Contents

About this book ........................................................................................................................................ 1
Summary of changes .............................................................................................................................. 1
Who should use this book ...................................................................................................................... 2
Typographic conventions ...................................................................................................................... 2
ISO 9000 ............................................................................................................................................ 2
Related information ............................................................................................................................. 3
Bibliography ....................................................................................................................................... 5
Redbooks ........................................................................................................................................... 5
CSM product information ..................................................................................................................... 5
Getting help from IBM ........................................................................................................................ 5
Finding service information ................................................................................................................ 6
Calling IBM for help ............................................................................................................................ 6
How to send your comments ............................................................................................................... 6
Chapter 1. CSM overview .................................................................................................................. 8
Managing a CSM cluster ...................................................................................................................... 8
Installing and updating software on the cluster nodes ....................................................................... 8
Running distributed commands across the cluster ............................................................................. 9
Synchronizing files across the cluster ................................................................................................. 9
Running user-provided customization scripts .................................................................................. 9
Monitoring the cluster nodes ............................................................................................................. 9
Controlling cluster hardware ........................................................................................................... 10
Managing node and device groups .................................................................................................... 10
Running diagnostic tools .................................................................................................................. 11
Configuring additional network adapters ......................................................................................... 11
Communicating with CSM ................................................................................................................. 11
Command line interface ..................................................................................................................... 11
Distributed Command Execution Manager (DCEM) ....................................................................... 11
IBM Web-based System Manager ..................................................................................................... 12
SMIT ................................................................................................................................................ 12
Chapter 2. Planning for cluster hardware ......................................................................................... 13
Scaling .............................................................................................................................................. 13
Planning for a CSM for AIX management server ............................................................................ 13
Memory and disk space requirements ............................................................................................... 13
Network requirements ....................................................................................................................... 14
Security guidelines ............................................................................................................................ 14
Using an LPAR management server ............................................................................................... 14
Planning for CSM for AIX install servers ....................................................................................... 15
Planning for CSM for AIX nodes ....................................................................................................... 15
Compatibility with Advanced POWER Virtualization ................................................................. 16
Planning for a CSM for Linux management server ........................................................................ 16
Memory and disk space requirements ............................................................................................... 16
Network requirements ....................................................................................................................... 16
Security guidelines ............................................................................................................................ 17
Planning for CSM for Linux install servers .................................................................................... 17
Planning for CSM for Linux nodes .................................................................................................... 17
System p hardware support for Linux ............................................................................................ 18
System x hardware support for Linux ............................................................................................ 18
Install server and node hardware ..................................................................................................... 18
Linux distributions and hardware support ....................................................................................... 19
Planning for Cluster-Ready Hardware Server (CRHS) ................................................................ 22
Chapter 22. Updating CSM for AIX .......................................................................................................... 318

Chapter 21. Upgrading the Linux operating system................................................................................... 301

Chapter 20. Migrating the AIX operating system ...................................................................................... 296

Chapter 18. Uninstalling CSM ................................................................................................................... 281

Chapter 19. Installation scenarios................................................................................................................ 283

 Obtaining CSM updates...................................................................................................................... 318
 Upgrading Linux nodes ...................................................................................................................... 303
 Upgrading a Linux install server ........................................................................................................ 302

 Migrating the AIX operating system ................................................................................................... 296

 Migrating an AIX management server ................................................................................................ 296
 Backing up CSM for AIX data.............................................................................................................. 296
 Update CSM for AIX prerequisites .................................................................................................... 296
 Perform the AIX system migration ..................................................................................................... 297
 Accept the CSM for AIX license agreement ....................................................................................... 297
 Copy the files to /csminstall .............................................................................................................. 298
 Using a NIM server ............................................................................................................................ 298
 Verifying the AIX installation (optional) ............................................................................................. 298

 Migrating an AIX install server ........................................................................................................... 299

 Migrating AIX nodes.......................................................................................................................... 299
 Remote AIX migration ......................................................................................................................... 299
 Using the remote alternate disk to perform AIX migration ............................................................... 300

 Chapter 21. Upgrading the Linux operating system................................................................................ 301

 Upgrading the Linux management server .......................................................................................... 301
 Backing up CSM for Linux data........................................................................................................... 301
 Performing the Linux upgrade or reinstallation ............................................................................... 302
 Restoring your CSM for Linux data ................................................................................................... 302

 Upgrading a Linux install server ......................................................................................................... 302

 Upgrading Linux nodes ...................................................................................................................... 303
 Upgrading Linux on nodes .................................................................................................................. 303

 Chapter 22. Updating CSM for AIX ......................................................................................................... 318

 Obtaining CSM updates...................................................................................................................... 318
 Updating the CSM for AIX management server ................................................................................ 318
 Backing up CSM data......................................................................................................................... 318
 Commit previous levels of software .................................................................................................. 319
 Update CSM Blue Gene support ........................................................................................................ 319
 Gather updates ...................................................................................................................................... 319
 Install the software.............................................................................................................................. 320
 Accept the new CSM license if required ............................................................................................ 321
 Copy the files to /csminstall .............................................................................................................. 321
 Verify the installation (optional) ......................................................................................................... 321

