Bull NovaScale 5xx0 & 6xx0

User’s Guide

ORDER REFERENCE
86 A1 94EM 01

Bull NovaScale 5xx0 & 6xx0

User's Guide

Hardware

October 2005

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

ORDER REFERENCE
86 A1 94EM 01

Printed in France

Suggestions and criticisms concerning the form, content, and presentation of this book are invited. A form is provided at the end of this book for this purpose.

To order additional copies of this book or other Bull Technical Publications, you are invited to use the Ordering Form also provided at the end of this book.

Trademarks and Acknowledgements

Preface

Table of Contents

List of Figures

List of Tables

Intended Readers

This guide is intended for use by the Administrators and Operators of NovaScale 5xx0/6xx0 Servers.

Chapter 1. Introducing the Server
describes server hardware components and user environment.

Chapter 2. Getting Started
explains how to connect to and use the server.

Chapter 3. Managing Domains
describes how to perform straightforward server domain management tasks.

Chapter 4. Monitoring the Server
explains how to supervise server operation.

Chapter 5. Tips and Features for Administrators
explains how, as Customer Administrator, you can configure the server to suit your environment.

Appendix A. Specifications

Appendix Error Messages and Recovery Information

Highlighting

The following highlighting conventions are used in this guide:

Bold	Identifies predefined commands, subroutines, keywords, files, structures, buttons, labels, and icons.
Italics	Identifies referenced publications, chapters, sections, figures, and tables.
< >	Identifies parameters to be supplied by the user.

Abbreviations, acronyms and concepts are documented in the *Glossary*.

Related Publications

Site Preparation Guide, 86 A1 87EF
explains how to prepare a Data Processing Center for Bull NovaScale Servers, in compliance with the standards in force. This guide is intended for use by all personnel and trade representatives involved in the site preparation process.

Installation Guide, 86 A1 93EM
explains how to set up and start NovaScale 5xx0/6xx0 Servers for the first time. This guide is intended for use by qualified support personnel.

NovaScale 5000/6000 Series Cabling Guide, 86 A1 34ER
describes server cabling.

Bull 1300H/L & 1100H/L Cabinets, 86 A1 91EM
explains how to install and fit out rack cabinets for Bull NovaScale Servers and peripheral devices.

Bull NovaScale Series Documentation Overview, 86 A2 27EM
describes the hardware, software and online documentation available for Bull NovaScale Servers, related Operating Systems, and licensed programs.

☞ **Note:**
According to server configuration and version, certain features and functions described in this guide may not be accessible. Please contact your Bull Sales Representative for sales information.

Regulatory Specifications and Disclaimers

Declaration of the Manufacturer or Importer

We hereby certify that this product is in compliance with European Union EMC Directive 89/336/EEC, using standards EN55022 (Class A) and EN55024 and Low Voltage Directive 73/23/EEC, using standard EN60950. The product has been marked with the CE Mark to illustrate its compliance.

Safety Compliance Statement

- UL 60950 (USA)
- IEC 60950 (International)
- CSA 60950 (Canada)

European Community (EC) Council Directives

This product is in conformity with the protection requirements of the following EC Council Directives:

Electromagnetic Compatibility

- 89/336/EEC

Low Voltage

- 73/23/EEC

EC Conformity

- 93/68/EEC

Telecommunications Terminal Equipment

- 1999/5/EC

Neither the provider nor the manufacturer can accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product.

Compliance with these directives requires:

- an EC declaration of conformity from the manufacturer
- an EC label on the product
- technical documentation

Federal Communications Commission (FCC) Statement

Note:

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. Neither the provider nor the manufacturer are responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

Any changes or modifications not expressly approved by the grantee of this device could void the user's authority to operate the equipment. The customer is responsible for ensuring compliance of the modified product.

FCC Declaration of Conformity

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Canadian Compliance Statement (Industry Canada)

This Class A digital apparatus meets all requirements of the Canadian Interference Causing Equipment Regulations.

Cet appareil numérique de la classe A est conforme à la norme NMB–003 du Canada.

This product is in conformity with the protection requirements of the following standards:

Electromagnetic Compatibility

- ICES–003
- NMB–003

Laser Compliance Notice

This product that uses laser technology complies with Class 1 laser requirements.

A CLASS 1 LASER PRODUCT label is located on the laser device.

Class 1 Laser Product
Luokan 1 Laserlaite
Klasse 1 Laser Apparat
Laser Klasse 1

Definition of Safety Notices

DANGER
A *Danger* notice indicates the presence of a hazard that has the potential of causing death or serious personal injury.

CAUTION:
A *Caution* notice indicates the presence of a hazard that has the potential of causing moderate or minor personal injury.

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

Electrical Safety

The following safety instructions shall be observed when connecting or disconnecting devices to the system.

DANGER
The Customer is responsible for ensuring that the AC electricity supply is compliant with national and local recommendations, regulations, standards and codes of practice.
An incorrectly wired and grounded electrical outlet may place hazardous voltage on metal parts of the system or the devices that attach to the system and result in an electrical shock.
It is mandatory to remove power cables from electrical outlets before relocating the system.

CAUTION:
This unit has more than one power supply cable. Follow procedures for removal of power from the system when directed.

Laser Safety Information

The optical drive in this system unit is classified as a Class 1 level Laser product. The optical drive has a label that identifies its classification.

The optical drive in this system unit is certified in the U.S. to conform to the requirements of the Department of Health and Human Services 21 Code of Federal Regulations (DHHS 21 CFR) Subchapter J for Class 1 laser products. Elsewhere, the drive is certified to conform to the requirements of the International Electrotechnical Commission (IEC) 60825–1: 2001 and CENELEC EN 60825–1: 1994 for Class 1 laser products.

CAUTION:
Invisible laser radiation when open. Do not stare into beam or view directly with optical instruments.

Class 1 Laser products are not considered to be hazardous. The optical drive contains internally a Class 3B gallium–arsenide laser that is nominally 30 milliwatts at 830 nanometers. The design incorporates a combination of enclosures, electronics, and redundant interlocks such that there is no exposure to laser radiation above a Class 1 level during normal operation, user maintenance, or servicing conditions.

Data Integrity and Verification

Warning:
Bull NovaScale Servers are designed to reduce the risk of undetected data corruption or loss. However, if unplanned outages or system failures occur, users are strongly advised to check the accuracy of the operations performed and the data saved or transmitted by the system at the time of outage or failure.

PAM Writing Rules

Illegal Characters

The following table lists the illegal characters that must not be used in PAM identifiers.

Illegal Characters	
à, é, è, ù, ^, ¨	Accentuated letters
/	Slash
\	Backslash
“	Double quote
’	Simple quote
‘	Inverted comma
&	Ampersand
+	Plus
*	Asterisk
%	Percent
=	Equal sign
<	Less–than sign
>	Greater–than sign
:	Colon
!	Exclamation mark
?	Question mark
;	Semi–colon
,	Comma
~	Tilde
|	Pipe operator
	Space. Use – (dash) or _ (underscore)

Table 1. PAM illegal characters

String Lengths

The following table lists authorized string lengths.

String Type	Length
CellBlock / System Name	16
Scheme Name	32
History Name	64
Archive Name	75 (History Name: + 11 (_JJMMAA_nnn)
LUN Name	32
Switch Name	32
Event Name	32
Description	256 (Scheme: unlimited)
Domain Identity Name	16

Table 2. String length rules

Registry Keys

PAM obtains file paths via 2 registry keys:

- **ReleaseRoot**:
  Contains PAP application file paths (DLL, WEB pages, models,...).
  Two versions of PAM software can be installed and used indifferently on the same machine: each new version is installed in a new directory.
- **SiteRoot**:
  Contains site data file paths.
  Site data remains valid when the PAM software version changes.

Registry keys are generally stored under:
HKEY_LOCAL_MACHINE\SOFTWARE\BULL\PAM

AZERTY/QWERTY Keyboard Lookup Table

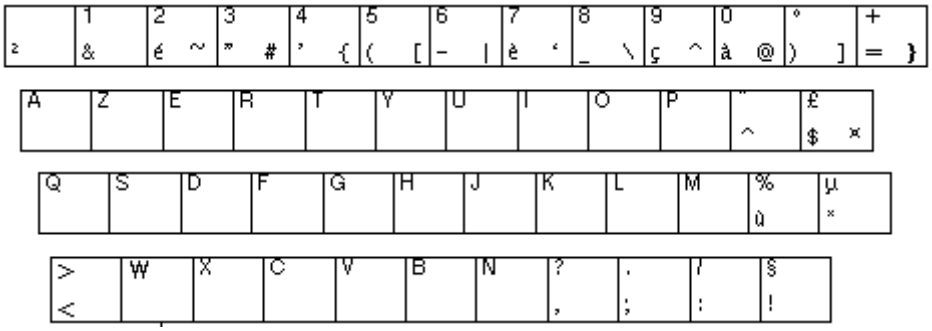


Figure 1. AZERTY keyboard

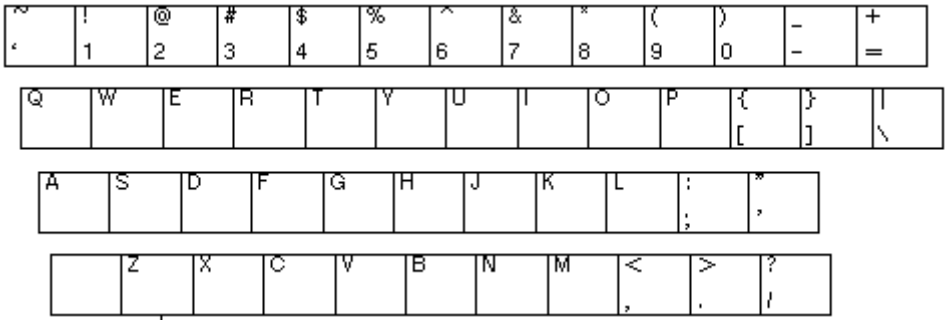


Figure 2. QWERTY keyboard

Administrator's Memorandum

Domains
• Manage Domain Schemes, on page 3-5 • Power ON a Domain, on page 3-14 • Power OFF a Domain, on page 3-18 • Perform a Manual Domain Reset, on page 3-24 • Perform a Domain Force Power OFF, on page 3-21 • Perform a Domain Memory Dump, on page 3-26 • View Domain Functional Status, on page 3-27 • View Domain Power Logs, on page 3-28 • View Domain Powering Sequences, on page 3-29 • View Domain BIOS Info, on page 3-30 • View Domain Request Logs, on page 3-31 • View Domain Configuration, Resources and Status, on page 3-32 • Modify Domain Configuration, on page 3-39* • Solve Incidents, on page 3-69 * Reserved for partitioned servers and extended systems.
Monitoring
• Refresh the PAM Display, on page 4-2 • View CSS Availability Status and System Functional Status, on page 4-4 • View Event Message Status, on page 4-4 • Display Hardware Presence / Functional Status, on page 4-5 • View PAM Web Site User Information, on page 4-11 • View PAM Version Information, on page 4-12 • View Server Hardware Status, on page 4-13 • Use the Hardware Search Engine, on page 4-9 • Display Detailed Hardware Information, on page 4-15 • Exclude / Include Hardware Elements, on page 4-25 • Manage PAM Event Messages, History Files, Archives, Fault Lists, on page 4-28 • Understand Message Severity Levels, on page 4-29 • View, Acknowledge WEB Event Messages, on page 4-31 • Sort and Locate Messages, on page 4-32 • Solve Incidents, on page 4-39 • Create an Action Request Package, on page 4-47 • Create a Custom Package, on page 4-48

Configuration

* Reserved for partitioned servers and extended systems.

Operator’s Memorandum

Domains
• Power ON a Domain, on page 3-14 • Power OFF a Domain, on page 3-18 • Perform a Domain Force Power OFF, on page 3-21 • Perform a Manual Domain Reset, on page 3-24 • Perform a Domain Memory Dump, on page 3-26 • View Domain Functional Status, on page 3-27 • View Power Logs, on page 3-28 • View Domain Powering Sequences, on page 3-29 • View BIOS Info, on page 3-30 • View Domain Request Logs, on page 3-31 • View Domain Configuration, Resources and Status, on page 3-32 • Solve Incidents, on page 3-69
Histories
• Manage PAM Event Messages, History Files, Archives, Fault Lists, on page 4-28 • Understand Event Message and History Severity Levels, on page 4-29 • Sort and Locate messages, on page 4-32
Status
• Check System Functional Status, on page 4-4 • Check CSS Availability, on page 4-4 • View, Acknowledge WEB Event Messages, on page 4-31 • Sort, Locate WEB event messages, on page 4-32

Chapter 1. Introducing the Server

This chapter describes the main hardware components and user environment for NovaScale 5xx0/6xx0 Servers. It includes the following topics:

Note:
Customer Administrators and Customer Operators are respectively advised to consult the *Administrator's Memorandum*, on page xxviii or the *Operator's Memorandum*, on page xxx for a detailed summary of the everyday tasks they will perform.

For further information about user accounts and passwords, see *Setting up PAP Unit User*s, on page 5-17.

Bull NovaScale Server Overview

Bull NovaScale Servers for business and scientific applications are based upon the FAME architecture (Flexible Architecture for Multiple Environments), leveraging the latest generation of Intel® Itanium® 2 processors.

NovaScale 5xx0 Servers are designed to operate as single SMP systems and are delivered with one pre–configured domain englobing all the hardware and software resources managed by the Operating System.

NovaScale 6xx0 Servers are designed to operate as one, two, three or four hardware–independent SMP systems or domains, each running an Operating System instance and a specific set of applications.

According to version, servers are delivered rack–mounted and ready–to–use in high or low cabinets.

Figure 3. Bull NovaScale Server cabinets

Dynamic Partitioning

Bull NovaScale 6000 Series servers can be dynamically partitioned into physically independent ccNUMA (Cache Coherent Non Uniform Memory Access) SMP systems or domains, each running an Operating System instance and a specific set of applications.

Extended Configurations

Several Bull NovaScale Servers may be administered through a single instance of PAM software.

Cluster Configurations

Several Bull NovaScale Servers may be grouped to act like a single system, enabling high availability, load balancing and parallel processing.

Server Features

The main features of Bull NovaScale Servers are:

Intel® Itanium® Processor Family architecture:

- Modularity, predictable performance and growth

High availability:

- Component redundancy
- Capacity to isolate or replace a faulty component without service disruption
- Global and unified system visibility
- Round–the–clock operation

Scalability:

- Dynamic partitioning
- Power on demand : capacity to dynamically adapt resources to load requirement

Simultaneous support of multiple environments:

- Microsoft® Windows® Server
- Linux®

High performance computing capabilites:

- Technical and scientific applications:
  - High Performance Computing (HPC)
- Business Intelligence:
  - Datawarehousing
  - Datamining
- Large enterprise applications:
  - ERP
  - CRM
  - SCM ...
- Large database applications for Internet transactions.
- Large business sector applications:
  - Online billing
  - Online reservations
  - Online banking ...

Built–in Platform Administration and Maintenance (PAM) software suite:

- Proactive administration
- Optimization of resources
- Automatic generation of corrective actions and calls to support centers
- Dynamic configuration

Bull NovaScale Master System Management (NSM) software suite:

- Windows, Linux, and Platform management
- Monitoring, Information, Control, and Event Handling
- Client / Server / Agent architecture
- WEB standard OpenSource solutions

Server Hardware

Note:
Abbreviations and acronyms are documented in the *Glossary*.

Main server hardware components are:

Central SubSystem Module (CSS Module)

The CSS Module houses core hardware components:

- 2 or 4 QBBs
- 1 or 2 IOBs
- 1 or 2 IORs
- 1 PMB
- 1 MPB
- 4 DPS units

Notes:

- The NovaScale 6xx0 Server CSS Module can be logically divided into two **Cells**, each with one or two QBBs and one IOB, to allow dynamic partitioning.
- The NovaScale 6320 Server is equipped with two inter–connected CSS modules.

Quad Brick Block (QBB)

The QBB is equipped with 1 to 4 Itanium 2 processors and 16 DDR DIMMs. The QBB communicates with the rest of the system the high–speed bidirectional link **Scalability Port Switches (SPS)** located on the Midplane.

IO Board (IOB)

The IOB provides 4 PCI–X bridges for the connection of up to 11 PCI–X boards, and a PCI Hot Plug Board (PHPB). The IOB communicates with the rest of the system through the high–speed bidirectional link **Scalability Port Switches (SPS)** located on the Midplane.

IO Riser (IOR)

The IOR is an IOB daughter board providing legacy IO connections: 2 USB ports, 1 LAN port, 2 serial ports, 1 video port, and 1 CD/DVD Rom drive.

Platform Maintenance Board (PMB)

The PMB concentrates logistics access and links the platform to the Platform Administration Processor (PAP Unit) running Platform Administration and Maintenance (PAM) software.

Midplane (MPB)

The MPB houses the high–speed directional link **Scalability Port Switch (SPS)**. The MPB is divided into two physical **Cells**, each capable of connecting 2 QBBs and 1 IOB, which communicate with the rest of the system through the SPS. The MPB also houses the system clock and connects all other system boards.

Distributed Power Supply (DPS) Unit

Each DPS Unit supplies 48V AC/DC power to the server. Each CSS module is equipped with 4 DPS units for full redundancy.

Platform Administration Processor (PAP) Unit

The PAP Unit hosts all server administration software, in particular Platform Administration and Maintenance (PAM) software.

KVM Switch

The KVM Switch allows the use of a single keyboard, monitor and mouse for the local server domains and the local PAM console.

Console

The Console contains the keyboard, monitor and touch pad / mouse used for local access to the server domains and to the PAP Unit.

Disk Subsystem

A SCSI RAID or FC disk subsystem is required for OS disk partitions.

Additional Peripherals

Additional peripherals such as disk subsystems, storage area networks, communication networks, archiving peripherals etc. can be connected to the server via PCI adapters located in the IOBs. Such peripherals may either be rack–mounted in the server cabinet (if free space is available) or in external cabinets.

Server Firmware and Software

Operating Systems (OS)

The server is certified for the following Operating Systems:

- Windows Server 2003, Enterprise Edition
- Windows Server 2003, Datacenter Edition
- Linux Red Hat Enterprise Linux Advanced Server
- Novell SUSE

BIOS

The BIOS controls the server startup process, dynamic resource allocation (Domain reconfiguration, hot–plugging), and error handling. The BIOS also includes:

- The **Extended Firmware Interface (EFI)**, which provides the OS with system services.
- The **EFI Shell**, an autonomous environment used to run Off–line Test & Diagnostic suites.

Platform Administration and Maintenance (PAM) suite

The PAM Web–based software suite is used to operate, monitor, and configure the server. PAM can be accessed locally or remotely through Microsoft Internet Explorer or Mozilla browsers, under the protection of appropriate access rights. PAM provides the administration functions needed to manage and maintain the server:

- Domain configuration and resource allocation
- Alert or maintenance requests to the Customer Service Center
- Error logging …

Test & Diagnostics suites

The server is delivered with the following T & D suites:

- Online Test & Diagnostic suite
- Offline Test & Diagnostic suite
- Power–On Self–Test suite

NovaScale Master (NSM) Management suite

The NSM software suite allows you to monitor and manage NovaScale Windows and Linux systems.

Conformance to Standards

Intel

Bull NovaScale Servers conform to all Intel platform standards:

- ACPI (Advanced Configuration and Power Interface)
- IPMI (Intelligent Platform Management Interface)
- EFI (Extended Firmware Interface)
- SMBIOS (System Management BIOS)
- DIG64 (Developer Interface Guide for Intel Itanium Architecture)

Windows

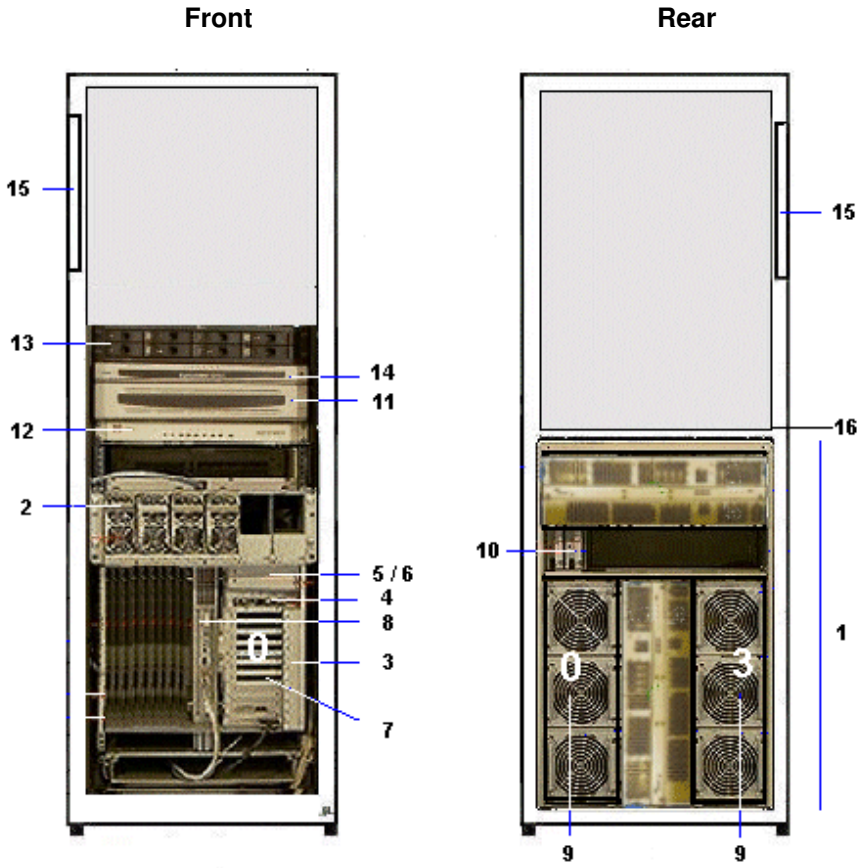
Bull NovaScale Servers conform to the standards set out in the Windows Hardware Design Guide.

Getting to Know the Server

NovaScale 5080 Server

Note:
Server components and configuration may differ according to the version chosen.

The server is delivered rack–mounted and pre–cabled in a high cabinet, containing the following components:



1	CSS module with midplane, redundant power supply and AC power cable			11	Console drawer with monitor, keyboard and mouse
	2	DPS units		12	KVM switch
	3	1 or 2 IOB (s) with:		13	1 or two SCSI or FC disk rack(s) with RAID controller(s) and disks
		4	IOR	14	PAP unit with CD–ROM drive, FDD and disk(s)
		5	LS240 disk drive (optional)	15	PDU with AC power cable
				16	Ethernet hub with power bar (FC disk rack)
		6	DVD / CD–ROM drive	**Dual IOB configuration:** – IOB #0 = Master – IOB #1 = Slave **NovaScale 5080 Server configuration:** – QBB #0 and QBB #3	
		7	PCI hot plug board (11 slots)		
	8	PMB			
	9	1 or 2 QBB subsets with fan boxes			
	10	SPS fan boxes			

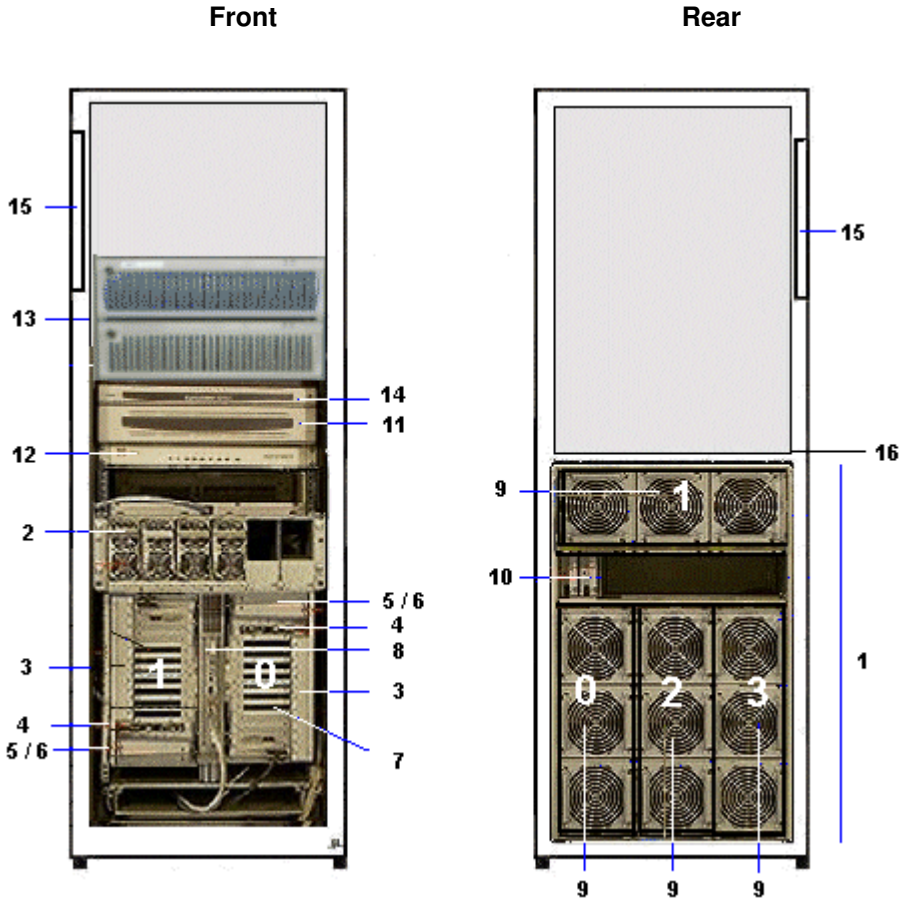
Figure 4. NovaScale 5080 Server components (example)

Note:
Abbreviations and acronyms are documented in the *Glossary*.

NovaScale 5160 Server

Note:
Server components and configuration may differ according to the version chosen.

The server is delivered rack–mounted and pre–cabled in a high cabinet, containing the following components:



1	CSS module with midplane, redundant power supply and AC power cable			11	Console drawer with monitor, keyboard and mouse
	2	DPS units		12	KVM switch
	3	1 or 2 IOB (s) with:		13	1 or two SCSI or FC disk rack(s) with RAID controller(s) and disks
		4	IOR	14	PAP unit with CD–ROM drive, FDD and disk(s)
		5	LS240 disk drive (optional)	15	PDU with AC power cable
				16	Ethernet hub with power bar (FC disk rack)
		6	DVD / CD–ROM drive	**Dual IOB configuration:** – IOB #0 = Master – IOB #1 = Slave **NovaScale 5160 Server configuration:** – QBB #0, QBB #1, QBB #2, and QBB #3	
		7	PCI hot plug board (11 slots)		
	8	PMB			
	9	1 up to 4 QBB subsets with fan boxes			
	10	SPS fan boxes			

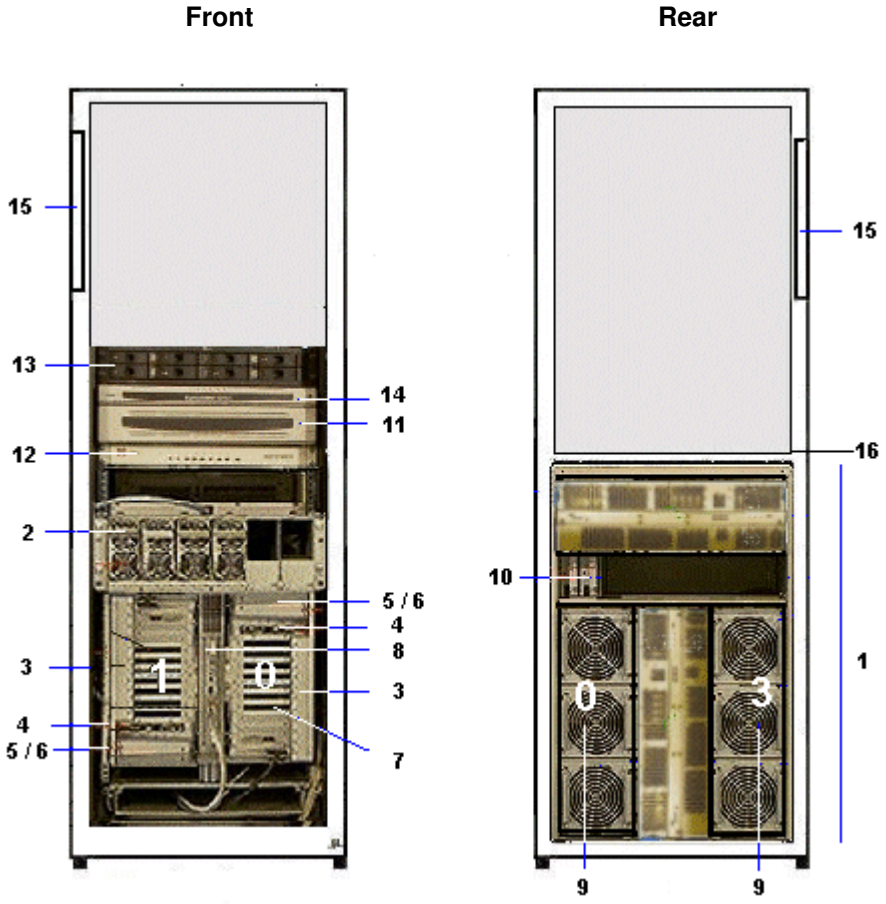
Figure 5. NovaScale 5160 Server components (example)

Note:
Abbreviations and acronyms are documented in the *Glossary*.

NovaScale 6080 Server

Note:
Server components and configuration may differ according to the version chosen.

The server is delivered rack–mounted and pre–cabled in a high cabinet, containing the following components:



1	CSS module with midplane, redundant power supply and AC power cable			11	Console drawer with monitor, keyboard and mouse
	2	DPS units		12	KVM switch
	3	2 IOB (s) with:		13	1 or two SCSI or FC disk rack(s) with RAID controller(s) and disks
		4	IOR	14	PAP unit with CD–ROM drive, FDD and disk(s)
		5	2 USB ports	15	PDU with AC power cable
				16	Hub with power bar
		6	DVD / CD–ROM drive	**NovaScale 6080 configuration:** – QBB #0 and QBB #3	
		7	PCI hot plug board (11 slots)		
	8	PMB			
	9	2 QBBs with fan boxes			
	10	SPS fan boxes			

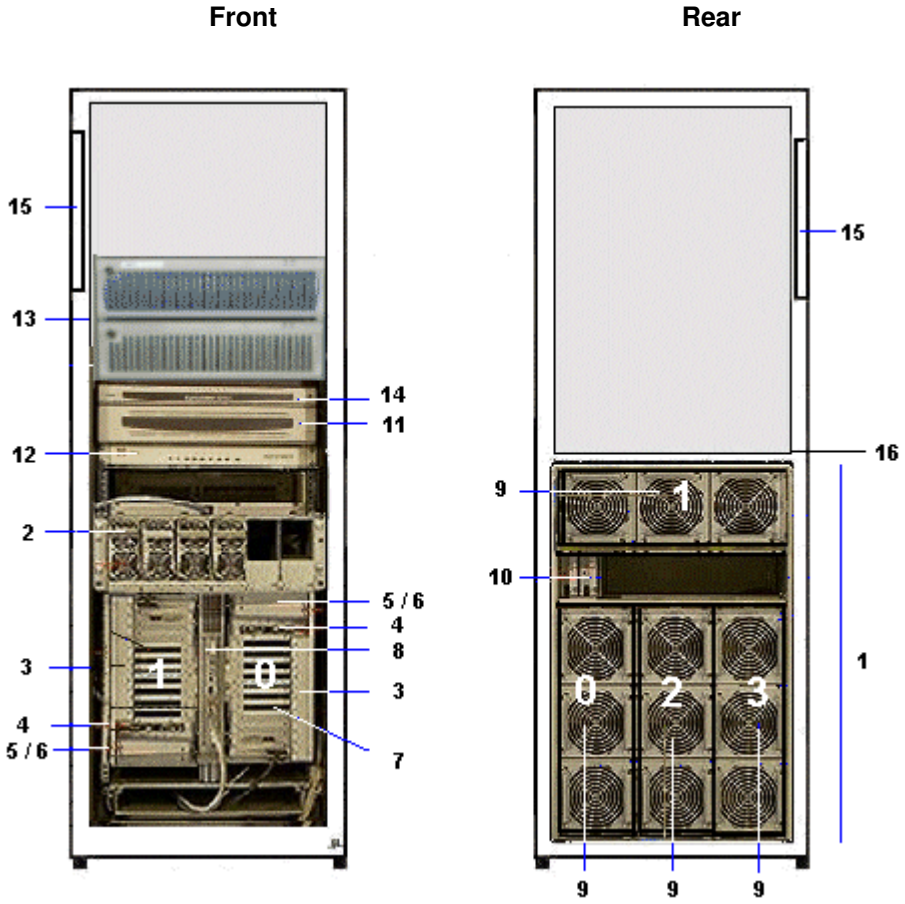
Figure 6. NovaScale 6080 Server components (example)

Note:
Abbreviations and acronyms are documented in the *Glossary*.

NovaScale 6160 Server

Note:
Server components and configuration may differ according to the version chosen.

The server is delivered rack–mounted and pre–cabled in a high cabinet, containing the following components:



1	CSS module with midplane, redundant power supply and AC power cable			11	Console drawer with monitor, keyboard and mouse
	2	DPS units		12	KVM switch
	3	2 IOB (s) with:		13	1 or two SCSI or FC disk rack(s) with RAID controller(s) and disks
		4	IOR	14	PAP unit with CD–ROM drive, FDD and disk(s)
		5	2 USB ports	15	PDU with AC power cable
				16	Hub with power bar
		6	DVD / CD–ROM drive	**NovaScale 6160 configuration:** – QBB #0, QBB #1, QBB #2, and QBB #3	
		7	PCI hot plug board (11 slots)		
	8	PMB			
	9	4 QBBs with fan boxes			
	10	SPS fan boxes			

Figure 7. NovaScale 6160 Server components (example)

Note:
Abbreviations and acronyms are documented in the *Glossary*.

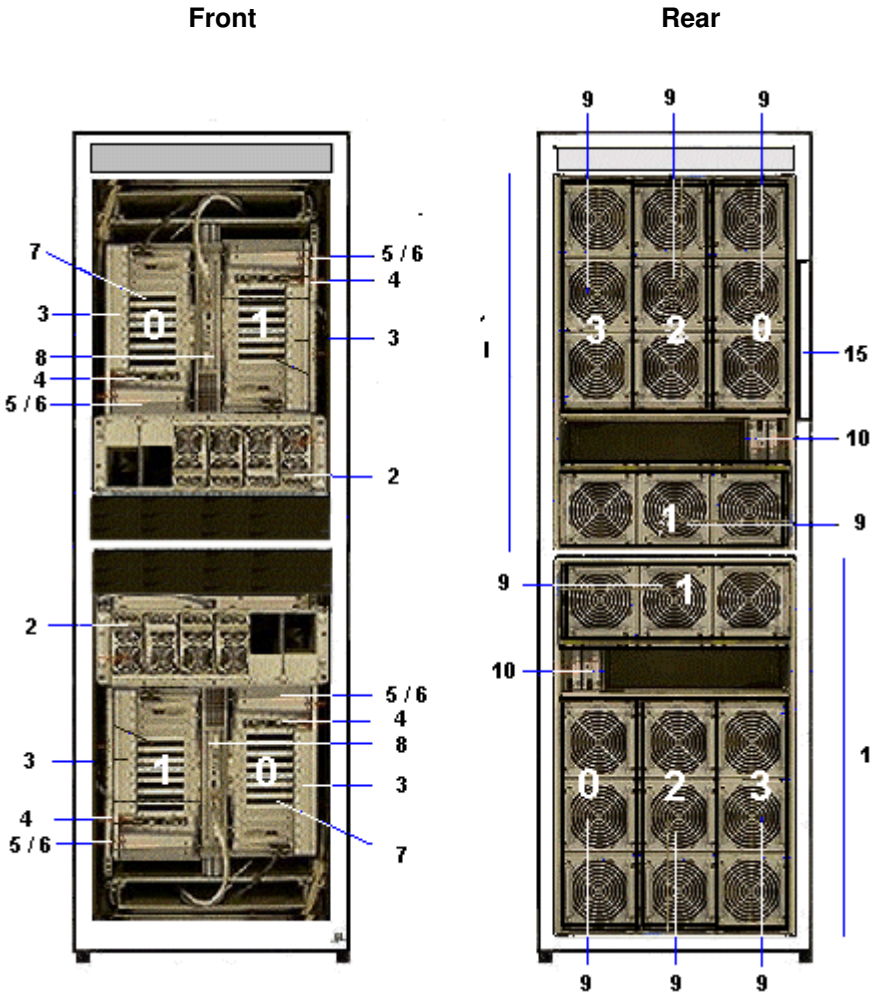
NovaScale 6320 Server

Note:
Server components and configuration may differ according to the version chosen.

The server is delivered rack–mounted and pre–cabled in a high cabinet, containing the following components:

Main Cabinet

The main cabinet contains the following components:



1	2 CSS modules, each with midplane, redundant power supply and AC power cable			8	PMB
	2	DPS units		9	1 to 4 QBBs with fan boxes
	3	1 or 2 IOB (s) with:		10	SPS fan boxes
		4	IOR	15	PDU with AC power cable
		5	2 USB ports	**NovaScale 53206320 configuration:** – QBB #0, QBB #1, QBB #2, and QBB #3 Module 0 – QBB #0, QBB #1, QBB #2, and QBB #3 Module 1	
		6	DVD / CD–ROM drive		
		7	PCI hot plug board (11 slots)		

Figure 8. NovaScale 6320 Server main cabinet components (example)

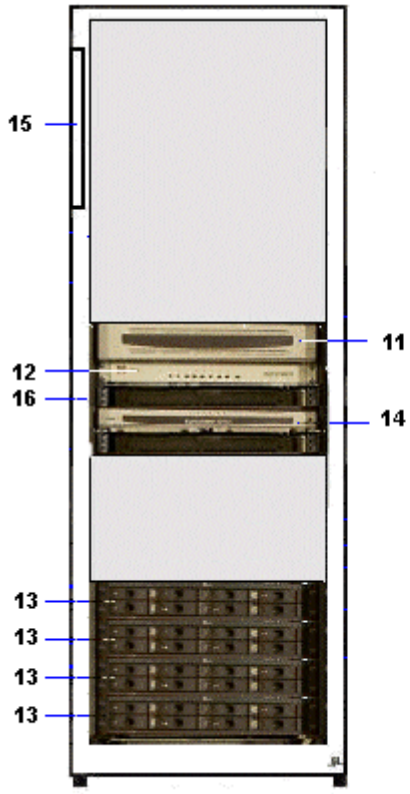
Note:
Abbreviations and acronyms are documented in the *Glossary*.

I/O Cabinet

The I/O cabinet contains the following components:

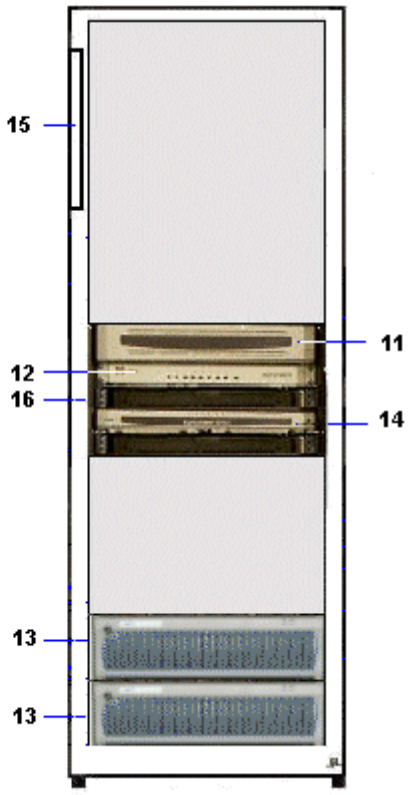
I/O cabinet with SCSI disks

Front



I/O cabinet with FC disks

Front



11	Console drawer with monitor, keyboard and mouse
12	KVM switch
13	1 up to 4 SCSI disk rack(s) with RAID controller(s) and disks, or 1 or two FC disk rack(s) with RAID controller(s) and disks
14	PAP unit with CD–ROM drive, FDD and disk(s)
15	PDU with AC power cable
16	Hub with power bar

Figure 9. NovaScale 6320 Server I/O cabinet components (examples)

Note:
Abbreviations and acronyms are documented in the *Glossary*.

Server Components

Central Subsystem (CSS) Module

The CSS Module houses main hardware components. The NovaScale 5080/5160 Server and the NovaScale 6080/6160 Server are equipped with one CSS module, located at the bottom of the cabinet. The NovaScale 6320 Server is equipped with two CSS modules, located at the top and bottom of the main cabinet.

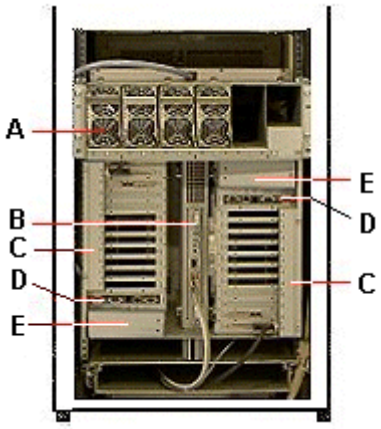
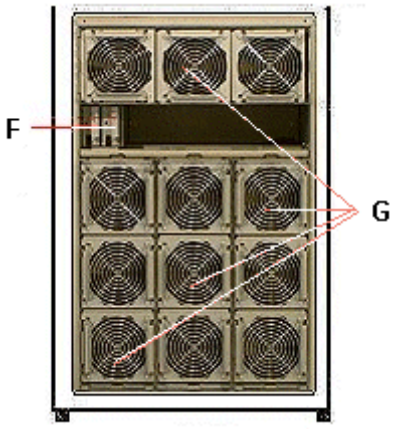
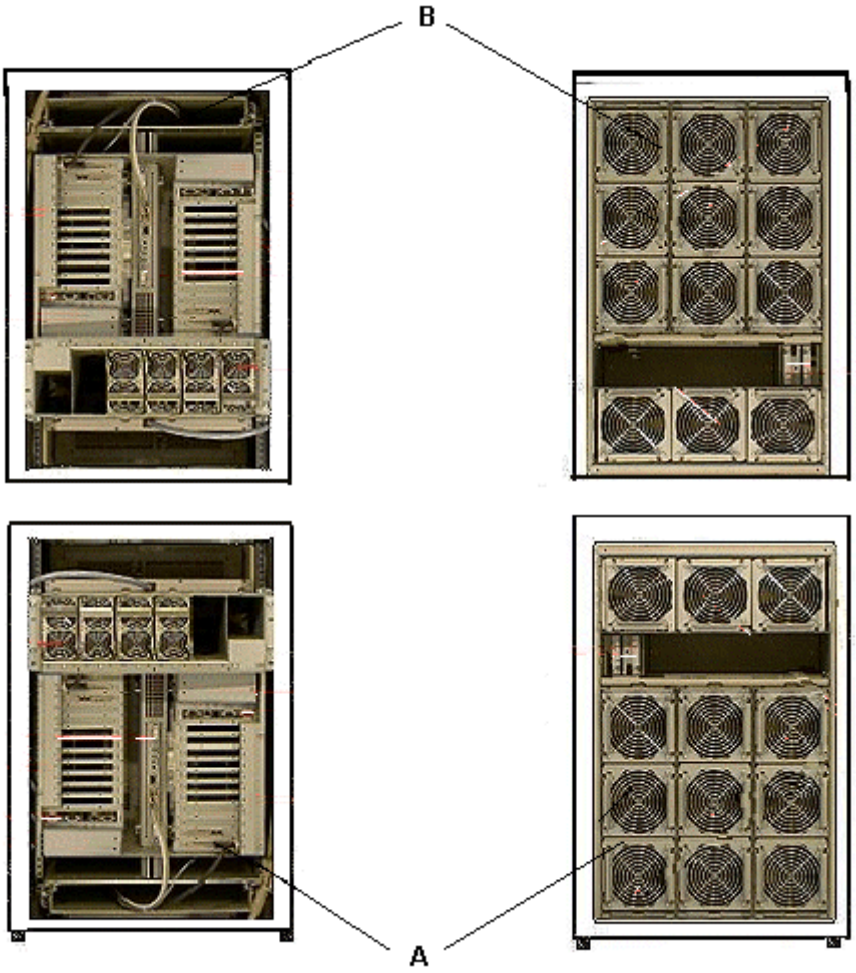
Front view	Rear view
	
(A): 2 to 6 DPSs (Distributed Power Supply: **(B): PMB (Platform Management Board)**: This active board links the server to the Platform Administration Processor (PAP) Unit (via an Ethernet link). **(C): IOBs (Input / Output Box)**: Each IOB box houses: • 1 IOB (Input / Output Board) • 1 PHPB (PCI Hot Plug Board) • 11 hot–plug PCI–X (100–133 MHz) slots with optional: – 1 SCSI HBA – 1 PCI SCSI card – 1 PCI FC card – 1 PCI Giga Ethernet card – 8 free slots • **(D):** 1 IOR (Input / Output Riser): – 2 A–type USB ports • 1 RJ45 10/100 Mbps Ethernet port – 2 DB9–M RS232 serial ports – 1 HD15–F VGA port • **(E):** 1 DVD/CD–ROM drive • 1 LS240 drive (optional) Each IOB is cooled by the corresponding QBB fan box.	**(F): 2 SPS fan boxes** Each Midplane is equipped with two redundant fan boxes for cooling. **(G): 1, 2, 3 or 4 QBB fan boxes**: Each QBB subset is equipped with a fan box for cooling. **(G): 1, 2, 3 or 4 QBB subsets**: Each QBB subset houses: • 1 mother board • 2 memory boards • 4 processors • 16 DIMMs **1 MidPlane (MP)** This active board is used to interconnect the QBBs, IOBs and the PMB.

Figure 10. CSS module features (full CSS module example)

NovaScale 6320 Server CSS Modules



A: Module 0, B: Module 1

Figure 11. CSS modules (NovaScale 6320 Server example)

Note:
See Figure 10 for CSS module details.

Integrated Platform Administration Processor (PAP) Unit

Warning:
The PAP unit has been specially configured for Bull NovaScale Server administration and maintenance. NEVER use the PAP unit for other purposes and NEVER change PAP unit configuration unless instructed to do so by an authorized Customer Service Engineer.

The PAP unit is linked to the server via the Platform Management Board (PMB). It hosts Platform Administration Software (PAM). According to version, the PAP unit is located in the center of a high cabinet or at the top of a low cabinet.

Or

PAP Unit 1U	PAP Unit 2U
• 1 P4C / 3 GHz PC – 1 GB RAM – 2 x 80 GB SATA disks (RAID1) – 1 CD/DVD–ROM drive – 1 1 FDD – 2 serial ports – 1 parallel port – 3 PCI slots – 2 Gigabit Ethernet ports (1 free) – 3 USB 2.0 ports (1 front + 2 rear) – 1 SVGA video port – 2 PS/2 ports	• 1 P4C / 2.6 GHz PC – 1 GB RAM – 2 x 80 GB SATA disks (RAID1) – 1 free disk slot – 1 CD/DVD–ROM drive – 1 FDD – 2 serial ports – 1 parallel port – 3 PCI slots – 2 Gigabit Ethernet ports (1 free) – 3 USB 2.0 ports (1 front + 2 rear) – 1 SVGA video port – 2 PS/2 ports
• Microsoft Windows operating system • Internet Explorer software • PAM software • 1 power cable	

Figure 12. PAP unit

Integrated Console

According to version, the integrated console is located in the center of a high cabinet or at the top of a low cabinet.

The Integrated Console contains the keyboard, monitor and touch pad used for local access to the server and to the Platform Administration Processor (PAP) Unit.

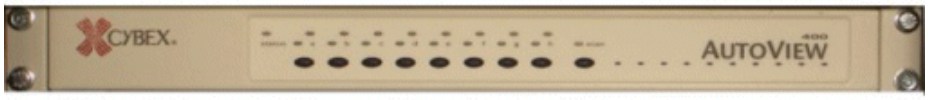
- 1 monitor
- 1 QWERTY keyboard and touch pad
- 1 power cable

Figure 13. Integrated Console features

Keyboard / Video / Mouse (KVM) Switch

The KVM Switch allows the use of the integrated console for the local server and the local Platform Administration and Maintenance console.

8–Port KVM Switch



Or

- 8 ports
- 1 power cable

Figure 14. 8–port KVM switch features

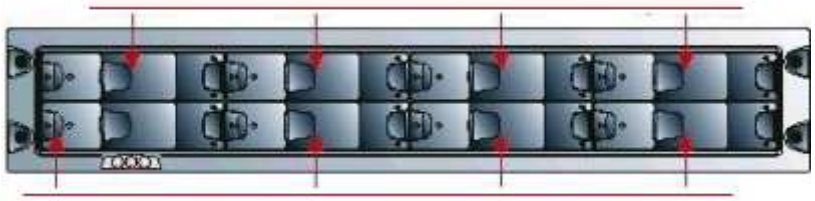
16–Port KVM Switch

- 16 ports
- 1 power cable

Figure 15. 16–port KVM switch features

SR–0812 SCSI RAID / SJ–0812 SCSI JBOD Disk Racks

SR–0812 SCSI RAID / SJ–0812 SCSI JBOD Disk Racks are delivered with pre–installed system disks (two RAID#1 and one spare disk per domain). Empty slots can be used for data disks. According to version, the Disk Rack is located in the main or I/O cabinet.

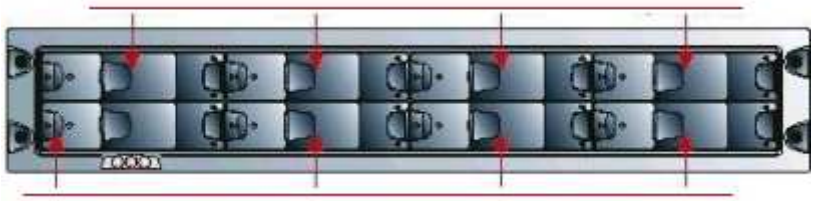


- 8 slots
- 1 RAID controller card
- 3 disks per domain (2 RAID#1 + 1 spare)
- 2 power cables (redundant power supply)

Figure 16. SR–0812 SCSI RAID / SJ–0812 SCSI JBOD disk rack features

SJ–0812 SCSI JBOD Extension Disk Rack

The SJ–0812 SCSI JBOD Extension Disk Rack offers eight empty slots for Customer data disks. According to version, the Extension Disk Rack is located in the main or I/O cabinet.



- 8 slots
- 2 power cables (redundant power supply)

Figure 17. SJ–0812 SCSI JBOD extension disk rack features

FDA 1x00 FC Disk Rack

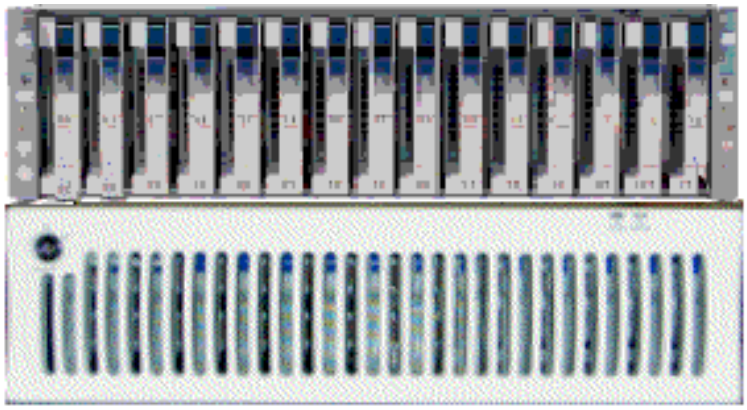
The FDA 1x00 FC Disk Rack is delivered with pre–installed system disks (two RAID#1 and one spare disk per domain). Empty slots can be used for data disks. According to version, the Disk Rack is located in the main or I/O cabinet.

- 15 slots
- 2 FC RAID controller cards, 1 FC port per controller
- 3 disks per domain (2 RAID#1 + 1 spare)
- 2 power cables (redundant power supply)

Figure 18. FDA 1x00 FC disk rack features

FDA 2x00 FC Disk Rack

The FDA 2x00 FC Disk Rack is delivered with pre–installed system disks (two RAID#1 and one spare disk per domain). Empty slots can be used for data disks. According to version, the Disk Rack is located in the main or I/O cabinet.



- 1 controller unit & 1 disk unit
- 15 slots
- 2 FC RAID controller cards, 2 FC ports per controller
- 3 disks per domain (2 RAID#1 + 1 spare)
- 2 power cables (redundant power supply)

Figure 19. FDA 2x00 FC disk rack features

FDA 1x00 FC Extension Disk Rack

The FDA 1x00 FC Extension Disk Rack offers15 empty slots for data disks. According to version, the Disk Rack is located in the main or I/O cabinet.

- 15 slots
- 2 power cables (redundant power supply)

Figure 20. FDA 1x00 FC extension disk rack features

Ethernet Hub

The optional Maintenance LAN Ethernet Hub is used to connect PMB, PAP Unit and external FDA FC Disk Rack Ethernet ports.

Ethernet Hub	– 8 ports – 1 power cable – 1 power bar

Figure 21. Ethernet hub features

USB Modem

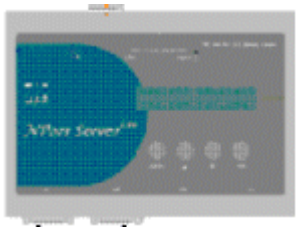
The optional USB modem is used to transmit Autocalls to the Remote Maintenance Center, if your maintenance contract includes the Autocall feature.

USB Modem	– 1 USB cable – 1 RJ11 cable

Figure 22. USB modem features

NPort Server

The Nport Server is used connect the administration port of the SR–0812 SCSI RAID disk rack to the PAP Unit.



NPort Server	– 2 DB9 to Jack cable – 1 RJ45 – RJ45 Ethernet cable

Figure 23. NPort Server features

Power Distribution Unit (PDU)

The PDU supplies mains power to the PAP unit, the external Disk Rack, the KVM Switch, the Integrated Console, and the Ethernet Hub. When the server is equipped with an FDA 1x00 FC or an FDA 2x00 FC, the PDU also supplies mains power to the Power Bar. The PDU is located in the top left part of the cabinet.According to version, the PDU is located in the top left part of the main or I/O cabinet.

Front **Rear**

- 6 (8A) sockets (front):
- 2 (1A) sockets (rear):
- 1 (20A) power cable

Figure 24. PDU features

Accessing Server Components

During normal operation, cabinet components can be accessed from the front. Customer Service Engineers may also remove the rear and side covers for certain maintenance operations.

Important:
Optimum cooling and airflow is ensured when the cabinet door is closed.

Opening the Front Door

Tools Required:

- Cabinet key

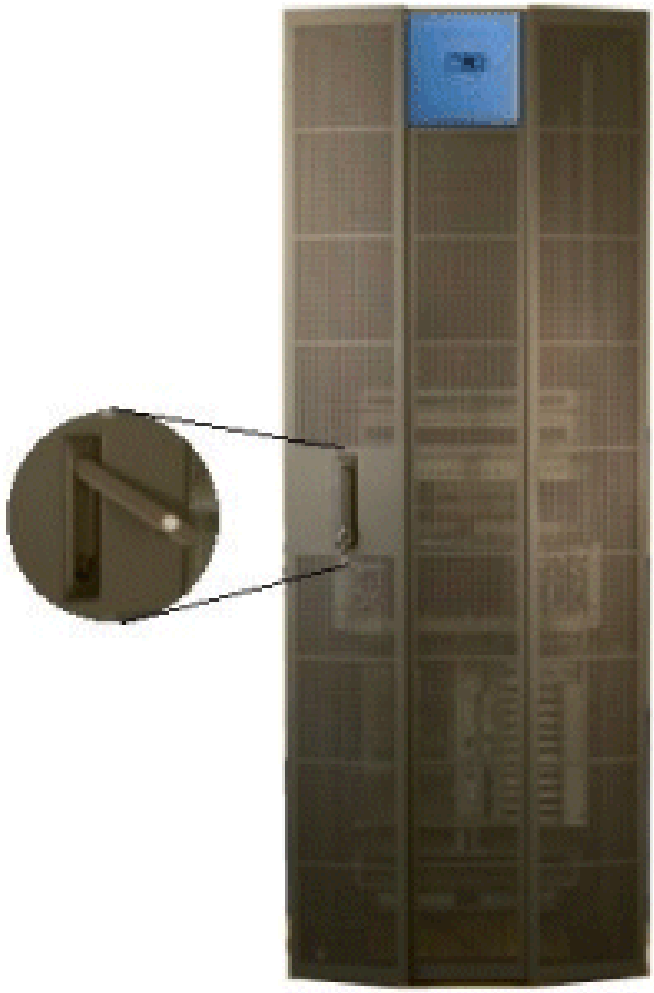


Figure 25. Opening the front door

1. Unlock the front door with the key.
2. Pull out the locking mechanism and turn to open.
3. Open the door as required.

Closing the Front Door

1. Close the door.
2. Turn the locking mechanism to close and push back into place.
3. Lock the front door with the key.

Opening / Closing the Integrated Console

The server is equipped with an integrated console for local administration and maintenance operations.

Figure 26. Integrated console

To open the integrated console:

1. Slide the console forward until it clicks into place.
2. Use the front bar to lift the screen panel into position.

To close the integrated console:

1. Press the 2 buttons marked PUSH on either side of the keyboard panel to release the console.
2. Lower the front bar to close the screen panel.
3. Slide the console back into the cabinet.

Bull NovaScale Server Resources

Note:
According to server configuration and version, certain features and functions described in this guide may not be accessible. Please contact your Bull Sales Representative for sales information.

System Resource and Documentation CD–Roms

The Bull NovaScale Server System Resource and Documentation CD–Roms contain all the firmware and documentation referred to in this guide.

PAM Software Package

The Bull NovaScale Server is equipped with an integrated Platform Administration and Maintenance software package, otherwise known as the PAM software package.

One part of PAM software is an embedded application (MAESTRO) running on the Platform Management Board(s) (PMB) and the other is an external application (PAM Kernel / Web User Interface) running on the Platform Administration Processor (PAP) unit under Microsoft Windows.

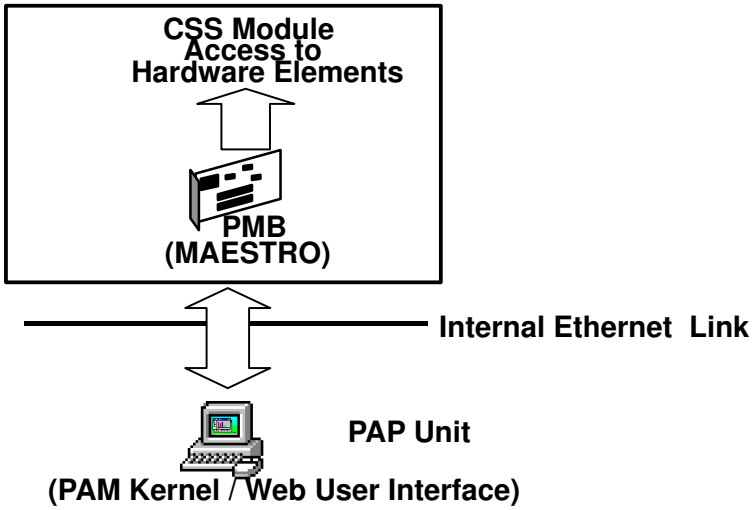


Figure 27. PAM software deployment

The PAM Web–based administration and maintenance tools give you immediate insight into system status and configuration. You will use PAM software to operate, monitor, and configure your Bull NovaScale Server.

As soon as your system is connected to the power supply, the PAP unit running Microsoft Windows and PAM software also powers up. For further information about connecting to PAM, see *Connecting to the PAM Web Site*, on page 2-2.

PAP Unit Mirroring and Failover Policy

Most configuration, administration, and maintenance activities are carried out from the PAP unit. To ensure a high level of data integrity and availability, the PAP unit is equipped with two extractable mirrored disks. Mirroring writes and updates data across both disks, creating a single logical volume with completely redundant information on each disk. If one disk fails, it can be replaced without losing data.

Note:
For enhanced data integrity and availability, the PAP unit can be equipped with a third disk. Contact your Customer Representative for details.

EFI Utilities

The Bull NovaScale Server EFI utilities provide a complete set of configuration, operation, and maintenance tools:

- EFI driver,
- EFI Shell,
- EFI system utility,
- EFI system diagnostic,
- Operating System loader.

For further details, see Chapter 5. *Tips and Features for Administrators*.

Chapter 2. Getting Started

This chapter explains how to connect to and start server domains. It includes the following topics:

Note:
Customer Administrators and Customer Operators are respectively advised to consult the *Administrator's Memorandum*, on page xxviii or the *Operator's Memorandum*, on page xxx for a detailed summary of the everyday tasks they will perform.

For further information about user accounts and passwords, see *Setting up PAP Unit User*s, on page 5-17.

Connecting to the PAM Web Site

The server is equipped with an integrated Platform Administration and Maintenance software package, otherwise known as PAM software. One part of PAM software is an embedded application (MAESTRO) running on the Platform Management Board (PMB) and the other is an external application running on the Platform Administration Processor (PAP) unit under Microsoft Windows.

The PAM Web–based administration and maintenance tools give you immediate insight into system status and configuration. You will use PAM software to operate, monitor, and configure your server.

Notes:
Local and remote access rights to the PAP unit and to the PAM Web site must be configured by the Customer Administrator. For further details, refer to the Microsoft Windows documentation and to *Setting up PAP Unit Users*, on page 5-17.
Customer Administrator rights are required for all PAM configuration tasks.

Connecting to the PAM Web Site from the Local / Integrated Console

CAUTION:
Access to the local / integrated console should be restricted to Customer / Support Administrators and Operators ONLY to avoid inadvertent damage to software and/or hardware components.

1. Check that the KVM switch is set to the **PAP Unit** port. See *Toggling the Local / Integrated Console Display*, on page 2-9.
2. From the PAP unit Microsoft Windows desktop, double–click the PAM icon (**http://localhost/PAM**).
3. When prompted, enter the appropriate Administrator or Operator **User Name** and **Password**. The PAM home page appears.

Connecting to the PAM Web Site from a Remote Computer/Workstation

The PAM Software utility can be accessed from any PC running Microsoft Windows with the Internet Explorer (6 or later) browser installed and/or from any workstation running Linux with the Mozilla (1.6 or later) browser installed.

Important:
Before connecting to PAM from a remote computer, you are advised to disconnect from your local Windows session on the PAP unit by clicking Start → Log Off.

If Pop–up Blocker is turned on in your Web Browser, you MUST add the PAM Web site to the list of allowed sites.

Do NOT use the Mozilla browser on the PAP unit.

Enabling Remote Access to the PAM Web Site with Internet Explorer

1. From the remote computer, configure Internet Explorer to connect directly to the PAM Web site:
   a. From the Internet Explorer main menu bar, click **Tools** → **Internet Options**.
   b. Under the **General** tab, type the PAM Web site URL defined during the PAP installation procedure in the **Home Page Address** field:
   http://*<PAPname>*/pam
   (where ***<PAPname>*** is the name allocated to the PAP unit during setup).
   c. Click **Advanced** → **Restore Defaults** to validate default settings.
   d. Save your changes and close Internet Explorer.
2. Launch Internet Explorer to connect directly to the PAM web site.
3. When prompted, enter the appropriate Administrator or Operator **User Name** and **Password**. The PAM home page appears.

Enabling Remote Access to the PAM Web Site with Mozilla

1. From the remote computer, configure Mozilla to connect directly to the PAM Web site:
   a. From the Mozilla main menu bar, select **Edit** → **Preferences** → **Navigator**.
   b. Select the **Home Page** checkbox and enter the PAM Web site URL defined during the PAP installation procedure in the location field:
   http://*<PAPname>*/pam
   (where ***<PAPname>*** is the name allocated to PAP unit during setup).
   c. Select the **Restore Defaults** checkbox to validate default settins.
   d. Save your changes and close Mozilla.
2. Launch Mozilla to connect directly to the PAM web site.
3. When prompted, enter the appropriate Administrator or Operator **User Name** and **Password**. The PAM home page appears.

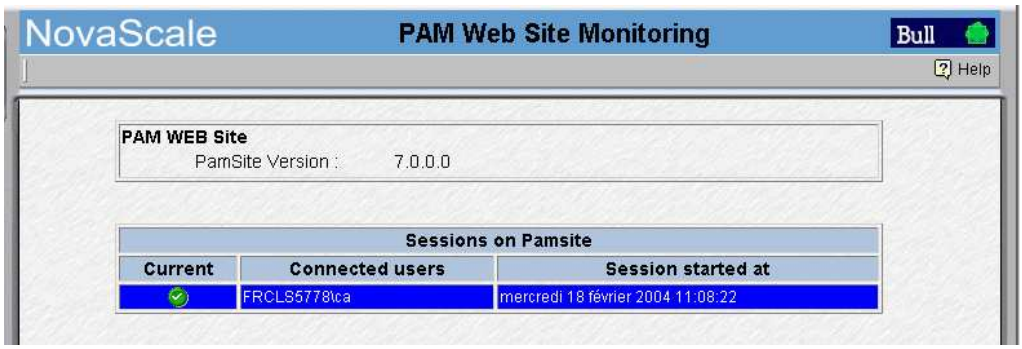
Simultaneous Connection to the PAM Web Site

Several users can access the PAM Web site simultaneously.

Important:
If configuration changes are made, they may not be visible to other users unless they refresh the PAM Tree.

As Customer Administrator, you can view the list of PAM users currently logged onto the PAM Web site by clicking **Hardware Monitor** → **PAM Web Site**.

The Web site version and a list of connected users and session details are displayed in the **Control** pane.



The icon indicates the current session.

Figure 28. PAM Web site session details

You can also open several browser sessions from the same computer to obtain different views of system operation. For example, as Customer Administrator, you may want to open a first session for permanent and easy access to powering on/off functions, a second session for access to system histories and archives, and a third session for access to configuration menus, as shown in the following figure.

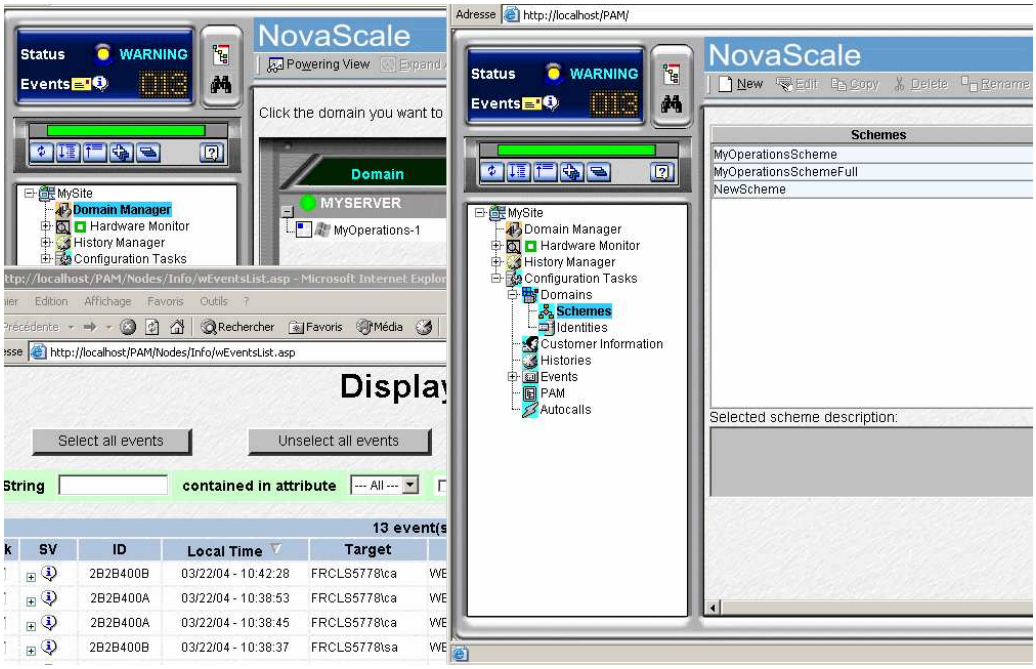
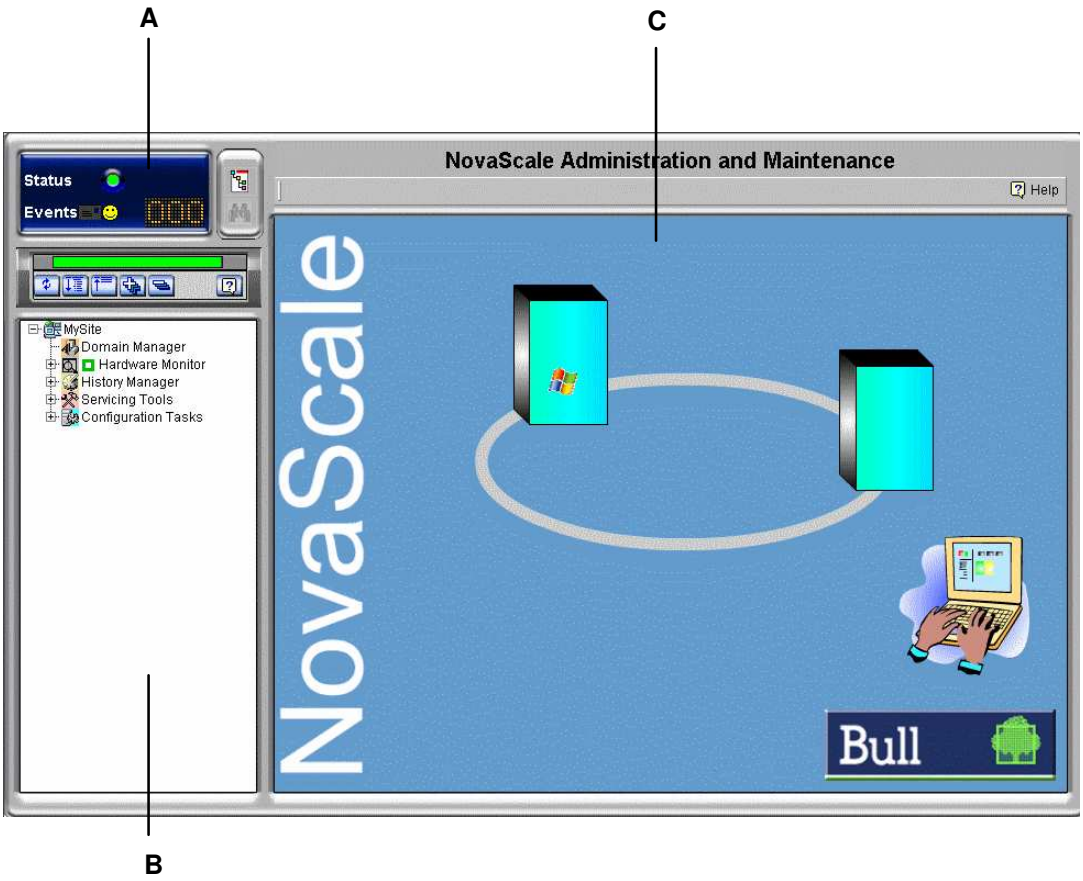


Figure 29. Multiple session example

PAM User Interface

The PAM user interface is divided into three areas in the browser window: a **Status** pane, a **PAM Tree** pane, and a **Control** pane.



A	Status pane, on page 2-6
B	PAM Tree pane, on page 2-7
C	Control pane, on page 2-6

Figure 30. PAM user interface

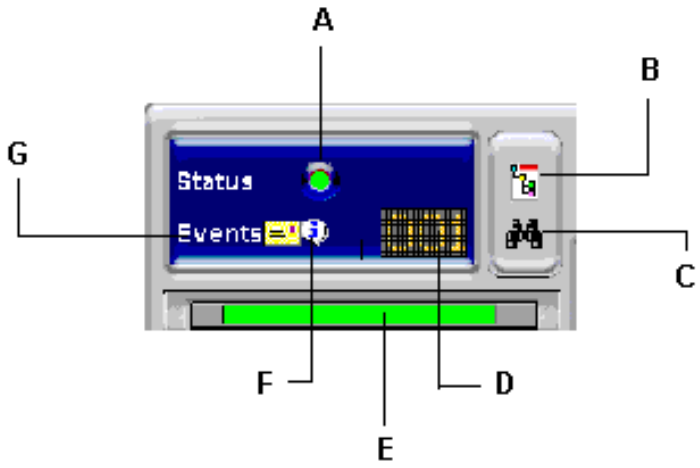
Checking Server Status via PAM

The PAM user interface allows you to check system status at a glance. If the **Functional Status** icon in the **Status** pane and the **CSS Availability Status** bar are green, the server is ready to be powered up.

PAM Status Pane

The **Status** pane, which is automatically refreshed every few seconds, provides quick access to the following synthetic information:

- **Functional Status**: if the system is operating correctly, the status icon is green,
- **Event Messages**: shows the number and maximum severity of pending event messages,
- **CSS Availability Status**: if the CSS Module PMB is detected as present, is configured correctly, and is ready to operate, the status bar is green.



A	System Functional Status icon	**E**	CSS Availability Status icon
B	Presence/Functional Status toggle button	**F**	Event Message Severity icon
C	Event Message Viewer	**G**	New Event Message icon
D	Pending Event Message icon		

Figure 31. Status pane

PAM Control Pane

When an item is selected in the **PAM Tree** pane, details and related commands are displayed in the **Control** pane, which is automatically refreshed at one minute intervals.

CSS Availability Status Bar

The CSS availability status bar reflects the operational status of the data link(s) between the Platform Management Board (PMB) embedded in each CSS Module and the PAP Unit. Each CSS module is represented by a zone in the status bar.

- When a CSS Module PMB is detected as **PRESENT**, the corresponding zone in the status bar is **GREEN**.
- When a CSS Module PMB is detected as **ABSENT**, the corresponding zone in the status bar is **RED**.
- When you hover the mouse over the status bar, an **Infotip** displays the **presence status** of CSS Module PMB – PAP Unit data links.

The following figure represents the status bar for a bi–module server. One CSS Module PMB is detected as PRESENT and the other is detected as ABSENT.

A: Bar red (CSS Module_0 not available)

Figure 32. CSS Module availability status bar (bi–module server)

PAM Tree Pane

☞ **Note:**
The PAM tree builiding process may take one to two minutes. The PAM tree pane is refreshed on request.

The **PAM Tree** pane provides access to server administration and maintenance features:

Tree Nodes	Function
Domain Manager	to power on / off and manage domains. See Chapter 3. Managing Domains.
Hardware Monitor	to display the status of hardware components and assemblies. See Chapter 4. Monitoring the Server.
History Manager	to view logs and manage archives.See Chapter 4. Monitoring the Server.
Configuration Tasks	to customize server features.See Chapter 5. Tips and Features for Administrators.

Table 3. PAM Tree nodes

PAM Tree Toolbar

The PAM Tree toolbar, located at the top of the PAM Tree, is used to refresh, expand, or collapse the tree display.

Toolbar Buttons	Explanation
	Refresh /rebuild the PAM Tree to view changes.
	Expand the complete tree.
	Collapse the complete tree.
	Expand selected node.
	Collapse selected node.
	View the related **Help** topic.

Figure 33. PAM Tree toolbar

Setting up Users

As Customer Administrator, you must set up user accounts and passwords to control access to the PAP unit. See *Setting up PAP Users*, on page 5-17.

Toggling the Local / Integrated Console Display

During the powering up / down sequences, you will be requested to toggle the local / integrated console from the PAP unit display to the server domain display, or vice versa, as explained below.

CAUTION:
Access to the local / integrated console should be restricted to Customer / Support Administrators and Operators ONLY to avoid inadvertent damage to software and/or hardware components.

The KVM Switch allows the integrated console to be used as the local server domain and local PAP unit console. KVM ports are configured as shown in Table 4.

NovaScale 5xx0 Server

8–Port KVM Switch (AutoView)	Console Display	Domain
Port A	PAP Unit	N/A
Port B (PS2)	Microsoft Windows Domain	N/A
Port C (USB)	Linux Domain	N/A

or

8–Port KVM Switch (MasterView)	Console Display	Domain
Port 1	PAP Unit	N/A
Port 2	Server Domain	N/A

NovaScale 6xx0 Server

8–Port KVM Switch	Console Display	Domain
Port 1	PAP Unit	N/A
Port 2	CSS0–Mod0–IO0	MyOperations–xx–1
Port 3	CSS0–Mod0–IO1	MyOperations–xx–2

or

16–Port KVM Switch	Console Display	Domain
Port 1	PAP Unit	N/A
Port 3	CSS0–Mod0–IO0	MyOperations–xx–1
Port 4	CSS0–Mod0–IO1	MyOperations–xx–2
Port 5	CSS0–Mod1–IO0	MyOperations–xx–3
Port 6	CSS0–Mod1–IO1	MyOperations–xx–4

Table 4. KVM port configuration

You can easily toggle from the server domain display to the PAP unit display, or vice versa:

1. From the keyboard, press the **Control** key twice to display the KVM Switch Command Menu.
2. Select the required port with the ↑↓ keys and press **Enter**.
3. The selected display appears on the Console monitor.

Powering Up / Down Server Domains

To power up / down the server, see:

- *Powering Up / Down the* NovaScale 5xx0 Server *Domain*, on page 2-10
- *Powering Up / Down* NovaScale 6080/6160 Server *Domains*, on page 2-12
- *Powering Up / Down* NovaScale 6320 Server *Domains*, on page 2-17

Powering Up the NovaScale 5xx0 Server Domain

NovaScale 5xx0 Servers are designed to operate as single SMP systems and are delivered with one pre–configured domain.

When server status has been checked – functional status icon and CSS availability status bar green in the Status pane – the server domain can be powered up.

Note:
If an error dialog box appears during this sequence, see Chapter 3. *Managing Domains*.

To power up server domains:

4. From the PAM Tree, click **Domain Manager** to open the **Control** pane. A dialog box invites you to load the server domain.
5. Click **OK** to confirm. The domain appears in the Control pane. If the domain is ready to be powered up, **INACTIVE** is displayed in the **Domain State** box and the **Power On** button is accessible.
6. Select the domain and click **Power On** to power up the server domain and associated hardware components.

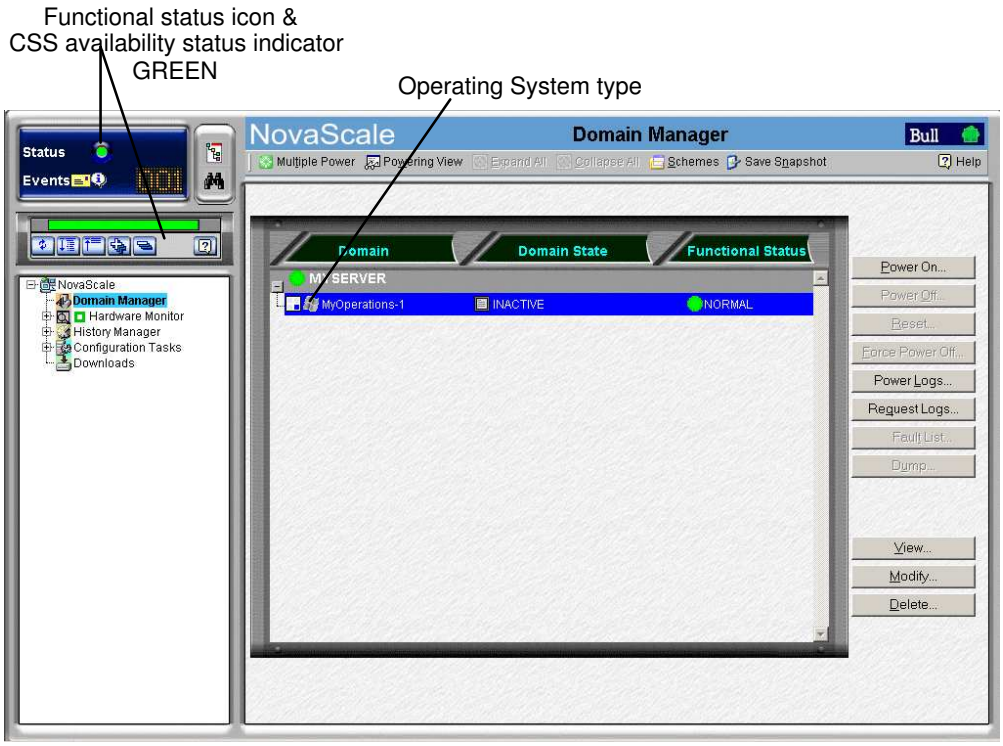


Figure 34. Domain Manager Control pane

7. Follow the power–on steps displayed in the **Domain State** box, until **RUNNING** is displayed.

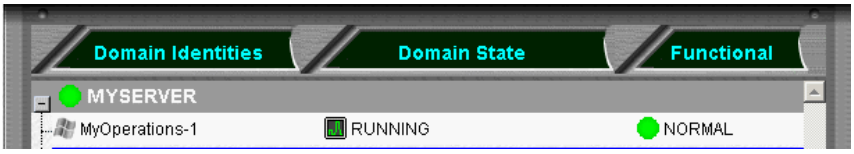


Figure 35. Domain state

8. Toggle the local / integrated console from the PAP unit display to the server display. See *Toggling the Local / Integrated Console Display*, on page 2-9.
9. Wait for the Operating System to load completely. The domain is now fully functional.
10. Check the Operating System environment pre–installed on the domain.
11. As Customer Administrator, you can now prepare each domain for remote access via the Enterprise LAN and/or via the Web. See *Preparing Server Domains for Remote Access via the Enterprise LAN*, on page 2-22 and *Preparing Server Domains for Remote Access via the Web*, on page 2-24.

Powering Down the NovaScale 5xx0 Server Domain

Note:
If an error dialog box appears during this sequence, see Chapter 3. *Managing Domains*.

1. Shut down the Operating System to power down the domain to the stand–by mode.
2. Toggle the local / integrated console to the PAP unit display. **INACTIVE** is displayed in the **Domain State** box and the **Power ON** button is accessible.

Note:
For further details about the **Power ON** / **OFF** sequences, see *Powering ON a Domain*, on page 3-14 and *Powering OFF a Domain*, on page 3-18.

- If the same PAP unit administers more than one server, all servers can be powered on simultaneously as follows:
  a. Click **Multiple Power**. The **Multiple Power Domains On/Off** dialog opens.
  b. Click **Power On All** → **Execute** to power on the servers and associated hardware components.
- For further details about the **Power ON** / **OFF** sequences, see *Powering ON a Domain* and *Powering OFF a Domain* in the *User's Guide*.

Powering Up NovaScale 6080/6160 Server Domains

The NovaScale 6080/6160 Server is designed to operate as two hardware–independent SMP systems, or domains.

For easy configuration and optimum use of the physical and logical resources required for simultaneous operation, domains are defined by the Customer Administrator via the **PAM Domain Scheme** wizard.

For further details about domain configuration, see *Configuring Domains*, on page 5-28.

The server is delivered with a default scheme, or configuration file, called **MyOperationsScheme–xx** containing two domains, **MyOperations–xx–1** and **MyOperations–xx–2**.your An Operating System instance is pre–installed on each domain boot disk (EFI LUN). According to your requirements, identical or different Operating System instances may be pre–installed on each EFI LUN. The default scheme allows domains to be booted simultaneously or independently. A brief summary of the organization of physical and logical resources in **MyOperationsScheme–xx** is given in the following table.

Notes:

- **xx** in the default scheme and domain names represents the Central Subsystem HW identifier (from 00 to 16). For further details, refer to *Checking PMB Code Wheel Settings*, on page 0.
- In the screen shots, tables, and examples in this guide:
  - **MyOperationsScheme–xx** is referred to as **MyOperationsScheme**
  - **MyOperations–xx–1** is referred to as **MyOperations–1**
  - **MyOperations–xx–2** is referred to as **MyOperations–2**
- In the screen shots in this guide, an instance of Microsoft Windows is pre–installed on **MyOperations–xx–1** and an instance of Linux is pre–installed on **MyOperations–xx–2**.

  Operating System type is indicated by the Microsoft Windows or Linux logo in the **Domain Identities** box.

MyOperationsScheme Organization

Domain Identity: MyOperations–1	
Hardware Cell	Cell_0
Operating System (customer–specific)	 Windows or  Linux
EFI LUN**	*<*MyServer*>_0LU0 / <*SAN*>LUN0
IOB	Module0_IOB0
QBBs	Module0_QBB0, Module0_QBB1
Domain KVM Ports	***CSS0_Mod0_IO0
Domain Identity: MyOperations–2	
Hardware Cell	Cell_1
Operating System (customer–specific)	 Windows or  Linux
EFI LUN**	*<*MyServer*>_0LU0 / <*SAN*>LUN1
IOB	Module0_IOB1
QBBs	Module0_QBB2, Module0_QBB3
Domain KVM Ports	***CSS0_Mod0_IO1

* <*MyServer*> = default server name, e.g.: NS6080–0, NS6160–0

** EFI LUN: xLUx = Local boot LUN device location (*Mod*x LU*IO*x):
0LU0 = LUN device connected to Module0, IOB0
0LU1 = LUN device connected to Module0, IOB1
0LU2 = LUN device connected to Module1, IOB0
0LU3 = LUN device connected to Module1, IOB1

***CSSx = CSS number, Modx = Module number, IOx = IO box number

Note:
The NovaScale 6080 Server is equipped with QBB_0 and QBB_3, only.

Table 5. MyOperationsScheme organization – mono–module server

Note:
If an error dialog box appears during these sequences, see Chapter 3. *Managing Domains*.

To power up server domains:

1. From the PAM Tree, click **Domain Manager** to open the **Control** pane. You are invited to load a domain configuration scheme.
2. Click **Schemes.** The **Schemes List** dialog opens displaying the pre–configured scheme.
3. Select **MyOperationsScheme** and click **Apply**.

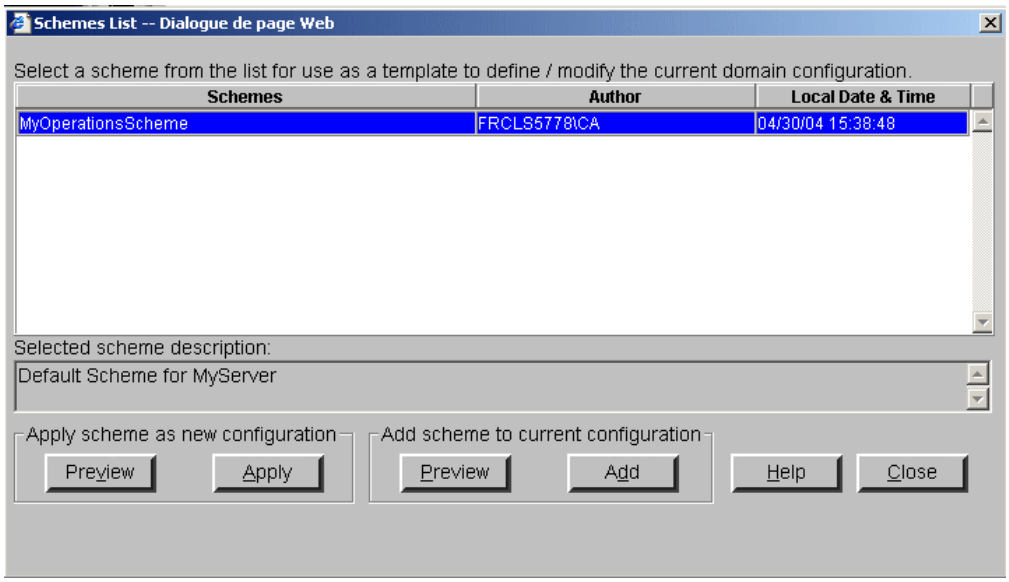


Figure 36. Domain schemes list dialog

4. When requested, click **Yes** to confirm. **MyOperations–1** and **MyOperations–2** domains are loaded in the **Control** pane.

If the domains are ready to be powered up, **INACTIVE** is displayed in the **Domain State** boxes and the **Power On** button is accessible for each domain.

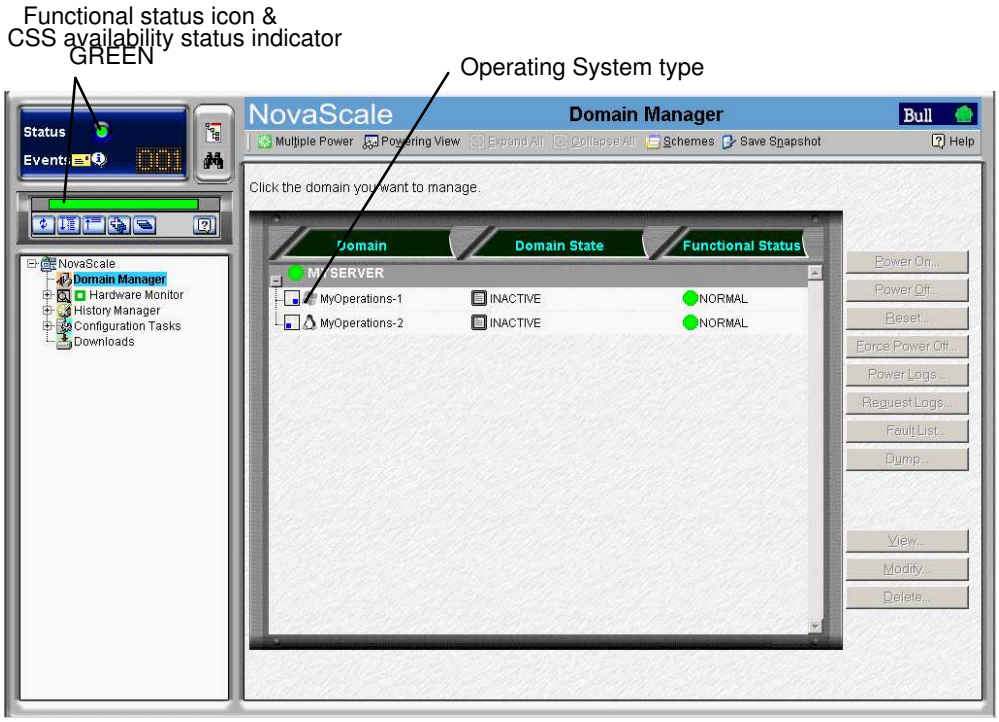


Figure 37. Domain Manager Control pane

5. Click **Multiple Power**. The **Multiple Power Domains On/Off** dialog opens.
6. Click **Power On All** → **Execute** to simultaneously power on the domains and associated hardware components.

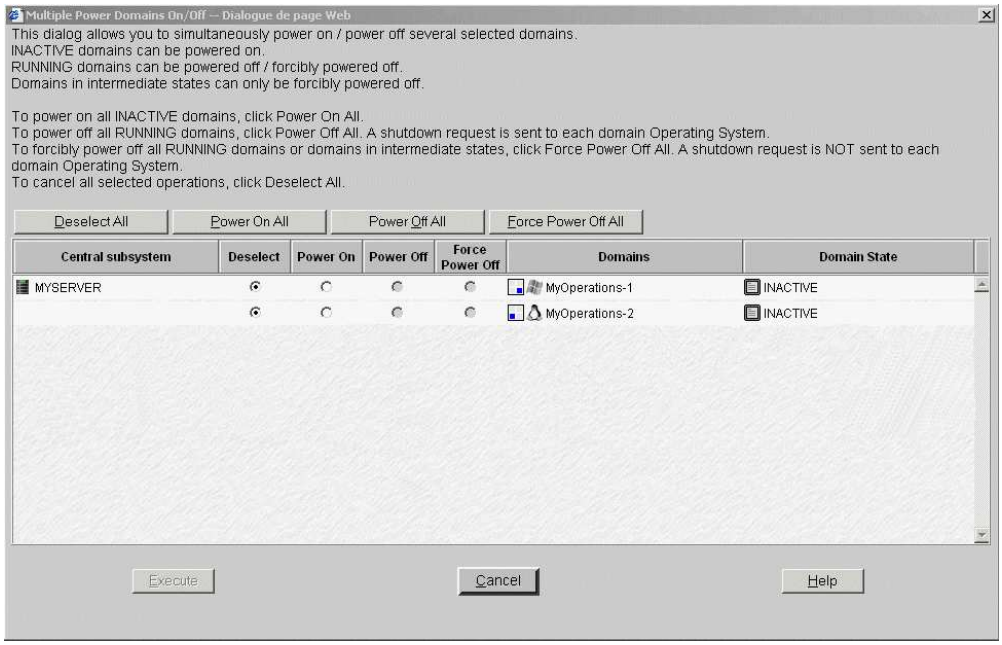


Figure 38. Multiple power dialog

Note:
Domains can also be powered on sequentially from the **Control** pane:

- Select **MyOperations–1** in the **Control** pane and click **Power On** to power up the domain and associated hardware components.
- Select **MyOperations–2** in the **Control** pane and click **Power On** to power up the domain and associated hardware components.

7. Follow the power–on steps displayed in the **Domain State** boxes, until **RUNNING** is displayed in both **Domain State** boxes.

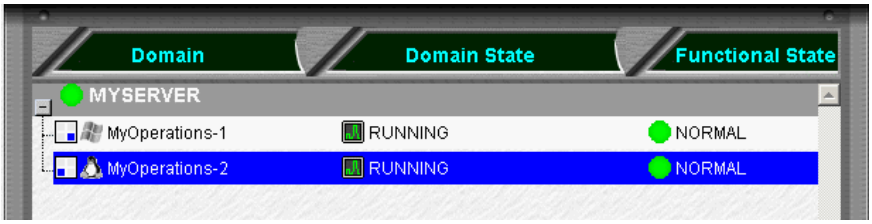


Figure 39. Domain state

8. Toggle the local / integrated console from the PAP unit display to **MyOperations–1** display. See *Toggling the Local / Integrated Console Display*, on page 2-9.
9. Wait for the Operating System to load completely. **MyOperations–1** domain is now fully functional.
10. Toggle the local / integrated console from **MyOperations–1** display to **MyOperations–2** display.
11. Wait for the Operating System to load completely. **MyOperations–2** domain is now fully functional.
12. Check the Operating System environment pre–installed on each domain.
13. As Customer Administrator, you can now prepare each domain for remote access via the Enterprise LAN and/or via the Web. See *Preparing Server Domains for Remote Access via the Enterprise LAN*, on page 2-22 and *Preparing Server Domains for Remote Access via the Web*, on page 2-24.

Powering Down NovaScale 6080/6160 Server Domains

Note:
If an error dialog box appears during this sequence, see Chapter 3. *Managing Domains*.

1. Shut down each Operating System to power down the corresponding domain to the stand–by mode.
2. Toggle the local / integrated console to the PAP unit display. **INACTIVE** is displayed in the **Domain State** boxes and the **Power ON** button is accessible for each domain.

Note:
For further details about the **Power ON** / **OFF** sequences, see *Powering ON a Domain*, on page 3-14 and *Powering OFF a Domain*, on page 3-18.

Powering Up NovaScale 6320 Server Domains

The NovaScale 6320 Server is designed to operate as four hardware–independent SMP systems, or domains.

For easy configuration and optimum use of the physical and logical resources required for simultaneous operation, domains are defined by the Customer Administrator via the **PAM Domain Scheme** wizard. For further details about domain configuration, see *Configuring Domains*, on page 5-28.

The server is delivered with a default scheme, or configuration file, called **MyOperationsScheme–xx**, containing up to four domains, **MyOperations–xx–1**, **MyOperations–xx–2**, **MyOperations–xx–3**, **MyOperations–xx–4**. An Operating System instance is pre–installed on each domain boot disk (EFI LUN). According to your requirements, identical or different Operating System instances may be pre–installed on each EFI LUN. The default scheme allows you to simultaneously boot all domains. A brief summary of the organization of physical and logical resources in **MyOperationsScheme–xx** is given in the following table.

Notes:

- **xx** in the default scheme and domain names represents the Central Subsystem HW identifier (from 00 to 16). For further details, refer to *Checking PMB Code Wheel Settings*, on page 0.
- In the screen shots, tables, and examples in this guide:
  - **MyOperationsScheme–xx** is referred to as **MyOperationsScheme**
  - **MyOperations–xx–1** is referred to as **MyOperations–1**
  - **MyOperations–xx–2** is referred to as **MyOperations–2**
  - **MyOperations–xx–3** is referred to as **MyOperations–3**
  - **MyOperations–xx–4** is referred to as **MyOperations–4**
- In the screen shots in this guide, an instance of Microsoft Windows is pre–installed on **MyOperations–xx–1** and **MyOperations–xx–3** and an instance of Linux is pre–installed on **MyOperations–xx–2** and **MyOperations–xx–4**.

