

# Distributed Software Management for AIX 5L

Setup Guide

AIX



REFERENCE  
86 A2 81HX 15



# ESCALA

# Distributed Software Management for AIX 5L Setup Guide

AIX

## **Software**

June 2005

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

REFERENCE  
86 A2 81HX 15

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 1992, 2005

Printed in France

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

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

### **Trademarks and Acknowledgements**

We acknowledge the right of proprietors of trademarks mentioned in this book.

AIX® is a registered trademark of International Business Machines Corporation, and is being used under licence.

UNIX® is a registered trademark in the United States of America and other countries licensed exclusively through the Open Group.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries

*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.*

---

## About this Book

This Guide concerns the setting-up and use of:

- “Distributed Software Management for AIX” software. (DSM)

The AIX DSM workstation provides a single point of control for managing Escala P series.

ClusterAssistant & DSM is an application manager that runs on any dedicated AIX node or partition of a DLPAR Server. It is used for configuring, managing, and monitoring clusters. ClusterAssistant & DSM is integrated in the CDE (Common Desktop Environment), which provides a windows/icons/mouse-based user interface.

### **DSM Features:**

- Quick configuration
- Support of nodes without HACMP
- Customization of alarms
- Applications Management:
  - NIM (Network Installation Management)
  - Rlogin
  - SMIT from DSM server
  - WatchWare from DSM server
  - AIX errorlog Alarms
  - Link Equipment
  - Cleanup
  - Check

---

## Audience

This manual addresses an audience of System Administrators and Customer Engineers who want to set up and/or use the DSM with ClusterAssistant & DSM.

---

## Document Overview

AIX DSM workstation and ClusterAssistant & DSM Applications are described in the following sections:

<b>Chapter 1</b>	<b>AIX DSM workstation</b> Describes the use of a AIX DSM workstation as a user interface for managing a powercluster.
<b>Chapter 2</b>	<b>DSM for AIX</b> Describes the use of DSM for Escala P series management.
<b>Glossary</b>	Alphabetical list of terms and abbreviations used in this manual.
<b>Index</b>	General index.

## Highlighting

The following highlighting conventions are used in this book:

<b>Bold</b>	Identifies commands, subroutines, keywords, files, structures, directories, and other items whose names are predefined by the system. Also identifies graphical objects such as buttons, labels, and icons that the user selects, as well as simple words to which particular attention must be paid.
<i>Italics</i>	Identifies parameters whose actual names or values are to be supplied by the user.
<code>Monospace</code>	Identifies examples of specific data values, examples of text similar to what you might see displayed, examples of portions of program code similar to what you might write as a programmer, messages from the system, or information you should actually type.

---

## Operating System Level

This revision, applies to AIX™ Versions for POWER version 5.2 and 5.3

---

# Terminology

## Hardware

The term "AIX DSM workstation" is used to indicate the machine providing the DSM platform, in this case Escala P Series.

## Software

### Operating System

This term is used to indicate the proprietary operating system software, in this case AIX.

### ClusterAssistant & DSM

**Objects** used in ClusterAssistant & DSM are defined as follows:



#### **standalone node**

An Escala server. Its icon name is suffixed by **.node**. For example, if the node name is **foo**, its icon name is **foo.node**.



#### **HA node**

An Escala server running HACMP. Its icon name is suffixed by **.node**.



#### **HACMP cluster**

A set of HA nodes managed by HACMP. Its icon name is suffixed by **.cluster**.



#### **powercluster**

All the nodes to be managed from the DSM with ClusterAssistant & DSM. Its icon name is suffixed by **.epc**.

**domain** An object instance of type: powercluster, HACMP cluster, HA node, standalone node.

**cluster** A synonym for HACMP cluster.

**node** A generic term for HA node or standalone node.

**cluster node** A generic term for an HA node of an HACMP cluster.

#### **Notes:**

1. The powercluster is made of zero, one or several standalone nodes and/or zero, one or several HACMP clusters.
2. An HACMP cluster is made of two or more HA nodes.

See also *Relationships Between Objects*, on page 2-3.

---

## Related Publications

### Software Release Bulletin

Read the *Software Release Bulletin* (SRB) that comes with the software. It includes environment requirements and restrictions, the procedure to install the software, as well as late-breaking news.

### Escala EPC & HA Solutions

The following documents apply to Escala Powercluster and HA Solutions:

- EPC & HA Solutions Setup Guide, Order Number 86 A2 79HX, is intended for system administrators and customer engineers who want to set up and/or manage Powercluster or Escala HA Solution.
- Powercluster & HA Solutions: Using the Sample HA Scripts, Order Number 86 A7 82HX, is mainly intended for Bull technical personnel. It gives hints on using the sample start and stop scripts that come with the BullCluster software package.
- *Site Preparation for Rack Systems*, Order Number 86 A1 30PX, includes site preparation details for the P series family.

The following documents apply only to Powercluster:

- Powercluster Cluster Management Tools: ClusterWatch, Order Number 86 A2 80HX, explains how to set up and use the ClusterWatch utility. ClusterWatch is a Web-based facility for monitoring cluster operations (a SMIT-based version of ClusterWatch is also provided).
- Distributed Software Management Setup Guide, Order Number 86 A2 81HX, this present guide.

### Hardware

The following hardware publications are referenced in this document:

- *Hardware Technical Files Escala P Series, Part II: Console*, Order Number 76728502
- PortServer User's Guide, Reference: Vendor publication. P/N: 90028700C.
- *Hardware Management Console Operations Guide*, Order Number 86 A1 83EF.

### Link Equipment Devices

Link Equipment devices are described in the following documents:

- LinkBuilder FDDI Workgroup Hub User Guide: 09-0447-000
- ONcore Integrated System Hub Installation and Operation Guide: 17-00362-7
- ONcore Distributed Management Module User Guide: 17-00370-9
- ONcore SwitchModule User Guide: 17-00755-2
- Ethernet SuperStack II Hub 10 User Guide: DUA1667-2AAA03
- Fast Ethernet SuperStack II Switch 300010/100 User Guide: DUA1694-2AAA03
- Fast Ethernet SuperStack II Switch 300010/100 Reference Guide: DQA1694-2AAA03
- Fast Ethernet SuperStack II Switch 300010/100 Installation Guide: DIA1694-2AAA03
- Fast Ethernet SuperStack II Switch 300010/100 Release Note: DNA1694-2AAA03
- Fast Ethernet SuperStack II Switch 330010/100 User Guide: DUA1698-0AAA02

- Fast Ethernet SuperStack II Switch 330010/100 Reference Guide: DQA1698-0AAA0x
- Fast Ethernet SuperStack II Switch 330010/100 Installation Guide: DIA1698-0AAA0x
- Fast Ethernet SuperStack II Switch 330010/100 Release Note: DNA1698-0AAA0x
- Gigabit Ethernet SuperStack II Switch 9300 Getting Started Guides
- Gigabit Ethernet SuperStack II Switch 9300 Administration Guide
- Gigabit Ethernet SuperStack II Switch 9300 Unpacking Instructions
- Gigabit Ethernet SuperStack II Switch 9300 Quick Installation Guide
- Gigabit Ethernet SuperStack II Switch 9300 Command Quick Reference Card
- Gigabit Ethernet SuperStack II Switch 9300 Release Note
- BROCADE SilkWorm 2800 Hardware Reference Manual
- BROCADE SilkWorm 2400/2800 Quick Install and Setup Guide
- BROCADE SilkWorm Fabric Developers Guide
- BROCADE Fabric Operating System
- BROCADE WEB TOOLS Reference Manual
- BROCADE ZONING Reference Manual
- BROCADE SES Reference Manual
- BROCADE Quick Loop Reference Manual
- SuperStack 3 Switch 4900 Getting Started Guide
- SuperStack 3 Switch 4900SX Getting Started Guide
- SuperStack 3 Switch Implementation Guide for the Switch 4900 Series
- SuperStack 3 Switch 4900 Series Management Interface Reference Guide
- SuperStack 3 Switch 4900 Series Management Quick Reference Guide
- PortServer User's Guide
- PortServer TS 8/16 Configuration and Administration Guide
- PortServer TS 8/16 Command Reference

## Other Publications

The AIX document set, as well as manuals accompanying machines, disks, and other hardware involved in the configuration, also provide indispensable information, particularly:

- *AIX Windows Desktop Advanced Users and System Administrator's Guide*, Order Number 86 A2 31AQ.
- *AIX 5. NIM Network Installation Management Guide and Reference*, Order Reference 86 A2 23EF.
- *WatchWare User's Guide*, Order Number 86 A2 75EF.
- *System Management Guide Operating System and Devices for AIX 5L*, Order Number 86 A2 26EF.

## Ordering Publications

To order additional copies of this Guide, use Order Number 86 A2 81HX.

# Table of Contents

About this Book.....	iii
Audience.....	iii
Document Overview.....	iv
Highlighting.....	iv
Operating System Level.....	iv
Terminology.....	v
Hardware.....	v
Software.....	v
Operating System.....	v
ClusterAssistant & DSM.....	v
Related Publications.....	vi
Software Release Bulletin.....	vi
Escala EPC & HA Solutions.....	vi
Hardware.....	vi
Link Equipment Devices.....	vi
Other Publications.....	vii
Ordering Publications.....	vii
<b>Chapter 1.    AIX DSM workstation.....</b>	<b>1-1</b>
Introducing the AIX DSM workstation.....	1-1
Hardware.....	1-1
Hardware Platforms.....	1-1
PortServer.....	1-2
Hardware Management Console (HMC).....	1-2
Ethernet Hub.....	1-2
Setting-up the AIX DSM workstation.....	1-3
AIX DSM workstation Typical Configuration.....	1-3
Set-up the AIX DSM workstation and the Escala P series Hardware.....	1-4
Cabling Guidelines.....	1-4
Hub Concerns.....	1-5
DSM Network Connections.....	1-5
Dedicated Administration Network.....	1-5
Setting-up the PortServer.....	1-6
Preliminary Remarks.....	1-6
Booting the PortServer.....	1-6
Setting-up the PortServer Base Parameters.....	1-6
Configuring the PortServer Ports.....	1-7
Checking the PortServer Settings.....	1-7
Checking the PortServer Network Connection.....	1-8
Display Current Users of the PortServer.....	1-8
Useful commands.....	1-8
Using the PortServer to Gain Access to Node Console Ports from the AIX DSM workstation.....	1-11
AIX DSM workstation Configuration.....	1-11
Using the HMC to Gain Access to Virtual Terminal of a Partition Node from the DSM.....	1-12
Updating the /etc/hosts file on the AIX DSM workstation.....	1-12
Gaining Access to Virtual Terminal of a Partition Node.....	1-12
Using the AIX DSM workstation.....	1-14
Advantages.....	1-14

Options .....	1-14
Remote Maintenance .....	1-14
Other User Console Facilities.....	1-14

## **Chapter 2. DSM for AIX..... 2-1**

Introducing ClusterAssistant & DSM.....	2-1
Terminology Used with ClusterAssistant & DSM .....	2-2
Relationships Between Objects.....	2-3
Software .....	2-3
Setting-up ClusterAssistant & DSM .....	2-4
Setup Operations for SMP Servers (without HMC).....	2-4
Setup Operations for LPAR Servers (with HMC) .....	2-5
Set-up Summary.....	2-6
Step 1: Set Up the AIX DSM workstation and the Escala P series Hardware .....	2-6
Step 2: Set Up ClusterAssistant & DSM .....	2-6
Step 3: Register Powercluster.....	2-6
Step 4: Configure the HACMP Cluster Topology.....	2-6
Step 5: Complete Setup of ClusterAssistant & DSM .....	2-7
Step 6: Complete the HACMP Cluster Setup .....	2-7
Checking that ClusterAssistant & DSM is Pre-installed .....	2-7
Checking that bclwd Daemon is Running on DSM & HA Nodes.....	2-7
Setting Up the "classist" User Password .....	2-8
Updating /etc/hosts and /.rhosts Files .....	2-8
Updating /etc/hosts .....	2-8
Updating /.rhosts .....	2-8
Registering Powercluster.....	2-8
Configuring the HACMP Cluster Topology .....	2-8
Use of DSM with Dedicated Administration Networks .....	2-9
Register an HACMP Cluster with ClusterAssistant & DSM.....	2-9
Setting Up the devices.config File .....	2-9
ClusterAssistant & DSM Administration and Troubleshooting .....	2-10
bclwd Daemon Troubleshooting .....	2-10
/etc/hosts and /.rhosts Files.....	2-10
ClusterWatch and WatchWare Passwords .....	2-10
Using ClusterAssistant & DSM .....	2-11
Users .....	2-11
Function Selection .....	2-11
Drag and Drop Capability.....	2-11
Front Panel - Common Desktop Environment.....	2-12
How to View Online Help .....	2-12
How to Bring Up the ClusterAssistant Application Group .....	2-12
Launching a ClusterAssistant Application .....	2-13
ClusterAssistant Folder.....	2-14
ClusterAssistant & DSM Applications.....	2-14
HACMP Cluster .....	2-14
Network Install Manager .....	2-14
Domains .....	2-14
Register Powercluster .....	2-15
System Console .....	2-15
Hardware Management Console .....	2-15
Rlogin .....	2-15
Powercluster State .....	2-15
SMIT from DSM Server.....	2-15
WatchWare from DSM Server.....	2-15
Link Equipment.....	2-15
Alarms Application .....	2-15

Cleanup .....	2-16
Check .....	2-16
<hr/>	
<b>HACMP Cluster Folder .....</b>	<b>2-17</b>
HACMP Cluster Applications .....	2-17
Cluster Configuration .....	2-17
Cluster Diagnostics .....	2-17
Cluster Users & Groups .....	2-17
ClusterWatch.....	2-17
ClusterWatch SMIT .....	2-18
Start Cluster Services .....	2-18
Stop Cluster Services.....	2-18
<hr/>	
<b>Cluster Configuration Folder .....</b>	<b>2-19</b>
Cluster Configuration Applications .....	2-19
Custom Events .....	2-19
Snapshot .....	2-19
Register Cluster .....	2-19
Deregister Cluster .....	2-20
Cluster Configuration (smit) .....	2-20
Cluster Worksheets .....	2-20
<hr/>	
<b>Network Install Manager Folder .....</b>	<b>2-21</b>
Network Install Manager.....	2-22
NIM Setup Assistant.....	2-22
Backup System .....	2-22
Restore System.....	2-22
NIM - SMIT .....	2-22
NIM on Node .....	2-22
<hr/>	
<b>Domains Folder.....</b>	<b>2-23</b>
Example of Domains Folder .....	2-23
<hr/>	
<b>Alarms.....</b>	<b>2-24</b>
Enabling the Alarms Capability .....	2-24
Monitoring Alarms with the Alarms Capability.....	2-24
Viewing Alarms .....	2-25
Clearing Alarms.....	2-25
Add AIX errlog Alarms.....	2-25
Configuring User Alarms.....	2-26
<hr/>	
<b>System Console .....</b>	<b>2-27</b>
Prerequisites for using System Console .....	2-27
Using System Console .....	2-27
How to retrieve partition ID, model type and serial number .....	2-28
<hr/>	
<b>Hardware Management Console .....</b>	<b>2-32</b>
Prerequisites for Using Hardware Management Console .....	2-32
Using Hardware Management Console .....	2-32
<hr/>	
<b>Register Powercluster .....</b>	<b>2-34</b>
New Powercluster.....	2-35
Modify Powercluster .....	2-37
Remove Powercluster .....	2-38
<hr/>	
<b>Cleanup Application .....</b>	<b>2-39</b>
Bringing Up Cleanup .....	2-39
Purpose .....	2-39
Using Cleanup .....	2-39
<hr/>	
<b>Check Application .....</b>	<b>2-40</b>
Bringing Up Check.....	2-40
Using Check .....	2-40
<hr/>	
<b>Powercluster State.....</b>	<b>2-42</b>
Standalone Node .....	2-42

HA Node.....	2-42
HACMP Cluster.....	2-43
Cluster State.....	2-43
Node State.....	2-44
HA Node State.....	2-44
<b>Cluster Configuration (smit) .....</b>	<b>2-45</b>
<b>Link Equipment Application .....</b>	<b>2-47</b>
<b>Multiple Displays on One Screen.....</b>	<b>2-49</b>
Overview of VNC .....	2-49
Installation.....	2-49
VNC-Server, on the AIX DSM workstation.....	2-49
VNC-Viewer, on "usual" display stations.....	2-49
Starting a VNC Server Session .....	2-50
Unix VNC-server options.....	2-51
Identifying the Active VNC Sessions .....	2-52
Stopping a VNC Server Session .....	2-52
Displaying a VNC Session.....	2-52
On an AIX Station .....	2-52
On a Windows System .....	2-53
On a Java-enabled Browser.....	2-54
Closing a VNC Desktop Session .....	2-54
<b>Chapter 3. Glossary .....</b>	<b>3-1</b>
<b>Chapter 4. Index .....</b>	<b>4-1</b>



---

## Chapter 1. AIX DSM workstation

Describes the use of a AIX DSM workstation as a user interface for managing a powercluster.

---

### Introducing the AIX DSM workstation

The AIX DSM workstation (a preferred option with Powerclusters) is an independent workstation that provides a single point of control for managing a powercluster.

Functional details:

- Hardware, on page 1-1.
- Setting-up the AIX DSM workstation, on page 1-3.
- Using the PortServer to Gain Access to Node Console Ports from the AIX DSM workstation, on page 1-11.
- Using the HMC to Gain Access to Virtual Terminal of a Partition Node from the AIX DSM workstation, on page 1-12.
- Using the AIX DSM workstation, on page 1-14.

---

## Hardware

### Hardware Platforms

The AIX DSM workstation serves both, as the access point to the system consoles of the different nodes, and as a powerful workstation able to run any administration utility, notably the ClusterAssistant & DSM application.



**Figure 1.** AIX DSM workstation

## PortServer

The **PortServer** provides the means to concentrate the console serial ports (S1) of all the nodes (except for LPAR servers), and thus to make them available from a single access point. This avoids having one ASCII terminal per node, which could be found cumbersome.

All the serial ports of the PortServer can be reached via the concentrator, using network communications (telnet session).

The management of the concentrator can be performed from an **ASCII terminal**.

- it must be connected to the port (16) of the PortServer

## Hardware Management Console (HMC)

The **Hardware Management Console** which is delivered with LPAR servers is a desktop PC running Linux and providing hardware management applications. The HMC provides a graphical user interface based on WebSM for configuration, partition management and **Virtual Terminal** access. The **Virtual Terminal** window provides a virtual system console access to every partition without any physical device assigned.

The HMC is connected to the LPAR server using a serial connection. To establish this connection, use one of the two native serial ports of the HMC and one of the two dedicated serial ports (HMC1 or HMC2) on the LPAR server.

## Ethernet Hub

The **Ethernet hub** is primarily intended to implement an independent dedicated administration network that interconnects the console-related devices (PortServer, HMC, AIX DSM workstation) and the nodes. Having such a dedicated administration network provides basic security. Otherwise the AIX DSM workstation, the PortServer and HMC are connected to the Enterprise's private network (to which are connected the powercluster nodes), in this case a 10 Mbps LAN.

For more details, refer to *Setting Up the AIX DSM workstation*, on page 1-3.

---

## Setting-up the AIX DSM workstation

This section summarizes the different steps related to AIX DSM workstation that you must perform when initially setting up an Escala Powercluster.

The AIX DSM workstation must be set up before attempting the installation of ClusterAssistant & DSM (see page 2-4).

### AIX DSM workstation Typical Configuration

This section presents a typical DSM configuration with comments, which should help you to understand the role of the different components and how they are tied together.

Figure 2 shows a sample cluster with two nodes, whose one console is handled through a PortServer and the other console (Virtual Terminal window) is handled on the Hardware Management Console HMC.

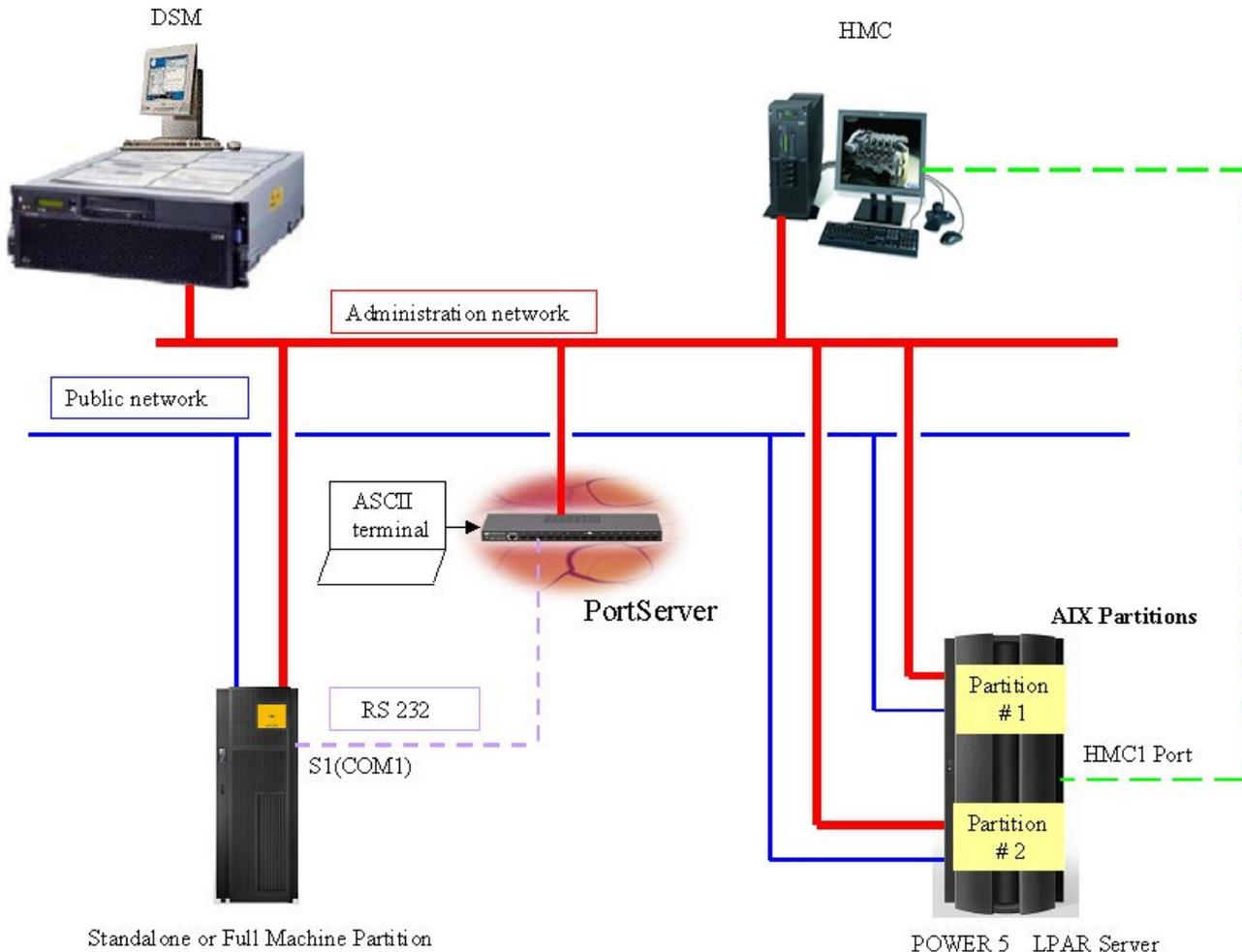
**Note:** Although this example shows a 2-node cluster, similar configurations can be achieved as well for clusters that have 2 nodes, or more than 2 nodes.

