

# bullx cluster suite XR 5v3.1 U3

## Installation and Configuration Guide





# extreme computing

## bullx cluster suite

### XR 5v3.1 U3

## Installation and Configuration Guide

**Hardware and Software**

August 2010

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

**REFERENCE**  
86 A2 19FA 04

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

Copyright © Bull SAS 2010

Printed in France

## **Trademarks and Acknowledgements**

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

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

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

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

---

# Table of Contents

<b>Chapter 1.</b>	<b>extreme computing Cluster Overview .....</b>	<b>1-1</b>
1.1	Hardware Architecture .....	1-1
1.1.1	Architecture Diagrams .....	1-1
1.2	Node Types.....	1-3
1.2.1	Service Nodes.....	1-3
1.2.2	Compute Nodes .....	1-4
1.3	Networks .....	1-4
1.3.1	Administration Network .....	1-4
1.3.2	Backbone.....	1-5
1.3.3	High Speed Interconnection .....	1-5
1.4	Software Environment Overview .....	1-6
<b>Chapter 2.</b>	<b>Upgrading to bullx cluster suite XR 5v3.1 U3 .....</b>	<b>2-1</b>
	Upgrade Process Overview .....	2-2
2.1	Pre-upgrade Procedures - All Clusters.....	2-3
2.1.1	Save the SSH Keys for the Nodes and for the root User .....	2-3
2.1.2	Nagios Configuration Files .....	2-3
2.1.3	syslog-ng.conf.....	2-3
2.1.4	Optional - For NFS Clusters.....	2-3
2.1.5	Optional - Lustre Clusters.....	2-4
2.1.6	Optional - SLURM Clusters .....	2-5
2.1.7	Optional - PBS Professional Clusters .....	2-5
2.2	Updating the Management Node to bullx cluster suite XR 5v3.1 U3.....	2-6
2.2.1	Stop the Bull Cool Cabinet Doors - if any .....	2-6
2.2.2	Save the Cluster Database .....	2-6
2.2.3	Update the Management Node Software.....	2-6
2.2.4	Install the bullx cluster suite XR 5v3.1 Update 3 Software .....	2-8
2.2.5	Configure the Management Node .....	2-9
2.3	Updating Highly Available Management Nodes .....	2-10
2.3.1	Update the Primary Management Node .....	2-10
2.3.2	Update the Secondary Management Node .....	2-12
2.3.3	Final Steps for Updating High Availability on the Management Nodes.....	2-13
2.4	Update and Configure the Reference Nodes.....	2-14
2.4.1	Install the bullx cluster suite XR 5v3.1 Update 3 Software .....	2-14

2.4.2	Optional - PBS Professional clusters .....	2-15
<b>2.5</b>	<b>Deployment of the bullx cluster suite XR 5v3.1U3 Reference Nodes .....</b>	<b>2-16</b>
2.5.1	Pre Deployment Operations.....	2-16
2.5.2	Deployment Pre-Requisites .....	2-17
2.5.3	Create the Images .....	2-18
2.5.4	Deploy the Images on the Cluster .....	2-18
<b>2.6</b>	<b>Post Deployment Configuration .....</b>	<b>2-19</b>
2.6.1	postconfig command .....	2-19
2.6.2	Configure the Interconnect Interfaces .....	2-19
<b>2.7</b>	<b>Post Installation Operations .....</b>	<b>2-20</b>
2.7.1	Restore the I/O Node aliases .....	2-20
2.7.2	Install the Intel Compilers and Tools on the Login Nodes .....	2-21
2.7.3	Optional - PBS Professional clusters .....	2-21
2.7.4	Optional - for NFS clusters .....	2-21
2.7.5	Optional - for Lustre clusters only.....	2-21
2.7.6	Post Installation Checks .....	2-24
<b>2.8</b>	<b>Known issues for the Upgrade Process .....</b>	<b>2-24</b>
2.8.1	Lustre Performance Loss.....	2-24
2.8.2	Kdump.....	2-24
<b>2.9</b>	<b>Updating NFS High Availability I/O Nodes with minimal loss of service</b>	<b>2-25</b>
2.9.1	I/O Node Upgrade Procedure with no loss of Service.....	2-25

### **Chapter 3. Installing bullx cluster suite XR 5v3.1 U3 Software on the Cluster Nodes.. 3-1**

	Installation Process Overview.....	3-2
--	------------------------------------	-----

<b>3.0</b>	<b>Pre-installation Backup Operations when Re-installing bullx cluster suite XR 5v3.1 U3 .....</b>	<b>3-3</b>
3.0.1	Save the ClusterDB.....	3-3
3.0.2	Save SSH Keys of the Nodes and of root User.....	3-3
3.0.3	Save the Storage Configuration Information .....	3-4
3.0.4	Save the Lustre File Systems .....	3-4
3.0.5	Save the SLURM Configuration .....	3-4
3.0.6	Save the KSIS Images .....	3-4
<b>3.1</b>	<b>STEP 1: Install Red Hat Enterprise Linux Software on the Management Node</b>	<b>3-5</b>
3.1.1	Optional - Configure Internal RAID discs for bullx cluster suite clusters .....	3-5
3.1.2	Red Hat Enterprise Linux 5 Installation .....	3-5
3.1.3	Red Hat Linux Management Node Installation Procedure .....	3-6
3.1.4	Disk partitioning.....	3-9
3.1.5	Network access Configuration.....	3-12

3.1.6	Time Zone Selection and Root Password .....	3-13
3.1.7	Red Hat Enterprise Linux 5 Package Installation .....	3-14
3.1.8	First boot settings .....	3-16
3.1.9	Network Configurations.....	3-16
3.1.10	External Storage System Installation .....	3-17
3.1.11	Disk Health Monitoring Configuration .....	3-17
<b>3.2</b>	<b>STEP 2: Install bullx cluster suite software on the Management Node....</b>	<b>3-18</b>
3.2.1	DVD Mount Point .....	3-18
3.2.2	Prepare the Installation of the software on the Cluster Nodes .....	3-18
3.2.3	Run the install dvd script to copy bullx cluster suite software onto the Management Node	3-20
3.2.4	Install the bullx cluster suite software .....	3-21
3.2.5	Database Configuration.....	3-23
<b>3.3</b>	<b>STEP 3: Configure Equipment and Install Utilities on the Management Node</b>	<b>3-25</b>
3.3.1	Generate the SSH keys .....	3-25
3.3.2	Configure the Ethernet Switches .....	3-25
3.3.3	Update the MAC Addresses in the Cluster Database .....	3-26
3.3.4	Configure postfix .....	3-30
3.3.5	Configure the Management Tools with the Database Information.....	3-31
3.3.6	Configure ganglia.....	3-32
3.3.7	Configure syslog-ng .....	3-33
3.3.8	Configure NTP.....	3-33
3.3.9	Configure the kdump kernel dump tool .....	3-34
3.3.10	Optional - Install and Configure LDAP .....	3-35
3.3.11	Optional - Install and Configure SLURM.....	3-35
3.3.12	Optional - Install and Configure PBS Professional Batch Manager.....	3-35
3.3.13	Optional - Small clusters only .....	3-35
<b>3.4</b>	<b>STEP 4: Install RHEL5.3, bullx cluster suite XR 5v3.1U3 Software, and optional extreme computing software products on other nodes .....</b>	<b>3-36</b>
3.4.1	R421 E1 machines only.....	3-36
3.4.2	Configuration for installnfs script.....	3-36
3.4.3	installnfs script prerequisites .....	3-36
3.4.4	Prepare the software installation .....	3-36
3.4.5	Launch the NFS Installation of the bullx cluster suite XR 5v3.1U3 Software.....	3-40
<b>3.5</b>	<b>STEP 5: Configure the Administration Software on LOGIN, I/O, COMPUTE and COMPUTEX Reference Nodes.....</b>	<b>3-41</b>
3.5.1	Configure SSH and /etc/hosts .....	3-41
3.5.2	Disk Health Monitoring Configuration .....	3-42
3.5.3	Configure Ganglia.....	3-42
3.5.4	Optional - Configure LDAP .....	3-43
3.5.5	Configure the kdump kernel dump tool .....	3-43

3.5.6	Optional - Install and Configure SLURM .....	3-44
3.5.7	Optional - Install and Configure the PBS Professional Batch Manager .....	3-44
3.5.8	Configure the MPI user environment .....	3-44
3.5.9	Bull Scientific Studio .....	3-46
3.5.10	Optional - NVIDIA Tesla Graphic Card accelerators.....	3-46
3.5.11	Optional - NVIDIA CUDA Toolkit 3.0 .....	3-47
3.5.12	Optional - Install RAID Monitoring Software .....	3-47
3.5.13	Optional - NFS High Availability Clusters.....	3-48
<b>3.6</b>	<b>STEP 6: Create and Deploy Reference Node Images .....</b>	<b>3-49</b>
3.6.1	Install, Configure and Verify the Image Server .....	3-49
3.6.2	Create an Image .....	3-50
3.6.3	Deploy the Image on the Cluster .....	3-50
3.6.4	Post Deployment Configuration .....	3-51
3.6.5	Install the Intel Compilers and Tools on the Login Nodes .....	3-51
<b>3.7</b>	<b>STEP 7: Final Cluster Checks .....</b>	<b>3-52</b>
3.7.1	Check the Installation Details .....	3-52
3.7.2	Test pdsh.....	3-53
3.7.3	Check NTP .....	3-54
3.7.4	Check syslog-ng .....	3-54
3.7.5	Check Nagios .....	3-55
3.7.6	Check nscrl.....	3-57
3.7.7	Check conman.....	3-57
3.7.8	Software Stack Checks.....	3-58
3.7.9	Test kdump .....	3-58
<b>Chapter 4.</b>	<b>Configuring Storage Management Services .....</b>	<b>4-1</b>
4.1	Enabling Storage Management Services .....	4-2
4.2	Enabling the Administration of StoreWay FDA and Optima1500 (NEC) Storage System.....	4-3
4.2.1	Installing and Configuring iSM server on a Linux system .....	4-4
4.2.2	Configuring iSM Access Information from the Management Node .....	4-6
4.2.3	Initializing the FDA or Optima1500 Storage System .....	4-6
4.3	Enabling the Administration of DataDirect Networks S2A (DDN) Storage Systems .....	4-7
4.3.1	Enabling Access from Management Node .....	4-7
4.3.2	Enabling Date and Time Control .....	4-7
4.3.3	Enabling Event Log Archiving .....	4-7
4.3.4	Enabling Management Access for Each DDN .....	4-7
4.3.5	Initializing the DDN Storage System .....	4-8



<b>4.4</b>	<b>Enabling the Administration of Optima1250 (Xyratex) Storage Systems</b>	<b>4-11</b>
4.4.1	Optima1250 Storage System Management Prerequisites.....	4-11
4.4.2	Initializing the Optima1250 Storage System .....	4-11
<b>4.5</b>	<b>Enabling the Administration of EMC/Clariion (DGC) Storage Systems..</b>	<b>4-13</b>
4.5.1	Initial Configuration .....	4-13
4.5.2	Complementary Configuration Tasks for EMC/Clariion CX series storage devices .....	4-13
4.5.3	Complementary Configuration Tasks for EMC/CLARiiON AX4-5 storage devices.....	4-14
4.5.4	Configuring the EMC/Clariion (DGC) Access Information from the Management Node	4-14
<b>4.6</b>	<b>Updating the ClusterDB with Storage Systems Information .....</b>	<b>4-15</b>
<b>4.7</b>	<b>Storage Management Services .....</b>	<b>4-15</b>
<b>4.8</b>	<b>Enabling the Administration of Brocade Fibre Channel Switches.....</b>	<b>4-16</b>
4.8.1	Enabling Access from Management Node .....	4-16
4.8.2	Updating the ClusterDB .....	4-16
<b>Chapter 5.</b>	<b>Configuring I/O Resources for the Cluster .....</b>	<b>5-1</b>
<b>5.1</b>	<b>Automatic Deployment of the I/O Configuration .....</b>	<b>5-1</b>
5.1.1	Storage Model Files .....	5-1
5.1.2	Automatic Configuration of a Storage System.....	5-2
5.1.3	Automatic Deployment of the configuration of I/O resources for the nodes .....	5-3
<b>5.2</b>	<b>Manual Configuration of I/O Resources .....</b>	<b>5-4</b>
5.2.1	Manual Configuration of Storage Systems .....	5-4
5.2.2	Manual Configuration of I/O resources for Nodes.....	5-5
<b>Chapter 6.</b>	<b>Configuring the NIS and NFS File Systems.....</b>	<b>6-1</b>
<b>6.1</b>	<b>Setting up NIS to share user accounts.....</b>	<b>6-1</b>
6.1.1	Configure NIS on the Login Node (NIS server) .....	6-1
6.1.2	Configure NIS on the Compute or/and the I/O Nodes (NIS client).....	6-2
<b>6.2</b>	<b>Configuring NFS v3/v4 to share the /home_nfs and /release directories</b>	<b>6-3</b>
6.2.1	Preparing the LOGIN node (NFS server) for the NFSv3/v4 file system .....	6-3
6.2.2	Setup for NFS v3/v4 file systems .....	6-4
<b>Chapter 7.</b>	<b>Installing Intel Tools and Applications.....</b>	<b>7-1</b>
<b>7.1</b>	<b>Installing Intel Compilers with MKL and IDB .....</b>	<b>7-1</b>
<b>7.2</b>	<b>Intel Trace Analyzer and Collector Tool.....</b>	<b>7-1</b>
<b>7.3</b>	<b>Intel VTune Performance Analyzer for Linux .....</b>	<b>7-2</b>

7.4	Intel Runtime Libraries .....	7-2
<b>Chapter 8.</b>	<b>Configuring Switches and Cards .....</b>	<b>8-1</b>
8.1	Configuring Ethernet Switches.....	8-1
8.1.1	Ethernet Installation scripts.....	8-1
8.1.2	swtAdmin Command Option Details .....	8-2
8.1.3	Automatic Installation and Configuration of the Ethernet Switches .....	8-2
8.1.4	Ethernet Switch Configuration Procedure.....	8-3
8.1.5	Ethernet Switches Configuration File .....	8-5
8.1.6	Ethernet Switches Initial Configuration .....	8-6
8.1.7	Basic Manual Configuration .....	8-7
8.1.8	Broadcom Switch Configuration for bullx blade systems.....	8-14
8.2	Installing Additional Ethernet Boards .....	8-17
8.3	Configuring InfiniBand Interconnects .....	8-17
8.3.1	Configuring Voltaire Devices .....	8-17
8.4	Configuring a Brocade Switch .....	8-18
<b>Appendix A.</b>	<b>Cluster Database Operations .....</b>	<b>A-1</b>
A.1	Saving and Reinstalling the Cluster DB data .....	A-1
A.1.1	Saving the Data files.....	A-1
A.1.2	Reinstalling the Data files .....	A-1
A.2	Initializing the Cluster Database using the preload file .....	A-2
<b>Appendix B.</b>	<b>Manual Installation of Software .....</b>	<b>B-1</b>
B.1	Bull Additional Software Options.....	B-1
B.2	Custom Directories .....	B-1
B.3	Bonus Directories .....	B-2
<b>Appendix C.</b>	<b>Configuring Interconnect Interfaces .....</b>	<b>C-1</b>
C.1	The config_ip command.....	C-1
C.2	Interface Description file .....	C-1
C.2.1	Checking the interfaces.....	C-2
C.2.2	Starting the InfiniBand interfaces .....	C-3

<b>Appendix D.</b>	<b>Binding Services to a Single Network .....</b>	<b>D-1</b>
<b>Appendix E.</b>	<b>PCI Slot Selection and Server Connectors.....</b>	<b>E-1</b>
E.1	How to Optimize I/O Performance .....	E-1
E.2	Creating the list of Adapters.....	E-2
E.3	Connections for R4xx Servers.....	E-2
E.3.1	R421 Series – Compute Node.....	E-3
E.3.2	R422 Series – Compute Node.....	E-4
E.3.3	R460 Series – Service Node .....	E-5
E.3.4	R421 E1 Series – Compute Nodes.....	E-6
E.3.5	R422 E1 Series – Compute Nodes.....	E-7
E.3.6	R425 Series – Compute Nodes .....	E-8
E.3.7	R423 E1 Series – Service Node .....	E-9
E.3.8	R422 E2 Series – Compute Nodes.....	E-12
E.3.9	R423 E2 Series – Compute or Service Nodes .....	E-13
E.3.10	R425 E2 Series – Compute Nodes.....	E-17
E.3.11	R424 E2 Series – Compute Nodes.....	E-18
<b>Appendix F.</b>	<b>Activating your Red Hat account.....</b>	<b>F-1</b>
	<b>Glossary and Acronyms .....</b>	<b>G-1</b>
	<b>Index.....</b>	<b>I-1</b>

---

## List of Figures

Figure 1-1.	Small Cluster Architecture .....	1-1
Figure 1-2.	Medium-sized Cluster Architecture .....	1-2
Figure 1-3.	Large Cluster Architecture .....	1-2
Figure 1-4.	bullx cluster suite environment .....	1-7
Figure 2-1.	First Install Window.....	2-7
Figure 2-2.	<b>installvd</b> script run options .....	2-7
Figure 3-1.	The Welcome Screen .....	3-6
Figure 3-2.	Keyboard installation screen .....	3-7
Figure 3-3.	RHEL5 installation number dialog box .....	3-7
Figure 3-4.	Skip screen for the installation number .....	3-8
Figure 3-5.	First RHEL5 installation screen.....	3-8
Figure 3-6.	Partitioning screen .....	3-9
Figure 3-7.	Confirmation of the removal of any existing partitions .....	3-10
Figure 3-8.	Modifying the partitioning layout – 1st screen .....	3-10
Figure 3-9.	Confirmation to remove existing partitions .....	3-11
Figure 3-10.	RHEL5 Partitioning options screen .....	3-11
Figure 3-11.	Confirmation of previous partitioning settings .....	3-12
Figure 3-12.	Network Configuration Screen .....	3-12
Figure 3-13.	Time Zone selection screen. ....	3-13
Figure 3-14.	Root Password Screen .....	3-14
Figure 3-15.	Software selection screen.....	3-14
Figure 3-16.	Installation screen .....	3-15
Figure 3-17.	First Install Window.....	3-20
Figure 3-18.	<b>installvd</b> script run options.....	3-21
Figure 3-19.	Bull System Manager Welcome screen.....	3-55
Figure 3-20.	<b>Bull System Manager</b> Authentication Window .....	3-56
Figure 3-21.	The <b>Bull System Manager</b> console.....	3-56
Figure 3-22.	<b>Bull System Manager Monitoring</b> Window.....	3-57
Figure E-1.	R421 rear view of Riser architecture .....	E-3
Figure E-2.	R421 rear view connectors .....	E-3
Figure E-3.	R422 rear view of Riser architecture .....	E-4
Figure E-4.	R422 Rear view connectors .....	E-4
Figure E-5.	R460 risers and I/O subsystem slotting .....	E-5
Figure E-6.	Rear view of R460 Series .....	E-5
Figure E-7.	Rear view of R421 E1 Series.....	E-6
Figure E-8.	Rear view of R422 E1 Series (2 Compute Nodes in 1U).....	E-7
Figure E-9.	Rear view of R422 E1 Series (2 Compute Nodes in 1U with Integrated InfiniBand) .....	E-7
Figure E-10.	Rear view of R425 Series .....	E-8
Figure E-11.	Rear view of R423 E1 Series.....	E-9

---

## List of Tables

Table 3-1.	<b>bullx cluster suite XR</b> installation types .....	3-1
Table 3-2.	Red Hat Consoles and Switching Key Strokes .....	3-6
Table E-1.	PCI-X Adapter Table.....	E-2
Table E-2.	PCI-Express Table .....	E-2



---

# Preface

## Scope and Objectives

**bullx cluster suite** is used for the management of all the nodes of a Bull extreme computing cluster.

This guide describes how to install, or re-install, or upgrade to the **bullx cluster suite XR 5v3.1 U3** software distribution, and all other associated software, on Bull extreme computing clusters. It also describes the configuration tasks necessary to make the cluster operational.

## Intended Readers

This guide is for Administrators of **bullx cluster suite** systems.

## Prerequisites

Refer to the **bullx cluster suite XR 5v3.1 U3 Software Release Bulletin** (SRB) for details of any restrictions that apply to your release. Use this manual in conjunction with the **bullx cluster suite High Availability Guide** if your cluster includes any form of High Availability.

## Bibliography

Refer to the manuals included on the documentation CD delivered with your system OR download the latest manuals for your **bullx cluster suite** release, and for your cluster hardware, from: <http://support.bull.com/>

The *bullx cluster suite Documentation* CD-ROM (86 A2 12FB) includes the following manuals:

- *bullx cluster suite Installation and Configuration Guide* (86 A2 19FA)
- *bullx cluster suite Administrator's Guide* (86 A2 20FA)
- *bullx cluster suite Application Developer's Guide* (86 A2 22FA)
- *bullx cluster suite Maintenance Guide* (86 A2 24FA)
- *bullx cluster suite High Availability Guide* (86 A2 25FA)
- *InfiniBand Guide* (86 A2 42FD)
- *LDAP Authentication Guide* (86 A2 41FD)
- *SLURM Guide* (86 A2 45FD)
- *Lustre Guide* (86 A2 46FD)

The following document is delivered separately:

- *The Software Release Bulletin* (SRB) (86 A2 80EJ)



**Important** The Software Release Bulletin contains the latest information for your delivery. This should be read first. Contact your support representative for more information.

---

For **Bull System Manager**, refer to the *Bull System Manager* documentation suite.

For clusters that use the **PBS Professional** Batch Manager, the following manuals are available on the *PBS Professional CD-ROM*:

- *Bull PBS Professional Guide* (86 A2 16FE)
- *PBS Professional 10.2 Administrator's Guide*
- *PBS Professional 10.2 User's Guide* (on the *PBS Professional CD-ROM*)

For clusters that use **LSF**, the following manuals are available on the LSF CD-ROM:

- *Bull LSF Installation and Configuration Guide* (86 A2 39FB)
- *Installing Platform LSF on UNIX and Linux*

For clusters which include the **Bull Cool Cabinet**:

- *Site Preparation Guide* (86 A1 40FA)
- *R@ck'nRoll & R@ck-to-Build Installation and Service Guide* (86 A1 17FA)
- *Cool Cabinet Installation Guide* (86 A1 20EV)
- *Cool Cabinet Console User's Guide* (86 A1 41FA)
- *Cool Cabinet Service Guide* (86 A7 42FA)

## Highlighting

- Commands entered by the user are in a frame in 'Courier' font, as shown below:

```
mkdir /var/lib/newdir
```

- System messages displayed on the screen are in 'Courier New' font between 2 dotted lines, as shown below.

```
-----  
Enter the number for the path :  
-----
```

- Values to be entered in by the user are in 'Courier New', for example:  
COM1
- Commands, files, directories and other items whose names are predefined by the system are in 'Bold', as shown below:  
The **/etc/sysconfig/dump** file.
- The use of *Italics* identifies publications, chapters, sections, figures, and tables that are referenced.
- < > identifies parameters to be supplied by the user, for example:  
<node\_name>



### WARNING

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



# Chapter 1. extreme computing Cluster Overview

This chapter provides an overview of the hardware and software components for **bullx cluster suite extreme computing** clusters.

## 1.1 Hardware Architecture

A **bullx cluster suite** cluster consists of **Service Nodes** for the management, storage and software development services and **Compute Nodes** for intensive calculation operations.

The cluster architecture and node distribution differ from one configuration to another. Each customer must define the node distribution that best fits their needs, in terms of computing power, application development and I/O activity.

**Important** The System Administrators must have fully investigated and confirmed the planned node distribution in terms of Management Nodes, Compute Nodes, Login Nodes, I/O Nodes, etc., before beginning software installation and configuration operations.

### 1.1.1 Architecture Diagrams

#### Small Clusters

On small clusters all the cluster services – Management, Login, and I/O – run on a single Service Node as shown in Figure 1-1.

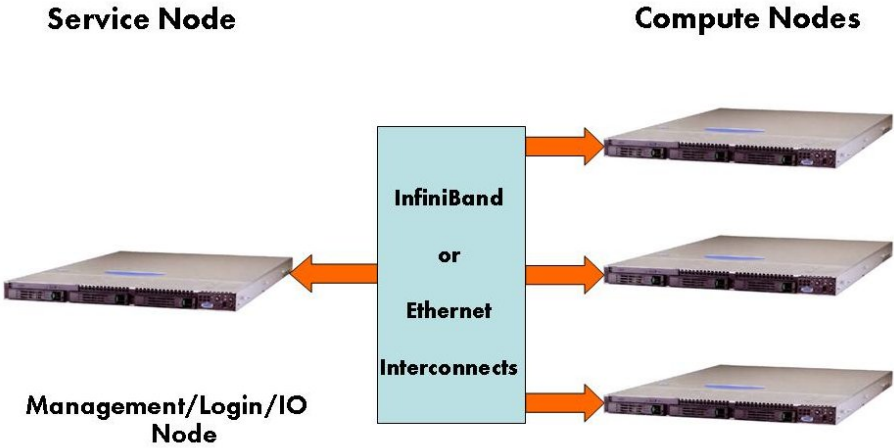


Figure 1-1. Small Cluster Architecture

### Medium-sized Clusters

On medium-sized clusters, one Service Node will run the cluster management services and a separate Service Node will be used to run the Login and I/O services.

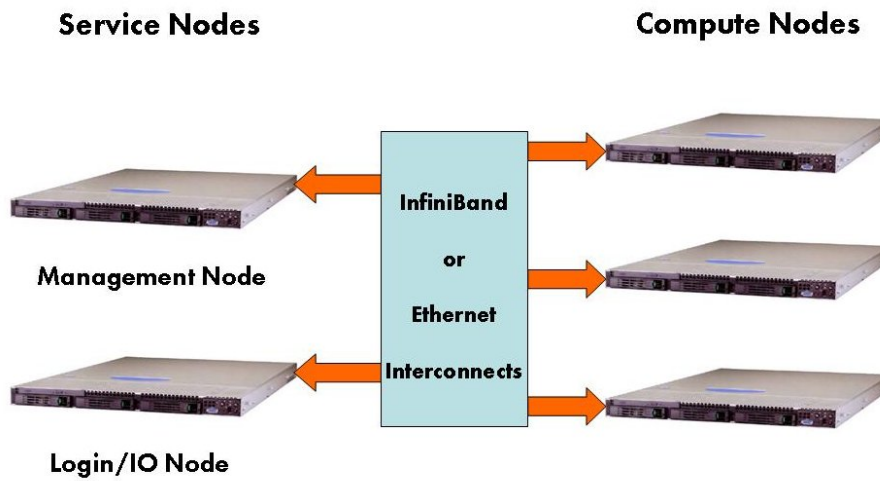


Figure 1-2. Medium-sized Cluster Architecture

### Large clusters

On large clusters, the cluster management services run on dedicated nodes. The Login and I/O services also run on separate dedicated nodes. Clusters which use the **Lustre** parallel file system will need at least two separate Service Nodes dedicated to it.

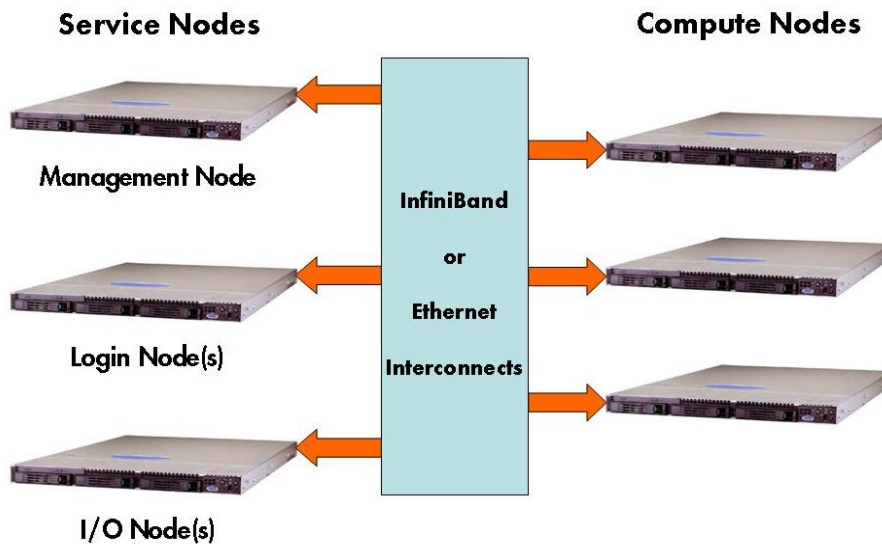


Figure 1-3. Large Cluster Architecture

## 1.2 Node Types

The **bullx cluster suite** clusters feature nodes that are dedicated to specific activities.

- **Service Nodes** are configured to run the **cluster services**. The cluster services supported by **bullx cluster suite** are:
  - **Cluster Management**, including installation, configuration settings, general administration and the monitoring of all the hardware in the cluster.
  - **Login**, to provide access to the cluster and its specific software development environment.
  - **I/O**, to transfer data to and from storage units, using a powerful shared file system service, either **NFS** or **Lustre** (ordered as an option).

Depending on the size and the type of cluster, a single Service Node will cover all the Management, Login and I/O Node functions OR there will be several Service Nodes providing the different functions as shown in the diagrams above.

- **Compute Nodes** are optimized for code execution; limited daemons run on them. These nodes are not used for saving data but instead transfer data to Service Nodes. There are two types of Compute Nodes possible for **bullx cluster suite**.
  - Minimal Compute or **COMPUTE** Nodes, which include minimal functionality, are quicker and easier to deploy, and require less disk space for their installation. These are ideal for clusters which work using data files (non graphical environment).
  - Extended Compute or **COMPUTEX** Nodes, which include additional libraries and require more disk space for their installation. These are used for applications that require a graphical environment (X Windows), and also for most **ISV** applications. They are also installed if there is a need for **Intel Cluster Ready** compliance.

### 1.2.1 Service Nodes

The Bull **R423**, **R423 E2**, **R440**, **R460** and **bullx S6030** servers can all be used for the Service Nodes for **bullx cluster suite XR 5v3.1 U3** Clusters.



**Important** From this point onwards the Service Node running the management services will be known as the Management Node. For small clusters, as explained, this node may also include Login and I/O services.

---

#### Management Node Services

The **Management Node** provides services and runs the cluster management software. All management and monitoring functions are concentrated on this one node. For example, the following services may be included: **NTP**, **Cluster DataBase**, **Kerberos**, **snmtrapd**, **ganglia**, **dhcpcd**, **httpd**, and **conman**.

The Management Node can also be configured as a gateway for the cluster. You will need to connect it to the external LAN and to the management LAN using two different **Ethernet** cards. A monitor, keyboard and mouse will also need to be connected to the Management Node.

The Management Node houses a lot of reference and operational data, which can then be used by the **Resource Manager** and other administration tools. It is recommended to store data on an external **RAID** storage system. The storage system should be configured **BEFORE** the creation of the file system for the management data stored on the Management Node.

### Login Node Services

**Login Node(s)** are used by cluster users to access the software development and run-time environment. Specifically, they are used to:

- Login
- Develop, edit and compile programs
- Debug parallel code programs.

### I/O Node Services

I/O Nodes provide access to a shared storage area that is used by the Compute Nodes when carrying out computations. Either **NFS** or the **Lustre** parallel file system may be used to carry out the Input/Output operations for **bullx cluster suite** clusters.



**Important** Lustre must use dedicated service nodes for the I/O functions and NOT combined Login-I/O service nodes. NFS can be used on both dedicated I/O service nodes and on combined Login-I/O service nodes.

---

## 1.2.2 Compute Nodes

The **Compute Nodes** are optimized to execute parallel code. Interconnect Adapters (**InfiniBand** or **Gigabit Ethernet**) are connected to these nodes.

The Bull R421, R421 E1, R422, R422 E1, R422 E2, R424 E2, R425, R480 E1 servers, **bullx B500 compute blade** systems and **bullx S6010 super-nodes** may all be used as Compute Nodes for **bullx cluster suite XR 5v3.1 U3**.

## 1.3 Networks

The cluster contains different networks, dedicated to particular functions, including:

- An **Administration Network**.
- **High speed interconnects**, consisting of switches and cable/boards to transfer data between Compute Nodes and I/O Nodes.

### 1.3.1 Administration Network

The **Administration network** uses an **Ethernet** network so that the Management Node can monitor and control the operating system, middleware, hardware (switches, fibre channel cabinets, etc.) and applications.

---

**Note** An optional Ethernet link is necessary to connect the cluster's Login Node(s) to a LAN backbone that is external to the cluster.

---

This network connects all the **LAN1** native ports and the **BMCs** for the nodes using a 10/100/1000 Mb/s network. This network has no links to other networks and includes 10/100/1000 Mb/s Ethernet switch(es).

## 1.3.2 Backbone

The **Backbone** is the link between the cluster and the external world. This network links the Login Node to the external network through a **LAN** network using Ethernet switches. For performance and cluster security reasons it is recommended that the backbone is connected to the Login and Management Nodes only.

## 1.3.3 High Speed Interconnection

### InfiniBand Networks

The following devices may be used for **InfiniBand** clusters.

- **Voltaire® Switching** Devices
- **Mellanox ConnectX™ Dual-Port** Cards
- **Mellanox ConnectX-2 InfiniBand** HBAs

### Ethernet Gigabit Networks

The **bullx cluster suite** Ethernet Gigabit networks can use either **CISCO** or **FOUNDRY** switches.

## 1.4 Software Environment Overview

**bullx cluster suite** has been designed to help you to get the best performance out of your cluster, and ensures easy management and reliability as a single system.

**bullx cluster suite** includes:

- A stock **Red Hat Enterprise Linux 5** distribution, to benefit from the support and certification of most **extreme computing ISV** applications that are available for **Red Hat** environments.
- Centralized cluster installation, management and monitoring tools.
- Support of parallel processing.
- Support of the **Lustre** and **NFS** file systems.
- Support of **InfiniBand** and **Ethernet** Gigabit interconnects.
- Tools and libraries for scientific applications.
- A large selection of development tools.

Specific extensions to meet the needs of **extreme computing** applications, such as a global shared file system or a cutting edge **InfiniBand** stack, are developed, provided and supported by Bull. They are built-in, and their integration is done in such a way that the environment remains compatible with the base **Red Hat** environment.

### Tools

**bullx cluster suite** supports a complete set of tools that enable users to exploit the cluster efficiently at the different operation steps:

- System management:
  - **Bull System Manager - HPC Edition**
    - **Nagios** - monitoring of hardware and software components monitoring
    - **Ganglia** - monitoring of system activity
  - **Ksis** - preparation and deployment of software images and patches
  - **pdsh** - parallel commands
  - **Conman** - centralized console management
  - **NS Commands** - platform management of nodes through IPMI
- Optimized execution environment
  - Interconnect network drivers integration and optimization; **InfiniBand** network support relies on the latest qualified version of **OFED** OpenFabrics
  - Scientific computation and communication libraries: **MPIBull2**, **bullx MPI**, **FFTW**, **BlockSolve95**, **Intel MKL** (commercial) etc.
  - **Lustre** parallel file-system optimized and integrated within **bullx cluster suite** to improve ease of configuration (commercial)
  - Resource management software: **SLURM**
  - Job scheduling software tightly integrated with **MPIBull2** and **bullx MPI** libraries: **Platform LSF™** (commercial) or **Altair PBS Pro™** (commercial)

- Development and tuning environment
  - Compilers: **GNU Compilers, Intel C/C++/Fortran 11** (commercial)
  - Debuggers: **IDB, GDB, TotalView** (commercial), **Alinea DDT** (commercial)
  - Profilers: **oprofile, GNU profiler, Intel Vtune** (commercial), **Intel Trace Analyzer and Collector** (commercial)

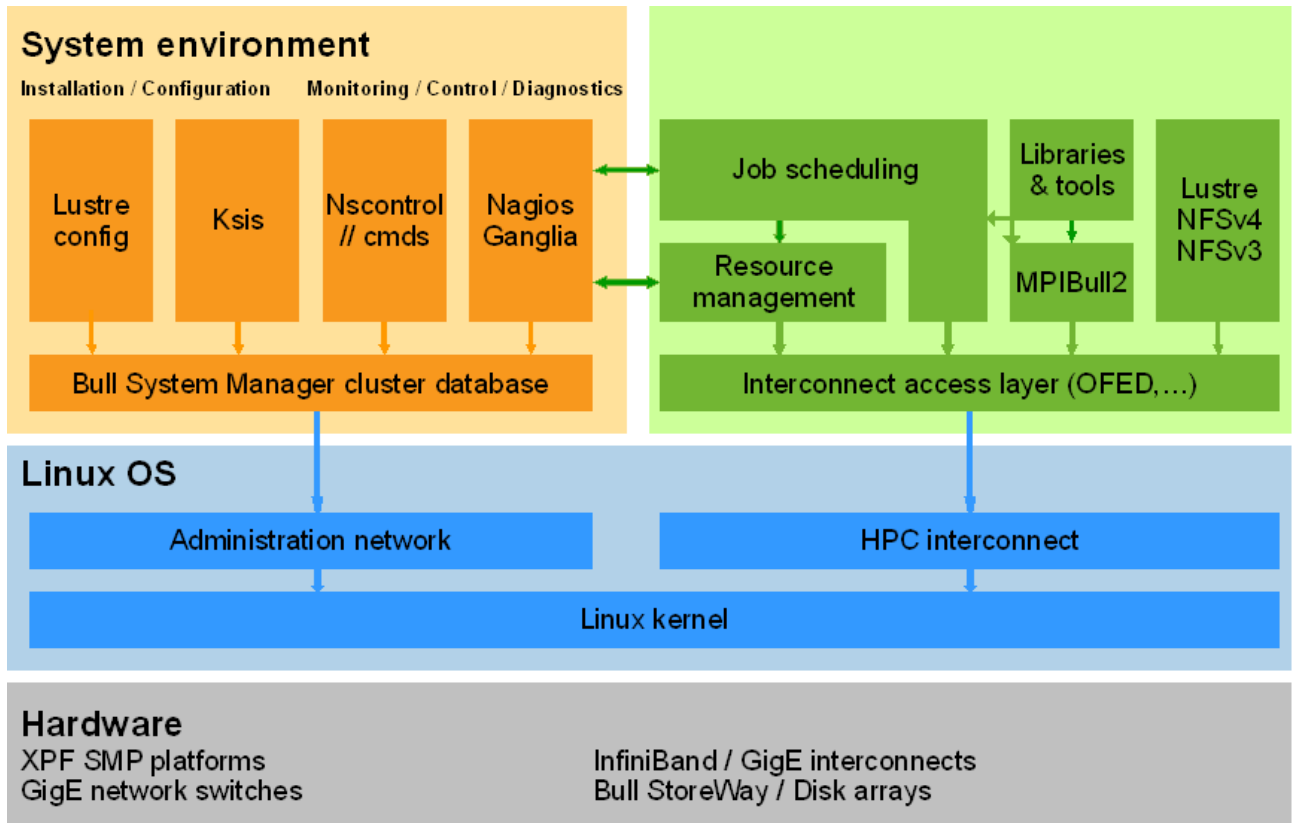


Figure 1-4. bullx cluster suite environment





---

## Chapter 2. Upgrading to bullx cluster suite XR 5v3.1 U3

bullx cluster suite XR 5v3.1U3 can be installed on top of the BAS5 for Xeon v3.1 and bullx cluster suite XR 5v3.1 U1 and U2 releases, including ADDONs.

---



**Important** This chapter describes the upgrade to bullx cluster suite XR 5v3.1 U3 from BAS5 for Xeon V3.1 and bullx cluster suite XR 5v3.1 U1/U2 clusters, with no addition of new hardware.

bullx cluster suite XR 5v3.1 U3 must be installed from scratch, as described in *Chapter 3*, for clusters which include new hardware.

As a precaution, in case there is a problem when upgrading to bullx cluster suite XR 5v3.1 U3, the existing versions of the following files should be backed up:

- The Management Node system.
  - A copy of the Reference Node images for each type of node.
  - See the *bullx cluster suite Maintenance Guide* for more information on using Bull System Backup Restore.
- 



### WARNING

All activity on the cluster must be stopped, softly and cleanly, before starting the upgrade process.

Refer to the table, on the next page, and carry out the operations that apply to your cluster.

---

### See

Contact Bull Technical Support for details of how to upgrade from BAS5 for Xeon v1.1 and v1.2.

---

## Upgrade Process Overview

Section 2.1	<b>Pre-upgrade Procedures - All Clusters</b> <ul style="list-style-type: none"> <li>• Save the SSH Keys for the Nodes and for the root user</li> <li>• Specific procedures for <b>Lustre, NFS, SLURM</b> and <b>PBS Professional</b> clusters</li> </ul>	Page 2-3
Section 2.2	<b>Upgrade to bullx cluster suite XR 5v3.1U3</b> <ul style="list-style-type: none"> <li>• Update the Management Node</li> </ul>	Page 2-6
Section 2.3	<b>Updating Highly Available Management Nodes</b>	Page 2-10
Section 2.4	<b>Update and Configure the Reference Nodes</b> <ul style="list-style-type: none"> <li>• Update <b>bullx cluster suite XR 5V3.1 U1/U2</b> Reference Nodes to <b>bullx cluster suite XR 5V3.1 U3</b></li> </ul>	Page 2-14
Section 2.5	<b>Deployment of Reference Nodes - All Clusters</b> <ul style="list-style-type: none"> <li>• Pre-deployment procedures and pre-requisites</li> <li>• Image Creation and Deployment</li> </ul>	Page 2-16
Section 2.6	<b>Post deployment configurations</b>	Page 2-19
Section 2.7	<b>Post Installation Operations - All Clusters</b> <ul style="list-style-type: none"> <li>• Restore the I/O Node Aliases</li> <li>• Specific procedures for <b>Lustre, NFS, SLURM</b> and <b>PBS Professional</b> clusters</li> <li>• Post Installation Checks</li> </ul>	Page 2-20
Section 2.8	<b>Known Issues for the Upgrade Process - All Clusters</b>	Page 2-24
Section 2.9	<b>Upgrading NFS High Availability I/O Node with minimal loss of service</b>	Page 2-25

## 2.1 Pre-upgrade Procedures - All Clusters

---



**Important** For clusters with Highly Available Management Nodes the actions described in sections 2.1.1, 2.1.3 and 2.1.7. must be carried out on both the Primary and Secondary Management Nodes.

---

### 2.1.1 Save the SSH Keys for the Nodes and for the root User

To avoid RSA identification changes, the **SSH** keys must be kept.

- To keep the node SSH keys, save the `/etc/ssh` directory for each node type (Management Node, Compute Node, Login Node, etc.), assuming that the SSH keys are identical for all nodes of the same type.
- To keep the root user SSH keys, save the `/root/.ssh` directory on the Management Node, assuming that its content is identical on all nodes.

These directories must be restored once the installation has finished.

### 2.1.2 Nagios Configuration Files

Save the following **Nagios** configuration files, if customized services were added:

```
/etc/nagios/services-tpl.cfg  
/etc/nagios/hpccommands.cfg  
/etc/nagios/hosts-tpl.cfg  
/etc/nagios/hostgroups-tpl.cfg
```

### 2.1.3 syslog-ng.conf

Before **bullx cluster suite XR 5v3.1 U3** is installed, the existing `/etc/syslog-ng/syslog-ng.conf` file on the Management Node must be saved on an external back-up device (as this will be used later).



**Important** The existing `syslog-ng.conf` file will be overwritten when **bullx cluster suite XR 5v3.1U3** is installed.

---

### 2.1.4 Optional - For NFS Clusters

1. Stop NFS activity before upgrading to **bullx cluster suite XR 5v3.1U3**

```
service nfs stop
```

## 2.1.5 Optional - Lustre Clusters

---

 **Important** This section applies to clusters with the Lustre file system installed, and that include data that has to be kept.

---

### Actions to be performed before updating

#### 1. Stop Lustre activity

Ensure **Lustre** is stopped correctly for all **Lustre** file systems:

```
lustre_util umount -f <fsname> -n <client nodes list | all>
lustre_util stop -f <fsname>
```

#### 2. Stop Cluster Suite - Lustre High Availability Clusters only

a. If necessary, relocate the **Lustre** services on their Primary Node by using the commands below:

```
lustre_migrate hastat -n <io_node_list>
lustre_migrate relocate -n <node>
```

b. Stop the **Lustre** services:

```
lustre_migrate hastop -n <io_node_list>
```

c. Stop **HA Cluster Suite**:

```
stordepha -c stop -i <all | io_node_list>
```

---

 **Important** Do not use the "all" option, above, or stop the MGS and ldap services, below, if your cluster includes Highly Available Management Nodes.