  Operating System type is indicated by the Microsoft Windows or Linux logo in the **Domain Identities** box.

MyOperationsScheme Organization

Domain Identity: MyOperations–1	
Hardware Cell	Cell_0
Operating System (customer–specific)	 Windows or  Linux
EFI LUN**	*<*MyServer*>_0LU0 / <*SAN*>LUN0
IOB	Module0_IOB0
QBBs	Module0_QBB0, Module0_QBB1
Domain KVM Ports	***CSS0_Mod0_IO0
Domain Identity: MyOperations–2	
Hardware Cell	Cell_1
Operating System (customer–specific)	 Windows or  Linux
EFI LUN**	*<*MyServer*>_0LU0 / <*SAN*>LUN1
IOB	Module0_IOB1
QBBs	Module0_QBB2, Module0_QBB3
Domain KVM Ports	***CSS0_Mod0_IO1
Domain Identity: MyOperations–3 (NovaScale 6320 Server)	
Hardware Cell	Cell_2
Operating System (customer–specific)	 Windows or  Linux
EFI LUN**	*<*MyServer*>_0LU0 / <*SAN*>LUN2
IOB	Module1_IOB0
QBBs	Module1_QBB0, Module1_QBB1
Domain KVM Ports	***CSS0_Mod1_IO0
Domain Identity: MyOperations–4 (NovaScale 6320 Server)	
Hardware Cell	Cell_3
Operating System (customer–specific)	 Windows or  Linux
EFI LUN**	*<*MyServer*>_0LU0 / <*SAN*>LUN3
IOB	Module1_IOB1
QBBs	Module1_QBB2, Module1_QBB3
Domain KVM Ports	***CSS0_Mod1_IO1

* <*MyServer*> = default server name, e.g.: NS6080–0, NS6160–0, NS6320–0

** EFI LUN: xLUx = Local boot LUN device location (*Mod*x LU*IO*x):
0LU0 = LUN device connected to Module0, IOB0
0LU1 = LUN device connected to Module0, IOB1
0LU2 = LUN device connected to Module1, IOB0
0LU3 = LUN device connected to Module1, IOB1

***CSSx = CSS number, Modx = Module number, IOx = IO box number

Table 6. MyOperations Scheme organization – bi–module server

Note:
If an error dialog box appears during these sequences, see Chapter 3. *Managing Domains*.

To power up server domains:

3. From the PAM Tree, click **Domain Manager** to open the **Control** pane. You are invited to load a domain configuration scheme.
4. Click **Schemes**. The **Schemes List** dialog opens displaying the pre–configured scheme.
5. Select **MyOperationsScheme** and click **Apply**.

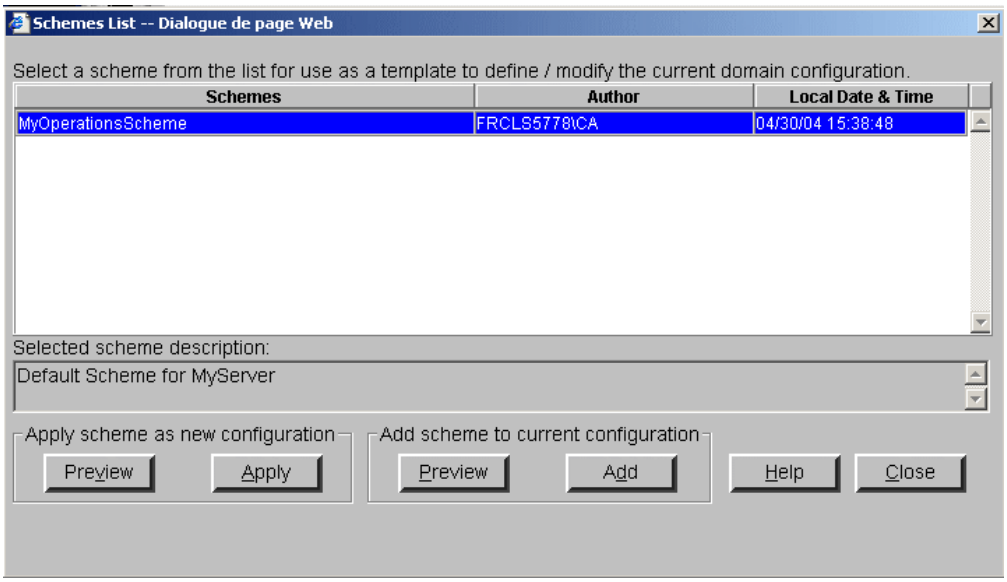


Figure 40. Domain schemes list dialog

6. When requested, click **Yes** to confirm. **MyOperations–1, MyOperations–2, MyOperations–3,** and **MyOperations–4** domains are loaded in the **Control** pane. If the domains are ready to be powered up, **INACTIVE** is displayed in the **Domain State** boxes and the **Power On** button is accessible for each domain.

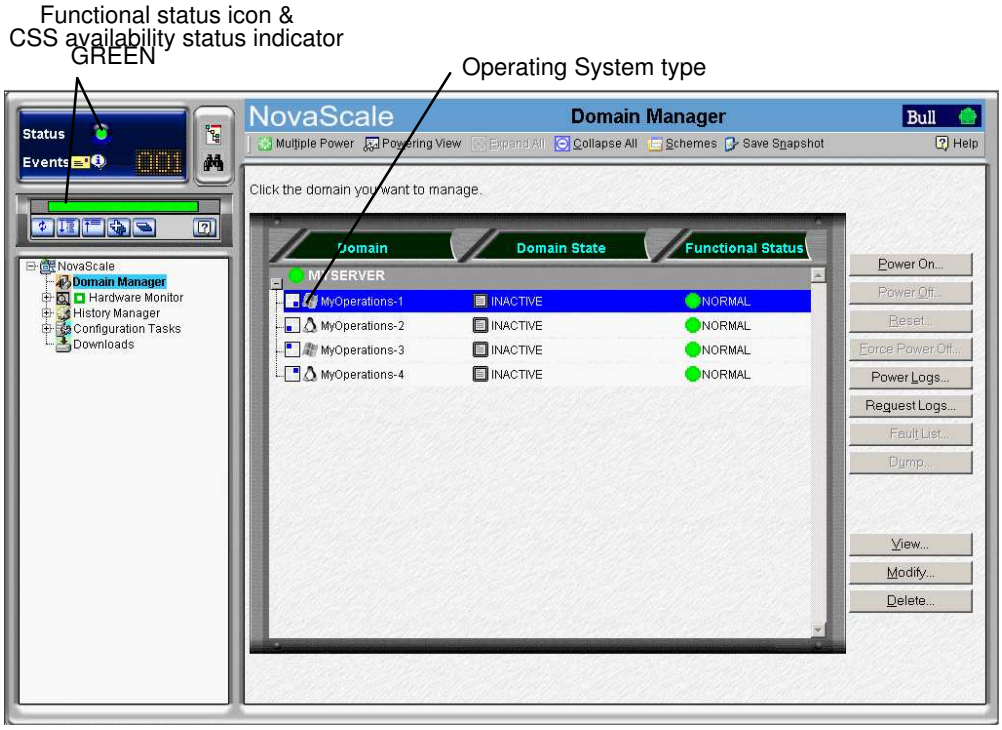


Figure 41. Domain Manager Control pane

7. Click **Multiple Power**. The **Multiple Power Domains On/Off** dialog opens.

8. Click **Power On All** → **Execute** to simultaneously power on the domains and associated hardware components.

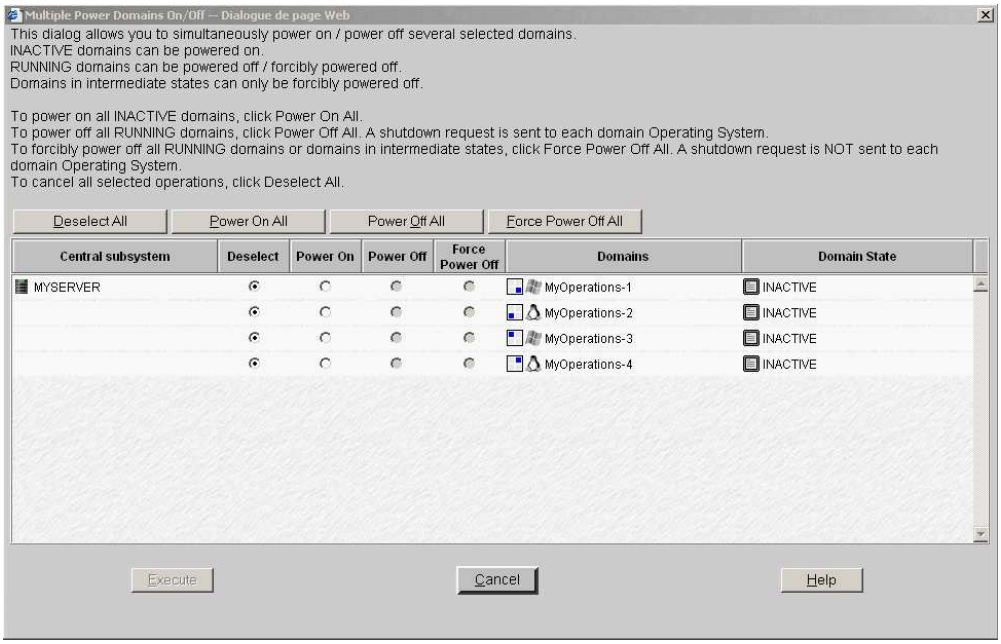


Figure 42. Multiple power dialog

Note:
Domains can also be powered on sequentially from the **Control** pane:

- Select **MyOperations–1** in the **Control** pane and click **Power On** to power up the domain and associated hardware components. Repeat this step for each domain in the **Control** pane.

9. Follow the power–on steps displayed in the **Domain State** boxes, until **RUNNING** is displayed in all **Domain State** boxes.

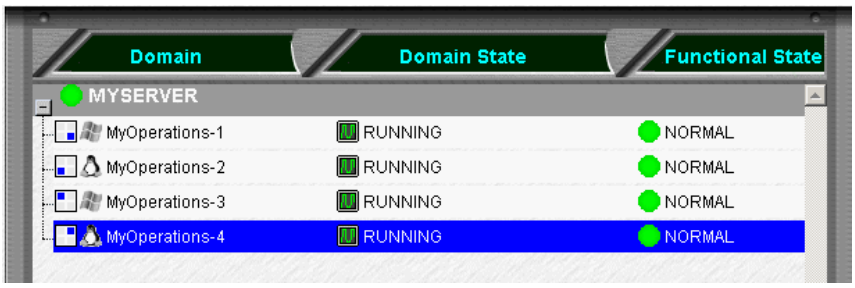


Figure 43. Domain state

10. Toggle the local / integrated console from the PAP unit display to the first domain display. See *Toggling the Local / Integrated Console Display*, on page 2-9.
11. Wait for the Operating System to load completely. The domain is now fully functional.
12. Toggle the local / integrated console from this domain display to the next domain display.
13. Wait for the Operating System to load completely. The domain is now fully functional.
14. Repeat Steps 12 and 13 for each domain.
15. Check the Operating System environment pre–installed on each domain.

16. As Customer Administrator, you can now prepare each domain for remote access via the Enterprise LAN and/or via the Web. See *Preparing Server Domains for Remote Access via the Enterprise LAN*, on page 2-22 and *Preparing Server Domains for Remote Access via the Web*, on page 2-24.

Powering Down NovaScale 6320 Server Domains

☞ **Note:**
If an error dialog box appears during this sequence, see Chapter 3. *Managing Domains*.

1. Shut down each Operating System to power down the corresponding domain to the stand–by mode.
2. Toggle the local / integrated console to the PAP unit display. **INACTIVE** is displayed in the **Domain State** boxes and the **Power ON** button is accessible for each domain.

☞ **Note:**
For further details about the **Power ON** / **OFF** sequences, see *Powering ON a Domain*, on page 3-14 and *Powering OFF a Domain*, on page 3-18.

Preparing Server Domains for Remote Access via the Enterprise LAN

CAUTION:
Access to the local / integrated console should be restricted to Customer / Support Administrators and Operators ONLY to avoid inadvertent damage to software and/or hardware components.

Note:
Required networking data is indicated in the *Read Me First* document delivered with the server and is also recorded under the corresponding PAM **Domain Identity**.
Customer Administrator rights are required for all PAM configuration tasks.

Microsoft Windows Domain

1. Toggle the integrated console to the corresponding Windows domain port. See *Toggling the Local / Integrated Console Display*, on page 2-9.
2. From the Windows desktop, right click **My Computer** and select **Properties** → **Remote**.
3. Check the **Allow remote connection** box.
4. Share the ***<system root>*\system32\clients\tsclient** directory via the Explorer.
5. Toggle the integrated console to the PAP unit port.
6. From the Customer Administrator PAM tree, click **Configuration Tasks** → **Domains** → **Identities** to open the **Identities** page.
7. Select the corresponding Windows domain from the list and click **Edit** to open the **Edit an Identity** dialog.
8. Check that the **Network Name**, **IP Address**, and **URL** fields are completed. If not, complete these fields with the networking data entered during the Windows setup completion procedure and click **OK**.

Linux Redhat Domain

1. Toggle the integrated console to the corresponding Linux domain port. See *Toggling the Local / Integrated Console Display*, on page 2-9.
2. From the Linux desktop, enable remote connection via **telnet, rlogin, ftp,** ...:
3. From the PAP unit Internet Explorer or Mozilla browser, enter the Webmin URL: **http://*<networkname>*:10000**, where ***<networkname>*** is the network name given to the server domain during the Linux setup completion procedure.
   The **Login to Webmin** dialog box opens.
4. Click the **Networking** icon. The **Networking** main page opens.
5. Click **Extended Internet Services** to display the list of available services.
6. From the service list, check that **Yes** is displayed in the status column. If **No** is displayed in the status column, proceed as follows to enable the service:
   a. Select the required service from the list.
   b. Complete the fields accordingly.
   c. Click **Yes** after **Service enabled?**
   d. Click **Save**.
7. Repeat step 3 for each required service.

8. Click **Apply changes** to apply all changes.
9. Click **Return to index**.
10. Click **Log Out** to exit **Webmin**.
11. Toggle the integrated console to the PAP unit port.
12. From the Customer Administrator PAM tree, click **Configuration Tasks** → **Domains** → **Identities** to open the **Identities** page.
13. Select the corresponding Linux domain from the list and click **Edit** to open the **Edit an Identity** dialog.
14. Check that the **Network Name**, **IP Address**, and **URL** fields are completed. If not, complete these fields with the networking data entered during the Linux setup completion procedure and click **OK**.

Linux SuSE Domain

1. Toggle the integrated console to the corresponding Linux domain port. See *Toggling the Local / Integrated Console Display*, on page 2-9.
2. From the Linux desktop, enable remote connection via **telnet, rlogin, ftp,** ...:
3. Launch the **yast2** command to open the **Yast Control Center** screen.
4. Click the **Network**/**Basic** icon in the left pane.
5. Click **Start**/**stop services (inetd)**.
6. From the **Network Services** page, select **On with customer configuration** and click **Next** to open the **Enable**/**disable network services** page.
7. From the service list, check that **Active** is displayed in the status column. Proceed as follows to enable the service:
   a. Select the required service from the list.
   b. Click **Activate**.
8. Repeat step 5 for each required service.
9. Click **Finish** to apply all changes.
10. Click **Close** to exit **yast2**.
11. Toggle the integrated console to the PAP unit port.
12. From the Customer Administrator PAM tree, click **Configuration Tasks** → **Domains** → **Identities** to open the **Identities** page.
13. Select the corresponding Windows domain from the list and click **Edit** to open the **Edit an Identity** dialog.
14. Check that the **Network Name**, **IP Address**, and **URL** fields are completed. If not, complete these fields with the networking data entered during the Linux setup completion procedure and click **OK**.

Preparing Server Domains for Remote Access via the Web

CAUTION:
Remote access via the Web is a potential security hazard. Customers are strongly advised to protect their systems with up–to–date protection devices such as virus–prevention programs and firewalls, and to maintain a detailed record of authorized users.

Microsoft Windows Domain

1. Toggle the integrated console to the corresponding Windows domain port. See *Toggling the Local / Integrated Console Display*, on page 2-9.
2. Left click **Start** → **Control Panel** → **Add or Remove Programs**.
3. Select **Add** / **Remove Windows Components**.
4. Click **Web Application Services** → **Details** → **Internet Information Services** → **Details** → **World Wide Web Services** → **Details** → **Remote Desktop Web Connection**. Validate where required by clicking **OK** or **Next**.
5. Insert the the Microsoft Windows CD–ROM in the CD–ROM / DVD drive.
6. The Microsoft Windows setup wizard is launched automatically and guides you through the setup completion procedure.
7. Toggle the integrated console to the PAP unit port.
8. From the Customer Administrator PAM tree, click **Configuration Tasks** → **Domains** → **Identities** to open the **Identities** page.
9. Select the corresponding Windows domain from the list and click **Edit** to open the **Edit an Identity** dialog.
10. Check that the **Network Name**, **IP Address**, and **URL** fields are completed. If not, complete these fields with the networking data entered during the Windows setup completion procedure and click **OK**.

Linux Domain

Virtual Network Computing (VNC) remote control software allows users to interact with the server from a remote computer via Internet.

The server domain is ready for remote connection.

1. Toggle the integrated console to the PAP unit port.
2. From the Customer Administrator PAM tree, click **Configuration Tasks** → **Domains** → **Identities** to open the **Identities** page.
3. Select the corresponding Linux domain from the list and click **Edit** to open the **Edit an Identity** dialog.
4. Check that the **Network Name**, **IP Address**, and **URL** fields are completed. If not, complete these fields with the networking data entered during the Linux setup completion procedure and click **OK**.

Connecting to a Server Domain via the Enterprise LAN

Microsoft Windows Domain

1. Check that **Client for Microsoft Networks** is installed on the remote computer and that the remote computer is connected to the same LAN as the server domain.
2. Check that **Client for Remote Desktop** is installed on the remote computer. If the **Remote Desktop Connection** menu does not exist:
   a. Click **Start** → **Run**.
   b. Type ***<networkname>****tsclient\win32\setup.exe** in the box, where ***<networkname>*** is the network name given to the server domain during the Windows setup completion procedure.
3. Connect to the server domain by running:
   a. Microsoft Windows XP (and later):
   All Programs → **Accessories** → **Communication** → **Remote Desktop Connection**.
   b. All other versions of Microsoft Windows:
   Programs → **Remote Desktop Connection** → **OK**.
4. Type **Administrator** (default administrator user name) in the **User name** field.
5. Type the administrator password defined during the Windows setup completion procedure in the **Password** field.
6. The remote computer connects to the server domain.

Linux Domain

1. Enter the following command:

   ssh *<networkname>* –l user_name, where ***<networkname>*** is the network name given to the server domain during the Linux setup completion procedure.
2. The remote computer connects to the server domain.

Connecting to the Server via the Web

Microsoft Windows Domain

1. Check that **Internet Explorer** (6 or later) and **Terminal Server Client** are installed on the remote computer.
2. Launch the Internet Explorer or Netscape browser and connect to the server desktop, url: **http:**//***<networkname>***/**tsweb**/, where ***<networkname>*** is the network name given to the server domain during the Windows setup completion procedure. See the *Read Me First* document delivered with the server.

Linux Domain

Virtual Network Computing (VNC) remote control software allows users to interact with the server from a remote computer via Internet.

1. Check that **VNC Server** is installed.
2. Execute the **vncpasswd** command to initialize the password.
3. Execute the **vncserver** command to start the process.
4. Record the ***<networkname>*** display number for the remote computer, where ***<networkname>*** is the network name given to the server domain during the Linux setup completion procedure.

Installing Applications

When you install an application protected by a system serial number, you are requested to supply this serial number.

For optimum flexibility, PAM software allows you to replace the physical serial number by a logical licensing number so that you can run the application on any physical partition and, in the case of extended systems, on any of the Central Subsystems within the extended configuration.

For details on how to define and manage the logical licensing number, please refer to *Creating, Editing, Copying, Deleting a Domain Identity*, on page 5-47.

Chapter 3. Managing Domains

This chapter explains how, as Customer Administrator and/or Customer Operator, you can manage server domains. It includes the following topics:

Note:
Customer Administrators and Customer Operators are respectively advised to consult the *Administrator's Memorandum*, on page xxviii or the *Operator's Memorandum*, on page xxx for a detailed summary of the everyday tasks they will perform.

For further information about user accounts and passwords, see *Setting up PAP Unit User*s, on page 5-17.

Important:
Certain domain configuration and management tools are reserved for use with partitioned servers and extended systems. Please contact your Bull Sales Representative for sales information.

Introducing PAM Domain Management Tools

Important:
Certain domain configuration and management tools are reserved for use with partitioned servers and extended systems. Please contact your Bull Sales Representative for sales information.

A Bull NovaScale Server domain englobes all the hardware and software resources managed by an Operating System instance.

NovaScale 5xx0 Servers are designed to operate as single SMP systems and are delivered with one pre–configured domain.

NovaScale 6xx0 Servers are designed to operate as one, two, three or four hardware–independent SMP systems or domains, each running an Operating System instance and a specific set of applications.

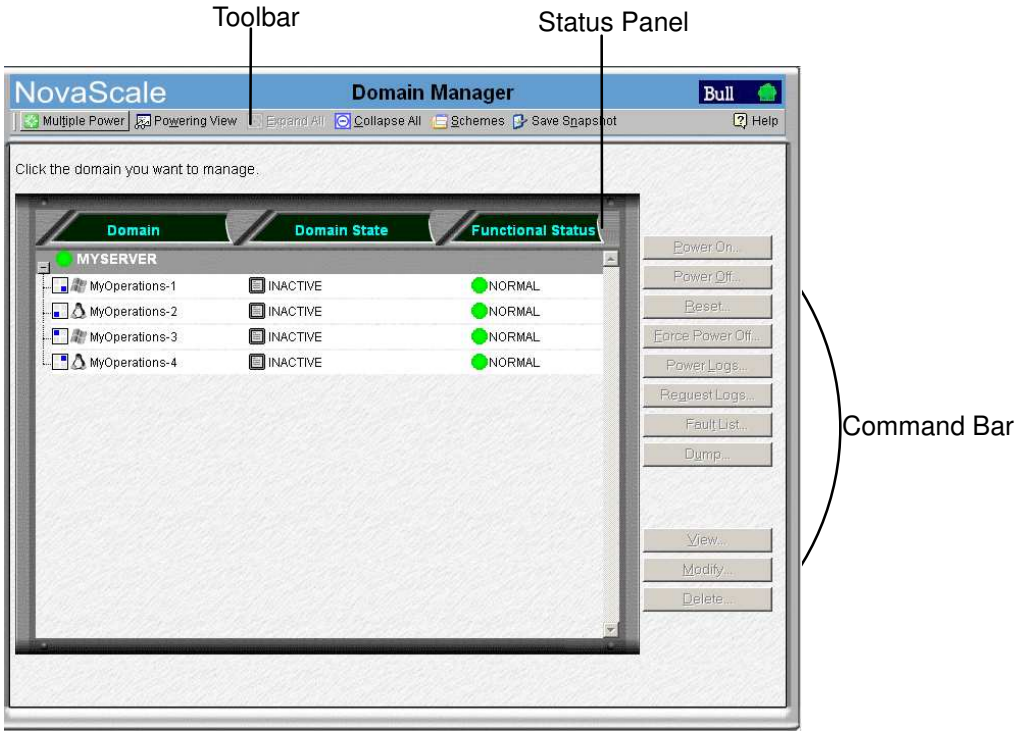
The PAM **Domain Manager** is at the heart of server operation. Customer Administrators and Operators have equal access rights to **Domain Manager** functions and the Control pane is frequently used during operation. The **Domain Manager** Control pane gives access to all domain commands and domain details.

What You Can Do
Via the **Domain Manager** Control pane, you can:

- *Manage domain configuration schemes*
- *Power on a domain*
- *Power off a domain*
- *Perform a domain reset*
- *Perform a domain force power off*
- *Request a domain memory dump*
- *View functional status*
- *View power logs*
- *View powering sequences*
- *View BIOS info*
- *View request logs*
- *View domain configuration, resources and status*

Note:
Access to certain hardware resources, such as system disks can be limited by using the **Exclusion** / **Inclusion** function. See *Limiting Access to Hardware Resources*, on page 5-62 and *Excluding / Including Hardware Elements*, on page 4-25. This function must be used with care.

From the PAM Tree, click **Domain Manager** to open the **Control** pane.



Toolbar	
Multiple Power	Allows you to simultaneously power on /off several domains. See *Powering ON a Domain*, on page 3-14 and *Powering OFF a Domain*, on page 3-18.
Powering View	Dynamically displays domain power sequences and gives access to **Power Logs**, see details on page 3-28 and **BIOS Info**, see details on page 3-30.
Expand All	Expands the list of domains included in the current domain configuration.
Schemes	Loads a selected scheme and displays **Scheme Properties**, see details on page 3-8.
Save Snapshot	Saves current domain configuration as a new scheme for future use, see details on page 3-11.
Status Panel	
Domain Identities	The names given to clearly identify domains, see details on page 5-28.
Domain State	Power sequence state. See *Powering ON a Domain*, on page 3-14 and *Powering OFF a Domain*, on page 3-18.
Functional Status	Status of the last action performed on a domain. See *Viewing Domain Functional Status*, on page 3-27.

Command Bar	
Power On	Powers on the selected domain, see details on page 3-14.
Power Off	Powers off the selected domain, see details on page 3-18.
Reset	Resets the selected domain, see details on page 3-24.
Force Power Off	Forcibly powers off the selected domain, see details on page 3-21.
Power Logs	Displays power sequence logs, see details on page 3-28.
Request Logs	Displays Power On, Power Off, and Reset requests and requestors, see details on page 3-31.
Fault List	Gives access to the domain fault list, see details on page 3-25.
Dump	Performs a domain memory dump, see details on page 3-26.
View	Displays **Domain Resources**, see details on page 3-32 and **BIOS Info**, see details on page 3-30 and gives access to the **Domain Modification** dialog, see details on page 3-39.
Modify	Used to change current domain settings, see details on page 3-39.
Delete	Removes the selected domain from the current domain configuration, see details on page 3-66.

Table 7. PAM Domain Manager tools

Managing Domain Configuration Schemes

Important:
Reserved for partitioned servers and extended systems.
Certain features described below are only available if you are connected to a Storage Area Network (SAN).
Please contact your Bull Sales Representative for sales information.

What You Can Do

- *View a domain configuration scheme*
- *Load a domain configuration scheme*
- *Add domains to the current domain configuration*
- *Replace the current domain configuration*
- *Save the current domain configuration snapshot*

A **Domain Configuration Scheme** is the template or configuration file used to define and manage a set of domains that can be active simultaneously. For easy configuration and optimum use of the physical and logical resources required for simultaneous operation, domains are defined via the **PAM Domain Configuration Scheme** wizard.

Note:
Server components and configuration may differ according to site requirements.

NovaScale 5xx0 Server

NovaScale 5xx5 Servers are designed to operate as single SMP systems and are delivered with one pre–configured domain.

NovaScale 6080/6160 Servers

NovaScale 6080/6160 Servers are designed to operate as one or two hardware–independent domains. Servers are delivered with a pre–configured domain configuration scheme called **MyOperationsScheme** containing one or two domains, **MyOperations–1** and **MyOperations–2**, allowing you to manage and administer all server resources.

NovaScale 6320 Server

The NovaScale 6320 Server is designed to operate as one, two, three or four hardware–independent domains. The server is delivered with a pre–configured domain configuration scheme called **MyOperationsScheme** containing one to four domains, **MyOperations–1**, **MyOperations–2**, **MyOperations–3** and **MyOperations–4**, allowing you to manage and administer all server resources.

An Operating System instance is pre–installed on each domain boot disk (EFI LUN). According to your requirements, identical or different Operating System instances may be installed on each EFI LUN. A brief summary of the organization of physical and logical resources in **MyOperationsScheme** is given in *MyOperationsScheme Organization*, on page 3-12.

Note:
As Customer Administrator, you may configure other schemes for domain management. For further details about domain configuration options, see *Configuring Domains*, on page 5-28.

To power on server domains, you must first load the required **Domain Configuration Scheme** from the **Domain Manager** Control pane. Once the domain configuration scheme has been loaded, domains can be powered up simultaneously or sequentially.

Synchronizing NovaScale 5xx0 Server Domains

The **Synchronize Domains** command is used to load the NovaScale 5xx0 Server domain. Each NovaScale 5xx0 Server is delivered with one pre–configured domain.

To load the server domain:

Click **Synchronize Domains** in the toolbar. The server domain(s) appear(s) in the Control pane for management.

The other **Schemes** tool options are reserved for partitioned (NovaScale 6xx0 Servers) or extended systems. See *Configuring and Managing Extended Systems*, on page 5-108.

Note:
Extended systems: this command will load all the NovaScale 5xx5 Server domains adminstered by your PAP unit.

Viewing a Domain Configuration Scheme

Before loading a domain configuration scheme, you may want to know more about its scope.

To view a scheme:

1. Click **Domain Manager** to open the Control pane.
2. Click **Schemes** in the Toolbar to open the **Schemes List** dialog.

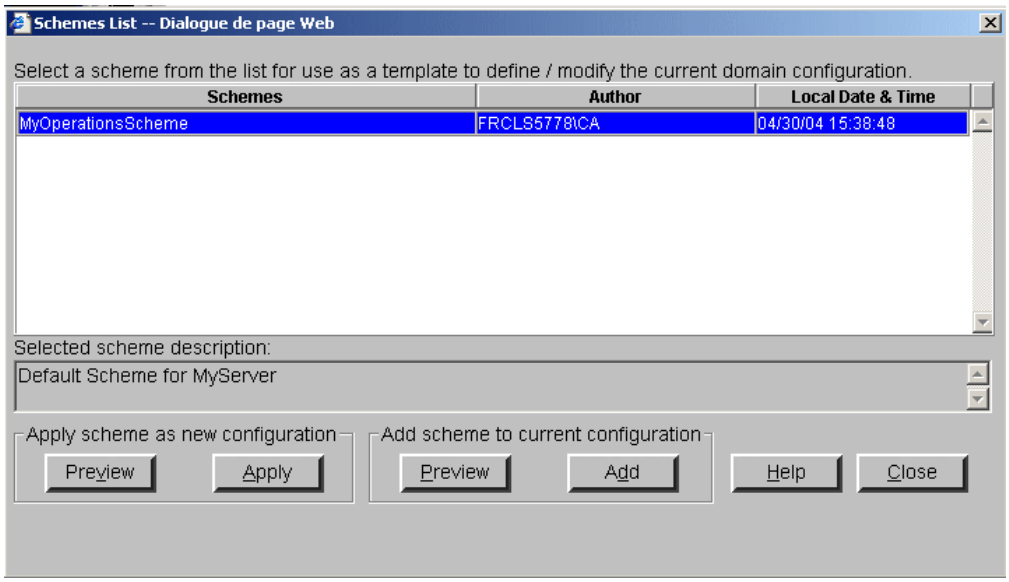
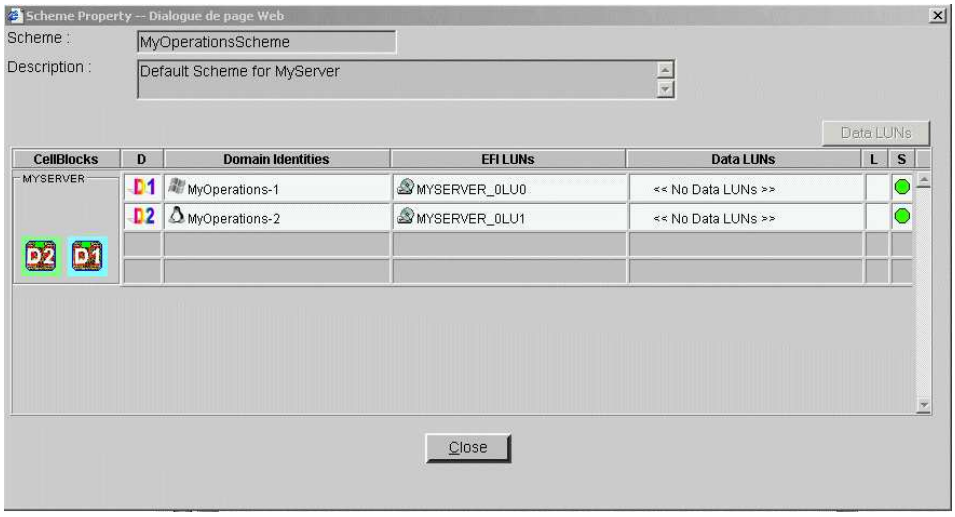


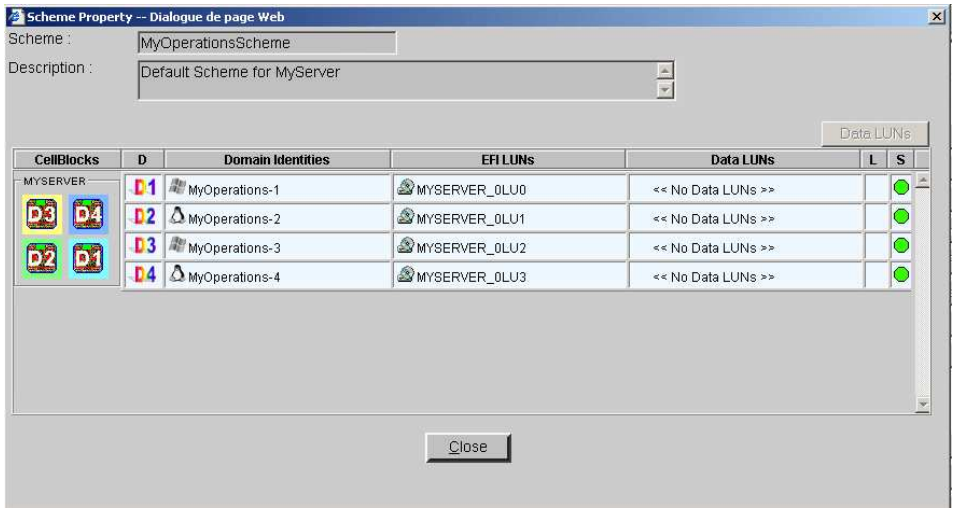
Figure 44. Schemes list dialog

3. Select the required **Scheme** from the list and click **Preview** to view scheme properties.

NovaScale 6080/6160 Server



NovaScale 6320 Server



CellBlocks	Shows the Central Subsystems included in the scheme and how they are partitioned into domains.
D	Identifies physical partitions.
Domain Identities	Shows the Identities allocated to each domain.
EFI LUNs	Indicates the EFI LUNs used to boot each domain.
Data LUNs	Indicates the Data LUNs used by each domain.
L	Indicates whether domain boot and data LUNs are linked to a fibre channel host. Reserved for systems connected to a SAN.
S	Indicates domain configuration status. A Green status icon indicates that the domain is configured correctly and is ready for use, a Red status icon indicates that the domain is not configured correctly and is not ready for use. If the status icon is Red, see *Configuring Domains*, on page 5-28.

Figure 45. Scheme properties dialog

Loading a Domain Configuration Scheme

To power on server domains, you must first load the required **Domain Configuration Scheme** from the **Domain Manager** Control pane. Once the domain configuration scheme has been loaded, domains can be powered up simultaneously or independently.

To load a scheme:

1. Click **Domain Manager** to open the Control pane. If a scheme has not been previously loaded, you are invited to load one.

Note:
If the required scheme is already loaded, it is available for domain management.
If a scheme is already loaded, but is not the required scheme, see *Adding Domains to the Current Domain Configuration* and *Replacing the Current Domain Configuration* below.

2. Click **Schemes** in the Toolbar to open the **Schemes List** dialog.

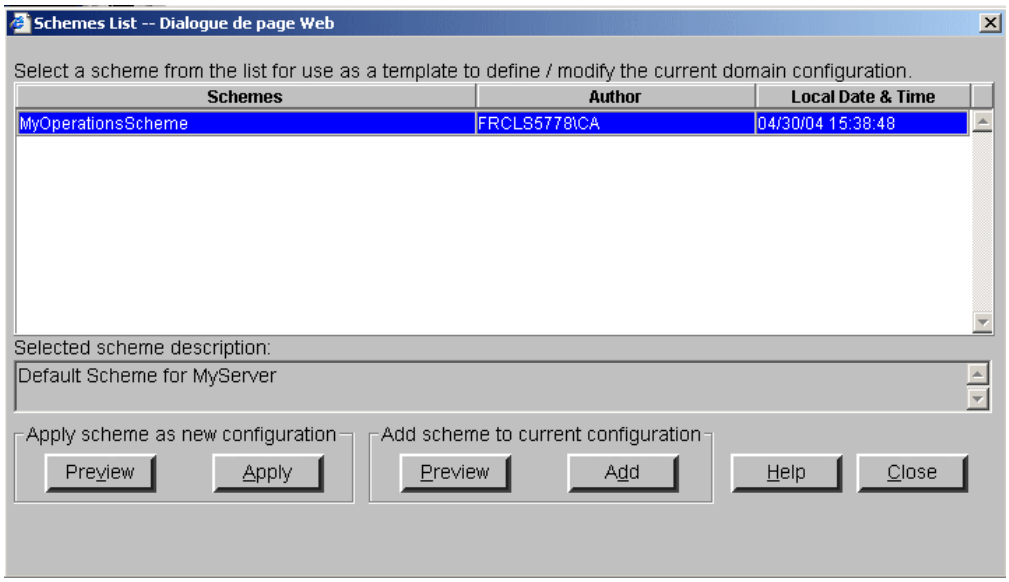
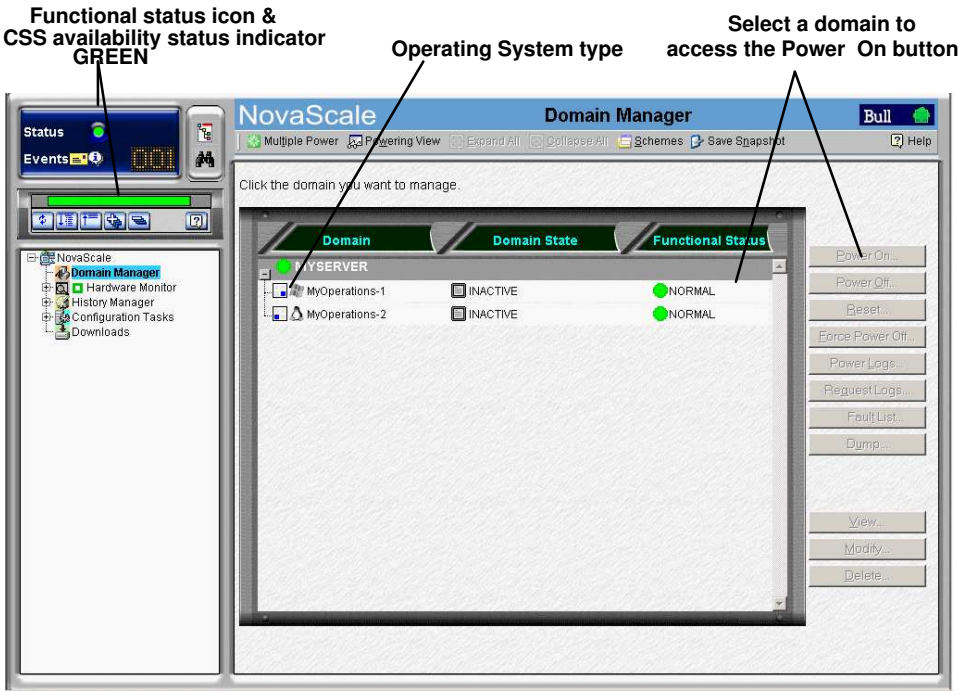


Figure 46. Schemes list dialog

3. Select the required **Scheme** from the list and click **Preview** to view scheme properties. See *Viewing a Domain Configuration Scheme*, on page 3-6.
4. Click **Apply**. A dialog box informs you that the selected scheme will replace the current domain configuration.
5. Click **Yes** to confirm. All the domains included in the selected scheme are loaded in the Control pane and are available for management.

If the domains are ready to be powered up, **INACTIVE** is displayed in the **Domain State** boxes. The **Power On** button becomes accessible once a domain has been selected.

NovaScale 6080/6160 Server



NovaScale 6320 Server

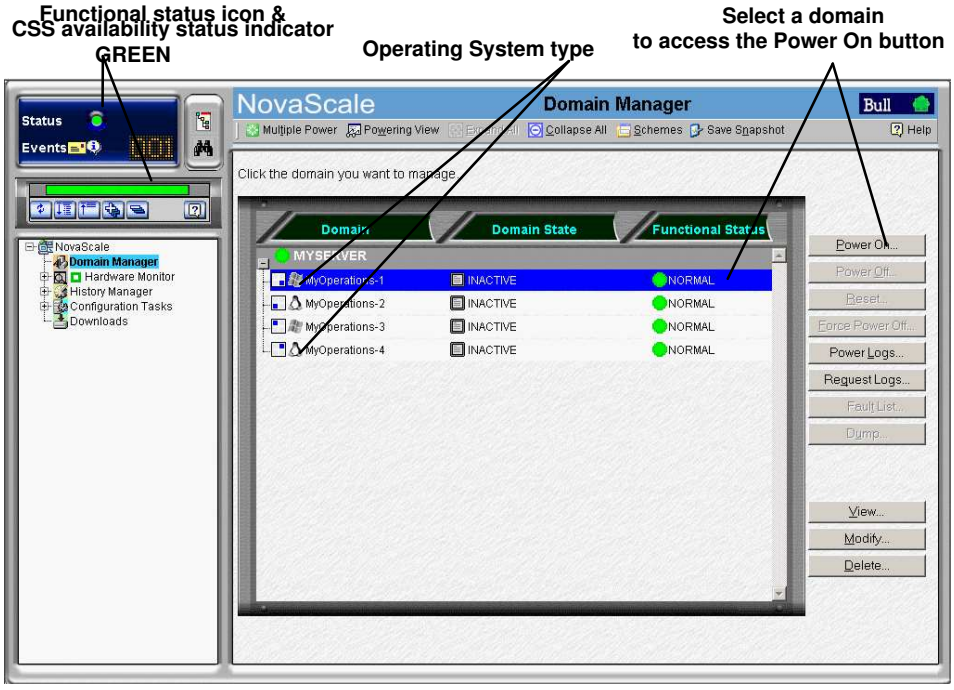


Figure 47. Domain Manager control pane

Note:
To display an Infotip listing the domain IP address, network name, cell composition and/or EFI LUN, hover the mouse over the icon:

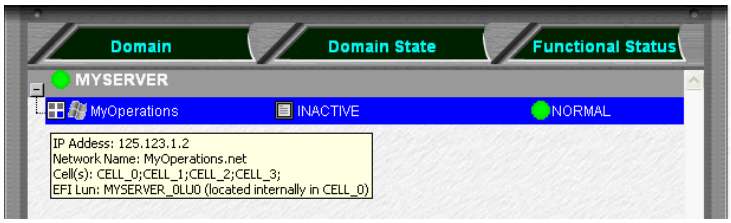


Figure 48. Domain Infotip

Adding Domains to the Current Domain Configuration

A scheme can include domains from one or more Central Subsystems. More domains can be made available for domain management by adding one or more schemes to the current domain configuration.

Notes:

- New domains can only include resources that are **INACTIVE** in the current domain configuration.
- The current domain configuration can be partially replaced by first deleting **INACTIVE** domains and then adding a new domain scheme
- New domains must be configured via **Configuration Tasks** before they are available for domain management. For further details, see *Configuring Domains*, on page 5-28.

To add domains:

1. Click **Domain Manager** to open the Control pane.
2. Click **Schemes** in the Toolbar to open the **Schemes List** dialog.
3. Select the required **Scheme** from the list and click **Preview** to view scheme properties. See *Viewing Domain Configuration Schemes*, on page 3-6.
4. Click **Add**. All the domains included in the scheme added are now available for management in the Control pane.

Replacing the Current Domain Configuration

Note:
All domains must be **INACTIVE** before the current domain configuration can be replaced.

To replace the current domain configuration:

1. Click **Domain Manager** to open the Control pane.
2. Check that all domains are **INACTIVE**. If a domain is not **INACTIVE**, it must be powered down before the current domain configuration can be replaced. See *Powering OFF a Domain*, on page 3-18.
3. If required, save the current domain configuration. See *Saving the Current Domain Configuration Snapshot*, on page 3-11.
4. Click **Schemes** in the Toolbar to open the **Schemes List** dialog.
5. Select the required scheme from the list and click **Preview** to view scheme properties. See *Viewing a Domain Configuration Scheme*, on page 3-6.

6. Click **Apply**. A dialog box informs you that the selected scheme will replace the current domain configuration.
7. Click **Yes** to confirm. All the domains included in the selected scheme are loaded in the Control pane and are available for management.

Saving the Current Domain Configuration Snapshot

You may want to save the current domain configuration, in particular if more than one scheme has been loaded and/or if you have modified domain configuration. When you save the current domain configuration, you create a new domain configuration scheme which is then available for domain management.

To save the current domain configuration snapshot:

1. Click **Domain Manager** to open the Control pane.
2. Click **Save Snapshot**. The **Save Snapshot** dialog opens.

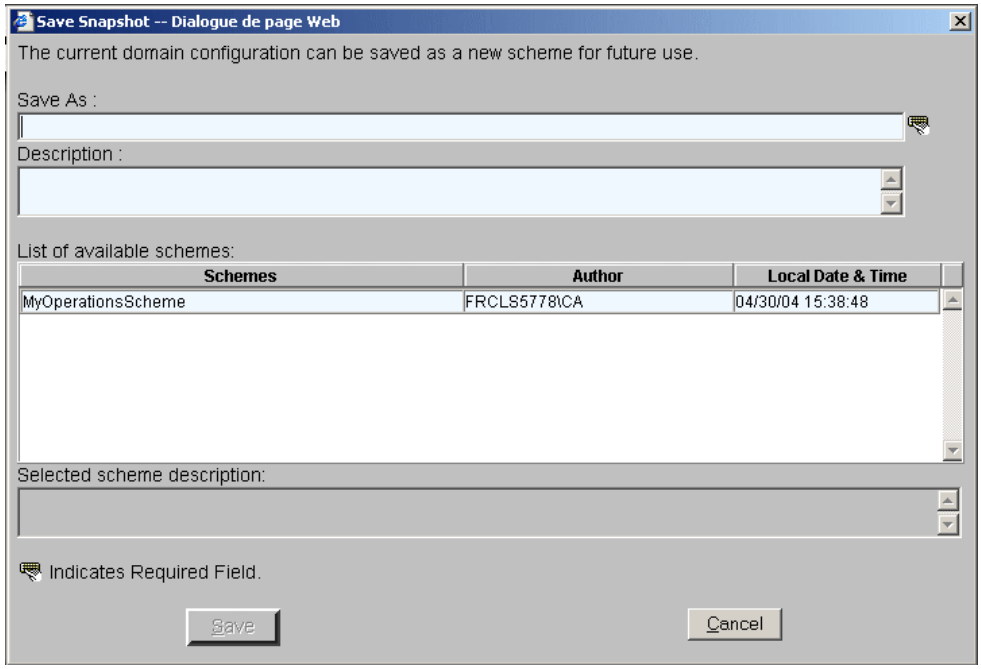


Figure 49. Save Snapshot dialog

3. Enter a name and description for the new domain configuration scheme and click **Save**. The **Snapshot** is now available as a scheme for domain management. For further details, see *Configuring Domains*, on page 5-28.

MyOperationsScheme Organization – NovaScale 6xx0 Servers

Domain Identity: MyOperations–1	
Hardware Cell	Cell_0
Operating System (customer–specific)	Windows or Linux
EFI LUN**	**<MyServer*>_0LU0 / <SAN>_LUN0
IOB	Module0_IOB0
QBBs	Module0_QBB0, Module0_QBB1
Domain KVM Ports	***CSS0_Mod0_IO0
Domain Identity: MyOperations–2	
Hardware Cell	Cell_1
Operating System (customer–specific)	Windows or Linux
EFI LUN**	**<MyServer*>_0LU1 / <SAN>_LUN1
IOB	Module0_IOB1
QBBs	Module0_QBB2, Module0_QBB3
Domain KVM Ports	***CSS0_Mod0_IO1
Domain Identity: MyOperations–3 (NovaScale 6320 Server)	
Hardware Cell	Cell_2
Operating System (customer–specific)	Windows or Linux
EFI LUN**	**<MyServer*>_0LU2 / <SAN>_LUN2
IOB	Module1_IOB0
QBBs	Module1_QBB0, Module1_QBB1
Domain KVM Ports	***CSS0_Mod1_IO0
Domain Identity: MyOperations–4 (NovaScale 6320 Server)	
Hardware Cell	Cell_3
Operating System (customer–specific)	Windows or Linux
EFI LUN**	**<MyServer*>_0LU3 / <SAN>_LUN3
IOB	Module1_IOB1
QBBs	Module1_QBB2, Module1_QBB3
Domain KVM Ports	***CSS0_Mod1_IO1

* *<MyServer>* = default server name, e.g.: NS6080–0, NS6160–0, NS6320–0

** EFI LUN: xLUx = Local boot LUN device location (*Modx*LU*IOx*):
0LU0 = LUN device connected to Module0, IOB0
0LU1 = LUN device connected to Module0, IOB1
0LU2 = LUN device connected to Module1, IOB0
0LU3 = LUN device connected to Module1, IOB1

***CSSx = CSS number, Modx = Module number, IOx = IO box number

Operating System type is indicated by the Microsoft Windows or Linux logo in the **Domain Identities** box.

Table 8. MyOperations Scheme organization

Notes:

- In the screen shots, tables, and examples in this guide:
  - **MyOperationsScheme–xx** is referred to as **MyOperationsScheme**
  - **MyOperations–xx–1** is referred to as **MyOperations–1**
  - **MyOperations–xx–2** is referred to as **MyOperations–2**
  - **MyOperations–xx–3** is referred to as **MyOperations–3**
  - **MyOperations–xx–4** is referred to as **MyOperations–4**
- **xx** in the default scheme and domain names represents the Central Subsystem HW identifier (from 00 to 16). For further details, refer to *PMB LEDs and Code Wheels*, on page 4-46.

Powering On a Domain

What You Can Do

During the domain power–on sequence, you can:

- *View functional status*
- *View power logs*
- *View powering sequences*
- *View BIOS info*
- *View request logs*
- *View domain configuration, resources and status*

Important:
Certain domain configuration and management tools are reserved for use with partitioned servers and extended systems. Please contact your Bull Sales Representative for sales information.

Once connected to the Customer's site power supply, the server initializes to the stand–by mode and the integrated PAP unit powers up. The server is not equipped with a physical power button and server domains are powered up from the PAM **Domain Manager** Control pane.

Check server functional status via the PAM **Status Pane**. If functional status is normal and the **CSS Availability** bar is green, server domains can be powered up.

Notes:

- When more than one domain is loaded in the Control pane, domains can be powered up sequentially or simultaneously. See *Powering on a Single Domain*, on page 3-14 and *Powering On Multiple Domains*, on page 3-15.
- Server domains may be powered up even if the server presents a minor fault. See *System Functional Status*, on page 4-4. However, you are advised to contact your Customer Service Engineer so that the fault can be repaired.

Powering On a Single Domain

NovaScale 5xx0 Servers

– If the domain is already loaded, it is available for domain management. Go to Step 2 below.

– If the domain is not already loaded, click **Synchronize Domains** in the toolbar to load the domain.

NovaScale 6xx0 Servers

1. Click **Domain Manager** to open the Control pane:

   – If the required domain configuration scheme is already loaded, the corresponding domain(s) are available for domain management. Go to Step 2.

   – If a scheme has not been previously loaded, you are invited to select and load a scheme. See *Viewing a Domain Configuration Scheme*, on page 3-6 and *Loading a Domain Configuration Scheme*, on page 3-8.

   – If a Scheme is already loaded, but is not the required Scheme, see *Adding Domains to the current Domain Configuration* and *Replacing the current Domain Configuration*, on page 3-10.

2. Select the required domain. If the domain is in the stand–by mode, **INACTIVE** is displayed in the **Domain Status** panel and the **Power On** button is accessible.

Important:
If INACTIVE is not displayed in the Domain Status panel and the Power On button is not accessible, check whether another user has already launched the power–up sequence on this domain. If the power–up sequence is not already in progress, see What To Do if an Incident Occurs, on page 3-69.

3. Click **Power On** to power up the domain and associated hardware components. The **Power On Confirmation** dialog opens.
4. Select the **View Power–On Logs** checkbox if you want power–on logs to be automatically displayed during the power–on sequence and click **Yes** to confirm.

   Domain hardware is powered up from the stand–by mode to the main mode and the Operating System is booted. As the power–on sequence progresses, power–on steps and domain state are displayed in the **Domain Status** panel, as shown in the following table.

Power On States
POWERING ON
POWERED ON – LOADING BIOS
BIOS READY – STARTING EFI
EFI STARTED – BOOTING OS
RUNNING

Table 9. Power–on states

   Once the **Power On** sequence has been successfully completed, **RUNNING** is displayed in the **Domain Status** panel and the **Power Off**, **Reset** and **Force Power Off** buttons become accessible.

   For a detailed view of the **Power On** sequence, click **Powering View** in the Toolbar. See *Viewing Domain Powering Sequences*, on page 3-29.

5. Repeat Steps 2 to 4 for each domain to be powered up.

Note:
If an error message is displayed in the **Domain Status** panel, the **Power On** sequence has failed. See *What To Do if an Incident Occurs*, on page 3-69.

Powering On Multiple Domains

To power up more than one domain:

NovaScale 5xx0 Servers

- If the domains are already loaded, they are available for domain management. Go to Step 2 below.
- If the domains are not already loaded, click **Synchronize Domains** in the toolbar to load all domains.

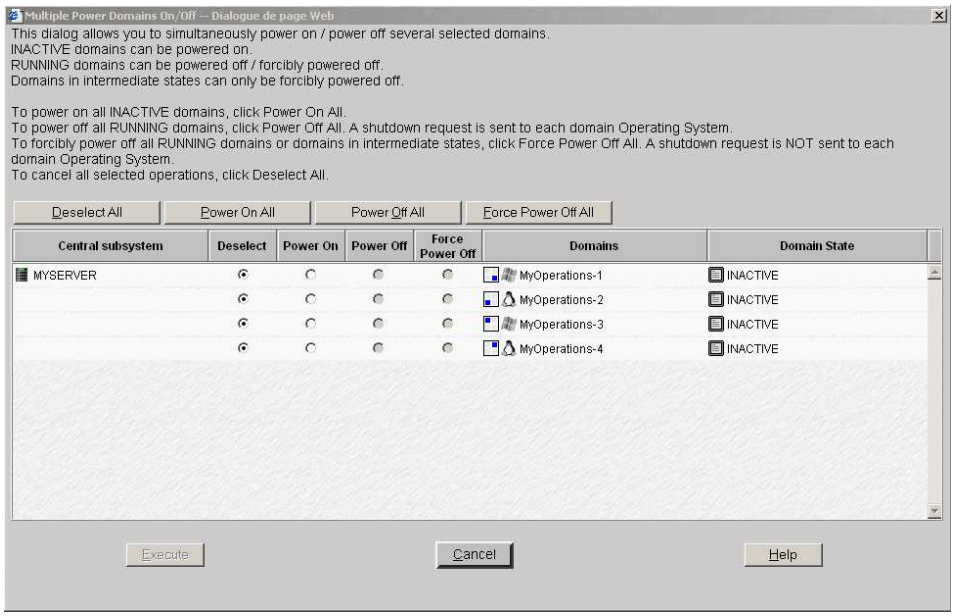
NovaScale 6xx0 Servers

1. Click **Domain Manager** to open the Control pane:
   - If the required domain configuration scheme is already loaded, the corresponding domain(s) are available for domain management. Go to Step 2.

– If a scheme has not been previously loaded, you are invited to select and load a scheme. See *Viewing a Domain Configuration Scheme*, on page 3-6 and *Loading a Domain Configuration Scheme*, on page 3-8.

– If a Scheme is already loaded, but is not the required Scheme, see *Adding Domains to the current Domain Configuration* and *Replacing the current Domain Configuration*, on page 3-10.

2. Click **Multiple Power**. The **Multiple Power Domains On/Off** dialog opens.



Deselect All	Cancels all selected operations.
Power On All	Powers on all INACTIVE domains.
Power Off All	Powers off all RUNNING domains.
Force Power Off All	Forcibly powers off all RUNNING or HUNG domains.
Deselect	Cancels the selected operation for this domain.
Power On	Powers on this domain if INACTIVE.
Power Off	Powers off this domain if RUNNING.
Force Power Off	Forcibly powers of this domain if RUNNING or HUNG.
Execute	Applies all selected operations.
Cancel	Cancels all selected operations.

Figure 50. Multiple power dialog – quadri–domain example

3. Click **Power On All** → **Execute** or select the required domain **Power On** radio buttons and click **Execute** to simultaneously power on the selected **INACTIVE** domains and associated hardware components.

   Domain hardware is powered up from the stand–by mode to the main mode and the Operating System is booted. As the power–on sequence progresses, power–on steps and domain state are displayed in the **Domain Status** panel, as shown in the following table.

Power On States
POWERING ON
POWERED ON – LOADING BIOS
BIOS READY – STARTING EFI

EFI STARTED – BOOTING OS
RUNNING

Table 10. Power–on states

Once the **Power On** sequence has been successfully completed, **RUNNING** is displayed in the **Domain Status** panel and the **Power Off**, **Reset** and **Force Power Off** buttons become accessible.

For a detailed view of the **Power On** sequence, click **Powering View** in the Toolbar. See *Viewing Domain Powering Sequences*, on page 3-29.

Note:
If an error message is displayed in the **Domain Status** panel, the **Power On** sequence has failed. See *What To Do if an Incident Occurs*, on page 3-69.

Powering Off a Domain

What You Can Do

During the domain power–off sequence, you can:

- *View functional status*
- *View power logs*
- *View powering sequences*
- *View BIOS info*
- *View request logs*
- *View domain configuration, resources and status*

Server domains can either be powered off from the Operating System (RECOMMENDED) or from the PAM **Domain Manager**, according to Operating System power settings.

The PAM **Power Off** command is a shutdown request to the Operating System. If the Operating System is configured to accept a PAM power off request, it will save data, close open applications and shut down. Domain hardware will power down to the stand–by mode. The Operating System may also be configured to request Operator confirmation before accepting a PAM power off request. Refer to the applicable documentation delivered with the Operating System for further details.

Notes:

- When more than one domain is loaded in the Control pane, domains can be powered off sequentially or simultaneously. See *Powering Off a Single Domain*, on page 3-18 and *Powering Off Multiple Domains*, on page 3-19.
- Server domains may be powered up even if the server presents a minor fault. See *System Functional Status*, on page 4-4. However, you are advised to contact your Customer Service Engineer so that the fault can be repaired.

Powering Off a Single Domain

1. Click **Domain Manager** to open the Control pane.
2. Select the required domain. If the domain is in the powered–on mode, **RUNNING** is displayed in the **Domain Status** panel and the **Power OFF** button is accessible.

Important:
If RUNNING is not displayed in the Domain Status panel and the Power OFF button is not accessible, another user may have already launched the power–off sequence or may be working under EFI SHELL. If the power–off sequence is not already in progress and/or if EFI STARTED is not displayed in the Domain Status panel, see *What To Do if an Incident Occurs*, on page 3-69.

3. Click **Power Off** to power down the domain and associated hardware components. The **Power Off Confirmation** dialog opens.
4. Select the **View Power–Off Logs** checkbox if you want power–off logs to be automatically displayed during the power–off sequence and click **Yes** to confirm.

   The Operating System saves data, closes open applications and shuts down. Domain hardware is powered down from the main mode to the stand–by mode. As the power–off sequence progresses, power–off steps and domain state are displayed in the **Domain Status** panel, as shown in the following table.

Power Off States
POWERING DOWN
INACTIVE

Table 11. Power–off states

Once the **Power Off** sequence has been successfully completed, **INACTIVE** is displayed in the **Domain Status** panel and the **Power On** button becomes accessible.

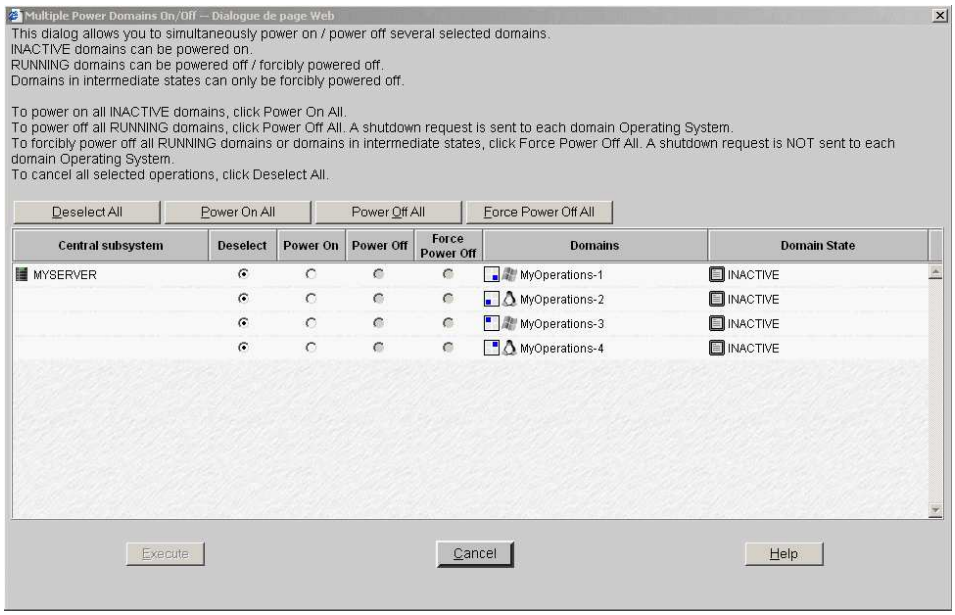
For a detailed view of the **Power Off** sequence, click **Powering View** in the Toolbar. See *Viewing Domain Powering Sequences*, on page 3-29.

5. Repeat Steps 2 to 4 for each domain to be powered down.

Note:
If an error message is displayed in the **Domain Status** panel, the **Power Off** sequence has failed. See *What To Do if an Incident Occurs*, on page 3-69.

Powering Off Multiple Domains

1. Click **Domain Manager** to open the Control pane.
2. Click **Multiple Power**. The **Multiple Power Domains On/Off** dialog opens.



Deselect All	Cancels all selected operations.
Power On All	Powers on all INACTIVE domains.
Power Off All	Powers off all RUNNING domains.
Force Power Off All	Forcibly powers off all RUNNING or HUNG domains.
Deselect	Cancels the selected operation for this domain.
Power On	Powers on this domain if INACTIVE.
Power Off	Powers off this domain if RUNNING.
Force Power Off	Forcibly powers of this domain if RUNNING or HUNG.
Execute	Applies all selected operations.
Cancel	Cancels all selected operations.

Figure 51. Multiple power dialog – quadri–domain example

3. Click **Power Off All** → **Execute** or select the required domain **Power Off** radio buttons and click **Execute** to simultaneously power off the selected **RUNNING** domains and associated hardware components.

   The Operating System saves data, closes open applications and shuts down. Domain hardware is powered down from the main mode to the stand–by mode. As the power–off sequence progresses, power–off steps and domain state are displayed in the **Domain Status** panel, as shown in the following table.

Power Off States
POWERING DOWN
INACTIVE

Table 12. Power–off states

Once the **Power Off** sequence has been successfully completed, **INACTIVE** is displayed in the **Domain Status** panel and the **Power On** button becomes accessible.

For a detailed view of the **Power Off** sequence, click **Powering View** in the Toolbar. See *Viewing Domain Powering Sequences*, on page 3-29.

Note:
If an error message is displayed in the **Domain Status** panel, the **Power Off** sequence has failed. See *What To Do if an Incident Occurs*, on page 3-69.

Forcing a Domain Power Off

What You Can Do

During the domain force power–off sequence, you can:

- *View functional status*
- *View power logs*
- *View powering sequences*
- *View BIOS info*
- *View request logs*
- *View domain configuration, resources and status*

The **Force Power Off** command powers down domain hardware to the standby mode independently of the Operating System. This command should only be used if the Operating System is not running or is not configured / not able to respond to a standard power off command.

Note:
A standard power off command is a shutdown request to the Operating System. Refer to the applicable documentation delivered with the Operating System for further details.

In the event of a critical fault, PAM software automatically forces a domain power off.

Notes:

- When more than one domain is loaded in the Control pane, domains can be forcibly powered off sequentially or simultaneously. See *Forcibly Powering Off a Single Domain*, on page 3-22 and *Forcibly Powering off Multiple Domains*, on page 3-22.
- Server domains may be powered up even if the server presents a minor fault. See *System Functional Status*, on page 4-4. However, you are advised to contact your Customer Service Engineer so that the fault can be repaired.

Warning:
The Force Power Off command may result in domain data loss and file corruption. NEVER use the Force Power Off command if a RECOVERING BIOS error message is displayed. (The BIOS recovery program automatically re–flashes the BIOS when certain problems occur during initialization).

Forcibly Powering Off a Single Domain

1. Click **Domain Manager** to open the Control pane.
2. Select the required domain. If **INACTIVE** is NOT displayed in the **Domain Status** panel, the **Force Power Off** button is accessible.
3. Click **Force Power Off** to override the Operating System and forcibly power down the domain and associated hardware components without closing running applications and saving data. The **Force Power Off Confirmation** dialog opens.
4. Select the **View Power–Off Logs** checkbox if you want power–off logs to be automatically displayed during the power–off sequence and click **Yes** to confirm.

   Domain hardware is powered down from the main mode to the stand–by mode. As the force power–off sequence progresses, power–off steps and domain state are displayed in the **Domain Status** panel, as shown in the following table.

Force Power Off States
POWERING DOWN
INACTIVE

Table 13. Force power–off states

Once the **Force Power Off** sequence has been successfully completed, **INACTIVE** is displayed in the **Domain Status** panel and the **Power On** button becomes accessible.

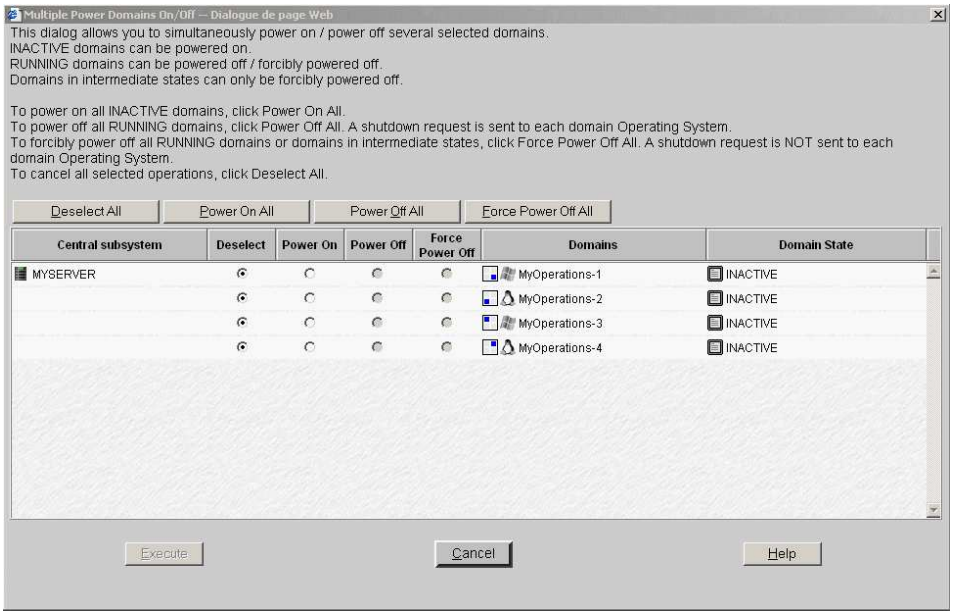
For a detailed view of the **Force Power Off** sequence, click **Powering View** in the Toolbar. See *Viewing Domain Powering Sequences*, on page 3-29.

5. Repeat Steps 2 to 4 for each domain to be forcibly powered down.

Note:
If an error message is displayed in the **Domain Status** panel, the **Power Off** sequence has failed. See *What To Do if an Incident Occurs*, on page 3-69.

Forcibly Powering Off Multiple Domains

1. Click **Domain Manager** to open the Control pane.
2. Click **Multiple Power**. The **Multiple Power Domains On/Off** dialog opens.



Deselect All	Cancels all selected operations.
Power On All	Powers on all INACTIVE domains.
Power Off All	Powers off all RUNNING domains.
Force Power Off All	Forcibly powers off all RUNNING or HUNG domains.
Deselect	Cancels the selected operation for this domain.
Power On	Powers on this domain if INACTIVE.
Power Off	Powers off this domain if RUNNING.
Force Power Off	Forcibly powers of this domain if RUNNING or HUNG.
Execute	Applies all selected operations.
Cancel	Cancels all selected operations.

Figure 52. Multiple power dialog – quadri–domain example

3. Click **Force Power Off All**→ **Execute** or select the required domain **Force Power Off** radio buttons and click **Execute** to to override the Operating System and forcibly power down the selected domains and associated hardware components without closing running applications and saving data.

Power Off States
POWERING DOWN
INACTIVE

Table 14. Power–off states

Once the **Power Off** sequence has been successfully completed, **INACTIVE** is displayed in the **Domain Status** panel and the **Power On** button becomes accessible.

For a detailed view of the **Power Off** sequence, click **Powering View** in the Toolbar. See *Viewing Domain Powering Sequences*, on page 3-29.

☞ **Note:**
If an error message is displayed in the **Domain Status** panel, the **Power Off** sequence has failed. See *What To Do if an Incident Occurs*, on page 3-69.

Manually Resetting a Domain

What You Can Do

During the domain reset sequence, you can:

- *View functional status*
- *View power logs*
- *View powering sequences*
- *View BIOS info*
- *View request logs*
- *View domain configuration, resources and status*

The **Reset** command is used to restart the current Operating System without powering off/on the domain.

Warning:
The Reset command should only be used if the Operating System is not running or is not able to respond to a standard Power Off command. The Reset command may result in domain data loss and file corruption. The Reset command does not power down domain hardware (warm reboot).

To manually reset a domain:

1. Click **Domain Manager** to open the Control pane.
2. Select the required domain. If **INACTIVE** is NOT displayed in the **Domain Status** panel, the **Reset** button is accessible.
3. Click **Reset** to override the Operating System and forcibly perform a warm reboot of the domain BIOS, EFI and Operating System without closing running applications and saving data. The **Reset Confirmation** dialog opens.
4. Click **Yes** to confirm the **Reset** command.

   As the reset sequence progresses, reset steps and domain state are displayed in the **Domain Status** panel, as shown in the following table.

Reset States
POWERED ON – LOADING BIOS
BIOS READY – STARTING EFI
EFI STARTED – BOOTING OS
RUNNING

Table 15. Reset states

   Once the **Reset** sequence has been successfully completed, **RUNNING** is displayed in the **Domain Status** panel and the **Power Off**, **Reset** and **Force Power Off** buttons become accessible.
   For a detailed view of the **Reset** sequence, click **Powering View** in the Toolbar. See *Viewing Domain Powering Sequences*, on page 3-29.

5. Repeat Steps 2 to 4 for each domain to be reset.

Note:
If an error message is displayed in the **Domain Status** panel, the **Power On** sequence has failed. See *What To Do if an Incident Occurs*, on page 3-69.

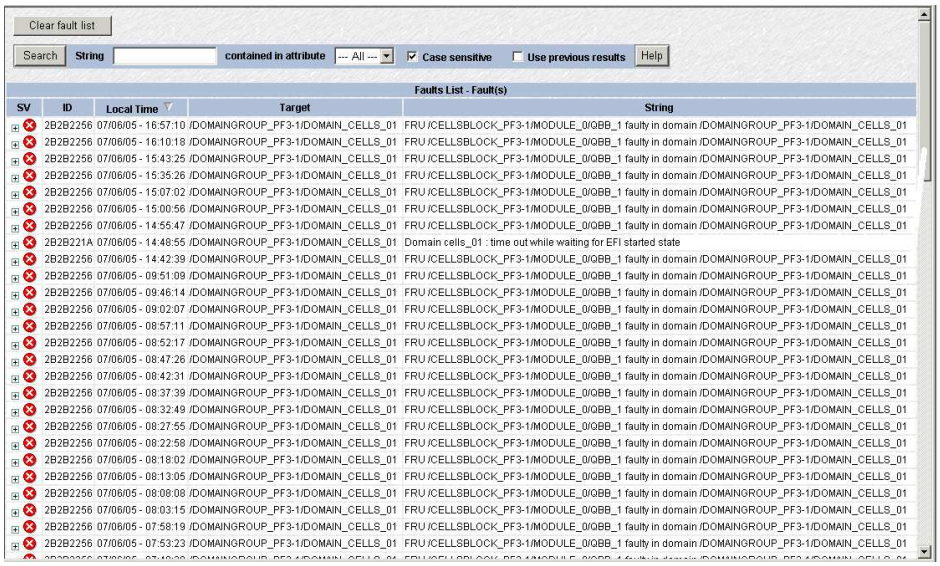
Viewing a Domain Fault List

The **Domain Fault List** page allows you to view messages about the faults encountered since the beginning of the last power–on sequence on the selected domain. The fault list is automatically cleared when a new domain power–on sequence is started.

Note:
For details about PAM messages, see *Viewing and Managing PAM Messages, History Files and Archives*, on page 4-28.

To view the domain fault list:

1. Click **Domain Manager** to open the Control pane.
2. Select the required domain and click **Fault List** in the Command bar to open the **Fault List** dialog.



Button	Use
Clear fault list	To manually clear the fault list.
Help	To access context sensitive help.
Search – **String** – **Contained in attribute** – **Case sensitive** – **Use previous results**	To search for specific messages, according to: – Alphanumeric identifier (ID), e.g. 2B2B2214 above. – Message Source, Target, String, Data attributes. – Upper case / lower case letters. – Multiple search option used to search again from the results obtained from the previous search(es).
+	To view the message and access context sensitive help.
Help on message	To view the related help message.
Column Header	**Use**
SV	To sort messages according to severity level.
ID	To sort messages according to Message IDentifier.
Local Time	To sort messages according to message local time and date.
Target	To sort messages according to the component referred to in the message.
String	To sort messages according to message text string.

Figure 53. Domain fault list dialog – example

Performing a Domain Memory Dump

The **Dump** command is used when the Operating System hangs and allows technicians to diagnose software problems by saving domain memory.

Warning:
The Dump command should only be used if the Operating System is not able to respond to a standard Power OFF command. The Dump command may result in domain data loss and file corruption.
The Dump command does not power down domain hardware (automatic warm reboot).

To perform a domain memory dump:

1. Click **Domain Manager** to open the Control pane.
2. Select the required domain. If **RUNNING** is displayed in the **Domain Status** panel, the **Dump** button is accessible.
3. Click **Dump** to override the Operating System and forcibly clear domain core memory which will be copied to the PAP unit hard disk for analysis. The **Dump Confirmation** dialog opens.
4. Click **Yes** to confirm the **Dump** command.

   The **Dump** sequence results in a warm reboot of the domain BIOS, EFI and Operating System (without closing running applications and saving data).

   As the dump sequence progresses, dump steps and domain state are displayed in the **Domain Status** panel, as shown in the following table.

Dump States
POWERED ON – LOADING BIOS
BIOS READY – STARTING EFI
EFI STARTED – BOOTING OS
RUNNING

Table 16. Dump states

   Once the **Dump** sequence has been successfully completed, **RUNNING** is displayed in the **Domain Status** panel and the **Power Off**, **Reset** and **Force Power Off** buttons become accessible.

5. Repeat Steps 2 to 4 for each domain on which you want to perform a memory dump.

Note:
If an error message is displayed in the **Domain Status** panel, the **Dump** sequence has failed. See *What To Do if an Incident Occurs*, on page 3-69.

Viewing Domain Functional Status

The **Domain Functional Status** indicator in the **Domain Manager** Control pane shows the **functional status of the last action** performed on each domain, e.g. if the last **Power ON/OFF** sequence was successful, the indicator is green, and also reflects **the status of domain hardware component**s.

As Customer Administrator, you can toggle the **PAM Tree** to display the synthetic functional status (round, colored indicator next to the **Domain Manager** node) of all the domains loaded in the **Domain Manager** Control pane. For example:

- If the last **Power ON/OFF** sequence was successful on all domains and the status of all domain hardware components is normal, the indicator is green
- If the last **Power ON/OFF** sequence failed on at least one domain and/or the status of at least one domain hardware component is fatal, the indicator is red.

Indicator	Status	Explanation
Green	**NORMAL**	**Control Pane** The last command on this domain was successful. or The domain fault list has been cleared. **Note:** Domain functional status is reset to **NORMAL** when a new domain power–on sequence is started. **PAM Tree** The last command on all domains was successful. or All domain fault lists have been cleared.
Yellow	**WARNING**	**Control Pane** An automatic **Recovery** command has been launched on this domain. or A **WARNING** status for a domain hardware component has been detected by the BIOS and a warning error has been added to the domain fault list. or The domain fault list was not empty when PAM was started. **PAM Tree** An automatic **Recovery** command has been launched on at least one domain. or A **WARNING** status for at least one domain hardware component has been detected by the BIOS and a warning error has been added to the domain fault list. or At least one domain fault list was not empty when PAM was started. **Note:** The BIOS recovery program automatically re–flashes the BIOS when certain problems occur during initialization
Orange	**CRITICAL**	**Control Pane** The last command on this domain was not successful and a critical error has been added to the domain fault list. **PAM Tree** The last command on at least one domain was not successful.
Red	**FATAL**	**Control Pane** The last command on this domain has failed and a fatal error has been added to the domain fault list. **PAM Tree** The last command on at least one domain has failed.

Table 17. Domain functional status indicators

Viewing Domain Power Logs

Power logs are recorded during domain power ON/OFF sequences. This information is particularly useful for troubleshooting. See *What To Do if an Incident Occurs*, on page 3-69.

During a Power ON/OFF Sequence

1. Click **Domain Manager** to open the Control pane.
2. Select the required domain and launch the domain power ON/OFF sequence, as required.
3. Select the **View Power Logs** checkbox in the **Power Confirmation** dialog to automatically display power logs during the powering sequence.

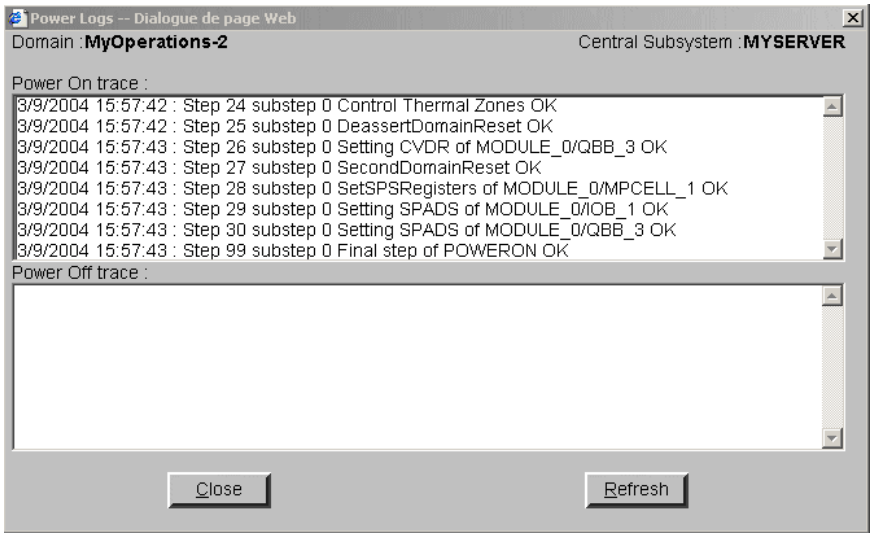


Figure 54. Power logs dialog

Outside a Power ON/OFF Sequence

NovaScale 5xx0 Servers

- Click the **Power Logs** button in the Domain Manager Command bar.

NovaScale 6xx0 Servers

- Click **Powering View** → **Power Logs** in the Domain Manager Toolbar.

Note:
Existing power logs are erased when a new power ON sequence is launched.

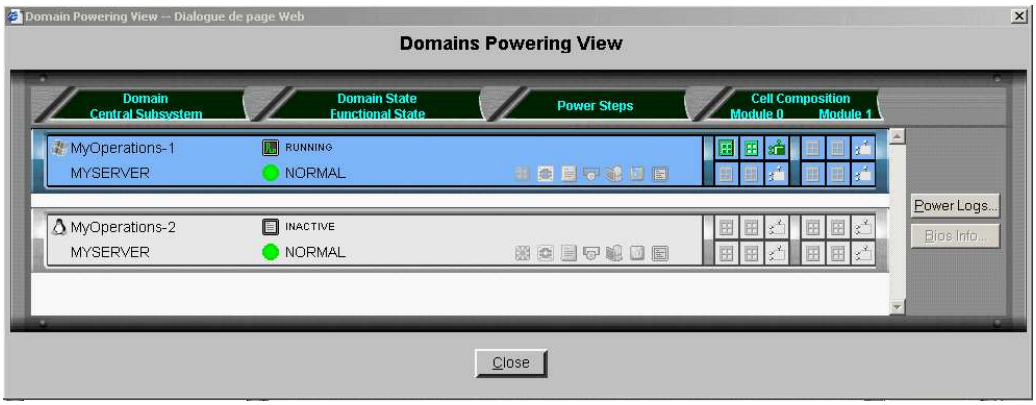
Viewing Domain Powering Sequences

NovaScale 5xx0 Servers

Domain powering sequence steps and states can be viewed from the **Domain Status** panel.

NovaScale 6xx0 Servers

A detailed view of powering sequences can be displayed by clicking **Powering View** in the Domain Manager Toolbar after a power request.



Status Panel Item	Explanation
Domain	Selected domain identity.
Central Subsystem	Name of the Central Subsystem containing the domain.
Domain State	Current power sequence step.
Functional Status	Functional status of the last action performed on the domain. See *Viewing Domain Functional Status*, on page 3-27.
Power Steps	Dynamic, graphic representation of power sequence steps.
Cell Composition	Graphic representation of the core hardware elements in each cell (hardware partition): QBB(s), IOB(s) – Master / Slave. See *Configuring Domains*, on page 5-28.

Figure 55. Powering view dialog

Note:
An Infotip can be obtained by hovering the mouse over the required element.

Viewing Domain BIOS Info

BIOS information is particularly useful for troubleshooting. See *What To Do if an Incident Occurs*, on page 3-69.

To view BIOS information:

1. Click **Domain Manager** to open the Control pane.
2. Select the required domain.
3. Click:

   NovaScale 5xx0 Servers
   – **View** → **BIOS Info** in the Command bar.

   NovaScale 6xx0 Servers
   – **Powering View** → **BIOS Info** in the Toolbar.

   The **BIOS Info** dialog opens, displaying the following information:

   – BIOS version used by the domain,

   – BIOS boot post codes. See *BIOS POST Codes*, on page 0.
4. Click **Refresh** to update BIOS information.

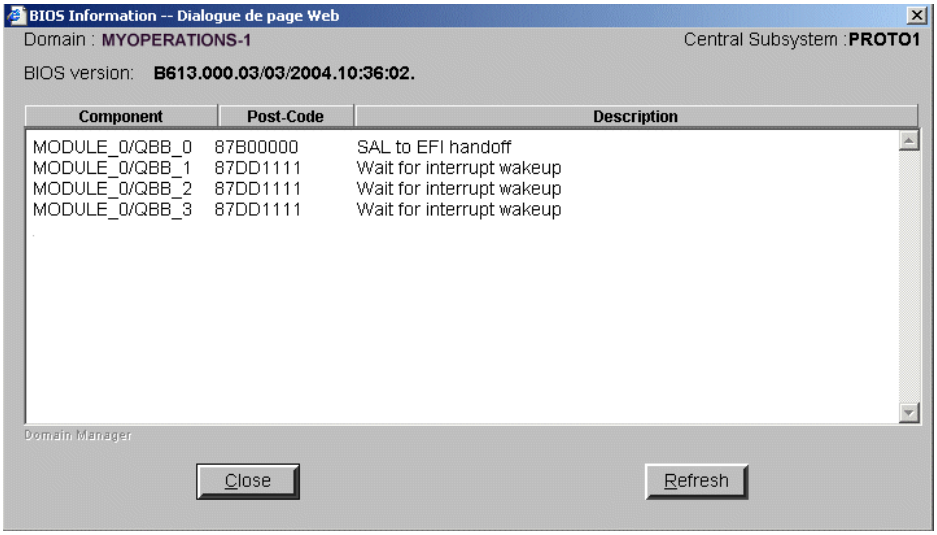


Figure 56. BIOS Info dialog

Viewing Domain Request Logs

Important:
NovaScale 6xx0 Servers ONLY. Please contact your Bull Sales Representative for sales information.

The **Request Logs** dialog gives direct access to a trace of major domain operations (requests) and indicates their initiators (requestors).

To view Request logs:

1. Click **Domain Manager** to open the Control pane.
2. Select the required domain.
3. Click **Request Logs** in the Command bar.

   The **Request Logs** dialog displays the following information:

   – **Power On** requests and requestors,

   – **Power Off** requests and requestors,

   – **Reset** requests and requestors.

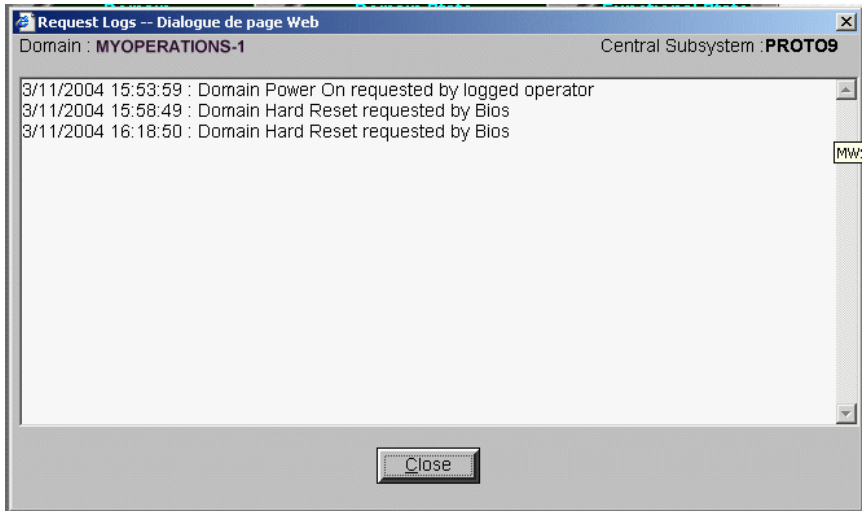


Figure 57. Request Logs dialog

Note:
Existing request logs are erased when a new power ON sequence is launched.

Viewing Domain Configuration, Resources and Status

Important:
NovaScale 6xx0 Servers ONLY. Please contact your Bull Sales Representative for sales information.

Notes:

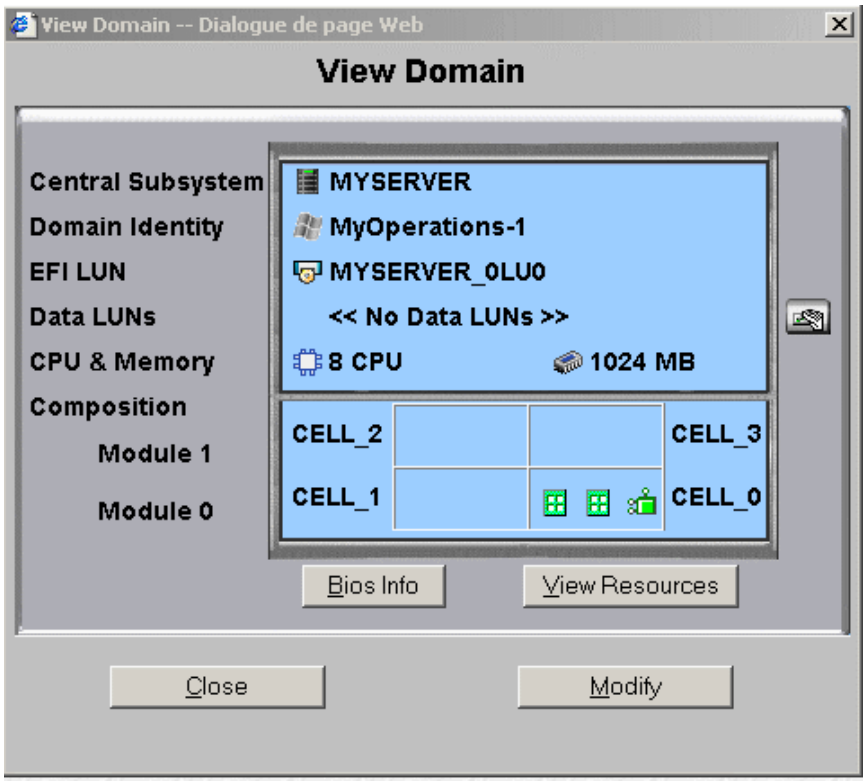
- Certain features described below are only available if you are connected to a Storage Area Network (SAN).
  Please contact your Bull Sales Representative for sales information.
- In the screen shots, tables, and examples in this guide:
  - **MyOperationsScheme–xx** is referred to as **MyOperationsScheme**
  - **MyOperations–xx–1** is referred to as **MyOperations–1**
  - **MyOperations–xx–2** is referred to as **MyOperations–2**
  - **MyOperations–xx–3** is referred to as **MyOperations–3**
  - **MyOperations–xx–4** is referred to as **MyOperations–4**

Information about the resources allocated to each domain is permanently accessible from the **Domain Manager** Control pane:

- Graphic representation of domain configuration.
- Non–graphic summary of the hardware resources allocated to a domain.
- Graphic summary of the hardware resources allocated to a domain and their status.

Viewing Domain Configuration

1. Click **Domain Manager** to open the Control pane.
2. Select the required domain.
3. Click **View** in the Command bar to open the **View Domain** dialog.



* Module 1 (Cell_2 & Cell_3): does not equip mono–module servers

Figure 58. View Domain dialog

View Domain Dialog Items

Domain Item	Explanation
Central Subsystem	Name of the Central Subsystem containing the domain.
Domain Identity	Logical name and profile given to the domain.
EFI LUN	Boot LUN device location: **NovaScale 6080/6160 Server** 0LU0 = LUN device connected to Module0, IOB0 0LU1 = LUN device connected to Module0, IOB1 **NovaScale 6320 Server** 0LU0 = LUN device connected to Module0, IOB0 0LU1 = LUN device connected to Module0, IOB1 0LU2 = LUN device connected to Module1, IOB0 0LU3 = LUN device connected to Module1, IOB1
Data LUNs	The Data LUNs allocated to this domain. Reserved for systems connected to a SAN.
CPU	Number of processors used by the domain.
Memory	Size of memory used by the domain.
Composition	Graphic representation of the main hardware elements used by the domain. See **Note** below.
Module	Module housing the cell(s) used by the domain. **Module0** = Cell_0 and Cell_1 **Module1** = Cell_2 and Cell_3*
Cell	Cell(s) or hardware partition(s) used by the domain. **NovaScale 6080/6160 Server** **Cell_0** = Mod0_QBB0, Mod0_QBB1, Mod0_IOB0 **Cell_1** = Mod0_QBB2, Mod0_QBB3, Mod0_IOB1 **NovaScale 6320 Server** **Cell_0** = Mod0_QBB0, Mod0_QBB1, Mod0_IOB0 **Cell_1** = Mod0_QBB2, Mod0_QBB3, Mod0_IOB1 **Cell_2** = Mod1_QBB0, Mod1_QBB1, Mod1_IOB0 **Cell_3** = Mod1_QBB2, Mod1_QBB3, Mod1_IOB1 See *Configuring Domains*, on page 5-28.

* Module 1 (Cell_2 & Cell_3): does not equip mono–module servers

Figure 59. View Domain dialog

Note:
When the domain is **RUNNING**, an Infotip identifying the Master QBB / IOB can be obtained by hovering the mouse over the QBB / IOB icons.
Master IOB = IOB to which the domain boot LUN device is connected.
Master QBB = QBB required to start the domain.

Viewing Domain Hardware Resources

1. Click **Domain Manager** to open the Control pane.
2. Select the required domain and click **View Resources** in the **View Domain** dialog to open the **Domain Hardware Resources** dialog.

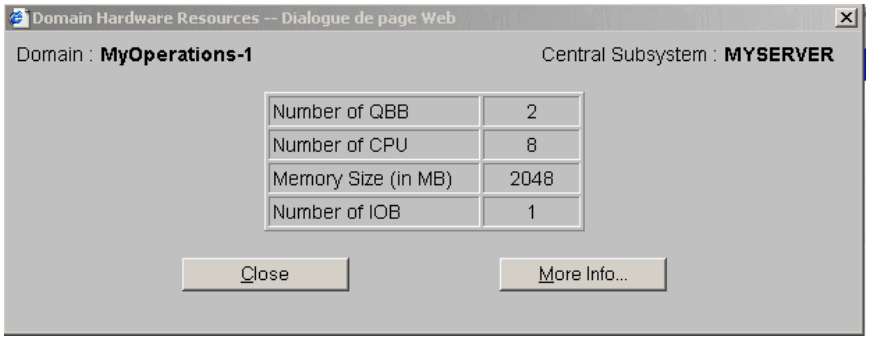


Figure 60. Domain Hardware Resources dialog

Viewing Domain Details and Status

1. Click **Domain Manager** to open the Control pane.
2. Click **View** → **View Resources** → **More Info...** in the Command bar to open the **Domain Hardware Details** dialog.

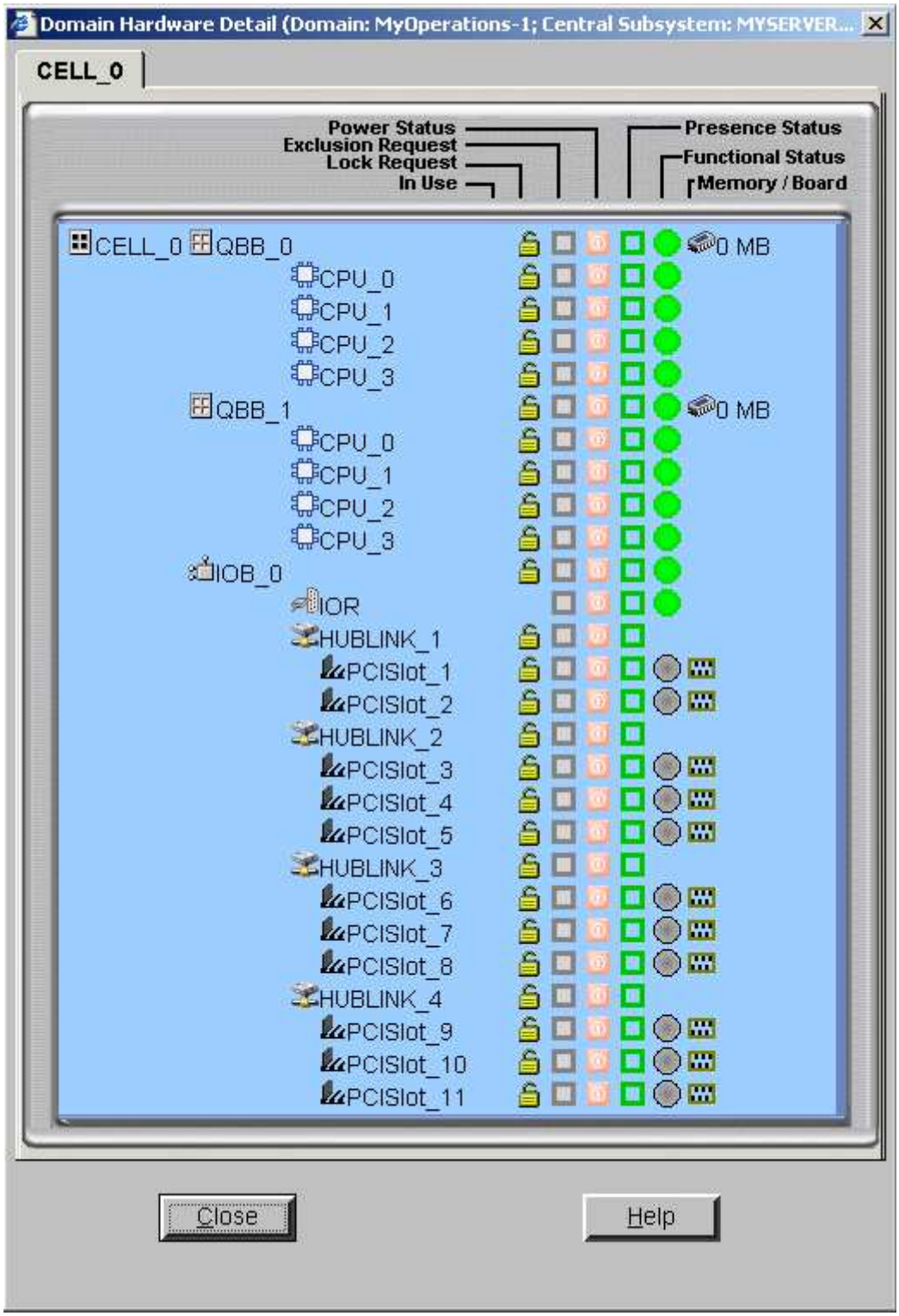


Figure 61. Domain Hardware Details dialog

Domain Hardware Details icons are explained in the following table.

