IBM Cluster Systems Management for Linux

Hardware Control Guide

Version 1.3.2

SA22-7856-07

IBM Cluster Systems Management for Linux

Hardware Control Guide

Version 1.3.2

SA22-7856-07

Note

Before using this information and the product it supports, read the information in “Notices” on page 59.

Eighth Edition (September 2003)

This edition of the *IBM Cluster Systems Management for Linux Hardware Control Guide* applies to version 1, release 3, modification 2 of IBM Cluster Systems Management (CSM) for Linux licensed program, product number 5765–E88, CSM for Linux on pSeries, product number 5765-G16, and to all subsequent releases and modifications of this product until otherwise indicated in new editions. Significant changes or additions to the text and illustrations are indicated by a vertical line (|) to the left of the change.

IBM welcomes your comments. A form for readers’ comments may be provided at the back of this publication, or you may address your comments to the following address:

International Business Machines Corporation
Department 55JA, Mail Station P384
2455 South Road
Poughkeepsie, NY 12601-5400
United States of America

FAX (United States & Canada): 1+845+432-9405
FAX (Other Countries):
Your International Access Code +1+845+432-9405

IBMLink™ (United States customers only): IBMUSM10(MHVRCFS)
IBM Mail Exchange: USIB6TC9 at IBMMAIL
Internet e-mail: mhvrcfs@us.ibm.com

If you would like a reply, be sure to include your name, address, telephone number, or FAX number.

Make sure to include the following in your comment or note:

- Title and order number of this book
- Page number or topic related to your comment

When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

Contents

About this book . . . v
Who should use this book . . . v
Typographic conventions . . . v
ISO 9000 . . . vi
Prerequisite and related information . . . vi
How to send your comments . . . viii

Chapter 1. CSM hardware control . . . 1
Hardware control commands . . . 1
Hardware control terminology . . . 2
Hardware and network requirements . . . 3
  Virtual LANs (VLANs) . . . 4
  Conceptual diagram: xSeries, BladeCenter, IntelliStation, and eServer 325 . . 5
| Linux node attributes example . . . 7
  Conceptual diagram: Linux on pSeries . . . 9
| Linux on pSeries node attributes example . . . 11
  Node hardware attributes . . . 13

Chapter 2. Remote power software and configuration . . . 17
Remote power attributes . . . 17
  Remote power attribute values . . . 17
Remote power software configuration . . . 18
  Hardware control security . . . 18
  HMC-attached pSeries server configuration . . . 19
  xSeries server configuration . . . 20
  APC configuration . . . 21
| eServer 325 configuration . . . 23
  System ID attributes . . . 24
Testing remote power hardware control . . . 25
Remote power diagnostics . . . 26
  Remote power log and trace files . . . 26
  Remote access to hardware control points . . . 27
  tcp port numbers . . . 28
  Set up and configuration problems . . . 28
  Connection problems . . . 30
  APC MasterSwitch set up and configuration problems . . . 31
  APC MasterSwitch connection problems . . . 32
  APC MasterSwitch operation problems . . . 33

Chapter 3. Remote console software and configuration . . . 35
Remote console attributes . . . 35
  Remote console attribute values . . . 36
  Remote console fonts . . . 36
| Remote console tiling . . . 37
Conserver multiple read-only consoles . . . 37
Remote console configuration . . . 38
  MRV IR-8000 series configuration . . . 38
  MRV LX-4000 series configuration . . . 39
  ELS configuration . . . 39
  ESP configuration . . . 40
  Computone configuration . . . 41
  CPS configuration . . . 42
Remote console redirection . . . 42

Console redirection on Linux using grub 42
xSeries console redirection 43
BladeCenter console redirection 44
IntelliStation console redirection. 44
Testing remote console hardware control 44
Remote console diagnostics 44
Syntax problems 45
Set up and configuration problems. 45
Connection problems 47
Conserver problems 48
Other problems. 50

Appendix. Hardware configuration 51
eServer 325 51
x360. 51
x440. 51
IntelliStation 52
BladeCenter 52
Configuring the management module. 52
Configuring the switch module 54
Configuring the blade server 55
Launching a remote console 56

Notices 59
Trademarks 60
Publicly Available Software 61
GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION 64

Glossary 69

Bibliography 75
Related information 75
Obtaining publications 75
Redbooks. 75
Other CSM information 75
Getting XCAT tools 76
Getting help from IBM 76
Finding service information 76
Calling IBM for help 76
Contacting CSM development 77

Index 79

About this book

This book describes the hardware, network, software, and configuration requirements for using IBM Cluster Systems Management (CSM) for Linux hardware control functions. This book focuses on the architecture of CSM hardware and how to use CSM remote power and remote console software in a Linux cluster. This book also documents CSM for Linux on pSeries, product #5765–G16. CSM for Linux currently supports Linux nodes only; for information on using Linux and AIX 5L nodes in the same cluster, see the CSM for AIX 5L documentation.

Attention!

- Except where noted, the information in this book also applies to Linux on pSeries clusters. Linux on pSeries clusters must be homogeneous – both a management server and Managed nodes running Linux on pSeries servers only.
- Refer to the Statement of Direction in the IBM Cluster Systems Management V1.3.2 Announcement Letter for information on support for the eServer 325.
- If you are using CSM as part of a prepackaged @server Cluster 1350 solution that you purchased from IBM or an IBM solutions provider, then all of the prerequisite hardware is included. Cluster 1350 hardware and networking are delivered preconfigured for using CSM.

Who should use this book

This book is intended for system administrators who want to use IBM Cluster Systems Management (CSM) for Linux. It describes tools that are provided to use remote hardware control for CSM nodes. The system administrator should:

- Be highly skilled in using most Linux commands and utilities.
- Be comfortable with most basic system administration tools and processes.
- Possess a solid understanding of a Linux-based operating system.
- Be familiar with fundamental networking/distributed computing environment concepts.

Typographic conventions

This book uses the following typographic conventions:

Convention	Usage
bold	**Bold** words or characters represent system elements that you must use literally, such as: command names, file names, option names, and path names.
`constant width`	Examples and information that the system displays appear in `constant-width` typeface.
italic	*Italicized* words or characters represent variable values that you must supply. *Italics* are also used for book titles, for the first use of a glossary term, and for general emphasis in text.
[item]	Used to indicate optional items.
<Key>	Used to indicate keys you press.

ISO 9000

ISO 9000 registered quality systems were used in the development and manufacturing of this product.

Prerequisite and related information

See “Bibliography” on page 75 for:

- A list of related publications
- How to get help from IBM
- Information on Linux XCAT tools.

See the following references for information related to CSM hardware control:

Notes:

1. IBM provides linking information to third party Web sites as a convenience. These Web sites and the information available through these Web sites are not under IBM’s control. If you have any questions or concerns regarding the information available through a third party Web site, please contact the third party directly.
2. For formatting purposes, some of the URLs below contain blank spaces. If you copy and paste these URLs to your Web browser, you must delete the blank spaces to connect to the Web site.

Web site	URL	Resources
IBM CSM for Linux Hardware Control Guide	http://www.ibm.com/servers/eserver/clusters/ library/csmremot.html	• PDF version • BIOS level updates
IBM eserver Clusters library	http://www.ibm.com/servers/eserver/clusters/ library/	• CSM Books • CSM FAQ
IBM Clusters Hardware	http://www.ibm.com/servers/eserver/clusters/ hardware/index.html	• IBM eserver Cluster information • Linux Clusters white paper • Linux education • Linux services
Cluster 1350 InfoCenter	http://publib.boulder.ibm.com/cluster/	HTML version
IBM Hardware Management Console (HMC) for pSeries documentation	http://www.ibm.com/servers/eserver/pseries/ library/hardware_docs/hmc.html	• installation and operations guide • hardware maintenance guide
pSeries hardware documentation	http://www.ibm.com/servers/eserver/pseries/ library/hardware_docs/	• product documentation • service documentation • installation options
BladeCenter documentation	http://www.pc.ibm.com/us/eserver/xseries/ bladecenter_family.html	product documentation
BladeCenter firmware updates	http://www.pc.ibm.com/qtechinfo/ MIGR-4JTS2T.html	• README files • firmware downloads
xSeries 330 documentation	http://www.pc.ibm.com/us/eserver/ xseries/x330.html	• specifications • publications
xSeries 335 documentation	http://www.pc.ibm.com/us/eserver/ xseries/x335.html	• specifications • publications

Web site	URL	Resources
xSeries 342 documentation	http://www.pc.ibm.com/us/eserver/xseries/x342.html	• specifications • publications
xSeries 345 documentation	http://www.pc.ibm.com/us/eserver/xseries/x345.html	• specifications • publications
xSeries 360 documentation	http://www.pc.ibm.com/us/eserver/xseries/x360.html	• specifications • publications
xSeries 360 firmware updates	http://www.pc.ibm.com/qtechinfo/MIGR-4JTS2T.html	• README files • firmware downloads
xSeries 440 documentation	http://www.pc.ibm.com/us/eserver/xseries/x440.html	• specifications • publications
xSeries 445 documentation	http://www.pc.ibm.com/us/eserver/xseries/x445.html	• specifications • publications
eServer 325 documentation	http://www.pc.ibm.com/us/eserver/opteron/325/view_models.html	• specifications • publications
IntelliStation documentation	http://www.pc.ibm.com/us/intellistation/tech_library.html	• specifications • publications
Remote Supervisor Adapter (RSA) documentation	http://www.pc.ibm.com/qtechinfo/MIGR-4UKSML.html	• specifications • publications
Virtual LAN (VLAN) documentation	http://standards.ieee.org/	IEEE standards
Conserver serial console application information	http://www.conserver.com/	• FAQ • Source code and documentation
MRV IR-8020 and IR-8040 information	http://www.mrv.com/product/MRV-IR-003	• Specifications • Product description
MRV LX-4000 information	http://www.mrv.com/product/MRV-IR-008	• Specifications • Product description
Equinox Ethernet Serial Provider (ESP) Installation Guide	http://www.equinox.com/Hardware_Manuals192.html	• FAQ • Product installation
Equinox Ethernet Serial Provider (ESP) Device Drivers	http://www.equinox.com/Driver_Search152.cfm	• ESP Driver for Linux
Computone IntelliServer information	http://www.computone.com	• Specifications • FAQ • Documentation
American Power Conversion (APC) MasterSwitch information	http://www.apc.com/products/family/index.cfm?id=70	• Specifications • Installation Manual • User's Guides
Avocent CPS1600 information	http://www.avocent.com	• Specifications • FAQ • Product manual

Web site	URL	Resources
ECT for Linux	http://www.alphaworks.ibm.com/tech/ect4linux	• Product overview • Requirements • Downloads
Linux Documentation Project	http://www.ibiblio.org/mdw/index.html	• Serial-HOWTO • Serial-Programming-HOWTO • Modem-HOWTO

How to send your comments

Your feedback is important in helping us to produce accurate, high-quality information. If you have any comments about this book or any other CSM documentation:

- Send your comments by e-mail to: mhvrcfs@us.ibm.com.

  Include the book title and order number, and, if applicable, the specific location of the information you have comments on (for example, a page number or a table number).
- Fill out one of the forms at the back of this book and return it by mail, by fax, or by giving it to an IBM representative.

To contact IBM CSM development, send your comments by e-mail to: cluster@us.ibm.com.

Chapter 1. CSM hardware control

IBM Cluster Systems Management (CSM) for Linux hardware control software provides remote hardware control functions for CSM cluster nodes from a single point of control. CSM allows a system administrator to control cluster nodes remotely through access to the cluster management server. From the management server, an administrator runs cluster management commands using the command line.

CSM hardware control functions depend on the specific hardware, software, network, and configuration requirements described in this book. The requirements for remote power are separate and distinct from the requirements for remote console. Linux clusters without the hardware, software, network, or configuration required to use CSM hardware control can still have CSM installed on some or all cluster nodes. However, in such clusters the hardware control commands may be inoperable or provide only limited function.

CSM for Linux supports remote hardware control for xSeries, pSeries, BladeCenter, IntelliStation, and eServer 325 servers from a Linux management server.

A CSM for Linux on pSeries cluster must be exclusively pSeries – it must include a Linux on pSeries management server and Linux on pSeries nodes only.

Attention!

- Except where noted, the information in this book also applies to Linux on pSeries clusters. Linux on pSeries clusters must be homogeneous – both a management server and Managed nodes running Linux on pSeries servers only.
- Refer to the Statement of Direction in the IBM Cluster Systems Management V1.3.2 Announcement Letter for information on support for the eServer 325.
- If you are using CSM as part of a prepackaged @server Cluster 1350 solution that you purchased from IBM or an IBM solutions provider, then all of the prerequisite hardware is included. Cluster 1350 hardware and networking are delivered preconfigured for using CSM.

Hardware control commands

The following list describes the CSM hardware control commands; see the man pages or the *IBM CSM for Linux: Command and Technical Reference* for detailed command usage information.

chrconsolecfg
Removes, adds, or rewrites console entries in the Conserver configuration file.

chsnmp
Sets the SNMP agent configuration information for xSeries and BladeCenter servers.

getadapters
Collects information for LAN adapters.

lshwinfo
Collects node information from one or more hardware control points. This command is not supported on IntelliStation workstations.

lshwstat Collects environmental and Vital Product Data (VPD) information. This command is not supported for CSM for Linux on pSeries.

lssnmp Collects SNMP agent configuration information from xSeries and BladeCenter servers.

rconsole Opens a remote console for a node.

rconsolerefresh
refreshes the Conserver daemon.

reventlog Collects service processor log information for xSeries and BladeCenter servers.

rpower Boots, resets, powers on and off, and queries node hardware and CECs.

systemid Stores the user ID and password required for internal programs to access remote hardware.

Hardware control terminology

Terms used in this book include:

apc The *PowerMethod* attribute value for IBM IntelliStation workstations. CSM remote power for IntelliStations is controlled by the APC MasterSwitch. The hardware control point for IntelliStations is the IP address or host name of the APC MasterSwitch.

bmc The *PowerMethod* attribute value for IBM eServer 325 servers. CSM remote power for the eServer 325 is controlled by the baseboard management controller (BMC).

CEC Central Electronics Complex. A CEC is a single HMC-attached pSeries server, which might have the option of being divided into LPARs.

console server
The hardware device through which the management server opens a remote console session for a node.

hardware control point
The hardware device through which the management server controls node hardware.

hmc The *PowerMethod* attribute value for HMC-attached pSeries servers.

HMC The Hardware Management Console (HMC) is the hardware control point for HMC-attached pSeries servers.

IBM.HWCTRLRM
The IBM Hardware Control resource manager, which manages the **IBM.NodeHwCtrl** and **IBM.HwCtrlPoint** resource classes.

ISMP The IBM Integrated System Management Processor (ISMP) device provides monitoring and remote power control for xSeries servers. ″ISMP″ can be used synonymously with ″ASM.″

LPAR Logical partition. A single HMC-attached pSeries server can be divided into multiple LPARs, or nodes.

management module
The hardware control point for blade servers is the BladeCenter chassis management module (MM).

RCONSOLE_FONT
Environment variable specifying the X-Windows font to be used by the **rconsole** command.

RCONSOLE_LIST
Environment variable specifying a file that lists the nodes to open console sessions for. The file must contain only one node name per line.

RSA The IBM Remote Supervisor Adapter (RSA) is the hardware control point for xSeries servers.

SPM The Cluster 1350 Serial Port Module (SPM) is an optional component that provides **rconsole** command function for BladeCenter.

xseries
The *PowerMethod* attribute value for xSeries and BladeCenter servers.

VLAN virtual LAN – A division of a local area network by software rather than by physical arrangement of cables.

Hardware and network requirements

CSM for Linux hardware control depends on the specific hardware and network requirements described in this book. The management server can be connected to cluster nodes and external networks using various configurations of IBM and non-IBM hardware and software that meet the CSM architecture requirements described in this book. For the specific cluster hardware models required to use CSM 1.3, see the *IBM CSM for Linux: Planning and Installation Guide*. See "Hardware configuration," on page 51 for model-specific hardware control configuration requirements.

The **rpower** command communicates with hardware control points to request node power status, reboot, and power on and off functions. A hardware control point is the specific piece of hardware through which the management server controls node hardware. Hardware control points should be on the management virtual LAN (VLAN) and connected to the hardware that ultimately controls the power functions. The supported hardware control points are the HMC for HMC-attached pSeries, RSA for xSeries, the management module for BladeCenter, the BMC for the eServer 325, and the APC MasterSwitch for IntelliStation.

The **rconsole** command communicates with console server hardware to open a console window for a node on the CSM management server. Console servers must be on the management VLAN, which connects the management server to the cluster hardware, and connected to node serial ports. This out of band network configuration allows a remote console to be opened from the management server even if the cluster VLAN is inaccessible. For example, if the cluster VLAN is offline, remote console can still access the target node to open a console window. xSeries servers and IntelliStations can use any of the following console servers:

- MRV IR-8020, IR-8040, LX-4008S, LX-4016S, and LX-4032S
- Equinox ESP-8, ESP-16, and ELS-16 II (CSM supports the ESP console server on Red Hat 7.2, 7.3, and 8.0 management servers only.)
- Computone IntelliServer RCM4, RCM8, and RCM24
- Avocent CPS1600

Linux on pSeries clusters use the HMC for remote console; no additional console device is required or supported.

Remote console for BladeCenter must use the MRV IR-8020 or IR-8040 console server and be part of an IBM Cluster 1350 with the Serial Port Module option.

Virtual LANs (VLANs)

A VLAN (virtual Local Area Network) is a division of a local area network by software rather than by physical arrangement of cables. Dividing a LAN into subgroups can simplify and speed up communications within a workgroup. Switching a user from one VLAN to another using software is also more efficient than rewiring the hardware.

IBM suggests creating one VLAN for the CSM management server and hardware control points, and a separate VLAN for the CSM management server and cluster nodes. Although cluster hardware control points and nodes can be on the same VLAN, limiting access to the management VLAN reduces security exposure for IP traffic on the management VLAN and access to hardware control points.

The VLANs discussed in this book refer to VLANs as defined by IEEE standards – see http://standards.ieee.org/ for details. Figure 1 on page 6 shows a network partitioned into three virtual LANs; management, cluster, and public VLANs, which are defined as follows:

management VLAN
Hardware control commands such as **rpower** and **rconsole** are run on the management server and communicate to nodes through the management VLAN. The management VLAN connects the management server to the cluster hardware through an Ethernet connection. For optimal security, the management VLAN must be restricted to hardware control points, remote console servers, the management server, and root users. Routing between the management VLAN and cluster or public VLANs could compromise security on the management VLAN.

Note: The management VLAN is subject to the RSA restriction of 10/100 Mb/s.

cluster VLAN
The cluster VLAN connects nodes to each other and to the management server through an Ethernet connection. Installation and CSM administration tasks such as running **dsh** are done on the cluster VLAN. Host names and attribute values for nodes on the cluster VLAN are stored in the CSM database.

public VLAN
The public VLAN connects the cluster nodes and management server to the site network. Applications are accessed and run on cluster nodes over the public VLAN. The public VLAN can be connected to nodes through a second Ethernet adapter in each node, or by routing to each node through the Ethernet switch.

Conceptual diagram: xSeries, BladeCenter, IntelliStation, and eServer 325

Attention!

The diagrams discussed in this book are provided for conceptual explanation only. They are not intended to be literal depictions of how to configure a specific cluster. See the @server Cluster 1350 documentation resources listed in “Prerequisite and related information” on page vi for specific cluster hardware configuration details. For specific RSA and ISMP connectivity requirements, see the hardware documentation resources listed in “Prerequisite and related information” on page vi.

Figure 1 on page 6 shows the hardware and networking configuration required for using CSM hardware control with xSeries, eServer 325, and BladeCenter servers running Linux and IntelliStation workstations running Linux.

The management server shown in the diagram connects to the management and cluster VLANs through Ethernet adapters. The console servers (**mrv01, mrv02**) connect to the management VLAN through Ethernet adapters, to the xSeries and eServer 325 servers and IntelliStation workstations through serial (COM) ports, and to BladeCenter servers through the Cluster 1350 Serial Port Module option.

The IBM Cluster 1350 Serial Port Module is an optional part that must be ordered separately to connect BladeCenter servers to an MRV console server. This connection provides **rconsole** command function for BladeCenter servers. See “Launching a remote console” on page 56 for the part numbers and configuration required for this alternative to using a Web browser for BladeCenter remote console function.

The management VLAN connects to the IBM Remote Supervisor Adapter (RSA) in select xSeries servers. The servers must be connected to the cluster VLAN through their first Ethernet adapters (eth0), and directly or indirectly to an RSA. An RSA connects to its node Internal Systems Management Processor (ISMP) port, and up to 24 node ISMP ports can be daisy-chained from the RSA ISMP port. See the RSA documentation listed in “Prerequisite and related information” on page vi for the number of nodes supported.

The management VLAN connects to IntelliStation workstations through the APC MasterSwitch (**apc01**) Ethernet port. Power cables connect the IntelliStations to the APC MasterSwitch. The management VLAN connects to blade servers through the BladeCenter chassis management module (**mm01**), and to eServer 325 through the baseboard management controller (BMC).

Applications usually run on the public VLAN, which connects to the servers through Ethernet ports. Configuration for a public VLAN is flexible and can be defined by the system administrator. See “Node hardware attributes” on page 13 for example node attribute definitions corresponding to Figure 1.

