <c_freebytes>
```

<w_freebytes> lowest free swap space that result in a WARNING message.

<c_freebytes> lowest free swap space that result in a CRITICAL message.

All the arguments are required.

This command can measure either the percentage of used swap space, or the value of free swap space in bytes. This depends of the presence or not of the '%' sign.

If '%' is specified, the measure is the percentage of **used** space, so the critical limit must be more than the warning limit.

If '%' is not specified, the measure is the **free** space left in bytes, so the warning limit must be more than the critical limit.

Output

OK, WARNING or CRITICAL state	<status> - Swap used: <used-percent>% (<used-mbytes> Mb out of <swap-mbytes>)	
	<status>	service state ("Swap ok", WARNING or CRITICAL)
	<used-percent>	percentage of used swap space
	<used-mbytes>	used swap space in Mbytes
	<swap-mbytes>	size of the swap in Mbytes.

Table C-15. check_swap (Linux)output

Example

```
check_swap -w 50% -c 80%
```

```
Swap ok - Swap used: 0% (0 Mb out of 1992)
```

This command checks the used swap percentage for the local host.
Status is set to **warning** if the used swap is **more than 50%**.
Status is set to **critical** if the used swap is **more than 80%**.
The size of the swap is 1992 Mbytes.

C.16 check_users (Linux, AIX)

Usage

```
check_users -w <wlimit> -c <climit>
```

<wlimit> number of logged in users that result in a WARNING message.
<climit> number of logged in users that result in a CRITICAL message.

All the arguments are required.

This command checks the number of users currently logged in on the local system.

Output

OK, WARNING or CRITICAL state	USERS <status> - <nb-users> users currently logged in	
	<status>	service state (OK, WARNING or CRITICAL)
	<nb-users>	number of users currently logged in.

Table C-16. check_users (Linux) output

Example

```
check_users -w 10 -c 20
```

```
USERS WARNING - 18 users currently logged in
```

Status is set to **warning** if there are **10 or more users** logged in.

Status is set to **critical** if there are **20 or more users** logged in.

C.17 check_httpURL (Windows, Linux and AIX)

Usage

```
check_httpURL <port>!<url>!<response_substring>'!<content_response>'
```

<port>	port on which URL is to be tested.
<url>	URL to be tested. Do not forget the character '/'. Do not forget the character '!'.
<response_substring>	search this substring in the first line of the HTTP response.
<content_substring>	search this substring in the content of the returned page.

response_substring and **contents_substring** must be surrounded by single quotes.

To know which substring to check in the HTTP response (**response_substring**), you may launch the following command if the Bull System Manager Server is installed on a Linux operating system:

```
<Bull System Manager server install dir>/engine/nagios/libexec/check_httpURL  
-H <hostname> -p <port> -u <url>
```

The output of this command is the HTTP response, in which you can choose a substring to be checked. If the output indicates an error, correct the port or the url parameters.

Status is set to **warning** for HTTP errors: 400, 401, 402, 403 or 404 such as unauthorized access.

Status is set to **critical** if:

- the substring <response_substring> is not found in the first line of the HTTP response. The error message is: "Invalid HTTP response received from host on port xx"
- the substring <contents_substring> is not found in the returned page. The error message is "string not found"
- the response time exceeds 10 seconds
- there is an HTTP error 500, 501, 502 or 503
- the connection with the server is impossible.

Output:

OK state	HTTP ok: HTTP/1.0 200 Document follows - 0 second response time
WARNING state	HTTP WARNING: HTTP/1.0 401 Unauthorized
CRITICAL state	Invalid HTTP response received from host on port HTTP CRITICAL: string not found Connection refused by host Socket timeout after 10 seconds

Table C-17. check_httpURL (Windows and Linux) output

C.18 check_mrtg (Windows, AIX and Linux)

Usage

check_mrtg -F <reporting_logfile> -a AVG -v 1 -e 10 -w <warning_threshold> -c
<critical_threshold> -l <status_info_label> -u <status_info_unit>

<reporting_logfile>	Each reporting indicator, associated to a host, has its values logged in a log file named "<host_name>+<indicator_name>.log". This log file is located in <install_dir>/core/share/reporting/var.
<warning_threshold>	Minimum value of free space that result in a WARNING message. The default value is 80.
<critical_threshold>	Minimum value of free space that result in a CRITICAL message. The default value is 90.
<status_info_label>	The status information of the monitoring service looks like "<status_info_label>: <last value> <status_info_unit>". The default value for status_info_label is "Load". This parameter is used only to be displayed in the status information in the console.
<status_info_unit>	The status information of the monitoring service looks like "<status_info_label>: <last value> <status_info_unit>". The default value for status_info_unit is "%". This parameter is used only to be displayed in the status information in the console.

This command gets, then checks the last value of a reporting indicator, from a reporting log file located in <install_dir>/core/share/reporting/var.

Notes

- The reporting log file contains the name of the host associated to the reporting indicator. Therefore, the monitoring service cloned from **reporting.perf_indic** must have a **hostlist** containing only one host. By default, hostlist=none for the **Perf_indic** service and the **reporting** category.
 - The warning limit must be greater than the critical limit.
-

Example