Item	Icon	Meaning
Power Status	 Green	Main power is ON.
	 Red	Main power is OFF. Stand–by power is ON.
	 Pink	Main power is OFF. Stand–by power is OFF.
	 Blinking pink	Stand–by power is Faulty.
	 Blinking red	Main power is Faulty. Stand–by power may be ON, OFF or Faulty.
	 Gray	Main power status is Unknown.
Exclusion Request	 Gray	To be logically included at the next domain power ON.
	 Yellow/ red	To be logically excluded at the next domain power ON.
Lock Request		To be functionally included in the domain (unlocked).
		To be functionally excluded from the domain (locked).
Used	 Green	Used by the domain.
	 Gray	Not used by the domain.
Presence Status	 Green	Physically present and accessible.
	 Red	Was present in a previous configuration but has disappeared.
	 Purple	Cannot be computed (detection circuit error).
Functional Status	 Green	No problem detected, operating correctly.
	Yellow	Minor problem reported, still operational.
	 Orange	Serious problem reported, no longer capable of operating correctly. PAM may generate an OS shutdown request.
	 Red	Major problem reported. PAM may automatically shut down the OS. System integrity is jeopardized.
	 Purple	Cannot be computed (detection circuit error).
Memory		Memory available per QBB.
Board		PCI slot occupied.
		PCI slot empty.

Table 18. Domain hardware details icons

Note:
When the domain is **INACTIVE**, the **Domain Hardware Details** dialog indicates the resources that PAM will try to initialize for the domain during the next **Power ON** sequence. When the domain is **RUNNING**, the **Domain Hardware Details** dialog indicates the resources that PAM successfully initialized for the domain during the last **Power ON** or **Reset** sequence.

For more information about domain hardware, see:

- Presence Status Indicators, on page 4-6
- Functional Status Indicators, on page 4-7
- Viewing Server Hardware Status, on page 4-13
- Configuring Domains, on page 3-27
- Excluding/Including Hardware Elements, on page 4-25
- Limiting Access to Hardware Resources, on page 5-62

Modifying Domain Configuration

Important:
Reserved for partitioned servers and extended systems.
Certain features described below are only available if you are connected to a Storage Area Network (SAN).
Please contact your Bull Sales Representative for sales information.

What You Can Do

- *Swap a Domain EFI Boot LUN*
- *Add a Data LUN*
- *Remove a Data LUN*
- *Link a LUN to a Fibre Channel Host*
- *Add Cells to a Domain*
- *Remove Cells from a Domain*
- *Lock Hardware Components*
- *Delete a Domain*

The Bull NovaScale 6000 Series server is designed around a flexible, cell–based, midplane architecture for enhanced performance, scalability and availability and is designed to operate as:

- two SMP systems, one using the hardware resources in Cell_0, the other using the hardware resources in Cell_1 (default configuration),
  or
- a single SMP system, using the hardware resources in both Cell_0 and Cell_1,
  or
- a single SMP system, using the hardware resources in Cell_0 only,
  or
- a single SMP system, using the hardware resources in Cell_1 only.
- four SMP systems, each using the hardware resources in one cell (default configuration),
  or
- a single SMP system, using the hardware resources in all cells,
  or
- a single SMP system, using the hardware resources in a selection of cells.

As Customer Administrator, you are advised to configure schemes for domain management via the **PAM Domain Configuration Scheme** wizard. For further details about domain configuration options, see *Configuring Domains*, on page 5-28.

During operation, you may want to re–define server domains to meet variations in workload, for example. As Customer Administrator or Operator you can modify the configuration of any **INACTIVE** domain loaded in the **Domain Manager** Control pane, at any time, provided that the required resources are available (IO boxes and QBBs) and that they are supported by the domain Operating System.

Each CSS Module is divided into two Cells or hardware partitions, as shown in the following table:

NovaScale 6080/6160 Server

Hardware Cell	Cell_0	Cell_1
EFI LUN	<*MyServer*>_0LU0	<*MyServer*>_0LU1
IOB	Mod0_IOB0	Mod0_IOB1
QBBs	Mod0_QBB0, Mod0_QBB1*	Mod0_QBB2*, Mod0_QBB3

* QBB1 and QBB2 only equip the NovaScale 6160 Server

NovaScale 6320 Server

Hardware Cell	Cell_0	Cell_1
EFI LUN	<*MyServer*>_0LU0	<*MyServer*>_0LU1
IOB	Mod0_IOB0	Mod0_IOB1
QBBs	Mod0_QBB0, Mod0_QBB1	Mod0_QBB2, Mod0_QBB3
Hardware Cell	**Cell_2**	**Cell_3**
EFI LUN	<*MyServer*>_0LU2	<*MyServer*>_0LU3
IOB	Mod1_IOB0	Mod1_IOB1
QBBs	Mod1_QBB0, Mod1_QBB1	Mod1_QBB2, Mod1_QBB3

Table 19. Bull NovaScale 6000 Series server cell configuration

NovaScale 6080/6160 Server

NovaScale 6320 Server

Notes:

- **xx** in the default configuration scheme and domain names represents the Central Subsystem HW identifier (from 00 to 16). For further details, refer to *PMB LEDs and Code Wheels*, on page 4-46.
- In the screen shots, tables, and examples in this guide:
  - **MyOperationsScheme–xx** is referred to as **MyOperationsScheme**
  - **MyOperations–xx–1** is referred to as **MyOperations–1**
  - **MyOperations–xx–2** is referred to as **MyOperations–2**
  - **MyOperations–xx–3** is referred to as **MyOperations–3**
  - **MyOperations–xx–4** is referred to as **MyOperations–4**
- In the screen shots in this guide, an instance of Microsoft Windows is pre–installed on **MyOperations–xx–1** and **MyOperations–xx–3** and an instance of Linux is pre–installed on **MyOperations–xx–2** and **MyOperations–xx–4**.

  Operating System type is indicated by the Microsoft Windows or Linux logo in the **Domain Identities** box.

Swapping a Domain EFI Boot LUN

Important:
Certain features described below are only available if you are connected to a Storage Area Network (SAN).
Please contact your Bull Sales Representative for sales information.

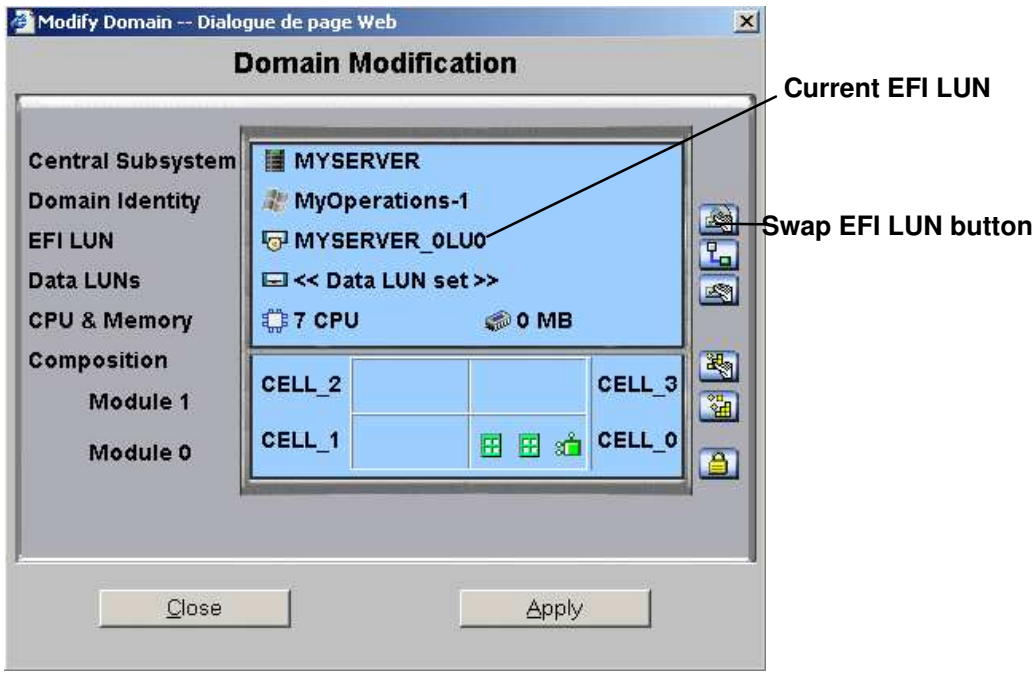
Notes:

- The domain must be **INACTIVE** before configuration changes can be made.
- When you change the EFI boot LUN, you will also change the Operating System instance.
- Domain modifications are not automatically saved and are only applicable while the selected domain is loaded in the **Domain Manager** Control pane. If required, you can manually save the new configuration for future use. See *Saving the Current Domain Configuration Snapshot*, on page 3-11.

To change the domain EFI boot LUN:

1. Click **Domain Manager** to open the Control pane.
2. Select the required domain.
3. Click **Modify** in the Command bar to open the **Modify Domain** dialog.

Note:
The **Modify Domain** dialog can also be accessed from the **View Domain** dialog.



* Module 1 (Cell_2 & Cell_3): does not equip mono–module servers

Figure 62. Modify Domain – Swap EFI LUN

4. Click the **Swap EFI LUN** button. The **Select LUN** dialog opens.

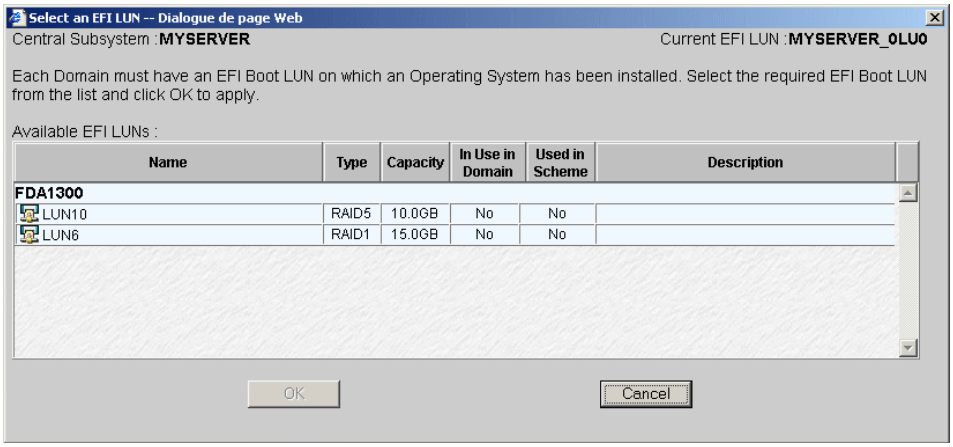
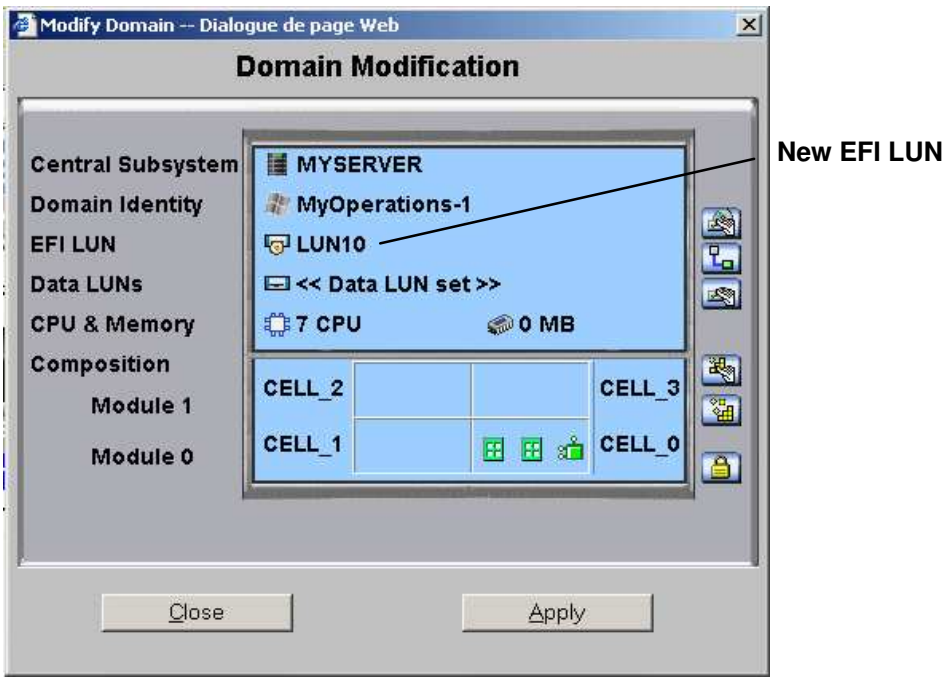


Figure 63. Select EFI LUN dialog

5. Select the required LUN and click **OK**.

   New domain configuration is displayed in the **Modify Domain** dialog.



* Module 1 (Cell_2 & Cell_3): does not equip mono–module servers

Figure 64. Modify Domain – New EFI Lun

6. Click **Apply**. Changes will be applied at the next domain power on.
7. If the LUN is on the SAN, it must be linked to the corresponding Fibre Channel Host. See *Linking a LUN to a Fibre Channel Host*, on page 0.

Adding a Data LUN

Important:
Reserved for systems connected to a Storage Area Network (SAN).
Please contact your Bull Sales Representative for sales information.

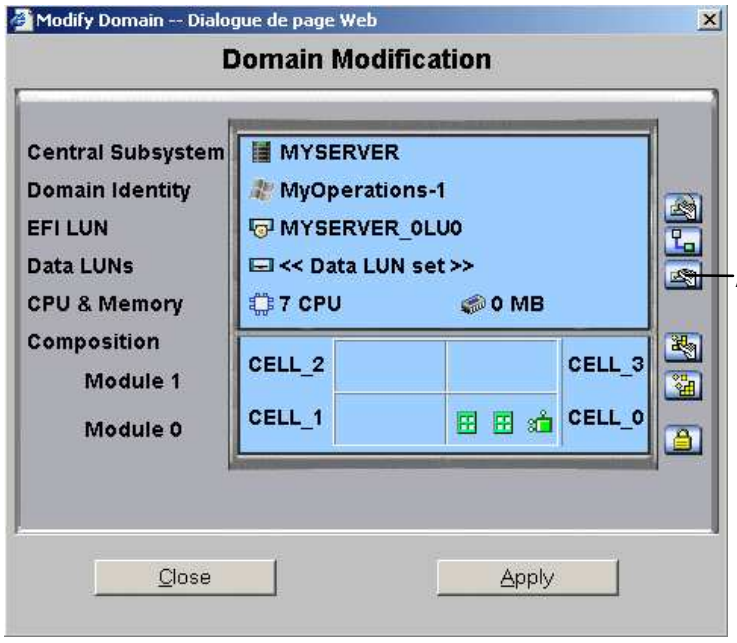
Notes:

- The domain must be **INACTIVE** before configuration changes can be made.
- Domain modifications are not automatically saved and are only applicable while the selected domain is loaded in the **Domain Manager** Control pane. If required, you can manually save the new configuration for future use. See *Saving the Current Domain Configuration Snapshot*, on page 3-11.

To add a data LUN:

1. Click **Domain Manager** to open the Control pane.
2. Select the required domain.
3. Click **Modify** in the Command bar to open the **Modify Domain** dialog.

Note:
The **Modify Domain** dialog can also be accessed from the **View Domain** dialog.



* Module 1 (Cell_2 & Cell_3): does not equip mono–module servers

Figure 65. Modify Domain – Add Data LUN

4. Click the **Add Data LUN** button. The **Select Data LUN** dialog opens.

Note:
If the message **LUNs used in the domain are not on the SAN** is displayed, your domain has not been configured to use LUNs on the SAN. See *Configuring Domains*, on page 5-28.

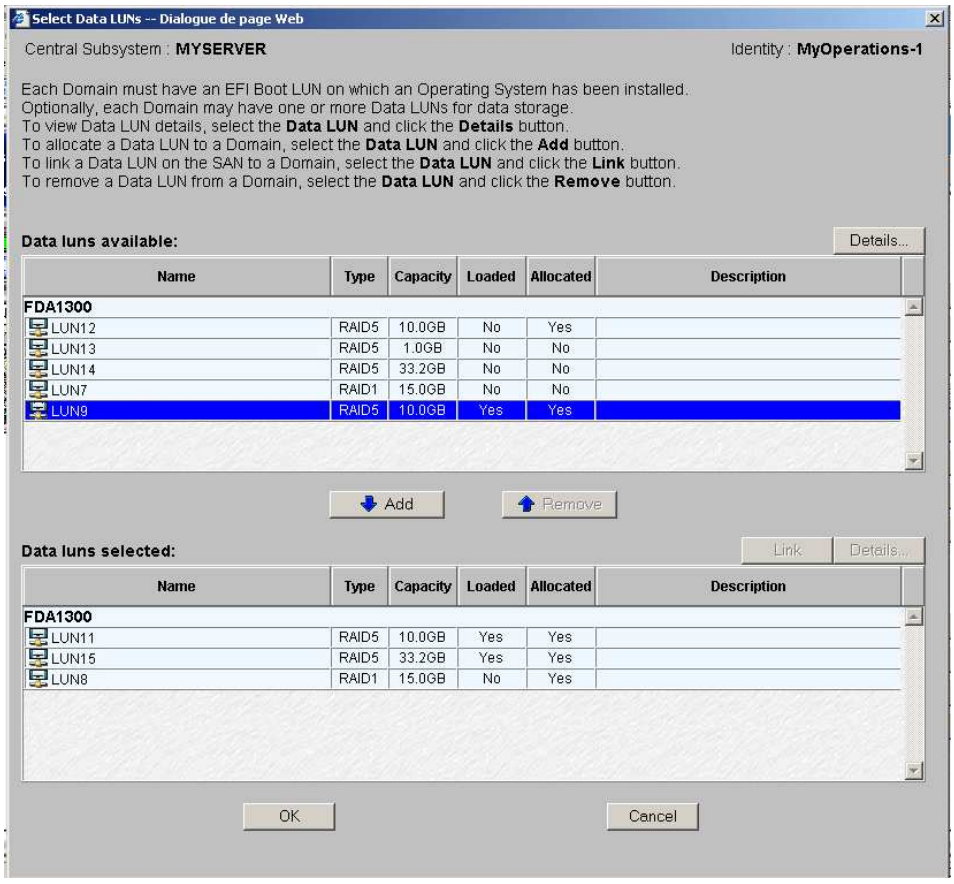
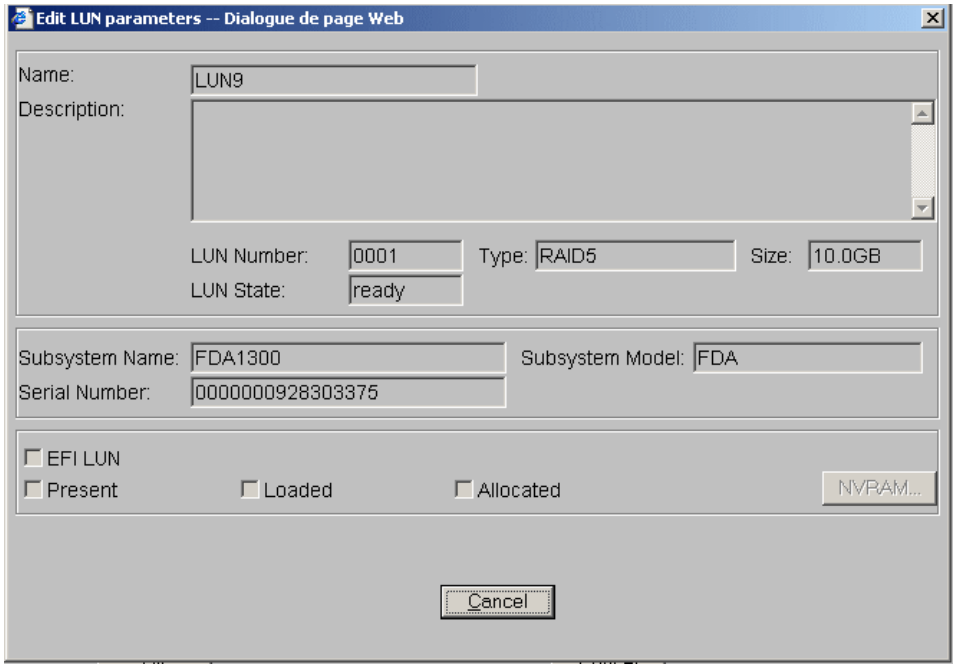


Figure 66. Select Data LUN dialog – Data luns available list

5. Select the LUN you want to add to the current domain configuration in the **Data LUNs available** list and click **Details** to view LUN parameters, if required.



Name	Name given to the LUN when created.
Description	Brief description of the LUN.
LUN Number	Number allocated to the LUN when created.
LUN State	If the LUN is ready for use, READY is displayed.
Type	LUN configuration mode.
Size	LUN size.
Subsystem Name	Name of the subsystem containing the LUN.
Subsystem Model	Type of subystem containing the LUN.
Serial Number	Serial number of the subsystem containing the LUN.
EFI LUN	If this box is checked, the LUN is an EFI boot LUN. If this box is not checked, the LUN is a data LUN.
Present	If this box is checked, the LUN is detected. If this box is checked, the LUN is not detected.
Loaded	If this box is checked, the LUN is loaded in the Domain Manager Control pane. If this box is not checked, the LUN is not loaded in the Domain Manager Control pane.
Allocated	If this box is checked, the LUN is already allocated to a scheme. If this box is not checked, the LUN is not allocated to a scheme.

Figure 67. View LUN parameters dialog

6. Click **Add**. The selected data LUN is moved to the **Data LUNs selected** list.

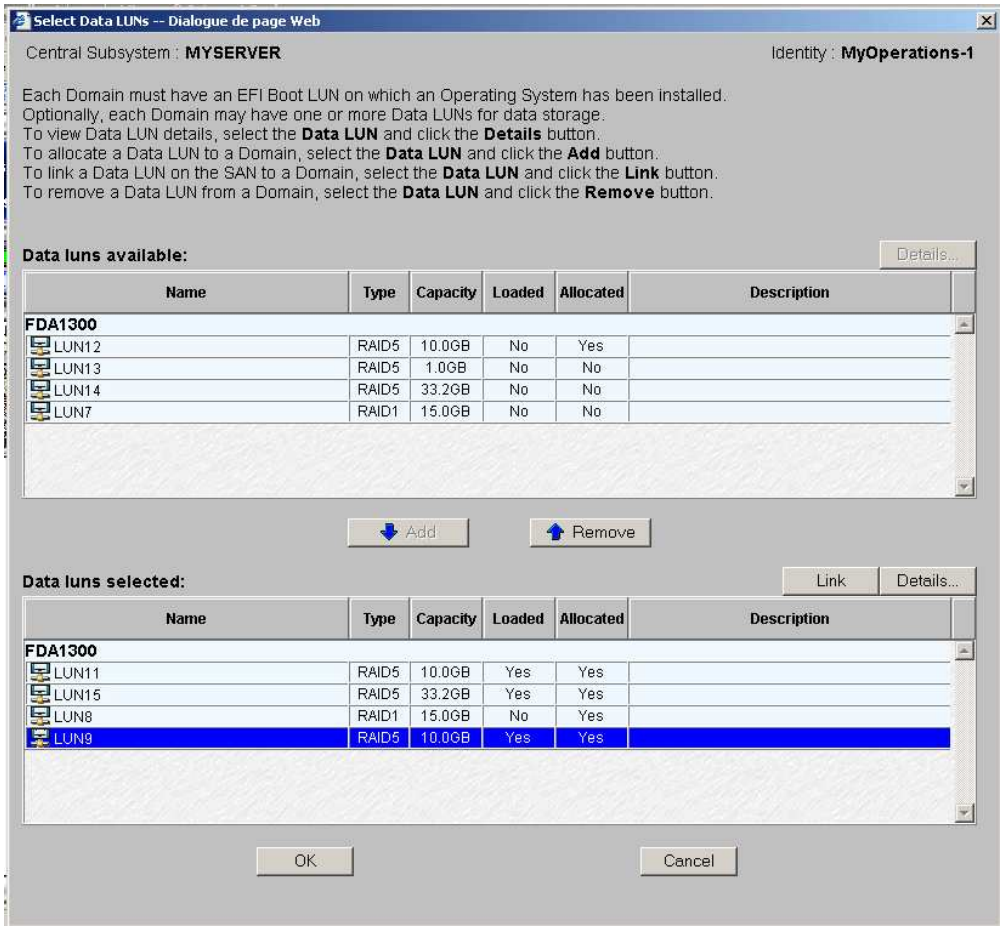


Figure 68. Select Data LUN dialog – Data luns selected list

Note:
If the selected data LUN is loaded in the current domain configuration or allocated to another domain, you will be requested to confirm that you want to add this LUN to the domain. Click **OK** to confirm or **Cancel** to return to the **Select Data LUN** dialog.

7. If the LUN is on the SAN, it must be linked to the corresponding Fibre Channel Host. Click **Link**. The **Link LUNs to HBA** dialog opens.

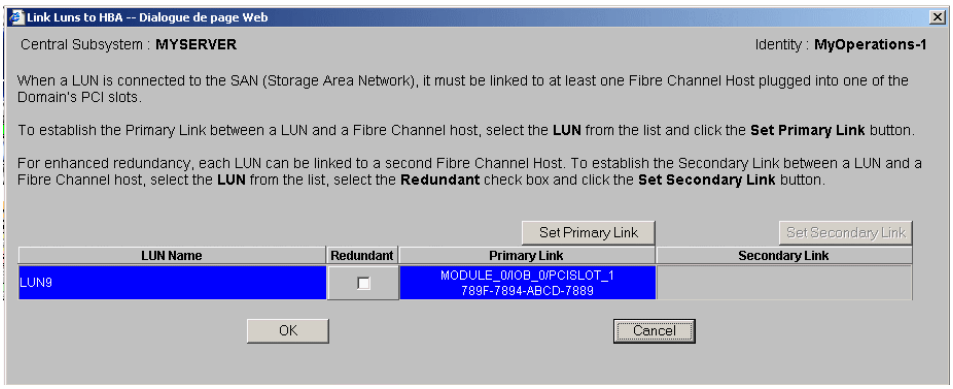


Figure 69. Link LUNs to HBA dialog

8. Select the **Redundant** checkbox if you want to define two links to the LUN.

Note:
If you select the **Redundant** mode, you will be informed that dedicated software is required to enable this mode and you will be requested to confirm your choice.

9. Click **Set Primary Link** to define the main access path to the SAN. The **Select HBA** dialog opens, allowing you to select the domain PCI slot you want to use to access the LUN.

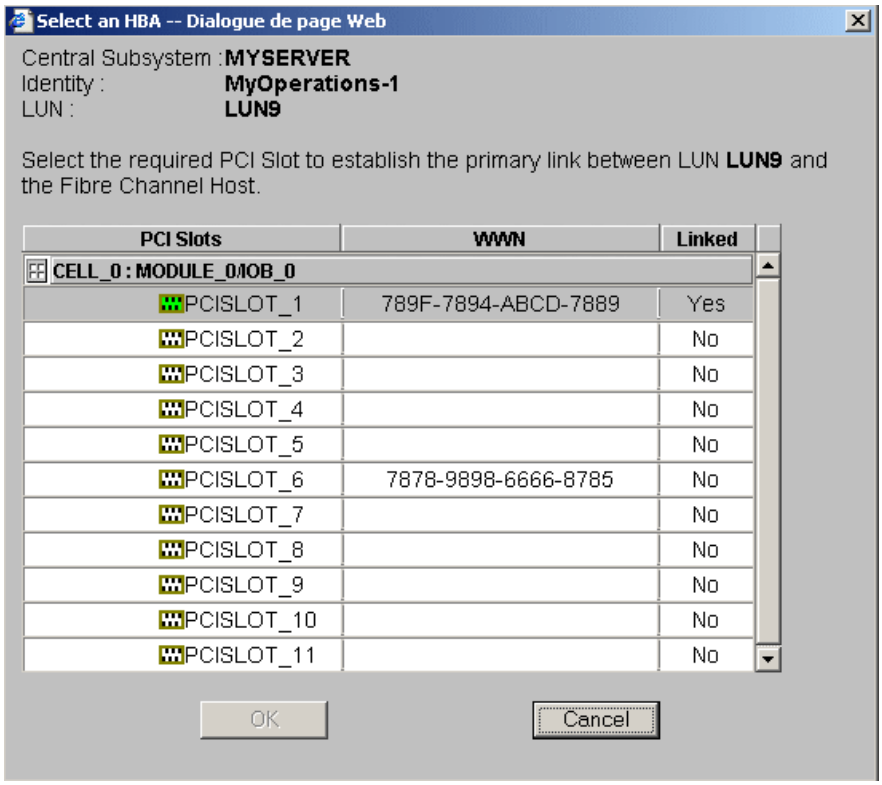


Figure 70. Select an HBA dialog

10. Select the PCI slot containing the HBA to be used as the primary link to the SAN and click **OK**. The primary link is now set.
11. Where applicable, click **Set Secondary Link** to define the backup access path to the SAN.
12. Select the PCI slot containing the HBA to be used as the secondary link to the SAN and click **OK**. The secondary link is now set.
13. Click **OK** → **Apply**. Changes will be applied at the next domain power on.

Note:
If you do not define the data LUN link, a message will appear requesting you to link the LUN to a fibre channel host before saving changes. See *Linking a LUN to a Fibre Channel Host*, on page 0 for details.

Removing a Data LUN

Important:
Reserved for systems connected to a Storage Area Network (SAN).
Please contact your Bull Sales Representative for sales information.

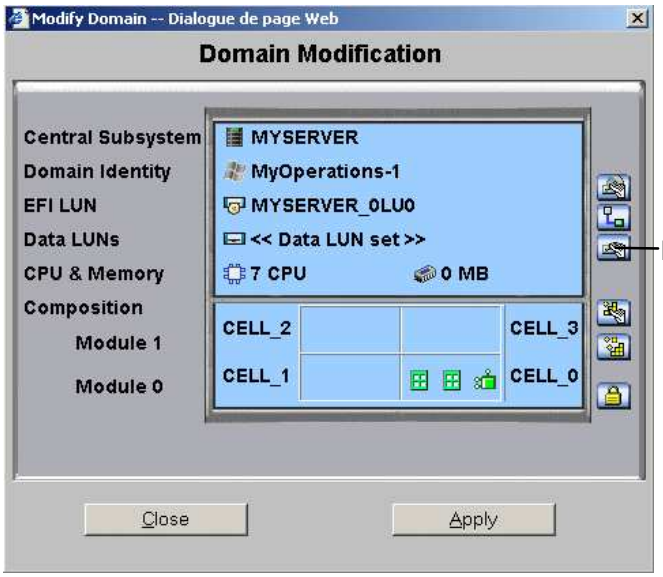
Notes:

- The domain must be **INACTIVE** before configuration changes can be made.
- Domain modifications are not automatically saved and are only applicable while the selected domain is loaded in the **Domain Manager** Control pane. If required, you can manually save the new configuration for future use. See *Saving the Current Domain Configuration Snapshot*, on page 3-11.

To remove a data LUN:

1. Click **Domain Manager** to open the Control pane.
2. Select the required domain.
3. Click **Modify** in the Command bar to open the **Modify Domain** dialog.

Note:
The **Modify Domain** dialog can also be accessed from the **View Domain** dialog.



* Module 1 (Cell_2 & Cell_3): does not equip mono–module servers

Figure 71. Modify Domain – Remove Data LUN

4. Click the **Remove Data LUN** button. The **Select Data LUN** dialog opens.

Note:
If **LUNs used in the domain are not on the SAN** is displayed, your domain has not been configured to use LUNs on the SAN. See *Configuring Domains*, on page 5-28.

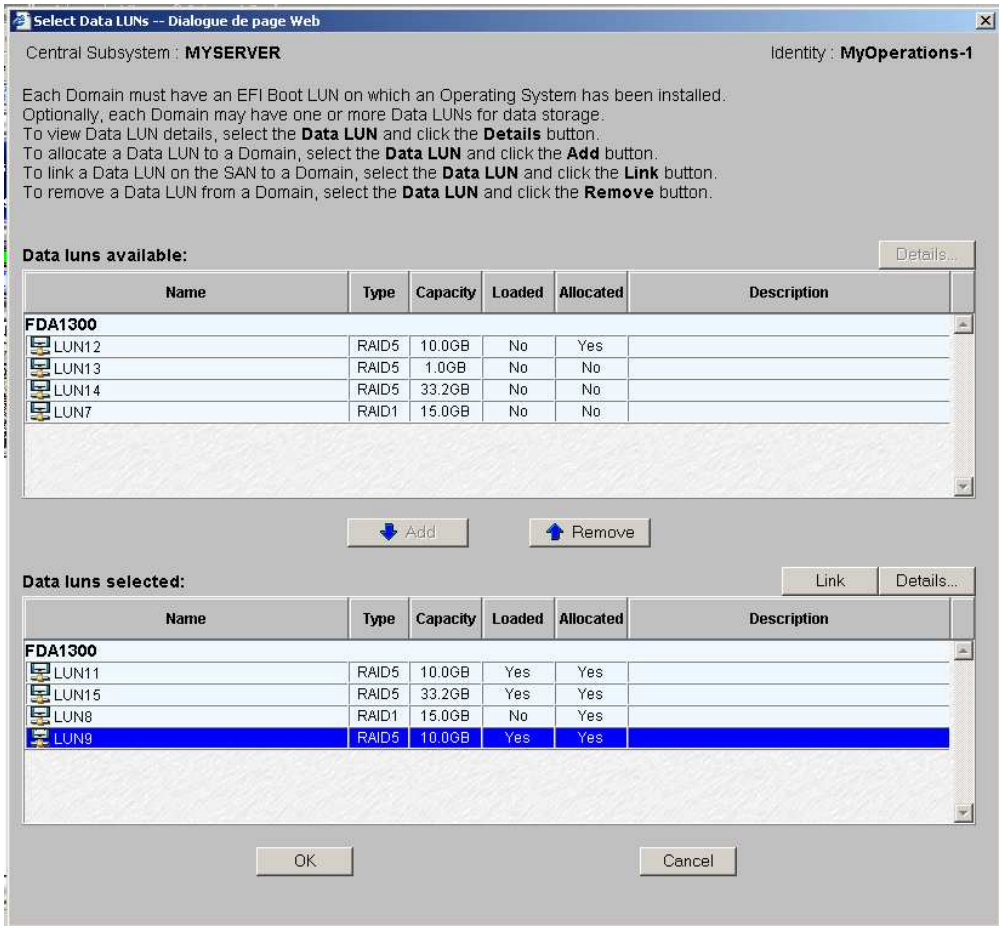
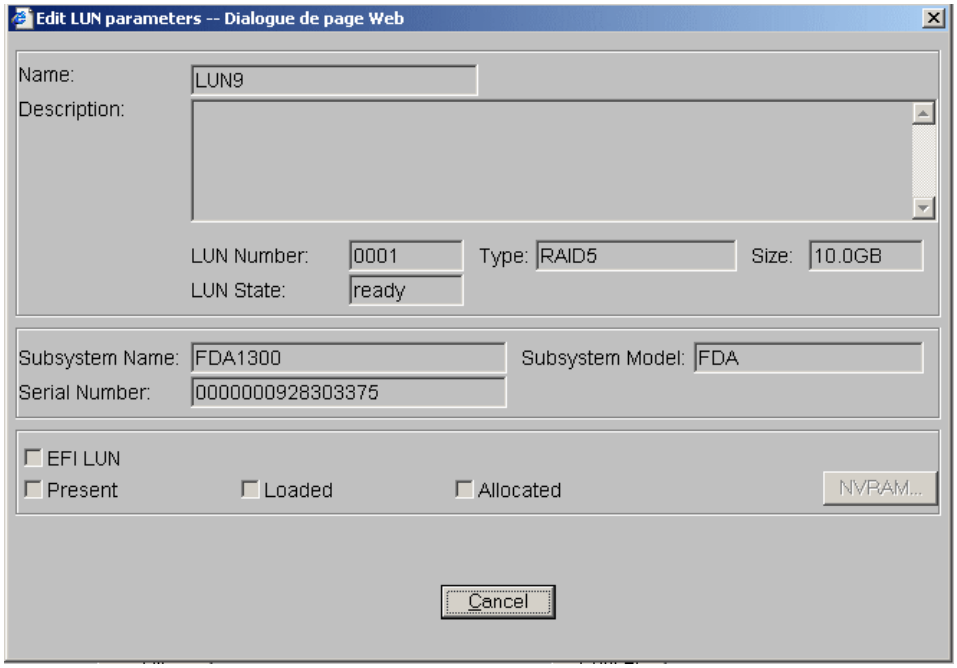


Figure 72. Select Data LUN dialog – Data luns selected list

5. Select the LUN you want to remove from the current domain configuration in the **Data LUNs available selected** list and click **Details** to view LUN parameters, if required.



Name	Name given to the LUN when created.
Description	Brief description of the LUN.
LUN Number	Number allocated to the LUN when created.
LUN State	If the LUN is ready for use, READY is displayed. If the LUN is not ready for use ???? is displayed.
Type	LUN configuration mode.
Size	LUN size.
Subsystem Name	Name of the subsystem containing the LUN.
Subsystem Model	Type of subystem containing the LUN.
Serial Number	Serial number of the subsystem containing the LUN.
EFI LUN	If this box is checked, the LUN is an EFI boot LUN. If this box is not checked, the LUN is a data LUN.
Present	If this box is checked, the LUN is detected. If this box is checked, the LUN is not detected.
Loaded	If this box is checked, the LUN is loaded in the Domain Manager Control pane. If this box is not checked, the LUN is not loaded in the Domain Manager Control pane.
Allocated	If this box is checked, the LUN is already allocated to a domain. If this box is not checked, the LUN is not allocated to a domain.

Figure 73. View LUN parameters dialog

6. Click **Remove**. The selected data LUN is moved to the **Data LUNs available** list.

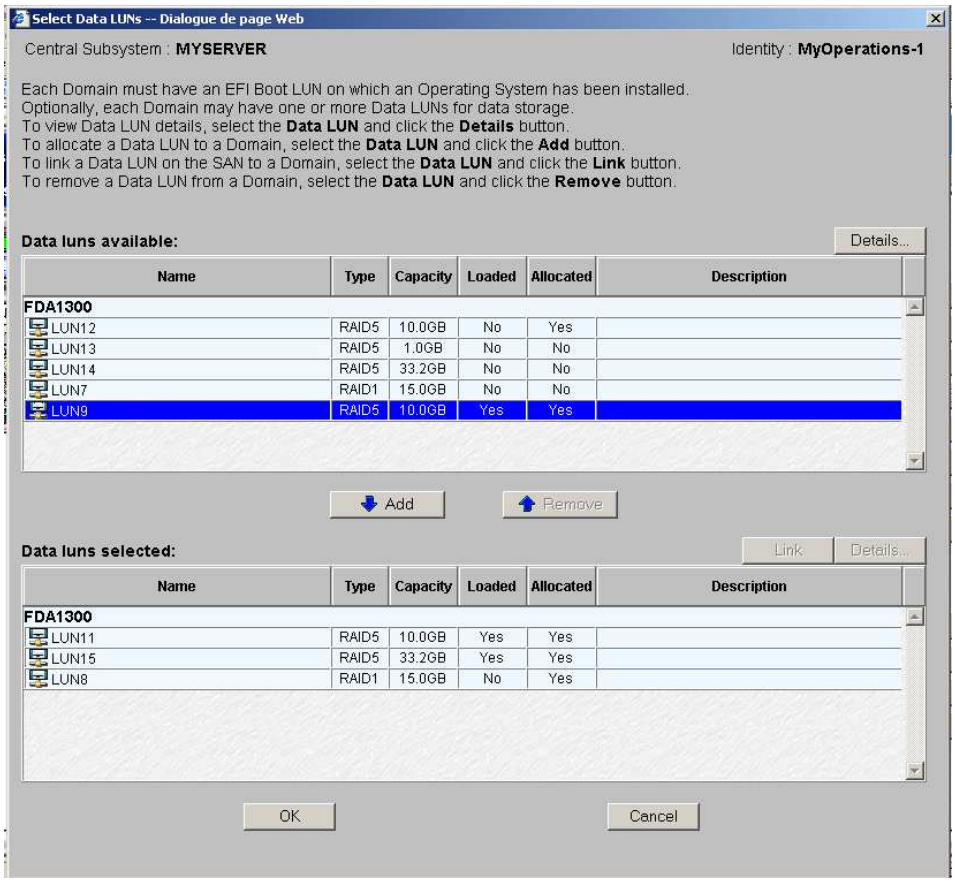


Figure 74. Select Data LUN dialog – Data luns available list

Note:
If the selected data LUN is loaded in the current domain configuration or allocated to another domain, you will be requested to confirm that you want to remove this LUN from the domain. Click **OK** to confirm or **Cancel** to return to the **Select Data LUN** dialog.

7. Click **OK** → **Apply**. Changes will be applied at the next domain power on.

Linking a LUN to a Fibre Channel Host

Important:
Reserved for systems connected to a Storage Area Network (SAN).
Please contact your Bull Sales Representative for sales information.

Notes:

- Disk subsystems may be connected to the server via one or two HBAs.
- The redundant mode (two HBAs) requires the use of dedicated software.
- The domain must be **INACTIVE** before configuration changes can be made.
- Domain modifications are not automatically saved and are only applicable while the selected domain is loaded in the **Domain Manager** Control pane. If required, you can manually save the new configuration for future use. See *Saving the Current Domain Configuration Snapshot*, on page 3-11.

To link a LUN to a Fibre Channel Host:

1. Click **Domain Manager** to open the Control pane.
2. Select the required domain.
3. Click **Modify** in the Command bar to open the **Modify Domain** dialog.

Note:
The **Modify Domain** dialog can also be accessed from the **View Domain** dialog.

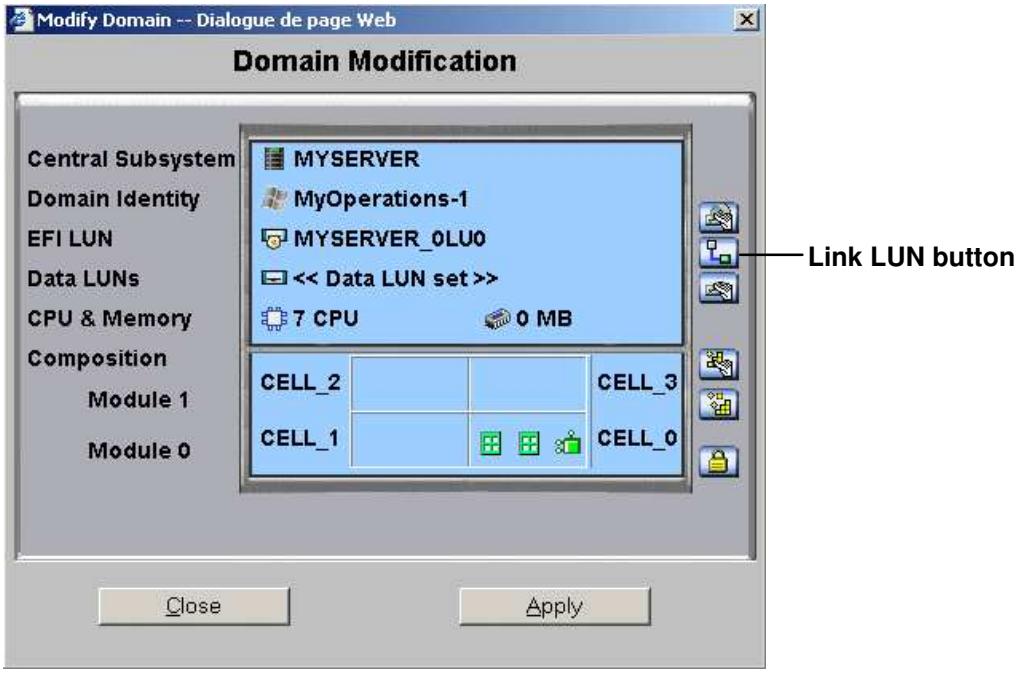


Figure 75. Modify Domain – Link LUN dialog

4. Click the **Link LUN** button. The **Link LUNs to HBA** dialog opens, allowing you to select the primary and secondary link to the disk subsystem containing the LUN.

Note:
If the message **LUNs used in the domain are not on the SAN** is displayed, your domain has not been configured to use LUNs on the SAN. See *Configuring Domains*, on page 5-28.

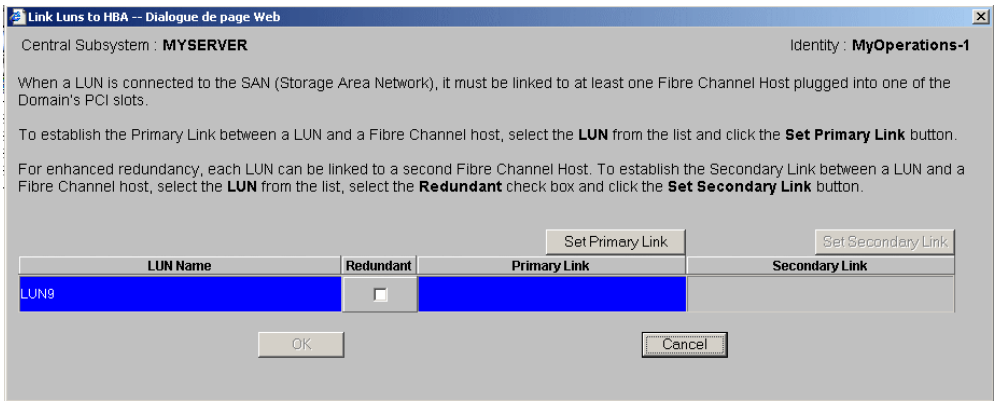


Figure 76. Modify domain – Link Luns to HBA dialog

5. Select the **Redundant** checkbox if you want to define two links to the LUN.

Note:
If you select the **Redundant** mode, you will be informed that dedicated software is required to enable this mode and you will be requested to confirm your choice.

6. Click **Set Primary Link** to define the main access path to the SAN. The **Select HBA** dialog opens, allowing you to select the domain PCI slot you want to use to access the LUN.

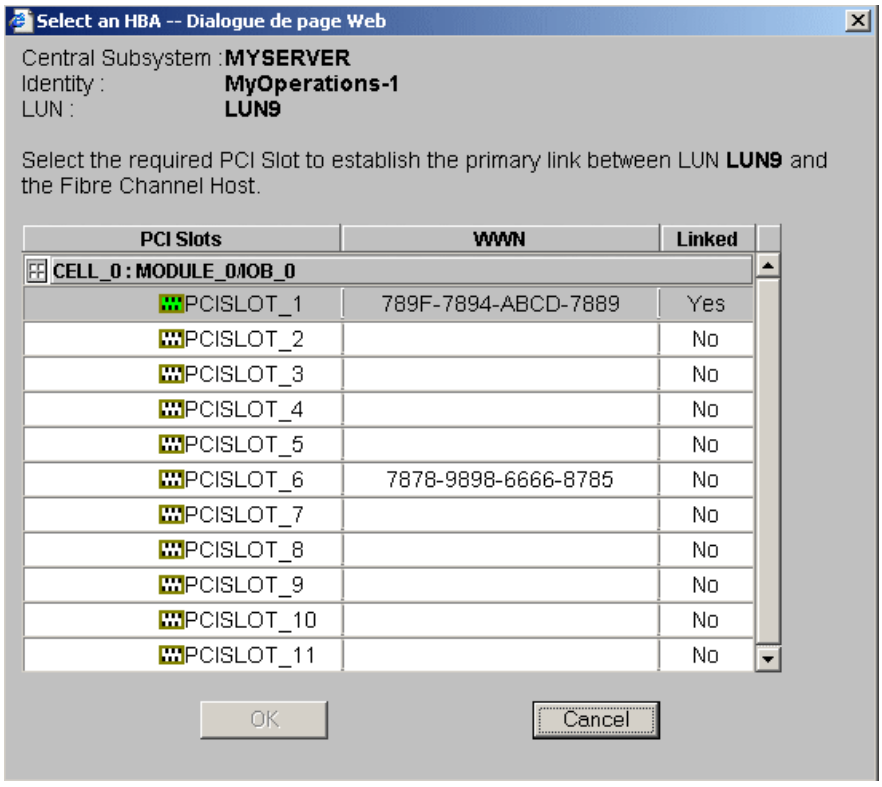


Figure 77. Select an HBA dialog

7. Select the PCI slot containing the HBA to be used as the primary link to the SAN and click **OK**. The primary link is now set.

8. Where applicable, click **Set Secondary Link** to define the backup access path to the SAN.
9. Select the PCI slot containing the HBA to be used as the secondary link to the SAN and click **OK**. The secondary link is now set.
10. Click **OK** → **Apply**. Changes will be applied at the next domain power on.

Adding Cells to a Domain

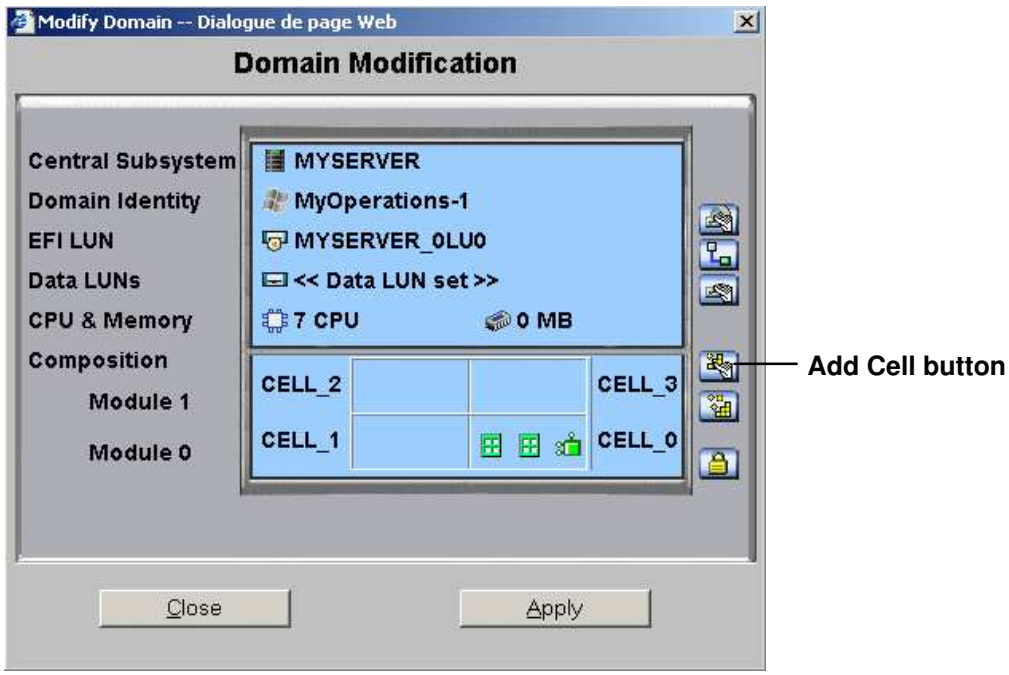
Notes:

- At least one Cell, containing one IOB and one QBB, must be available.
- The Operating System must support added hardware.
- The domain must be **INACTIVE** before configuration changes can be made.
- When you add a Cell to a NovaScale 6080/6160 Server domain, the server will operate as a single SMP system, using all hardware resources.
- Domain modifications are not automatically saved and are only applicable while the selected domain is loaded in the **Domain Manager** Control pane. If required, you can manually save the new configuration for future use. See *Saving the Current Domain Configuration Snapshot*, on page 3-11.

To add Cells to a domain:

1. Click **Domain Manager** to open the Control pane.
2. Select the required domain.
3. Click **Modify** in the Command bar to open the **Modify Domain** dialog.

Note:
The **Modify Domain** dialog can also be accessed from the **View Domain** dialog.



* Module 1 (Cell_2 & Cell_3): does not equip mono–module servers

Figure 78. Modify Domain – Add Cell dialog

4. Click the **Add Cell** button. The **Add Cells to Domain** dialog opens.

Note:
If a **No CELLs available** message appears, you must first delete the domain using the cell. See *Deleting a Domain*, on page 3-66.

NovaScale 6080/6160 Server

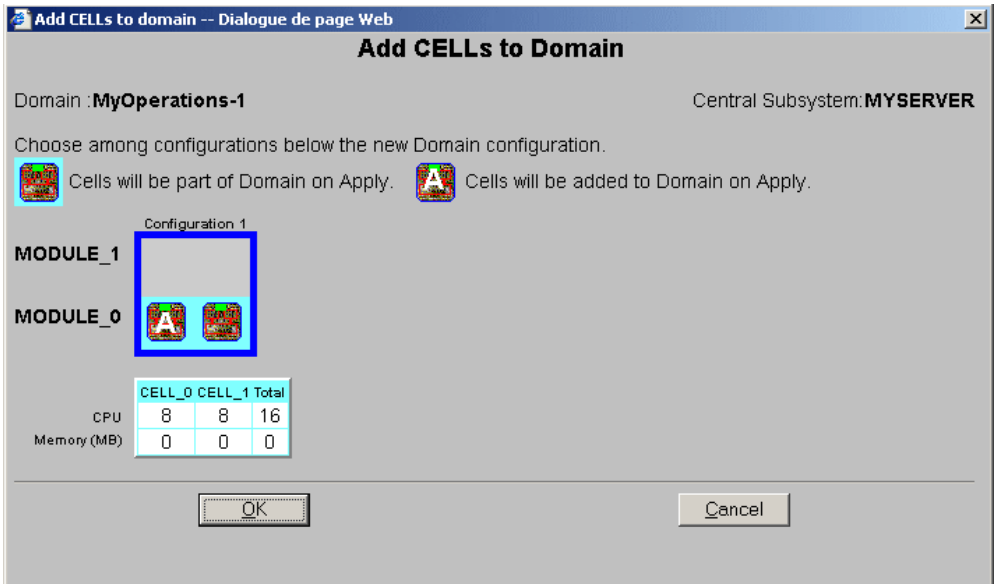


Figure 79. Add Cells to Domain dialog (mono–module server)

NovaScale 6320 Server

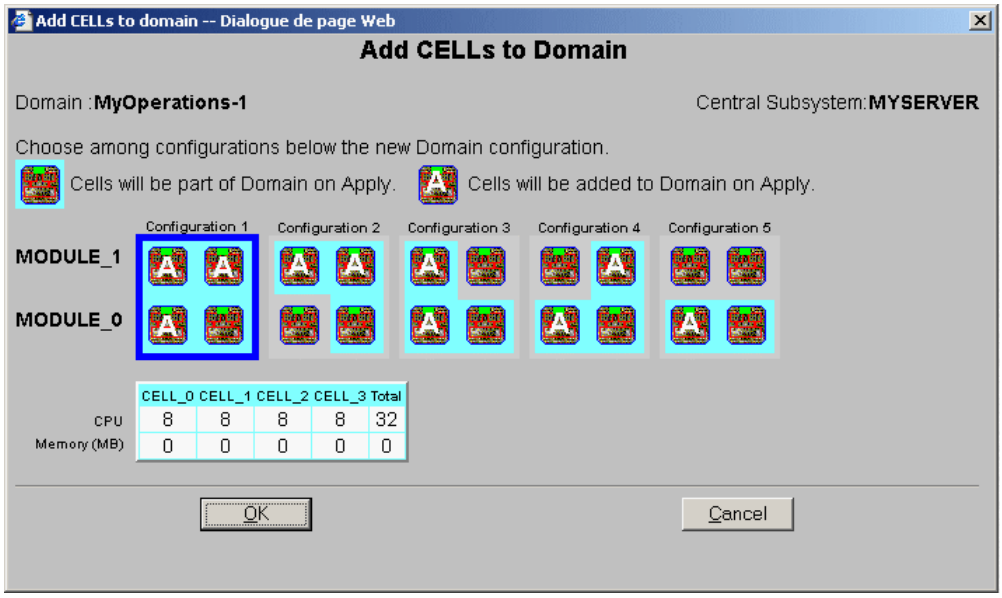
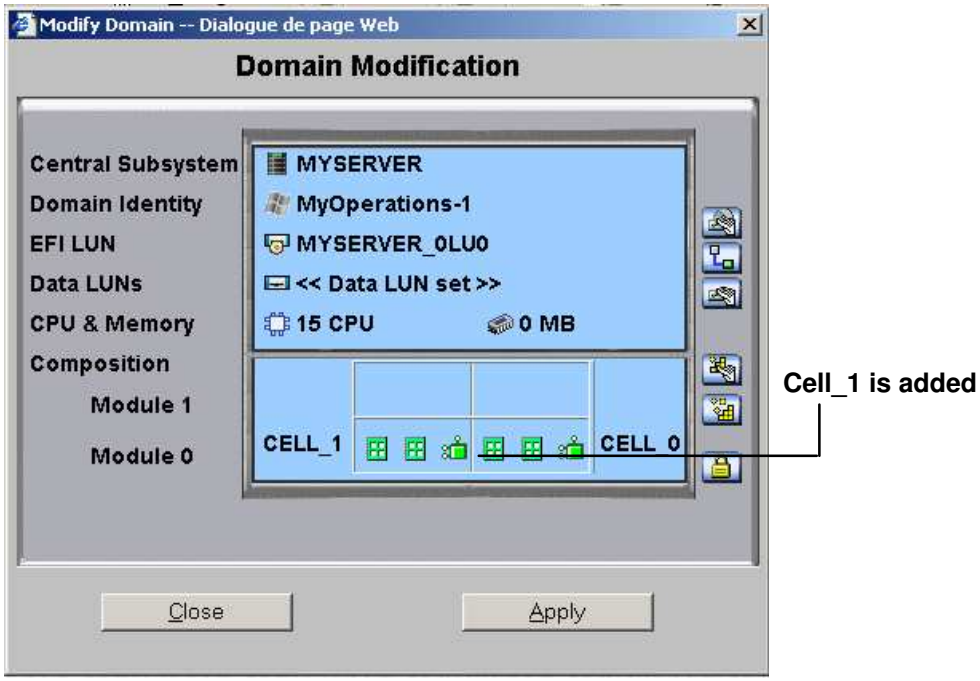


Figure 80. Add Cells to Domain dialog (bi–module server)

5. Select the required configuration and click **OK**. The letter **A** indicates the cell that will be added to the domain.

The new domain configuration is displayed in the **Modify Domain** dialog.

NovaScale 6080/6160 Server



* Module 1 (Cell_2 & Cell_3): does not equip mono–module servers

Figure 81. Modify Domain – Add Cell confirmation dialog (mono–module server)

NovaScale 6320 Server

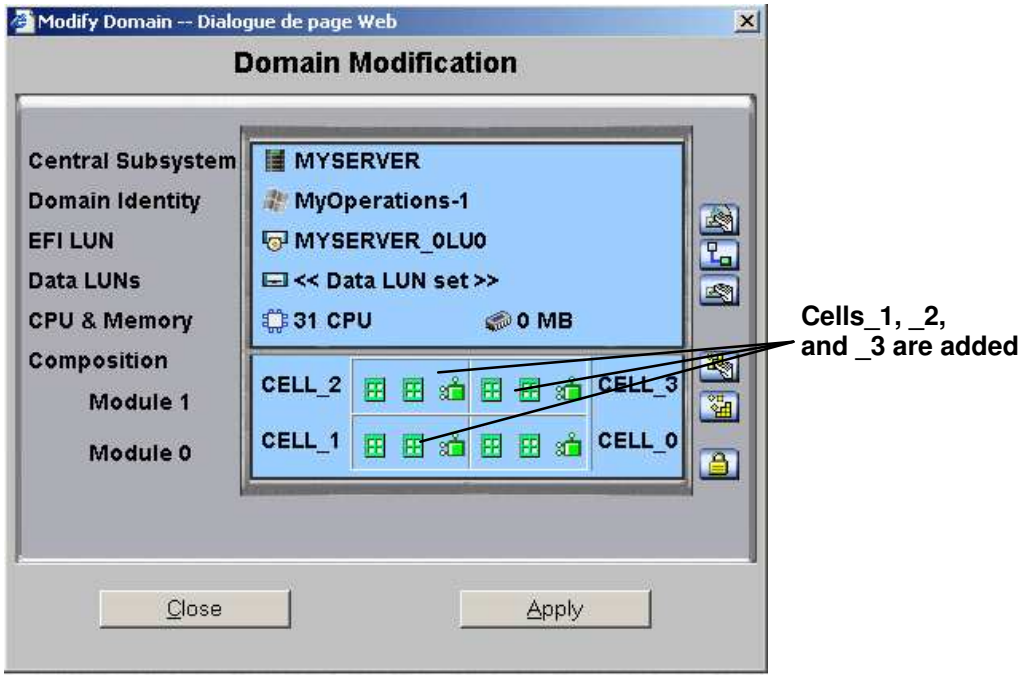


Figure 82. Modify Domain – Add Cell confirmation dialog (bi–module server)

6. If required, click **View Resources** for hardware details. See *Viewing Domain Hardware Resources*, on page 3-35.
7. Click **Apply**. Changes will be applied at the next domain power on.

Removing Cells from a Domain

Notes:

- At least one Cell, containing one IOB and one QBB, must remain.
- The domain must be **INACTIVE** before configuration changes can be made.
- When you remove a Cell from a NovaScale 6080/6160 Server domain, the server can either operate as a single SMP system, using only the hardware resources in the remaining Cell, or as two SMP systems if the removed Cell is allocated to another domain.
- Domain modifications are not automatically saved and are only applicable while the selected domain is loaded in the **Domain Manager** Control pane. If required, you can manually save the new configuration for future use. See *Saving the Current Domain Configuration Snapshot*, on page 3-11.

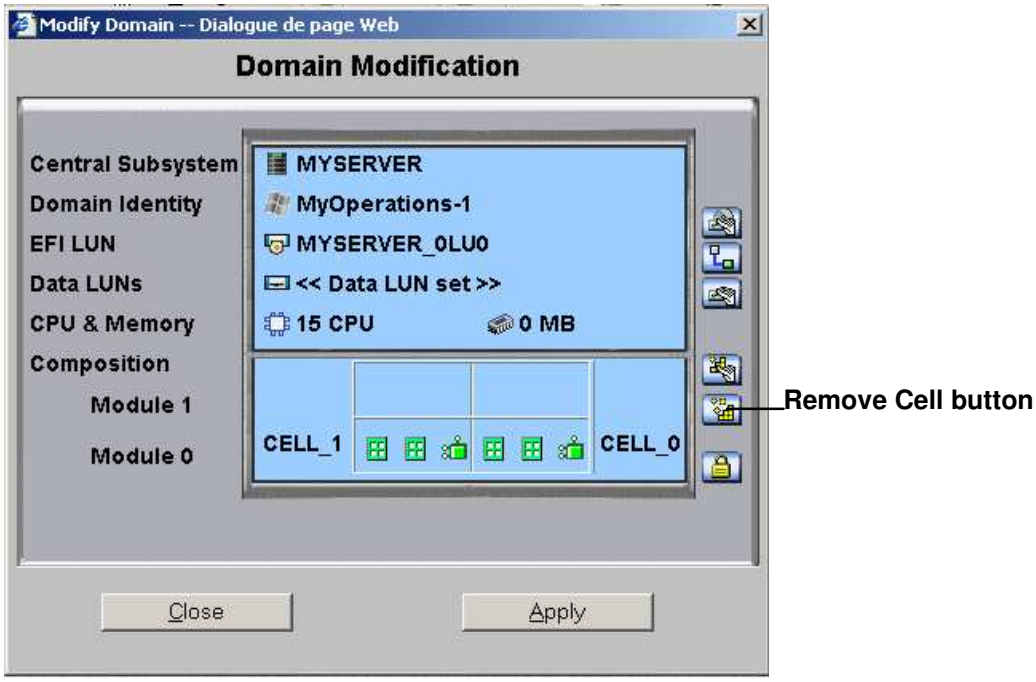
Warning:
When you remove a Cell from a domain, the devices attached to the corresponding IOB board are no longer available for this domain.

To remove Cells from a domain:

1. Click **Domain Manager** to open the Control pane.
2. Select the required domain.
3. Click **Modify** in the Command bar to open the **Modify Domain** dialog.

Note:
The **Modify Domain** dialog can also be accessed from the **View Domain** dialog.

NovaScale 6080/6160 Server



* Module 1 (Cell_2 & Cell_3): does not equip mono–module servers

Figure 83. Modify Domain – Remove Cell dialog (mono–module server)

NovaScale 6320 Server

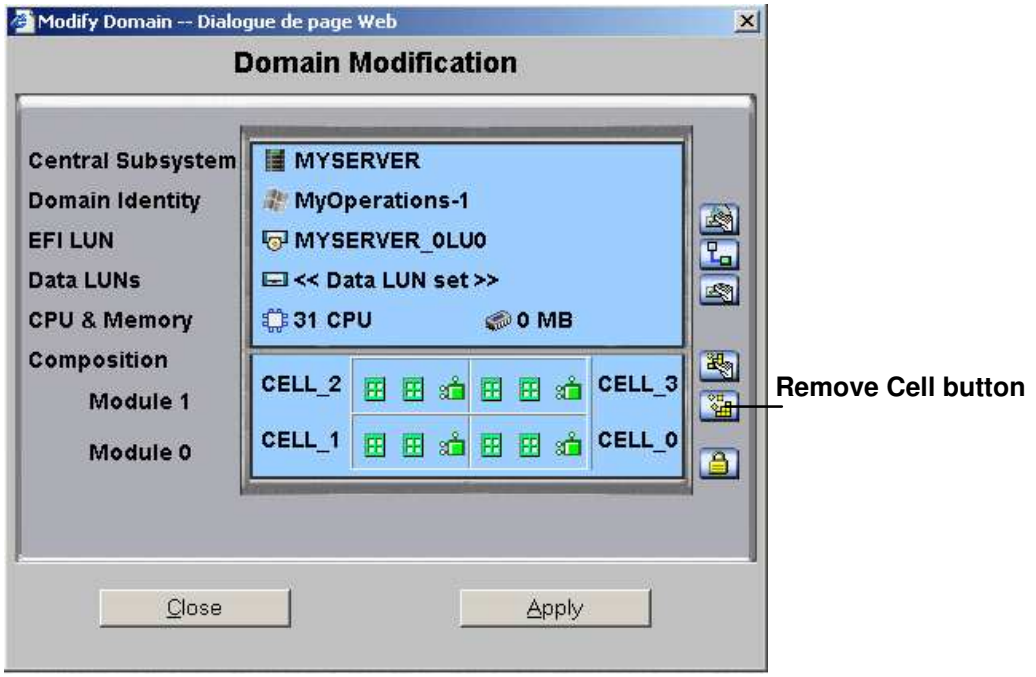


Figure 84. Modify Domain – Remove Cell dialog (bi–module server)

4. Click **Remove Cell**. The **Remove Cells from Domain** dialog opens.

NovaScale 6080/6160 Server

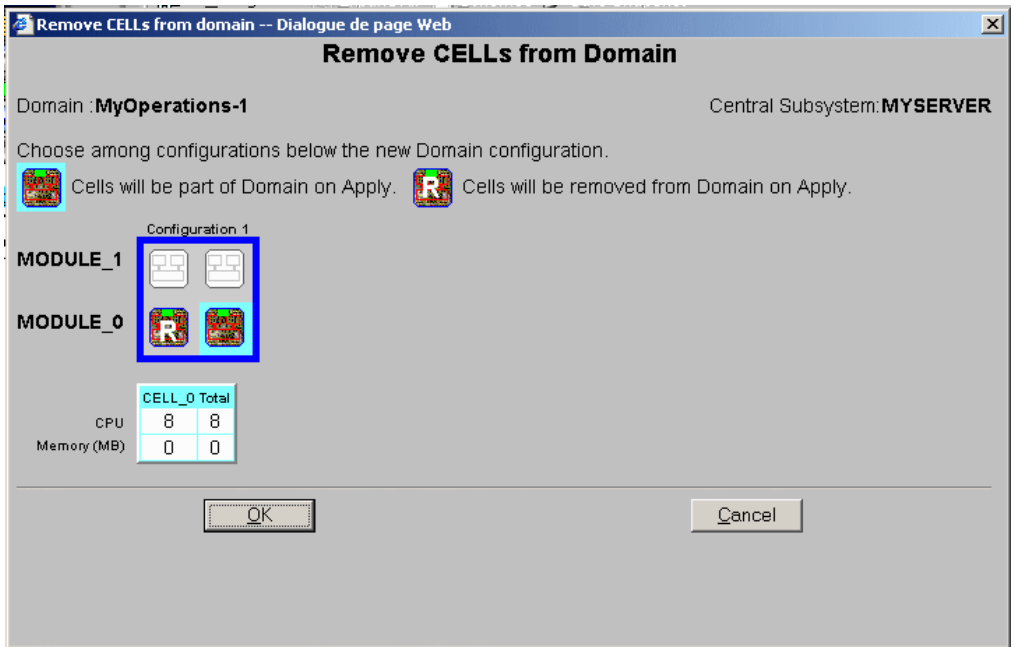


Figure 85. Remove Cells from Domain dialog (mono–module server)

NovaScale 6320 Server

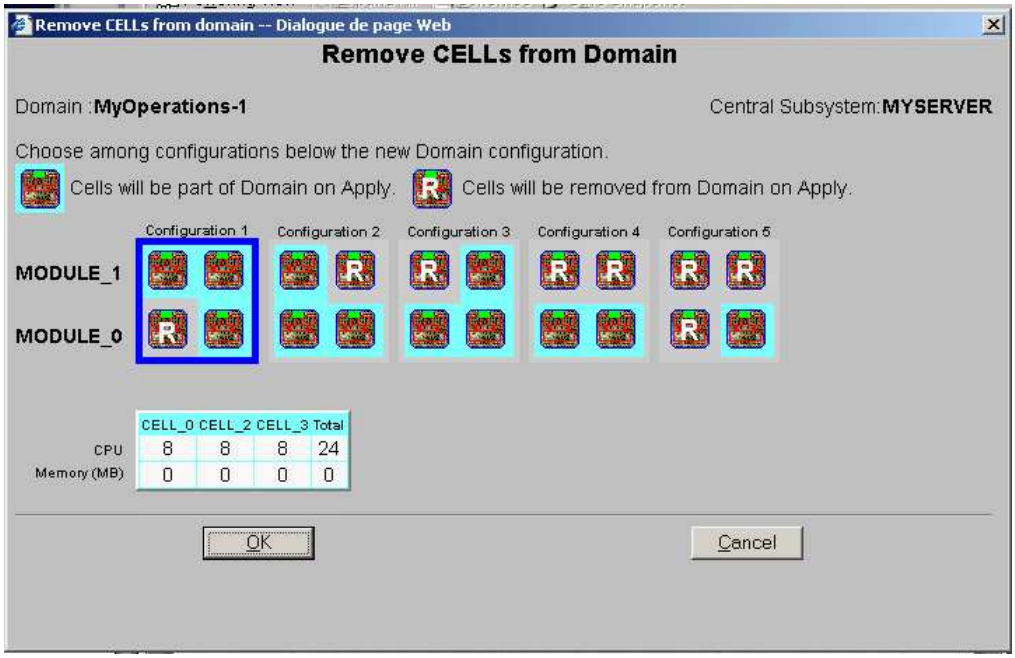
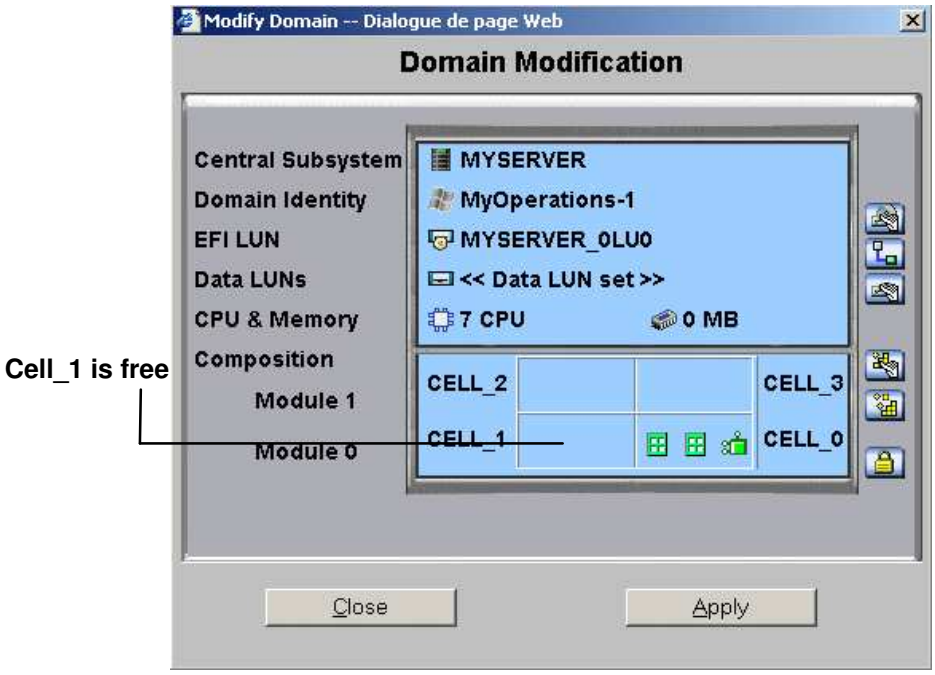


Figure 86. Remove Cells from Domain dialog (bi–module server)

5. Select the required configuration and click **OK**. The letter **R** indicates the cell that will be removed from the domain.

The new domain configuration is displayed in the **Modify Domain** dialog.

NovaScale 6080/6160 Server



* Module 1 (Cell_2 & Cell_3): does not equip mono–module servers

Figure 87. Modify Domain – Remove Cell confirmation dialog (mono–module server)

NovaScale 6320 Server

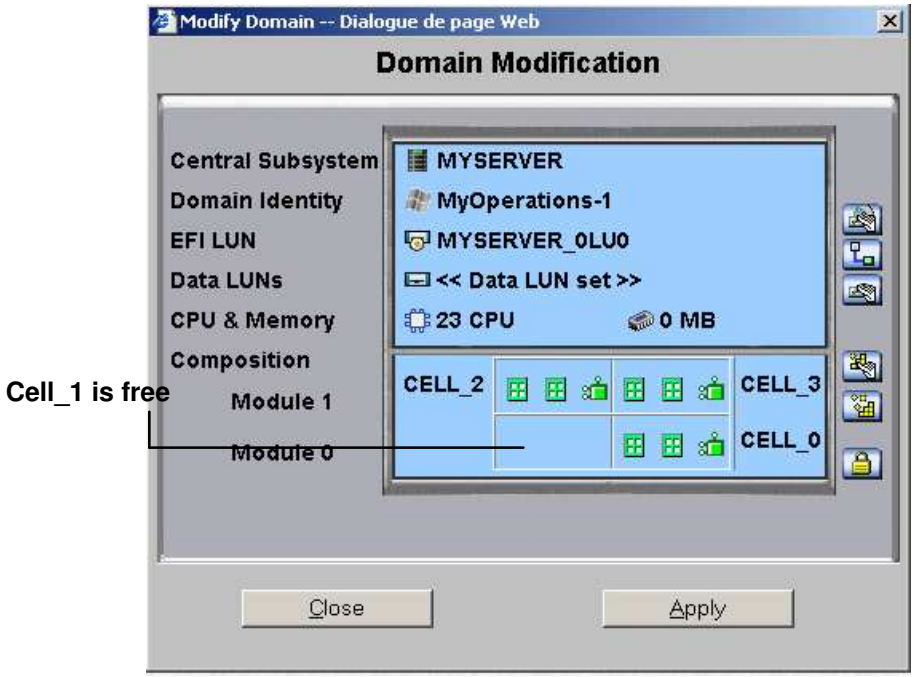


Figure 88. Modify Domain – Remove Cell confirmation dialog (bi–module server)

6. If required, click **View Resources** for hardware details. See *Viewing Domain Hardware Resources*, on page 3-35.
7. Click **Apply**. Changes will be applied at the next domain power on.

Locking / Unlocking Hardware Elements

You can functionally limit access to certain hardware elements. Locked elements can no longer be accessed by the current domain, but are still physically available for access by other domains. Previously locked elements can be unlocked so that they can be accessed by the domain. For details, see *Limiting Access to Hardware Resources*, on page 5-62.

Notes:

- The domain must be **INACTIVE** before configuration changes can be made.
- Hardware locking / unlocking is only taken into account at the next domain power ON.
- Hardware components to be functionally included (unlocked) in the domain at the next domain power ON are marked with a yellow icon in the **Lock Request** column in the **Domain Hardware Details** page.
- Hardware components to be functionally excluded (locked) from the domain at the next domain power ON are marked with a red / yellow icon in the **Lock Request** column in the **Domain Hardware Details** page.

  See *Viewing Domain Configuration, Resources and Status*, on page 3-32.
- Domain modifications are not automatically saved and are only applicable while the selected domain is loaded in the **Domain Manager** Control pane. If required, you can manually save the new configuration for future use. See *Saving the Current Domain Configuration Snapshot*, on page 3-11.

The following domain hardware elements can be locked / unlocked from the **Domain Manager** control pane:

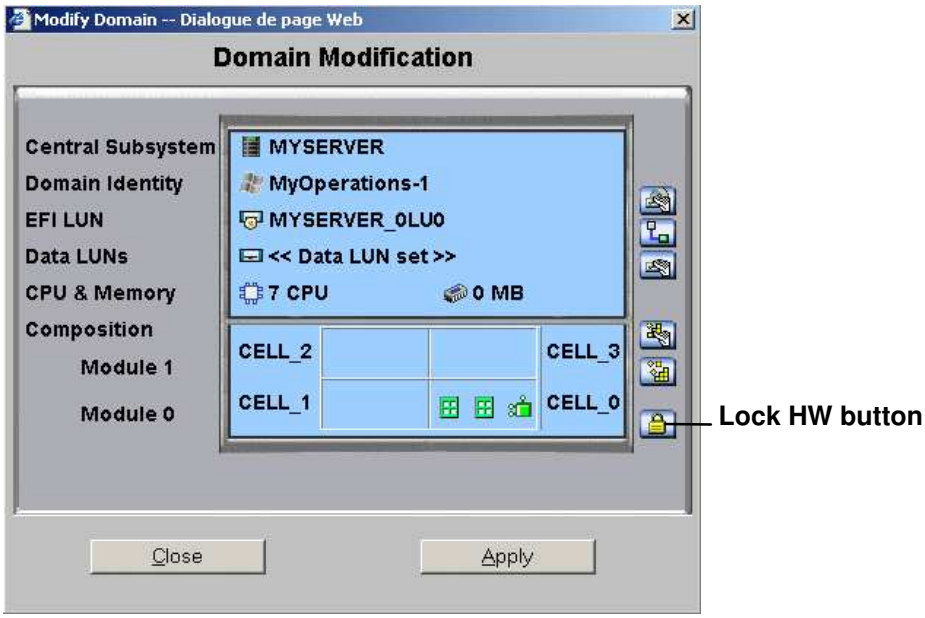
IOBs	When a domain comprises more than one cell (therefore more than one IOB), the Master IOB is the one hosting the boot disk. The other IOBs in the domain are Slave IOBs. Slave IOBs can be safely locked from a domain, but connected peripherals will no longer be accessible. **Note:** **If the Master IOB is locked, system disks may no longer be accessible and the domain may not power up.**
IOB HubLinks	All IOB HubLinks can be safely locked from a domain, but connected peripherals will no longer be accessible. IOB HubLinks are organized as follows: HubLink_1 controls PCI Slots 1 & 2 HubLink_2 controls PCI slots 3, 4, & 5 HubLink_3 controls PCI slots 6, 7, & 8 HubLink_4 controls PCI slots 9, 10, & 11 **Note:** **If Master IOB HubLink_1 is locked, system disks may no longer be accessible and the domain may not power up.**
PCI Slots	All PCI slots not connected to a boot disk can be safely locked from a domain, but connected peripherals will no longer be accessible. **Note:** **If Master IOB PCI Slots 1, 2 are locked, system disks may no longer be accessible and the domain may not power up.**
IORs	Slave IORs can be safely locked from a domain, but connected peripherals will no longer be accessible. **Note:** **If the Master IOR is locked, the domain will not power up.**

Table 20. Hardware locking options

To lock / unlock a domain hardware element:

1. Click **Domain Manager** to open the Control pane.
2. Select the required domain.
3. Click **Modify** in the Command bar to open the **Modify Domain** dialog.

☞ **Note:**
The **Modify Domain** dialog can also be accessed from the **View Domain** dialog.



* Module 1 (Cell_2 & Cell_3): does not equip mono–module servers

Figure 89. Modify Domain – Lock Hardware

4. Click the **Lock Hardware Components** button. The **Lock Domain Hardware Resources** dialog opens.

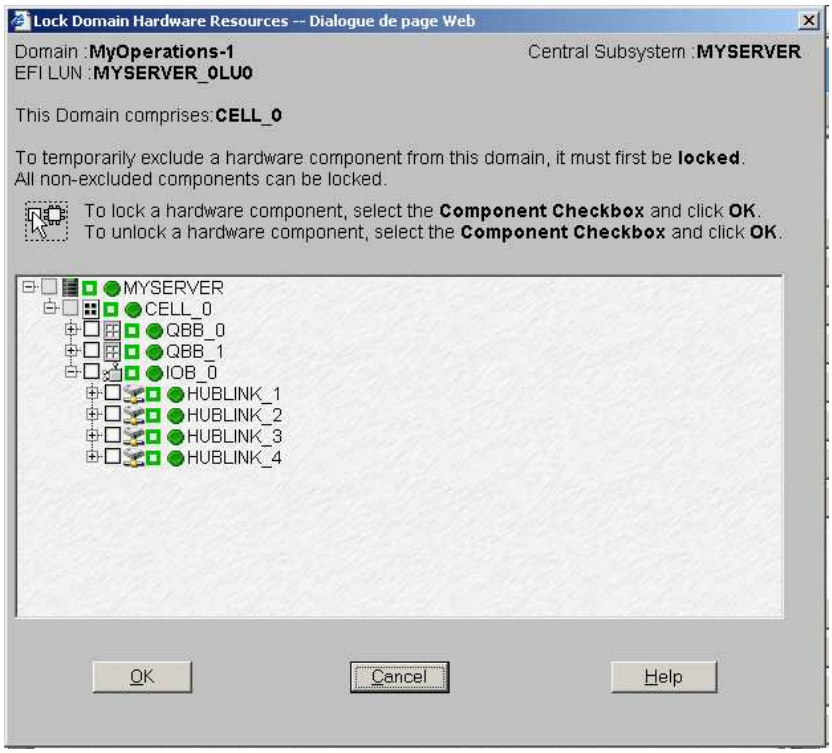


Figure 90. Lock domain hardware resources dialog

5. Expand the component tree to view the hardware element you want to lock / unlock.
6. Select the corresponding checkbox to lock the element or deselect to unlock a previously locked element.

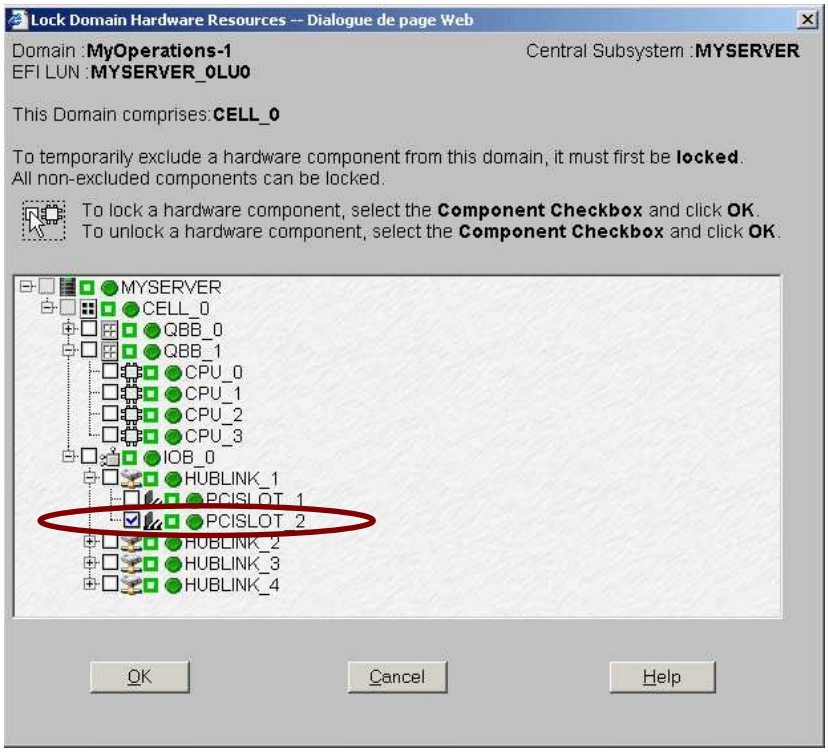


Figure 91. Lock domain hardware resources dialog – PCI slot selected

7. Click **OK** → **Apply**. Changes will be applied at the next domain power on.

Deleting a Domain

Note:
The domain must be **INACTIVE** to be deleted.

Once loaded in the **Domain Manager** Control pane, a domain can be deleted from the current configuration. When the domain has been deleted, the corresponding resources can be re–allocated to another domain.

To delete a domain from the current configuration:

1. Click **Domain Manager** to open the Control pane.
2. Select the required domain.
3. Click **Delete** in the Command bar. The **Confirm Remove Domain** dialog opens.

NovaScale 6080/6160 Server

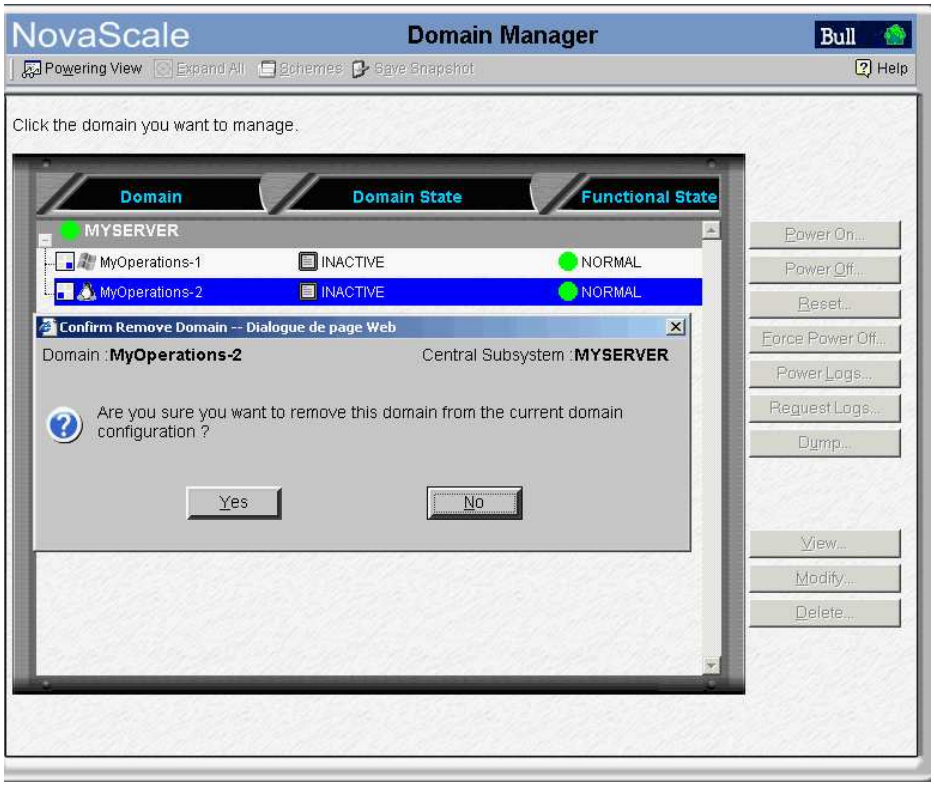


Figure 92. Delete domain dialog – mono–module server

NovaScale 6320 Server

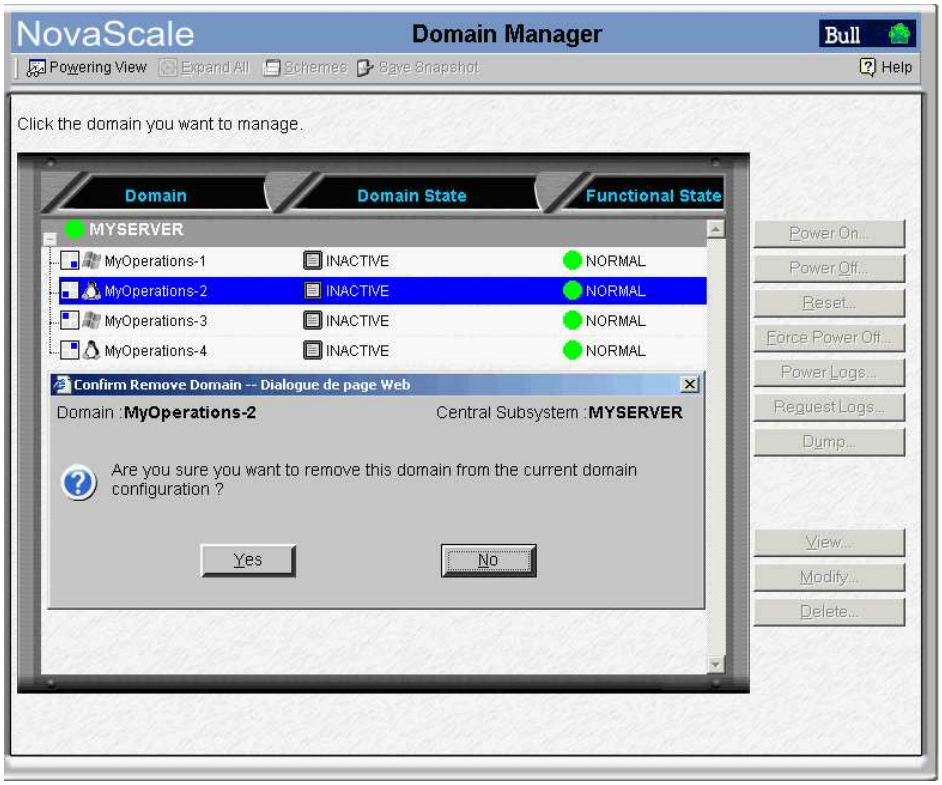


Figure 93. Delete Domain dialog – bi–module server

4. Click **Yes** to confirm deletion of the selected domain from the current configuration.

An information box opens, informing you that the domain has been successfully deleted. The domain is no longer visible in the Control pane.

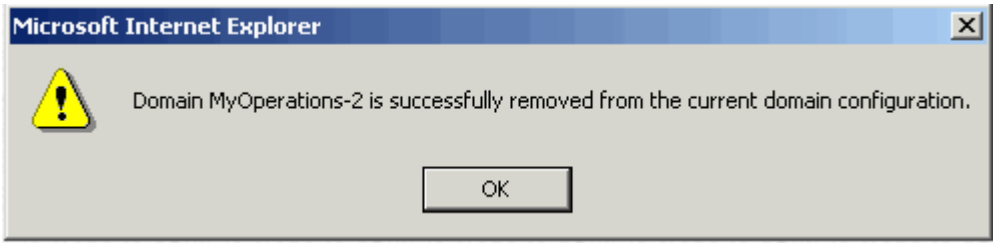


Figure 94. Domain deleted information box

5. Click **OK** to continue.

   You can now re–allocate the resources of the deleted domain. See *Adding a Cell to a Domain*, on page 3-55

Note:
Domain modifications are not automatically saved and are only applicable while the selected domain is loaded in the **Domain Manager** Control pane. If required, you can manually save the new configuration for future use. See *Saving the Current Domain Configuration Snapshot*, on page 3-11.

What To Do if an Incident Occurs

When an incident occurs during a domain **Power ON** / **Power OFF** / **Force Power OFF** / **Reset** sequence, a message is displayed in the **Domain Status** panel and a trace is recorded in the **Domain POWER Logs**. Table 21 indicates the messages that may be displayed during an incorrect power sequence.

NovaScale 5xx0 Servers

SEQUENCE	ERROR MESSAGE
Powering up	**Powering up all components failed**
	Timeout during Power On
Bios loading	**BIOS initialization timeout**
	BIOS init timeout during recovery
Starting EFI	**Timeout during starting EFI**
Powering down	**Powering down failed**
	Powering down timeout
Force Power OFF	**Terminating timeout**
	Terminating KO

NovaScale 6xx0 Servers

SEQUENCE	ERROR / INFORMATION MESSAGE
POWERING ON	**POWERING ON FAILED**
	TIMEOUT DURING POWER ON
	POWERING ON SUSPENDED
	DOMAIN HALTED
POWERED ON – LOADING BIOS	**RECOVERING BIOS**
	BIOS LOADING TIMEOUT
BIOS READY – STARTING EFI	**TIMEOUT DURING START EFI**
POWERING DOWN	**POWER DOWN FAILED**
	TIMEOUT DURING POWER DOWN

Table 21. Domain power sequence error messages

PAM software also informs connected and non–connected users via:

- the PAM Web interface (**Status Pane** and/or **User History** files),
- e–mail (users with an appropriate Event Message subscription),

- an autocall to the Bull Service Center (according to your maintenance contract) for analysis and implementation of the necessary corrective or preventive maintenance measures, where applicable.

As Customer Administrator, you have access to the **System History** files and associated **Help Files**. As Customer Operator, you have access to the **User History** and/or **Web Event Messages**, and associated **Help Files**, pre–configured by your Customer Administrator.

You will find all the advice you need in the **Help Files** associated with the **System** / **User History** and **Web Event Messages** you are authorized to view.

Whether you open a **Web Event Message** or a **System** / **User History** file, the resulting display and utilities are the same. See *Viewing and Managing PAM Event Messages and History Files*, on page 4-28.

Note:
All incidents are systematically logged in the **System History** files, which you can view as Customer Administrator at any time.

Dealing with Incidents

When you open the incident **Help File**, you may be requested to contact your Customer Service Engineer or perform straightforward checks and actions:

Checking POST Codes

If you are requested to check POST Codes, see *Viewing Domain BIOS Info*, on page 3-30.

Checking Hardware Exclusion Status

If you are requested to check hardware exclusion status, see *Excluding / Including Hardware Elements*, on page 4-25.

Checking Hardware Connections

If you are requested to check hardware connections, use Appendix *Cabling Diagrams* to manually and visually ensure that all cables are correctly inserted in their corresponding hardware ports.

Rebooting Maestro / Resetting the PMB

If you are requested to reboot Maestro or to reset the PMB, see *Checking, Testing, and Resetting the PMB* , on page 4-45.