Figure 1. CSM hardware control configuration for xSeries, BladeCenter, IntelliStation, and eServer 325

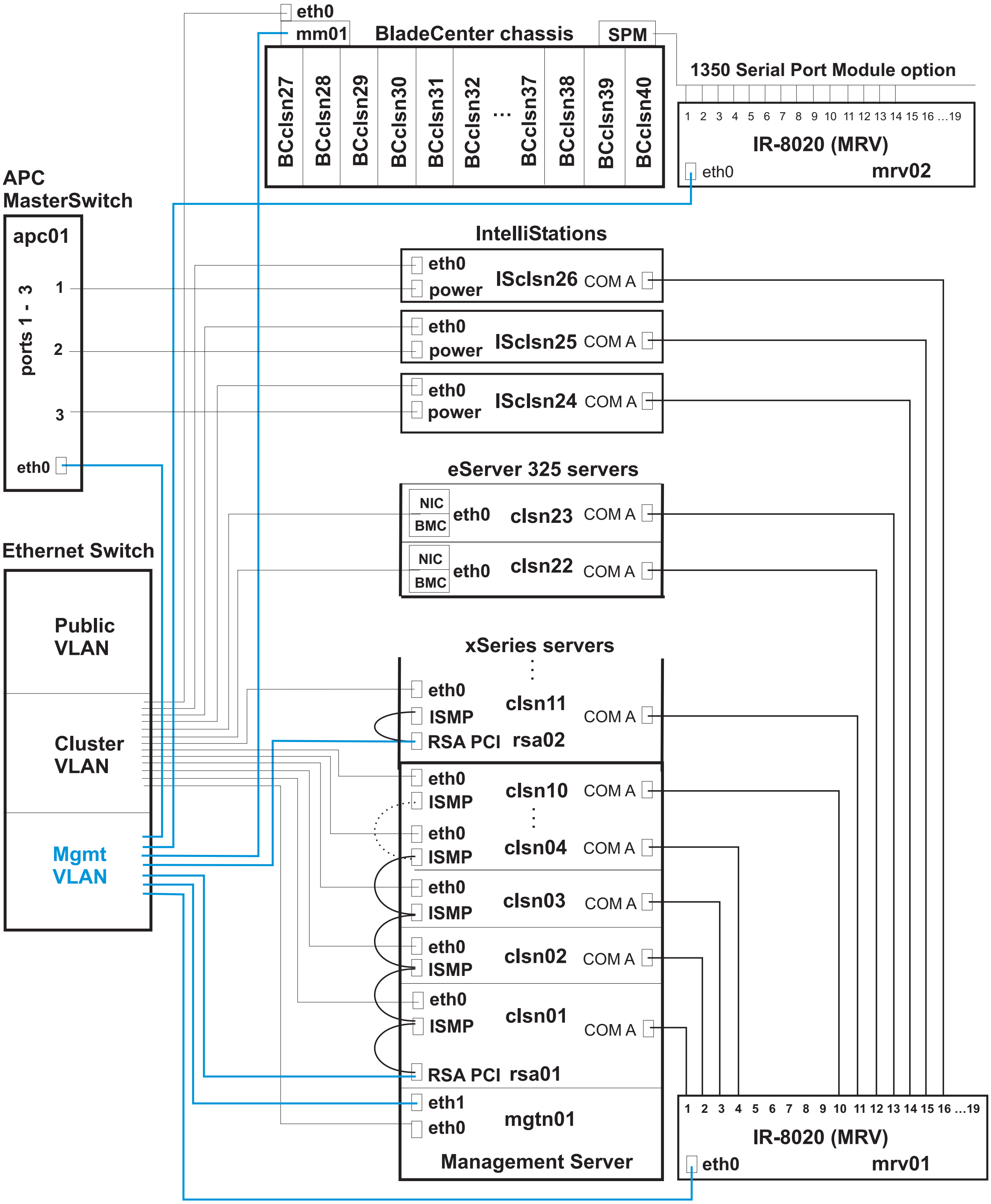
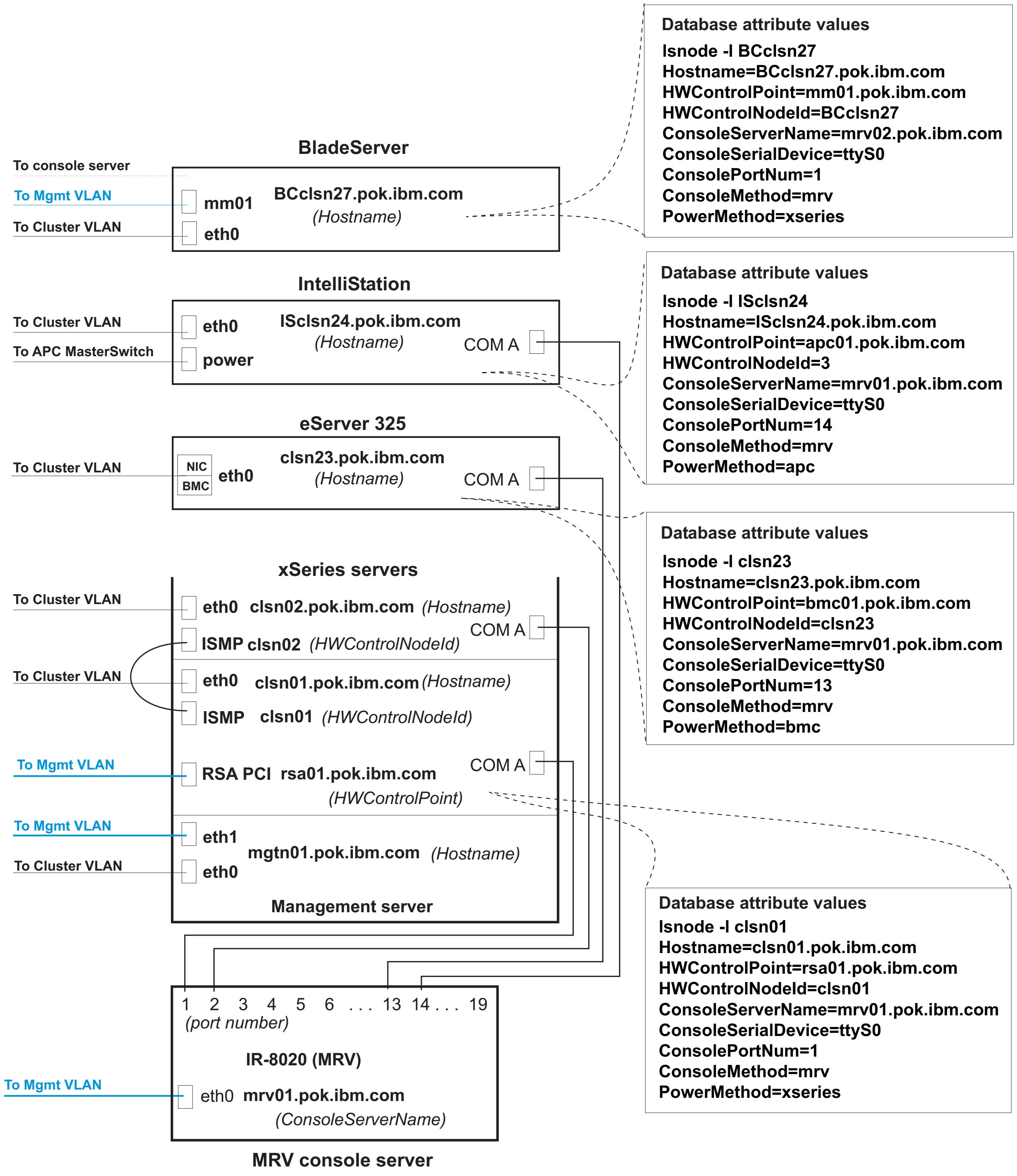


Figure 1. CSM hardware control configuration for xSeries, BladeCenter, IntelliStation, and eServer 325

Linux node attributes example

Figure 2 on page 8 shows the relationship between the CSM node database attributes and the internal hardware names used in Figure 1. For remote power and remote console to work as expected, this matching of database attribute names to the internal hardware values must be correct for all management processors (ISMPs), remote supervisor adapters (RSAs), management modules, APCs, BMCs, and console servers in the CSM cluster.

Figure 2. CSM hardware control attribute values for Linux nodes



Database attribute values

lsnode -l BCclsn27
Hostname=BCclsn27.pok.ibm.com
HWControlPoint=mm01.pok.ibm.com
HWControlNodeId=BCclsn27
ConsoleServerName=mrv02.pok.ibm.com
ConsoleSerialDevice=ttyS0
ConsolePortNum=1
ConsoleMethod=mrv
PowerMethod=xseries

Database attribute values

lsnode -l ISclsn24
Hostname=ISclsn24.pok.ibm.com
HWControlPoint=apc01.pok.ibm.com
HWControlNodeId=3
ConsoleServerName=mrv01.pok.ibm.com
ConsoleSerialDevice=ttyS0
ConsolePortNum=14
ConsoleMethod=mrv
PowerMethod=apc

Database attribute values

lsnode -l clsn23
Hostname=clsn23.pok.ibm.com
HWControlPoint=bmc01.pok.ibm.com
HWControlNodeId=clsn23
ConsoleServerName=mrv01.pok.ibm.com
ConsoleSerialDevice=ttyS0
ConsolePortNum=13
ConsoleMethod=mrv
PowerMethod=bmc

Database attribute values

lsnode -l clsn01
Hostname=clsn01.pok.ibm.com
HWControlPoint=rsa01.pok.ibm.com
HWControlNodeId=clsn01
ConsoleServerName=mrv01.pok.ibm.com
ConsoleSerialDevice=ttyS0
ConsolePortNum=1
ConsoleMethod=mrv
PowerMethod=xseries

Figure 2. CSM hardware control attribute values for Linux nodes

Conceptual diagram: Linux on pSeries

Figure 3 on page 10 shows the hardware and networking configuration required for using CSM hardware control with HMC-attached pSeries servers running Linux. The HMC-attached pSeries server in the diagram is a single piece of hardware that has been partitioned by HMCs into 16 LPARs (nodes). The management server connects to the management and cluster VLANs through Ethernet adapters. Nodes on HMC-attached pSeries servers must be connected to the cluster VLAN and directly or indirectly to an HMC. Configuration for a public VLAN is flexible and can be defined by the system administrator. See “Node hardware attributes” on page 13 for example node attribute definitions.

Figure 3. CSM hardware control hardware configuration for pSeries

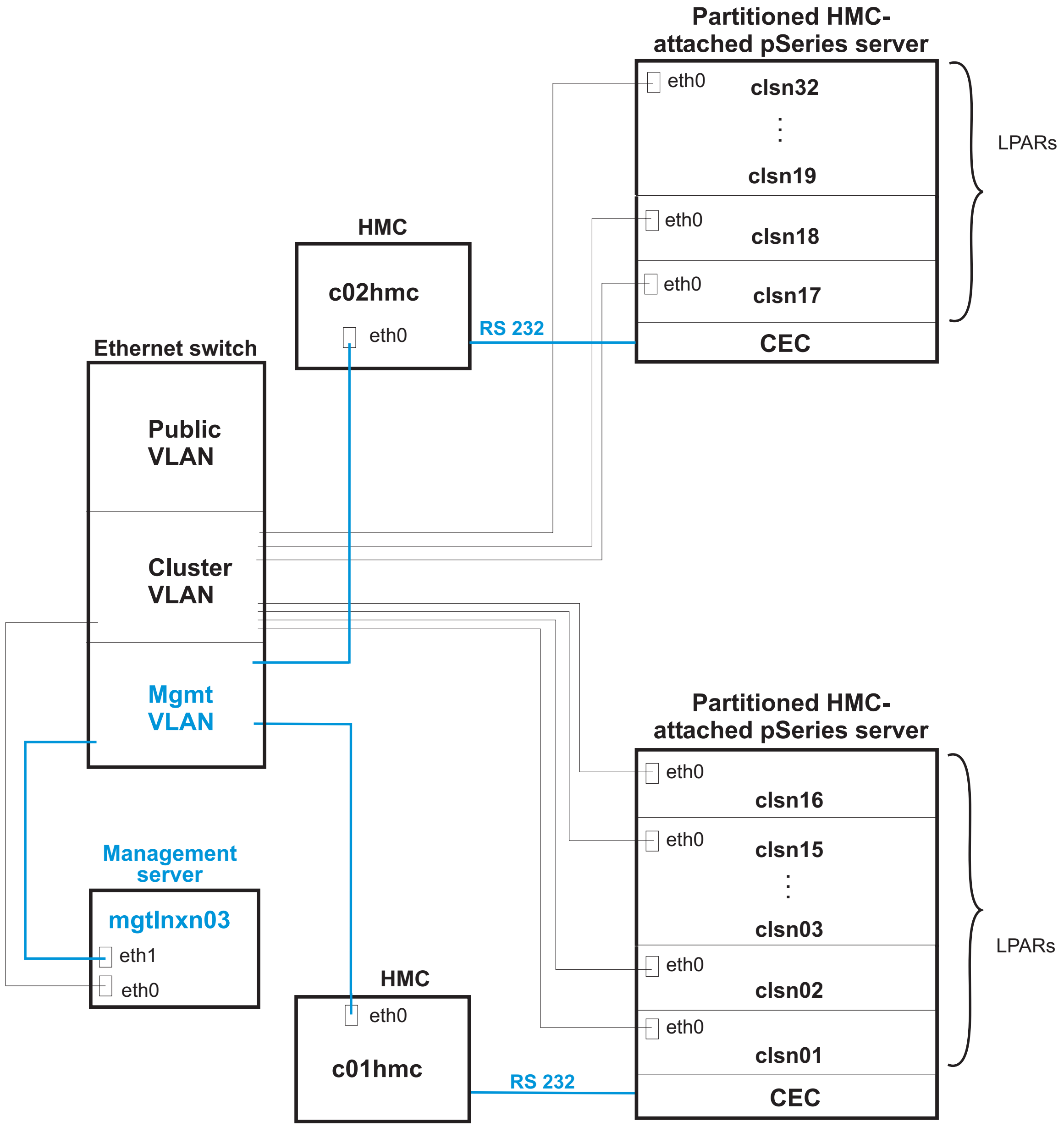
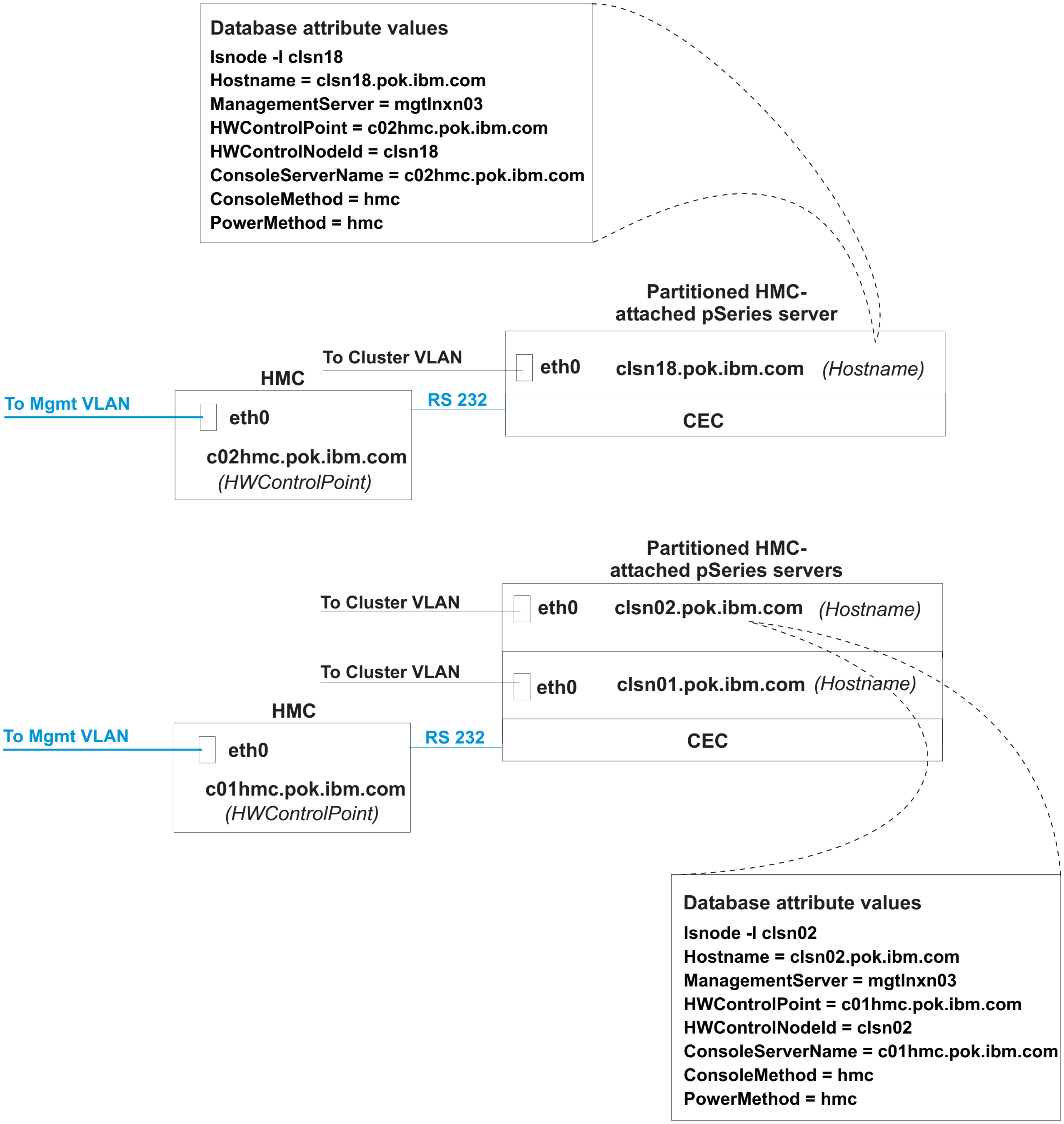


Figure 3. CSM hardware control hardware configuration for Linux on pSeries

Linux on pSeries node attributes example

Figure 4 on page 12 is a detailed view of some nodes from Figure 3. The diagram shows the relationship between the CSM node database attributes and the internal hardware names used in Figure 3. For remote power and remote console to work as expected, this matching of database attribute names to the internal hardware values must be correct for all management processors (MPs), management processor adapters (MPAs), and console serial providers in the cluster.

Figure 4. CSM hardware control database attribute values for Linux nodes



Database attribute values

lsnode -l clsn18
Hostname = clsn18.pok.ibm.com
ManagementServer = mgtlnxn03
HWControlPoint = c02hmc.pok.ibm.com
HWControlNodeId = clsn18
ConsoleServerName = c02hmc.pok.ibm.com
ConsoleMethod = hmc
PowerMethod = hmc

Database attribute values

lsnode -l clsn02
Hostname = clsn02.pok.ibm.com
ManagementServer = mgtlnxn03
HWControlPoint = c01hmc.pok.ibm.com
HWControlNodeId = clsn02
ConsoleServerName = c01hmc.pok.ibm.com
ConsoleMethod = hmc
PowerMethod = hmc

Figure 4. CSM hardware control database attribute values for Linux nodes

Node hardware attributes

CSM hardware control configuration can be facilitated by completing a table describing the cluster node hardware attribute values; see Table 1 on page 14 for an example. Attribute values for the nodes correspond to the hardware and network configuration shown in Figure 1 on page 6. See Table 2 on page 15 for node attribute values corresponding to Figure 3 on page 10. See Chapter 2, “Remote power software and configuration,” on page 17 and Chapter 3, “Remote console software and configuration,” on page 35 for detailed descriptions of the attributes described in Table 1 on page 14. See the *IBM CSM for Linux: Planning and Installation Guide* for a blank node attributes planning worksheet.

An alternative to filling out hardcopy planning sheets is to create a host name mapping file, which can be specified using the **definenode –M** option. For example, you can run the **lshwinfo** command to collect node information and write the results to a **nodedef** file. For detailed information see the section on determining and storing node hardware attribute values in the *IBM CSM for Linux: Planning and Installation Guide*.