In this sample configuration:

- A system console (ASCII terminal) is connected to the serial port 16 for a PortServer (this port is special in the sense they is used to access the menus and commands to manage the concentrator).
- The HMC1 port of one node is connected to one of the serial ports of the HMC.
- From the AIX DSM workstation, you can access at any time, through the concentrator functions, any of the concentrator ports. Thus, you can gain control of the console (S1 or COM1 serial port) of one node. From the AIX DSM workstation, you can also access at any time, through the HMC, the Virtual Terminal window of the partitions.

In addition, note the following:

- For enhanced security, we have chosen in this typical configuration to use the hub to implement an independent, dedicated *administration network*, which interconnects the nodes, the PortServer, the HMC and the AIX DSM workstation. From the latter, you can access the nodes via the network, and run administration utilities as desired, taking advantage of the computing power of the AIX DSM workstation.



**Figure 2.** DSM – Typical Configuration

## Set-up the AIX DSM workstation and the Escala P series Hardware

This step consists of the following tasks:

- Before proceeding, read the *Software Release Bulletins* which come with the Escala P series product. They include environment requirements and restrictions, as well as late-breaking news.
- Cable the AIX DSM workstation components as well as the hardware components of the cluster.
- Configure the PortServer.

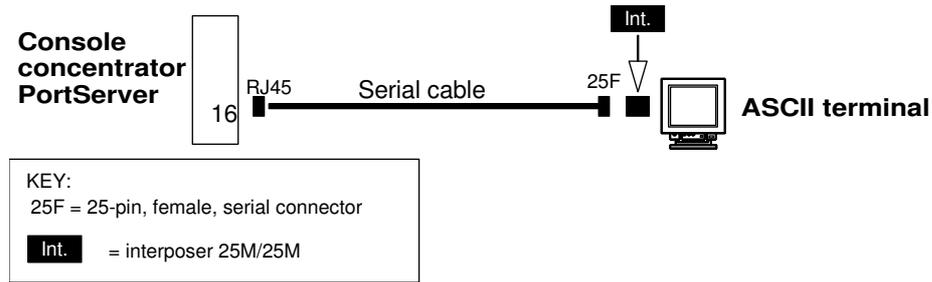
Once this step is performed, the AIX DSM workstation is ready to access the nodes through their console serial port (via the PortServer). Thus, you are able to gain access to the consoles of the nodes for further configuration tasks.

## Cabling Guidelines

This section only discusses how to connect the ports of the PortServer to the different involved devices, and how to implement an Ethernet connection between the PortServer and the hub.

If you need detailed cabling information related to the S1 or COM1 console ports of the servers (cluster nodes), refer to the server's hardware documentation and to Hardware Technical Files.

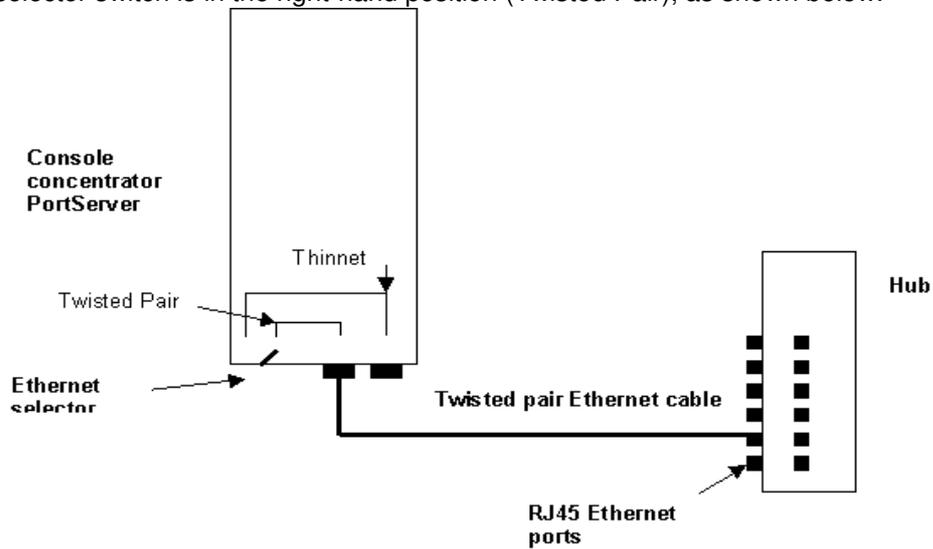
Figure 3 shows the parts you need if you want to implement a serial connection between a **BQ306** ASCII terminal and a serial port (16 for PortServer) of the concentrator.



**Figure 3.** Serial Connection between BQ306 Terminal and PortServer Concentrator

### Hub Concerns

The PortServer is equipped with a BNC coaxial connector and a 10BaseT connector. If you plan to connect the concentrator to the provided hub, which is equipped with RJ45 (twisted pair Ethernet) ports, you must plug the cable into the 10BaseT connector and make sure the selector switch is in the right-hand position (Twisted Pair), as shown below.



**Figure 4.** Ethernet Connection between Hub and PortServer Concentrator

## DSM Network Connections

### Dedicated Administration Network

On each node, the Ethernet network interface (with the administration network) must be configured as follows:

- AIX Configuration

Use the command **smit chinnet** on each node to configure the Ethernet interfaces of the dedicated administration network. On each node, update the */etc/host* file with the new interface names and addresses.

---

## Setting-up the PortServer

Two models of PortServer are available; both provide connection of up to 16 ports:

- PortServer 16–port model
- PortServer TS 16 model (the newest model).

### Preliminary Remarks

The procedures below are given as guidelines only. For detailed information on setting up, using and managing the PortServer, refer to the PortServer documentation:

- *Digi PortServer User's Guide* (PortServer 16–port model),
- or *Digi PortServer TS 8/16 Configuration and Administration Guide* (PortServer TS 16 model).

In the sample procedures below, we assume that your configuration includes an ASCII terminal (BQ306) connected to the port 16 of the PortServer and used as a terminal dedicated to PortServer management. The terminal data transmission rate must be 9600 bauds.

**Note:** Other, non-standard, configurations are possible (for example the port 16 could be connected to the AIX DSM workstation).

For PortServer TS 16 model, a web interface is available to configure the PortServer. However this method does not work for the initial IP address configuration. To access the web interface, enter directly the IP address assigned to the PortServer TS 16 as URL in your browser. Not all the commands are available from the web interface (see the PortServer TS 8/16 documentation).

### Booting the PortServer

- The ASCII terminal (connected to the port 16 of the PortServer) should be properly set up, with the following characteristics : baud rate 9600, 8 bits per character, 1 stop bit, no parity, DTR ignored, full duplex, and echo off.
- The following applies only to a PortServer 16–port model:
  - The selector switch for network must be in the correct position (Twisted Pair).
- Power-on the PortServer.
- The PortServer firmware's Power On Self Test (POST) sequence will now run automatically.

### Setting-up the PortServer Base Parameters

- When the PortServer boot process is completed, press the Return or Enter key on your keyboard; you should get the login: prompt.
- Enter root. When asked for the root password, enter: `dbps`
- When you see the `#>` prompt, you are logged in.
- Setup the IP address for the PortServer unit (for example 190.184.33.100), enter the following command:

```
#>set config ip=190.184.33.100 <Enter>
```

For PortServer TS 16 model, disable **dhcp** with the following command:

```
#>set config dhcp=off <Enter>
```

- Optionally, you can also set up the subnet mask, gateway and PortServer name.
  - Setup the Network Subnet Mask with the subnet mask of the client LAN network, (for example : 255.255.0.0); enter the following command:

```
#>set config submask=255.255.0.0 <Enter>
```

Default value is 255.255.255.0 for PortServer 16–port model and 255.0.0.0 for PortServer TS 16 model.

- If you have a gateway, set its address (for example 190.184.1.10); enter the following command:

```
#>set config gateway=190.184.1.10 <Enter>
```

Default value is 255.255.255.255 for PortServer 16–port model and 0.0.0.0 for PortServer TS 16 model.

- Set up the name you have assigned for the PortServer (for example portserver); enter the following command:

```
#>set config myname=portserver <Enter>
```

Default value is PORTSERV for PortServer 16–port model. No default value for PortServer TS 16 model.

For additional configuration as setting up the domain name, the domain server's name, the password, etc., see the PortServer Documentation.

To take into account the network configuration, reboot the PortServer by the command:

```
#>boot action=reset <Enter>
```

## Configuring the PortServer Ports

By default, all the ports are configured as terminal connected ports with 9600 value for baud rate parameter and with on value for ixon flow control parameter.

Keep default port settings for port 16 where the ASCII console is connected.

- In order to change the configuration of ports 1 to 15 to be as host connected port (S1 or COM1 plug of a node), enter the following commands:

```
#>set port dev=prn range=1 <Enter>
#>set flow ixon=off range=1 <Enter>
```

where 1 is the port 1, 2 port 2, ...etc. To set all the ports from 1 to 15, use the value 1-15 for range, to set ports 1 2 3 10 11, use the value 1,2,3,10,11 or 1-3,10-11 for range.

- Assign an IP address to each port connected to a host with the command:

```
#>set altip ip=@IP1 group=1 <Enter>
```

where @IP1 is the Ethernet address chosen for the Node #1 connected on port 1, @IP2 is the Ethernet address chosen for the Node #2 connected on the port 2,..etc. For example : @IP1 = 190.184.33.11 , @IP2 = 190.184.33.12,..etc.

If you have to connect a POWER 5system on the PortServer, you have to set the baud rate parameter to 19200 bauds.

To change the configuration of this port, enter the following command:

```
#>set line baud=19200 range=xx
```

## Checking the PortServer Settings

- To display the network configuration:

```
#>set config <Enter>
```

- To display the configuration of the IP addresses of ports 1 to 15:

```
#>set altip <Enter >
```

- To display the configuration of the Host ports 1 to 15:

```
#>set port range=1-15 <Enter>
#>set flow range=1-15 <Enter>
```

## Checking the PortServer Network Connection

- You should now be able to establish communications with another network machine (for example the AIX DSM workstation station). Enter the following command:

```
#>ping @IP_PWC<Enter>
```

- The PortServer software should respond:

```
@IP_PWC is alive
```

## Display Current Users of the PortServer

Enter the command:

```
#>who <Enter>
```

The output looks like:

```
tty username nsess    connected_from    connected_to
 16 root          0                local_tty16      local_shell
```

Information includes each user's name and tty, the number of sessions each user is using and where each user is connected from and connected to.

## Useful commands

- On-line help for PortServer's command language is available to you through context-sensitive help screens. Help is available by entering a ? (question mark) either by itself or after part of a command line. The screen will tell you which parameters are available to complete the command line.
- Password modification : use the **newpass** command.
- Boot the PortServer: use the **boot** command.

To reset the PortServer using the current parameters stored in memory, use the command:

```
#>boot action=reset <Enter>
```

To reset the PortServer to factory default settings stored in ROM, use the command:

```
#>boot action=eewrite <Enter> (for PortServer 16-port model)
#> boot action=factory <Enter> (for PortServer TS 16 model)
```

Note that all user configuration will be lost !

- Saving/restoring configuration:

All changes are by default saved to EEPROM memory.

The **cpconf** command allows saving and restoring the configuration of the PortServer to a disk file.

The format of the save file is a list of set commands needed to set up the PortServer in the current configuration. These commands will be read and acted on by the server (just as if the user had typed them on the command line) when the configuration is restored.

You can store and retrieve the configuration file from a host computer that serves TFTP file requests.

To save the configuration to a TFTP server, use the command `cpconf tohost <hostname> <dirname>/<filename>`. `hostname` is the IP address of the host computer and `dirname/filename` is the full path name of the file to be written.

The TFTP server may require that the file already exist and that it is world-writable before the TFTP transfer will be allowed.

For example, the host computer may be the AIX DSM workstation (its IP address is `@IP_PWC`):

- On the AIX DSM workstation:

- Check that `tftpd` daemon is running. If not, start it:

```
uncomment tftp in /etc/inetd.conf
```

```
startsrc -s tftpd
```

- If `/etc/tftpaccess.ctl` file exist, add the following line:

```
allow:<dirname> where dirname is an existing directory name  
(for example, allow:/tmp)
```

- Make the file world-writable:

```
touch <dirname>/<filename> ; chmod 666 <dirname>/<filename>  
for example: touch /tmp/digi ; chmod 666 /tmp/digi
```

- On the PortServer:

```
#> cpconf tohost @IP_PWC <dirname>/<filename>
```

```
for example: cpconf tohost @IP_PWC /tmp/digi
```

PortServer 16-port model displays:

```
TFTP request accepted.  
Line 238  
Closing...  
#>
```

PortServer TS 16 model displays:

```
Transfer Successful.  
#>
```

To restore a configuration saved via TFTP, use the command:

```
cpconf fromhost <hostname> <dirname>/<filename>
```

Restoring the configuration takes quite a bit longer than saving it. This is because writing to the EEPROM that stores the PortServer's configuration is a lot slower than reading.

- On the PortServer:

```
#> cpconf fromhost @IP_PWC <dirname>/<filename>
```

```
(for example: cpconf fromhost @IP_PWC /tmp/digi)
```

PortServer 16-port model displays:

```
TFTP read started  
Line 10 err#17 : bootfile= : invalid value specified.  
Line 237  
TFTP transfer completed.  
#>
```

(don't worry about the error message).

PortServer TS 16 model displays:

```
Line 4: DHCP changes will be valid on next reboot.  
Line 98: Transfer Successful.  
#>
```

On PortServer TS 16 model only, after restoring the configuration, enter the following command to disable again **dhcp**:

```
#> set config dhcp=off <Enter>
```

---

## Using the PortServer to Gain Access to Node Console Ports from the AIX DSM workstation

### Notes:

- A dedicated administration network has no restrictions on addresses. A powercluster public network imposes restriction on addresses. Consult your public network administrator.
- To gain access to a partition of a LPAR server from the AIX DSM workstation, refer to *Using the HMC to Gain Access to Virtual Terminal of a Partition Node from the DSM* on page 1-12.

Refer to Figure 2, on page 1-4.

### On each node

configure an IP address on the Ethernet adapter connected to the administration network.

Connect to the node, using the IP address associated with the port connected to the S1 port of the node:

```
# telnet <@IP1> <Enter> (for example, telnet 1.0.0.11 for port 1 and node#1)
```

Configure the network adapter used to connect the node to the administration network:

```
# smit chinet <Enter>
```

```
INTERNET ADDRESS      [1.0.0.1] (for example node#1)
```

```
Network MASK          [255.0.0.0]
```

Update the */etc/hosts* file with the label associated to this address, for example:

```
1.0.0.1 Node1_adm #@IP (of node 1 on the administration network)
```

To quit, simultaneously hit the **Ctrl** and **]** keys, then type:

```
# q <Enter>
```

Repeat these steps for each node.

### AIX DSM workstation Configuration

Update the */etc/hosts* file with the different addresses configured on the PortServer, for example:

```
1.0.0.10      Concentrator      #@IP (of PortServer itself)
```

```
1.0.0.11      Node1_cons        #@IP (of port 1 connected to S1 or COM1  
port of node1)
```

and so on.

Update the */etc/hosts* file with the different addresses configured on the nodes, for example:

```
1.0.0.1      Node1_adm        #@IP (of node 1 on administration network)
```

```
1.0.0.2      Node2_adm        #@IP (of node 2 on administration network)
```

and so on.

---

## Using the HMC to Gain Access to Virtual Terminal of a Partition Node from the DSM

This applies only to nodes which are partition nodes of a LPAR server .

The AIX DSM workstation and the Hardware Management Console (HMC) must be connected to the same network.

### Updating the /etc/hosts file on the AIX DSM workstation

On the AIX DSM workstation, update the **/etc/hosts** file by adding the IP address of the Hardware Management Console.

### Gaining Access to Virtual Terminal of a Partition Node

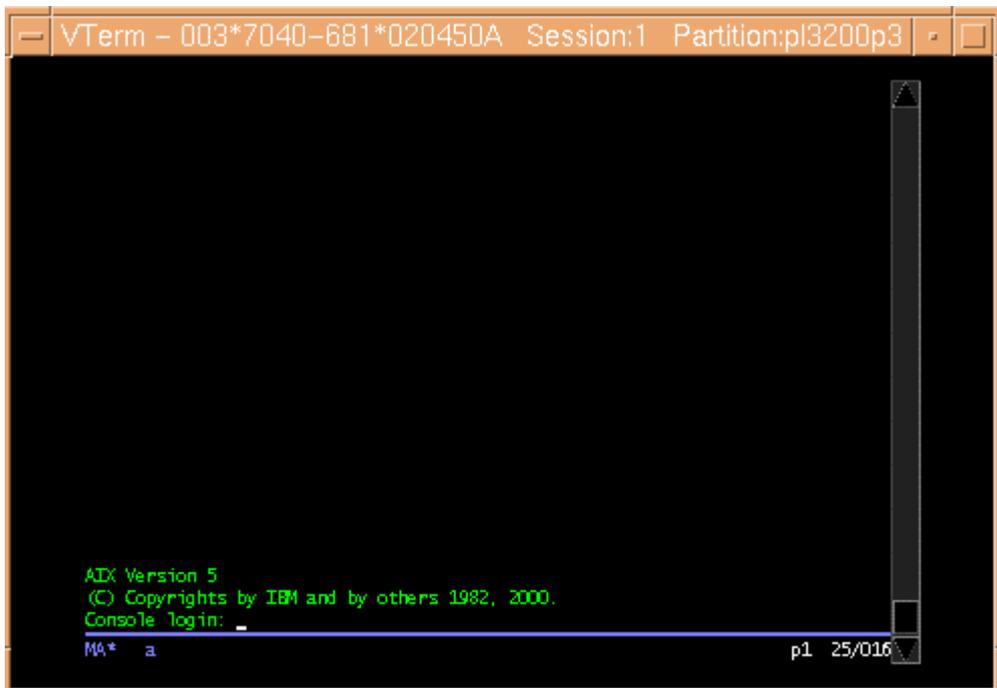
#### First method

Launch **the Hardware Management Console** application on the DSM, in the Cluster Assistant & DSM main window.

Refer to *Hardware Management Console* on page 2-32.

Select **Partition Management** application then click on **Partitions** to see the existing partitions.

Right-click on the partition and select **Open Terminal Window** to open the Virtual Terminal for that partition. The following window appears:



**Figure 5.** Virtual terminal Window.

To close the window, right-click on the partition and select **Close Terminal Window**.

**Note:** You can open only one Virtual Terminal window per partition.

## Second method

To gain access directly to the Virtual Terminal window of a partition node from the DSM, you can invoke the following command with the desired parameters:

```
/usr/sbin/bullcluster/classistant/utils/bclt_telnet_hmc <hmc_addr>  
<port> <partition_id> <model>*<serial_nb> <session>
```

where:

`hmc_addr` is the HMC address

`port` is the port control number of the HMC: fixed value, 9734

`partition_id` is the partition ID

`model` is the model type of the PL3200R

`serial_nb` is the serial number of the PL3200R

`session` is the TTY session number: fixed value, 1

To retrieve partition ID, model type and serial number, refer to *How to retrieve partition ID, model type and serial number*, on page 2-28.

The command **bclt\_telnet\_hmc** establishes a connection through a socket on port 9735 on the HMC, using a specific connection string. Then a telnet connection between the partition and the HMC using port 9734 is established.

## Example

To open a virtual terminal window on the partition number 3 of a PL3200R, model 7040-681, serial number 020450A, managed by HMC named hmc, enter:

```
/usr/sbin/bullcluster/classistant/utils/bclt_telnet_hmc hmc 9734 3  
7040-681*020450A 1
```

To disconnect a session opened with the **bclt\_telnet\_hmc** command, simultaneously hit the **Ctrl** and **]** keys:

```
<CTRL> ]
```

The session is disconnected and returns to the **telnet** program.

Then, after the telnet> prompt, to exit, enter:

```
telnet> q <Enter>
```

---

## Using the AIX DSM workstation

### Advantages

The AIX DSM workstation provides comprehensive OS backup and AIX version management features with savings on the hardware investment. One central tape on the AIX DSM workstation is enough, with no need for a tape device on each Escala powercluster node.

### Options

In addition to the dedicated Administration Network, an optional, extra communications adapter (FDDI, Ethernet, ATM or Token-Ring) can be used to allow the AIX DSM workstation to be connected to the customer's LAN network.

With this option, an X-terminal attached to the customer's network can remotely access the DSM, provided that it is configured to run the Common Desktop Environment (CDE) windows manager of the AIX DSM workstation.

### Remote Maintenance

Details for the use of an AIX DSM workstation with Remote Maintenance connections are in the following document:

- *Escala P Series - EPC Connecting Guide*

### Other User Console Facilities

Although the AIX DSM workstation provides enhanced functionality, other hardware solutions for console handling are available with the Escala P product. These solutions, based on ordinary ASCII terminals or X terminals.

Further information is to be found in **Implementing Other Console Solutions**, in the *EPC and HA Solutions Setup Guide*.

If the AIX DSM workstation can access the same Enterprise network as the X-terminals, one or more of them can be configured for the requesting login services (from the AIX DSM workstation). Setting-up details are to be found in **Customizing the Display Manager** in the *AIX Windows Desktop Advanced User's and System Administrator's Guide*.