Rebooting the PAP Application

If you are requested to reboot the PAP application:

1. From the Microsoft Windows home page, click **Start** → **Programs** → **Administrative Tools** → **Component Services**.
2. From **Component Services**, click **Console Root** → **Component Services** → **Computers** → **My Computer** → **COM+ Applications** → **PAP**.
3. Right click **PAP** to open the shortcut menu. Click **Shutdown**.
4. Activate the required PAM version to reboot the PAP application. See *Deploying a PAM Release*, on page 5-23 and *Activating a PAM Version*, on page 5-24.

Powering OFF/ON the Domain

If you are requested to Power OFF/ON or Force Power OFF a domain, ensure that you have saved data and closed open applications. See *Powering ON a Domain*, on page 3-14, *Powering OFF a Domain*, on page 3-18, and *Forcing a Domain Power OFF*, on page 3-21.

Resetting a Domain

If you are requested to Reset a domain, see *Manually Resetting a Domain*, on page 3-24.

Performing a Domain Memory Dump

If you are requested to perform a domain memory Dump, see *Performing a Domain Memory Dump*, on page 3-26.

Turning the Site Breaker Off

The server is not equipped with a physical power button and can only be completely powered down by turning the site breaker off.

Chapter 4. Monitoring the Server

This chapter explains how, as Customer Administrator, you can supervise server operation and how as Customer Administrator and/or Operator you can view and manage PAM Messages, Histories, Archives and Fault Lists. It includes the following topics:

☞ **Note:**
Customer Administrators and Customer Operators are respectively advised to consult the *Administrator's Memorandum*, on page xxviii or the *Operator's Memorandum*, on page xxx for a detailed summary of the everyday tasks they will perform.

For further information about user accounts and passwords, see *Setting up PAP Unit User*s, on page 5-17.

Introducing PAM Monitoring Tools

Main Central SubSystem (CSS) hardware components are managed by the comprehensive Platform Administration and Maintenance (PAM) software specifically designed for Bull NovaScale Servers.

☞ **Note:**
Peripheral devices such as disk racks, PCI adapters, KVM switch, local console, and the PAP unit are managed by the Operating System and/or by dedicated software.
For details on how to monitor these devices, please refer to the user documentation provided on the Bull NovaScale Server Resource CD–Rom.

PAM software permanently monitors and regulates CSS hardware during operation, ensuring automatic cooling for compliance with environmental requirements, power ON / OFF sequences, component presence and functional status checks, and event handling and forwarding.

In–depth monitoring is a Customer Administrator function and the PAM **Hardware Monitor** is only available to users with administrator access rights. However, all connected users are permanently and automatically informed of CSS functional status via the PAM **Status** pane and of domain status via the PAM **Domain Manager Control** pane.

The PAM **Event Messaging** system offers comprehensive event message subscription options allowing both connected and non–connected users to be informed of server status. See *Customizing the PAM Event Messaging System*, on page 5-114 for details.

To refresh the PAM display:

- Click the **Refresh Tree** button in the PAM Tree toolbar to refresh the PAM Tree.
- Click a node in the PAM Tree to refresh the corresponding Control pane display.
- Click the **Refresh Web Page** button to return to the PAM Home Page.

☞ **Note:**
DO NOT use the Refresh option obtained by right clicking the mouse in the browser window.

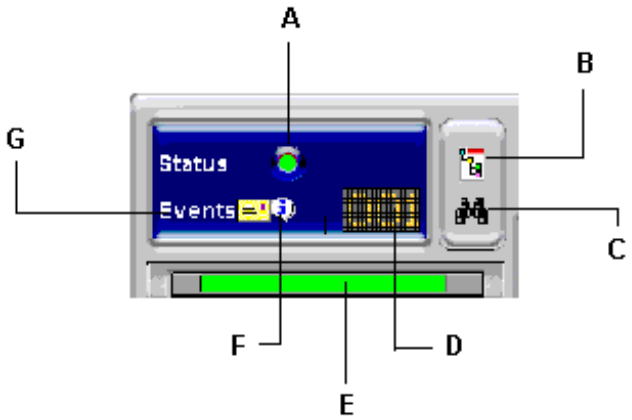
Viewing System / Component Status

What You Can Do

- *Check system status*
- *Check CSS module availability status*
- *Check event message status*
- *View hardware presence status*
- *View hardware functional status*
- *View server hardware status*
- *View FRU information*
- *View firmware information*
- *View thermal status*
- *View power status*
- *View temperature status*
- *View fan status*
- *View jumper status*
- *View PCI slot status*

PAM Status Pane

When you log onto the PAM Web site, you are able to check system status at a glance via the **Status** pane which provides quick access to CSS Module availability status, server functional status, and pending event message information.



A	System Functional Status icon	**E**	CSS Availability Status icon
B	Presence/Functional Status toggle button	**F**	Event Message Severity icon
C	Event Message Viewer		New Event Message icon
D	Pending Event Message icon		

Figure 95. PAM Status pane

CSS Availability Status

The CSS availability status bar reflects the operational status of the data link(s) between the Platform Management Board (PMB) embedded in each CSS Module and the PAP Unit. Each CSS module is represented by a zone in the status bar.

- When a CSS Module PMB is detected as **PRESENT**, the corresponding zone in the status bar is **GREEN**.
- When a CSS Module PMB is detected as **ABSENT**, the corresponding zone in the status bar is **RED**.
- When you hover the mouse over the status bar, an **Infotip** displays the **presence status** of CSS Module PMB – PAP Unit data links.

The following figure represents the status bar for a bi–module server. One CSS Module PMB is detected as PRESENT and the other is detected as ABSENT.

A: Bar red (CSS Module_0 not available)

Figure 96. CSS Module availability status bar

System Functional Status

If the system is operating correctly, the **System Functional Status** icon is green. Table 22. explains possible system functional status indications.

Icon	Status	Explanation
Green	**NORMAL**	No problem detected. The system is operating correctly.
Yellow	**WARNING**	Minor problem reported. The system is still operational.
Orange	**CRITICAL**	Serious problem reported. The system is no longer capable of operating correctly. PAM may generate an OS shutdown request.
Red	**FATAL**	Major problem reported. PAM may automatically shut down the OS. The system is partially or totally stopped.
Purple	**NOT ACCESSIBLE**	Status cannot be computed (detection circuit error).

Table 22. CSS hardware functional status icons

Important:
If the system functional status icon and/or CSS availability status bar is/are not green, see *What to Do if an Incident Occurs*, on page 4-39.

Event Message Status

The **New Event Message** icon informs you that new messages have arrived and that you can click the **View Event Message** icon to view them (the number of unprocessed event messages is also displayed). See *Consulting Event Messages, Hardware Faults and History/Archive Files*, on page 0.

The **Event Message Severity** icon indicates the set maximum severity level of unprocessed event messages. See *Understanding Message Severity Levels*, on page 4-29.

PAM Tree Pane

As Customer Administrator, you can view the presence and functional status of each hardware element from the PAM Tree pane. The PAM Tree pane is refreshed at your request. Use the **Refresh PAM Tree** button to update the display when required.

Important:
To maintain a trace of transient faults, PAM Tree functional and/or presence status indicators will not change color until the domain has been powered OFF/ON, even if the error has been corrected.

Displaying Presence Status

When, as Customer Administrator, you log onto the PAM Web site, server hardware presence status is displayed in the PAM Tree by default (square, colored indicator next to the **Hardware Monitor** node). If you expand the PAM Tree, the presence status of all hardware elements is displayed.

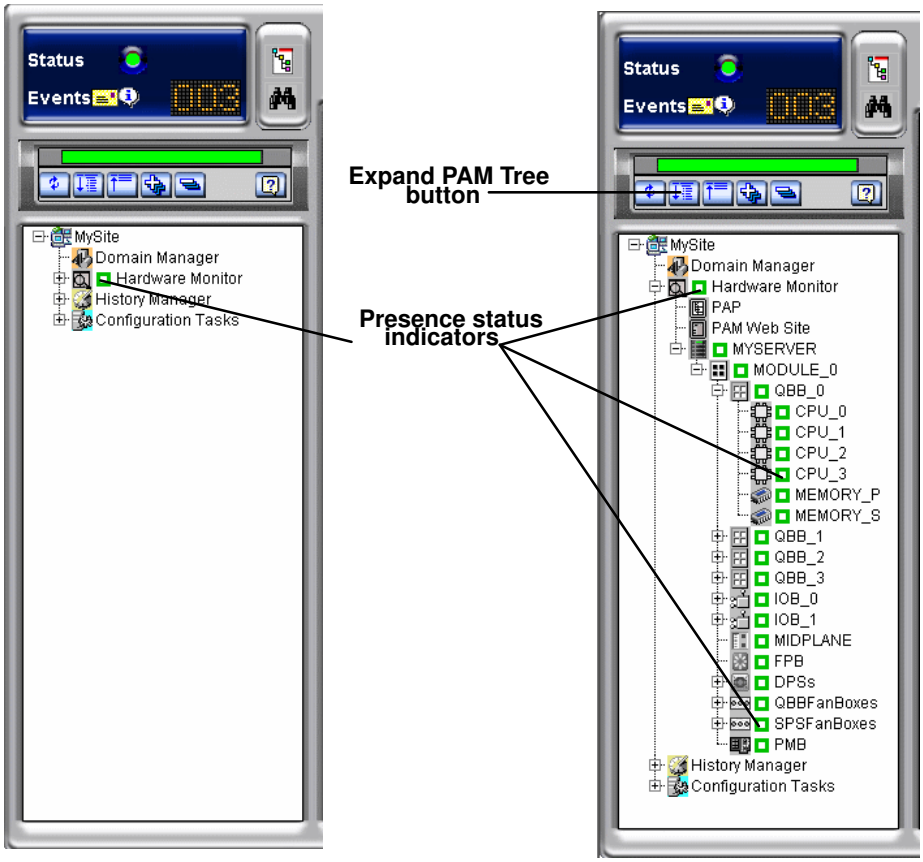


Figure 97. PAM Tree hardware presence status display

When hardware presence status is normal, all presence status indicators are green. Table 23. explains possible hardware presence status indications.

Presence Status Indicators

Indicator	Status	Explanation
 Green	**NORMAL**	This hardware element: – is physically present and accessible.
 Red	**MISSING**	This hardware element: – was present in a previous configuration but has disappeared.
 Red/white	**MISSING**	A sub–component of this hardware element: – was present in a previous configuration but has disappeared.
 Purple	**NOT ACCESSIBLE**	This hardware element: – cannot be computed (detection circuit error).
 Purple/white	**NOT ACCESSIBLE**	A sub–component of this hardware element: – cannot be computed (detection circuit error).
 Purple/red	**MISSING AND NOT ACCESSIBLE**	A sub–component of this hardware element: – was present in a previous configuration but has disappeared. A sub–component of this hardware element: – cannot be computed (detection circuit error).

Table 23. Hardware presence status indicators

Important:
If a PAM Tree hardware presence status indicator is not green, this could be normal if a hardware element has been removed for maintenance. See *What to Do if an Incident Occurs*, on page 4-39.

Displaying Functional Status

You can toggle the PAM Tree to view system / hardware functional status (round, colored indicator next to the **Hardware Monitor** node). If you expand the PAM Tree, the functional status of all hardware elements is displayed. Functional Status is a composite indicator summarizing Failure Status, Fault Status, Power Status, and Temperature Status indicators, where applicable.

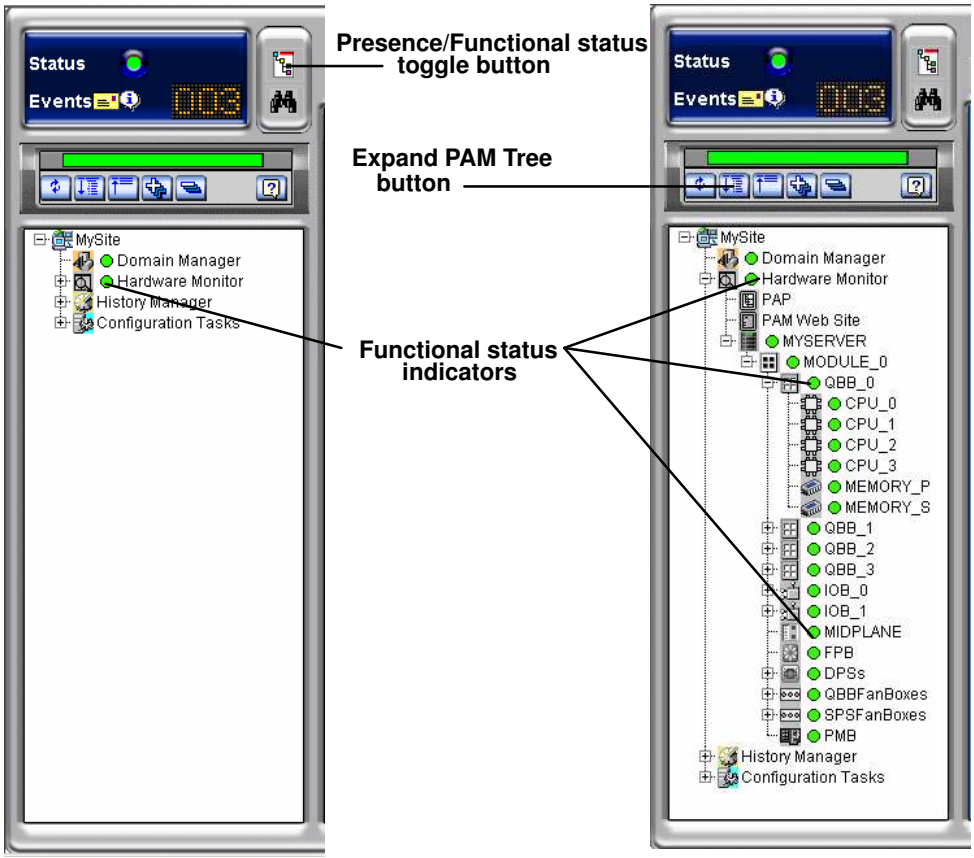


Figure 98. PAM Tree functional status display

When hardware functional status is normal, all functional status indicators are green. Table 24. explains possible hardware functional status indications.

Functional Status Indicators

Indicator	Status	Explanation
Green	**NORMAL**	No problem detected. This hardware element is operating correctly.
Yellow	**WARNING**	Minor problem reported. This hardware element is still operational.
Orange	**CRITICAL**	Serious problem reported. This hardware element is no longer capable of operating correctly. PAM may generate an OS shutdown request.
Red	**FATAL**	Major problem reported. PAM may automatically shut down the OS. System integrity is jeopardized.
Purple	**NOT ACCESSIBLE**	The functional status of this hardware element cannot be computed (detection circuit error).

Table 24. Hardware functional status indicators

Important:
To maintain a trace of transient faults, PAM Tree functional and/or presence status indicators will not change color until the domain has been powered OFF/ON, even if the error has been corrected. Overall server functional status is indicated by the system Functional Status icon in the Status pane. For further details, see *What to Do if an Incident Occurs*, on page 4-39.

Note:
If, when you toggle the PAM Tree to view hardware functional status, the functional status of a hardware element is not normal, the **Hardware Monitor** node will automatically expand to the level of the malfunctioning hardware element, as shown in Figure 99.

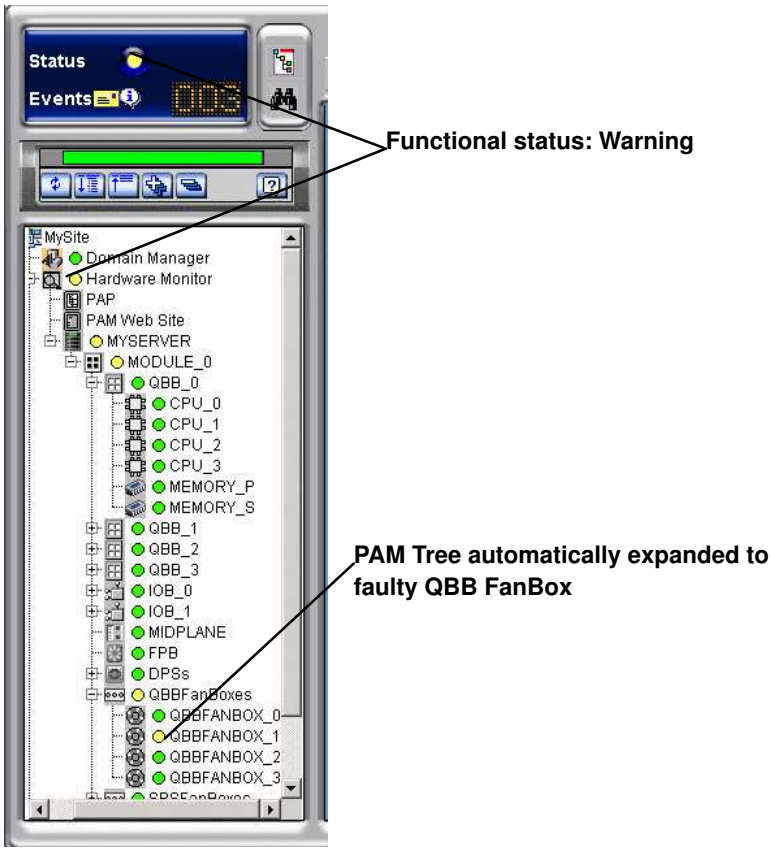


Figure 99. PAM Tree – automatically expanded functional status display

Using PAM Utilities

What You Can Do

- *Search for excluded hardware elements*
- *Search for missing hardware elements*
- *View PAM Web site information*
- *View PAM version information*
- *Exclude / include hardware elements*

Using the Hardware Search Engine

The **Hardware Search** engine allows you to search for and view hardware elements corresponding to selected criteria, for example **Excluded** or **Missing** hardware elements.

Notes:

- Excluded hardware elements are those that have been **logically** excluded from the server. See *Excluding / Including Hardware Elements*, on page 4-25.
- Missing hardware elements are those that have been **physically** removed from the server (e.g. for maintenance).

To search for specific hardware:

1. Click **Hardware Monitor** in the PAM tree to open the **Hardware Search** page.

Figure 100. Hardware Search engine

2. Select the required search criteria from the dropdown box and click **OK**.

3. Once the search is complete, results are displayed in the control pane.

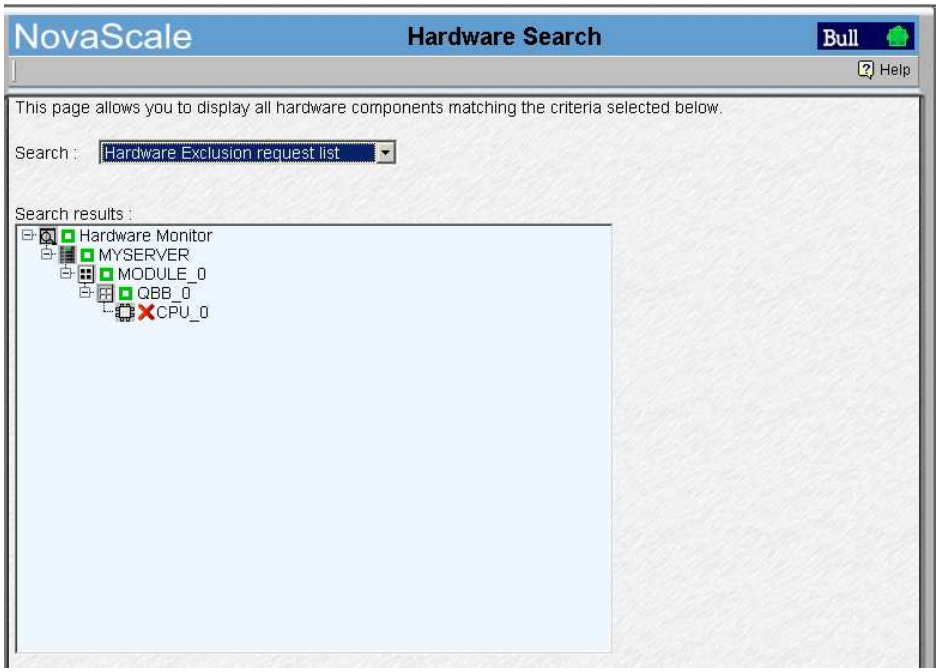


Figure 101. Hardware Search result list (example)

Viewing PAM Web Site User Information

As Customer Administrator, you can view the list of PAM users currently logged onto the PAM Web site by clicking **Hardware Monitor** → **PAM Web Site**.

The Web site version and a list of connected users and session details are displayed in the **Control** pane. The current session is indicated by the icon.

Note:
You can view user roles by selecting a user and clicking **View Roles** in the toolbar. The roles associated with this user are displayed in the **Roles for selected session** dialog.

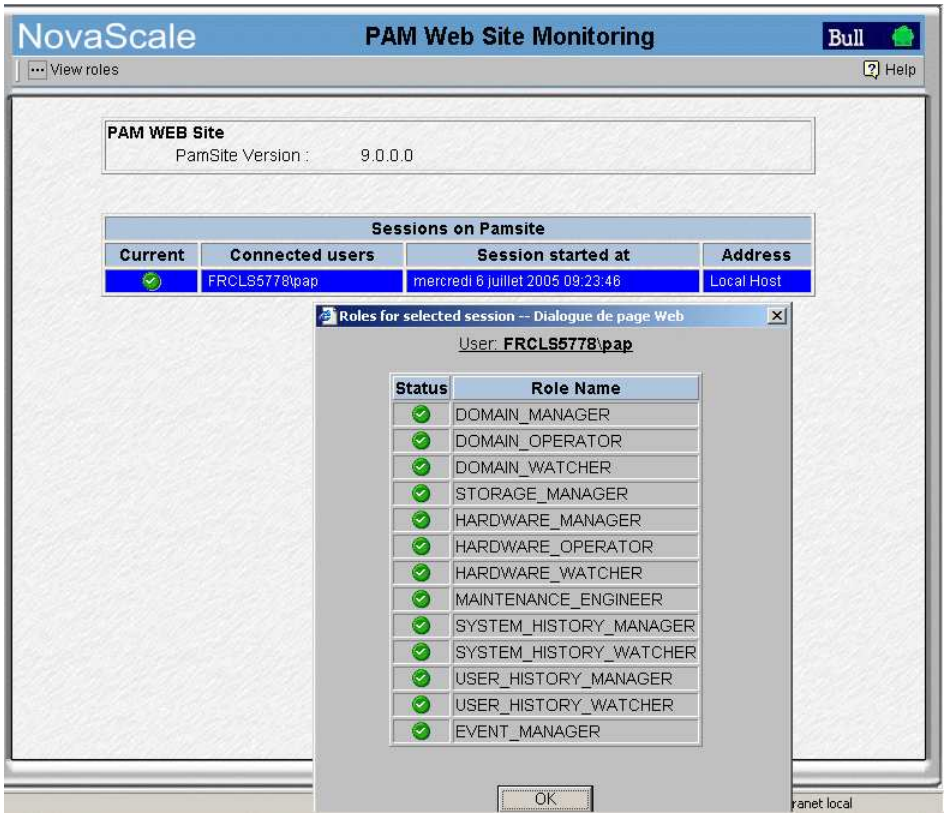


Figure 102. PAM Web Site user information

Viewing PAM Version Information

PAM version information may be useful to help your Customer Service Engineer solve software–related problems.

To view PAM version, site data and release data, click **Hardware Monitor** → **PAP**. The **PAP Unit Information** Control pane opens, indicating PAM software version details along with **PAM Site Data** and **Release Data** directory paths:

- the PAM **Release Data** directory is used for all the files delivered as part of PAM software to ensure configuration consistency.
- the PAM **Site Data** directory is used for all the the files produced by PAM software (history files, configuration files) concerning Customer site definition and activity.

To view complete PAM resource file information, click **More Info**. The **PAM Versions** dialog opens.

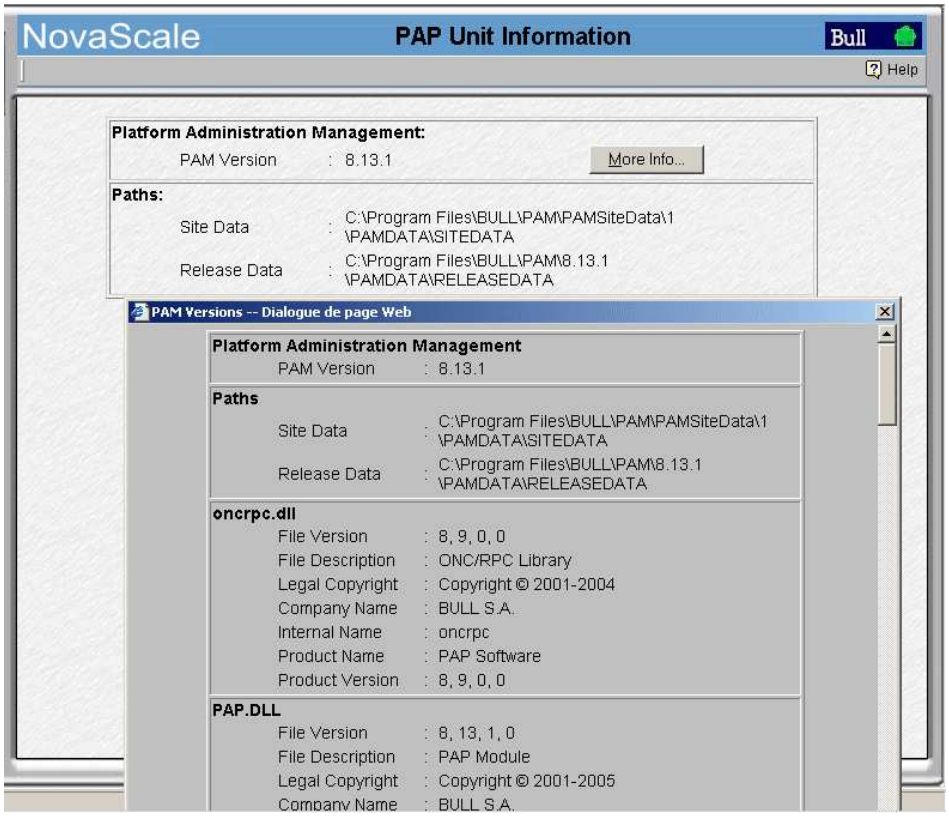


Figure 103. PAP unit information

If you want to deploy a new PAM release or activate another PAM version, see *Deploying a New PAM Release*, on page 5-23 and *Activating a PAM Version*, on page 5-24.

Viewing Server Hardware Status

When you click the **CSS Name** in the PAM tree (e.g. **MYSERVER** in the figure), the **Hardware Monitor** displays a visual representation of the presence and functional status of CSS module components in the Control pane. Each primary hardware element functional status indicator is a clickable hotspot leading directly to the detailed **Hardware Status** page.

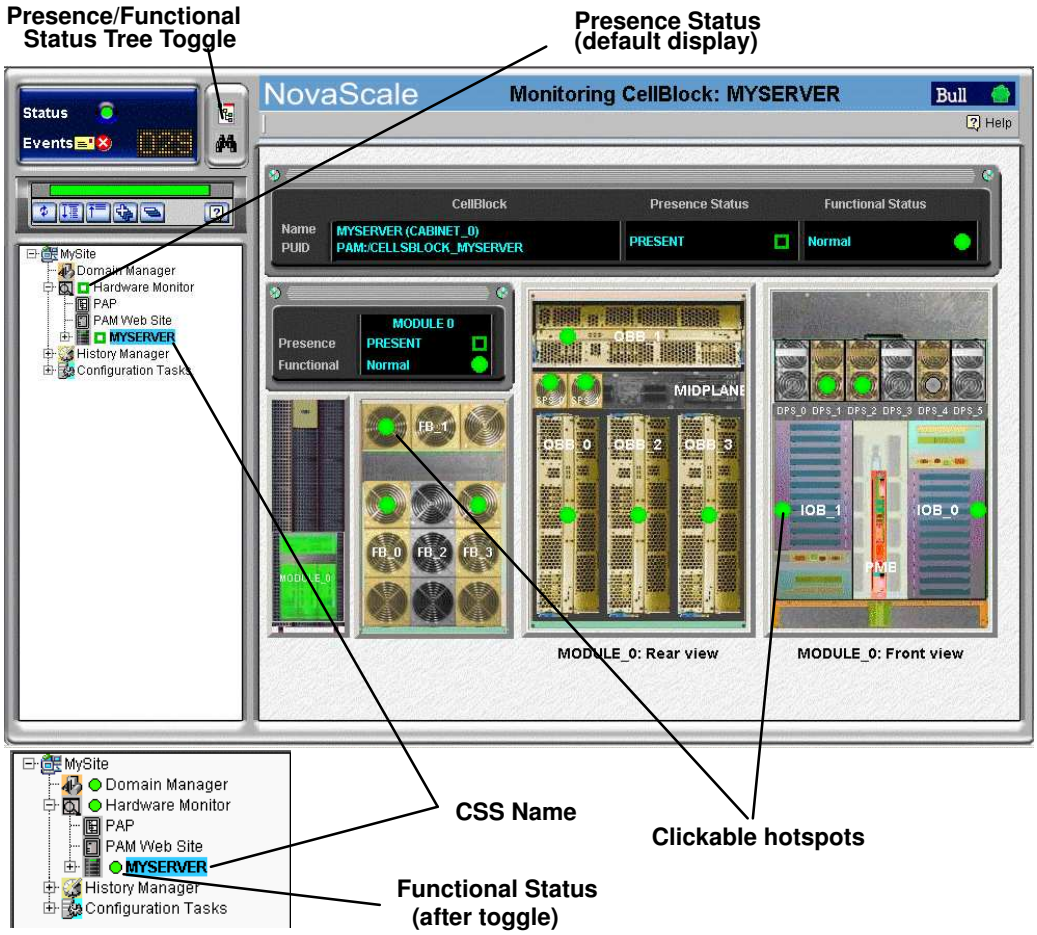


Figure 104. PAM Hardware Monitor

As you click a hardware element hotspot in the Control pane, you will notice that the PAM Tree automatically expands to the selected component level.

Note:
If a component is not part of your configuration, it is grayed out in the display.
If a component is part of your configuration but has been detected as “missing”, it is displayed in red.

The meanings of presence and functional status indicators are explained in Table 23. *Presence Status Indicators*, on page 4-6 and Table 24.*Functional Status Indicator*s, on page 4-7.

Important:
If a functional status indicator is not green, see *What to Do if an Incident Occurs*, on page 4-39.

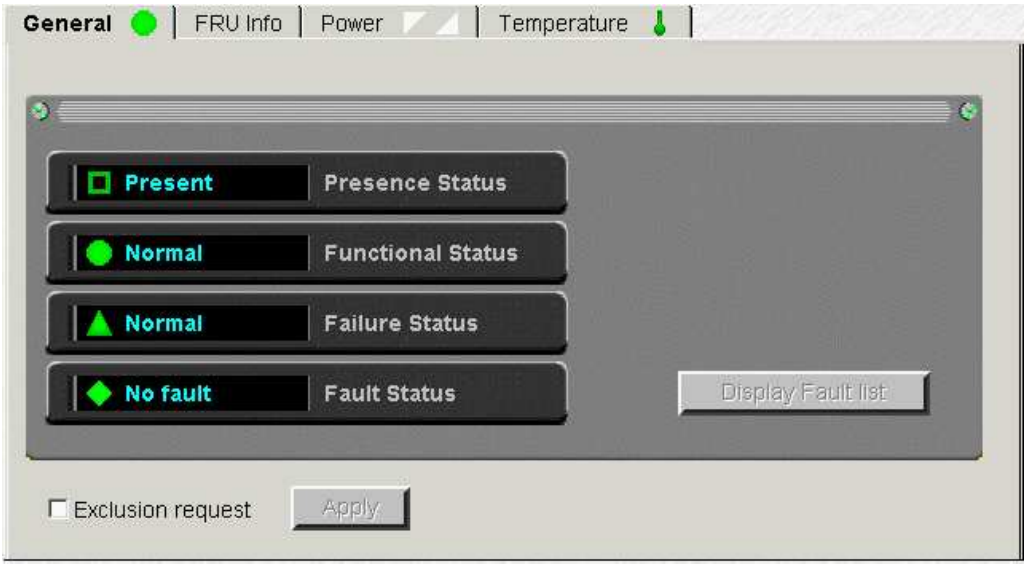
Note:
The NovaScale 6320 Server Hardware Monitor Control pane displays a visual representation of the presence and functional status of the components of both CSS modules.

Viewing Detailed Hardware Information

For detailed information about module / component / sub–component status, you can either click the corresponding hotspot in the **Hardware Monitor** Control pane or click the required hardware element in the PAM Tree to open the **Hardware Status** page.

General Tab

The **General** tab gives access to the following information:



Presence Status	Indicates if the hardware element is physically present and correctly configured. See *Presence Status Indicators*, on page 4-6.
Functional Status	Indicates if the hardware element is functioning correctly. See *Displaying Functional Status*, on page 4-7. **NOTE:** Functional Status is a composite indicator summarizing Failure Status, Fault Status, Power Status, and Temperature Status indicators, where applicable.
Failure Status	Indicates if a failure has been detected on the hardware element. **NOTE:** This feature is reserved for future use. See *Failure Status Indicators*, on page 4-16.
Fault Status	Indicates if a fault has been detected on the hardware element. See *Fault Status Indicators*, on page 4-16.
Display Fault List	When a fault is detected, a fault message is generated and the **Display Fault List** button gives direct access to the list of faults recently encountered by this hardware element. See *Consulting Event Messages, the Hardware Faults List, and History Files*, on page 0.
Exclusion Request	The Exclusion Request checkbox is used to logically exclude/include hardware elements from the domain at the next power–on. See *Excluding / Including Hardware Elements*, on page 4-25.

Figure 105. General Hardware Status page (example)

Failure Status Indicators:

Indicator	Status	Explanation
Green	**NORMAL**	PAM software has detected no failures on this hardware element.
Orange	**DEGRADED**	PAM software has detected that this hardware element is running at sub–standard capacity but is not jeopardizing system performance.
Red	**FAILED**	PAM software has detected a failure that may be jeopardizing system performance.
Gray	**UNKNOWN**	PAM software is not receiving diagnostic information from this hardware element.

Fault Status Indicators

Fault Status**,** accessible via the **General** tab,

Indicator	Status	Explanation
Green	**NORMAL**	PAM software has detected no faults on this hardware element.
Red	**FAULTY**	PAM software has detected 1 or more fault(s) on this hardware element.
Gray	**UNKNOWN**	PAM software is temporarily meaningless (e.g. hardware element missing).

Table 25. Fault status indicators

FRU Info Tab

The **FRU Info** tab gives access to Field Replaceable Unit identification data for the hardware element, such as Manufacturer's name, product name, part number, ...

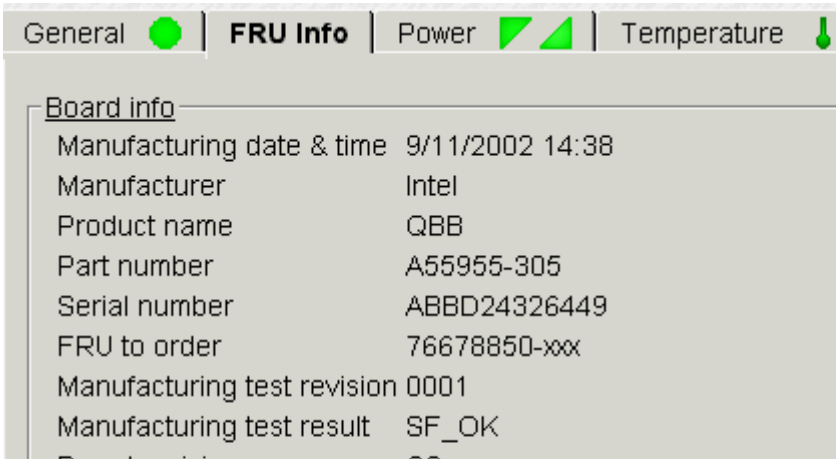


Figure 106. FRU data (example)

Firmware Tab (Midplane & PMB only)

The **Firmware** tab gives access to firmware version data for the hardware element.

Note:
Firmware versions may differ.

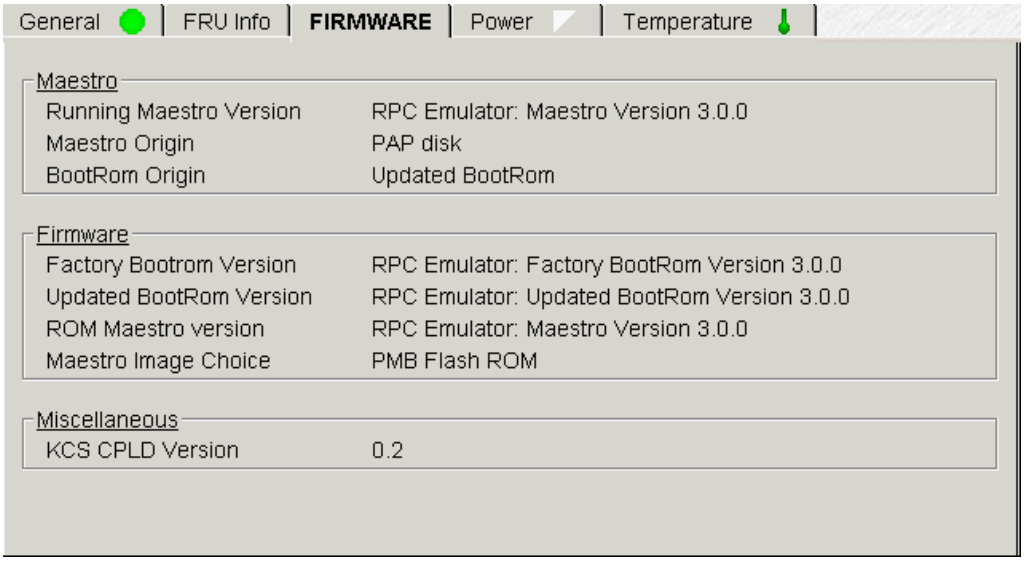


Figure 107. Firmware data (example)

Thermal Zones (CSS module only)

Thermal Zones, accessible via the **Thermal zones** tab, shows the thermal zones monitored by PAM software. A cooling error in a thermal zone will affect all the hardware elements in that zone. See *Displaying Functional Status*, on page 4-7.

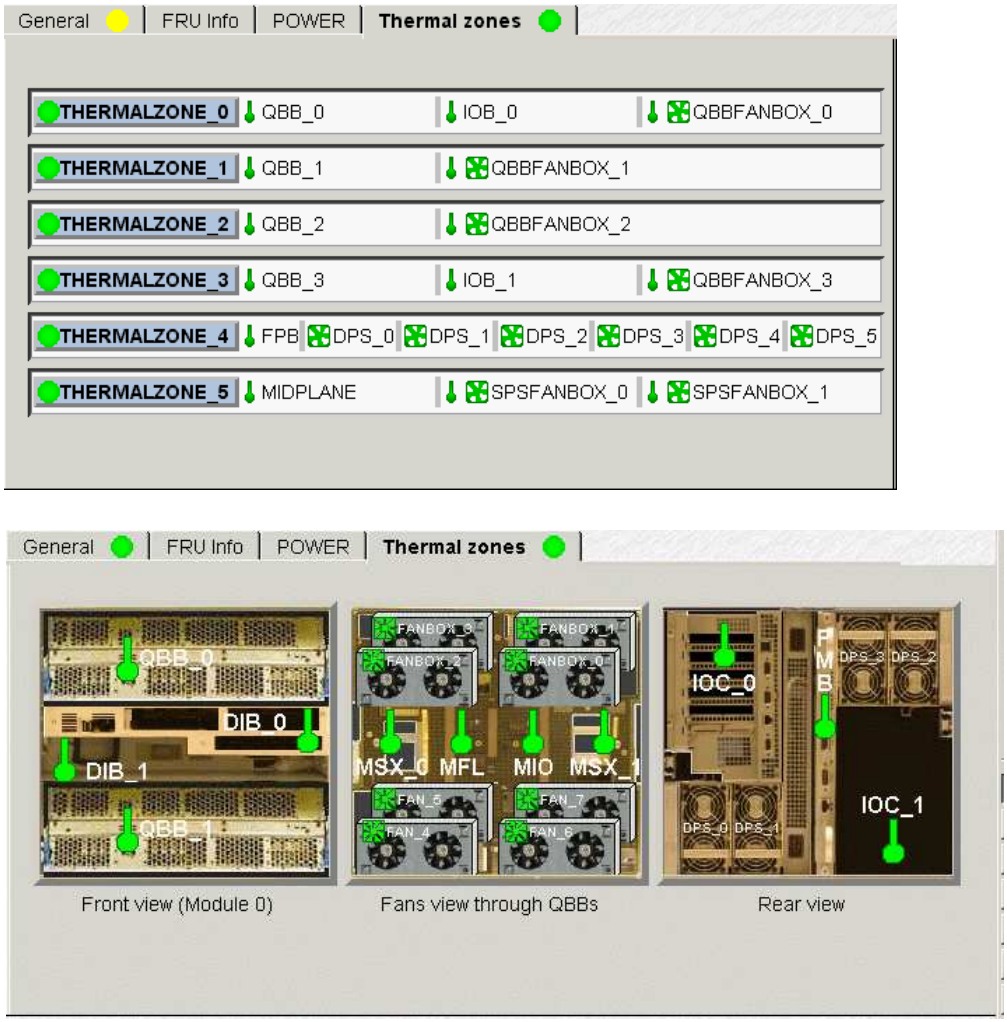


Figure 108. CSS module thermal zone details

Note:
When a thermal fault is detected, a fault message is generated and the **General** tab **Display Faults List** button gives direct access to the corresponding logs.

Power Tab

The **Power** tab gives access to power status data for the hardware element, indicating main and standby power state and/or power–specific faults for each converter. See *Displaying Functional Status*, on page 4-7.

Once connected to the Customer's site power supply, server hardware elements initialize to the stand–by mode. Server hardware elements initialize to the main mode when the domain is powered up.

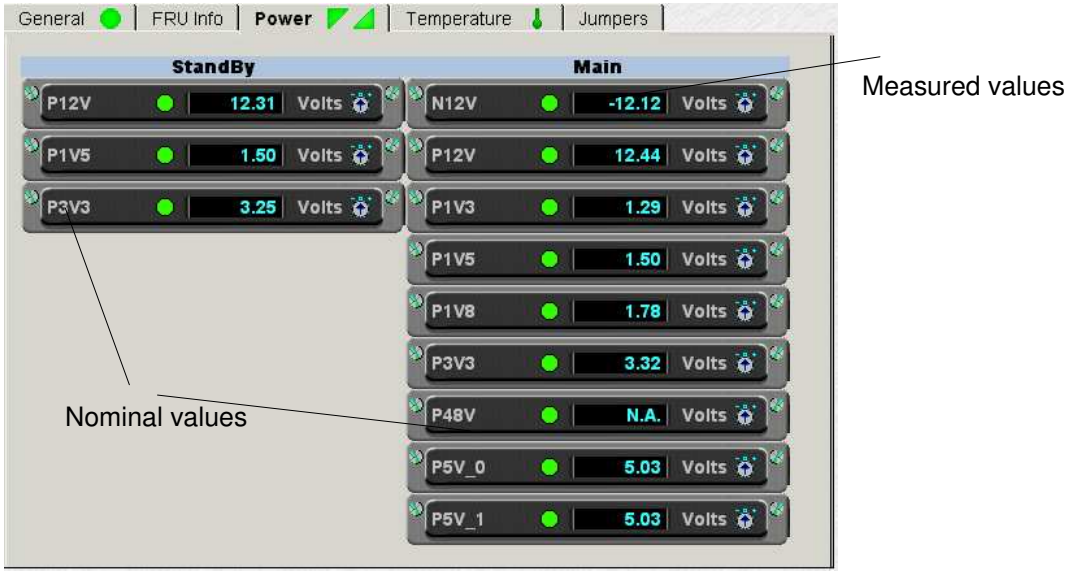


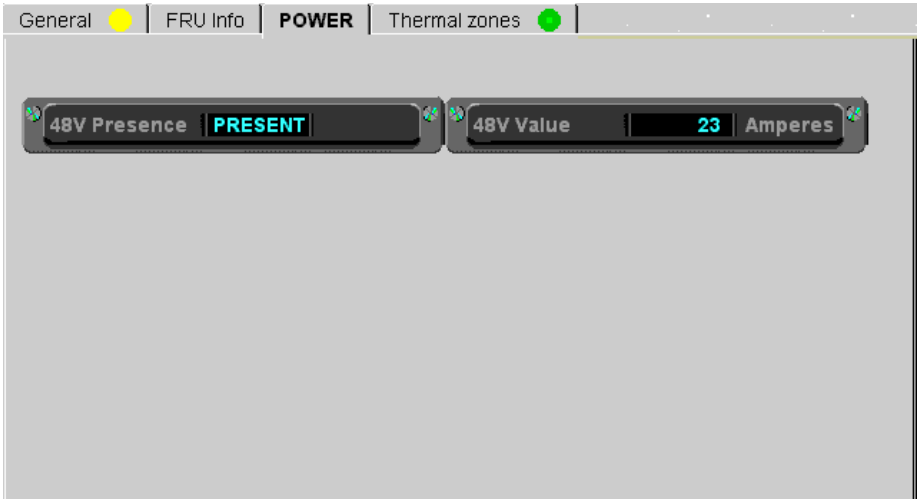
Figure 109. Converter power status details (example)

Indicator	Status	Explanation
Green	**MAIN POWER ON**	Hardware element main / standby power is on.
Green	**STANDBY POWER ON**	
White	**MAIN POWER OFF**	Hardware element main / standby power is off.
White	**STANDBY POWER OFF**	
Red	**MAIN POWER FAULT/FAILED**	PAM software has detected 1 or more main / standby power fault(s) on this hardware element.
Red	**STANDBY POWER FAULT/FAILED**	
Gray	**MAIN POWER MISSING/UNKNOWN**	PAM software cannot read main / standby power status on this hardware element.
Gray	**STANDBY POWER MISSING/UNKNOWN**	

Table 26. Power tab status indicators

CSS Module Power Tab

The **Power** tab gives access to power status data for the CSS module DPS units.



48V Presence	Meaning
PRESENT	At least 1 DPS unit is ON.
ABSENT	All DPS units are OFF.
Not Found	PAM software cannot read CSS module power status.
48V Value	Current intensity in Amperes (varies according to configuration).

Figure 110. CSS module power status details

Note:
When a power–specific fault is detected, a fault message is generated and the **General** tab **Display Faults List** button gives direct access to the corresponding logs.

Temperature Tab

The **Temperature** tab gives access to temperature status data for the hardware element, indicating overtemperature or temperature–specific faults.

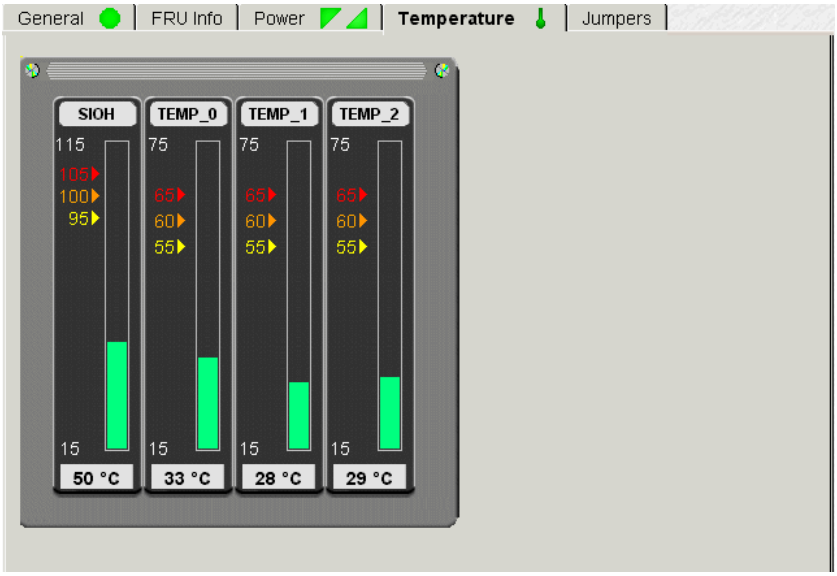


Figure 111. Temperature probe status details (example)

Indicator	Status	Explanation
Green	**NORMAL**	Hardware element temperature is normal.
Yellow	**WARNING**	PAM software has detected a rise in temperature on this hardware element, but it is still operational and is not jeopardizing system performance.
Orange	**CRITICAL**	PAM software has detected a critical rise in temperature on this hardware element. PAM will generate an OS shutdown request.
Red	**FATAL**	PAM software has detected a fatal rise in temperature on this hardware element. PAM will automatically shut down the OS.
Gray	**UNKNOWN**	PAM software cannot read temperature status on this hardware element.

Table 27. Temperature tab status indicators

Note:
When a temperature–specific fault is detected, a fault message is generated and the **General** tab **Display Faults List** button gives direct access to the corresponding logs.

Fan Status (QBB Fanboxes, SPS Fanboxes and DPS units only)

Fan Status, accessible via the **Fans** tab, indicates fan status, speed and supply voltage. See *Displaying Functional Status*, on page 4-7.

During normal operation, the display depicts fan rotation.

Each fanbox is equipped with 2 hot–swap, redundant, automatically controlled fans.

Note:
If all fans are halted in the display, check that your browser allows you to play animations in Web pages.

Figure 112. Fanbox details (example)

Jumper Status (IOB only)

Reserved for Customer Service Engineers.

Jumper Status, accessible via the **Jumpers** tab, indicates the current position of BIOS Recovery, ClearCMOS, and ClearPassword jumpers. Reserved for Customer Service Engineers.

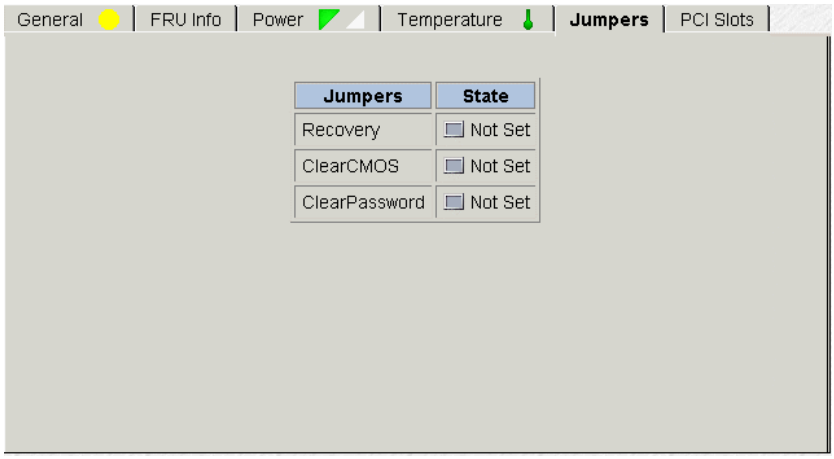


Figure 113. IOB jumpers tab

PCI Slots (IOB only)

PCI Slot Status, accessible via the **PCI Slots** tab, shows PCI board type and the functional and power status of PCI slots at the last domain power–on.

When a fault is detected on a PCI slot, a fault message is generated and an **IOB Fault List** button gives direct access to the list of faults recently encountered on the IOB.
The **Exclude** checkboxes are used to exclude / include one or more PCI slots in the domain at the next power–on. See *Excluding / Including Hardware Elements*, on page 4-25.

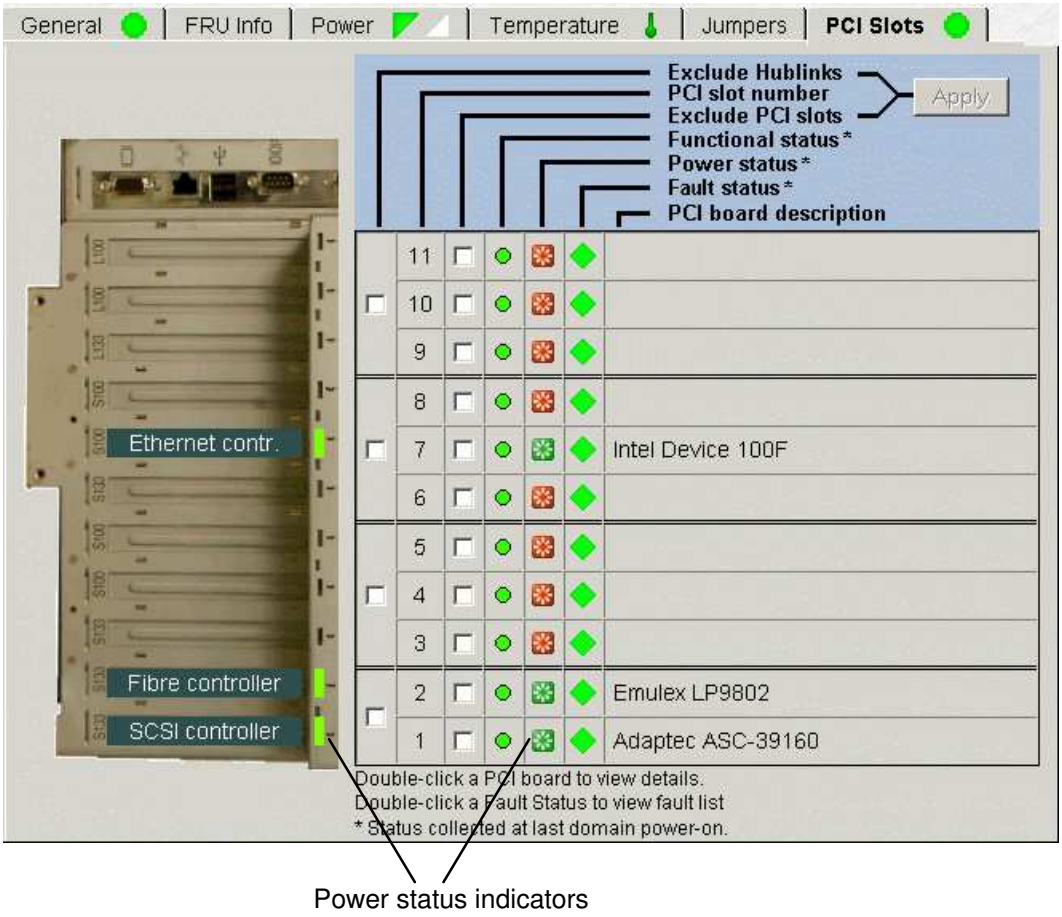


Figure 114. PCI slots tab

Clicking a PCI board gives access to **PCI Slot Details**: such as Minor and Signal status, Logical, Bus and Device numbers, Bus and Board frequencies, Vendor, Device and Revision identifiers, Susbsystem Vendor and Device identifiers and Class code.

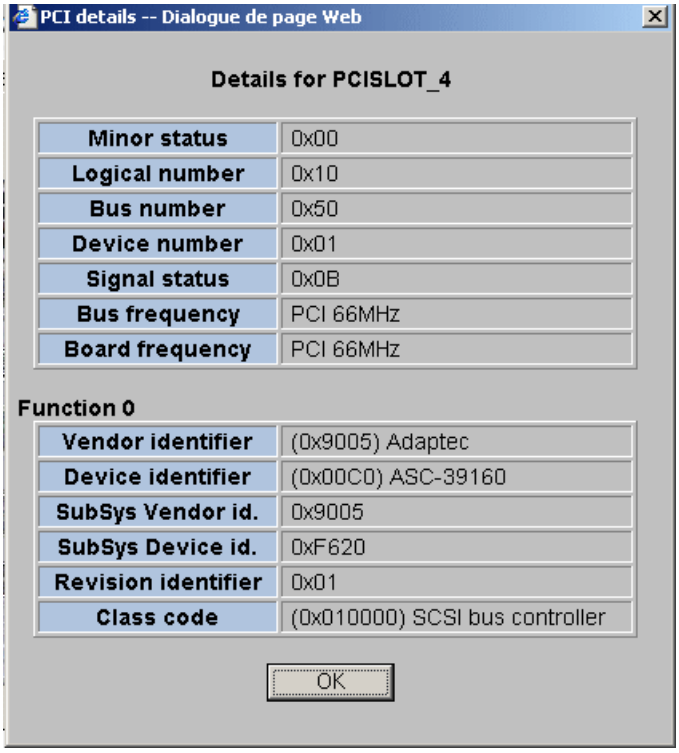


Figure 115. PCI slot details dialog (example)

Excluding / Including Hardware Elements

As Customer Administrator, if a redundant hardware element is faulty, you can logically **Exclude** it from the domain until it has been repaired or replaced. To be taken into account, exclusion requires domain power OFF/ON.

A complete list of logically excluded hardware elements can be obtained via the Hardware Monitor search engine. See *Using the Hardware Search Engine*, on page 4-9.

Important:
Hardware elements must be excluded with care. The exclusion of non–redundant hardware elements will prevent the server domain from booting. Exclusion guidelines are given in the Hardware exclusion guidelines table, on page 4-27.

Excluding a Hardware Element

Important:
The exclusion of a hardware element is only taken into account at the next domain power ON. A complete list of logically excluded hardware elements can be obtained via the Hardware Monitor search engine. See *Using the Hardware Search Engine*, on page 4-9.

1. Check that the hardware element is “excludable” and that exclusion will not affect domain availability. See *Hardware Exclusion Guidelines*, on page 4-27.
2. Click the required hardware element in the **PAM Tree** to open the **Hardware Status** page.

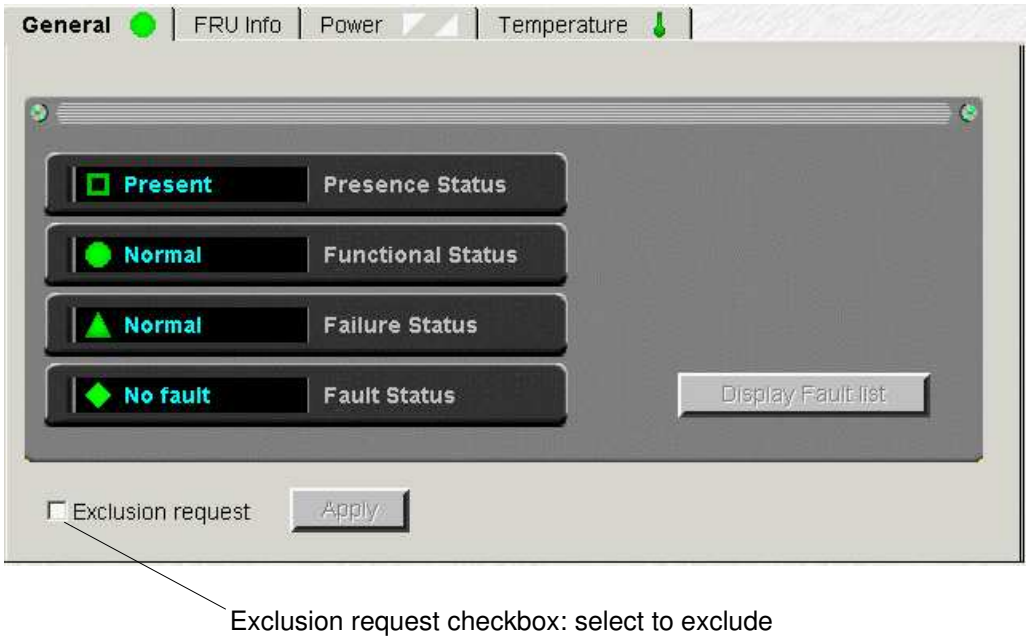


Figure 116. Inclusion

3. Select the **Exclude** checkbox and click **Apply**. The **Exclude** dialog box opens.
4. Click **Yes** to confirm exclusion of the selected hardware element. Exclusion will be taken into account at the next domain power ON.

Notes:
If you want to check domain hardware status, click **Domain Manager** → **Resources** → **More info...** to open the **Domain Hardware Details** page.

- Hardware components to be logically excluded from the domain at the next domain power ON are marked with a red / yellow icon in the **Lock Request** column in the **Domain Hardware Details** page.

See *Viewing Domain Configuration, Resources and Status*, on page 3-32.

Including a Hardware Element

Important:
The inclusion of a hardware element is only effective once the domain has been powered OFF/ON.

1. Click the required hardware element in the **PAM Tree** to open the **Hardware Status** page.

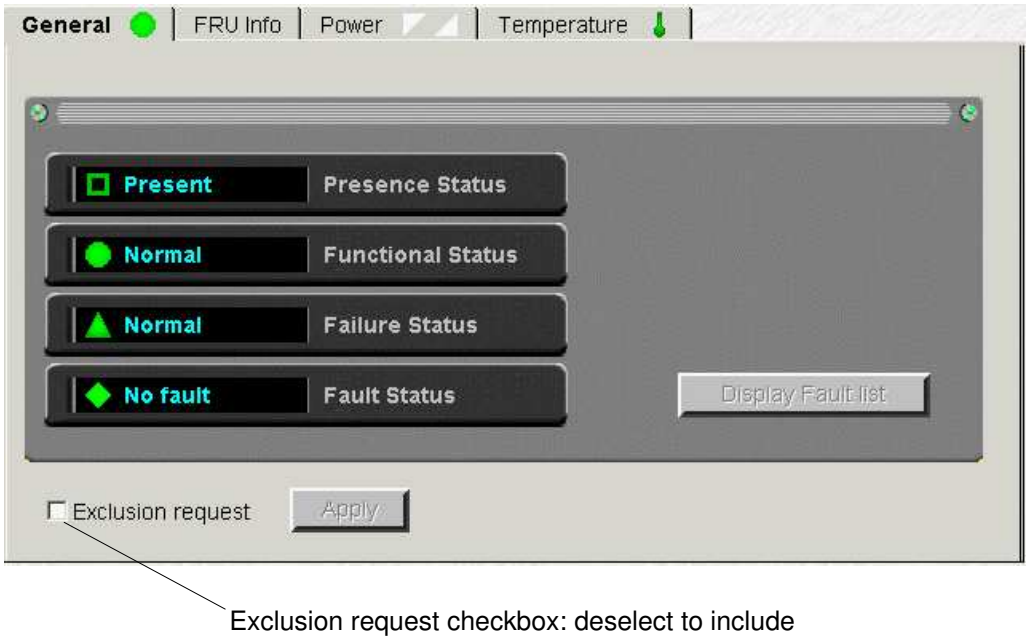


Figure 117. Example Hardware Status page

2. Deselect the **Exclude** checkbox and click **Apply**. The **Include** dialog box opens.
3. Click **Yes** to confirm inclusion of the selected hardware element. Inclusion will be taken into account at the next domain power ON.

Notes:
If you want to check domain hardware status, click **Domain Manager** → **Resources** → **More info...** to open the **Domain Hardware Details** page.

- Hardware components to be logically included in the domain at the next domain power ON are marked with a gray icon in the **Exclusion Request** column in the **Domain Hardware Details** page.

See *Viewing Domain Configuration, Resources and Status*, on page 3-32.

Hardware Exclusion Guidelines

Hardware Element	Exclusion Guidelines
IMPORTANT: **If the following hardware elements are excluded, the corresponding server domain will not power up:** • **Master IOB** • **Master IOB HubLink 1** • **Master IOB PCI Slots 1 & 2** • **Master IOR** • **Master IOB QBB FanBox (0 or 3)** **Note:** When a domain comprises more than one cell (therefore more than one IOB), the Master IOB is the one hosting the boot disk. The other IOBs in the domain are Slave IOBs.	
IOB	• Slave IOBs can be safely excluded from a domain, but connected peripherals will no longer be accessible. If the Master IOB is excluded, system disks will no longer be accessible and the domain will not power up.
IOB HubLink	• All IOB HubLinks can be safely excluded from a domain, but connected peripherals will no longer be accessible. IOB HubLinks are organized as follows: HubLink_1 controls PCI Slots 1 & 2 HubLink_2 controls PCI slots 3, 4, & 5 HubLink_3 controls PCI slots 6, 7, & 8 HubLink_4 controls PCI slots 9, 10, & 11 If Master IOB HubLink_1 is excluded, system disks will no longer be accessible and the domain will not power up.
PCI Slot	• All PCI slots can be safely excluded from a domain, but connected peripherals will no longer be accessible. If Master IOB PCI Slots 1, 2 are excluded, system disks will no longer be accessible and the domain will not power up. See *PCI Slots*, on page 4-23.
IOR	• Slave IORs can be safely excluded from a domain, but connected peripherals will no longer be accessible. If the Master IOR is excluded, the domain will not power up.
QBB	• At least one QBB must be “included” in a domain.
CPU	• At least one CPU must be “included” in a QBB. If all CPUs are excluded from a QBB, the QBB itself is excluded.
SPS	• At least one SPS must be “included” in a Midplane.
DPS Unit	• Only one DPS unit can be safely excluded at a given time. At least two DPS units are required to ensure server operation.
QBB FanBox	• If QBB FanBox_0 is excluded, QBB_0, IOB_0 and IOR_0 will be automatically excluded. If QBB FanBox_3 is excluded, QBB_3 and IOB_1 will be automatically excluded. If the excluded IOB is a Slave IOB, connected peripherals will no longer be accessible. If the excluded IOB is the Master IOB, system disks will no longer be accessible and the domain will not power up. • If QBB FanBox_1 and/or QBB FanBox_2 are excluded, QBB_1 and/or QBB_2 will be automatically excluded.
SPS FanBox	• Only one SPS FanBox can be excluded at a given time. One SPS FanBox is required to ensure server operation.

Table 28. Hardware exclusion guidelines

Managing PAM Messages, Histories, Archives and Fault Lists

What You Can Do

- *View Web event messages*
- *Acknowledge Web event messages*
- *Sort and locate Web event messages*
- *View e–mailed event messages*
- *Display the hardware faults list*
- *View history files online*
- *View archive files online*
- *View history files offline*
- *View archive files offline*
- *Manually archive history files*
- *Manually delete archive files*

A comprehensive set of Event Message subscriptions allows connected and non–connected users to be notified of system status and activity. Pre–defined **Event Message Subscriptions** forward event messages for viewing/archiving by targeted individuals and/or groups, with an appropriate subscription, via:

- the PAM Web interface (connected Customer Administrator / Operator),
- User History files (connected Customer Administrator / Operator),
- e–mail (non–connected recipients – Customer Administrator / Operator / other)
- SNMP traps (non–connected recipients – Customer Administrator / Operator / other),
- an autocall to the Bull Service Center (according to your maintenance contract).

Note:
Subscriptions can be customized to suit your working environment. For further details, see *Customizing the PAM Event Messaging System*, on page 5-114.

Understanding PAM Message Severity Levels

Messages are graded into four severity levels as shown in the following table.

Icon	Severity Level	Explanation
	**SUCCESS**	An action requested by a user has been performed correctly or a function has been completed successfully. **Information message, for guidance only.**
	**INFORMATION**	System operation is normal, but status has changed. **Information message, for guidance and verification.**
	**WARNING**	An error has been detected and overcome by the system or a processed value is outside standard limits (e.g. temperature). System operation is normal, but **you are advised to monitor the hardware concerned to avoid a more serious error**. See *What to Do if an Incident Occurs*, on page 4-39.
	**ERROR**	An error has been detected and has not been overcome by the system. System integrity is jeopardized. **Immediate action is required**. See *What to Do if an Incident Occurs*, on page 4-39.

Table 29. Message severity levels

During normal operation, messages will be marked with the **SUCCESS** or **INFORMATION** icon.

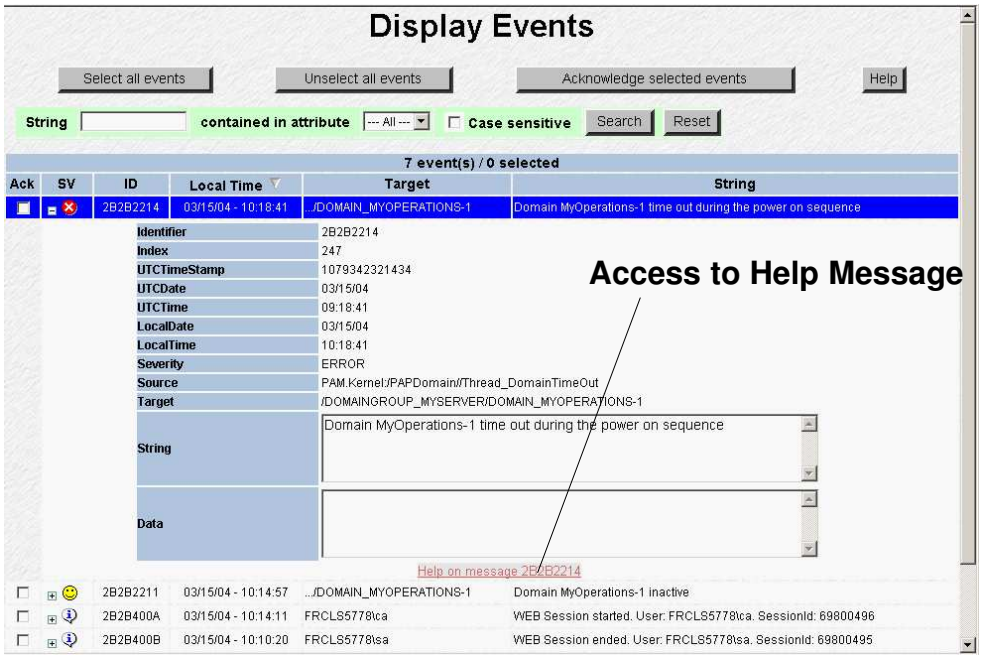
Note:
A single message may have different severity levels. For example, the message <*Unit absent*> may be the result of a:

- **Presence Status** request, indicating component status (information level).
- **Action** request, indicating an error. The command cannot be executed because the component is absent (error level).

Important:
If a message is marked with the WARNING or ERROR symbol, see *What to Do if an Incident Occurs*, on page 4-39.

Viewing PAM Messages and Fault Lists

Whether you consult a **Web Event Message**, a **Faults List**, a **System** / **User History** or **Archive**, the resulting display and utilities are the same.



Button	Use
Acknowledge selected events	To remove viewed messages from the pending event list.
Select all events	To select all **Ack** checkboxes.
Unselect all events	To deselect all **Ack** checkboxes.
Help	To access context sensitive help.
Search – **String** – **Contained in attribute** – **Case sensitive**	To search for specific messages, according to: – Alphanumeric identifier (ID), e.g. 2B2B2214 above. – Message Source, Target, String, Data attributes. – Upper case / lower case letters.
Reset	To delete the current search history.
Ack	To select the message for acknowledgement.
+	To view the message and access context sensitive help.
Help on message	To view the related help message.

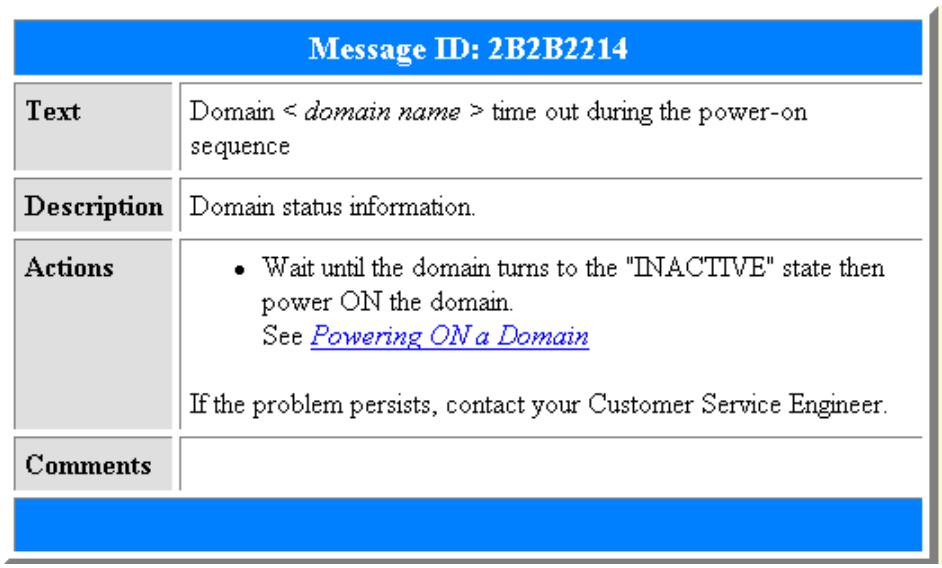
Column Header*	Use
Type	To sort messages according to severity level.
ID	To sort messages according to Message IDentifier, e.g. 2B2B2214 above.
Local Time	To sort messages according to message local time and date.
Target	To sort messages according to the component referred to in the message.
String	To sort messages according to message text string.

* Double click the column header to sort messages

Figure 118. Display Events page

Specimen Message Help File

The **Help File** explains the message and indicates related actions, where applicable, as shown in Figure 119.



Message ID: 2B2B2214	
Text	Domain < *domain name* > time out during the power-on sequence
Description	Domain status information.
Actions	• Wait until the domain turns to the "INACTIVE" state then power ON the domain. See *Powering ON a Domain* If the problem persists, contact your Customer Service Engineer.
Comments	

Figure 119. Specimen message help file

Viewing and Acknowledging PAM Web Event Messages

To consult Web event messages:

1. From the **Status** pane, click the icon to open the **Display Events** page. See Figure 118. *Display Events page*, on page 4-30.
2. Click the **+** sign to expand the required message.
3. Click the **Help on message <xxx>** button at the bottom of the message page for direct access to the corresponding **Help File**. See Table 119 *Specimen message help file*, on page 4-31.

In addition to standard utilities, the **Web Event Message** display allows users to acknowledge messages.

Important:
A maximum of 100 messages are accessible from the Status Pane. Users are advised to regularly acknowledge processed messages to allow the arrival of new messages. Acknowledged messages are stored in the PAMHistory file and can be viewed when required.
See *Viewing, Archiving, and Deleting History Files*, on page 0.

To acknowledge Web event messages:

1. Select the required checkbox(es) in the **Ack** column or click **Select all events** to automatically select all checkboxes in the **Ack** column.
2. Click **Acknowledge selected events**.
   Acknowledged messages are removed from the pending event list and are no longer accessible via the **Status** pane. The **Pending Event Message Indicator** in the **Status** pane is updated automatically.

Sorting and Locating Messages

From the message display, when you hover the mouse in the **Type** column, an **InfoTip** gives a brief summary of the message allowing you to rapidly scan the list for the required message(s). Use the standard **+** and **–** signs to expand and collapse selected messages.

It may be difficult to locate a message if the list is long, the following short–cuts can be used to organize the display and to locate required messages.

Sorting Messages

Messages can be sorted by clicking a column header to sort the column, e.g. by **Severity (SV)**, **ID**, **Time**, **Target**, **String**. Once sorted, messages will be displayed according to the selected column header.

Locating messages

The **Search** engine can be used to filter the number of displayed logs according to **Source**, **Target**, **String**, **Data** attributes. All four attributes are selected by default, but a single attribute can be selected from the dropdown menu.

To search the message list:

1. If known, enter an alphanumeric message string in the **String** field.
2. Select the required attribute field from the **contained in attribute** dropdown menu.
3. **Case sensitive** is selected by default, deselect if required.
4. Click **Search** to display search results.
5. If you want to carry out another search, click **Reset** to delete the search history.

Viewing E–mailed Event Messages

These messages contain the same information as those available to connected users, but do not contain the corresponding help file. See Figure 118. *Display Events page*, on page 4-30.

Viewing Hardware / Domain Fault Lists

The **Fault List** page allows you to view messages corresponding to the faults recently encountered by a given hardware element.

To view a **Hardware Fault List**:

1. Toggle the **PAM Tree** to display hardware functional status.
2. Click the faulty element node to open the **Hardware Status** page.
3. Click **Display Fault List** to open the **Fault List** page.
4. Click the **+** sign to expand the required message.
5. Click the **Help on message <*xxx*>** button at the bottom of the message page for direct access to the corresponding **Help File**.

To view a **Domain Fault List**, see *Viewing a Domain Fault List* , on page 3-25.

Viewing, Archiving and Deleting History Files

History and archive files are systematically stored in the **PAMSiteData** directory:

<*WinDrive*>:\Program Files\BULL\PAM\PAMSiteData\<*DataCompatibilityRelease*>

The **PAM History Manager** allows you to view, archive and delete history files online and provides you with the tools required to download and view history and archive files offline.

As Customer Administrator / Operator, you will frequently consult **PAMHistory** files for information about system operation.

Note:
System histories and/or archives are only accessible to members of the Customer Administrator group, whereas User histories and/or archives are accessible to members of both the Customer Administrator and Customer Operator groups. For further details about histories and archives, see *Creating a User History*, on page 5-125 and *Editing History Parameters*, on page 5-126.

Viewing History Files Online

Note:
Empty history files cannot be viewed.

To view a history file online:

1. From the **PAM Tree** pane, click **History Manager** to open the Control pane.
2. Select the **Histories** tab.

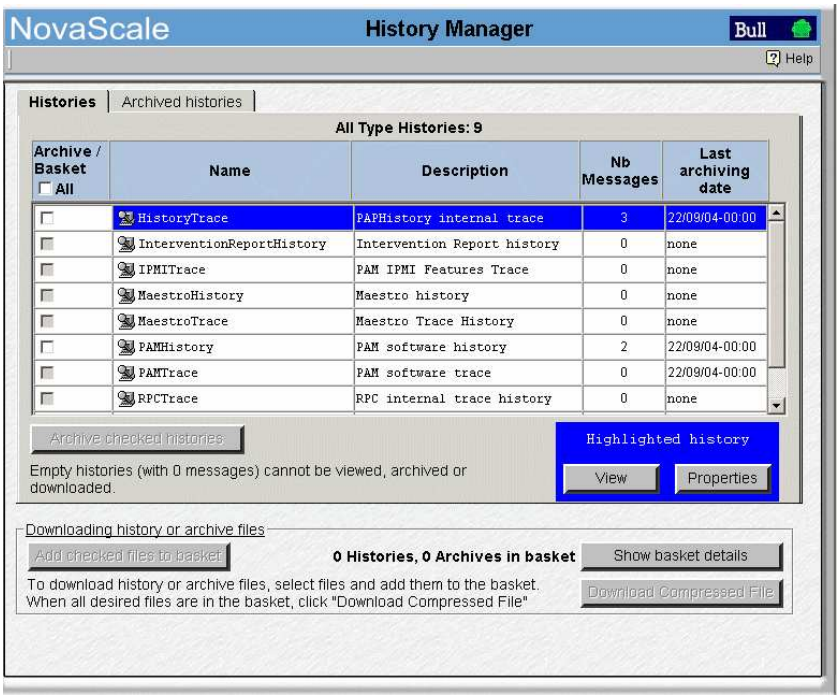


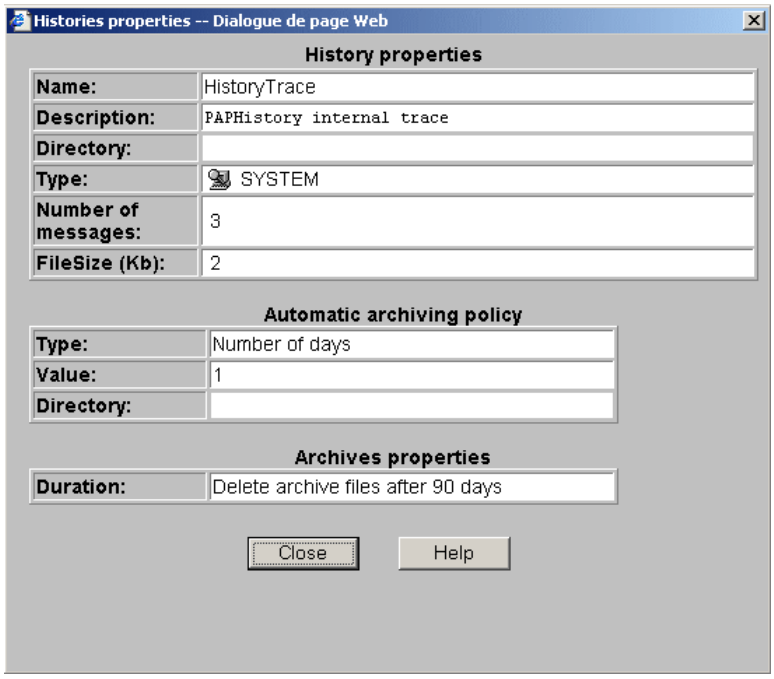
Figure 120. History Manager Control pane – Histories tab

3. Highlight the required type of history and click **View**. All the messages contained in the selected history are displayed.
4. Select the message you want to view in detail. The resulting display is the same as for event messages. See Table 118 *Display Events page*, on page 4-30.

Viewing History Properties

To view history properties:

1. From the **PAM Tree** pane, click **History Manager** to open the Control pane.
2. Select the **Histories** tab.
3. Highlight the required type of history and click **Properties**. The **History Properties** dialog opens.



Name	History name.
Description	Optional description of history contents.
Directory	Pathname of the directory used to store histories. If this field is blank, the default **Histories** directory is used.
Automatic Archiving Policy	
Type	**Number of days:** The system will automatically create an archive for this history after the number of days specified in the **Value** field. **Size in KBytes:** The system will automatically create an archive when this history reaches the size in KBytes specified in the **Value** field. **Number of Records:** The system will automatically create an archive when this history reaches the number of records specified in the **Value** field.
Value	Number of days / KBytes / records – according to archiving type.
Archive Properties	
Duration	Regular interval at which the archive is automatically deleted.

Figure 121. History properties

Note:
As Customer Administrator, you can modify History properties from the **Histories** Control pane. See *Editing History Parameters*, on page 5-126.

Manually Archiving History Files

In general, history files are automatically archived at regular periods. However, you can choose to manually archive a history file at any time, if required.

Note:
Empty history files cannot be archived.

To manually archive a history file:

1. From the **PAM Tree** pane, click **History Manager** to open the Control pane.
2. Select the **Histories** tab.
3. Select the required type of history checkbox or select the **Archive All** checkbox to archive all histories.
4. Click **Archive checked histories**. A dialog box opens, requesting you to confirm file archiving.
5. Click **OK** to confirm. The selected history(ies) are archived.

Viewing Archive Files Online

Note:
Empty archive files cannot be viewed.

To view an archive file online:

1. From the **PAM Tree** pane, click **History Manager** to open the Control pane.
1. Select the **Archived histories** tab.

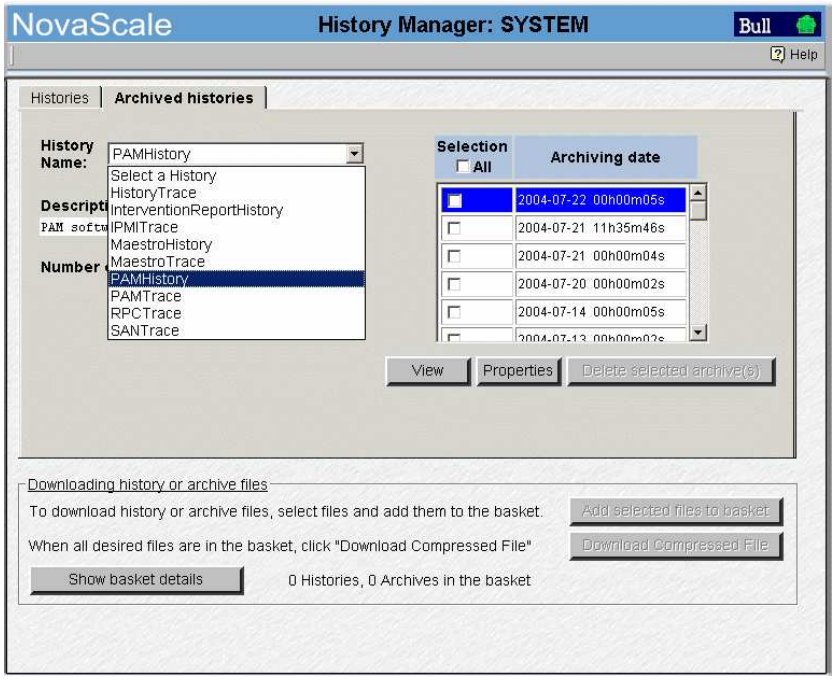


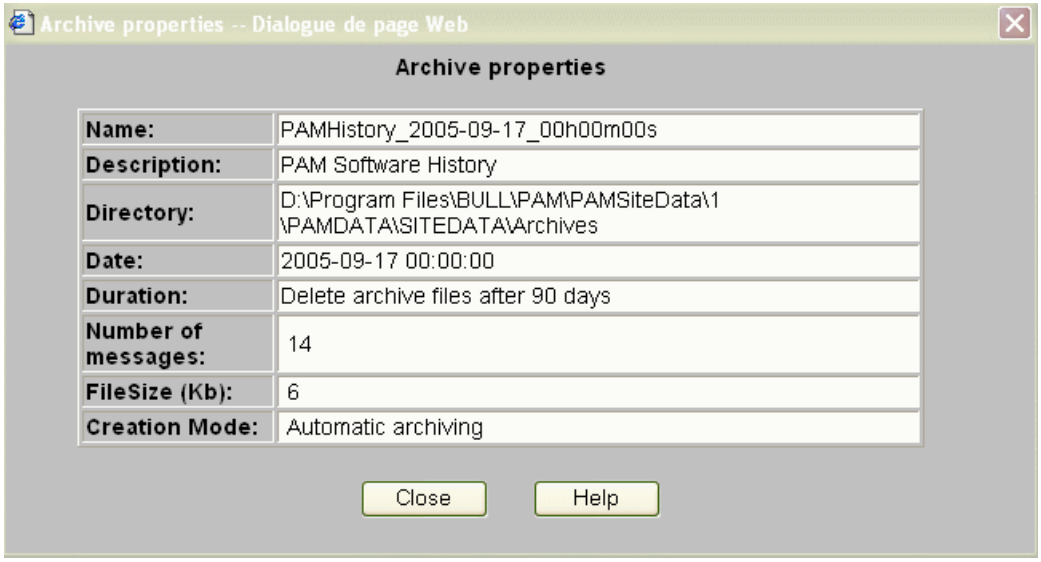
Figure 122. History Manager Control pane – Archived histories tab

2. Use the scroll–down menu to select the type of history archive you want to display. The corresponding list of archived histories appears in the **Archiving date** zone.
3. Highlight the required archiving date and click **View**. All the messages contained in the selected archive are displayed.
4. Select the message you want to view in detail. The resulting display is the same as for event messages. See Table 118 *Display Events page*, on page 4-30.

Viewing Archive Properties

To view archive properties:

1. From the **PAM Tree** pane, click **History Manager** to open the Control pane.
2. Select the **Archived histories** tab.
3. Use the scroll–down menu to select the type of history archive you want to display. The corresponding list of archived histories appears in the **Archiving date** zone.
4. Highlight the required archiving date and click **Properties**. The **Archive Properties** dialog opens.



Name	History name, archiving date and time.
Description	Optional description of history contents.
Directory	Pathname of the directory used to store histories. If this field is blank, the default **Histories** directory is used.
Date	Archiving date and time.
Duration	Regular interval at which the archive is automatically deleted.
Number of messages	Number of messages in the archive.
File Size (Kb)	Archive size in Kb.
Creation Mode	Mode used to create the archive: •Automatic archiving •Manual archiving •History error

Figure 123. Archive properties

Note:
As Customer Administrator, you can modify Archive properties from the **Histories** Control pane. See *Editing History Parameters*, on page 5-126.

Manually Deleting a History Archive File

In general, history archive files are automatically deleted at regular periods. However, you can choose to manually delete a history archive file at any time, if required.

To manually delete a history archive file:

1. From the **PAM Tree** pane, click **History Manager** to open the Control pane.
2. Select the **Archived histories** tab.
3. Use the scroll–down menu to select the type of history archive you want to delete. The corresponding list of archived histories appears in the **Archiving date** zone.
4. Select the required archive checkbox or select the **Delete All** checkbox to delete all archives.
5. Click **OK** to confirm. The selected archives are deleted.

Downloading History / Archive Files for Offline Viewing

The **PAM History Manager** allows you to compress and download history and/or archive files to a local or network directory for offline viewing. The downloaded files can then be viewed with the **History Viewer** tool which displays all the sort options available online, but does not contain the corresponding help file.

☞ **Note:**
Empty history / archive files cannot be downloaded.

Downloading History Viewer

Before downloading history and/or archive files for offline viewing, you are advised to download the **History Viewer** tool:

1. From the **PAM Tree** pane, click **Downloads** → **History Viewer** to download the **HistoryViewer.zip** file.
2. Unzip all the files in the **HistoryViewer.zip** file to a directory of your choice.
3. Select the **HistoryViewer.htm** file and create a shortcut on your desktop. The History Viewer tool is now ready for use.

Downloading History / Archive Files

To download history / archive files:

1. From the **PAM Tree** pane, click **History Manager** to open the Control pane.
2. Select the **Histories** or **Archived histories** tab, as required.
3. Select the required type of history or archive:

   Histories

   – Select the required history checkbox or select the **Basket All** checkbox to download all histories.

   Archives

   – Use the scroll–down menu to select the required archive. The corresponding list of archived histories appears in the **Archiving date** zone.

   – Select the required archive checkbox or select the **Basket All** checkbox to download all archives.
4. Click **Add selected files to basket**.

☞ **Note:**
Files already selected for downloading can be viewed by clicking **Show basket details**.

5. Click **Download Compressed File** to compress and download the histories/archives to the required local or network directory for offline viewing.

Viewing History / Archive Files Offline

1. Unzip all the files in the **History.zip** file to a directory of your choice.
2. Click the **HistoryViewer.htm** file to open the **View History File** page**.**
3. Complete the **History File Name** field and click **Read**, or click **Browse** to search for and load the required history or archive file.
4. Select the message you want to view in detail. The resulting display is the same as for event messages. See Table 118 *Display Events page*, on page 4-30.

Note:
For further details about histories and archives, see *Creating a User History*, on page 5-125 and *Editing History Parameters*, on page 5-126.

What to Do if an Incident Occurs

Server activity is systematically logged in the **System History** files, which you can view as Customer Administrator at any time.

When an incident occurs, PAM software informs users via:

- the **Status** pane,
- **Event Message** / **History** file,
- e–mail / **SNMP** traps (users with an appropriate Event Message subscription),
- an **Autocall** to the Bull Service Center (according to your maintenance contract).

In most cases, PAM software handles the incident and ensures operational continuity while the Bull Service Center analyzes the incident and implements the necessary corrective or preventive maintenance measures.

Whenever you are informed of an incident:

- functional or presence status indicators / icon **NOT green**,
- event message or history file marked with the **WARNING** or **ERROR** symbol,

you are advised to connect to the PAM Web site (if you are not already connected) and to investigate the incident.

Investigating Incidents

1. Check the system functional status icon in the **Status** pane. If the icon is not green, the server is not operating correctly. See Table 31. *System Functional Status / Expected Domain State*, on page 4-40.
2. Open the **Domain Manager** Control pane and identify the domain using the faulty hardware element by hovering the mouse over the **Domain Memo**  icons to display the Cell infotip.

NovaScale 5080/5160 Server

Cell 0	Module0_IOB0, Module0_QBB0, Module0_QBB1
Cell 1	Module0_QBB2, Module0_QBB3

NovaScale 6080/6160 Server

Cell 0	Module0_IOB0, Module0_QBB0, Module0_QBB1
Cell 1	Module0_IOB1, Module0_QBB2, Module0_QBB3

NovaScale 6320 Server

Cell 0	Module0_IOB0, Module0_QBB0, Module0_QBB1
Cell 1	Module0_IOB1, Module0_QBB2, Module0_QBB3
Cell 2	Module1_IOB0, Module1_QBB0, Module1_QBB1
Cell 3	Module1_IOB1, Module1_QBB2, Module1_QBB3

Table 30. Domain cells

– If the domain is operating normally, **RUNNING** is displayed in the **Domain State** field.

– If the domain has been automatically powered down, **INACTIVE** is displayed in the **Domain State** field. See Table 31. *System Functional Status / Expected Domain State*, on page 4-40 and Chapter 3. *Managing Domains*, on page 3-1.

Warning:
If system functional status is critical (flashing red icon), immediately save data, close open applications and shut down the domain Operating System.

System Functional Status / Expected Domain State

Icon	System Functional Status	Expected Domain State
Green	**NORMAL**	**RUNNING**
Yellow	**WARNING**	**RUNNING**
Orange Flashing	**CRITICAL**	**INACTIVE** (auto Power OFF) / **RUNNING** An automatic **Power OFF** request may be sent by PAM software to the domain Operating System: – If the domain Operating System is configured to accept PAM **Power OFF** requests, it automatically saves data, closes open applications and shuts down. – If the Operating System is not configured to accept PAM **Power OFF** requests, you are advised to manually save data, close open applications and shut down the Operating System. **Note:** When system functional status is FATAL, the icon does not always remain red. Therefore, an orange functional status icon may indicate a FATAL hardware status.
Red Flashing	**FATAL**	**INACTIVE** An automatic **Force Power OFF** command may be performed by PAM software on the domain Operating System. **Note:** The Operating System does not have time to save data and close applications before it is shut down.
Purple	**NOT ACCESSIBLE**	**INACTIVE**

Table 31. CSS functional status / domain state

3. Toggle the **PAM Tree** to view hardware functional status (round, colored indicator next to the **Hardware Monitor** node). The PAM Tree will automatically expand down to the faulty hardware element.
4. Check domain state by clicking **Domain Manager** in the PAM tree.
5. Click the faulty hardware element to open the corresponding **Hardware Status** page.
6. Check **Power** and **Temperature** tabs. If a power and/or temperature indicator is NOT green, a power– and/or temperature–specific fault has occurred. See *Power Status Indicators* and *Temperature Status Indicators*, on page 4-19.
7. Click **Display Faults List** for direct access to server logs. If the **Display Faults List** button is not accessible, click **History Manager** → **System** → **PAM History** for the corresponding log. See *Viewing Detailed Hardware Status*, on page 4-15.

8. Expand the log for direct access to the corresponding **Help File** (at the bottom of the page). The **Help File** explains the message and how to deal with the incident.

Important:
To maintain a trace of transient faults, PAM Tree functional and/or presence status indicators will not change color until the domain has been powered OFF/ON, even although the error has been corrected.

Dealing with Incidents

When you open the incident **Help File**, you may be requested to perform straightforward checks and actions or to contact your Customer Service Engineer. This section explains how to respond to the following requests:

- *Check Environmental Conditions*
- *Check Hardware Availability*
- *Check Hardware Connections*
- *Exclude a Hardware Element*
- *Check Hardware Exclusion Status*
- *Check Hardware Fault Status*
- *Check Power Status*
- *Check Temperature Status*
- *Check Histories and Events*
- *Check SNMP Settings*
- *Check Autocall Settings*
- *Check PAM Version*
- *Check MAESTRO Version*
- *Check Writing Rules*
- *Power ON/OFF the Domain*
- *Reboot the PAP Application*
- *Modify LUN Properties*
- *Check, Test, and Reset the PMB*
- *Create an Action Request Package*

Checking Environmental Conditions

If you are requested to check environmental conditions, ensure that the computer room is compliant with the specifications set out in Appendix A.*Specifications*.

Checking Hardware Availability

If you are requested to check hardware availability:

1. Check that the CSS module availability status bar is green. If the status bar is not green, the CSS module has not been detected by PAM software. Check the physical PMB to PAP unit Ethernet link connection.
2. Toggle the **PAM Tree** to view hardware presence status (square, colored indicator next to the **Hardware Monitor** node).
3. Expand the **Hardware Monitor** node to view the presence status of all hardware elements. If a hardware presence status indicator is NOT green, the hardware element is either missing or not accessible.

Important:
If a PAM Tree hardware presence status indicator is not green, this could be normal if the corresponding hardware element has been removed for maintenance.

Checking Hardware Connections

If you are requested to check hardware connections, use *Cabling Diagrams* to manually and visually ensure that all cables are correctly inserted in their corresponding hardware ports.

Excluding a Hardware Element and Checking Exclusion Status

As Customer Administrator, you can logically **Exclude** a redundant hardware element from the domain until it has been repaired or replaced. Exclusion is taken into account at the next domain power ON. See *Excluding / Including Hardware Elements*, on page 4-25.

If you are requested to check hardware exclusion status, use the **Hardware Search** engine to search for and view **Excluded** hardware elements. See *Using the Hardware Search Engine*, on page 4-9.

You can also view domain hardware exclusion status from the **Domain Hardware Details** page. See *Viewing Domain Configuration, Resources and Status*, on page 3-32.