Table 1. Linux node attribute values for Figure 1

Hostname	*HWControlPoint*	*PowerMethod*	*HWControl NodeId*	*ConsoleServerName*	*ConsoleServerNumber*	*Console Method*	*Console PortNum*	*Console Serial Device*
clsn01.pok.ibm.com	rsa01.pok.ibm.com	xseries	clsn01	mrv01.pok.ibm.com	not applicable	mrv	1	ttyS0
clsn02.pok.ibm.com	rsa01.pok.ibm.com	xseries	clsn02	mrv01.pok.ibm.com	not applicable	mrv	2	ttyS0
clsn03.pok.ibm.com	rsa01.pok.ibm.com	xseries	clsn03	mrv01.pok.ibm.com	not applicable	mrv	3	ttyS0
clsn04.pok.ibm.com	rsa01.pok.ibm.com	xseries	clsn04	mrv01.pok.ibm.com	not applicable	mrv	4	ttyS0
clsn05.pok.ibm.com	rsa01.pok.ibm.com	xseries	clsn05	mrv01.pok.ibm.com	not applicable	mrv	5	ttyS0
clsn06.pok.ibm.com	rsa01.pok.ibm.com	xseries	clsn06	mrv01.pok.ibm.com	not applicable	mrv	6	ttyS0
clsn07.pok.ibm.com	rsa01.pok.ibm.com	xseries	clsn07	mrv01.pok.ibm.com	not applicable	mrv	7	ttyS0
clsn08.pok.ibm.com	rsa01.pok.ibm.com	xseries	clsn08	mrv01.pok.ibm.com	not applicable	mrv	8	ttyS0
clsn09.pok.ibm.com	rsa01.pok.ibm.com	xseries	clsn09	mrv01.pok.ibm.com	not applicable	mrv	9	ttyS0
clsn10.pok.ibm.com	rsa01.pok.ibm.com	xseries	clsn10	mrv01.pok.ibm.com	not applicable	mrv	10	ttyS0
(continued ...)								
clsn21.pok.ibm.com	rsa02.pok.ibm.com	xseries	clsn21	mrv01.pok.ibm.com	not applicable	mrv	11	ttyS0
clsn22.pok.ibm.com	bmc01.pok.ibm.com	bmc	clsn22	mrv01.pok.ibm.com	not applicable	mrv	12	ttyS0
clsn23.pok.ibm.com	bmc02.pok.ibm.com	bmc	clsn23	mrv01.pok.ibm.com	not applicable	mrv	13	ttyS0
ISclsn24.pok.ibm.com	rsa02.pok.ibm.com	apc	3	mrv01.pok.ibm.com	not applicable	mrv	14	ttyS0
ISclsn25.pok.ibm.com	rsa02.pok.ibm.com	apc	2	mrv01.pok.ibm.com	not applicable	mrv	15	ttyS0
ISclsn26.pok.ibm.com	rsa02.pok.ibm.com	apc	1	mrv01.pok.ibm.com	not applicable	mrv	16	ttyS0
BCclsn27.pok.ibm.com	mm01.pok.ibm.com	xseries	BCclsn27	mrv02.pok.ibm.com	not applicable	mrv	1	ttyS0
BCclsn28.pok.ibm.com	mm01.pok.ibm.com	xseries	BCclsn28	mrv02.pok.ibm.com	not applicable	mrv	2	ttyS0
BCclsn29.pok.ibm.com	mm01.pok.ibm.com	xseries	BCclsn29	mrv02.pok.ibm.com	not applicable	mrv	3	ttyS0
(continued ...)								
BCclsn40.pok.ibm.com	mm01.pok.ibm.com	xseries	BCclsn40	mrv02.pok.ibm.com	not applicable	mrv	14	ttyS0

Table 2. Linux node attribute values for Figure 3.

Hostname	*HWControlPoint*	*Power Method*	*HWControl NodeId*	*ConsoleServerName*	*Console Method*	*ConsolePortNum*
clsn01.pok.ibm.com	c01hmc.pok.ibm.com	hmc	clsn01	c01hmc.pok.ibm.com	hmc	not applicable
clsn02.pok.ibm.com	c01hmc.pok.ibm.com	hmc	clsn02	c01hmc.pok.ibm.com	hmc	not applicable
clsn03.pok.ibm.com	c01hmc.pok.ibm.com	hmc	clsn03	c01hmc.pok.ibm.com	hmc	not applicable
(continued ...)						
clsn16.pok.ibm.com	c01hmc.pok.ibm.com	hmc	clsn16	c01hmc.pok.ibm.com	hmc	not applicable
clsn17.pok.ibm.com	c02hmc.pok.ibm.com	hmc	clsn17	c02hmc.pok.ibm.com	hmc	not applicable
clsn18.pok.ibm.com	c02hmc.pok.ibm.com	hmc	clsn18	c02hmc.pok.ibm.com	hmc	not applicable
clsn19.pok.ibm.com	c02hmc.pok.ibm.com	hmc	clsn19	c02hmc.pok.ibm.com	hmc	not applicable
(continued ...)						
clsn26.pok.ibm.com	c02hmc.pok.ibm.com	hmc	clsn26	c02hmc.pok.ibm.com	hmc	not applicable
clsn27.pok.ibm.com	c02hmc.pok.ibm.com	hmc	clsn27	c02hmc.pok.ibm.com	hmc	not applicable
clsn28.pok.ibm.com	c02hmc.pok.ibm.com	hmc	clsn28	c02hmc.pok.ibm.com	hmc	not applicable
(continued ...)						
clsn32.pok.ibm.com	c02hmc.pok.ibm.com	hmc	clsn32	c02hmc.pok.ibm.com	hmc	not applicable

Chapter 2. Remote power software and configuration

Once your CSM hardware and networking have been configured, you must install and configure CSM software to enable remote power functions. The **installms** command installs the required CSM packages, including the remote power commands, on the management server. For detailed CSM installation instructions, see the *IBM CSM for Linux: Planning and Installation Guide*. For detailed remote power command usage information, see the **rpower**, **definenode**, **installms**, **reventlog**, **lshwinfo**, **lshwstat**, **chsnmp**, and **lssnmp** man pages or the *IBM CSM for Linux: Command and Technical Reference*.

Remote power attributes

Using the CSM **rpower** remote power command requires node attribute definitions in the CSM database for each hardware control point in the cluster. When defining new nodes using the **definenode** command, you must specify the required *PowerMethod*, *HWControlPoint*, and *HWControlNodeId* attribute values. Run the **lshwinfo** command to retrieve the current node hardware attribute values from the hardware control point. To change node attribute values in the CSM database, use the **chnode** or **definenode –m** command.

To use the **rpower** command, you must correctly define the following remote power attributes in the CSM database:

PowerMethod
The method used by CSM to control a specific node hardware type: **apc**, **hmc**, **bmc**, or **xseries**.

HWControlPoint
The name assigned to the hardware device through which CSM controls the node hardware.

HWControlNodeId
The ID defined for the node.

Remote power attribute values

The following table describes the CSM node hardware types and their required remote power attribute values. For more information about these node hardware types, see the product Web site URLs listed in “Prerequisite and related information” on page vi.

Table 3. Remote power attribute values

attribute	**xSeries**	**pSeries**	**BladeCenter**	**IntelliStation**	**eServer 325**
PowerMethod	**xseries**	**hmc**	**xseries**	**apc**	**bmc**
HWControlPoint	RSA short host name, long host name, or IP address	HMC short host name, long host name, or IP address	Management module short host name, long host name, or IP address	APC MasterSwitch short host name, long host name, or IP address	bmc short host name, long host name, or IP address
HWControlNodeId	ISMP hardware text ID	user-defined LPAR name	ASM name	APC MasterSwitch outlet port number	node name

Note: For xSeries servers, setting the hardware text ID to the short host name of the node can simplify the node definition process. See the **definenode** man page or the *IBM CSM for Linux: Planning and Installation Guide* for examples.

Remote power software configuration

Accessing a hardware control point, which is the intermediate hardware device for node hardware control, requires a user ID and password. You must run the **systemid** command on the management server to define or change the hardware control point user IDs and passwords in the CSM database. This information is then used by the **rpower** command to communicate with hardware control points. If you use the default hardware user IDs and passwords on xSeries hardware, then you do not need to run the **systemid** command. For optimal security, IBM suggests running the **systemid** command to define the user IDs and passwords required to access hardware control points. See Table 3 on page 17 for the hardware control point attribute values required for each hardware type.

Whenever an ID or password is changed on the hardware, the corresponding ID and password must also be changed in the password files using the **systemid** command. The user IDs and encrypted passwords are stored in files in the **/etc/opt/csm/system_config** directory. The file names are the IP address of the node or the hardware control point if the host name can be resolved. If the host name cannot be resolved, the actual node name entered in the **systemid** command becomes the file name.

Hardware control security

Access to the hardware control classes and actions is controlled by stanzas in the **/var/ct/cfg/ctrmc.acls** file. If this file does not exist then a sample **ctrmc.acls** file can be copied from the **/usr/sbin/rsct/cfg** directory to **/var/ct/cfg** and modified.

By default, only root on the CSM management server can perform actions such as **rpower** and **lshwinfo**, which call actions on the **IBM.NodeHwCtrl** and **IBM.HwCtrlPoint** resources classes, respectively. Other users on the CSM management server have read-only access by default, which allows users to view attribute data from these classes but does not allow them to perform actions.

The following example stanzas for the **IBM.NodeHwCtrl** and **IBM.HwCtrlPoint** resource classes give the user IDs **root** and **user** on the local host (the CSM management server) read and write access, and all other users on the CSM management server read-only access:

```
IBM.NodeHwCtrl
    root@LOCALHOST       *       rw
    user@LOCALHOST       *       rw
    LOCALHOST            *       r

IBM.HwCtrlPoint
    root@LOCALHOST       *       rw
    user@LOCALHOST       *       rw
    LOCALHOST            *       r
```

To limit remote power control to certain users, you must set user permissions in the **ctrmc.acls** file. The **refresh –s ctrmc** command must be run after modifying the **ctrmc.acls** file for the updated access changes to take effect. For detailed information on the **ctrmc.acls** file see the *IBM RSCT for Linux: Administration Guide*.

HMC-attached pSeries server configuration

To configure remote power for HMC-attached pSeries servers, run the **systemid** command on the management server to define the user ID and passwords required to access the HMC. There are no default ID and password values for an HMC. To change a user ID on the HMC, see the *IBM Hardware Management Console for pSeries Operations Guide* listed in “Prerequisite and related information” on page vi. If you change the user ID for an HMC, you must subsequently run the **systemid** command to set the new information for the management server.

HMC-attached pSeries configuration examples

The following examples show how to create system IDs for HMC-attached pSeries servers on the management server. The commands will prompt for a valid password. In the examples the node being defined has the following hardware control attributes:

```
Hostname = clsn01.pok.ibm.com
HWControlPoint = c01hmc.pok.ibm.com
HWControlNodeId = clsn01
PowerMethod = hmc
```

Note: To change attributes for nodes that have already been defined, use the **chnode** command.

1. If you are not using the default user ID and passwords, then rerun the **systemid** command to define them. See “Creating and testing system IDs” on page 24 for detailed examples.
2. Run the **systemid** command to define the user ID and password required to access the HMC that controls the node:

   ```
   systemid c01hmc.pok.ibm.com USERID
   ```

   Enter the password when prompted.
3. Define the node in the CSM database. Note that there are several options for the **definenode** command. This example shows the specification of all information required for hardware control of the node. See the **definenode** man page or the *IBM CSM for AIX 5L: Administration Guide* for detailed command usage information.

   ```
   definenode -n clsaixn01.pok.ibm.com -H c01hmc.pok.ibm.com \
   HWControlNodeId=clsaixn01 PowerMethod=hmc
   ```
4. Verify that the node attributes are correct:

   ```
   lsnode -l clsaixn01.pok.ibm.com
   ```

   Verify that the attribute values returned for *Hostname*, *HWControlPoint*, *HWControlNodeId* and *PowerMethod* are correct. If any are incorrect, use the **chnode** command to correct them.
5. Test remote power control by entering:

   ```
   rpower -n clsaixn01.pok.ibm.com query
   ```

   Output from this command should be similar to:

   ```
   clsaixn01.pok.ibm.com on
   ```

   If there was a problem determining the query value then a message is returned indicating the problem. See “Remote power diagnostics” on page 26 for help determining the problem and resolution.

The following examples would require rerunning the **systemid** command and possibly changing node configuration information in the CSM database.

1. If the HMC IP address or host name has changed:
   a. Run the **systemid** command with the new IP address or host name and the HMC user ID. Enter the HMC password when prompted.
   b. Run the **chnode** command for all the nodes using this HMC as their hardware control point. Modify the *HWControlPoint* and *ConsoleServerName* attribute values to match the new HMC host name. For example, if the HMC host name changed to c01hmc.pok.ibm.com then run:

      ```
      chnode clsaixn01.pok.ibm.com HWControlPoint=c01hmc.pok.ibm.com \
      ConsoleServerName=c01hmc.pok.ibm.com
      ```
2. If the HMC user ID or password has changed:
   a. Run the **systemid** command with the IP address or host name of the HMC and the HMC user ID. Enter the HMC password when prompted.
3. If the HMC user-defined LPAR name has changed:
   a. Run the **chnode** command for the node corresponding to the changed LPAR. Modify the *HWControlNodeId* attribute to match the new user-defined LPAR name. For example, if the user defined LPAR name changed to clsaixn01.pok.ibm.com then run:

      ```
      chnode clsaixn01.pok.ibm.com HWControlNodeId=clsaixn01
      ```
4. If the HMC user-defined CEC name has changed:
   a. If the CEC is in Partition Standby (LPAR) mode, no changes are necessary.
   b. If the CEC is in Full System Partition (SMP) mode, run the **chnode** command for the node corresponding to the changed CEC. Modify the *HWControlNodeId* attribute to match the new user-defined CEC name. For example, if the node was defined in the CSM database with the host name CEC01.pok.ibm.com and the user-defined CEC name changed to CEC05.pok.ibm.com, then run:

      ```
      chnode CEC01.pok.ibm.com HWControlNodeId=CEC05.pok.ibm.com
      ```

xSeries server configuration

To configure remote power, IBM suggests changing the default hardware control point user IDs and passwords using the utility disks and documentation provided with the hardware. For xSeries RSAs the default user ID is ″USERID″ and the default password is ″PASSW0RD″ (P-A-S-S-W-zero-R-D). CSM software uses these defaults if you do not change them. When you run the **rpower** command, the user ID and password information is automatically retrieved and decrypted.

Note: For the latest information on the minimum BIOS levels required for using xSeries servers with CSM, see the CSM FAQ on the Web at http://techsupport.services.ibm.com/server/cluster/tips/csm_faq.html.

RSA user IDs and passwords stored on the management server must match the nodes' user IDs and passwords in the hardware. The **systemid** command must be run once for each RSA to encrypt password information on the management server.

The following hardware control attribute values are required for each node:

HWControlPoint
The host name or IP address of the xSeries RSA.

HWControlNodeId
The text ID associated with the xSeries ISMP.

PowerMethod
This attribute value must be **xseries**.

xSeries configuration examples

The following examples show how to create system IDs for xSeries servers on the management server. The commands will prompt for a valid password. In the examples the node being defined has the following hardware control attributes:

```
Hostname = clsn05.pok.ibm.com
HWControlPoint = rsa01.pok.ibm.com
HWControlNodeId = clsn05
PowerMethod = xseries
```

Note: To change attributes for nodes that have already been defined, use the **chnode** command.

1. If you are not using the default user ID and passwords, then rerun the **systemid** command to define them. See “Creating and testing system IDs” on page 24 for detailed examples.
2. Run the **systemid** command to define the user ID and password required to access the RSA that controls the node:

   ```
   systemid rsa01.pok.ibm.com USERID
   ```

   Enter the password when prompted.
3. Define the node in the CSM database. Note that there are several options for the **definenode** command. This example shows the specification of all information required for hardware control of the node. See the **definenode** man page or the *IBM CSM for AIX 5L: Administration Guide* for detailed command usage information.

   ```
   definenode -n clsn05.pok.ibm.com -H rsa01.pok.ibm.com \
   HWControlNodeId=clsn05 PowerMethod=xseries
   ```
4. Verify that the node attributes are correct:

   ```
   lsnode -l clsn05.pok.ibm.com
   ```

   Verify that the attribute values returned for *Hostname*, *HWControlPoint*, *HWControlNodeId* and *PowerMethod* are correct. If any are incorrect, use the **chnode** command to correct them.
5. Test remote power control by entering:

   ```
   rpower -n clsn05.pok.ibm.com query
   ```

   Output from this command should be similar to:

   ```
   clsn05.pok.ibm.com on
   ```

   If there was a problem determining the query value then a message is returned indicating the problem. See “Remote power diagnostics” on page 26 for help determining the problem and resolution.

APC configuration

The APC MasterSwitch retrieves TCP settings from a BOOTP server on the local subnet by default, provided that the BOOTP server is configured with the unit’s MAC address. Otherwise, you must establish a serial connection and update the TCP settings using a terminal emulator by establishing a 2400 baud serial connection to the APC MasterSwitch serial port. For specific details see the configuration documentation that is shipped with the product or available from http://www.apcc.com/products/family/index.cfm?id=70.

APC configuration examples

The following examples show how to create system IDs for IntelliStation servers on an AIX management server in a mixed cluster. In the examples the node being defined has the following hardware control attributes:

```
Hostname = ISclsn24.pok.ibm.com
HWControlPoint = apc01.pok.ibm.com
HWControlNodeId = 3
PowerMethod = apc
```

1. If the APC MasterSwitch user ID and password are not set to the default, then run the **systemid** command to define the user ID and password required to access the MasterSwitch. This is the same value that is assigned to the *HWControlNodeId* attribute in the CSM database:

   ```
   systemid apc01.pok.ibm.com USERID
   ```

   Enter the password when prompted.

2. Define the node in the CSM database. Note that there are several options for the **definenode** command. This example shows the specification of all information required for hardware control of the node. See the **definenode** man page for detailed command usage information.

   ```
   definenode -n ISclsn24.pok.ibm.com -H apc01.pok.ibm.com \
   HWControlNodeId=3 PowerMethod=apc
   ```

3. Verify that the node attributes are correct:

   ```
   lsnode -l ISclsn24.pok.ibm.com
   ```

   Verify that the attribute values returned for *Hostname*, *HWControlPoint*, *HWControlNodeId*, and *PowerMethod* are correct. If they are incorrect, use the **chnode** command to correct them.

4. Test remote power control:

   ```
   rpower -n ISclsn24.pok.ibm.com query
   ```

   Output from this command should be similar to:

   ```
   ISclsn24.pok.ibm.com on
   ```

If there was a problem determining the query value then a message will be returned indicating the problem. See “Remote power diagnostics” on page 26 for detailed scenarios.

The following examples demonstrate using the **systemid** command and the **chnode** command to change node configuration information in the CSM database. If an APC MasterSwitch host name or IP address has changed, then you must run the **systemid** command, specifying the MasterSwitch host name, IP address, and user ID. For example:

1. If an APC MasterSwitch host name, IP address, user ID, or password has changed, you must run the **systemid** command as follows:

   ```
   systemid [hostname | ipaddress] USERID
   ```

2. If the APC MasterSwitch host name or IP address has changed, you must reset the MasterSwitch *HWControlPoint* attribute value in the CSM database using the **chnode** command. You must run the **chnode** command for each node attached to the APC MasterSwitch:

   ```
   chnode -n nodes_attached_to_MasterSwitch HWControlPoint=[MasterSwitch_hostname \
   | MasterSwitch_ipaddress]
   ```

3. Additional trace information is available for the APC power control library. If the hardware control resource manager **IBM.HWCTRLRM** is started as follows:

   ```
   startsrc -s IBM.HWCTRLRM -e HC_APC_VERBOSE=1
   ```

then a trace file called **apc.debug_trace** will be written to the **/var/log/csm** directory. This step should only be used if you are having problems with APC power control and are directed to do so by IBM Service. This file can become large over time, so tracing should not be enabled unless necessary. In a mixed cluster, both the APC and Java traces can be enabled by starting the hardware control resource manager as follows:

```
startsrc -s IBM.HWCTRLRM -e "HC_JAVA_VERBOSE=/directory/filename \
HC_APC_VERBOSE=1"
```

Note: When passing more the one argument with the **–e** option, quotation marks are required.

eServer 325 configuration

Configuration instructions are planned to be made available for setting up the NIC BMC IP addresses in your CSM cluster. See the CSM Documentation Errata http://publib.boulder.ibm.com/clresctr/docs/csm/docerrata.html and Frequently Asked Questions (FAQ) http://techsupport.services.ibm.com/server/cluster/tips/csm_faq.html Web pages for details.

eServer 325 configuration examples

The following examples show how to create system IDs for eServer 325 servers on the management server. The commands will prompt for a valid password. In the examples the node being defined has the following hardware control attributes:

```
Hostname = clsn23.pok.ibm.com
HWControlPoint = bmc01.pok.ibm.com
HWControlNodeId = clsn23
PowerMethod = bmc
```

Note: To change attributes for nodes that have already been defined, use the **chnode** command.

1. If you are not using the default user ID and passwords, then rerun the **systemid** command to define them. See “Creating and testing system IDs” on page 24 for detailed examples.
2. Run the **systemid** command to define the user ID and password required to access the BMC that controls the node:

   ```
   systemid bmc01.pok.ibm.com USERID
   ```

   Enter the password when prompted.
3. Define the node in the CSM database. Note that there are several options for the **definenode** command. This example shows the specification of all information required for hardware control of the node. See the **definenode** man page or the *IBM CSM for AIX 5L: Administration Guide* for detailed command usage information.

   ```
   definenode -n clsn23.pok.ibm.com -H bmc01.pok.ibm.com \
   HWControlNodeId=clsn23 PowerMethod=bmc
   ```
4. Verify that the node attributes are correct:

   ```
   lsnode -l clsn23.pok.ibm.com
   ```

   Verify that the attribute values returned for *Hostname*, *HWControlPoint*, *HWControlNodeId* and *PowerMethod* are correct. If any are incorrect, use the **chnode** command to correct them.
5. Test remote power control by entering:

   ```
   rpower -n clsn23.pok.ibm.com query
   ```

Output from this command should be similar to:

```
clsn23.pok.ibm.com on
```

If there was a problem determining the query value then a message is returned indicating the problem. See “Remote power diagnostics” on page 26 for help determining the problem and resolution.

System ID attributes

The following table shows the internal hardware attributes which must match the corresponding CSM hardware attribute values defined in the CSM database. If any of the internal hardware attribute values change, you must run the **systemid** command, and in some cases, the **chnode** command.

The servers listed in the following table are shipped with default user IDs and passwords. IBM suggests changing these default user IDs and passwords. See the links in “Prerequisite and related information” on page vi for documentation on your specific server types.