---

## Chapter 2. DSM for AIX

Describes the use of DSM for Escala P series.

**Note:** This section applies to both software Distributed Software Management and ClusterAssistant & DSM

---

### Introducing ClusterAssistant & DSM

ClusterAssistant & DSM is a control interface for performing powercluster-wide administration tasks (configuration, operation, control and monitoring).

For a check-list of the normal sequence of operations, see the *Setup Operations* sections, from page 2-4.

Functional details:

- Terminology Used with ClusterAssistant & DSM, on page 2-2.
- Software, on page 2-3.
- Setting-up ClusterAssistant & DSM, on page 2-4.
- ClusterAssistant & DSM Administration and Troubleshooting, on page 2-10.
- Using ClusterAssistant & DSM, on page 2-11.
- ClusterAssistant & DSM Folder, on page 2-14.
- HACMP Cluster Folder, on page 2-17.
- Cluster Configuration Folder, on page 2-19.
- Network Install Manager Folder, on page 2-21.
- Domains Folder, on page 2-23.
- Alarms, on page 2-24.
- System Console, on page 2-27.
- Hardware Management Console, on page 2-32.
- Register Powercluster, on page 2-34.
- Cleanup Application, on page 2-39.
- Check Application, on page 2-40.
- Powercluster State, on page 2-42.
- Cluster Configuration (smit), on page 2-45.
- Link Equipment Application, on page 2-47.
- Multiple Displays on One Screen, on page 2-49.

---

## Terminology Used with ClusterAssistant & DSM

It is important to clearly understand the ClusterAssistant & DSM terminology.

**Objects** used in ClusterAssistant & DSM are defined as follows:



**standalone node**

An Escala server. Its icon name is suffixed by `.node`. For example, if the node name is `foo`, its icon name is `foo.node`.



**HA node**

An Escala server running HACMP. Its icon name is suffixed by `.node`.



**HACMP cluster**

A set of HA nodes managed by HACMP. Its icon name is suffixed by `.cluster`.



**powercluster**

All the nodes to be managed from the DSM with ClusterAssistant & DSM. Its icon name is suffixed by `.epc`.

**domain** An object instance of type: powercluster, HACMP cluster, HA node, standalone node.

**cluster** A synonym for HACMP cluster.

**node** A generic term for HA node or standalone node.

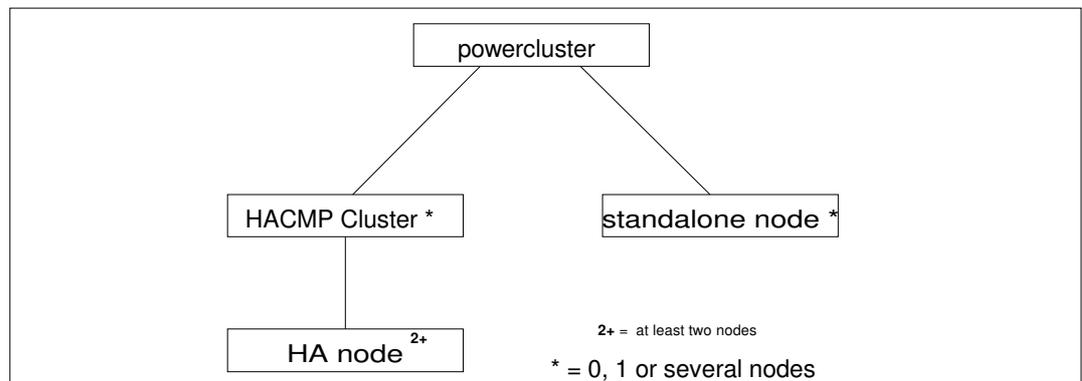
**cluster node** A generic term for an HA node of an HACMP cluster.

**Notes:**

1. The powercluster is made of zero, one or several standalone nodes and/or zero, one or several HACMP clusters.
2. An HACMP cluster is made of two or more HA nodes.

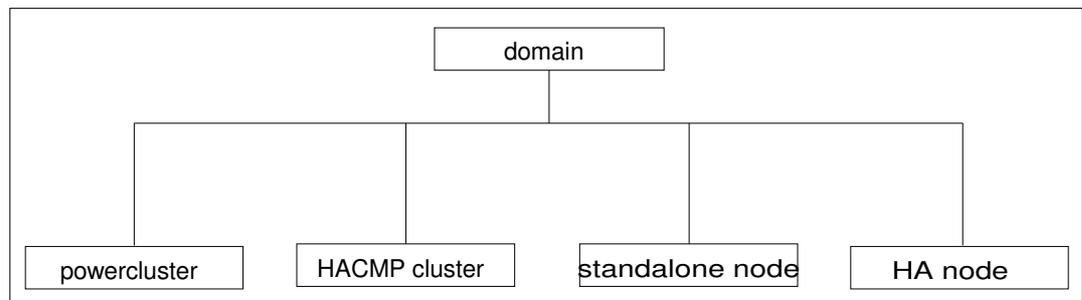
## Relationships Between Objects

The following figure illustrates the relationship between objects showing the scope of application.



**Figure 6.** Scope of Application Between Objects

The following figure shows the domain types.



**Figure 7.** Types of Domains

---

## Software

ClusterAssistant & DSM is packaged, on a CD-ROM, as a set of Licensed Program Products (LPP) which have to be installed selectively on the AIX DSM workstation and each node.

Refer to the ClusterAssistant & DSM *Software Release Bulletin* for software installation details.

---

## Setting-up ClusterAssistant & DSM

This section summarizes the different steps related to DSM and ClusterAssistant & DSM that you must perform when initially setting up a Powercluster. If you are about to set up a Powercluster equipped with a DSM, use the list of steps below as a roadmap to the tasks you must perform.

Before attempting the installation of ClusterAssistant & DSM, set up the AIX DSM workstation (see page 1-3).

The following setup procedures are guidelines only. For detailed information see further in this guide.

### Setup Operations for SMP Servers (without HMC)

In the following procedures we assume that:

- the PortServer, the AIX DSM workstation and the nodes are connected to the network,
- the PortServer ports (1, 2, ...) are connected to the S1 or COM1 console ports of nodes.

Follow these steps:

1. Boot and set up the PortServer base parameters using the ASCII terminal connected to the administrative port of the PortServer. (See *Setting up the PortServer* on page 1-6).
2. On the AIX DSM workstation, copy the update the `/usr/sbin/bullcluster/classistant/data/devices.config` file by adding an entry for the IP address of the PortServer (optionally, update the `/etc/hosts` file). (See *Setting Up the devices.config File*, on page 2-9).
3. From the DSM, configure the PortServer ports using the **Link Equipement** application of Cluster Assistant & DSM. Ports are connected either to S1 or COM1 ports of nodes.

Perform steps 4 to 6 for each node.

4. From the DSM, open system console of a node with the application **System Console** (if the node is not yet registered on DSM, select `NODE_NOT_YET_REGISTERED` item in the list, and enter the IP address assigned to the PortServer port for the S1 or COM1 port of that node)
5. Boot the node. From the DSM, follow the boot phases of the node in the system console window previously opened for that node.
6. When the boot is completed, log on the node and configure its Ethernet network using `smit`; update the `/etc/hosts` file with the new interface name and address and update `.rhosts` file to give access to user `root` and `classist` from the DSM.

Return to step 4 for another node.

7. On the AIX DSM workstation, update the `/etc/hosts` file and `.rhosts` file of user `root` and `classist` for the node (see page 2-8).
8. **Register** the **powercluster** and its nodes using the **Register Powercluster** application, (see on page 2-34). From this step, the access to the basic applications of ClusterAssistant & DSM is available:
  - Rlogin
  - WatchWare from DSM
  - SMIT from DSM
  - Alarms
  - Powercluster State
  - ...

9. If **Network Installation Management (NIM)** is required for distributing software on the powercluster nodes and for backup/restore operations, set up the NIM configuration using the **NIM Setup Assistant** application (see on page 2-21).
10. If **HACMP clusters** are **already configured**, register them using the **Register Cluster** Application (see on page 2-19). The HACMP clusters will then be manageable from the DSM.
11. If **HACMP clusters** are **not yet configured**, use the **Cluster Configuration (smit)** application to automatically configure and register the clusters (see on page 2-45).
12. When **HACMP cluster registration is completed**, the HACMP–related applications in the **Cluster Configuration** folder (see on page 2-19), are made available:
  - Start Cluster Services
  - Stop Cluster Services
  - ClusterWatch
  - Cluster Diagnostics
  - ... etc..

## Setup Operations for LPAR Servers (with HMC)

In the procedure below, we assume that:

- your configuration includes an LPAR server with its Hardware Management Console (HMC).
- partitions are already defined on the server and are in a 'Ready' state and each partition has a network adapter assigned.
- the Hardware Management Console (HMC), the AIX DSM workstation and partitions are connected to the same network.

Follow the steps described below:

1. On the AIX DSM workstation, update the **/etc/hosts** file by adding an entry for the IP address of the HMC.
2. From the DSM, open system console of a partition node (virtual terminal) with the application **System Console** (if the partition node is not yet registered on DSM, select **NODE\_NOT\_YET\_REGISTERED** item in the list, select LPAR Node(s) option and enter an address with the following syntax:

```
hmc address;partition id;model;serial number
```

where:

- `hmc address` is the address of the HMC
- `partition id` is the partition id of the partition node
- `model` is the model type of the LPAR server
- `serial number` is the serial number of the LPAR server

See *How to retrieve partition ID, model type and serial number* on page 2-28 for further information.

3. From the ClusterAssistant & DSM, if you want to install AIX on that partition node, follow the instructions described in **NIM Setup Assistant** application under item **Installing AIX in a LPAR Environment**.
4. Configure NIM environment:
  - configure the NIM master,
  - create the file structure for storing NIM resources,
  - create the basic NIM resources needed for a BOS installation,

- define the partition node as a NIM client,
  - define NIM machine group for the partitions.
5. Perform AIX installation on the partitions from the DSM:
- initiate the AIX installation on the partitions the DSM,
  - activate the partitions using the **Hardware Management Console** application to boot in *SMS* mode,
  - initiate the network boot from *SMS menu* for each partition you want to install in opened system console (virtual terminal).
6. - Perform further configuration of the partitions when installation is finished:
- change the boot mode of the partition profile associated to the partitions you are installing to *Normal* otherwise, they will show the *SMS menu* for every reboot,
  - edit the topology file `/usr/sbin/bullcluster/classistant/data/node.config` to add the partitions you have just installed for further NIM utilisation,
  - perform installation of additionnal LPP on your partitions **using Software Distribution Assistant** application.

Then continue performing the tasks described in the previous section, from step 5.

## Set-up Summary

### Step 1: Set Up the AIX DSM workstation and the Escala P series Hardware

Refer to *Setting-up the AIX DSM workstation*, on page 1-3.

### Step 2: Set Up ClusterAssistant & DSM

This step consists of the following tasks:

- Check that the required software is pre-installed on the AIX DSM workstation and the nodes (if you are installing a new Escala P series, this should be the case, since software pre-installation is normally performed at the factory). For details, see *Checking that ClusterAssistant & DSM is Pre-installed*, on page 2-7.
- Set up the password for the new UNIX user **classist**, created during the software installation phase. For details, see *Setting Up the "classist" User Password*, on page 2-8.
- Set up `/etc/hosts` and `.rhosts` files as appropriate (on the AIX DSM workstation and on the nodes). For details, see *Updating /etc/hosts and /.rhosts Files*, on page 2-8.

From now on, you can use a number, but not all, of ClusterAssistant & DSM features:

- NIM
- Link Equipment

### Step 3: Register Powercluster

This step consists of defining the powercluster, i.e. all the nodes to be managed from the DSM with ClusterAssistant & DSM. For details, see **Register Powercluster**, on page 2-34.

### Step 4: Configure the HACMP Cluster Topology

This step consists in defining the HACMP cluster topology. You can take advantage of ClusterAssistant & DSM, which provides handy access to the different cluster configuration tools (HACMP tools as well as BullCluster tools). For details, see *Configuring the HACMP Cluster Topology*, on page 2-8.

Repeat this step for each HACMP cluster.

In addition, refer to *Configuring the Cluster Topology* in the *EPC & HA Solutions Setup Guide*.

## Step 5: Complete Setup of ClusterAssistant & DSM

This step consists of the following tasks:

- Set up the `/usr/sbin/bullcluster/classistant/data/devices.config` configuration file on the AIX DSM workstation. This file is used to declare the correspondence between Interconnect devices (switches and hubs) and IP addresses used to access these devices. For details, see *Setting Up the devices.config File*, on page 2-9.

## Step 6: Complete the HACMP Cluster Setup

This step consists of tasks like setting up HACMP application servers and resources, setting up LVM components (volume groups...), and so on. You can perform all these tasks from the DSM, using the utilities of ClusterAssistant & DSM. Once this is done, your HACMP cluster is ready to operate.

Refer to **Completing the Cluster Setup** in the EPC & HA Solutions Setup Guide.

## Checking that ClusterAssistant & DSM is Pre-installed

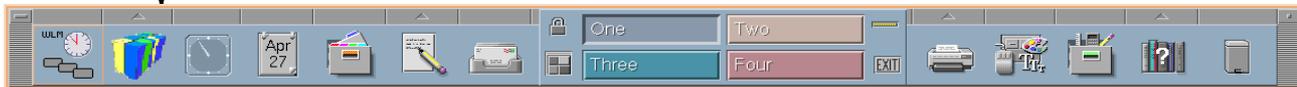
You may want to check that the required software is preinstalled on the DSM and the nodes. If you are installing a new Escala P series, this should be the case, since software pre-installation is normally performed at the factory.

Proceed as explained below.

### Check that ClusterAssistant & DSM is Pre-installed on the DSM

1. On the AIX DSM workstation, login as the **root** user.
2. Check for the presence of the ClusterAssistant icon in the front panel of the CDE desktop.

↓ If ClusterAssistant is installed, you should see this icon.



**Figure 8.** CDE Front Panel showing ClusterAssistant Icon

If the icon is not present, ClusterAssistant & DSM is not installed on the DSM.

Refer to the *Software Release Bulletin (SRB)* that comes with the ClusterAssistant library software. It includes the procedure to install the software.

## Checking that bclwd Daemon is Running on DSM & HA Nodes

Many ClusterAssistant & DSM utilities rely on the BullCluster **bclwd** daemon, which continuously runs on the DSM and the HA nodes.

When the BullCluster software is installed (on the cluster nodes and on the DSM), an entry is automatically added to the `/etc/inittab` file, so that the **bclwd** daemon is automatically started whenever the system boots.

Check that the daemon is running using the following AIX command:

```
lssrc -s bclwd
```

This command (to be run on the cluster nodes and on the DSM) should show the **bclwd** daemon with the "active" status. If this is not the case, refer to the *Software Release Bulletin* for installation instructions.

**Note:** The **bclwd** daemon is integrated with the AIX System Resource Controller (SRC), so that you can use the **lssrc**, **startsrc** and **stopsrc** AIX commands to manage it.

## Setting Up the "classist" User Password

Login as **root**.

Use the standard AIX method to set a new UNIX password for **classist** user.

Logout.

Login as **classist** user.

## Updating /etc/hosts and /.rhosts Files

ClusterAssistant & DSM (and the **bclwd** daemon) must be able to access all the nodes in order to run the required commands.

Consequently, for ClusterAssistant & DSM to work properly, you have to update the */etc/hosts* and */.rhosts* files on the AIX DSM workstation and on all the nodes, as explained below.

### Updating /etc/hosts

Login as **root**.

Edit the */etc/hosts* files on the different involved machines (AIX DSM workstation and cluster nodes):

- Add entries for the different network addresses (boot or persistent, service, standby) for cluster nodes only and specify the network addresses for each standalone node.
- Also add an entry for the AIX DSM workstation address.
- Add an entry for the HMC address if you have a LPAR server.

### Updating /.rhosts

Login as **root**.

Edit the */.rhosts* files on the different involved machines (AIX DSM workstation and nodes):

- Add entries for the different network interfaces (boot, service, standby) for cluster nodes only and specify the network interface for each standalone node, with access rights granted to **root**.
- Add an entry for the AIX DSM workstation, with access right granted to **root**.
- Add an entry for the AIX DSM workstation, with access right granted to **classist**.
- On the cluster nodes, the */.rhosts* file must (in addition to the entries above) also include the following entry (for the local loopback interface):

```
127.0.0.1 root
```

## Registering Powercluster

A powercluster can be registered, modified or removed from ClusterAssistant & DSM using this utility which is accessed through its icon in the **Application Manager - ClusterAssistant** group. For details, see *Register Powercluster*, on page 2-34.

## Configuring the HACMP Cluster Topology

To define the HACMP cluster topology for the cluster you are setting up, you can take advantage of ClusterAssistant & DSM, which provides handy access to the different cluster configuration tools (HACMP tools as well as BullCluster tools). Note the following:

- The cluster configuration tools can be brought up through the icons of the **Cluster Configuration** sub-folder of the **HACMP Cluster** folder of the ClusterAssistant & DSM application group.
- To define the HACMP cluster topology, you may want to use one of these icons:
  - **Cluster Configuration** (smit): up the Quick Configuration graphical utility.

- **Cluster Worksheets** : Calls up **Cluster Worksheets**, which is a standard configuration utility that comes with HACMP. This utility is based on the VSM (Visual System Management) interface.

Equivalent SMIT menus for these functions are also available.

For information about configuring the HACMP cluster topology, refer to “Configuring the Cluster Topology” in the EPC & HA Solutions Setup Guide.

**Notes:**

1. Registration is automatic when using **Cluster Configuration (smit)**.
2. In all other applications, the newly-configured HACMP cluster must be manually registered using the **Register Cluster** application.

## Use of DSM with Dedicated Administration Networks

For details, see *AIX DSM workstation Typical Configuration*, on page 1-3.

## Register an HACMP Cluster with ClusterAssistant & DSM

For an HACMP cluster to be fully manageable through ClusterAssistant & DSM features, the cluster must be registered with ClusterAssistant & DSM. This task is to be performed once the cluster topology has been defined for HACMP.

To register a cluster with ClusterAssistant & DSM, use the **Register Cluster** icon.

- This icon is in the **Cluster Configuration** sub-folder of the **HACMP Cluster** folder of the ClusterAssistant & DSM application group.
- When you activate the icon, you are prompted to designate a node of the cluster to be registered. Enter the node name of any server which is member of the cluster.

For further information, refer to the online help for the **Register Cluster** icon.

## Setting Up the devices.config File

The **Link Equipment** facility requires that the configuration file `/usr/sbin/bullcluster/classistant/data/devices.config` must also be configured on the AIX DSM workstation.

A template **devices.config\_template** is provided to help the user to write this file. An entry has the following format:

```
<device_name>:<device_type>:<device_IP_address>
```

Where `device_name` is the name of the device (in alpha-numeric characters and underscore `_`) and `device_type` is one of the following:

- `fddi_hub`
- `fddi_switch`
- `ethernet_hub`
- `fast_ethernet_switch` (for switch 3000)
- `fast_ethernet_switch` (for switch 3300)
- `gigabit_ethernet_switch` (for switch 9300)
- `gigabit_ethernet_sw4900` (for switch 4900)
- `brocade-fibre-switch`
- `other_equipment`
- `other_equipment_telnet` (for telnet)
- `port_server`

and `device_IP_address` is the address of the equipment.

Example: `PORTSERVER_01: digi_port_server:120.154.33.56`

---

## ClusterAssistant & DSM Administration and Troubleshooting

### bclwd Daemon Troubleshooting

If you experience problems with the **bclwd** daemon, see *Check that the bclwd Daemon is Running*, on page 2-7, we suggest that you stop it, and then you restart it, using successively the following two AIX commands:

```
stopsrc -s bclwd
startsrc -s bclwd
```

The **bclwd** daemon logs errors to the file `/var/bullcluster/bclwd.log`.

See also the *Software Release Bulletin* that comes with the Escala P series and DSM.

### /etc/hosts and /.rhosts Files

Keep in mind that, for ClusterAssistant & DSM to work properly, the `/etc/hosts` and `/.rhosts` files must be maintained with the appropriate entries, see *Updating /etc/hosts and /.rhosts Files*, on page 2-8.

#### Special Alias in /etc/hosts for the DSM

When an HACMP cluster is registered with ClusterAssistant & DSM, the **Register Cluster** utility adds an alias to the `/etc/hosts` file of the AIX DSM workstation. This alias is the name of the registered cluster.

For example, assume that the hostname of the AIX DSM workstation is `bird`. Then, the `/etc/hosts` initially contains an entry like the following:

```
120.154.33.65  bird
```

When a cluster is registered with the `foobar` name, the previous entry is changed as follows:

```
120.154.33.65  bird  foobar
```

When another cluster is also registered with the `xyz` name, the previous entry is changed as follows:

```
120.154.33.65  bird  foobar  xyz
```

These changes are made so that, when you use the ClusterWatch Web-based monitoring application, you can specify a cluster name in the host part of the URL

#### Notes:

1. This special behavior is mentioned here because it may cause a conflict if a host on the network has a name which is also the name of a cluster registered with ClusterAssistant & DSM.
2. For detailed information about ClusterWatch, refer to the *Powercluster Cluster Management Tools: ClusterWatch* document.

### ClusterWatch and WatchWare Passwords

The ClusterWatch and WatchWare Web-based monitoring applications are protected through passwords. When the application prompts you for a name and a password, enter respectively **smwadmin** and **bullsmw**.

**Note:** For enhanced security, it is recommended that you change the default password. To do so, perform specific procedure described in ClusterWatch and WatchWare user documentation.

In the event of the loss of a password, refer to the *Software Release Bulletin* for the DSM Library. The full recovery procedure is detailed in the *WatchWare Server Monitor User's Guide*.

---

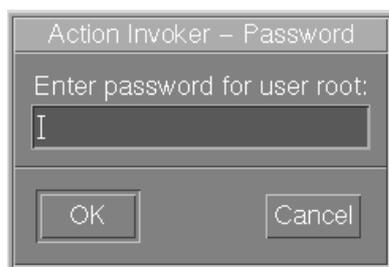
## Using ClusterAssistant & DSM

### Users

The **classist** user can only access and run all of the monitoring applications of ClusterAssistant & DSM:

- Alarms  
The **classist** user can use **Alarms** to display Alarms, but only the **root** user can clear Alarms. An error message is displayed if the **classist** user tries to clear Alarms.
- Cluster Diagnostics
- Powercluster State
- ClusterWatch (Web interface)
- ClusterWatch (SMIT interface).