---

#### 3. Stop the Lustre daemons and save the backend files

---

 **Important** The MGS, ldap, lustredbd service back-end files will not be altered by the RPM upgrade. The files are saved as a precaution.

---

a. **MGS** service

```
service mgs stop
```

The MGS back-end can be saved at this point. However, this is optional as **MGS** is able to rebuild itself when **Lustre** starts. The back-end file is configured in the `/etc/lustre/lustre.cfg` file, and can be checked by using the command below:

```
grep LUSTRE_MGS_ABSOLUTE_LOOPBACK_FILENAME /etc/lustre/lustre.cfg
```

- b. **ldap** - Lustre High Availability Clusters only
  - i. Backup your **LDAP** Directory

```
ldapsearch -LLL -x -D cn=Manager,fs=lustre -w secret -H ldap:/// -b fs=lustre>/tmp/lustre_ldap_backup.ldif
```

- c. Be careful to put the **LDIF** file somewhere that will be backed up.

```
service ldap stop
```

The back-end files are in the `/var/lib/ldap/lustre` folder.



**Important** The ldap backend files will not be altered by the RPM upgrade. The files are saved as a precaution:

```
cp -r /var/lib/ldap/lustre /var/lib/ldap/lustre.bkp
```

- d. **lustredbd** - Lustre High Availability Clusters only

```
service lustredbd.sh stop
```

There is no backend file for this daemon.

#### 4. Save the Lustre configuration file

On the Management Node, save the `/etc/lustre` directory, as a precaution.

#### 5. Save the storage configuration files

On all I/O nodes: save the `/etc/storageadmin/disknaming.conf` file. This file is not modified by the upgrade RPMs, but if it is lost you will have to manually upgrade the **OST** and **MDT** mapping (Using the `lustre_ost_dba update` and `lustre_mdt_dba update` commands, or by updating the `/etc/lustre/storage.conf` file) to maintain coherency with the mapping provided by the `stormap -l` command.

## 2.1.6 Optional - SLURM Clusters



### WARNING

All jobs that are running should be saved and backed up before they are cancelled.

#### Save the SLURM Configuration File

The `/etc/slurm/slurm.conf` file is used by the **SLURM** resource manager. It is strongly recommended that this file is saved from the Management Node onto a non-formattable media.

## 2.1.7 Optional - PBS Professional Clusters

**See** See *Section 3.1* in the Bull *PBS Professional Guide* for details of the *Pre-upgrade procedures* for PBS Professional clusters.

## 2.2 Updating the Management Node to bullx cluster suite XR 5v3.1 U3

BAS5 for Xeon V3.1 and bullx cluster suite XR 5v3.1 U1/U2 Management Nodes are updated to bullx cluster suite XR 5v3.1 U3 by copying and installing the bullx cluster suite XR 5v3.1 U3 and the bullx cluster suite XR SN-OS Errata3 for RHEL 5.3 (EM64T) media on to the Management Nodes.

### 2.2.1 Stop the Bull Cool Cabinet Doors - if any

- Notes**
- The *Cool Cabinet Door Console User's Guide* for details about using the GUI console to power on/off the Cool Cabinet Door.
  - *Maintenance Guide* for details about using the `nsclusterstop` command to stop the Bull Cool Cabinet Door.

### 2.2.2 Save the Cluster Database

**Note** The Cluster Database files should be saved and backed up as a precaution.

1. Login as the root user on the Management Node.
2. Enter:

```
su - postgres
```

3. Enter the following commands:

```
cd /var/lib/pgsql/backups
pg_dump -Fc -C -f/var/lib/pgsql/backups/<name_of_clusterdball.sav> clusterdb
pg_dump -Fc -a -f/var/lib/pgsql/backups/<name_of_clusterdbdata.sav> clusterdb
```

For example, `<name_of_clusterdbdata.sav>` might be `clusterdbdata-2006-1105.sav`.

4. Copy the two `.sav` files onto a non-formattable media outside of the cluster.

### 2.2.3 Update the Management Node Software

The `installvdv` script is used to copy across the bullx cluster suite XR 5v3.1U3 software to the `/release/XBAS5V3.1` directory on the Management Node. The media to be installed depend on the cluster type and the software options purchased.

**See** The *Software Release Bulletin* for more information on the installation media included with your delivery.

#### bullx cluster suite XR 5v3.1U3 media

1. bullx cluster suite XR 5v3.1U3 - Mandatory installation for all clusters.
2. bullx cluster suite XR SN-OS Errata3 for Red Hat Enterprise Linux 5.3 (EM64T) - Mandatory installation for all clusters.
3. bullx cluster suite XR CN-OS Errata3 for Linux 5.3 (EM64T)

## Installvdv script installation procedure for the media

1. Insert the **bullx cluster suite XR 5v3.1 U3** media.

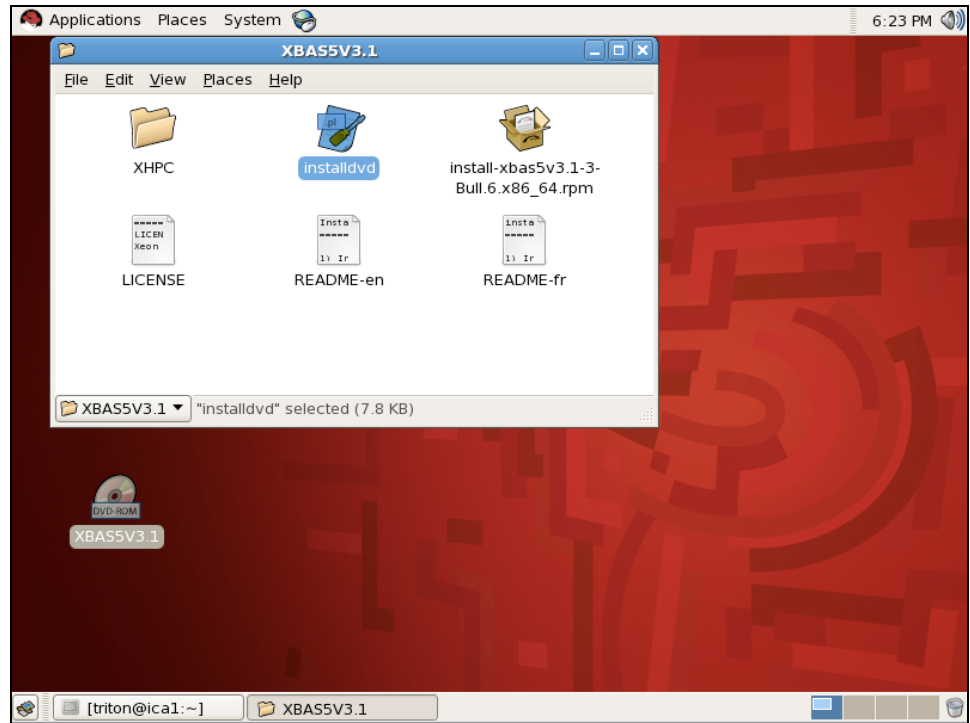


Figure 2-1. First Install Window

2. Double-click on the **installvdv** script, as shown above.

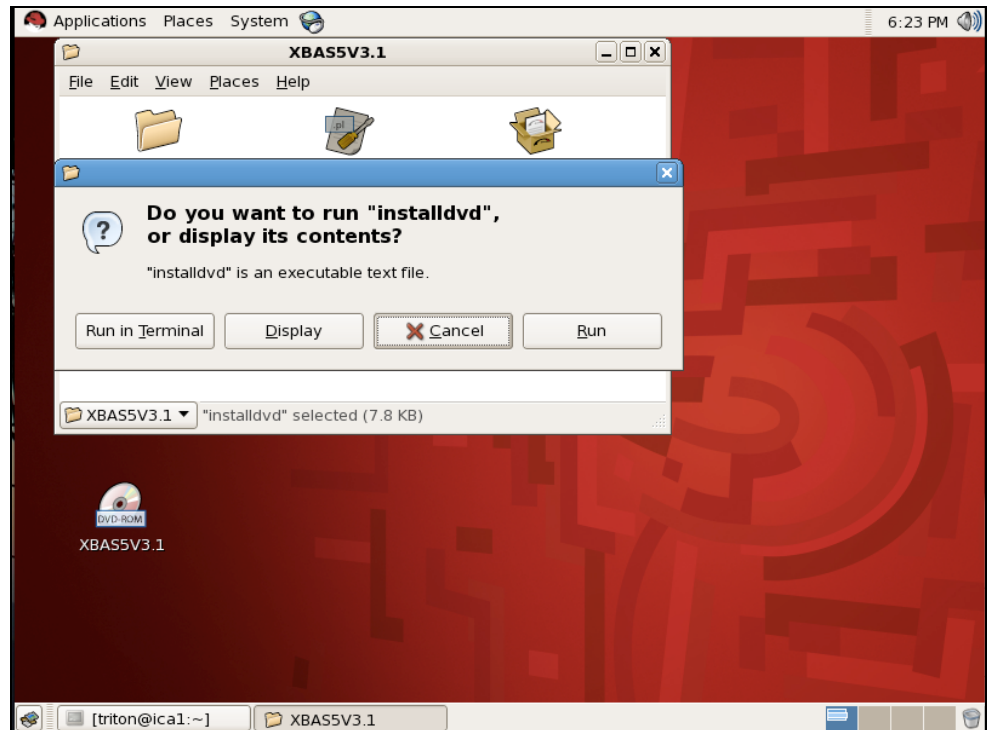


Figure 2-2. **installvdv** script run options

3. Select **Run in Terminal** from the run options displayed above.

4. Repeat steps 1. to 3. for the **bullx cluster suite XR SN-OS Errata3 for Red Hat Enterprise Linux 5.3 (EM64T)** media.
5. **bullx cluster suite XR 5v3.1 U1 clusters only**

---

**Note** This point only applies to **bullx cluster suite XR 5v3.1 U1** clusters that use the **bullx cluster suite XR CN** distribution for Compute Nodes.

---

Rename the previous "CSXR5v3.1U1CN" directory on MANAGEMENT Node by running the following command:

```
mv /release/CSXR5v3.1U1CN/ /release/bullxLinux5.3
```

6. Repeat steps 1. to 3. for the **bullx cluster suite XR CN-OS Errata3 for Linux 5.3 (EM64T)** media.

---

**See** Go to Section 2.3 if your cluster included Highly Available Management Nodes.

---

## 2.2.4 Install the bullx cluster suite XR 5v3.1 Update 3 Software

1. Go to the `/release/XBAS5V3.1` directory:

```
cd /release/XBAS5V3.1
```

2. Execute the command:

```
./install
```

3. Confirm all the update options that appear.

---

 **Important** See the *Software Release Bulletin* for details of any BONUS RPMS to be installed manually on the Management Node.

---

**Note** Please note that the upgrade installation process will take a while (approximately 5 minutes).

---

4. Check that the upgrade has installed correctly by:
  - a. Looking at the last line in the `/root/xbas5_installation.log` file, this has to have the following format:

```
==== - ===== ending installation script - <date_and_time_of_your_installation>
```

Example:

```
==== - ===== ending installation script - 2010/04/08 11:58:11
```
  - b. Looking at the differential for the log files (before and after the installation). An example of the **sdiff** command, used to produce the differential, is shown below:

```
sdiff -s list-01before-instal-XBAS5V3.1-<date_and_time_before>  
list-02after-instal-XBAS5V3.1-<date_and_time_after> | more
```



---

**Note** If there are any problems, the last lines in the `/root/xbas5_installation.log` file will provide more information; for example:

```
yum INFO - Error: Missing Dependency: ruby-libs = 1.8.5-5.el5_2.6
is needed by package ruby-1.8.5-5.el5_2.6.x86_64 (installed)
ERROR - processing packages upgrading stopped
ERROR - Error: Missing Dependency: ruby-libs = 1.8.5-5.el5_2.6 is
needed by package ruby-1.8.5-5.el5_2.6.x86_64 (installed)
```

See the **Software Release Bulletin** for more information on dependency problems.

---

## 2.2.5 Configure the Management Node

The **bullx cluster suite XR 5v3.1U3** Management Node will be configured automatically except for the files listed below, where a manual intervention is required.

### 2.2.5.1 Nagios Configuration Files

For clusters that include customized services, the following **nagios** configuration files should be updated with the configuration details included in the files saved previously - see *Section 2.1.2*.

```
/etc/nagios/services-tpl.cfg
/etc/nagios/hpccommands.cfg
/etc/nagios/hosts-tpl.cfg
/etc/nagios/hostgroups-tpl.cfg
```

---

**Notes**

- These files will overwrite the newly installed versions.
- Customized **nagios** services, as well as the new services delivered by **bullx cluster suite**, will thus be available.

---

### 2.2.5.2 syslog-ng Configuration Files

Restore the **syslog-ng.conf** file saved externally once **bullx cluster suite XR 5v3.1U3** has been installed.

### 2.2.5.3 Optional - PBS Professional clusters

---

**See** See *Section 3.2* in the *Bull PBS Professional Guide* and carry out the operations described.

---

### 2.2.5.4 Reboot the Management Node

Reboot the Management Node if your cluster does NOT include High Availability for the Management Node.

## 2.3 Updating Highly Available Management Nodes

This section describes the update procedure for Highly Available Management Nodes.

Both the Primary and Secondary Management Nodes must have been properly configured, as described in the **Chapter 3** of the **bullx cluster suite High Availability Guide**.

Run the `installvdvd` script from the **bullx cluster suite XR 5v3.1U3** media as described in section 2.2.2. This will update the `/release` directory with the **bullx cluster suite XR 5v3.1U3** packages. The `/release` directory has to be updated on **BOTH** Management Nodes in the cluster. **HA Cluster Suite** has to be started on both nodes.

The `HA_MGMT` and `HA_NFS` services have to be disabled on both Management Nodes. If this is not the case, run the commands below:

```
clusvcadm -d HA_MGMT
clusvcadm -d HA_NFS
```

The file systems from the shared storage system must be unmounted on both Management Nodes.

### 2.3.1 Update the Primary Management Node

1. Mount all the file systems used by the `HA_MGMT` group of services from the shared storage system. This includes the file systems used by the Batch and Resource Managers.

- a. If the `gfs2` file system type is used, run the commands below:

```
mount LABEL=HA_MGMT:clusterdb /var/lib/pgsql/data
mount LABEL=HA_MGMT:syslog /var/log/HOSTS
mount LABEL=HA_MGMT:ganglia /var/lib/ganglia/rrds
mount LABEL=HA_MGMT:cyrus /var/lib/imap
mount LABEL=lustr_mgs /home/lustre
```

- b. If the `ext3` file system type is used, run the commands below:

```
mount LABEL=clusterdb /var/lib/pgsql/data
mount LABEL=syslog /var/log/HOSTS
mount LABEL=ganglia /var/lib/ganglia/rrds
mount LABEL=cyrus /var/lib/imap
mount LABEL=lustr_mgs /home/lustre
```

---

**See** The **bullx cluster suite High Availability Guide** and *Software Release Bulletin* for more information regarding the file system type to be used for each service.

---

2. Update the Primary Management Node by running the command:

```
/release/XBAS5V3.1/install
```

---

**Note** Please note that the update installation process will take a while (approximately 5 minutes).

---

3. Check that the upgrade has installed correctly by:
  - a. Looking at the last line in the `/root/xbas5_installation.log` file, this has to have the following format:

```
==== - ===== ending installation script - <date_and_time_of_your_installation>
```

Example:

```
==== - ===== ending installation script - 2010/04/08 11:58:11
```

- b. Looking at the differential for the log files (before and after the installation). An example of the **sdiff** command, used to produce the differential, is shown below:

```
sdiff -s list-01before-instal-XBAS5V3.1-<date_and_time_before>  
list-02after-instal-XBAS5V3.1-<date_and_time_after> | more
```

**Note** If there are any problems, the last lines in the `/root/xbas5_installation.log` file will provide more information; for example:

```
yum INFO - Error: Missing Dependency: ruby-libs = 1.8.5-5.el5_2.6  
is needed by package ruby-1.8.5-5.el5_2.6.x86_64 (installed)  
ERROR - processing packages upgrading stopped  
ERROR - Error: Missing Dependency: ruby-libs = 1.8.5-5.el5_2.6 is  
needed by package ruby-1.8.5-5.el5_2.6.x86_64 (installed)
```

See the **Software Release Bulletin** for more information on dependency problems.

4. Reapply the High Availability parameters, after disabling the automatic start-up of the High Availability services at boot with the command:

```
/usr/lib/clustmngt/ha/bin/haunwantedfiles start
```

5. Remount all the file systems listed in point 1 according to your file system type.
6. Check that the **HA\_MGMT** services start without any problems by running the command.

```
/usr/sbin/haservices start
```

7. If no errors are reported, stop the **HA\_MGMT** services.

```
/usr/sbin/haservices stop
```

8. Unmount the shared file systems.

```
umount /var/lib/pgsql/data  
umount /var/log/HOSTS  
umount /var/lib/ganglia/rrds  
umount /var/lib/imap  
umount /home/lustre
```

9. Stop **HA Cluster Suite**.

```
storioha -c stop
```

10. Reboot the Primary Management Node.

```
reboot
```

## 2.3.2 Update the Secondary Management Node

1. Mount the file systems from the shared storage system on the Secondary Management Node, as done for the Primary Management Node above.
2. Check that **HA Cluster Suite** is running and both the **HA\_MGMT** and **HA\_NFS** group of services are in a disabled state. Stop the **haservices** and **NFS** services.

```
clustat
/usr/sbin/haservices stop
/etc/init.d/nfs stop
```

3. Update the Secondary Management Node by running the command:

```
/release/XBAS5V3.1/install
```

---

**Note** Please note that the update installation process will take a while (approximately 5 minutes).

---

4. Check that the upgrade has installed correctly by:
  - a. Looking at the last line in the `/root/xbas5_installation.log` file, this has to have the following format:

```
==== - ===== ending installation script - <date_and_time_of_your_installation>
```

Example:

```
==== - ===== ending installation script - 2010/04/08 11:58:11
```

- b. Looking at the differential for the log files (before and after the installation). An example of the **sdiff** command, used to produce the differential, is shown below:

```
sdiff -s list-01before-instal-XBAS5V3.1-<date_and_time_before>
list-02after-instal-XBAS5V3.1-<date_and_time_after> | more
```

---

**Note** If there are any problems, the last lines in the `/root/xbas5_installation.log` file will provide more information; for example:

```
yum INFO - Error: Missing Dependency: ruby-libs = 1.8.5-5.el5_2.6
is needed by package ruby-1.8.5-5.el5_2.6.x86_64 (installed)
ERROR - processing packages upgrading stopped
ERROR - Error: Missing Dependency: ruby-libs = 1.8.5-5.el5_2.6 is
needed by package ruby-1.8.5-5.el5_2.6.x86_64 (installed)
```

See the **Software Release Bulletin** for more information on dependency problems.

---

5. Reapply the High Availability parameters, after disabling the automatic start-up of the High Availability services at boot with the command:

```
/usr/lib/clustmngt/ha/bin/haunwantedfiles start
```

6. Remount all the file systems listed in point 1 in section 2.3.1 according to your file system type.
7. Check that the **HA\_MGMT** services start without any problems by running the command.

```
/usr/sbin/haservices start
```

8. If no errors are reported, stop the HA\_MGMT services.

```
/usr/sbin/haservices stop
```

9. Unmount the shared file systems.

```
umount /var/lib/pgsql/data
umount /var/log/HOSTS
umount /var/lib/ganglia/rrds
umount /var/lib/imap
umount /home/lustre
```

10. Stop HA Cluster Suite.

```
storioha -c stop
```

11. Reboot the Secondary Management Node.

```
reboot
```

### 2.3.3 Final Steps for Updating High Availability on the Management Nodes

1. Start HA Cluster Suite on both Management Nodes.

```
pdsh -w mgmt1,mgmt2 storioha -c start
```

2. Launch the HA\_GMT group of services on the Primary Management Node.

```
clusvcadm -e HA_MGMT
```

3. Load the new Management Node High Availability settings for the HA Cluster Suite software, using the same parameters as were previously in place, with the addition of the -H flag, for example:

```
stordepha -c configure -o admin+nfs -H -i mgmt1,mgmt2
```

4. Disable the HA\_MGMT group of services, and restart HA Cluster Suite.

```
clusvcadm -d HA_MGMT
umount /var/lib/pgsql/data
umount /var/log/HOSTS
umount /var/lib/ganglia/rrds
umount /var/lib/imap
pdsh -w mgmt1,mgmt2 storioha -c stop
pdsh -w mgmt1,mgmt2 storioha -c start
clusvcadm -e HA_MGMT
```



**Important** Configure both Management Nodes as described in *Section 2.2.5*

## 2.4 Update and Configure the Reference Nodes

### 2.4.1 Install the bullx cluster suite XR 5v3.1 Update 3 Software

Update all the existing Reference Nodes to **bullx cluster suite XR 5v3.1 U3** by carrying out the following procedure:

1. Check that the **/release** directory of the Management Node is mounted on the Reference Node.

```
mount
```

If it is not, mount it.

2. Go to the **/release/XBAS5V3.1/** directory:

```
cd /release/XBAS5V3.1/
```

3. Run the command below:

```
./install
```

---

**Note** Please note that the update installation process will take a while (approximately 5 minutes).

---

4. The error message below can be ignored:

```
WARNING: according to /etc/bull-infos,  
'XBAS5' is already installed on this system.
```

5. Confirm the update by pressing the **enter** key when the prompt stops. An example for a **COMPUTE** node is shown below.

```
Please confirm that you want to upgrade XBAS5 products.  
Do you want to upgrade:  
- RHEL mandatory packages  
- XHPC product  
- XIB product  
- XLUSTRE product  
for COMPUTE node on this system ? [y]/n :
```



**Important** See the *Software Release Bulletin* for details of any BONUS RPMS to be installed manually on the Reference Nodes.

---

6. Check that the upgrade has installed correctly by:
  - a. Looking at the last line in the **/root/xbas5\_installation.log** file, this has to have the following format:

```
==== - ===== ending installation script - <date_and_time_of_your_installation>
```

For example:

```
==== - ===== ending installation script - 2010/04/08 11:58:11
```

- b. Looking at the differential for the log files (before and after the installation). An example of the **sdiff** command, used to produce the differential, is shown below:

```
sdiff -s list-01before-instal-XBAS5V3.1-<date_and_time_before>  
list-02after-instal-XBAS5V3.1-<date_and_time_after> | more
```

---

**Note** If there are any problems, the last lines in the `/root/xbas5_installation.log` file will provide more information; for example:

```
yum INFO - Error: Missing Dependency: ruby-libs = 1.8.5-5.e15_2.6  
is needed by package ruby-1.8.5-5.e15_2.6.x86_64 (installed)  
ERROR - processing packages upgrading stopped  
ERROR - Error: Missing Dependency: ruby-libs = 1.8.5-5.e15_2.6 is  
needed by package ruby-1.8.5-5.e15_2.6.x86_64 (installed)
```

See the **Software Release Bulletin** for more information on dependency problems.

---

## 2.4.2 Optional - PBS Professional clusters

---

**See** See *Section 3.3* in the Bull *PBS Professional Guide*.

---

## 2.5 Deployment of the bullx cluster suite XR 5v3.1 U3 Reference Nodes

### 2.5.1 Pre Deployment Operations

#### 2.5.1.1 Configure the MPI user environment

Configure the **MPI** user environment according to the **MPI** library.

##### **MPIBull2**

Any **MPIBull2** environment shell scripts previously installed in the `/etc/profile.d/` directories will need to be upgraded with the new **bullx cluster suite XR 5v3.1 U3** versions. These scripts are upgraded on the reference nodes as follows:

```
cp /opt/mpi/mpibull2-<version>/share/mpibull2.sh /etc/profile.d
```

##### **bullx MPI**

The **bullx MPI RPM** includes 2 automatic setup files that define the default environment settings:

```
/opt/mpi/bullxmpi/<version>/bin/mpivars-<version>.*sh
```

Run one of the commands below to configure the **MPI** user environment:

```
source /opt/mpi/bullxmpi/<version>/bin/mpivars.csh
```

```
source /opt/mpi/bullxmpi/<version>/bin/mpivars.sh
```

The **MPI** user environment variables are set by either running a setup file or by loading a **bullx MPI** module.

##### **Loading bullx MPI with the oscar module**

If your operating system includes the **oscar** module then load it by running the command below:

```
module load bullxmpi-<version>
```



**Important** When migrating from **MPIBull2** to **bullx MPI** all existing applications that used the **MPIBull2** environment will need to be recompiled in the **bullx MPI** environment.

#### 2.5.1.2 Optional - NVIDIA Toolkit 3.0

For clusters that upgrade from **NVIDIA Toolkit 2.3**, the `PATH` and `LD_LIBRARY_PATH` environment variables must be updated with:

```
source /opt/cuda/3.0/cuda.sh
```

Reboot the Reference Node or run the command below:

```
/etc/init.d/cuda restart
```



### 2.5.1.3

#### Optional - NFS High Availability Clusters Only

1. In the `/etc/modprobe.conf` and `/etc/modprobe.d/lpfc` files, add the line:

```
options lpfc lpfc_nodev_tmo=5
```

2. Identify the kernel version installed on the node by running the command:

```
uname -r
```

3. Save the old `initrd` image using the kernel version, identified above:

```
mv /boot/initrd-<kernel_version>.img /boot/initrd-<kernel_version>.img-orig
```

4. Generate a new `initrd` image:

```
mkinitrd -v /boot/initrd-<kernel_version>.img <kernel_version>
```

### 2.5.1.4

#### Optional - NIS Clusters Only

The `NISDOMAIN` definition line has to be added manually to the `/etc/sysconfig/network` file on the Reference Nodes before deployment, as follows:

```
NISDOMAIN=<DOMAIN>
```

## 2.5.2

### Deployment Pre-Requisites

The following pre-requisites should be in place before the new **bullx cluster suite XR 5v3.1U3** images are created and deployed by **Ksis**:

- **Ksis Image Server** has been installed on the Management Node.
- The cluster database is accessible. This can be checked by running the command:

```
ksis list
```

The result must be "*no data found*" or an image list with no error messages.

- All the nodes that will receive a particular image, for example the `COMPUTEX` image, are hardware equivalent, that is use the same platform, disks and network interfaces.
- All system files are on local disks and not on the disk subsystem.
- Each node is configured to boot from the network via the `eth0` interface. If necessary edit the BIOS menu and set the Ethernet interface as the primary boot device.
- All the nodes for the deployment are powered on. This can be checked by running the `nsctrl` command, for example:

```
nsctrl status xena[1-100]
```

Any nodes that are shown as **inactive** will need to be powered on.

- All the nodes for the deployment must be **up**. This can be checked using the command below from the Management Node:

```
ksis nodelist
```

- If the status for any of the nodes is different from **up**, then restart **Nagios** by running the following command from the root prompt on the Management Node:

```
service nagios restart
```



**Important** The node descriptions and administration network details in the cluster database must be up to date and correct before the KSIS deployment is launched. If the ClusterDB has changed following the installation of BAS5 for Xeon V3.1 or bullx cluster suite XR 5v3.1 U1/U2 (new hardware added, descriptions changed etc.), then run the command below to update the KSIS information:

```
ksis builddatanode
```

**Note** Before carrying out the deployment the **rms** status of the nodes must be **OUT**.

## 2.5.3 Create the Images

Create an image of each **bullx cluster suite XR 5v3.1U3** Reference Node.

```
ksis create <image_name> <reference_node_name> -D "image_description"
```

### Example

```
ksis create image1 ns1 -D "My_Cluster_Compute_Node_Image"
```

**Note** If the **-D** option is not used, the creation of the image will stop until an image description is entered.

The **ksis create** command will also ask for a check level. Select the **basic** level. If no level is selected, the **basic** level will be selected automatically by default after the timeout.

## 2.5.4 Deploy the Images on the Cluster

Start the deployment by running the command:

```
ksis deploy <image_name> node[n-m]
```

If, for example, 3 Compute Nodes are listed as ns[2-4], then enter the following command for the deployment:

```
ksis deploy image1 ns[2-4]
```

**Note** The Reference nodes may be kept as reference nodes. Alternatively, they may be included in the deployment for the cluster, in the same way as the other nodes. It is recommended that this second option is chosen.

## 2.6 Post Deployment Configuration

### 2.6.1 postconfig command

---

**Note** Wait until the deployment has finished, including the reboot of the nodes, before carrying out the post deployment configuration.

---

The cluster nodes will now need to be configured according to their type - Compute, I/O, etc. Post deployment configuration is mandatory as it configures **Ganglia**, **Syslog-ng**, **NTP**, and **SNMP** on the nodes.

The **Ksis postconfig** command configures each node of a particular type in the same way, ensuring that they are all homogenous.

**Ksis** post-configuration is carried out by running the command:

```
ksis postconfig run PostConfig <cluster_name>[nodelist]
```

**For example**

```
ksis postconfig run PostConfig xena[1-100]
```

### 2.6.2 Configure the Interconnect Interfaces

Use the **config\_ip** command to configure the interconnect interfaces for BOTH **InfiniBand** and **Ethernet** networks.

---

**See** *Appendix C - Configuring Interconnect Interfaces* in this manual for details on using the **config\_ip** command.

---

## 2.7 Post Installation Operations

### 2.7.1 Restore the I/O Node aliases

Once the **bullx cluster suite XR 5v3.1U3** I/O Reference Nodes have been deployed, the aliases have to be restored on each I/O Node. According to whether or not a storage model exists for the cluster, either **a.** or **b.**, below, is used to restore the aliases.

- a. Where a storage model exists, then use the deployment command from the Management Node, as shown below:

```
stordepmap -m <model_name> -i <nodelist>
```

- b. If no storage model exists, use the **stordiskname** command to create a new **disknaming.conf** file, as shown below.



**Important** The existing **disknaming.conf** file will be erased when the new I/O nodes are deployed. The **stordiskname** command should be used with the **-r** option (remote) from the Management Node enabling backups and restorations of the **/etc/storageadmin/disknaming.conf** file to be managed automatically. If the **-r** option is not used, the Administrator will have to manage the backup of the **/etc/storageadmin/disknaming.conf** file manually.

When used remotely (**-r** option) - immediately after the I/O node deployment - the **stordiskname** command must be used in **update** mode (**-u** option). This ensures that the LUNs are addressed by the same symbolic link names, as used previously, and avoids having to configure the file system again.

- i. The **stordiskname** command should be executed from the Management Node as shown below.

#### If the node is NOT in a High-Availability pair

```
stordiskname -u -r <node_name>
```

#### If the node is in a High-Availability pair

```
stordiskname -u -r <node1_name>,<node2_name>
```

**Note** For some storage systems, not including **FDA** and **DDN**, the **stordiskname** command may return an error similar to the one below:

```
Error : -= This tool does not manage configuration where a given UID appears more than once on the node = -
```

If this happens try running it with the **-m SCSI\_ID** option.

- ii. The symbolic links (aliases) must be recreated on each node using the information contained within the **disknaming.conf** file, newly created by **stordiskname**. To do this, run the **stormap** command, as below.

If the node is NOT in a High-Availability pair

```
ssh root@<node_name> "stormap -c"
```

If the node is in a High-Availability pair

```
ssh root@<node1_name> "stormap -c"  
ssh root@<node2_name> "stormap -c"
```

## 2.7.2 Install the Intel Compilers and Tools on the Login Nodes

---

**See** Chapter 7 - *Installing Intel Tools and Applications* in this manual for more information.

---

## 2.7.3 Optional - PBS Professional clusters

---

**See** See Section 3.4 in the Bull PBS Professional Guide.

---

## 2.7.4 Optional - for NFS clusters

Restart the NFS service:

```
service nfs start
```

**NFS Clusters with High Availability**

Reconfigure **HA Cluster Suite** on High Availability I/O Nodes.

---

**See** The **bullx cluster suite High Availability Guide** for details of how to use the **stordepha** command for clusters which have **High Availability** in place for the NFS I/O nodes.

---

## 2.7.5 Optional - for Lustre clusters only

Carry out the actions, below, following the upgrade to **bullx cluster suite XR 5v3.1U3**.

1. Check the storage configuration
    - a. If necessary, restore the **/etc/storageadmin/disknaming.conf** files on the I/O nodes.
- 

**Note** The RPM upgrade to **bullx cluster suite XR 5v3.1U3** does not modify the **disknaming.conf** files, therefore in most situations this operation will not be necessary.

---

- b. If there is a problem and it is not possible to restore the previous version of the **disknaming.conf** file, then run the command, below, on the Management Node to regenerate the **disknaming.conf** file on each I/O node.

```
stordepmap -m </etc/storageadmin/models/model file> -p -c
```

- c. Quit this step only when the **stormap -l** command, run on each I/O node, indicates that all I/O node devices are **UP**.

## 2. Restore and update the Lustre configuration files

### a. `lustre.cfg` file:

- i. If the `lustre.cfg` installed by the **bullx cluster suite XR 5v3.1U3** RPM is same as the `lustre.cfg` file installed by the previous **BAS5 for Xeon** release RPM, then the `lustre.cfg.rpmnew` file will not be created. This is normal and no further action is required.

OR

- ii. After the upgrade to **bullx cluster suite XR 5v3.1U3**, edit the newly installed `/etc/lustre/lustre.cfg.rpmnew` file, and add any modifications that have been previously made to the old `/etc/lustre/lustre.cfg` file. Use the `diff` command to compare the existing `lustre.cfg` file and the new `lustre.cfg.rpmnew` file.

After backporting the changes into the `lustre.cfg.rpmnew` file, rename it as the `/etc/lustre/lustre.cfg` file. Then distribute the `lustre.cfg` file onto the I/O nodes by using the `lustre_util set_cfg` command.

### b. File system model files:

- i. If the `fs1.lmf` installed by the **bullx cluster suite XR 5v3.1U3** RPM is same as the `fs1.lmf` file installed by the previous **BAS5 for Xeon** release RPM, then the `fs1.lmf.rpmsave` file will not be created. This is normal and no further action is required.

OR

- ii. After the upgrade to **bullx cluster suite XR 5v3.1U3**, edit the newly installed `fs1.lmf` file, and add any modifications that have been previously made to the old `/etc/lustre/models/fs1.lmf.rpmsave` file. Use the `diff` command to compare the existing `fs1.lmf.rpmsave` file and the new `fs1.lmf` file.



**Important** For large Lustre file systems, before running the `lustre_util update` command, below, the index must be generated by running the command `lustre_ldap index`

---

Run the command below, to apply any changes that have been made to the tuning parameters for the **Lustre** installation:

```
lustre_util update -f /etc/lustre/models/<modified lmf file>.lmf
```

## 3. Start the Lustre daemons and test SSH connectivity

### a. Test **SSH** connectivity by running the command below:

```
pdsh -w <IO node list> "ssh <management node> echo 'OK'" | dshbak -c
```

If there is a problem with **SSH** reconfigure it so that it works.

### b. Launch the **MGS** service.

Restore the **MGS** backend, as and when needed, by running the command:

```
service mgs start
```

If the Management Node is NOT Highly Available, add the **MGS** service to the `chkconfig` file:

```
chkconfig --add mgs
```

- c. Launch the **LDAP** service - **Lustre High Availability Clusters** only.  
Restore the **LDAP** backend, as and when needed, by running the command:

```
service ldap start
```

Verify the **LDAP** content by running the command:

```
lustre_ldap show
```

This command will show details of the **Lustre High Availability** file systems that are installed.

---

**Note** If an error occurs and no data is displayed, the **LDAP** directory has to be populated with the content that has been backed-up previously, as described in the pre-install section, using the commands below.

---

```
lustre_ldap init
lustre_ldap override -l
/somewhere/on/the/management/node/lustre_ldap_backup.ldif
lustre_ldap dump -l /tmp/temporary.ldif
```

If the Management Node is NOT Highly Available, add the **LDAP** service to the **chkconfig** file:

```
chkconfig --add ldap
```

- d. Launch **lustredbd** - **Lustre High Availability Clusters** only.

```
service lustredbd.sh start
```

If the Management Node is NOT Highly Available, add the **lustredbd** to the **chkconfig** file:

```
chkconfig --add lustredbd.sh
```

#### 4. Setup and start HA Cluster Suite - Lustre High Availability Clusters only

- a. **HA Cluster Suite** configuration files will already be in place, and updating to **bullx cluster suite XR 5v3.1U3** does not affect them. However, the new version of **HA Cluster Suite** template configuration files includes some significant bug fixes, and so it is important to regenerate the configuration files to avoid these bugs. Run the command below to do this:



**Important** It is recommended that the Heuristic functionality of **stordepha** command (option **-H**) is used for High Availability node pairs.

---

```
stordepha -c configure -i <all | IO node list> -o lustre [-H]
```

- b. Start **HA Cluster Suite** daemons:

```
stordepha -c start -i <all | IO node list>
```

- c. Start the **Lustre** High Availability services:

```
lustre_migrate hastart -n <all | IO node list>
```

## 5. Start Lustre - All Lustre clusters

- a. Start **Lustre**:

```
lustre_util start -f <fsname> [-V]
```

- b. Mount the **Lustre** clients:

```
lustre_util mount -f <fsname> -n <all | client nodes list> [-V]
```

## 2.7.6 Post Installation Checks

Carry out the post installation checks that are described in **STEP 7** in Chapter 3 in this manual.

## 2.8 Known issues for the Upgrade Process

### 2.8.1 Lustre Performance Loss

**Problem description:** If the Lustre **stripe\_size** parameter was set to a value lower than **1MB** with **4KB** pages, performance loss may result after updating Lustre to the new version. This is due to the fact that for the previous **Lustre** version, the **stripe\_size** parameter was automatically (and silently) adjusted regarding the page size: **1MB** minimum on **4KB** page size kernels.

**Solution:** The recommended solution is to comment the **stripe\_size** line in the **Lustre** model file corresponding to your filesystem, and run the command **lustre\_util update -f <path to .lmf file>**.

### 2.8.2 Kdump

Ensure that the kernel options remain the same when upgrading from **BAS5 for Xeon V3.1** to **bullx cluster suite XR 5v3.1 U3**

If there are any problems with a particular piece of hardware, add the "**acpi=off nomsi nolapic noapic**" options to the **KDUMP\_COMMANDLINE\_APPEND** parameter in the **/etc/sysconfig/kdump** configuration file, so that the parameters appear, as below:

```
-----  
KDUMP_COMMANDLINE_APPEND="irqpoll maxcpus=1 reset_devices acpi=off  
nomsi nolapic noapic"  
-----
```



## 2.9 Updating NFS High Availability I/O Nodes with minimal loss of service

See *bullx cluster suite High Availability Guide* for more information on NFS High Availability.

This section describes how to upgrade a pair of **bullx cluster suite** NFS I/O nodes, within an I/O cell, to **bullx cluster suite XR 5v3.1U3** with **no loss of service** in an **active/passive** NFS architecture.



**Important** It is assumed that the **bullx cluster suite XR 5v3.1 U3** software installation and configuration operations described in this chapter have been carried on the **Management Node** before this procedure is undertaken.

### 2.9.1 I/O Node Upgrade Procedure with no loss of Service

For this procedure, the **HA\_NFS** service is active on **Primary Node1** and the **Secondary Node2** is passive. Carry out the following steps:

1. Save the existing **Cluster Suite** `/etc/cluster/cluster.conf` file for the I/O cell onto a non formattable device, exterior to the cluster.
2. Stop **Cluster Suite** locally on **Secondary Node2**, by running the command:

```
storioha -c stop
```

3. Mount **NFS** from the `/release` directory on the Management Node to the `/release` directory on the **Secondary Node2**:

```
ssh <Secondary_Node2>  
mount -t nfs <Management_Node_VIP>:/release /release
```

4. Go to the `/release/XBAS5V3.1` directory:

```
cd /release/XBAS5V3.1
```

5. Execute the install command:

```
./install
```

6. Confirm all the installation options that appear.
7. Modify the `/etc/modprobe.conf` and `/etc/modprobe.d/lpfc` files as described in Section 2.5.1.2.
8. Reboot **Secondary Node2**.
9. Copy the `cluster.conf` file saved in Step 1. back onto **Secondary Node2**.
10. Stop Cluster Suite on the **Primary Node1**:

```
storioha -c stop
```

11. Restart **Cluster Suite** locally on **Secondary Node2**:

```
storioha -c start
```

12. Launch the **HA\_NFS** service on **Secondary Node2**, by running the command:

```
clusvcadm -e HA_NFS
```

13. Mount **NFS** from the **/release** directory on the Management Node to the **/release** directory on **Primary Node1**:

```
ssh <Primary_Node1>  
mount -t nfs <Management_Node_VIP>:/release /release
```

14. Go to the **/release/XBAS5V3.1** directory:

```
cd /release/XBAS5V3.1
```

15. Execute the install command:

```
./install
```

---

**Note** Please note that the update installation process will take a while (approximately 5 minutes).

---

16. Check that the upgrade has installed correctly by:

- a. Looking at the last line in the **/root/xbas5\_installation.log** file, this has to have the following format:

```
==== - ===== ending installation script - <date_and_time_of_your_installation>
```

Example:

```
==== - ===== ending installation script - 2010/04/08 11:58:11
```

- b. Looking at the differential for the log files (before and after the installation). An example of the **sdiff** command, used to produce the differential, is shown below:

```
sdiff -s list-01before-instal-XBAS5V3.1-<date_and_time_before>  
list-02after-instal-XBAS5V3.1-<date_and_time_after> | more
```

---

**Note** If there are any problems, the last lines in the **/root/xbas5\_installation.log** file will provide more information; for example:

```
yum INFO - Error: Missing Dependency: ruby-libs = 1.8.5-5.el5_2.6  
is needed by package ruby-1.8.5-5.el5_2.6.x86_64 (installed)  
ERROR - processing packages upgrading stopped  
ERROR - Error: Missing Dependency: ruby-libs = 1.8.5-5.el5_2.6 is  
needed by package ruby-1.8.5-5.el5_2.6.x86_64 (installed)
```

See the **Software Release Bulletin** for more information on dependency problems.

---

17. Confirm all the installation options that appear.

18. Modify the **/etc/modprobe.conf** and **/etc/modprobe.d/lpfc** files as described in Section 2.5.1.2

19. Reboot **Primary Node1**.

20. Copy the **cluster.conf** file saved in Step 1. back onto **Primary Node1**.

21. Restart **Cluster Suite** locally on **Primary Node1**:

```
storioha -c start
```

22. Relocate the **HA\_NFS** service onto **Primary Node1**, by running the command:


```
clusvcadm -r nfs_service -m
```

---

## Chapter 3. Installing bullx cluster suite XR 5v3.1 U3 Software on the Cluster Nodes

This chapter describes the complete installation process for a **FIRST** installation of the **bullx cluster suite XR 5v3.1 U3** software environment on all nodes of a Bull **extreme computing** cluster. The same process can also be used for a **reinstallation** of **bullx cluster suite XR 5v3.1 U3** using the existing configuration files – see section 3.0.

---

 **Important** Read this chapter carefully. Pay particular attention to the different **bullx cluster suite XR** installation options available, and be sure to select those that apply to your cluster.

---

**See** The **Software Release Bulletin** delivered with your **bullx cluster suite XR 5v3.1 U3** release for details of any restrictions that may apply.

---

**bullx cluster suite XR** covers two separate distributions:

- **bullx cluster suite XR SN** based on the **Red Hat Enterprise Linux 5.3** operating system.
- **bullx cluster suite XR CN** based on the **bullx cluster suite XR CN-OS** operating system. This distribution is compatible with **Red Hat Enterprise Linux 5.3** and is only available for the Compute Nodes.

The table below shows the two **bullx cluster suite XR** installation options for the cluster nodes.

Cluster Type	Service Node Distribution	Compute Node Distribution
1	bullx cluster suite XR SN	bullx cluster suite XR SN
2	bullx cluster suite XR SN	bullx cluster suite XR CN

Table 3-1. **bullx cluster suite XR** installation types


Other previously existing **BAS5 for Xeon** installation options still apply.

- Bull **XIB** software – for clusters which use **InfiniBand** interconnects.
- Bull **XLustre** software – for clusters which use the **Lustre** parallel file system.
- Bull **HPC Toolkit** monitoring tools – all clusters.

Two functional possibilities exist for the Compute Nodes. These are:

- A Minimal Compute or **COMPUTE** Node, which includes minimal functionality and is quicker and easier to deploy.
- An Extended Compute or **COMPUTEX** Node, which includes additional libraries and will take longer to deploy. These nodes are used for most ISV applications and for applications that require a graphical environment (X Windows). They are also installed if there is a need for **Intel® Cluster Ready** compliance.

---

 **Important** This chapter describes **bullx cluster suite XR 5v3.1 U3** installation process for clusters without any form of High Availability in place. Refer to the *High Availability Guide* and the product manuals (*Lustre Guide*, *SLURM Guide* etc.) for more information on High Availability.