Table 4. System IDs

Hardware Model	User ID	Password	Host specification
HMC-attached pSeries	HMC User ID	HMC password	HMC IP address or host name
xSeries	RSA User ID	RSA password	RSA IP address or host name, or ISMP name
BladeCenter HS20	MM User ID	MM ID	MM IP address or host name
IntelliStation 6221	APC User ID	APC password	APC IP address or host name
eServer 325	BMC User ID	BMC password	BMC IP address or host name

Creating and testing system IDs

The following example shows how to create a system ID for an xSeries server. In the examples the node being defined has the following hardware control attributes:

```
Hostname = clsn02.pok.ibm.com
HWControlPoint = rsa01.pok.ibm.com
HWControlNodeId = clsn02
PowerMethod = xseries
```

1. If the user ID and password used to access the RSA are **not** set to the manufacturer’s default, then run the **systemid** command to define the user ID and password required to access the RSA. This is the same value that is assigned to the *HWControlNodeId* attribute in the CSM database:

   ```
   systemid rsa01.pok.ibm.com USERID
   ```

   Enter the password when prompted.
2. If the user ID and password used to access the xSeries ISMP are **not** set to the manufacturer’s default, then run the **systemid** command to define the user ID and password required to access the ISMP. The first argument passed to **systemid** is the string that identifies the node to the RSA. This is the same value that is assigned to the *HWControlNodeId* attribute in the CSM database:

   ```
   systemid clsn02 USERID
   ```

   Enter the password when prompted.
3. Verify that the node attributes are correct:

   ```
   lsnode -l clsn02.pok.ibm.com
   ```

Verify that the attributes values returned for *Hostname*, *HWControlPoint*, *HWControlNodeId*, and *PowerMethod* are correct. If they are incorrect, then use the **chnode** command to correct them.

4. Test remote power control:

   ```
   rpower -n clsn02.pok.ibm.com query
   ```

   Output from this command should be similar to:

   ```
   clsn02.pok.ibm.com on
   ```

   If there was a problem determining the query value then a message is returned indicating the problem. See “Remote power diagnostics” on page 26 for help determining the problem and resolution.

Changing system IDs

The following example demonstrates using the **systemid** command and the **chnode** command to change node configuration information for an xSeries server in the CSM database. If an RSA’s host name, IP address, or ISMP text ID has changed, then you must run the **systemid** command, specifying the RSA’s host name, IP address, and user ID. If the user ID or password for the RSA’s IP address or ISMP text ID has changed, then you must also run the **chnode** command to set the new RSA host name, IP address, or ISMP text ID in the CSM database. For example:

1. If an RSA’s host name, IP address, user ID, or password has changed, you must run the **systemid** command as follows:

   ```
   systemid  [hostname | ipaddress] USERID
   ```

   If the RSA host name or IP address has changed, you must reset the RSA’s *HWControlPoint* attribute value in the CSM database using the **chnode** command. You must run the **chnode** command for each node attached to the RSA:

   ```
   chnode -n nodes_attached_to_RSA HWControlPoint=[RSA_hostname | RSA_ipaddress]
   ```

2. If a node’s ISMP text ID has changed, you must reset the node’s *HWControlNodeId* attribute value in the CSM database using the **chnode** command:

   ```
   chnode node HWControlNodeId=ISMP_text_ID
   ```

Testing remote power hardware control

To ensure that your CSM cluster is configured correctly for remote power hardware control, all remote power functions should be tested before using them in a production environment. Run the **rpower** command with the **query**, **on**, **off**, **reboot**, **resetsp_host**, and **resetsp_hcp** options to verify that all nodes are configured correctly and responding. See the **rpower** man page or the *IBM CSM for Linux: Administration Guide* for examples.

Note: The **resetsp_host** option is not supported for the APC MasterSwitch. The **resetsp_host** and **resetsp_hcp** options are not supported on Linux on pSeries nodes.

Node power status is determined using one of two methods: polling or event notification. The *PowerStatus* attribute value reflects the status returned from RSAs, APCs and HMCs: **on**, **off**, or **unknown**. Polling is used to determine power status for x335, x345, x360, x440, x445, BladeCenter, eServer 325, and APC MasterSwitch hardware. You can set the polling interval using the RSCT **chrsrc** command, or use the default value of five minutes. The *PollingInterval* attribute value cannot be set to less than **30** (seconds). Set the *PollingInterval* to **0** to turn off polling. Power status methods can be configured – see the *IBM CSM for Linux: Planning and Installation Guide* for details.

Event notification is used to determine power status for x330, x342, and HMC-attached pSeries servers. The power status update frequency could differ between server types if the power status method is different.

The following examples provide some methods for testing remote power configuration:

1. To view current attribute values for nodes in a cluster, enter the following command on the management server:

   ```
   lsnode -l
   ```

   Output for each node in the cluster should be similar to:

   ```
   Hostname = clsn16.pok.ibm.com
   HWControlPoint = rsa01.pok.ibm.com
   HWControlNodeId = clsn16
   PowerMethod = xseries
   ```

2. To power on multiple cluster nodes simultaneously, enter:

   ```
   rpower -n clsn01,clsn07,clsn13,clsn16 on
   ```

Remote power diagnostics

The following sections describe problems, descriptions, and actions for specific instances of using remote power. To return messages from the remote power commands, use the **–v** option. For the latest information on CSM diagnostics, see the diagnostics chapter in the *IBM CSM for Linux: Administration Guide* and the CSM FAQ on the Web at http://techsupport.services.ibm.com/server/cluster/tips/csm_faq.html.

Remote power log and trace files

Attention!

Running remote power commands with the **–v** option, or starting the hardware control resource manager using the **startsrc –e** command, should only be done as a result of direction from your IBM service representative.

The following log and trace files are always generated when running a remote power command:

- **apc/apc[***APC_MasterSwitch_IPaddress***].trace**

The following log and trace files are generated when an error occurs running a remote power command:

- **hmc[***ip_address***].***julian_date*
- **xseries[***ip_address***].***julian_date*
- **hw_logfile[***port_number***].***julian_date*

The following log and trace files are generated when specifying the **–v** option with a remote power command, or when starting the hardware control resource manager with a command similar to the following example:

```
startsrc -s IBM.HWCTRLRM -e HC_JAVA_VERBOSE=/directory/filename
```

To enable tracing and logging of multiple remote power libraries, you must specify the libraries within quotation marks. For example:

```
startsrc -s IBM.HWCTRLRM -e "HC_JAVA_VERBOSE=/directory/filename HC_APC_VERBOSE=1"
```

The following log and trace files are generated:

- **hmc[***ip_address***].java_trace**
- **xseries[***ip_address***].java_trace**
- **bmc[***ip_address***].java_trace**
- **apc.debug_trace**
- **hmc_logfile.***julian_date*
- **xseries_logfile.***julian_date*
- **bmc_logfile.***julian_date*

Remote access to hardware control points

Remote access to hardware control points through a telnet or Web session provides an alternative interface for tasks such as debugging. User IDs and passwords are required, and appropriate security measures should be implemented to restrict remote power control to users on the management VLAN, as described in “Hardware and network requirements” on page 3. Once you are logged into a hardware control point, you can control the node remotely.

RSA and management module

The RSA (xSeries) and management module (BladeCenter) hardware control points can be controlled through a Web browser by doing the following:

1. Log in to the management server.
2. Run **export DISPLAY=***localhost***.com:0**
3. Run the **lsnode** command to return the hardware control point attribute name – the RSA (xSeries) or management module (BladeCenter) IP address or host name.
4. Start your Web browser and direct it to the RSA or management module’s IP address or host name.
5. In the login window, type your user ID and password. The hardware control point will be accessible through your Web browser.

The RSA (xSeries) and management module (BladeCenter) hardware control points can be controlled through a telnet session by doing the following:

1. Log in to the management server.
2. Run the **lsnode** command to return the hardware control point attribute name – RSA (xSeries) or management module (BladeCenter) IP address or host name.
3. Run **telnet** *hostname or IP address*
4. Enter your user ID and password.
5. Use the **Tab** key to move the cursor.

APC MasterSwitch

The APC MasterSwitch provides command line and Web-based interfaces for configuration. In either case you need the default user name and password for the MasterSwitch, which can be found in the product documentation. To access the MasterSwitch using the command line:

1. Open a telnet session to the power strip's IP address or host name.
2. Enter the power strip's user name and password when prompted.

To access the MasterSwitch using a Web interface:

1. Point your Web browser to the power strip's IP address or host name.
2. Enter the power strip's user name and password when prompted.

tcp port numbers

The **IBM.HWCTRLRM** Hardware Control resouce manager starts one daemon for each unique hardware control type. The corresponding hardware control library communicates with this daemon though a TCP socket whose port number is written to /**etc**/**services** during the installation process. The service-name entry in /**etc**/**services** for this port is **ibm_hcdx** for xSeries and BladeCenter servers, **ibm_bmc** for the eServer 325, and **ibm_hcdh** for HMC-attached pSeries servers. IntelliStation (APC) workstations have no daemon or port number in /**etc**/**services**.

Set up and configuration problems

Table 5. rpower set up and configuration problems

Problem:	Cannot log in to the hardware control point.
Description:	Connection to the hardware control point cannot be established. Attempts to log in to the targeted hardware control point were unsuccessful or returned an error.
Action:	Run the **systemid** command to verify that the user ID and password are correct.
Problem:	Java interface error for method *action*: communication session is not valid.
Description:	The hardware control library successfully logged in to the service processor specified by the node *HWControlPoint* attribute, but could not log in to the node's service processor.
Action:	Confirm the user ID and password for the hardware control node ID for the node and rerun the **systemid** command with the correct user ID and password.
Problem:	Java interface error for method *action*: node not found.
Description:	The hardware control point specified by the node *HWControlPoint* attribute is not configured to control this node.
Action:	Check the CSM configuration to ensure that the specified node *HWControlPoint* and *HWControlNodeId* attributes are correct for the node. If correct, ensure that the hardware control point service processor is configured correctly to control the node.
Problem:	Java interface error for method *connect*: service processor host name is not valid.
Description:	The service processor specified by the node's *HWControlPoint* attribute is not valid for the node's *PowerMethod* attribute specified.
Action:	Verify that the node *HWControlPoint* and *PowerMethod* attributes are valid for the node using the **lsnode –F** *Hostname* command. If they are not correct, change them using the **chnode** *Hostname* **HWControlPoint=***HWControlPoint* **PowerMethod=***PowerMethod* command.

Table 5. rpower set up and configuration problems (continued)

Problem:	Java interface error for method *connect*: SPException.
Description:	The hardware control library was unable to log in to the service processor specified by the node *HWControlPoint* attribute.
Action:	Confirm the user ID and password for the hardware control point and run the **systemid** command again with the correct user ID and password.
Problem:	Could not perform action because one or more *HWControlPoint*, *HWControlNodeId*, and *PowerMethod* attributes are not set.
Description:	For the command to work properly the *HWControlPoint*, *HWControlNodeId* and *PowerMethod* attributes must be defined.
Action:	Verify that the *HWControlPoint*, *HWControlNodeId*, and *PowerMethod* attributes are defined using the **lsnode –F** *Hostname* command. If these attributes are not set, then set them to their correct values using the **chnode** command and rerun the **rpower** command.
Problem:	Could not load hardware control library.
Description:	CSM hardware control requires setting *PowerMethod* attribute values to **xseries** for xSeries and BladeCenter, **hmc** for HMC-attached pSeries, **apc** for IntelliStation, and **bmc** for the eServer 325. The hardware control library corresponding to the attributes must also reside in **/opt/csm/lib**. For example, the *PowerMethod* hardware control library must be **/opt/csm/lib/lib***PowerMethod***_power.so**.
Action:	Verify that the *PowerMethod* attribute is set correctly using the **lsnode –F** *Hostname* command. If it is not correct then set the value using the **chnode** *Hostname* **PowerMethod=***PowerMethod* command. If the power method is set correctly, then verify that the **/opt/csm/lib/lib***PowerMethod***_power.so** library exists. If it does not, then reinstall the **csm.server** package.
Problem:	The hardware control point address specified is not valid.
Description:	The hardware control library could not resolve the host name or IP address of the service processor specified by the *HWControlPoint* attribute.
Action:	Verify that the *HWControlPoint* attribute is valid for the node and that the management server can reach the node.
Problem:	The *Hostname* attribute value specified for the node is not valid.
Description:	The specified host name is not a defined node resource.
Action:	Verify that the node specified by the *Hostname* attribute value for the **rpower** command is a node resource using the **lsnode** *Hostname* command. If it is not valid then choose a valid node returned by the **lsnode** command or add the host name as a node resource.

Connection problems

Table 6. rpower connection problems

Problem:	Connectivity to the hardware control point cannot be established.
Description:	Attempts to use traceroute or ping to the target hardware control point are unsuccessful. Connectivity from the management server to the target hardware control point cannot be established.
Action:	Contact your network administrator and check the hardware connectivity documentation to diagnose and solve the network connectivity problem.
Problem:	Cannot log in to the hardware control point.
Description:	Connection to the hardware control point cannot be established. Attempts to log in to the targeted hardware control point were unsuccessful or returned an error.
Action:	Run the **systemid** command to verify that the user ID and password are correct.
Problem:	Java interface error for method *connect*: SPException.
Description:	The hardware control library was unable to log in to the service processor specified by the node *HWControlPoint* attribute.
Action:	Confirm the user ID and password for the hardware control point and run the **systemid** command again with the correct user ID and password.
Problem:	The hardware control point address specified is not valid.
Description:	The hardware control library could not resolve the host name or IP address of the service processor specified by the *HWControlPoint* attribute.
Action:	Verify that the *HWControlPoint* attribute is valid for the node and that the management server can reach the node.
Problem:	Cannot run the command because the IBM.HWCTRLRM resource manager is not available.
Description:	The **rpower** command could not make a connection to the IBM.HWCTRLRM daemon. This daemon contains the IBM.NodeHWCtrl and IBM.HwCtrlPoint resource classes. The **rpower** command runs actions on these resource classes which in turn calls the appropriate hardware control library.
Action:	Ensure that the IBM.HWCTRLRM daemon is running on the management server using the **lssrc –s IBM.HWCTRLRM** command. If the output status field is ″inoperative″ then start the daemon using the **startsrc –s IBM.HWCTRLRM** command.
Problem:	Could not find hardware control point for the node.
Description:	There is no corresponding hardware control point resource for the *HWControlPoint* attribute.
Action:	Stop the IBM.HWCTRLRM daemon using the **stopsrc –s IBM.HWCTRLRM** command. Remove the hardware control point resources from the registry table using the **/usr/sbin/rsct/bin/rmsrtbl/IBM/HwCtrlPoint/Resources** command. Restart the IBM.HWCTRLRM daemon using the **startsrc –s IBM.HWCTRLRM** command. Rerun the command. If this problem persists, contact your IBM service representative.

Table 6. rpower connection problems (continued)

Problem:	The session timed out waiting for access to the RSA.
Description:	The command could not gain access to the RSA. Another command has access to the RSA and has not released the lock.
Action:	Rerun the command. If the problem persists, reset the RSA.
Problem:	The command cannot determine the hardware control daemon port number.
Description:	The hardware control library could not find an entry in **/etc/services** for the hardware control daemon or an available port between 9095 and 9134.
Action:	Make a port available between 9095 and 9134 (including 9095 and 9134) for use by the hardware control daemon. Restart the **IBM.HWCTRLRM** daemon using the **startsrc -s IBM.HWCTRLRM** command.
Problem:	The **rpower** command is slow to power off xSeries servers with an RSA installed at the default settings.
Description:	The RSA has a default timeout that waits for 30 seconds before powering off the node.
Action:	Point your Web browser to the host name or IP address of the RSA. Click on **System Settings**. Under **Server Timeouts**, set the **Power off delay** to **0** to immediately power off the node.
Problem:	A power status query to pSeries nodes returns ″unknown.″
Description:	For pSeries nodes, the HMC sends the management server asynchronous events indicating node power status. To accomplish this, the HMC must be able to resolve the management server **hostname**.
Action:	Ping the management server from the HMC using the management server host name you would use when running the **hostname** command on the management server.

APC MasterSwitch set up and configuration problems

Table 7. APC MasterSwitch set up and configuration problems

Problem:	The *Hostname* attribute value specified for the hardware control point is not valid.
Description:	The specified hardware control point host name could not be resolved.
Action:	Verify that the specified *Hostname* attribute value is correct and rerun the command.
Problem:	The hardware control node ID is out of range for the hardware control point.
Description:	The *HWControlNodeId* attribute value for this node is not valid for the specified hardware control point.
Action:	Verify that the node's *HWControlNodeId* attribute value in the CSM database is between 1 and 8, and rerun the command.

Table 7. APC MasterSwitch set up and configuration problems (continued)

Problem:	Could not access the trace directory.
Description:	The specified trace directory could not be accessed.
Action:	Verify that the directory exists, create the directory if necessary, and rerun the command.
Problem:	Could not write log messages.
Description:	The program cannot write messages to its log file.
Action:	Verify that there is space available in **/var**, or check the error log for disk errors.
Problem:	Incorrect login for the hardware control point.
Description:	The user ID or password is not correct for the hardware control point.
Action:	Rerun the **systemid** command with the correct user ID and password for the hardware control point, and then rerun the command.
Problem:	Unable to open the password file for the hardware control point.
Description:	The password file for this hardware control point cannot be opened.
Action:	Run the **systemid** command to generate a key file and a password file for this hardware control point.
Problem:	Cannot load the shared library.
Description:	The shared library specified cannot be loaded.
Action:	Verify that the library is available and rerun the command.

APC MasterSwitch connection problems

Table 8. APC MasterSwitch connection problems

Problem:	Internal error – unable to spawn a connection process to the hardware control point.
Description:	An internal program problem has occurred.
Action:	Verify that the telnet program exists on the management server. If it does, save the error message and contact IBM support.
Problem:	The session timed out waiting for a response from the hardware control point.
Description:	The expected response from the hardware control point was not received within the allowed time.
Action:	Check the network connection to the hardware control point and rerun the command.
Problem:	The connection to the hardware control point terminated unexpectedly.
Description:	The network connection to the hardware control point terminated unexpectedly.
Action:	Check the network connection to the hardware control point and rerun the command.

APC MasterSwitch operation problems

Table 9. APC MasterSwitch operation problems

Problem:	The hardware control action is not supported by the hardware control point.
Description:	The specified hardware control point does not support the specified hardware control action.
Action:	Rerun the command with a supported hardware control action.
Problem:	The command is not supported for a node of this hardware type.
Description:	The hardware control point received a hardware control action that it does not support. Not all hardware control points support the same hardware control actions.
Action:	Rerun the command with one of the supported hardware control actions: **on**, **off**, **reboot**, **query**, or **resetsp_hcp**.

Chapter 3. Remote console software and configuration

Once your cluster hardware and networking have been configured, you must install and configure CSM software to enable remote console functions. The **installms** command installs the required **csm.server** package, including the remote console commands, on the management server. For detailed CSM installation instructions, see the *IBM CSM for Linux: Planning and Installation Guide*. For detailed command usage information, see the **installms**, **rconsole**, and **definenode** command man pages or the commands chapter in the *IBM CSM for Linux: Administration Guide*.

Notes:

1. Remote console function is not supported on the x440.
2. Using the **rconsole** command with BladeCenter hardware requires that you order and install additional serial port module parts. As an alternative, you can point your Web browser to the IP address or host name of the BladeCenter management module. See "Launching a remote console" on page 56 for detailed information on ordering parts and using remote console for BladeCenter hardware.

Remote console attributes

CSM remote console uses the following attributes for each node defined in the CSM database. These attributes can be set initially when new nodes are defined in the cluster using the **definenode** command, or changed for existing nodes using the **chnode** or **definenode –m** command. See Table 10 on page 36 for the console server types that can be used with CSM and the associated attribute values that are valid for each type.

ConsoleMethod

The ConsoleMethod attribute specifies the type of console servers used in the cluster. When new nodes are defined in the cluster using the **definenode** command, a *ConsoleMethod* attribute can be set for each new node in the CSM database.

ConsoleServerName

The *ConsoleServerName* attribute value specifies the short host name, long host name, or IP address of the console server used for the node.

ConsoleServerNumber

The *ConsoleServerNumber* attribute (applicable to Equinox ESPs only) is the number assigned by the Equinox configuration tool (**espcfg** command) when the ESP console server is installed. The attribute value must be the number assigned to the Equinox ESP providing remote console for the target node. The **espcfg** command also displays the current number value.

Note: (CSM supports the ESP console server on Red Hat 7.2, 7.3, and 8.0 management servers only.)

ConsolePortNum

The *ConsolePortNum* attribute is the physical port that the node's serial port is connected to in the console server hardware. For the HMC, the *ConsolePortNum* attribute is not used; the *HWControlNodeId* attribute is used to identify the LPAR's console connection.

ConsoleSerialDevice

The console serial port device *ConsoleSerialDevice* attribute specifies the device definition of the serial port on the node that is connected to the console server. By default, CSM uses the first serial port on the node hardware: COM-A (**ttyS0**). If the node hardware has two serial ports and you connect the console server to the second serial port: COM-B (**ttyS1**), you must change the *ConsoleSerialDevice* attribute value to **ttyS1**. If the hardware has no serial port defined, or if you do not want console output redirect to the serial port, the *ConsoleSerialDevice* attribute value must be set to **NONE**, which disables the **rconsole** command for that node. If the *ConsoleSerialDevice* attribute is set to a null value, the device name **ttyS1** is used to maintain compatibility with previous CSM releases.

Remote console attribute values

The following table describes the console server models that can be used with CSM node hardware models and their required remote console attribute values. For more information about these console servers, see the product Web site URLs listed in "Prerequisite and related information" on page vi.