```
check_mrtg -F ' c:/PROGRA~1/Bull/BULLSY~1/core/share/reporting/var/  
frcls2703+2703_memory.log' -a AVG -v 1 -e 10 -w 10 -c 90 -l Load -u %
```

C.19 check_PowerStatus (IPMI servers)

Usage

```
check_PowerStatus [[!user]!password]
```

<user>	The IPMI user name if it exists
<password>	The IPMI password associated to the user if this last one exists, or the IPMI authentication key.

This command gets, then checks the power status via the IPMIoverLAN protocol to the BMC of the server.

Example

```
check_PowerStatus!user!pass
```

C.20 check_IPMI_sensor (IPMI servers)

Usage

```
check_IPMI_sensor!<sensor_name>[!<-c lower_critical>][!<-w lower_non-critical>][!<-W  
upper_non-critical>][!<-C upper_critical>]
```

<sensor name>	The name of a numeric sensor listed in the SDR.
<lower_critical>	Lower critical threshold value that results in a CRITICAL state.
<lower_non-critical>	Lower non-critical threshold value that results in a WARNING state.
<upper_non-critical>	Upper non-critical threshold value that results in a WARNING state.
<upper_critical>	Upper critical threshold value that results in a CRITICAL state.

sensor name must be surrounded by single or double quotes.

This command gets a numeric sensor value, then checks it to the thresholds values defined in the SDR or to the thresholds values passed in arguments if any.

Note The unit (V, degrees C, rpm ...) is automatically extracted from the sensor information.

Output:

OK state	The current sensor value is in the NORMAL area (lower non-critical threshold < current value < upper non-critical threshold)
WARNING state	The current value is in the WARNING area (lower critical threshold < current value < lower non-critical threshold or upper non-critical threshold < current value < upper critical threshold)
CRITICAL state	The current value is in the CRITICAL area (current value < lower critical threshold or current value > upper critical threshold)
UNKNOWN state	The current value cannot be retrieved (sensor not found, unable to establish LAN session ...)

Table C-18. check_IPMI_sensor (IPMI servers) output

Example

```
check_IPMI_sensor! "Valve Aperture"
```

```
OK : 55.380 %
```

C.21 check_IPMI_sensor_avg (IPMI servers)

Usage

```
check_IPMI_sensor_avg!<sensor name list>[!<-c lower_critical>][!<-w lower_non-critical>][!<-W upper_non-critical>][!<-C upper_critical>]
```

<sensor name list>	A list of names of numeric sensors (listed in the SDR) separated with a comma.
<lower_critical>	Lower critical threshold value that results in a CRITICAL state.
<lower_non-critical>	Lower non-critical threshold value that results in a WARNING state.
<upper_non-critical>	Upper non-critical threshold value that results in a WARNING state.
<upper_critical>	Upper critical threshold value that results in a CRITICAL state.

Each **sensor name** must be surrounded by single quotes.

This command gets the current value of a list of numeric sensors, then calculates the average value, and checks it to the contextual thresholds if any.

Note	The unit (V, degrees C, rpm ...) must be the same for all the sensors, and is automatically extracted from the sensor information.
-------------	--

Output:

OK state	The average of the sensors values is in the NORMAL area (lower non-critical threshold < average value < upper non-critical threshold)
WARNING state	The average of the sensors values is in the WARNING area (lower critical threshold < average value < lower non-critical threshold or upper non-critical threshold < average value < upper critical threshold)
CRITICAL state	The average of the sensors values is in the WARNING area (average value < lower critical threshold or average value > upper critical threshold)
UNKNOWN state	The average value cannot be calculated (sensor not found, unable to establish LAN session, sensors types are different ...)

Table C-19. check_IPMI_sensor_avg (IPMI servers) output

Example