 Updating AIX nodes and install servers ............................................................................................. 321
 Gather updates ...................................................................................................................................... 322
 Commit previous levels of CSM software (optional) ......................................................................... 322
 Export the directory containing the updates ....................................................................................... 322
Contract with IBM Corp.
About this book

This book provides detailed information about IBM(R) Cluster Systems Management (CSM) for AIX(TM), CSM for Linux(R) Multiplatform, and CSM for Linux on POWER(TM). It provides information about the tasks required for planning and installing a CSM cluster. Certain sections of this book might not apply to your cluster environment. The size and complexity of your cluster is also a factor in using this book.

Attention!

If you are using CSM as part of a prepackaged IBM Cluster 1350(TM) solution that you purchased from IBM or an IBM solutions provider, all of the prerequisite hardware is included. Cluster 1350 hardware and networking are delivered preconfigured for using CSM.

If you are using CSM as part of an IBM Cluster 1600, see the IBM Cluster 1600 resources at http://www.ibm.com/systems/clusters/hardware/1600.html for specific cluster hardware configuration details.

Summary of changes

The following changes are documented in the CSM 1.7.0.0 library:

- CSM 1.7.0.0 provides support for AIX 6.1.
- CSM 1.7.0.0 provides support for new IBM Blue Gene/P Solution.
- CSM 1.7.0.0 introduces support for IBM POWER6 processor-based IBM Power Systems 520 and 550 server.
- CSM 1.7.0.0 introduces support for the IBM system x3350 with model type 4192, x3850(m2) with model type 7141, x3455 with model type 7940.
- CSM 1.7.0.0 provides installation enhancements, including DVD support and enhanced support for Linux diskless installation.
- CSM 1.7.0.0 provides enhancements for CSM administrative functions such as dsh utilities and CFM.
- CSM 1.7.0.0 provides enhancements to error and system monitoring and logging.

Some updates in regard to new function and support in the CSM 1.7.0.10

- CSM 1.7.0.10 provides support for AIX 6.1 TL1 and AIX 5.3 TL8
- CSM 1.7.0.10 provides support for HAMS for AIX61 TL1 working with SAM 2.3
- CSM 1.7.0.10 provides support for IBM Power Systems 575 and 595
- CSM 1.7.0.10 provides support for IBM BladeCenter JS22 and JS12
- CSM 1.7.0.10 provides support for InfiniBand Qlogic Switch

Some updates in regard to new function and support in the CSM 1.7.0.17

- CSM 1.7.0.17 provides support for AIX6.1 TL2 and AIX5.3 TL9
- CSM 1.7.0.17 provides support for Red Hat EL4.7 installation
- CSM 1.7.0.17 provides support for Red Hat EL5.2 installation
- CSM 1.7.0.17 provides support for Red Hat EL5.3 installation
- CSM 1.7.0.17 provides support for SLES10 SP2 installation
- CSM 1.7.0.17 provides support for POWER6 8234-EMA, GFW340, and HMC 7.3.4

The following change is documented in the CSM 1.7.1.0 library:

- CSM 1.7.1.0 provides support for AIX6.1 TL3 and AIX5.3 TL10
- CSM 1.7.1.0 provides support for POWER6 8203-E4A and 8204-E8A
- CSM 1.7.1.0 provides support for IBM BladeCenter JS23 and JS43

Who should use this book

This book is intended for system administrators who want to use IBM Cluster Systems Management. The CSM cluster can contain nodes running AIX, Linux, or both AIX and Linux operating systems. The system administrator should have experience in UNIX(R) administration and network systems and have the following skills:

- Understanding of most basic system administration tools and processes.
- Skills using most AIX or Linux commands and utilities where appropriate.
- Understanding of an AIX(R) 5L-based or Linux-based operating system where appropriate
- Fundamental networking and distributed computing environment concepts.

Typographic conventions

This book uses the following typographic conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>bold</td>
<td>Bold words or characters represent system elements that you must use literally, such as: command names, file names, flag names, and path names.</td>
</tr>
<tr>
<td>constant width</td>
<td>Examples and information that the system displays appear in constant-width typeface.</td>
</tr>
<tr>
<td>italic</td>
<td>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.</td>
</tr>
<tr>
<td>[item]</td>
<td>Brackets indicate optional items.</td>
</tr>
</tbody>
</table>

ISO 9000

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

See the Bibliography for:

- Additional CSM publications
- Information on contacting IBM and CSM Development

Note:
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, contact the third party directly.