Table 10. Remote console attribute values

Node hardware type	**Console server type**	*ConsoleMethod*	*ConsoleServerNumber*	*ConsolePortNum*
HMC-attached pSeries	HMC	**hmc**	not applicable	not applicable
xSeries, BladeCenter, IntelliStation, eServer 325	MRV IR-8020; IR8040	**mrv**	not applicable	1-20; 1-40
xSeries, IntelliStation	MRV LX-4008S; LX-4016S; LX-4032S	**mrv**	not applicable	1-8, 1-16, 1-32
xSeries, IntelliStation	Equinox ELS-16 II	**els**	not applicable	1-16
xSeries, IntelliStation	Equinox ESP-8; ESP-16	**esp**	1 or more (value is returned by the **espcfg** command)	0-7; 0-f
xSeries, IntelliStation	Computone IntelliServer RCM4; RCM8; RCM24	**computone**	not applicable	1-4; 1-8; 1-24
xSeries, IntelliStation	Avocent CPS1600	**cps**	not applicable	1-16

When the **csm.client** package is installed on Linux nodes on xSeries, pSeries, BladeCenter, or IntelliStation hardware, CSM automatically adds entries to the **/etc/lilo.conf** file to define the console serial device. If your *ConsoleSerialDevice* attribute value is not set to **NONE**, then CSM will automatically add entries to the **/etc/inittab** and **/etc/lilo.conf** files to start the **agetty** terminal process for the console, substituting the *ConsoleSerialDevice* attribute value. If you are using a **grub.conf** file, see "Console redirection on Linux using grub" on page 42 for details on how to redirect grub output to a remote console. See the *IBM CSM for Linux: Planning and Installation Guide* for software installation details.

Remote console fonts

By default, the **rconsole** command opens each new console session in an xterm window. The font used for the xterm window is determined by the total number of consoles the command is asked to open. The command's choice of font can be overridden by specifying the name of a valid X-Windows font in the **RCONSOLE_FONT** environment variable. If this variable is defined, the **rconsole** command will use this font in all the xterm windows it opens. This can be especially useful if five or more consoles are opened by one **rconsole** command. In this case the nil2 font is used by default. The nil2 font is not intended to be readable; it only provides a general idea of the node status. If you intend to read the information displayed on these consoles, define a font name in the **RCONSOLE_FONT** environment variable. The fonts available vary among X-Servers. Consult your X-Server documentation for details.

Remote console tiling

By default, the **rconsole** command does not position the xterm windows it opens; it relies on the window manager to position the windows on the screen. To tile multiple windows so they are displayed adjacent to one another, use the **rconsole –o** command. When the screen cannot accomodate more tiled windows, subsequent windows are positioned on top of existing ones.

Note: Tiling is not available for Linux nodes on pSeries servers.

Conserver multiple read-only consoles

The **rconsole** command uses the Conserver open source package to provide support for multiple read-only consoles on a single node. For example, if a user has a read-write console session open on node clsn01, other users could also log in to that console session on clsn01 as read-only users. This allows sharing a console server session between multiple users for diagnostic or other collaborative purposes.

Conserver software is packaged with CSM. Once CSM is installed, the Conserver software will reside on the management server. The Conserver configuration file is located in **/etc/opt/conserver/conserver.cf**. In previous CSM releases, the **rconsole** command would invoke specific console methods to access the target console. This restricted users to a single read-write session for each node. In CSM 1.3 the **rconsole** command invokes the Conserver software by default, which allows for multiple read-only console sessions. To limit **rconsole** to a single read-write console session, use the **rconsole –c** command.

By default, CSM is configured to automatically update the Conserver configuration file and refresh the Conserver daemon whenever nodes are added or removed from a cluster. This allows the software to recognize node additions and removals in the cluster so the **rconsole** command will function as expected. The updating is done by the predefined **NodeChanged** condition and **rconsoleUpdateResponse** response pair. If this predefined condition-response pair is removed, then the **chrconsolecfg** and **rconsolerefresh** commands must be run manually after running **definenode** to refresh the Conserver daemon.

Note: Defining or removing large numbers of nodes simultaneously could degrade system performance. To avoid this consequence you can temporarily disable the **rconsoleUpdateResponse** response by running the following command on the management server:

```
stopcondresp NodeChanged rconsoleUpdateResponse
```

When the node definition or removal is complete, run the following commands on the management server to reactivate the **rconsoleUpdateResponse** response and update the Conserver configuration:

```
startcondresp NodeChanged rconsoleUpdateResponse
chrconsolecfg -a
rconsolerefresh
```

The **rconsole –r** command opens a read-only session for the target node. If a read-write console has been left unattended on a node, an authorized read-only user can force their session to become the single read-write session using **rconsole –f**. The unattended read-write session will be changed to read only. If you run the **rconsole** command on the node a second time, the session will be read-only. The **–r** and **–f** options are not available when **rconsole** is run with the **–c** option, because **rconsole –c** bypasses the Conserver daemon. Conserver is required for read-only or force write functionality.

Remote console configuration

The following remote console configuration details are provided to assist you in setting up remote console function for your specific console servers. These steps are for xSeries, BladeCenter, InstelliStation, and eServer 325 servers only. For HMC-attached pSeries servers, the HMC provides remote console function.

Attention!

The console server hardware configuration tips in this section are provided as a convenience only. These tips are not a replacement for reading and using the installation and configuration documentation provided with the specified remote console hardware.

The specific hardware used to connect to the console servers can be different from the types described here. You must read your hardware documentation before attempting to configure your console servers.

MRV IR-8000 series configuration

1. Insert the included PCMCIA flash card into the slot in the front of the unit.
2. Power the unit on and attach a serial terminal to the command port. The default command port is port 20 or port 40, depending on the total ports in the unit.
3. Press Enter until you get a login prompt.
4. At the login prompt, enter **access** and press Enter. This will prompt for a user name.
5. Enter any user name at the prompt; in this mode it does not verify user names. Press Enter to display the In-Reach prompt.
6. At the In-Reach prompt, enter **set priv** and press Enter to prompt for the privileged mode password.
7. At the password prompt, enter **system** and press Enter to display the **In-Reach_Priv** prompt.
8. Enter **show ip** to see the current network settings.
9. Enter **define ip address ##.##.##.##** to set the IP address.
10. Enter **define ip primary gateway address ##.##.##.#** to set the gateway address
11. Enter **define ip subnet mask ### ###.### #** to set the subnet mask.
12. Log off.
13. You must modify the command port (port 20 or port 40, depending on the total ports in the unit) before using it for remote access. After completing the

configuration steps above, telnet into the unit using the IP address given in step 9 and a port number of 2000. Then follow steps 3 through 8 above to get to the **In-Reach_Priv** prompt.

14. Enter the command **define port ## access remote**, where ## is either 20 or 40, depending on the number of ports in the unit.
15. Enter the command **log port ##**, where ## is either 20 or 40, depending on the number of ports in the unit.
16. Enter **exit** to log off.

MRV LX-4000 series configuration

1. Power the unit on and attach a serial cable to the command port. The default command port is the highest numbered port on the unit.
2. Press the **Enter** key until you get a **login** prompt.
3. At the **login** prompt, enter **InReach**, and press the **Enter** key. This login name is case-sensitive.
4. At the **password** prompt, enter **access** and press the **Enter** key. This password is case-sensitive.
5. From the command prompt, enter **enable** and press the **Enter** key. This enters super user mode and prompts for a password.
6. At the super user **password** prompt, enter **system** and press the **Enter** key. If this is the initial configuration, a menu will be displayed allowing configuration of the network parameters. If this is not the initial configuration, enter **setup** and press the **Enter** key to start the configuration menu.
7. After the network parameters are set and saved, enter **config** and press the **Enter** key. This enters configuration mode.
8. At the **configuration** prompt, enter **port async 1 ##**, where ## is the highest numbered port on the unit, and press the **Enter** key. This enters **async** configuration mode.
9. From the **async configuration** prompt, enter **no outbound authentication** and press the **Enter** key. This disables the console server's internal authentication.
10. Log off.
11. You must modify the command port (the highest numbered port in the unit) before using it for remote access. After completing the configuration steps above, telnet into the unit using the IP address given in step 6. Follow steps 2 through 7 above to get to the **configuration** prompt.
12. At the **configuration** prompt enter **port async ##**, where ## is the highest numbered port on the unit, and press the **Enter** key. This enters **async** configuration mode.
13. From the **async configuration** prompt, enter **no autobaud** and press the **Enter** key.
14. From the **async configuration** prompt, enter **access remote** and press the **Enter** key.
15. Log off.

ELS configuration

1. Connect a serial terminal or terminal emulator to port 1 of the ELS console device. Set the terminal to 9600 bps; 8-bit data; No Parity; 1 stop bit. Press the return key to get an ELS login prompt.

2. Login as root. IBM suggests changing the default user IDs and passwords shipped with external devices since failure to do so could compromise cluster security.
3. At the ″Local″ prompt enter privileged mode by typing ″set priv″. When prompted for a password, enter ″system″.
4. Reset the current ELS configuration by entering ″init database″.
5. Enter the following required information:

   ```
   change server ip IP address of ELS
   change server subnet mask mask
   change node gw ip default gateway IP address gateway en
   ```

   For example:

   ```
   change server ip ###.##.##.##
   change server subnet mask ###.###.###.0
   change node gw ip ###.##.##.# gateway en
   ```

6. Disconnect the serial terminal and connect the ELS to the network. Telnet to the ELS and press return to get a ″#″ prompt. Type ″access″ to get a ″Local″ prompt, then enter the ″set priv″ command and password as described in step 3.
7. The ELS ports must be set to Reverse Telnet mode to work properly with CSM remote console. Set the ELS ports to Reverse Telnet by entering the following:

   ```
   define port 1-16 access remote
   define port 1-16 flow control xon
   define port 1-16 speed 9600 lo port 1-16
   ```

8. Enter ″exit″ to quit.

ESP configuration

The ESP console device requires the installation of software and drivers that are shipped with the device. Once these are installed the device can be configured using the **espcfg** command. Refer to the ESP device installation instructions for details at http://www.equinox.com/Hardware_Manuals192.html. The ESP can be used for Linux node remote console support on xSeries and IntelliStation hardware. The ESP is not supported on BladeCenter hardware.

Note: CSM supports the ESP console server on Red Hat 7.2, 7.3, and 8.0 management servers only.

To successfully build the ESP RPM packages for the ESP console server, you must have the following RPM packages installed from your Linux distribution CD:

- gcc
- glibc-devel
- kernel-headers (exact RPM is dependent on the installed kernel)
- libgcc
- cpp
- kernel-source (exact RPM is dependent on the installed kernel)
- ncurses-devel
- rpm-build

To run the **rconsole** command with the ESP, the following packages must be installed from your Linux distribution CD:

- uucp

- lockdev
- lockdev-devel

In addition, the sources and headers kernel versions must match the kernel version you are running. For example, if the current running kernel returned by the **uname –r** command is 2.4.7-10, then the kernel sources RPM package **kernel-source-2.4.7-10.i386.rpm** must be installed.

Computone configuration

The Computone console device requires a BIOS level of 1.6.002 or higher to work with CSM remote console.

1. Connect a serial terminal or terminal emulator to the console port of the Computone console device. Set the terminal to 9600 bps; 8-bit data; No Parity; 1 stop bit. Press return until prompted for a user name.
2. Enter ″root″ as the user name and ″root″ as the password. IBM suggests changing the default user IDs and passwords shipped with external devices since failure to do so could compromise cluster security.
3. At the prompt, enter ″config″ to enter the configuration utility. The prompt should change to ″config #″.
4. Enter the console device's IP address and subnet mask as follows:

   ```
   set ether address Computone IP Address/# of bits in mask
   ```

   The device's IP address and subnet mask are entered in a single string. The subnet mask is entered as the number of bits that are set in the mask, and is appended to the IP address by a forward slash (/). Each of the four parts of the subnet mask is composed of eight bits, for a possible maximum of 32 bits set. For example, if the subnet mask is 255.255.255.0, the number of bits set is 8 + 8 + 8 + 0 = 24 bits. If the subnet mask is 255.255.255.192, the number of bits set is 8 + 8 + 8 + 2 = 26 bits. If the device IP address is 123.45.67.89, and the subnet mask is 255.255.255.192, then you would enter the following command:

   ```
   set ether address 123.45.67.89/26
   ```

5. Enter the default gateway information as follows:

   ```
   set gateway 0 destination 0.0.0.0 gateway Default Gateway IP address/# of
   bits in mask
   ```

   The gateway address requires the subnet mask also, and is entered as it was for the device IP address in step 4. If the gateway address is 123.45.67.1, and the subnet mask is 255.255.25.192, enter the command:

   ```
   set gateway 0 destination 0.0.0.0 gateway 123.45.67.1/26
   ```

6. Configure the serial ports for Reverse Telnet as follows:

   ```
   set port 1 type "reverse tcp"
   ```

   Repeat this step for the remaining ports. Note that Computone refers to Reverse Telnet as ″Reverse TCP.″
7. Enable the telnet interface as follows:

   ```
   set apps telnetd enabled
   ```

8. Enter ″exit″ to return to the system prompt. Enter ″save″ to save the settings. Enter ″exit″ once more to terminate the session.
9. Disconnect the terminal and attach the Computone device to the network.

CPS configuration

The CPS 1610 console device requires a BIOS level of 1.5 or higher to work properly with CSM remote console.

1. Connect a serial terminal or terminal emulator to port 1 of the CPS console device. Set the terminal to 9600 bps; 8-bit data; No Parity; 1 stop bit. Press return until prompted for a user name.
2. Enter ″Admin″ as the user name and press return. Press return again at the password prompt; there is no initial password for the Admin user. IBM suggests changing the default user IDs and passwords shipped with external devices since failure to do so could compromise cluster security.
3. For initial configuration, the CPS will prompt for an IP address, subnet mask, and Admin password. Enter this information, pressing return after each item.
4. After all the required information is entered, the configuration will be saved. Complete the network configuration by entering the following command:

   ```
   SERVER SET IP=CPS IP Address MASK=subnet mask GATEWAY=Default gateway
   IP address
   ```
5. For CSM remote console to work properly with the CPS console device, user authentication must be disabled for the device by entering the following:

   ```
   SERVER SECURITY AUTHENTICATION=NONE
   ```
6. Quit by entering ″quit″. Disconnect the terminal and connect the CPS to the network.

A CPS device does not require explicit configuration to set the ports to Reverse Telnet mode. However, by default the CPS serial Command Line Interface (CLI) is enabled on CPS port 1. Any CPS ports that have the CLI enabled cannot be used for Reverse Telnet, and therefore will not work with CSM remote console. If the default CLI setting is not changed, CPS port 1 will not be available for remote console access. Once the telnet interface has been defined and tested, the serial CLI interface can be disabled. To disable the CLI on port 1 and allow the port to be used for remote access, perform the following steps:

1. Telnet to the CPS device using the IP address set in step 4 above.
2. Log in to the device as outlined in step 2 above.
3. From the command line, enter:

   ```
   port 1 set cli=off
   ```
4. Press the **Enter** key, and allow the console device to be rebooted when prompted.

Remote console redirection

Remote console redirection allows you to remotely control some Linux servers using keyboard and video redirected through system serial ports. The intended use of this function is to allow you to remotely view POST execution, change system configuration settings in the POST set up utility, and to support DOS-based configuration utilities. Remote console redirection does not support graphical output.

Console redirection on Linux using grub

By default, grub output does not appear on the remote console; it only appears on the local terminal. However, you can configure your **grub.conf** file to redirect all grub output to the remote console. Redirection will display the grub output on the remote console, but not on the local terminal. To redirect grub output, make the following changes to your **/etc/grub.conf** file:

1. Add the following lines:

   ```
   serial --unit=0 ---speed=9600 (--unit=0 corresponds to the serial port number)
   terminal --timeout=0 serial
   ```

2. Remove or comment out the following line:

   ```
   splashimage=(hd0,0)/grub/splash.xpm.gz
   ```

On **Red Hat Linux nodes**, the following changes send Linux boot console output to the local console and an **rconsole** window:

- Set **SAFE=YES** in **/etc/sysconfig/kudzu**
- Add the bold text below to the **/boot/grub.conf** file.

```
#boot=/dev/sda
default=0
timeout=10
splashimage=(hd0,0)/grub/splash.xpm.gz
```

Add the following lines to **/etc/grub.conf**:

```
serial --unit=0 --speed=9600 --word=8 --parity=no --stop=1
terminal --timeout=5 console serial
```

Append the following to any ″kernel″ lines in **/etc/grub.conf**. The **ttyS0** value should match your *ConsoleSerialDevice* attribute value:

```
console=ttyS0,9600n8 console=tty0
```

xSeries console redirection

The **rconsole** command can provide access to the POST/BIOS panels on certain xSeries servers. The latest information on the supported xSeries servers and their minimum BIOS levels required is available at the CSM FAQ Web site at http://techsupport.services.ibm.com/server/cluster/tips/csm_faq.html.

To enable remote console redirection for xSeries servers, the BIOS settings must be changed. Use the BIOS Configuration/Setup Utility to enable and configure remote console redirection. Select **Remote Console Redirection** located under **Devices and I/O Ports**. Configure remote console redirection by selecting the following menu options:

1. Remote Console Active – Select ″Enabled″
2. Remote Console COM Port – Select the COM port that is connected to the terminal server
3. Remote Console Baud Rate – Select ″9600″
4. Remote Console Data Bits – Select ″8″
5. Remote Console Parity – Select ″None″
6. Remote Console Stop Bits – Select ″1″
7. Remote Console Emulation – Select ″VT100″
8. Remote Console Active After Boot – Select ″Enabled″

During the initial IBM logo screen, the remote console will begin to be updated in real time with the host server video. You will be given the ability to control the system remotely using the keyboard during operation. You can also fully control the server in BIOS setup, PXE setup, SCSI setup, and any standard DOS application.

Notes:

1. Once remote console redirection has been enabled in BIOS setup, the remote control feature of the Remote Supervisor Adapter (RSA), Integrated System Management Processor (ISMP), or both, will not be functional.

2. On some x330 systems COM1 can be shared with the ISMP. With remote console redirection enabled, this COM port will be dedicated for redirection support and cannot be used to control the ISMP.

BladeCenter console redirection

Remote console redirection is not supported for BladeCenter blade servers. For remote console on blade servers, you can use a Web browser to connect to the BladeCenter management module. See “BladeCenter” on page 52 for configuration details.

IntelliStation console redirection

Hardware is controlled for the IntelliStation 6221 through the APC MasterSwitch. For remote console support, you must redirect console in the BIOS using a direct attached terminal. The **rconsole** command will not display the BIOS output during node boot processing.

Testing remote console hardware control

To ensure that your cluster is configured correctly for remote console hardware control, all remote console functions should be tested before using them in a production environment. Run the **rconsole** command to verify that all nodes are configured correctly and are responding accordingly. See the **rconsole** man page or the *IBM CSM for Linux: Administration Guide* for detailed examples.

1. Before running the **rconsole** command, check that the following attributes are set correctly. For example, enter

   ```
   lsnode -l
   ```

   Output for each node in the cluster should include information similar to:

   ```
   Hostname = clsn02.pok.ibm.com
   ConsoleServerName = mrv01.pok.ibm.com
   ConsoleSerialDevice = ttyS0
   ConsolePortNum = 2
   ConsoleMethod = mrv
   ```

2. To open console windows for multiple nodes using short host names, long host names, or IP addresses, enter:

   ```
   rconsole -n clsn03,clsn09,clsn15,clsn19
   ```

3. To open a console session to each of the nodes defined in the CSM cluster, enter:

   ```
   rconsole -a
   ```

4. To open windows for each node defined in the specified node groups, enter:

   ```
   rconsole -N nodegrp1,nodegrp2
   ```

5. To start a console session to the specified node in the current window, enter:

   ```
   rconsole -t -n clsn03
   ```

Remote console diagnostics

The following sections describe problems, descriptions, and actions for specific instances of using remote console. For the latest information on CSM diagnostics, see the CSM FAQ on the Web at http://techsupport.services.ibm.com/server/cluster/tips/csm_faq.html.

Note: See “Remote power diagnostics” on page 26 for details on the hardware control command log files.

If a remote console window opens, but then immediately closes and no messages are displayed, an error has occurred during connection to the remote console session. The error could have been written to the remote console window, but the window was immediately closed when the session ended prematurely. Rerun the **rconsole** command with the **–t** option. This forces **rconsole** to open the console session in the current window, and should allow the error to be viewed.

Syntax problems

Table 11. rconsole syntax problems

Problem:	Incorrect argument on **–n** or **–N** option.
Description:	The argument supplied with the **–n** or **–N** option is not valid.
Action:	Verify the list of node names or node groups supplied does not start or end with a comma.
Problem:	Missing option.
Description:	An option switch was encountered with no option, such as **rconsole –node1**, instead of **rconsole –n node1**.
Action:	Verify that all options are complete.
Problem:	Too many arguments specified.
Description:	Options were specified on the command line that are not valid for the specified command.
Action:	Verify the command syntax and ensure that only valid options are specified.

Set up and configuration problems

Table 12. rconsole set up and configuration problems

Problem:	The CSM command could not resolve one or more of the specified node groups.
Description:	A node group specified with the **–N** option could not be resolved.
Action:	Verify the node group name was entered correctly, or use the **nglist** command to verify that the node group exists.
Problem:	The **rconsole** node list environment variable RCONSOLE_LIST is not set.
Description:	If a node list or node group list is not specified on the command line, **rconsole** checks the RCONSOLE_LIST environment variable for the name of the file that contains a list of nodes.
Action:	Either enter a node list with the **–n** option, a node group with the **–N** option, or create a file with the list of nodes to use and set the RCONSOLE_LIST environment variable to the name of this file.