```
check_IPMI_sensor_avg! "TH_0 Temp." , "TH_1 Temp." , "TH_3 Temp."

OK : 23.100 degrees C
```

C.22 check_pressure (IPMI servers)

Usage

```
check_pressure!<sensor name>[!<-c lower_critical>][!<-w lower_non-critical>][!<-W upper_non-critical>][!<-C upper_critical>]
```

<sensor name>	The name of a numeric sensor listed in the SDR.
<lower_critical>	Lower critical threshold value that result in a CRITICAL state.
<lower_non-critical>	Lower non-critical threshold value that result in a WARNING state.
<upper_non-critical>	Upper non-critical threshold value that result in a WARNING state.
<upper_critical>	Upper critical threshold value that result in a CRITICAL state.

sensor name must be surrounded by single or double quotes.

This command, dedicated to pressure sensor, is similar to check_IPMI_sensor but, if the sensor unit is "kPa", multiplies the current value by 1000 and changes the unit to "Pa".

Note The unit (kPa ...) is automatically extracted from the sensor information.

Output:

OK state	The current sensor value is in the NORMAL area (lower non-critical threshold < current value < upper non-critical threshold)
WARNING state	The current value is in the WARNING area (lower critical threshold < current value < lower non-critical threshold or upper non-critical threshold < current value < upper critical threshold)
CRITICAL state	The current value is in the CRITICAL area (current value < lower critical threshold or current value > upper critical threshold)
UNKNOWN state	The current value cannot be got (sensor not found, unable to establish LAN session ...)

Table C-20. check_pressure (IPMI servers) output

Example