---

## Installation Process Overview

The process to install **bullx cluster suite XR 5v3.1U3** on the extreme computing cluster's nodes is divided into different steps, to be carried out in the order shown below:

<b>Backup Operations when Re-installing bullx cluster suite XR 5v3.1U3</b> Skip this step if you are installing for the first time.		
<b>STEP 1</b>	<b>Install the RHEL5.3 software on the Management node</b> 1) Optional - RAID configuration 2) Installation of the <b>Red Hat Enterprise Linux 5</b> Server software 3) First boot settings 4) Configure the Network 5) Install an external Storage System	Page 3-4
<b>STEP 2</b>	<b>Install bullx cluster suite software on the Management Node</b> 1) Prepare the installation of <b>bullx cluster suite XR SN</b> distribution on the other cluster nodes 2) Optional - Prepare the installation of <b>bullx cluster suite XR CN</b> distribution on the Compute Nodes (Cluster Type 2 - see Table 3-1) 3) Installation of <b>bullx cluster suite XR SN</b> software on the Management Node 4) Configuration of the Cluster Database	Page 3-18
<b>STEP 3</b>	<b>Configure equipment and install utilities on the Management Node</b> 1) Generate the SSH keys 2) Configure Ethernet switches 3) Update the MAC addresses in the Cluster Database 4) Optional - Configure the Bull Cool Cabinet Door 5) Install and configure <b>postfix, ganglia, syslog-ng, NTP, kdump, LDAP, SLURM</b> and <b>PBS Pro</b>	Page 3-25
<b>STEP 4</b>	<b>Install RHEL5.3, bullx cluster suite XR 5v3.1U3 Software, and optional extreme computing software products on other nodes</b> 1) Specify the software and the nodes to be installed 2) Run the <b>installnfs</b> script	Page 3-36
<b>STEP 5</b>	<b>Configure Administration Software on Login, I/O, COMPUTE and COMPUTEX Reference Nodes</b> 1) Install and configure <b>ssh, ganglia, kdump, LDAP, SLURM, and PBS Pro</b> 2) Configure the <b>MPI</b> User environment 3) Optional - Install <b>NVIDIA</b> accelerators and <b>CUDA</b> Toolkit 4) Optional - Install <b>RAID</b> monitoring software 5) Optional - <b>NFS HA</b> Clusters	Page 3-41
<b>STEP 6</b>	<b>Create and deploy a reference node image on the cluster nodes using Ksis</b> 1) Installation and configuration of the image server 2) Create and deploy reference images of <b>Login, I/O and COMPUTE(X)</b> nodes 3) Post deployment configuration 4) Install <b>Intel</b> compilers and tools on the Login Nodes	Page 3-49
<b>STEP 7</b>	<b>Final Cluster Checks</b>	Page 3-52

## 3.0 Pre-installation Backup Operations when Re-installing bullx cluster suite XR 5v3.1 U3

This step describes how to save the **ClusterDB** database and other important configuration files. Use this step only when re-installing **bullx cluster suite XR 5v3.1 U3** where the cluster has already been configured (or partially configured), and there is the need to save and reuse the existing configuration files.

Skip this step when installing for the first time.



### WARNING

The Operating System will be installed from scratch, erasing all disk contents in the process.

It is the customer's responsibility to save data and their software environment, before using the procedure described in this chapter. For example, the `/etc/passwd`, `/etc/shadow` files, `/root/.ssh` directory and the **home** directory of the users must be saved.



**Important** All the data must be saved onto a non-formattable media outside of the cluster. It is recommended to use the `tar` or `cp -a` command, which maintains file permissions.

### 3.0.1 Save the ClusterDB

1. Login as the root user on the Management Node.
2. Enter:

```
su - postgres
```

3. Enter the following commands:

```
cd /var/lib/pgsql/backups
pg_dump -Fc -C -f /var/lib/pgsql/backups/<name_of_clusterdball.sav> clusterdb
pg_dump -Fc -a -f /var/lib/pgsql/backups/<name_of_clusterdbdata.sav> clusterdb
```

For example, `<name_of_clusterdbdata.sav>` might be `clusterdbdata-2006-1105.sav`.

4. Copy the two `.sav` files onto a non-formattable media outside of the cluster.

### 3.0.2 Save SSH Keys of the Nodes and of root User

To avoid RSA identification changes, the **SSH** keys must be kept.

- To keep the node SSH keys, save the `/etc/ssh` directory for each node type (Management Node, Compute Node, Login Node, etc.), assuming that the SSH keys are identical for all nodes of the same type.
- To keep the root user SSH keys, save the `/root/.ssh` directory on the Management Node, assuming that its content is identical on all nodes.

These directories must be restored once the installation has finished (see 3.5.1 *Configure SSH*).

### 3.0.3 Save the Storage Configuration Information

The following configuration files, in the `/etc/storageadmin` directory of the Management Node, are used by the storage management tools. It is strongly recommended that these files are saved onto a non-formattable media, as they are not saved automatically for a re-installation.

- `storframework.conf` configured for traces, etc.
- `stornode.conf` configured for traces, etc.
- `nec_admin.conf` configured for **FDA** and **Optima1500** disk array administration access
- `ddn_admin.conf` configured for **DDN** disk array administration access
- `xyr_admin.conf` configured for **Optima1250** disk array administration access
- `dgc_admin.conf` configured for **EMC/Clariion (DGC)** disk array administration access

Also save the storage configuration models (if any) used to configure the disk arrays. Their location will have been defined by the user.

### 3.0.4 Save the Lustre File Systems

The following files are used by the Lustre system administration framework. It is strongly recommended that these files are saved onto a non-formattable media (from the Management Node):

- Configuration files: `/etc/lustre` directory
- File system configuration models (user defined location; by default `/etc/lustre/models`)
- **LDAP** directory if the High-Availability capability is enabled: `/var/lib/ldap/lustre` directory.

### 3.0.5 Save the SLURM Configuration

The `/etc/slurm/slurm.conf` file is used by the **SLURM** resource manager. It is strongly recommended that this file is saved from the Management Node onto a non-formattable media.

### 3.0.6 Save the KSIS Images

As a precaution, save the **KSIS** images of the **bullx cluster suite XR 5v3.1U3** Reference Nodes previously deployed.

## 3.1 STEP 1: Install Red Hat Enterprise Linux Software on the Management Node

This step describes how to install the Red Hat Enterprise Linux software on the Management Node(s). It includes the following sub-tasks:

- 1) Optional - RAID configuration
- 2) Installation of the Red Hat Enterprise Linux 5 Server software
- 3) First boot settings
- 4) Configuring the Network
- 5) Installing an external Storage System (small clusters only)

### 3.1.1 Optional - Configure Internal RAID discs for bullx cluster suite clusters

**Note** This step is not necessary if you are carrying out a re-installation of **bullx cluster suite** as the existing RAID configuration remains in place.

#### 3.1.1.1 Configure RAID for AOC-USAS-S8iR-LP Adapters

This kind of adapter is installed on **R423** and **R425** machines only. Each machine has to be configured individually.

### 3.1.2 Red Hat Enterprise Linux 5 Installation

#### 3.1.2.1 Initial Steps



**Important** Before starting the installation read all the procedures carefully

Start with the following operations:

1. Power up the machine.
2. Switch on the monitor.
3. Insert the **RHEL 5.3 for EM64T DVD** into the slot-loading drive.

**Note** The media must be inserted during the initial phases of the internal tests (while the screen is displaying either the logo or the diagnostic messages); otherwise the system may not detect the device.

4. At the next screen, scroll down to the boot prompt and enter the following text.

```
linux driverload=igb
```

Press the **enter** key.

**Note** The **Red Hat** installation program allows commands to be entered from a shell prompt and displays different diagnostic messages on five *virtual consoles*. The table below displays the different types of consoles available and the keystrokes used to switch between them. Generally, there is no reason to leave the X graphical default console (virtual console 7 below) unless you are attempting to diagnose an installation problem.

Console	Contents	Switching Keystrokes
1	Installation dialog	[Ctrl]-[Alt]-[F1]
2	Shell prompt	[Ctrl]-[Alt]-[F2]
3	Install log (messages from installation program)	[Ctrl]-[Alt]-[F3]
4	System-related messages	[Ctrl]-[Alt]-[F4]
5	Other messages	[Ctrl]-[Alt]-[F5]
7	X graphical display	[Ctrl]-[Alt]-[F7]

Table 3-2. Red Hat Consoles and Switching Key Strokes

### 3.1.3 Red Hat Linux Management Node Installation Procedure

A suite of screens helps you to install the **RHEL5** software on the Service Node that includes the Management Node Services.



Figure 3-1. The Welcome Screen

1. The Welcome screen will appear at the beginning of the installation process.



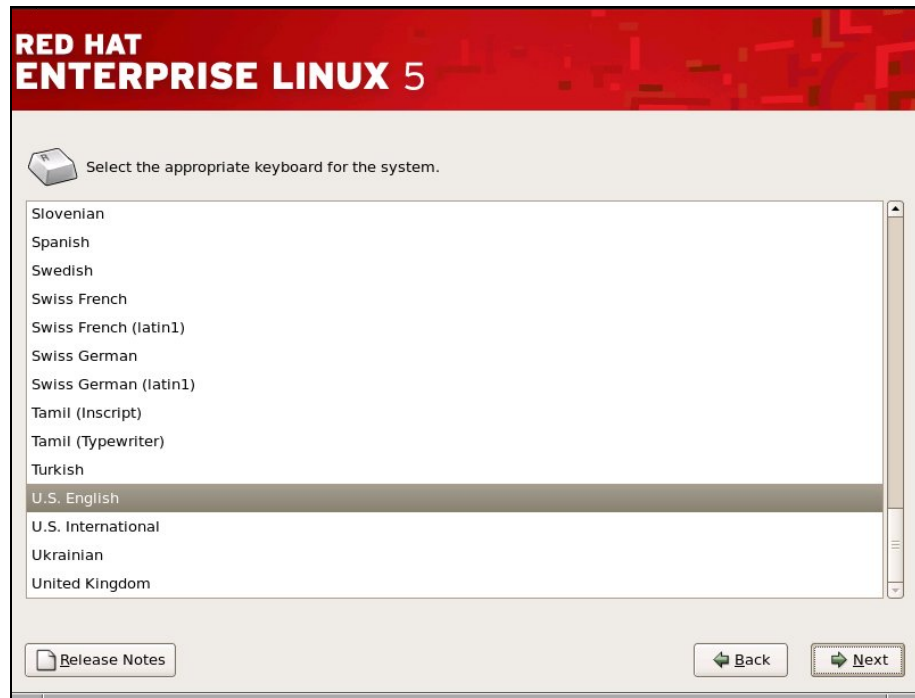


Figure 3-2. Keyboard installation screen

2. Select the language to be used for installation. Click the **Next** button. Select the keyboard that is used for your system. Click the **Next** button.

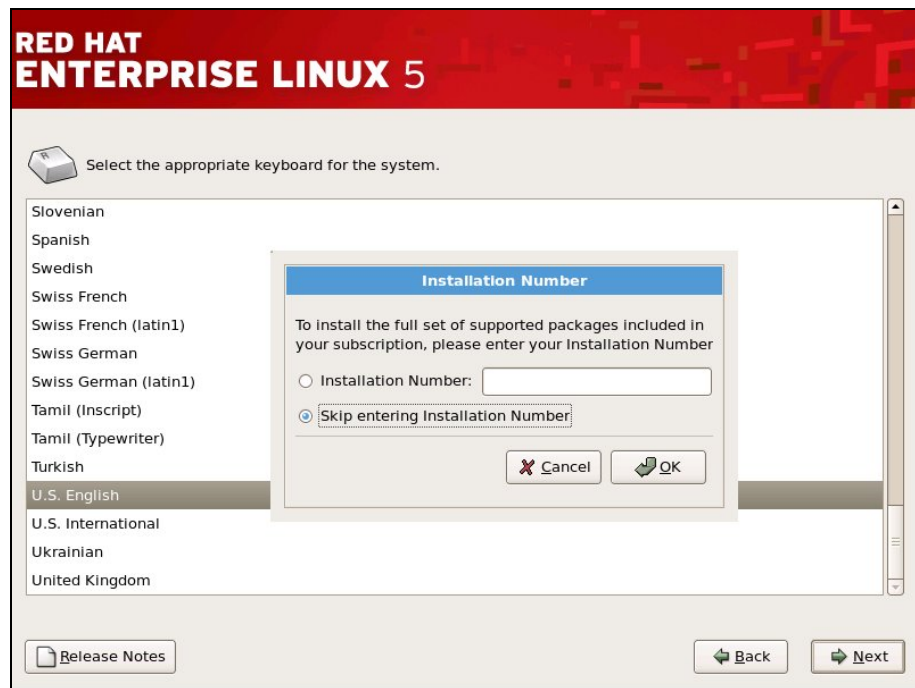


Figure 3-3. RHEL5 installation number dialog box

3. The **bullx cluster suite** installation procedure requires that the **Red Hat** Installation Number is NOT entered now. The Installation Number can be entered later so that you can benefit from the **Red Hat** support network. Select **Skip entering Installation Number**.

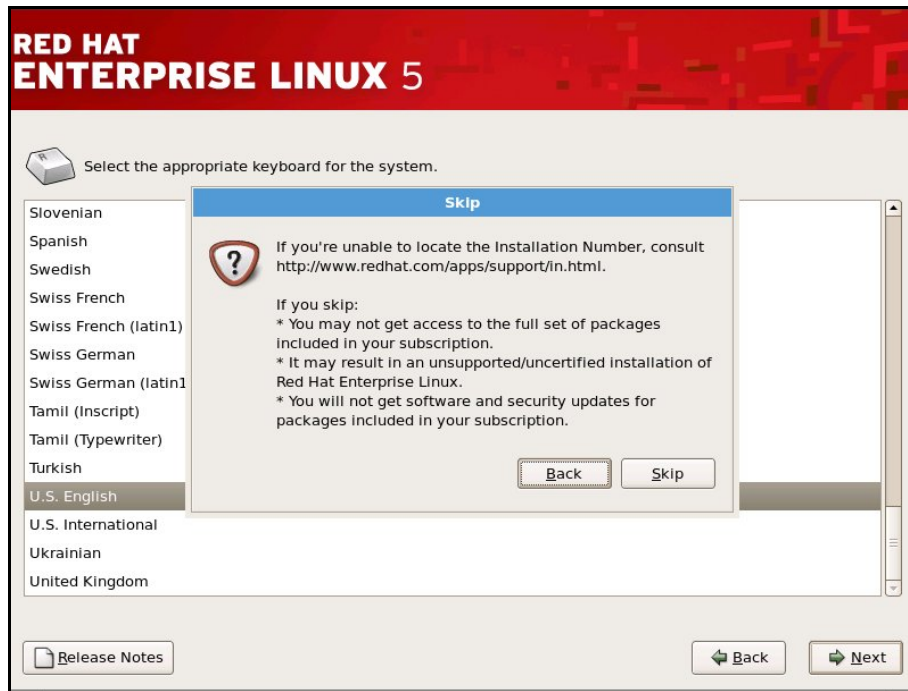



Figure 3-4. Skip screen for the installation number

4. Click **Skip**, as shown in Figure 3.4. Click **Next**.

---

 **Important** See *Appendix G- Activating your Red Hat account* - for important information regarding the use of installation numbers.

---



Figure 3-5. First RHEL5 installation screen

5. Select the option **Install Red Hat Enterprise Linux Server** as shown in Figure 3-5.

## 3.1.4 Disk partitioning

There are different disk partitioning options available according to whether you are installing for the first time and using the default partitioning provided by LVM, or are carrying out a reinstallation and wish to use the partitioning that already exists.

### 3.1.4.1 Default partitioning



Figure 3-6. Partitioning screen

The default disk partitioning screen will appear as shown above. Usually, all the default options can be left as shown above, as the partitioning will be handled automatically by Logical Volume Manager (**LVM**). Click **Next**.

---

**Note** If there is more than one disk for the Management Node, they will all appear checked in the drive list in Figure 3-6 and will all be reformatted and have the Red Hat software installed on them. Deselect those disks where you wish to preserve the existing data.

---



Figure 3-7. Confirmation of the removal of any existing partitions

Select **Yes** to confirm the removal of any existing partitions as shown in Figure 3-7, if this screen appears.

If the default partitioning is to be left in place, go to section 3.1.5 *Network access Configuration*.

### 3.1.4.2 Reinstallation using the existing partitioning layout

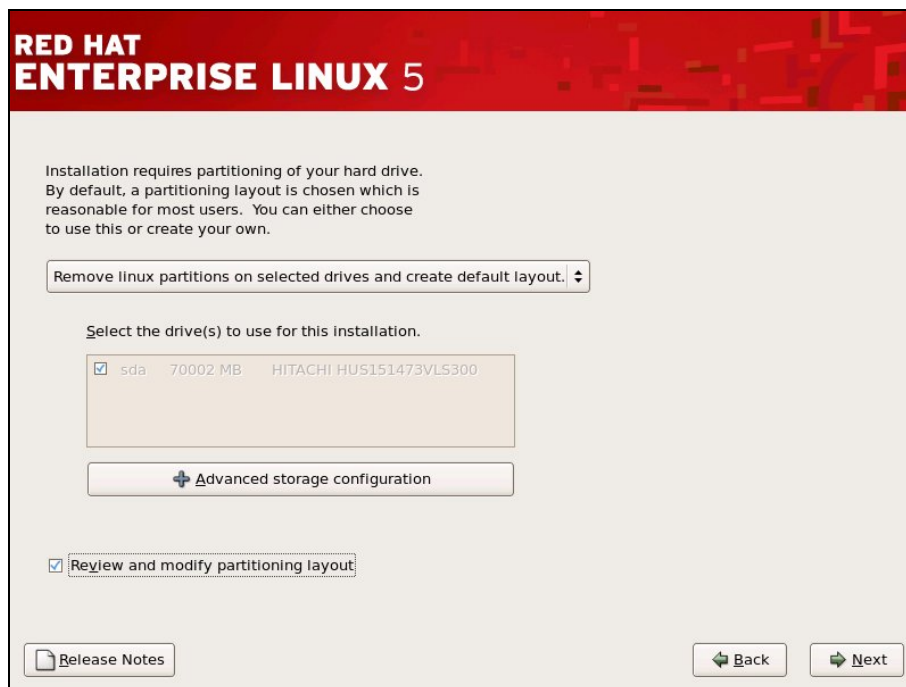


Figure 3-8. Modifying the partitioning layout – 1st screen

- a. Tick the **Review and modify partitioning layout** box, as shown above.

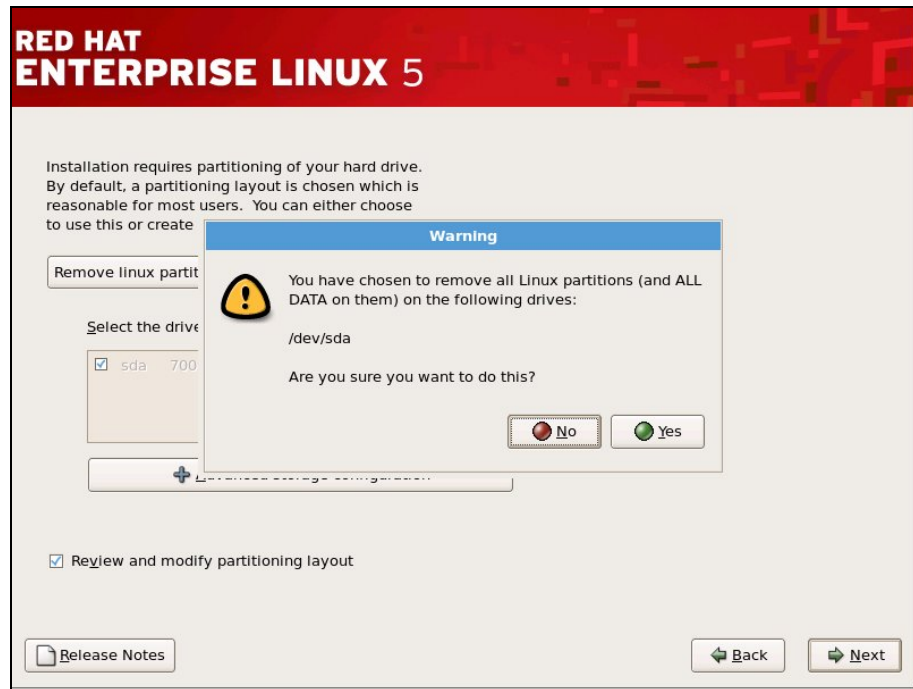


Figure 3-9. Confirmation to remove existing partitions

- b. Click **Yes**, above, to confirm the removal of all existing Linux partitions.

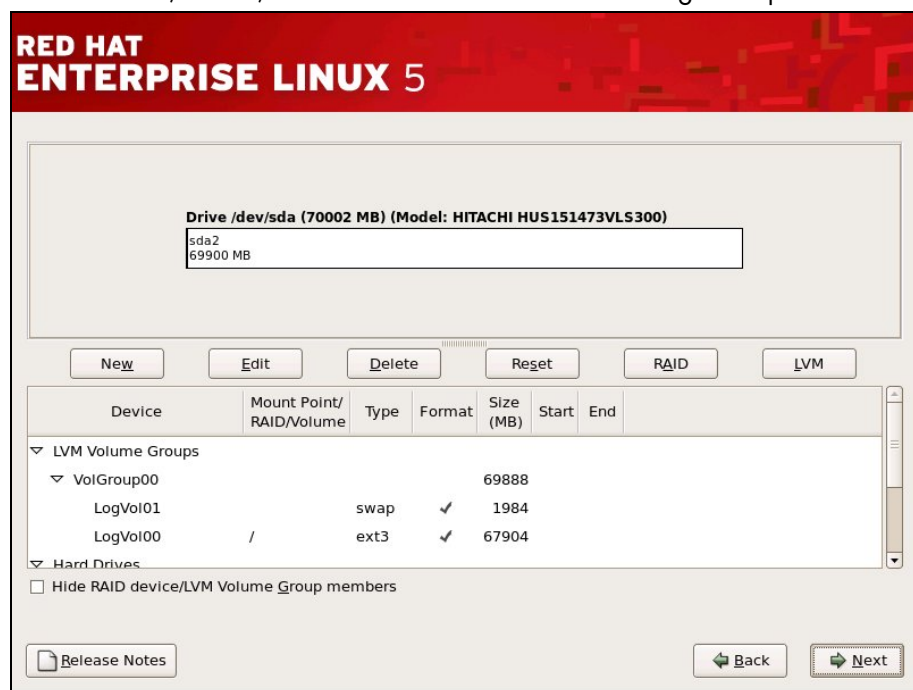


Figure 3-10. RHEL5 Partitioning options screen

- c. If you wish to keep the partitioning options as they were previously, click **Reset** in the screen above, as shown in Figure 3-10, and confirm the settings, including the mount point, that appear.



Figure 3-11. Confirmation of previous partitioning settings

### 3.1.5 Network access Configuration

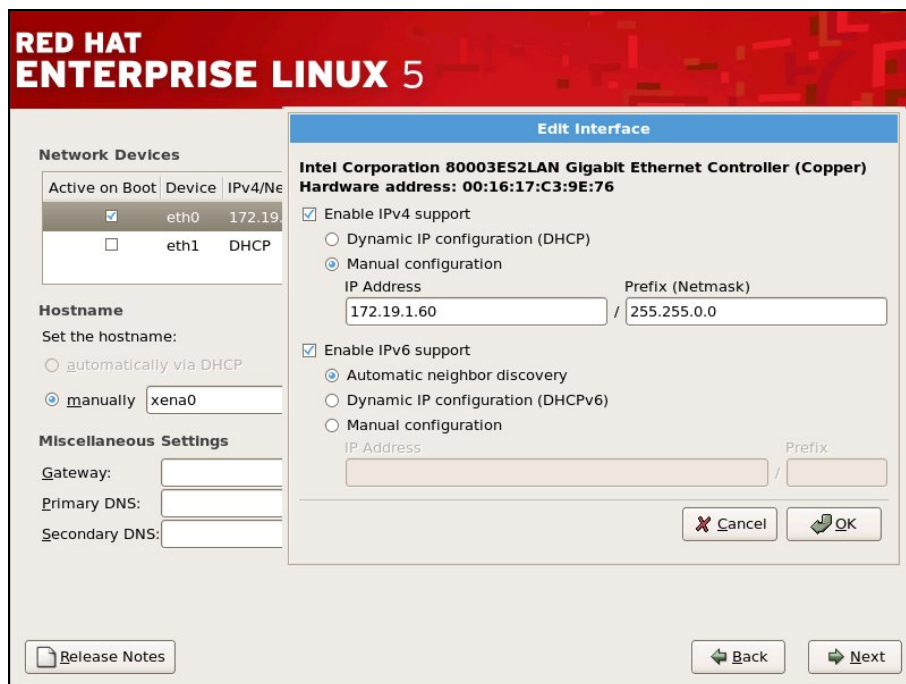


Figure 3-12. Network Configuration Screen

6. The next step to configure network access for the Management Node. Select **manually** and enter the hostname (this is shown as xena0 in the example above). Select the device connected to the cluster management network (normally this is eth0) and click the **Edit** button. Enter the IP address and NetMask configuration settings– see Figure 3-12.

If necessary, the miscellaneous settings for the Gateway, Primary DNS and Secondary DNS can be configured. Warning messages may appear if this is not done and can be ignored.

Click the **OK** and **Next** buttons in Figure 3-12 when all the network configurations have been set.

---

**Note** The host name in the screen grab must be replaced by the name of the Management Node. The IP addresses in the screen above are examples and will vary according to the cluster.

---

### 3.1.6 Time Zone Selection and Root Password



Figure 3-13. Time Zone selection screen.

7. Select the Time Zone settings required, as shown in Figure 3-13, and click Next.

---

**Note** Bull recommends using UTC, check the **System clock uses UTC** box to do this.

---



Figure 3-14. Root Password Screen

8. Set the Root password as shown in Figure 3-14. This must use a minimum of 6 characters.

### 3.1.7 Red Hat Enterprise Linux 5 Package Installation



Figure 3-15. Software selection screen

9. Leave the screen with the additional tasks deselected, as shown in Figure 3-15. Click **Next**.





Figure 3-16. Installation screen

10. Click **Next** in Figure 3-16 to begin the installation of **Red Hat Enterprise Linux Server**.
11. When the **Congratulations the installation is complete** screen appears carry out the procedure below to avoid problems later (There may be problems with the graphic display: the bottom part of the screen does not appear on some machines).
  - a. Hold down the **Ctrl Alt F2** keys to go to the shell prompt for console 2.
  - b. Save the **xorg.conf** file by using the commands below:

```
cd /mnt/sysimage/etc/X11
cp -p xorg.conf xorg.conf.orig
```

- c. Edit the **xorg.conf** file by using the command below:

```
vi /mnt/sysimage/etc/X11/xorg.conf
```

- d. Go to the Screen section, subsection Display and after the Depth 24 line add the following line.

```
-----
                Modes      "1024x768"  "832x624"
-----
```

- e. Save the file and exit vi.
- f. Confirm that the modifications have been registered by running the command:

```
diff xorg.conf.orig xorg.conf
```

This will give output similar to that below:

```
27a28
>                Modes      "1024x768"  "832x624"
-----
```

- g. Check the screen appearance is OK by holding down the **Ctrl Alt F6** keys.
- h. Click the **Reboot** button.

---

**Note** The screen resolution can be changed if there are any display problems by holding down **Ctrl Alt -** or **Ctrl Alt +** on the keyboard.

---

### 3.1.8 First boot settings

1. After the system has rebooted the Administrator must configure the list of post boot settings which appear. In particular the follow settings **MUST** be made:
  - Disable the firewall
  - Disable SELinux
  - Enable Kdump and select 128 MBs of memory for the kernel dump
2. The time and date must be set.
3. Select **Register later** for the software update.
4. The option **Create the Linux user** appears and can be set if required.
5. Ignore the No sound card screen which appears.
6. Ignore the Additional CDs screen
7. Click **Finish**.
8. Click **Reboot**.

### 3.1.9 Network Configurations

---

**Note** The IP addresses used will depend on the address plan for the system. Those used in this section are examples.

---

To configure the network use the **system-config-network** command, as below, this will launch the graphical tool used for the configuration.

```
system-config-network
```

#### 3.1.9.1 Administration Network Configuration

---

**Note** The section only applies for those devices which have not been configured earlier, or if you wish to change an existing address.

---


Configure other network interfaces, e.g. **eth1**, **eth2** if required.

##### Example

1. In the **Devices** panel select device eth1.
2. Click **Edit**.
3. Select **Activate device** when computer starts.
4. Select **Statically set IP addresses** and set the following values, according to your cluster type:

IP ADDRESS	XXX.YYY.0.1
SUBNETMASK	255.255.0.0
DEFAULT GATEWAY	none

---

 **Important** The address settings used for the IP addresses must match the addresses declared in the Management Database (ClusterDB). If these are not known please contact Bull technical support. The IP addresses given in this section are examples and are for information only.

---

**Note** `bullx cluster suite` clusters do not support VLAN.

---

### 3.1.9.2 Alias Creation on eth0 (Management Node)

---

 **Important** Skip this section for clusters with Management Node High Availability.

---

Aliases provide hardware independent IP addresses for cluster management purposes. The alias created below is used by the administration software.

1. Go to the `/etc/sysconfig/network-scripts/` directory.
2. Copy the `ifcfg-eth0` file to the `ifcfg-eth0:0` file.
3. Edit the `ifcfg-eth0:0` file and modify the **DEVICE** setting so that it reads `eth0:0` as shown.  
`DEVICE=eth0:0`
4. Modify **IPADDR** with the alias IP address.

### 3.1.9.3 Restarting the network service

Run the command:

```
service network restart
```

### 3.1.10 External Storage System Installation

The Management Node may be connected to an external storage system, when the I/O and Login functions are included in the same Service Node as the Management functions.

**See** Chapter 4 *Configuring Storage Management Services*, in this manual, for more information regarding the installation, and also refer to the documentation provided with the storage system for details on how to install the storage system.

---

### 3.1.11 Disk Health Monitoring Configuration

By default the `/etc/smartd.conf` file is recreated automatically each time the system boots and contains a line for each disk device detected on the system. Some of the disk devices may correspond to **RAID** volumes or remote LUNs on storage sub-systems. Smart monitoring is not supported for these devices and the lines, which correspond to them plus the first line, below, must be deleted from the `/etc/smartd.conf` file.

```
#DEVICESCAN -H -m root
```

---

## 3.2 STEP 2: Install bullx cluster suite software on the Management Node

This step describes how to copy and install the **bullx cluster suite XR 5v3.1U3** software on the Management Node(s). It includes the following sub-tasks:

1. Preparation for the installation of **bullx cluster suite XR SN** distribution on the other cluster nodes.
2. Optional - Preparation for the installation of **bullx cluster suite XR CN** distribution on the Compute Nodes (Cluster Type 2 - see Table 3-1).
3. Installation of **bullx cluster suite XR SN** software on the Management Node.
4. Configuration of the Cluster Database.

### 3.2.1 DVD Mount Point

Before the `/media/cdrecorder/` mount point for the **RHEL 5.3 for EM64T, RHEL5.3-Supplementary** and **bullx cluster suite** media can be recognised, the following line will need to be added to the `/etc/fstab` file:

```
-----  
/dev/cdrom /media/cdrecorder iso9660 user,exec,noauto 0 0  
-----
```

Create a mount point for the media by running the command below:

```
mkdir -p /media/cdrecorder/
```

During the installation procedure for **Red Hat Enterprise Linux Server 5** some software packages are loaded that are specifically required for **bullx cluster suite** clusters. The following sections describe the installation of these packages along with the Bull **XHPC**, and optional **InfiniBand**, **XLustre** and **XToolkit** software.

### 3.2.2 Prepare the Installation of the software on the Cluster Nodes

#### 3.2.2.1 Red Hat Enterprise Linux 5.3 for EM64T

1. Create the directory for the software:

```
mkdir -p /release/RHEL5.3
```

2. Insert the **RHEL5.3 for EM64T** media into the reader and mount it:

```
mount /dev/cdrom /media/cdrecorder/
```

3. Copy the **RHEL5.3 for EM64T** files to the `/release/RHEL5.3` directory:

```
cp -a /media/cdrecorder/* /media/cdrecorder/.discinfo /release/RHEL5.3
```

---

**Note** This step will take approximately 7 minutes.

---

4. Eject the DVD:

```
umount /dev/cdrom
```

or use the eject command:

```
eject
```

### 3.2.2.2 RHEL5.3 for EM64T Supplementary media

If the RHEL5.3 for EM64T Supplementary media is part of your delivery:

1. Create the directory for the software:

```
mkdir -p /release/RHEL5.3-Supplementary/
```

2. Insert the RHEL5.3 for EM64T Supplementary media into the reader and mount it:

```
mount /dev/cdrom /media/cdrecorder/
```

3. Copy the RHEL5.3 for EM64T Supplementary files into the /release/RHEL5.3-Supplementary directory:

```
cp -a /media/cdrecorder/* /media/cdrecorder/.discinfo /release/RHEL5.3-Supplementary/
```

4. Eject the media:

```
umount /dev/cdrom
```

or use the eject command:

```
eject
```

### 3.2.2.3 bullx cluster suite XR CN (Cluster Type 2 - see Table 3.1)

If the bullx cluster suite XR CN distribution is to be installed on your Compute Nodes then carry out the following actions, if not skip this step.

1. Create the directory for the software:

```
mkdir -p /release/bullxLinux5.3/
```

2. Insert the bullx cluster suite XR CN-OS Linux 5.3 for EM64T media into the reader and mount it:

```
mount /dev/cdrom /media/cdrecorder/
```

3. Copy the bullx cluster suite XR CN-OS Linux 5.3 for EM64T files into the /release/bullxLinux5.3/ directory:

```
cp -a /media/cdrecorder/* /media/cdrecorder/.discinfo /release/bullxLinux5.3/
```

4. Eject the media:

```
umount /dev/cdrom
```

or use the eject command:

```
eject
```

### 3.2.3 Run the `installvdv` script to copy bullx cluster suite software onto the Management Node

The `installvdv` script is used to copy across the rest of **bullx cluster suite XR 5v3.1U3** software to the `/release` directory on the Management Node.

**Note** The media to be installed depends on the cluster type and the software options purchased.

#### Software copied by `installvdv`

The following software is copied onto the Management Node by the `installvdv` script:

1. **BAS5 for Xeon V3.1 - XHPC** - Mandatory installation for all clusters.
2. **bullx cluster suite XR 5v3.1U3** - Mandatory installation for all clusters.
3. **bullx cluster suite XR SN-OS Errata3 for Red Hat Enterprise Linux 5.3 (EM64T)** - Mandatory installation for all clusters.
4. **BAS5 for Xeon V3.1 - XIB InfiniBand** - Optional, according to cluster.
5. **BAS5 for Xeon V3.1 - XLustre** - Optional, according to cluster.
6. **bullx cluster suite XR CN-OS Errata3 for Linux 5.3 (EM64T)** - Must be installed if the **bullx CS XR CN-OS Linux 5.3 for EM64T** media (see section 3.2.2.3) has been installed.

**See** The *Software Release Bulletin* for more information on the installation media included with your delivery.

#### Using the `installvdv` script to copy the media onto the Management Node

- a. Insert the **BAS5 for Xeon V3.1 XHPC** media.

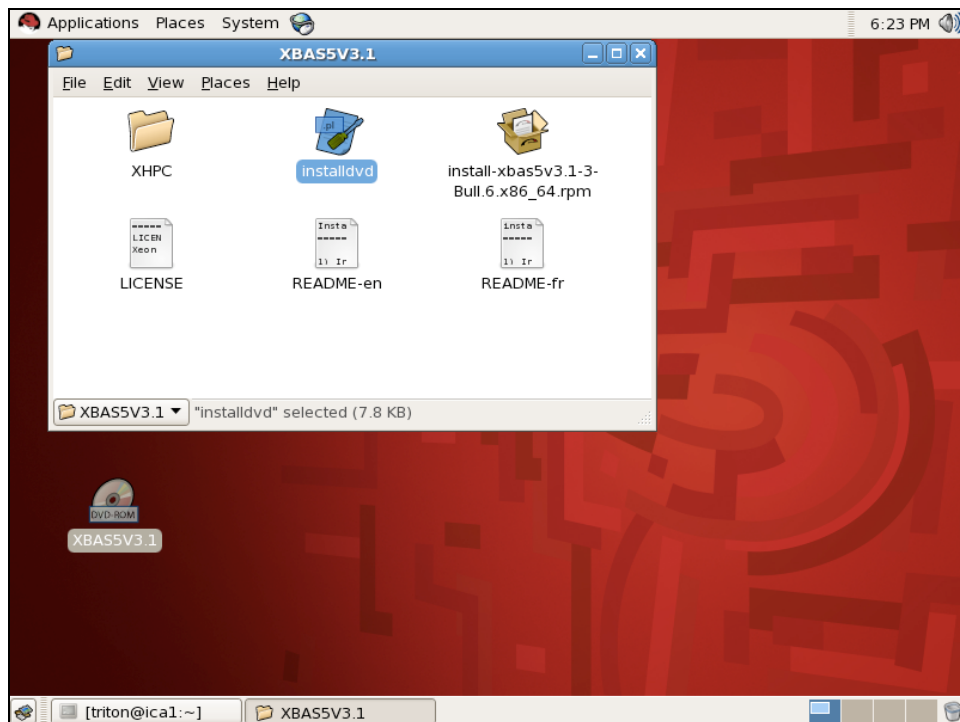


Figure 3-17. First Install Window

- b. Double-click on the `install dvd` script as shown in Figure 3-17.

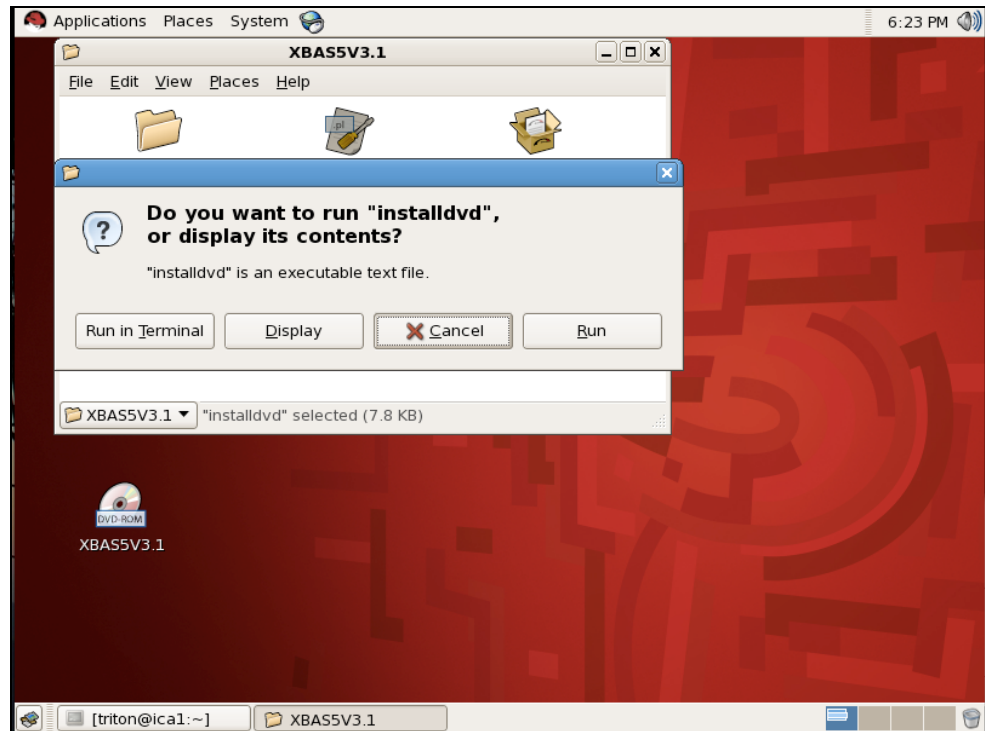



Figure 3-18. `install dvd` script run options

- c. Select **Run in Terminal** from the run options displayed in Figure 3-18.
- d. Repeat steps 1. to 3. for the additional media to be installed.

### 3.2.4 Install the bullx cluster suite software

 **Important** The mandatory RHEL packages and general bullx cluster suite products will be installed automatically by default.

Go to the `/release/XBAS5V3.1` directory:

```
cd /release/XBAS5V3.1
```

The software installation commands for the Management Node correspond to the Function/Product combination applicable to the Service Node, which includes the Management Node.

**See** *Chapter 1* for a description of the different architectures and functions possible.

The **bullx cluster suite** install command syntax is shown below.

```
./install -func MNGT [IO] [LOGIN] [-prod [XIB] [XLUSTRE] [XTOOLKIT]]
```

The `-func` option is used to specify the node function(s) to be installed and can be a combination of the following:

- **MNGT** which includes installation, configuration, general administration and the monitoring of all the hardware in the cluster.

- **LOGIN** which provides access to the cluster and its specific software development environment.
- **IO** for IO functions.

Different combinations of products can be installed using the **-prod** flag. The **-prod** options include the following:

- **XIB** to install the software for the **InfiniBand** interconnects.
- **XLUSTRE** to install the software for the **Lustre** parallel file system.
- **XTOOLKIT** to install the HPC Toolkit software.

---

**See**

- The *InfiniBand Guide* and the *System Release Bulletin* for more details regarding the **InfiniBand** RPMs and tools.
  - The **bullx cluster suite** *Application Tuning Guide* for details on configuring and using HPC Toolkit.
- 

---

**Note**

If Intel<sup>®</sup> VTune Performance Analyzer for Linux is to be installed on the cluster, the HPC Toolkit (XTOOLKIT) product must be installed.

---

For example, use the command below to install the **MNGT** and **LOGIN** functions with the **InfiniBand**, **Lustre** and **HPC Toolkit** products:

```
./install -func MNGT LOGIN -prod XIB XLUSTRE XTOOLKIT
```



**Important** See the *Software Release Bulletin* for details of any **BONUS** RPMS to be installed manually on the Management Node.

---

Please note that the installation process will take a while (approximately 5 minutes).

---

Check that the installation is OK by:

- Looking at the last line in the `/root/xbas5_installation.log` file, this has to have the following format:

```
==== - ===== ending installation script - <date_and_time_of_your_installation>
```

**Example**

```
==== - ===== ending installation script - 2010/04/08 11:58:11
```

- Looking at the differential for the log files (before and after the installation). An example of the **sdiff** command, used to produce the differential, is shown below:

```
sdiff -s list-01before-instal-XBAS5V3.1-<date_and_time_before>
list-02after-instal-XBAS5V3.1-<date_and_time_after> | more
```



## 3.2.5 Database Configuration

Please go to the section, below, that corresponds to your installation and follow the instructions carefully:

- *First Installation - Initialize the Cluster Database*
- *Re-installation of bullx cluster suite XR 5v3.1 U3 with ClusterDB Preservation*

### 3.2.5.1 First Installation - Initialize the Cluster Database

**Note** This paragraph applies only when performing the first installation of **bullx cluster suite XR 5v3.1U3** and the cluster has been delivered with no Cluster DB preloaded by Bull. Contact Bull Technical Support to obtain the Cluster DB preload file.

1. Run the following commands (the IP addresses and Netmasks below have to be modified according to your system):

```
su - postgres
cd /usr/lib/clustmngt/clusterdb/install
loadClusterdb --basename <clustername> --adnw xxx.xxx.0.0/255.255.0.0
--bknw xxx.xxx.0.0/255.255.0.0 --bkgw <ip_gateway> --bkdom
<domain_name>
--icnw xxx.xxx.0.0./255.255.0.0
--preload <load_file>
```

Where:

**basename** (mandatory) designates both the node base name, the cluster name and the virtual node name

**adnw** (mandatory) is administrative network

**bknw** (option) is backbone network

**bkgw** (option) is backbone gateway

**bkdom** (option) is backbone domain

**icnw** (option) is ip over interconnect network

**Note** See the **loadClusterdb** man page and the preload file for details of the options that apply to your system.

Preload sample files are available in:

**/usr/lib/clustmngt/clusterdb/install/preload\_xxxx.sql**  
(xxxx in the path above corresponds to your cluster).

2. Save the complete database or save the database data
  - a. Save the complete database using the command:

```
pg_dump -Fc -C -f /var/lib/pgsql/backups/clusterdball.dmp clusterdb
```

- b. Save the database data using the command:

```
pg_dump -Fc -a -f /var/lib/pgsql/backups/clusterdbata.dmp clusterdb
```

### 3.2.5.2 Re-installation of bullx cluster suite XR 5v3.1 U3 with ClusterDB Preservation

---

**Note** This paragraph applies when re-installing an existing version of **bullx cluster suite XR 5v3.1 U3** with the restoration of the existing Cluster Database.