Checking Hardware Fault Status

If you are requested to check hardware fault status:

1. Click the corresponding hardware element in the PAM Tree to open the **Hardware Status** page.
2. Check the **General** tab. If the fault status indicator is NOT green, a fault has occurred. See *Fault Status Indicators*, on page 4-16.

Checking Hardware Power Status

If you are requested to check hardware power status:

1. Click the corresponding hardware element in the PAM Tree to open the **Hardware Status** page.
2. Check the **Power** tab. If a power indicator is NOT green, a power–specific fault has occurred. See *Power Status Indicators*, on page 4-19.

Checking Hardware Temperature Status

If you are requested to check temperature status:

1. Click the corresponding hardware element in the PAM Tree to open the **Hardware Status** page.
2. Check the **Temperature** tab. If a temperature indicator is NOT green, a temperature–specific fault has occurred. See *Temperature Status Indicators*, on page 4-21.

Checking Histories and Events

If you are requested to check histories / events, refer to *Viewing and Managing PAM Event Messages and History Files*, on page 4-28.

Checking SNMP Settings

If you are requested to check SNMP settings, IP address, or server name for an event subscription:

1. From the PAM Tree, click **Configuration Tasks** → **Events** → **Channels** and check that the **SNMP Channel** is enabled.
2. Click **Subscriptions** to view configured subscriptions. Channel type is indicated in the **Channel** column.
3. Select the required **SNMP Channel** subscription from the list and click **Edit** to view / modify **SNMP** settings.

Checking Autocall Settings

If you are requested to check Autocall settings:

1. From the PAM Tree, click **Configuration Tasks** → **Autocalls** and check that the **Enable Autocalls** checkbox is selected.
2. Check dispatch modes and corresponding settings.

Checking PAM Version

If you are requested to check PAM version:

From the PAM Tree, click **PAP** to display the **PAP Unit Information** page. PAM version is displayed at the top of the page.

Checking MAESTRO Version

If you are requested to check MAESTRO version:

From the PAM Tree, click **Hardware Monitor** → **PMB** to open the **PMB Status** page. Click the **FIRMWARE** tab to view MAESTRO version.

Checking Writing Rules

If you are requested to check writing rules, see *PAM Writing Rules*, on page xxv.

Powering OFF/ON a Domain

If you are requested to Power OFF/ON or Force Power OFF a domain, ensure that you have saved data and closed open applications. See *Managing Domains*, on page 3-1.

Rebooting the PAP Application

If you are requested to reboot the PAP application:

1. From the Microsoft Windows home page, click **Start** → **Programs** → **Administrative Tools** → **Component Services**.
2. From **Component Services**, click **Console Root** → **Component Services** → **Computers** → **My Computer** → **COM+ Applications** → **PAP**.
3. Right click **PAP** to open the shortcut menu. Click **Shutdown**.
4. Activate the required PAM version to reboot the PAP application. See *Deploying a New PAM* Release, on page 5-23 and *Activating a PAM Version*, on page 5-24.

Modifying LUN Properties

If you are requested to modify LUN properties:

- Refer to *Configuring SCSI Data Disks*, on page 5-4 and to the appropriate Disk Subsystem documentation.
- Refer to *Configuring FDA Data Disks*, on page 0 and to the appropriate Disk Subsystem documentation.

Checking, Testing and Resetting the PMB

The PMB is located in the module at the base of the cabinet and links the server to the PAP unit via an Ethernet link. You may be required to carry out the following checks / actions:

- Check that PMB LED #0 is blinking green (PMB booted correctly):
  When the system is powered on, the 7 activity and status LEDs (LED #1–LED #7) are switched off and LED #0 is blinking. See *PMB Leds and Code Wheel*s, on page 4-46.
- Check PMB code wheel settings. See *PMB Leds and Code Wheel*s, on page 4-46.
- Check that the Ethernet cable linking the server to the PAP unit is correctly inserted and that the Ethernet link LED is green.
- Check the PAP – PMB link by pinging the PAP and the PMB:

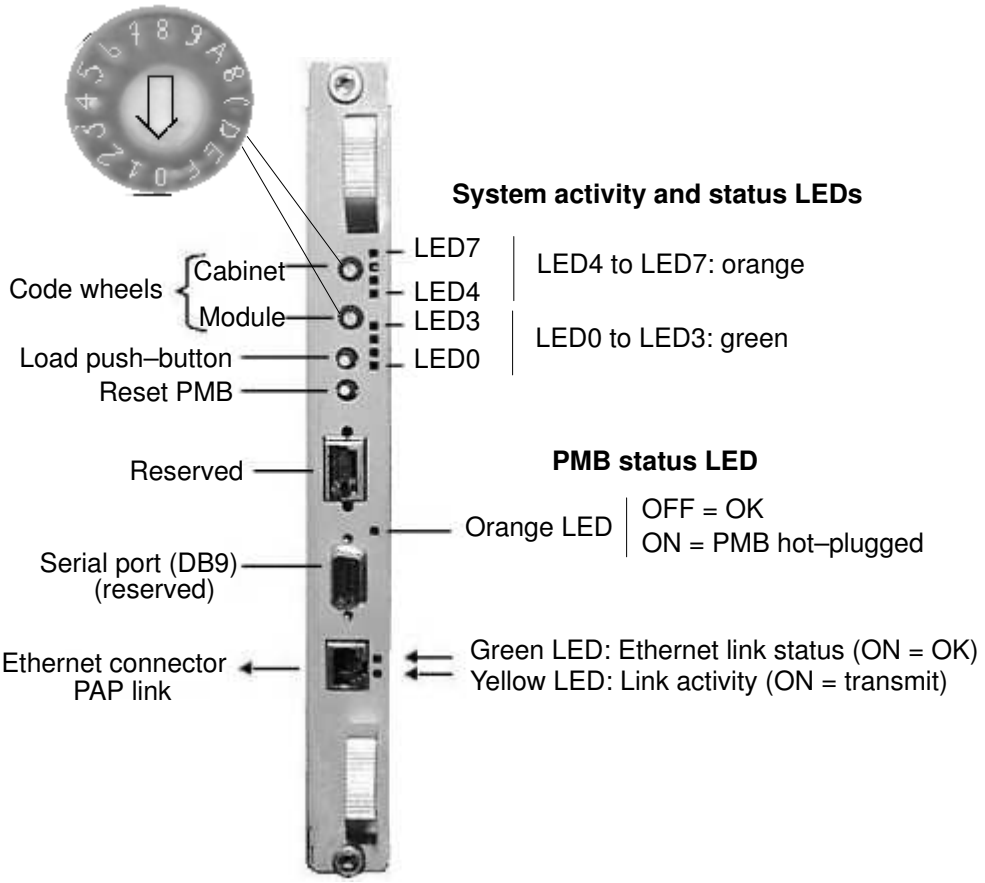
PAP Address	PMB 0 Address	PMB 1 Address
10.10.240.240	10.10.0.1	10.10.0.2

- Reset the PMB by pressing the RESET button. PMB firmware will be rebooted. See *PMB Leds and Code Wheel*s, on page 4-46.

PMB LEDs and Code Wheels

Up to 16 Central Subsystems can be linked, via Platform Management Boards (PMBs) to a single PAP unit, to provide a single point of administration and maintenance.

Each PMB is equipped with two code wheels used to identify each Central Subsystem and each CSS module in your configuration. These code wheels are set prior to shipping (factory default setting), according to configuration.



For guidance, PMB code wheel settings are indicated in the following table:

CSS	CSS PMB Code Wheel	PAM CSS HW Identifier	CSS Module PMB Code Wheel	
			CSS Module 0	CSS Module 1
1st	0	00	0	1
2nd	1	01	0	1
3rd	2	02	0	1
4th	3	03	0	1
5th	4	04	0	1
6th	5	05	0	1
7th	6	06	0	1
8th	7	07	0	1
9th	8	08	0	1
10th	9	09	0	1
11th	A	10	0	1
12th	B	11	0	1
13th	C	12	0	1
14th	D	13	0	1
15th	E	14	0	1
16th	F	15	0	1

Figure 124. PMB LED location

Creating an Action Request Package

PAM software allows you to collect all the files required to troubleshoot a Bull NovaScale Server via the **Action Request Package** tool. Once collected, files are compressed to ZIP format for easy transfer to the BULL Remote Maintenance Center.

Note:
Before PAM Release 8, the **BackUpRestore** tool is used to copy and restore the files stored in the **PAM SiteData** directory.

Creating a Default Action Request Package

1. From the **PAM Tree** pane, click **Downloads**. The **Action Request Package** page opens.

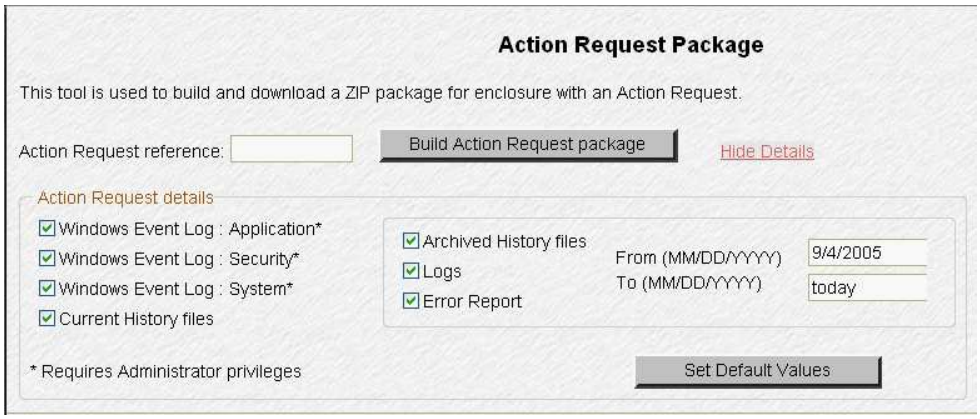
Figure 125. Action Request Package control pane

2. Enter the **Action Request reference** given by the Customer Support Center and click **Build Action Request package** to collect, compress and download ALL the files contained in the various directories.
3. Transfer the ZIP to the BULL Remote Maintenance Center for analysis.

Creating a Filtered Action Request Package

Important:
To ensure the consistency of Action Request Package contents, you are advised to only use filtering options if specifically required.

1. From the **PAM Tree** pane, click **Downloads**. The **Action Request Package** page opens.
2. Enter the **Action Request reference** given by the Customer Support Center and click **Show Details** to display filtering options.



Filterable File Types	Action	Dates
Current Files		
Windows Event Log: Application	These files are selected by default. If you do not want to include these files, deselect the corresponding checkboxes.	All current Windows Event Log files.
Windows Event Log: Security		
Windows Event Log: System		
Current History Files		All history files in the PAM Site Directory.
Archived Files		
Archived History Files	These files are selected by default. If you do not want to include these files, deselect the corresponding checkboxes.	Default dates: Today + 3 preceding days. Enter new **From** / **To** dates to include archives outside the default dates.
Logs		
Error Reports		

Figure 126. Action Request Package details

3. Clear filterable checkboxes as required and/or change archive collection dates.
4. Click **Build Action Request package** to collect, compress and download ALL the files contained in the various directories.
5. Transfer the ZIP file to the BULL Remote Maintenance Center for analysis.

Creating a Custom Package

PAM software allows you to collect one or more selected files from the PAM Site Data Directory via the **Custom Package** tool. Once collected, files are compressed to ZIP format.

To create a Custom Package:

1. From the **PAM Tree** pane, click **Downloads**. The **Custom Package** page opens.

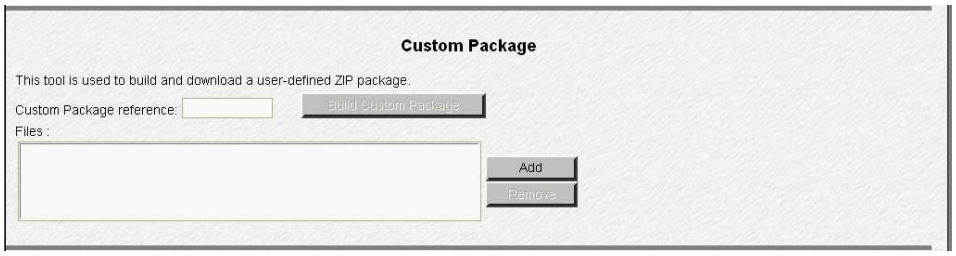


Figure 127. Custom Package control pane

2. Enter the **Custom Package reference** and click **Add** to select the PAM Site Data files to be included in the package.

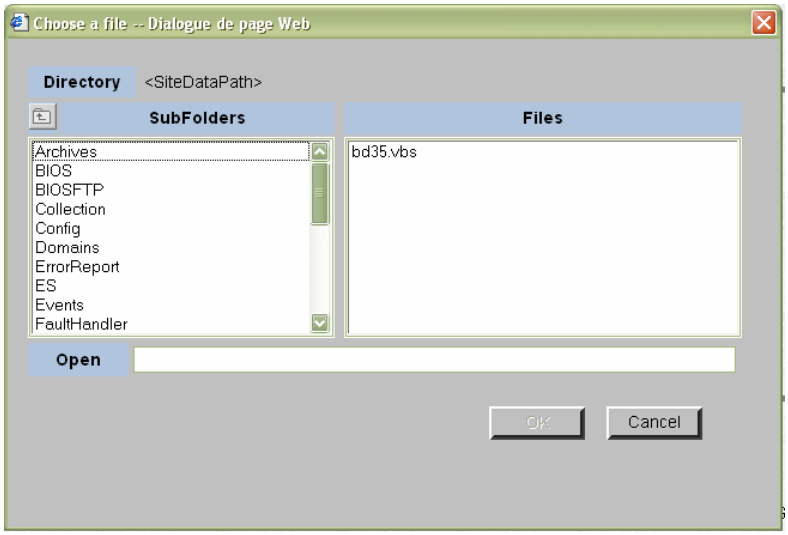


Figure 128. Custom Package Add files pane

3. Click **Build Custom Package** to collect, compress and download the selected files.
4. Save the resulting ZIP file as required.

Chapter 5. Tips and Features for Administrators

This chapter explains how, as Customer Administrator, you can configure the server to suit your working environment. It includes the following sections:

- Section I – Setting up Server Users and Configuring Disks, on page 5-2
- Section II – Using EFI Utilities, on page 5-7
- Section III – Customizing PAM Software, on page 5-16
- Section IV – Configuring Domains, see page 5-28
- Section V – Creating Event Subscriptions and User Histories, on page 5-113

Notes:
Customer Administrators and Customer Operators are respectively advised to consult the *Administrator's Memorandum*, on page xxviii or the *Operator's Memorandum*, on page xxx for a detailed summary of the everyday tasks they will perform.
Before proceeding to configure the server, please refer to *PAM Writing Rules*, on page xxv.

For further information about user accounts and passwords, see *Setting up PAP Unit User*s, on page 5-17.

Important:
Certain domain configuration and management tools are reserved for use with partitioned servers, extended systems and/or a Storage Area Network(SAN). Please contact your Bull Sales Representative for sales information.

Section I – Setting up Users and Configuring Data Disks

This section explains how to:

- Set up Server Users, on page 5-3
- Configure System and Data Disks, on page 5-4

Setting up Server Users

As Customer Administrator, you must set up user accounts and passwords to control access to the server.

The operating system pre–installed on the server provides standard security features for controlling access to applications and resources.

For further details, refer to the Microsoft Windows / Linux documentation, as applicable.

Note:
You are advised to maintain a detailed record of authorized users.

Microsoft Windows

Default user access control is not pre–configured on systems running under Microsoft Windows.
You are advised to set up the Administrator account before proceeding to set up users and groups via the standard Microsoft Windows administration tools.

Linux

Two default users are pre–configured on systems running under Linux:

	User Name	**Password**
Administrator	root	root
User	linux	root

You are advised to change the default Administrator name and password before proceeding to set up users and groups via the standard Linux administration tools.

Configuring System and Data Disks

For optimum storage, security and performance, the server is delivered with one or two pre–configured disk racks.

New system and/or data disks can be created via the utility delivered with the storage sub–system.

Delivered storage sub–systems vary according to Customer requirements. See:

- *Creating a New SCSI Disk Array and Array Partition*, on page 5-4
- *Creating New FC Logical System or Data Disk* , on page 5-6

Creating a New SCSI Disk Array and Array Partition

The addition of data disks involves the creation of a new array and new array partitions (LUNs) via the embedded **Disk Array Administrator** software.

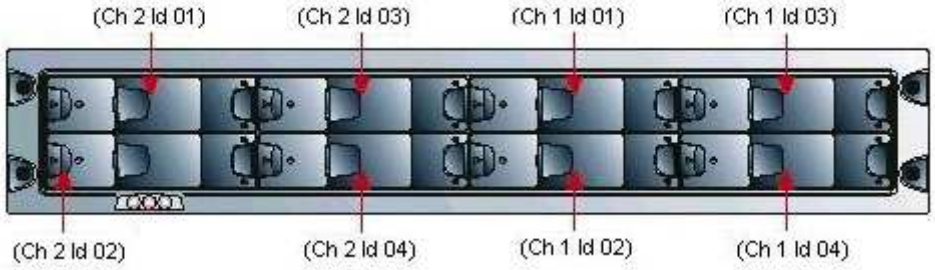
Note:
For further details about configuring system and data disks, refer to the appropriate Disk Subsystem documentation.

SCSI Disk Location

For guidance, local SCSI disks are located as shown in the following figures:

SJ–0812 SCSI JBOD / SR–0812 SCSI RAID Disk Racks

Optionally, the server may be delivered with one or two disk racks (one per domain). Each disk rack contains two RAID #1 system disks and one pool spare disk, and offers free slots for data disks.



	OS Disks (RAID #1)	Spare Disks (Pool)
SJ–0812 SCSI JBOD disk rack 1 Cell 0 (CSS Module_0, IOB_0)	Ch 2 Id 01 Ch 2 Id 02	Ch 2 Id 04
SJ–0812 SCSI JBOD disk rack 1 Cell 1 (CSS Module_0, IOB_1)	Ch 1 Id 01 Ch 1 Id 02	Ch 1 Id 04
SJ–0812 SCSI JBOD disk rack 2 Cell 2 (CSS Module_1, IOB_0)	Ch 2 Id 01 Ch 2 Id 02	Ch 2 Id 04
SJ–0812 SCSI JBOD disk rack 2 Cell 3 (CSS Module_1, IOB_1)	Ch 1 Id 01 Ch 1 Id 02	Ch 1 Id 04

Figure 129. SJ–0812 SCSI JBOD / SR–0812 SCSI RAID disk configuration

Creating a New SCSI Disk Array

1. From the Microsoft Windows desktop on the PAP unit, launch a HyperTerminal session with the following parameters:

Parameter	Value
Name	Disk Rack
Connect using	COM1 or COM2
Bits per second	115200
Data bits	8
Parity	None
Stop bits	1
Flow control	None
Emulation	ANSI

Table 32. HyperTerminal parameters

2. Press **CTRL–R** to refresh the screen and display the initial Disk Array Administrator screen.
3. Press **Enter** to display the System Menu.
4. Select **Add an Array**.
5. Enter the name of the Array: e.g. **Data**.
6. Enter the RAID level, number of disks and disk ID.
7. When prompted to **Create one partition now for entire Array?**, select **NO** to create a Multiple–Partition Array.
8. Select **Array parameters**.
9. Select the required number of free drives:

	Free Slots (population order)
SJ–0812 SCSI JBOD disk rack	N/A
SR–0812 SCSI RAID disk rack	Ch 2 Id 03 Ch 2 Id 04 Ch 1 Id 01 Ch 1 Id 02 Ch 1 Id 03

Table 33. SCSI data disk population order

10. Select **Array Init options**: **Offline Initialization**.
11. When prompted to confirm, enter **YES**.

Creating a New SCSI Array Partition

1. Select **Array Menu**.
2. Select **Data Array** and press **Enter**.
3. Select **Add a Partition**.
4. Enter the size of the disk partition, e.g. **10,000 MB**.
5. Enter the name of the disk partition: e.g. **USER1**.
6. Enter a LUN number or select the suggested LUN number (from 0 to 63).
7. Repeat this procedure for each new disk partition.

The new Array and associated disk partitions are now configured for use.

Creating New FC Logical System or Data Disks

FDA 1x00 FC / FDA 2x00 FCDisk Rack

Optionally, the server may be delivered with one or two disk rack(s) each containing two RAID #1 system disks per domain and one pool spare disk, and offering ten free slots for data disks. Slots are numbered from 0 to14 (from left to right).

	OS Disks (RAID #1)	Spare Disk
NovaScale 5xx0 Server		
FDA 1x00 FC disk rack or **FDA 2x00 FC disk rack**	PD0 PD1	PD14
NovaScale 6080/6160 Server		
FDA 1x00 FC disk rack 1 controller #0 **Cell_0, IOB_0** **FDA 1x00 FC disk rack 1 controller #1** **Cell_1, IOB_1**	PD0 PD1 PD2 PD3	PD14
NovaScale 6320 Server		
FDA 1x00 FC disk rack 1 controller #0 **Cell_0, CSS Module_0, IOB_0** **FDA 1x00 FC disk rack 1 controller #1** **Cell_1, CSS Module_0, IOB_1** **FDA 1x00 FC disk rack 2 controller #0** **Cell_2, CSS Module_1, IOB_0** **FDA 1x00 FC disk rack 2 controller #1** **Cell_3, CSS Module_1, IOB_1**	PD0 PD1 PD2 PD3 PD0 PD1 PD2 PD3	PD14 PD14
FDA 2x00 FC disk rack 1 controller #0 **Cell_0, CSS Module_0, IOB_0** **Cell_1, CSS Module_0, IOB_1** **FDA 2x00 FC disk rack 1 controller #1** **Cell_2, CSS Module_1, IOB_0** **Cell_3, CSS Module_1, IOB_1**	PD0 PD1 PD2 PD3	PD14

Table 34. FDA 1x00 FC / FDA 2x00 FC disk configuration

Note:
For optimum storage, performance, and reliability, you are advised to use RAID level 1 for system disk configuration and RAID level 5 for data disk configuration.

To create a new logical system or data disk:

1. From the Microsoft Windows desktop on the PAP unit, launch iSM Client.
2. Follow the instructions on the screen.

Note:
For further details about configuring system and data disks, refer to the appropriate Disk Subsystem documentation.

Section II – Using EFI Utilities

This section explains how to:

Using the EFI Boot Manager

The EFI (Extensible Firmware Interface) Boot Manager allows you to control the server's booting environment. From the Boot Manager, you can choose to invoke the Extensible Firmware Interface (EFI) Shell or to go to the Boot Option Maintenance Menu.

Warning:
The EFI shell can only manage QWERTY keyboards. If you have an AZERTY keyboard, please refer to the AZERTY/QWERTY keyboard lookup table on page xxvii.

To enter the EFI Boot Manager:

1. From the PAM Tree, click **Domain Manager** → **Power ON** to power up the required domain.
2. From the keyboard, press the **Control** key twice to display the KVM Switch Command Menu.
3. Select the required system channel port with the ↑↓ keys, according to configuration. See *KVM port configuration*, in the User's Guide.
4. Press **Enter** to activate the required system channel and exit the Command Mode.

Note:
The system automatically boots on the first option in the list without user intervention after a timeout. To modify the timeout, use **Set Auto Boot Timeout** in the Boot Option Maintenance Menu.

5. From the Boot Manager Menu, select the EFI Shell option with the ↑↓ keys and press **Enter**.

EFI Boot Manager Options

EFI Shell

A simple, interactive environment that allows EFI device drivers to be loaded, EFI applications to be launched, and operating systems to be booted. The EFI shell also provides a set of basic commands used to manage files and the system environment variables. For more information on the EFI Shell, refer to Using the EFI Shell on page 5-10.

Boot Options

Files that you include as boot options. You add and delete boot options by using the Boot Maintenance Menu. Each boot option specifies an EFI executable with possible options. For information on the Boot Maintenance Menu options, refer to Table 35.

Boot Option Maintenance Menu

The EFI Boot Maintenance Manager allows the user to add boot options, delete boot options, launch an EFI application, and set the auto boot time out value.

If there are no boot options in the system (and no integrated shell), the Boot Maintenance Menu is presented. If boot options are available, then the set of available boot options is displayed, and the user can select one or choose to go to the Boot Maintenance Menu.

If the time out period is not zero, then the system will auto boot the first boot selection after the time out has expired. If the time out period is zero, then the EFI Boot Manager will wait for the user to select an option. Table 35 describes each menu item in the Boot Maintenance Menu.

Note:
You can use the → ← ↑↓ keys to scroll through the Boot Maintenance Menu.

Boot Option	Description
Boot from a File	This option searches all the EFI System Partitions in the system. For each partition it looks for an EFI directory. If the EFI directory is found, it looks in each of the subdirectories below EFI. In each of those subdirectories, it looks for the first file that is an executable EFI Application. Each of the EFI Applications that meet this criteria are automatically added as a possible boot option. In addition, legacy boot options for A: and C: are also added if those devices are present. This option allows the user to launch an application without adding it as a boot option. The EFI Boot Manager will search the root directories and the \EFI\TOOLS directories of all of the EFI System Partitions present in the system for the specified EFI Application.
Add a Boot Option	Allows the user to specify the name of the EFI Application to add as a boot option. The EFI Boot Manager searches the same partitions and directories as described in *Boot from a File*, until it finds an EFI Application with the specified name. This menu also allows the user to provide either ASCII or UNICODE arguments to the option that will be launched.
Delete Boot Options	Allows you to delete a specific boot option or all boot options. Highlight the option you want to delete and enter <d>. Enter <y> to confirm.
Change Boot Order	Allows you to control the relative order in which the EFI Boot Manager attempts boot options. To change the boot order, highlight the boot option and enter <u> to move the item up one order, <d> to move the item down one order. For help on the control key sequences you need for this option, refer to the help menu.
Manage Boot Next Setting	Allows you to select a boot option to use one time (the next boot operation).
Set Auto Boot Timeout	Allows you to define the value in seconds that pass before the system automatically boots without user intervention. Setting this value to zero disables the timeout feature.
Cold Reset	Performs a platform–specific cold reset of the system. A cold reset traditionally means a full platform reset.
Exit	Returns control to the EFI Boot Manager main menu. Selecting this option will display the active boot devices, including a possible integrated shell (if the implementation is so constructed).

Table 35. Boot Option Maintenance Menu

Using the EFI Shell

The EFI (Extensible Firmware Interface) Shell is a simple, interactive user interface that allows EFI device drivers to be loaded, EFI applications to be launched, and operating systems to be booted. In addition, the Shell provides a set of basic commands used to manage files and the system environment variables.

The EFI Shell supports command line interface and batch scripting.

Warning:
The EFI shell can only manage QWERTY keyboards. If you have an AZERTY keyboard, please refer to the AZERTY/QWERTY keyboard lookup table on page xxvii.

Entering the EFI Shell

To enter the EFI Shell:

1. From the PAM Tree, click **Domain Manager** → **Power ON** to power up the required domain.
2. From the keyboard, press the **Control** key twice to display the KVM Switch Command Menu.
3. Select the required system channel port with the ↑↓ keys, according to configuration. See *KVM port configuration*, in the User's Guide.
4. Press **Enter** to activate the required system channel and exit the Command Mode. After a few seconds, the Boot Manager menu is displayed.
5. From the Boot Manager Menu, select the EFI Shell option with the ↑↓ keys and press **Enter**.

When the EFI Shell is invoked, it first looks for commands in the file ***startup.nsh*** on the execution path defined by the environment. There is no requirement for a startup file to exist. Once the startup file commands are completed, the Shell looks for commands from console input device.

Note:
The system automatically boots on the first option in the list without user intervention after a timeout. To modify timeout, use **Set Auto Boot Timeout** in the Boot Option Maintenance Menu.

EFI Shell Command Syntax

The EFI Shell implements a programming language that provides control over the execution of individual commands. When the Shell scans its input, it always treats certain characters specially: (**`#`**, **`>`**, **`%`**, **`*`**, **`?`**, **`[`**, **`^`**, **`space`**, and **`newline`**).

When a command contains a defined alias, the Shell replaces the alias with its definition (see **`alias`** command in this chapter). If the argument is prefixed with the **`^`** character, however, the argument is treated as a literal argument and alias processing is not performed.

Note:
In interactive execution, the Shell performs variable substitution, then expands wildcards before the command is executed.
In batch script execution, the Shell performs argument substitution, then variable substitution, then expands wildcards before the command is executed.

Variable Substitution

Environment variables can be set and viewed through the use of the **set** command (see **set** command in this chapter). To access the value of an environment variable as an argument to a Shell command, delimit the name of the variable with the **%** character before and after the variable name; for example, ***%myvariable%***.

The Shell maintains a special variable, named ***lasterror***. The variable contains the return code of the most recently executed Shell command.

Wildcard Expansion

The ***, ?** and **[** characters can be used as wildcard characters in filename arguments to Shell commands.

If an argument contains one or more of these characters, the Shell processes the argument for ***file meta–arguments*** and expands the argument list to include all filenames matching the pattern.

These characters are part of patterns which represent file and directory names.

Character Sequence	Meaning
"*****"	Matches zero or more characters in a file name
"**?**"	Matches exactly one character of a file name
"**[***chars***]**"	Defines a set of characters; the pattern matches any single character in the set. Characters in the set are not separated. Ranges of characters can be specified by specifying the first character in a range, then the **–** character, then the last character in the range. Example: [a–zA–Z]

Table 36. Wildcard character expansion

Output Redirection

Output of EFI Shell commands can be redirected to files, according to the following syntax:

Command	Output Redirection
> unicode_output_file_pathname	standard output to a unicode file
>a ascii_output_file_pathname	standard output to an ascii file
1> unicode_output_file_pathname	standard output to a unicode file
1>a ascii_output_file_pathname	standard output to an ascii file
2> unicode_output_file_pathname	standard error to a unicode file
2>a ascii_output_file_pathname	standard error to an ascii file
>> unicode_output_file_pathname	standard output appended to a unicode file
>>a ascii_output_file_pathname	standard output appended to an ascii file
1>> unicode_output_file_pathname	standard output appended to a unicode file
1>>a ascii_output_file_pathname	standard output appended to an ascii file

Table 37. Output redirection syntax

The Shell will redirect standard output to a single file and standard error to a single file. Redirecting both standard output and standard error to the same file is allowed. Redirecting Standard output to more than one file on the same command is not supported. Similarly, redirecting to multiple files is not supported for standard error.

Quoting

Quotation marks in the EFI Shell are used for argument grouping. A quoted string is treated as a single argument to a command, and any whitespace characters included in the quoted string are just part of that single argument.

Quoting an environment variable does not have any effect on the de–referencing of that variable. Double quotation marks `"` are used to denote strings. Single quotation marks are not treated specially by the Shell in any way. Empty strings are treated as valid command line arguments.

Executing Batch Scripts

The EFI Shell has the capability of executing commands from a file (batch script). EFI Shell batch script files are named using the *.nsh* extension. Batch script files can be either UNICODE or ASCII format files. EFI Shell script files are invoked by entering the filename at the command prompt, with or without the filename extension.

Up to nine (9) positional arguments are supported for batch scripts. Positional argument substitution is performed before the execution of each line in the script file. Positional arguments are denoted by **`%n`**, where n is a digit between 0 and 9. By convention, **`%0`** is the name of the script file currently being executed. In batch scripts, argument substitution is performed first, then variable substitution. Thus, for a variable containing **`%2`**, the variable will be replaced with the literal string **`%2`**, not the second argument on the command line. If no real argument is found to substitute for a positional argument, then the positional argument is ignored. Script file execution can be nested; that is, script files may be executed from within other script files. Recursion is allowed.

Output redirection is fully supported. Output redirection on a command in a script file causes the output for that command to be redirected. Output redirection on the invocation of a batch script causes the output for all commands executed from that batch script to be redirected to the file, with the output of each command appended to the end of the file.

By default, both the input and output for all commands executed from a batch script are echoed to the console. Display of commands read from a batch file can be suppressed via the **`echo -off`** command (see **`echo`**). If output for a command is redirected to a file, then that output is not displayed on the console. Note that commands executed from a batch script are not saved by the Shell for DOSkey history (up–arrow command recall).

Error Handling in Batch Scripts

By default, if an error is encountered during the execution of a command in a batch script, the script will continue to execute.

The ***`lasterror`*** Shell variable allows batch scripts to test the results of the most recently executed command using the **`if`** command. This variable is not an environment variable, but is a special variable maintained by the Shell for the lifetime of that instance of the Shell.

Comments in Script Files

Comments can be embedded in batch scripts. The **#** character on a line is used to denote that all characters on the same line and to the right of the **#** are to be ignored by the Shell. Comments are not echoed to the console.

EFI Shell Commands

Most Shell commands can be invoked from the EFI Shell prompt. However there are several commands that are only available for use from within batch script files.

☞ **Note:**
The “Batch–only” column indicates if the command is only available from within script files. The following sections provide more details on each of the individual commands. Command ***help command_name*** displays the details of the ***command_name*** .

Command	Batch only	Description
alias	No	Displays, creates, or deletes aliases in the EFI Shell
attrib	No	Displays or changes the attributes of files or directories
bcfg	No	Displays/modifies the driver/boot configuration
break	No	Executes a break point
cd	No	Displays or changes the current directory
cls	No	Clears the standard output with an optional background color
comp	No	Compares the contents of two files
connect	No	Binds an EFI driver to a device and starts the driver
cp	No	Copies one or more files/directories to another location
date	No	Displays the current date or sets the date in the system
dblk	No	Displays the contents of blocks from a block device
devices	No	Displays the list of devices being managed by EFI drivers
devtree	No	Displays the tree of devices that follow the EFI Driver Model
dh	No	Displays the handles in the EFI environment
disconnect	No	Disconnects one or more drivers from a device
dmem	No	Displays the contents of memory
dmpstore	No	Displays all NVRAM variables
drivers	No	Displays the list of drivers that follow the EFI Driver Model
drvcfg	No	Invokes the Driver Configuration Protocol
drvdiag	No	Invokes the Driver Diagnostics Protocol
echo	No	Displays messages or turns command echoing on or off
edit	No	Edits an ASCII or UNICODE file in full screen.
err	No	Displays or changes the error level
exit	No	Exits the EFI Shell
for/endfor	Yes	Executes commands for each item in a set of items
goto	Yes	Makes batch file execution jump to another location
guid	No	Displays all the GUIDs in the EFI environment
help	No	Displays commands list or verbose help of a command
hexedit	No	Edits with hex mode in full screen
if/endif	Yes	Executes commands in specified conditions
load	No	Loads EFI drivers
loadbmp	No	Displays a Bitmap file onto the screen
ls	No	Displays a list of files and subdirectories in a directory
map	No	Displays or defines mappings
memmap	No	Displays the memory map
mkdir	No	Creates one or more directories
mm	No	Displays or modifies MEM/IO/PCI
mode	No	Displays or changes the mode of the console output device
mount	No	Mounts a file system on a block device
mv	No	Moves one or more files/directories to destination
openInfo	No	Displays the protocols on a handle and the agents
pause	No	Prints a message and suspends for keyboard input
pci	No	Displays PCI devices or PCI function configuration space
reconnect	No	Reconnects one or more drivers from a device
reset	No	Resets the system
rm	No	Deletes one or more files or directories
set	No	Displays, creates, changes or deletes EFI environment variables
stall	No	Stalls the processor for some microseconds
time	No	Displays the current time or sets the time of the system
type	No	Displays the contents of a file
unload	No	Unloads a protocol image
ver	No	Displays the version information
vol	No	Displays volume information of the file system

Table 38. List of EFI Shell Commands

EFI Network Setup and Configuration

The EFI (Extensible Firmware Interface) Utilities delivered with the system provide a complete set of TCP/IPv4 network stack and configuration tools. Ethernet adapters utilizing 6 bit UNDI option ROMs are supported.

Important:
To access this feature, please connect the Enterprise network to the embedded Ethernet board on the IOR of the domain master IO board. Intel PRO 1000T and 1000F adapters are not supported.

Note:
These utilities are installed in the EFI partition of the system disk in the EFI\Tools directory. The list and respective manual pages for each utility can be found on the Bull NovaScale Server Resource CD–Rom.

Network stack configuration commands must be executed after booting to EFI Shell. To simplify network setup, these commands should be grouped, via an EFI batch script, to form a single one–line command.

Manual EFI Network Configuration

1. Load the TCP/IP protocol via the EFI **load** command.

Note:
As the **load** command does not use the search path to locate protocols, specify the path and the **.efi** extension.

```
fso:\efi\tools\tcpipv4.efi
```

2. Configure the network interfaces with the **ifconfig** command:

   The simple form of the command is:

   ```
   ifconfig <interface> inet <ip address> up
   ```

   where <*ip address*> is the address assigned to the system. If the system is connected to a network that uses subnetting, a subnet mask would also need to be specified as follows:

   ```
   ifconfig sni0 inet <ip address> netmask <netmask> up
   ```

   where <*netmask*> is the network mask assigned to the network.

Note:
The TCP/IP stack contains a *"lo0"* loopback interface which can be optionally be configured with the *"sni0"* Ethernet interface if a compatible UNDI Ethernet adapter is installed. Configuration is performed with the **ifconfig** command.

3. If multiple network or subnetwork networking is required, set a gateway address for the appropriate gateway(s) attached to the network, via the **route** command as follows:

   ```
   route add <destination> <gateway ip address>
   ```

   where <*destination*> specifies the target network or host and <*gateway ip address*> specifies the network gateway address responsible for routing data to the destination.

   If **default** is used for <*destination*>, a default route will be set.

Example Network Configuration Batch File

An example network configuration batch file named **NetConf.nsh** is installed in the EFI directory of the EFI Service Partition.

This file loads the TCP/IP, configures the Ethernet interface to the IP address given as first argument to this file, configures the optional second argument as the gateway, and loads the FTP Server (daemon).

```
echo -off
if %1empty == empty then
 echo usage netconf {local ip-addr} [router ip addr]
 goto End
endif
load fs0:\efi\tools\tcpipv4.efi
ifconfig sni0 %1 netmask 255.255.255.0
if not %2empty == empty then
  route add default %2
endif
load fs0:\EFI\Tools\ftpd.efi
:End
```

Note:

The IP addresses and netmask indicated in this file and in the following example are only examples and must be modified to reflect site network configuration:

```
fs0:\> Netconf 129.182.189.3 129.182.189.1
```

`129.182.189.3` is the <*ip address*>

`129.182.189.1` is the <*gateway ip address*>

File Transfer Protocol (FTP)

An FTP Client and an FTP Server are provided with the EFI Utilities.

1. Configure the network. See *Manual Network Configuration*.
2. Load the FTP Server via the EFI **load** command.
3. Load the FTP Client via the EFI **ftp** command. This Client supports most ftp directives (open, get, put, ...). Use the **help** directive if you need help.

Note:

As the **load** command does not use the search path to locate protocols, specify the path if it is not in the current working directory and the **.efi** extension.

```
load fs0:\efi\tools\ftpd.efi
```

The FTP Server is now available for use and accepts anonymous connections (one at a time).

Important:

Once the EFI drivers for the TCP/IP, the FTP Server or FTP Client are loaded, you cannot load an Operating System.
To load an Operating System, reset the domain and return to Boot Manager.

Section III – Customizing PAM Software

This section explains how to:

Setting up PAP Unit Users

As Customer Administrator, you must set up user accounts and passwords to control access to the PAP unit.

The Microsoft Windows operating system pre–installed on the PAP unit provides standard security features for controlling access to applications and resources. PAM software security is based on Windows user management and you are advised to give Windows administrator rights to at least one member of the PAP Customer Administrator user group. For further details about user management, refer to the Microsoft Windows documentation on the Bull NovaScale Server System Resource CD.

Note:
You are advised to change the temporary Administrator password (**administrator**) used for setup purposes and to maintain a detailed record of authorized users.

Predefined PAP User Groups

For optimum security and flexibility, the Microsoft Windows software environment is delivered with two predefined Customer user groups:

Pap_Customer_Administrators Group (CA)
This group is designed for customer representatives responsible for the overall management, configuration, and operation of the system. Members of the Customer Administrator group are allowed to configure and administrate the server and have full access to the PAM **Domain Manager**, **Hardware Monitor**, **History Manager** and **Configuration Tasks** menus, as shown in Table 39.

Pap_Customer_Operators (CO)
This group is designed for customer representatives responsible for the daily operation of the system. Members of the Customer Operator group are allowed to operate the server and have full access to the **Domain Manager** menu and partial access to the **History Manager** menu, as shown in Table 39.

Notes:

- Group membership also conditions which Event Messages a user will receive via the PAM Web interface. See *Setting up Event Subscriptions*, on page 5-115.
- The predefined Customer user groups have been designed to suit the needs of most Administrator and Operators. Contact your Customer Service Engineer if you require a customized user group.

Warning:
The two predefined Support user groups:

- **Pap_Support_Administrators**
- **Pap_Support_Operators**

are reserved EXCLUSIVELY for authorized Customer Service Engineers in charge of monitoring, servicing, and upgrading the system.

PAM Tools	Associated Actions	CA	CO
Domain Manager	Load/delete domains	X	X
	Power on/off/reset domains	X	X
	View/modify domain settings	X	X
	View domain status	X	X
	View domain resources	X	X
	View BIOS info	X	X
	View BIOS version	X	X
	View loaded BIOS image	X	X
	View power logs	X	X
	View request logs	X	X
	Request a system dump	X	X
Hardware Monitor	View hardware functional/presence status	X	
	View detailed hardware status information	X	
	Use the hardware Search engine	X	
	Exclude/include hardware components	X	
	View current PAM Web site user information	X	
	View PAM version information	X	
History Manager	View system history files and messages	X	
	Manually archive system history files	X	
	View/delete system history archives	X	
	View user history files	X	X
	Manually archive user history files	X	X
	View/delete user history archives	X	X
Configuration Tasks	View/modify customer information	X	
	Modify the system history automatic archiving policy	X	
	Create/modify/delete domain schemes and identities	X	
	Modify domain schemes and identities	X	
	Create/delete user histories	X	
	Modify user history automatic archiving policy	X	
	Customize the event messaging system	X	
	View/ modify PAM parameters	X	
	Display/modify autocall parameters	X	
Status Pane	View/acknowledge WEB event messages	X	X
	Check system functional status	X	X
	Check CSS availability	X	X

Table 39. User access to PAM features

CA = Customer Administrator
CO = Customer Operator

Modifying Customer Information

Customer information is configured during the initial installation procedure, via the PAM configuration setup Wizard. This information is used by PAM software for the **PAM Tree** display and to complete Intervention Reports.
As Customer Administrator, you may modify this information.

To modify Customer information:

1. From the PAM Tree, click **Configuration Tasks** → **Customer Information**.
   The **Customer Information** configuration page opens.
2. Enter the new information and click **Save** to confirm changes.

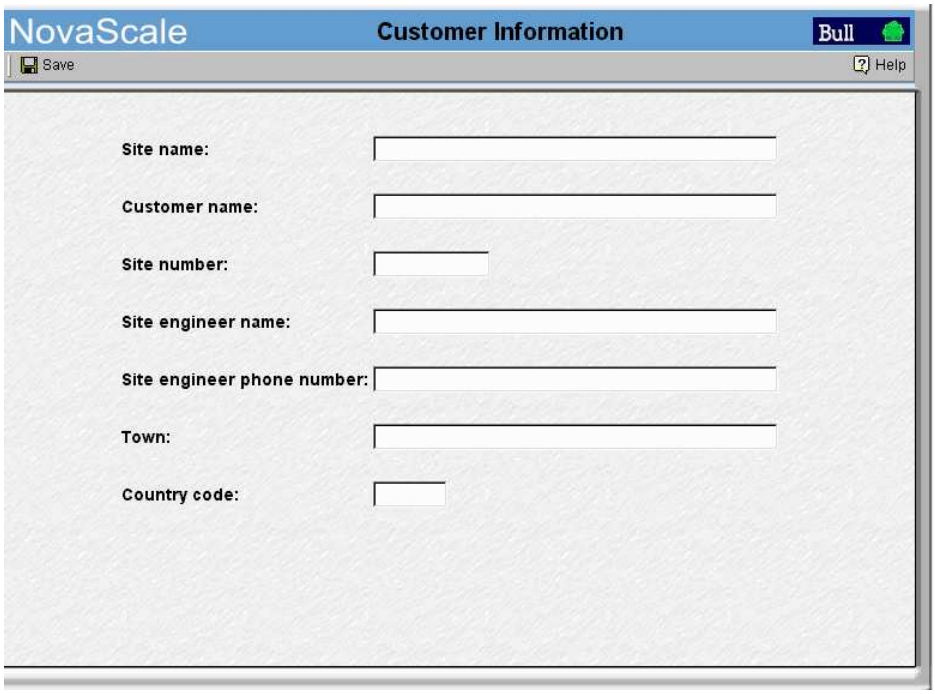


Figure 130. Customer Information configuration page

Note:
The value entered in the **Site name** field will be used for the PAM tree root node.

Configuring Autocalls

The **Autocall** feature is part of the BULL Remote Maintenance contract. It is used to automatically route system events to the Remote Maintenance Center. Full details are given in the BULL *Remote Maintenance Guide*.

If your maintenance contract includes the Autocall feature, configure Autocall parameters as follows:

3. Click **Configuration Tasks** → **Autocalls**. The **Autocalls** configuration page opens.

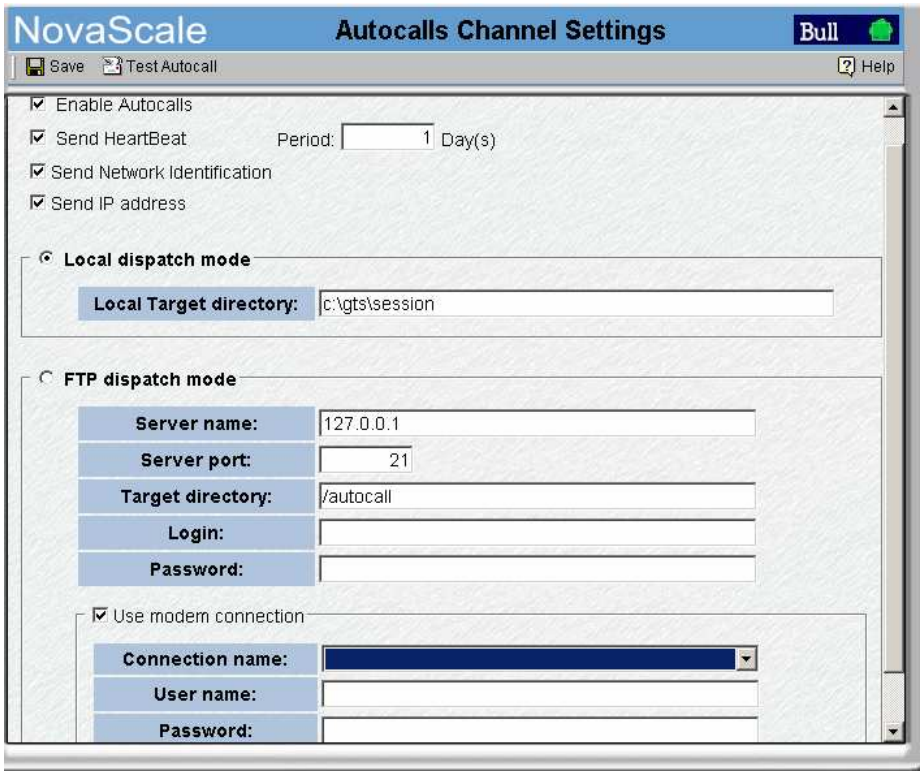


Figure 131. Autocalls Channel Settings control pane

4. Select the **Enable Autocalls** checkbox.
5. Select the **Send Heartbeat** checkbox and enter a value “in days” for the autocall channel control in the **Period** box. Recommended value = 1.
6. Select the autocall dispatch mode :
   - **Local dispatch mode** (default mode) sends autocalls to the local target directory indicated under **Local Settings**,
   - **FTP dispatch mode** sends autocalls to the server indicated under **FTP Settings**.
7. If **Local dispatch mode** (default mode) is selected, complete the **Local Settings** field with the following information:

Field	Explanation	Value
Local target directory	Default GTS directory used to store autocalls.	c:\gts\session

8. If **FTP dispatch mode** is selected, complete the **FTP Settings** fields with the following information:

Field	Explanation	Value
Server name	Remote Maintenance Center server IP address	127.0.0.1
Server port	Default server port	21
Target directory	Default server directory	/autocall
Login	Declared authorized user name	X
Password	Declared authorized user password	X

9. If a modem connection is to be used:
   a. From the PAP Unit Microsoft Windows desktop, configure the dial–up connection (**Control Panel** → **Phone and Modem Options**).
   b. From the PAM **Autocalls Control Pane**, select the **Use modem connection** checkbox.
   c. Use the **Connection name** drop–down menu to select the required modem connection.
   d. Complete the **User name** and **Password** fields with the declared authorized user name and user password.

Setting Thermal Units

By default, PAM software displays thermal measurements in degrees Celsius. As Customer Administrator, you may change the default setting to degrees Fahrenheit.

To change PAM thermal units:

1. Click **Configuration Tasks** → **PAM**. The **PAM Configuration** control pane opens.
2. Click the **Celsius** or **Fahrenheit** radio button, as required.
3. Click **Save**. A green icon appears in the top left corner of the control pane to confirm the change.

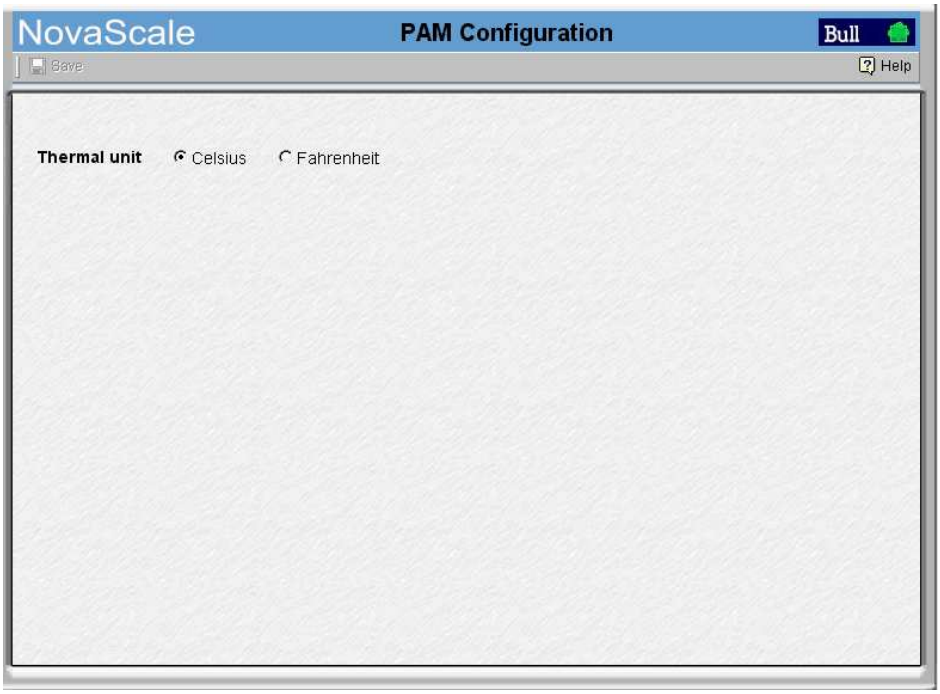


Figure 132. PAM configuration control pane

Deploying a New PAM Release

As Customer Administrator, you can deploy a new PAM release by running the new *PAM Installation package x.y.z. msi* (*x.y.z* being the PAM version e.g. 7.15.0 2.1.9) file.

To install a new PAM Release:

1. From the local PAP unit console, power down all server domains and close the current PAM session.
2. From the default *PAM Installation* directory, double click the **.msi file** to launch the *PAM Installation InstallShield Wizard*.
3. Select **Complete** to install all program features and to accept the default path for the installation folder:

   <WinDrive>:\Program Files\BULL\PAM\installation\<*Release Version*>
   (e.g. d:\Program Files\BULL\PAM\installation\7.15.0 2.1.9).

   or, select **Custom** to select program features and to define a path for the installation folder.

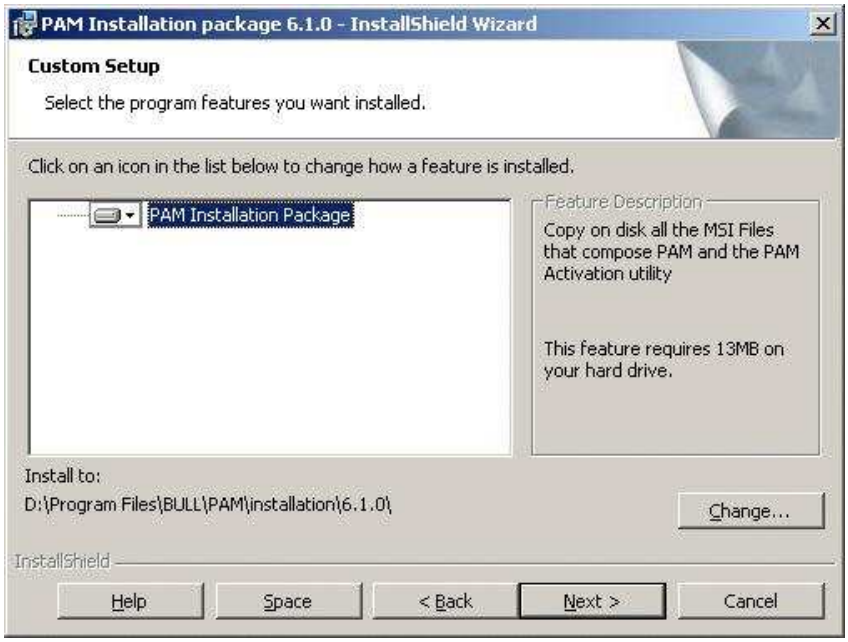


Figure 133. PAM Installation InstallShield Wizard

Note:
This path is the repository for activation files. NEVER delete this folder after activation as it is required to repair and re–activate the release.

4. Click **Install** to begin setup.
5. Select the **Launch PAM Activation** utility checkbox and click **Finish**. The **PAM Activation** utility is automatically launched.

   The **PAM Activation** icon is installed on the PAP unit desktop and the **Platform Administration and Maintenance** program group, giving access to the **PAM Activation** and **PAP Configuration** executable files, is installed in the **Program Files** directory.

Activating a PAM Version

The *PAM InstallShield Wizard* automatically creates a shortcut to the **PAM Activation** utility on the PAP unit desktop that can be used at any time to activate an installed PAM Version.

Note:
A previous PAM Version can be re–activated at any time, in the event of a problem with the current release.

To activate / re–activate a PAM Version:

1. From the local PAP unit console, power down all server domains and close the current PAM session.
2. From the *PAM Activation* utility on the Microsoft Windows desktop, select the required PAM Version and click **Activate** to launch the *PAM Activation InstallShield Wizard*.
3. Select **Complete** to accept the default paths for the PAM Release and PAM Site Data folders:

   The default PAM **Release** directory for all the files delivered as part of PAM software is:

   <*WinDrive*>:\Program Files\BULL\PAM\<*Release Version*>
   (e.g. d:\Program Files\BULL\PAM\7.15.0).

   The default PAM **Site Data** directory for all the files produced by PAM software (history files, configuration files) concerning Customer site definition and activity is:

   <*WinDrive*>:\Program Files\BULL\PAM\PAMSiteData\<*DataCompatibilityRelease*>
   (e.g. d:\Program Files\BULL\PAM\PAMSiteData\1).

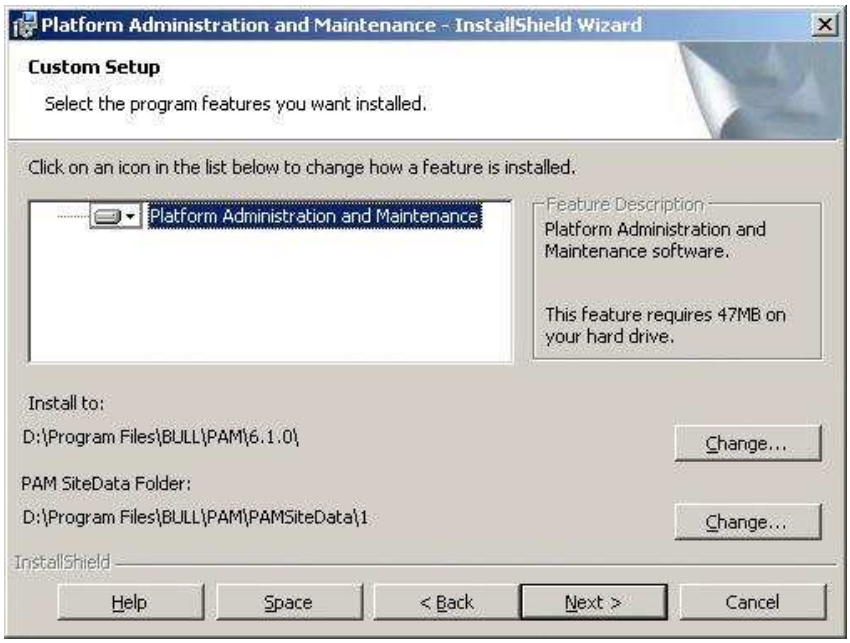


Figure 134. PAM Activation InstallShield Wizard

Important:
PAM releases use the same data directory to ensure configuration consistency.
Before activating / re–activating a PAM Version, ensure that the <Data Compatibility Release> level of deployed releases is compatible.
If it is NOT compatible, PAM configuration options (e.g. Event subscription options, Domain Schemes and Identities, ...) may be lost.

4. Click **Install** to begin activation.
5. Select the **Launch PAP Configuration** utility checkbox if you want to configure or reconfigure PAP unit settings. Otherwise, click **OK** to complete activation.
6. From the local PAP unit console, right click the **Microsoft Internet Explorer** icon on the desktop and click **Properties** → **General** → **Delete Files** to delete all the files in the Temporary Internet Folder.
7. Launch a new PAM session.

Important:
Notify all authorized users, connecting to PAM from a remote console, that a new PAM Version has been activated and request them to:

a. Close their current PAM session.

b. Delete all the files in their Temporary Internet Folder.

c. Launch a new PAM session.

Backing Up and Restoring PAM Configuration Files

As Customer Administrator, you are advised to regularly save PAM configuration data to a removable media or to a network directory so that it can be rapidly restored in the event of PAP unit failure.

PAM software can be deployed on any standard PC running the appropriate version of Microsoft Windows and you can restore your configuration data to rebuild your working environment.

To ensure carefree, reliable and regular configuration data backup, the Bull NovaScale Server Resource CD contains two scripts, **PamBackupData.js** and **PamRestoreData.js**, that can be scheduled to run via the Microsoft Windows **Task Scheduler** to save and restore PAM configuration data.

☞ **Notes:**

- PAM configuration data is automatically saved to the default PAM Site Data directory on the PAP unit:

  <*WinDrive*>:\Program Files\BULL\PAM\PAMSiteData\<*DataCompatibilityRelease*>

- The **PamBackupData.js** and **PamRestoreData.js** scripts are stored in the PAM Site Data directory on the PAP unit:

  <*WinDrive*>:\Program Files\BULL\PAM\PAMSiteData\ReleaseData\Utilities

Backing Up PAM Configuration Files

To create a Microsoft Windows automatic backup task:

1. Select or create the local or network directory to be used for saving configuration data, e.g. ***<MyPamBackupDirectory>***.
2. Create a local directory for the **PamBackupData.js** and **PamRestoreData.js** script files, e.g. ***<MyPamBackupTools>***.
3. Copy the **PamBackupData.js** and **PamRestoreData.js** script files into the ***<MyPamBackupTools>*** directory.
4. Create a Text File and enter the following command line:

   Cscript PamBackupData.js <***MyPamBackupDirectory***>

5. Save the Text File as a batch file with a **.BAT** extension, e.g. <***MyPamBackupCommand***>**.bat**.
6. Click **Control Panel** → **Scheduled Tasks** → **Add Scheduled Task** to open the **Task Scheduler** wizard and follow the instructions. PAM configuration data will be automatically saved at the interval indicated in the wizard.

Restoring PAM Configuration Data

Warning:
The same PAM software release must be deployed on the PAP unit and on the backup PC to allow data restoration. See *Deploying a New PAM Release*, on page 5-23 and *Activating a PAM Version*, on page 5-24.
PAM releases use the same data directory to ensure configuration consistency. Before activating / re–activating a PAM Version, ensure that the <DataCompatibilityRelease> level of deployed releases is compatible.

To restore PAM configuration data:

7. From the Microsoft Windows desktop, open a command window. Browse to the ***<MyPamBackupTools>*** directory containing the script files and enter the following command line:

   Cscript PamRestoreBackupData.js <***MyPamBackupDirectory***>

   Saved PAM configuration data is restored.

Section IV – Configuring Domains

Important:
This section describes domain configuration and management tools that are reserved for use with partitioned servers and extended systems. Please contact your Bull Sales Representative for sales information.

This section explains how to:

Partitioning your Server

Bull NovaScale Servers are designed around a flexible, cell–based, midplane architecture allowing dynamic partitioning into physically independent domains. A domain is a coherent set of hardware and software resources managed by a single Operating System instance.

The NovaScale 6080/6160 Server is designed to operate as one or two hardware–independent SMP systems, or domains.

The NovaScale 6320 Server is designed to operate as one, two, three or four hardware–independent SMP systems, or domains.

Note:
Server components and configuration may differ according to site requirements. At least one IOB and one QBB are required for each server domain.

Partitioning allows you to optimize your server to:

- meet variations in workload – peak / off–peak periods,
- allow different time and date settings,
- use the same environment for tests and production,
- carry out software tests prior to deployment / upgrades,
- reduce downtime for servicing or re–configuration.

PAM software provides you with all the tools and features required to partition and manage your server as independent SMP systems. For easy configuration and optimum use of the physical and logical resources required for simultaneous operation, domains are defined via the **Domain Configuration Scheme** wizard. From the PAM tree, expand the **Configuration Tasks** and **Domains** nodes to display domain configuration options.

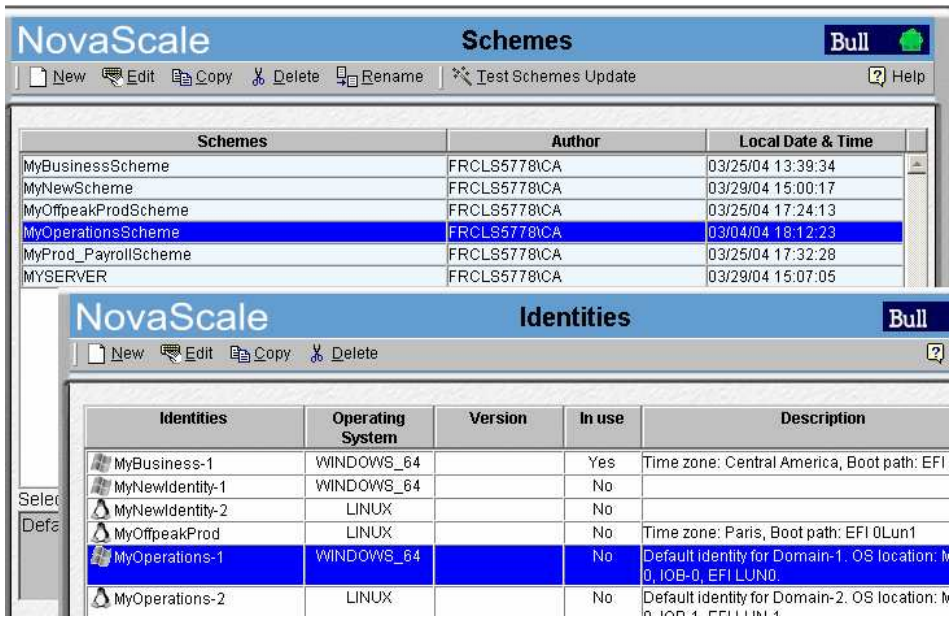


Figure 135. Schemes and Identites panes

A **Domain Configuration Scheme** is used to define and manage a set of domains that can be active simultaneously. The **Schemes** control pane allows you to create, edit, copy, delete, and rename domain configuration schemes and update default test schemes.

A **Domain Identity** is used to define and manage domain context information. The **Identities** control pane allows you to create, edit, copy, and delete domain identities.

The server is delivered with a pre–configured domain configuration scheme called **MyOperationsScheme**, allowing you to simultaneously manage and administer all server resources. However, as Customer Administrator, you may want to create other schemes and identities to suit your working environment.

Before proceeding to create a new Scheme and/or new Domain Identities, you are advised to assess your configuration requirements. See *Assessing Configuration Requirements*, on page 5-31.

Assessing Configuration Requirements

At least one IOB and one QBB are required for each server domain.

You can use the following checklist to help you make an accurate plan of how you want to partition and manage your system. For easy planning, you can print a copy of the Scheme, Domain Identity, and Resources checklist templates provided on page 5-109.

Scheme Checklist	
Name	What name do I want to use for my Scheme? Examples: • *MyFullConfigScheme* • *MyPartConfigScheme* • *MyNightScheme* • *MyDayScheme* • *MyTest_ProductionScheme*
Description	How can I describe my Scheme to reflect its scope? Examples: • *Central Subsystems included* • *Resources used* • *Domain Identities used*
Central Subsystem(s)	Which Central Subsystem(s) do I want to use?
Number of Domains	How many domains do I need?
Domain Size	How many cells do I want to assign to each domain?
EFI Boot LUNs	Which EFI boot LUN do I want to use for each domain? Do I need to create a new EFI boot LUN from the disk subsystem utility before defining my new scheme?
Data LUNs *	Which data LUNs do I want to assign to each domain? Do I need to create a new data LUN from the disk subsystem utility before defining my new scheme?
Fibre Channel Hosts *	Which fibre channel host do I want to use to access LUNs?
I/O Resource Location	Which cells host the I/O resources I want to use?
Resource Access	Do I want to limit access to certain hardware resources?

* Reserved for systems connected to a Storage Area Network (SAN).

Table 40. Domain configuration assessment criteria – 1

Domain Identity Checklist	
Name	What name do I want to use for my Domain Identity to reflect the tasks/jobs it will run? Examples: • *MyDataMiningIdentity* • *MyDataBaseIdentity* • *MyProductionIdentity* • *MyTestIdentity*
Description	How can I describe my Domain Identity to reflect its use? Examples: • *OS and applications* • *Time zone* • *Boot path* • *IP address* • *Network name* • *URL* • *Production / test conditions*
Operating System	Which OS do I want to run on this domain? Does this OS support assigned hardware (CPUs, DIMMs)?
Domain Network Name	Which network name will be used to identify this domain?
Domain IP Address	Which IP address will be used to reach this domain?
Domain URL	Which URL can be used to reach my domain Web site (if any)?
Multithreading Mode	Do the CPUs used by this domain support the multithreading mode? Do I want to enable the multithreading mode for this domain?
High Memory IO Space	Do I need more than 4GB PCI gap space for the PCI boards used by this domain?
Machine Check	Do I want this domain to halt or to automatically reset if a machine check error occurs?
Licensing number	Do I intend to install an application protected by a system serial number on this domain? Do I want to substitute the physical system serial number with the logical licensing number for optimum flexibility?
Force Halt on Machine Check Reset	Has my Customer Service Engineer requested me to check this box to troubleshoot my server?

Table 41. Domain configuration assessment criteria – 2

Managing Domain Configuration Schemes

What You Can Do

From the **Schemes** Control pane, you can:

- *Create a domain configuration scheme*
- *Edit a domain configuration scheme*
- *Copy a domain configuration scheme*
- *Delete a domain configuration scheme*
- *Rename a domain configuration scheme*

Creating a Domain Configuration Scheme

Pre–requisites

- Required EFI LUNs and Data LUNs must be created from the utility delivered with the storage subsystem.
  See *Configuring System and Data Disks*, on page 5-4.
- SAN LUN and/or Local LUN lists must be updated from the **Logical Units** page.
  See *Updating SAN LUNs*, on page 5-53 and/or *Updating Local LUNs*, on page 5-54 and on page 5-59.
- SAN Fibre Channel HBA World Wide Name (WWN) parameters must be up–to–date.
  See *Checking and Updating Fibre Channel HBA World Wide Names*, on page 5-60.
- Domain Identities can either be created via the Domain Scheme wizard or, independently, via the **Identities** configuration page. See *Creating a Domain Identity*, on page 5-48.
- At least one IOB and one QBB are required for each server domain.

Steps

- Assess requirements
- Create EFI and/or Data LUNs
- Update the LUN lists
- Update Fibre Channel World Wide Name (WWN) parameters*
- Select the Central Subsystem(s)
- Define the number of domains

For each domain in the scheme:

- Select / create a domain identity
- Select an EFI LUN
- Select Data LUNs*
- Link LUNs to the Fibre Channel Host*
- Lock access to hardware resources

* Reserved for systems connected to a Storage Area Network (SAN)

To create a domain configuration scheme:

1. Assess your configuration requirements. See *Assessing Configuration Requirements*, on page 5-31.
2. If required:
   - Create EFI and/or Data LUNs from the utility delivered with the storage subsystem. You are advised to use **RAID level 1** for **EFI LUNs** and **RAID level 5** for **Data LUNs**.
   - Update the SAN LUN and/or Local LUN lists from the Logical Units page. See *Updating SAN LUNs*, on page 5-53 and/or *Updating Local LUNs*, on page 5-54 and on page 5-59.
   - Update Fibre Channel HBA World Wide Name (WWN) parameters.
3. Click **Configuration Tasks** → **Domains** → **Schemes** in the PAM tree to open the **Schemes** control pane.

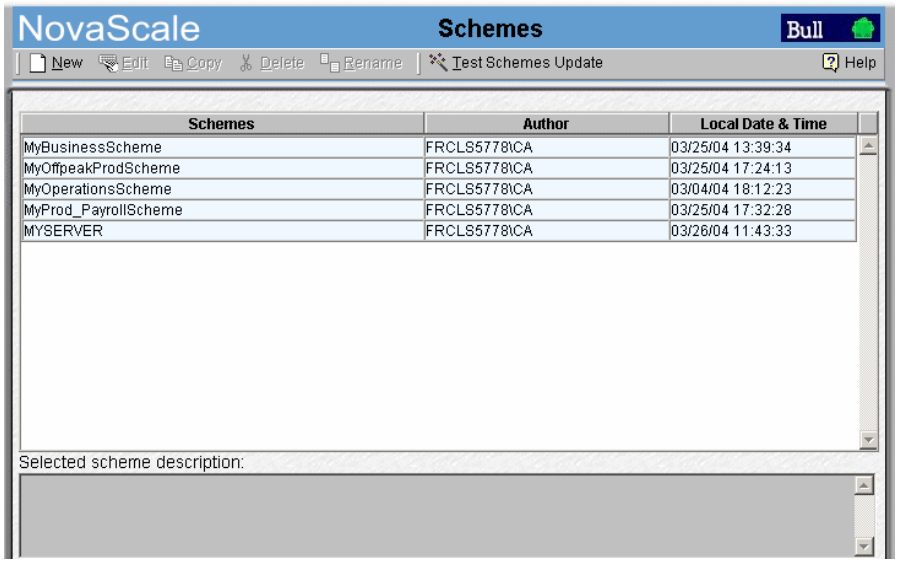


Figure 136. Schemes control pane

4. Click **New** in the toolbar to open the **Scheme Management** dialog.

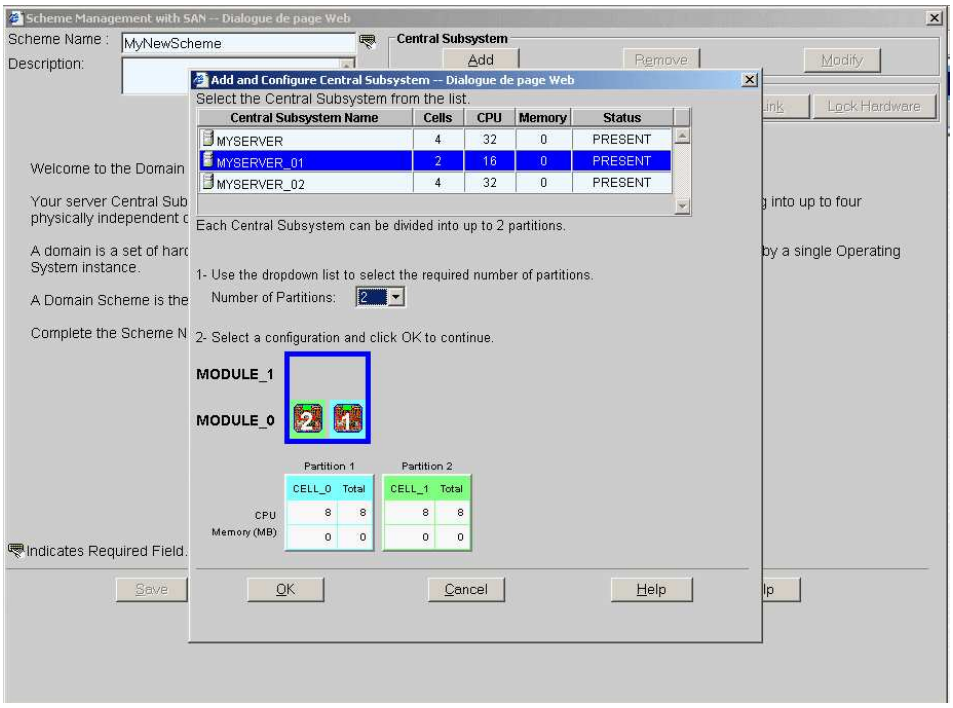
Central Subsystem	
Scheme Name	Name used to identify the scheme.
Description	Brief description of scheme configuration.
Add	Select the Central Subsystem used in the scheme.
Remove	Remove a Central Subsystem from the scheme.
Modify	Select the number of hardware partitions in the scheme.
Domains	
Remove	Remove the selected domain from the scheme.
Identity	Select a domain identity.
EFI LUNs	Select an EFI Boot LUN.
Data LUNs *	Assign Data LUNs to the domain.
Link *	Define the fibre channel host to be used to access LUNs.
Lock Hardware	Limit access to certain hardware resources.

* Reserved for systems connected to a Storage Area Network (SAN)

Figure 137. Scheme Management dialog

5. Complete the **Scheme Name** and **Description** fields, as required. See *Assessing Configuration Requirements*, on page 5-31.
6. Click **Central Subsystem** → **Add** to select the Central Subsystem to be used by the domain configuration scheme. The **Central Subystem Configuration** dialog opens.

NovaScale 6080/6160 Server



NovaScale 6320 Server

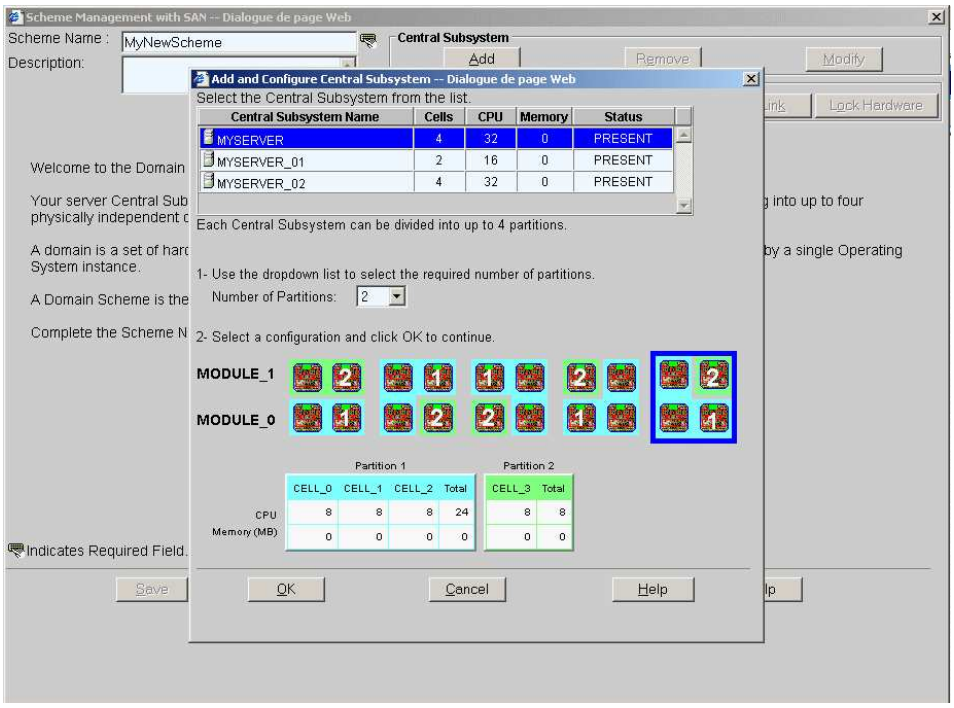
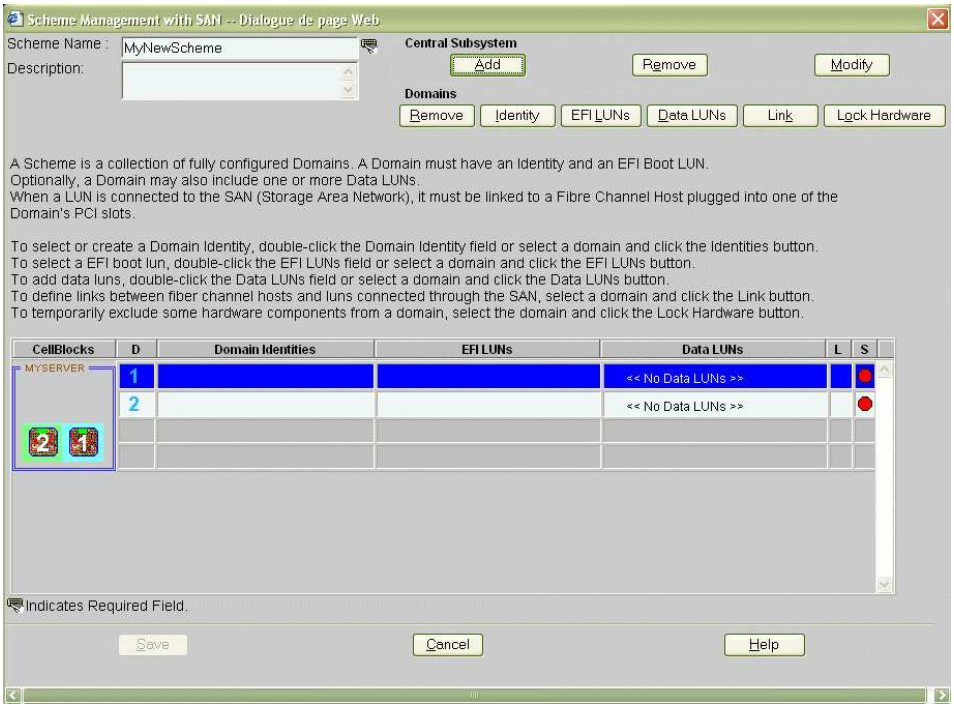


Figure 138. Scheme Creation and Central Subsystem Configuration dialogs

7. Select a Central Subsystem and use the **Number of Parts** dropdown list to select the required number of hardware partitions (**2** in the examples).
8. Select the required partition configuration and click **OK** to return to the **Scheme Management** dialog.

   Status icons are red because **Domain Identities** and **EFI LUNs** are required to complete domain configuration.

NovaScale 6080/6160 Server



NovaScale 6320 Server

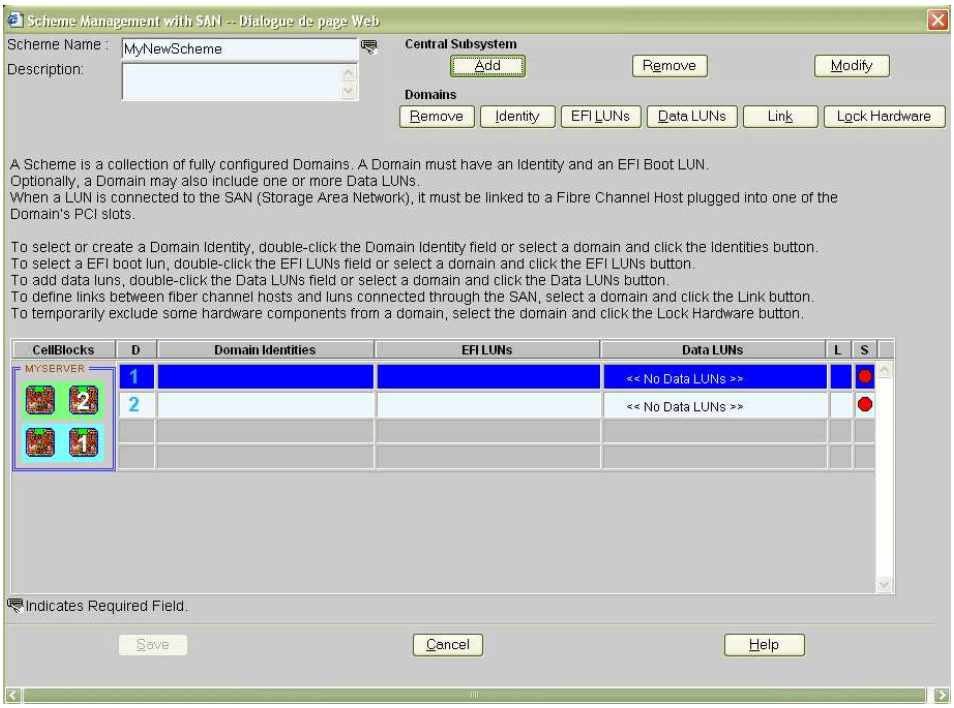


Figure 139. Scheme Management dialog

9. Click **Domains** → **Identity** to open the **Identities List** dialog.

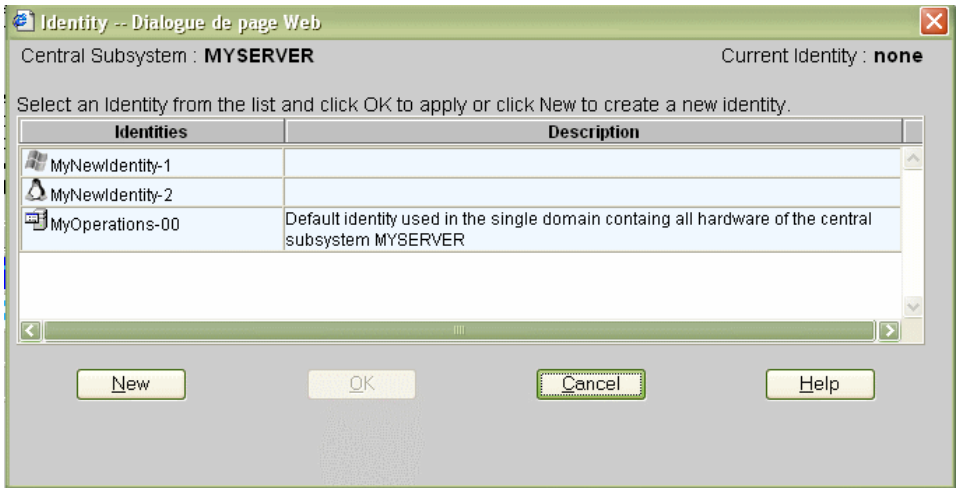
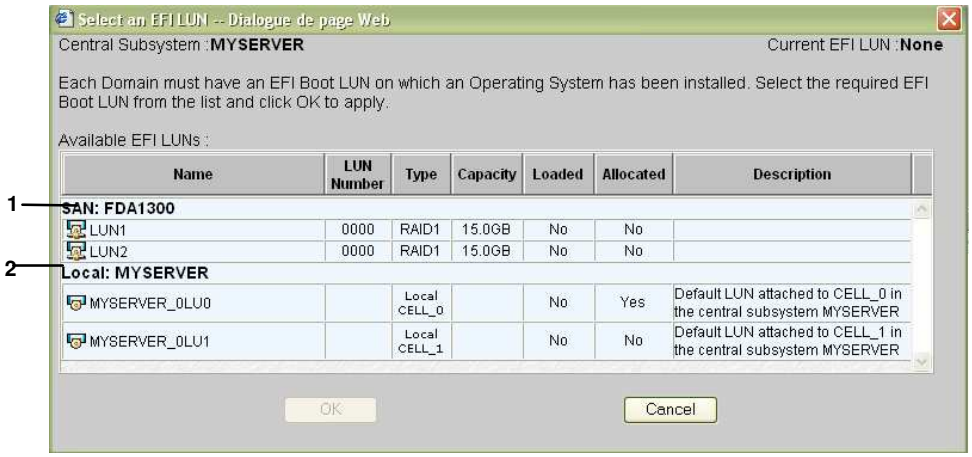


Figure 140. Domain Identities list

10. If the required identity is in the list, go to Step 11.
    If you want to create a new identity for this domain, click **New** to open the **Create New Identity** dialog. See *Creating a Domain Identity*, on page 5-47.
11. Select the required identity from the list of available identities and click **OK** to return to the **Scheme Management** dialog. The selected identity is now displayed in the **Domain Identities** field.
12. Click **Domains** → **EFI LUNs** to open the **Select EFI LUN** dialog.



1 SAN storage subsystem **2** Local storage subsystem

13. If the required EFI LUN is in the list, go to Step 14.
    If the required EFI LUN is not in the list, you must exit the Domain Scheme wizard to configure the EFI LUN. See *Pre–requisites*, on page 5-33.
14. Select the required EFI Boot Lun from the list of available Luns and click **OK** to return to the **Scheme Management** dialog. The selected LUN is now displayed in the **EFI LUNs** field.
15. If the EFI LUN is a Local LUN, the **Status** icon turns green, go to Step 16.

    If the EFI LUN is a SAN LUN, the **Status** icon remains red and the **No Link** icon appears.

16. If the EFI LUN is a Local LUN and you do not want to add one or more Data LUNs to the domain, go to Step 26.
    If the EFI LUN is a SAN LUN and you do not want to add one or more Data LUNs to the domain, go to Step 20.
    If the EFI LUN is a Local or SAN LUN and you want to add one or more SAN Data LUNs to the domain, click **Domains** → **Data LUNs** to open the **Select Data LUN** dialog.

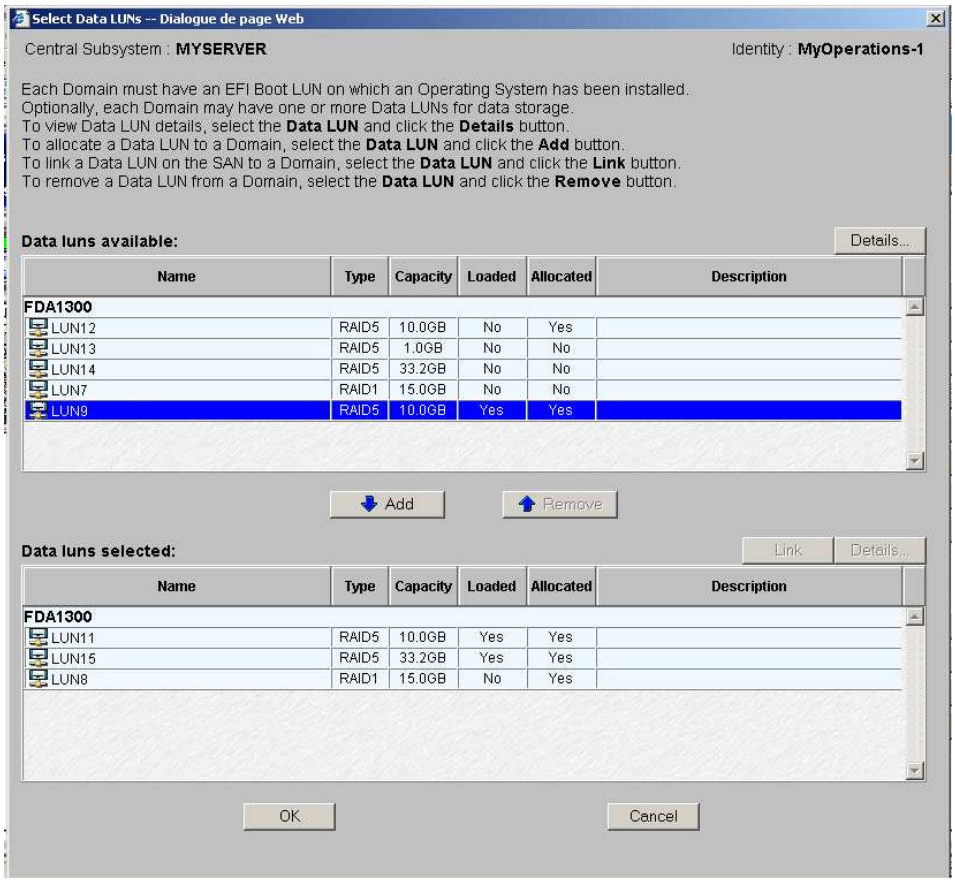
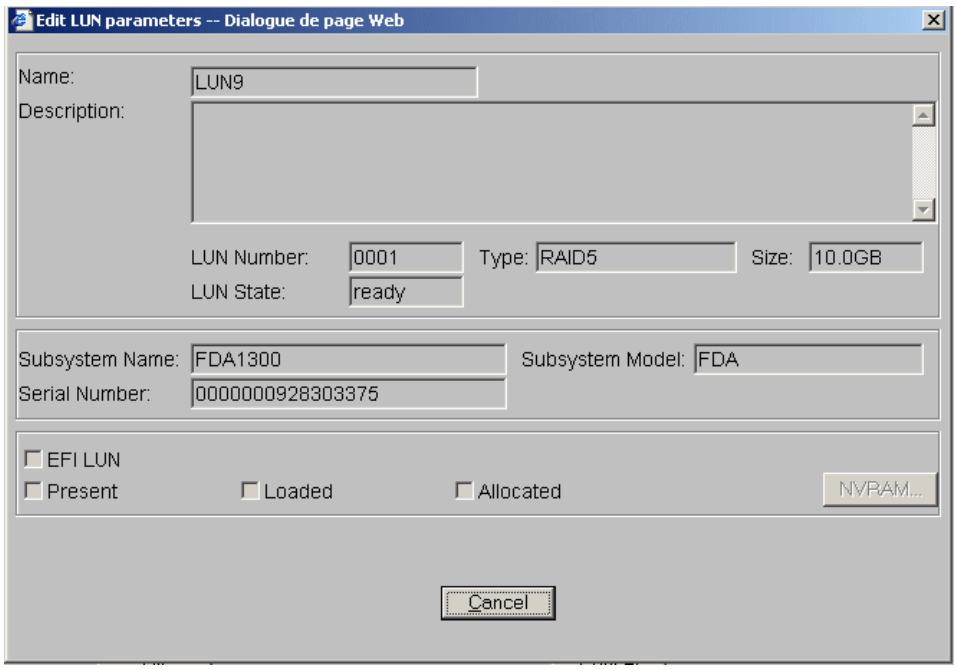


Figure 141. Select Data LUN dialog – Data luns available list

17. Select the LUN you want to add to the domain in the **Data LUNs available** list and click **Details** to view LUN parameters, if required.



Name	Name given to the LUN when created.
Description	Brief description of the LUN.
LUN Number	Number allocated to the LUN when created.
LUN State	If the LUN is ready for use, READY is displayed.
Type	LUN configuration mode.
Size	LUN size.
Subsystem Name	Name of the subsystem containing the LUN.
Subsystem Model	Type of subystem containing the LUN.
Serial Number	Serial number of the subsystem containing the LUN.
EFI LUN	If this box is checked, the LUN is an EFI boot LUN. If this box is not checked, the LUN is a Data LUN.
Present	If this box is checked, the LUN is detected. If this box is checked, the LUN is not detected.
Loaded	If this box is checked, the LUN is loaded in the Domain Manager Control pane. If this box is not checked, the LUN is not loaded in the Domain Manager Control pane.
Allocated	If this box is checked, the LUN is already allocated to a scheme. If this box is not checked, the LUN is not allocated to a scheme.

Figure 142. View LUN parameters dialog

18. Click **Add**. The selected Data LUN is moved to the **Data LUNs selected** list.

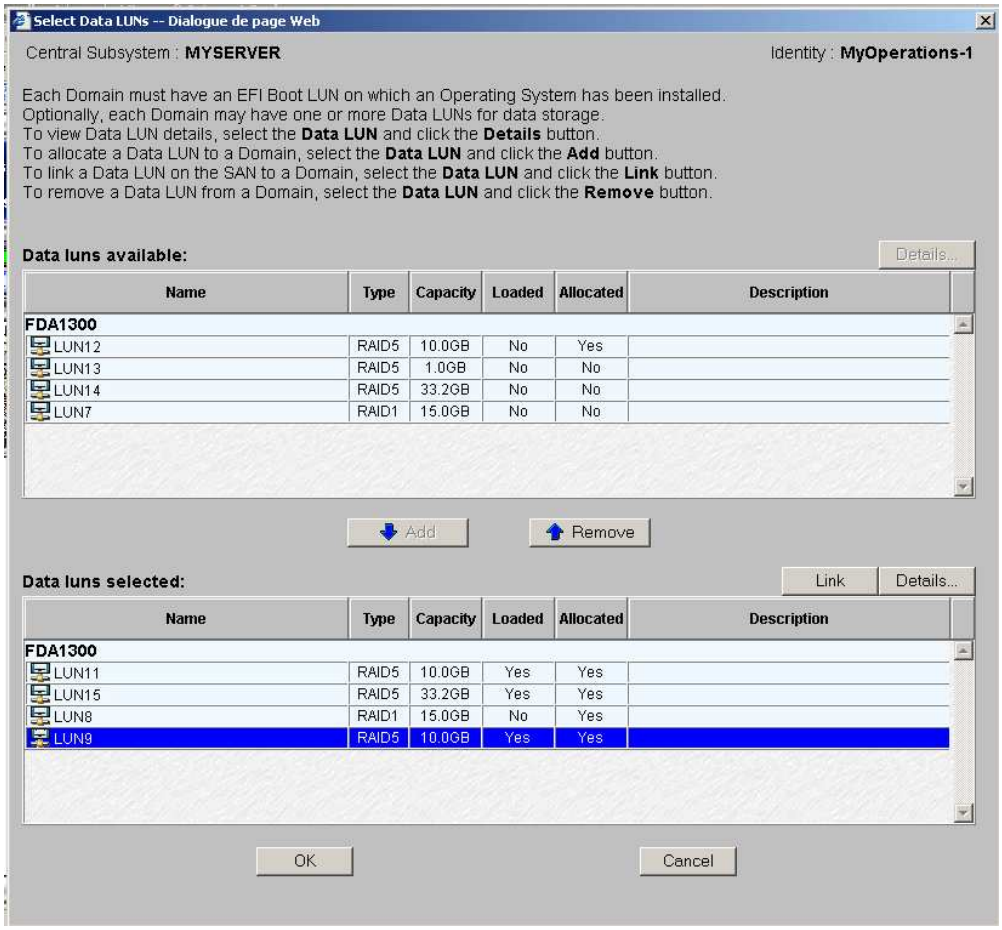


Figure 143. Select Data LUN dialog – Data luns selected list

19. Repeat Steps 17 and 18 for each Data LUN you want to add to the domain and click **OK** to return to the **Scheme Management** dialog. **Data LUN set** is now displayed in the **Data LUNs** field.

    The **Status** icon remains red and the **No Link** icon is displayed. You must now link the selected EFI and Data LUNs to the Fibre Channel Host you want to use to access these LUNs.

20. Click **Domains** → **Link** to open the **Link LUNs to HBA** dialog.

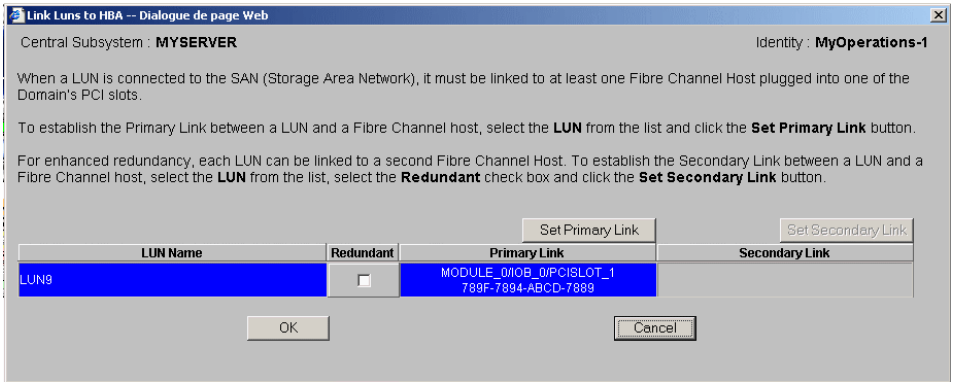


Figure 144. Link LUNs to HBA dialog

21. Select the **Redundant** checkbox if you want to define two links to the LUN.

Note:
If you select the **Redundant** mode, you will be informed that dedicated software is required to enable this mode and you will be requested to confirm your choice.