Table 2. Reference information for CSM

<p>| IBM PRODUCTS AND INFORMATION: |  |
|-------------------------------|  |
| IBM Cluster Information Center | <a href="http://publib.boulder.ibm.com/infocenter/clresctr/vxrx/index.jsp">http://publib.boulder.ibm.com/infocenter/clresctr/vxrx/index.jsp</a> |
| IBM Systems Information Centers | <a href="http://publib.boulder.ibm.com/eserver/">http://publib.boulder.ibm.com/eserver/</a> |
| IBM Cluster servers | <a href="http://www.ibm.com/systems/clusters/">http://www.ibm.com/systems/clusters/</a> |
| Cluster 1350 Information Center | <a href="http://publib.boulder.ibm.com/cluster/">http://publib.boulder.ibm.com/cluster/</a> |
| IBM System x servers | <a href="http://www.ibm.com/systems/x/">http://www.ibm.com/systems/x/</a> |</p>
<table>
<thead>
<tr>
<th>Documentation</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM BladeCenter documentation</td>
<td><a href="http://www.ibm.com/systems/bladecenter/">http://www.ibm.com/systems/bladecenter/</a></td>
</tr>
<tr>
<td>IBM Linux servers</td>
<td><a href="http://www.ibm.com/systems/browse/linux/">http://www.ibm.com/systems/browse/linux/</a></td>
</tr>
<tr>
<td>IBM Systems technical support</td>
<td><a href="http://www-304.ibm.com/jct01004c/systems/support/">http://www-304.ibm.com/jct01004c/systems/support/</a></td>
</tr>
</tbody>
</table>

**THIRD-PARTY PRODUCTS AND INFORMATION:**

<table>
<thead>
<tr>
<th>Product</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat Enterprise Linux</td>
<td><a href="http://www.redhat.com">http://www.redhat.com</a></td>
</tr>
<tr>
<td>SUSE Linux Enterprise Server (SLES)</td>
<td><a href="http://www.novell.com/products/server/">http://www.novell.com/products/server/</a></td>
</tr>
<tr>
<td>Virtual LAN (VLAN) documentation</td>
<td><a href="http://standards.ieee.org/">http://standards.ieee.org/</a></td>
</tr>
<tr>
<td>conserver serial console application</td>
<td><a href="http://www.conserver.com/">http://www.conserver.com/</a></td>
</tr>
<tr>
<td>MRV IR-8000 information</td>
<td><a href="http://www.mrv.com/product/MRV-IR-003">http://www.mrv.com/product/MRV-IR-003</a></td>
</tr>
<tr>
<td>MRV LX-4000 information</td>
<td><a href="http://www.mrv.com/product/MRV-IR-008">http://www.mrv.com/product/MRV-IR-008</a></td>
</tr>
<tr>
<td>Avocent ESP and CPS support</td>
<td><a href="http://www.avocent.com/web/en.nsf/Content/ProductUpgradesLanding">http://www.avocent.com/web/en.nsf/Content/ProductUpgradesLanding</a></td>
</tr>
<tr>
<td>Altura IntelliServer information</td>
<td><a href="http://www.alturaxl.com/Products/console_management.html">http://www.alturaxl.com/Products/console_management.html</a></td>
</tr>
<tr>
<td>American Power Conversion (APC) MasterSwitch information</td>
<td><a href="http://www.apc.com/products/family/index.cfm?id=70">http://www.apc.com/products/family/index.cfm?id=70</a></td>
</tr>
<tr>
<td>Linux Documentation Project</td>
<td><a href="http://en.tldp.org/">http://en.tldp.org/</a></td>
</tr>
</tbody>
</table>
Bibliography

This bibliography includes documentation resources for Cluster Systems Management (CSM) and IBM contact information.

The following Web sites allow you to view or download information about or related to CSM:

- Cluster Information Center: includes publications for CSM, RSCT, Cluster 1600, and other clusters products. See http://publib.boulder.ibm.com/infocenter/clresctr/vxrx/index.jsp
- AIX 6.1 Information Center. See http://publib.boulder.ibm.com/infocenter/systems/scope/aix/index.jsp
- Clusters 1350 Information Center. See http://publib.boulder.ibm.com/cluster/

Redbooks

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


CSM product information

See the following resources for CSM information:


Getting help from IBM

Before you call for help, verify that the latest service updates have been applied to your systems. Also check the CSM for AIX and Linux: Administration Guide to 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 contain all the service bulletins and flashes, as well as PTF and APAR reports for all current releases of CSM:


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 CSM product numbers are:
   - 5765-F67 (CSM for AIX 5.3 and later)
   - 5765-E88 (CSM for Linux Multiplatform)
   - 5765-G16 (CSM for Linux on POWER)
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 AIX support is **1-800-CALL-AIX**.

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

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.
Chapter 1. CSM overview

Cluster Systems Management (CSM) software provides a distributed systems management solution that allows a system administrator to set up and maintain a cluster of nodes that run the AIX or Linux operating system. CSM simplifies cluster administration tasks by providing management from a single point-of-control. CSM can be used to manage homogeneous clusters of servers that run Linux, homogeneous servers that run AIX, or mixed clusters which include both AIX and Linux.