---

1. Run the commands:

```
su - postgres
psql -U clusterdb clusterdb

<Enter Password>
clusterdb=> truncate config_candidate;truncate config_status;\q
TRUNCATE TABLE
TRUNCATE TABLE
```

2. Restore the Cluster DB files which have been stored under `/var/lib/pgsql/backups`:

```
pg_restore -Fc --disable-triggers -d clusterdb
/var/lib/pgsql/backups/clusterdbata.dmp
```

**See** Section 3.0.1 *Save the ClusterDB* for details of the Cluster database files that have been saved. See the *bullx cluster suite Administrator's Guide* for more details about restoring data.

---

3. Go back to root by running the **exit** command.

## 3.3 STEP 3: Configure Equipment and Install Utilities on the Management Node

This step describes how to:

- Generate the SSH keys
- Configure Ethernet switches
- Update the MAC addresses in the Cluster Database
- Configure the Bull Cool Cabinet Doors, Blade Servers, Nodes
- Install and configure **postfix**, **ganglia**, **syslog-ng**, **NTP**, **kdump**, **SLURM** and **PBS Pro**
- Install compilers (only on Management Nodes which include Login functionality)
- Configure the **MPI** user environment

### 3.3.1 Generate the SSH keys

1. Go to the root directory:

```
cd /root
```

2. Enter the following commands:

```
ssh-keygen -t rsa
```

Accept the default choices and do not enter a password.

```
cat .ssh/id_rsa.pub >> .ssh/authorized_keys
```

3. Test the configuration:

```
ssh localhost uname
```

```
-----  
The authenticity of host 'localhost (127.0.0.1)' can't be established.  
RSA key fingerprint is  
91:7e:8b:84:18:9c:93:92:42:32:4a:d2:f9:38:e9:fc.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added 'localhost,127.0.0.1' (RSA) to the list of  
known hosts.  
Linux
```

Then enter:

```
ssh <clustername>0 uname
```

```
Linux
```

### 3.3.2 Configure the Ethernet Switches



**Important**

Only carry out this task during the first installation, or if new Ethernet switches have been added to the cluster. The Ethernet switches should be as initially set (factory settings).

Install Ethernet switches by running the command below, as root:

```
# swtAdmin auto
```

See Chapter 8 - *Configuring Switches and Cards* in this manual for more details.

### 3.3.3 Update the MAC Addresses in the Cluster Database



**Important** Only carry out this task during the very first installation. If you have saved your Cluster Database from a previous installation, go to the section *Configure the Management Tools with the Database Information*, on page 3-31.

This section describes how to collect hardware component MAC Addresses and to store them in the Cluster Database. Once this is done an administration IP address is configured for each hardware component; as an alternative the DHCP server can provide an administration IP address for hardware components that are dynamically configurable.

#### 3.3.3.1 Starting from the MAC Address Files Provided by Manufacturing

Look for the **MAC** address files in the `/usr/lib/clustmngt/clusterdb/install/` directory. These files will have been provided by manufacturing and are named `Type_Rack+Xan_Rack.final`. For each of these files you have to:

- Identify its corresponding rack label
  - Update the MAC addresses in the Cluster Database
  - Configure the BMC IP addresses.
1. Identify the corresponding **rack\_label** from ClusterDB **rack** table.  
For example `<Type_Rack+Xan.final>` might be `SNRXA2.final`, where **Type\_Rack** is **SNR**, 'a' (the **x\_coord** of rack) is **A** and 'n' (the **y\_coord** of rack) is **2**. Run the command below as the **postgres** user in order to retrieve the **rack\_label**:

```
$ psql -c "select label from rack where x_coord='A' and y_coord='2'"  
clusterdb label
```

```
RACK1  
(1 row)
```

2. Update the database with the rack **MAC** addresses for the node and hardware manager by running the command below as the **postgres** user:

```
$ /usr/lib/clustmngt/clusterdb/install/updateMacAdmin  
<Type_Rack+Xan.final> --rack <rack label>
```

Example:

```
$ /usr/lib/clustmngt/clusterdb/install/updateMacAdmin SNRXA2.final  
--rack RACK1
```

3. Configure the IP addresses for the rack **BMCs** by running the command below as the root user:

```
# /usr/lib/clustmngt/BMC/bmcConfig --input <Type_Rack+Xan.final>
```

Example:

```
# /usr/lib/clustmngt/BMC/bmcConfig --input SNRXA2.final
```

### 3.3.3.2 Update the Cluster Database with the MAC Addresses

The **equipmentRecord** command updates the cluster database dynamically with the MAC addresses of various types of hardware equipment: Bull Cool Cabinet Door, Blade Server (Chassis and inherent Nodes), Nodes and their Hardware Managers. This command also collects the **MAC** addresses from the Ethernet switches; these must be configured and connected to the target equipment both electrically and by Ethernet.

Options exist to support blade chassis and to address the **CMCs** (Chassis Management Controllers)


### 3.3.3.3 Using the equipmentRecord command with Cool Cabinet Doors

---

**See** The Bull *Cool Cabinet Door* documentation, listed in the *Bibliography* in the *Preface*, for more information.

---

---

 **Important** All the Cool Cabinet Doors that are included in the cluster must be configured separately, before the machines in the cabinets are started and configured.

---

#### Prerequisites

- Auto-Configuration for the IP address for the Cool Cabinet Door should be set to **DHCP** (factory settings).
- The Cluster Database **rack\_port** table should include all the parameters for the **Cool Cabinet Door** - See *Chapter 3* in the *bullx cluster suite Administrator's Guide* for more details.

#### Configuring the Cluster Database

The **equipmentRecord** command is used to update the Cluster Database automatically with the MAC address of the Embedded Management Board (**OPMA**) for the Cool Cabinet Door(s):

```
/usr/sbin/equipmentRecord coolCD
```

While this command is being carried out, a message similar to the one below will appear (non verbose mode):

```
-----  
Cold door RACK0-0_p1 mac address 00:0d:5d:xx:xx:x0 found  
Cold door RACK1-0_p1 mac address 00:0d:5d:xx:xx:x1 found  
UPDATE command [ OK ]  
-----
```

In the example, above, the database has been updated successfully. The log file will contain additional information regarding the Cool Cabinet Door, as shown in the example below.

---

```
Jan 19 11:4:47 2009 1:

Cold door RACK0-0_p1 connected to switch: eswu0c0 (172.17.0.210)
switch vendor: CISCO
switch slot: 0
switch port: 23
cold door mac address: 00:0d:5d:xx:xx:x0
```

---

If one of the Cool Cabinet Doors is unreachable, a message similar to that below will appear (non verbose mode):

---

```
Cold door RACK0-0_p1 mac address not found!
Cold door RACK1-0_p1 mac address 00:0d:5d:xx:xx:x1 found
UPDATE command [ OK ]
```

---


### Power on the Cool Cabinet Doors

---

**See** The *Cool Cabinet Door Console User's Guide* for details about using the GUI Console to power on/off the Cool Cabinet Door.

---

---

 **Important** The Cool Cabinet Door(s) **MUST** be powered on, and the cooling system and the fans running, before the nodes in the cabinet are configured. This is to prevent any risk of overheating when the nodes are powered on.

---

### Start the Cool Cabinet Doors

The `coldoorStart` command is used to start one or more Cool Cabinet Doors.

- To start a door individually use a command, similar to the one below:

```
/usr/sbin/coldoorStart --door RACK0-0_p1
```

While this command is running for the Cool Cabinet Door specified, a message similar to that below will appear:

---

```
RACK0-0_p1 Chassis Power Control: Up/On
Note: Powering on a Cool Cabinet Door takes about 40 seconds to be
effective.
```

---

- To start all the doors in the cluster use a command, similar to the one below:

```
/usr/sbin/coldoorStart --startall
```

While this command is running for the Cool Cabinet Doors listed in the Cluster Database, a message similar to the one below will appear:

---

```
RACK0-0_p1 Chassis Power Control: Up/On
Note: Powering on a Cool Cabinet Door takes about 40 seconds to be
effective.
```

---

The `coldoorStart` log file can be checked for powering on details, as shown in the example below.

```
-----  
Jan 20 18:13:56 2009 coldoorStart: RACK0-0_p1 cooled water door is ON  
-----
```

### 3.3.3.4 Using the `equipmentRecord` command with Blade Servers

The `equipmentRecord` command used with blade servers updates the Cluster Database with the MAC address of the chassis for the blade servers, the nodes, and any corresponding Hardware Manager equipment, e.g. **BMC**. In addition, it configures the IP addresses for the chassis, the nodes and for the Hardware Manager.

```
/usr/sbin/equipmentRecord blades
```

Once the procedure has finished, a message similar to the one below will appear (non verbose mode):

```
-----  
MAC addresses record procedure for Blade Servers DONE  
-----
```

### 3.3.3.5 Using the `equipmentRecord` command with Nodes

The `equipmentRecord` command, used with the `node` type, updates the Cluster Database with the **MAC** address of the nodes and the corresponding Hardware Manager, e.g. **BMC**, and configures the IP addresses for the nodes and the Hardware Manager.

#### Prerequisites

- The nodes whose MAC addresses are to be stored in the Cluster Database should be in **DHCP** auto configuration mode (**PXE** boot).
- The Cluster Database must include all the **Ethernet** connection information (`admin_eth_switch_id`, `admin_eth_switch_slot`, `admin_eth_switch_port`) for target nodes.

#### Procedure

The procedure to record one or more nodes consists of the following steps:

1. Check that any system installation (`ksis`, `nfsinstall`) is not running.
2. Start the node record procedure:

```
# /usr/sbin/equipmentRecord node --action start
```

3. Manually reboot the nodes you want to record.
4. Check that all rebooted nodes have been recorded:

```
# /usr/sbin/equipmentRecord node --action status
```

This step may take several minutes; repeat this command until all rebooted nodes appear in the status report. However, if after 5 minutes, some nodes are still missing, check the error messages in the log file.

5. Stop the record procedure:

```
#/usr/sbin/equipmentRecord node --action stop
```

### 3.3.3.6

## Manually Updating the MAC Addresses in the Cluster Database (if necessary)

If a hardware item has been installed (as an add-on for example), and its MAC address files has not been found, then update the cluster database as follows.

1. Start the **DHCPD** service by running the command:

```
dbmConfig configure --service sysdhcpd
```

2. Configure the new hardware item so that it boots on the network.
3. Reboot the item and collect its MAC address in the `/var/log/messages` file.
4. Create the file that contains the MAC address, IP address and cluster elements. Its format is as follows:

```
<type> <name> <mac address>
  <type> : name of the Database table for the hardware item,
  <name> : hardware item name
  <mac address> MAC address for the hardware item.
```

An example, similar to that below, is available from:

`/usr/lib/clustmngt/clusterdb/install/mac_file.exp`

---

node	valid0	00:04:23:B1:DF:AA
node	valid1	00:04:23:B1:DE:1C
node	valid2	00:04:23:B1:E4:54
node	valid3	00:04:23:B1:DF:EC
hwmanager	hwm0	00:05:21:B1:AF:BB
rack_port	RACK0-0_p1	00:0D:5D:AB:43:70
eth_switch	eswu0c0	00:1C:F9:CE:28:C0

---

5. Run the command:

```
su - postgres
```

6. Run the command:

```
cd /usr/lib/clustmngt/clusterdb/install
```

7. Run the following command to load the MAC addresses for the network interfaces for the administration network:

```
updateMacAdmin <file>
```

`<file>` is the name of the file that has been created previously – see above. The full path must be included so that it can be easily retrieved, for example `updateMacAdmin /root/cluster-mac-address`

8. Go back to root by running the **exit** command.

## 3.3.4 Configure postfix

1. Edit the `/etc/postfix/main.cf` file.
2. Uncomment or create or update the line that contains **myhostname**

```
myhostname = <adminnode>.<mindomain>
```

You must specify a domain name.



Example: myhostname = node0.cluster

3. This step ONLY applies to configurations that use **CRM** (Customer Relationship Management); for these configurations, the Management Node is used as Mail Server, and this requires that Cyrus be configured.

Uncomment the line:

```
mailbox_transport = cyrus
```

4. Start the postfix service:

```
# service postfix start
```

### 3.3.5 Configure the Management Tools with the Database Information

1. Run the following commands and check that there are no errors. These must be corrected before continuing.

```
dbmCluster check --ipaddr  
dbmCluster check --rack
```

2. Configure the tools with the following command, as root:

```
dbmConfig configure --restart --force
```

An output example for this command follows:

```
-----  
Wed Jul 30 09:09:06 2008 NOTICE: Begin synchro for syshosts  
Wed Jul 30 09:09:06 2008 NOTICE: End synchro for syshosts  
Wed Jul 30 09:09:06 2008 NOTICE: Begin synchro for sysdhcpd  
Shutting down dhcpd: [ OK ]  
Starting dhcpd: [ OK ]  
Wed Jul 30 09:09:07 2008 NOTICE: End synchro for sysdhcpd  
Wed Jul 30 09:09:07 2008 NOTICE: Begin synchro for group  
INSERT group ALL [ OK ] (xena[1-18,30-33,140-141])  
INSERT group IO [ OK ] (xena[1-2,11,17-18,140-141])  
INSERT group COMP [ OK ] xena[3-8,14]  
INSERT group META [ OK ] (xena[10,12])  
INSERT group NODES8GB [ OK ] (xena[0-18,30-33,140-141])  
INSERT group ADMIN [ OK ] (xena0)  
Wed Jul 30 09:09:08 2008 NOTICE: End synchro for group  
Wed Jul 30 09:09:08 2008 NOTICE: Begin synchro for pdsh  
Wed Jul 30 09:09:08 2008 NOTICE: End synchro for pdsh  
Wed Jul 30 09:09:08 2008 NOTICE: Begin synchro for conman  
Stopping ConMan: conmand[ OK ]  
Starting ConMan: conmand[ OK ]  
Wed Jul 30 09:09:08 2008 NOTICE: End synchro for conman  
Wed Jul 30 09:09:08 2008 NOTICE: Begin synchro for snmptt  
Wed Jul 30 09:09:08 2008 NOTICE: End synchro for snmptt  
Wed Jul 30 09:09:08 2008 NOTICE: Begin synchro for nagios  
INITIALIZATION of the services  
Running configuration check...done  
Resetting host status in DB, update by Nagios will take a few minutes  
Stopping Bull System Manager nagios ...[ OK ]  
Starting Bull System Manager nagios ...Resetting host status in DB,  
update by Nagios will take a few minutes  
[ OK ]syslog-ng (pid 2998) is running...  
Reloading syslog-ng: [ OK ]  
-----
```

```
-----  
syslog-ng (pid 2998) is running...  
Reloading syslog-ng: [ OK ]  
Wed Jul 30 09:09:10 2008 NOTICE: End synchro for nagios  
Wed Jul 30 09:09:10 2008 NOTICE: Begin synchro for bsm  
  
Wed Jul 30 09:09:10 2008 NOTICE: End synchro for bsm  
-----
```

3. Switch to **postgres**:

```
su - postgres
```

4. Save the complete database or save the database data.

- a. Save the complete database using the command:

```
pg_dump -Fc -C -f /var/lib/pgsql/backups/clusterdball.dmp clusterdb
```

- b. Save the database data using the command:

```
pg_dump -Fc -a -f /var/lib/pgsql/backups/clusterdbata.dmp clusterdb
```

5. Go back to root by running the **exit** command.

6. Reboot the Management Node:

```
exit  
reboot
```

### 3.3.6 Configure ganglia

1. Copy the file:

`/usr/share/doc/ganglia-gmond-3.0.5/templates/gmond.conf` into `/etc`.

2. Edit the `/etc/gmond.conf` file:

- In line 9, replace "deaf = yes" with "deaf = no".
- In line 18, replace xxxxx with the base name of the cluster.  
name = "xxxxx" /\* replace with your cluster name \*/
- In line 24 replace x.x.x.x with the alias IP address of the Management Node.  
host = x.x.x.x /\* replace with your administration node ip  
address \*/

3. Start the **gmond** service:

```
service gmond start  
chkconfig --level 235 gmond on
```

4. Edit the `/etc/gmetad.conf` file:

In Line 39, replace "data\_source "mycluster" localhost" with data\_source "basename" localhost

Example: data\_source "ns" localhost

5. Start **gmetad**:

```
service gmetad start  
chkconfig --level 235 gmetad on
```

## 3.3.7 Configure syslog-ng

### Syslog Ports Usage

**584 / udp** This port is used by cluster nodes to transmit the I/O status information to the Management Node. A non-standard port is used. This value must be consistent with the value defined in the `syslog-ng.conf` file for the cluster nodes and this is ensured by the Bull tools. There is no need for action here.

### Modify the `syslog-ng.conf` file

Modify the `/etc/syslog-ng/syslog-ng.conf` file, as follows, adding the alias IP address (Ethernet `eth0:0` for the administration network) which the server will use for tracking purposes.

1. Search for all the lines which contain the `SUBSTITUTE` string, for example:  
`# Here you HAVE TO SUBSTITUTE ip("127.0.0.1").....`
2. Make the changes as explained in the messages (3 substitutions with the alias IP address).

### Restart `syslog-ng`

After modifying the configuration files, restart the `syslog-ng` service:

```
service syslog-ng restart
```

## 3.3.8 Configure NTP

The Network Time Protocol (NTP) is used to synchronize the computer client time with another server or reference time source. This section does not cover time setting using an external time source, such as a radio or satellite receiver. It covers only time synchronization between the Management Node and other cluster nodes, the Management Node being the reference time source.

---

**Note** It is recommended that the System Administrator synchronizes the Management Node with an external time source.

---

Modify the Management Node `/etc/ntp.conf` file as follows.

1. The first two lines must be marked as comments:

```
#restrict default kod nomodify notrap nopeer noquery  
#restrict -6 default kod nomodify notrap nopeer noquery
```

2. Leave the lines:

```
restrict 127.0.0.1  
restrict -6 ::1
```

3. The next line should have the following syntax, assuming that the parameters used are for a management network with an associated netmask:

```
restrict <mgt_network_IP_address> mask <mgt_network_mask nomodify  
notrap>
```

For example, if the IP address of the Management Node alias is 172.17.0.99:

---

```
restrict 172.17.0.0 mask 255.255.0.0 nomodify notrap
```

---

4. Put the following lines in as comments:

---

```
#server 0.rhel.pool.ntp.org  
#server 1.rhel.pool.ntp.org  
#server 2.rhel.pool.ntp.org
```

---

5. Leave the other lines and parameters unmodified.
6. Start the **ntpd** service:

```
service ntpd restart
```

7. Start **ntpdate** with the IP address as the Management Node alias (x.x.0.99). Example:

```
ntpdate 172.17.0.99
```

---

```
ns0: stratum 11, offset 0.000000, synch distance 0.012515
```

---

### 3.3.9 Configure the **kdump** kernel dump tool

**kdump** will have been enabled during the Red Hat installation on the Management Node

1. The following options must be set in the **/etc/kdump.conf** configuration file:
  - a. The path and the device partition where the dump will be copied should be identified by its **LABEL**, **/dev/sdx** or **UUID** label either in the **/home/** or **/** directories.

Examples:

```
path /var/crash  
ext3 /dev/volgroup00/logvol100
```

- b. The tool used to capture the dump must be configured. Uncomment the **core\_collector** line and add **-d 1**, as shown below:

```
core_collector makedumpfile -c -d 1
```

**-c** indicates the use of compression and **-d 1** indicates the dump level.



#### Important

It is essential to use non-stripped binary code within the kernel. Non-stripped binary code is included in the debuginfo RPM, **kernel-debuginfo-  
<kernel\_release>.rpm**, available from:

<http://people.redhat.com/duffy/debuginfo/index-js.html>

This package will install the kernel binary in the

**/usr/lib/debug/lib/modules/<kernel\_version>/** folder.

---

**Note** The size for the dump device must be larger than the memory size if no compression is used.

---

2. Add the "**acpi=off nomsi nolapic noapic**" options to the **KDUMP\_COMMANDLINE\_APPEND** parameter in the **/etc/sysconfig/kdump** configuration file, so that the parameter appears as below:

```
KDUMP_COMMANDLINE_APPEND="irqpoll maxcpus=1 reset_devices acpi=off  
nomsi nolapic noapic"
```

3. Use the command below to launch **kdump** automatically when the system restarts:

```
chkconfig kdump on
```

### 3.3.10 Optional - Install and Configure LDAP

**See** The Bull *Extreme Computing LDAP Authentication Guide* for more information.

### 3.3.11 Optional - Install and Configure SLURM



**Important** SLURM is not compatible with the PBS Professional Batch manager and must only be installed on clusters which do not use PBS Professional.

The **SLURM** files are installed under the **/usr** and **/etc** directories.

#### 3.3.11.1 Install the SLURM RPMs

Run the command below to install the **SLURM** RPMs:

```
yum install slurm-devel slurm slurm-munge slurm-plugins slurm-sql slurm-  
slurmdbd slurm-auth-none slurm-pam_slurm slurm-sjstat
```

**See** The Bull *SLURM Guide* for details on configuring **SLURM** for the Management Node

### 3.3.12 Optional - Install and Configure PBS Professional Batch Manager

**See** The Bull *PBS Professional Guide* for details of the installation and configuration routines for the Management Node for PBS Professional.

### 3.3.13 Optional - Small clusters only

For small clusters where the Management Services and the Login Services are on the same Service Node, the compilers and MPI user environment must be configured for the Login Services.

**See**

- Chapter 7 - *Installing Intel Tools and Applications* in this manual for more information on installing Intel Compilers and the Math Kernel Library (if required).
- Section 3.5.8 in this chapter for more information on configuring the MPI user environment.

## 3.4 STEP 4: Install RHEL5.3, bullx cluster suite XR 5v3.1U3 Software, and optional extreme computing software products on other nodes

### 3.4.1 R421 E1 machines only

Configure **RAID** for the **LSI 1064** chip. This kind of adapter is installed on **R421 E1** machines only.

### 3.4.2 Configuration for installnfs script

The Management Node has to be configured to be the **NFS** server that will install the **Red Hat Linux** distribution and the **bullx cluster suite extreme computing** software on all the other nodes of the cluster. Once the **NFS** environment has been correctly set, all that is required is that the individual nodes are booted for the Linux distribution to be installed on them.



**Important** Only one node of each type (**COMPUTE**, **COMPUTEX**, **LOGIN**, **I/O**) has to be created and installed using the **installnfs** script. **KSIS** is then used to deploy images of each node type on the cluster. See **STEP 6**

Before running the **installnfs** script, the prerequisites, below, must be satisfied.

**Note** If the steps in the previous section have been followed correctly, these prerequisites will already be in place.

### 3.4.3 installnfs script prerequisites

- The node(s) that are to be installed must have been configured in the **dhcpd.conf** file in order that an IP address is obtained on **DHCP** request.
- The **next-server** option, and the **filename** option for each host, has to be set correctly.
- The **DHCPD** service must be running, if not the script will try to start it.
- The **XINETD** service must be running and configured to run **ftpp**, if not the **installnfs** script will try to configure **ftpp** and start the service.
- The **BMCs** of the nodes must have already been configured.

### 3.4.4 Prepare the software installation

Run the **installnfs** command:

```
installnfs
```

Use the **--verbose** option for a more detailed trace of the execution of the **installnfs** script to be stored in the **installnfs** log file:

```
installnfs --verbose
Use the --interactive option to force the script to run in interactive
mode. All the Linux installation steps will be pre-filled, and will
have to be confirmed or changed:installnfs --interactive
```

The script will ask for the following information:

1. The mode to use - choose **install** mode.


```
-----
Please enter the mode to use ('install' will erase all data on the
node) ? [install] | upgrade :
-----
```

2. The path containing the operating system you want to use. In the example, below, number **2** would be entered from the options displayed to choose **/release/RHEL5.3/**.

```
-----
The following Operating System(s) have been found in the /release
directory :
```

- ```
0 : Choose Custom PATH
1 : Bull Advanced Server for Xeon 5.3 (/release/bullxLinux5.3)
2 : Red Hat Enterprise Linux Server 5.3 (/release/RHEL5.3)
-----
```

---

 **Important** Option 1 for Bull Advanced Server for Xeon 5.3 must be installed for bullx cluster suite CN OS (Cluster Type 2 - see Table 3.1).

---

Select the line for the Operating System you want to use.

3. The partitioning method to be used for the installation.

```
-----
Select the partitioning method you want to use for the installation :
- manual : user defined partitioning (you will be asked
interactively for the partitioning)
- auto : kickstart will use a predefined partitioning
-----
```

The **auto** option will only handle the **sda** disk, and will leave other node disks as previously partitioned. Use the **manual** partitioning option if other disks, previously partitioned, need to be repartitioned.

---

 **Important** For manual (re)partitioning a maximum of 3 disks can be used. Only the **sda**, **sdb** and **sdc** disk can be used for manual (re)partitioning.

---

The auto kickstart options are shown below:

|        | <b>/</b> | <b>/usr</b> | <b>/opt</b> | <b>/tmp</b> | <b>/var</b>              |
|--------|----------|-------------|-------------|-------------|--------------------------|
| swap   | ext3     | ext3        | ext3        | ext3        | ext3                     |
| 16 GBs | 10 GBs   | 10 GBs      | 10 GBs      | 10 GBs      | The remaining disk space |
| sda    | sda      | sda         | sda         | sda         | sda                      |

4. The question *Do you want to enable vnc mode?* will appear. If you answer no, it will be possible to follow the installation via a serial line (conman).

5. The question *Do you want to install the Bull HPC Software Suite?* will appear. If you answer **no**, go to step 9.
6. The path that includes the **bullx cluster suite XR 5v3.1U3** software installer. This will be something like `/release/XBAS5V3.1`. A list of potential paths will be displayed, as shown below.

---

Select the path for the Bull HPC installer:

```
0 : Choose Custom PATH
1 : /release/XBAS5V3.1
```

Enter the number for the path :

---

7. The extreme computing node functions that you want to install. The possible options are: **IO, LOGIN, COMPUTE, COMPUTEX** – See *Chapter 1* for more details regarding the different **bullx cluster suite** architectures. Some of these functions may be installed together, as shown for the group C functions, below:

---

Select the node functions to be installed. Node functions from the same group can be added together, for example IO and LOGIN. Node functions from different groups are exclusive.

```
1 : COMPUTE      (group A)
2 : IO          (group C)
3 : LOGIN       (group C)
4 : COMPUTEX    (group B)
```

Enter the node functions required using a comma separated list, when more than one product is to be installed, for example: 2,3 :

---

8. The **bullx cluster suite** optional extreme computing product(s) to be installed for the cluster, as shown below. By default, the Bull **XHPC** software is installed.

---

Select any optional Bull HPC software product(s) to be installed. N.B. The media corresponding to your choice(s) must have been copied into the `/release/XBAS5V3.1` directory.

```
0 : NONE
1 : XIB
2 : XLUSTRE
3 : XTOOLKIT
```

Enter the product(s) to be installed using a comma separated list when more than one product is to be installed, for example : 1,2 :

---



---

**See** **bullx cluster suite** optional extreme computing products can be installed later manually (see *Appendix B*).

---

9. Additional **RPMs** from custom specific directories can also be installed by the Bull **HPC** installer. If the **installnfs** script detects additional custom directories, it will check to see if any additional **RPMs** should be installed by asking the question *Custom directories containing additional RPMs have been found, do you want to install some of these RPMs via the HPC installer?* If you answer **no**, go to step 12. Custom directories containing **RPMs** must be put into the `/release/CUSTOM` directory.
10. The path for the **bullx cluster suite** software installer, if not provided earlier at step 6 (**install** mode only).
11. The custom directories to install:

---

Select any custom dirs to be installed.

---



---

```

N.B. The media corresponding to your choice(s) must have been copied
into the CUSTOM directory as follows /release/CUSTOM/<your
directory(ies)>
    1 : C1
Enter the directory(ies) to be installed, using a comma separated list
when more than one is to be installed :

```

---

**Note** Custom directory(ies) and RPMs can be installed manually later (see *Appendix B*)

---

12. The IP address of the NFS server node. This node must be the same as the one on which the script runs.
13. A list of the different nodes that are included in the Cluster database will be displayed, as shown in the example below. The node name(s) of the node(s) to be installed or upgraded must then be entered using the following syntax: `basename2` or `basename[2-15,18]`. The use of square brackets is mandatory.

---

| Node names               | Type     | Status      |
|--------------------------|----------|-------------|
| basename1                | A-----   | not_managed |
| basename0                | A-----   | up          |
| basename[1076-1148]      | -C-----  | not_managed |
| basename[26-33,309-1075] | -C-----  | up          |
| basename[2-23]           | --I----- | up          |

---

The nodes that are included in the Cluster database are shown above. Enter the list of nodes to be installed or upgraded using NFS (syntax examples - `basename2` or `basename[2-15,18]`) :

---

14. A detailed summary is then displayed listing the options to be used for the installation, as shown in the example below. The Administrator has to confirm that this list is correct or exit the script.

---

SUMMARY:

```

PXE boot files will be copied from
/release/RHEL5.3/images/pxeboot
Path containing Linux Distribution : /release/RHEL5.3
NFS Server IP address is : 10.30.1.99
Serial Line option is : ttyS1,115200
Vnc mode is : Disabled
Partitioning method is : auto
The following hexa file(s) will be generated in
/tftpboot/pxelinux.cfg : 0A1F0106
The path containing Bull HPC installer : /release/XBAS5V3.1
Installation function(s): IO LOGIN
Optional HPC product(s) : XIB XLUSTRE
Optional CUSTOM dir(s) : C1

Please confirm the details above or exit : [confirm] | exit :

```

---

**Note** Some **hexa** files will be created in the `/tftpboot/pxelinux.cfg` directory. These files are called **hexa** files because their name represents an IP address in hexadecimal format, and they are required for the PXE boot process. Each file corresponds to the IP address of a node.

For convenience, the **installnfs** script creates links to these files using the node names

---

15. A line appears regarding the use of **nsctrl** commands to reboot the node where the software is going to be installed, as shown below. Before you click yes to confirm this, check that the **BMC** for the node is reachable. If this is not the case, answer no and manually reboot your node later.

---

```
Do you want installnfs to perform a hard reboot, via the
/usr/sbin/nsctrl command, on the node(s) listed? [y] | n :
```

---

### 3.4.5 Launch the NFS Installation of the bullx cluster suite XR 5v3.1U3 Software

1. The **bullx cluster suite XR 5v3.1 U3** software will be installed immediately after the reboot. The progress of the install can be followed using **conman** via a serial line, and/or by using **vncviewer** if you have chosen to use **VNC**.
2. Once the **Linux** distribution has been installed, the **kickstart** will then manage the installation of the optional **extreme computing** product(s) selected for the installation, and the node will then reboot. The node can then be accessed to carry out any post-installation actions that are required using the **ssh** command (the **root** password is set to root by default).
3. The **installnfs** script will generate a log file: **/root/installnfs.log** on the Management Node which can be checked if there are any problems.



**Important** See the *Software Release Bulletin* for details of any **BONUS RPMS** to be installed manually on the Reference Nodes.

---


**See** Appendix C - *Manual Installation of Software*, in this manual, if there is a need to install any of the additional software options (**XIB**, **XLUSTRE** and **XTOOLKIT**), or any RPMs from the custom directories, later after completing this step.

---

## 3.5 STEP 5: Configure the Administration Software on LOGIN, I/O, COMPUTE and COMPUTEX Reference Nodes

This step describes how to install and configure the Reference Nodes to be deployed. The configuration of the **MPI** user environment, the optional installation of **NVIDIA** accelerators and **CUDA** Toolkit, and RAID monitoring installation are also described.

### 3.5.1 Configure SSH and /etc/hosts

 **Important** These tasks must be performed before deployment.

#### 3.5.1.1 For a reinstallation of bullx cluster suite XR 5v3.1U3

Retrieve the **SSH** keys of the nodes and of the root user, which have been saved previously – see section 3.0.2. To do this:

- Restore the **/etc/ssh** directory of each type of node to its initial destination.
- Restore the **/root/.ssh** directory on the Management Node.
- Go to the root directory:

```
cd /root
```

- From the management Node copy the **/root/.ssh** directory on to the **COMPUTE(X)** and **LOGIN** and **I/O** Nodes.

```
scp -r .ssh <node_name>:/root/
```

- Restart the **SSH** service on each type of node:

```
service sshd restart
```

- Notes**
- The **SSH** keys of the users can be restored from the files saved by the administrator (for example **/<username>/.ssh**).
  - The **sudo** configuration will have been changed during Bull **XHPC** software installation to enable administrators and users to use the **sudo** command with **ssh**. By default, **sudo** requires a pseudo-tty system call to be created in order to work, and this is set by the **requiretty** option in the **/etc/sudoers** configuration file. In order that the automated commands run over **ssh/sudo**, the installer will have modified the default configuration file by commenting out this option.

#### Copy the /etc/hosts file onto the Reference Node

Copy the **/etc/hosts** file from Management Node using the **scp** command with the IP address of the Management Node as the source parameter.

Example:

```
scp root@<Management_Node_IP_address>:/etc/hosts /etc/hosts
```

### 3.5.1.2

#### For a first installation of bullx cluster suite XR 5v3.1 U3

1. Copy the `/root/.ssh` directory from the Management Node on to the Reference Nodes.

```
scp -r .ssh <reference_node>:.
```

2. Test this configuration:

```
> ssh <reference_node> uname
```

```
-----  
The authenticity of host 'ns1 (127.0.0.1)' can't be established.  
RSA key fingerprint is  
91:7e:8b:84:18:9c:93:92:42:32:4a:d2:f9:38:e9:fc.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added 'ns1,127.0.0.1' (RSA) to the list of known  
hosts.  
Linux  
-----
```

---

**Note** With this **SSH** configuration, no password is required for root login from the Management Node to the other **extreme computing** nodes.

---

#### Copy the `/etc/hosts` file onto the Reference Node

Copy the `/etc/hosts` file from Management Node using the `scp` command with the IP address of the Reference Node as the destination parameter.

Example:

```
scp /etc/hosts root@<Reference_Node_IP_address>:/etc/hosts
```

### 3.5.2

#### Disk Health Monitoring Configuration

By default the `/etc/smartd.conf` file is recreated automatically each time the system boots and contains a line for each disk device detected on the system. Some of the disk devices may correspond to **RAID** volumes or remote LUNs on storage sub-systems. Smart monitoring is not supported for these devices and the lines, which correspond to them, plus the first line, below, must be deleted from the `/etc/smartd.conf` file.

```
-----  
#DEVICESCAN -H -m root  
-----
```

### 3.5.3

#### Configure Ganglia

1. Copy the file below:  
`/usr/share/doc/ganglia-gmond-3.0.5/templates/gmond.conf` into `/etc`.
2. Edit the `/etc/gmond.conf` file:
  - In line 18, replace `xxxxx` with the basename of the cluster.  
`name = "xxxxx" /* replace with your cluster name */`
  - In line 24 replace `x.x.x.x` with the alias IP address of the Management Node.  
`host = x.x.x.x /* replace with your administration node ip  
address */`

3. Start the **gmond** service:

```
service gmond start
chkconfig --level 235 gmond on
```

### 3.5.4 Optional - Configure LDAP

---

**See** The Bull *Extreme Computing LDAP Authentication Guide* for more information.

---

### 3.5.5 Configure the kdump kernel dump tool

1. Reserve memory in the kernel that is running for the second kernel that will make the dump by adding '**crashkernel=128M@16M**' to the grub kernel line, so that 128MBs of memory at 16MBs is reserved in the **/boot/grub/grub.conf** file, as shown in the example below:

```
kernel /vmlinuz-2.6.18-53.el5 ro root=LABEL=/ nodmraid
console=ttyS1,115200 rhgb quiet crashkernel=128M@16M
```

It will be necessary to reboot after this modification.

2. The following options must be set in the **/etc/kdump.conf** configuration file:
  - a. The path and the device partition where the dump will be copied to should be identified by its **LABEL**, **/dev/sdx** or **UUID** label, either in the **/home/** or **/** directories.

Examples:

```
path /var/crash
ext3 /dev/sdb1
#ext3 LABEL=/boot
#ext3 UUID=03138356-5e61-4ab3-b58e-27507ac41937
```

- b. The tool to be used to capture the dump must be configured. Uncomment the **core\_collector** line and add **-d 1**, as shown below:

```
core_collector makedumpfile -c -d 1
```

**-c** indicates the use of compression and **-d 1** indicates the dump level:



#### Important

It is essential to use non-stripped binary code within the kernel. Non-stripped binary code is included in the **debuginfo** RPM, **kernel-debuginfo-  
<kernel\_release>.rpm**, available from <http://people.redhat.com/duffy/debuginfo/index-js.html>

This package will install the kernel binary in the folder **/usr/lib/debug/lib/modules/<kernel\_version>/**

---

**Note** The size for the dump device must be larger than the memory size if no compression is used.

---

3. Add the "**acpi=off nomsi nolapic noapic**" options to the **KDUMP\_COMMANDLINE\_APPEND** parameter in the **/etc/sysconfig/kdump** configuration file, so that the parameter appears as below:

```
KDUMP_COMMANDLINE_APPEND="irqpoll maxcpus=1 reset_devices acpi=off  
nomsi nolapic noapic"
```

4. Use the command below to launch **kdump** automatically when the system restarts:

```
chkconfig kdump on
```

## 3.5.6 Optional - Install and Configure SLURM

**See** The *SLURM Guide* for configuration details for the Reference Nodes.

The **SLURM** files are installed under the **/usr** and **/etc** directories.

**Note** These steps must be carried out for each **COMPUTE(X)** and **LOGIN** Reference Node.

### 3.5.6.1 Installing SLURM on the Reference Nodes

1. Mount NFS from the **/release** directory on the Management Node to the **/release** directory on the Node:

```
mount -t nfs <Management_Node_IP>:/release /release
```

2. Run the command below to install the **SLURM** RPMs:

```
yum install slurm-devel slurm slurm-munge slurm-plugins slurm-sql slurm-  
slurmdbd slurm-auth-none slurm-pam_slurm slurm-sjstat
```

## 3.5.7 Optional - Install and Configure the PBS Professional Batch Manager

**See** The *Bull PBS Professional Guide* for more information on installing and configuring PBS Professional on the **COMPUTE(X)/LOGIN** reference nodes.

## 3.5.8 Configure the MPI user environment

Configure the **MPI** user environment using either the **MPIBull2** or **bullx MPI** libraries.

### 3.5.8.1 MPIBull2

**MPIBull2** comes with different communication drivers and with different process manager communication protocols.

When using the **InfiniBand** OFED/SLURM pairing, the System Administrator has to verify that:

- Users are able to find the OFED libraries required

- User jobs can be linked with the SLURM PMI library and then launched using the SLURM process manager.

The **MPiBull2** RPMs include 2 automatic setup files

`/opt/mpi/mpibull2-<version>/share/mpibull2.*sh`, which are used to define default settings for the cluster.

### User access to MPiBull2

The administrator has a choice of 3 different way of making **MPiBull2** available to all users:

1. Copying the `mpibull2.*` environment initialization shell scripts from `/opt/mpi/mpibull2-<version>/share` to the `/etc/profile.d/` directory, according to the environment required. For example:

For **MPI**:

```
cp /opt/mpi/mpibull2-<version>/share/mpibull2.*sh /etc/profile.d
```

For **Intel C**:

```
cp /opt/intel/cce/<compiler_version>/bin/iccvars.*sh /etc/profile.d
```

For **Intel Fortran**:

```
cp /opt/intel/fce/<compiler_version>/bin/ifortvars.*sh /etc/profile.d
```

2. Use the command below to enable the module with the profile files:

```
test -e /opt/mpi/modulefiles/mpibull2/<version> && echo "export  
MODULEPATH=\$MODULEPATH:/opt/mpi/modulefiles/mpibull2/" >>  
/etc/profile
```

Then the end user can load their environment by running the command below:

```
module load your_mpi_version
```

3. Asking users to customize their environment by sourcing the `/opt/mpi/mpibull2_your_version/share/setenv_mpiBull2.*` files.

Depending on the setup solution chosen, the Administrator must define two things: a default communication driver for their cluster and the default libraries to be linked to, according to the software architecture.

In all the files mentioned above, the following must be specified:

- a. A **MPiBull2\_COMM\_DRIVER**, this can be done by using the `mpibull2-devices -d=` command to set the default driver. For **InfiniBand** systems, the name of the driver is `ibmr_gen2`.
- b. **MPiBull2\_PRELIBS** variable must be exported to the environment containing the reference to the **SLURM** PMI library.

Some examples are provided in the files.

For a cluster using the **OpenIB** InfiniBand communication protocol, the following line must be included in the `mpibull*` file:

```
mpibull2-devices -d=ibmr_gen2
```

For a cluster using SLURM, set the following line, and if necessary add the path to the PMI library:

```
export MPIBULL2_PRELIBS="-lpmi"
```

When using the **MPI InfiniBand** communication driver, memory locking must be enabled. There will be a warning during the InfiniBand RPM installation if the settings are not correct. The `/etc/security/limits.conf` file must specify both soft memlock and hard memlock settings, according to the memory capacity of the hardware. These should be set around 4GBs or unlimited.

---

**Note** It is mandatory to restart the **sshd** daemons after changing these limits.

---

### 3.5.8.2 bullx MPI

The **bullx MPI RPM** includes 2 automatic setup files that define the default environment settings:

```
/opt/mpi/bullxmpi/<version>/bin/mpivars-<version>.*sh
```

Run one of the commands below to configure the **MPI** user environment:

```
source /opt/mpi/bullxmpi/<version>/bin/mpivars-<version>.csh
```

```
source /opt/mpi/bullxmpi/<version>/bin/mpivars-<version>.sh
```

The MPI user environment variables are set by either running a setup file or by loading a **bullx MPI** module.

#### Loading bullx MPI with the oscar module

If your operating system includes the **oscar** module then load it by running the command below:

```
module load bullxmpi-<version>
```

### 3.5.9 Bull Scientific Studio

The Bull Scientific Studio RPMs are installed automatically on the **COMPUTE(X)/LOGIN** reference nodes.

---

**See** The **bullx cluster suite** *Application Developer's Guide* and *System Release Bulletin* for more information on the libraries included in Scientific Studio.

---

### 3.5.10 Optional - NVIDIA Tesla Graphic Card accelerators

The drivers for the **NVIDIA Tesla C1060**, **Tesla S1070** and **Tesla 20 series (C2050, M2050 and S2050)** accelerators are installed automatically on the **COMPUTE(X)/LOGIN** reference nodes.



## 3.5.11 Optional - NVIDIA CUDA Toolkit 3.0

NVIDIA CUDA™ Toolkit and Software Development Kit are installed automatically on the LOGIN, COMPUTE and COMPUTEX reference nodes for clusters that include Tesla graphic accelerators, so that the NVIDIA compilers and mathematical/scientific libraries are in place for the application.

### Configure NVIDIA CUDA Toolkit 3.0

Run the command below to ensure the environmental variables are correct:

```
source /opt/cuda/3.0/cuda.sh
```

**See** The *bullx cluster suite Application Developer's Guide* and *System Release Bulletin* for more information on the NVIDIA compilers and libraries.

The *NVIDIA CUDA Compute Unified Device Architecture Programming Guide* and the other documents in the `/opt/cuda/3.0/doc` directory for more information.

## 3.5.12 Optional - Install RAID Monitoring Software

### 3.5.12.1 Monitoring using the LSI MegaRAID 8408E Adapter

**Note** This kind of adapter is only installed on R440 and R460 machines.

Install the **MegaCli-xxxx.i386.rpm** package, which is available on the *Bull Extension Pack CD-ROM*, below, delivered with the machines which use these adapters:

*Bull Extension Pack for NovaScale Universal Rack-Optimized & Tower Series with RHEL5.3*

No further configuration is required for the R440 and R460 machines once the **MegaCli-xxxx.i386.rpm** is installed.