22. Click **Set Primary Link** to define the main access path to the SAN. The **Select HBA** dialog opens, allowing you to select the domain PCI slot you want to use to access the LUN.

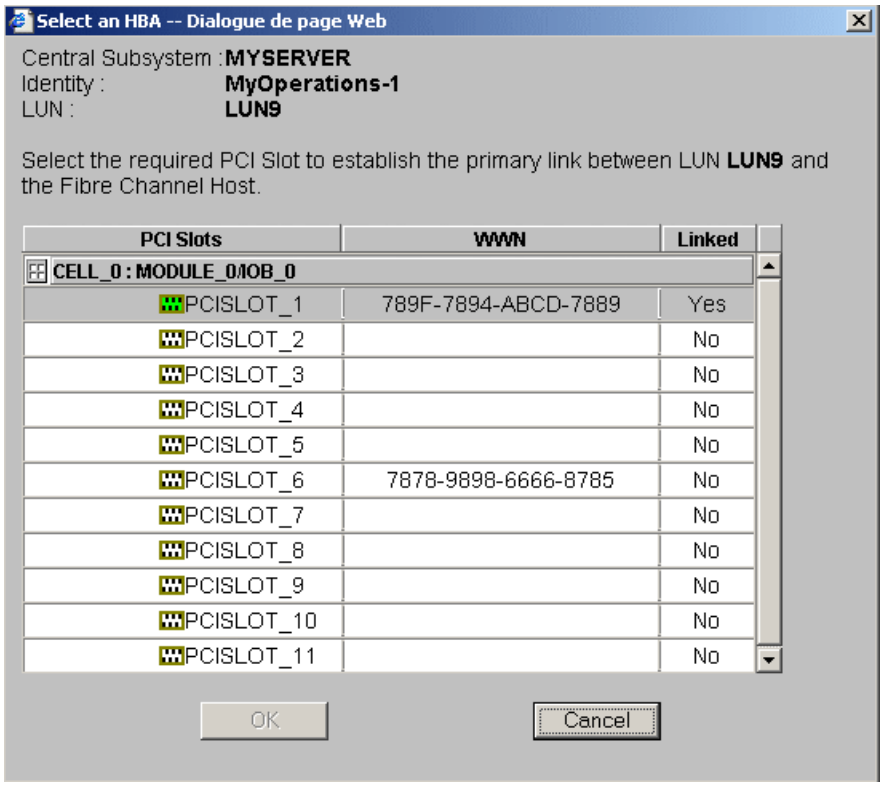
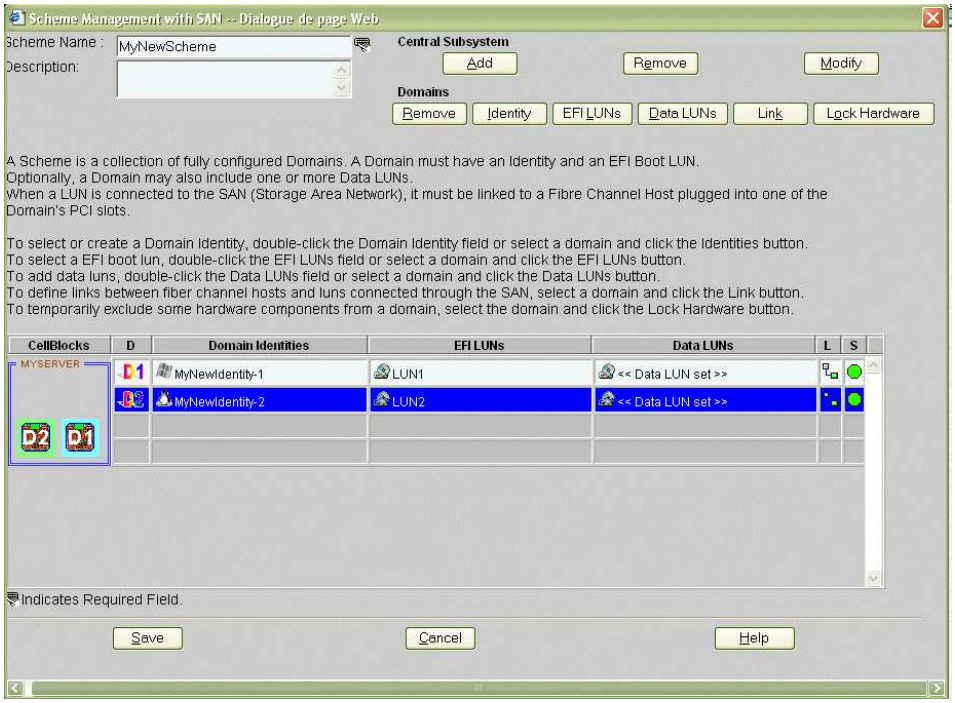


Figure 145. Select an HBA dialog

23. Select the PCI slot containing the HBA to be used as the primary link to the SAN and click **OK**. The primary link is now set.
24. Where applicable, click **Set Secondary Link** to define the backup access path to the SAN. Select the PCI slot containing the HBA to be used as the secondary link to the SAN and click **OK**. The secondary link is now set.
25. Click **OK** → **Apply** to return to the **Scheme Management** dialog. The **Status** icon turns green and the **Linked** icon appears.
26. Repeat Steps 9 to 25 for the other domains. All **Status** icons turn green.

NovaScale 6080/6160 Server



NovaScale 6320 Server

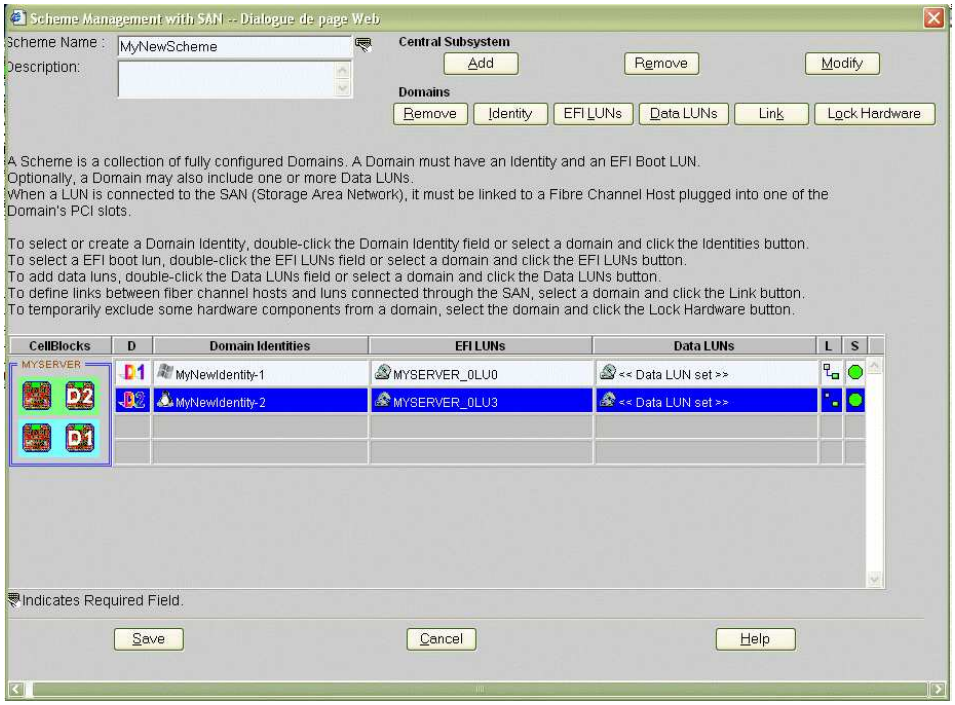


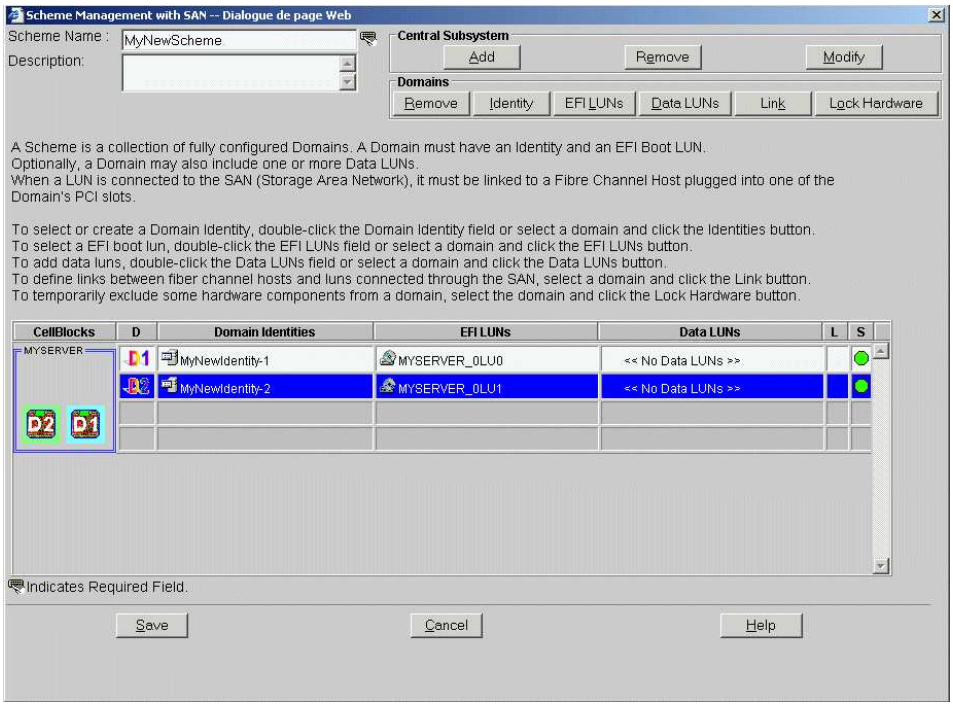
Figure 146. Scheme Management dialog

27. If you do not want to functionally limit access to certain hardware elements, go to Step 28.
    If you want to functionally limit domain access to certain hardware elements, click **Domains** → **Lock Hardware** to open the **Lock Domain Hardware Resources** dialog. See *Limiting Access to Hardware Resources*, on page 5-62.
28. Click **Save**. The domain configuration scheme is now available for domain management.

Editing a Domain Configuration Scheme

To edit a domain configuration scheme:

1. Assess your configuration requirements. See *Assessing Configuration Requirements*, on page 5-31.
2. Click **Configuration Tasks** → **Domains** → **Schemes** in the PAM tree to open the **Schemes** pane. See Figure 136 above.
3. Select the required scheme from the list.
4. Click **Edit** in the toolbar to open the **Edit Scheme** dialog.



Central Subsystem	
Add	Click here to add another Central Subsystem to your scheme. See *Creating a Domain Configuration Scheme*, on page 5-33.
Remove	Click here to remove a Central Subsystem from your scheme.
Modify	Click here to change the number of hardware partitions in your scheme.
Domains	
Remove	Click here to remove the selected domain from the scheme.
Identity	Click here to select a domain identity.
EFI LUNs	Click here to select an EFI Boot LUN.
Data LUNs *	Click here to assign Data LUNs to the domain.
Link *	Click here to define the fibre channel host to be used to access LUNs.
Lock Hardware	Click here to limit access to certain hardware resources.

* Reserved for systems connected to a Storage Area Network (SAN).

Figure 147. Edit Scheme dialog

5. Make the required changes and click **Save**. The modified domain configuration scheme is now available for domain management.

Copying a Domain Configuration Scheme

To copy a domain configuration scheme:

1. Click **Configuration Tasks** → **Domains** → **Schemes** in the PAM tree to open the **Schemes** pane. See Figure 136 above.
2. Select the required scheme from the list.
3. Click **Copy** in the toolbar. The **Copy Scheme** dialog opens.
4. Enter a name for the new scheme and click **OK**. The new domain configuration scheme is now available for domain management.

Deleting a Domain Configuration Scheme

To delete a domain configuration scheme:

1. Click **Configuration Tasks** → **Domains** → **Schemes** in the PAM tree to open the **Schemes** pane. See Figure 136 above.
2. Select the required scheme from the list.
3. Click **Delete** in the toolbar. You are requested to confirm scheme deletion.
4. Click **OK** to confirm. The domain configuration scheme is removed from the **Schemes List** and is no longer available for domain management.

Renaming a Domain Configuration Scheme

To rename a domain configuration scheme:

1. Click **Configuration Tasks** → **Domains** → **Schemes** in the PAM tree to open the **Schemes** pane. See Figure 136 above.
2. Select the required scheme from the list.
3. Click **Rename** in the toolbar.
4. Enter a new name for the scheme and click **OK**. The renamed domain configuration scheme is now available for domain management.

Updating Test Schemes

The **Domain Wizard** allows you to automatically generate and update a set of **Test Schemes**. These test schemes take into account all the hardware in your configuration. You may need to update your test schemes after a service intervention entailing the addition/removal of hardware elements.

To update test schemes:

1. Click **Configuration Tasks** → **Domains** → **Schemes** in the PAM tree to open the **Schemes** pane. See Figure 136 above.
2. Click **Test Schemes Update** in the toolbar. Default test schemes are automatically updated.

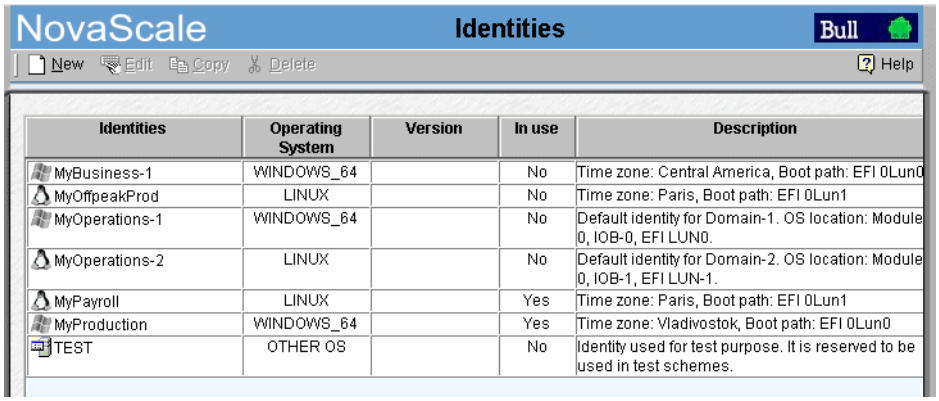
Creating, Editing, Copying, Deleting a Domain Identity

Note:
Domain Identities can either be created via the **Domain Configuration Scheme** wizard or, independently, via the **Identities** configuration page. See *Creating a Domain Configuration Scheme*, on page 5-33.

Creating a Domain Identity

To create a domain identity:

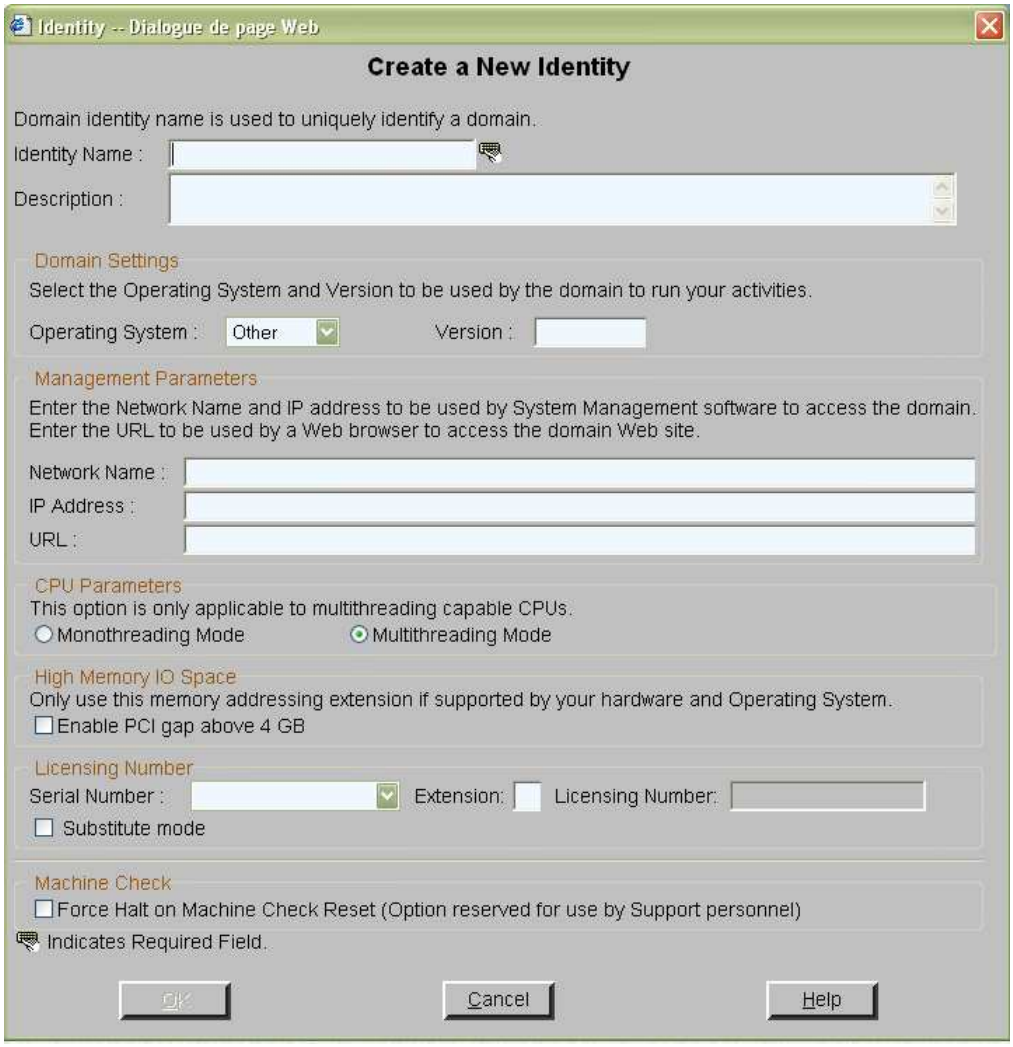
1. Assess your configuration requirements. See *Assessing Configuration Requirements*, on page 5-31.
2. Click **Configuration Tasks** → **Domains** → **Identities** in the PAM tree to open the **Identities Management** page.



Identities	Operating System	Version	In use	Description
MyBusiness-1	WINDOWS_64		No	Time zone: Central America, Boot path: EFI 0Lun0
MyOffpeakProd	LINUX		No	Time zone: Paris, Boot path: EFI 0Lun1
MyOperations-1	WINDOWS_64		No	Default identity for Domain-1. OS location: Module 0, IOB-0, EFI LUN0.
MyOperations-2	LINUX		No	Default identity for Domain-2. OS location: Module 0, IOB-1, EFI LUN-1.
MyPayroll	LINUX		Yes	Time zone: Paris, Boot path: EFI 0Lun1
MyProduction	WINDOWS_64		Yes	Time zone: Vladivostok, Boot path: EFI 0Lun0
TEST	OTHER OS		No	Identity used for test purpose. It is reserved to be used in test schemes.

Figure 148. Identities List page

3. Click **New** in the toolbar to open the **Create New Identity** dialog.



Name	Name reflecting the tasks/jobs to be run by the domain.
Description	Brief description reflecting domain use.
Operating System Version	OS and OS version to be run on this domain. **Note:** Check that the selected OS supports assigned hardware (CPUs, DIMMs)?
Domain Network Name	Network name used to identify this domain.
Domain IP Address	IP address used to reach this domain.
Domain URL	URL used to reach the domain Web site (if any).
Multithreading Mode	Enable / disable multithreading. **Note:** Check that the CPUs used by this domain support the multithreading mode.
High Memory IO Space	Enable / disable extended PCI gap memory space. **Note:** Only use if this domain uses PCI boards requiring more than 4GB PCI gap space. Compatibility problems may arise under Windows.
Licensing Number	Licensing number used by protected applications, created by adding a two digit extension to the system serial number. Enable / disable substitute mode. **Note:** Check this box to substitute the physical system serial number with the logical licensing number for optimum flexibility.
Force Halt on Machine Check Reset	Enable / disable automatic domain reset when a machine check error occurs. **Note:** Check this box when requested by your Customer Service Engineer.

Figure 149. Create New Identity dialog

4. Complete the **Name**, **Description**, **Domain Settings**, **Management Parameters**, **Multithreading Mode**, **HMMIO Space**, **Machine Check**, **Licensing Number** and **Force Halt on Machine Check Reset** fields, as required:

   a. Select:

      Multithreading Mode if you want this domain to use multithreading features (if the CPUs used by the domain support the multithreading mode)
      or
      Monothreading Mode if you do not want this domain to use multithreading features or if the CPUs used by the domain do not support the multithreading mode.

   b. Select **Enable PCI gap above 4 GB** if the PCI boards used by the domain require more than 4 GB PCI gap space.

☞ **Note:**
Please read the documentation delivered with your PCI boards for details about features and requirements.

   c. Select a system **Serial Number** from the scroll–down list and add a two digit extension to automatically create the **Licensing Number** to be used by protected applications running on this domain.

   d. Select **Substitute Mode** if you want to substitute the physical system serial number with the logical licensing number for optimum flexibility.

Note:
Please read the documentation delivered with your application for details about licensing requirements.

e. If requested by your Customer Service Engineer, select **Force Halt on Machine Check Reset** to halt the domain when a machine check error occurs.

Note:
When this box is NOT checked, the domain will automatically reset when a machine check error occurs.

5. Click **OK**. The new identity appears in the **Identities List** page and can be applied to a hardware partition via the **Domain Configuration Scheme** wizard.

Editing a Domain Identity

To modify domain identity settings, management parameters and/or description:

1. Assess your configuration requirements. See *Assessing Configuration Requirements*, on page 5-31.
2. Click **Configuration Tasks** → **Domains** → **Identities** in the PAM tree to open the **Identities Management** page. See Figure 148 above.
3. Select the required identity from the list.
4. Click **Edit** in the toolbar. The **Edit an Identity** dialog opens, allowing you to modify domain identity settings, management parameters and/or description. See Figure 149 above.
5. Change settings as required.
6. Click **OK** to confirm the modification.

Copying a Domain Identity

To copy a domain identity:

1. Click **Configuration Tasks** → **Domains** → **Identities** in the PAM tree to open the **Identities Management** page. See Figure 148 above.
2. Select the required identity from the list.
3. Click **Copy** in the toolbar. The **Copy Identity** dialog opens.
4. Enter the name for the new identity and click **OK** to confirm.
5. The new identity appears in the **Identities List** page and can be applied to a hardware partition via the **Domain Configuration Scheme** wizard.

Deleting a Domain Identity

Important:
If a Domain Identity is used in a Scheme, it cannot be deleted.

To delete a domain identity:

1. Click **Configuration Tasks** → **Domains** → **Identities** in the PAM tree to open the **Identities List** page. See Figure 148 above.
2. Select the required identity from the list.
3. Click **Delete** in the toolbar and click **OK** to confirm. The selected identity is removed from the **Identities List**.

Managing Logical Units (Servers Connected to a SAN)

Important:
Certain features described below are only available if you are connected to a Storage Area Network (SAN).
Please contact your Bull Sales Representative for sales information.

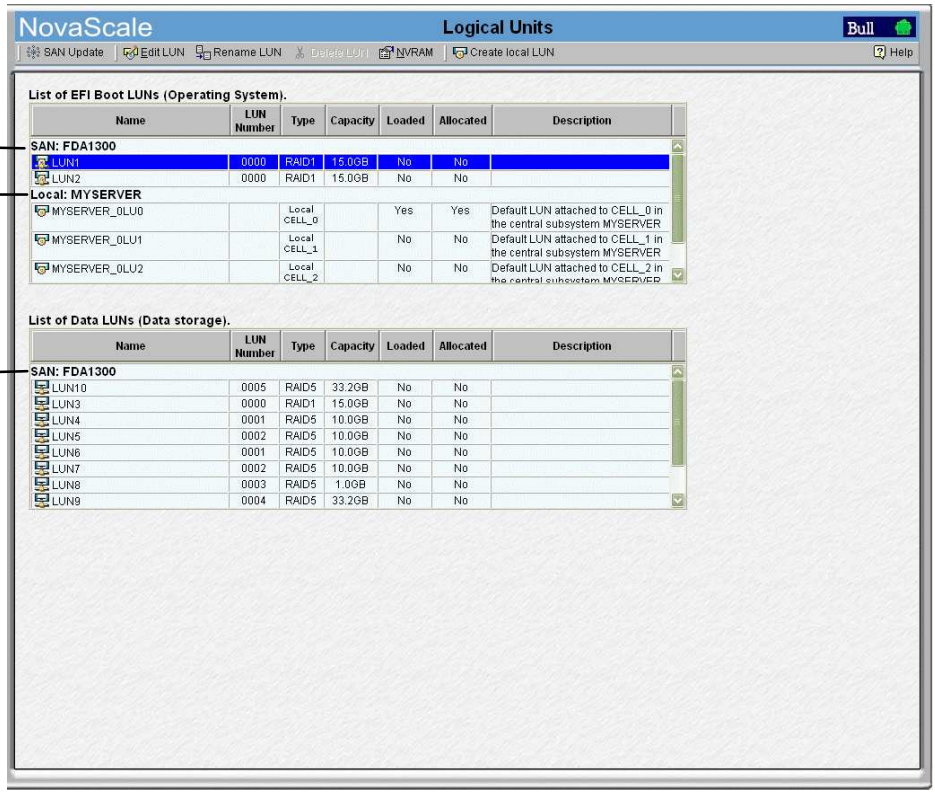
What You Can Do

- Update SAN LUN Lists
- Create Local LUNs
- Edit LUNs
- Rename LUNs
- Delete LUNs
- Clear, Load, Save NVRAM Variables

Note:
EFI LUNs and Data LUNs must be created from the utility delivered with the storage subsystem. See *Configuring System and Data Disks*, on page 5-4.

To open the Logical Units management page:

1. Click **Configuration Tasks** → **Domains** → **LUNs** in the PAM tree.



1 SAN storage subystem **2** Local storage subsystem

☞ **Notes:**

- **EFI Boot LUNs**, on which Operating Systems are installed, are listed at the top of the pane.
- **Data LUNs**, on which data can be stored, are listed at the bottom of the pane.

Command Bar	
SAN Update	Update the lists of SAN LUNs.
Edit LUN	Modify the LUN name, description, and change a Data LUN into an EFI LUN and vice–versa.
Rename LUN	Modify the LUN name.
NVRAM	Clear, load and save EFI Boot LUN NVRAM variables.
Create Local LUN	Create a new local LUN.
Delete Local LUN	Delete a non–allocated local LUN.
LUN Lists	
Name	LUN name.
LUN Number	Number allocated to the LUN.
Type	RAID configuration type. RAID1 is recommended for EFI LUNs and RAID5 for Data LUNs.
Capacity	LUN storage capacity.
Loaded	**Yes** LUN used by a currently loaded domain. **No** LUN not used by a currently loaded domain.
Allocated	**Yes** LUN allocated to a domain within a Domain Configuration Scheme. **No** LUN not allocated to a domain within a Domain Configuration Scheme.
Description	Description, indicating LUN location (Central Subsystem name and Cell and/or storage subsystem name).

Figure 150. Logical Units page – servers connected to a SAN

Updating SAN LUN Lists

Important:
Reserved for systems connected to a Storage Area Network (SAN).
Please contact your Bull Sales Representative for sales information.

When new LUNs are added to / removed from your Storage Area Network, they can be automatically added to / removed from the list of available LUNs by using the **PAM SAN Update** command, which allows you to update the lists of available LUNs on the SAN at any time.

Notes:

- This command **CANNOT** be used to update the lists of local LUNs.
- This command is automatically performed when a PAM session is launched on the PAP unit and when a disk subsystem change takes place.
- When a new LUN is found, PAM considers it as a Data LUN by default. If you want to change this LUN into an EFI Boot LUN, use **Edit LUN**.

To update the lists of available SAN LUNs:

1. Click **Configuration Tasks** → **Domains** → **LUNs** in the PAM tree to open the **Logical Units** page.
2. Click **SAN Update**. A confirmation dialog opens.
3. Click **Yes** to update the lists of available LUNs. The **SAN Update Progress Bar** is displayed.

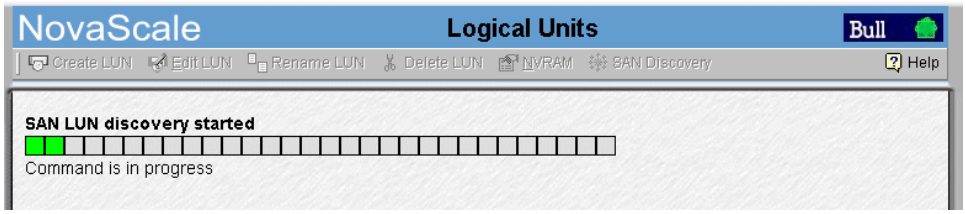


Figure 151. SAN Update progress bar

Once the process is complete, the LUN lists are updated to reflect configuration changes.

Creating Local LUNs

When you create a new LUN via the software delivered with your local storage subsystem, you must also declare this new LUN by using the **PAM Create Local LUN** command.

Note:
This command **CANNOT** be used to create new SAN LUNs.

To update the list of available local LUNs:

1. Click **Configuration Tasks** → **Domains** → **LUNs** in the PAM tree to open the **Logical Units** page.
2. Click **Create LUN** to open the **Create Local LUN** dialog.

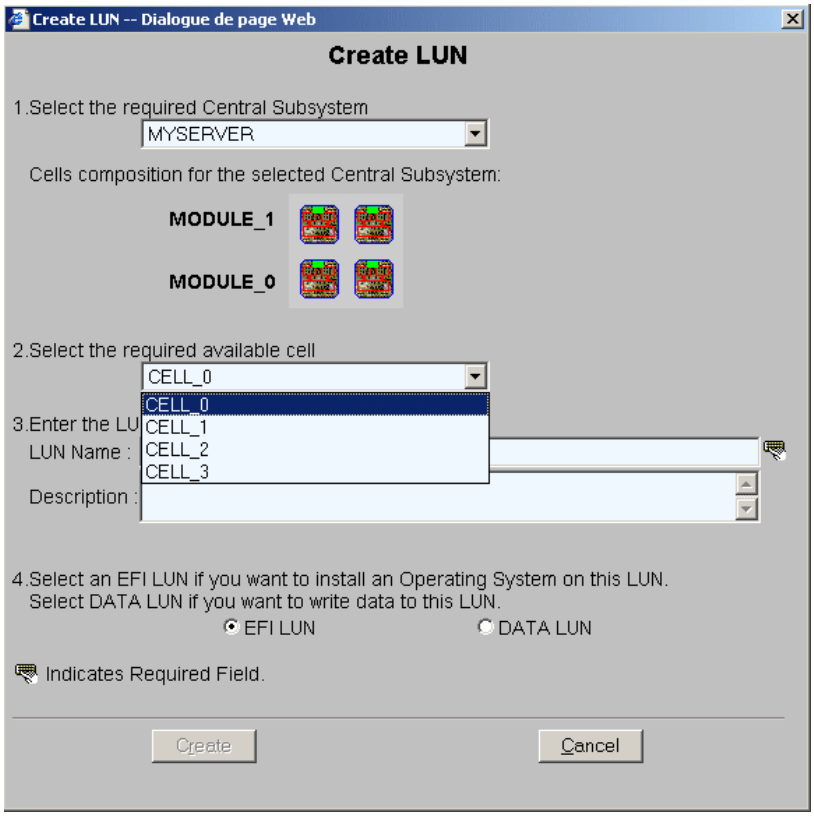


Figure 152. Create Local LUN dialog

3. Use the **Central Subsystem** drop–down menu to select the Central Subsystem to which the LUN is connected.
4. Use the **Available Cell** drop–down menu to select the cell to which the LUN is connected.
5. Enter the name given to the LUN in the **LUN Name** field with a brief description.
6. Select the **EFI LUN** or **DATA LUN** radio button, as required and click **Create**. The list of available local LUNs is updated.

Deleting LUNs

Notes:

- A LUN **CANNOT** be deleted if it is allocated to a Scheme.

To delete a LUN:

1. Click **Configuration Tasks** → **Domains** → **LUNs** in the PAM tree to open the **Logical Units** page.
2. Select the required LUN from the lists of available local LUNs and click **Delete LUN** to open the **Delete LUN** dialog.

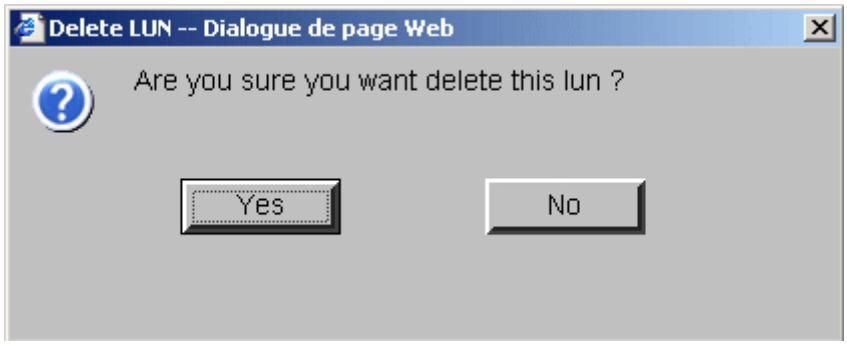


Figure 153. Delete LUN dialog

3. Click **Yes** to confirm. The LUN is removed from the list of available LUNs.

Editing LUNs

Important:
Reserved for systems connected to a Storage Area Network (SAN).
Please contact your Bull Sales Representative for sales information.

Notes:

- A LUN **CANNOT** be edited if it is allocated to a Scheme.
- The **NVRAM** button is **NOT ACCESSIBLE** if no NVRAM variables are available for the selected LUN.

If required, you can modify the EFI / Data LUN names, description, NVRAM variables, and/or change a Data LUN into an EFI LUN or vice–versa.

To edit a LUN:

1. Click **Configuration Tasks** → **Domains** → **LUNs** in the PAM tree to open the **Logical Units** page.
2. Select the LUN you want to modify from the lists of available LUNs and click **Edit LUN** to open the **Edit LUN** dialog.

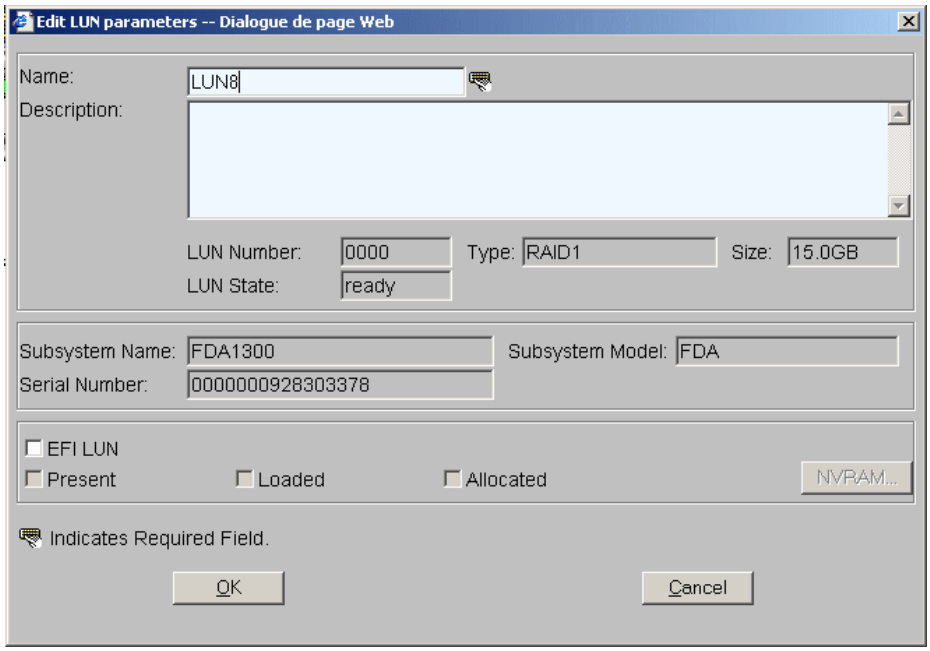


Figure 154. Edit LUN dialog

3. Modify LUN parameters as required:
   a. Enter a new name in the **Name** field if you want to change the LUN name.
   b. Enter a new description in the **Description** field if you want to change the LUN description.
   c. Select the **EFI LUN** checkbox if you want to change a Data LUN into an EFI LUN.
   d. Deselect the **EFI LUN** checkbox if you want to change an EFI LUN into a Data LUN.
4. Click **OK** to apply changes.

Renaming LUNs

Important:
Reserved for systems connected to a Storage Area Network (SAN).
Please contact your Bull Sales Representative for sales information.

Note:
A LUN **CANNOT** be renamed if it is allocated to a Scheme.

To rename a LUN:

1. Click **Configuration Tasks** → **Domains** → **LUNs** in the PAM tree to open the **Logical Units** page.
2. Select the LUN you want to rename from the lists of available LUNs and click **Rename LUN** to open the **Rename LUN** dialog.

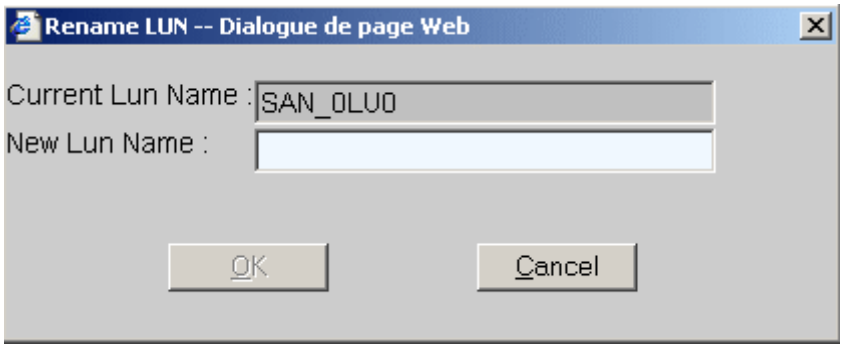


Figure 155. Rename LUN dialog

3. Enter the new name and click **OK** to apply the change.

Clearing, Loading, Saving NVRAM Variables

NVRAM variables are available for each EFI boot LUN. According to requirements, these variables can be cleared, saved and/or loaded.

Note:
NVRAM variables can only be saved when the corresponding domain is active.

To clear, save and/or load NVRAM variables:

1. Click **Configuration Tasks** → **Domains** → **LUNs** in the PAM tree to open the **Logical Units** page.
2. Select the required LUN from the list of available EFI boot LUNs and click **NVRAM**. The **NVRAM Variables** dialog opens:
   a. Click **Clear** to clear displayed NVRAM variables. When requested, click **OK** to confirm.
   b. Click **Save** to save NVRAM variables for the selected LUN (currently used by an active domain). When requested, enter the name of the file to which NVRAM variables are to be saved. The NVRAM variables file is stored in the PAM SiteData directory.
   c. Click **Load** to load previously saved NVRAM variables from the PAM SiteData directory.

Managing Logical Units (Servers Not Connected to a SAN)

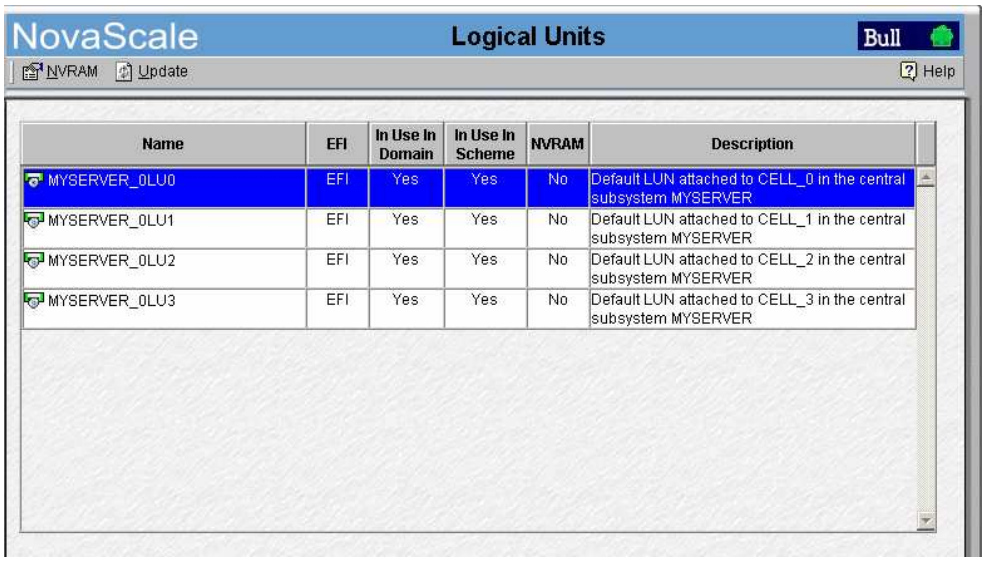
Your server is delivered with default EFI Boot LUNs. You can use the software delivered with your storage subsystem to define data LUNs.

What You Can Do

- Clear, Load, Save NVRAM Variables
- Update the Local LUN Lists

To open the Logical Units management page:

1. Click **Configuration Tasks** → **Domains** → **LUNs** in the PAM tree.



Name	Default LUN name
EFI	**EFI** This LUN is a boot LUN. **DATA** This LUN is a data LUN.
In Use in Domain	**Yes** This LUN is used by a domain currently loaded in the Domain Manager Control pane. **No** This LUN is not used by a domain currently loaded in the Domain Manager Control pane.
In Use in Scheme	**Yes** This LUN has been allocated to a domain within a Domain Configuration Scheme. **No** This LUN has not been allocated to a domain within a Domain Configuration Scheme.
NVRAM	**Yes** NVRAM variables have been saved for this LUN. **No** NVRAM variables have not been saved for this LUN.
Description	Default description, indicating LUN location (Central Subsystem name and Cell).

Figure 156. Logical Units page – servers not connected to a SAN

Updating the Local LUN Lists

The lists of available local LUNs are automatically created when a Central Subsystem is declared and/or added. You can update the lists of available local LUNs at any time to reflect configuration changes.

To update the local LUN lists:

1. Click **Configuration Tasks** → **Domains** → **LUNs** in the PAM tree to open the **Logical Units** page.
2. Click **Update**. When requested, click **OK** to confirm. The new LUN lists are displayed in the **Logical Units** page.

Clearing, Loading, Saving NVRAM Variables

NVRAM variables are available for each EFI boot LUN. According to requirements, these variables can be cleared, saved and/or loaded.

1. Click **Configuration Tasks** → **Domains** → **LUNs** in the PAM tree to open the **Logical Units** page.
2. Select the required LUN from the list of available EFI Boot LUNs and click **NVRAM**. The **NVRAM Variables** dialog opens.
   a. Click **Clear** to clear displayed NVRAM variables. When requested, click **OK** to confirm.
   b. Click **Save** to save NVRAM variables for the selected EFI Boot LUN (currently used by an active domain). When requested, enter the name of the file to which NVRAM variables are to be saved. The NVRAM variables file is stored in the PAM SiteData directory.
   c. Click **Load** to load previously saved NVRAM variables from the PAM SiteData directory.

Checking and Updating Fibre Channel HBA World Wide Names

To control LUN access, Bull NovaScale Servers use LUN masking at Host Bus Adapter (HBA) driver level. Each Fibre Channel HBA driver contains a masking utility using the World Wide Name (WWN) to limit LUN access. As a result, users are only aware of the LUNs to which they have access.

Whenever you add, change or move a Fibre Channel HBA, you must update the corresponding World Wide Name (WWN) parameters via the PAM interface.

To update an HBA World Wide Name:

1. Click **Configuration Tasks** → **Domains** → **HBAs** in the PAM tree.
2. Expand the required Central Subsystem node down to the IOB housing the HBA concerned.
3. Select the IOB. The **HBA Worldwide Name** page opens.

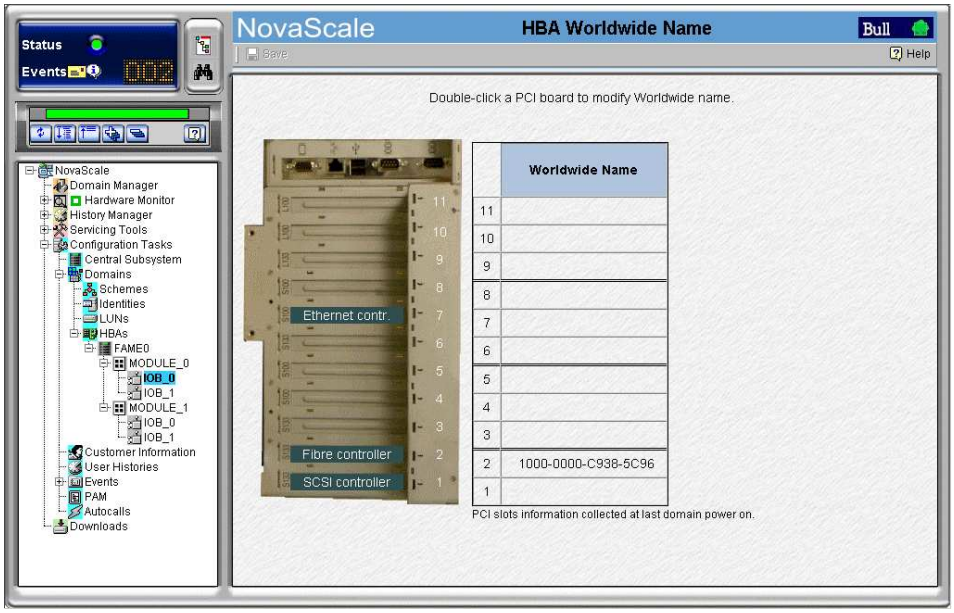


Figure 157. HBA Worldwide Name page

4. Double–click the required PCI board to update the WWN. The **Modify PCI HBA Worldwide Name** dialog opens.

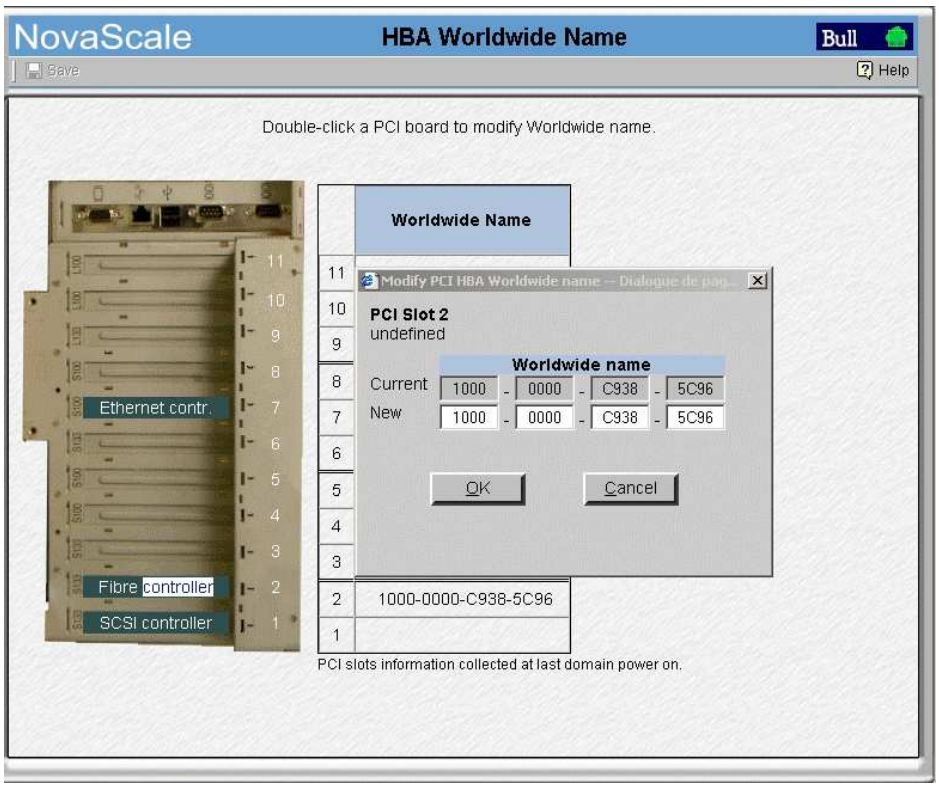


Figure 158. Modify PCI HBA Worldwide Name dialog

5. Enter the WWN supplied with the HBA and click **Save** to apply changes.

Limiting Access to Hardware Resources

You can functionally limit access to certain hardware elements. Locked elements can no longer be accessed by the current domain, but are still physically available for access by other domains. Previously locked elements can be unlocked so that they can be accessed by the domain.

Notes:

- The domain must be **INACTIVE** before configuration changes can be made.
- Hardware locking / unlocking is only taken into account at the next domain power ON.
- Hardware components to be functionally included (unlocked) in the domain at the next domain power ON are marked with a yellow icon in the **Lock Request** column in the **Domain Hardware Details** page.
- Hardware components to be functionally excluded (locked) from the domain at the next domain power ON are marked with a red / yellow icon in the **Lock Request** column in the **Domain Hardware Details** page.

See *Viewing Domain Configuration, Resources and Status*, on page 3-32.

The following domain hardware elements can be locked / unlocked:

Table 42. Hardware locking options

To lock / unlock a domain hardware element:

1. Open the **Lock Domain Hardware Resources** dialog:
   a. If you are configuring a domain scheme:

      From the **Scheme Management** dialog, select the required domain and click **Lock Hardware**.

   b. If you want to edit a previously defined domain scheme:

      . From the Customer Administrator PAM tree, click **Configuration Tasks** → **Domains** → **Schemes** → **Edit**.

      . Select the required domain and click **Lock Hardware**

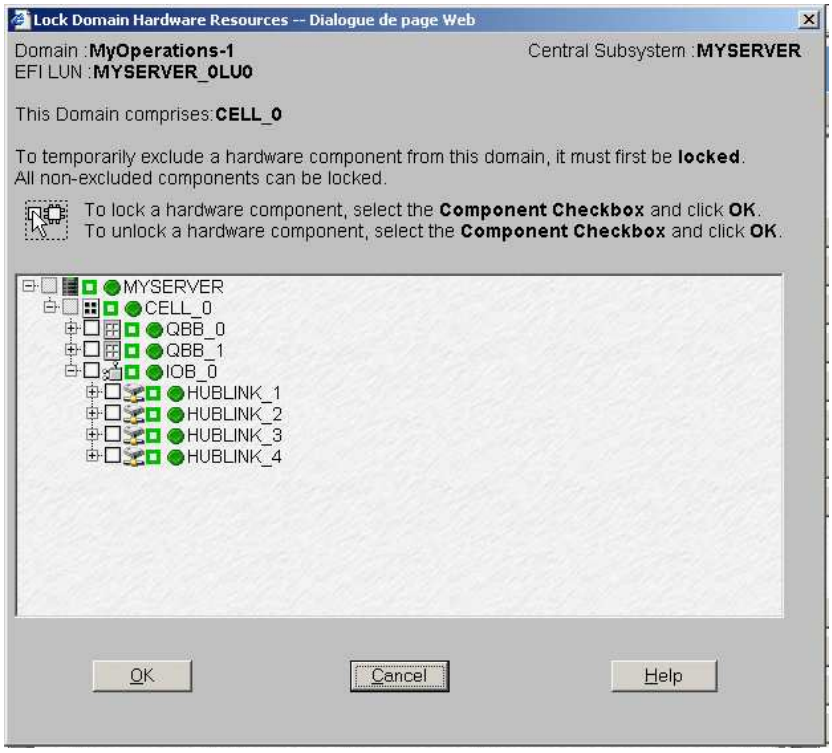


Figure 159. Lock domain hardware resources dialog

2. Expand the component tree to view the hardware element you want to lock / unlock.
3. Select the corresponding checkbox to lock the element or deselect to unlock a previously locked element.

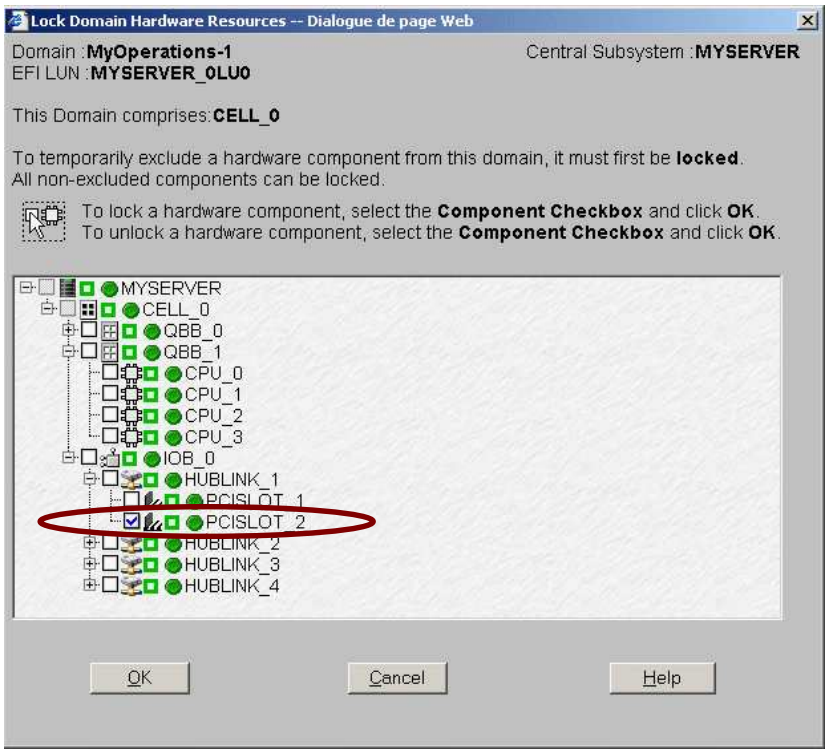


Figure 160. Lock domain hardware resources dialog – PCI slot selected

4. Click **OK** → **Apply** to return to the **Schemes Management** pane.

Creating a Mono–Domain Scheme Using All Server Resources

Notes:

- A domain configuration scheme can include more than one Central Subsystems. If you have more than one Bull NovaScale Server, see *Configuring and Managing Extended Systems*, on page 5-108.
- For more information about scheme configuration options, refer to:
  - *Assessing Configuration Requirements*, on page 5-31
  - *Creating a Domain Configuration Scheme*, on page 5-33
  - *Creating a Domain Identity*, on page 5-48

The configuration criteria set out in the following tables is used to illustrate this example:

NovaScale 6080/6160 Server

Scheme	
Name	MyBusinessScheme
Description	Mono–domain, Cells 0 & 1, Boot 0Lun0, MyBusiness–1
Central Subsystem(s)	MyServer
Number of domains	1
Domain size	2 cells: Cell0 & Cell 1
EFI boot LUNs	SAN: FDA1300 LUN1
Data LUNs *	SAN: FDA 1300 LUN10, LUN6
Fibre channel hosts *	Primary Link: Cell_0: Module_0/IOB_0/PCISLOT_1 Secondary Link: Cell_1: Module_0/IOB_1/PCISLOT_1
IO resource location	0IOB0 mandatory, 0IOB1 optional
Resource access	All resources unlocked
Domain Identity	
Name	MyBusiness–1
Description	Time zone: Central America
Operating System	Windows
Domain network name	MyBusiness–1Net
Domain IP address	123.123.12.1
Domain URL	http://www.MyBusiness–1Web.com
Domain threading mode	Monothreading
HMMIO space	Disabled
Licensing number	XAN–YYY–12345/11
Substitute mode	Disabled
Halt on machine check reset	Disabled

* Reserved for systems connected to a Storage Area Network (SAN).

Table 43. Scheme configuration criteria – example 1 – mono–module server

NovaScale 6320 Server

Scheme	
Name	MyBusinessScheme
Description	Mono–domain, Cells 0, 1, 2 & 3, Boot 0Lun0, MyBusiness–1
Central Subsystem(s)	MyServer
Number of domains	1
Domain size	4 cells: Cell0, Cell1, Cell2 & Cell 3
EFI boot LUNs	SAN: FDA1300 LUN1
Data LUNs *	SAN: FDA 1300 LUN10, LUN6
Fibre channel hosts *	Primary Link: Cell_0: Module_0/IOB_0/PCISLOT_1 Secondary Link: Cell_3: Module_1/IOB_1/PCISLOT_1
IO resource location	0IOB0 mandatory, 0IOB1, 1IOB0, & 1IOB1 optional
Resource access	All resources unlocked
Domain Identity	
Name	MyBusiness–1
Description	Time zone: Central America, Boot path: EFI 0Lun0
Operating System	Windows
Domain network name	MyBusiness–1Net
Domain IP address	123.123.12.1
Domain URL	http://www.MyBusiness–1Web.com
Domain threading mode	Monothreading
HMMIO space	Disabled
Licensing number	XAN–YYY–12345/11
Substitute mode	Disabled
Halt on machine check reset	Disabled

* Reserved for systems connected to a Storage Area Network (SAN).

Table 44. Scheme configuration criteria – example 1 – bi–module server

To create a mono–domain scheme using all server resources:

1. Check that the required hardware resources are available (at least one IOB and one QBB are required for each server domain) and that the domain Operating System supports the required hardware resources (CPUs, DIMMs, ...).
2. From the Customer Administrator PAM tree, click **Configuration Tasks** → **Domains** → **Schemes** to open the **Schemes Management** pane.
3. Click **New** to open the **Scheme Creation** dialog.
4. Complete the **Scheme** and **Description** fields.

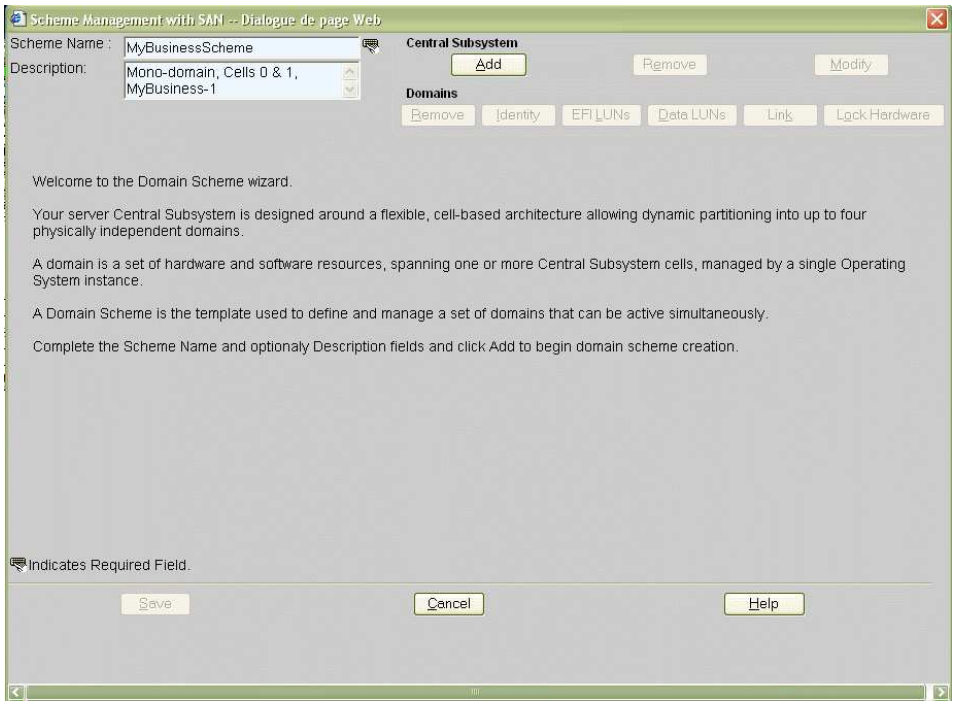
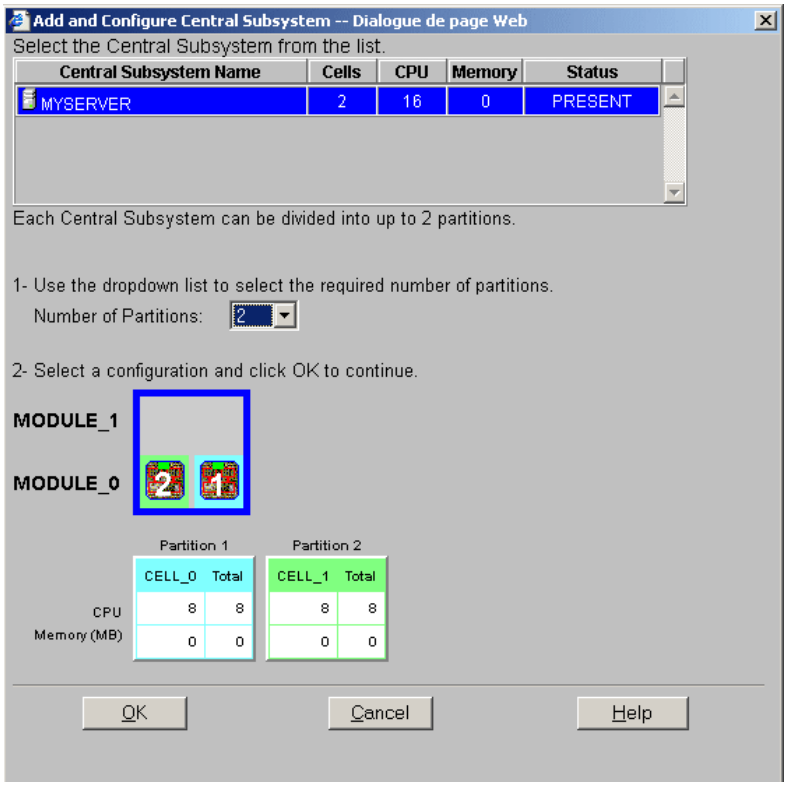


Figure 161. Scheme creation dialog – example 1

5. Click **Central Subsystem** → **Add** to select the Central Subsystem to be used by the domain configuration scheme. The **Central Subsystem Configuration** dialog opens.

NovaScale 6080/6160 Server



NovaScale 6320 Server

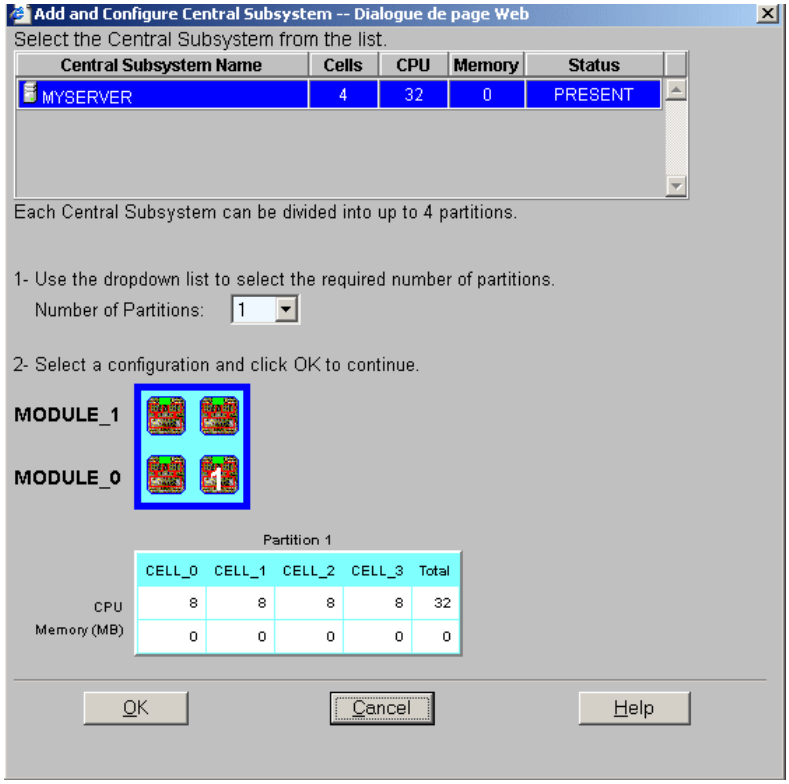
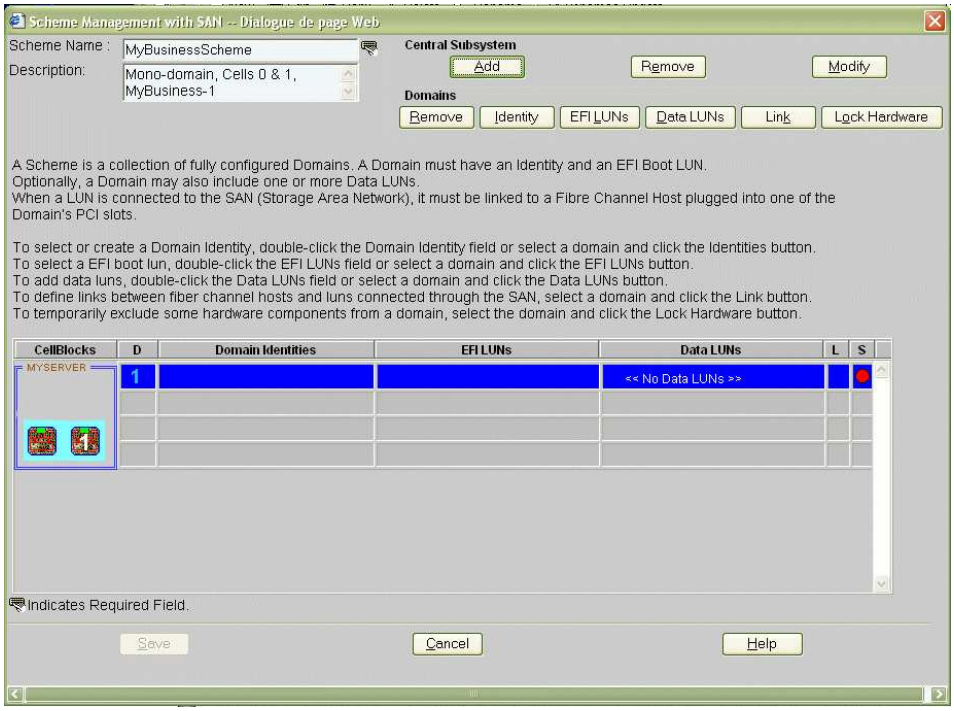


Figure 162. Central Subsystem configuration dialog – example 1

6. Check that the required Central Subsystem is highlighted and select **1** in the **Number of Parts** dropdown list.
7. Select the required partition configuration and click **OK** to return to the **Scheme Management** dialog.

   The **Status** icon is red because a **Domain Identity** and an **EFI LUN** are required to complete domain configuration.

NovaScale 6080/6160 Server



NovaScale 6320 Server

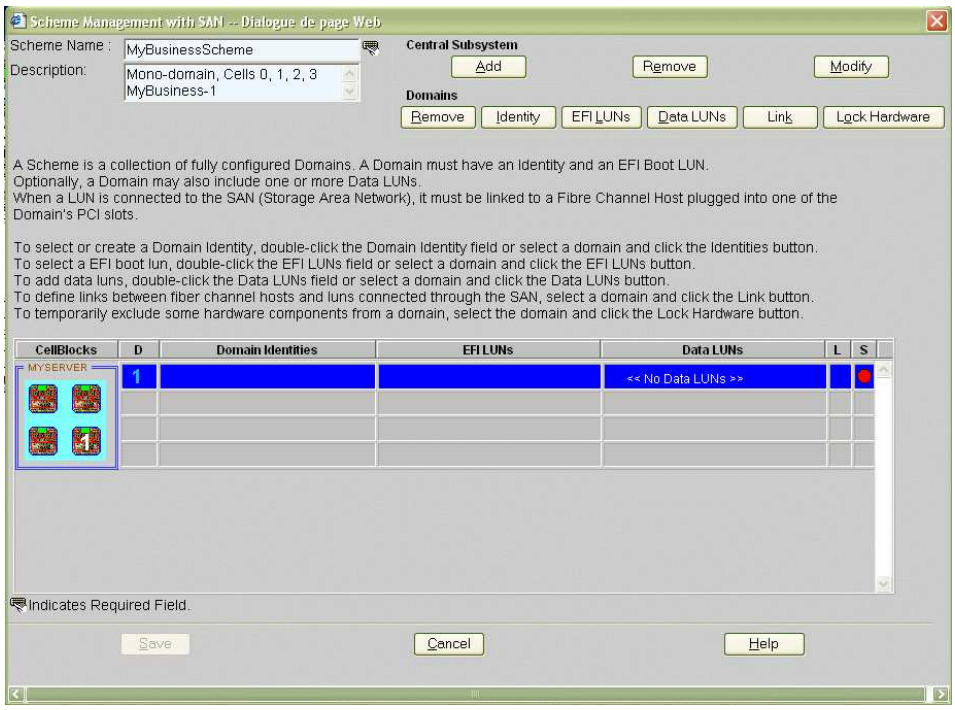


Figure 163. Scheme Management dialog – example 1

8. Double–click the empty **D1 Identities** field. The **Identities List** dialog opens.

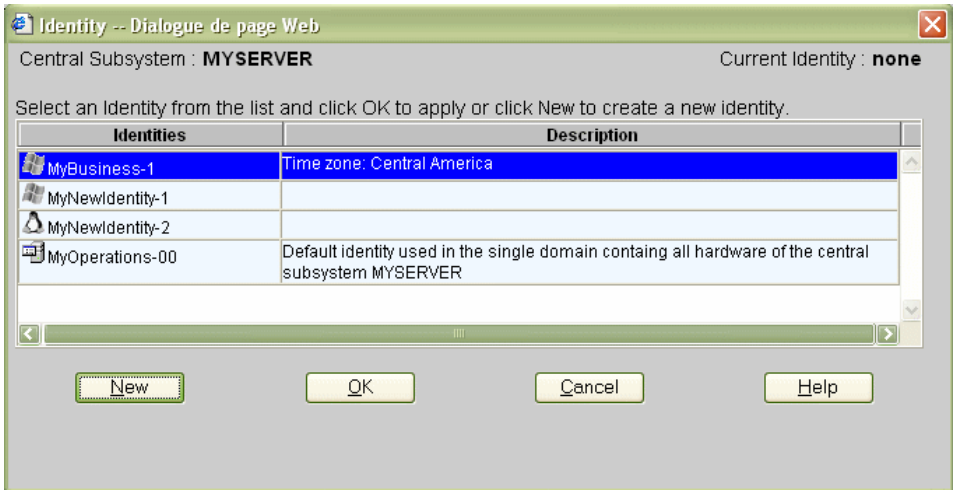


Figure 164. Identities list dialog – example 1

9. If the required identity is in the list, go to Step 12.
   If you want to create a new identity for this domain, click **New** to open the **Create New Identity** dialog. See *Creating a Domain Identity*, on page 5-47 for details.

10. Complete the **Name**, **Description**, **Domain Settings**, **Management Parameters**, **Multithreading Mode**, **HMMIO Space**, **Licensing Number** and **Machine Check** fields.

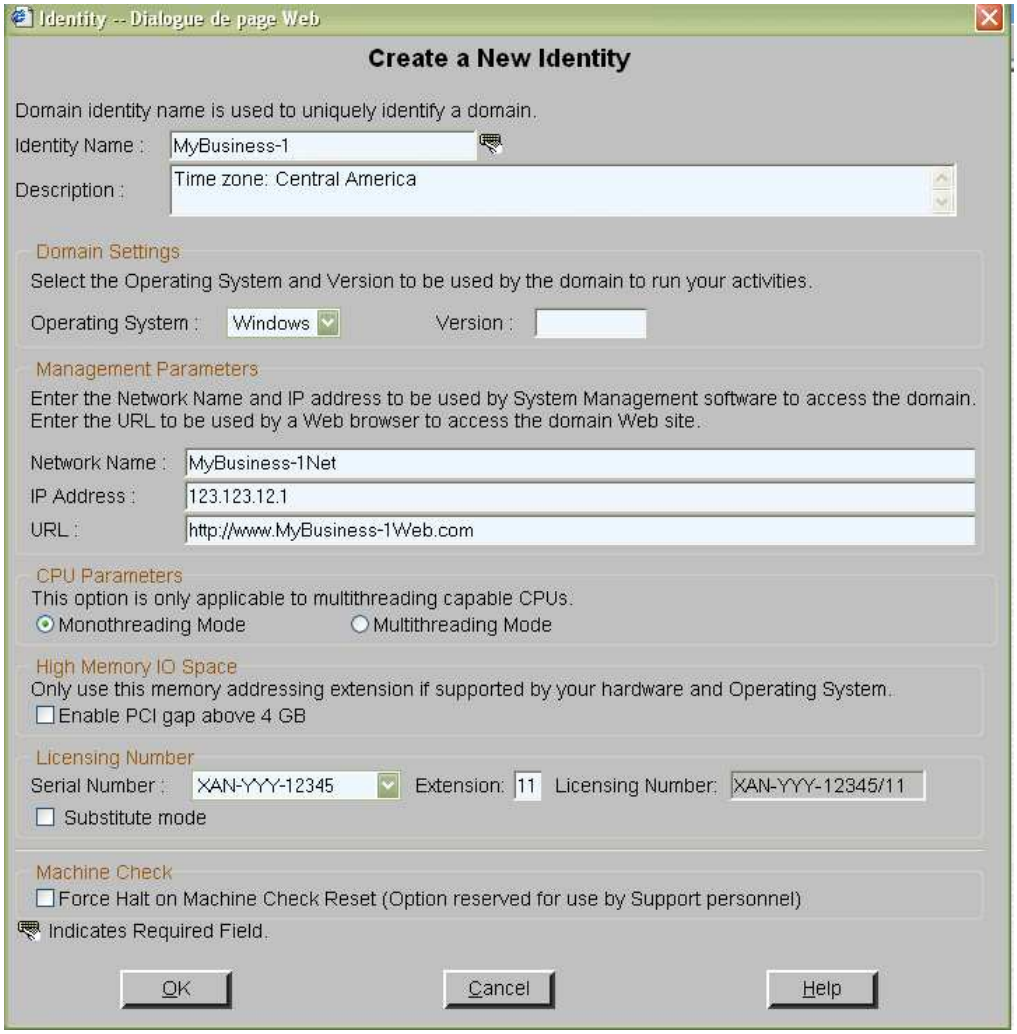


Figure 165. Create new identity dialog – example 1

11. Click **OK**. The new identity appears in the **Identities List** dialog.

12. Select the required identity from the list of available identities and click **OK** to return to the **Scheme Management** dialog. The selected identity is now displayed in the **Domain Identities** field.

13. Double–click the **EFI LUNs** field. The **Select EFI LUN** dialog opens, allowing you to choose the required EFI Boot LUN from the list of available LUNs.

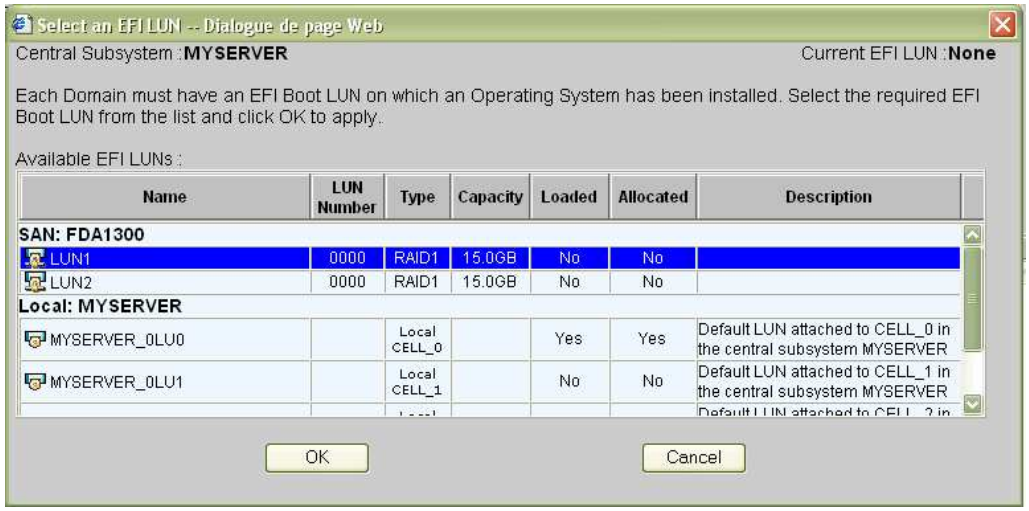


Figure 166. Select EFI LUN dialog – example 1

14. Select the required EFI Boot LUN from the list of available LUNs and click **OK** to return to the **Scheme Management** dialog. The selected LUN is now displayed in the **EFI LUNs** field.

    As the selected LUN is a SAN LUN, the **Status** icon remains red and the **No Link** icon  appears.

15. Double–click the **Data LUNs** field. The **Select Data LUN** dialog opens, allowing you to choose the required Data LUNs from the list of available LUNs.

16. Select the required Data LUNs from the list of available LUNs and click **Add** to move the selected Data LUNs to the **Data LUNs selected** list.

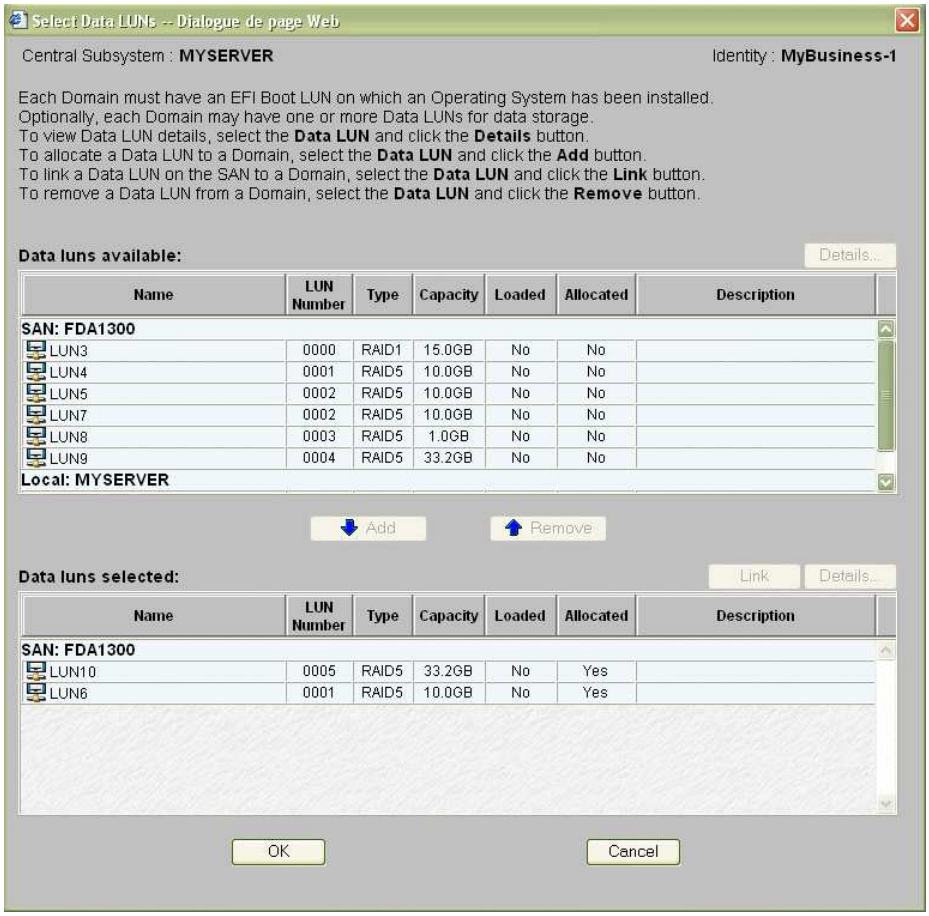


Figure 167. Select Data LUN dialog – example 1

17. Click **OK** to return to the **Scheme Management** dialog. **Data LUN set** is now displayed in the **Data LUNs** field.

    The **Status** icon remains red and the **No Link** icon is displayed. You must now link the selected EFI and Data LUNs to the Fibre Channel Host you want to use to access these LUNs.

18. Click **Domains** → **Link** to open the **Link LUNs to HBA** dialog.

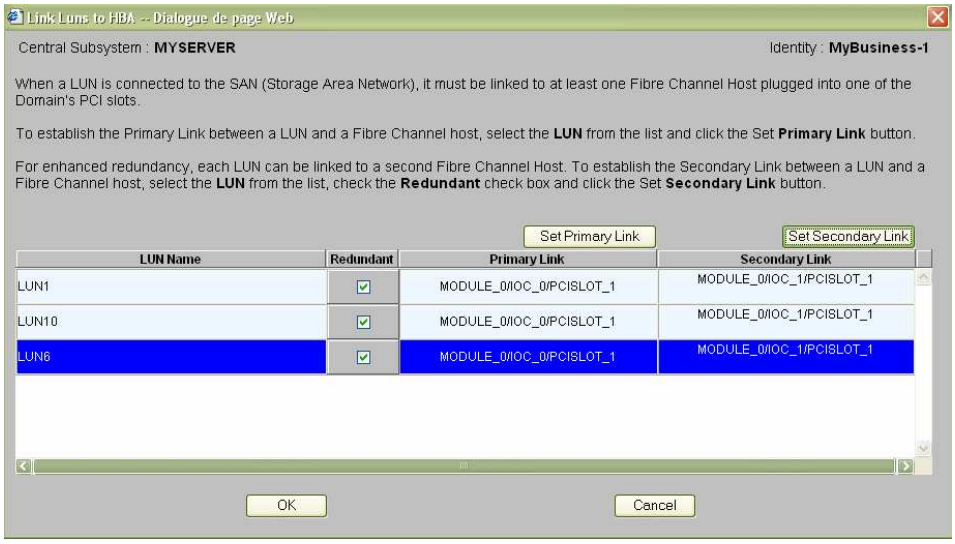


Figure 168. Link LUN to HBA dialog – example 1

19. Select the first LUN in the list and select the **Redundant** mode.
You are informed that dedicated software is required to enable this mode and you are requested to confirm your choice.
Click **OK** to confirm.

20. Click **Set Primary Link** to define the main access path to the SAN. The **Select HBA** dialog opens, allowing you to select the domain PCI slot you want to use to access the LUN.

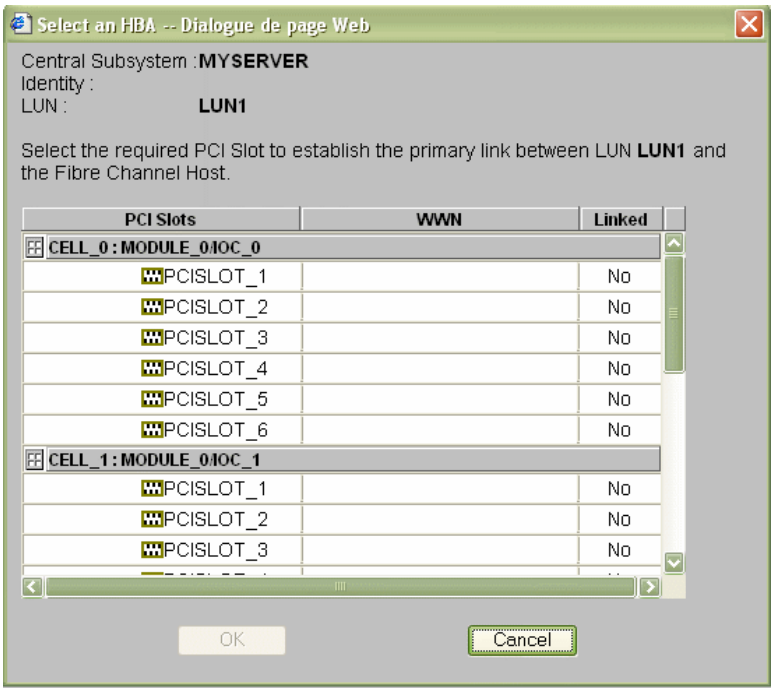


Figure 169. Select HBA dialog – example 1

21. Select the required PCI slot and click **OK**. The primary link is now set.

22. Click **Set Secondary Link** to define the backup access path to the SAN.

23. Select the required PCI slot and click **OK**. The secondary link is now set.

24. Repeat Steps 19 to 23 for each LUN in the list and click **OK** → **Apply** to return to the **Scheme Management** dialog. The **Status** icon turns green and the **Linked** icon  appears.
25. Click **Save**. The domain configuration scheme is now available for domain management.

Creating a Mono–Domain Scheme Using a Selection of Server Resources

Notes:

- A domain configuration scheme can include more than one Central Subsystems. If you have more than one Bull NovaScale Server, see *Configuring and Managing Extended Systems*, on page 5-108.
- For more information about scheme and identity configuration options, refer to:
  - *Assessing Configuration Requirements*, on page 5-31
  - *Creating a Domain Configuration Scheme*, on page 5-33
  - *Creating a Domain Identity*, on page 5-48

The configuration criteria set out in the following tables is used to illustrate this example:

NovaScale 6080/6160 Server

Scheme	
Name	MyOffpeakProdScheme
Description	Mono–domain, Cell 1, MyOffpeakProd
Central Subsystem(s)	MyServer
Number of domains	1
Domain size	1 cell: Cell 1
EFI boot LUNs	SAN: FDA1300 LUN1
Data LUNs *	SAN: FDA 1300 LUN10, LUN6
Fibre channel hosts *	Primary Link: Cell_1: Module_0/IOB_1/PCISLOT_1
IO resource location	0IOB1
Resource access	All resources unlocked
Domain Identity	
Name	MyOffpeakProd
Description	Time zone: Paris
Operating System	Linux
Domain network name	MyOffpeakProdNet
Domain IP address	124.124.1.0
Domain URL	http://www.MyOffpeakProdWeb.com
Domain threading mode	Monothreading
HMMIO space	Disabled
Licensing number	XAN–YYY–12345/12
Substitute mode	Enabled
Halt on machine check reset	Disabled

* Reserved for systems connected to a Storage Area Network (SAN).

Table 45. Scheme configuration criteria – example 2 – mono–module server

NovaScale 6320 Server

Scheme	
Name	MyOffpeakProdScheme
Description	Mono–domain, Cell 1, Boot 0Lun1, MyOffpeakProd
Central Subsystem(s)	MyServer
Number of domains	1
Domain size	1 cell: Cell 1
EFI boot LUNs	SAN: FDA1300 LUN1
Data LUNs *	SAN: FDA 1300 LUN10, LUN6
Fibre channel hosts *	Primary Link: Cell_1: Module_0/IOB_1/PCISLOT_1
IO resource location	0IOB1
Resource access	All resources unlocked
Domain Identity	
Name	MyOffpeakProd
Description	Time zone: Paris, Boot path: EFI 0Lun1
Operating System	Linux
Domain network name	MyOffpeakProdNet
Domain IP address	124.124.1.0
Domain URL	http://www.MyOffpeakProdWeb.com
Domain threading mode	Monothreading
HMMIO space	Disabled
Licensing number	XAN–YYY–12345/12
Substitute mode	Enabled
Halt on machine check reset	Disabled

* Reserved for systems connected to a Storage Area Network (SAN).

Table 46. Scheme configuration criteria – example 2 – bi–module server

To create a mono–domain scheme using a part of server resources:

1. Check that the required hardware resources are available (at least one IOB and one QBB are required for each server domain) and that the domain Operating System supports the required hardware resources (CPUs, DIMMs, ...).
2. From the Customer Administrator PAM tree, click **Configuration Tasks** → **Domains** → **Schemes** to open the **Schemes Management** pane.
3. Click **New** to open the **Scheme Creation** dialog.
4. Complete the **Scheme** and **Description** fields.

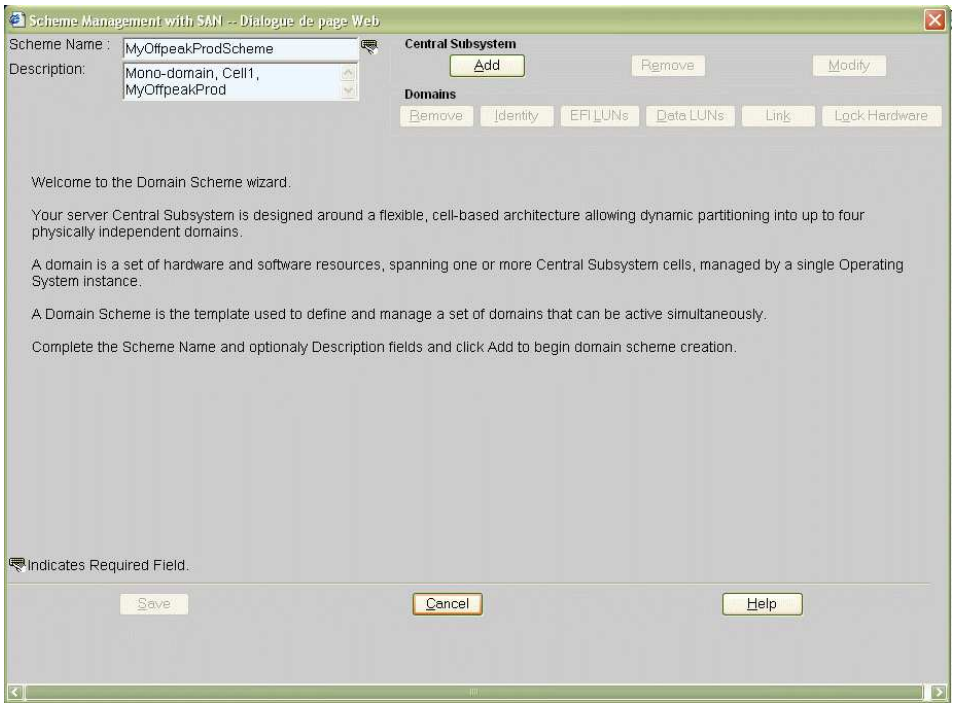
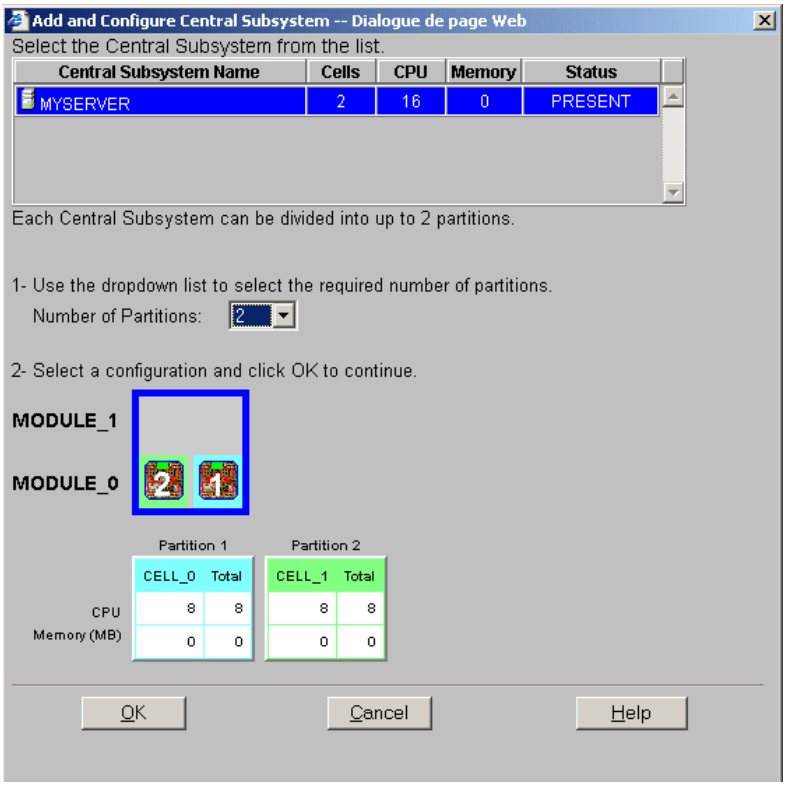


Figure 170. Scheme creation dialog – example 2

5. Click **Central Subsystem** → **Add** to select the Central Subsystem to be used by the domain configuration scheme. The **Central Subsystem Configuration** dialog opens.

NovaScale 6080/6160 Server



NovaScale 6320 Server

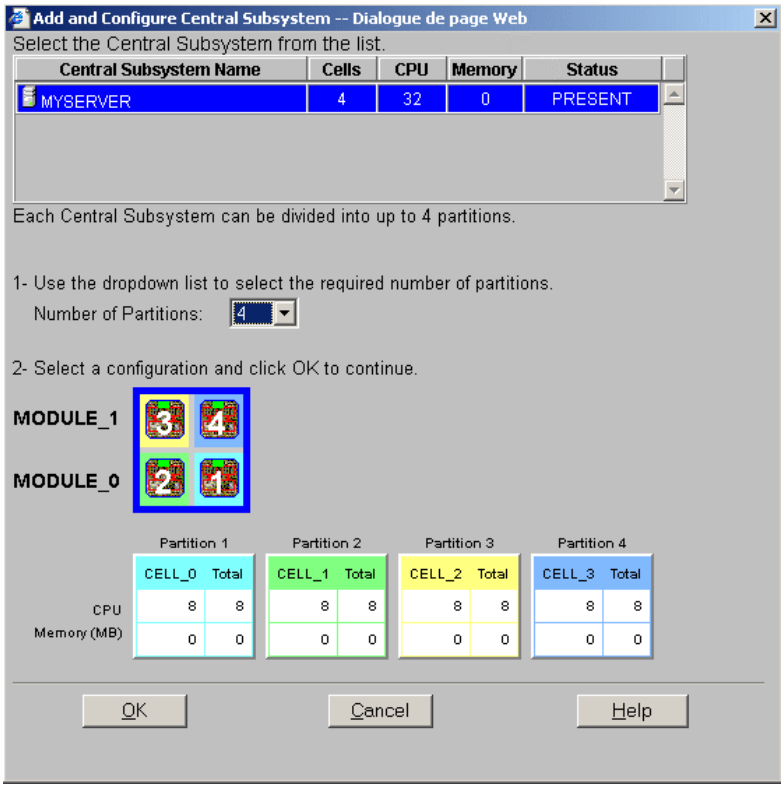
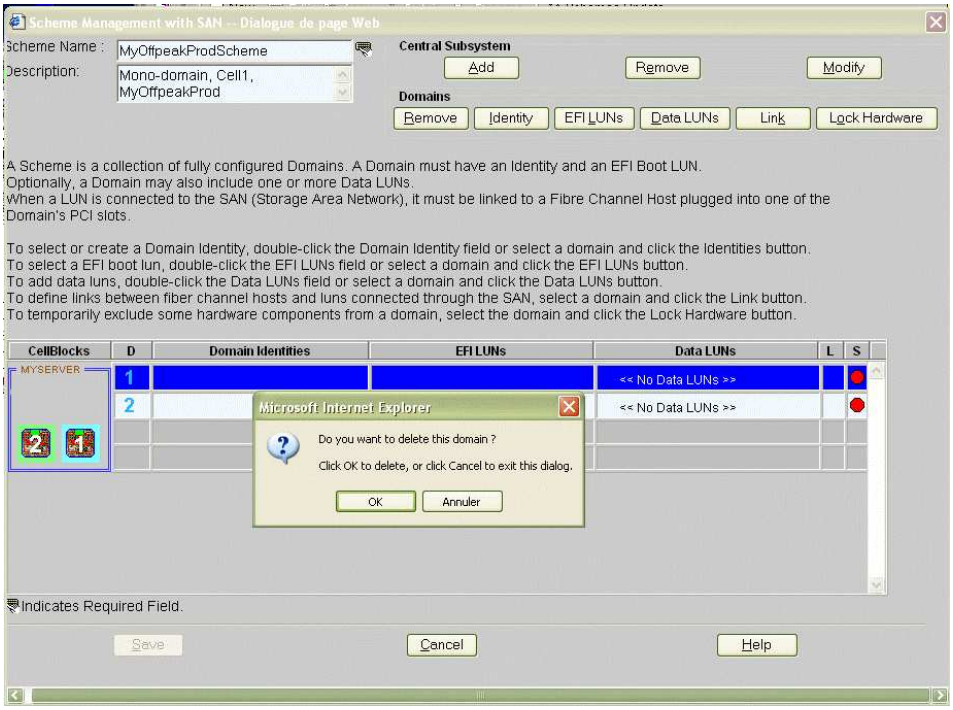


Figure 171. Central Subsystem configuration dialog – example 2

6. Check that the required Central Subsystem is highlighted and select **2** (mono–module server) or **4** (bi–module server) in the **Number of Parts** dropdown list.
7. Select the required partition configuration and click **OK** to return to the **Scheme Management** dialog.
8. As you want this scheme to only use Cell 1, you must remove the domains using the other cells. Hover the mouse over the cells represented in the **CellBlocks** diagram to identify the domain using Cell 1. **D2** is using Cell 1.