CSM supports the following IBM hardware for your CSM management server, install servers, and nodes:

**CSM for AIX and CSM for Linux on POWER:**
IBM System p servers: System POWER 6, System p5\(^{\text{TM}}\), pSeries, BladeCenter JS, eServer OpenPower\(^{\text{TM}}\)

**CSM for Linux Multiplatform:**
IBM System x servers: System x, xSeries\(^{\text{R}}\), BladeCenter HS and LS, and eServer 325, 326, and 326m

The CSM management server is the server designated to operate, monitor, and maintain the CSM cluster. Install servers are the servers used to install cluster nodes. By default, the management server is the install server; separate install servers are also supported. Managed nodes are instances of the operating system that you can manage in the cluster. Managed devices are the non-node devices for which CSM supports power control and remote console access. For hardware and software support information, see Planning for CSM software.

Managing a CSM cluster

CSM enables system administrators to manage a number of system management challenges. Some of the tasks you can perform from the management server are:

- Installing and updating operating system software on cluster nodes
- Installing and updating CSM, RSCT, and optional software on cluster nodes
- Running distributed commands across the cluster
- Synchronizing files across the cluster
- Running user-provided customization scripts during node installation or updates
- Monitoring the cluster nodes and devices
- Controlling cluster hardware
- Managing node or device groups
- Running diagnostic tools
- Configuring additional network adapters.

Installing and updating software on the cluster nodes

From the CSM management server, you can install the AIX or Linux operating system on the nodes and add them to the CSM cluster. You can also install and update CSM software and application software on
cluster nodes. CSM also contains support for installing and managing diskless nodes using Warewulf and Yellow dog Updater, Modified (YUM) open source software.

**Running distributed commands across the cluster**

As an administrator, you can run commands in parallel across cluster nodes and gather output using the `dsh` (distributed shell) command. You can set up `dsh` to use either `rsh` (UNIX basic remote shell) or `ssh` (secure shell). In addition, you can use CSM to set up Kerberos Version 5 `rsh` or `ssh` for AIX or Linux.

For general information about CSM and Kerberos, see CSM for AIX Kerberos setup and CSM for Linux Kerberos setup.

For Kerberos options, see Set up Kerberos Version 5 for CSM for AIX remote command processing (optional) and Set up Kerberos Version 5 for remote Linux command processing (optional).

**Synchronizing files across the cluster**

The **configuration file manager (CFM)** provides a repository for synchronizing configuration files across the cluster nodes. CFM works by storing all shared configuration files in one location on the management server and automatically propagating changes to these files throughout the cluster. As a result, you only need to update files once, on the management server, instead of manually updating all the cluster nodes.

With CFM you can configure applications, set up services, and perform basic management tasks in the cluster. CFM allows different sets of files to be distributed to different sets of nodes or node groups, and the files on the nodes do not have to be the same as the files on the management server.

If you plan to use CSM Configuration File Manager (CFM) in a mixed cluster environment to synchronize files on the management server with the managed nodes, you must take additional steps and note the format and location of those files on both AIX and Linux. For example, the format and content of `/etc/passwd` file are different on AIX and Linux.

For more information about CFM, see the CSM for AIX and Linux: Administration Guide.

**Running user-provided customization scripts**

CSM provides support for automatically running user-provided customization scripts on the cluster nodes. You can run the scripts when you install nodes or when you update nodes through the CSM `updatenode` command.

Also see the **Optional tools and services** in the CSM for AIX and Linux: Administration Guide for other sample scripts.

**Monitoring the cluster nodes**

CSM allows an administrator to set up monitoring for various conditions across nodes or node groups, and designate specific actions to be run in response to events that occur in the cluster. For monitoring, CSM uses the **Resource Monitoring and Control (RMC)** application, which is part of RSCT (Reliable
Scalable Cluster Technology). RMC offers a comprehensive set of monitoring and response capabilities that lets you detect, and in many cases correct, system resource problems such as a critical file system becoming full. You can monitor virtually all aspects of your system resources and specify a wide range of actions to be taken when a problem occurs, from simple notification by e-mail to recovery that runs a customized script.

The conditions that you can monitor include

- Network reachability
- Power status
- Status of applications or daemons running on a node (whether they are up or down)
- CPU, memory, and file system utilization.

Actions that you can designate to be run in response to the occurrence of one of these conditions (an event) include:

- Commands that can be run on the management server or any node of the cluster
- Notifications such as logging, e-mailing, or paging
- Recovery actions for cleaning up file systems that are filling up, restarting applications that go down, generating an SNMP trap that you can use to forward event information to consoles, and so on.

Predefined conditions and predefined responses are included with CSM, and you can customize these conditions and responses.

For more information about monitoring with CSM, see CSM for AIX and Linux: Administration Guide.

**Controlling cluster hardware**

The hardware control software of CSM allows an administrator to power on, power off, reboot, bring up the remote hardware console, and query the nodes and devices of the cluster from a single point-of-control: the CSM management server. Cluster hardware control commands are run on the CSM management server. For planning information about hardware control with CSM, see Planning for cluster hardware.