### 3.5.12.2 Monitoring using the AOC-USAS-S8iR-LP Adapter

**Note** This kind of adapter is installed on R423 and R425 machines only.

1. Install the **StorMan-xxxx.x86\_64.rpm** package which is available on the CD-ROM, below, delivered with the machines which use these adapters:

*SUPERMICRO AOC-USAS-SRL*

2. Then run the commands below:

```
service stor_agent stop
chkconfig stor_agent off
```

3. Check that RAID has been configured correctly by running the command:

```
lsiocfg -cv |more
```

4. Look for the host that has **aacraid** displayed against it. Verify that the detailed information for the Logical and Physical disks displays correctly, as shown in the example below.

```

-----
host7 aacraid 0 256 - Optimal SMC AOC-USAS-S8iR-LP
DRV= 1,1-5 (2437)
FW= 5,2-0 (15575)
Interface=SAS/SATA
Slot=7
SN=4FAFF0
LogicalDisks=2
  Number=1 Name=RD1 Device=sdd Status=Optimal Raid=1 Size=239190 DiskLocations="0,3 0,1"
  Number=2 Name=RD5SAS Device=sde Status=Optimal Raid=5 Size=280188 DiskLocations="0,4 0,5 0,6"
PhysicalDisks=8
  Device=0 SN=WD-WCAPW5321110 WWN=Unknown State=Ready Location=0,0 Vendor=WDC Size=476940 LogicalDisk= Role=
  Device=1 SN=WD-WCANY3792200 WWN=Unknown State=Online Location=0,1 Vendor=WDC Size=239372 LogicalDisk=RD1 Role=
  Device=2 SN=WD-WCANY3792290 WWN=Unknown State=Ready Location=0,2 Vendor=WDC Size=239372 LogicalDisk= Role=
  Device=3 SN=WD-WCANY3600678 WWN=Unknown State=Online Location=0,3 Vendor=WDC Size=239372 LogicalDisk=RD1 Role=
  Device=4 SN=DQ00P65004LP WWN=500000E01203CF60 State=Online Location=0,4 Vendor=FUJITSU Size=140272 LogicalDisk=RD5SAS Role=
  Device=5 SN=DQ00P65004ND WWN=500000E01203D2A0 State=Online Location=0,5 Vendor=FUJITSU Size=140272 LogicalDisk=RD5SAS Role=
  Device=6 SN=DQ00P65004L9 WWN=500000E01203CE80 State=Online Location=0,6 Vendor=FUJITSU Size=140272 LogicalDisk=RD5SAS Role=
  Device=7 SN=WD-WCANY3792380 WWN=Unknown State=Ready Location=0,7 Vendor=WDC Size=239372 LogicalDisk= Role=
-----

```

### 3.5.13 Optional - NFS High Availability Clusters

1. In the `/etc/modprobe.conf` and `/etc/modprobe.d/lpfc` files, add the line:

```
options lpfc lpfc_nodev_tmo=5
```

2. Identify the kernel version installed on the node by running the command:

```
uname -r
```

3. Save the old `initrd` image using the kernel version, identified above:

```
mv /boot/initrd-<kernel_version>.img /boot/initrd-<kernel_version>.img-orig
```

4. Generate a new `initrd` image:

```
mkinitrd -v /boot/initrd-<kernel_version>.img <kernel_version>
```

## 3.6 STEP 6: Create and Deploy Reference Node Images

This step describes how to perform the following tasks:

1. Installation and configuration of the image server
2. Creation of an image of the **COMPUTE(X)**, and **LOGIN** and **I/O** or **LOGIN/IO** Reference Nodes previously installed.
3. Deployment of these images on the cluster nodes.
4. Post Deployment Configuration.

These operations have to be performed from the Management Node.



**Important** Please refer to *bullx cluster suite High Availability Guide* if High Availability is to be included for any part of your cluster to check that all the High Availability configurations necessary are in place on the Reference Node image.

**Note** To create and deploy a node image using **Ksis**, all system files must be on local disks and not on the disk subsystem.



**Important** It is only possible to deploy an image to nodes that are equivalent and have the same hardware architecture, including:

- Platform
- Disks
- Network interface

**See** The *bullx cluster suite Administrator's Guide* for more information about **Ksis**.

### 3.6.1 Install, Configure and Verify the Image Server

#### 3.6.1.1 Installing the Ksis Server

The **Ksis** server software is installed on the Management Node from the **XHPC** CDROM. It uses **NovaScale** commands and the cluster management database.

#### 3.6.1.2 Configuring the Ksis Server

**Ksis** only works if the cluster management database is correctly loaded with the data which describes the cluster (in particular the data for the node descriptions and the administration network).

The preload phase that updates the database must have finished before **ksis** is used.

#### 3.6.1.3 Verifying the Ksis Server

In order to deploy an image using **Ksis**, various conditions for the nodes concerned must have been met. If the previous installation steps completed successfully then these conditions will be in place. These conditions are listed below.

1. Each node must be configured to boot from the network via the **eth0** interface. If necessary, edit the BIOS menu and set the Ethernet interface as the primary boot device.
2. The access to cluster management database should be checked by running the command:

```
ksis list
```

The result must be "no data found" or an image list with no error messages.

3. Check the state of the nodes by running the **nsctrl** command:

```
nsctrl status node_name
```

The output must not show nodes in an inactive state, meaning that they are not powered on.

4. Check the status of the nodes by running the **ksis nodelist** command:

```
ksis nodelist
```

## 3.6.2 Create an Image

Create an image of the **bullx cluster suite XR 5v3.1 U3 COMPUTE(X)**, and **LOGIN** and **I/O** or **LOGIN/IO** reference nodes, previously installed, using the command below.

```
ksis create <image_name> <reference_node_name> -D "image_description"
```

### Example

```
ksis create imagel ns1 -D "My_Cluster_Compute_Node_Image"
```

---

**Note** If the **-D** option is not used, the image creation will stop until an image description is entered.

---

The **ksis create** command will also ask for a check level. Select the **basic** level. If no level is selected, the **basic** level will be selected automatically by default, after the timeout.

## 3.6.3 Deploy the Image on the Cluster

---

**Note** Before deploying the image, it is mandatory that the equipment has been configured – see **STEP 3**.

1. Before deploying check the status of the nodes by running the command below:

```
ksis nodelist
```

2. If the status for any of the nodes is different from up then restart **Nagios** by running the following command from the root prompt on the Management Node:

```
service nagios restart
```

- Each node must be configured to boot from the network via the **eth0** interface. If necessary, edit the BIOS menu and set the Ethernet interface as the primary boot device.
- Start the deployment by running the command:

```
ksis deploy <image_name> node[n-m]
```

- If, for example, 3 Compute Nodes are listed as ns[2-4], then enter the following command for the deployment:

```
ksis deploy image1 ns[2-4]
```

---

**Note** The reference nodes may be kept as reference nodes. Alternatively, they may be included in the deployment for the cluster, in the same way as the other nodes. It is recommended that this second option is chosen.

---

## 3.6.4 Post Deployment Configuration

### 3.6.4.1 postconfig command

Once the image deployment has finished, the cluster nodes will need to be configured according to their type, Compute, I/O, etc. Post deployment configuration is mandatory as it configures **ganglia**, **syslog-ng**, **NTP**, and **SNMP** automatically on these machines.

The **ksis postconfig** command configures each node that the image has been deployed to, ensuring that all the cluster nodes of a particular type are homogenous.

**ksis** post-configuration is carried out by running the command:

```
ksis postconfig run PostConfig <cluster_name>[nodelist]
```

#### For example

```
ksis postconfig run PostConfig ns[1-100]
```

### 3.6.4.2 Configure the Interconnect Interfaces

The interconnect interface description file is generated from the Management Node for each node by using the **config\_ip** command.

---

**See** *Appendix C- Configuring Interconnect Interfaces* for more details regarding the use of the **config\_ip** command.

---

## 3.6.5 Install the Intel Compilers and Tools on the Login Nodes

---

**See** Chapter 7 - *Installing Intel Tools and Applications* in this manual for more information.

---

## 3.7 STEP 7: Final Cluster Checks

### 3.7.1 Check the Installation Details

The Bull information file, found at `/etc/bull-infos` provides information about the **BAS5 for Xeon** software installed on the cluster, including the following:

**Installation func** Node type functions installed, for example **MANAGEMENT** for Management Node

**Product** Software products installed, for example **XIB** for **InfiniBand** software.

The Red Hat information file, found at `/etc/redhat-release` provides the version details for the **Red Hat Enterprise Linux Server** installed.

#### 3.7.1.1 Package Details for Node Functions and Products

1. To see and verify the package details that have been installed on a node, run the command below:

```
/release/XBAS5V3.1/install --pkglst
```

The output from the command is divided into sections for each product that has been installed on the node, as shown below in the example for **XLUSTRE**.

```
-----  
"XLUSTRE product"  
lustre lustre_e2fsprogs lustre_ldap lustre-modules lustre_mgmt  
lustre_utils lustre-source keep_port  
mdm  
-----
```

2. To obtain more information regarding the package versions for the **bullx cluster suite** release, use the **rpm -q** option with the list of packages for the product, as shown in the command example below.

```
rpm -q lustre lustre_e2fsprogs lustre_ldap lustre-modules lustre_mgmt  
lustre_utils lustre-source keep_port  
mdm
```

#### Output example for the command above

```
-----  
lustre-1.6.4.3-b.5.1.202  
lustre_e2fsprogs-1.40.4.cfs1-b.5.1.202  
lustre_ldap-1.6-b.5.1.203  
lustre-modules-1.6.4.3-2.6.18_53.1.21.e15.Bull.1_b.5.1.202  
lustre_mgmt-1.6-b.5.1.203  
lustre_utils-1.6-b.5.1.203  
lustre-source-1.6.4.3-b.5.1.202  
keep_port-1.0-1.Bull  
mdm-1.2.5-1_2.6.18_53.1.21.e15.Bull.1  
-----
```

3. To see details of all the packages included in the **bullx cluster suite** delivery, including all node functions and products, run the command below:

```
/release/XBAS5V3.1/install --pkglst all
```

---

**Note** If you are not on the Management Node, mount NFS from the `/release` directory on the Management Node to the `/release` directory for the node you are on, using the command below before looking at the package details:

```
ssh <Node_name>
mount -t nfs <Management_Node_IP>: /release /release
```

---

## 3.7.2 Test pdsh

**pdsh** is a utility that runs commands in parallel on all the nodes or on a group of nodes for a cluster. This is tested as follows:

### All nodes

1. Run a command similar to that below from the Management Node as root:

```
pdsh -w ns[8-10] hostname
```

2. This will give output similar to that in the example below:

```
ns10: ns10
ns9: ns9
ns8: ns8
```

### Groups of nodes

1. Run the `dbmGroup` command

```
dbmGroup show
```

2. This will give output similar to that in the example below:

```
-----
Group Name  Description                               Nodes Name
-----
ADMIN       Nodes by type:ADMIN                       ns[0,12]
ALL         All nodes except node admin               ns[1-10]
Burning    Burning group                             ns5
COMP       Nodes by type:COMP                         ns[1-4,7-8]
COMP128GB  COMPUTE node with 128GB                   ns8
COMP48GB   COMPUTE node with 48GB                    ns4
Deploy     Deploy group                              ns3
HwRepair   HwRepair group                           ns8
IO         Nodes by type:IO                          ns[6,10]
META       Nodes by type:META                        ns[5,9]
MYFAME     ensemble des fame du cluster              ns[0,4-6,8-10]
NODES128GB Nodes by memory size:128GB                ns8
NODES16GB  Nodes by memory size:16GB                 ns[1-3,7]
NODES48GB  Nodes by memory size:48GB                 ns[4,6,10]
NODES64GB  Nodes by memory size:64GB                 ns[0,5,9,12]
QxTest    QxTest group                             ns[0,6]
TEST      TEST group                               ns[5,9]
UnitTest   UnitTest group                           ns[1,9]
-----
```

3. Run a test command for a group of nodes, as shown below:

```
pdsh -g IO date | dshbak -c
```

4. If **pdsh** is functioning correctly this will give output similar to that in the example below:

```
ns[6,10]
Thu Aug 7 15:35:27 CEST 2008
```

### 3.7.3 Check NTP

1. Run the following command on a COMPUTE(X) node and on a combined LOGIN/IO Login or dedicated LOGIN nodes:

```
ntpq -p
```

Check that the output returns the name of the NTP server, and that values are set for the **delay** and **offset** parameters.

2. On the Management Node, start **ntptrace** and check if the Management Node responds:

```
ntptrace 172.17.0.99
```

```
ns0: stratum 11, offset 0.000000, synch distance 0.012695
```

3. From the Management Node, check that the node clocks are identical:

```
pdsh -w ns[0-1] date
```

```
ns0: Tue Aug 30 16:03:12 CEST 2005
```

```
ns1: Tue Aug 30 16:03:12 CEST 2005
```

### 3.7.4 Check syslog-ng

1. Check on the Management Node and node host that the **syslog-ng** service has started on both hosts:

```
service syslog-ng status
```

The output should be:

```
syslog-ng (pid 3451) is running...
```

2. On the node host, run the command below to test the configuration:

```
logger "Test syslog-ng"
```

3. On the node host, verify that the *'Test syslog-ng'* message is included in the **/var/log/messages** file.
4. On the Management Node, verify that the *'Test syslog-ng'* message is included **/var/log/HOSTS/<node\_hostname>/messages** file.



### 3.7.5 Check Nagios

Both **nagios** and **httpd** services have to be running on the Management Node, check these as follows:

```
service nagios status
```

#### Example output

```
bsm_nagios (pid 31356 31183 19413) is running...
```

```
service httpd status
```

#### Example output

```
> httpd (pid 18258 18257 18256 18255 18254 18253 18252 18251 5785) is running...
```

1. Start a web browser (Firefox, Mozilla, etc.) and enter the following URL:  
`http://<Management_Node_name>/BSM`
2. Then, left click the **Start Console** button.

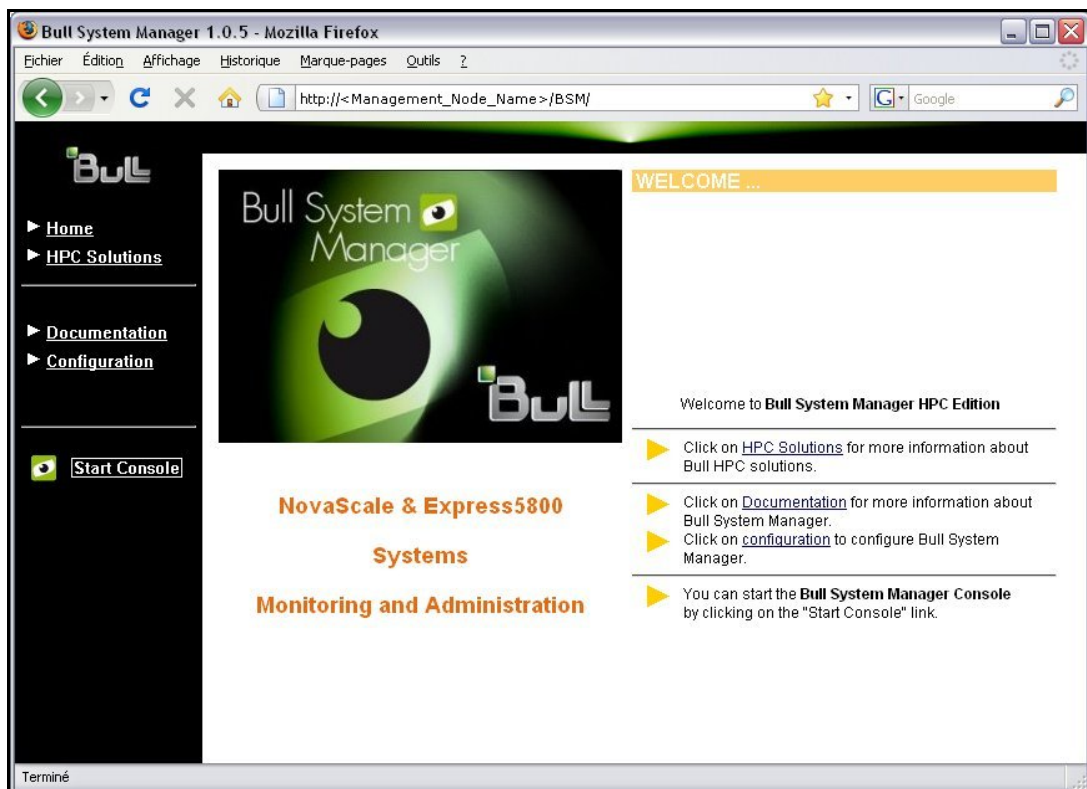


Figure 3-19. Bull System Manager Welcome screen

An authentication window appears asking for a user name and a password.

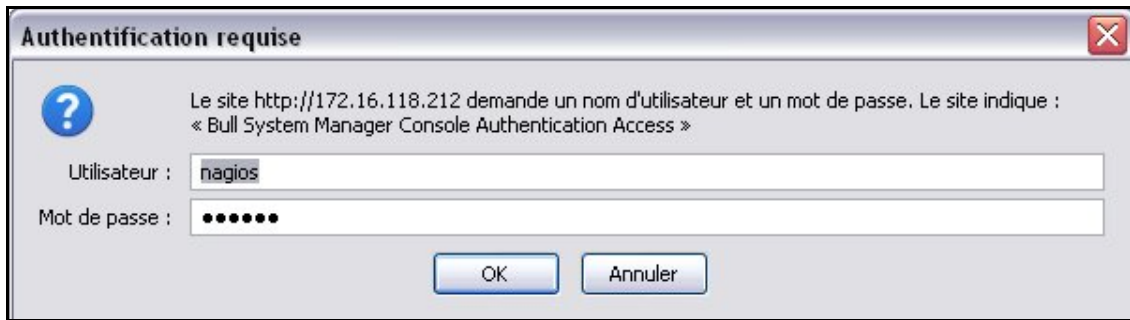


Figure 3-20. Bull System Manager Authentication Window

3. Once authenticated, the Bull System Manager console appears.

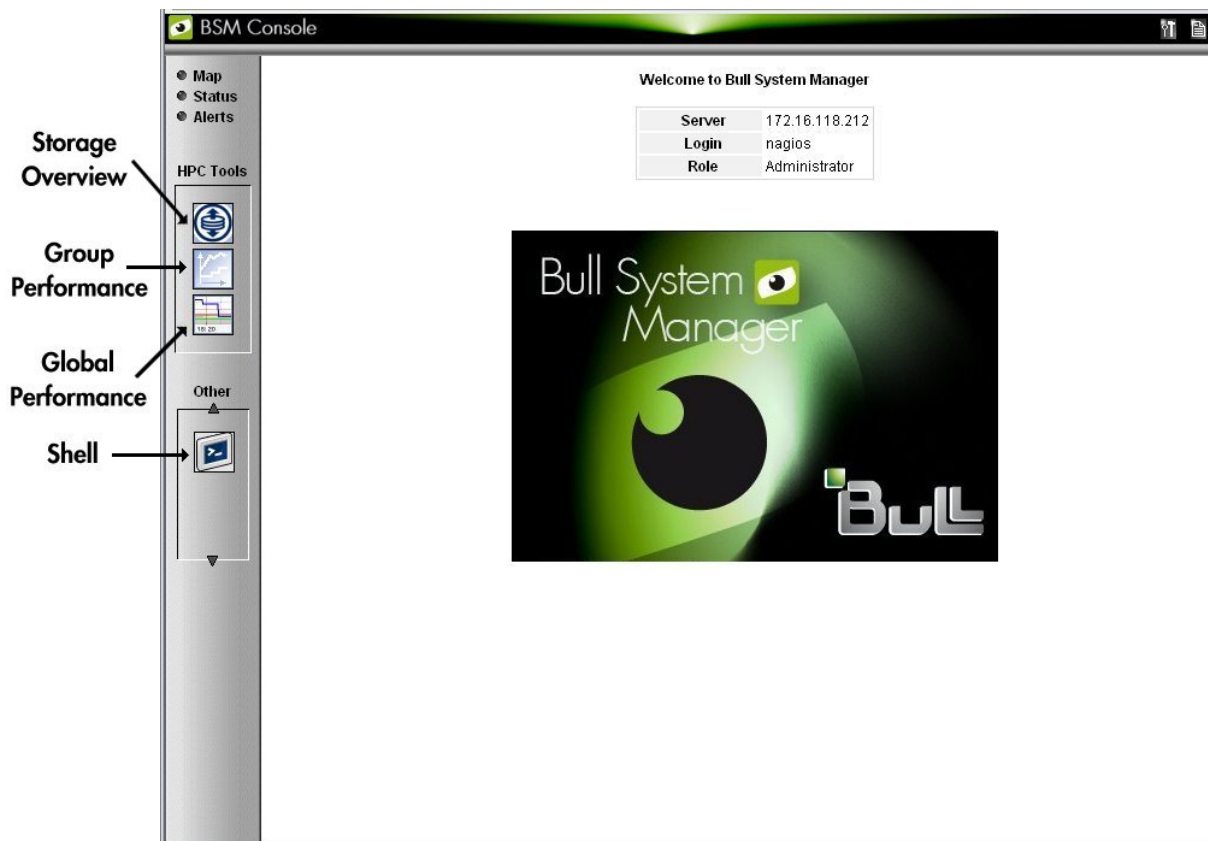


Figure 3-21. The Bull System Manager console

Click the **Map** link (top left) to display all the elements that are being monitored.

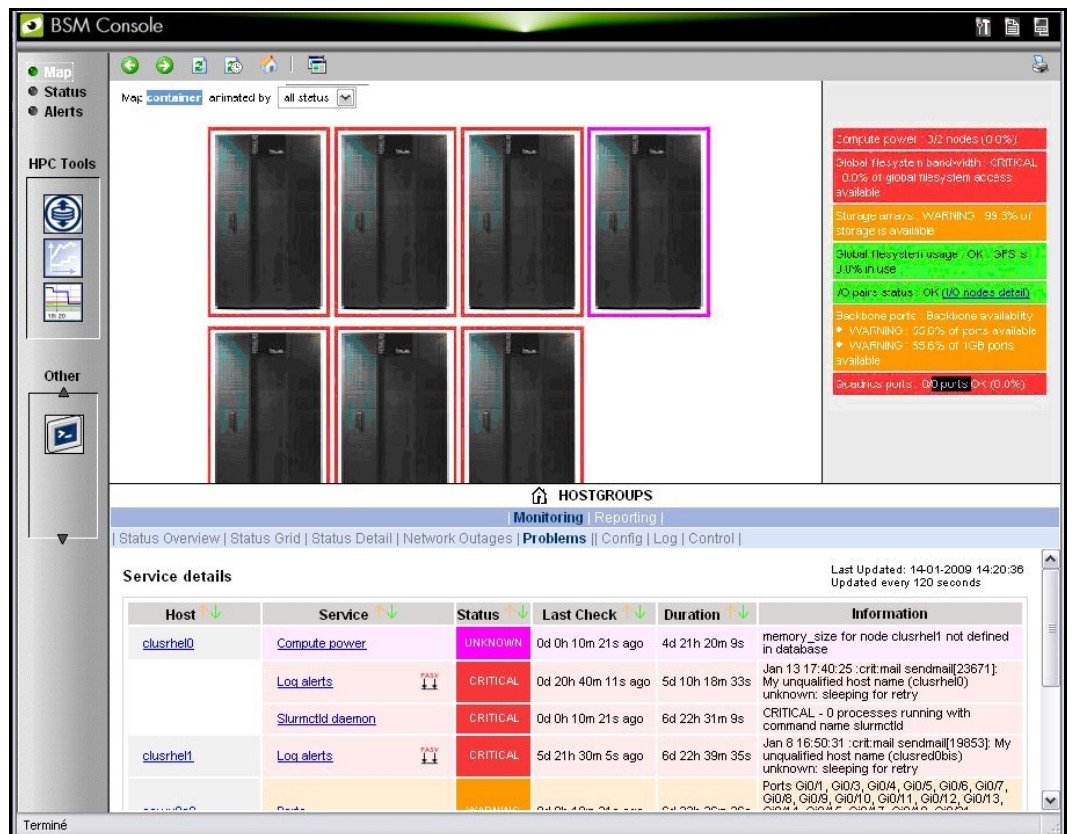


Figure 3-22. Bull System Manager Monitoring Window

### 3.7.6 Check nsctrl

To test `nsctrl`, run a command similar to that below:

```
[root@ns0 ~]# nsctrl status ns[1-5]
```

This will give output similar to that below:

```
ns2 : Chassis Power is on
ns1 : Chassis Power is on
ns3 : Chassis Power is on
ns5 : Chassis Power is on
ns4 : Chassis Power is on
[root@ns0 ~]#
```

See *The Maintenance Guide* for more information on `nsctrl`.

### 3.7.7 Check conman

1. Run the command below to check the `conmand` daemon:

```
[root@ns0 ~]# service conman status
```

```
conmand (pid 5943) is running...
[root@ns0 ~]#
```

2. Run a command similar to the one below to check **conman**.

```
[root@ns0 ~]# conman ns2
```

```
<ConMan> Connection to console [ns2] opened.  
Red Hat Enterprise Linux Server release 5.3 (Tikanga)  
Kernel 2.6.18-53.1.21.el5.Bull.1 on an x86_64  
ns2 login:
```

---

**See**    The *Maintenance Guide* for more information on **conman**.

---

## 3.7.8    Software Stack Checks

Refer to the software component manuals, for example, *SLURM Guide*, *PBS Professional Guide*, etc., for details of any post installation configurations and checks that apply to the components installed on your cluster.

## 3.7.9    Test kdump



### Important

It is essential to use non-stripped binary code within the kernel. Non-stripped binary code is included in the debuginfo RPM, **kernel-debuginfo-`<kernel_release>.rpm`**, available from

<http://people.redhat.com/duffy/debuginfo/index-js.html>

This package will install the kernel binary in the folder  
`/usr/lib/debug/lib/modules/<kernel_version>/`

---

In order to test that **kdump** is working correctly a dump can be forced using the commands below.

```
echo 1 > /proc/sys/kernel/sysrq  
echo c > /proc/sysrq-trigger
```

The end result can then be analysed using the crash utility. An example command is shown below. The **vmcore** dump file may also be found in the `/var/crash` folder.

```
crash /usr/lib/debug/lib/modules/<kernel_version>/vmlinux vmcore
```

---

## Chapter 4. Configuring Storage Management Services

This chapter describes how to:

- Configure the storage management software installed on the Management Node
- Initialize the management path to manage the storage systems of the cluster
- Register detailed information about each storage system in the ClusterDB.

The following topics are described:

4.1 *Enabling Storage Management Services*

4.2 *Enabling the Administration of StoreWay FDA and Optima 1500 (NEC) Storage Systems*

4.3 *Enabling the Administration of DataDirect Networks S2A (DDN) Storage Systems*

4.4 *Enabling the Administration of Optima 1250 (Xyratex) Storage Systems*

4.5 *Enabling the Administration of EMC/Clariion (DGC) Storage Systems*

4.6 *Updating the ClusterDB with Storage Systems Information*

4.7 *Storage Management Services*

4.8 *Enabling the Administration of Brocade Fibre Channel Switches*

---

**Note** When installing the **storageadmin-xxx** rpms in update mode (**rpm -U**), all the configuration files described in this section and located in **/etc/storageadmin** are not replaced by the new files. Instead the new files are installed and suffixed by **.rpmnew**. Thus, the administrators can manually check the differences, and update the files if necessary.

---

---

**See** For more information about setting up the storage management services, refer to the *Storage Devices Management* chapter in the *bullx cluster suite Administrator's Guide*.

---

Unless specified, all the operations described in this section must be performed on the cluster management station, using the root account.

## 4.1 Enabling Storage Management Services

Carry out these steps on the Management Node.

1. Configure ClusterDB access information:  
The ClusterDB access information is retrieved from the `/etc/clustmngt/clusterdb/clusterdb.cfg` file.
2. Edit the `/etc/cron.d/storcheck.cron` file to modify the period for regular checks of the status for storage devices. This will allow a periodic refresh of status info by pooling storage arrays. Two (2) hours is the default value, but four (4) hours is a recommended value for clusters with tens of storage systems. For smaller clusters, it is possible to reduce the refresh periodicity to one (1) hour.

```
0 */2 * * * root /usr/bin/storcheck > /var/log/storcheck.log 2>&1
```

## 4.2 Enabling the Administration of StoreWay FDA and Optima1500 (NEC) Storage System

---

 **Important** This section only applies when installing for the first time.

---

**See** The *User's Guide* and *Maintenance Guide* specific to the StoreWay FDA or Optima1500 model that is being installed and configured.

---

The management of **FDA** and **Optima1500** storage arrays requires an interaction with the **iSM** server, (delivered on the CDs provided with the storage arrays). The Cluster management software installed on the cluster Management Node checks the FDA and Optima1500 management software status. Several options are available regarding the installation of this **iSM** server.

### The iSM server and CLI

These two components are mandatory for the integration of **FDA** and **Optima1500** monitoring in the cluster management framework. An **iSM** server is able to manage up to 32 storage arrays. The server and CLI components must be installed on the same system, for as long as the cluster contains less than 32 **FDA** and/or **Optima1500** systems.

### The iSM GUI client

The GUI client provides an easy to use graphical interface, which may be used to configure, and diagnose any problems, for FDA and Optima1500 systems. This component is not mandatory for the integration of the storage system in a cluster management framework.

- 
- Notes**
- The Storage Manager **GUI** client can only be installed on Windows.
  - The external Windows station must have access to the host installed with the **iSM** server.
- 

The Linux **rdesktop** command can be used to provide access to the GUI from the cluster Management Node.

### FDA and Optima1500 Storage System Management prerequisites

- A laptop is available and is connected to the maintenance port (MNT) using an Ethernet cross cable. Alternatively, a maintenance port of the storage system is connected to a Windows station.
- The electronic license details are available. These have to be entered during the initialisation process.
- Knowledge of installing and configuring **FDA** and **Optima1500** storage systems.
- The User manuals for this storage system should be available.
- The storage system name must be the same as in the disk array table for the **ClusterDB** and for the **iSM** server.

- The iSM user name and password have to have been transferred to the respective `necadmin` and `necpasswd` fields in the `/etc/storageadmin/nec_admin.conf` file.
- The addresses predefined in the **ClusterDB** for the management ports. These may be retrieved using the `storstat` command.

## 4.2.1 Installing and Configuring iSM server on a Linux system

On Linux, the `disk_array` table in the **ClusterDB** contains the `mgmt_node_id` field which is a foreign key in the **Node** table corresponding to the node installed with the iSM server (generally the Cluster Management Node).

1. Install the RPMs.

```
rpm -iv ISMSMC.RPM ISMSVR.RPM
```

- The **ISMSMC.RPM** is located on the *StoreWay iSM Integration Base CDROM*.
- The **ISMSVR.RPM** is located on the *StoreWay iSM Storage Manager CDROM*.

2. **iSM** Configuration.

- a. Copy the `/etc/iSMsvr/iSMsvr.sample` file into the `/etc/iSMsvr/iSMsvr.conf` file. Add the lines that define the disk arrays to be managed, using the syntax shown in the example below:

```
# 3fda1500
# Two IP addresses are defined
diskarray1 =(
ip =(172.17.0.200, 172.17.0.201)
)
# 4fda2500
# Two IP addresses are defined
diskarray2 =(
ip =(172.17.0.210, 172.17.0.211)
)
```

- b. Add the following line in the client section after the default line for `login1` in the `iSMsvr.conf` file:

```
login2 = (<necadmin>, <necpassword>, L3)
```

Note that the `<necadmin>` and the `<necpassword>` values must be consistent with the corresponding fields in the `/etc/storageadmin/nec_admin.conf` file. Default values are `admin` and `password` respectively.

- c. Then restart the **iSM** manager service:

```
/etc/init.d/iSMsvr restart
```

3. **CLI** Configuration.

- a. Copy the `/etc/iSMSMC/iSMSM.sample` file into the `/etc/iSMSM/iSMSM.conf` file.

- b. Restart the CLI manager service:

```
/etc/init.d/iSMSMC restart
```



## Enabling ssh access from the Management Node on a Linux System

---

**Note** This part of the process is only required when the iSM server is installed on a system other than the Management Node. There is no need to enable **ssh** access if the NEC software is located locally on the Management Node. If this is the case, skip this paragraph.

---

**ssh** is used by the management application to monitor the storage systems. **ssh** must be enabled so that storage system management tools operate correctly on the cluster Management Node.

Distribute **RSA** keys to enable password-less connections from the cluster Management Node:

1. Log on as root on the cluster Management Node and generate asymmetric **RSA** keys.
2. Go to the directory where the RSA keys are stored. Usually, it is "**~/ssh**". You should find **id\_rsa** and **id\_rsa.pub** files. The **.pub** file must be appended to the **authorized\_keys** file on the Linux iSM system. The **authorized\_keys** file defined in the **/etc/sshd\_config** file, (by default: **~/ssh/authorized\_keys**) must be used.
3. If no key has been generated, generate a key with the **ssh-keygen** command

```
ssh-keygen -b 1024 -t rsa
```



**Important** The default directory should be accepted. This command will request a passphrase to retrieve the password. Do not use this function; press the return key twice to ignore the request.

---

4. The public key for the iSM Linux system should be copied with **ssh**:

```
scp id_rsa.pub <administrator>@<LinuxISMhost>:~
```

< **LinuxISMhost** > can be a host name or an IP address. Replace <**administrator**> with the existing administrator login details.

5. Connect to the Linux system iSM:

```
ssh <administrator>@<LinuxISMhost>
```

6. Do not destroy the **~/ssh/authorized\_keys** file. Run:

```
mkdir -p .ssh
cat id_rsa.pub >> .ssh/authorized_keys
rm id_rsa.pub
```

**Note** If necessary, repeat this operation for other pairs of Linux and iSM users.

---

## 4.2.2 Configuring iSM Access Information from the Management Node

1. Obtain the Linux or Windows host user account, and the iSM client user and password which have been defined. All the FDA and Optima1500 arrays should be manageable using a single login/password.
2. Edit the `/etc/storageadmin/nec_admin.conf` file, and set the correct values for the parameters:

```
# On Linux iSMpath="/opt/iSMSMC/bin/iSMcmd"  
# On Windows iSMpath="/cygdrive/c/Program\  
Files/FDA/iSMSM_CMD/bin/iSMcmd"  
iSMpath = /opt/iSMSMC/bin/iSMcmd  
# iSMpath="/cygdrive/c/Program\  
Files/FDA/iSMSM_CMD/bin/iSMcmd"  
# NEC iStorage Manager host Administrator  
hostadm = administrator  
# NEC iStorage Manager administrator login  
necadmin = admin  
# NEC iStorage Manager administrator password  
necpasswd = password
```

## 4.2.3 Initializing the FDA or Optima1500 Storage System

1. Initialise the storage system using the maintenance port (MNT). The initial setting must be done through the Ethernet maintenance port (MNT), using the Internet Explorer browser. Refer to the documentation provided with the storage system to perform the initial configuration.



**Important** The IP addresses of the Ethernet management (LAN) ports must be set according to the values predefined in the ClusterDB.

```
storstat -d -n <nec_name> -i -H
```

2. Carry out the following post configuration operations using the iSM GUI. Start the iSM GUI and verify that the storage system has been discovered. Make the following settings:
  - Set a storage system name which is the same as the name already defined in the ClusterDB `disk_array` table.
  - Enable the **SNMP** traps, and send the traps to the cluster Management Node.

It is possible to connect to the server via the browser using one of the storage system Ethernet IP addresses if the iSM GUI is not available. Use the password 'C' to access the configuration menu.

**See** The *User's Guide* for the storage system for more information.

3. Check that end-to-end access is correctly setup for the cluster Management Node:

```
nec_admin -n <nec_name> -i <ip-address-of-the-iSMserver-host>  
-c getstatus -all
```

If the iSM server is installed on the Management Node, the local host IP address can be used (127.0.0.1).

## 4.3 Enabling the Administration of DataDirect Networks S2A (DDN) Storage Systems

### 4.3.1 Enabling Access from Management Node

Edit the `/etc/storageadmin/ddn_admin.conf` file to configure the singlet connection parameters.

```
# Port number used to connect to RCM API server of ddn  
port = 8008
```

```
# login used to connect to ddn  
login = admin
```

```
# Password used to connect to ddn  
password = password
```

The configuration file uses the factory defaults connection parameters for the S2A singlets. The `login` and `password` values may be changed.

### 4.3.2 Enabling Date and Time Control

If the extreme computing cluster includes DDN storage systems check, and if necessary update, the `/etc/cron.d/ddn_set_up_date_time.cron` file to modify regular time checks. Ensure that the default period (1 1 pm) is acceptable for your environment:

```
0 23 * * * root /usr/sbin/ddn_set_up_date_time -s all -f -l
```

This cron synchronizes times for DDN singlets daily.

---

**Note** If the configuration does not include DDN storage systems then the line above must be commented.

---

### 4.3.3 Enabling Event Log Archiving

The `syslog` messages generated by each DDN singlet are stored in the `/var/log/DDN` directory or in the `/varha/log/DDN` directory if the Management Node is configured for High Availability.

---

**Note** The log settings, for example, size of logs are configured by default. Should there be a need to change these sizes, edit the `/etc/logrotate.d/syslog-ng` file. See the `logrotate` man page for more details.

---

### 4.3.4 Enabling Management Access for Each DDN

1. List the storage systems as defined in the cluster management database:

```
storstat -a |grep DDN
```

This command returns the name of the DDNs recorded in the cluster management database. For example:

```
-----  
ddn0 |      DDN |      9500 |  WARNING |      |      RACK-A2 |  K  
No faulty subsystem registered !  
-----
```

The next operation must be done once for each DDN system.

2. Retrieve the addressing information:

```
storstat -d -n <ddn_name> -i -H
```

**Tip:** To simplify administrative tasks, Bull preloads the **ClusterDB** with the following conventions:

| DDN system name | IP name for singlet 1 | IP name for singlet 2 | Console name for singlet 1 | Console name for singlet 2 |
|-----------------|-----------------------|-----------------------|----------------------------|----------------------------|
| <ddn_name>      | <ddn_name>_1          | <ddn_name>_2          | <ddn_name>_1s              | <ddn_name>_2s              |

IP names and associated IP address are automatically generated in the `/etc/hosts` directory. The conman consoles are automatically generated in the `/etc/conman.conf` file. Otherwise, refer to the **dbmConfig** command.

## 4.3.5 Initializing the DDN Storage System

Initialize each DDN storage system either from the cluster Management Node or from a laptop, as described below.

### 4.3.5.1 Initialization from a Cluster Management Node with an existing Serial Interface between the Management Node and the DDNs

Check that **ConMan** is properly configured to access the serial ports of each singlet:

```
conman <console name for the singlet>
```

When you hit return, a prompt should appear.

#### **ddn\_init** command

The **ddn\_init** command has to be run for each DDN. The target DDN system must be up and running, with 2 singlets operational. The serial network and the Ethernet network must be properly cabled and configured, with **ConMan** running correctly, to enable access to both serial and Ethernet ports, on each singlet.

- 
- Notes**
- The **ddn\_init** command is not mandatory to configure DDN storage units. The same configuration can be achieved via other means such as the use of DDN CLI (**ddn\_admin**) or DDN telnet facilities (to configure other items).
  - The **ddn\_init** command can only be run at the time of the first installation or if there is a demand to change the IP address for some reason.
  - Note2
- 

```
ddn_init -I <ddn_name>
```

This command performs the following operations:

- Set the IP address on the management ports
- Enable telnet and API services
- Set prompt
- Enable syslog service, messages directed to the Management Node, using a specific UDP port (514)
- Enable SNMP service, traps directed to the Management Node
- Set date and time
- Set common user and password on all singlets
- Activate SES on singlet 1
- Restart singlet
- Set self heal
- Set network gateway.

#### ddn\_init command tips

- The **ddn\_init** command should not be run on the DDN used by the cluster nodes, as this command restarts the DDN.
- Both singlets must be powered on, the serial access configured (conman and portserver) and the LAN must be connected and operational before using the **ddn\_init** command.
- Randomly, the DDN may have an abnormally long response time, leading to time-outs for the **ddn\_init** command. Thus, in case of error, try to execute the command again.
- The **ddn\_init** command is silent and takes time. Be sure to wait until it has completed.



#### WARNING

The **ddn\_init** command does not change the default tier mapping. It does not execute the **save** command when the configuration is completed.

### 4.3.5.2

#### Initialization from a Laptop without an existing Serial Interface between the Management Node and the DDNs

Connect to the laptop to each serial port and carry out the following operations:

- Set the IP address on the management ports according to the values of the ClusterDB.
- Enable telnet and API services.
- Set prompt.
- Configure and enable the syslog service and transmit the messages to the Cluster Management Node, using a specific UDP port (514).
- Configure and enable SNMP service, traps directed to the Cluster Management Node.
- Set date and time.
- Set admin user and password and all singlets, according to the values defined in **/etc/storageadmin/ddn\_admin.conf** file.
- Activate SES on singlet 1.
- Set the tier mapping mode.
- Enable the couplet mode.
- Activate cache coherency.
- Disable cache write back mode.
- Set self heal.
- Set network gateway.

- 
- Notes**
- The laptop has to be connected to each one of the 2 **DDN** serial ports in turn. This operation then has to be repeated for each DDN storage unit.
  - The administrator must explicitly turn on the 8 and 2 mode on DDN systems where dual parity is required. This operation is not performed by the **ddn\_init** command.
- 



**Important** SATA systems may require specific settings for disks. Consult technical support or refer to the *DDN User's Guide* for more information.  
When the default command has been performed on the system, it is recommended to restart the complete initialisation procedure.  
After a power down or a reboot, check the full configuration carefully.

---

Check that initialization is correct, that the network access is setup, and that there is no problem on the DDN systems:

```
ddn_admin -i <ip-name singlet 1> -c getinfo -o HW  
ddn_admin -i <ip-name singlet 2> -c getinfo -o HW
```

## 4.4 Enabling the Administration of Optima1250 (Xyratex) Storage Systems

---

 **Important** This section only applies when installing for the first time.

---

**Note** The *High Availability* solution does not apply to nodes that are connected to Optima1250 Storage Bays.

---

**See** The *StoreWay Optima1250 Quick Start Guide* for more details on the installation and configuration.

---

**StoreWay Master** is a web interface module embedded into the Optima1250 controllers.

It allows an Optima1250 storage system to be managed and monitored from a host running **StoreWay Master** locally using a web browser across the internet or an intranet.

There is no particular software which needs to be installed to manage an Optima1250 storage system.

### 4.4.1 Optima1250 Storage System Management Prerequisites

- If the initial setup was not done by manufacturing, a laptop should be available and connected to the Ethernet Port of the **Optima1250** storage system via an Ethernet cross cable.
- The **SNMP** and **syslogd** electronic licenses sent by e-mail should be available. The Global Licence is included in the standard product.
- The *StoreWay Optima1250 Quick Start Guide* specific to the storage system should be available.
- The addresses predefined in the **ClusterDB** must be the same as those set in **StoreWay Master** for the Optima1250. These may be retrieved using the **storstat -di** command.

### 4.4.2 Initializing the Optima1250 Storage System

1. The network settings of the Optima1250 storage system will need to be configured for the first start up of the **StoreWay Master** module, if this has not already been done by manufacturing.
  - Configure you LAPTOP with the local address 10.1.1.10
  - Connect it to the Ethernet Port of the Optima1250 storage system using an Ethernet cross cable
  - Insert the Software and manual disk, delivered with the Optima1250 storage system, into you CD drive. The autorun program will automatically start the navigation menu.
  - Select **Embedded StoreWay Master set up**

- Review the information on the screen and click the next button. The program searches the embedded master module using the addresses 10.1.1.5 and 10.1.1.6
- Use the embedded module MAC address for each controller whose network settings are being configured. The IP addresses of the Ethernet management (LAN) ports must be set according to the values predefined in the ClusterDB.
- Enter and confirm the new password and then click the configure button.

---

**See** The *StoreWay Optima1250 Quick Start Guide* for more information.

---

2. Once the network settings are configured, you can start **StoreWay Master** using a web browser by entering the explicit IP address assigned to the embedded StoreWay Master server followed by the port number (9292), for example **http://<IP\_address>:9292**
3. If the default settings are changed (user name =admin, password = password), then the user name and password settings in the **xradmin** and **xypasswd** fields of the **/etc/storageadmin/xyr\_admin.conf** file will have to be updated.
4. Configure **SNMP** using the **StoreWay Master** GUI, firstly select the **Settings** button and then the **SNMP** button. If this is the first time that SNMP has been set you will be asked for the paper licence details that are included with the Optima1250 storage system. Using the **SNMP** menu enter the IP address of the management station and deselect the information level box for this trap entry (leave the warning and error levels checked).
5. Check that end-to-end access has been correctly set up for the cluster Management Node using the command below:

```
xyr_admin -i <optima_1250_IP_address> -c getstatus -all
```



## 4.5 Enabling the Administration of EMC/Clariion (DGC) Storage Systems

### 4.5.1 Initial Configuration

**See** The appropriate *EMC CLARiiON CX3-Series* or *CX4-Series Setup Guide* delivered with the storage system for more details on the initial configuration. A Windows laptop and a RS232 cable will be required.

The initialization parameters are saved in the cluster database (`da_ethernet_port` table) and can be retrieved as follows:

1. Run the command below to see the **EMC/Clariion** storage system information defined in the cluster management database.

```
storstat -a | grep DGC
```

This command will list the **DGC** disk arrays to be configured on the cluster.