For other applications, the root password is required within the Action Invoker window:



**Figure 9.** Action Invoker Window

The **root** user on the AIX DSM workstation can access and run all of the applications of ClusterAssistant & DSM.

### Function Selection

Functions are selected using the mouse cursor and clicking once, or double-clicking, on the icon representing the desired facility.

#### Drag and Drop Capability

Most of the ClusterAssistant & DSM applications support the drag and drop capability of CDE. Instead of double-clicking on the icon, a domain icon can be dragged and dropped on the desired application.

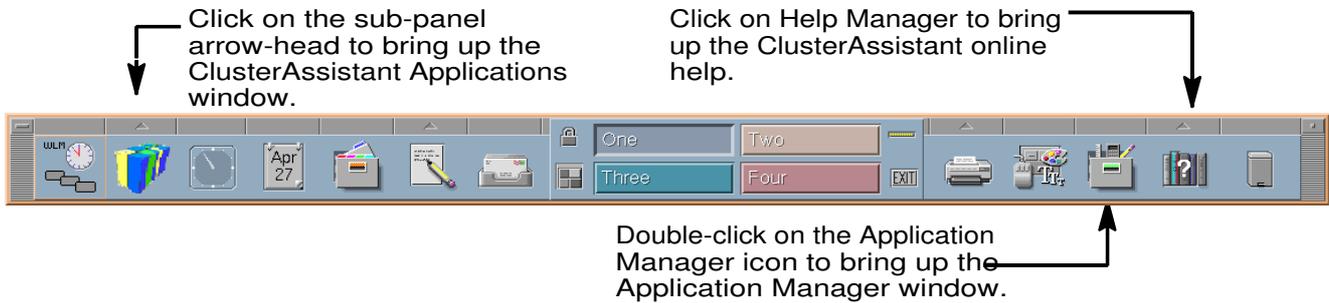
The icons for powercluster, HACMP clusters, HA nodes and standalone nodes are stored in the Domains folder when the powercluster has been **registered** and when the HACMP clusters have been **registered** with ClusterAssistant & DSM

To select two or more domains, click once on the first icon, then maintain the **Control key** pressed on the keyboard while clicking once on the second (and subsequent) icons. Drag and drop the selected icons as required.

ClusterAssistant & DSM applications have their own domain scope. An error message is displayed when a domain icon, out of the scope of the application, is dropped.

## Front Panel - Common Desktop Environment

Within the CDE, a Front Panel is displayed across the bottom of the screen and is present on all workspaces, Figure 10:



**Figure 10.** CDE Front Panel

Frequently used applications can be put in the front panel or in one of the workspaces. Refer to Common Desktop Environment documentation for more details.

### How to View Online Help

ClusterAssistant comes with extensive contextual online help information, available from the **Help Manager** in the CDE front panel or from the **Help** button of the current operational window.

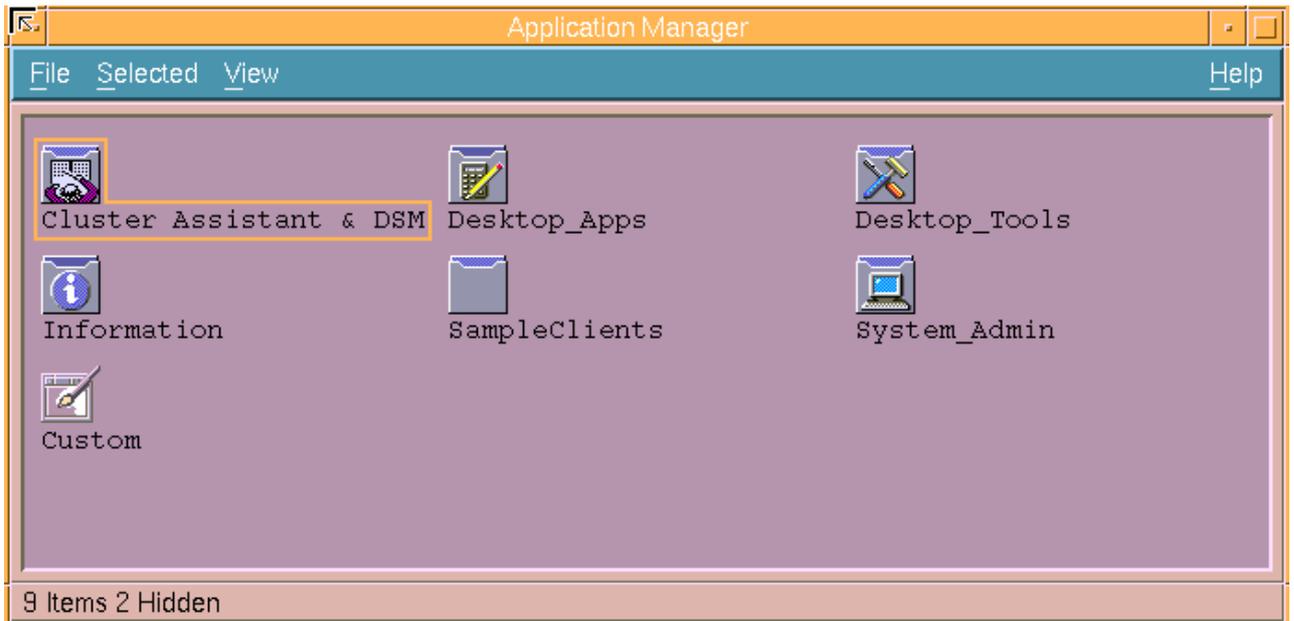
### How to Bring Up the ClusterAssistant Application Group

Applications within ClusterAssistant are accessible through graphic icons which are stored in nested folders. Access to these folders is via the **Cluster Assistant Applications** window, opened in various ways. By a single click on the sub-panel arrowhead, to open the **ClusterAssistant & DSM Applications** window, Figure 11. Or by a double-click on the Application Manager icon, to open the Application Manager window, Figure 12.



**Figure 11.** ClusterAssistant & DSM Applications Window

The ClusterAssistant & DSM Applications window displays a list of icons corresponding to some ClusterAssistant applications and to the ClusterAssistant folder. Double-click on an icon to open the selected function.



**Figure 12.** Application Manager Window Showing Icons for Application Group Folders

## Launching a ClusterAssistant Application

A ClusterAssistant Application can be launched in one of the following ways:

- dragging of a domain icon and dropping it on the application icon
- double-clicking on the application icon, then selecting a domain from the displayed list.
- single-clicking with the right-hand mouse button on a domain icon and selecting the desired application in the displayed list.

## ClusterAssistant Folder

From either the **ClusterAssistant Applications** window or the **Application Manager** window, double-click on the **ClusterAssistant** folder icon to open the **Application Manager - ClusterAssistant & DSM** window, as shown below.



**Figure 13.** Application Manager - ClusterAssistant & DSM Window

Some applications can accept several types of domain as input data.

## ClusterAssistant & DSM Applications

### HACMP Cluster

For details, see page 2-17.

### Network Install Manager

For details, see page 2-21.

### Domains

For details, see page 2-23.

## Register Powercluster

**Scope of application** - **input** NONE, **output** standalone node, powercluster.

Allows the registration, modification and removal of a powercluster from ClusterAssistant & DSM. See *Register Powercluster*, on page 2-34.

## System Console

**Scope of application** - HA node, standalone node, HACMP cluster, powercluster, NONE.

Also accessible from the **ClusterAssistant & DSM Applications** window, Figure 11.

Allows the connection to an AIX console system of a standalone node or HA node by means of a telnet session using the PortServer or the HMC for LPAR servers. See *Setting up the PortServer*” on page 1-6).

See *System Console*, on page 2-27.

## Hardware Management Console

**Scope of application** – NONE.

Launches the WebSM interface of the Hardware Management Console.

See *Hardware Management Console*, on page 2-32.

## Rlogin

**Scope of application** - HA node, standalone node, HACMP cluster, powercluster.

Provides an easy way to connect to a given node, by running *rlogin* in a terminal window. IP addresses/names currently available to access to the desired node are automatically determined and proposed for selection.

Opens a remote login session on all the nodes of a selected domain. The application is started separately for each node of the domain.

If the node can be reached by different addresses, one of these addresses can be selected for a **rlogin session**.

## Powercluster State

**Scope of application** - HA node, standalone node, HACMP cluster, powercluster.

Displays the state of HACMP clusters and standalone nodes. See *Powercluster State*, on page 2-42.

## SMIT from DSM Server

**Scope of application** - HA node, standalone node.

Gives access the local administration tools of a node (SMIT). Starts a SMIT interface on a specified node.

## WatchWare from DSM Server

**Scope of application** - HA node, standalone node.

Launches WatchWare on a specified node.

## Link Equipment

**Scope of application** - NONE.

Launches a Telnet session. Allows configuration of interconnected devices.

See *Link Equipment Application* , on page 2-47.

## Alarms Application

**Scope of application** - powercluster.

Monitors the powercluster for the occurrence of:

- permanent hardware errors (logged in AIX errlog files)

- HACMP events:
  - node\_up
  - node\_down
  - network\_down
  - Fail\_standby
  - swap\_adapter
  - EVENT FAILED.
- user-defined alarms.

Also accessible from the **ClusterAssistant & DSM Applications** window, Figure 11.

**Note:** Alarms are automatically configured when registering a powercluster and HACMP clusters.

The alarm mechanism is based on RSF; RSF sends alarms to the DSM.

The alarm file on the DSM is associated with a control on the front panel which changes appearance when the file is modified to alert the user.

See also *Monitoring Alarms with the Alarms Capability*, on page 2-24.

The **Alarms** main window lists the HACMP clusters and standalone nodes on which problems occur.

A node or cluster can be selected to examine alarms (**Show Alarms** button) or to remove alarms (**Clear Alarms** button).

The **Configure User Alarms** button allows any ASCII files to be scanned for specific messages and provides warning of the occurrence of these messages in the **Alarms** application.

If there is no longer an alarm, the associated control in the front panel changes to the no-alarm icon.

## Cleanup

**Scope of application** - standalone node, HACMP cluster, powercluster.

Brings up a utility that allows the clean up of registered nodes and/or HACMP clusters when normal deregister operations fail.

See **Cleanup**, on page 2-39.

## Check

**Scope of application** - NONE.

Brings up a utility that helps with debugging. It checks that the DSM, nodes and HACMP clusters are correctly configured for Cluster Assistant applications.

See **Check**, on page 2-40.

---

## HACMP Cluster Folder

This folder contains applications available for HACMP clusters only.

From the **Application Manager - ClusterAssistant & DSM** window, Figure 13, click the **HACMP Cluster** folder icon to open the **Application Manager - HACMP Cluster** window:



**Figure 14.** Application Manager - HACMP Cluster Window

## HACMP Cluster Applications

### Cluster Configuration

Details, see page 2-19.

### Cluster Diagnostics

**Scope of application** - HACMP cluster.

Brings up a utility that provides diagnostics information about an HACMP cluster. These diagnostics apply to AIX, HACMP and CX.

### Cluster Users & Groups

**Scope of application** - HACMP cluster.

Brings up a standard, SMIT-based HACMP utility providing menus to manage users and groups in an HACMP cluster.

### ClusterWatch

**Scope of application** - HACMP cluster.

Brings up the Web-based version of this monitoring facility allowing the monitoring of HACMP cluster operations. ClusterWatch provides synthetic and detailed information on the status and configuration of the different HACMP cluster components.

## **ClusterWatch SMIT**

**Scope of application** - HACMP cluster.

Brings up the SMIT-based version of this monitoring facility. To be used when there is no Web browser installed on the AIX DSM workstation.

## **Start Cluster Services**

**Scope of application** - HACMP cluster.

Calls up the utility displaying a dialog window allowing the user to start HACMP cluster services on one node or all nodes of a given HACMP cluster.

## **Stop Cluster Services**

**Scope of application** - HACMP cluster.

Calls up the utility displaying a dialog window allowing the user to stop HACMP cluster services on one node or all nodes of a given HACMP cluster.

## Cluster Configuration Folder

From the **Application Manager - HACMP Cluster** Window, Figure 14, click the **Cluster Configuration** folder icon to open the **Application Manager - Cluster Configuration** window:

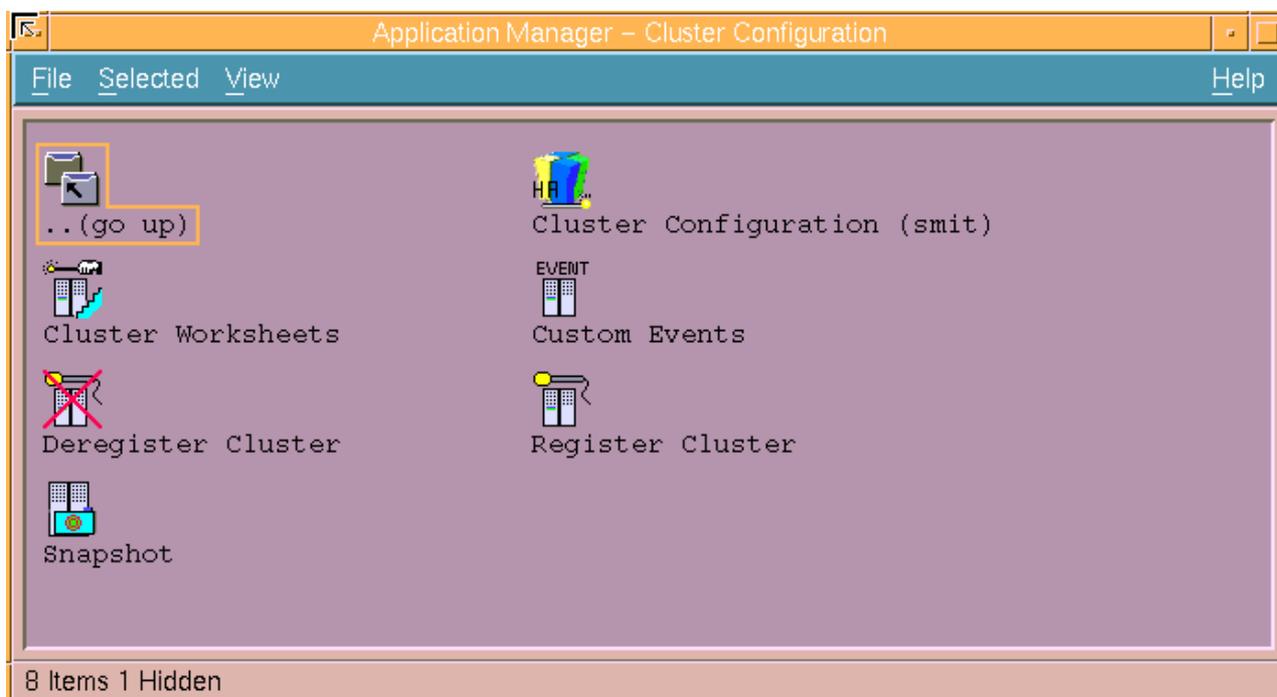


Figure 15. Application Manager - Cluster Configuration Window

## Cluster Configuration Applications

### Custom Events

**Scope of application** - HACMP cluster.

The icon calls up the **Cluster Events** SMIT menu.

Cluster events can be customized using the **Define Custom Cluster Events** SMIT menu and then the **Change/Show Cluster Events** SMIT menu.

**Note:** Do not forget to synchronize cluster resources.

### Snapshot

**Scope of application** - standalone node, HA node, HACMP cluster.

**Scope of application** - standalone node, HA node, HACMP cluster.

Calls up **snapshot**, a standard utility that comes with HACMP. This SMIT-based utility allows you to save in a file a record of all the HACMP data (cluster topology and resource ODM classes) that defines a cluster, as well as a record of cluster state information.

### Register Cluster

**Scope of application** - **input** standalone node, **output** HACMP cluster.

Calls up the utility to register an HACMP cluster. Once registered, an HACMP cluster can be managed using the various ClusterAssistant & DSM utilities.

A new icon, representing the registered HACMP cluster, appears in the **Domain** folder and icons representing the cluster nodes are changed to HA node icons.

Configures **Alarms** for HACMP events.

**Notes:**

1. This utility is called automatically by the **Cluster Configuration (smit)** application, see page 2-45.
2. If the HACMP cluster has been configured with another utility (Cluster Worksheets, SMIT, ...) the user must explicitly call **Register Cluster**.

**Deregister Cluster**

**Scope of application** - **input** HACMP cluster, **output** standalone node.

Calls up the utility to deregister an HACMP cluster. Once deregistered, an HACMP cluster can no longer be monitored and managed using the various ClusterAssistant & DSM utilities.

Deconfigures **Alarms** for HACMP events.

Called by **Register Powercluster** automatically when an powercluster domain is removed.

**Note:** Must be called before deconfiguring an HACMP cluster.

If Deregister Cluster fails, use Cleanup application to remove the cluster definition on the DSM.

**Cluster Configuration (smit)**

**Scope of application** - **input** standalone node, HACMP cluster, **output** HACMP cluster.

Utility used to define the HACMP cluster topology at initial HACMP cluster time.

For details, see **Cluster Configuration (smit)**, on page 2-45.

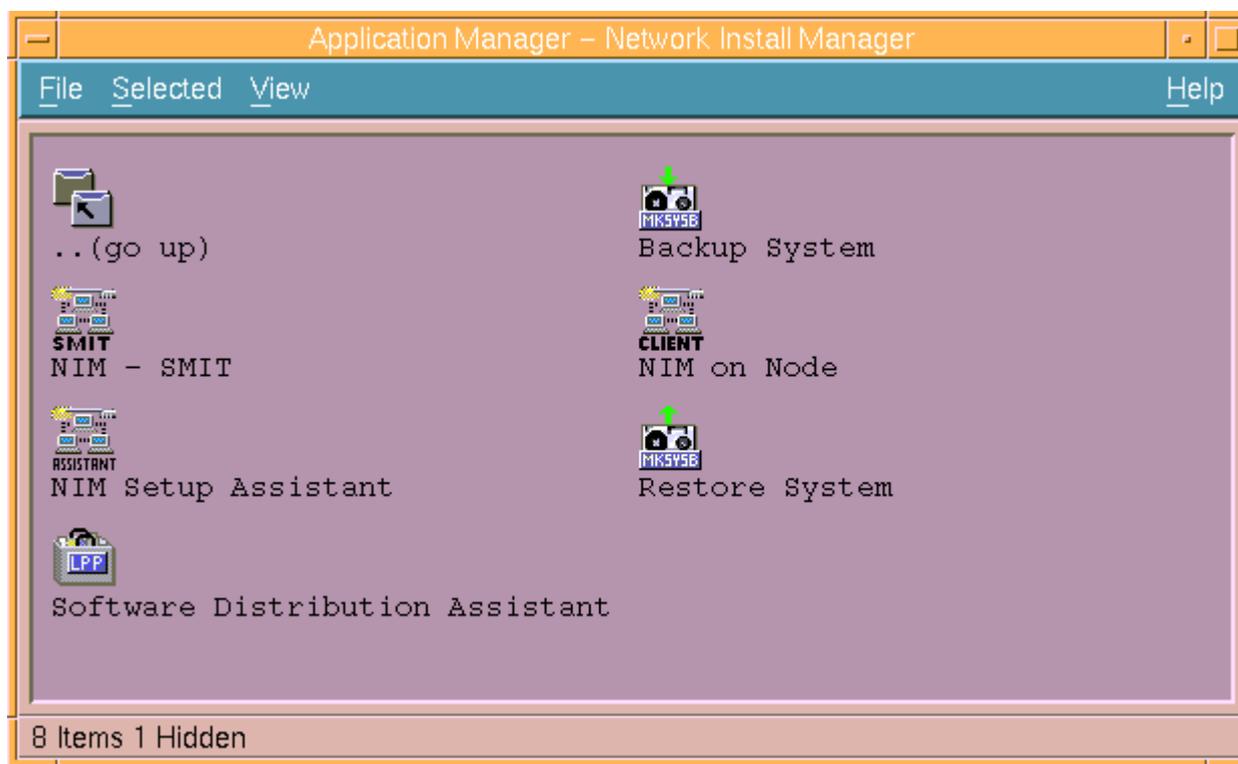
**Cluster Worksheets**

**Scope of application** - **input** standalone node, HACMP cluster, **output** HACMP cluster.

Calls up **Cluster Worksheets**, which is a standard configuration utility that comes with HACMP. This utility, based on the VSM (Visual System Management) interface, is optionally used to initially set up a cluster and to maintain its configuration.

## Network Install Manager Folder

From the **Application Manager - ClusterAssistant & DSM** window, Figure 13, double-click the **Network Install Manager** icon to open the **Application Manager - Network Install Manager** window:



**Figure 16.** Application Manager - Network Install Manager Window

The integration of NIM enables software to be distributed between nodes and allows **rootvg** Backup/Restore files to be created on the disk of the AIX DSM workstation, removing the need for tape backup for each node.

The AIX DSM workstation is both NIM Master and NIM Server.

## Network Install Manager

The Network Install Manager window contains icons you can use to call up the various utilities of the Network Install Manager application group.

The **Help** button provides more detail.

### NIM Setup Assistant

Guides you through the tasks needed to configure NIM on a powercluster.

You must be a **root** user to access the NIM Setup Assistant.

The main steps are as follows:

- AIX DSM workstation is configured as **NIM Master** and **NIM Resource Server**
- powercluster nodes are configured as **NIM Clients**
- creation of NIM resources for Backup/Restore (LPP\_SOURCE, SPOT, MKSYSB).
- creation of NIM resources for Base Operating System installation (LPP\_SOURCE, SPOT, MKSYSB, INSTALLP\_BUNDLE).

**Note:** Special considerations, depending on hardware and software configurations, are detailed in the on-line help.

Once this configuration is completed, go to the **Software Distribution Assistant** tasks.

### Backup System

Provides a graphical, interactive, application of the Network Install Manager to create system backup made on the disk of the AIX DSM workstation.

### Restore System

Provides a graphical, interactive, application of the Network Install Manager to perform system restore.

### NIM - SMIT

Brings up the SMIT-based version of the Network Install Manager on the AIX DSM workstation (NIM Master).

### NIM on Node

Brings up the SMIT-based version of the Network Install Manager on a Node (NIM Client).

---

## Domains Folder

From the **Application Manager - ClusterAssistant & DSM** window, Figure 13, double-click the **Domains** icon to open the **Application Manager - Domains** window, Figure 17.