9. Click **D1** → **Domains** → **Remove** and click **OK** to remove the unwanted domain from the scheme.

NovaScale 6080/6160 Server



NovaScale 6320 Server

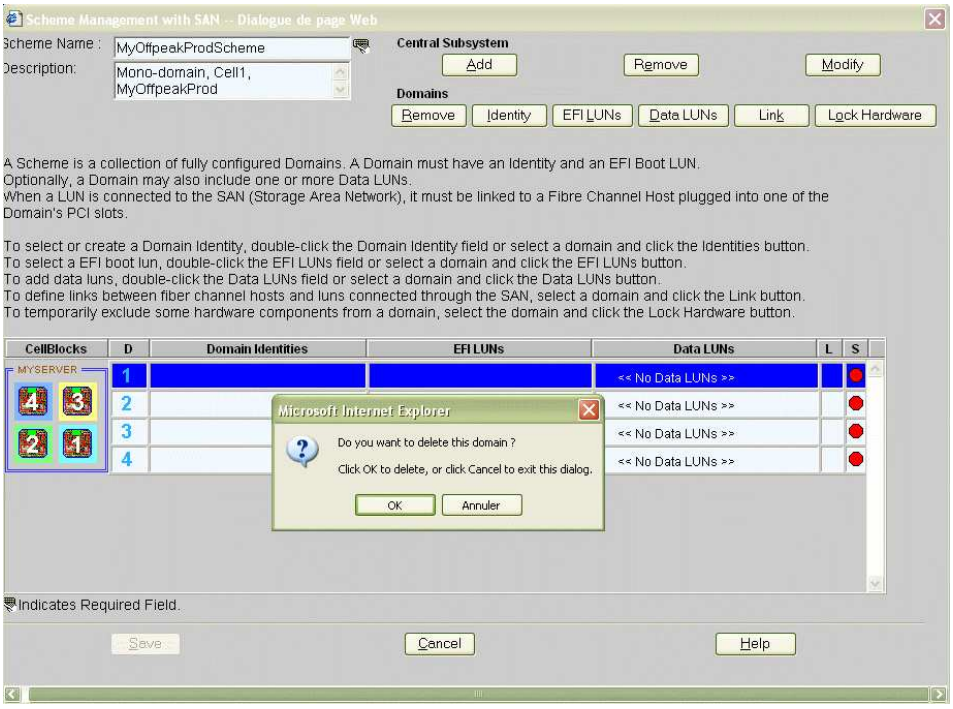


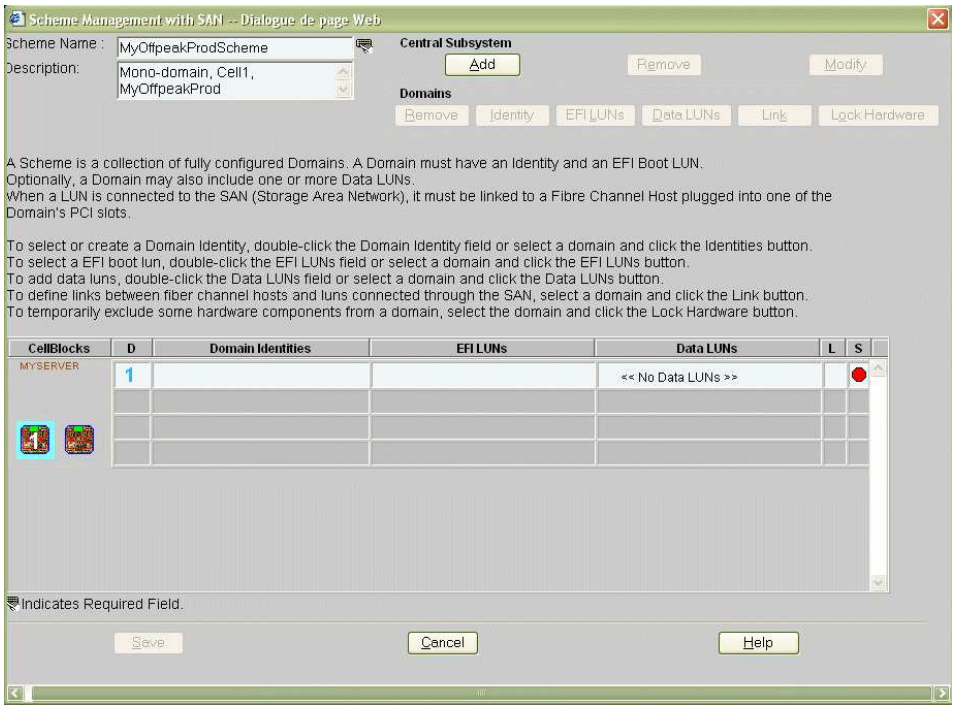
Figure 172. Remove domain confirmation dialog – example 2

10. Repeat Step 11 for **D3** and **D4**, where applicable.

12. Now, only one domain appears in the **Scheme Management** dialog.

    The **Status** icon is red because a **Domain Identity** and an **EFI LUN** are required to complete domain configuration.

NovaScale 6080/6160 Server



NovaScale 6320 Server

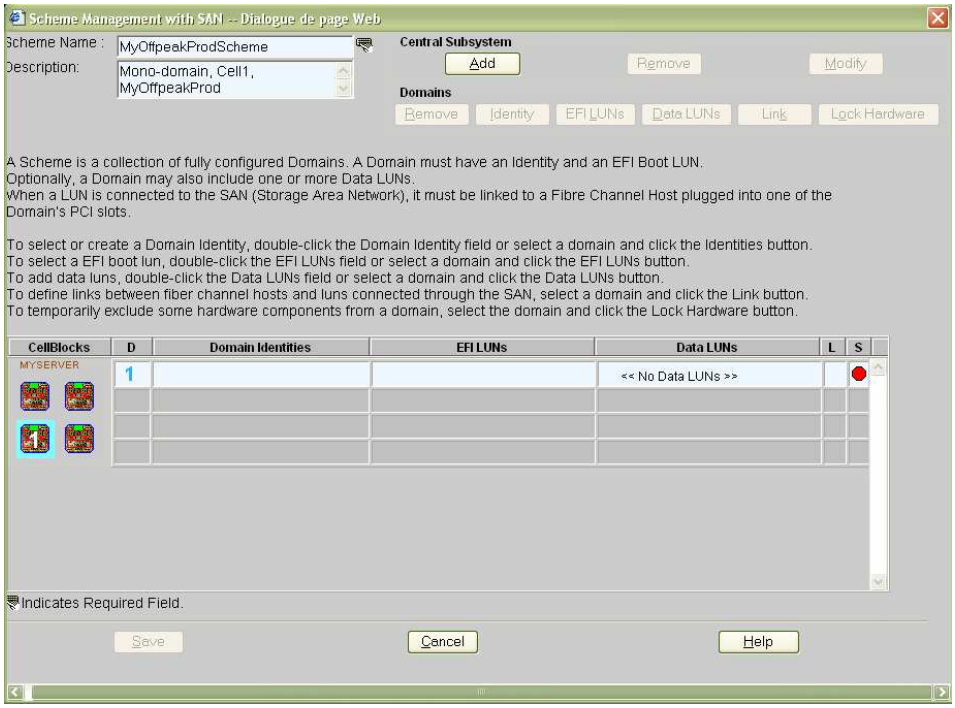


Figure 173. Scheme Management dialog – example 2

13. Double–click the empty **D1 Identities** field. The **Identities List** dialog opens.

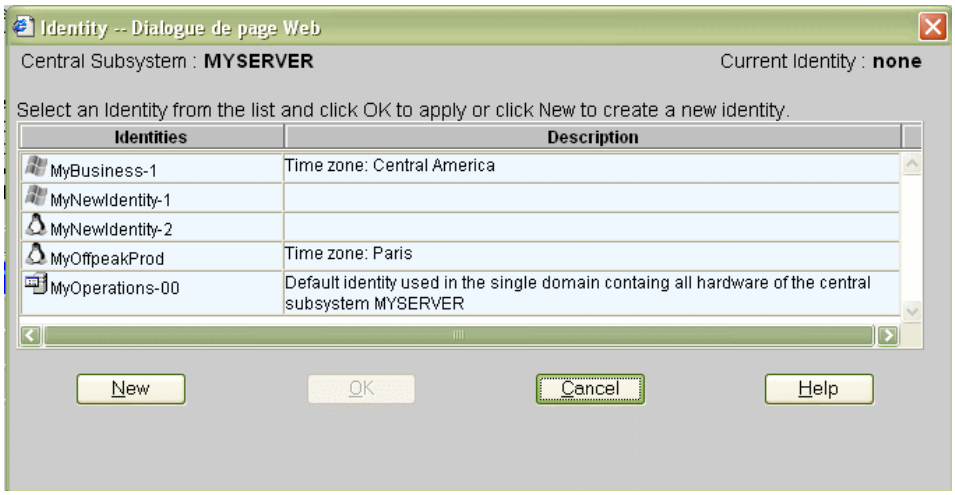


Figure 174. Identities list dialog – example 2

14. If the required identity is in the list, go to Step 17.
    If you want to create a new identity for this domain, click **New** to open the **Create New Identity** dialog. See *Creating a Domain Identity*, on page 5-47 for details.

15. Complete the **Name**, **Description**, **Domain Settings**, **Management Parameters**, **Multithreading Mode**, **HMMIO Space**, **Licensing Number** and **Machine Check** fields.

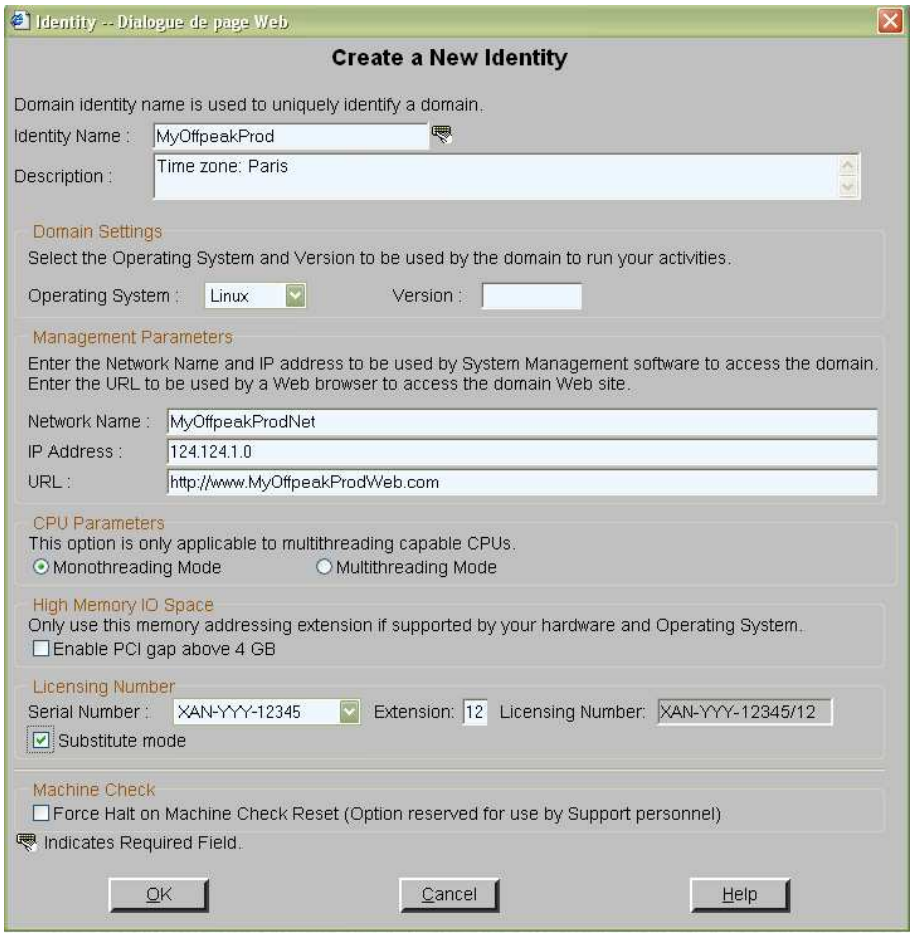


Figure 175. Create new identity dialog – example 2

16. Click **OK**. The new identity appears in the **Identities List** dialog.

17. Select the required identity from the list of available identities and click **OK** to return to the **Scheme Management** dialog. The selected identity is now displayed in the **Domain Identities** field.

18. Double–click the **EFI LUNs** field. The **Select EFI LUN** dialog opens, allowing you to choose the required EFI Boot LUN from the list of available LUNs.

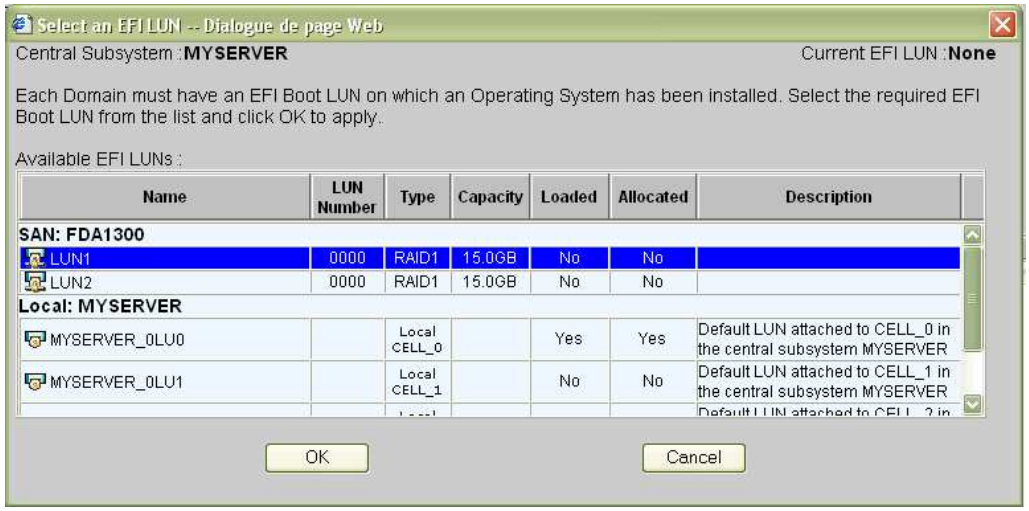


Figure 176. Select EFI LUN dialog – example 2

19. Select the required EFI Boot LUN from the list of available LUNs and click **OK** to return to the **Scheme Management** dialog. The selected LUN is now displayed in the **EFI LUNs** field.

    As the selected LUN is a SAN LUN, the **Status** icon remains red and the **No Link** icon  appears.

20. Double–click the **Data LUNs** field. The **Select Data LUN** dialog opens, allowing you to choose the required Data LUNs from the list of available LUNs.

21. Select the required Data LUNs from the list of available LUNs and click **Add** to move the selected Data LUNs to the **Data LUNs selected** list.

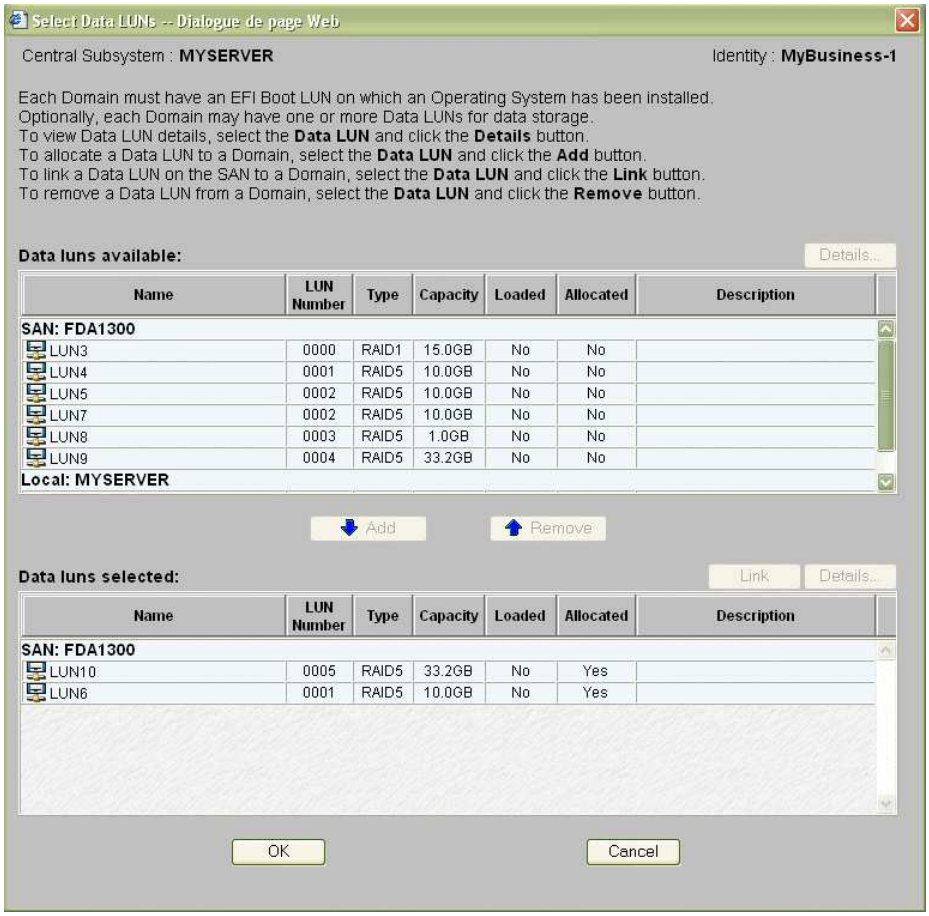


Figure 177. Select Data LUN dialog – example 2

22. Click **OK** to return to the **Scheme Management** dialog. **Data LUN set** is now displayed in the **Data LUNs** field.

    The **Status** icon remains red and the **No Link** icon is displayed. You must now link the selected EFI and Data LUNs to the Fibre Channel Host you want to use to access these LUNs.

23. Click **Domains** → **Link** to open the **Link LUNs to HBA** dialog.

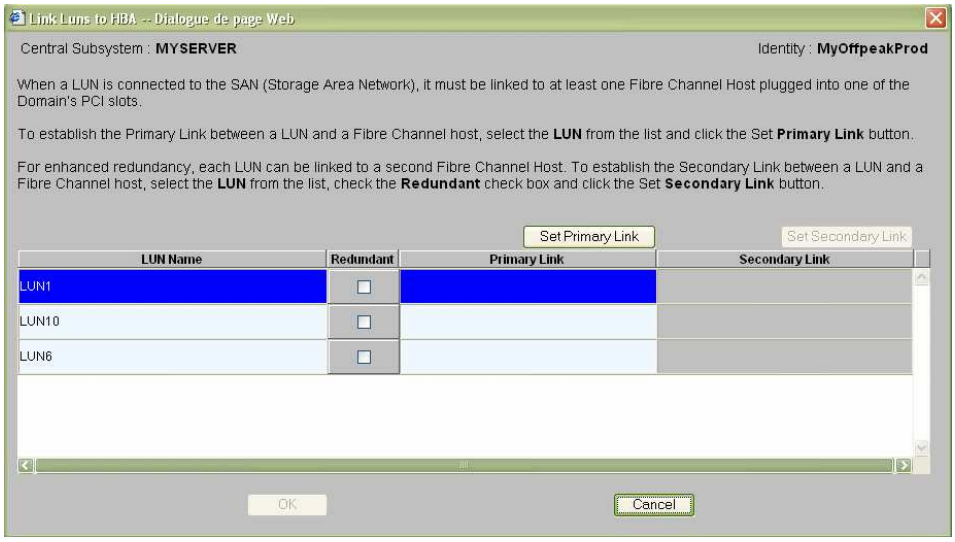


Figure 178. Link LUN to HBA dialog – example 2

24. Select the first LUN in the list and click **Set Primary Link** to define the main access path to the SAN. The **Select HBA** dialog opens, allowing you to select the domain PCI slot you want to use to access the LUN.

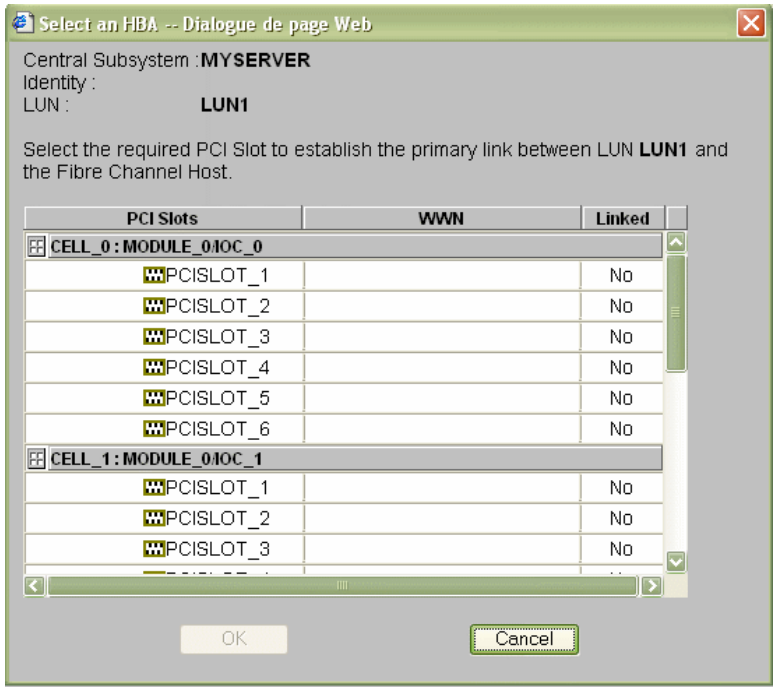


Figure 179. Select HBA dialog – example 2

25. Select the required PCI slot and click **OK**. The primary link is now set.
26. Repeat Steps 19 to for each LUN in the list and click **OK** → **Apply** to return to the **Scheme Management** dialog. The **Status** icon turns green and the **Linked** icon appears.
27. Click **Save**. The domain configuration scheme is now available for domain management.

Creating a Multi–Domain Scheme Using All Server Resources

Notes:

- A domain configuration scheme can include more than one Central Subsystems. If you have more than one Bull NovaScale Server, see *Configuring and Managing Extended Systems*, on page 5-108.
- For more information about scheme and identity configuration options, refer to:
  - *Assessing Configuration Requirements*, on page 5-31
  - *Creating a Domain Configuration Scheme*, on page 5-33
  - *Creating a Domain Identity*, on page 5-48

The configuration criteria set out in the following tables is used to illustrate this example:

NovaScale 6080/6160 Server

Scheme	
Name	MyProd_PayrollScheme
Description	Multi–domain, Cells 0 & 1, MyProduction & MyPayroll
Central Subsystem(s)	MyServer
Number of domains	2
Domain size	1 cell per domain: Cell 0 for MyProduction (Domain 1) Cell 1 for MyPayroll (Domain 2)
EFI boot LUNs	SAN: FDA 1300 LUN1 for MyProduction Local: 0Lun1 for MyPayroll
Data LUNs *	SAN: FDA 1300 LUN10, LUN6 for MyProduction SAN: FDA 1300 LUN4 for MyPayroll
Fibre channel hosts *	Primary Link: Cell_0: Module_0/IOB_0/PCISLOT_1 for MyProduction Primary Link: Cell_1: Module_0/IOB_1/PCISLOT_1 for MyPayroll
IO resource location	0IOB0 for MyProduction 0IOB1 for MyPayroll
Resource access	All resources unlocked
Domain Identity 1	
Name	MyProduction
Description	Time zone: Vladivostok
Operating System	Windows
Domain network name	MyProductionNet
Domain IP address	121.121.12.1
Domain URL	http://www.MyProductionWeb.com
Domain threading mode	Monothreading
HMMIO space	Disabled
Licensing number	XAN–S11–99999/13
Substitute mode	Enabled
Halt on machine check reset	Disabled
Domain Identity 2	
Name	MyPayroll
Description	Time zone: Paris
Operating System	Linux
Domain network name	MyPayrollNet
Domain IP address	122.122.1.0
Domain URL	http://www.MyPayrollWeb.com
Domain threading mode	Monothreading
HMMIO space	Enabled
Licensing number	XAN–S11–99999/14
Substitute mode	Enabled
Halt on machine check reset	Disabled

* Reserved for systems connected to a Storage Area Network (SAN)

Table 47. Scheme configuration criteria – example 3 – mono–module server

NovaScale 6320 Server

Scheme	
Name	MyProd_PayrollScheme
Description	Multi–domain, Cells 0,1,2&3, MyProduction & MyPayroll
Central Subsystem(s)	MyServer
Number of domains	2
Domain size	Cells 0, 1 & 2 for Domain 1 Cell 3 for Domain 2
EFI boot LUNs	SAN: FDA 1300 LUN1 for MyProduction Local: 0Lun3 for MyPayroll
Data LUNs *	SAN: FDA 1300 LUN10, LUN6 for MyProduction SAN: FDA 1300 LUN4 for MyPayroll
Fibre channel hosts *	MyProduction: Primary Link: Cell_0: Module_0/IOB_0/PCISLOT_1 MyPayroll: Primary Link: Cell_3: Module_1/IOB_1/PCISLOT_1
IO resource location	0IOB0 mandatory, 0IOB1 & 1IOB0 optional, for MyProduction 1IOB1 mandatory for MyPayroll
Resource access	All resources unlocked
Domain Identity 1	
Name	MyProduction
Description	Time zone: Vladivostok
Operating System	Windows
Domain network name	MyProductionNet
Domain IP address	121.121.12.1
Domain URL	http://www.MyProductionWeb.com
Domain threading mode	Monothreading
HMMIO space	Disabled
Licensing number	XAN–S11–99999/13
Substitute mode	Enabled
Halt on machine check reset	Disabled
Domain Identity 2	
Name	MyPayroll
Description	Time zone: Paris
Operating System	Linux
Domain network name	MyPayrollNet
Domain IP address	122.122.1.0
Domain URL	http://www.MyPayrollWeb.com
Domain threading mode	Monothreading
HMMIO space	Enabled
Licensing number	XAN–S11–99999/14
Substitute mode	Enabled
Halt on machine check reset	Disabled

* Reserved for systems connected to a Storage Area Network (SAN)

Table 48. Scheme configuration criteria – example 3 – bi–module server

To create a multi–domain scheme using all server resources:

1. Check that the required hardware resources are available (at least one IOB and one QBB are required for each server domain) and that the domain Operating System supports the required hardware resources (CPUs, DIMMs, ...).
2. From the Customer Administrator PAM tree, click **Configuration Tasks** → **Domains** → **Schemes** to open the **Schemes Management** pane.
3. Click **New** to open the **Scheme Creation** dialog.
4. Complete the **Scheme** and **Description** fields.

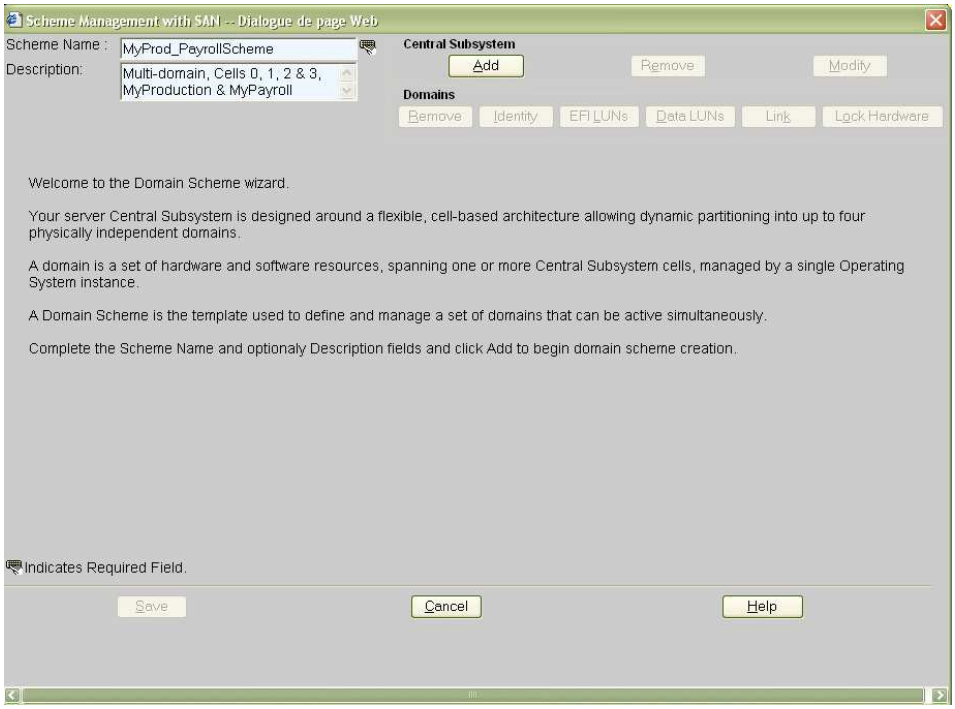
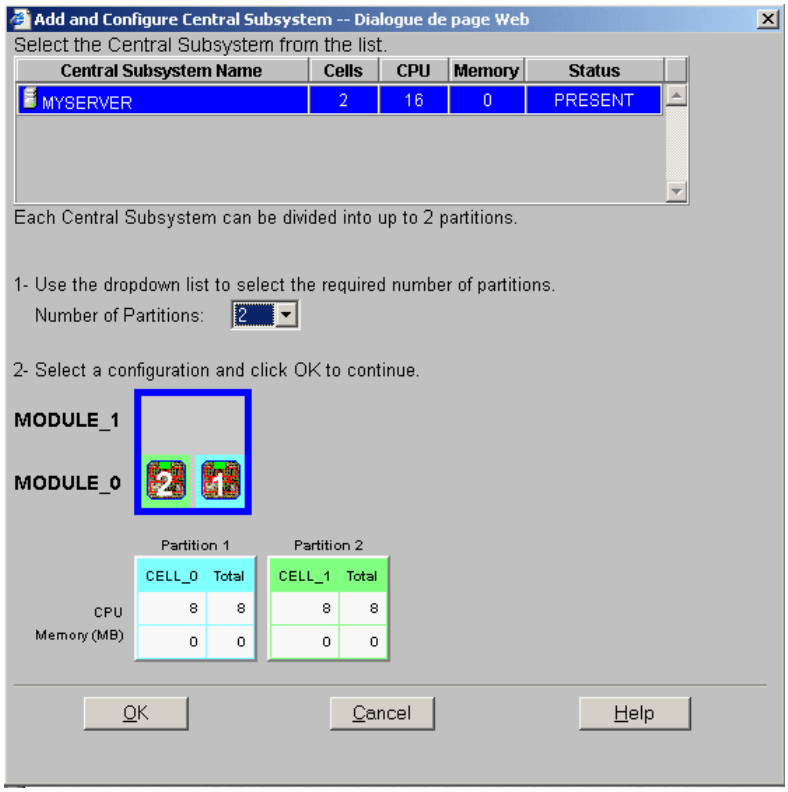


Figure 180. Scheme creation dialog – example 3

5. Click **Central Subsystem** → **Add** to select the Central Subsystem to be used by the domain configuration scheme. The **Central Subsystem Configuration** dialog opens.

NovaScale 6080/6160 Server



NovaScale 6320 Server

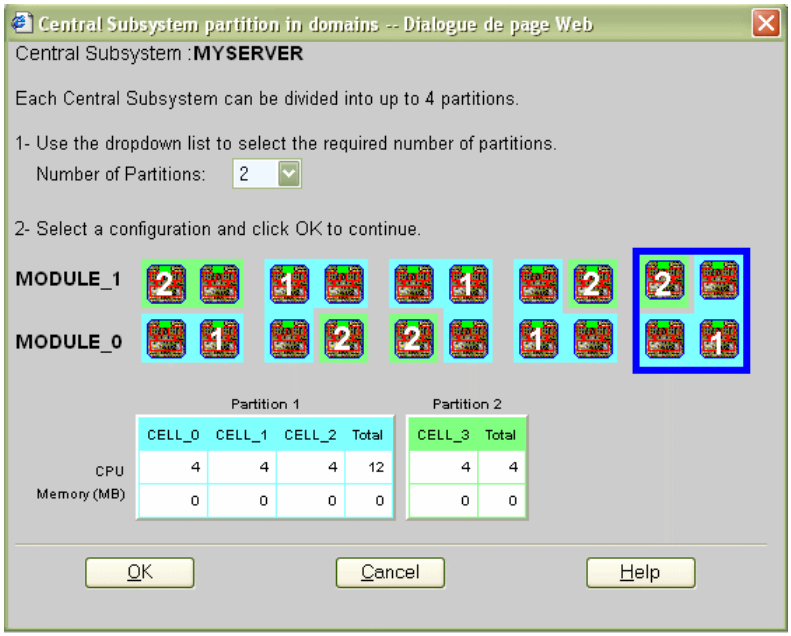
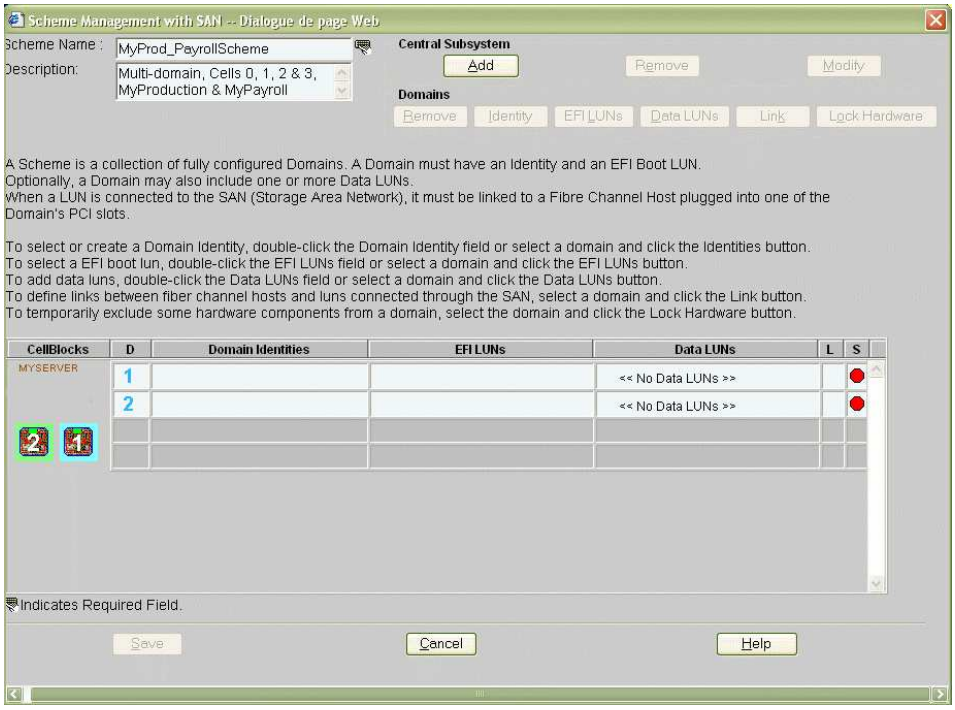


Figure 181. Central Subsystem configuration dialog – example 3

6. Check that the required Central Subsystem is highlighted and select **2** in the **Number of Parts** dropdown list.
7. Select the required partition configuration and click **OK** to return to the **Scheme Management** dialog.

The **Status** icons are red because **Domain Identities** and **EFI LUNs** are required to complete domain configuration.

NovaScale 6080/6160 Server



NovaScale 6320 Server

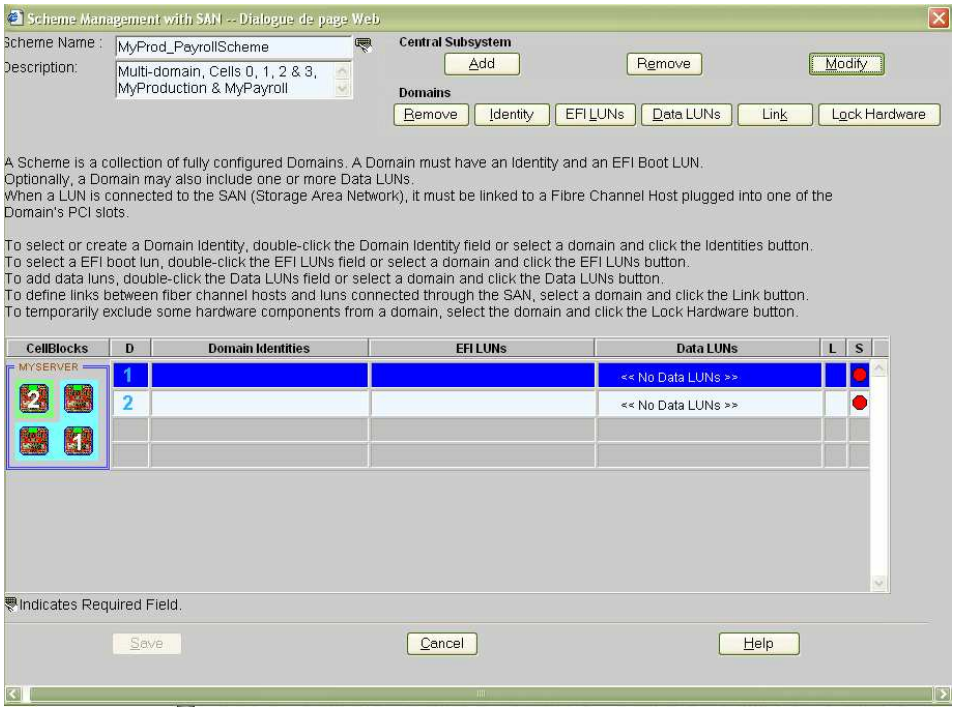


Figure 182. Scheme Management dialog – example 3

8. Double–click the empty **D1 Identities** field. The **Identities List** dialog opens.

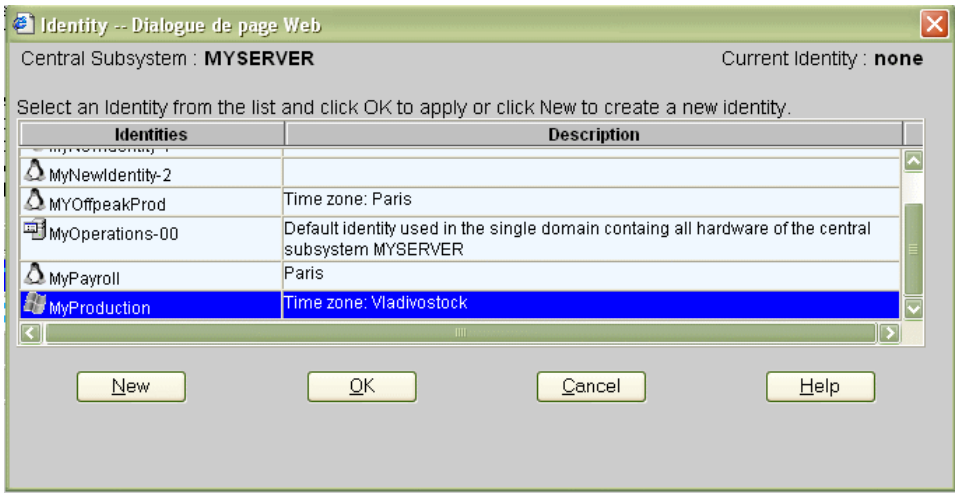


Figure 183. Identities list dialog – example 3

9. If the required identity is in the list, go to Step 12.
To create a new identity for this domain, click **New** to open the **Create New Identity** dialog. See *Creating a Domain Identity*, on page 5-47 for details.

10. Complete the **Name**, **Description**, **Domain Settings**, **Management Parameters**, **Multithreading Mode**, **HMMIO Space**, **Licensing Number** and **Machine Check** fields for **Domain Identity D1**.

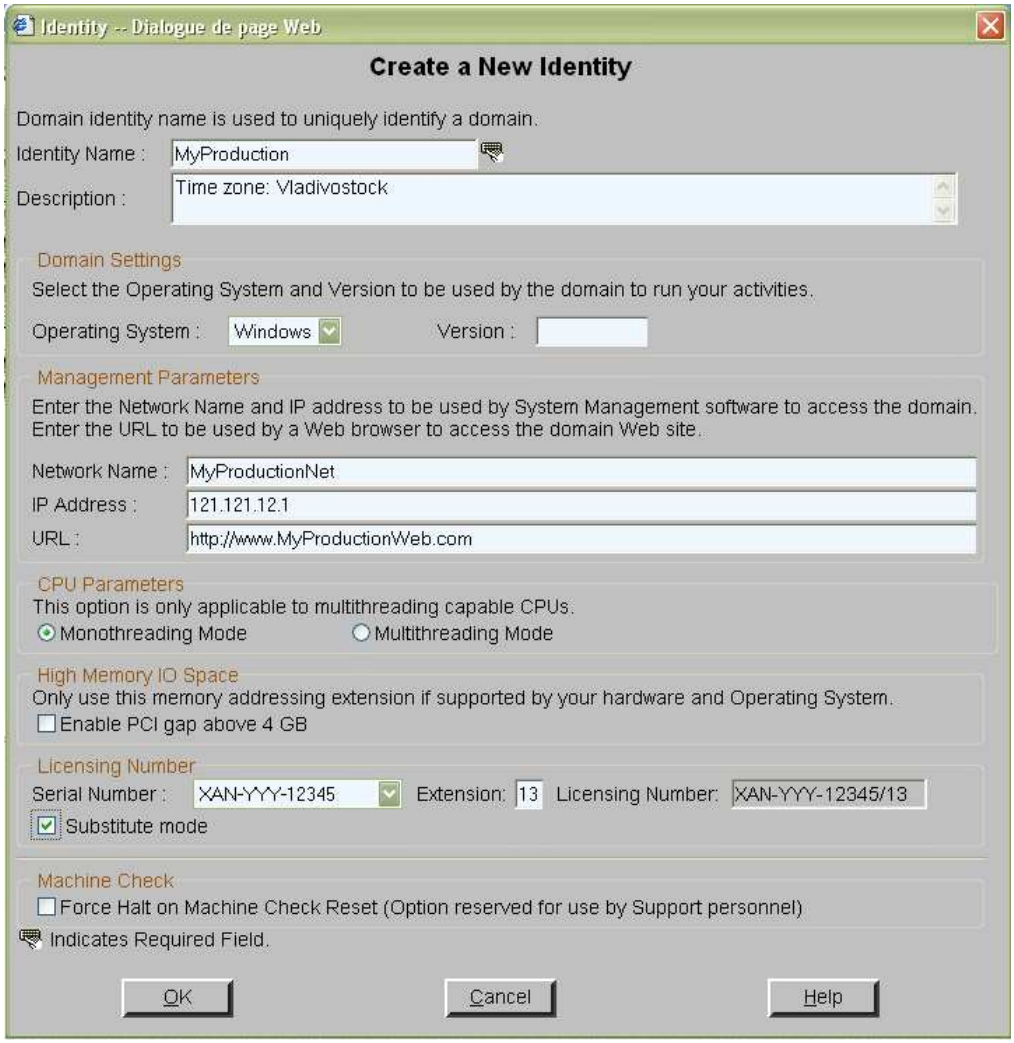


Figure 184. Create new identity dialog – example 3

11. Click **OK**. The new identity appears in the **Identities List** dialog.

12. Select the required identity from the list of available identities and click **OK** to return to the **Scheme Management** dialog. The selected identity is now displayed in the **Domain Identities** field.

13. Repeat Steps 8 to 12 for **Domain Identity D2**.

14. Double–click the **D1 EFI LUNs** field. The **Select EFI LUN** dialog opens, allowing you to choose the required EFI Boot LUN from the list of available LUNs.

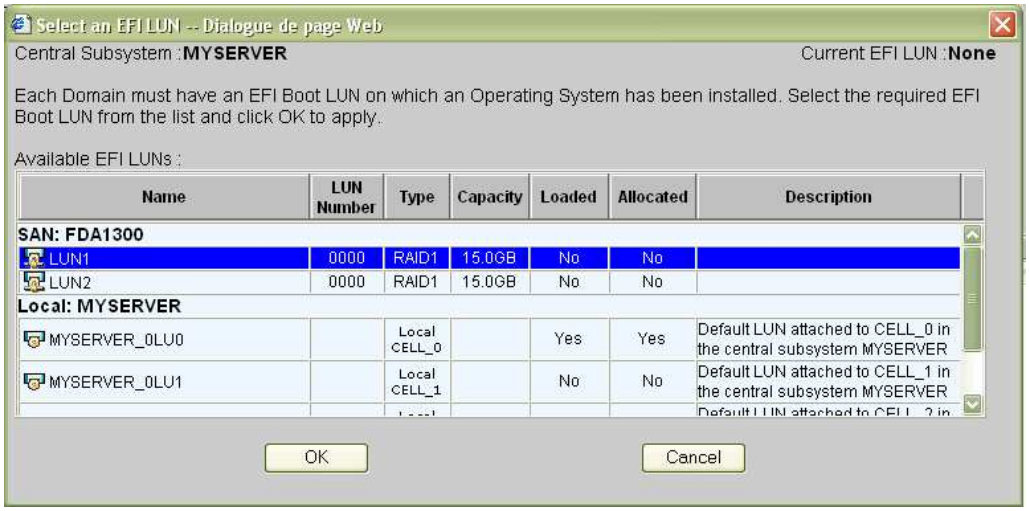


Figure 185. Select SAN EFI LUN dialog – example 3

15. Select the required EFI Boot LUN from the list of available SAN LUNs and click **OK** to return to the **Scheme Management** dialog. The selected LUN is now displayed in the **EFI LUNs** field.

    As the selected EFI LUN is a SAN LUN, the **Status** icon remains red and the **No Link** icon appears.

16. Double–click the **D2 EFI LUNs** field. The **Select EFI LUN** dialog opens, allowing you to choose the required EFI Boot LUN from the list of available Local LUNs.

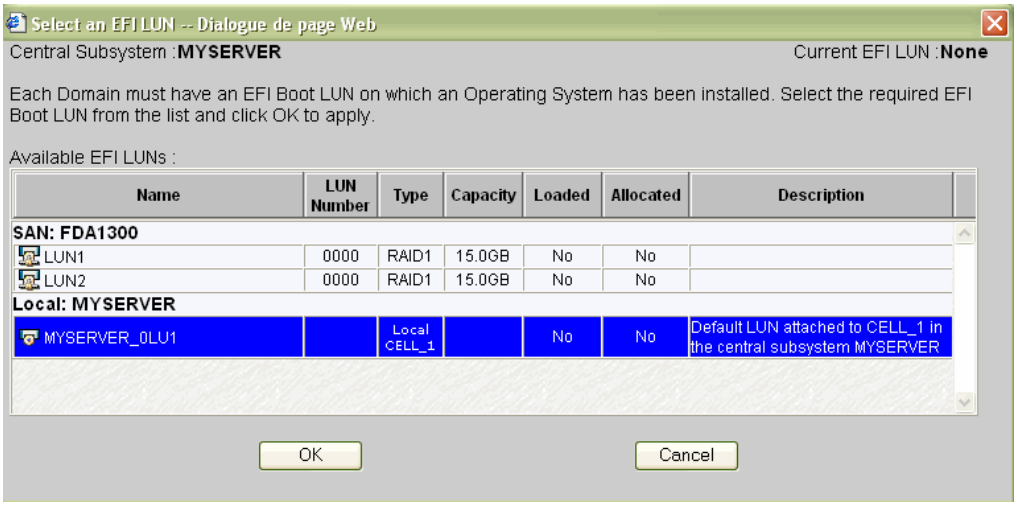


Figure 186. Select Local EFI LUN dialog – example 3

As the selected EFI LUN is a Local LUN, the **Status** icon turns green.

17. Double–click the **D1 Data LUNs** field. The **Select Data LUN** dialog opens, allowing you to choose the required Data LUNs from the list of available LUNs.

18. Select the required Data LUNs from the list of available LUNs and click **Add** to move the selected Data LUNs to the **Data LUNs selected** list.

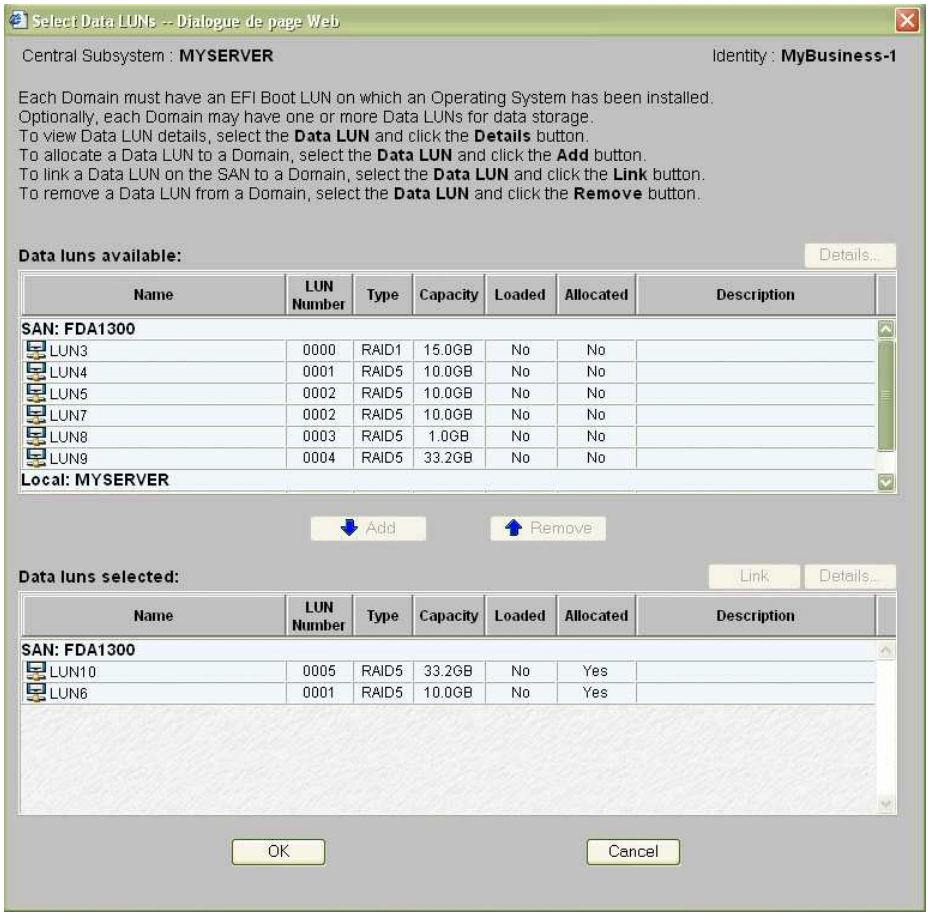


Figure 187. Select Data LUN dialog – example 2

19. Click **OK** to return to the **Scheme Management** dialog. **Data LUN set** is now displayed in the **Data LUNs** field.

    The **Status** icon remains red and the **No Link** icon is displayed. You must now link the selected EFI and Data LUNs to the Fibre Channel Host you want to use to access these LUNs.

20. Repeat Steps 17 to 19 for **D2 Data LUNs**.

    As the selected Data LUN is a SAN LUN, the **Status** icon turns red and the **No Link** icon is displayed. You must now link the selected Data LUN to the Fibre Channel Host you want to use to access this LUN.

21. Double–click the **D1 No Link** icon to open the **Link LUNs to HBA** dialog.

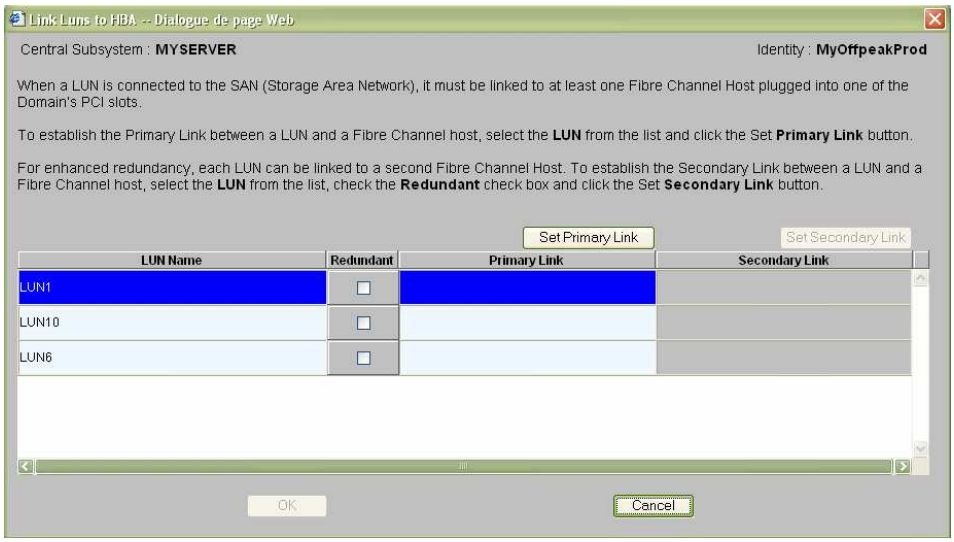


Figure 188. Link LUN to HBA dialog – example 3

22. Select the first LUN in the list and click **Set Primary Link** to define the main access path to the SAN. The **Select HBA** dialog opens, allowing you to select the domain PCI slot you want to use to access the LUN.

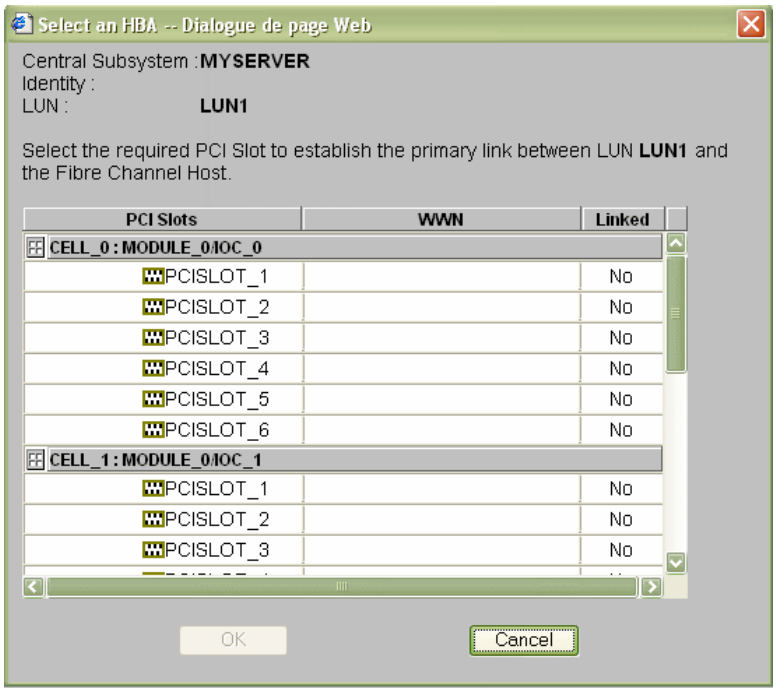


Figure 189. Select HBA dialog – example 3

23. Select the required PCI slot and click **OK**. The primary link is now set.
24. Repeat Steps 19 to 23 for each LUN in the list and click **OK** → **Apply** to return to the **Scheme Management** dialog. The **D1 Status** icon turns green and the **Linked** icon appears.
25. Repeat Steps 21 to 23 for **D2**. All **Status** icons are green.
26. Click **Save**. The domain configuration scheme is now available for domain management.

Creating a Multi–Domain Scheme Using a Selection of Server Resources

☞ **Notes:**

- A domain configuration scheme can include more than one Central Subsystems. If you have more than one Bull NovaScale Server, see *Configuring and Managing Extended Systems*, on page 5-108.
- For more information about scheme and identity configuration options, refer to:
  - *Assessing Configuration Requirements*, on page 5-31
  - *Creating a Domain Configuration Scheme*, on page 5-33
  - *Creating a Domain Identity*, on page 5-48

The configuration criteria set out in the following tables is used to illustrate this example:

NovaScale 6320 Server

Scheme	
Name	MyTest_DevptScheme
Description	Multi–domain, Cells 1, 2 & 3, MyTest & MyDevpt
Central Subsystem(s)	MyServer
Number of domains	2
Domain size	1 cell / 2 cells: Cell 1 for MyTest (Domain 1) Cells 2 & 3 for MyDevpt (Domain 2)
EFI boot LUNs	SAN: FDA 1300 LUN1 for MyTest Local: 0Lun3 for MyDevpt
Data LUNs *	SAN: FDA 1300 LUN10, LUN6 for MyTest SAN: FDA 1300 LUN4 for MyDevpt
Fibre channel hosts *	MyTest: Primary Link: Cell_1: Module_0/IOB_1/PCISLOT_1 MyDevpt: Primary Link: Cell_3: Module_1/IOB_1/PCISLOT_1 Secondary Link: Cell_2: Module_1/IOB_0/PCISLOT_1
IO resource location	0IOB0 for MyProduction 1IOB1 for MyPayroll
Resource access	Cell1, Hublink 1 / Cell2, Cell3, Hublinks 2 & 3
Domain Identity 1	
Name	MyTest
Description	Time zone: Paris
Operating System	Linux
Domain network name	MyTestNet
Domain IP address	126.126.1.2
Domain URL	http://www.MyProductionWeb.com
Domain threading mode	Multithreading
HMMIO space	Enabled
Licensing number	XAN–S22–88888/15
Substitute mode	Enabled
Halt on machine check reset	Disabled
Domain Identity 2	
Name	MyDevpt
Description	Time zone: Paris
Operating System	Windows
Domain network name	MyDevptNet
Domain IP address	126.126.1.0
Domain URL	http://www.MyPayrollWeb.com
Domain threading mode	Multithreading
HMMIO space	Disabled
Licensing number	XAN–S22–88888/16
Substitute mode	Enabled
Halt on machine check reset	Disabled

* Reserved for systems connected to a Storage Area Network (SAN)

Table 49. Scheme configuration criteria – example 4 – bi–module server

To create a multi–domain scheme using a part of server resources:

1. Check that the required hardware resources are available (at least one IOB and one QBB are required for each server domain) and that the domain Operating System supports the required hardware resources (CPUs, DIMMs, ...).
2. From the Customer Administrator PAM tree, click **Configuration Tasks** → **Domains** → **Schemes** to open the **Schemes Management** pane.
3. Click **New** to open the **Scheme Creation** dialog.
4. Complete the **Scheme** and **Description** fields.

Figure 190. Scheme creation dialog – example 4

5. Click **Central Subsystem** → **Add** to select the Central Subsystem to be used by the domain configuration scheme. The **Central Subsystem Configuration** dialog opens.

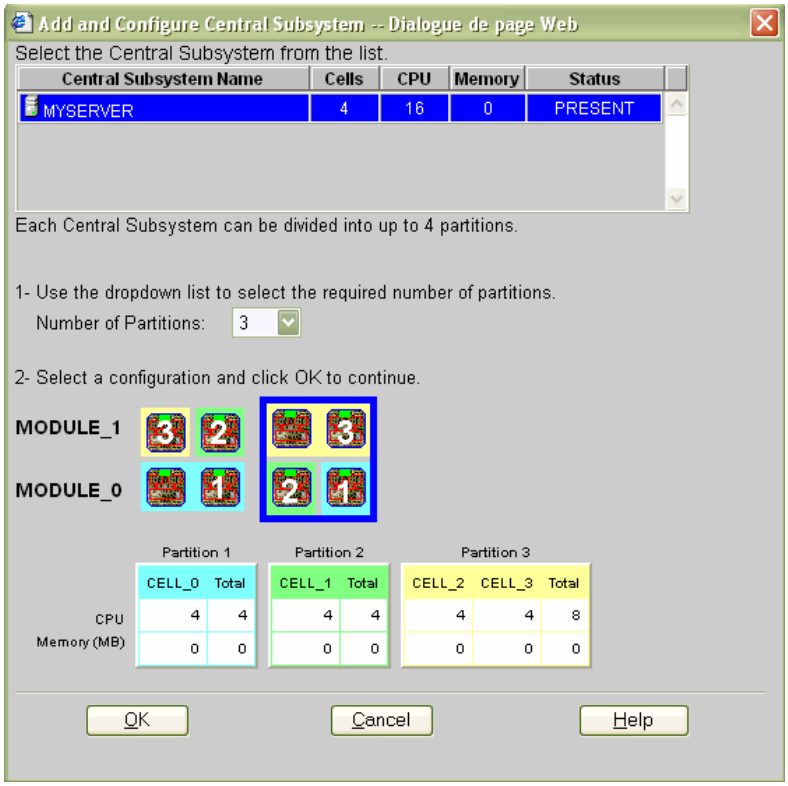


Figure 191. Central Subsystem configuration dialog – example 4

6. Check that the required Central Subsystem is highlighted and select **3** in the **Number of Parts** dropdown list.
7. Select the required partition configuration and click **OK** to return to the **Scheme Management** dialog.
8. As you want this scheme to only use Cells 1, 2 and 3, you must remove the domain using Cell 0. Hover the mouse over the cells represented in the **CellBlocks** diagram to identify the domain using Cell 0. **D1** is using Cell 0.

9. Click **D1** → **Domains** → **Remove** and click **OK** to remove the domain from the scheme.

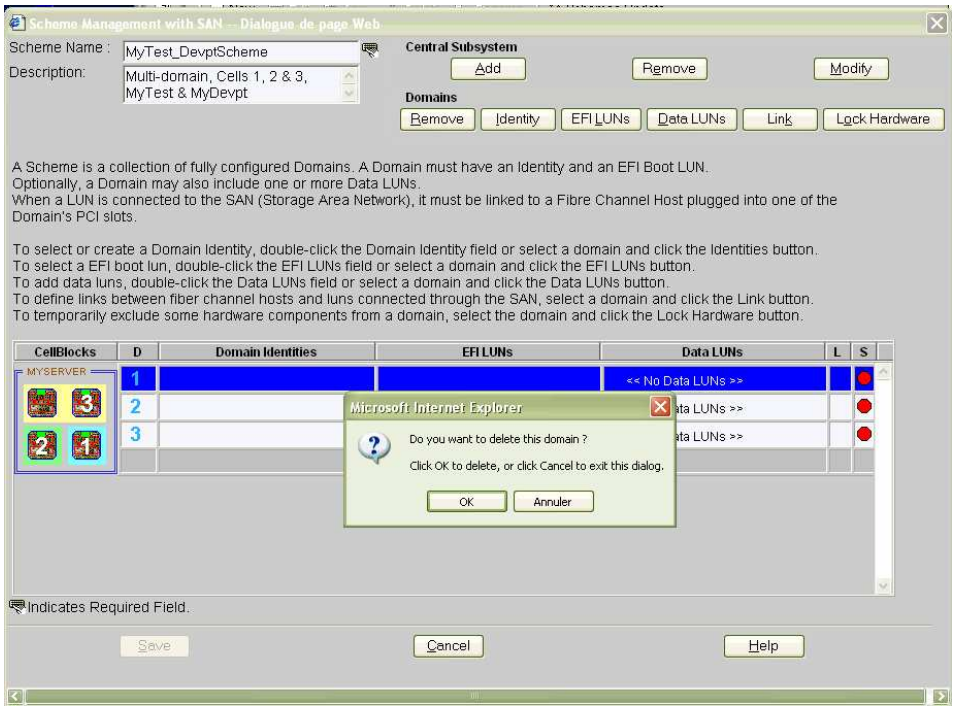


Figure 192. Remove domain confirmation dialog – example 4

10. Now, only two domains appear in the **Scheme Management** dialog.

    The **Status** icons are red because **Domain Identities** and **EFI LUNs** are required to complete domain configuration.

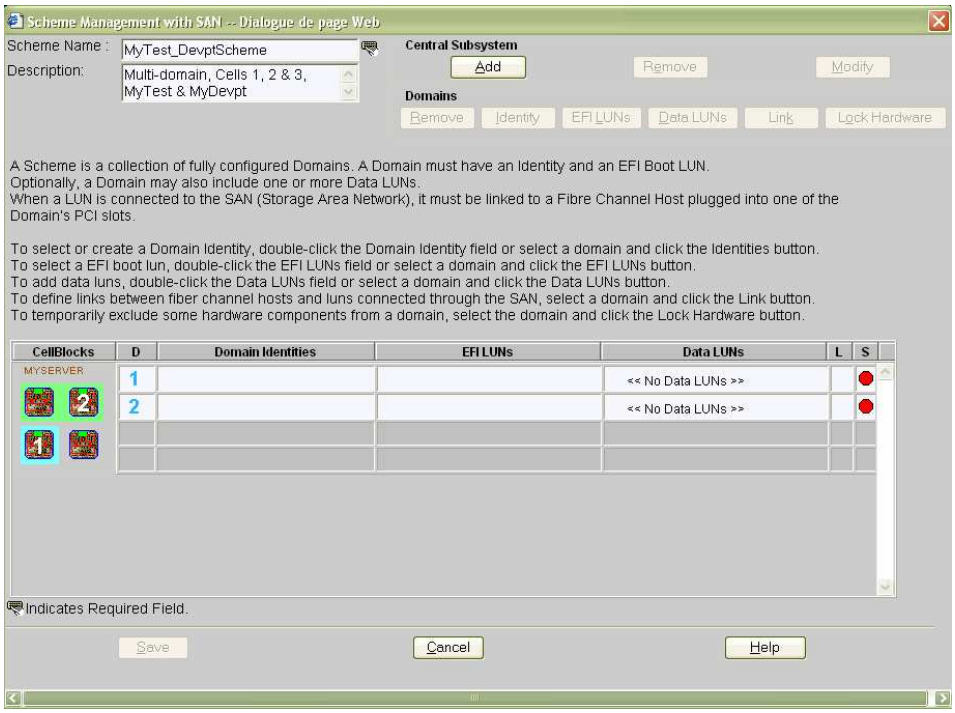


Figure 193. Scheme Management dialog – example 4

11. Double–click the empty **D1 Identities** field. The **Identities List** dialog opens.

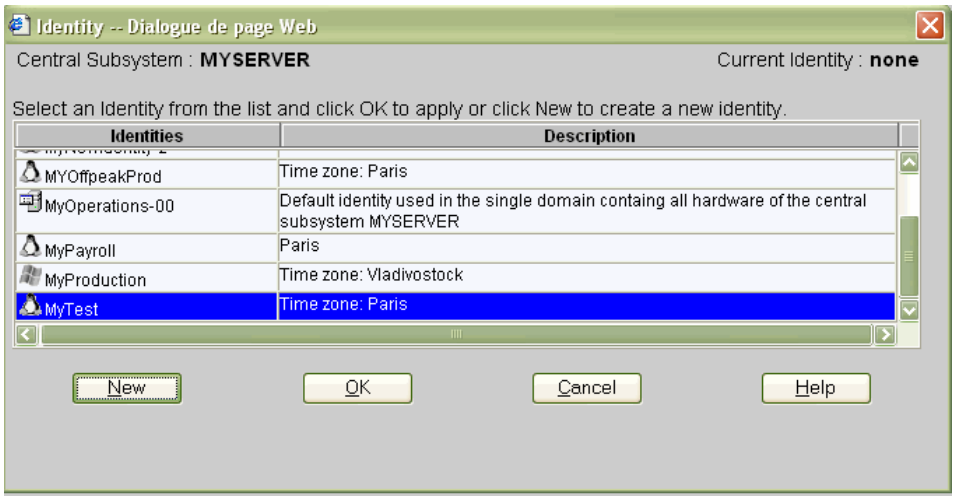


Figure 194. Identities list dialog – example 4

12. If the required identity is in the list, go to Step 17.
    If you want to create a new identity for this domain, click **New** to open the **Create New Identity** dialog. See *Creating a Domain Identity*, on page 5-47 for details.

13. Complete the **Name**, **Description**, **Domain Settings**, **Management Parameters**, **Multithreading Mode**, **HMMIO Space**, **Licensing Number** and **Machine Check** fields.

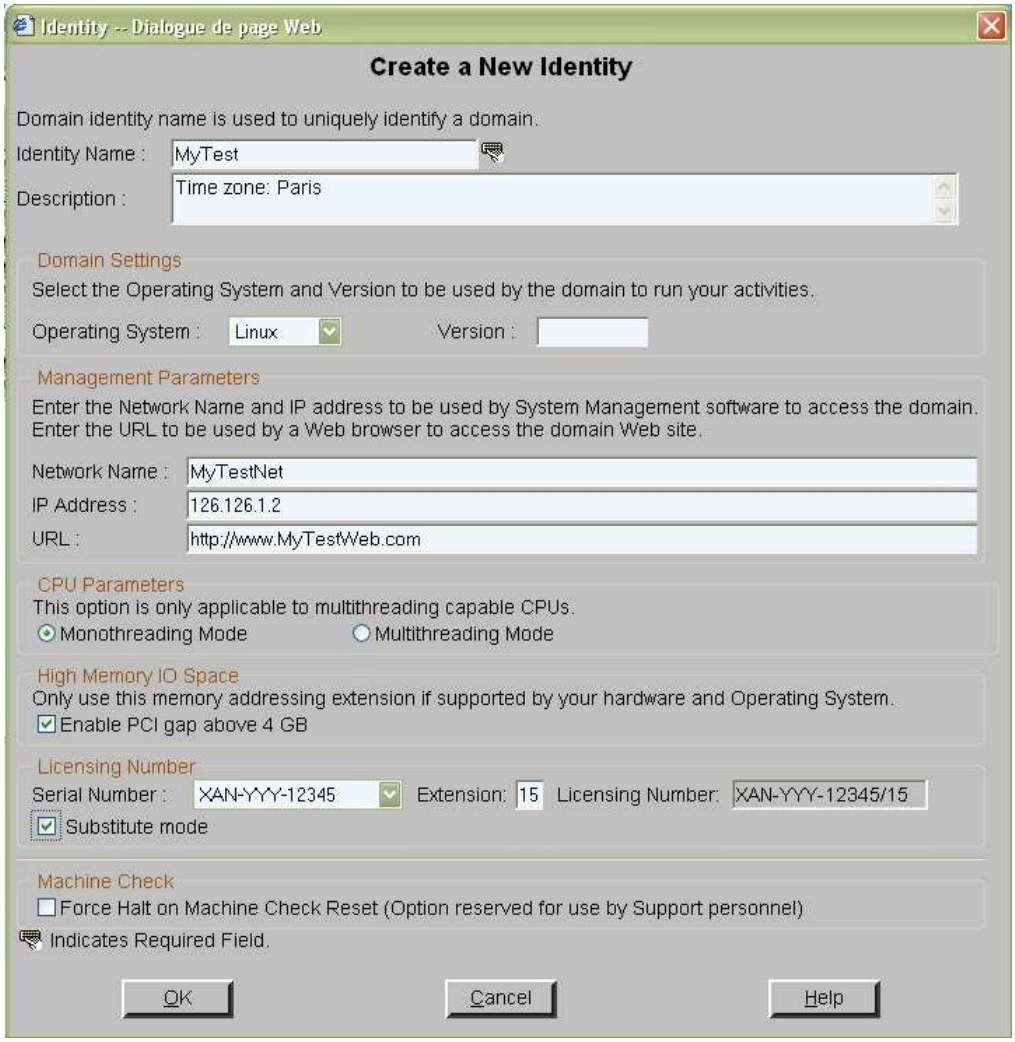


Figure 195. Create new identity dialog – example4

14. Click **OK**. The new identity appears in the **Identities List** dialog.

15. Select the required identity from the list of available identities and click **OK** to return to the **Scheme Management** dialog. The selected identity is now displayed in the **Domain Identities** field.

16. Repeat Steps 11 to 15 for **Domain Identity D2**.

17. Double–click the **D1 EFI LUNs** field. The **Select EFI LUN** dialog opens, allowing you to choose the required EFI Boot LUN from the list of available LUNs.

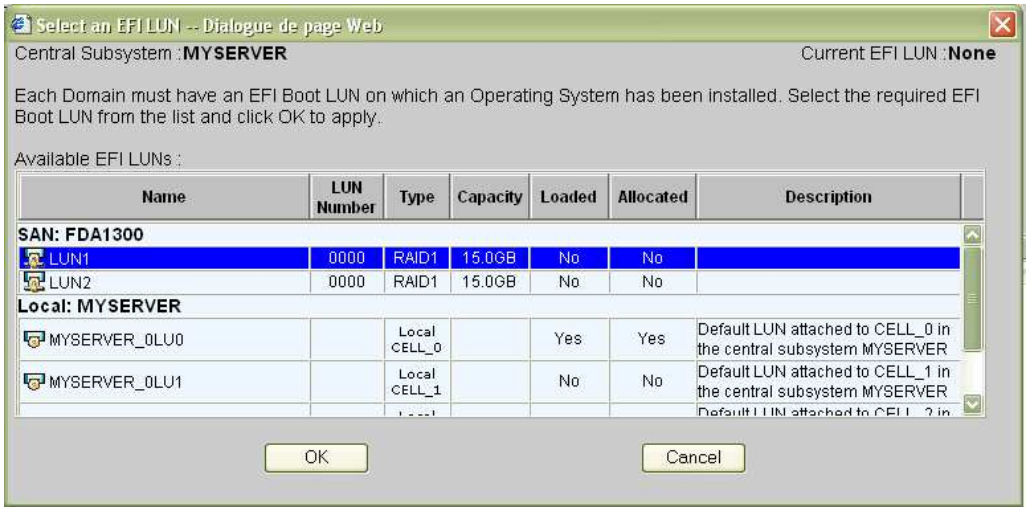


Figure 196. Select EFI LUN dialog – example 4

18. Select the required EFI Boot LUN from the list of available LUNs and click **OK** to return to the **Scheme Management** dialog. The selected LUN is now displayed in the **EFI LUNs** field.

    As the selected EFI LUN is a SAN LUN, the **Status** icon remains red and the **No Link** icon appears.

19. Double–click the **D2 EFI LUNs** field. The **Select EFI LUN** dialog opens, allowing you to choose the required EFI Boot LUN from the list of available LUNs.

    As the selected EFI LUN is a Local LUN, the **Status** icon turns green.

20. Double–click the **D1 Data LUNs** field. The **Select Data LUN** dialog opens, allowing you to choose the required Data LUNs from the list of available LUNs.

21. Select the required Data LUNs from the list of available LUNs and click **Add** to move the selected Data LUNs to the **Data LUNs selected** list.

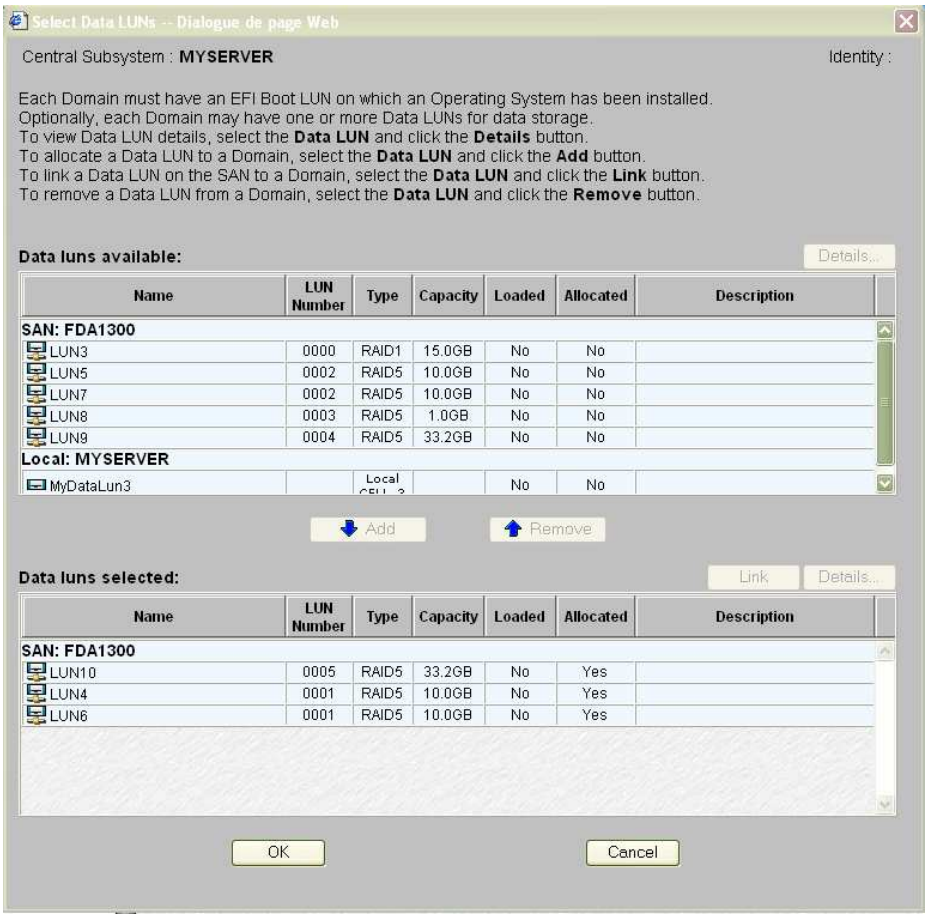


Figure 197. Select Data LUN dialog – example 4

22. Click **OK** to return to the **Scheme Management** dialog. **Data LUN set** is now displayed in the **Data LUNs** field.

    The **Status** icon remains red and the **No Link** icon is displayed. You must now link the selected EFI and Data LUNs to the Fibre Channel Host you want to use to access these LUNs.

23. Repeat Steps 20 to 22 for **D2 Data LUNs**.

    As the selected Data LUN is a SAN LUN, the **Status** icon turns red and the **No Link** icon is displayed. You must now link the selected Data LUN to the Fibre Channel Host you want to use to access these LUN.

24. Double–click the **D1 No Link** icon to open the **Link LUNs to HBA** dialog.

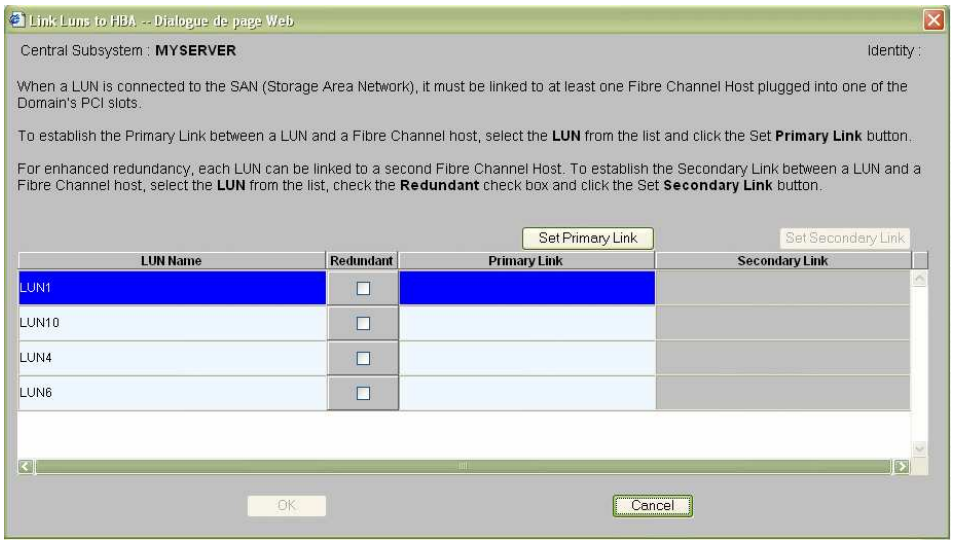


Figure 198. Link LUN to HBA dialog – example 2

25. Select the first LUN in the list and click **Set Primary Link** to define the main access path to the SAN. The **Select HBA** dialog opens, allowing you to select the domain PCI slot you want to use to access the LUN.

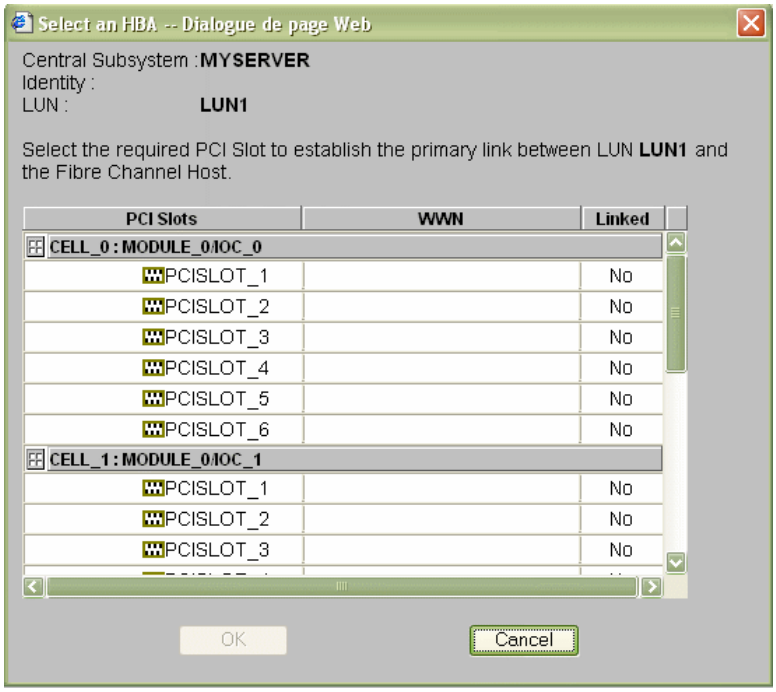


Figure 199. Select HBA dialog – example 4

26. Select the required PCI slot and click **OK**. The primary link is now set.
27. Repeat Steps 25 to 26 for each LUN in the list and click **OK** → **Apply** to return to the **Scheme Management** dialog. The **D1 Status** icon turns green and the **Linked** icon appears.
28. Repeat Steps 24 to 27 for **D2**. All **Status** icons are green.

29. Select **D2** and click **Lock Hardware** to open the **Lock Domain Hardware Resources** dialog.

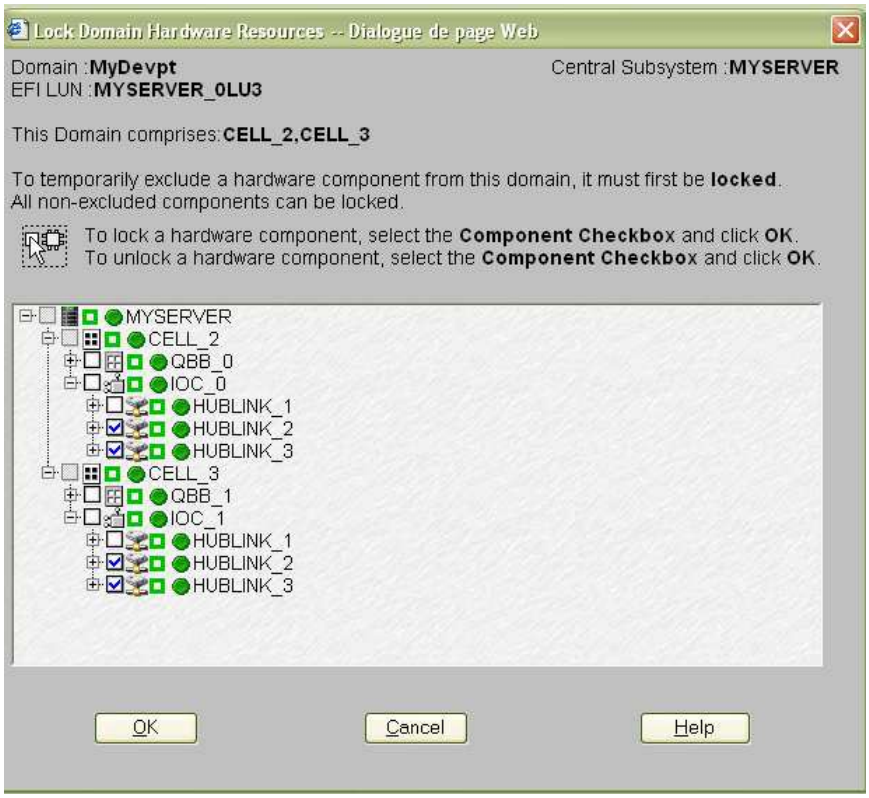


Figure 200. Lock domain hardware resources – example 4

30. Select the resources you want to lock and click **OK** to return to the **Scheme Management** dialog. See *Limiting Access to Hardware Resources*, on page 5-62 for details.

31. Click **Save**. The domain configuration scheme is now available for domain management.

Note:
Cell 0 is free and available for use by another scheme, if required.

Configuring and Managing Extended Systems

A single PAP unit can administer, monitor, and manage several Central Subsystems.

The PAM **Domain Configuration Scheme Wizard** allows easy configuration of extended systems.

Please contact your BULL Customer Sales Representative for details.

Scheme, Domain Identity, and Resources Checklists

Scheme Checklist	
Name	What name do I want to use for my Scheme?
Description	How can I describe my Scheme to reflect its scope?
Central Subsystem(s)	Which Central Subsystem(s) do I want to use?
Number of Domains	How many domains do I need?
Domain Size	How many cells do I want to assign to each domain?
EFI Boot LUNs	Which EFI boot LUN do I want to use for each domain?
Data LUNs *	Which data LUNs do I want to assign to each domain?
Fibre Channel Hosts *	Which fibre channel host(s) do I want to use to access LUNs?
I/O Resource Location	Which cells host the I/O resources I want to use?
Resource Access	Do I want to limit access to certain hardware resources?

* Reserved for systems connected to a Storage Area Network (SAN).

Table 50. Scheme configuration checklist

Domain Identity Checklist	
Name	What name do I want to use for my Domain Identity to reflect the tasks/jobs it will run?
Description	How can I describe my Domain Identity to reflect its use?
Operating System	Which OS do I want to run on this domain? Will this OS support assigned hardware (CPUs, DIMMs)?
Domain Network Name	Which network name will be used to identify this domain?
Domain IP Address	Which IP address will be used to reach this domain?
Domain URL	Which URL can be used to reach my domain Web site (if any)?
Multithreading Mode	Do the CPUs used by this domain support the multithreading mode? Do I want to enable the multithreading mode for this domain?
High Memory IO Space	Do I need more than 4GB PCI gap space for the PCI boards used by this domain?
Licensing Number	Do I intend to install an application protected by a system serial number on this domain? Do I want to substitute the physical system serial number with the logical licensing number for optimum flexibility?
Force Halt on Machine Check Reset	Has my Customer Service Engineer requested me to check this box to troubleshoot my server?

Table 51. Domain Identity configuration checklist

Resources Checklist			
Central Subsystem:			
Cell 0		**Cell 1**	
QBBs	QBB0	**QBBs**	QBB2
	QBB1		QBB3
IO Box	IOB0	**IO Box**	IOB1
EFI Boot Lun	0Lu0	**EFI Boot Lun**	0Lu1
OS instance		**OS instance**	
I/O Resources		**I/O Resources**	
IOB0_Slot 1		**IOB1_Slot 1**	
IOB0_Slot 2		**IOB1_Slot 2**	
IOB0_Slot 3		**IOB1_Slot 3**	
IOB0_Slot 4		**IOB1_Slot 4**	
IOB0_Slot 5		**IOB1_Slot 5**	
IOB0_Slot 6		**IOB1_Slot 6**	
IOB0_Slot 7		**IOB1_Slot 7**	
IOB0_Slot 8		**IOB1_Slot 8**	
IOB0_Slot 9		**IOB1_Slot 9**	
IOB0_Slot 10		**IOB1_Slot 10**	
IOB0_Slot 11		**IOB1_Slot 11**	

Table 52. Resources checklist – part 1

Resources Checklist			
Central Subsystem:			
Cell 2		**Cell 3**	
QBBs	QBB0	**QBBs**	QBB2
	QBB1		QBB3
IO Box	IOB0	**IO Box**	IOB1
EFI Boot Lun	1Lu0	**EFI Boot Lun**	1Lu1
OS instance		**OS instance**	
I/O Resources		**I/O Resources**	
IOB0_Slot 1		**IOB1_Slot 1**	
IOB0_Slot 2		**IOB1_Slot 2**	
IOB0_Slot 3		**IOB1_Slot 3**	
IOB0_Slot 4		**IOB1_Slot 4**	
IOB0_Slot 5		**IOB1_Slot 5**	
IOB0_Slot 6		**IOB1_Slot 6**	
IOB0_Slot 7		**IOB1_Slot 7**	
IOB0_Slot 8		**IOB1_Slot 8**	
IOB0_Slot 9		**IOB1_Slot 9**	
IOB0_Slot 10		**IOB1_Slot 10**	
IOB0_Slot 11		**IOB1_Slot 11**	

Table 53. Resources checklist – part 1

Table 54. Resources checklist – part 2

Section V – Creating Event Subscriptions and User Histories

This section explains how to:

Customizing the PAM Event Messaging System

During operation, all Central Subsystem activity messages are automatically logged in predefined System Histories that can be viewed and archived by members of the Customer Administrator group. In addition, PAM software reports and logs environmental, command, and hardware errors.

A comprehensive set of Event Message subscriptions allows connected and non–connected users to be notified of system status and activity.

The PAM event messaging system is based on a subscription mechanism allowing the Customer Administrator to send precisely filtered event messages to targeted individuals and/or groups via four channels (WEB Interface, E–mail, User History, SNMP) as shown in Figure 201.

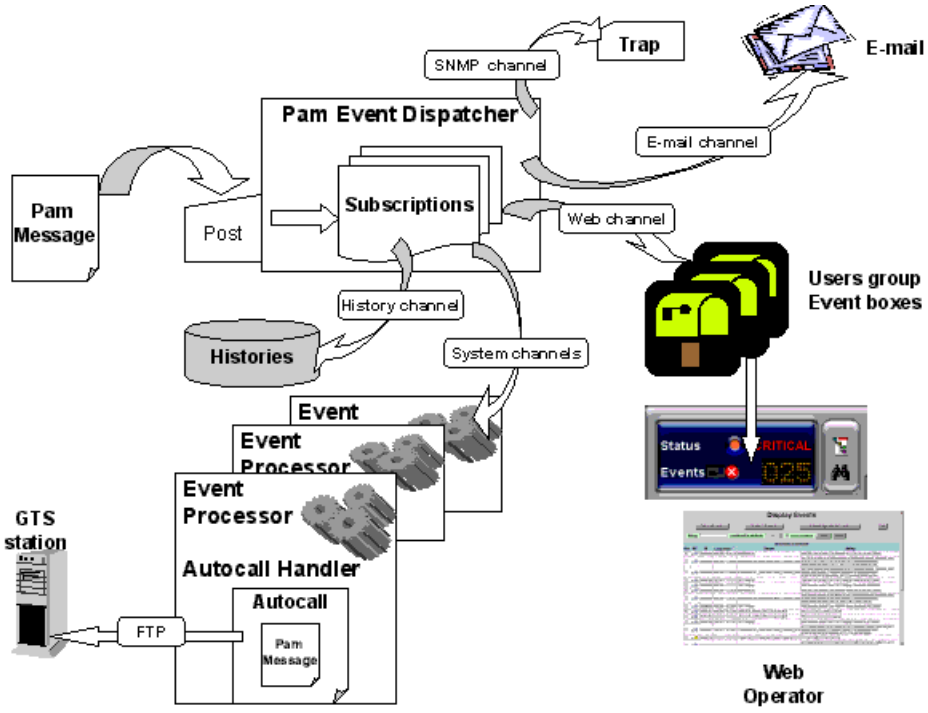


Figure 201. PAM event messaging system features

Note:
PAM software is delivered with a set of predefined subscriptions that have been designed to suit the needs of most Administrators and Operators. If required, you can use PAM **Configuration** tools to set up customized subscriptions.

From the PAM tree, expand the **Configuration Tasks** and **Events** nodes to display event configuration options.

Setting up Event Subscriptions

Before creating an event subscription, you should establish:

- the set of messages you want a user or a group of users to receive (**Filter**),
- how you want the user or group of users to receive messages (**Channel**).

Selecting a Filter

The comprehensive event message filtering system allows you to use a predefined filter or to create a specific filter, according to your needs.
See *Preselecting an Event Filter*, on page 5-121 and *Creating an Event Filter*, on page 5-122.

Selecting a Channel

Four channels can be used to forward event messages, according to targeted recipients:

Channel	Advantage
E–mail	Allows a specific user to receive system notifications/ alerts.
User history	Records specific system operations/alerts into a dedicated log file.
Web	Allows a specific group of users to be warned of system operations/alerts when connected to the PAM Web interface.
SNMP	Forwards specific messages as SNMP traps to the selected SNMP application.

Table 55. Event channels

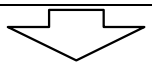
Event Subscription Flowcharts

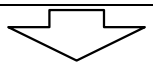
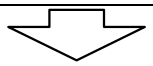
Once you have established who the targeted recipients are and which channel you want to use, you can use the following flowcharts as a quick guide to event subscription procedures.

E–mail Event Subscription
Allows a specific user to receive system notifications/alerts via e–mail.
Preselect an Event filter, on page 5-121, or *Create an Event Filter*, on page 5-122.

Select or *Create an E–mail Server*, on page 5-117.

Select or *Create an E–mail Account*, on page 5-119.

Create the Event Subscription, on page 5-130.
User History Event Subscription
Records specific system operations/alerts into a dedicated log file.
Preselect an Event filter, on page 5-121, or *Create an Event Filter*, on page 5-122.

Select or *Create a User History*, on page 5-125.

Create the Event Subscription, on page 5-130.
Web Event Subscription
Allows a specific group of users to be warned of system operations/alerts when connected to the PAM Web interface.
Preselect an Event filter, on page 5-121, or *Create an Event Filter*, on page 5-122.

Create the Event Subscription, on page 5-130.
SNMP Event Subscription
Forwards system operations/alerts as SNMP traps to the selected SNMP Manager.
Preselect an Event filter, on page 5-121, or *Create an Event Filter*, on page 5-122.

Create the Event Subscription, on page 5-130.

Creating, Editing, Deleting an E–mail Server

To send messages via the e–mail channel, you must first create an e–mail server. Several e–mail accounts can then be attached to the same e–mail server, see *Creating an E–mail Account*, on page 5-119.

Creating an E–mail Server

To create an e–mail server:

1. Click **Configuration Tasks** → **Events** → **E–mail servers** in the PAM tree. The e–mail servers configuration page opens.

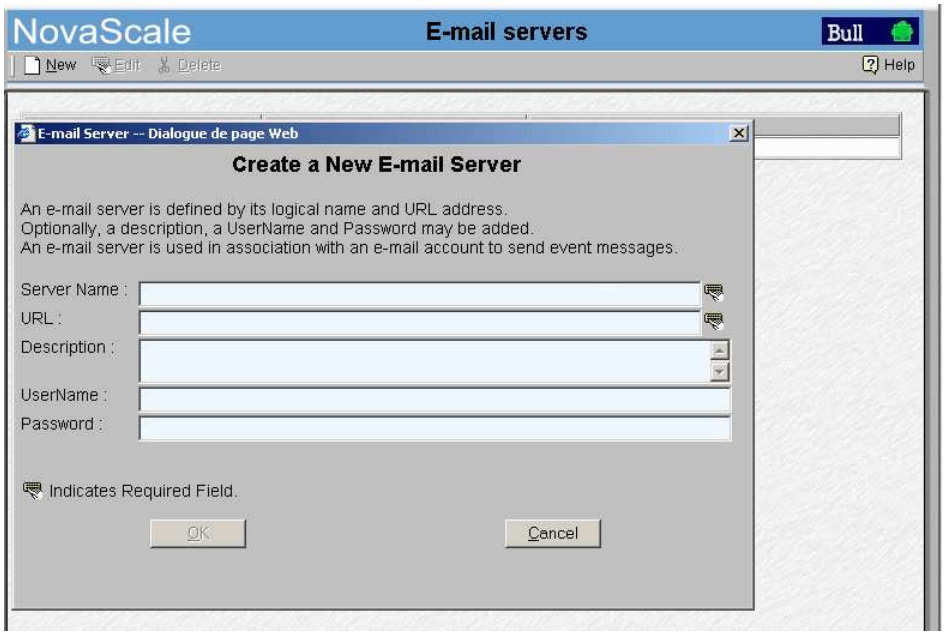


Figure 202. E–mail servers configuration page

2. Click **New** in the toolbar.
3. Enter the server name in the **Name** field, the address of the existing e–mail server you intend to use in the **URL** field, and a brief description, if required, in the **Description** field.
4. Enter a user name and password, if required and click **OK** to confirm the creation of the new e–mail server.