2. For each DGC storage system retrieve the IP addressing information by using the command below.

```
storstat -d -n <dgc_name> -i -H
```

3. For each Service Processor (SPA and SPB) of each **CX3** or **CX4** storage system set the IP configuration parameters for the:
  - IP address
  - Hostname (for SPA : `<dgc_name>_0`, for SPB : `<dgc_name>_1`)
  - Subnet Mask
  - Gateway
  - Peer IP address (IP address of the other SP of the same DGC disk array)

Once these settings have been made, the Service Processor will reboot and its IP interface will be available.

4. The **Java** and **Firefox** plugins are installed and linked by default, so that the http interface for the **EMC Navisphere Management Suite** can be used for the complementary configuration tasks.

Start the **Firefox** browser by running the command:

```
/usr/bin/firefox-32bits
```

### 4.5.2 Complementary Configuration Tasks for EMC/Clariion CX series storage devices

The disk array is configured via the **Navisphere Manager** interface in a web browser using the following URLs:

`http://<SPA-ip-address>` or `http://<SPB-ip-address>`

1. Set the disk array name by selecting the disk array and opening the properties tab.

2. Set the security parameters by selecting the disk array and then selecting the following option in the menu bar:

**Tools -> Security -> User Management**

Add a username and a role for the administrator.

3. Set the monitoring parameters as follows
  - a. Using the **Monitors** tab, create a Monitoring template with the following parameters:

**General** tab:

    - **Events** = General
    - **Event Severity** = Warning + Error + Critical
    - **Event Category** = Basic Array Feature Events

**SNMP** Tab:

    - **SNMP Management Host** = <IP address of the extreme computing Storage Management station>
    - **Community** = public
  - b. Using the **Monitors** tab, associate the new template to each Service Processor by selecting the **Monitor Using Template** option.

### 4.5.3 Complementary Configuration Tasks for EMC/CLARiiON AX4-5 storage devices

The disk array is configured via the **Navisphere Express** interface in a web browser using the following URLs:

<http://<SPA-ip-address>> or <http://<SPB-ip-address>>

1. Set the disk array name in the *Manage / Storage System* page
2. Set the security parameters in the *System / Settings / User Management* page:  
Add a username and a password for the administrator.
3. Set the monitoring parameters in the *System / Settings / Event Notification* page:  
Set *SNMP Trap Destination* = <IP address of the Management node>

### 4.5.4 Configuring the EMC/Clariion (DGC) Access Information from the Management Node

1. Install the **Navisphere CLI rpm** on the Administration Node.

---

**Note** This package is named **navicli.noarch.rpm** and is available on the *EMC CLARiiON Core Server Support* CD-ROM, which is delivered with an **EMC/Clariion** storage system.

---

2. Edit the `/etc/storageadmin/dgc_admin.conf` file, and set the correct values for the security parameters, including:
  - Navisphere CLI security options (for navisecli only)
  - The same user and password must be declared on each disk array by using the command below.

```
dgc_cli_security = -User <user> -Password <password> -Scope 0
```

## 4.6 Updating the ClusterDB with Storage Systems Information

1. For each storage system, run the command below.

```
storregister -u -n <disk_array_name>
```

As a result the **ClusterDB** should now be populated with details of disks, disk serial numbers, **WWPN** for host ports, and so on.

2. Check that the operation was successful by running the command below.

```
storstat -d -n <disk_array_name> -H
```

If the registration has been successful, all the information for the disks, manufacturer, model, serial number, and so on should be displayed.

3. Run the command below to update the monitoring services.

```
dbmConfig configure --restart -force
```

## 4.7 Storage Management Services

The purpose of this phase is to build, and distribute on the cluster nodes attached to fibre channel storage systems, a data file which contains a human readable description for each **WWPN**. This file is very similar to `/etc/hosts`. It is used by the `lsiocfg` command to display a textual description of each fibre channel port instead of a 16 digit **WWPN**.

1. Build a list of **WWPNs** on the management station:

```
lsiocfg -W > /etc/wwn
```

---

**Note** This file must be rebuilt if a singlet is changed, or if FC cables are switched, or if new LUNs are created.

---

2. Distribute the file on all the nodes connected to fibre channel systems (for example all the I/O nodes).

The file can be included in a **KSIS** patch of the Compute Nodes. The drawback is that there are changes to the **WWPN** then a new patch will have to be distributed on all the cluster nodes.

Another option is to copy the `/etc/wwn` file on the target nodes using the `pdcp` command:

```
pdcp -w <target_nodes> /etc/wwn /etc
```

## 4.8 Enabling the Administration of Brocade Fibre Channel Switches

### 4.8.1 Enabling Access from Management Node

The ClusterDB is preloaded with configuration information for **Brocade** switches. Refer to the `fc_switch` table. If this is not the case, then the information must be entered by the administrator.

Each Brocade switch must be configured with the correct IP/netmask/gateway address, switch name, login and password, in order to match the information in the ClusterDB.

Please refer to the Chapter on the switch configuration for more information. You can also refer to Brocade's documentation.

### 4.8.2 Updating the ClusterDB

When the Brocade switches have been initialized, they must be registered in the ClusterDB by running the following command from the Management Node for each switch:

```
fcsregister -n <fibrechannel switch name>
```

---

## Chapter 5. Configuring I/O Resources for the Cluster

The configuration of I/O resources for the cluster consists of two phases:

### Phase 1: The configuration of the storage systems

- Definition of the data volumes (LUNs) with an acceptable fault tolerance level (RAID)
- Configuration of the data access control rules for the I/O nodes
- Configuration of specific parameters (cache size, cache policy, watermarks, etc.)

### Phase 2: The configuration of coherent naming for I/O node resources

- Definition of logical names (aliases) for LUNs that maintain device names following reboots.

The I/O configuration can either be automatically deployed (with some exceptions) or configured manually.

## 5.1 Automatic Deployment of the I/O Configuration



**Important** Automatic deployment of the I/O configuration is not possible for Optima1250 and EMC/CLARiiON AX4-5 storage systems. These systems must be configured manually.

---

The automatic deployment of the storage configuration uses a *model* file, which describes the data volumes that have to be created, and how the nodes can access them.

---

**See** The **bullx cluster suite Administrator's Guide** for more detailed information about configuration models and the deployment process.

---

### 5.1.1 Storage Model Files

A template for the creation of a storage configuration model can be obtained with the following command:

```
stormodelctl -c showtemplate
```

This template contains declaration examples for storage systems supported from the different storage vendors. A model file is specific to storage systems of the same type from a specific vendor.

The model file contains the following information:

- The storage vendor name
- The list of storage system names to which the model is applicable
- Vendor-specific information (cache configuration, watermarks, etc.)
- Declaration of RAID groups (grouping disks in pools)
- Declaration of spare disks
- Declaration of LUNs
- Declaration of LUN access control groups and mappings of internal/external LUN numbers

- **LUSTRE** specific declarations for storage systems which use the **LUSTRE** global file system deployment.

---

**Note** With some versions of Fibre Channel adapter node drivers, the correct detection of the LUNs for a storage device port is dependent on the accessibility of a LUN numbered 0. It is recommended the Access Control groups for a storage device are configured so that the list of LUNs declared for each group always includes an external LUN that is numbered 0.

---

A model file is created by manual by editing the file, and its syntax is checked when the model is deployed to the storage systems.

Although there is no constraint about the location of storage model files, a good practice is to store them in the `/etc/storageadmin` directory of the Management Node.

---

 **Important** The Administrator should backup storage model files as model files may be reused later to reinstall a particular configuration.

---

## 5.1.2 Automatic Configuration of a Storage System

The automatic configuration of storage system using a model file requires that the storage devices declared in the model are initialized correctly and are accessible via their management interface.

---

 **Important** When a storage model is deployed any existing configuration details that are in place are overwritten. All previous data will be lost.

---

### Initial conditions

For some storage systems (**EMC/CLARiiON**), the LUNs can only be accessed using authorized Fibre Channel adapters (HBAs) for the hosts connected to the storage system. This access control is based on the Worldwide Names (**WWN**) of the FC adapters. So these WWN details must be collected and stored in the Cluster Database using the following command:

```
ioregister -a
```

The collection of I/O information may fail for those nodes which are not yet operational in the cluster. Check that it succeeded for the nodes referenced by the Mapping directives in the model file (i.e. for the nodes that are supposed to be connected to the storage system).

### Configuration process

1. Create or reuse a storage configuration model and copy it into the `/etc/storageadmin` directory on the Management node:

```
cd /etc/storageadmin
```

2. Apply the model to the storage systems:

```
stormodelctl -m <model_name> -c applymodel
```



### WARNING

This command is silent and long. Be certain to wait until the end.

To have better control when applying the model on a single system it is possible to use the verbose option, as below:

```
stormodelctl -m <model_name> -c applymodel -i <disk_array_name> -v
```

3. Check the status of formatting operations on the storage systems.

When the **applymodel** command has finished, the disk array proceeds to LUN formatting operations. Depending on the type of storage system, this operation can take a long time (several hours). The progress of the formatting phase can be checked periodically using the following command:

```
stormodelctl -m <model_name> -c checkformat
```

The message *'no formatting operation'* indicates that the formatting phase has finished and is OK.



### WARNING

Ensure that all formatting operations are completed on all storage systems before using these systems for other operations.

4. Once the storage systems have been fully configured, reboot all the nodes that are connected to them so that the storage systems and their resources can be detected.

---

**Note** The LUN Access control information (zoning) can be reconfigured, using the **stormodelctl -c applyzoning** option, once the configuration model has been deployed. The LUN configuration and all other parameters are preserved.

---

## 5.1.3 Automatic Deployment of the configuration of I/O resources for the nodes

---

**Note** All the storage systems connected to the nodes must have been configured, their LUNs formatted, and the nodes rebooted before this phase is carried out.

---

1. Check that each node is connected to the correct storage system.

Check the connection of each DDN storage system using the following command.

```
ddn_conchk -I <ddn_name> -f
```

**Note** This command can only be used if **Conman** is in place for the DDN storage systems.

---

Check that the LUNs are accessible for the storage systems connected to each node by using the command below:

```
lsiocfg -dv
```

2. Deploy the aliases for the I/O resources from the Management Node.

As a prerequisite **ssh** must have been configured “password-less” to allow the Management Node to run remote operations on the nodes connected to storage systems. Run the command below, using the model file created previously when the storage system was automatically configured:

```
stordepmap -m <model_name>
```



#### WARNING

This command is silent and long. Be sure to wait until the end.

This operation transmits configuration information to each node attached to the storage system defined in the specified model file. A check is made to ascertain which storage resources are accessible from each node compared with the LUNs defined in the model file for it. A symbolic link (alias) is then created for each disk resource that corresponds to a storage system LUN declared in the model file for the node.

3. Check aliases created for I/O resources.

Use the following command on each node to check that the aliases have been created correctly:

```
stormap -L
```

All device aliases listed must return an ‘up’ status.

#### Restoring a node

After restoring the system on a node, the aliases also have to be restored using the deployment command, below, from the Management Node:

```
stordepmap -m <model_name> -i <node_name>
```

## 5.2 Manual Configuration of I/O Resources



**Important** It is not recommended to configure the I/O resources manually except for those storage systems where automatic configuration is not supported i.e. Optima1250 and EMC/CLARiiON AX4-5.

### 5.2.1 Manual Configuration of Storage Systems

Please refer to the documentation provided with the storage system to understand how to use the storage vendor’s management tools. Most of the configuration operations can also be performed from the Management Node using the CLI management commands (**ddn\_admin**, **nec\_admin**, **dgc\_admin**, **xyr\_admin** commands) provided by the storage administration packages.

**See** The **bullx cluster suite Administrator’s Guide** for more information.



## 5.2.2 Manual Configuration of I/O resources for Nodes

**Note** All the storage systems connected to the nodes must have been configured, their LUNs formatted, and the nodes rebooted before this phase is carried out.

1. Check that each node is connected to the correct storage system.

Check the connection of each DDN storage system using the following command.

```
ddn_conchk -I <ddn_name> -f
```

**Note** This command can only be used if **ConMan** is in place for the DDN storage systems.

Check that the LUNs are accessible for the storage systems connected to each node by using the command below:

```
lsiocfg -dv
```

2. Create aliases from the Management Node without using a model file.

An alias must be created for each LUN of a storage system connected to a node. If I/O multipathing has been configured, ensure that all paths to all devices are in the *alive* state by using the **lsiocfg -x** command.

**If the node is NOT in a High-Availability pair:**

From the Management Node, run the command:

```
stordiskname -c -r <node_name>
```

Then run the command:

```
ssh root@<node_name> "stormap -c"
```

**If the node is in a High-Availability pair (node1,node2):**

From the Management Node run the command:

```
stordiskname -c -r <node1_name>,<node2_name>
```

Then run the command:

```
ssh root@<node1_name> "stormap -c"  
ssh root@<node2_name> "stormap -c"
```

3. Check the aliases created for the I/O resources.

Use the following command on each node to check that the aliases have been created correctly:

```
stormap -L
```

All device aliases listed must return an *'up'* status.


---

**Note** For some storage systems, not including FDA and DDN, the **stordiskname** command may return an error similar to the one below:

```
Error : -= This tool does not manage configuration where a given
UID appears more than once on the node = -
```

If this happens try running it with the **-m SCSI\_ID** option.


---

 **Important** The **stordiskname** command builds a **/etc/storageadmin/disknaming.conf** file which contains, among other things, details of symbolic link names, the LUN UIDs and the WWPN access for the LUN's. Only the **stordiskname** command can create or modify the node specific information in this file.

---

### Restoring a node

---

 **Important** The **disknaming.conf** file will be erased when redeploying the **ksis** reference image, or when the system is restored for a node. Therefore, the **stordiskname** command should be used with the **-r** option (remote) from the Management Node enabling backups and restorations of the **/etc/storageadmin/disknaming.conf** file to be managed automatically. This is highly recommended.

---

If the **-r** option is not used, the Administrator will have to manage the backup of the **/etc/storageadmin/disknaming.conf** file himself.

When used remotely (**-r** option) - immediately after a **ksis** image re-deployment, or a node system restoration - the **stordiskname** command must be used in **update** mode (**-u** option). This ensures that the LUNs are addressed by the same symbolic link names as used previously, and avoids having to configure the file system again.

The **stordiskname** command should be executed from the Management Node as shown below (possibly with the **-m SCSI\_ID** option, see *Note* above).

#### If the node is NOT in a High-Availability pair

```
stordiskname -u -r <node_name>
```

#### If the node is in a High-Availability pair

```
stordiskname -u -r <node1_name>,<node2_name>
```

The symbolic links (aliases) must be recreated on each node using the information contained within the **disknaming.conf** file newly created by **stordiskname**. To do this, run the **stormap** command as described previously:

```
ssh root@<node_name> "stormap -c"
```

---

## Chapter 6. Configuring the NIS and NFS File Systems

Three types of file systems are possible for sharing data and user accounts for **bullx cluster suite** clusters:

- **NIS** (Network Information Service) can be used so that user accounts on Login Nodes are available on the Compute Nodes.
- **NFS** (Network File System) can be used to share file systems in the home directory across all the nodes of the cluster.
- **Lustre** Parallel File System

This chapter describes how to configure the NIS and NFS file systems.


---

**See** The *Lustre Guide* for information on configuring **Lustre**.

---

### 6.1 Setting up NIS to share user accounts

---

 **Important** There is no need to use NIS on the Management Node for clusters which include dedicated I/O + LOGIN nodes.

---

#### 6.1.1 Configure NIS on the Login Node (NIS server)

1. Edit the `/etc/sysconfig/network` file and add a line for the **NISDOMAIN** definition .

```
NISDOMAIN=<DOMAIN>
```

Any domain name may be used for `<DOMAIN>`, however, this name should be the same on the Login node, which is acting as the NIS server, and on all the Compute Nodes (NIS clients).

2. Start the **ypserv** service

```
service ypserv start
```

3. Configure **ypserv** so that it starts automatically whenever the server is started.

```
chkconfig ypserv on
```

4. Initialize the **NIS** database.

```
/usr/lib64/yp/ypinit -m
```

---

**Note** When a new user account is created the YP database should be updated by using the command:  
`cd /var/yp`  
`make`

---

## 6.1.2 Configure NIS on the Compute or/and the I/O Nodes (NIS client)

1. Edit the `/etc/sysconfig/network` file and add a line for the NISDOMAIN definition.

```
NISDOMAIN=<DOMAIN>
```

Any domain name may be used for `<DOMAIN>`, however, this name should be the same on the Login node, which is acting as the NIS server, and on all the Compute or I/O Nodes (NIS clients).

2. Edit `/etc/yp.conf` and add a line to set the Login Node as the NIS domain server

```
domain <DOMAIN> server <login_node>
```

3. Modify the `/etc/nsswitch.conf` file so that `passwd`, `shadow` and `group` settings are used by NIS.

```
passwd: files nisplus nis
shadow: files nisplus nis
group: files nisplus nis
```

4. Connect to the NIS YP server.

```
service ypbind start
```

5. Configure the `ypbind` service so that it starts automatically whenever the server is restarted.

```
chkconfig ypbind on
```

---

**Note** The NIS status for the Compute or I/O Node can be verified by using the `ypcat hosts` command. This will return the list of hosts from the `/etc/hosts` file on the NIS server.

---

### NISDOMAIN definition on all Compute and I/O Nodes

The definition of the NISDOMAIN has to be added manually to the files that exist on all the Compute or I/O Nodes by using the command below.

```
pdsh -w cluster[x-y] 'echo NISDOMAIN=<DOMAIN> >>
/etc/sysconfig/network'
```

The `restart ypbind` service then has to be restarted so that the NIS domain is taken into account.

```
pdsh -w cluster[x-y] 'service ypbind restart'
```

## 6.2 Configuring NFS v3/v4 to share the /home\_nfs and /release directories

### 6.2.1 Preparing the LOGIN node (NFS server) for the NFSv3/v4 file system

Firstly, create a dedicated directory (mount point) for the NFS file system which is dedicated to 'home' usage. As the /home directory is reserved for local accounts, it is recommended that /home\_nfs is used as the dedicated 'home' directory for the NFS file system.

#### Recommendations

- Use dedicated devices for NFS file systems (one device for each file system that is exported).
- The `lsioctg -d` command will provide information about the devices which are available.
- Use the **LABEL** identifier for the devices.
- Use disks that are partitioned.



**Important** If a file system is created on a disk which is not partitioned, then mount cannot be used with the **LABEL** identifier. The disk device name (e.g. `/dev/sdx`) will have to be specified in the `/etc/fstab` file.

- Notes**
- The following instructions only apply if dedicated disks or storage arrays are being used for the NFS file system.
  - The following examples refer to configurations that include both **home\_nfs** and **release** directories. If the 'release' NFS file system has already been exported from the Management Node, ignore the operations that relate to the **release** directory in the list of operations below.

1. Create the directories that will be used to mount the physical devices:

#### NFSv3:

```
mkdir /home_nfs
mkdir /release
```

#### NFSv4:

```
mkdir /home_nfs
mkdir /home_nfs/release
```

2. Mount the physical devices:

#### NFSv3:

```
mount <home_nfs dedicated block device> /home_nfs
mount <release dedicated block device> /release
```

or, if labels have been applied to the file systems:

```
mount LABEL=<label for home_nfs dedicated block device> /home_nfs
mount LABEL=<label for release dedicated block device> /release
```

**NFSv4:**

```
mount <home_nfs dedicated block device> /home_nfs
mount <release dedicated block device> /home_nfs/release
```

or, if labels have been applied to the file systems:

```
mount LABEL=<label for home_nfs dedicated block device> /home_nfs
mount LABEL=<label for release dedicated block device>
/home_nfs/release
```

3. Edit the `/etc/fstab` file and add the following lines for the settings which are permanent:

**NFSv3:**

```
# these are physical devices (disks) dedicated to NFS usage
LABEL=release /release auto defaults 0 0
LABEL=home_nfs /home_nfs auto defaults 0 0
```

**NFSv4:**

```
# these are physical devices (disks) dedicated to NFS usage
LABEL=release /home_nfs/release auto defaults 0 0
LABEL=home_nfs /home_nfs auto defaults 0 0
```

4. Use the `adduser` command with the `-d` flag to set the `/home_nfs` directory as the home directory for new user accounts.

```
adduser -d /home_nfs/<NFS user login> <NFS user_login>
```

## 6.2.2 Setup for NFS v3/v4 file systems

### 6.2.2.1 Configuring the NFSv3/v4 Server

1. Edit the `/etc/exports` file and add the directories that are to be exported.

**NFSv3:**

```
/release *(ro, sync)
/home_nfs *(rw, sync)
```

**NFSv4:**

```
/home_nfs *(rw, sync, fsid=0)
/home_nfs/release *(ro, sync, nohide)
```

2. Restart the NFS service

**NFSv3 and NFSv4:**

```
service nfs restart
```

3. Configure the **NFS** service so that it is automatically started whenever the server is restarted.

**NFSv3 and NFSv4:**

```
chkconfig nfs on
```

---

**Note** Whenever the **NFS** file systems configuration is changed (**/etc/exports** modified), then the **exportfs** command is used to configure the **NFS** services with the new configuration.

---

**NFSv3 and NFSv4:**

```
exportfs -r  
exportfs -f
```

**NFSv4 only:**

Edit the **/etc/idmapd.conf** file and modify the Mapping entries to:

```
[Mapping]  
  
Nobody-User = nfsnobody  
Nobody-Group = nfsnobody
```

## 6.2.2.2 Configuring the NFSv3/v4 Client

1. Create the directories that will be used to mount the **NFS** file systems.

```
mkdir /release  
mkdir /home_nfs
```

2. Edit the **/etc/fstab** file and add the **NFSv3** and **NFSv4** file systems as below:

**NFSv3:**

```
<nfs server>:/release /release nfs defaults 0 0  
<nfs server>:/home_nfs /home_nfs nfs defaults 0 0
```

**NFSv4:**

```
<nfs server>:/ /home_nfs nfs4 defaults 0 0  
<nfs server>:/release /release nfs4 defaults 0 0
```

3. Mount the **NFS** file systems.

```
mount /release  
mount /home_nfs
```





---

## Chapter 7. Installing Intel Tools and Applications

This chapter describes how to install Intel compilers and tools. Intel<sup>®</sup> Math Kernel Library and the Intel Debugger (IDB) are supplied with Intel Professional Edition for Linux version 11 Compilers.

---

**See** Intel compilers require that the Intel<sup>®</sup> License Manager for FLEXlm is in place. See the **INSTALL.txt** file provided by Intel<sup>®</sup> for more details regarding the installation of the Intel<sup>®</sup> License Manager for FLEXlm. See the Licensing chapter in the *Software Release Bulletin* for more information on FLEXlm.

---

### 7.1 Installing Intel Compilers with MKL and IDB

Follow the installation routine below to install the Intel<sup>®</sup> C++ and the Fortran compilers, together with the Intel<sup>®</sup> Math Kernel Library and the Intel<sup>®</sup> Debugger. These tools are installed on the node that contains the Login functionality (this may be a dedicated node or one which is combined with the I/O and/or Management functionalities).

---

**Note** Compilers and tools must be installed on each Login Node separately.

---

1. Install the Intel Compilers (Fortran, C/C++) on the Login Node.
  2. Install the Intel MKL on the Login Node.
  3. Install the Intel Debugger (IDB) on the Login Node.
- 

**See** The **INSTALL.txt** file provided by Intel for more details regarding the installation of the Compilers, MKL and IDB.

---

4. Export the `/opt/intel` directory via NFS and mount it on the Compute or Extended Compute nodes.
- 

### 7.2 Intel Trace Analyzer and Collector Tool

Intel Trace Analyzer and Collector is supplied directly by Intel to the customer. The Intel Trace Tool uses the FlexLM license scheme. The recommended path for installation is `/opt/intel/itac/<rel number 1>`.

1. Install the Intel Trace Tool on the Login Node.
  2. Export the `/opt/intel` directory via NFS and mount it on the Compute or Extended Compute nodes.
- 

**See** The **INSTALL.txt** file provided by Intel, and the documentation available from the Intel site, for more details regarding the installation of Intel Trace Analyzer and Collector.

---

## 7.3 Intel VTune Performance Analyzer for Linux

For more details about the installation procedure, see the *Intel® VTune Performance Analyzer for Linux Installation Guide* on the internet site:

<http://www.intel.com/software/products/cluster>

---

**Note** If Intel® VTune Performance Analyzer for Linux is to be installed on the cluster, the HPC Toolkit (XTOOLKIT) product must be installed - see Chapter 3 in this manual.

---

## 7.4 Intel Runtime Libraries

---

 **Important** This section only applies to clusters where Intel Compilers are NOT installed.

---

Intel version 11.1 runtime libraries are included with Intel Compiler Suite version 11.1 media (a **tgz** file with a **.sh** installation script) and must be installed on all nodes (LOGIN, COMPUTE and COMPUTEX) which will not have the **version 11.1** compilers installed.

**BEFORE** the Intel version 11.1 runtime libraries are installed, remove the version 11.0.69 Runtime libraries, previously installed, from all nodes by running the command below:

```
# yum remove intelruntime-11.0.069-Bull.1
```

---

**Note** There is no need to recompile programs compiled with earlier Intel compiler version, as forward compatibility is guaranteed by Intel.

---

The `/opt/intelruntime/<version>` path should be added to the `LD_LIBRARY_PATH` environment variable in the shell configuration file.

If a different version of an Intel compiler is used, then its runtime libraries have to be installed on the nodes without the compilers, in order to ensure coherency, and the path in the `LD_LIBRARY_PATH` variable modified to include the new version reference.

---

## Chapter 8. Configuring Switches and Cards

This chapter describes how to configure **bullx cluster suite** switches and cards.

### 8.1 Configuring Ethernet Switches

The Ethernet switches are configured automatically using the ClusterDB database information and the configuration file- see section 8.1.5 *Ethernet Switches Configuration File*.

#### Prerequisites

- The Management Node must be installed. In particular, the Ethernet interface of the Administration Network and its alias must be configured and the **netdisco** package installed.
- The **ClusterDB** database must be preloaded and reachable.
- **CISCO** switches must remain as configured initially (factory settings). **Foundry Network** switches must have the default IP address preinstalled (see section 8.1.6 Ethernet Switches Initial Configuration)

#### 8.1.1 Ethernet Installation scripts

The tool is supplied in the form of a RPM package (**ethswitch-tools1.0-0.Bull.noarch.rpm**) on the Cluster Management CD. It should be installed on the Management Node.

This package includes the following scripts:

**/usr/sbin/swtAdmin**: The main script used to install switches

**/usr/sbin/swtConfig**: A script that enables configuration commands to be run on the switches.

Also, the package includes the **/usr/lib/clustmngt/ethswitch-tools** directory which contains the following directories:

**bin** Perl scripts, called by the **swtAdmin** main script.

**lib** The libraries required to execute the scripts.

**data** The configuration file and DTD files.

## 8.1.2 swtAdmin Command Option Details

```
/usr/sbin/swtAdmin auto|step-by-step|generate|preinstall|
netdisco|mac-update|install|save|clear
[--switch_number <number of new switches> ]
[--netaddress <network ip for temporary config.> ]
[--netmask <netmask for temporary configuration> ]
[--network <admin|backbone> ]
[--first <device name to start netdisco> ]
[--dbname <database name> ]
[--logfile <logfile name> ]
[--verbose ] [--help ]
```

### Example

```
/usr/sbin/swtAdmin auto --switch_number 4 --network backbone
```

### Actions

|                     |                                                                                                                   |
|---------------------|-------------------------------------------------------------------------------------------------------------------|
| <b>generate</b>     | Generate configuration files                                                                                      |
| <b>preinstall</b>   | Copy configuration files in the <b>/ftpboot</b> and restart <b>DHCPD</b> for the pre-installation of the switches |
| <b>netdisco</b>     | Run <b>netdisco</b> in order to discover new switches                                                             |
| <b>mac-update</b>   | Update database with the MAC address of the new switches                                                          |
| <b>install</b>      | Install new switches                                                                                              |
| <b>save</b>         | Save the configuration of the new switches                                                                        |
| <b>auto</b>         | Full configure and installation of switches                                                                       |
| <b>step-by-step</b> | Interactive configuration and installation of switches                                                            |
| <b>clear</b>        | Delete temporary configuration files                                                                              |

### Options

|                      |                                                                            |
|----------------------|----------------------------------------------------------------------------|
| <b>help</b>          | Display this message                                                       |
| <b>dbname</b>        | Specifies the name of the database (default value: ClusterDB )             |
| <b>verbose</b>       | Debug mode                                                                 |
| <b>logfile</b>       | Specifies the <b>logfile</b> name (default <b>/var/log/switchcfg.log</b> ) |
| <b>switch_number</b> | Number of switches to install (default 1)                                  |
| <b>first</b>         | Specifies the IP address or name of device to start <b>netdisco</b>        |
| <b>netaddress</b>    | Specifies the network IP to use for the pre-install configuration          |
| <b>netmask</b>       | Specifies the netmask to use for the pre-install configuration             |
| <b>network</b>       | Specifies the type of network to be installed, admin or backbone           |

## 8.1.3 Automatic Installation and Configuration of the Ethernet Switches

The Ethernet switches can be configured automatically by running the command:

```
swtAdmin auto
```

All the steps (1–6), below, in the *Ethernet Switch Configuration Procedure* are executed in order, with no user interaction. If the automatic installation fails at any stage, you will only need to execute the steps which remain (including the one that failed).

Alternatively, the switches can be installed and configured interactively by using the command below:

```
swtAdmin step-by-step --switch_number <number_of_new_switches>
```

All the installation and configuration steps (1-6) are executed in order, but the user is asked to continue after each one.

## 8.1.4 Ethernet Switch Configuration Procedure

### 1. Generating Configuration Files

There are two kinds of configuration files: (1) files for the temporary configuration of the network and DHCPD services on the Service Node and (2) configuration files for the switches.

The switch configuration files are generated by running the command:

```
swtAdmin generate [--dbname <database name> ]
                  [--netaddress <network ip for temporary config.> ]
                  [--netmask <netmask for temporary configuration> ]
                  [--network <admin|backbone> ]
                  [--logfile <logfile name> ]
                  [--verbose ] [--help ]
```

While this command is being carried out the following message will appear.

```
-----
Generate configuration files
/tmp/CfgSwitches/eswu0c1-config
/tmp/CfgSwitches/eswulc0-config
/tmp/CfgSwitches/eswulc1-config
Temporary configuration files will start
with 192.168.101.1 ip address (255.255.255.0 netmask)
-----
```

### 2. Pre-installation of switches

At this stage, the following actions are carried out:

- Temporary configuration of the **eth0** network interface aliases and reconfiguration of the DHCPD service on the Service Node
- The configuration files are copied to the **/tftpboot/** directory
- The **DHCP** service is reconfigured and restarted

These actions are carried out by running the command:

```
swtAdmin preinstall [--dbname <database name> ]
                   [--network <admin|backbone> ]
                   [--logfile <logfile name> ]
                   [--verbose ] [--help ]
```

While this command is being carried out the following message will appear.

```
-----
Pre-installation of switches
copy configuration files in /tftpboot/ directory
WARNING: we are looking for uninstalled switches. Please wait ...
Pre-installed X new switches.
-----
```

---

**Note** After this step has finished, the switches will use the temporary configuration.

---

### 3. Discovering new switches on the network

If the cluster includes more than one switch, the **netdisco** application runs automatically in order to discover the network topology.

This is carried out by running the command:

```
swtAdmin netdisco [--first <device name to start netdisco> ]
                  [--network <admin|backbone> ]
                  [--dbname <database name> ]
                  [--logfile <logfile name> ]
                  [--verbose ] [--help ]
```

While this command is being carried out a message similar to the one below will appear.

```
-----
Discover new switches on the network
clear netdisco database
network discovering by netdisco application starting from
192.168.101.5 ip
WARNING: not all new switches has been discovered, retry ...
netdisco discovered X new devices.
-----
```

#### 4. Updating MAC address in the eth\_switch table

When the topology has been discovered it is compared with the database topology. If there are no conflicts, the corresponding MAC addresses of switches are updated in the **eth\_switch** table of the database. This is done by running the command:

```
swtAdmin mac-update [--dbname <database name> ]
                   [--logfile <logfile name> ]
                   [--verbose ] [--help ]
```

The following message will appear:

```
-----
Update MAC address in the eth_switch table
Updating mac address values in clusterdb database ...
-----
```

#### 5. Restarting Switches and final Installation Configuration

At this step, all the switches are restarted and their final configuration is implemented by **TFTP** according to the parameters in the **DHCP** configuration file. The **DHCP** configuration file is regenerated and will now include the MAC addresses of the switches, obtained during the previous step.

This is carried out by running the command:

```
swtAdmin install [--dbname <database name> ]
                 [--network <admin|backbone> ]
                 [--logfile <logfile name> ]
                 [--verbose ] [--help ]
```

This will display a message similar to that below:

```
-----
Final install and restart dhcp service
stop the dhcpd service
Shutting down dhcpd: [ OK ]
Installing switches ...
installing eswulc0 switch (192.168.101.5 fake ip)
installing eswu0c0 switch (192.168.101.4 fake ip)
installing eswulc1 switch (192.168.101.3 fake ip)
installing eswu0c1 switch (192.168.101.2 fake ip)
installed eswulc0 switch
installed eswu0c0 switch
installed eswulc1 switch
installed eswu0c1 switch
switches installed.
dbmConfig configure --service sysdhcpd --force --nodeps --dbname
clusterdb
-----
```

---

```
Tue Oct 16 12:48:33 2007 NOTICE: Begin synchro for sysdhcpd
Shutting down dhcpd: [FAILED]
Starting dhcpd: [ OK ]
Tue Oct 16 12:48:34 2007 NOTICE: End synchro for sysdhcpd
```

---

## 6. Delete the temporary configuration files

```
swtAdmin clear
```

## 7. Save the switches configuration

Finally, when the switches have been installed, the configuration parameters will be stored locally in their memory and also sent by TFTP to the Management Node `/tftpboot` directory.

This is carried out by running the command:

```
swtAdmin save [--dbname <database name> ]
              [--logfile <logfile name> ]
              [--verbose ] [--help ]
```

This will display a message similar to that below:

---

```
Save configuration of switches
Saving switches configuration ...
saving configuration of eswu0c0 switch
saving configuration of eswu0c1 switch
saving configuration of eswulc1 switch
saving configuration of eswulc0 switch
saved configuration of eswu0c0 switch
saved configuration of eswu0c1 switch
saved configuration of eswulc1 switch
saved configuration of eswulc0 switch
save done.
```

---

## 8. Checking the configuration of a switch

The configuration of a switch is displayed by running the command:

```
swtConfig status --name <name_of_switch>
```

### 8.1.5 Ethernet Switches Configuration File

This file describes the parameters used to generate the switches configuration file.

A configuration file is supplied with the package as `/usr/lib/clustmngt/ethswitch-tools/data/cluster-network.xml`. The file structure is defined by `/usr/lib/clustmngt/ethswitch-tools/data/cluster-network.dtd` file.

The file contains the following parameters:

---

```
<!DOCTYPE cluster-network SYSTEM "cluster-network.dtd">
<cluster-network>
  <mode type="any">
    <login acl="yes" />
    <netadmin name="admin" />
    <vlan id="1" type="admin" dhcp="yes" svi="yes" />
    <mac-address logger="yes" />
    <logging start="yes" level="warnings" facility="local0" />
    <ntp start="yes" />
  </mode>
</cluster-network>
```

---

It specifies that:

- Only the workstations of the administration network are allowed to connect to the switches
- **DHCP** requests are forwarded
- The Management IP address is configured
- Log warnings are sent to the node service **syslog** server
- The switches system clock is synchronized with the **NTP** server for the node

For clusters configured with **VLAN** (Virtual Local Area Network,) or with the virtual router configuration, additional parameters must be defined using the `/usr/lib/clustmngt/ethswitch-tools/bin/config` script.

## 8.1.6 Ethernet Switches Initial Configuration

### 8.1.6.1 CISCO Switches

CISCO switches must be reset to the factory settings. This is done manually.

#### 1. Hardware reinitialization

Hold down the mode button located on the left side of the front panel, as you reconnect the power cable to the switch.

For **Catalyst 2940, 2950** Series switches, release the Mode button after approximately 5 seconds when the Status (**STAT**) LED goes out. When you release the Mode button, the **SYST LED** blinks amber.

For **Catalyst 2960, 2970** Series switches, release the Mode button when the **SYST LED** blinks amber and then turns solid green. When you release the Mode button, the **SYST LED** blinks green.

For **Catalyst 3560, 3750** Series switches, release the Mode button after approximately 15 seconds when the **SYST LED** turns solid green. When you release the Mode button, the **SYST LED** blinks green.

#### 2. From a serial or Ethernet connection

Enter the following commands:

```
switch>enable
```

Enter the password [admin] when requested

```
switch#delete flash:/config.text
```

Answer the default questions (ENTER)

```
switch#reload
```

Confirm without saving (ENTER).

Ignore the question *"Would you like to enter the initial configuration dialog? [yes/no]"* and disconnect.



## 8.1.6.2

### Foundry Network Switches

Foundry Network switches must be configured with the IP address: 192.168.1.200/24.

#### 1. Erase the configuration

From a serial or Ethernet connection enter the following commands:

```
switch>enable
```

Enter the password [admin] when requested

```
switch#erase startup-config
```

Answer the default questions (ENTER)

```
switch#reload
```

Confirm without saving (ENTER).

#### 2. Configure the 192.168.1.200/24 IP address

```
FLS648 Switch>enable
No password has been assigned yet...
FLS648 Switch#configure terminal
FLS648 Switch(config)#
```

a. on FastIron **FLS624** or **FLS648** models:

```
FLS648 Switch(config)#ip address 192.168.1.200 255.255.255.0
FLS648 Switch(config)#end
FLS648 Switch#write mem
```

b. on BigIron **RX4**, **RX8** and **RX16** models:

```
RX Switch(config)#vlan 1
RX Switch(config-vlan-1)# router-interface ve 1
RX Switch(config-vlan-1)#interface ve 1
RX Switch(config-vif-1)#ip address 192.168.1.200 255.255.255.0
RX Switch(config-vif-1)# end
RX Switch# write mem
```

## 8.1.7

### Basic Manual Configuration

Please use this method when configuring the **Foundry Network** switches initially with the IP address 192.168.1.200/24 or for a temporary configuration of an Ethernet switch (**Cisco** or **Foundry**).

#### Pre-Requisites

Before an Ethernet switch can be configured ensure that the following information is available:

- The name of the switch
- The IP address of the switch
- The IP address of the Netmask
- Passwords for the console port and the enable mode. These must be consistent with the passwords stored in the **ClusterDB** database.

1. **Connect the Console port of the switch to the Linux machine**

Using a serial cable, connect a free serial port on a Linux machine to the CONSOLE port of the switch. Make a note of the serial port number, as this will be needed later.

2. **From the Linux machine establish a connection with the switch:**

- Connect as **root**.
- Open a terminal.
- In the **/etc/inittab** file, comment the **tty** lines that enable a connection via the serial port(s) ; these lines contain **ttyS0** and **ttyS1**:

```
# S0:2345:respawn:/sbin/agetty 115200 ttyS0
# S1:2345:respawn:/sbin/agetty 115200 ttyS1
```

Run the command:

```
kill -1 1
```

Connect using one of the commands below:

- If the serial cable connects using port 0, then run:

```
cu -s 9600 -l /dev/ttyS0
```

- If the serial cable connects using port 1, then run:

```
cu -s 9600 -l /dev/ttyS1
```

Enter 'no' to any questions which may appear until the following message, below, is displayed.

```
Connected.
Switch>
```

### 8.1.7.1 **Configuring a CISCO Switch**

1. Set the enable mode:

```
Switch>enable
```

2. Enter configuration mode:

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
```

3. Set the name of the switch in the form: *hostname <switch\_name>*. For example:

```
Switch(config)#hostname myswitch
myswitch(config)#
```

4. Enter the **SVI Vlan 1** interface configuration mode:

```
myswitch(config)#interface vlan 1
myswitch(config-if)#
```

5. Assign an IP address to the **SVI** of Vlan 1, in the form:  
*ip address <ip : a.b.c.d> <netmask : a.b.c.d>*

```
myswitch(config-if)#ip address 10.0.0.254 255.0.0.0
myswitch(config-if)#no shutdown
```

6. Exit the interface configuration:

```
myswitch(config-if)#exit
myswitch(config)#
```

7. Set the *portfast* mode as the default for the spanning tree:

```
myswitch(config)#spanning-tree portfast default
%Warning: this command enables portfast by default on all interfaces.
You should now disable portfast explicitly on switched ports leading
to hubs, switches and bridges as they may create temporary bridging
loops.
```

8. Set a password for the enable mode. For example:

```
myswitch(config)#enable password myswitch
```

9. Set a password for the console port:

```
myswitch(config)#line console 0
myswitch(config-line)#password admin
myswitch(config-line)#login
myswitch(config-line)#exit
```

10. Enable the telnet connections and set a password:

```
myswitch(config)#line vty 0 15
myswitch(config-line)#password admin
myswitch(config-line)#login
myswitch(config-line)#exit
```

11. Exit the configuration:

```
myswitch(config)#exit
```

12. Save the configuration in RAM:

```
myswitch#copy running-config startup-config
```

13. Update the switch boot file on the Management Node.

Run the following commands from the Management Node console:

```
touch /tftpboot/<switch_configure_file>
chmod ugo+w /tftpboot/< switch_configure_file>
```

---

**Note** The switch configure file name must include the switch name followed by '**-config**', for example, **myswitch-config**.

---

14. Save and exit the switch configuration from the switch prompt:

```
myswitch#copy running tftp
myswitch#exit
```

Enter the information requested for the switch. For the **tftp** server, indicate the IP address of the Service Node, which is generally the **tftp** server.

15. Disconnect the **CISCO** Switch.

Once the switch configuration has been saved and the Administrator has exited from the interface it will then be possible to disconnect the serial line which connects the switch to the **Linux** Management Node.

16. You can check the configuration as follows:

From the Management Node run the following command:

```
telnet 10.0.0.254
```

Enter the password when requested.

Set the enable mode

```
enable
```

Enter the password when requested.

Display the configuration with the show configuration command. An example is shown below:

```
#show configuration
```

```
-----
Using 2407 out of 65536 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname eswu0c1
!
enable secret 5 $1$ljvR$vnD1S/KOUD4tNmIm.zLTl/
!
no aaa new-model
ip subnet-zero
!
no file verify auto
spanning-tree mode pvst
spanning-tree portfast default
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
 interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface GigabitEthernet0/3
!
interface GigabitEthernet0/4
!
interface GigabitEthernet0/5
!
interface GigabitEthernet0/6
!
interface GigabitEthernet0/7
!
interface GigabitEthernet0/8
!
interface GigabitEthernet0/9
!
interface GigabitEthernet0/10
!
interface GigabitEthernet0/11
!
interface GigabitEthernet0/12
!
interface GigabitEthernet0/13
-----
```

```

!
interface GigabitEthernet0/14
!
interface GigabitEthernet0/15
!
interface GigabitEthernet0/16
!
interface GigabitEthernet0/17
!
interface GigabitEthernet0/18
!
interface GigabitEthernet0/19
!
interface GigabitEthernet0/20
!
interface GigabitEthernet0/21
!
interface GigabitEthernet0/22
!
interface GigabitEthernet0/23
!
interface GigabitEthernet0/24
!
interface Vlan1
 ip address 10.0.0.254 255.0.0.0
 no ip route-cache
!
ip http server
logging history warnings
logging trap warnings
logging facility local0
snmp-server community public RO
!
control-plane
!
line con 0
 password admin
 login
line vty 0 4
 password admin
 login
line vty 5 15
 password admin
 login
!
end

```

## 8.1.7.2 Configure a Foundry Networks Switch

The following procedure works for the **FastIron** and **BigIron** models

1. Set the enable mode:

```

FLS648 Switch>enable
No password has been assigned yet...
FLS648 Switch#

```

2. Enter the configuration mode:

```

FLS648 Switch#configure terminal
FLS648 Switch(config)#

```

3. Set the name of the switch in the form: *hostname <switch\_name>*. For example:

```

FLS648 Switch(config)#hostname myswitch
myswitch(config)#

```

4. Assign a management IP address, in the form:

a. on **FastIron FLS624** or **FLS648** models

- Assign IP address to the switch:  
*ip address <ip : a.b.c.d> <netmask : a.b.c.d>*

```
myswitch(config)#ip address 10.0.0.254 255.0.0.0
myswitch(config)#
```

b. on **BigIron RX4, RX8** and **RX16** models

- Enter the **Vlan 1** interface configuration mode:

```
myswitch(config)#vlan 1
myswitch(config-vlan-1)#
```

- Set the corresponding virtual interface (this allows the management IP address to be configured)

```
myswitch(config-vlan-1)#router-interface ve 1
```

- Enter the virtual interface **ve 1** interface configuration mode:

```
myswitch(config-vlan-1)#interface ve 1
myswitch(config-vif-1)#
```

- Assign an IP address to the virtual interface **ve 1**:  
*ip address <ip : a.b.c.d> <netmask : a.b.c.d>*

```
myswitch(config-vif-1)#ip address 10.0.0.254 255.0.0.0
```

- Exit the interface configuration:

```
myswitch(config-vif-1)#exit
myswitch(config)#
```

5. The *portfast* mode for the spanning tree is the default mode:

```
myswitch(config)# fast port-span
```

6. Set a password for the enable mode. For example:

```
myswitch(config)#enable password myswitch
```

7. Enable the **telnet** connections and set a password:

```
myswitch(config)# enable telnet password admin
```

8. Exit the configuration:

```
myswitch(config)#exit
```

9. Save the configuration in RAM:

```
myswitch#write memory
```

10. Update the switch boot file on the Management Node

11. Run the following commands from the Management Node console.