Objects managed by ClusterAssistant & DSM are logically grouped into **domains**. The different domain types are defined in *Terminology Used with ClusterAssistant & DSM*, on page 2-2.

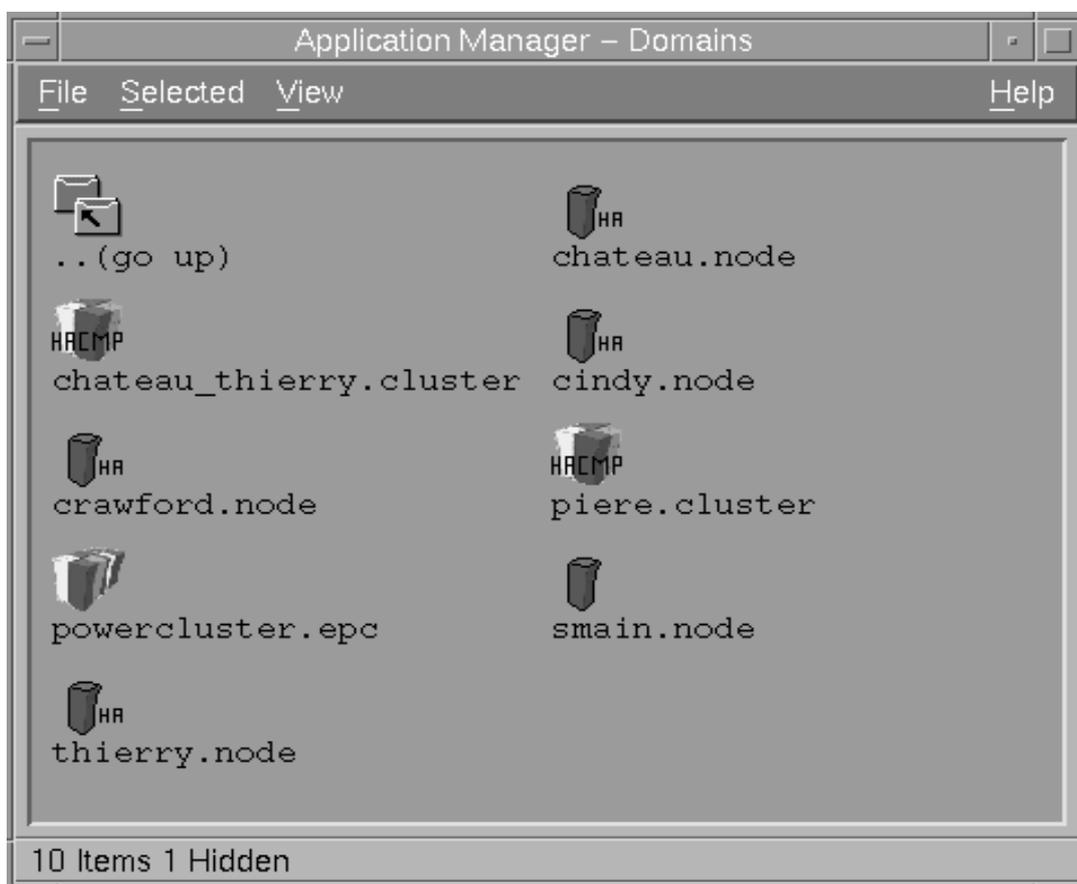
### Example of Domains Folder

A typical example of the contents of such a folder is shown in Figure 17:

- a powercluster (powercluster)

**Note:** Only one powercluster can be registered and managed with ClusterAssistant & DSM. See *Relationships Between Objects*, on page 2-3

- one standalone node (**smain**)
- two HACMP clusters of 2 nodes (**piere**, **chateau\_thierry**)



**Figure 17.** Content of Domains Folder (Typical)

Domain icons can be dragged and dropped on actions in ClusterAssistant & DSM application group. See *Drag and Drop Capability*, on page 2-11.

---

## Alarms

The **Alarms** application permits the monitoring of a cluster for detection of the following alarms:

- permanent hardware errors logged in the AIX errlog of a node
- any of these following HACMP events:
  - node\_up
  - node\_down
  - network\_down
  - swap\_adapter
  - fail\_standby
  - EVENT\_FAILED (or an event provoking this chain of characters)
- user-defined alarms.

**Alarms** requires that the Filesets of Remote Services Facilities (RSF) are installed on the powercluster nodes. This should be the case since all the platforms normally come with RSF preloaded at the factory.

### Enabling the Alarms Capability

The monitoring of a powercluster by Alarms is effective when both of the following conditions are met:

- **Bullcluster** software is operational on the different powercluster nodes
- The powercluster has been registered with the **Register Powercluster** utility so that it is taken into account by **Alarms**.

### Monitoring Alarms with the Alarms Capability

The registered powercluster icon is added to the CDE desktop front panel. When an alarm is detected, a red zig-zag is superimposed on this icon, as shown in Figure 18:

ClusterAssistant adds this icon to the front panel of the CDE desktop. Its appearance changes when "Alarms" detects an error (the alarm status is shown here).



**Figure 18.** Front Panel with Alarms State Active

## Viewing Alarms

When Alarms are detected, bring up the **Alarms** window, either by clicking the **Alarms control** icon (on the Front Panel), or by activating the **Alarms** icon in the **ClusterAssistant & DSM** application group.



**Figure 19.** Alarms Window

The dark grey box indicates the list of HACMP clusters or standalone nodes on which the alarms occurred.

A **NO ALARM** message is shown when there is no alarm state.

To display the alarms, select the HACMP cluster or standalone node name in the list, then click on the **Show Alarms** button.

## Clearing Alarms

Alarms can be cleared by clicking on the **Clear Alarms** button. This action means that they are no longer considered as new alarms. The Alarms control icon reverts to its "no-alarm" appearance and the Alarms application window shows "NO ALARM".

## Add AIX errlog Alarms

By default, hardware permanent errors logged in the AIX *errlog* file of a node are monitored. The error identifiers related to monitored errors are listed in the following file on each node:  
**/usr/sbin/bullcluster/classistant/utils/bcla\_hardalarm.init**

To be warned of the occurrence of an error logged in the AIX *errlog* file (for example, a software error) which is not listed in the file:

- edit the file to add the line:

```
<errorID> 0 1-day 0
```

where `errorID` is the error identifier related to the error of interest.

- run the command to register this file in RSF:

```
chmsrc -n hardalarmlog  
-f /usr/sbin/bullcluster/classistant/utils/bcla_hardalarm.init
```

- repeat these steps on all the nodes where the error may occur.

When new drivers are installed on the node, new hardware permanent errors can appear in the AIX **errlog** file.

To record these new error identifiers in the **bcla-hardalarminit** file, run the command:

```
/usr/sbin/bullcluster/classistant/utils/bclt_init_hardalarm
```

Repeat these steps on all the nodes where the error may occur.

## Configuring User Alarms

This function allows any ASCII log files to be scanned for specific messages and warns of the occurrence of these messages in the Alarms application.

User-defined actions can also be launched automatically when these messages appear in the log files.

The Configure User Alarm functionality is based on the Bull Extended RSF utility. Extended RSF is an application dedicated to log file monitoring:

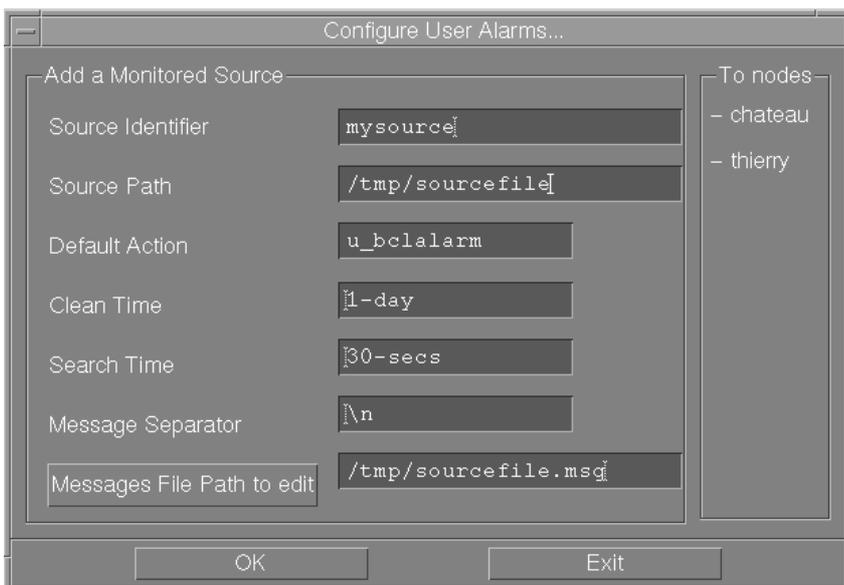
- scanning ASCII log files looking for specific messages
- when messages are detected, it executes specific, user-configurable actions (if an over-threshold condition is detected).

**Note:** Details on Extended RSF concepts and use are provided in the *Bull Escala & Escala Powercluster Extended RSF Reference Manual*.

Examples of the configuration window are shown in the figures below figures 15 and 16.



**Figure 20.** Configure User Alarms Window



**Figure 21.** User Alarms - create a Monitored Source Window

---

## System Console

The **System Console** utility allows the connection to console systems of the nodes by means of a telnet session through a **PortServer** or the **Hardware Management Console (HMC)** for LPAR servers.

### Prerequisites for using System Console

The DSM must have been set up properly.

Notably, the S1 or COM1 console ports of the nodes must be connected to a PortServer which must be configured for this purpose. See *Setting up the PortServer* on page 1-6.

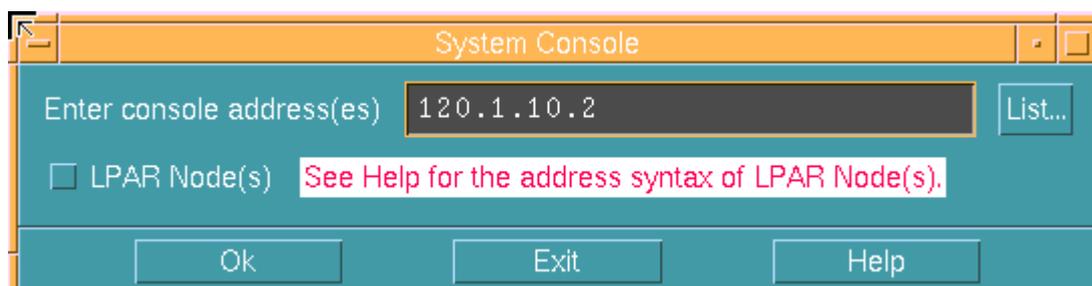
In a LPAR environment, partitions are not connected to a PortServer. Their system consoles, known as Virtual Terminals, are accessible through the Hardware Management Console (HMC).

### Using System Console

When you double-click on the **System Console** icon, you are prompted to enter an address or a list of addresses or to select a domain in a pop-up dialog.

#### If the powercluster and the nodes are not yet registered:

You can gain access to the system consoles of the different nodes by entering the system console address or a list of system console addresses separated by a space (in dot format or IP label).



**Figure 22.** System Console.

If the nodes you want to connect are partition nodes (on a LPAR server), validate the **LPAR Node(s)** button and enter an address value (or several separated by a space) according to the following syntax: four fields separated by the ';' character:

```
hmc address;partition id;model;serial number
```

where:

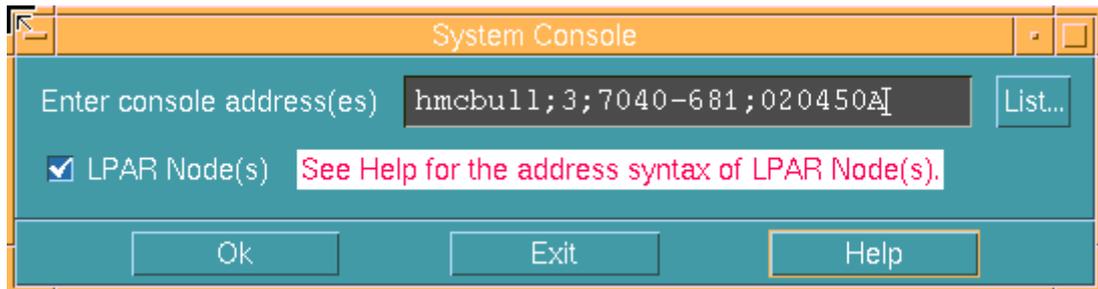
`hmc address` is the address of the HMC

`partition id` is the partition id of the partition node

`model` is the model type of the LPAR server

`serial number` is the serial number of the LPAR server

See *How to retrieve partition ID, model type and serial number* on page 2-28 for more details.



**Figure 23.** System Console (LPAR node)

A **telnet** session is started separately in a terminal window for each entered address. The addresses are saved and can be used as long as the nodes are not registered.

**If the powercluster has been registered but the node you want to access is not yet registered:**

Choose item "NODE\_NOT\_YET\_REGISTERED" in the pop-up list. A dialog which prompts you to enter a console address is then displayed, as shown Figure 23.

For a partition node (on a LPAR server), validate the **LPAR Node(s)** button and enter an address with the syntax explained above.

Once you have entered a console address, a **telnet** session is started in a terminal window acting as the system console for the node.

**If the nodes are already registered (using Register Powercluster application):**

You can gain access to the system consoles of the different nodes by selecting the corresponding domain in the pop-up list.

A **telnet** session is started separately in a terminal window for each node of the selected domain.

It means that for each node of the Powercluster, the **Console Address** field or **LPAR Node Information** fields have been filled to have a correct mapping between PortServer's ports and connected nodes or HMC and partition nodes, when adding these nodes in the **Register Povercluster** application.

In any case, in the opened terminal window, you are directly connected (through the PortServer or through the HMC) to the S1 or COM1 console port of the node or to the Virtual Terminal of a partition node. Consequently, you can do any operation you would do with an ordinary console directly attached to the node.

## How to retrieve partition ID, model type and serial number

To retrieve these values for a partition node, you have to launch the graphical user interface of the HMC. Use the **Hardware Management Console** application on the DSM or log in directly to the HMC.

If you launch the **Hardware Management Console** application from the DSM specify the HMC address in the **Enter HMC address(es)** field or select one from the **List** button.

After a few seconds, the HMC login window is displayed.

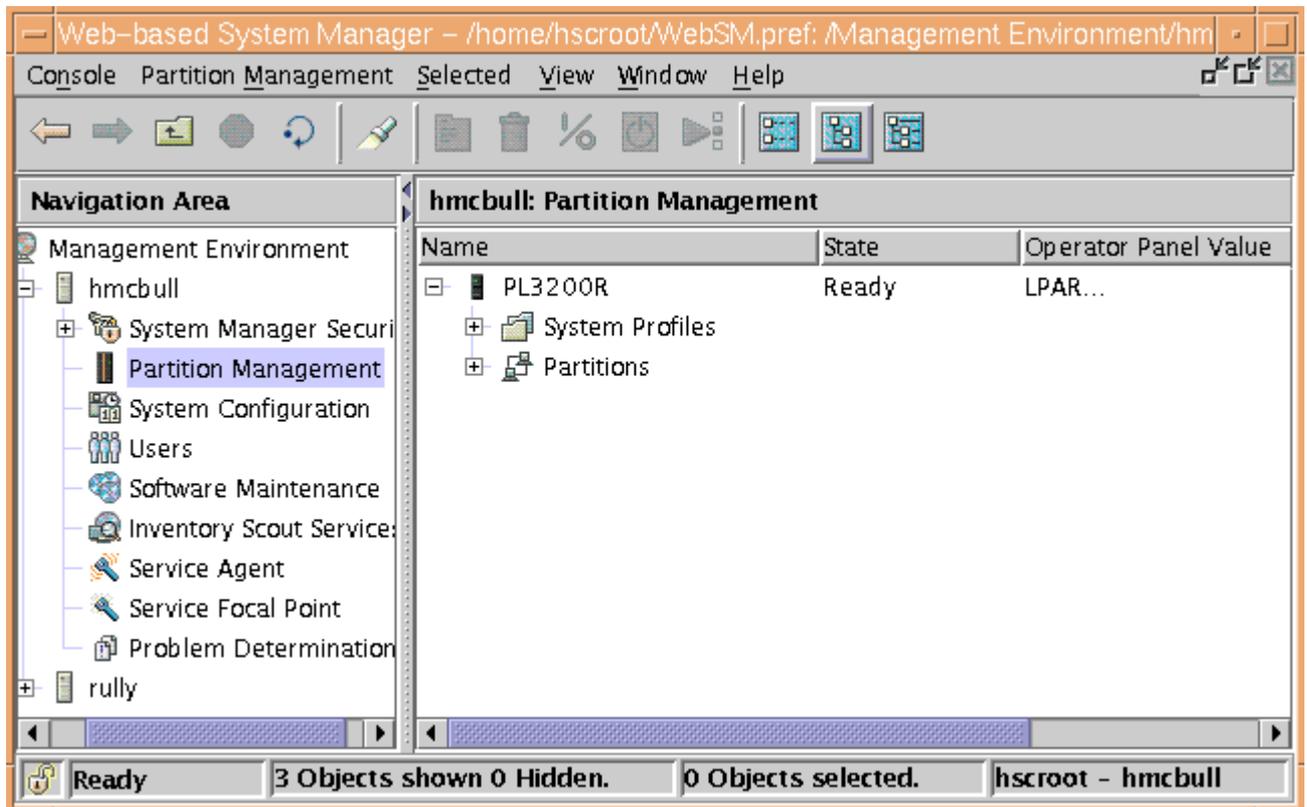


**Figure 24.** HMC login window

- Enter the **User name** (usually *hscroot*) and the **Password** (default is *abc123*), then click on the **Log On** button.

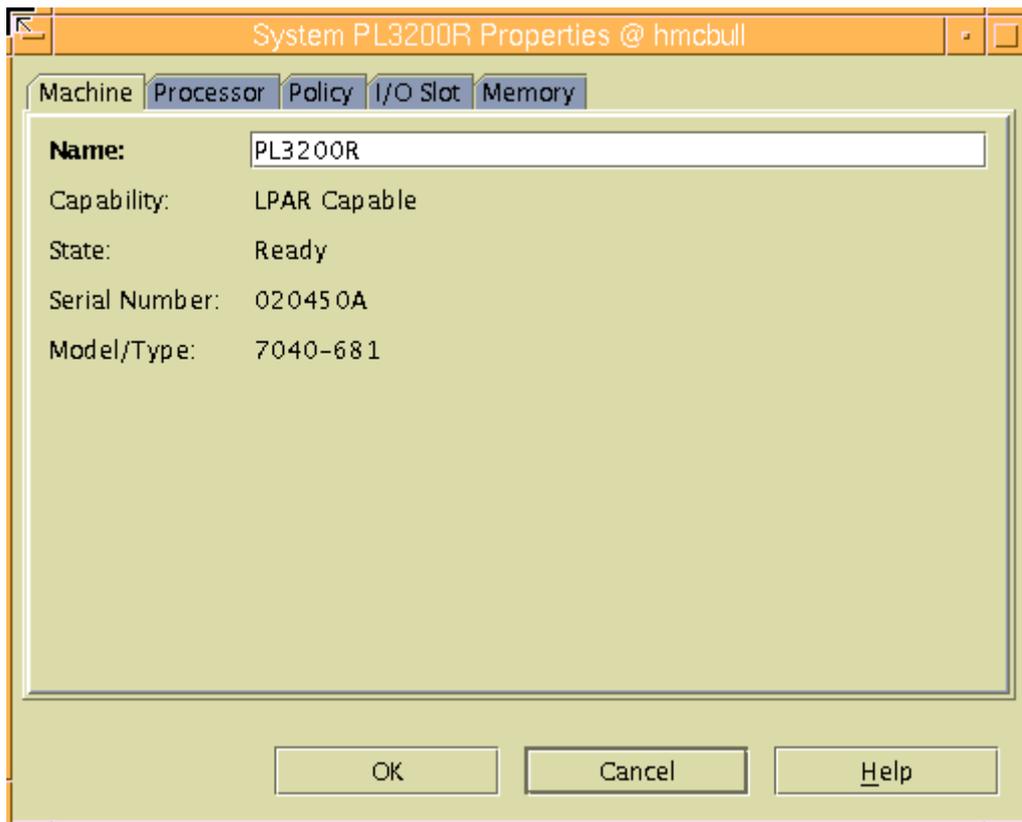
Refer to *Hardware Management Console Operations Guide (86 A1 83EF)* for more information.

- In the main window, select **Partition Management**:



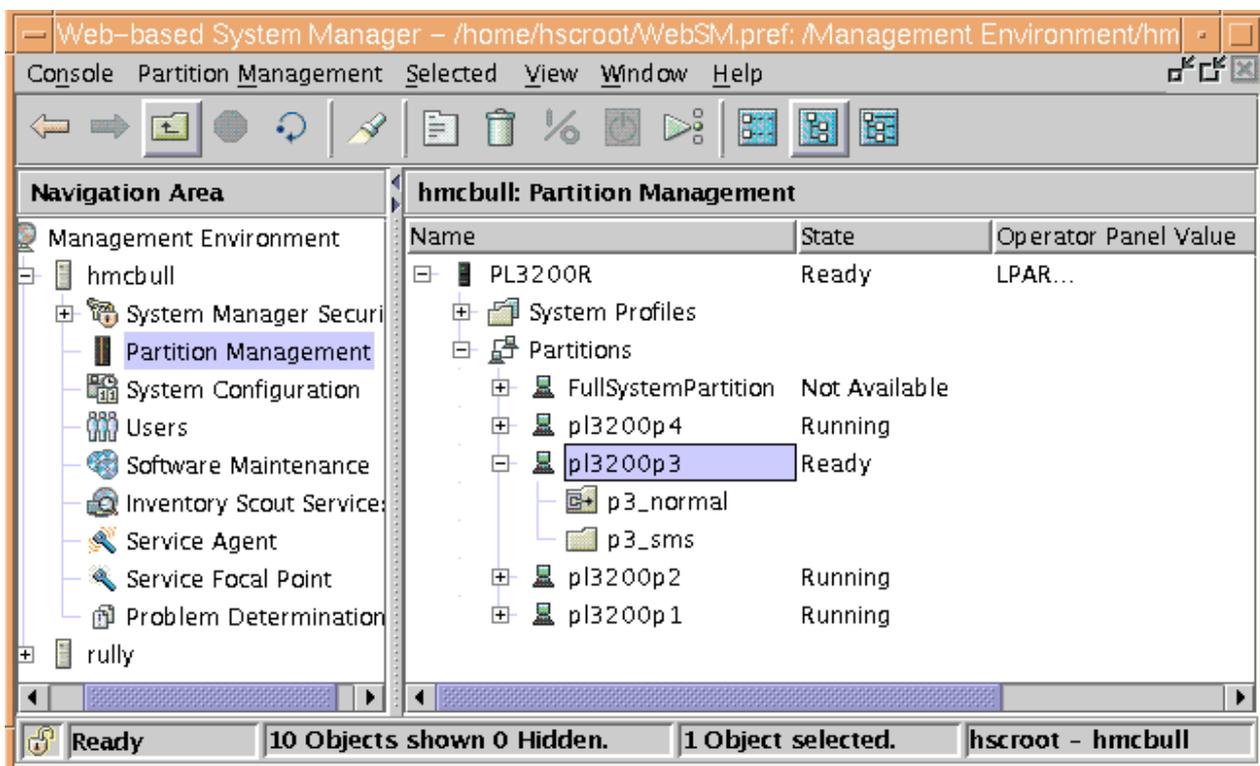
**Figure 25.** HMC WebSM interface

- Right-click on the LPAR server name and select **Properties** in the pop-up menu. Enter the values for **Model/Type** and **Serial Number**.