For HMC-attached System p nodes, including OpenPower, Cluster-Ready Hardware Server (CRHS) enables hardware discovery, HMC to server assignment, and server processor password management from the CSM management server. See Planning for Cluster-Ready Hardware Server (CRHS).

**Managing node and device groups**

As a system administrator, you can create node or device groups within the cluster that can be managed and monitored as distinct entities. You can define node or device groups as a static set of nodes or static set of devices, or as a dynamic set of nodes or a dynamic set of devices. Static node or device groups are created by explicitly specifying names, group names, or both. When you define a dynamic group, you can designate a particular characteristic for those nodes. For example, you can create a node group for a specific type of hardware and then monitor that node group. If a new machine of that hardware type is added to the cluster, monitoring will automatically start for that machine. For more information about creating and using node groups, see the CSM for AIX and Linux: Administration Guide.
Running diagnostic tools

CSM includes a set of diagnostic probes that administrators can use to check the health of specific software functions and identify the cause of system problems. You can set up these probes to run periodically, or automatically as a response to a condition occurring in the system. CSM also provides support for you to create your own probes. For more information about using the CSM probes, see *CSM for AIX and Linux: Administration Guide*.

Configuring additional network adapters

CSM supports the configuration of secondary network adapters during a node installation or when updating a node with the CSM `updatenode -c` command. Secondary adapters are any additional adapters, other than the ones that are used to do a remote network installation of the node. For more information, see *Secondary adapter interface configuration*.

Communicating with CSM

CSM offers you several options for issuing commands to the cluster:

- Command line interface
- Distributed Command Execution Manager (DCEM)
- IBM Web-based System Manager
- SMIT

Command line interface

CSM includes command line interfaces for all CSM functions. The command line interface allows you to access all the resources in the system, the attributes of those resources, and state values. It also allows you to query and control the nodes, file systems, CPU and memory statistics, global cluster parameters, and so on. For more information about the CSM commands, see the *CSM for AIX and Linux: Command and Technical Reference*.

Distributed Command Execution Manager (DCEM)

The Distributed Command Execution Manager (DCEM) graphical user interface allows you to construct command specifications for running commands on multiple target machines, while providing real-time status as commands are run. DCEM allows you to perform the following functions:

- Enter the command definition, run time options, and selected hosts and groups for a command specification
- Save command specifications for future use
- Create and modify node groups to use as targets for a command directly from DCEM.

For information about DCEM, see the *CSM for AIX and Linux: Administration Guide*.
IBM Web-based System Manager

The IBM Web-based System Manager is a graphical user interface application for managing and monitoring a cluster. It provides point-and-click control of objects as an alternative to learning and using AIX commands. For more information about using the Web-based System Manager, see the *CSM for AIX and Linux: Administration Guide*.

SMIT

System Management Interface Tool (SMIT) panels are currently provided with CSM for AIX for installation, setup, hardware control functions and for most CSM commands.
Chapter 2. Planning for cluster hardware

Using CSM involves tasks such as creating a CSM management server, defining cluster nodes, and adding nodes to a cluster. You might also be installing nodes, creating device definitions, and creating CSM install servers. Before you create your cluster definitions, you must decide which hardware to use for each cluster component. Your choice of cluster hardware can be affected by your choice of other cluster options, including operating systems, hardware control, install servers, diskless nodes, and hierarchical CSM.

Parallel Systems Support Program (PSSP) and CSM non-compatibility

PSSP must not be installed on the management server or any of the cluster nodes. Coexistence between PSSP and CSM is not supported.

Scaling

The CSM scaling limit for System p nodes is 512 and 1024 nodes for all other servers; each operating system (OS) image is one node. Node OS images can be AIX or Linux on IBM System x or System p hardware.

Planning for a CSM for AIX management server

The following requirements apply to the management server:

- Your management server must have a CD-ROM, DVD-ROM, or DVD-RAM drive.
- The CSM for AIX management server must be a model supported with AIX Version 5.3, or later.
- A sufficient number of network adapters are required to accommodate the required management, cluster and public VLANs. For information on the network options and requirements, see the Hardware and network requirements.

Memory and disk space requirements

On the management server, a minimum of 512 MB of memory and 250 MB of disk space is required for installing CSM. When using an AIX CSM management server to manage and install Linux nodes, an additional 100 MB of space is required in the /var directory. Additional disk space on the management server is required to support installation of the AIX operating system and CSM on the managed nodes. Typically, each version of AIX requires a minimum of 2.0 GB of disk space.
Network requirements

You must create one or more virtual local area networks (VLANs) for the CSM management server and hardware control points, and one or more separate VLANs for the CSM management server and cluster nodes. The VLAN used for the management server and the hardware control points is called the management VLAN. The VLAN used for the management server and the nodes is called the cluster VLAN. 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. For more information about network requirements, see Hardware and network requirements. For more information on VLANs, see Virtual LANs (VLANs).