Table 12. rconsole set up and configuration problems (continued)

Problem:	Could not open node list file.
Description:	The node list file was specified in RCONSOLE_LIST but could not be opened.
Action:	Verify that the filename in RCONSOLE_LIST is correct and has read permissions set.
Problem:	The CSM **lsnode** command is not installed.
Description:	The **lsnode** command is not available. The **rconsole** command uses **lsnode** to acquire node attribute information, and cannot proceed if the command is not available.
Action:	**lsnode** is a program in the **csm.server** package. Contact your system administrator to verify CSM installation.
Problem:	Could not resolve a host name.
Description:	One or more of the host names specified could not be resolved.
Action:	Verify the host names are specified correctly and can be resolved on the network by the **–n** option, the **–N** option, or by the file specified by the RCONSOLE_LIST environment variable.
Problem:	A *ConsoleMethod* attribute is missing in the CSM database.
Description:	The specified node does not have an entry in the CSM database for the *ConsoleMethod* attribute.
Action:	Use the **lsnode** command with the **–l** option to verify the entry for *ConsoleMethod* for this node. If necessary, use the **chnode** command to add the *ConsoleMethod* attribute value to the CSM database.
Problem:	A console command does not exist.
Description:	The **rconsole** command requires a console command corresponding to the name of the *ConsoleMethod* in the CSM database. This console command does not exist in the **/opt/csm/bin** directory.
Action:	Verify that the console command exists in the **/opt/csm/bin** directory.
Problem:	Environment variable DISPLAY has not been set.
Description:	The **rconsole –o** tiling option requires the DISPLAY environment variable to be set.
Action:	Set the DISPLAY environment variable to point to the location of the X Server.
Problem:	The package containing the **xwininfo** program has not been installed.
Description:	The **rconsole –o** tiling option requires the **xwininfo** command to be installed.
Action:	Make sure the RPM containing the **xwininfo** command is installed on the management server.

Table 12. rconsole set up and configuration problems (continued)

Problem:
The **rconsole** command does not open windows for some nodes.

Description:
Setting the *ConsoleSerialDevice* attribute in the CSM database to **NONE** for a node will disable remote console support for that node. No sessions will open for these nodes.

Action:
Check the *ConsoleSerialDevice* attribute value in the CSM database for the problem node. If it is not set to **NONE**, proceed with the instructions for diagnosing the problem for a remote console window opening, then immediately closing, given at the beginning of this section.

Problem:
All specified nodes have their *ConsoleSerialDevice* attribute set to **NONE**.

Description:
If the **rconsole** command is invoked for one or more nodes, and all nodes in the list have their *ConsoleSerialDevice* attribute in the CSM database set to **NONE**, this message is displayed.

Action:
Check the *ConsoleSerialDevice* attribute value in the CSM database for the problem nodes.

Connection problems

Table 13. rconsole connection problems

Problem: Connection refused.

Description: The remote console device is not accepting connections.

Action: This indicates a potential network problem or a problem with the console device. Ping the console device's IP address – if the ping is successful, try to telnet directly into the device. For the MRV IR-8000 series, telnet to port 2000; for all other console devices used by CSM hardware control, no port number is required. If a direct telnet is refused, verify that the console device's IP address is not active elsewhere on the network. Verify that the telnet service is available and enabled on the console device. Reset the console device and check its TCP/IP settings. If the direct telnet succeeds, verify that the IP address of the console device matches or resolves to the value entered in the *ConsoleServerName* attribute in the CSM database. If the value is correct, try to telnet to the serial port on the device. Using the port number in the *ConsolePortNum* attribute of the target node from the CSM database as a base, calculate the telnet port as follows:

- For CPS or ELS console devices, add the *ConsolePortNum* to 3000 to obtain the telnet port.
- For Computone console devices, add the *ConsolePortNum* to 9000 to obtain the telnet port.
- For MRV console devices, multiply the *ConsolePortNum* by 100, then add the result to 2000 to obtain the telnet port.

If the telnet directly to the desired port is not successful, then another process has a session open. Refer to the console device documentation to determine which IP address has the port, and how to reset it.

Table 13. rconsole connection problems (continued)

Problem:	A remote console window opens, but no console login prompt is displayed. This problem can be caused by several different scenarios.
Description:	The remote console device cannot establish a connection through the HMC or the node's serial port.
Action:	Check the connection between the target's serial port and the console device. Verify that the *ConsolePortNum* attribute value configured in the CSM database for this node matches the actual port the target is plugged into.
Problem:	The Enter key returns random characters.
Description:	The node's COM port has not been enabled.
Action:	Verify that the COM port corresponding to the *ConsoleSerialDevice* attribute is enabled in the BIOS on the node.
Problem:	A remote console window opens, but no console login prompt is displayed. This problem can be caused by several different scenarios.
Description:	The agetty process is not running on the node port.
Action:	If you ran the **updatenode** command for the first time without rebooting, reboot the node. If the problem persists, log on to the node and run the **ps –ef** command to list the processes running, and look for an agetty entry for the serial port the console device is connected to. Verify that the **/etc/inittab** file contains an entry to start the agetty session on this port at system boot. Verify that the boot loader entries for remote console in the **lilo.conf** file are correct.
Problem:	The S1 port in frame x slot y cannot be accessed. It either does not exist or you do not have S1 permission.
Description:	The **rconsole** command did not find an S1 port in the given location.
Action:	Verify that the *ConsoleServerName* and *ConsolePortNum* values defined for the target node are correct. Verify that an **rpower** query is successful to the same node. If it is, make sure the *ConsoleServerName* attribute value matches the *HWControlPoint* attribute value, and the *ConsolePortNum* value matches the *HWControlNodeId* value. If the **rpower** query is not successful, verify that the SP frame or p660 server is connected to the correct tty port. Note that **frame** *x* refers to the SP frame or p660 server connected to **/dev/tty/***x***-1**. Therefore, if the message returned information about frame 2, the target node's *ConsoleServerName* has been defined as **/dev/tty1** in the CSM database. Verify that a node is actually installed in the given slot number.

Conserver problems

Table 14. rconsole Conserver problems

Problem:	The Conserver software is not functioning as expected.
Description:	A console session cannot be established on a node that uses Conserver software.
Action:	Run the **rconsole –c** command to bypass the Conserver daemon and run the console methods directly. If **rconsole –c** works, then proceed with the following Conserver diagnostic steps.

Table 14. rconsole Conserver problems (continued)

Problem:	A message is returned similar to: clsn06.pok.ibm.com: console 'clsn08.pok.ibm.com' not found.
Description:	The Conserver daemon running on mgtn03.pok.ibm.com does not have the console named clsn08.pok.ibm.com configured.
Action:	Verify that the conserver configuration file **/etc/opt/conserver/conserver.cf** on mgtn03.pok.ibm.com: contains an entry for the given node. If it does not, run the **chrconsolecfg –n** command and specify the name of the node, for example: **chrconsolecfg –n clsn08.pok.ibm.com** to add the entry to the configuration file, then run the **rconsolerefresh** command to update the daemon.
Problem:	console: mgtn03.pok.ibm.com: access from your host refused.
Description:	The host name that the Conserver daemon is configured to accept requests from does not match the host name on the system.
Action:	Verify that the **allowed:** entry at the bottom of the conserver configuration file **/etc/opt/conserver/conserver.cf** on clsn06.pok.ibm.com matches the host name of the system. Depending on how the system is configured, you might need to add the short host name in this field. For example, **allowed: clsn06.pok.ibm.com,clsn06**.
Problem:	A message is returned saying the Conserver daemon is not running.
Description:	A command that expected the conserver daemon to be present has detected the daemon is not running.
Action:	Verify that the Conserver daemon is not running by issuing the **ps -ef | grep opt/conserver/bin/conserver** command. If it is running there should be at least two Conserver processes shown by this command. If the daemon is not running, run the **rconsolerefresh** command, and then run the full **ps** command again. If the daemon is still not running, check the **/etc/opt/conserver/conserver.cf** file for at least one defined console. If the daemon is running, verify that a startup script called **conserver** is present in the **/etc/init.d** directory. If the daemon does not come up after running **rconsolerefresh** and at least one console entry appears in the configuration file, check the **/var/log/conserver** file for more information.
Problem:	The following message is displayed repeatedly: `No environment-specified terminal type.`
Description:	The Conserver daemon does not recognize an environment-specified terminal type.
Action:	Run the **rconsolerefresh –r** command to reinitialize the Conserver daemon.

Other problems

Table 15. rconsole other problems

Problem:	The **rconsole** window font size is too small.
Description:	Using the **rconsole –a** command on a system with more than four nodes caused the default console font size to be set too small.
Action:	Set the RCONSOLE_FONT environment variable to a fixed or desired value. The exact syntax depends on your shell. For example, enter: `export RCONSOLE_FONT=fixed`
Problem:	CSM **lsnode** error. The **rconsole** command runs **lsnode** internally to collect node attribute information.
Description:	The **lsnode** command was run to acquire node attribute information, but did not complete successfully.
Action:	Determine and resolve the problem with **lsnode**. Run **lsnode** from the command line without arguments to check the error results.
Problem:	Running a command resulted in a non-zero return code. The command continued.
Description:	The **rconsole** command invokes a console command for each node. A console command did not complete successfully for one of the nodes. Processing will continue for any other nodes that were specified.
Action:	Determine the error being returned by the console command and contact IBM support.
Problem:	The remote console **xinit** command did not complete successfully.
Description:	The **rconsole** command attempts to open a console by opening a new xterm session. The xterm session could not be started.
Action:	Resolve the problems with **xinit** based on any additional error messages that were provided.

Appendix. Hardware configuration

The following configuration details describe prerequisites for using IBM xSeries x360, IntelliStation 6221, BladeCenter HS20, and the eServer 325 in a CSM cluster.

Note: Check the CSM documentation updates file at http://publib.boulder.ibm.com/clresctr/docs/csm/docerrata.html for late-breaking configuration details.

eServer 325

Refer to the Statement of Direction in the IBM Cluster Systems Management V1.3.2 Announcement Letter for information on support for the eServer 325.

Configuration instructions are planned to be made available for setting up the NIC BMC IP addresses in your CSM cluster. See the CSM Documentation Errata http://publib.boulder.ibm.com/clresctr/docs/csm/docerrata.html and Frequently Asked Questions (FAQ) http://techsupport.services.ibm.com/server/cluster/tips/csm_faq.html Web pages for details.

x360

IBM xSeries 360 (x360) servers can be used in CSM for Linux clusters as Managed nodes running Linux and as the cluster management server. See the *IBM CSM for Linux: Planning and Installation Guide* for the specific software supported on x360 hardware. To use remote console with x360s, you must configure the Serial Port Cable for the x360. To order an x360 Serial Port Cable, retrieve the serial number from your x360 server and call 1-800-IBM-SERV.

For product details on the x360, see http://www.pc.ibm.com/us/eserver/xseries/x360.html.

To download the latest device drivers for the x360, go to http://www.pc.ibm.com/qtechinfo/MIGR-4JTS2T.html and scroll down to the **Server Device Driver File Matrices** section. Click on the x360 link to access the downloads page.

x440

IBM xSeries 440 (x440) servers can be used in CSM for Linux clusters as Managed nodes running Linux and as the cluster management server. See the *IBM CSM for Linux: Planning and Installation Guide* for the specific software supported on x440 hardware. CSM remote console function, MAC address collection, and remote installation is not supported on the x440.

For product details on the x440, see http://www.pc.ibm.com/us/eserver/xseries/x440.html.

To download the latest device drivers for the x440, go to http://www.pc.ibm.com/qtechinfo/MIGR-4JTS2T.html and scroll down to the **Server Device Driver File Matrices** section. Click on the x440 link to access the downloads page.

IntelliStation

IBM IntelliStation 6221 (Intel-based) workstations can be included in CSM for Linux clusters as Managed nodes running Linux. See the *IBM CSM for Linux: Planning and Installation Guide* for the specific software supported on IntelliStation hardware. IntelliStations use the American Power Conversion (APC) MasterSwitch for power; the node *PowerMethod* attribute must be set to **apc**. The APC MasterSwitch enables you to turn on power remotely through a modem or other RS-232 device for initialization in recovery situations. For details on IntelliStation workstations, see http://www.pc.ibm.com/us/intellistation/tech_library.html.

Once you have configured the MasterSwitch IP address using **dhcp**, you can point your Web browser to the MasterSwitch IP address for further configuration or to access the system management interface. For details on the APC MasterSwitch, see http://www.apc.com/products/family/index.cfm?id=70.

Updating the BIOS on IntelliStation hardware must be done using a direct attached terminal. The **rconsole** command will not display the BIOS output during node boot processing.

CSM hardware control commands currently offer limited support for IntelliStation workstations. The **rpower** command is supported using the APC MasterSwitch and a *PowerMethod* attribute value of **apc**. The **rconsole** command is supported using the supported console servers. The **lshwinfo** and **lshwstat** commands are not supported on IntelliStation workstations.

BladeCenter

IBM BladeCenter HS20 servers can be included in CSM for Linux clusters as Managed nodes running Linux and as the cluster management server. See the *IBM CSM for Linux: Planning and Installation Guide* for the specific software supported on BladeCenter hardware. For details on BladeCenter, including the *IBM BladeCenter Planning and Installation Guide*, see http://www.pc.ibm.com/us/eserver/xseries/bladecenter_family.html.

To download the latest device drivers for BladeCenter, go to http://www.pc.ibm.com/qtechinfo/MIGR-4JTS2T.html. Scroll down to the **Server Device Driver File Matrices** section and click on the BladeCenter link to access the downloads page.

Configuring the management module

The BladeCenter **management module** is a hot-swappable hardware device plugged into the BladeCenter chassis management bay. The management module functions as a system-management processor (service processor) and keyboard, video, and mouse (KVM) multiplexor for blade servers. To provide a greater level of security and a backup network path to the BladeCenter chassis, the management module must be connected to the cluster management VLAN (see “Virtual LANs (VLANs)” on page 4). To configure the BladeCenter management module for use in a CSM cluster, take the following steps:

1. **Cable the Ethernet port**
   a. Connect the management module to the network switch using the Ethernet port on the management module. This Ethernet interface should be on the management VLAN. The network for the management module must be *speed* = **100** and *duplex* = **full**.

   b. Connect one end of a Category 5 or higher Ethernet cable to the Ethernet port on the management module. Connect the other end of the Ethernet cable to the management VLAN network switch.
   c. Check the Ethernet LEDs to ensure that the network connection is working.
2. **Configure the IP address for the management module (2 methods)**
   - **Using a DHCP server**
     a. Make sure the DHCP server is running on the CSM management server.
     b. Remove the management module from the chassis and manually record the MAC address which is written on the side of the management module.
     c. Add the MAC address and IP address you will be using for the management module in the **/etc/dhcpd.conf** file and refresh the dhcp daemon on the management server.
     d. Power on the chassis. The management module will broadcast its MAC address, the management server dhcp daemon will return the IP address, and the management module will configure itself with this IP address.
     e. Point your Web browser to the IP address assigned to the management module.
   - **Using the default static IP address from the management module**
     a. The default IP address is 192.168.70.125 and the default subnet is 255.255.255.0. On the CSM management server, create an Ethernet alias IP address which should be on same subnet as the default IP address.
     b. Point your Web browser to the default IP address 192.168.70.125.
3. In the login window, enter the default user ID ″USERID″ and password ″PASSW0RD″ (PASSWzeroRD).
4. Choose **Network Interfaces** under **MM Control** (management module control). The **Network Interfaces** option contains two Ethernet interfaces; external eth0 and internal eth1. eth0 is the interface for the remote management and console port. To disable DHCP, click on the **DHCP** box and select **Disable-Use Static IP Configuration**. Then click on **Save**. From **Advanced Ethernet Setup**, you can choose to set the data rate, duplex mode, and maximum transmission unit.
5. eth1 is the interface for communicating with the switch module. The IP address for eth1 on the management module must be on same subnet as eth0 on the management module. The data rate, duplex mode, and maximum transmission unit are read-only fields for eth1.
6. Once you have set the static IP and disabled DHCP, remove the management module MAC address and IP information from the CSM management server **/etc/dhcpd.conf** file and refresh the DHCP daemon on the management server.
7. Restart the management module using the restart option on the management module Web browser interface. Once the Management Module has been restarted, you can use the management module's new IP address to open its Web browser window.

Management module firmware updates

The management module firmware level must be above BRET36A. To check the firmware level, log in to the management module using a Web browser and check the the Firmware VPD page. To update firmware on the management module using a Web browser, take the following steps:

1. Connect to http://www.pc.ibm.com/qtechinfo/MIGR-4JTS2T.html.
2. Scroll down to **Server Device Driver File Matrices**, and select the BladeCenter link.

3. Download the firmware file for the BladeCenter management module (8677). Follow the instructions in the ReadMe file, create a PKT format file, and place it in a directory on CSM management server. After you download the firmware image and extract it, you will have 5 PKT files. For example:

   ```
   CNETBRUS.PKT ----> Boot ROM
   CNETMNUS.PKT ----> Main Application
   CNETRGUS.PKT ----> Remote GUI Application
   DUALPS2.PKT  ----> PS/2 to USB Convert
   REMOTEKM.PKT ----> Remote keyboard and mouse
   ```

   Each of these files must be updated using the following steps. Repeat steps 7 and 8 for each file.
4. Open a BladeCenter management module window with a Web browser.
5. Enter user ID ″USERID″ and password ″PASSW0RD″ (PASSWzeroRD) at the login window.
6. Click **Firmware Update** in the **MM Control** section. An **Update MM Firmware** window opens.
7. Click the **Browse** button. A **Browse** window opens.
8. In the **Filter** field, enter the directory name in which the firmware images reside, and a wild card with the extension **.pkt**.
9. Press the **Enter** key. All files with the extension **.pkt** are listed on the right side of the window. Repeat this step for each file.
10. Select the correct firmware file, and click on **OK**. The firmware update will start. Repeat this step for each file.
11. After the firmware update finishes, restart the management module.

Configuring the switch module

The BladeCenter **switch module** is a hot-swappable Ethernet switch module plugged into switch-module bay 2 in the BladeCenter chassis. This switch module connects all blade servers in the BladeCenter unit to Ethernet Link 1 (eth0). Connecting each Blade Server to Ethernet Link 2 (eth1) would require an Ethernet switch module in switch-module bay 2. See the *IBM BladeCenter Planning and Installation Guide* for detailed BladeCenter configuration information. The attaching LAN switch must have a compatible multi-port trunk configuration.

BladeCenter HS20 8832 servers recognize the bay 1 switch module as eth0, and the bay 2 switch module as eth1. BladeCenter HS20 8676 and 8678 recognize the switch module in exactly the opposite way: the bay 1 switch module is eth1, and bay 2 switch module is eth0. To use the 8832s in the same chassis as the 8676 or 8678, you must have the latest BIOS level on your 8676 or 8678, and you must take the following manual step for each 8676 and 8678:

```
BIOS setup --> Advanced Setup --> Core Chipset Control --> Swap the numbering of
onboard NICs [Yes]
```

The external ports on the switch modules are set to **autosense** by default. An Ethernet cable will work if you did not manually define the speed for the external ports in the switch module. If you defined the speed for the external ports in the switch module, then you must use a crossover cable to connect the switch module and attached LAN equipment.

Note: For switch communication through the management module's external Ethernet port, which is the switch module's internal network interface:

- Only one IP address can be assigned to each switch module, so it does not require a logic device named **eth1**.

- The management module's internal **eth1** interface and external interfaces must be on the same subnet.

When when using a 100 Mbps link, a crossover cable must connect the switch module and attached LAN equipment. To configure the switch module IP address, take the following steps:

1. Point your Web browser to the IP address of the management module.
2. At the login window prompt, type the management module's user ID and password.
3. From the Web browser window, choose **Switch Tasks --> Management**.
4. Select a switch module to configure.
5. Set an IP address for the switch module; the IP address should be on same subnet as the management module.
6. Click **Save**.
7. Click on **Advanced Switch Management** and select **Send Ping Test** to ping the switch module.
8. From the **Advanced Switch Management** menu, enable **External ports and External management over all ports**.

Switch configuration with mixed 8832 and 8678 blade servers

This section applies to a mixed BladeCenter environment only, where the BladeCenter chassis contains both 8678 and 8832 blade servers. BladeCenter HS20 8832 blade servers recognize the bay 1 switch module as **eth0**, and the bay 2 switch module as **eth1**. BladeCenter HS20 8678 blade servers recognize the switch module in exactly the opposite way: the bay 1 switch module is **eth1**, and bay 2 switch module is **eth0**. To use the 8832 in the same chassis as the 8678, you must have BIOS level 1.05 or later on your 8678, and you must take the following manual step for each 8678:

```
BIOS setup --> Advanced Setup --> Core Chipset Control -->
Swap the numbering of onboard NICs [Yes]
```

Note: The 8678 and the 8832 blade servers require different versions of BIOS and this change is only required to configure the 8678 blades to have the same switch and blade NIC relationship as the 8832 blades.

Configuring the blade server

A BladeCenter HS20 blade server is a hot-swappable independent server containing one or more processors, memory, disk storage, and network controllers. Blade servers are inserted into slots in the BladeCenter chassis and connect to shared components such as power, blowers, CD-ROM and diskette drives, integrated Ethernet and Fibre Channel switches, and the management module. Each blade server runs its own operating system and applications. See the *IBM BladeCenter Planning and Installation Guide* for detailed BladeCenter configuration information.