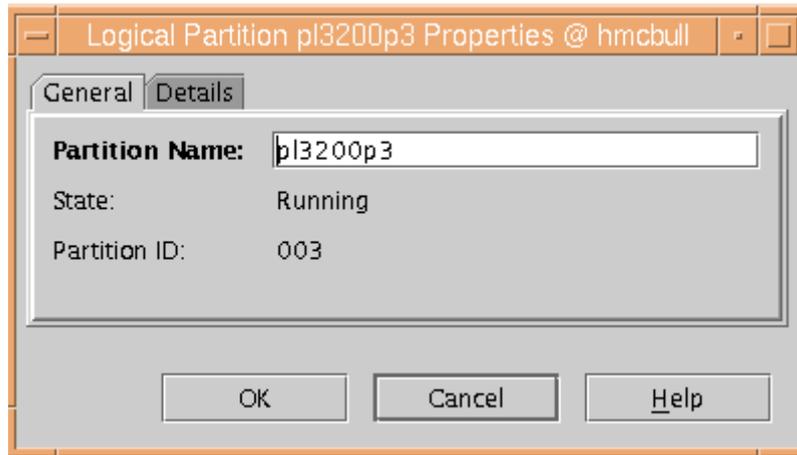
**Figure 26.** HMC – Properties window

- Click on **Partitions** to see the existing partitions.



**Figure 27.** HMC – Partition Management window

- Right-click on each partition and select **Properties** in the pop-up menu. Enter the value for **Partition ID** (without the leading zeros).



**Figure 28.** HMC – Partition Properties window

---

## Hardware Management Console

This utility brings up the WebSM interface that allows you to gain access to the **Hardware Management Console (HMC)**.

The **Hardware Management Console** is the management console connected by a serial connection on a LPAR server. Its main functions are:

- creating and maintaining a logical partition (LPAR) environment,
- detecting, reporting and storing changes in hardware conditions,
- powering managed systems on and off,
- displaying a **Virtual Terminal** Window acting as a system console for each partition.

### Prerequisites for Using Hardware Management Console

Using the Hardware Management Console requires the following:

- the AIX DSM workstation and the Hardware Management Console must be connected on the same network (administration network if possible).

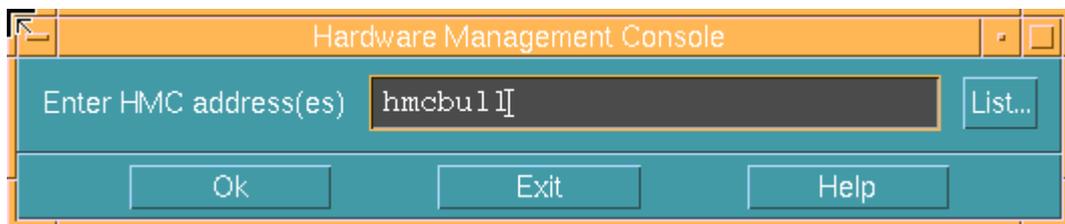
See *Setting-up the AIX DSM workstation*, on page 1-3.

- the Hardware Management Console address must be added to the `/etc/hosts` file of the AIX DSM workstation.

### Using Hardware Management Console

When you double-click on the icon, you are prompted to enter a HMC address.

Fill in the **Enter HMC address(es)** field with the HMC address or select one from the **List** button.



**Figure 29.** Hardware Management Console

After a few seconds, the HMC login window is displayed.



**Figure 30.** HMC login window

Enter the **User name** (usually *hscroot*) and the **Password** (default is *abc123*), then click on the **Log On** button to display the main window of the WebSM interface.

Refer to *Hardware Management Console Operations Guide (86 A1 83EF)* for more information.

---

## Register Powercluster

From the **Application Manager – ClusterAssistant & DSM** window, Figure 13, double-click on the **Register Powercluster** icon to open the **Application Manager - Register Powercluster** window.

**Scope of application - input** NONE, **output** standalone node, powercluster.

This utility allows a powercluster to be:

- registered
- modified
- removed from

ClusterAssistant & DSM.

### CAUTION:

**If the topology of an HACMP cluster, belonging to the Powercluster, has been modified, remember to deregister/register the cluster again in order to maintain a coherent domain database on the DSM. A domain (standalone node, HACMP cluster, HA Node) can be registered on only one DSM. If you want to register a domain on another DSM, you must deregister/remove it from the first DSM.**

This powercluster is a particular domain containing all the nodes to be managed by the DSM. It also contains the HACMP clusters that have been registered with the **Register Cluster Application** (HACMP cluster / Configuration folder).

Only one powercluster can be registered to make it and all its nodes manageable by ClusterAssistant & DSM applications.

For a LPAR server , partitions have been seen as standalone nodes. The registration of such nodes requires some additional information as explained in this section.

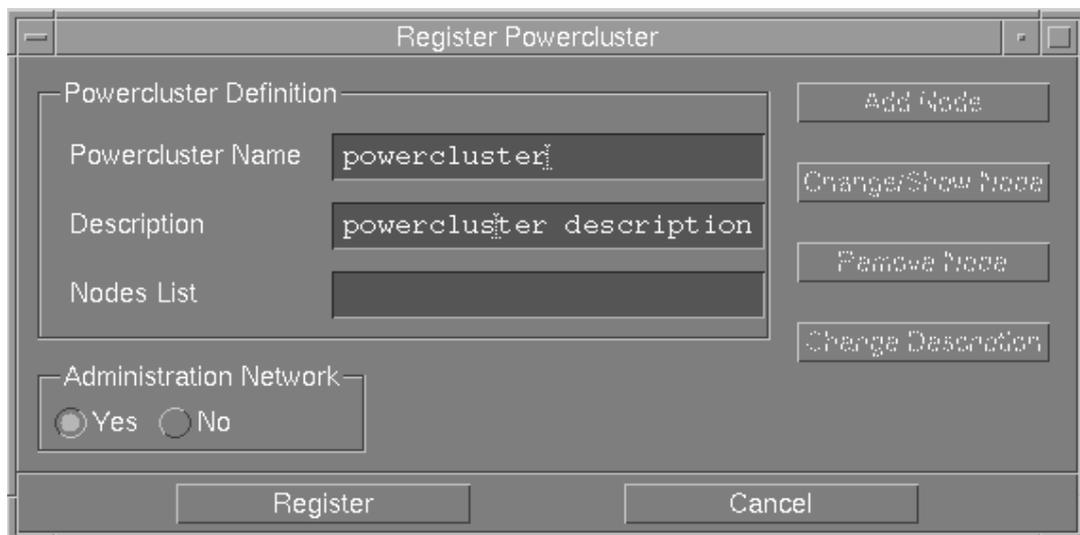
The first dialog displayed is shown below:



**Figure 31.** Register Powercluster Window with Powercluster Domain Not Yet Registered

## New Powercluster

When no powercluster has been registered yet, only the **New** button is enabled. Press it and the following window is displayed:



**Figure 32.** Register Powercluster Window - Powercluster Name

Enter the name and description of the powercluster and indicate if there is an administration network or not.

Click on the **Register** button. A powercluster icon appears in the **Domains** folder. The DSM is also configured to receive alarms.

**Note:** All the nodes administered by the DSM must be registered before registering this cluster, even those belonging to an HACMP cluster.

If the operation is successful, nodes belonging to the newly created powercluster can be defined or its description modified. In addition, nodes can be modified or removed.

Click on the **Add Node** button. A secondary dialog is displayed for the entry of node information: node name and node addresses.

The dialog is divided into 2 sections:

- **Node Definition** section
- **LPAR Node Information** section, used to register a node which is part of a LPAR server.

### Node Definition section

Enter the name, description and addresses of each node.

- the **Node Name** is the hostname or the HACMP node name if the node is already part of an HACMP cluster or is expected to be.
- the **Description** is a brief description of the node.

The addresses are given in IP Address or IP Label formats. These addresses are:

- Administration address - the IP address or label that is used by ClusterAssistant & DSM for accessing the Node.

With an Administration Network, it is the address of the node on this network.

Without an Administration Network, it is any address allowing to reach the node from the AIX DSM workstation.

These addresses must be reachable during registration.

**Note:** If the node is expected to be part of an HACMP cluster, choose a boot or persistent address.

- **Console Address** - the IP address or label corresponding to the system console of the node, as defined in the PortServer configuration. If the node is a partition of a LPAR server, the node is not connected to the PortServer, this field is empty. If you have already used the System Console application for that node, an address may have been saved, click on the **List** button to select it.

The screenshot shows a window titled "Register Powercluster" with a teal background. It is divided into two main sections. The top section, "Node Definition", contains four text input fields: "Node Name" (filled with "node1"), "Description" (filled with "node number one"), "Administration Address" (filled with "120.1.10.1"), and "Console Address" (filled with "120.1.10.2"). A "List..." button is positioned to the right of the "Console Address" field. The bottom section, "LPAR Node Information", starts with an unchecked checkbox labeled "LPAR Node". Below it are four text input fields: "Partition ID", "HMC Address", "Model Type", and "Serial Number". Each of these four fields has a "List..." button to its right. At the very bottom of the window are two buttons: "Apply" and "Cancel".

**Figure 33.** Register PowerCluster - Add Node

#### **LPAR Node Information section**

This section must be filled in if the node being registered is a partition (of a LPAR server).

Click on **LPAR Node** button, then fill in the other fields.

- **Partition ID** is the partition id of the partition node
- **HMC Address** is the address of the HMC
- **Model Type** is the model type of the LPAR server
- **Serial Number** is the serial number of the LPAR server

See *How to retrieve partition ID, model type and serial number* on page 2-28 for further information.

If you have already used the **System Console** application for that node, the different values may have been saved, click on the **List** button to select each of them.

**Figure 34.** Register Powercluster – Add Node (LPAR Node)

Click on the **Apply** button. The following tasks are performed:

- an icon to represent the node is created in **Domains** folder
- The configuration of alarms is automatically performed when adding a node to the Powercluster definition in order that the permanent hardware errors logged in the AIX errlog of the node are taken into account by the Alarms application of Cluster Assistant & DSM.

Click on the **Remove Node** button to remove a node from the powercluster definition (corresponding icon is removed and alarms are deconfigured for the node).

Click on the **Change/Show Node** button to display or modify a specific node information.

Click on the **Change Description** button to modify the powercluster definition.

**Notes:**

1. If the alarm configuration/deconfiguration step fails, the user is warned via a dialog box or by messages.
2. The `/var/bullcluster/rsf.logFile:/var/bullcluster/rsf.log` file contains information about the alarm configuration steps.

## Modify Powercluster

In the main window of the application, click on the **Modify** button to modify an existing powercluster definition (add, modify or remove nodes).

## Remove Powercluster

To remove the powercluster definition, click on the Remove button of the Register powercluster panel (opened from the Register Powercluster icon). A confirmation dialog is opened, indicating the list of domains (nodes and HACMP clusters) that will be removed by this operation. Removing a powercluster definition from ClusterAssistant & DSM can be a rather long operation, so progress dialogs are displayed to the user, indicating the current task. For each HACMP cluster to deregister, a progress dialog is displayed. After deregistration of HACMP clusters, a last progress dialog is run while deregistering the nodes themselves. The trace of the different steps of the deregistration are written in the */var/bullcluster/deregister\_epc* File:*/var/bullcluster/deregister\_epcfile*.

Click on the **Remove** button to deregister the powercluster definition (removes the powercluster, all its members and related icons, un-configure alarms).

**Note:** If the powercluster contains HACMP clusters, they are also deregistered (**Deregister Cluster** application is called).

If remove Powercluster fails, use Cleanup application to remove Powercluster definitions on the DSM.

---

## Cleanup Application

The **Cleanup** utility allows you to clean up registered nodes and/or HACMP clusters when normal de-register operations fail.

The utility removes all information on the DSM and on the nodes created at registration time.

This procedure is of interest if normal de-register operations fail.

### Bringing Up Cleanup

Double-click on the **Cleanup** icon to display a pop-up dialog prompting selection of a domain.

The Cleanup window, allowing the clean up of previously-selected nodes, HACMP cluster and/or powercluster, is then displayed.

### Purpose

Cleanup must be used to maintain consistency between registered domains in the following cases:

- when the Remove Node operation in the Register Powercluster Application fails, Modify Powercluster, on page 2-37.
- when the Remove operation in the Register Powercluster Application fails, Remove Powercluster, on page 2-38.
- when the Deregister Cluster Application fails, Deregister Cluster, on page 2-20.

### Using Cleanup

The main window displays a message indicating the domains to clean up.

If one of the selected domains is the powercluster, the cleanup mode can be chosen; the **forced** mode must be used if the **normal** mode fails. In **forced** mode, no check is done and the */etc/hosts* file on the AIX DSM workstation must be edited to suppress aliases related to HACMP clusters.

Cleanup trace is logged in the */var/bullcluster/cleanup.log* file.

Click the **OK** button. A confirmation window is displayed. If you confirm, the cleanup procedure is launched and operation progress is shown in a window.

Press the `Control-C` key to close this window.

If a node is unreachable, a message is displayed asking you to execute the following script on the node:

```
usr/sbin/bullcluster/classistant/utills/bclt_cleanup_node node  
<nodename>
```

or

```
/usr/sbin/bullcluster/classistant/utills/bclt_cleanup_node hanode  
<nodename>
```

---

## Check Application

The Check utility checks configuration information on the DSM, nodes and HACMP clusters and warns if potential problems are detected.

This procedure is of interest if ClusterAssistant & DSM applications do not work correctly.

### Bringing Up Check

When you double-click the icon, the main options check window is displayed.

Select the options to be checked from the **Verify** list:

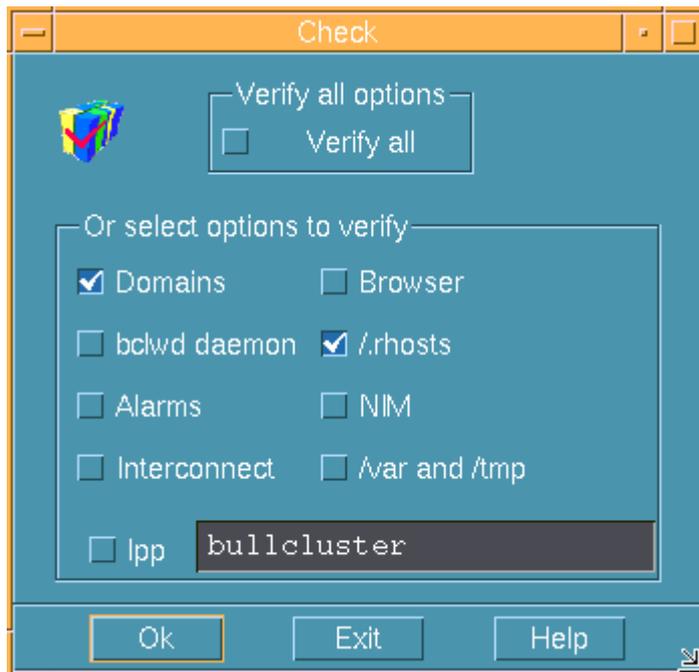


Figure 35. Check Options Selection Window

### Using Check

**Any** or **all** of the options can be checked. Their operation are defined as follows:

- |                      |   |
|----------------------|---|
| <b>Domains</b>       | Prints out all information about registered domains.  |
| <b>/.rhosts</b>      | Checks if AIX DSM workstation entry exists in <i>/.rhosts</i> file on nodes.<br>Checks if nodes network interfaces (boot, standby, service, administration) exist in <i>/.rhosts</i> file on AIX DSM workstation. |
| <b>bclwd daemon</b>  | Checks if <i>bclwd</i> daemon is running on AIX DSM workstation and cluster nodes.  |
| <b>NIM</b>           | Runs the verification tool for NIM.   |
| <b>Alarms</b>        | Checks if alarms are correctly configured on AIX DSM workstation and nodes and if RSF is running.   |
| <b>/var and /tmp</b> | Checks if <i>/var</i> and <i>/tmp</i> file systems are more than 90% used on AIX DSM workstation and nodes.   |

**Interconnect** Checks if the administration port of the console concentrator is defined and reachable on AIX DSM workstation.

**Mozilla** Checks if Mozilla is installed on AIX DSM workstation.

**lpp** Prints out the version of specified lpp on AIX DSM workstation and nodes.

By default, the lpp checked is **bullcluster**. Another lpp name can be entered when the lpp option is selected.

Click the OK button. The check procedure is launched and operation progress is shown in a window.

Press the `Control-C` keys to close the window.

If a node is unreachable, a message is displayed asking for the following script to be executed on a node:

```
/usr/sbin/bullcluster/classistant/utills/bclt_check node <nodename>  
<oslevel> <powerconsole> <optionlist>
```

or

```
/usr/sbin/bullcluster/classistant/utills/bclt_check hanode  
<nodename> <oslevel> <powerconsole> <optionlist>
```

where:

**nodename** is the node name used when it was registered.

**oslevel** is the AIX DSM workstation AIX Version (example: if version is 5.2, oslevel is 5.2).

**powerconsole** is the AIX DSM workstation hostname.

**optionlist** is the list of options to check, separated by a space character; the possible values are as follows:

domain	for Domains
rhosts	for <i>/.rhosts</i>
bclwd	for <i>bclwd</i> daemon
alarm	for Alarms
fsfull	for <i>/var and /tmp</i>
autodetect	for Fast Ethernet

Other options (Mozilla, Interconnect, ...) are not significant on nodes.

---

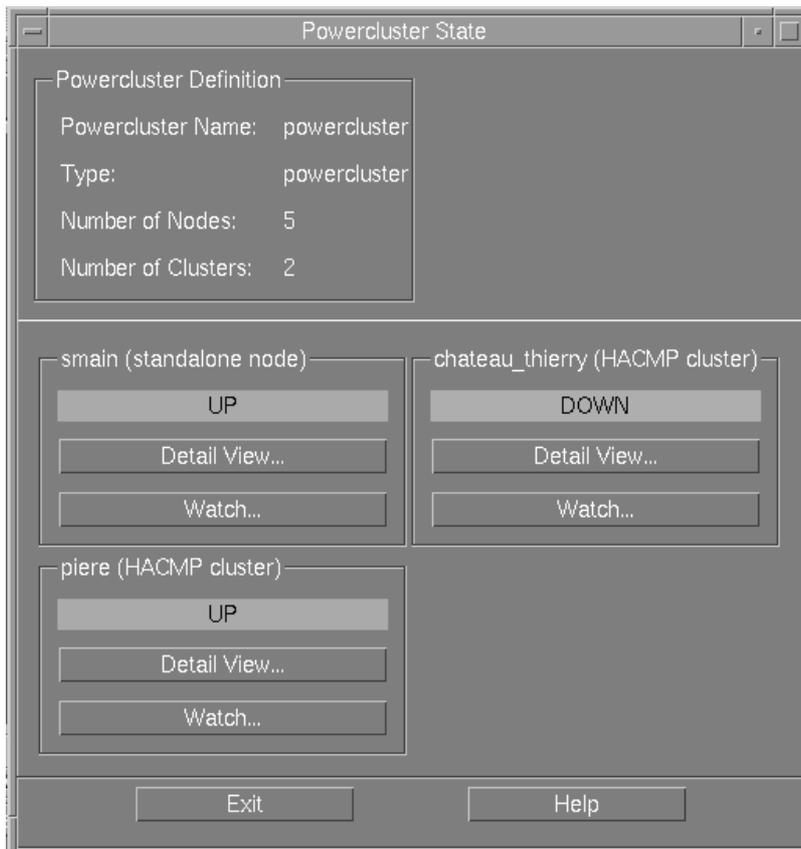
## Powercluster State

**Scope of application** - HA node, standalone node, HACMP cluster, powercluster.

From the **Application Manager - ClusterAssistant & DSM** window, Figure 13, double-click the **Powercluster State** icon to open a pop-up menu which prompts the selection of a domain.

This utility displays the state of HACMP clusters and standalone nodes.

Depending upon the type of selected domain, the **Powercluster State** window displays general information about the selected domain (name, type, number of members) and an animated map of its members. A refresh of the members map is periodically performed to reflect the current state of the domain.



**Figure 36.** Powercluster State Window

This example displays a synthetic view of a powercluster domain with 5 nodes: 1 standalone node (**smain**) and 2 HACMP clusters of 2 nodes (**piere** and **chateau\_thierry**).

### Standalone Node

The state is:

- **UP** in a green box if the node is reachable
- **UNREACHABLE** in a red box if the node is unreachable.

### HA Node

The state is:

- **DOWN** in an orange box if HACMP is not running
- **UP** in a green box if HACMP is running
- **UNREACHABLE** in a red box if the node is unreachable

- **TAKEOVER** in a blue box if the node has taken over IP service address of another node.

## HACMP Cluster

Two views are available:

- a synthetic view (the default)
- a detailed view.

### Synthetic View

In the synthetic view, the state of the cluster is:

- **UP** in a green box if all its nodes are UP
- **DOWN** in an orange box if all its nodes are DOWN
- **UNREACHABLE** in a red box if all its nodes are UNREACHABLE
- **UNSTABLE** in a yellow box in other cases.