```
check_pressure!"Air Pressure"
```

```
OK : 18 Pa
```

Appendix D. Administration Commands

Several Bull System Manager server menus allow you, as administrator, to perform the most frequently used operations.

To display these menus, from the Bull System Manager Console:

- click the  icon representing the BSM Control GUI in the Administration zone (top right),
- or
- click the `Control` link on the Bull System Manager Home Page.

When the GUI is launched, an authentication dialog is displayed:

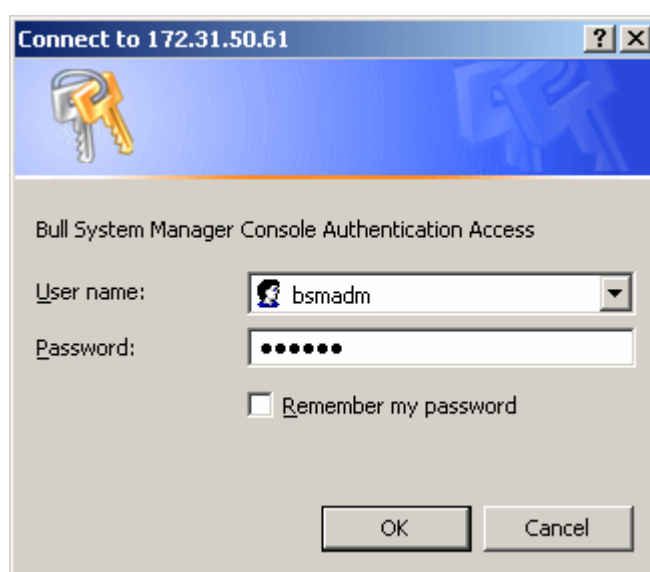


Figure D-1. Authenticating the Bull System Manager control user

- On Windows, Authenticated users are users declared in the Windows users database. The user name must be entered in the following format: **DOMAINNAME\Username**
- On Linux, enter **bsmadm / bsmadm**.

This user is associated with a Role: **Administrator** or **Operator**. The Administrator role has write access to the configuration; the Operator role has only read access. The execution of the BSM Control requires the Administrator role.

Note This user (and role) is created during the installation process. Refer to the *Bull System Manager Installation Guide* (86 A2 54FA) to learn how to configure the Bull System Manager Configuration tool authentication feature.

The **Bull System Manager ServerControl** GUI allows you to start, stop, or restart the BSM Server, according to your requirements. When the BSM Control GUI is launched, the current status of the server is displayed, as shown in the following figure :

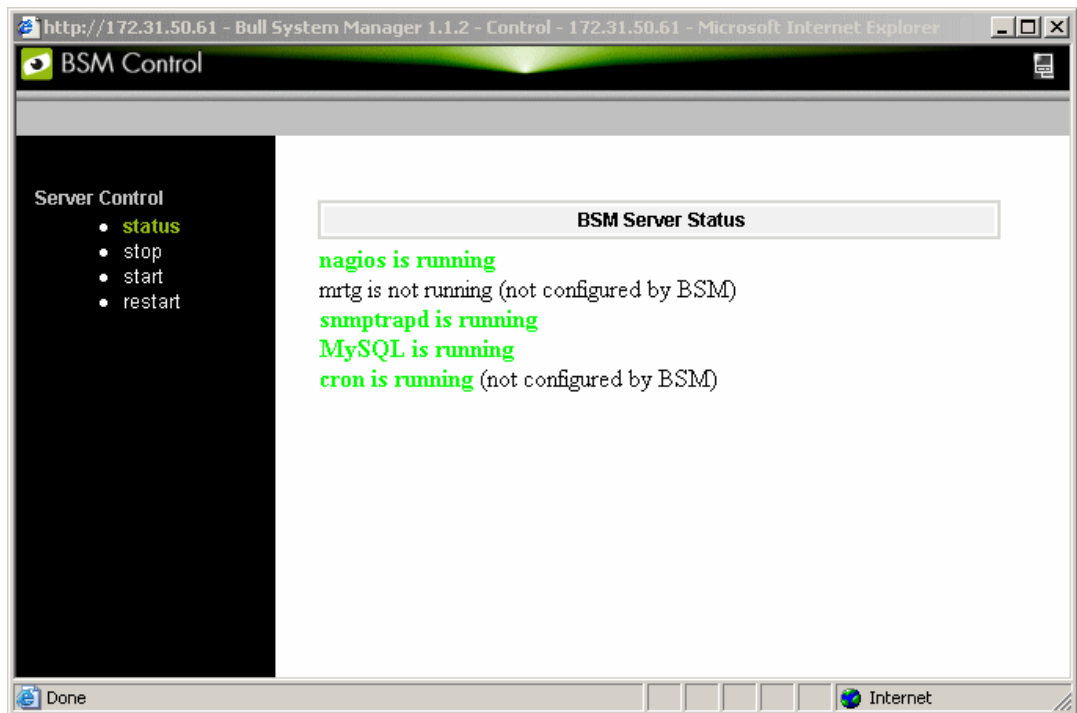


Figure D-2. BSM Server Status

Appendix E. SSH Configuration

The SSH configuration specific to the BSM Applications is localized into the directory <BSM installation directory>/engine/etc/ssh/.

E.1 SSH client configuration on Bull System Manager Server

The file <BSM installation directory>/engine/etc/ssh/config_bsm delivered by Bull System Manager, contains SSH configuration parameters. It can be used to perform non-prompt connection when executing ssh.

Parameters setting in config_bsm (Linux case):