```
touch /tftpboot/<switch_configure_file>
chmod ugo+w /tftpboot/< switch_configure_file>
```

**Note** The switch configure file name must include the switch name followed by '**-confg**', for example, **myswitch-confg**.

12. Save and exit the switch configuration from the switch prompt.

```
myswitch#copy running tftp <tftp server> <switch_configure_file>
myswitch#exit
```

Indicate the IP address of the Service Node for the **tftp** server, this is generally the same as the **tftp** server.

13. Disconnect the Foundry Networks Switch.

Once the switch configuration has been saved and the Administrator has exited from the interface it will then be possible to disconnect the serial line which connects the switch to the Linux Management Node.

14. The configuration can be checked as follows:

From the Management Node run the following command:

```
telnet 10.0.0.254
```

Enter the password when requested.

Set the enable mode:

```
enable
```

Enter the password when requested.

Display the configuration with the **show configuration** command. Two examples are shown below:

```
Model FLS648:
telnet@myswitch#show configuration
```

```
-----
!
Startup-config data location is flash memory
!
Startup configuration:
!
ver 04.0.00T7e1
fan-threshold mp speed-3 50 90
!
module 1 fls-48-port-copper-base-module
!
hostname myswitch
ip address 10.0.0.254 255.0.0.0
!
end
-----
```

```
Model RX4 :
telnet@myswitch#show configuration
```

```
!
Startup-config data location is flash memory
!
Startup configuration:
!
ver V2.3.0dT143
module 1 rx-bi-10g-4-port
module 2 rx-bi-10g-4-port
module 3 rx-bi-1g-24-port-copper
!

vlan 1 name DEFAULT-VLAN
  router-interface ve 1
!
enable telnet password .....
enable super-user-password .....
logging facility local0
hostname myswitch
!
interface management 1
  ip address 209.157.22.254/24
!
interface ve 1
  ip address 172.17.18.210/16
!
end

telnet@myswitch#
```

## 8.1.8 Broadcom Switch Configuration for bullx blade systems

The configuration procedure for a **Broadcom** switch connected to **bullx blade systems** is as follows:

1. Start the **DHCPD** service by running the command:

```
dbmConfig configure --service sysdhcpd
```

2. Check that the **bullx** blade is switched on electrically.
3. Make a note of the **MAC** address listed in the `/var/log/message` file.
4. Run the following command to associate an **IP** address with the switch:

```
# dbmConfig configure --service sysdhcpd
```

---

 **Important** Do not try to configure a fixed IP address for the switch.

---

5. Connect to the switch by telnet (press **Enter** when the **Password** prompt appears):

```
#telnet myswitch
```

```
Trying 10.0.0.203...
Connected to 10.0.0.203 (10.0.0.203).
Escape character is '^]'.
(Broadcom FASTPATH Switching)
```



```
-----  
User:admin  
Password:  
(Broadcom FASTPATH Switching) >  
-----
```

6. Set the **enable** mode for the switch (press **Enter** when the **Password** prompt appears):

```
(Broadcom FASTPATH Switching) >enable
```

```
-----  
Password:  
-----
```

7. Define the name of the switch in the form: **hostname <switch\_name>**. For example:

```
Broadcom FASTPATH Switching) #hostname myswitch
```

```
-----  
(myswitch)#  
-----
```

8. Set the password for the **enable** mode (The password must be identical to the one already defined in the cluster database).

```
(myswitch) #enable passwd
```

```
-----  
Enter new password:*****  
Confirm new password:*****  
Password Changed!  
(myswitch) #  
-----
```

9. Enter configuration mode:

```
(myswitch) #configure  
(myswitch) (Config)#
```

10. Set a password for the **admin** user (The password must be identical to the one already defined in the Cluster Database).

```
(myswitch) (Config)#users passwd admin
```

```
-----  
Enter old password: <Enter>  
Enter new password:*****  
Confirm new password:*****  
Password Changed!  
(myswitch) (Config)#  
-----
```

11. Exit the configuration mode :

```
(myswitch) (config)#exit
```

```
-----  
(myswitch) #  
-----
```

12. Save the configuration details in the **RAM** of the switch:

```
(myswitch) #write memory
```

```
-----  
This operation may take a few minutes.  
Management interfaces will not be available during this time.  
Are you sure you want to save? (y/n) y  
Configuration Saved!  
(myswitch) #  
-----
```

13. Run the following commands from the Management Node console.

```
touch /tftpboot/<switch_configure_file>
chmod ugo+w /tftpboot/< switch_configure_file>
```

**Note** The `switch_configure_file` name must be the switch name followed by `-config`, for example, `myswitch-config`.

14. Save the switch configuration file on the Management Node:

```
(myswitch) #copy nvram:startup-config tftp://<tftp
server>/<switch_configure_file>
```

```
Mode..... TFTP
Set Server IP..... <tftp server>
Path..... ./
Filename.....
<switch_configure_file>
Data Type..... unknown
Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y
File transfer operation completed successfully.
```

15. The configuration can be checked as follows:

```
(myswitch) #show running-config
```

```
!Current Configuration:
!
!System Description "Broadcom FASTPATH Switching"
!System Software Version "5.2.0.4"
!System Up Time "0 days 23 hrs 51 mins 7 secs"
!Additional Packages FASTPATH QOS,FASTPATH Stacking
!Current SNTP Synchronized Time: Jun 13 14:33:35 200 UTC
!
set prompt "myswitch"
enable passwd encrypted
855c751745a6e4aafb716195c608374c221664257ff1e59156c2ce6847b870e51c482d
6d559ce3e730547d15f92fd8beb1ee8273aea54c4bdb5e8ee0eaaf36d3
network protocol dhcp
vlan database
exit
configure
stack
member 1 6
exit
slot 1/0 7
set slot power 1/0
no set slot disable 1/0
users passwd "admin" encrypted
855c751745a6e4aafb716195c608374c221664257ff1e59156c2ce6847b870e51c482d
6d559ce3e730547d15f92fd8beb1ee8273aea54c4bdb5e8ee0eaaf36d3
lineconfig
serial baudrate 115200
exit
spanning-tree
spanning-tree configuration name "08-00-38-35-90-C5"
!
exit
(myswitch) #
```

16. Close the switch connection:

```
(myswitch) #exit
(myswitch) >quit
```

```
Connection closed by foreign host.
#
```

## 8.2 Installing Additional Ethernet Boards

When installing additional Ethernet cards, the IP addresses of the Ethernet interfaces may end up by being misconfigured.

The Ethernet interfaces are named (**eth0**, **eth1**, **eth2**, etc.) according to the **PCI** bus order. So when a new Ethernet board is added, the Ethernet interface names may be changed if the PCI bus detects the new board before the existing on-board Ethernet interfaces (PCI bus detection is related to the position of the PCI slots).

To avoid misconfiguration problems of this type, before installing a new Ethernet board, you should:

1. Obtain the **MAC** addresses of the on-board Ethernet interfaces by using the **ifconfig eth0** and **ifconfig eth1** commands.
2. After the new Ethernet board has been installed, obtain the MAC addresses of the new Ethernet interfaces (obtain all the MAC addresses using the **ifconfig** command)
3. Edit each `/etc/sysconfig/network-scripts/ifcfg-ethX` file (ethX = eth0, eth1, etc.) and add an **HWADDR=<MAC\_ADDRESS>** attribute for each interface in each file, according to the Ethernet interface name and the MAC address obtained in Step 2, above.

## 8.3 Configuring InfiniBand Interconnects

---

**See** The *InfiniBand Guide* and the *System Release Bulletin* for more details regarding the **InfiniBand** RPMs and tools.

---

### **SLURM Resource Manager with InfiniBand stacks and Voltaire switches**

For more information on the **SLURM** Resource Manager used in conjunction with InfiniBand stacks and Voltaire switches, see the *Administrator's Guide*, *Application Developer's Guide* and the *SLURM Guide*.

### 8.3.1 Configuring Voltaire Devices

---

**See** For more detailed information on configuring Voltaire devices, updating the firmware, **Voltaire CLI** commands, and the management utilities available for the your Voltaire equipment refer to the documentation available from [www.voltaire.com](http://www.voltaire.com)

---

## 8.4 Configuring a Brocade Switch

1. Set the Ethernet IP address for the Brocade switch. Use a portable PC to connect the serial port of the switch.

- 
- Notes**
- The Real Value (IP address, name of the switch) to be used may be found in the cluster database (**FC\_SWITCH** table).
  - It is mandatory to use the serial cable provided by Brocade for this step.
- 

The initial configuration of the **Brocade** Fibre Channel Switch is made using a serial line (see *Silkworm 200E Hardware Reference Manual*).

2. Open a serial session:

```
cu -s 9600 -l /dev/ttyS0
```

```
login : admin
Password: password
switch:admin>
```

3. Initialize the IP configuration parameters (according to the addressing plan).
  - Check the current IP configuration:

```
switch:admin> ipAddrShow
```

```
Ethernet IP Address: aaa.bbb.ccc.ddd
Ethernet Subnetmask: xxx.yyy.zzz.ttt
Fibre Channel IP Address: none
Fibre Channel Subnetmask: none
Gateway Address: xxx.0.1.1
```

- Set the new IP configuration.

```
s3800:admin> ipAddrSet
```

```
Ethernet IP Address [aaa.bbb.ccc.ddd]: <new-ip-address>
Ethernet Subnetmask [xxx.yyy.zzz.ttt]: <new-subnet-mask>
Fibre Channel IP Address [none]:
Fibre Channel Subnetmask [none]:
Gateway Address [none]: <new-gateway-address>
```

4. Initialize the switch name, using the name defined in the ClusterDB.

```
switch:admin> switchName "<new_switch_name>"
```

Then:

```
exit
```

---

## Appendix A. Cluster Database Operations

### A.1 Saving and Reinstalling the Cluster DB data

Follow the procedure, described below, to save and to restore cluster database data for a **bullx cluster suite XR 5v3.1U3** clusters.

#### A.1.1 Saving the Data files

1. Login as the root user on the Management Node.
2. Enter:

```
su - postgres
```

3. Enter the following commands:

```
cd /var/lib/pgsql/backups
pg_dump -Fc -C -f/var/lib/pgsql/backups/<name_of_clusterdball.sav> clusterdb
pg_dump -Fc -a -f/var/lib/pgsql/backups/<name_of_clusterdbdata.sav> clusterdb
```

For example, **<name\_of\_clusterdbdata.sav>** might be `clusterdbdata-2009-1105.sav`.

4. Copy the two **.sav** files onto a non-formattable media outside of the cluster.

#### A.1.2 Reinstalling the Data files

1. Switch to **postgres**:

```
su - postgres
```

2. Go to the install directory:

```
cd /usr/lib/clustmgt/clusterdb/install
```

3. Remove the existing cluster DB:

```
dropdb clusterdb
```

---

**Note** If the *'database "clusterdb" is being accessed by other users'* error message appears, then stop and start the **postgresql** service.

---

4. Create a new cluster DB schema:

```
create_clusterdb.sh --nouser
```

5. Truncate the default values:

```
psql -U clusterdb -c "truncate config_status; truncate
config_candidate" clusterdb
```

6. Restore the **.sav** files saved previously

```
pg_restore -Fc --disable-triggers -d clusterdb  
/var/lib/pgsql/backups/<name_of_clusterdb_saved_file>
```

7. Go back to root by entering the exit command:

```
exit
```

## A.2 Initializing the Cluster Database using the preload file

Contact Bull Technical Support to obtain the Cluster DB preload file for **bullx cluster suite XR 5v3.1U3**, and then follow the procedure described in *section 3.2.5.1* in this manual for the initialization of the Cluster Database.

---

## Appendix B. Manual Installation of Software

### B.1 Bull Additional Software Options

Do not use the `installnfs` script to install the additional software options (**XIB** and/or **XLUSTRE** and/or **XTOOLKIT**) but install them manually as follows:

1. Mount **NFS** from the `/release` directory on the Management Node to the `/release` directory on the Service Node :

```
ssh <Service_Node>
mount -t nfs <Management_Node_IP>:/release /release
```

2. Install the optional **bullx cluster suite** software products required. The products to be installed for the cluster must be listed after the `-prod` option, as shown in the example below. In this example all the software products will be installed:

```
cd /release/XBAS5V3.1
./install -prod XIB XLUSTRE XTOOLKIT
```



**Important** Lustre must use dedicated service nodes for the I/O functions and NOT combined Login/IO service nodes. NFS can be used on both dedicated I/O service nodes and on combined Login/IO service nodes.

---

**See** The **bullx cluster suite** *Application Developer's Guide* for details on configuring and using HPC Toolkit.

---

### B.2 Custom Directories

If the `installnfs` command was NOT used to install any custom directories that are required, the process to install them manually is described below.

1. Copy the **RPMs** to be installed into the custom directories in `/release/CUSTOM/<my custom directory1>`, `/release/CUSTOM/<my custom directory2>`, etc.
2. Mount NFS from the `/release` directory on the Management Node to the `/release` directory on the Service Node :

```
ssh <Service node>
mount -t nfs <Management_Node_IP>:/release /release
```

3. Run the HPC installer to install the RPMs contained in the custom directory(ies) :

```
cd /release/XBAS5v3.1
./install -prod <my custom directory1> <my custom directory2> ...
```

## B.3 Bonus Directories

The **BONUS** packages must be installed manually. Search for the latest version of these RPMs in the sub-directories of the **/release** directory on the Management Node and then install them on the node by using the command:

```
yum localinstall xx* xx*
```



---

## Appendix C. Configuring Interconnect Interfaces

### C.1 The `config_ip` command

The interconnect interface description file is generated from the Management Node for each node by using the `config_ip` command.

The interfaces parameters are obtained from the `/etc/hosts` file on the Management Node.

Different options have to be set for the `config_ip` command according to the configuration of the cluster. The command options are shown below:

#### Usage

```
config_ip -n node[a-b,x] [-d device] [-m netmask] [-s suffix]
```

#### Command options

- `-h --help` print this message
- `-n <node>` node to update, pdsh form node[a-b,x] or ssh form root@node
- `-d <device>` ip device (default ib0)
- `-m <masque>` ip net mask (default 255.255.0.0)
- `-s <suffix>` name suffix in `/etc/hosts` (default -ic0)

In the example below, the command will create the configuration file `ifcfg-eth1` on the nodes `zeus8` to `zeus16`, to configure the `eth1` interface for these nodes, using the IP addresses listed in the `/etc/hosts` file for the `zeus8-ic1` to `zeus16-ic1` interfaces.

```
config_ip -n zeus[8-16] -d eth1 -m 255.255.0.0 -s -ic1
```

### C.2 Interface Description file

#### Ethernet Adapters

The **Ethernet** interconnect adapter will be identified by a logical number by using the format `eth[1/2/...]`, for example `eth1` and `eth2`. The IP properties (address, netmask, etc.) for the Ethernet adapter are configured using a description file named:  
`/etc/sysconfig/network-script/ifcfg-eth[1/2/...]`

#### InfiniBand Adapters

The **InfiniBand** interconnect adapter will be identified by a logical number by using the format `ib[0/1/2/...]`, for example `ib0` and `ib1`. The IP properties (address, netmask, etc.) for the InfiniBand adapter are configured using a description file named  
`/etc/sysconfig/network-script/ifcfg-ib[0/1/2/...]`

#### Example

An example of a description file is shown below for a node with an **InfiniBand** interface:

```
# cat /etc/sysconfig/network-scripts/ifcfg-ib0
```

---

```
DEVICE=ib0
ONBOOT=yes
BOOTPROTO=static
NETWORK=172.18.0.0
IPADDR=172.18.0.4
```

---

**Note** The value of last byte (octet) of the IPADDR address is always 1 more than the value for the machine number. For example, in the interface above the machine number is 3 (ns3) and so the last byte in the IPADDR setting is 4.

---

## C.2.1 Checking the interfaces

It is recommended that the configuration of the **Ethernet** and **InfiniBand** interfaces are verified to ensure that all the settings are OK. This is done by running the command below for **InfiniBand** interfaces:

```
pdsh -w node[n,m] cat /etc/sysconfig/network-scripts/ifcfg-ib[0/1/2...]
```

or the command below for **Ethernet** interfaces:

```
pdsh -w node[n,m] cat /etc/sysconfig/network-scripts/ifcfg-eth[1/2/3...]
```

Alternatively, to see the interface settings separately in groups for a set of nodes, use the commands below:

**Note** The examples below show the commands to be used for **InfiniBand** interfaces. For **Ethernet** interfaces replace the adapter interface identifier accordingly, for example replace **ifcfg-ib0** with **ifcfg-eth1**.

---

```
pdsh -w node[n,m] cat /etc/sysconfig/network-scripts/ifcfg-ib0 |grep IPADDR
```

```
pdsh -w node[n,m] cat /etc/sysconfig/network-scripts/ifcfg-ib0 |grep NETMASK
```

```
pdsh -w node[n,m] cat /etc/sysconfig/network-scripts/ifcfg-ib0 |grep BROADCAST
```

```
pdsh -w node[n,m] cat /etc/sysconfig/network-scripts/ifcfg-ib0 |grep NETWORK
```

```
pdsh -w node[n,m] cat /etc/sysconfig/network-scripts/ifcfg-ib0 |grep ONBOOT
```

Reconfigure those settings, where the values returned by these commands do not match what is required for the cluster.

## C.2.2 Starting the InfiniBand interfaces

The following commands are used to load all the modules, and to start all the **InfiniBand** interfaces, on each node:

```
/etc/init.d/openibd start
```

or

```
service openibd start
```

These commands have to be executed for each node individually.

---

**Note** A node reboot may be used to load the **InfiniBand** modules automatically.

---



---

## Appendix D. Binding Services to a Single Network

The `bind` attribute in the `/etc/xinetd.conf` file is used to bind a service to a specific IP address. This may be useful when a machine has two or more network interfaces; for example, a backbone computer which is part of a cluster administration network and is at the same time connected to the customer LAN through a separate interface. In this situation there may be backbone security concerns coupled with a desire to limit the service to the LAN.

For example, to bind the ftp service to the LAN, the `/etc/xinetd.conf` file has to be configured as follows:

### LAN network configuration

```
{
  id          = ftp-local
  wait       = no
  user       = root
  server     = /usr/sbin/in.ftpd
  server_args = -l
  instances  = 4
  nice      = 10
  only_from  = 0.0.0.0/0 #allows access to all clients
  bind      = xxx.xxx.xxx.xxx #local IP address
}
```

### Administration network configuration