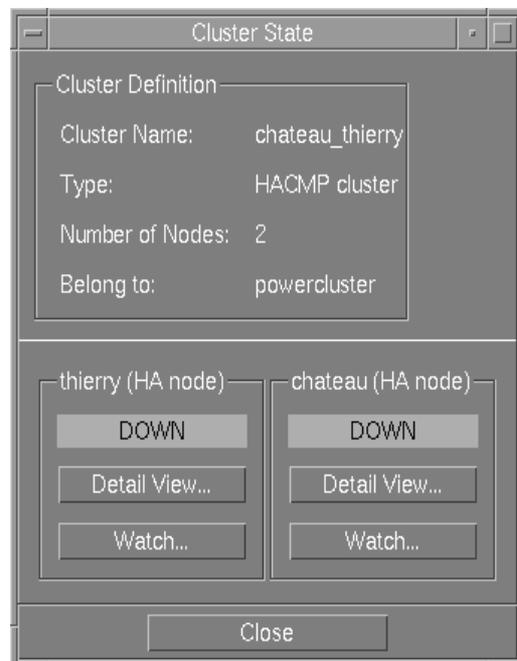
### Detailed View

The detailed view shows the state of all the nodes of the HACMP cluster according to the rules applying to HA nodes.

Use the **Detail View Button** to view details for a particular HACMP cluster, HA node or standalone node. The detailed view is displayed in a secondary window:

- Cluster State, see Figure 37.
- Node State, see Figure 38.
- HA node State, see Figure 39.

## Cluster State

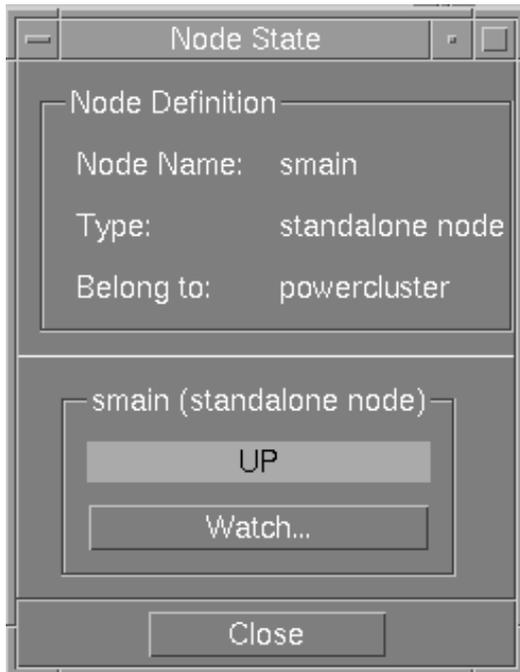


**Figure 37.** Cluster State - Detail Window

Press the **Watch** button to launch the **ClusterWatch** application to monitor the HACMP cluster.

**Note:** User identification and password are required for access to this application.

## Node State

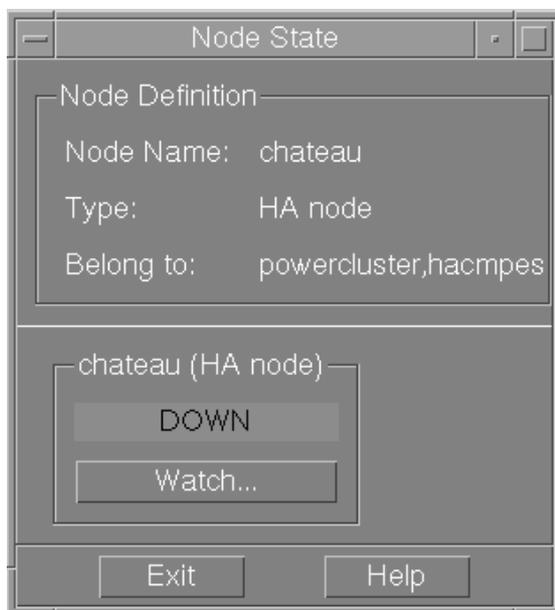


**Figure 38.** Node State - Detail Window

Press the **Watch** button to launch the **WatchWare** application to monitor a node.

**Note:** User identification and password are required for access to this application.

## HA Node State



**Figure 39.** HA Node State - Detail Window

Press the **Watch** button to launch the **WatchWare** application to monitor a HA node.

**Note:** User identification and password are required for access to this application.

---

## Cluster Configuration (smit)

From the **Application Manager - HACMP Cluster** folder, open the **Cluster Configuration** folder and then double-click on the **Cluster Configuration (smit)** icon to open the **Cluster Configuration** utility.

This utility can also be opened by dragging at least 2 node icons (or only one cluster icon) and dropping them on to the **Cluster Configuration (smit)** icon. See *Function Selection*, on page 2-11.

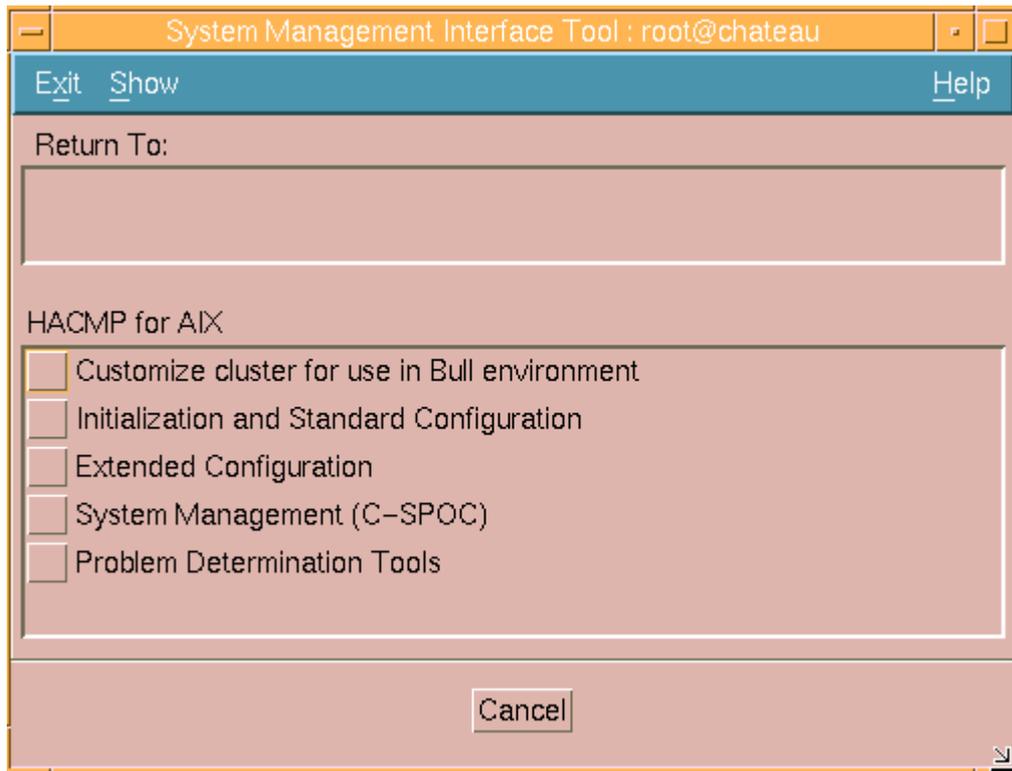
To **Configure a new Cluster**, select a minimum of 2 standalone nodes from the list of domains:



**Figure 40.** Cluster Configuration - List of Domains Window

To **Modify an existing Cluster**, select only one cluster from the list of domains.

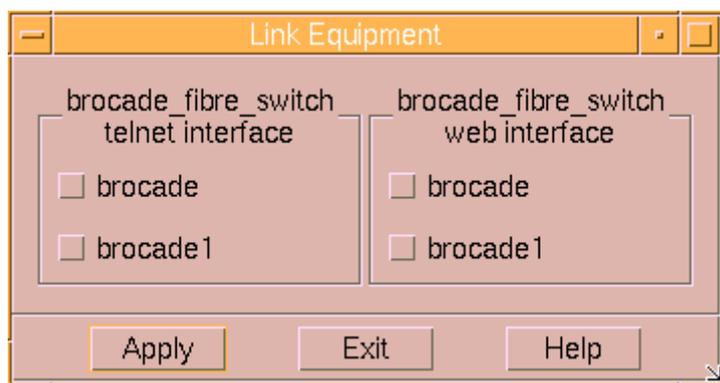
After selecting the nodes belonging to the new cluster, or selecting an existing cluster, confirm with OK, then the main window of the Cluster configuration (smit) application is displayed.



## Link Equipment Application

**Scope of application** - NONE.

Double click on the **Link Equipment** icon to open a dialog window, displaying all the Link Equipment types already configured. Choose one or more interconnect devices and launch a telnet session or a web interface to configure the interconnect devices. The web interfaces are available only for some interconnect devices.

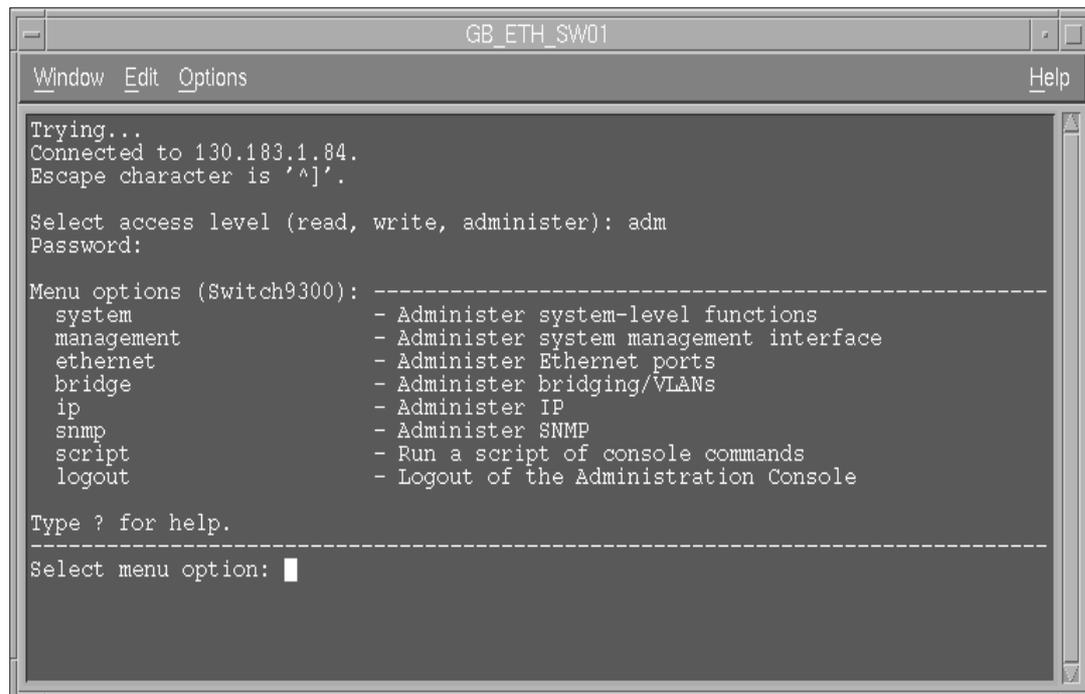


**Figure 41.** Link Equipment Window Showing Configured Devices (typical)

Brings up a **telnet** session or **web** interface to manage a Link Equipment device (hub, switch).

Link Equipment device documents are listed in **Reference Documents**.

A typical management screen is shown in Figure 42:



**Figure 42.** Link Equipment Device Management Screen (typical)

Alternatively, Link Equipment devices may be managed via the Internet. Typical interactive management Netscape screens are shown here in Figure 43 and in Figure 44.

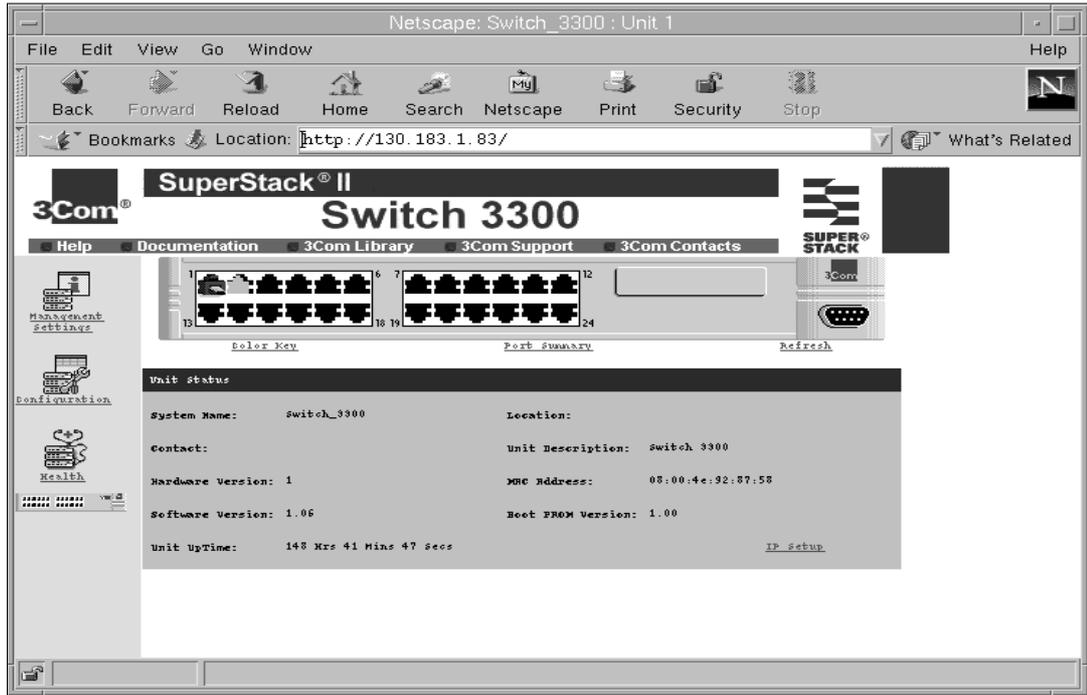


Figure 43. Link Equipment Device Management Mozilla Screen (typical)

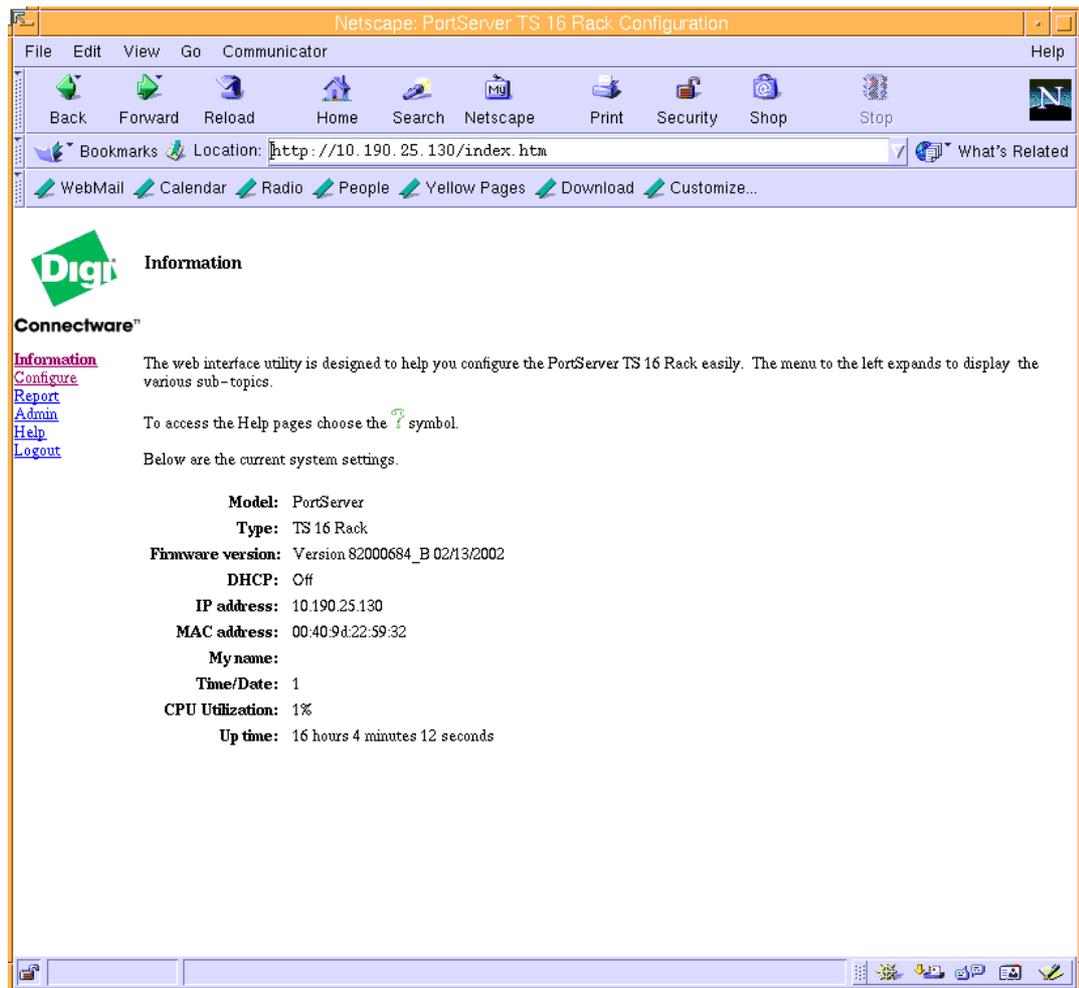


Figure 44. PortServer TS 16 Model Web Interface

---

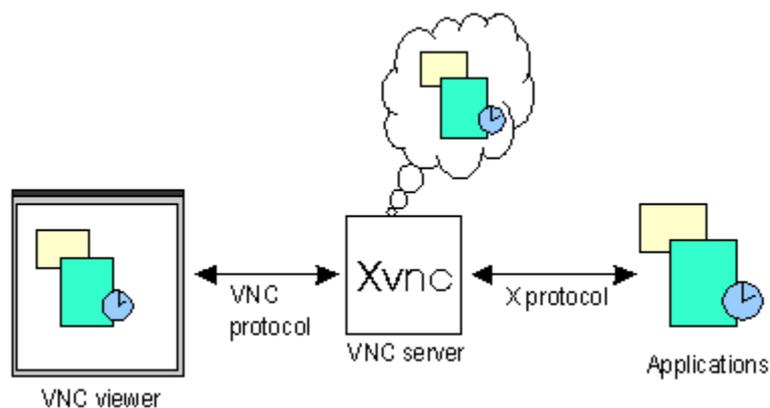
## Multiple Displays on One Screen

### Overview of VNC

VNC (Virtual Network Computing) is a freeware utility made available by an ATT research laboratory on the Web at the URL:

<http://www.uk.research.att.com/vnc/>

VNC creates a virtual X-Terminal to which X11 applications can connect without modifications. The virtual screen of this X-Terminal can then be displayed on almost any device equipped with a "graphic" display. The following diagram illustrates the architecture...



VNC acts as a virtual X-Terminal, on which a standard CDE session can be opened. The CDE session is started automatically when the `Xvnc` process is started and is only stopped when the `Xvnc` process is terminated. The VNC-viewer application can download the screen of the virtual X-Terminal on to whatever display device is being used. A port of the `vncviewer` application to Java allows the screen of the virtual X-Terminal to be displayed in any Java-enabled web browser.

### Installation

#### VNC-Server, on the AIX DSM workstation

The VNC lpp freeware `freeware.vnc.rte` is delivered with the DSM CD-ROM.

Install the VNC LPP using `smit`. This LPP requires that "perl" be already installed on the system.

#### VNC-Viewer, on "usual" display stations

While the Java port of the VNC-Viewer does not need to be installed (it is downloaded automatically when required), it is faster and more reliable to install and use platform-specific binaries when working in a stable environment

- On Windows (95, 98, NT)

The VNC-Viewer for Windows is included in the VNC LPP installed on the AIX DSM workstation, in the directory `/usr/local/lib/vnc-3.3.3`. There, you can get `vncviewer.exe`, the Java classes and the README files. These files can be transferred to the Windows system by FTP or by diskette.

- On AIX (5.2 or later)

Install the VNC LPP using `smit`.

## Starting a VNC Server Session

- Ensure that the directory `/usr/local/bin` is present in the path with the command:

```
$ type vncserver
vncserver is /usr/local/bin/vncserver
```

If the `vncserver` command is not found, type the following:

```
export PATH=$PATH:/usr/local/bin
```

- Execute `vncserver` with the option `-alwaysshared`
- The first time that `vncserver` is executed, it will request that a password be defined. This password can be the same as the user's normal login password. This password is not transmitted over the network and is encrypted before being stored to disk (in the file `$HOME/.vnc/passwd`).

Then you can change this password using the `/usr/local/bin/vncpasswd` command.

- The `vncserver` script will identify an appropriate "display number" for the virtual display (typically `:1` or `:2`, as opposed to the "real" display number, `:0`)

This "display number" identifies a desktop session and will have to be provided at connection time.

- If none exists, the `vncserver` script will autogenerate an Xsession startup script in `$HOME/.vnc/xstartup`.
- The `vncserver` script will then start the VNC virtual X-Server, `Xvnc`. `Xvnc` will then execute the `xstartup` script to start the CDE session. Here is an example of how `vncserver` is executed:

```
# vncserver -alwaysshared
You will require a password to access your desktops.
Password:
Verify:
Vncpasswd returned 228
New 'X' desktop is esther:1
Creating default startup script //.vnc/xstartup
Starting applications specified in //.vnc/xstartup
Log file is //.vnc/esther:1.log
esther # ps -f | grep Xvnc
    root 18942 19670    5 14:23:37 pts/0    0:00 grep Xvnc
    root 23294      1    0 14:23:17 pts/0    0:01 Xvnc :1 -desktop X -
httpd /usr/lo
cal/lib/vnc/classes -auth //.Xauthority -geometry 1024x768 -depth 8
-rfbwait 120
000 -rfbauth //.vnc/passwd -rfbport 5901 -fp
/usr/lib/X11/fonts/,/usr/lib/X11/fo
nts/misc/,/usr/lib/X11/fonts/75dpi/,/usr/lib/X11/fonts/100dpi/,/usr
/lib/X11/font
s/ibm850/ -co /usr/lib/X11/rgb
esther #
```

## Unix VNC-server options

Complete documentation is available on the Web at the URL:

<http://www.uk.research.att.com/vnc/xvnc.html>

The following is a short extract:

`-name name`

Each desktop has a name which may be displayed by the viewer. It defaults to 'X' but you can change it with this option.

`-geometry widthxheight`

Specify the size of the desktop to be created. Default is 1024x768.