```
PasswordAuthentication      no
NumberOfPasswordPrompts    0
StrictHostKeyChecking       no
UserKnownHostsFile
/opt/BSMServer/engine/etc/ssh/known_hosts_bsm
```

E.2 Keys generation on Bull System Manager Server

Private key for the Bull System Manager Server is automatically performed during the post-installation of a Bull System Manager Server, to allow BSM server to perform non-prompted connection on remote machine, from the Configuration GUI (as Web user) or from the nagios service (as nagios user). One key is generated and is copied in multiple files to respect the restricted permissions required for identity files.

The following table display the key files delivered by Bull System Manager and their characteristics:

Linux platform

File	Owner/Group	Right	Usage
id_dsa.bsm	bsmuser/bsmgroup	600	Private key used in Nagios plugin. Note: another filename can be used (can be specified during the configuration of the Vios in Bull System Manager).
id_dsa.www	apache*/bsmgroup	600	Private key used by the configuration GUI. Note: this name must not be changed
id_dsa.pub	bsmuser/bsmgroup	664	Corresponding public key.

* the name of the Apache user can differ among Linux distribution.

Windows platform

File	Owner	Right	Usage
id_dsa.bsm	SYSTEM	600	Private key used in Nagios plugin. Note: another filename can be used (it can be specified during the configuration of the Vios in Bull System Manager).
id_dsa.iis	administrator	600	Private key used by the configuration GUI when using IIS http server. Note: this name must not be changed.
id_dsa.apache	administrator	666	Private key used by the configuration GUI when using Apache http server. Note: this name must not be changed.
id_dsa.pub	bsmuser/bsmgroup	664	Corresponding public key.

The corresponding public key (id_dsa.pub) must be installed on the remote machine:

1. Copy the public key on the remote machine (use available protocols as ftp or scp)
2. Edit the file `<user home>/ssh/authorized_keys2` to add the key.

E.3 Use other identity file

You can use your own identity file, if you install it into the BSM SSH Configuration directory and execute the **set-ssh-key** script to generate the files used by BSM application.

1. Copy your key files (private and public key) into the BSM SSH Configuration directory.
2. Run the **set-ssh-key** file.
 - On Linux platform:

```
cd <BSM_install_directory>/core/bin
./set-ssh-key.sh -f <private_identity_file_name>
```

This script will generate the following files under the
<BSM_install_directory>/engine/etc/ssh directory:

`<private_identity_file_name>.www`
`<private_identity_file_name>.bsm`

- On Windows platform:

```
cd <BSM_install_directory>/core/bin
./set-ssh-key.bat <private_identity_file_name>
```

This script will generate the following files under the
<BSM_install_directory>/engine/etc/ssh directory:

`<private_identity_file_name>.apache`
`<private_identity_file_name>.iis`
`<private_identity_file_name>.bsm`

E.4 Test non-prompted connection

After key installation, you can test ssh connection:

- On Linux platform, execute the **ssh** command with the **-i** and **-F** parameters to use BSM SSH configuration:

```
cd <BSM_install_directory>/engine/etc/ssh  
ssh <remote_machine> -l <remote_user> -i id_dsa -F config_bsm <remote_command>
```

- On Windows platform, run the **test-ssh.bat** command delivered under <BSM_install_directory>/core/bin/directory:

```
cd <BSM_install_directory>/core/bin  
test-ssh.bat <remote_machine> <remote_user> <id_file_name><remote_command>
```

Index

A

access rules to GUI (read/write), 15
Active features link, 79, 162, 198
Add-LPAR button, 58
agent installation, 66
AIX services
 customizing, 111
alerts, 2
alerts service
 creating, 115
All Supervision Features, 198
Application Roll-over Facility (ARF), 186
authentication, 9
autocall
 properties, 179
Autocall server, 179

B

basebrd5.mib, 209
bmclanpet.MIB, 209
BPREE, 186
BPRSE, 186
Browse Mibs, 160
BSM concepts, 2
BSM hostgroup, 68
BSM Hostgroup, 7
Bull Remote Maintenance Center, 179
Bull Support, 186
buttons
 Add-LPAR, 58
 Discover, 31, 41, 50

Host Discovery, 19
New Chassis, 39
New Platform, 29
Re-discover, 43
Reports, 153

C

category
 CMM, 210
 creation, 85
 customization, 86
 default, 7, 83
 deleting, 87
 EventLog, 207
 FileSystems, 208
 Hardware, 209
 Internet, 209
 LinuxServices, 208
 PAM, 210
 properties, 84
 Reporting, 209
 Syslog, 208
 template, 86
 WindowsServices, 207
CEC, 57
CECStatus service, 52
Chassis, 39, 40, 47, 64
chassis name, 40
check command
 list, 98
 parameters, 90
 syntax, 213
check parameters
 URL, 113
check_cpuload (Linux, AIX), 226
check_disk (Linux, AIX), 224
check_disks.pl (Linux, AIX), 225
check_httpURL (Windows, Linux, AIX), 231

- check_IPMI_sensor (IPMI servers), 233
- check_IPMI_sensor_avg (IPMI servers), 234
- check_log2.pl (Linux, AIX), 222
- check_lpar_load (AIX), 227
- check_mem.pl (AIX), 228
- check_memory (Linux), 228
- check_mrtg (Windows, Linux, AIX), 232
- check_nrpe command, 213
- check_ns_disk (Windows), 215
- check_ns_eventlog, 109
- check_ns_eventlog (Windows), 213
- check_ns_load (Windows), 216
- check_ns_mem (Windows), 217
- check_ns_service (Windows), 218
- check_PowerStatus (IPMI servers), 233
- check_pressure (IPMI servers), 235
- check_procs (Linux, AIX), 220
- check_swap (Linux, AIX), 229
- check_users (Linux, AIX), 230
- check_windisks (Windows), 219
- checkConfig.log.txt, 23
- CMM (Chassis Monitoring Module), 39, 47, 64
- CMM category, 210
- collect mode, 155
- commands
 - administration, 237
 - check_nrpe, 213
 - check_ns_eventlog, 109
 - ping, 2
 - snmptrap, 180
- community, 156, 181
- concepts, 2
- configuration
 - autocall, 179
 - contact, 175
 - contactgroup, 176
 - event handler, 167
 - global settings, 195
 - hardware manager, 73
 - host, 25
 - hostgroup, 68
 - inventory, 79
 - main steps, 19
 - notifications, 173
 - performance indicators, 153
 - SNMP Manager, 180
 - storage manager, 75, 77
 - supervision, 81
 - supervision event reception, 149
 - topology, 25
 - user & role, 163, 197
- configuration overview, 7
- configuration tasks, 7
- console
 - customizing, 185
- contact, 178
 - default, 7
 - manager, 178
 - properties, 175
- contactgroup
 - default, 7
 - mgt-admins, 178
 - properties, 176
- creating resource, 19
- customization
 - default view, 188
 - focus pane, 192
- customization tasks, 8
- customizing BSM, 185

D

- default configuration, 7
- default map, 190
- default view
 - customizing, 188
- default_map, 7
- deleting resource, 19
- Discover button, 31, 41, 50
- discovering host, 19, 26

E

- Edit link, 19
- editing resource, 19
- element list, 177, 190
- Email contactGroup, 126
- e-mail notification
 - enabling, 174
- enable Bull autocall, 90, 180
- enable e-mail notification, 175
- enable SNMP trap, 90, 181
- Enable SNMP trap reception, 151
- Escala Hosts, 48
- event handler
 - command, 169
 - configuration, 167
 - configuration, 167
 - templates, 170
- event log
 - scanning, 109
 - threshold, 109
- EventLog category, 207
- executable command, 168, 169
- Express5800, 37
- external URL, 187

F

- features activation, 198
- files
 - checkConfig.log.txt, 23
- FileSystems category, 208
- filter options, 82
- focus pane, 5, 192
 - properties, 192
- FTP port, 179

G

- global settings, 195
 - configuration, 195
- graph legend, 156
- graph title, 156
- GUI
 - access rules, 15
 - authentication, 9
 - concurrent access, 15
 - configuration tasks, 7