If you have more than one gateway between a System p install server and the nodes it serves, set up the gateway closest to the node. For example, if the install server is connected to gateway A, gateway A connected to gateway B, and gateway B connected to the nodes, add the arp entries and the dhcp-relay daemon to gateway B. For more information, see Cluster configurations using install servers.

For examples of cluster network configurations, and how they affect the node attributes and the installation, see Setting up install servers.

If you are using a Linux install server, see Planning for CSM for Linux install servers.

Security guidelines

For security guidelines, see the CSM for AIX and Linux: Administration Guide and the IBM RSCT: Administration Guide.

Using an LPAR management server

You can use a logical partition (LPAR) as your CSM management server, with the following restrictions and limitations:

1. An HMC-attached System p management server can be powered down inadvertently by an HMC user deactivating the LPAR. Even without access to the CSM management server, a user with access to the attached HMC can power off the management server or move resources, such as CPU or I/O, from the LPAR.
2. If the firmware needs to be upgraded, the LPAR management server might also go down when the system is quiesced. However, bringing the CEC back up returns the system to normal.
3. There is no direct manual hardware control of the CSM management server. You must use the HMC for power control of the management server.
4. An LPAR management server cannot have an attached display. This limitation can affect the performance of your CSM GUIs.
5. You can assign a CD-ROM, DVD-ROM, or DVD-RAM drive to the management server LPAR on the CEC.
6. Do not define an LPAR management server as a managed node.
7. A cluster that is installed and configured can still function even if the management server goes down. For example, cluster applications can continue to run, and cluster nodes can be rebooted. However, tasks including monitoring, automated responses, and scheduled file and software updates cannot continue while the management server is down. For details on using a backup
management server, see the HA MS information in the *CSM for AIX and Linux: Administration Guide*.

8. You cannot manage 9076 SP(TM) Nodes or 7026 servers from an LPAR management server.

**Planning for CSM for AIX install servers**

Install servers are CSM nodes that provide basic operating system installation services and NFS file services during CSM node installations. Install servers provide improved scaling for installing large clusters, and support for mixed cluster environments.

An AIX install server is a NIM master that is used to install AIX on CSM nodes. Your AIX management server can also be your AIX install server. However, you may need to set up a separate AIX install server if you want to install AIX nodes at a later operating system level than exists on the CSM for AIX management server. NIM requires that the NIM master be at the same or later level of AIX as the level to be installed on the NIM clients. You will also need an AIX install server if you have a Linux management server and you want to install operating systems on your AIX nodes in an mixed cluster.

The requirements for CSM for AIX install servers are the following:

- The AIX install server model must be supported for AIX Version 5.3, or later, and CSM 1.6, or later.
- A sufficient number of network adapters are required to accommodate the network installation of all nodes to be served by this install server; see Network requirements.
- The nodes must be network connected to the install server directly through a local subnet, or indirectly through a gateway.
- A minimum of 512 MB of memory and 250 MB of disk space is required for CSM. Additional disk space is required to support the installation of the AIX operating system and CSM on the nodes to be served by this install server. Typically, each version of AIX requires a minimum of 2.0 GB of disk space.

The install server operating system determines the operating system that can be installed on a node, as shown in Table 27. For install server details, see Setting up install servers.

**Planning for CSM for AIX nodes**

On each managed node, a minimum of 256 MB of memory and 20 MB of disk space is required for CSM, and the required amount of additional disk space for the operating system and RPM packages that you choose to install.

CSM supports the following hardware for AIX nodes:

- IBM System p5: 505, 505Q, 510, 510Q, 520, 520Q, 550, 550Q, 560Q, 570, 575, 590, and 595
- IBM BladeCenter: JS20-8842, JS21-8844, JS22-7998, JS12-7998, JS23-7778, JS43-7778
- IBM pSeries: 615, 630, 650, 655, 670, and 690
Compatibility with Advanced POWER Virtualization

CSM is fully compatible with any of the Advanced POWER Virtualization features that are available for System p5 and POWER 6. The Advanced POWER Virtualization features include the following components:

- Firmware enablement for micro-partitioning
- Installation image for the Virtual I/O Server software which supports:
  - Shared ethernet adapter
  - Virtual SCSI server
  - Partition load manager

Planning for a CSM for Linux management server

CSM for Linux on Multiplatform and CSM for Linux on POWER management servers are supported on the following hardware and Linux distributions:

- Linux on System x
- Linux on x86 eServer and BladeCenter
- Linux on System p

Note:
Your management server must have a CD-ROM, DVD-ROM, or DVD-RAM drive.

Memory and disk space requirements

A minimum of 512 MB of memory and 250 MB of disk space is required to install CSM on your management server. An additional 100 MB of space is required in the /var directory on a Linux management server that installs and manages Linux nodes of a different architecture - for example, a System x management server and a System p install server and nodes. Each version of the Red Hat EL or SLES operating system installed on the nodes also requires additional space in the /csminstall directory; each Linux OS CD requires approximately 700 MB.