```
{
  id          = ftp-admin
  socket_type = stream
  wait       = no
  user       = root
  server     = /usr/sbin/in.ftpd
  server_args = -l
  only_from  = xxx.yyy.0.0/16 #only for internal use
  bind      = xxx.yyy.0.99 #local IP address
}
```

---

**Note** The configurations above can be adapted and used by other services.

---



---

## Appendix E. PCI Slot Selection and Server Connectors

This appendix provides detailed information regarding the choice of PCI slots for high bandwidth PCI adapters. The configuration rules put forward ensure the best performance levels, without I/O conflicts, for most type of applications. System diagrams are included which may be used to configure the hardware connections.

The following topics are described:

- E.1 *How to Optimize I/O Performance*
- E.2 *Creating the list of Adapters*
- E.3 *Connections for R4xx Servers*

### E.1 How to Optimize I/O Performance

The I/O performance of a system may be limited by the software, and by the hardware. The I/O architecture of servers can lead to data flows from PCI slots being concentrated on a limited number of internal components, leading to bandwidth bottlenecks.

Thus, it is essential to look at the installation of PCI adapters, and slot selection, carefully, to reduce any limitations as much as is possible. One good practice is to avoid connecting bandwidth hungry adapters to the same PCI bus.

The following details should be ascertained, in order to ensure the highest possible performance for the adapter installation:

- Adapter characteristics, maximum theoretical performance and expected performance in the operational context.
- The I/O architecture of the server.

The following paragraphs cover these aspects, and provide recommendations for the installation of adapters for different servers. The process to follow is quite easy:

1. Create a list of the adapters to be installed, sorted from the highest bandwidth requirement to the lowest.
2. Place these adapters in each server using the priority list specific to the platform, as defined in this Appendix.

## E.2 Creating the list of Adapters

The first step is to make a list of all the adapters that will be installed on the system.

Then, if the I/O flow for the server is known (expected bandwidth from the Interconnect, bandwidth to the disks, etc.), it will be possible to estimate the bandwidth required from each adapter, and then sort the adapters according to the requirements of the operational environment.

If there is no information about real/expected I/O flows, the adapters should be sorted according to their theoretical limits. As both PCI Express adapters and PCI-X adapters may be connected, 2 tables are provided for the adapters supported by **BAS5 for Xeon**. These are sorted by throughput, giving the HBA slotting rank.

Adapter	Bandwidth
Fibre channel dual ports	800 MB/s (1) (2)
Fibre channel single ports	400 MB/s (2)
Gigabit Ethernet dual port	250 MB/s (1) (2)
Gigabit Ethernet single port	125 MB/s (2)
Ethernet 100 Mbps	12,5 MB/s

Table E-1. PCI-X Adapter Table

(1) If both channels are used. Otherwise, the adapter must be categorised as a single channel/port adapter

(2) Full duplex capability is not taken into account. Otherwise, double the value listed.

It may be possible that these values will be reduced, due to the characteristics of the equipment attached to the adapter. For example, a **U230 SCSI HBA** connected to a **U160** SCSI disk subsystem will not be able to provide more than 160 MB/s bandwidth.

Adapter	Bandwidth
Infiniband Voltaire 400 or 410-EX-D	1500 MB/s
Fibre channel dual ports	800 MB/s
Fibre channel single ports	400 MB/s (2)
Gigabit Ethernet dual port	250 MB/s
Gigabit Ethernet single port	125 MB/s (2)

Table E-2. PCI-Express Table

## E.3 Connections for R4xx Servers

The following paragraphs illustrate the I/O subsystem architecture for each family of R4xx servers.



### E.3.1 R421 Series – Compute Node

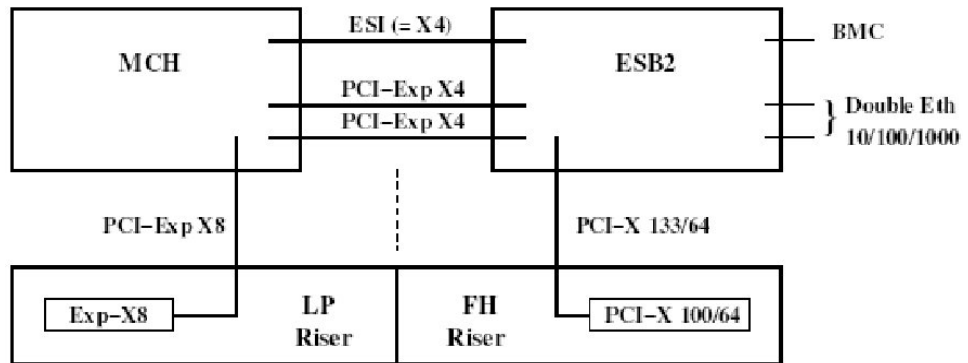


Figure E-1. R421 rear view of Riser architecture

The ports attached to the North Bridge or the Memory Controller Hub (MCH) offer a higher performance than those attached to the Enterprise South Bridge (ESB).

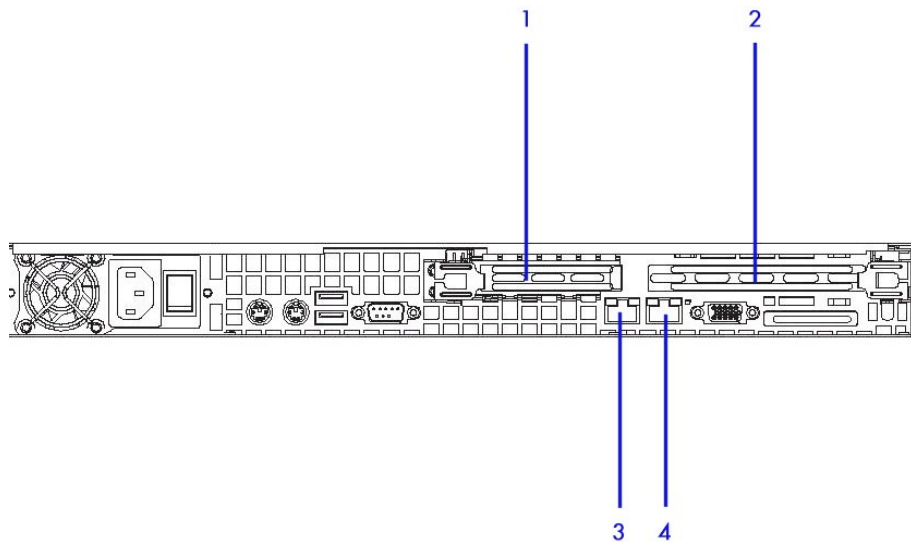


Figure E-2. R421 rear view connectors

Connector number	Port/Slot	Use
1	PCI-Express x8	InfiniBand interconnect or Ethernet 1000 Backbone (when slot 4 is used for Ethernet 1000 interconnect)
2	PCI-X 100MHz / 64 bit	
3	Ethernet	Administration Network or BMC Network
4	Gbit Ethernet	Ethernet 1000 interconnect or Ethernet Backbone (when slot 1 is used for InfiniBand interconnects)

## E.3.2 R422 Series – Compute Node

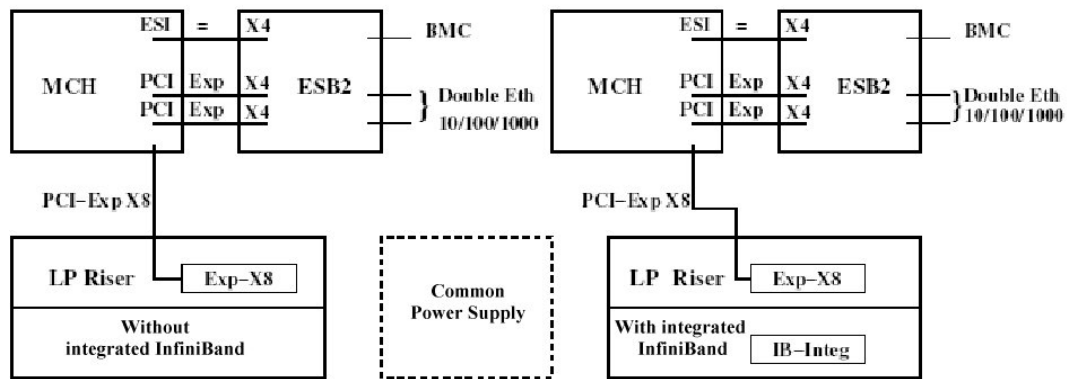


Figure E-3. R422 rear view of Riser architecture

The ports attached to the North Bridge or the Memory Controller Hub (MCH) offer a higher performance than those attached to the Enterprise South Bridge (ESB).

**Note** Depending on the model, an on-board **InfiniBand** controller with a dedicated port may be included. The two servers within a **R422** machine are identical, they either both include the **InfiniBand** controller or they both do not.

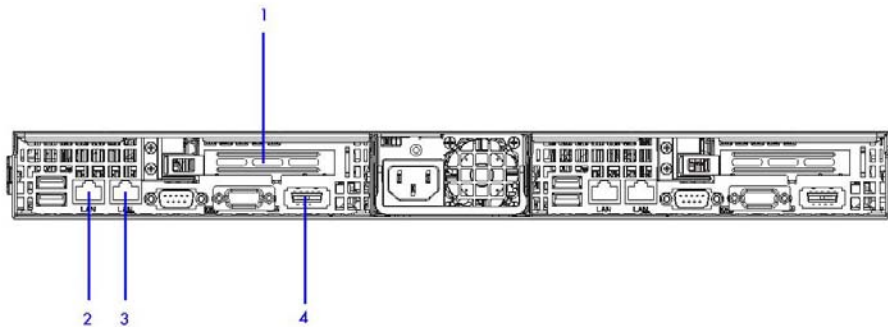


Figure E-4. R422 Rear view connectors

Connector number	Port/Slot	Use
1	PCI - Express x8	InfiniBand Interconnect or Ethernet 1000 Backbone
2	LAN port	Management Network or BMC Network
3	LAN port	Gbit Ethernet or Gbit Ethernet Interconnect or Ethernet 1000 backbone
4	InfiniBand port (optional)	InfiniBand Interconnect

### E.3.3 R460 Series – Service Node

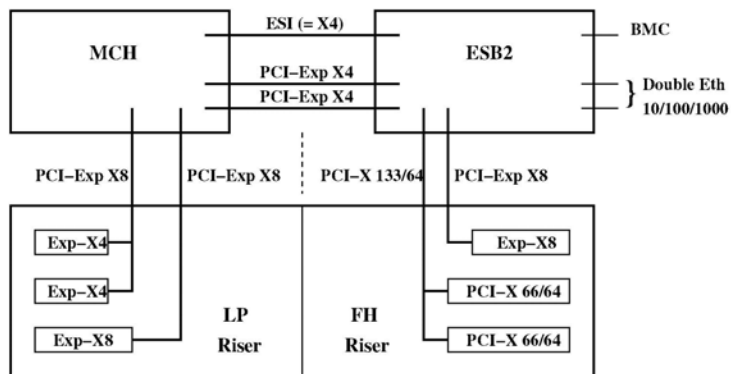


Figure E-5. R460 risers and I/O subsystem slotting

The ports attached to the North Bridge or the Memory Controller Hub (MCH) offer a higher performance than those attached to the Enterprise South Bridge (ESB).

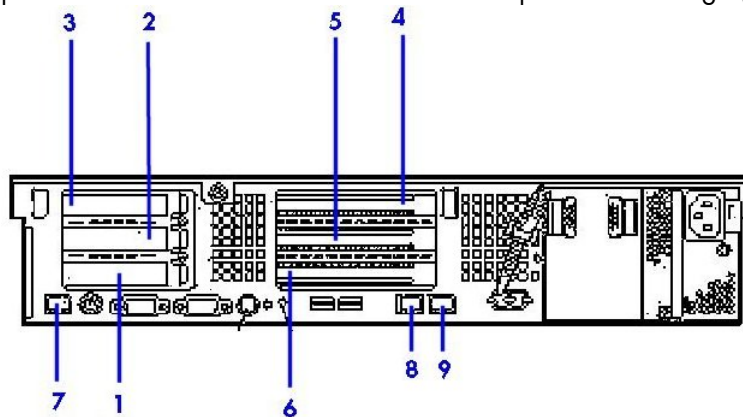


Figure E-6. Rear view of R460 Series

Connector number	Port/Slot	Use
1	PCI-Express x8	InfiniBand Double Data Rate Adapter
2	PCI-Express x4	Fibre Channel Disk Rack
3	PCI-Express x4	Fibre Channel Input\Output
4	PCI-Express x8	Optional backbone - 10 Gigabit Ethernet <b>Myricom Myri-10G</b> (x8) OR 1 Gbit Ethernet <b>Intel 82571</b> Ethernet Controller (x4)
5	PCI-X 66 MHz / 64 bit	
6	PCI-X 66 MHz / 64 bit	
7	Ethernet	Dedicated Board Management Controller (BMC) connector for the BMC network.
8	Ethernet	Administration Ethernet Connector
9	Ethernet	Gigabit Ethernet Interconnect

**Note** Either slot number 1 is used for **InfiniBand** interconnects OR connector number 9 is used for Gigabit **Ethernet** interconnects. These networks are exclusive.

## E.3.4 R421 E1 Series – Compute Nodes

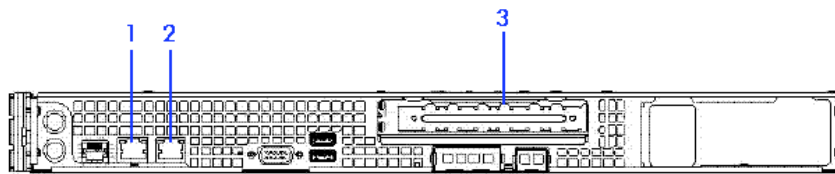


Figure E-7. Rear view of R421 E1 Series

### E.3.4.1 InfiniBand Interconnect

Connector number	Port/Slot	Use
1	Integrated ETH0	Management Network and BMC Network
2	Integrated ETH1	Backbone 1 Gbit Ethernet
3	SLOT 0	InfiniBand Interconnect

### E.3.4.2 Ethernet Interconnect

Connector number	Port/Slot	Use
1	Integrated ETH0	Management Network and BMC Network
2	Integrated ETH1	Ethernet Interconnect
3	SLOT 0	Backbone 1 Gbit Ethernet

### E.3.5 R422 E1 Series – Compute Nodes

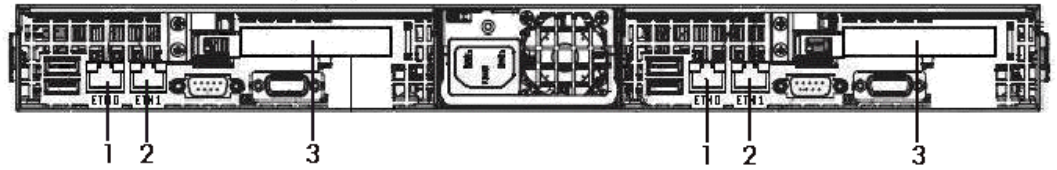


Figure E-8. Rear view of R422 E1 Series (2 Compute Nodes in 1U)

#### E.3.5.1 InfiniBand Interconnect

Connector number	Port/Slot	Use
1	Integrated ETH0	Management Network and BMC Network
2	Integrated ETH1	Backbone 1 Gbit Ethernet
3	SLOT 0	InfiniBand Interconnect

#### E.3.5.2 Ethernet Interconnect

Connector number	Port/Slot	Use
1	Integrated ETH0	Management Network and BMC Network
2	Integrated ETH1	Ethernet Interconnect
3	SLOT 0	Backbone 1 Gbit Ethernet

#### E.3.5.3 Integrated InfiniBand Interconnect

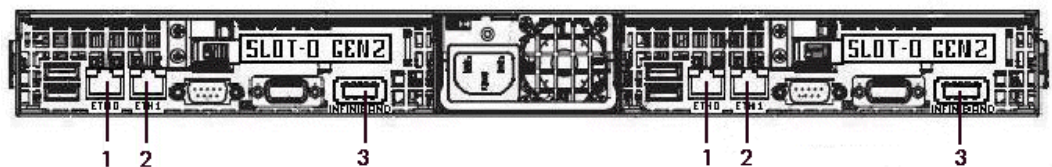


Figure E-9. Rear view of R422 E1 Series (2 Compute Nodes in 1U with Integrated InfiniBand)

Connector number	Port/Slot	Use
1	Integrated ETH0	Management Network and BMC Network
2	Integrated ETH1	Backbone 1 Gbit Ethernet
3	Integrated IB-0	InfiniBand Interconnect

## E.3.6 R425 Series – Compute Nodes

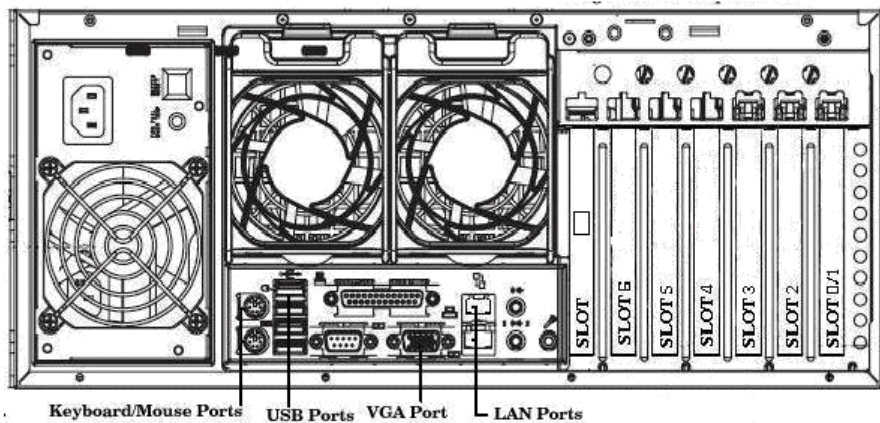


Figure E-10. Rear view of R425 Series

### E.3.6.1 1 Compute Node (2 GPU) with InfiniBand Interconnect

Port/Slot	Type	Use
LAN 1	1 Gbit Ethernet	Management Network
LAN 2	1 Gbit Ethernet	Backbone Ethernet
SLOT 0	DDR IB Gen2	InfiniBand Interconnect
SLOT 4+3	16x Pci-Exp Gen2	NVIDIA C1060
SLOT 6+5	16x Pci-Exp Gen2	NVIDIA C1060
SLOT 7	Dedicated BMC Port	BMC Network

### E.3.6.2 1 Compute Node (1 GPU) with InfiniBand Interconnect

Port/Slot	Type	Use
LAN 1	1 Gbit Ethernet	Management Network
LAN 2	1 Gbit Ethernet	Backbone Ethernet
SLOT 0	UIO PCI-Exp 8x	SAS RAID 0,1,5,10 Controller (Optional)
SLOT 4	DDR IB Gen2	InfiniBand Interconnect
SLOT 6+5	16x Pci-Exp Gen2	NVIDIA C1060
SLOT 7	Dedicated BMC Port	BMC Network

### E.3.6.3 1 Compute Node (1/2 GPU) with Ethernet Interconnect

Port/Slot	Type	Use
LAN 1	1 Gbit Ethernet	Management Network
LAN 2	1 Gbit Ethernet	Ethernet Interconnect
SLOT 0	UIO PCI-Exp 8x	SAS RAID 0,1,5,10 Controller (Optional)
SLOT 2	1 Gbit Ethernet	Backbone Ethernet
SLOT 4+3	16x Pci-Exp Gen2	NVIDIA C1060
SLOT 6+5	16x Pci-Exp Gen2	NVIDIA C1060
SLOT 7	Dedicated BMC Port	BMC Network

## E.3.7 R423 E1 Series – Service Node

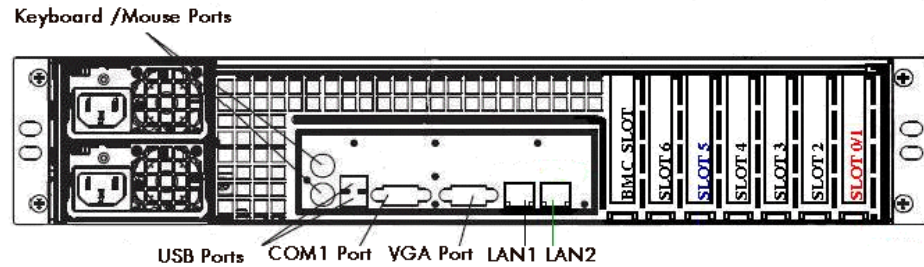


Figure E-11. Rear view of R423 E1 Series

### E.3.7.1 Standalone Management Node with InfiniBand Interconnect

Port/Slot	Type	Use
LAN 1	1 Gbit Ethernet	Management Network
LAN 2	1 Gbit Ethernet	Backbone Ethernet (if not on SLOT5)
SLOT 0	UIO PCI-Exp 8x	SAS RAID 0,1,5,10 Controller (Optional)
SLOT 5	10 Gbit Ethernet Optical	Backbone Ethernet (if not on LAN2)
SLOT 6	DDR IB Gen	InfiniBand Interconnect
SLOT 7	Dedicated BMC Port	BMC Network

### E.3.7.2 Standalone Management Node with Ethernet Interconnect

Port/Slot	Type	Use
LAN 1	1 Gbit Ethernet	Management Network
LAN 2	1 Gbit Ethernet	Ethernet Interconnect
SLOT 0	UIO PCI-Exp 8x	SAS RAID 0,1,5,10 Controller (Optional)
SLOT 4	1 Gbit Ethernet	Backbone Ethernet (if not on slot 5)
SLOT 5	10 Gbit Ethernet Optical	Backbone Ethernet (if not on slot 4)
SLOT 7	Dedicated BMC Port	BMC Network

### E.3.7.3 Standalone Management & I/O NFS Node with InfiniBand Interconnect

Port/Slot	Type	Use
LAN 1	1 Gbit Ethernet	Management Network
LAN 2	1 Gbit Ethernet	Backbone Ethernet (if not on SLOT5)
SLOT 0	UIO PCI-Exp 8x	SAS RAID 0,1,5,10 Controller (Optional)
SLOT 3	4 Gb/s FC	1 <sup>st</sup> Fiber Channel External Storage
SLOT 4	4 Gb/s FC	2 <sup>nd</sup> Fiber Channel External Storage
SLOT 5	10 Gbit Ethernet Optical	Backbone Ethernet (if not on LAN2)
SLOT 6	DDR IB Gen	InfiniBand Interconnect
SLOT 7	Dedicated BMC Port	BMC Network

#### E.3.7.4 Standalone Management & I/O NFS Node with Ethernet Interconnect

Port/Slot	Type	Use
LAN 1	1 Gbit Ethernet	Management Network
LAN 2	1 Gbit Ethernet	Ethernet Interconnect
SLOT 0	UIO PCI-Exp 8x	SAS RAID 0,1,5,10 Controller (Optional)
SLOT 3	4 Gb/s FC	Fiber Channel External Storage
SLOT 4	1 Gbit Ethernet	Backbone Ethernet (if not on slot 5)
SLOT 5	10 Gbit Ethernet Optical	Backbone Ethernet (if not on slot 4)
SLOT 7	Dedicated BMC Port	BMC Network

#### E.3.7.5 I/O NFS Node with InfiniBand Interconnect

Port/Slot	Type	Use
LAN 1	1 Gbit Ethernet	Management Network
LAN 2	1 Gbit Ethernet	Backbone Ethernet (if not on SLOT5)
SLOT 0	UIO PCI-Exp 8x	SAS RAID 0,1,5,10 Controller (Optional)
SLOT 3	4 Gb/s FC	1 <sup>st</sup> Fiber Channel External Storage
SLOT 4	4 Gb/s FC	2 <sup>nd</sup> Fiber Channel External Storage
SLOT 5	10 Gbit Ethernet Optical	Backbone Ethernet (if not on LAN2)
SLOT 6	DDR IB Gen	InfiniBand Interconnect
SLOT 7	Dedicated BMC Port	BMC Network

#### E.3.7.6 I/O NFS Node with Ethernet Interconnect

Port/Slot	Type	Use
LAN 1	1 Gbit Ethernet	Management Network
LAN 2	1 Gbit Ethernet	Ethernet Interconnect
SLOT 0	UIO PCI-Exp 8x	SAS RAID 0,1,5,10 Controller (Optional)
SLOT 3	4 Gb/s FC	Fiber Channel External Storage
SLOT 4	1 Gbit Ethernet	Backbone Ethernet (if not on slot 5)
SLOT 5	10 Gbit Ethernet Optical	Backbone Ethernet (if not on slot 4)
SLOT 7	Dedicated BMC Port	BMC Network

#### E.3.7.7 MDS Lustre I/O Node with InfiniBand Interconnect

Port/Slot	Type	Use
LAN 1	1 Gbit Ethernet	Management Network
SLOT 0	UIO PCI-Exp 8x	SAS RAID 0,1,5,10 Controller (Optional)
SLOT 3	4 Gb/s FC	2 <sup>nd</sup> Fiber Channel External Storage
SLOT 5	4 Gb/s FC	1 <sup>st</sup> Fiber Channel External Storage
SLOT 6	DDR IB Gen	InfiniBand Interconnect
SLOT 7	Dedicated BMC Port	BMC Network



### E.3.7.8 MDS Lustre I/O Node with Ethernet Interconnect

Port/Slot	Type	Use
LAN 1	1 Gbit Ethernet	Management Network
LAN 2	1 Gbit Ethernet	Ethernet Interconnect
SLOT 0	UIO PCI-Exp 8x	SAS RAID 0,1,5,10 Controller (Optional)
SLOT 3	4 Gb/s FC	2 <sup>nd</sup> Fiber Channel External Storage
SLOT 5	4 Gb/s FC	1st Fiber Channel External Storage
SLOT 7	Dedicated BMC Port	BMC Network

### E.3.7.9 OSS Lustre I/O Node with InfiniBand Interconnect

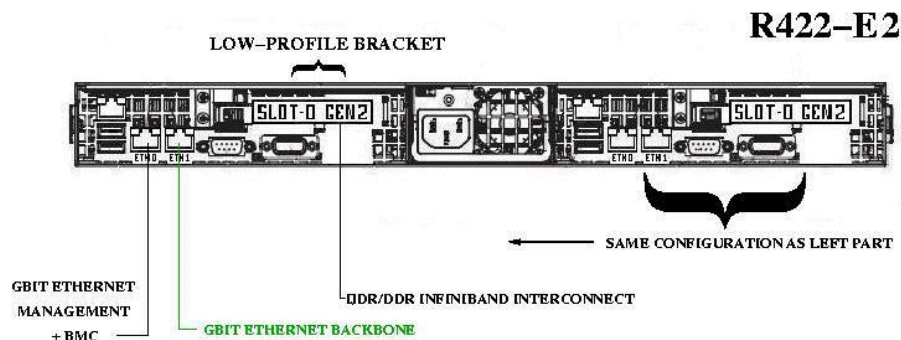
Port/Slot	Type	Use
LAN1	1 Gbit Ethernet	Management Network
SLOT0	UIO PCI-Exp 8x	SAS RAID 0,1,5,10 Controller (Optional)
SLOT3	4 Gb/s FC	2 <sup>nd</sup> Fiber Channel External Storage
SLOT4	4 Gb/s FC	3 <sup>rd</sup> Fiber Channel External Storage
SLOT5	4 Gb/s FC	1st Fiber Channel External Storage
SLOT6	DDR IB Gen	InfiniBand Interconnect
SLOT7	Dedicated BMC Port	BMC Network

### E.3.7.10 OSS Lustre I/O Node with Ethernet Interconnect

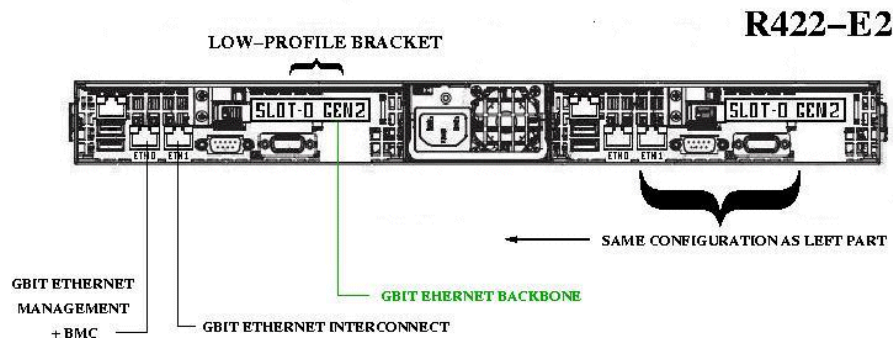
Port/Slot	Type	Use
LAN1	1 Gbit Ethernet	Management Network
LAN2	1 Gbit Ethernet	Ethernet Interconnect
SLOT0	UIO PCI-Exp 8x	SAS RAID 0,1,5,10 Controller (Optional)
SLOT3	4 Gb/s FC	2 <sup>nd</sup> Fiber Channel External Storage
SLOT4	4 Gb/s FC	3 <sup>rd</sup> Fiber Channel External Storage
SLOT5	4 Gb/s FC	1st Fiber Channel External Storage
SLOT7	Dedicated BMC Port	BMC Network

## E.3.8 R422 E2 Series – Compute Nodes

### E.3.8.1 2 Compute Nodes in 1U with InfiniBand Interconnect



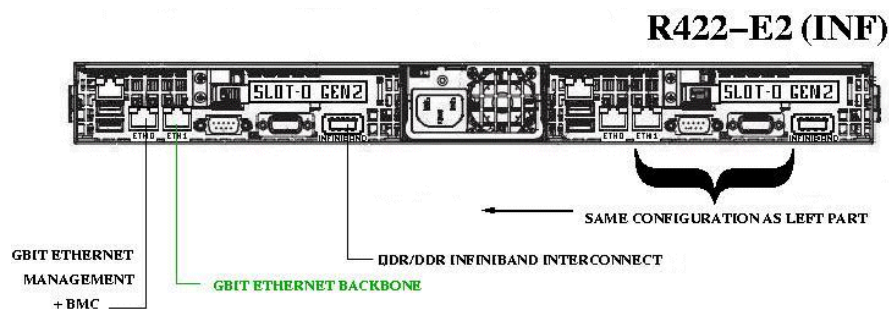
### E.3.8.2 2 Compute Nodes in 1U with Ethernet Interconnect



#### Connecting TESLA Switch Device:

Slot0 can be used to connect a TESLA switch device, using NVIDIA Expansion cables. In this configuration there is no GBit Ethernet Backbone.

### E.3.8.3 2 Compute Nodes in 1U with Integrated InfiniBand Interconnect

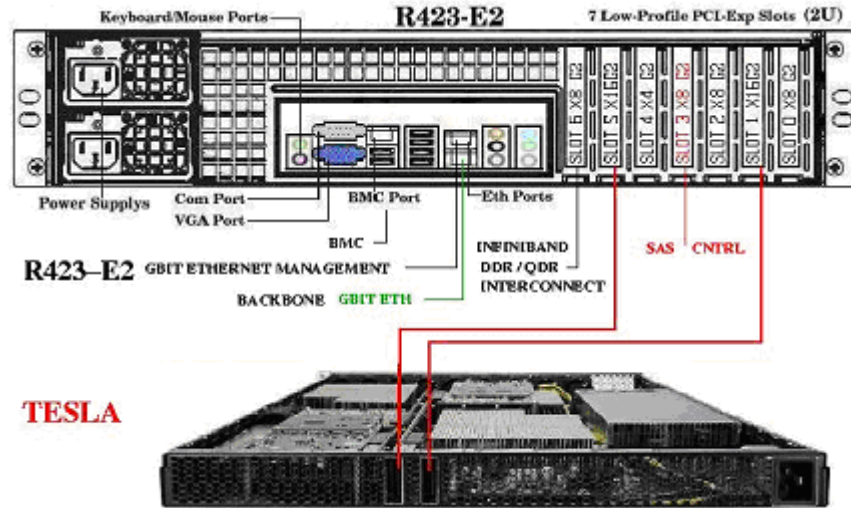


#### Connecting TESLA Switch Device:

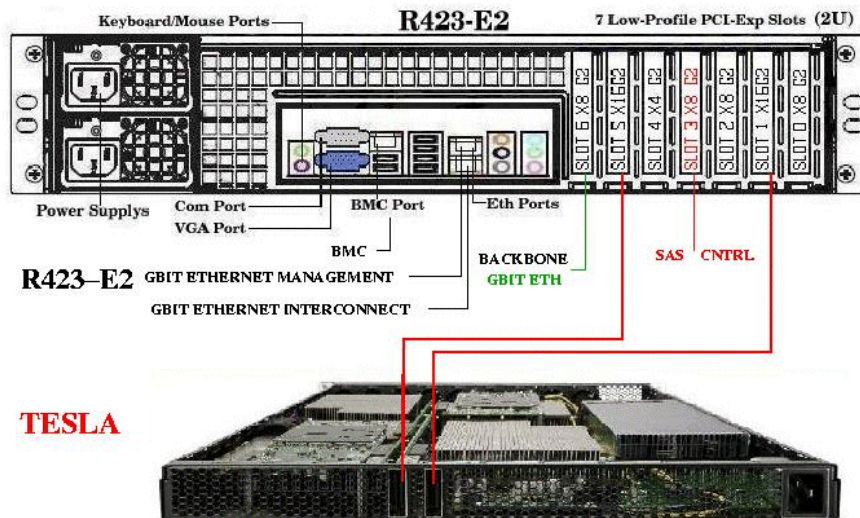
Slot0 can be used to connect a TESLA switch device, using NVIDIA PCI-Express Expansion cables.

## E.3.9 R423 E2 Series – Compute or Service Nodes

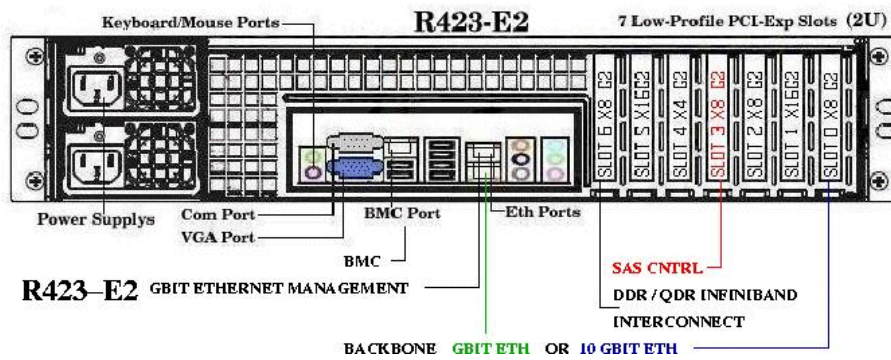
### E.3.9.1 1 Accelerated Compute Node in (2+1)U with InfiniBand Interconnect (Switched Attachment)



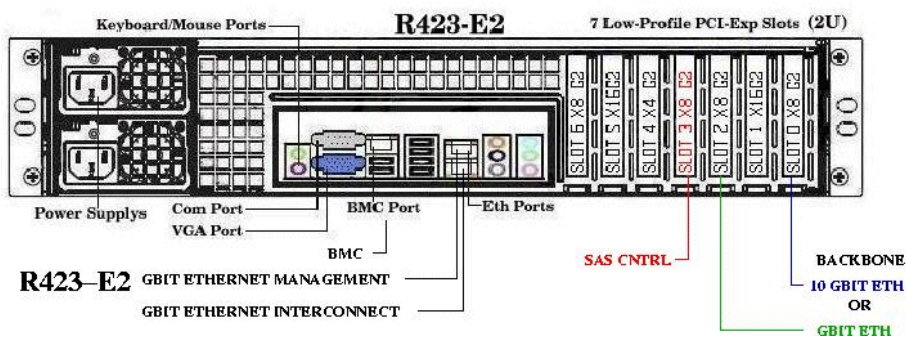
### E.3.9.2 1 Accelerated Compute Node in (2+1)U with Ethernet Interconnect (Switched Attachment)



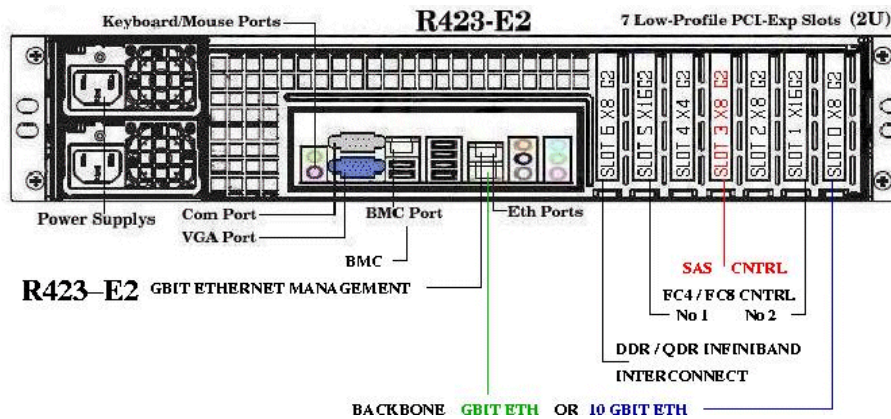
### E.3.9.3 Standalone Management Node with InfiniBand Interconnect



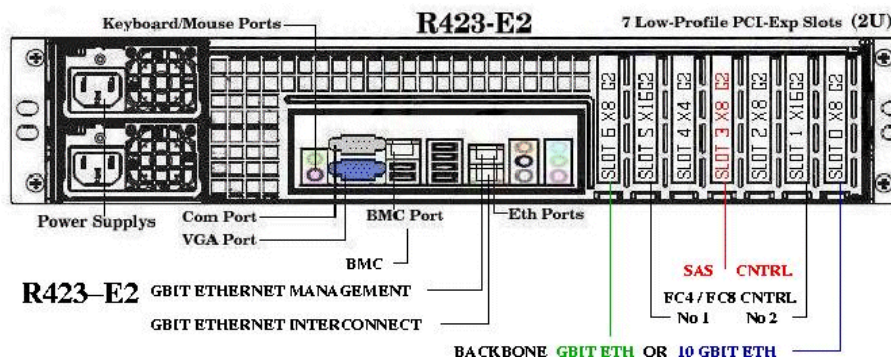
### E.3.9.4 Standalone Management Node with Ethernet Interconnect



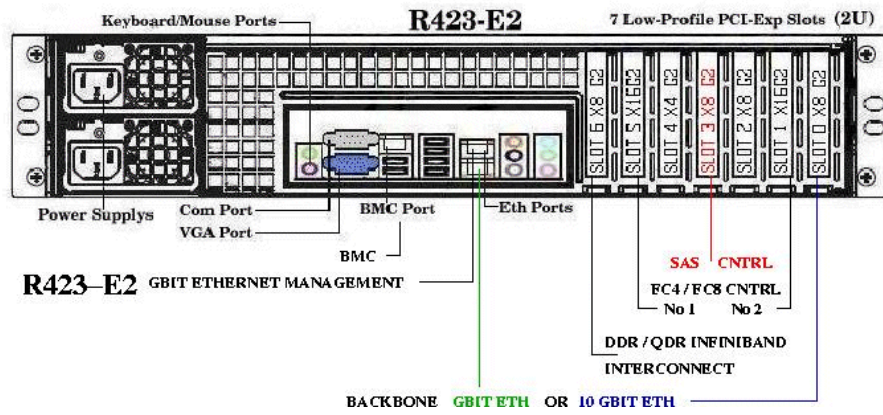
### E.3.9.5 I/O NFS Node with InfiniBand Interconnect



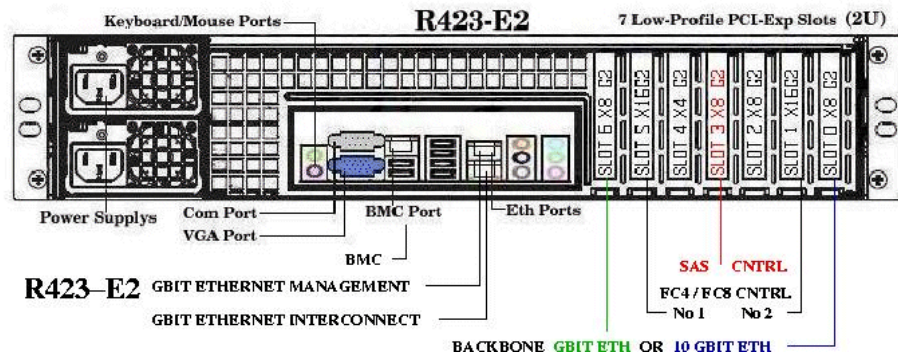
### E.3.9.6 I/O NFS Node with Ethernet Interconnect



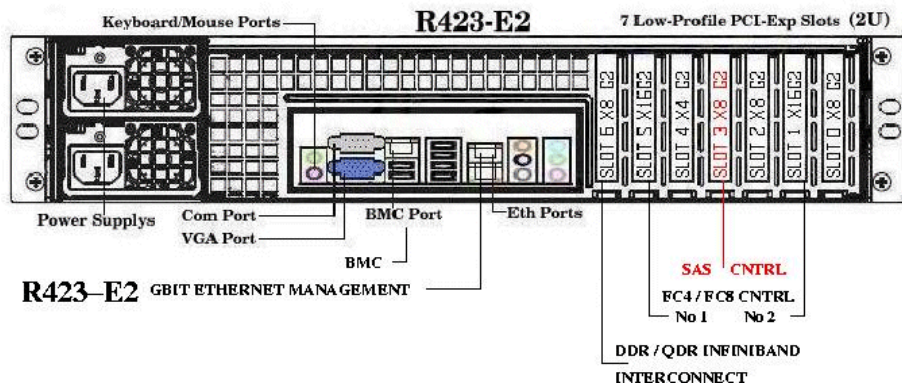
**E.3.9.7 Standalone Management & I/O NFS Node with InfiniBand Interconnect**



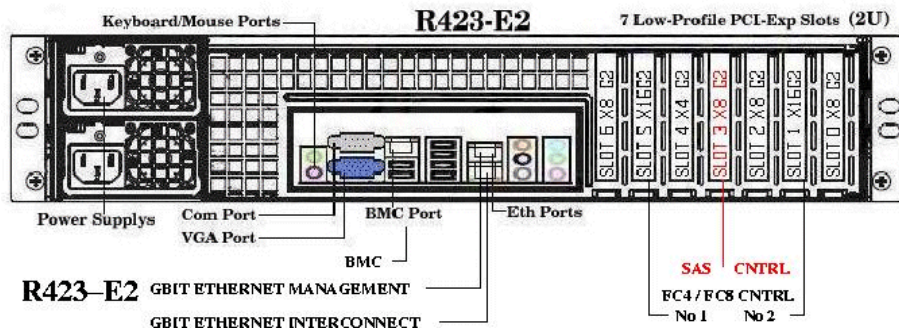
**E.3.9.8 Standalone Management & I/O NFS Node with Ethernet Interconnect**



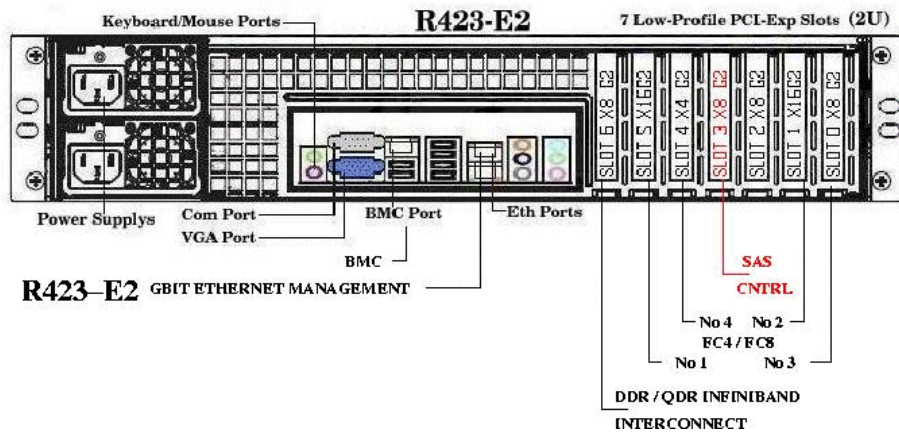
**E.3.9.9 MDS Lustre I/O Node with InfiniBand Interconnect**



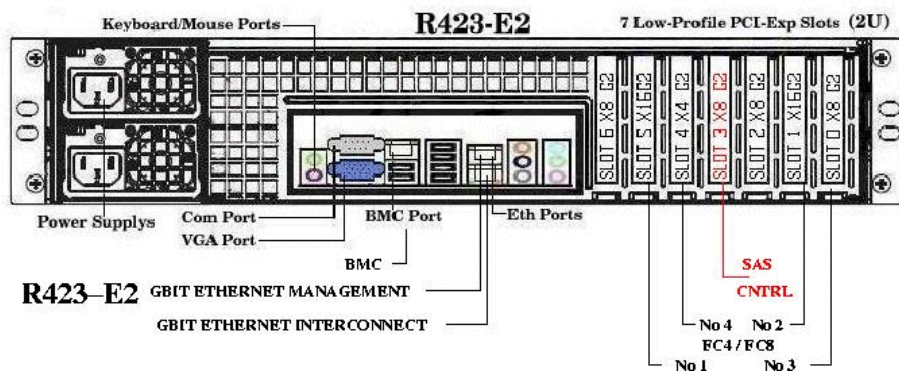
### E.3.9.10 MDS Lustre I/O Node with Ethernet Interconnect



### E.3.9.11 OSS Lustre I/O Node with InfiniBand Interconnect

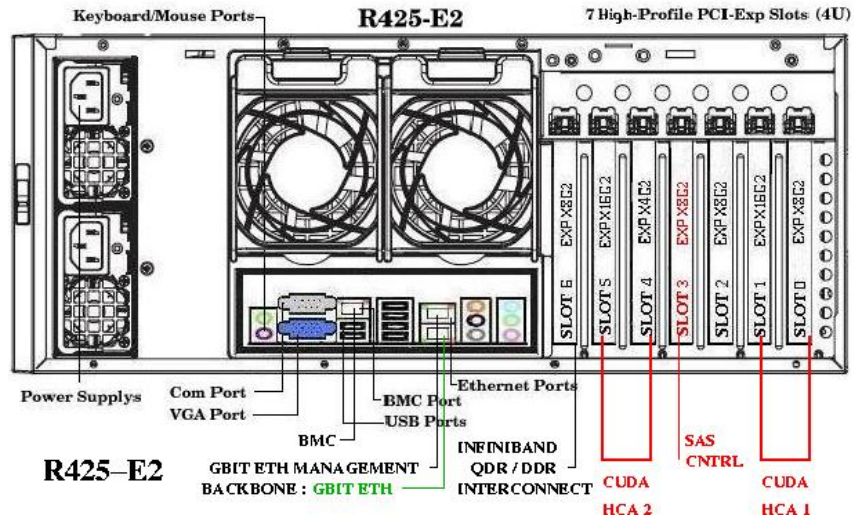


### E.3.9.12 OSS Lustre I/O Node with Ethernet Interconnect

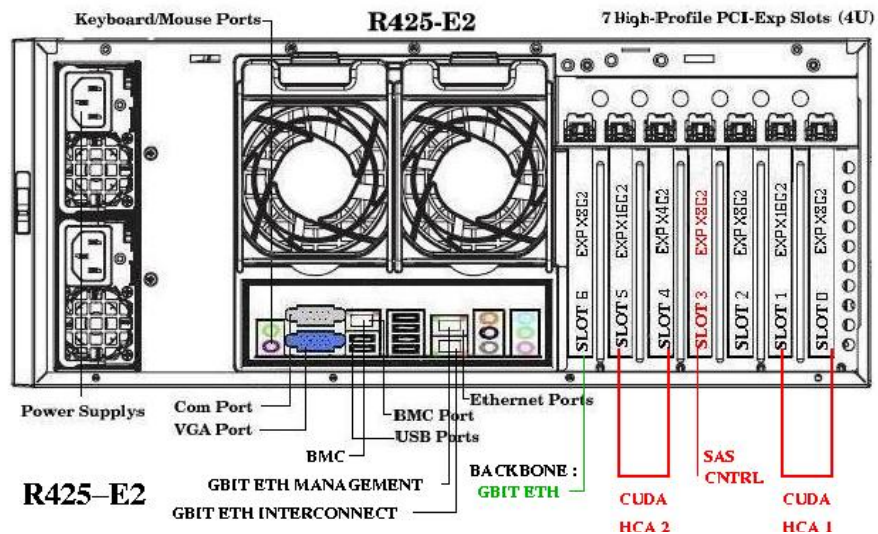


## E.3.10 R425 E2 Series – Compute Nodes

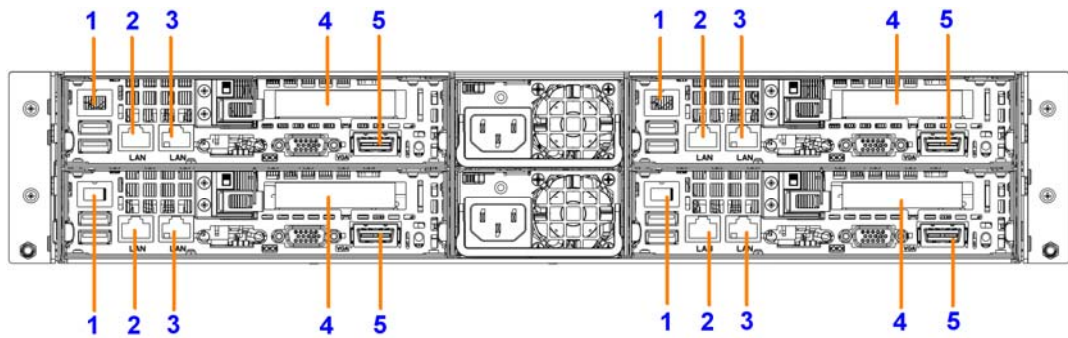
### E.3.10.1 1 Accelerated Compute Node in 4U with InfiniBand Interconnect (Direct Attachment)



### E.3.10.2 1 Accelerated Compute Node in 4U with Ethernet Interconnect (Direct Attachment)



## E.3.11 R424 E2 Series – Compute Nodes



Connector	Type / Function
1	Ethernet - BMC dedicated (unused)
2	Ethernet - Eth0 + BMC shared
3	Ethernet - Eth1
4	PCIe gen2 x16 (low profile) – Slot 0
5	QSFP - onboard InfiniBand QDR (Optional)

### E.3.11.1 4 Compute Nodes in 2U with Ethernet Interconnect

Connector	Type / Function
2 - Eth0 + shared BMC	Management Network
3 - Eth1	Gigabit Ethernet Interconnect
4 - PCIe gen2 x16 (low profile)	Optional: Add-on 1 or 10Gbps Ethernet Adapter for backbone

### E.3.11.2 4 Compute Nodes in 2U with integrated InfiniBand Interconnect (optional)

Connector	Type / Function
2 - Eth0 + shared BMC	Management Network
3 - Eth1	Gigabit Ethernet Backbone or unused
5 - onboard InfiniBand	InfiniBand Interconnect (integrated)

### E.3.11.3 4 Compute Nodes in 2U with add-on Infiniband Interconnect

Connector	Type / Function
2 - Eth0 + shared BMC	Management Network
3 - Eth1	Gigabit Eth Backbone or unused
4 - PCIe gen2 x16 (low profile)	Add-on InfiniBand – Interconnect



---

## Appendix F. Activating your Red Hat account

The command `rhncg_ks` can be used to activate your Red Hat account. For full details regarding installation numbers and activating your Red Hat account see:

[http://www.redhat.com/support/resources/faqs/installation\\_numbers/index.html#what\\_is](http://www.redhat.com/support/resources/faqs/installation_numbers/index.html#what_is)



### WARNING

Do not update the Red Hat RPMs from the Red Hat web site as Bull cannot guarantee the continued functioning of your BAS5 for Xeon cluster. Contact Bull technical support for more information regarding when the Red Hat and Bull RPMs can be updated.



---

# Glossary and Acronyms

---

## A

### ABI

Application Binary Interface

### ACL

Access Control List

### ACT

Administration Configuration Tool

### ANL

Argonne National Laboratory (MPICH2)

### API

Application Programmer Interface

### ARP

Address Resolution Protocol

### ASIC

Application Specific Integrated Circuit

---

## B

### BAS

Bull Advanced Server

### BIOS

Basic Input Output System

### Blade

Thin server that is inserted in a blade chassis

### BLACS

Basic Linear Algebra Communication Subprograms

### BLAS

Basic Linear Algebra Subprograms

### BMC

Baseboard Management Controller

### BSBR

Bull System Backup Restore

### BSM

Bull System Manager

---

## C

### CGI

Common Gateway Interface

### CLI

Command Line Interface

### ClusterDB

Cluster Database

### CLM

Cluster Management

### CMC

Chassis Management Controller

### ConMan

A management tool, based on telnet, enabling access to all the consoles of the cluster.

### Cron

A UNIX command for scheduling jobs to be executed sometime in the future. A cron is normally used to schedule a job that is executed periodically - for example, to send out a notice every morning. It is also a daemon process, meaning that it runs continuously, waiting for specific events to occur.

### CUBLAS

CUDA™ BLAS

### CUDA™

Compute Unified Device Architecture

### CUFFT

CUDA™ Fast Fourier Transform

## CVS

Concurrent Versions System

## Cygwin

A Linux-like environment for Windows. Bull cluster management tools use Cygwin to provide SSH support on a Windows system, enabling command mode access.

---

## D

### DDN

Data Direct Networks

### DDR

Double Data Rate

### DHCP

Dynamic Host Configuration Protocol

### DLID

Destination Local Identifier

### DNS

Domain Name Server:

A server that retains the addresses and routing information for TCP/IP LAN users.

### DSO

Dynamic Shared Object

---

## E

### EBP

End Bad Packet Delimiter

### ECT

Embedded Configuration Tool

### EIP

Encapsulated IP

### EPM

Errors per Million

## EULA

End User License Agreement (Microsoft)

---

## F

### FDA

Fibre Disk Array

### FFT

Fast Fourier Transform

### FFTW

Fastest Fourier Transform in the West

### FRU

Field Replaceable Unit

### FTP

File Transfer Protocol

---

## G

### Ganglia

A distributed monitoring tool used to view information associated with a node, such as CPU load, memory consumption, and network load.

### GCC

GNU C Compiler

### GDB

Gnu Debugger

### GFS

Global File System

### GMP

GNU Multiprecision Library

### GID

Group ID

### GNU

GNU's Not Unix

**GPL**

General Public License

**GPT**

GUID Partition Table

**Gratuitous ARP**

A gratuitous ARP request is an Address Resolution Protocol request packet where the source and destination IP are both set to the IP of the machine issuing the packet and the destination MAC is the broadcast address `xx:xx:xx:xx:xx:xx`.

Ordinarily, no reply packet will occur. Gratuitous ARP reply is a reply to which no request has been made.

**GSL**

GNU Scientific Library

**GT/s**

Giga transfers per second

**GUI**

Graphical User Interface

**GUID**

Globally Unique Identifier

---

**H****HBA**

Host Bus Adapter

**HCA**

Host Channel Adapter

**HDD**

Hard Disk Drive

**HoQ**

Head of Queue

**HPC**

High Performance Computing

**Hyper-Threading**

A technology that enables multi-threaded software applications to process threads in parallel, within

each processor, resulting in increased utilization of processor resources.

---

**IB**

InfiniBand

**IBTA**

InfiniBand Trade Association

**ICC**

Intel C Compiler

**ICH**

I/O Controller Hub

**IDE**

Integrated Device Electronics

**IFORT**

Intel<sup>®</sup> Fortran Compiler

**IMB**

Intel MPI Benchmarks

**INCA**

Integrated Cluster Architecture:  
Bull Blade platform

**IOC**

Input/Output Board Compact with 6 PCI Slots

**IOH**

Input/Output Hub

**IPMI**

Intelligent Platform Management Interface

**IPO**

Interprocedural Optimization

**IPoIB**

Internet Protocol over InfiniBand

**IPR**

IP Router

**iSM**

Storage Manager (FDA storage systems)

**ISV**

Independent Software Vendor

---

**K****KDC**

Key Distribution Centre

**KSIS**

Utility for Image Building and Deployment

**KVM**

Keyboard Video Mouse (allows the keyboard, video monitor and mouse to be connected to the node)

---

**L****LAN**

Local Area Network

**LAPACK**

Linear Algebra PACKage

**LDAP**

Lightweight Directory Access Protocol

**LDIF**

LDAP Data Interchange Format:

A plain text data interchange format to represent LDAP directory contents and update requests. LDIF conveys directory content as a set of records, one record for each object (or entry). It represents update requests, such as Add, Modify, Delete, and Rename, as a set of records, one record for each update request.

**LKCD**

Linux Kernel Crash Dump:

A tool used to capture and analyze crash dumps.

**LOV**

Logical Object Volume

**LSF**

Load Sharing Facility

**LUN**

Logical Unit Number

**LVM**

Logical Volume Manager

**LVS**

Linux Virtual Server

---

**M****MAC**

Media Access Control (a unique identifier address attached to most forms of networking equipment).

**MAD**

Management Datagram

**Managed Switch**

A switch with no management interface and/or configuration options.

**MDS**

MetaData Server

**MDT**

MetaData Target

**MFT**

Mellanox Firmware Tools

**MIB**

Management Information Base

**MKL**

Maths Kernel Library

**MPD**

MPI Process Daemons

**MPFR**

C library for multiple-precision, floating-point computations

**MPI**

Message Passing Interface

**MTBF**

Mean Time Between Failures

**MTU**

Maximum Transmission Unit

---

**N****Nagios**

A tool used to monitor the services and resources of Bull HPC clusters.

**NETCDF**

Network Common Data Form

**NFS**

Network File System

**NIC**

Network Interface Card

**NIS**

Network Information Service

**NS**

NovaScale

**NTP**

Network Time Protocol

**NUMA**

Non Uniform Memory Access

**NVRAM**

Non Volatile Random Access Memory

---

**O****OFA**

Open Fabrics Alliance

**OFED**

Open Fabrics Enterprise Distribution

**OPMA**

Open Platform Management Architecture

**OpenSM**

Open Subnet Manager

**OpenIB**

Open InfiniBand

**OpenSSH**

Open Source implementation of the SSH protocol

**OSC**

Object Storage Client

**OSS**

Object Storage Server

**OST**

Object Storage Target

---

**P****PAM**

Platform Administration and Maintenance Software

**PAPI**

Performance Application Programming Interface

**PBLAS**

Parallel Basic Linear Algebra Subprograms

**PBS**

Portable Batch System

**PCI**

Peripheral Component Interconnect (Intel)

**PDSH**

Parallel Distributed Shell

**PDU**

Power Distribution Unit

**PETSc**

Portable, Extensible Toolkit for Scientific Computation

**PGAPACK**

Parallel Genetic Algorithm Package

**PM**

Performance Manager

Platform Management

**PMI**

Process Management Interface

**PMU**

Performance Monitoring Unit

**pNETCDF**

Parallel NetCDF (Network Common Data Form)

**PVFS**

Parallel Virtual File System

---

**Q****QDR**

Quad Data Rate

**QoS**

Quality of Service:

A set of rules which guarantee a defined level of quality in terms of transmission rates, error rates, and other characteristics for a network.

**QPI**

Quick Path Interconnect

---

**R****RAID**

Redundant Array of Independent Disks

**RDMA**

Remote Direct Memory Access

**ROM**

Read Only Memory

**RPC**

Remote Procedure Call

**RPM**

RPM Package Manager

**RSA**

Rivest, Shamir and Adleman, the developers of the RSA public key cryptosystem

---

**S****SA**

Subnet Agent

**SAFTE**

SCSI Accessible Fault Tolerant Enclosures

**SAN**

Storage Area Network

**SCALAPACK**

SCALable Linear Algebra PACKage

**SCSI**

Small Computer System Interface

**SCIPOPT**

Portable implementation of CRAY SCILIB

**SDP**

Socket Direct Protocol

**SDPOIB**

Sockets Direct Protocol over Infiniband

**SDR**

Sensor Data Record

Single Data Rate

**SFP**

Small Form-factor Pluggable transceiver - extractable optical or electrical transmitter/receiver module.

**SEL**

System Event Log

**SIOH**

Server Input/Output Hub



**SIS**

System Installation Suite

**SL**

Service Level

**SL2VL**

Service Level to Virtual Lane

**SLURM**

Simple Linux Utility for Resource Management – an open source, highly scalable cluster management and job scheduling system.

**SM**

Subnet Manager

**SMP**

Symmetric Multi Processing:  
The processing of programs by multiple processors that share a common operating system and memory.

**SNMP**

Simple Network Management Protocol

**SOL**

Serial Over LAN

**SPOF**

Single Point of Failure

**SSH**

Secure Shell

**Syslog-ng**

System Log New Generation

---

**T****TCL**

Tool Command Language

**TCP**

Transmission Control Protocol

**TFTP**

Trivial File Transfer Protocol

**TGT**

Ticket-Granting Ticket

---

**U****UDP**

User Datagram Protocol

**UID**

User ID

**ULP**

Upper Layer Protocol

**USB**

Universal Serial Bus

**UTC**

Coordinated Universal Time

---

**V****VCRC**

Variant Cyclic Redundancy Check

**VDM**

Voltaire Device Manager

**VFM**

Voltaire Fabric Manager

**VGA**

Video Graphic Adapter

**VL**

Virtual Lane

**VLAN**

Virtual Local Area Network

**VNC**

Virtual Network Computing:  
Used to enable access to Windows systems and Windows applications from the Bull cluster management system.

---

## W

### WWPN

World-Wide Port Name

---

## X

### XFS

eXtended File System

### XHPC

Xeon High Performance Computing

### XIB

Xeon InfiniBand

### XRC

Extended Reliable Connection:

Included in Mellanox ConnectX HCAs for memory scalability

---

# Index

## A

adapters placement, E-1

## B

backbone network, 1-5

bind attribute, D-1

Blade Server

Configuring, 3-29

Brocade switch

configuration, 8-18

enabling, 4-16

Bull Additional Software

installation, B-1

Bull information file, 3-52

Bull Scientific Studio, 3-46

bull-infos file, 3-52

bullx blade systems, 8-14

## C

CISCO Switch

configuration, 8-7

cluster

architecture schemes, 1-1

large size, 1-2

medium size, 1-2

small size, 1-1

ClusterDB

rack\_port table, 3-27

Reinstalling, A-1

saving, 3-3

Saving, A-1

clusterdb.cfg file, 4-2

cluster-network.xml file, 8-5

ColdoorStart command, 3-28

Commands

ColdoorStart, 3-28

config\_ip, 2-19, 3-51, C-1

ddn\_admin, 4-8

ddn\_init, 4-8

equipmentRecord, 3-27

fcsregister, 4-16

installInfs, 3-36

lsiocfg, 4-15

rhncfg\_ks, F-1

swtAdmin, 8-1, 8-2

swtConfig, 8-1

updateMacAdmin, 3-30

Compilers, 7-1

config\_ip command, 2-19, 3-51, C-1

configuration

Disk Health, 3-42

Ethernet Switches, 3-26

Ganglia, 3-32, 3-42

Interconnect, C-1

Kdump, 3-43

network, 3-16

NFS file system, 6-3

NIS file system, 6-1

NTP, 3-33

overview, 3-2

postfix, 3-30

switch Brocade, 8-18

switches, 8-1

Voltaire device, 8-17

Configuring

Blade Server, 3-29

Cool Cabinet Door, 3-27

conman

testing, 3-57

Cool Cabinet Door

Configuring, 3-27

Custom Directories, B-1

## D

database

dump, 3-23, 3-32

initialization, 3-23

register storage information, 4-1

*DataDirect Networks S2A (DDN) Storage System,*  
4-1, 4-7

ddn\_admin command, 4-8

ddn\_admin.conf file, 3-4, 4-7

ddn\_init command, 4-8

ddn\_set\_up\_date\_time.cron file, 4-7

dgc\_admin.conf file, 3-4

Disk Health

configuration, 3-42

disk partitioning, 3-9

disknaming.conf file, 5-6

## E

EMC/Clariion (DGC) Storage Systems, 4-13

eth\_switch table, 8-4

Ethernet adapters

identification, C-1

installation, 8-17

Ethernet Switches, 8-1

configuration, 3-26

Configuration, 8-3, 8-5

## F

fcswwregister command, 4-16

FDA and Optima 1500 Storage Systems

Linux Systems, 4-4

FDA Storage Systems

Configuring, 4-3

Fibre Channel Switches, 4-16

Files

bull-infos, 3-52

clusterdb.cfg, 4-2

ddn\_admin.conf, 3-4, 4-7

ddn\_set\_up\_date\_time.cron, 4-7

dgc\_admin.conf, 3-4

disknaming.conf, 5-6

gmond.conf, 3-42

grub.conf, 3-43

idmapd.conf, 6-5

iSMsvr conf, 4-4

kdump.conf, 3-43

nec\_admin.conf, 3-4, 4-6

network, 6-2

nsswitch.conf, 6-2

storcheck.cron, 4-2

storframework.conf, 3-4

stornode.conf, 3-4

wwn, 4-15

xinetd.conf, D-1

xyr\_admin.conf, 3-4, 4-12

yp.conf, 6-2

## G

Ganglia

configuration, 3-32, 3-42

gmetad.conf file, 3-32

gmond.conf file, 3-32, 3-42

golden image

creating, 3-50

grub.conf file, 3-43

## I

I/O resources

configuring, 5-1

performance optimization, E-1

idmapd.conf file, 6-5

InfiniBand

adapters identification, C-1

equipment, 1-5

installation

Bull Additional Software, B-1

Intel compilers and tools, 7-1

Ksis server, 3-49

Management Node, 3-5

NVIDIA CUDA, 3-47

NVIDIA Tesla, 3-46

overview, 3-2

RAID monitoring, 3-47

installInfs command, 3-36

Intel

Compilers, 7-1

Trace Tool, 7-1

VTune Performance Analyzer, 7-2

Interconnect

configuration, C-1

iSMsvr conf file, 4-4

## K

Kdump

configuration, 3-43

kdump.conf file, 3-43

Ksis image

- creating, 3-50
- Ksis server
  - installation, 3-49
- L**
- Linux
  - rdesktop command, 4-3
- lsiocfg command, 4-15
- M**
- Mellanox ConnectX Dual-Port, 1-5
- model file, 5-1
- N**
- Nagios
  - testing, 3-55
- nec\_admin.conf file, 3-4, 4-6
- netdisco, 8-3
- network
  - administration network, 1-4, 3-16
  - backbone, 1-5
  - configuration, 3-16
  - high speed interconnect, 1-5
- network file, 6-2
- Network Time Protocol (NTP), 3-33
- NFS file system
  - configuration, 6-3
- NFSv3, 6-3
- NFSv4, 6-3
- NIS file system, 6-1
  - configuration, 6-1
- Node
  - Compute Node, 1-4
  - I/O Node, 1-4
  - Login Node, 1-4
  - Service Node, 1-3
- nsctrl
  - testing, 3-57
- nsswitch.conf file, 6-2
- NTP
  - configuration, 3-33
- testing, 3-54
- ntp.conf file, 3-33
- NVIDIA
  - CUDA installation, 3-47
  - Tesla installation, 3-46
- O**
- Optima1500 Storage Systems
  - Configuring, 4-3
- P**
- partitioning
  - disk, 3-9
- PCI slots
  - R421, E-3
  - R421 E1, E-6
  - R422, E-4
  - R422 E1, E-7
  - R422 E2, E-12
  - R423 E1, E-9
  - R423 E2, E-13
  - R425, E-8
  - R425 E2, E-17
  - R460, E-5
  - selection, E-1
- pdsh
  - testing, 3-53
- Performance (I/O)
  - optimization, E-1
- postfix
  - configuration, 3-30
  - main.cf file, 3-30
- R**
- RAID monitoring
  - installation, 3-47
- Red Hat account, F-1
- Red Hat information file, 3-52
- Reference Node Image
  - creation and deployment, 3-49
- S**
- saving
  - ClusterDB, 3-3

- Lustre file system, 3-4
- ssh keys, 2-3, 3-3
- storage information, 3-4
- Service Node, 1-3
- SSH
  - saving keys, 2-3, 3-3
- ssh-keygen, 4-5
- Storage Systems
  - iSMsvr conf file, 4-4
- storageadmin directory, 3-4
- storcheck.cron file, 4-2
- StoreWay Master, 4-11
- storframework.conf file, 3-4
- stornode.conf file, 3-4
- switch
  - configuration, 8-1
  - Ethernet, 8-1
- switch Brocade
  - configuration, 8-18
- switch CISCO
  - initial configuration, 8-6
  - manual configuration, 8-7
- switch Foundry Network
  - initial configuration, 8-7
  - manual configuration, 8-7
- Switches
  - Broadcom
    - Configuration, 8-14
  - CISCO
    - Configuring, 8-8
    - CISCO 2940, 8-6
    - CISCO 2950, 8-6
    - CISCO 2960, 8-6
    - CISCO 2970, 8-6
    - CISCO 3560, 8-6
    - CISCO 3750, 8-6
  - Foundry
    - Configuring, 8-11
  - Foundry BigIron RX4, RX8, RX16, 8-7
  - Foundry FastIron FLS624, 8-7
  - Foundry FastIron FLS648, 8-7
- swtAdmin command, 8-1
- swtConfig command, 8-1
- syslog-ng
  - port usage, 3-33
  - service, 3-33
  - testing, 3-54
- syslog-ng.conf file, 3-33
- syslog-ng/DDN file, 4-7
- system-config-network command, 3-16

## T

- Trace Tool (Intel)
  - installation, 7-1

## U

- updateMacAdmin command, 3-30

## V

- Voltaire
  - configuration, 8-17
  - Switching Devices, 1-5
- VTune Performance Analyzer, 7-2

## W

- wwn file, 4-15
- WWPN description, 4-15

## X

- xinetd.conf file, D-1
- xyr\_admin.conf file, 3-4, 4-12

## Y

- yp.conf file, 6-2
- ypbind service, 6-2



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

REFERENCE  
86 A2 19FA 04