To set the text ID for blade servers:

1. Point your Web browser to the IP address of the management module.
2. Choose **Blade Tasks --> Configuration**.
3. This section displays a table showing the user configured names for all blades in the chassis. The table includes rows for the 14 blade bays. To change a blade name, enter the name in the corresponding text box. You can enter a maximum of 15 alphanumeric characters.
4. Click on **Save**.

Blade server firmware updates

To update blade server firmware for the BladeCenter HS20, take the following steps:

1. Connect to http://www.pc.ibm.com/qtechinfo/MIGR-4JTS2T.html.
2. Scroll down to **Server Device Driver File Matrices**, and select the BladeCenter link.
3. Download the firmware file for the BladeCenter HS20.
4. Follow the instructions in the Read Me file, create a PKT format file, and place it in a directory on CSM management server.
5. Open a BladeCenter management module window with your Web browser.
6. Enter user ID "USERID" and password "PASSW0RD" (PASSWzeroRD) in the login window.
7. Click on **Blade Tasks --> Firmware Update** to open the **Update Blade Firmware** window.
8. From the **Target** window, select the blade server to update.
9. Click on the **Browse** button to open a **Browse** window.
10. In the **Filter** field, enter the directory name in which the firmware images reside, and a wild card with the extension **.pkt**.
11. Press the **Enter** key. All files with the extension **.pkt** appear on right side of window.
12. To start the firmware update, select the correct firmware file and click the **OK** button.
13. Once the firmware update has completed, restart the blade server.

Setting up CSM for blade server

To set up CSM to manage blade servers, define each blade server as a **Managed** node by defining the following CSM attributes:

```
PowerMethod=xseries
HWControlPoint=management module host name or IP address
HWControlNodeId=blade server text ID
```

Notes:

1. Each blade server requires a unique IP address associated with its Ethernet MAC address.
2. There is no CSM remote console support for blade servers, so you do not need to define the remote console attributes.

Launching a remote console

Remote console function for BladeCenter can be accessed through the management module as follows:

1. Point your Web browser to the IP address of the management module.
2. Select **Blade Tasks --> Remote Control --> Redirect Server Console**. This function allows you to access a blade server video console with keyboard, video, and mouse control (KVM).

Note: This remote console implementation is limited; only one blade server can own the KVM at a time.

Cluster 1350 Serial Port Module option

You can use the **rconsole** command for BladeCenter nodes and an MRV IR-8020 or IR-8040 console server if you are using a Cluster 1350 with the Serial Port Module option. However, you must first order the required parts and complete the required configuration to attach the serial port module to the BladeCenter chassis and MRV console server. You can order the following required parts from IBM or from an authorized IBM products vendor:

- Serial Port Module
- Serial Port Daughter Card
- Serial Port Cable

To configure the parts listed above for BladeCenter **rconsole** function, confirm or set the following hardware requirements:

1. The number on each Serial Port Cable must be matched to the slot position in the BladeCenter chassis.
2. Dip Switch #7 on the Blade must be in the **ON** position. The bank of switches are located next to the CPUs.
3. Attach the serial port module to the BladeCenter chassis' Slot 3.
4. The Daughter Card only plugs into one place on the Blade.
5. Plug the daughter card cable into the connector on the front of the Blade Server. The connector is between the CPUs and the ribbon cable for the Blade Server's bezel. The cable is keyed.

To configure the parts listed above for BladeCenter **rconsole** function, confirm or set the following BIOS requirements:

```
Devices and I/O Ports
 Serial Port A 3F8,IRQ4
 Remote Console
  Remote Console Active             Enabled
  Remote Console Com Port           Com 1
  Remote Console Baud Rate          9600
  Remote Console Data Bits           8
  Remote Console Parity              None
  Remote Console Stop Bits           1
  Remote Console Emulation           VT100
  Remote Console Active After Boot   Enabled
```

To configure the parts listed above for BladeCenter **rconsole** function, confirm or set the following Linux file requirements. In **/etc/lilo.conf**:

```
boot=/dev/hda
map=/boot/map
install=/boot/boot.b
prompt
default=linux
serial=0,9600n8
timeout=100

image=/boot/vmlinuz-2.4.18-3smp
label=linux
read-only
root=/dev/hda6
initrd=/boot/initrd-2.4.18-3smp
append="console=tty0 console=ttyS0,9600n8"
```

After saving the file, run the command:

```
lilo
```

In **/etc/inittab**:

```
1:2345:respawn:/sbin/mingetty tty1
#2:2345:respawn:/sbin/mingetty tty2
#3:2345:respawn:/sbin/mingetty tty3
#4:2345:respawn:/sbin/mingetty tty4
#5:2345:respawn:/sbin/mingetty tty5
#6:2345:respawn:/sbin/mingetty tty6
```

In **/etc/securetty** add:

```
ttyS0
```

Notices

This information was developed for products and services offered in the U.S.A.

IBM development plans are subject to change or withdrawal without further notice. Any reliance on the Statement of Direction is at the relying party's sole risk and will not create any liability or obligation for IBM.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION ″AS IS″ WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Department LJEB/P905
2455 South Road Road
Poughkeepsie, New York 12601-5400
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrates programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Trademarks

The following names are trademarks or registered trademarks in the United States, other countries, or both:

- IBM, alphaWorks, BladeCenter, eServer, the @server logo, IntelliStation, and xSeries are trademarks or registered trademarks of International Business Machines Corp.
- Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.
- Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

- Intel, Intel Inside (logos), MMX and Pentium are trademarks of Intel Corporation in the United States, other countries, or both.
- UNIX is a registered trademark of The Open Group in the United States and other countries.
- SET and the SET Logo are trademarks owned by SET Secure Electronic Transaction LLC.
- Other company, product and service names may be trademarks or service marks of others.

Publicly Available Software

IBM Cluster Systems Management (CSM) for Linux includes software that is publicly available:

Conserver 7.2 (CSM for Linux on xSeries and pSeries)
An application that adds logging and multi-user access for remote administration of serial ports, using locally installed multi-port serial interfaces or ″reverse-telnet″ to console servers, or both.

Expect 5.3 (CSM for Linux on xSeries only)
Tool for automating interactive applications, such as telnet, ftp, passwd, fsck, rlogin, tip.

Perl libnet 1.0703 (CSM for Linux on xSeries only)
Provides a perl client API to FTP, SMTP, NNTP, POP3.

SYSLinux 1.64 (CSM for Linux on xSeries only)
SYSLinux includes PXELINUX, which CSM uses to control the behavior of network boots. SYSLinux is licensed under the GNU GPL.

Tftp-HPA 0.34 (CSM for Linux on xSeries and pSeries)
An implementation of Trivial FTP. Allows download of files from a server when net booting a machine.

Rdist 6.15 (CSM for Linux on xSeries only)
Distributes files to multiple machines, enabling administrators to maintain identical copies of files across multiple machines.

Fping 2.42b (CSM for Linux on xSeries Only)
An implementation of PING for multiple hosts. Quickly ping multiple hosts to determine their reachability.

This book discusses the use of these products only as they apply specifically to the IBM Cluster Systems Management (CSM) for Linux product.

Note: The distribution for SYSLinux includes the source code and associated documentation. All copyright notices and license conditions in the documentation must be respected. You can find version and distribution information for each of these products in the *Specified Operating Environment* section of the *IBM CSM for Linux: Planning and Installation Guide*. For these non-IBM products, the following license terms apply in lieu of the International Program License Agreement.

The freeware package syslinux 1.64 (Freeware Package) is provided with CSM for Linux. The Freeware Package is provided ″AS IS″ and is not warranted or supported by IBM. IBM expressly disclaims all warranties express or implied as to such Freeware Package INCLUDING THE WARRANTY AGAINST NON-INFRINGEMENT, THE WARRANTY OF MERCHANTABILITY AND THE WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE. IBM further disclaims all liability for any damages (including without limitation direct and indirect damages) arising in connection with the Freeware Package. The Freeware Package is licensed under the terms of the GPL, a copy of which is included in the Freeware Package.

Open Source Software	Download site:
Autoupdate 4.3.4 or higher (only required for software maintenance: installation and upgrades of non-CSM RPM packages) (CSM for Linux on xSeries and pSeries)	http://freshmeat.net/projects/autoupdate
perl-XML-Parser (CSM for Linux on xSeries)	SuSE SLES 7: ftp://ftp.rpmfind.net/linux/SuSE-Linux/i386/7.2/full-names/i386/perl-XML-Parser-2.27-63.i386.rpm
perl-XML-Simple (CSM for Linux on xSeries)	• SuSE SLES 7: ftp://speakeasy.rpmfind.net/linux/Mandrake-devel/cookfire/i586/Mandrake/RPMS/perl-XML-Simple-1.05-1mdk.i586.rpm • SuSE SLES 8: ftp://ftp.suse.com/pub/suse/i386/8.1/suse/i586/perl-XML-Simple-1.08-43.i586.rpm

The following non-IBM software is required if you want to perform remote hardware control operations for IBM pSeries servers attached with a Hardware Management Console (HMC):

- openCIMOM Version 0.7

You can download the software from:

- https://techsupport.services.ibm.com/server/cluster.

The following non-IBM software is required for CSM for Linux on pSeries is required if you want to perform the software maintenance installation and upgrade of non-CSM RPMs on Linux Managed nodes from the management server:

- Autoupdate V4.8, or later levels which maintain full backward compatibility.

You can download the software from:

- http://freshmeat.net/projects/autoupdate.

In addition to the terms above, certain components of the Program have Program-unique terms, which are identified in a ″read me″ file in the Program.

EXCLUDED COMPONENTS: Notwithstanding the terms and conditions of any other agreement you may have with IBM or any of its related or affiliated companies (collectively ″IBM″), the following terms and conditions apply to all ″Excluded Components″ identified in this document: (a) all Excluded Components are provided on an ″AS IS″ basis; (b) IBM DISCLAIMS ANY AND ALL EXPRESS AND IMPLIED WARRANTIES AND CONDITIONS INCLUDING, BUT NOT LIMITED TO, THE WARRANTY OF NON-INFRINGEMENT OR INTERFERENCE AND THE IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE; (c) IBM will not be liable to you or indemnify you for any claims related to the Excluded Components; and (d) IBM will not be liable for any direct, indirect, incidental, special exemplary, punitive or consequential damages with respect to the Excluded Components.

The following components in the Program are Excluded Components: (a) conserver 7.2, (b) perl-libnet 1.0703, (c) expect 5.3, (d) perl-to-c extensions and (e) fping 2.4b2, (f) rdist 6.15, and (e) tftp-HPA 0.34.

CSM for Linux includes software developed by the Ohio State University and its contributors.

The inclusion herein of copies of various licenses is not meant to imply endorsement of the principles, methodologies, or views that are contained therein, either express or implied.

For SYSLinux code, licensed under the GNU GENERAL PUBLIC LICENSE Version 2, June 1991, see the following.

Copyright (c) 1989, 1991 Free Software Foundation, Inc. 59 Temple
Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The ″Program″, below, refers to any such program or work, and a ″work based on the Program″ means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term ″modification″.) Each licensee is addressed as ″you″.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.
2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:
   a. You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
   b. You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
   c. If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

   These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:
    a. Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
    b. Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
    c. Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

       The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

       If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.
4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.
5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.
6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You

may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

   If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

   This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

   Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and ″any later version″, you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE

COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM ″AS IS″ WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Glossary

action. The part of the event response resource that contains a command and other information about the command.

APAR. Authorized Program Analysis Report. A report of a problem caused by a suspected defect in a current unaltered release of a program.

ASM. See ISMP.

attribute. Attributes are either persistent or dynamic. A resource class is defined by a set of persistent and dynamic attributes. A resource is also defined by a set of persistent and dynamic attributes. Persistent attributes define the configuration of the resource class and resource. Dynamic attributes define a state or a performance-related aspect of the resource class and resource. In the same resource class or resource, a given attribute name can be specified as either persistent or dynamic, but not both.

Audit Log. A log file containing a record of system events and responses.

authentication. The process of validating the identity of an entity, generally based on user name and password. However, it does not address the access rights of that entity. Thus, it simply makes sure that a user is who he or she claims to be.

authorization. The process of granting or denying access to an entity to system objects or resources, based on the entity's identity.

AutoYaST. The part of the SuSE and SuSE SLES operating systems related to Linux OS installation. See also the **csmsetupyast** command.

BIOS. Basic Input/Output System. Microcode that controls basic hardware operations such as interactions with diskette drives, fixed-disk drives, and the keyboard.

BladeCenter. IBM consolidated high performance eServer hardware racks, which can be used in a CSM cluster.

BladeCenter chassis. A chassis that can hold up to 14 hot-swappable blade servers.

Blade server. An independent server containing one or more processors and associated memory, disk storage and network controllers, and running its own operating system and software.

BMC. The baseboard management controller (**bmc**) is firmware on the eServer 325 NIC card that handles all network traffic. If it detects a hardware control command, the **bmc** accepts and processes the command; otherwise, it ignores it and forwards it to the node.

bmc. **bmc** is the *PowerMethod* attribute value for nodes on eServer 325 servers.

CFM. The Configuration File Manager maintains files that are common across all nodes in a cluster.

client. Client applications are the ordinary user interface programs that are invoked by users or routines provided by trusted services for other components to use. The client has no network identity of its own: it assumes the identity of the invoking user or of the process where it is called, who must have previously obtained network credentials.

client node. In CSM, all nodes except the management server are considered client nodes. In a client/server model, the client system sends requests to a server system, who fulfills the request and returns status.

cluster. A group of servers and other resources that act like a single system and enable high availability and, in some cases, load balancing and parallel processing.

cluster hardware control point. See hardware control point.

clustering. The use of multiple computers (such as UNIX workstations), multiple storage devices, and redundant interconnections to form what appears to users as a single highly-available system. Clustering can be used for load balancing, for high availability, and as a relatively low-cost form of parallel processing for scientific and other applications that lend themselves to parallel operations.

Cluster Systems Management. IBM Cluster Systems Management software for AIX and Linux is designed for simple, low-cost management of distributed and clustered IBM eServers in technical and commercial computing environments. CSM, included with the Cluster 1350 (Linux) and optional with the IBM Cluster 1600 (AIX), simplifies cluster administration by providing management from a single point-of-control.

cluster VLAN. The cluster Virtual LAN (VLAN) connects nodes to each other and to the management server through an Ethernet connection. Installation and CSM administration tasks such as running **dsh** are done on the cluster VLAN.

coexistence. The ability of two different pieces of software, running either on the same machine or on machines that are interconnected, to function together. For example, an AIX node and a Linux node coexist in a mixed cluster having an AIX management server.

condition. A certain state of a node resource that can be monitored.

console. The main operating system display station. Synonym for system console.

console server. The hardware device through which the management server opens a remote console session for a node.

consumability. Uses the **snmptrap** command to generate traps containing ERRM event information that can be sent to an SNMP manager.

CSM. See Cluster Systems Management.

CSM database. A repository of cluster, node, and node group information that is created and used by CSM.

CSM GUIs. Graphical User Interfaces (GUIs) available for running CSM functions: IBM Web-based System Manager, SMIT, and DCEM GUIs.

CSM-only installation. The process of installing only CSM on the nodes, as opposed to a full installation, which involves installing both CSM and the operating system on the nodes.

CSM plug-ins. IBM Web-based System Manager GUI plug-ins, which provide an interface for monitoring and managing one or more CSM clusters.

DCEM. Distributed Command Execution Manager is a GUI that can run commands on multiple cluster nodes simultaneously.

distribution. One of the Linux operating systems used with CSM. For example, Red Hat, SuSE, or SuSE SLES.

domain. (1) A set of network resources (such as applications and printers, for example) for a group of users. A user logs in to the domain to gain access to the resources, which could be located on a number of different servers in the network. (2) A group of server and client machines that exist in the same security structure. (3) A group of computers and devices on a network that are administered as a unit with common rules and procedures. Within the Internet, a domain is defined by its Internet Protocol (IP) address. All devices that share a common part of the IP address are in the same domain.

Domain Management Server resource manager (IBM.DMSRM). Controls the Managed node (IBM.ManagedNode) resource class and the node group (IBM.NodeGroup) resource class.

device driver. (also, **driver**, **kernel module**.) A software program that interacts with a particular hardware device or with other software. Downloading or building kernel modules may be required to install an operating system on certain hardware. A different kernel module is required for each version of the Linux kernel.

dsh. A distributed shell program - a mechanism to issue commands to all systems in a network, in parallel.

dynamic attribute. A node attribute with a value that can change over time, such as node power status.

dynamic node group. A variable node group consisting of nodes with specific attribute values.

ERRM. RSCT Event Response Resource Manager controls events and responses on cluster nodes.

ESP. The Equinox Ethernet Serial Provider allows you to place COM serial ports anywhere on a local or remote LAN segment. The ESP units communicate with an Equinox SuperSerial NT driver located on Windows NT Server and Workstation systems. Ports on the ESP appear to the servers as standard COM ports as if they were right on the servers' system bus. All the facilities and functions of Windows NT and of application programs are fully available to these LAN-resident COM ports. The ESP units and the LAN are ″transparent″.

Ethernet. (1) Ethernet is the standard hardware for TCP/IP local area networks in the UNIX marketplace. It is a 10-megabit per second baseband type LAN that allows multiple stations to access the transmission medium at will without prior coordination. The Ethernet avoids contention by using carrier sense and deference, and resolves contention by collision detection (CSMA/CD). (2) A passive coaxial cable whose interconnections contain devices or components, or both, that are all active. It uses CSMA/CD technology to provide a best-effort delivery system.

event. Occurs when the event expression of a condition evaluates to True. An evaluation occurs each time an instance of a dynamic attribute is observed.

event expression. A definition of the specific state when an event is true.

event response. One or more actions as defined by the event response resource manager (ERRM), that take place in response to an event or a rearm event.

fanout. The number of systems or processors that are to receive software updates or communications simultaneously. For CSM, this is controlled by the environment variable **CSM_FANOUT**. The **DSH_FANOUT** environment variable is used by the **dsh** command to control the number of nodes on which to simultaneously run a remote command.

fileset. For AIX, a collection of files, usually used to install a piece of software. The equivalent Linux term is package.

fix. A correction or enhancement to software.

full installation. The process of installing both the CSM software and the operating system on the nodes of the cluster, as opposed to installing only CSM on the nodes, or installing only the operating system on the nodes.

GPFS. The IBM General Parallel File System (GPFS) for AIX and Linux allows users shared access to files that may span multiple disk drives on multiple nodes. It offers many of the standard AIX file system interfaces, allowing most applications to run without modification or recompiling. AIX file system utilities are also supported by GPFS.

hardware control point. The hardware device through which the management server controls node hardware.

Hardware Control resource manager. The IBM Hardware Control resource manager manages the IBM.NodeHwCtrl and IBM.HwCtrlPoint resource classes.

Hardware Management Console. The IBM Hardware Management Console for pSeries is an installation and service support processor that runs only the HMC software.

HMC. See Hardware Management Console.

| **hmc.** **hmc** is the *PowerMethod* and *ConsoleMethod* attribute value for nodes on HMC-attached pSeries servers

hostmap file. See hostname mapping file.

host name. (1) A name assigned to a computer connected to a network. The use of this term can be ambiguous as it can refer to either the short form name of the computer (see short host name), or the fully qualified name of the computer (see long host name). (2) The Internet address of a machine in the network. Also known as host ID.

hostname mapping file. A file containing a list of host names and associated hardware control information. This file can be created by the **lshwinfo** command and used as input to the **definenode** command.

IBM.DMSRM. See Domain Management Server resource manager.

IBM.HWCTRLRM. See Hardware Control resource manager.

IBM.NodeHwCtrl. See Node Hardware Control Resource Class.

ISMP. Integrated System Management Processor - a computer within a computer, the ISMP performs systems management tasks that help manage and maintain the health of your server. Integrated into select xSeries servers, the ISMP continuously monitors your system and notifies you of potential failures.

Through IBM Director, the ISMP alerts you to changes in system temperature, voltage, fan redundancy, memory and hard-drive performance. It also provides configuration management benefits with features like remote firmware updates, remote power control, and Automatic Server Restart (ASR).

On Linux, the IBM Integrated System Management Processor (ISMP) device monitors and provides remote power control for xSeries servers. ISMPs are also referred to as ASMs.

kernel. The essential component of the Linux and AIX operating system. The kernel is responsible for critical OS functions such as resource allocation, low-level hardware interfaces, and security. Installation on certain hardware, certain Linux distributions, or certain device drivers might require a minimum kernel version.

Kickstart. On Linux, part of the Red Hat operating system used to help install Red Hat. Using Kickstart, a system administrator can create a single file containing the answers to all the questions that would normally be asked during a typical Red Hat Linux installation.

Kickstart files can be kept on single server system, and read by individual computers during the installation. This installation method can support the use of a single Kickstart file to install Red Hat Linux on multiple machines, making it ideal for network and system administrators. For CSM, see the **csmsetupks** command.

kscfg.tmpl. This file is the template used by the **csmsetupks** command to create a Kickstart configuration file for each Linux node. The template is located in **/opt/csm/install/kscfg.tmpl.** *InstallDistributionNameInstallDistributionVersion*.

The Kickstart configuration file generated by **csmsetupks** from the template contains configuration information gathered by Kickstart during installation of the Linux operating system. The **kscfg.tmpl** file can be used as is, or modified. See the sample template in the Appendix of *IBM CSM for Linux: Software Planning and Installation Guide* for instructions on how to properly modify the template.

ksh. Korn shell

license key file. A file containing keys (passwords) necessary to run CSM.

license use key. A key (password) that is required to run CSM. A license key file, containing license use keys, is included with the CSM package.