Network requirements

Create one or more virtual local area network (VLAN) for the CSM management server and hardware control points, and one or more 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. For more information about network requirements, see Hardware and network requirements. For more information on VLANs, see Virtual LANs (VLANs).
Security guidelines

For security guidelines, see the *CSM for AIX and Linux: Administration Guide* and the *IBM RSCT: Administration Guide*.

Planning for CSM for Linux install servers

Install servers are CSM nodes that provide basic operating system installation services and NFS file services during CSM node installations. Install servers provide improved scaling for installing large clusters, and support for mixed cluster environments.

A Linux install server provides the DHCP, PXE or BOOTP, TFTP, HTTP and NFS services to install the Linux operating system on CSM nodes. Your Linux management server can also be your Linux install server. However, you must set up a separate Linux install server to install a different Linux distribution on your nodes, or to install Linux on nodes with a different hardware architecture. A Linux install server is also required to install Linux on nodes from an AIX management server. The requirements for a Linux install server are similar to those for a Linux management server:

- The Linux install server model must be supported in CSM 1.6.0, or later.
- A Linux install server must be running CSM 1.6.0, or later, before using it to install nodes.
- A sufficient number of network adapters are required to accommodate the network installation of all nodes to be served by this install server. See Network requirements.
- For Linux installations, the nodes must be network connected to the install server directly through a local subnet, or indirectly through one or more gateways. If the nodes are connected through gateways, you must do the following:
  - On the install server, add a stanza containing the node's subnet to the `/etc/dhcpd.conf` file.
  - On the gateway closest to the node, configure and enable the `dhcp-relay` daemon.
  - For Linux on POWER only, on the gateway closest to the node, add a permanent `arp` entry for each node and configure and enable the `dhcp-relay` daemon.
- For Linux on System x installations, the nodes must be network connected to this install server directly through a local subnet.
- For Linux on System x installations, you can have multiple install servers on the same subnet to improve performance.
- A minimum of 512 MB of memory and 256 MB of disk space is required for CSM. Additional disk space is required to support the installation of the Linux operating system and CSM on the nodes to be served by this install server. Typically, each version of Red Hat EL or SLES requires a minimum of 100 MB of disk space.

The operating system running on an install server determines which operating system can be installed on a node, as shown in Considerations for mixed clusters.

See Setting up install servers for more information.

Planning for CSM for Linux nodes

Each Managed Linux node requires a minimum of 128 MB of memory and 20 MB of disk space for CSM, and additional disk space for the operating system and RPM packages.
System p hardware support for Linux

The following System p hardware is supported for Linux:

- IBM System p5: 505, 505Q, 510, 510Q, 520, 520Q, 550, 550Q, 560Q, 570, 575, 590, and 595
- IBM pSeries: 615, 630, 650, 655, 670, and 690
- IBM OpenPower: 710 and 720
- IBM BladeCenter: JS20-8842, JS21-8844, JS22-7998, JS12-7998, JS23-7778 and JS43-7778

For compatibility information see Compatibility with Advanced POWER Virtualization.

System x hardware support for Linux

The following IBM System x hardware is supported for Linux:

- IBM System x 3455, 3550, 3650, 3655, 3755
- IBM xSeries 335, 336, 345, 346, 360, 366, 445

eServer and BladeCenter hardware support for Linux

The following eServer and BladeCenter hardware is supported for Linux:

- IBM eServer(TM) 325, 326, and 326m
- BladeCenter HS20 (7981, 8678, 8832, and 8843), HS21 (7795, 8853), and HS40 (8839)
- BladeCenter JS20 (8842), JS21 (8844), JS22 (7998), JS23(7778) and JS43(7778)
- BladeCenter LS20 (8850), LS21 (7971), and LS41 (7972)

For BladeCenter product information, see: http://www.ibm.com/servers/eserver/bladecenter/index.html.

For BladeCenter remote console details, see Using remote console on BladeCenter.

Install server and node hardware

Any supported hardware can be used as a CSM management server, but there are limitations on install server hardware support for installing different node hardware types. A management server acting as an install server has the same hardware restrictions as separate install servers. The following table illustrates the supported hardware combinations for install servers and the nodes they can install. In Table 3, YES indicates that an install server on the specified hardware can install a node on the specified hardware. NO means the install server cannot install a node on the specified hardware.

Table 3. Install server and node hardware

<table>
<thead>
<tr>
<th>Install server</th>
<th>Install server can install</th>
</tr>
</thead>
<tbody>
<tr>
<td>System x, xSeries, eServer</td>
<td>System POWER 6, System p5, BladeCenter HS, LS, BladeCenter JS</td>
</tr>
</tbody>
</table>
The following tables summarize hardware support for Red Hat EL and SLES distributions in a CSM cluster. Each table indicates the Linux distributions and architectures that can run on the specific hardware.