 - starting, 9
- GUI URL, 36, 74
- GUI_URL, 76, 78

H

- Handler, 167
- handler name, 168
- handler type, 168, 169
- Hardware category, 209
- hardware manager
 - configuration, 73
 - properties, 73
- Hardware monitoring, 125, 127
- HMC (Hardware Management Console), 48
- host
 - (de)activating monitoring, 125
 - blade, 44
 - CMM, 44
 - declaring, 66
 - discovering, 26
 - LPAR, 60
 - model**, 35, 37, 65
 - network name, 35, 37, 65
 - ns5005, 32
 - PAM, 32
 - parents, 35, 37, 65
 - properties, 65
- Host Discovery button, 19
- host list, 168
 - 'none' value, 84, 89
 - defining a list, 84, 89

- syntax, 84, 89, 91
- host list expression, 84
- hostgroup
 - default, 7, 68

I

- I/O Server host, 58
- image, 190
- Internet category, 209
- Internet Explorer, 9
- inventory
 - configuration, 79

L

- Linux services
 - customizing, 111
- LinuxServices category, 208
- local command, 187
- login, 179

M

- mail server, 174
 - properties, 175
- managament tree, 5
- manager
 - CMM, 45
 - contact, 7, 178
 - HMC, 52
 - PAM, 32
- map, 5
- mgt-admins contactgroup, 7, 178
- MIB
 - integration, 149
 - properties, 149
- MIB file, 150
- mibs tree, 161
- mmalert.mib, 210

- monitored hosts
 - customizing, 105
- monitoring
 - disabling, 198
- monitoring period, 90
- Monitoring Service, 150
- monitoring_status, 127
- Mozilla, 9

N

- Nagios, 6
- Nagios check commands, 213
- New Chassis button, 39
- New Platform button, 29
- notification
 - by SNMP trap, 180
- notification period, 126
 - customizing, 105
 - defining, 173
- notification period for host alerts, 176
- notification period for service alerts, 176, 180
- notification properties
 - host, 126
 - service, 90
- notifications, 2, 173
 - configuration, 173
- notify if down, 126
- notify if host down, 176
- notify if host recovery, 176
- notify if host unreachable, 176
- notify if recovery, 126
- notify if service critical, 176
- notify if service recovery, 176
- notify if service warning, 176
- notify if unreachable, 126
- NS 3005, 37
- NS 4000, 37

NS R400, 33
NS R422, 33
NS T800, 37
NS5005, 29
NS6000, 29

O

oid, 156
OS family, 36, 37, 65, 89
OS info, 36, 37, 66
Out-ofband attributes, 36

P

PAM category, 210
PAMeventtrap.MIB, 210
partitioning manager, 54
password, 179
perf_indic service, 115, 162, 164
performance indicator, 153
 properties, 155
performance indicators
 configuration, 153
PHP scripts, 6
PHP technology, 6
PHP-SNMP RPM, 154
Ping checking, 125
ping command, 2
ping monitoring option, 27
PL Server, 48
platform name, 30
polling interval, 90
port, 155
predefined resources, 7
properties
 red mark, 20

R

read/write access to GUI, 15
red mark on property, 20
Re-discover button, 43
relative, 155
Remote Maintenance Center, 179
re-notification interval, 126
report
 Save & Reload, 22
Reporting category, 209
Reports button, 153
result filter, 156

S

Save&Reload, 21
sender email, 175
service
 creation, 92
 customization, 94
 default, 88
 deleting, 97
 properties, 89
 template, 95
service name, 89
Service name, 110
SMTP port, 175
smtp_port, 177
SMU user, 38
SNMP community, 40
SNMP Manager
 properties, 181
SNMP port, 40
SNMP trap receiver, 151
SNMP trap receiver port, 151
snmptrap command, 180
snmptrapd port, 181, 183, 184

- storage manager
 - configuration, 75, 77
 - properties, 75
- supervision
 - configuration, 81
- supervision event reception
 - configuration, 149
- Syslog category, 208
- system command, 168, 169

T

- target directory, 179
- thresholds, 2
 - customizing, 107
- topology
 - configuration, 25
- Topology modification, 32, 44
- Trap name, 150
- Trap severity, 150

U

- URL
 - Bull System Manager main page, 9
 - customizing, 113, 164
 - GUI, 74
- user
 - bsmadm (Linux), 237
- User's Applications, 187
- Users & Roles, 196, 197
 - Windows command, 237

V

- view
 - default, 188
- virtualization monitoring, 125
- VM monitoring, 125, 127

W

- Windows services
 - customizing, 109
- WindowsServices category, 207

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

REFERENCE
86 A2 56FA 03