`-depth depth`

Specify the pixel depth in bits of the desktop to be created. Default is 8.

`-pixelformat format`

Specify pixel format for server to use (BGRnnn or RGBnnn)

`-alwaysshared`

Always treat new clients as shared (i.e. ignore client's shared flag).

`-nevershared`

Never treat new clients as shared (i.e. ignore client's shared flag).

`-dontdisconnect`

Do not disconnect existing clients when a new "non-shared" connection comes in. Instead the new connection is refused. New "shared" connections are still allowed in the normal way.

`-localhost`

Only allow connections from the same machine. Useful if you use SSH and want to stop non-SSH connections from any other hosts. See the guide to use VNC with SSH

`-cc n`

Sets the colour Visual class used by the server. Some X applications do not cope too well with the TrueColor visual normally used by an 8-bit-deep Xvnc. You can make the server use a PseudoColor visual by specifying `-cc 3`.

`-economictranslate`

The server normally uses a lookup table for translating pixel values when the viewer requests a different format from the native one used by the server. This can use up to 256Kbytes per connected viewer, so if you have many viewers you may wish to specify this option which will save memory at the expense of a little bit of speed; only relevant for 16-bit-deep desktops.

On a Unix system, a VNC Server session can be automatically started by adding the following line in `/etc/inittab`:

```
vnc:2:wait:/usr/local/bin/vnc1>/tmp/vnc 2>&1
```

where `/usr/local/bin/vnc1` is a script containing:

```
#!/bin/ksh
```

```
export PATH=$PATH:/usr/local/bin
```

```
export HOME=/
```

```
/usr/bin/rm /tmp/.X11-unix/X1
```

```
/usr/local/bin/vncserver -alwaysshared -geometry 800x600
```

```
exit 0
```

## Identifying the Active VNC Sessions

Run the following command:

```
ps -ef |grep Xvnc
```

which returns the vnc desktop session number (or display number), for example Xvnc:1.

## Stopping a VNC Server Session

To stop a VNC session, use the option `-kill` with the display number to stop the VNC Virtual X-Terminal. For example

```
# vncserver -kill :1
```

## Displaying a VNC Session

### On an AIX Station

To download a VNC session from a AIX DSM workstation and display it on the current session, run the `vncviewer` with the name of the `vncserver` host and the number of the display (as shown by the `vncserver` when it was executed). For example, with a AIX DSM workstation named `esther`:

```
# vncviewer esther:1
```

```
VNC server supports protocol version 3.3 (viewer 3.3)
```

```
Password:
```

```
VNC authentication succeeded
```

```
Desktop name "root's X desktop (esther:1)"
```

```
Connected to VNC server, using protocol version 3.3
```

```
VNC server default format:
```

```
8 bits per pixel.
```

```
True colour: max red 7 green 7 blue 3, shift red 0 green 3 blue 6
```

```
Using default colormap and translating from BGR233. Pixel format:
```

```
8 bits per pixel.
```

```
True colour: max red 7 green 7 blue 3, shift red 0 green 3 blue 6
```

```
Got 244 exact BGR233 colours out of 256
```

```
Using 1 existing shared colours
```

```
Same machine: preferring raw encoding
```

It may be useful to display a VNC session from the local machine in full-screen mode with the option `-fullscreen`, to be able to download the same screen that the operator sees to another supervisory console. To exit fullscreen mode, type `F8` and a popup menu will be displayed. Choose 'exit' from this menu.

### X-Windows VNC-viewer options:

The complete documentation is available on the Web at the URL

```
http://www.uk.research.att.com/vnc/xvncviewer.html
```

The following is a short extract:

```
-shared
```

When you make a connection to a VNC server, all other existing connections are normally closed. This option requests that they be left open, allowing you to share the desktop with someone already using it.

```
-display Xdisplay
```

Specifies the X display on which the VNC viewer window should appear.

`-passwd password-file`

If you are on a filesystem which gives you access to the password file used by the server, you can specify it here to avoid typing it in. It will usually be `"~/ .vnc/passwd"`.

`-viewonly`

Specifies that no keyboard or mouse events should be sent to the server. Useful if you want to view a desktop without interference; often needs to be combined with `-shared`.

`-fullscreen`

Start in full-screen mode.

`-geometry geometry`

Standard X position and sizing specification.

`-bgr233`

Tells the VNC server to send pixels that are only 8 bits deep. If your server desktop is deeper than this, it will translate the pixels before sending them. Less data will generally be sent over then network, which can be a big advantage on slow links, but the server may have to work a bit harder, and you may get some colour mismatches. "BGR233" means an 8-bit true colour pixel format, with the most significant two bits of each byte representing the blue component, the next three bits representing green and the least significant three representing red. The java client also uses this format.

`-encodings encodings`

This option specifies a list of encodings to use in order of preference, separated by spaces. The default is "copyrect hextile corre rre", or "raw copyrect hextile corre rre" for a VNC server on the same machine. For example, to use only raw and CopyRect, specify "raw copyrect".

`-owncmap`

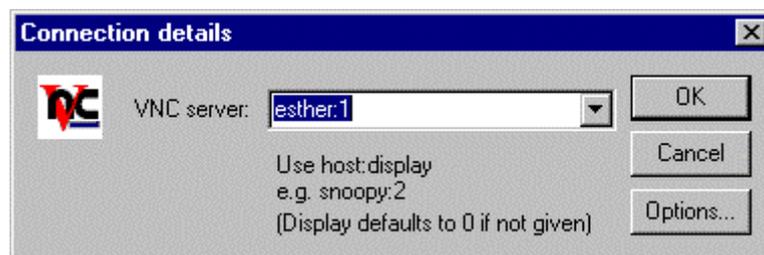
Try to use a PseudoColor visual and a private colormap - this allows the VNC server to control the colormap.

`-truecolour`

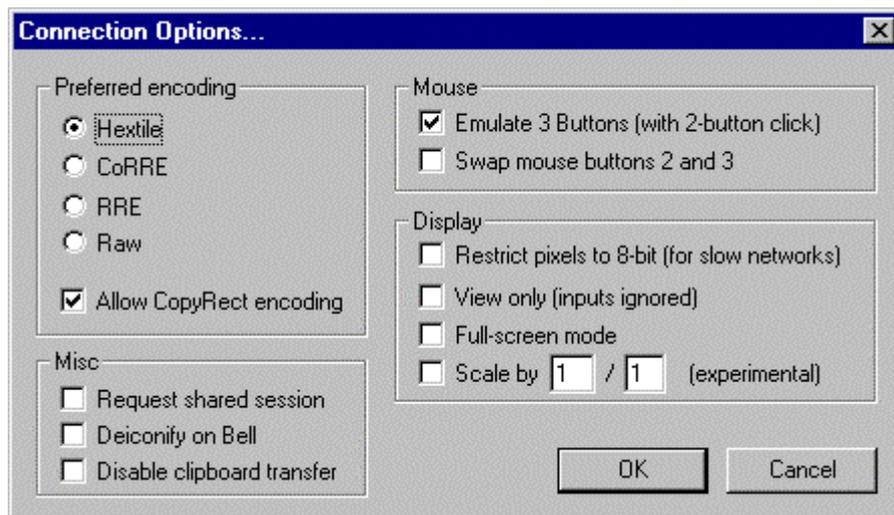
Try to use a TrueColor visual.

### On a Windows System

Click on the icon "VNCviewer" (or click on the file `vncviewer.exe` under *Explorer*). Type the name of the DSM and the number of the display in the main box as shown:



The same connection options are available as under the X-Windows command-line viewer:



To establish the connection you will be prompted for the VNC-server password:



### On a Java-enabled Browser

To connect to the VNC server from a Java-enabled browser, you need to transfer the Java classes from the AIX server directory `/usr/local/lib/vnc-3.3.3/classes`. Then you must provide a URL with the name of the machine and a special port number. The port number can be determined by adding 5800 to the display number chosen by the `vncserver` command. For example to connect to the VNC server running as the display `:1` on the system "esther" use the URL

```
http://esther:5801/
```

For the connection to succeed it is often necessary to deconfigure the use of Proxies in the web browser, and to activate the use of Java. Some older versions of Java work poorly with the VNC applet, and may force you to kill the browser.

### Closing a VNC Desktop Session

Close the window and do not use the 'EXIT' button in the CDE.

---

## Chapter 3. Glossary

This glossary contains abbreviations, key-words and phrases that can be found in this document.

### **10Base-T**

Twisted Pair ports.

### **AIX**

Advanced Interactive Executive. UNIX operating system implemented by IBM.

### **AUI**

Thick Ethernet port.

### **API**

Application Programming Interfaces.

### **BullCluster**

software package.

### **CDE**

Common Desktop Environment.

### **Clinfo**

Cluster Information Program.

### **CLM**

Cluster Lock Manager.

### **ClusterWatch**

Web-based facility for monitoring cluster operations.

### **DTR**

Data Terminal Ready.

### **Ethernet Hub**

3Com SuperStack II Hub 10 12-port TP.

### **HACMP**

High Availability Concurrent Multi Processing: the clustering software providing High Availability and parallelism capacities used with Powercluster and HA Solutions.

### **LPP**

Licensed Program Product: A standard AIX software package.

### **LVM**

Logical volume Group.

### **MIB**

Management Information Base

### **NIM**

Network Installation Manager. Standard AIX software used to manage remote Software Distribution and Maintenance.

### **ODM**

Object Data Manager: Standard AIX database used to store system-related data.

**RSF**

Remote Services Facilities.

**SRB**

Software Release Bulletin.

**TFTP**

Boot Protocol.

**timed server**

A time server that comes with AIX, useful for maintaining clocks synchronized on all the nodes of a cluster.

**SMIT**

System Management Interface Tool: A standard AIX text or motif user-interface used to perform various system management tasks.

**SNMP**

Simple Network Management Protocol.

**SRC**

System Resource Controller.

**URL**

Uniform Resource Locator.

**VG**

Volume Group: a group of disks viewed as a single entity.

**VNC**

Virtual Network Computing.

**VSM**

Visual System Management: A standard AIX Motif interface to perform various system management tasks.

---

## Chapter 4. Index

- /.rhosts file, 2-10
- /.rhosts Files
  - Updating, 2-8
- /etc/hosts file, 2-10
- /etc/hosts Files
  - Updating, 2-8
- Action Invoker Window
  - Password entry (Figure), 2-11
- Administration Address, 2-35
- Administration Network
  - Dedicated, 1-2
- AIX, 2-37
- AIX Configuration, 1-5
- AIX Console, 2-15
- Alarms, 2-15, 2-24
  - AIX errlog, 2-25
  - Clearing, 2-25
  - Configuring User, 2-26
  - Enabling, 2-24
  - Monitoring, 2-24
  - Viewing, 2-25
- Alarms Window
  - (Figure), 2-25
- Application Group, 2-12
- Application Manager - Cluster Configuration Window
  - (Figure), 2-19
- Application Manager - ClusterAssistant Window
  - (Figure), 2-14
- Application Manager - HACMP Cluster Window
  - (Figure), 2-17
- Application Manager - Network Install Manager Window
  - (Figure), 2-21
- Application Manager Window
  - (Figure), 2-13
- Applications
  - Alarms, 2-15
  - Cluster Alarm, 2-37
  - ClusterAssistant, 2-14
  - Launching, 2-13
- Backup System, 2-22
- Backup System on PowerConsole, 2-22
- bclerrdiag, 2-17
- bclwd daemon, 2-7, 2-10
- bclwd Daemon
  - Troubleshooting, 2-10
- Boot Address, 2-36
- BQ306, ASCII Terminal, 1-5
- BullCluster Diagnostic Tool, 2-17
- bullsmw, 2-10
- Buttons
  - Clear Alarms, 2-16
  - Configure User Alarms, 2-16
  - Detail View, 2-43
  - Show Alarms, 2-16
  - Watch, 2-43
- Cabling Guidelines, 1-4
- CDE, 2-11
- CDE Front Panel
  - (Figure), 2-12
- CDE Front Panel Showing ClusterAssistant Icon
  - (Figure), 2-7
- Change Decryption, 2-37
- Change/Show
  - Remove, 2-37
- Change/Show Node, 2-37
- Check, 2-16, 2-40
- Check Options Selection Window
  - (Figure), 2-40
- classist
  - User password, 2-8
- classist, user, 2-6
- Cleanup, 2-16
- Cleanup Application, 2-39
- Clear Alarms Button, 2-16
- Cluster Alarm, 2-37
- Cluster Assistant
  - Check, 2-40
  - Cleanup Application, 2-39
- Cluster Configuration, 2-17
  - Folder, 2-19
- Cluster Configuration (smit), 2-20, 2-45
- Cluster Configuration Applications, 2-19
- Cluster Configuration Folder, 2-45
- Cluster Diagnostics, 2-17
- Cluster State, 2-43
- Cluster State, Detail
  - (Figure), 2-43
- Cluster Topology, 2-6
- Cluster User & Groups, 2-17
- Cluster Worksheets, 2-20
- ClusterAssistant
  - Folder, 2-14
  - Online Help, 2-12
  - System Console, 2-15
  - Users, 2-11
- ClusterAssistant Applications window, 2-12
- ClusterWatch, 2-10, 2-17
- ClusterWatch SMIT, 2-18
- ClusterWatch, WatchWare
  - Passwords, 2-10
- Common Desktop Environment (CDE), 1-14
- Communications Adapters
  - ATM, 1-14
  - Ethernet, 1-14
  - FDDI, 1-14
  - Token-Ring, 1-14
- Configuration
  - AIX, 1-5
- Configure Alarms Window
  - (Figure), 2-26
- Configure User Alarms Button, 2-16
- Configuring

- User Alarms, 2-26
- Console Concentrator, 1-5
- Control key
  - use of, 2-11
- Custom Events, 2-19
- Decription
  - Change Button, 2-37
- Dedicated Administration Network, 1-2
- Deregister Cluster, 2-38
- De-register Cluster, 2-20
- Detail View Button, 2-43
- devices.config File
  - Setting up, 2-9
- Domain Types
  - (Figure), 2-3
- Domains, 2-14
- Domains Folder, 2-23, 2-37
  - (Figure), 2-23
- Drag and Drop, 2-11
- errlog, 2-37
- Ethernet Hub, 1-2
- Extended RSF, 2-26
- File
  - /var/bullcluster/deregister\_epc*, 2-38
  - /var/bullcluster/rsf.log*, 2-37
- Folder
  - Domains, 2-23
- Folders
  - Cluster Configuration, 2-19
  - ClusterAssistant, 2-14
  - HACMP Cluster, 2-17
- Front Panel
  - Alarms state active, 2-24
- Front Panel (CDE), 2-12
- Function Selection
  - Drag & Drop, 2-11
- Guidelines
  - Cabling, 1-4
- HA node, 2-2, 2-42
- HA Node State, 2-44
- HA Node State, Detail
  - (Figure), 2-44
- HACMP
  - Cluster Configuration, 2-17
  - Cluster Configuration (smit), 2-20
  - Cluster Diagnostics, 2-17
  - Cluster User & Groups, 2-17
  - Cluster Worksheets, 2-20
  - ClusterWatch, 2-17
  - ClusterWatch SMIT, 2-18
  - Custom Events, 2-19
  - De-register Cluster, 2-20
  - Register Cluster, 2-19
  - Snapshot, 2-19
  - Start Cluster Services, 2-18
  - Stop Cluster Services, 2-18
- HACMP cluster, 2-2, 2-43
- HACMP Cluster, 2-14
  - Folder, 2-17
- HACMP Cluster Applications, 2-17
- HACMP Cluster Folder, 2-45
- HACMP Cluster Topology, 2-6
- HACMP Clusters, 2-38
- Hardware Management Console, 2-15
- Hardware Platforms, 1-1
- Help button, 2-12
- Help Manager, 2-12
- HMC
  - login window, 2-29
  - Using, 2-32
  - Virtual Terminal of Partition Node Access, 1-12
  - WebSM interface, 2-29
- Hub
  - Console Concentrator, 1-5
- Independant Applications
  - Link Equipment, 2-15
- IP Address Format, 2-35
- IP Label Format, 2-35
- LAN Network, 1-14
- link equipment, 2-9
- Link Equipment, 2-15
  - Device Management Netscape Screen
    - (Figure), 2-48
  - Device Management Screen (Figure), 2-47
  - Device Window (Figure), 2-47
- Link Equipment Application, 2-47
- List of Domains Window
  - (Figure), 2-45
- LPAR servers
  - Setup Operations, 2-5
- LPP, 2-3
- LPP\_SOURCE, 2-22
- MKSYSB, 2-22
- Modify
  - Button, 2-37
- Modify Button, 2-37
- Monitoring
  - HA Nodes, 2-44
  - HACMP Cluster, 2-43
  - Nodes, 2-44
- Mozilla, 2-41
- Multiple Function Selection
  - Use of Control Key, 2-11
- Network Connections, 1-5
- Network Install Manager, 2-14
- New Powercluster, 2-35
- NIM, 2-22
  - Backup System, 2-22
  - NIM - SMIT, 2-22
  - Restore System, 2-22
- NIM - SMIT, 2-22
- NIM Clients, 2-22
- NIM Master, 2-22
- NIM on Node, 2-22
- NIM Resource Server, 2-22
- NIM Resources
  - LPP\_SOURCE, SPOT, MKSYSB, 2-22
- NIM Setup Assistant, 2-22
- Node
  - Remove, 2-37
- Node Addresses, 2-35
- Node Icon

- Creation, 2-37
- Node Management Applications
  - SMIT from DSM Server, 2-15
  - WatchWare from DSM Server, 2-15
- Node Name, 2-35
- Node State, 2-44
- Node State, Detail
  - (Figure), 2-44
- Objects
  - Inter-relationships, 2-3
- ODM Classes, 2-19
- Online Help, 2-12
- Partition, 1-1
- partitions, 1-3
- Passwords
  - ClusterWatch, WatchWare, 2-10
  - smwadmin, bullsmw, 2-10
- PortServer, 1-2
  - Configuring Ports, 1-7
  - Parameters, Setting Up, 1-6
- PortServer Console Concentrator
  - Booting, 1-6
  - Setting Up, 1-6
- POWER 5, 1-7
- powercluster, 2-2
- Powercluster
  - Modify, 2-37
  - New, 2-35
  - New registration, 2-35
  - Remove, 2-38
- Powercluster Definition
  - Modify, 2-37
- Powercluster State, 2-15, 2-42
  - HA Node, 2-42
  - HACMP Cluster, 2-43
  - Standalone Node, 2-42
- Powercluster State Window, 2-42
- Register Cluster, 2-19
- Register Powercluster, 2-15, 2-34**
  - Add Node Button, 2-35
  - Apply Button, 2-37
  - Change Description Button, 2-37
  - Change/Show Button, 2-37
  - Modify Button, 2-37
  - Register Button, 2-35
  - Remove Node Button, 2-37
- Register Powercluster window
  - (Figure), 2-34
- Register Powercluster window - Powercluster Name
  - (Figure), 2-35
- Remote Maintenance, 1-14
- Remove Node, 2-37
- Restore System, 2-22
- Rlogin, 2-15
- rlogin session, 2-15
- rootvg, 2-21
- RSF, 2-16, 2-24
  - Extended, 2-26
- Setting Up
  - Link Equipment Application, 2-47
  - Show Alarms Button, 2-16
  - SMIT from DSM Server (Node Management), 2-15
  - SMP servers
    - Setup Operations, 2-4
  - smwadmin, 2-10
  - Snapshot, 2-19
  - Special Considerations
    - NIM Setup Assistant, 2-22
  - SPOT, 2-22
  - Standalone node, 2-2, 2-42
  - Start Cluster Services, 2-18
  - Stop Cluster Services, 2-18
  - System Console, 2-15, 2-27
  - Tape Device, 1-14
  - telnet session, 2-47
  - Telnet session, 2-15
  - Troubleshooting
    - bclwd Daemon, 2-10
  - Typical Configuration, 1-3
  - URL, 2-10
  - User Alarms Window
    - (Figure), 2-26
  - User Password
    - classist, 2-8
  - Utilities
    - Network Install Manager, 2-21
  - Virtual Network Computing, 2-49
  - VNC, 2-49
  - VSM, 2-20
  - Watch button, 2-43
  - WatchWare from DSM Server, 2-15
  - X-terminal, 1-14



## Technical publication remarks form

<b>Title :</b> ESCALA Distributed Software Management for AIX 5L Setup Guide
--

<b>Reference N° :</b> 86 A2 81HX 15
-------------------------------------

<b>Date:</b> Jure 2005
------------------------

### ERRORS IN PUBLICATION

--

### SUGGESTIONS FOR IMPROVEMENT TO PUBLICATION

--

Your comments will be promptly investigated by qualified technical personnel and action will be taken as required.  
If you require a written reply, please include your complete mailing address below.

NAME : \_\_\_\_\_ Date : \_\_\_\_\_

COMPANY : \_\_\_\_\_

ADDRESS : \_\_\_\_\_

Please give this technical publication remarks form to your BULL representative or mail to:

Bull - Documentation D<sup>é</sup>pt.  
1 Rue de Provence  
BP 208  
38432 ECHIROLLES CEDEX  
FRANCE  
info@frec.bull.fr

# Technical publications ordering form

To order additional publications, please fill in a copy of this form and send it via mail to:

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

**Phone:** +33 (0) 2 41 73 72 66  
**FAX:** +33 (0) 2 41 73 70 66  
**E-Mail:** [srv.Duplicopy@bull.net](mailto:srv.Duplicopy@bull.net)

CEDOC Reference #	Designation	Qty
-- -- [ ]		
-- -- [ ]		
-- -- [ ]		
-- -- [ ]		
-- -- [ ]		
-- -- [ ]		
-- -- [ ]		
-- -- [ ]		
-- -- [ ]		
-- -- [ ]		
-- -- [ ]		
[ ] : The latest revision will be provided if no revision number is given.		

NAME: \_\_\_\_\_ Date: \_\_\_\_\_

COMPANY: \_\_\_\_\_

ADDRESS: \_\_\_\_\_

PHONE: \_\_\_\_\_ FAX: \_\_\_\_\_

E-MAIL: \_\_\_\_\_

**For Bull Subsidiaries:**

Identification: \_\_\_\_\_

**For Bull Affiliated Customers:**

Customer Code: \_\_\_\_\_

**For Bull Internal Customers:**

Budgetary Section: \_\_\_\_\_

**For Others: Please ask your Bull representative.**



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

REFERENCE  
**86 A2 81HX 15**