Linux node. One instance of a Linux operating system running on IBM xSeries hardware.

long host name. A fully-qualified host name (for example, node15.pok.ibm.com).

LPAR. Logical partition. The partitioning of an operating system and its associated resources, such as memory, to give the appearance and functionality of more than one operating system.

MAC address. The Media Access Control address is a hardware address that uniquely identifies each node of a network. On a local area network (LAN) or other network, the MAC address is the computer's unique hardware number. On an Ethernet LAN, it is the same as the computer's Ethernet address. CSM only uses the MAC address of the network adapter used to do network boot and installation – the network adapter on the cluster VLAN.

machine architecture. The type of hardware for a specific Linux node on xSeries hardware. For CSM, the machine architecture is specified by the *InstallPkgArchitecture* node attribute, and must be provided for hardware control. Currently, CSM supports i386 machine architecture only. However, i486, i586, and i686 processors can be used provided they are defined with an *InstallPkgArchitecture* of i386.

Managed node. A node in a CSM cluster under the control of the management server. This node has a Mode attribute of ″Managed″. The **updatenode** command converts PreManaged nodes to Managed nodes.

management control point. See management server.

management domain. A set of nodes that are configured for management by the Clusters Systems Management (CSM) licensed program. Such a domain has a management server that is used to administer a number of Managed nodes. Only management servers have knowledge of the whole domain. Managed nodes only know about the servers managing them; they know nothing of each other.

management server. A node with CSM cluster management server software installed.

management VLAN. The management Virtual LAN (VLAN) connects the management server to the cluster hardware through an Ethernet connection. For optimal security, the management VLAN must be restricted to hardware control points, remote console servers, the management server, and root users. Routing between the management VLAN and cluster or public VLANs could compromise security on the management VLAN.

migration. The process of moving to a later software version.

mixed cluster. A CSM cluster with an AIX 5L management server and both AIX and Linux nodes.

NFS. A distributed file system that allows users to access files and directories located on remote computers and treat those files and directories as if they were local. NFS allows different systems (UNIX or non-UNIX), different architectures, or vendors connected to the same network, to access remote files in a LAN environment as though they were local files.

node. One operating system image. See **Managed node**.

node attribute. Pieces of information that make up a node definition. For a CSM node, these attributes must be defined in the CSM database. See the **nodeattributes** man page for more details.

node attribute template. A worksheet used by the system administrator to record the attributes assigned to the nodes.

node configuration template. A worksheet used by the system administrator to record details of the node configuration.

nodedef file. See node definition file.

node definition file. A file containing a stanza of information for defining each node in a cluster. The information about each node is of the form *Attr=value*, such as *InstallOSName*=AIX. This file can be used by the **definenode** command. See the man page for **nodedef** for more details.

node group. Nodes having similar attribute values and defined as a group to facilitate node management.

Node Hardware Control Resource Class (IBM.NodeHwCtrl). Provides support for powering a node on and off, resetting a node, querying the power status of a node, resetting the node's service processor, and resetting the node's hardware control point.

null value. Empty, having no value, containing nothing.

Open source software. Any program whose source code is made available for use or modification as users or other developers see fit. Open source software is usually developed as a public collaboration and made freely available.

OpenSSH. For Linux, OpenSSH is a free version of the SSH protocol suite of network connectivity tools. For AIX, OpenSSH encrypts all traffic (including passwords) to effectively eliminate eavesdropping, connection hijacking, and other network-level attacks. Additionally, OpenSSH provides a myriad of secure tunneling capabilities, as well as a variety of authentication methods. See the OpenSSH Web site at http://www.openssh.com.

package. For Linux, a collection of files, usually used to install a piece of software. The equivalent AIX term is **fileset**. For Linux, a package is also referred to as an RPM (Red Hat Program Manager) package.

partition. (1) A logical division of storage on a fixed disk. (2) A fixed-size division of storage. (3) a group of non-overlapping nodes that act as a logical system.

persistent attribute. A node attribute with a value that does not change without manual user input, such as node name.

port number. A port number is a way to identify a specific process to which an Internet or other network message is to be forwarded when it arrives at a server. For the TCP/IP and UDP protocols, a port number is a 16-bit integer that is put in the header appended to a message unit. This port number is passed logically between client and server transport layers, and physically between the transport layer and the Internet Protocol layer.

predefined condition. A condition whose definition is supplied by the RMC portion of RSCT. Predefined conditions are used to monitor certain system events, and may be customized for a particular installation.

predefined dynamic node group. A node group whose members all have a certain attribute set to a certain value. The definitions of these groups are shipped with CSM. For example, the **LinuxNodes** group consists of those nodes whose *InstallOSName*=**Linux**.

predefined response. A response whose definition is supplied by the RMC component of RSCT. Predefined responses are defined to take action when a certain condition becomes true. They may be customized for a particular installation.

PreManaged node. A node that is part of a CSM cluster, but has not yet been put under the control of the management server. Such a node has a Mode attribute of ″Premanaged″. The **updatenode** command converts PreManaged nodes to Managed nodes.

probe. Diagnostic software that assesses the functionality of a single machine at a time.

| **pSeries.** IBM eServer hardware that runs the AIX 5L
| and Linux operating systems.

public VLAN. The public Virtual LAN (VLAN) connects the cluster nodes and management server to the site network. Applications are accessed and run on cluster nodes over the public VLAN. The public VLAN can be connected to nodes through a second Ethernet adapter in each node, or by routing to each node through the Ethernet switch.

rconsole. The remote console command. See remote console.

rearm event. An event that occurs when the rearm expression for a condition evaluates to True.

rearm expression. An expression that generates an event which alternates with an original event in the following way: the event expression is used until it is true; then, the rearm expression is used until it is true; then, the event expression is used. The rearm expression is commonly defined as the inverse of the event expression. It can also be used with the event expression to define an upper and lower boundary for a condition of interest.

Red Hat. Red Hat is a software company in the business of assembling open source components for the Linux operating system and related programs into a distribution package.

Red Hat Linux. A version of Linux produced by Red Hat Inc.

remote command. A command issued on the management server that is intended to run on one of the cluster nodes.

remote console. From the management server, access to the operator console of one or more CSM nodes. See the **rconsole** command.

remote hardware control. Management server control of cluster node hardware.

remote power. Management server control of the following CSM node hardware characteristics: power on or off, query power status, reboot, and reset of the service processor. See the **rpower** command.

remote shell. When using the **dsh** command, the shell where the remote command will run. Also, the shell set up on each node during installation. In CSM, the *RemoteShell* attribute value specifies which remote shell is used. The default value on AIX is **/usr/bin/rsh**. The default value on Linux is **/usr/bin/ssh**.

resource. An entity in the system that provides a set of services. Examples of hardware entities are processors, disk drives, memory, and adapters. Examples of software entities are database applications, processes, and file systems. Each resource in the system has one or more attributes that define the state of the resource.

resource class. A group of resources that have attributes, actions, and other characteristics of the resource class in common.

resource manager. A standalone daemon that maps resource and resource class abstractions into calls and commands for one or more specific types of resources.

response. An automated response to a node resource condition.

RMC. The IBM Resource Monitoring and Control component of RSCT, which monitors and controls cluster nodes.

RPM packages. Software and updates for Linux nodes.

rpower. The remote power command. See remote power.

RSA. The IBM Remote Supervisor Adapter (RSA) is the hardware control point for xSeries servers.

RSCT. IBM Reliable Scalable Cluster Technology is a set of software components that together provide a comprehensive clustering environment for AIX and Linux. RSCT is the infrastructure used by a variety of IBM products, including CSM, to provide clusters with improved system availability, scalability, and ease of use.

rsh. A variant of the **rlogin** command that invokes a command interpreter on a remote UNIX machine and passes the command line arguments to the command interpreter, skipping the LOGIN step completely.

Server File Repository. A directory on the management server named **/cfmroot**, which contains the cluster configuration files

servers. Hardware that has server programs running in the background on the OS without a user's inherited credentials. A server must acquire its own network identity to get to access other trusted services.

service processor. A computer attached to a processor, whose sole function is to control the hardware and provide diagnostic support.

shell. The shell is the primary user interface for the UNIX operating system. It serves as command language interpreter, programming language, and allows foreground and background processing. Implementations of the shell concept include Bourne, C, and Korn.

short host name. A host name that contains only the local identifier.

SIS. System Installation Suite - On Linux, an open source product that helps you install and configure SuSE and SuSE SLES. For use with CSM, see the **csmsetupsis** command.

SMS. Software Maintenance System maintains RPM packages on Linux nodes from an AIX or Linux management server.

SNMP. Simple Network Management Protocol. (1) An IP network management protocol that is used to monitor attached networks and routers. (2) A TCP/IP-based protocol for exchanging network management information and outlining the structure for communications among network devices.

ssh. Secure Shell, sometimes known as Secure Socket Shell, is a Unix-based command interface and protocol for securely getting access to a remote computer.

static node group. A node group consisting of nodes specified by the user.

SuSE. SuSE is a privately owned German company whose mission is to promote open source development and General Public License distribution and to be a Linux distribution provider. SuSE assembles open source components for the Linux operating system and related programs into a selection of distribution packages.

SuSE Linux. A version of Linux produced by SuSE, Inc.

SuSE SLES. SuSE Linux Enterprise Server is a server operating system for professional deployment in heterogeneous IT environment of all sizes and sectors.

update. Software fixes periodically installed on a system.

visual monitoring. An icon-based method for monitoring a CSM cluster.

VLAN. Virtual LAN - Virtual Local Area Network. A division of a local area network by software rather than by physical arrangement of cables. Division of the LAN into subgroups can simplify and speed up communications within a workgroup. Switching a user from one virtual LAN to another via software is also easier than rewiring the hardware.

xCAT. xCAT (Extreme Cluster Administration Toolkit) is a tool kit that can be used for the deployment and administration of Linux clusters. Its features are based on user requirements, and many of its features take advantage of IBM xSeries hardware.

xSeries. IBM eServer hardware based on the Intel architecture.

yastcfg XML file. Template used by the **csmsetupyast** command to create an AutoYaST configuration file for each Linux node. The template is located in **opt/csm/install/yastcfg.***InstallDistributionName* *InstallDistributionVersion***-Arch.xml**.

Bibliography

This Bibliography helps you find documentation related to Cluster Systems Management (CSM).

Related information

The following references contain information about IBM Cluster Systems Management for Linux:

- *IBM CSM for Linux: Software Planning and Installation Guide*, SA22–7853
- *IBM CSM for Linux: Administration Guide*, SA22–7873
- *IBM CSM for Linux: Hardware Control Guide*, SA22–7856
- *IBM CSM for Linux: Command and Technical Reference*, SA22–7933

The following references contain information about Reliable Scalable Computing Technology (RSCT) for Linux:

- *IBM RSCT for Linux: Administration Guide*, SA22–7892
- *IBM RSCT for Linux: Technical Reference*, SA22–7893
- *IBM RSCT for Linux: Messages*, GA22–7894
- *IBM RSCT for Linux: Group Services Programming Guide and Reference*, SA22–7888

Obtaining publications

The CSM and RSCT for Linux publications are available at either of the following Web sites:

- http://www.ibm.com/servers/eserver/clusters/library
- http://www.ibm.com/shop/publications/order

The @server Cluster 1350 InfoCenter is available at: http://publib.boulder.ibm.com/cluster/.

Redbooks

The IBM International Technical Support Organization (ITSO) publishes Redbooks related to CSM.

- Linux Clustering with CSM and GPFS

For a current list, see the IBM Redbooks Web site at: http://www.ibm.com/redbooks.

Other CSM information

See the following references for information related to CSM:

Information about CSM	Location
Service information (fixes and updates)	http://techsupport.services.ibm.com/server/cluster
CSM driver downloads	http://techsupport.services.ibm.com/server/cluster2/fixes/csmdriverdownload.html
README file	**/opt/csm/README/csm.README**
Documentation Errata	http://publib.boulder.ibm.com/clresctr/docs/csm/docerrata.html

Information about CSM	Location
Frequently Asked Questions (FAQ)	http://techsupport.services.ibm.com/server/cluster/tips/csm_faq.html
Read This First document	http://www.ibm.com/servers/eserver/clusters/library

Getting XCAT tools

If you are an XCAT user, you may find the IBM alphaWorks® *Enhanced Cluster Tools (ECT) for Linux* Web site useful. It is a repository of tools that complement CSM and enhance the management of Linux clusters. The ECT for Linux site provides tools that supplement CSM features such as remote access to hardware inventory and vitals, remote access to server processor logs, and support for the ELS console server. The ECT site includes early versions of tools that will eventually be merged into the CSM product, prototypes of new technology that is being investigated for CSM, and tools for specific vertical market segments. The ECT for Linux site is located at http://www.alphaworks.ibm.com/tech/ect4linux.

Getting help from IBM

CSM mailing list information is available at http://www.ibm.com/developerworks/oss/mailman/listinfo/csm. E-mail sent to this mailing list at csm@www-124.ibm.com is monitored by the CSM development team, providing a mechanism for users to ask questions and resolve problems. If the mailing list does not solve your problem, then you can send a note directly to the CSM development team at cluster@us.ibm.com, or call IBM Support at 1–800–IBM–SERV.

Before you call for help, check to see if all the latest service has been applied to your system. Then, see the diagnosis section in the *IBM CSM for Linux: Administration Guide* to help you diagnose problems before placing a call. If you still need help resolving the problem, call IBM. You might be asked to send relevant data, and to open a problem management record (PMR) for tracking purposes.

Finding service information

The following Web sites contains all the service bulletins and flashes, as well as PTF and APAR reports for all current releases of CSM:

- Cluster software: http://techsupport.services.ibm.com/server/support
- CSM software: https://techsupport.services.ibm.com/server/cluster/fixes/csmfixhome.html
- CSM for Linux on pSeries: https://techsupport.services.ibm.com/server/cluster/csmplinux_1.3.2.0down.html
- CSM for Linux: https://techsupport.services.ibm.com/server/cluster/csmlinux_1.3.2.0down.html

Calling IBM for help

You can get assistance by calling IBM Support. Before you call, be sure you have the following information:

1. Your access code (customer number).
2. The IBM product number. The product number for CSM is 5765–E88.
3. The name and version of the operating system you are using.
4. Any relevant machine type and serial numbers.

5. A telephone number where you can be reached.

The person with whom you speak will ask for the above information and give you a time period during which an IBM representative will call you back.

In the United States:

- The telephone number for IBM software support and IBM hardware support is **1–800–IBM–SERV**.
- The telephone number for IBM Linux support is **1–800–237–5511**.

Outside the United States, contact your local IBM Service Center.

Contacting CSM development

To contact CSM development by e-mail, send your comments to cluster@us.ibm.com.

Index

A

about this book v
APC configuration 21
APC configuration examples 22
APC MasterSwitch
  problems
    connection 32
    operation 33
    set up and configuration 31
attribute
  ConsoleMethod 35
  ConsolePortNum 35
  ConsoleSerialDevice 35
  ConsoleServerName 35
  ConsoleServerNumber 35
  HWControlNodeId 17
  HWControlPoint 17
  PowerMethod 17
attribute values
  remote console 36
  remote power 17
attributes
  remote console 35
  remote power 17
audience of this book v

B

Bibliography 75
blade server
  firmware updates 56
BladeCenter
  conceptual diagram 5
  mixed 8832 and 8678 blade servers 55
  remote console 56
    Cluster 1350 Serial Port Module option 56
  remote console redirection 44
BladeCenter blade server
  setting up CSM 56
BladeCenter blade server configuration 55
BladeCenter blade server firmware updates 56
BladeCenter configuration 51, 52
BladeCenter management module configuration 52
BladeCenter management module firmware updates 53
BladeCenter switch module configuration 54

C

calling IBM 76
cluster VLAN 4
commands 1
Computone configuration 41
conceptual diagram
  Linux on pSeries 9
  xSeries 5
configuration
  eServer 325 51
  remote console 35, 38
  remote power 17
  remote power software 18
  x360 51
configuration examples
  HMC-attached pSeries 19
Conserver
  diagnostics 48
  read-only consoles 37
console redirection
  grub.conf 42
ConsoleMethod attribute 35
ConsolePortNum attribute 35
ConsoleSerialDevice attribute 35
ConsoleServerName attribute 35
ConsoleServerNumber attribute 35
CPS configuration 42
CSM hardware control 1
CSM information 75
CSM project e-mail address 77

D

diagnostics
  APC MasterSwitch
    connection 32
    operation 33
    set up and configuration 31
  rconsole connection 47
  rconsole Conserver 48
  rconsole other 50
  rconsole set up and configuration 45
  rconsole syntax 45
  remote console 44
  remote power 26
  rpower connection 30
  rpower set up and configuration 28

E

e-mail address for CSM 76, 77
ELS configuration 39
eServer 325
  conceptual diagram 5
eServer 325 configuration 23, 51
eServer 325 configuration examples 23
ESP configuration 40

F

firmware updates
  BladeCenter blade server 56
  BladeCenter management module 53

G

glossary 67
grub.conf redirection 42

H

hardware and network requirements 3
hardware attributes
  node 13
hardware configuration 51
hardware control
  testing 25, 44
hardware control points
  remote access 27
    APC MasterSwitch 27
    RSA and management module 27
help from IBM 76
HMC-attached pSeries configuration examples 19
HMC-attached pSeries server configuration 19
HWControlNodeId attribute 17
HWControlPoint attribute 17

I

IntelliStation
  conceptual diagram 5
  remote console redirection 44
IntelliStation configuration 51, 52
ISO 9000 vi

L

Linux node attributes
  example 7
Linux on pSeries
  conceptual diagram 9
Linux on pSeries node attributes
  example 11
log files
  remote power 26

M

mailing list, CSM 76
management module
  firmware updates 53
  remote access to hardware control points 27
management VLAN 4
MRV IR-8000 series configuration 38
MRV LX-4000 series configuration 39

N

network requirements 3
node attributes example
  Linux 7
  Linux on pSeries 11

P

PowerMethod attribute 17
prerequisite knowledge for this book v
problems
  APC MasterSwitch
    connection 32
    operation 33
    set up and configuration 31
  rconsole connection 47
  rconsole Conserver 48
  rconsole other 50
  rconsole set up and configuration 45
  rconsole syntax 45
  remote console 44
  remote power 26
  rpower connection 30
  rpower set up and configuration 28
pSeries
  conceptual diagram 9
pSeries configuration examples
  HMC-attached 19
pSeries server configuration
  HMC-attached 19
public VLAN 4
publications
  obtaining 75
  related 75
publicly available software 61

R

rconsole
  other problems 50
rconsole configuration
  Computone 41
  CPS 42
  ELS 39
  ESP 40
  MRV IR-8000 38
  MRV LX-4000 39
rconsole connection
  diagnostics 47
rconsole Conserver
  problems 48
rconsole set up and configuration
  diagnostics 45
rconsole syntax
  problems 45
registered trademarks 60
related information 75
remote access to hardware control points 27
  APC MasterSwitch 27
  RSA and management module 27
remote console
  attribute values 36
  BladeCenter 56
  BladeCenter Cluster 1350 Serial Port Module option 56
  configuration 35
  fonts 36

remote console *(continued)*
  redirection, BladeCenter 44
  redirection, IntelliStation 44
  redirection, xSeries 43
  software 35
  tiling 37
  xSeries redirection 42
remote console attributes 35
remote console configuration 38
remote console diagnostics 44
remote console hardware control
  testing 44
remote power
  attribute values 17
  configuration 17
  software 17
remote power attributes 17
remote power diagnostics 26
remote power hardware control
  testing 25
remote power log and trace files 26
remote power software configuration 18
rpower
  connection problems 30
  set up and configuration problems 28
RSA
  remote access to hardware control points 27

S

security 18
server configuration
  HMC-attached pSeries 19
software
  remote console 35
  remote power 17
system ID attributes 24
system IDs
  creating and testing
    xSeries 24

T

tcp port numbers 28
terminology 2
testing remote console hardware control 44
testing remote power hardware control 25
trace files
  remote power 26
trademarks 60
typographic conventions v

V

virtual LAN (VLAN) 4
VLAN
  cluster 4
  management 4
  public 4

W

Web sites for publications 75

X

x360 configuration 51
XCAT tools 76
xSeries
  conceptual diagram 5
  remote console redirection 42, 43
xSeries 360 configuration 51
xSeries 440 configuration 51
xSeries configuration examples 21

Readers' Comments — We'd Like to Hear from You

IBM Cluster Systems Management for Linux
Hardware Control Guide
Version 1.3.2

Publication No. SA22-7856-07

Overall, how satisfied are you with the information in this book?

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Overall satisfaction	□	□	□	□	□

How satisfied are you that the information in this book is:

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Accurate	□	□	□	□	□
Complete	□	□	□	□	□
Easy to find	□	□	□	□	□
Easy to understand	□	□	□	□	□
Well organized	□	□	□	□	□
Applicable to your tasks	□	□	□	□	□

Please tell us how we can improve this book:

Thank you for your responses. May we contact you? □ Yes □ No

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

Name	Address
Company or Organization	
Phone No.	

Readers' Comments — We'd Like to Hear from You
SA22-7856-07

Cut or Fold
Along Line

Fold and Tape **Please do not staple** Fold and Tape

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

IBM Corporation
Department 55JA, Mail Station P384
2455 South Road
Poughkeepsie NY 12601-5400

Fold and Tape **Please do not staple** Fold and Tape

Cut or Fold
Along Line

Program Number: 5765–E88, 5765–G16

SA22-7856-07