Note:
The **OK** button is accessible once all mandatory fields have been completed.

Editing E–mail Server Attributes

To modify an e–mail server URL / description:

1. Click **Configuration Tasks** → **Events** → **E–mail servers** in the PAM tree. The e–mail server configuration page opens. See Figure 202 above.
2. Select the required server from the e–mail servers list.
3. Click **Edit** in the toolbar to modify the server URL / description.
4. Enter a new address in the **URL** field and/or a new description in the **Description** field, as applicable.
5. Click **OK** to confirm the modification.

Deleting an E–mail Server

Important:
Before deleting an e–mail server, all the accounts attached to that server must be attached to another server, or deleted.
At least one e–mail server must be defined to send messages via the e–mail channel.

If e–mail accounts are attached to this e–mail server:

- see *Editing E–mail Account Attributes*, on page 5-118 to attach these accounts to another server, or
- see *Deleting an E–mail Account*, on page 5-120 to delete these accounts.

To delete an e–mail server:

1. Click **Configuration Tasks** → **Events** → **E–mail Servers** in the PAM tree. The e–mail server configuration page opens. See Figure 202, on page 5-117.
2. Select the required server from the e–mail servers list.
3. Click **Delete** in the toolbar.
4. Click **OK** to confirm the deletion of the selected e–mail server.

Creating, Editing, Deleting an E–mail Account

To send messages via the e–mail channel, you must first create an e–mail server and then attach an e–mail address to this e–mail server. Several e–mail accounts can be attached to the same e–mail server.

Creating an E–mail Account

To create an e–mail account:

1. Click **Configuration Tasks** → **Events** → **E–mail accounts** in the PAM tree. The e–mail accounts configuration page opens.

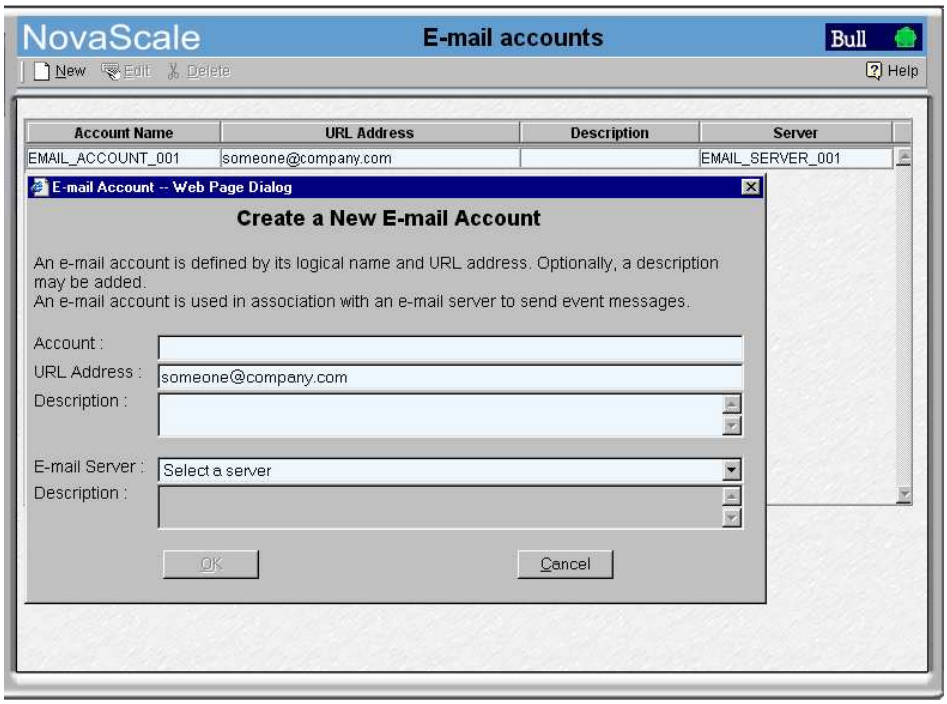


Figure 203. E–mail accounts configuration page

2. Click **New** in the toolbar.
3. Enter the new account name in the **Account** field and corresponding e–mail address in the **URL Address** field.
4. Select the server to be used to deliver messages to this address from the **E–mail Server** list. If the required e–mail server is not in the list, see *Creating an E–mail Server*, on page 5-117.
5. Enter a brief description, if required, in the **Description** field.
6. Click **OK** to confirm the creation of the new e–mail account.

The new e–mail account can now be selected when you set up an event subscription to be sent via the e–mail channel.

Note:
The **OK** button is accessible once all mandatory fields have been completed.

Editing E–mail Account Attributes

To modify an e–mail account name, address, server and/or description:

1. Click **Configuration Tasks** → **Events** → **E–mail accounts** in the PAM tree. The e–mail accounts configuration page opens. See Figure 203 above.
2. Select the required account from the e–mail accounts list.
3. Click **Edit** in the toolbar to modify the account name, address, server and/or description.
4. Enter the new attributes in the corresponding fields, as applicable. If the required e–mail server is not in the list, see *Creating an E–mail Server*, on page 5-117.
5. Click **OK** to confirm the modification.

Deleting an E–mail Account

Important:
Before deleting an e–mail account, all the event subscriptions attached to that account must be attached to another account, or deleted.

If event subscriptions are attached to this e–mail account, see:

- *Editing Event Subscription Attributes*, on page 5-131 to attach these event subscriptions to another account,
- or *Deleting an Event Subscription*, on page 5-131 to delete these event subscriptions.

To delete an e–mail account:

1. Click **Configuration Tasks** → **Events** → **E–mail accounts** in the PAM tree. The e–mail accounts configuration page opens. See Figure 203 above.
2. Select the required account from the e–mail accounts list.
3. Click **Delete** in the toolbar.
4. Click **OK** to confirm the deletion of the selected e–mail account.

Preselecting, Creating, Editing, Deleting an Event Filter

An event filter must be selected for all event subscriptions. The event messaging system is delivered with a set of predefined filters.

Preselecting an Event Filter

Before proceeding to set up an event subscription, you are advised to check which predefined filter is adapted to your needs:

1. Click **Configuration Tasks** → **Events** → **Filters** in the PAM tree. The filter configuration page opens.

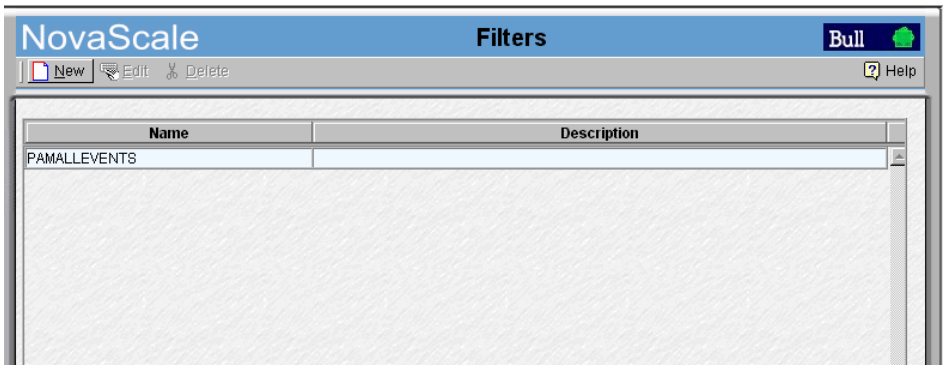


Figure 204. Filters configuration page

2. Check that the required filter is present.

You may also define a specific filter by using the comprehensive event message filtering utility. See *Creating an Event Filter*, on page 5-122.

Creating an Event Filter

Once you have established which filtering criteria you want to apply to your new filter, you can proceed to create a new event filter:

1. Click **Configuration Tasks** → **Events**→ **Filters** in the PAM tree. The filter configuration page opens with the list of existing event message filters.
2. Click **New** to display the **Create a New Event Filter** page. The standard event message filtering criteria table is displayed.

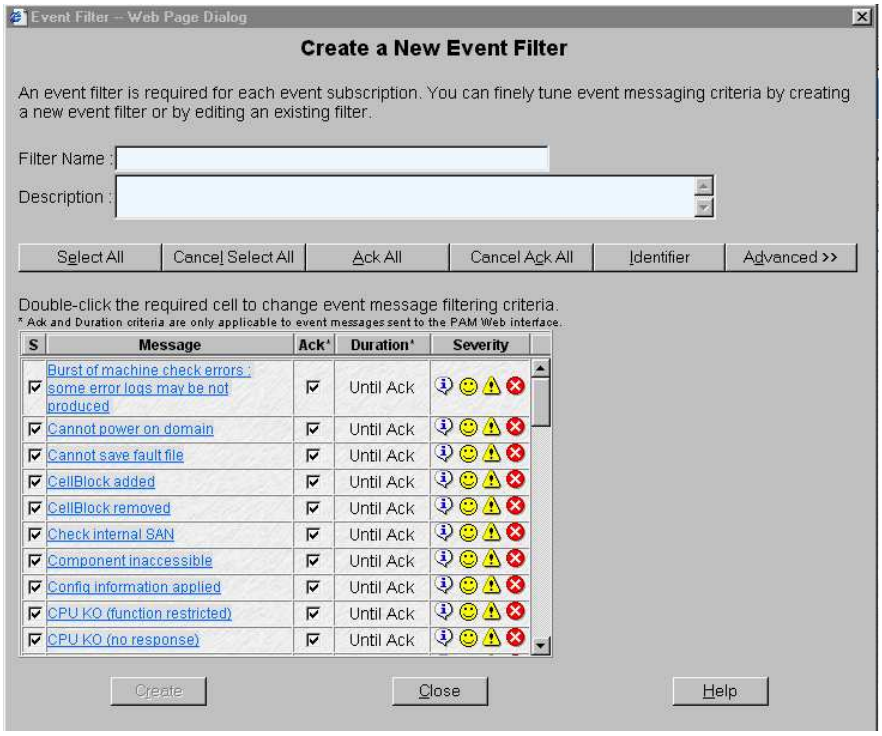


Figure 205. New Filter configuration page – standard event message filtering criteria table

3. Enter a relevant name in the **Filter Name** field and a brief description, if required, in the **Description** field.

Note:
For further details about event filtering criteria and options, see *Standard Event MessageFiltering Criteria*, on page 5-134 and *Advanced Event Message Filtering Criteria*, on page 5-137.

4. Deselect the **S** checkbox for the event messages not to be included in the filter.
5. If the filter is to be used to send messages to the PAM Web interface, select the **Ack** checkbox if you want the event message to be manually acknowledged by a user; or deselect the **Ack** checkbox to enter a display value in the **Duration** cell.
6. Double click the **Severity** cell to select the message severity level.

7. If required, click **Advanced** to access advanced filtering criteria. The advanced event message filtering criteria chart is displayed.

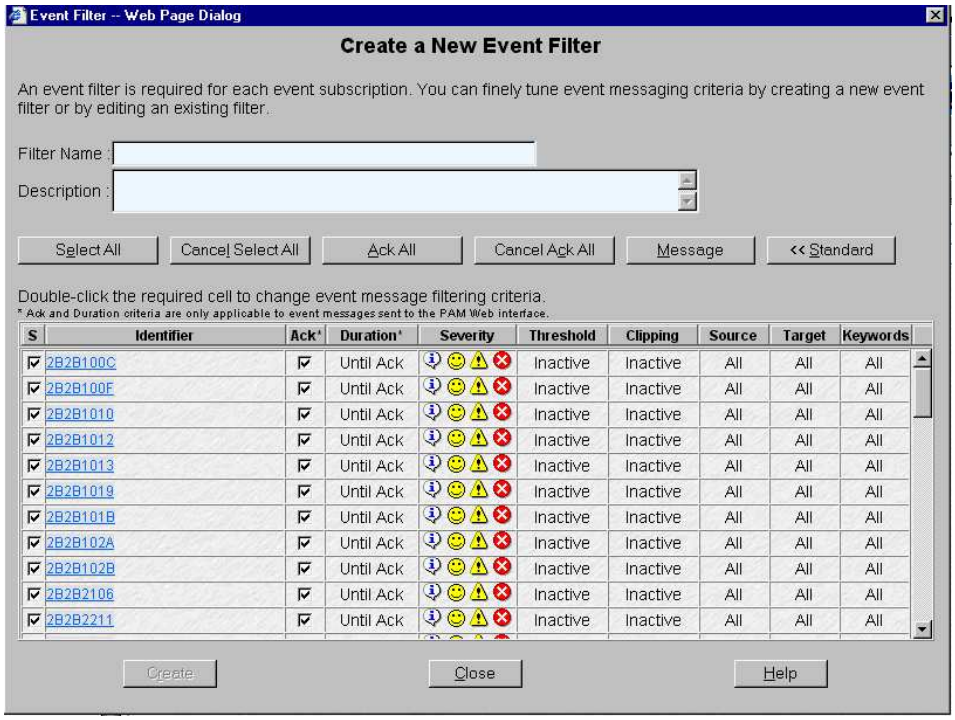


Figure 206. New Filter configuration page – advanced event message filtering criteria table

8. When you have finished configuring your event filter, click **Create**.
9. Repeat steps 3 to 8 for each new event filter you want to create.
10. Click **Close** to save changes. The new filter appears in the **Filters** list.

Editing Event Filter Attributes

1. Click **Configuration Tasks** → **Events**→ **Filters** in the PAM tree. The filter configuration page opens with the list of existing event message filters. See Figure 205 above.
2. Select the required filter from the event message filter list.
3. Click **Edit** in the toolbar to modify filter attributes.
4. Click **OK** to save changes.

Deleting an Event Filter

Important:
Before deleting an event filter, all the event subscriptions using that filter must either be modified to use another filter, or deleted.

1. Click **Configuration Tasks** → **Events**→ **Filters** in the PAM tree. The filter configuration page opens with the list of existing event message filters. See Figure 204 above.
2. Select the required filter from the event message filter list.
3. Click **Delete** in the toolbar.
4. Click **OK** to confirm the deletion of the selected event filter.

Creating, Editing, Deleting a User History

There are two types of histories: System histories and User histories.

System histories cannot be modified and are are only accessible to members of the Customer Administrator group.

User histories can be created, edited and deleted and are accessible to members of both the Customer Administrator and Customer Operator groups.

For guidance, System history contents are explained in the following table:

System History Contents

History Name	Contents
HistoryTrace	History Manager trace file. Logs archiving actions and history/archive processing errors.
InterventionReportHistory	Reserved for Support personnel.
IPMITrace	Reserved.
MaestroHistory	Reserved.
MaestroTrace	Reserved for Support personnel.
PAMHistory	Central PAM software history file. Logs all error or information messages concerning PAM software and all operator visible events.
PAMTrace	Logs domain power sequence trace data.
RPCTrace	Reserved for Support personnel.
SANTrace	Logs SAN–IT trace data.

Table 56. System history contents

Creating a User History

Note:
The Site Data Directory will be used, by default, if you do not specify a different directory when you create a user history. See *Viewing PAM Version Information*, on page 4-12

To create a user history:

1. Click **Configuration Tasks** → **Histories** in the PAM tree. The **Histories** control pane opens.
2. Click **New** in the toolbar. The **Create a New User History** dialog opens.

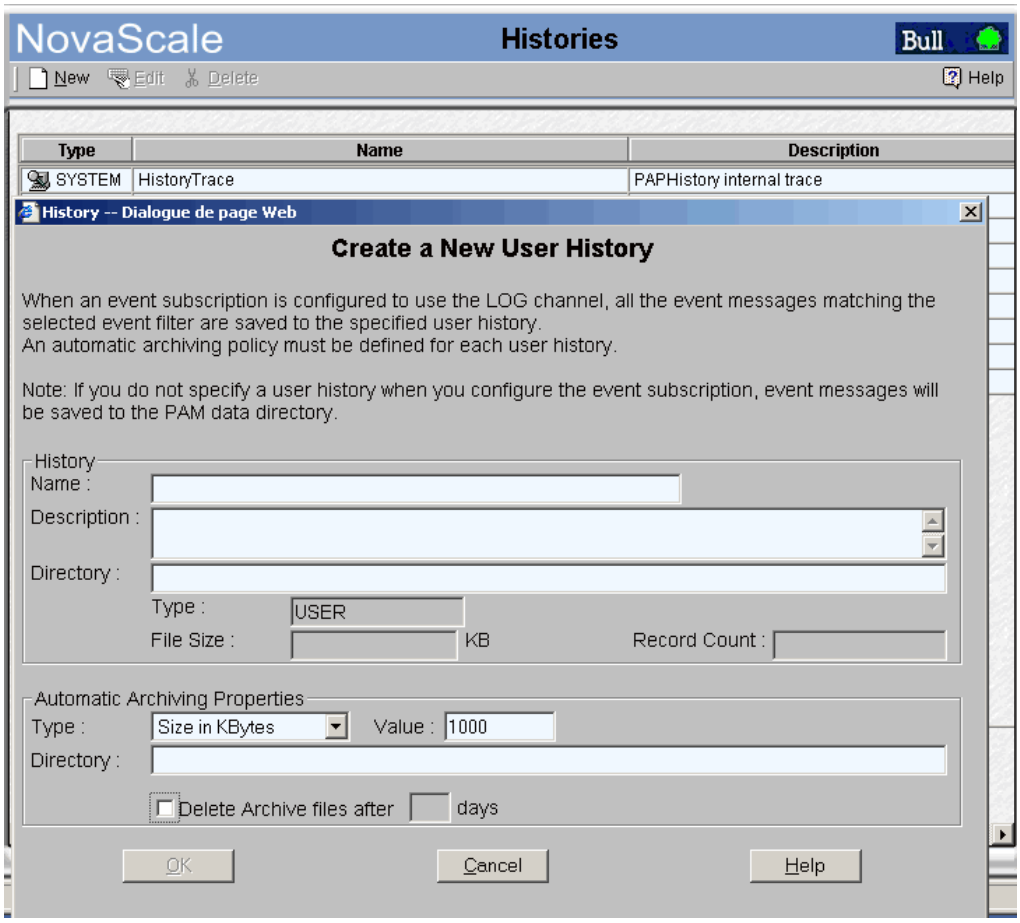


Figure 207. Create a New User History dialog

3. Enter a name in the **Name** field (mandatory) and a brief description, if required, in the **Description** field.
4. Enter a directory pathname in the **Directory** field. If this field is left blank, the default **Histories** directory will be used.

5. Use the drop–down menu to select an automatic archiving policy **Type**:

Type	Automatic Archiving Policy
Number of Days	The system will automatically create an archive for this history after the number of days specified in the **Value** field.
Size in KBytes	The system will automatically create an archive when this history reaches the size in KBytes specified in the **Value** field. **Note:** **Size in KBytes must be greater than 10.**
Number of Records	The system will automatically create an archive when this history reaches the number of records specified in the **Value** field. **Note:** **Number of Records must be greater than 10.**

Table 57. History automatic achiving policies

6. Enter the required number of days / KBytes / records in the **Value** field, as applicable.
7. Enter a directory pathname in the **Directory** field. If this field is left blank, the default **Archives** directory will be used.
8. If you want the archive to be automatically deleted at regular intervals, select the **Delete archive files** checkbox and enter the number of days you want to maintain the archive in the **days** field.
9. Click **OK** to confirm the creation of the new history. The new history appears in the list of available histories.

☞ **Note:**
The **OK** button is accessible once all mandatory fields have been completed.

Editing History Parameters

To modify the archiving parameters of system / user histories:

1. Click **Configuration Tasks** → **Histories** in the PAM tree. The **Histories** control pane opens.
2. Select the required History from the Histories list.
3. Click **Edit** in the toolbar to modify the archiving parameters for this History. The **Edit History Parameters** page opens.
4. Enter the new parameters in the corresponding fields.
5. Click **OK** to confirm the modification.

Deleting a User History

Important:
Before deleting a user history, all the event subscriptions attached to that history must be attached to another history, or deleted. System histories cannot be deleted.

If event subscriptions are attached to this history:

- see *Editing Event Subscription Attributes*, on page 5-131 to attach these event subscriptions to another history, or
- see *Deleting an Event Subscription*, on page 5-131 to delete these event subscriptions.

To delete a user history:

1. Check that no event subscriptions are attached to this history.
2. Click **Configuration Tasks** → **Histories** in the PAM tree. The **Histories** control pane opens.
3. Select the required History from the Histories list.
4. Click **Delete** in the toolbar.
5. Click **OK** to confirm the deletion of the selected user history.

Enabling / Disabling Event Channels

An event channel must be selected and enabled for all event subscriptions. The following table provides the Customer Administrator with guidelines for selecting an event channel.

Channel	Target	Enabled	Disabled
EMAIL	Specific recipient.	Allows a specific recipient to directly receive specific messages.	Advanced feature: Only to be used if the system generates too many messages and maintenance actions are to be carried out.
LOG (User History)	All user groups.	Allows all users to access specific messages.	
SNMP	SNMP application.	Forwards specific messages as SNMP traps to the selected SNMP application for processing.	
WEB (PAM Interface)	Selected users.	Allows a specific group of users to view specific messages.	

Table 58. Event channel selection guidelines

Note:
When an event channel is disabled, all messages sent via that channel are lost.
All event channels are enabled by default.

To enable / disable an event channel:

1. Click **Configuration Tasks** → **Events** → **Channels** in the PAM tree. The channels configuration page opens.

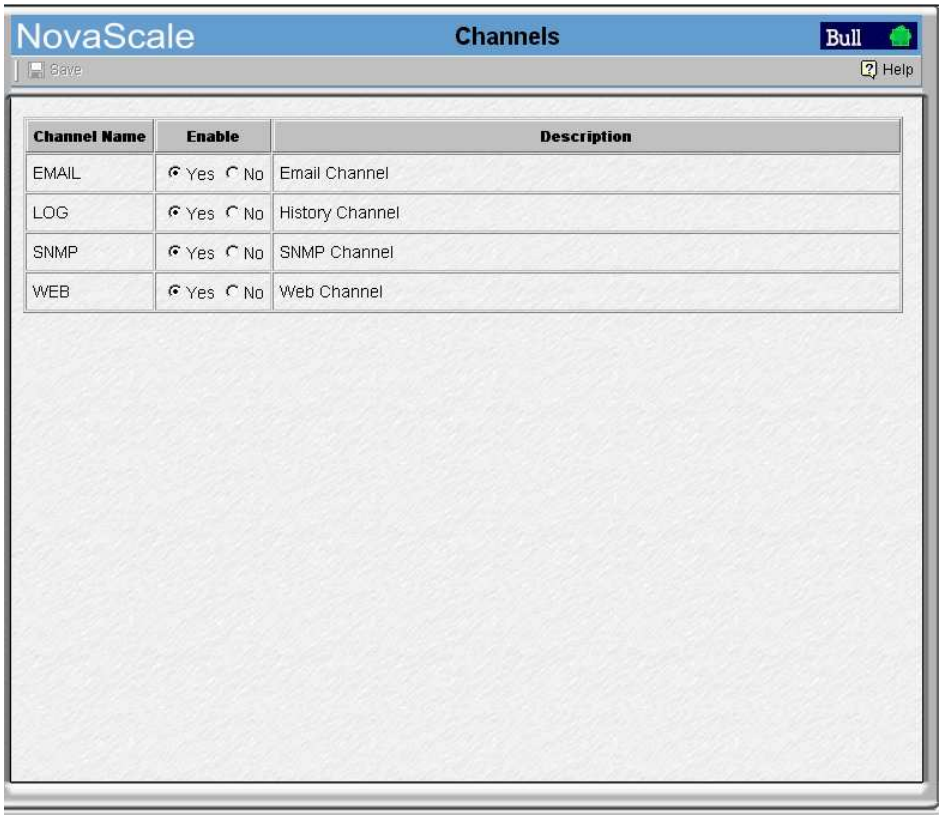


Figure 208. Event Channels configuration page

2. Select the **Yes** or **No** radio button in the **Enable** column to enable or disable the required channel.
3. Click the **Save** icon to confirm the new configuration.

Creating, Editing, Deleting an Event Subscription

Once event subscription prerequisites have been set up, you can create the event subscriptions required to send messages to their destinations. See *Event Subscription Flowcharts*, on page 5-116.

Creating an Event Subscription

To create an event subscription:

1. Click **Configuration Tasks** → **Events** → **Subscriptions** in the PAM tree. The event subscription configuration page opens.
2. Click **New** in the toolbar.

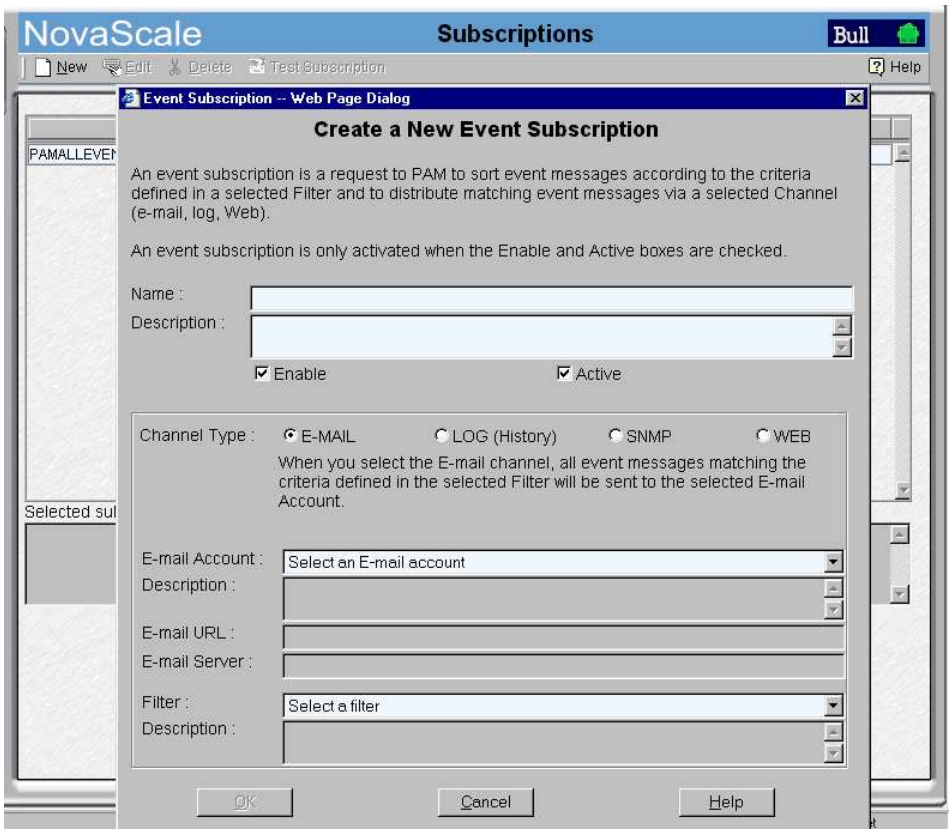


Figure 209. New Event Subscription dialog box

3. Select the **Active** and **Enable** checkboxes to activate and enable the new subscription.
4. Enter a short, readily identifiable name in the **Name** field and a brief description, if required, in the **Description** field.
5. Select the required channel radio button:
   - **E–MAIL**: to send event messages to an e–mail address.
   - **LOG**: to send event messages to a user history.
   - **SNMP**: to send event messages to the SNMP Manager.
   - **WEB**: to send event messages to the status pane in the PAM web interface.
6. Select a pre–configured E–mail Account, User History, or User Group from the drop–down menu or enter an SNMP Manager IP address or server name.
7. Select a pre–configured filter from the **Filter** drop–down menu.

8. Click **OK** to confirm the creation of the new event subscription.
9. The event subscription configuration page is automatically updated with the new subscription.
10. Click **Test Subscription** to check that the event subscription has been configured correctly. Subscription parameters will be used to send a test message.

Note:
The **OK** button is accessible once all mandatory fields have been completed.

Editing Event Subscription Attributes

To modify an event subscription description, channel, address and/or filter, or to activate / deactivate and/or enable / disable an event subscription:

1. Click **Configuration Tasks**→ **Events** → **Subscriptions** in the PAM tree. The event subscription configuration page opens.
2. Select the required event subscription in the event subscription table.
3. Click **Edit** to modify the attributes of this event subscription. The **Edit Event Subscription** dialog box opens.
4. Select the new channel, E–mail Account, User History, or User Group from the drop–down menu or enter a new SNMP Manager IP address or server name.
5. Modify the description.
6. If required, activate / deactivate and/or enable / disable the event subscription by selecting / deselecting the **Active** and **Enable** checkboxes.

Warning:
If you deactivate / disable an event subscription, no events will be sent to the recipient(s) until the event subscription is reactivated / re–enabled.

7. Click **OK** to confirm the modification.
8. Click **Test Subscription** to check that the event subscription has been re–configured correctly.

Note:
The **OK** button is accessible once all mandatory fields have been completed.

Deleting an Event Subscription

To delete an event subscription:

1. Click **Configuration Tasks** → **Events** → **Subscriptions** in the PAM tree. The event subscription configuration page opens.
2. Select the required event subscription in the event subscription table.
3. Click **Delete** in the toolbar. The **Delete Subscription** dialog box opens.
4. Click **OK** to confirm the deletion of the selected event subscription.

Understanding Event Message Filtering Criteria

The set of predefined filters supplied with PAM software covers everyday event messaging requirements. However, a comprehensive filtering system allows you to finely tune event messaging criteria, if required.

Before creating a new event filter, you should get to know filtering criteria options.

1. Click **Configuration Tasks** → **Events**→ **Filters** in the PAM tree. The filter configuration page opens with the list of existing event message filters.
2. Click **New** to display the **Standard Filter** page.

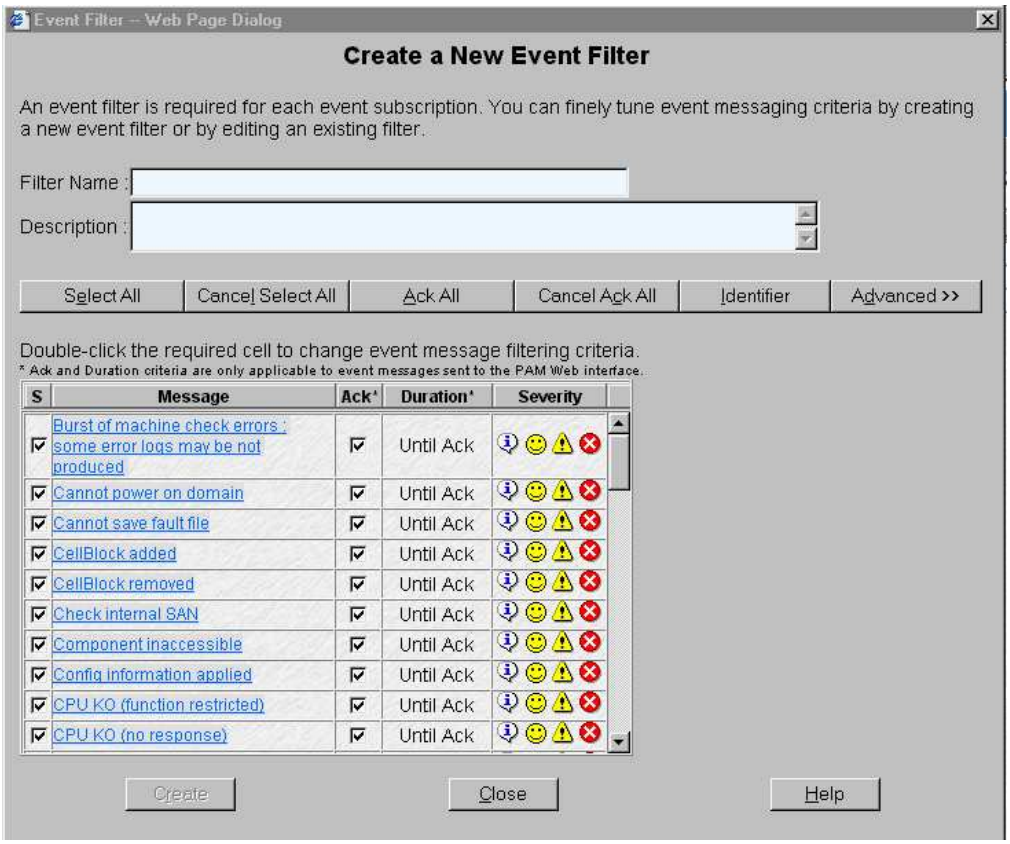


Figure 210. Event message standard filtering criteria chart

3. Click **Advanced** to display the **Advanced Filter** page.

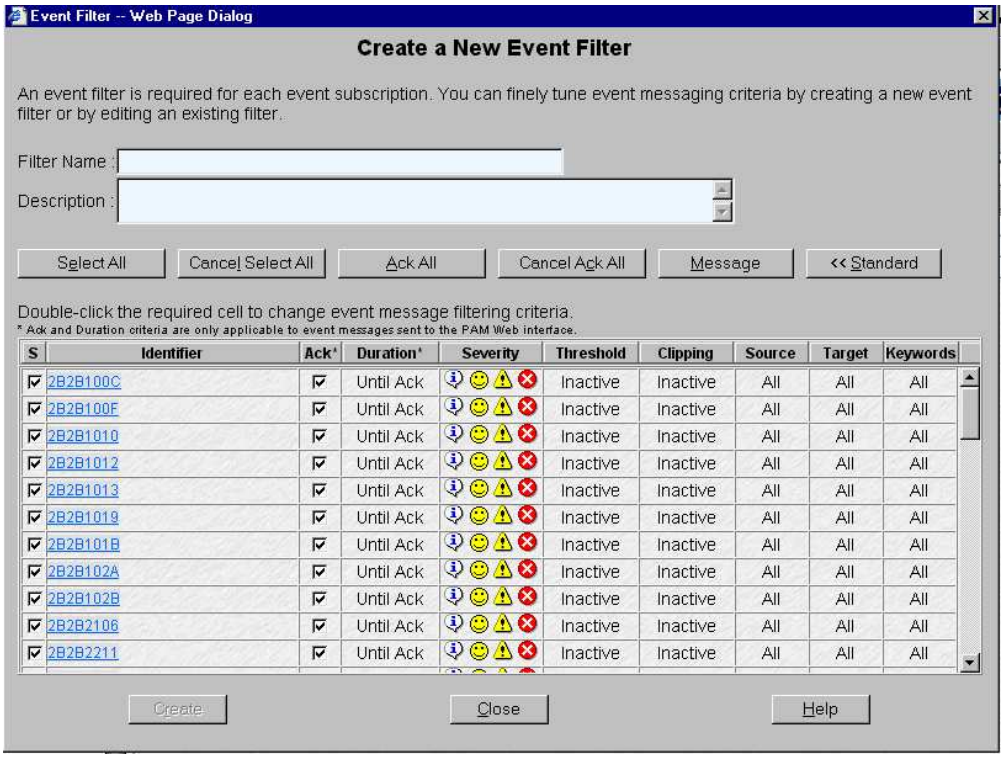
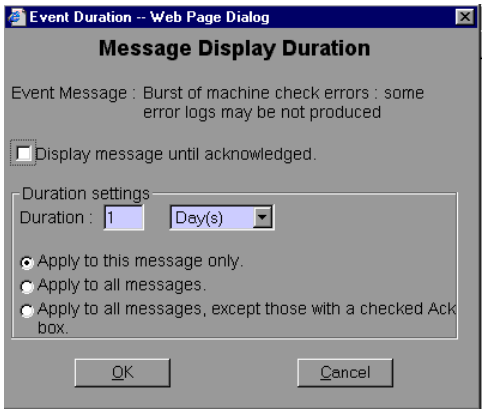


Figure 211. Event message advanced filtering criteria chart

4. Carefully analyze Tables 59 and 60 to understand the various options.

Standard Event Message Filtering Criteria

Criteria	Description
S (Select)	All the checkboxes in this column are selected by default. When an event message **S** checkbox is deselected, the event message is removed from the filter. **Actions** – Select the **S** checkbox if you want to include the event message in the new filter. – Deselect the **S** checkbox if you do not want to include the event message in the new filter.
Message/Identifier	Gives a message description and provides a clickable link to the associated help messages. **Actions** – Toggle the **Message/Identifier** column by clicking **Message** or **Identifier** in the toolbar. – Double click the required message. The corresponding help message opens.
Ack (Acknowledge)	This column is only applicable to messages sent to the PAM Web interface and is interactive with the **Duration** column (see below). All the checkboxes in this column are selected by default. When the message **Ack** checkbox is selected, the event message will be displayed in the event list until it is manually acknowledged by a user. **Note:** The PAM Web interface stores up to 150 event messages maximum per user group (100 messages by default). Once this limit has been reached, messages may be deleted in order of arrival, even if they have not been acknowledged. **Actions** – Select the **Ack** checkbox if you want the event message to be displayed until it is manually acknowledged by a user. – Deselect the **Ack** checkbox if you want the event message to be deleted automatically after a specified period of time. The **Duration** dialog box opens (see below).

Criteria	Description
Duration	This column is only applicable to messages sent to the PAM Web interface and is interactive with the **Ack** column (see above). When the specified duration expires, the event message is deleted automatically. **Note:** The PAM Web interface stores up to 150 event messages maximum per user group (100 by default). Once this limit has been reached, messages may be deleted in order of arrival, even if the set duration has not expired.  **Actions** – Double click the **Duration** cell to open the **Message Display Duration** dialog box. – Select the **Display message until acknowledged** checkbox if you want to manually acknowledge the message before it is removed from the display and click **OK** to apply. – Enter a value in the **Duration** field and use the drop–down menu to select the duration unit: seconds, minutes, hours, or days. – The **Apply to this message only** radio button is selected by default. If required, select another radio button to apply the duration setting to other messages included in the filter. – Click **OK** to set the duration. The new duration value is displayed in the **Duration** cell and the **Ack** checkbox is deselected (see above).

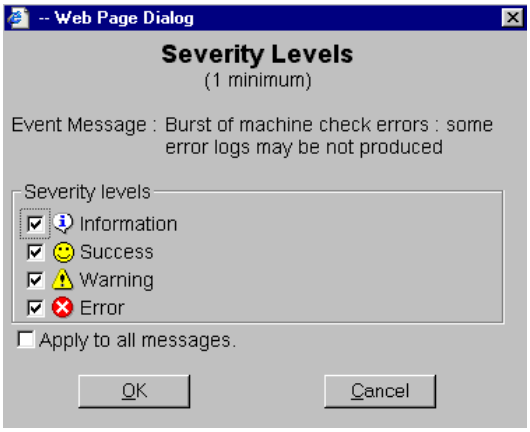
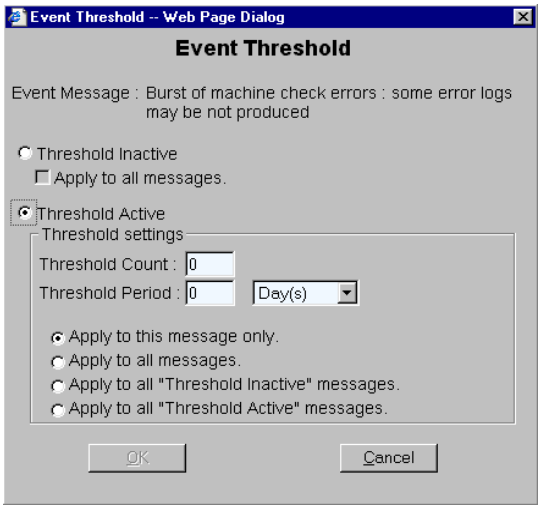
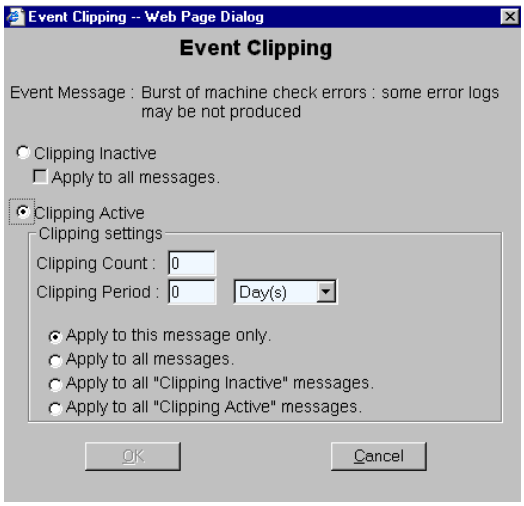
Criteria	Description
Severity Level	This column is used to set message severity level(s): **Information, Success, Warning,** and **Error**. At least one severity level must be selected to define the filter. **Actions** – Double click the **Severity** cell to open the dialog box.  – All severity levels are selected by default. Deselect the required checkbox to remove a severity level from the filter. – Select the **Apply to all messages** checkbox to apply this severity level to all the messages included in the filter. – Click **OK** to set and apply the severity level. The new severity level is displayed in the corresponding **Severity** cell.

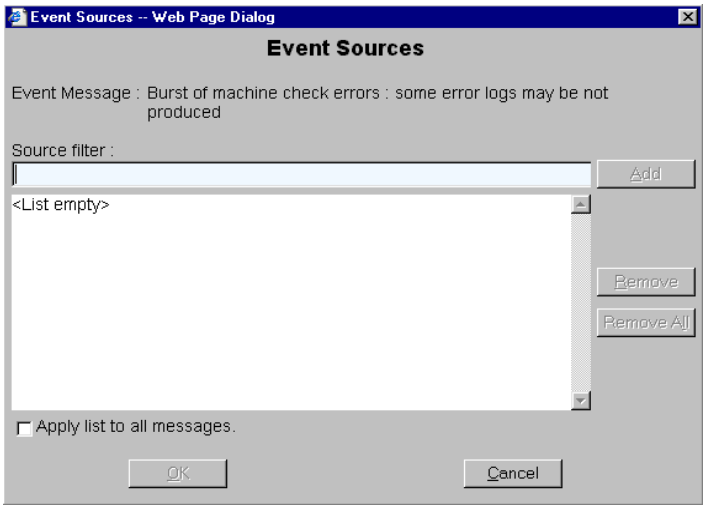
Table 59. Standard event message filtering criteria

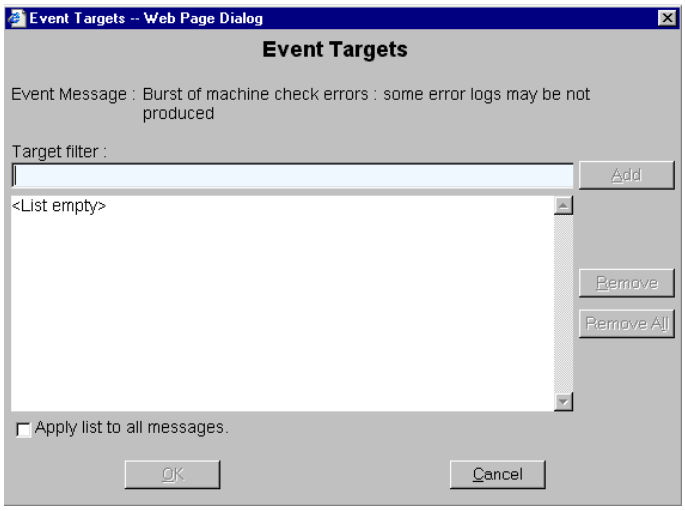
Advanced Event Message Filtering Criteria

Note:
Advanced filtering criteria are reserved for advanced users and are to be used with care.

Criteria	Description
Thresholding	Thresholding is defined on a Count / Period basis aimed at routing significant messages only. Identical messages are counted and when the number of messages indicated in the **Threshold Count** field is reached within the period of time indicated in the **Threshold Period** field, this message is selected for routing. **Actions** – Double click the **Threshold** cell to open the dialog box.  – Select the **Threshold Inactive** radio button to deactivate thresholding. – Select the **Apply to all messages** checkbox to deactivate the thresholding setting on all the messages included in the filter. – Select the **Threshold Active** radio button to activate thresholding. – Enter the required number of messages in the **Threshold Count** field, the required period of time in the **Threshold Period** field, and use the drop–down menu to select the time unit: seconds, minutes, hours, or days. – Select the corresponding radio button to apply thresholding settings to one or more messages included in the filter. **Note:** The **Apply to this message only** radio button is selected by default. – Click **OK** to set thresholding. The new **Threshold Count** and **Threshold Period** settings are displayed in the **Threshold** cell. **Note:** **Inactive** is displayed in the **Threshold** cell when thresholding is deactivated.

Criteria	Description
Clipping	Clipping is defined on a Count / Period basis aimed at routing a pre–defined number of messages only. Identical messages are counted and when the number of messages indicated in the **Clipping Count** field is reached within the period of time indicated in the **Clipping Period** field, no other messages will be selected for routing. **Actions** – Double click the **Clipping** cell to open the dialog box.  – Select the **Clipping Inactive** radio button to deactivate clipping. – Select the **Apply to all messages** checkbox to deactivate the thresholding setting on all the messages included in the filter. – Select the **Clipping Active** radio button to activate clipping. – Enter the required number of messages in the **Clipping Count** field, the required period of time in the **Clipping Period** field, and use the drop–down menu to select the time unit: seconds, minutes, hours, or days. – Select the corresponding radio button to apply clipping settings to one or more messages included in the filter. **Note:** The **Apply to this message only** radio button is checked by default. – Click **OK** to set clipping. The new **Clipping Count** and **Clipping Period** settings are displayed in the **Clipping** cell. **Note:** **Inactive** is displayed in the **Clipping** cell when clipping is deactivated.

Criteria	Description
Source	Each event message refers to a source (the component that generated the message) and a target (the component referred to in the message) (see below). This feature allows messages to be filtered according to one or more **Source** string(s) and is particularly useful for debugging and troubleshooting. **Actions** – Double click the **Source** cell to open the dialog box. – Select a source filter from the **Event Sources** list. – If the list is empty, enter a source string in the **Source filter** field and click **Add**. The new source filter is displayed in the **Event Sources** list. (Example source strings can be viewed in history files).  – Click **Remove** or **Remove All** to remove one or more source strings from the **Event Sources** list. – Repeat for each source string to be included in the filter. – Click **Apply list to all messages** to apply the specified source list to all the messages included in the filter. – Click **OK** to apply the source list. **Specified** is displayed in the **Source** cell. **Note:** **All** is displayed in the **Source** cell if the source is not specified.

Criteria	Description
Target	Each event message refers to a target (the component referred to in the message) and a source (the component that generated the message) (see above). This feature allows messages to be filtered according to one or more **Target** string(s) and is particularly useful for debugging and troubleshooting. **Actions** – Double click the **Target** cell to open the dialog box. – Select a target filter from the **Event Targets** list. – If the list is empty, enter a target string in the **Target filter** field and click **Add**. The new target filter is displayed in the **Event Targets** list. (Example target strings can be viewed in history files).  – Click **Remove** or **Remove All** to remove one or more target strings from the **Event Targets** list. – Repeat for each target string to be included in the filter. – Click **Apply list to all messages** to apply the specified target list to all the messages included in the filter. – Click **OK** to apply the target list. **Specified** is displayed in the **Target** cell. **Note:** **All** is displayed in the **Target** cell if the target is not specified.

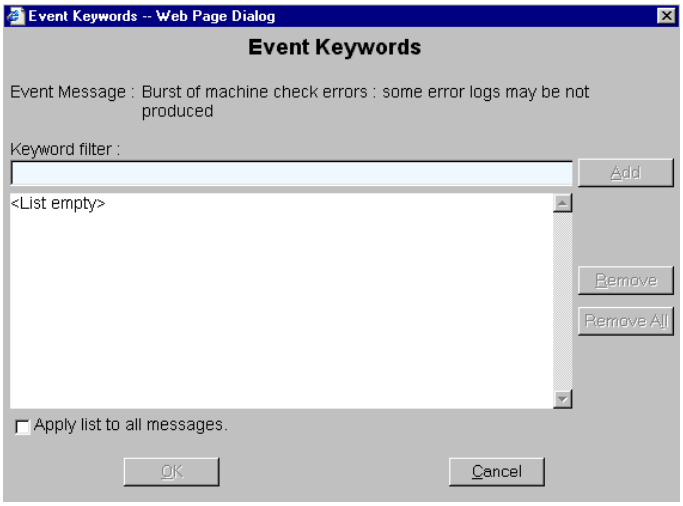
Criteria	Description
Keyword	This feature allows messages to be filtered according to a **Keyword** contained in the messages. Any relevant word(s) contained in source / target strings can be used. **Actions** – Double click the **Keywords** cell to open the dialog box. – Select a keyword filter from the **Event Keywords** list. – If the list is empty, enter a keyword in the **Keyword filter** field and click **Add**. The new keyword filter is displayed in the **Event Keywords** list. (Example keywords can be viewed in history files).  – Click **Remove** or **Remove All** to remove one or more keyword from the **Event Keywords** list. – Repeat for each keyword to be included in the filter. – Click **Apply list to all messages** to apply the specified keyword list to all the messages included in the filter. – Click **OK** to apply the keyword list. **Specified** is displayed in the **Keyword** cell. **Note:** **All** is displayed in the **Keywords** cell if the keyword is not specified.

Table 60. Advanced event message filtering criteria

Appendix A. Specifications

NovaScale 5080/5160 Server Specifications

NovaScale 5080/5160 Servers are delivered rack–mounted in 40U cabinets.
The following web site may be consulted for general site preparation information:
http://www.cs.bull.net/aise

Cabinet Dimensions / Weight	
Unpacked	**Packed**
1300H	**1300H**
Height: 195.5 cm (77.0 in)	Height: 200.0 cm (78.7 in)
Width: 60.0 cm (23.6 in)	Width: 80.0 cm (31.5 in)
Depth: 129.5 cm (51.0 in)	Depth: 140.0 cm (55.1 in)
Weight (max.): 943 kg (2079 lb)	Weight (max.): 973 kg (2145 lb)
Service Clearance	
Front	150 cm
Rear	100 cm
Side (left and right)	100 cm
Operating Limits	
Dry bulb temperature range	+15°C to +30°C (+59°F to +86°F) Gradient 5°C/h (41°F/h)
Relative humidity (non–condensing)	35 to 60% (Gradient 5%/h)
Max. wet bulb temperature	+24°C (+75.2°F)
Moisture content	0.019 kg water/kg dry air
Pressure / Elevation	Sea level ≤ 2500 m
Optimum Operational Reliability	
Temperature	+ 22°C (± 3°C) (+ 72°F (± 5°F)
Hygrometry	50% (± 5%)
Non–Operating Limits	
Dry bulb temperature range	+5°C to +50°C (+41°F to +122°F) Gradient 25°C/h (77°F/h)
Relative humidity (non–condensing)	5 to 95% (Gradient 30%)
Max. wet bulb temperature	+28°C (+82.4°F)
Moisture content	0.024 kg water/kg dry air
Shipping Limits	
Dry bulb temperature range	–35°C to +65°C (–31°F to +149°F) Gradient 25°C/h (77°F/h)
Relative humidity (non–condensing)	5 to 95% Gradient 30%/h
Acoustic Power at Room Temperature +20° C (+68° F)	
System Running	**System Idle**
Lw(A) 6.3 Bels	Lw(A) 6.1 Bels

Power Cables	
PDU–0–7–M–32A	
AC (32A)	1 per PDU
Cable type	3 x AWG10 (3 x 6 mm^2 / #10US)
Connector type	IEC60309–32A
CSS Module	
AC (20A)	1 per CSS Module
Cable type	3 x AWG12 (3 x 4mm^2 / #12US)
Connector type	IEC60309–32A
It is mandatory for power lines and terminal boxes to be located within the immediate vicinity of the system and to be easily accessible. Each power line must be connected to a separate, independent electrical panel and bipolar circuit breaker. PDUs require an extra cable length of 1.5 meters for connection inside the cabinet.	
Electrical Specifications (power supplies are auto–sensing and auto–ranging)	
Current draw	15 A max. at 200 VAC input
Power consumption	3000 VA (per full CSS module) 1500 VA (per PDU)
Thermal dissipation	2700 W / 9250 BTU (per full CSS module) 1300 W / 4610 BTU (per PDU
Europe	
Nominal voltage	230 VAC (Phase / Neutral)
Voltage range	207 – 244 VAC
Frequency	50 Hz $\pm$ 1%
United States of America	
Nominal voltage	208 VAC (Phase / Neutral)
Voltage range	182 – 229 VAC
Frequency	60 Hz $\pm$ 0.3%
Japan	
Nominal voltage	200 VAC (Phase / Neutral)
Voltage range	188 – 212 VAC
Frequency	60 Hz $\pm$ 0.2%
Brazil	
Nominal voltage	220 VAC (Phase / Neutral)
Voltage range	212 – 231 VAC
Frequency	60 Hz $\pm$ 2%
Breaker Protection (Mains Power)	
CSS module	20A Curve C
PDU–20A	20A Curve C
PDU–0–7–M–32A	32A Curve C
Maximum inrush current	210A / per quarter period

Table 61. NovaScale 5080/5160 Server specifications

NovaScale 6080/6160 Server Specifications

The following web site may be consulted for general site preparation information:
http://www.cs.bull.net/aise

NovaScale 6080/6160 Servers are delivered rack–mounted in 40U cabinets.

Cabinet Dimensions / Weight	
Unpacked	**Packed**
1300H	**1300H**
Height: 195.5 cm (77.0 in)	Height: 200.0 cm (78.7 in)
Width: 60.0 cm (23.6 in)	Width: 80.0 cm (31.5 in)
Depth: 129.5 cm (51.0 in)	Depth: 140.0 cm (55.1 in)
Weight (max.): 943 kg (2079 lb)	Weight (max.): 973 kg (2145 lb)
Service Clearance	
Front	150 cm
Rear	100 cm
Side (left and right)	100 cm
Operating Limits	
Dry bulb temperature range	+15°C to +30°C (+59°F to +86°F) Gradient 5°C/h (41°F/h)
Relative humidity (non–condensing)	35 to 60% (Gradient 5%/h)
Max. wet bulb temperature	+24°C (+75.2°F)
Moisture content	0.019 kg water/kg dry air
Pressure / Elevation	Sea level ≤ 2500 m
Optimum Operational Reliability	
Temperature	+ 22°C (± 3°C) (+ 72°F (± 5°F)
Hygrometry	50% (± 5%)
Non–Operating Limits	
Dry bulb temperature range	+5°C to +50°C (+41°F to +122°F) Gradient 25°C/h (77°F/h)
Relative humidity (non–condensing)	5 to 95% (Gradient 30%)
Max. wet bulb temperature	+28°C (+82.4°F)
Moisture content	0.024 kg water/kg dry air
Shipping Limits	
Dry bulb temperature range	–35°C to +65°C (–31°F to +149°F) Gradient 25°C/h (77°F/h)
Relative humidity (non–condensing)	5 to 95% Gradient 30%/h
Acoustic Power at Room Temperature +20° C (+68° F)	
System Running	**System Idle**
Lw(A) 6.3 Bels	Lw(A) 6.1 Bels

Power Cables	
PDU–0–7–M–32A	
AC (32A)	1 per PDU
Cable type	3 x AWG10 (3 x 6 mm^2 / #10US)
Connector type	IEC60309–32A
CSS Module	
AC (20A)	1 per CSS Module
Cable type	3 x AWG12 (3 x 4mm^2 / #12US)
Connector type	IEC60309–32A
It is mandatory for power lines and terminal boxes to be located within the immediate vicinity of the system and to be easily accessible. Each power line must be connected to a separate, independent electrical panel and bipolar circuit breaker. PDUs require an extra cable length of 1.5 meters for connection inside the cabinet.	
Electrical Specifications (power supplies are auto–sensing and auto–ranging)	
Current draw	15 A max. at 200 VAC input
Power consumption	3000 VA (per full CSS module) 1500 VA (per PDU)
Thermal dissipation	2700 W / 9250 BTU (per full CSS module) 1300 W / 4610 BTU (per PDU
Europe	
Nominal voltage	230 VAC (Phase / Neutral)
Voltage range	207 – 244 VAC
Frequency	50 Hz $\pm$ 1%
United States of America	
Nominal voltage	208 VAC (Phase / Neutral)
Voltage range	182 – 229 VAC
Frequency	60 Hz $\pm$ 0.3%
Japan	
Nominal voltage	200 VAC (Phase / Neutral)
Voltage range	188 – 212 VAC
Frequency	60 Hz $\pm$ 0.2%
Brazil	
Nominal voltage	220 VAC (Phase / Neutral)
Voltage range	212 – 231 VAC
Frequency	60 Hz $\pm$ 2%
Breaker Protection	
CSS module	20A Curve C
PDU–20A	20A Curve C
PDU–0–7–M–32A	32A Curve C
Maximum inrush current	210A / per quarter period

Table 62. NovaScale 6080/6160 Server specifications

NovaScale 6320 Server Specifications

The following web site may be consulted for general site preparation information:
http://www.cs.bull.net/aise

NovaScale 6320 Servers are delivered rack–mounted in 40U cabinets.

Cabinet Dimensions / Weight	
Unpacked	**Packed**
1300H	**1300H**
Height: 195.5 cm (77.0 in)	Height: 200.0 cm (78.7 in)
Width: 60.0 cm (23.6 in)	Width: 80.0 cm (31.5 in)
Depth: 129.5 cm (51.0 in)	Depth: 140.0 cm (55.1 in)
Weight (max.): 943 kg (2079 lb)	Weight (max.): 973 kg (2145 lb)
Service Clearance	
Front	150 cm
Rear	100 cm
Side (free side)	100 cm
Operating Limits	
Dry bulb temperature range	+15°C to +30°C (+59°F to +86°F) Gradient 5°C/h (41°F/h)
Relative humidity (non–condensing)	35 to 60% (Gradient 5%/h)
Max. wet bulb temperature	+24°C (+75.2°F)
Moisture content	0.019 kg water/kg dry air
Pressure / Elevation	Sea level ≤ 2500 m
Optimum Operational Reliability	
Temperature	+ 22°C (± 3°C) (+ 72°F (± 5°F)
Hygrometry	50% (± 5%)
Non–Operating Limits	
Dry bulb temperature range	+5°C to +50°C (+41°F to +122°F) Gradient 25°C/h (77°F/h)
Relative humidity (non–condensing)	5 to 95% (Gradient 30%)
Max. wet bulb temperature	+28°C (+82.4°F)
Moisture content	0.024 kg water/kg dry air
Shipping Limits	
Dry bulb temperature range	–35°C to +65°C (–31°F to +149°F) Gradient 25°C/h (77°F/h)
Relative humidity (non–condensing)	5 to 95% Gradient 30%/h
Acoustic Power at Room Temperature +20° C (+68° F)	
System Running	**System Idle**
Lw(A) 6.3 Bels	Lw(A) 6.1 Bels

Power Cables	
PDU–0–7–M–32A	
AC (32A)	1 per PDU
Cable type	3 x AWG10 (3 x 6 mm^2 / #10US)
Connector type	IEC60309–32A
CSS Module	
AC (20A)	1 per CSS Module
Cable type	3 x AWG12 (3 x 4mm^2 / #12US)
Connector type	IEC60309–32A
It is mandatory for power lines and terminal boxes to be located within the immediate vicinity of the system and to be easily accessible. Each power line must be connected to a separate, independent electrical panel and bipolar circuit breaker. PDUs require an extra cable length of 1.5 meters for connection inside the cabinet.	
Electrical Specifications (power supplies are auto–sensing and auto–ranging)	
Current draw	15 A max. at 200 VAC input
Power consumption	3000 VA (per full CSS module) 1500 VA (per PDU)
Thermal dissipation	2700 W / 9250 BTU (per full CSS module) 1300 W / 4610 BTU (per PDU)
Europe	
Nominal voltage	230 VAC (Phase / Neutral)
Voltage range	207 – 244 VAC
Frequency	50 Hz $\pm$ 1%
United States of America	
Nominal voltage	208 VAC (Phase / Neutral)
Voltage range	182 – 229 VAC
Frequency	60 Hz $\pm$ 0.3%
Japan	
Nominal voltage	200 VAC (Phase / Neutral)
Voltage range	188 – 212 VAC
Frequency	60 Hz $\pm$ 0.2%
Brazil	
Nominal voltage	220 VAC (Phase / Neutral)
Voltage range	212 – 231 VAC
Frequency	60 Hz $\pm$ 2%
Breaker Protection	
CSS module	20A Curve C
PDU–20A	20A Curve C
PDU–0–7–M–32A	32A Curve C
Maximum inrush current	210A / per quarter period

Table 63. NovaScale 6320 Server specifications

Glossary

A

AC: Alternating **C**urrent generated by the power supply. See DC.

ACPI: Advanced **C**onfiguration and **P**ower **I**nterface. An industry specification for the efficient handling of power consumption in desktop and mobile computers. ACPI specifies how a computer's BIOS, operating system, and peripheral devices communicate with each other about power usage.

Address: A label, name or number that identifies a location in a computer memory.

AMI: American **M**egatrends **I**ncorporated.

ANSI: American **N**ational **S**tandards **I**nstitute.

API: Application **P**rogram **I**nterface. The specific method prescribed by a computer operating system or by an application program by which a programmer writing an application program can make requests of the operating system or another application.

Archive: (Archive file). A file that is a copy of a history file. When a history file is archived, all messages are removed from the history file.

ASCII: American **N**ational **S**tandard **C**ode for **I**nformation **I**nterchange. A standard number assigned to each of the alphanumeric characters and keyboard control code keys to enable the transfer of information between different types of computers and peripherals.

B

Backup: A copy of data for safe–keeping. The data is copied form computer memory or disk to a floppy disk, magnetic tape or other media.

Backup battery: The battery in a computer that maintains real–time clock and configuration data when power is removed.

Baud rate: The speed at which data is transmitted during serial communication.

BERR: Bus Error signal pin used to signal a global machine check abort condition.

BINIT: Bus Initialization signal pin used to signal a global fatal machine check condition.

BIOS: Basic **I**nput / **O**utput **S**ystem. A program stored in flash EPROM or ROM that controls the system startup process.

BIST: Built–**I**n **S**elf–**T**est. See POST.

Bit: Derived from **BI**nary digi**T**. A bit is the smallest unit of information a computer handles.

BTU: British Thermal Unit.

Byte: A group of eight binary digits (bit) long that represents a letter, number, or typographic symbol.

C

Cache Memory: A very fast, limited portion of RAM set aside for temporary storage of data for direct access by the microprocessor.

CD-ROM: Compact **D**isK **R**ead-**O**nly **M**emory. High-capacity read-only memory in the form of an optically readable compact disk.

Cell: The smallest set of hardware components allocated to a single OS. A cell is functionally defined by:
– the number of available processors
– memory capacity
– I/O channel capacity.

CellBlock: A group of interconnected cells within a single domain. See Central Subsystem.

Central Subsystem: A group of interconnected cells gathered within a single domain. See CellBlock.

Chip: Synonym for integrated circuit. See IC.

Clipping: A PAM Event filter criterion. Clipping is defined on a Count / Time basis aimed at routing a pre–defined number of messages only. Identical messages are counted and when the number of messages indicated in the **Count** field is reached within the period of time indicated in the **Time** field, no other messages will be selected for routing.

CMC: Corrected **M**emory **C**heck condition is signaled when a hardware corrects a machine check error or when a MCA condition is corrected by firmware.

CMCI: Corrected **M**emory **C**heck **I**nterrupt.

CMCV: Corrected **M**emory **C**heck **V**ector.

CMOS: Complementary **M**etal **O**xide **S**emiconductor. A type of low–power integrated circuits. System startup parameters are stored in CMOS memory. They can be changed via the system setup utility.

COM: Component **O**bject **M**odel. Microsoft technology for component based application development under Windows.

COM +: Component **O**bject **M**odel +. Microsoft technology for component based application development under Windows. The external part of the PAM software package is a COM+ application.

COM1 or COM2: The name assigned to a serial port to set or change its address. See Serial Port.

Command: An instruction that directs the computer to perform a specific operation.

Configuration: The way in which a computer is set up to operate. Configurable options include CPU speed, serial port designation, memory allocation, ...

Configuration Tasks: A PAM feature used to configure and customize the server.

Control Pane: One of the three areas of the PAM web page. When an item is selected in the **PAM Tree** pane, details and related commands are displayed in the **Control** pane. See PAM Tree pane and Status pane.

Core Unit: A main CSS module unit interconnecting the MIO, MQB, MSX and MFL boards. See MIO, MQB, MSX, MFL.

COS: Cluster **O**perating **S**ystem.

CPE: Corrected **P**latform **E**rror.

CPEI: Corrected **P**latform **E**rror **I**nterrupt.

CPU: Central **P**rocessing **U**nit. See Microprocessor.

CSE: Customer **S**ervice **E**ngineer.

CSS: Central **S**ub–**S**ystem. See CellBlock.

CSS Module: A MidPlane with all its connected components (QBBs, IO boards, PMB) and utility devices. See Module.

D

D2D: DC **to D**C converter.

DC: Direct **C**urrent generated by the power supply. See AC.

Default Setting: The factory setting your server uses unless instructed otherwise.

Density: The capacity of information (bytes) that can be packed into a storage device.

Device Driver: A software program used by a computer to recognize and operate hardware.

DIB: Device **I**nterface **B**oard. The DIB provides the necessary electronics for the Internal Peripheral Drawer. See IPD.

DIG64: Developer **I**nterface **G**uide for IA64.

DIM Code: Device **I**nitialization **M**anager. Initializes different BUSes during the BIOS POST.

DIMM: Dual **I**n-line **M**emory **M**odule – the smallest system memory component.

Disk Drive: A device that stores data on a hard or floppy disk. A floppy disk drive requires a floppy disk to be inserted. A hard disk drive has a permanently encased hard disk.

DMA: Direct **M**emory **A**ccess. Allows data to be sent directly from a component (e.g. disk drive) to the memory on the motherboard). The microprocessor does not take part in data transfer enhanced system performance.

DMI: Desktop **M**anagement **I**nterface. An industry framework for managing and keeping track of hardware and software components in a system of personal computers from a central location.

DNS: Domain **N**ame **S**erver. A server that retains the addresses and routing information for TCP/IP LAN users.

Domain: is the coherent set of resources allocated to run a customer activity, i.e. the association –at boot time– of a Partition, an OS instance (including applications) and associated LUNs and an execution context including execution modes and persistent information (e.g. time, date of the OS instance). Domain definitions and initializations are performed via PAM. A Domain can be modified to run the same OS instance on a different Partition. When a Domain is running, its resources are neither visible nor accessible to other running Domains.

Domain Identity: a PAM Domain management logical resource. This resource contains context information related to the Customer activity running in a domain. The most visible attribute of this resource is the name that the Customer gives to the activity. For each domain created, the Domain management feature allows the operator to define a new activity or choose an activity from the list of existing activities. See Domain.

Domain Manager: A PAM feature used to power on / off and manage server domains. See Domain.

DPS: Distributed **P**ower **S**upply.

DRAM: Dynamic Random Access Memory is the most common type of random access memory (RAM).

E

ECC: Error **C**orrecting **C**ode.

EEPROM: Electrically **E**rasable **P**rogrammable **R**ead-**O**nly **M**emory. A type of memory device that stores password and configuration data. See also EPROM.

EFI: Extensible **F**irmware **I**nterface.

EFIMTA: EFI Modular **T**est **A**rchitecture.

EFI Shell: The EFI (Extensible Firmware Interface) Shell is a simple, interactive user interface that allows EFI device drivers to be loaded, EFI applications to be launched, and operating systems to be booted. In addition, the EFI Shell provides a set of basic commands used to manage files and the system environment variables. See Shell.

EMI: Electro–**M**agnetic **I**nterference.

EPROM: Erasable **P**rogrammable **R**ead-**O**nly **M**emory. A type of memory device that is used to store the system BIOS code. This code is not lost when the computer is powered off.

ERC: Error and **R**eset **C**ontroller. This controller allows PAM software to control error detection and reset propagation within each pre–defined CSS partition. The ERC is initialized by PAM software to ensure a partition–contained distribution of the reset, error, interrupt and event signals; and to contribute to error signaling and localization at platform level.

ERP: Error **R**ecovery **P**rocedure.

ESD: Electro**S**tatic **D**ischarge. An undesirable discharge of static electricity that can damage equipment and degrade electrical circuitry.

Event: The generation of a message (event message) by a software component and that is directed to the Event Manager.

Event address: Defines the destination for a message sent over a specified event channel. An address is one of: the name of a history file (for the HISTORY channel), an e–mail address (for the EMAIL channel), the name of a user group (for the WEB channel), the SNMP Manager IP address (for the SNMP channel).

Event channel: Defines how the Event Manager sends an event message. An event channel is one of: HISTORY (the message is logged in a history file), EMAIL (the message is sent to an e–mail address), WEB (the message is stored for analysis from the PAM web user interface), SNMP (the message is sent as an SNMP trap to the selected SNMP application).

Event filter: A list of selected messages among all possible event messages. If an event message is not included in the filter, the Event Manager discards the message.

Event Manager: A PAM feature used to forward event messages over a configured event channel. See Event.

Event message: A message sent by a software component to the Event Manager for routing to a destination that is configured by an administrator.

Event subscription: An object that defines the event channel, address, and filter for sending an event message. If no such object is defined, the event message is discarded.

Exclusion: Logical removal of a redundant faulty hardware element until it has been repaired or replaced. The hardware element remains physically present in the configuration, but is no longer detected by PAM software and can no longer be used by a domain.

External Disk Subsystem: Disk subsystem housed inside the NovaScale cabinet.

F

Fail–over: Failover is a backup operational mode in which the functions of a system component (such as a processor, server, network, or database, for example) are assumed by secondary system components when the primary component becomes unavailable through either failure or scheduled down time.

FAME: Flexible **A**rchitecture for **M**ultiple **E**nvironments.

FAST WIDE: A standard 16–bit SCSI interface providing synchronous data transfers of up to 10 MHz, with a transfer speed of 20M bytes per second.

FC: Fibre **C**hannel.

FCAL: Fibre **C**hannel **A**rbitrated **L**oop.

FCA: Fibre **C**hannel **A**dapter.

FCBQ: Fan **C**ontrol **B**oard for **Q**BB.

FCBS: Fan **C**ontrol **B**oard for **S**PS.

FDA: Fibre **D**isk **A**rray.

FDD: Floppy **D**isk **D**rive.

Flash EPROM: Flash Erasable Programmable Read-Only Memory. A type of memory device that is used to store the the system firmware code. This code can be replaced by an updated code from a floppy disk, but is not lost when the computer is powered off.

Firewall: A set of related programs, located at a network gateway server, that protects the resources of a private network from users from other networks.

Firmware: an ordered set of instructions and data stored to be functionally independent of main storage.

Format: The process used to organize a hard or floppy disk into sectors so that it can accept data. Formatting destroys all previous data on the disk.

FPB: FAME **P**ower **B**oard (FAME: Flexible Architecture for Multiple Environments).

FPGA: Field **P**rogrammable **G**ate **A**rray. A gate array that can reprogrammed at run time.

FRB: Fault **R**esilient **B**oot. A server management feature. FRB attempts to boot a system using the alternate processor or DIMM.

FRU: Field **R**eplaceable **U**nit. A component that is replaced or added by Customer Service Engineers as a single entity.

FSS: FAME **S**calability **S**witch. Each CSS Module is equipped with 2 Scalability Port Switches providing high speed bi–directional links between server components. See SPS.

FTP: File **T**ransfer **P**rotocol. A standard Internet protocol: the simplest way of exchanging files between computers on the Internet. FTP is an application protocol that uses Internet TCP/IP protocols. FTP is commonly used to transfer Web page files from their creator to the computer that acts as their server for everyone on the Internet. It is also commonly used to download programs and other files from other servers.

FWH: Firm**W**are **H**ub.

G

GB: Giga**B**yte: 1,073,741,824 bytes. See Byte.

Global MCA: Machine **C**heck **A**bort is visible to all processors, in a multiprocessor system and will force all of them to enter machine check abort.

GUI: Graphical **U**ser **I**nterface.

GTS: Global **T**elecontrol **S**erver.

H

HA: High **A**vailability. Refers to a system or component that is continuously operational for a desirably long length of time.

HAL: Hardware **A**bstraction **L**ayer.

HA CMP: High **A**vailability **C**lustered **M**ulti**P**rocessing.

Hard Disk Drive: HDD. See Disk Drive.

Hardware: The physical parts of a system, including the keyboard, monitor, disk drives, cables and circuit cards.

Hardware Monitor: A PAM feature used to supervise server operation.

HBA: Host **B**us **A**dapter.

HDD: Hard **D**isk **D**rive. See Disk Drive.

History File: A file in which the History Manager logs informative messages or error messages relating to system activity. Messages are sent from source components to target components.

History Manager: The component running on the PAP Windows operating system that logs messages to history files.

HMMIO Space: High Memory IO Space.

HPB: Hot **P**lug **B**oard. This board provides an interlock switch on each IO Box PCI slot for hot–swapping PCI boards. See P–HPB.

HPC: High **P**erformance **C**omputing.

Hot plugging: The operation of adding a component without interrupting system activity.

Hot swapping: The operation of removing and replacing a faulty component without interrupting system activity.

HTTP: Hyper**T**ext **T**ransfer **P**rotocol. In the World Wide Web, a protocol that facilitates the transfer of hypertext–based files between local and remote systems.

HW Identifier: Number (0 – F) used to identify Cellblock components. This number is identical to PMB code–wheel position.

I

I2C: Intra **I**ntegrated **C**ircuit. The I2C (Inter–IC) bus is a bi–directional two–wire serial bus that provides a communication link between integrated circuits (ICs).
The I2C bus supports 7–bit and 10–bit address space devices and devices that operate under different voltages.

IA64: is a **64**–bit **I**ntel processor **A**rchitecture based on Explicitly Parallel Instruction Computing (EPIC). The Itanium processor is the first in the Intel line of IA–64 processors.

IB: Infini **B**and.

IC: Integrated **C**ircuit. An electronic device that contains miniaturized circuitry. See Chip.

ICH2: I/O **C**ontroller **H**ub 2, component that contains the fundamental I/O interfaces required by the system. Flash memory, Keyboard, USB and IDE device interface.

ICH4: I/O **C**ontroller **H**ub 4.

ICMB: Intelligent **C**hassis **M**anagement **B**us.

ID: A number which uniquely identifies a device on a bus.

IDE: Integrated **D**rive **E**lectronics. A type of hard disk drive with the control circuitry located inside the disk drive rather than on a drive controller card.

Identity: See Domain Identity.

IIS: Internet **I**nformation **S**erver. A group of Internet servers (including a Web or HTTP server and a FTP server) with additional capabilities for Microsoft Windows NT and Microsoft Windows (and later) operating systems.

I/O: Input /**O**utput. Describes any operation, program, or device that transfers data to or from a computer.

Interface: A connection between a computer and a peripheral device enabling the exchange of data. See Parallel Port and Serial Port.

Internal Disk Subsystem: Disk subsystem housed inside the NovaScale Internal Peripheral Drawer (IPD).

IOB: Input / **O**utput **B**oard. The IOB connects up to 11 PCI–X boards.

IOC: Input / **O**utput Board **C**ompact. The IOC connects up to 6 PCI–X boards.

IOL: I/O Board **L**egacy. The IOL provides:
– I/O controller Hub
– USB ports
– 10/100/1000 Ethernet controller
– Video controller
– Serial / debug port

IOR: I/O Board **R**iser. The IOR provides:
– I/O controller Hub
– USB ports
– 10/100/1000 Ethernet controller
– Video controller
– Serial / debug port

IP: Internet **P**rotocol. The protocol by which data is sent from one computer to another via the Internet. Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it from all other computers on the Internet.

IPD: Internal **P**eripheral **D**rawer. The IPD houses legacy peripherals (DVD–Rom drive, USB port) and SCSI system disks.

IPF: Itanium **P**rocessor **F**amily.

IPL: Initial **P**rogram **L**oad. It defines the firmware functional phases during the system initialization.

IPMB: Intelligent **P**latform **M**anagement **B**us.

IPMI: Intelligent **P**latform **M**anagement **I**nterface.

ISA: Industry **S**tandard **A**rchitecture. An industry standard for computers and circuit cards that transfer 16 bits of data at a time.

J

Jumper: A small electrical connector used for configuration on computer hardware.

K

KVM: Keyboard **V**ideo **M**onitor.

KVM switch: the **K**eyboard **V**ideo **M**onitor switch allows the use of a single keyboard, monitor and mouse for more than one module.

L

LAN: Local **A**rea **N**etwork. A group of computers linked together within a limited area to exchange data.

LD: Logical **D**isk. A Storeway FDA 1x00/2x00 logical disk (or LUN) is visible to the OS as a Disk. See LUN and PD (Physical Disk).

LED: Light **E**mitting **D**iode. A small electronic device that glows when current flows through it.

Legacy Application: An application in which a company or organization has already invested considerable time and money. Typically, legacy applications are database management systems (DBMSs) running on mainframes or minicomputers.

Licensing Number: When you install an application protected by a system serial number, you are requested to supply this serial number.For optimum flexibility, PAM software allows you to replace the physical serial number by a logical licensing number so that you can run the application on any physical partition and, in the case of extended systems, on any of the Central Subsystems within the extended configuration.

LID: Local **I**nterrupt I**d**entifier (CPU).

Local Disk Subsystem: Disk subsystem housed inside the NovaScale cabinet and not connected to a SAN.

Local MCA: Machine **C**heck **A**bort is detected and handled by a single processor and is invisible to the other processor.

Locking: Means of functionally limiting access to certain hardware elements. Locked hardware elements can no longer be accessed by the current domain, but are still physically available for use by other domains. Previously locked elements can be unlocked so that they can be accessed by the domain.

LPT1 or LPT2: The name assigned to a parallel port to specify its address. See Parallel Port.

LS240: Laser **S**ervo super diskette holding up to 240 Mb.

LUN: Logical **U**nit **N**umber. Term used to designate Logical Storage Units (logical disks) defined through the configuration of physical disks stored in a mass storage cabinet.

LVDS: Low **V**oltage **D**ifferential **S**CSI.

M

MAESTRO: Machine Administration Embedded Software Real Time Oriented.
Part of the PAM software package embedded on the PMB board.

MCA: Machine **C**heck **A**bort.
See also Local MCA and Global MCA.

Memory: Computer circuitry that stores data and programs. See RAM and ROM.

Memory bank: The minimum quantity of memory used by the system. It physically consists of four memory DIMMs.

MFL: Midplane **F**an & **L**ogistics board. The MFL houses the Fan Boxes and is connected to the MIO and MQB. See MIO, MQB.

Microprocessor: An integrated circuit that processes data and controls basic computer functions.

Midplane: Mid–**P**lane. All system hardware components are connected to the Midplane.

MIMD: Multiple Instruction **M**ultiple **D**ata

MIO: Midplane **I**nput / **O**utput board. The MIO connects one or two IOC boards and the PMB. See Core Unit.

Mirrored volumes: A mirrored volume is a fault–tolerant volume that duplicates your data on two physical disks. If one of the physical disks fails, the data on the failed disk becomes unavailable, but the system continues to operate using the unaffected disk.

Module: a Midplane Board with all its connected components and utility devices. See CSS Module and MP.

MQB: Midplane **QBB** board. The MQB connects one or two QBBs and one or two IPDs. See QBB and IPD.

MSX: Midplane **S**PS & **X**PS board. The MSX houses a B–SPS switch and is connected to the MIO and the MQB. There are two MSX boards in a CSS module. All SP connections between a QBB and an IOC use an MSX. See B–SPS, MIO, MQB.

MTBF: Mean **T**ime **B**etween **F**ailure. An indicator of expected system reliability calculated on a statistical basis from the known failure rates of various components of the system. Note: MTBF is usually expressed in hours.

Multimedia: Information presented through more than one type of media. On computer systems, this media includes sound, graphics, animation and text.

Multitasking: The ability to perform several tasks simultaneously. Multitasking allows you to run multiple applications at the same time and exchange information among them. See Task.

Multithreading: The ability to manage more than one user/program or multiple requests by the same user/program at a time without running multiple copies of an application. Each user/program request is kept track of as a thread. See Thread.

N

NFS: Network **F**ile **S**ystem. A proprietary distributed file system that is widely used by TCP/IP vendors. Note: NFS allows different computer systems to share files, and uses user datagram protocol (UDP) for data transfer.

NMI: Non–**M**askable **I**nterrupt.

NUMA: Non **U**niform **M**emory **A**ccess. A method of configuring a cluster of microprocessors in a multiprocessing system so that they can share memory locally, improving performance and the ability of the system to be expanded.

nsh: nsh stands for **n**ew **sh**ell. See Shell and EFI Shell.

NVRAM: Non **V**olatile **R**andom **A**ccess **M**emory. A type of RAM that retains its contents even when the computer is powered off. See RAM and SRAM.

O

OF: Open **F**irmware. Firmware controlling a computer prior to the Operating System.

Operating System: See OS.

OS: Operating System. The software which manages computer resources and provides the operating environment for application programs.

P

PAL: Processor **A**bstraction **L**ayer: processor firmware that abstracts processor implementation differences. See also SAL.

PAM: Platform **A**dministration & **M**aintenance.

PAM software: Platform **A**dministration & **M**aintenance software. One part (PAP application and the PamSite WEB site) runs on the PAP unit. The other part (MAESTRO) is embedded on the PMB board.

PAM Tree pane: One of the three areas of the PAM web page. Server hardware presence and functional status are displayed in the PAM Tree pane. See Status pane and Control pane.

PAP unit: Platform **A**dministration **P**rocessor unit. The PC hosting all server administration software.

PAP application: Platform **A**dministration **P**rocessor application. Part of PAM software, PAP application is a Windows COM+ application running on PAP unit.

Parallel Port: Connector allowing the transfer of data between the computer and a parallel device.

PARM request: the PARM application is designed to handle Requests issued by the CSE (Customer Service Engineer)

Partition: Division of storage space on a hard disk into separate areas so that the operating system treats them as separate disk drives.

Password: A security feature that prevents an unauthorized user from operating the system.

PCI: Peripheral **C**omponent **I**nterconnect. Bus architecture supporting high-performance peripherals.

PD: Physical **D**isk. A Storeway FDA 1300/2300 physical disk is not visible to the OS. See LD.

PDU: Power **D**istribution **U**nit. Power bus used for the connection of peripheral system components.

Permanence: Property of a history file that determines whether or not the history file can be modified or deleted from the PAM user interface. Permanence is either *Static* (cannot be modified) or *Dynamic* (can be modified).

P–HPB: PCI **H**ot **P**lug **B**oard. This board provides an interlock switch on each IO Box PCI slot for hot–swapping PCI boards. See HPB.

PIC: Platform **I**nstrumentation **C**ontrol.

ping: A basic Internet program that lets you verify that a particular IP address exists and can accept requests. The verb “to ping” means the act of using the ping utility or command.

PIROM: Processor **I**nformation **ROM**. Processor Information ROM (PIROM) contains information about the specific processor in which it resides. This information includes robust addressing headers to allow for flexible programming and forward compatibility, core and L2 cache electrical specifications, processor part and S–spec numbers, and a 64–bit processor number.

PMB: Platform **M**anagement **B**oard. Links the server to the PAP unit.

PNP: Plug a**N**d **P**lay. The ability to plug a device into a computer and have the computer recognize that the device is there.

POST: Power **O**n **S**elf **T**est. When power is turned on, POST (Power–On Self–Test) is the diagnostic testing sequence (or “starting program”) that a computer runs to determine if hardware is working correctly.

PROM: Programmable **R**ead-**O**nly **M**emory.

PUID: PAM **U**niversal/Unique **ID**entifier. PAM software allocates a PUID (PAM Universal / Unique Identifier) to each hardware / software object to guarantee unambiguous identification.
The PUID for each hardware element can be obtained by hovering the mouse over the corresponding element in the PAM tree, e.g.: PAM:/CELLSBLOCK_<NAME>/MODULE_x/QBB_y/CPU_y.

Q

QBB: Quad **B**rick **B**oard. The QBB is the heart of the Bull NovaScale Server, housing 4 Itanium ® 2 processors and 16 DIMMs. Each QBB communicates with other CSS Module components via 2 high–speed bidirectional Scalability Port Switches.
See SPS or FSS.

R

RAID: Redundant **A**rray of **I**ndependent **D**isks. A method of combining hard disk drives into one logical storage unit for disk-fault tolerance.

RAM: Random **A**ccess **M**emory. A temporary storage area for data and programs. This type of memory must be periodically refreshed to maintain valid data and is lost when the computer is powered off. See NVRAM and SRAM.

RAS: Reliability, **A**vailability, **S**erviceability.

Real–time clock: The Integrated Circuit in a computer that maintains the time and date.

RFI: Radio **F**requency **I**nterference.

RJ45: 8–contact regular jack.

RMC: Remote **M**aintenance **C**onsole.

ROM: Read-**O**nly **M**emory. A type of memory device that is used to store the system BIOS code. This code cannot be altered and is not lost when the computer is powered off. See BIOS, EPROM and Flash EPROM.

RS-232 Port: An industry standard serial port. See Serial Port.

RSF: Remote **S**ervice **F**acilities.

RTC: Real **T**ime **C**lock.

S

S@N.IT: SAN Administration Tool.

SAL: System **A**bstraction **L**ayer. Firmware that abstract system implementation differences in IA–64 platform. See also PAL.

SAN: Storage **A**rea **N**etwork. A high–speed special–purpose network that interconnects different kinds of data storage devices with associated data servers on behalf of a larger network of users.

SAPIC: Streamlined **A**dvanced **P**rogrammable **I**nterrupt **C**ontroller message.

SBE: Single **B**it **E**rror.

Scheme: Configuration file ensuring optimum use and compatibility of the physical and logical resources used to simultaneously run multiple domains.

SCI: Scalable **C**oherent **I**nterface.

SCSI: Small **C**omputer **S**ystem **I**nterface. An input and output bus that provides a standard interface used to connect peripherals such as disks or tape drives in a daisy chain.

SDR: Sensor **D**ata **R**ecord.

SDRAM: Synchronous **D**ynamic **R**andom **A**ccess **M**emory. A type of DRAM that runs at faster clock speeds than conventional memory. See DRAM.

SEL: System **E**vent **L**og. A record of system management events. The information stored includes the name of the event, the date and time the event occurred and event data. Event data may include POST error codes that reflect hardware errors or software conflicts within the system.

Serial Communication: Data sent sequentially, one bit at a time.

Serial Port: Connector that allows the transfer of data between the computer and a serial device. See COM1 or COM 2.Shell is a Unix term for the interactive user interface with an operating system.

SIO: Server **I**/**O** / **S**uper **I**/**O**.

Shell: The Shell is the layer of programming that understands and executes the commands a user enters. As the outer layer of an operating system, the Shell can be contrasted with the kernel, the inmost layer or core of services of an operating system. See EFI Shell.

SIOH: Server **I**/**O H**ub. This component provides a connection point between various I/O bridge components and the Intel 870 chipset.

SMBIOS: System **M**anagement **BIOS**.

SM–BUS: System **M**anagement **Bus**.

SMIC: Server **M**anagement **I**nterface **C**hip.

SMP: Symmetrical **M**ulti **P**rocessor. The processing of programs by multiple processors that share a common operating system and memory.

SNC: Scalable **N**ode **C**ontroller. The processor system bus interface and memory controller for the Intel870 chipset. The SNC supports both the Itanium2 processors, DDR SDRAM main memory, a Firmware Hub Interface to support multiple Firmware hubs, and two scalability ports for access to I/O and coherent memory on other nodes, through the FSS.

SNM: System **N**etwork **M**odule.

SNMP: Simple **N**etwork **M**anagement **P**rotocol. The protocol governing network management and the monitoring of network devices and their functions.

Source: Each message refers to a source (the resource that generated the message) and a target (the component referred to in the message). This feature can be allows messages to be filtered according to one or more **Source** string(s) and is particularly useful for debugging and troubleshooting. See Target.

SPD: Serial **P**resence **D**etect. DIMM PROM.

SPS: Scalability **P**ort **S**witch. Each CSS Module is equipped with 2 Scalability Port Switches providing high speed bi–directional links between system components. See FSS.

SRAM: Static **RAM**. A temporary storage area for data and programs. This type of memory does not need to be refreshed, but is lost when the system is powered off. See NVRAM and RAM.

SSI: Server **S**ystem **I**nfrastructure.

Status Pane: One of the three areas of the PAM web page. Provides quick access to CSS Module availability status, server functional status, and pending event message information. See also Control pane and PAM Tree pane.

SVGA: Super **V**ideo **G**raphics **A**rray.

T

Target: Each message refers to a target (the component referred to in the message), identified by its PUID, and a source (the component that generated the message).This feature allows messages to be filtered according to one or more **Target** string(s) and is particularly useful for debugging and troubleshooting. See Source and PUID.

Task: Each message refers to a target (the component referred to in the message), identified by its PUID, and a source (the component that generated the message).This feature allows messages to be filtered according to one or more **Target** string(s) and is particularly useful for debugging and troubleshooting. See Source and PUID.

TCP: Transmission **C**ontrol **P**rotocol. A set of rules (protocol) used along with the Internet Protocol (IP) to send data in the form of message units between computers over the Internet.

TCP/IP: Transmission **C**ontrol **P**rotocol / **I**nternet **P**rotocol. The basic communication language or protocol of the Internet.

T&D: Tests and **D**iagnostics.

Thresholding: A PAM Event filter criterion. Thresholding is defined on a Count / Time basis aimed at routing significant messages only. Identical messages are counted and when the number of messages indicated in the **Count** field is reached within the period of time indicated in the **Time** field, this message is selected for routing.

U

UART: a **U**niversal **A**synchronous **R**eceiver **T**ransmitter. The microchip with programming that controls a computer interface to its attached serial devices.

ULTRA SCSI: An enhanced standard 16–bit SCSI interface providing synchronous data transfers of up to 20 MHz, with a transfer speed of 40M bytes per second. It is also called Fast-20 SCSI.

UML: Unified **M**odeling **L**anguage. A standard notation for the modeling of real–world objects as a first step in developing an object–oriented design methodology.

UPS: Uninterruptible **P**ower **S**upply. A device that allows uninterrupted operation if the primary power source is lost. It also provides protection from power surges.

URL: Uniform / **U**niversal **R**esource **L**ocator. The address of a file (resource) accessible on the Internet.

USB: Universal **S**erial **B**us. A plug–and–play interface between a computer and add–on devices. The USB interface allows a new device to be added to your computer without having to add an adapter card or even having to turn the computer off.

V

VCC: Voltage **C**ontinuous **C**urrent.

VGA: Video **G**raphics **A**rray.

VI: Virtual **I**nterface.

Visibility: A property of a history file. Visibility is either *System* (the history file is predefined by the PAM software and is visible only to an administrator) or *User* (the history file is created by an administrator and is visible to both an administrator and an operator).

VLAN: Virtual **L**ocal **A**rea **N**etwork. A local area network with a definition that maps workstations on some other basis than geographic location (for example, by department, type of user, or primary application).

VxWORKS: Platform Management Board Operating System.

W

WAN: Wide **A**rea **N**etwork. Geographically dispersed telecommunications network. The term distinguishes a broader telecommunication structure from a local area network (LAN).

WBEM: Web **B**ased **E**nterprise **M**anagement.

WMI: Windows **M**anagement **I**nterface.

WOL: A feature that provides the ability to remotely power on a system through a network connection.

X

XML: e**X**tended **M**arkUp **L**anguage. A flexible way to create common information formats and share both the format and the data on the World Wide Web, intranets, and elsewhere.

XSP: e**X**tended **S**calable **P**ort.

Y

No entries.

Z

No entries.

Index

E

F

G

H

I

K

L

M

N

T

U

V

W

Vos remarques sur ce document / Technical publication remark form

Titre / Title : Bull NovaScale 5xx0 & 6xx0 User's Guide

Nº Reférence / Reference Nº : 86 A1 94EM 01

Daté / Dated : October 2005

ERREURS DETECTEES / ERRORS IN PUBLICATION

AMELIORATIONS SUGGEREES / SUGGESTIONS FOR IMPROVEMENT TO PUBLICATION

Vos remarques et suggestions seront examinées attentivement.
Si vous désirez une réponse écrite, veuillez indiquer ci-après votre adresse postale complète.

Your comments will be promptly investigated by qualified technical personnel and action will be taken as required.
If you require a written reply, please furnish your complete mailing address below.

NOM / NAME : _____ Date : _____

SOCIETE / COMPANY : _____

ADRESSE / ADDRESS : _____

_____

Remettez cet imprimé à un responsable BULL ou envoyez-le directement à :

Please give this technical publication remark form to your BULL representative or mail to:

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

Technical Publications Ordering Form

Bon de Commande de Documents Techniques

To order additional publications, please fill up a copy of this form and send it via mail to:
Pour commander des documents techniques, remplissez une copie de ce formulaire et envoyez-la à :

BULL CEDOC
ATTN / Mr. L. CHERUBIN
357 AVENUE PATTON
B.P.20845
49008 ANGERS CEDEX 01
FRANCE

Phone / Téléphone : +33 (0) 2 41 73 63 96
FAX / Télécopie +33 (0) 2 41 73 60 19
E–Mail / Courrier Electronique : srv.Cedoc@franp.bull.fr

Or visit our web sites at: / Ou visitez nos sites web à:

http://www.logistics.bull.net/cedoc

`http://www-frec.bull.com`   `http://www.bull.com`

CEDOC Reference # Nº Référence CEDOC	**Qty** Qté	**CEDOC Reference #** Nº Référence CEDOC	**Qty** Qté	**CEDOC Reference #** Nº Référence CEDOC	**Qty** Qté
_ _ _ _ _ _ _ _ _ [_ _]		_ _ _ _ _ _ _ _ _ [_ _]		_ _ _ _ _ _ _ _ _ [_ _]	
_ _ _ _ _ _ _ _ _ [_ _]		_ _ _ _ _ _ _ _ _ [_ _]		_ _ _ _ _ _ _ _ _ [_ _]	
_ _ _ _ _ _ _ _ _ [_ _]		_ _ _ _ _ _ _ _ _ [_ _]		_ _ _ _ _ _ _ _ _ [_ _]	
_ _ _ _ _ _ _ _ _ [_ _]		_ _ _ _ _ _ _ _ _ [_ _]		_ _ _ _ _ _ _ _ _ [_ _]	
_ _ _ _ _ _ _ _ _ [_ _]		_ _ _ _ _ _ _ _ _ [_ _]		_ _ _ _ _ _ _ _ _ [_ _]	
_ _ _ _ _ _ _ _ _ [_ _]		_ _ _ _ _ _ _ _ _ [_ _]		_ _ _ _ _ _ _ _ _ [_ _]	
_ _ _ _ _ _ _ _ _ [_ _]		_ _ _ _ _ _ _ _ _ [_ _]		_ _ _ _ _ _ _ _ _ [_ _]	
[_ _] : **no revision number means latest revision** / pas de numéro de révision signifie révision la plus récente					

NOM / NAME : ______________________________ Date : __________

SOCIETE / COMPANY : ______________________________

ADRESSE / ADDRESS : ______________________________

____

PHONE / TELEPHONE : ______________________ FAX : ______________________

E–MAIL : ______________________________

For Bull Subsidiaries / Pour les Filiales Bull :

Identification: ______________________________

For Bull Affiliated Customers / Pour les Clients Affiliés Bull :

Customer Code / Code Client : ______________________________

For Bull Internal Customers / Pour les Clients Internes Bull :

Budgetary Section / Section Budgétaire : ______________________________

For Others / Pour les Autres :

Please ask your Bull representative. / Merci de demander à votre contact Bull.

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

ORDER REFERENCE
86 A1 94EM 01

Utiliser les marques de découpe pour obtenir les étiquettes.
Use the cut marks to get the labels.

NovaScale 5xx0
& 6xx0
User's Guide

86 A1 94EM 01

NovaScale 5xx0
& 6xx0
User's Guide

86 A1 94EM 01

NovaScale 5xx0
& 6xx0
User's Guide

86 A1 94EM 01