- Linux on System x
- Linux on x86 eServer and BladeCenter
- Linux on System p

### Linux on System x

The following table summarizes System x hardware support for Red Hat EL and SLES. Support includes Quarterly Updates (QU) for the specified Red Hat EL version, and Service Packs (SP) for the specified SLES version. An X indicates the Linux distribution is supported on the management server, install servers, and nodes.

#### Table 4. Linux distribution support on System x

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Architecture</th>
<th>x335, x345</th>
<th>x336, x346,</th>
<th>x360, x445</th>
<th>x366, x3455, x3550, x3650, x3655, x3750</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat EL 5-Server</td>
<td>x86 32 bit</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Red Hat EL 5-Server</td>
<td>x86 64 bit</td>
<td>not supported</td>
<td>X</td>
<td>not supported</td>
<td>X</td>
</tr>
<tr>
<td>Red Hat EL 5-Client</td>
<td>x86 32 bit</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Red Hat EL 5-Client</td>
<td>x86 64 bit</td>
<td>not supported</td>
<td>X</td>
<td>not supported</td>
<td>X</td>
</tr>
<tr>
<td>Red Hat EL AS 4 ¹</td>
<td>x86 32 bit</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Red Hat EL AS 4 ²</td>
<td>x86 64 bit</td>
<td>not supported</td>
<td>X</td>
<td>not supported</td>
<td>X</td>
</tr>
<tr>
<td>Red Hat EL ES 4</td>
<td>x86 32 bit</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
The following table summarizes x86 eServer and BladeCenter hardware support for Red Hat EL and SLES. Support includes Quarterly Updates (QU) for the specified Red Hat EL version, and Service Packs (SP) for the specified SLES version. An X indicates the Linux distribution is supported on the management server, install servers, and nodes.

Table 5. Linux distribution support on x86 eServer and BladeCenter

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Architecture</th>
<th>eServer 32*</th>
<th>BladeCenter HS 4</th>
<th>BladeCenter LS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat EL 5-Server 1</td>
<td>x86 32 bit</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Red Hat EL 5-Server</td>
<td>x86 64 bit</td>
<td>X</td>
<td>not supported</td>
<td>X</td>
</tr>
<tr>
<td>Red Hat EL 5-Client</td>
<td>x86 32 bit</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Red Hat EL 5-Client</td>
<td>x86 64 bit</td>
<td>X</td>
<td>not supported</td>
<td>X</td>
</tr>
<tr>
<td>Red Hat EL AS 4 2</td>
<td>x86 32 bit</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Red Hat EL AS 4</td>
<td>x86 64 bit</td>
<td>X</td>
<td>not supported</td>
<td>X</td>
</tr>
<tr>
<td>Red Hat EL ES 4</td>
<td>x86 32 bit</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Red Hat EL ES 4</td>
<td>x86 64 bit</td>
<td>X</td>
<td>not supported</td>
<td>X</td>
</tr>
<tr>
<td>Red Hat EL WS 4 3</td>
<td>x86 32 bit</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Red Hat EL WS 4 3</td>
<td>x86 64 bit</td>
<td>X</td>
<td>not supported</td>
<td>X</td>
</tr>
<tr>
<td>SLES 9</td>
<td>x86 32 bit</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>SLES 9</td>
<td>x86 64 bit</td>
<td>X</td>
<td>not supported</td>
<td>X</td>
</tr>
<tr>
<td>SLES 10</td>
<td>x86 32 bit</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>SLES 10</td>
<td>x86 64 bit</td>
<td>X</td>
<td>not supported</td>
<td>X</td>
</tr>
</tbody>
</table>
Red Hat EL 5 support (Server and Client) includes support for Red Hat EL 5, Red Hat EL 5.1, Red Hat EL 5.2 and Red Hat EL 5.3.

Red Hat EL 4 support (AS, ES, and WS) includes support for Red Hat EL 4, Red Hat EL 4.5, Red Hat EL 4.6 and Red Hat EL 4.7.

Red Hat EL WS 4 is supported on cluster nodes only.

The HS20(8843) and HS21 blades supports x86 64 bit.

**Linux on System p**

The following table summarizes CSM support for Red Hat EL and SLES on System p hardware. Support includes Quarterly Updates (QU) for the specified Red Hat EL version and Service Packs (SP) for the specified SLES version. An X indicates the Linux distribution is supported on the management server, install servers, and nodes.

**Table 6. Linux distribution support on System p hardware**

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Architecture</th>
<th>System p5 505, 510, 520, 520Q, 550, 550Q, 570, 590, 595</th>
<th>System POWER 6 520, 550, 560, 575, 595</th>
<th>OpenPower 710, 720</th>
<th>BladeCenter JS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat EL 5-Server1</td>
<td>POWER (ppc)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Red Hat EL AS 42</td>
<td>POWER (ppc)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X3</td>
</tr>
<tr>
<td>SLES 9</td>
<td>POWER (ppc)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>SLES 10</td>
<td>POWER (ppc)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

Red Hat EL 5 support (Server and Client) includes support for Red Hat EL 5, Red Hat EL 5.1, Red Hat EL 5.2 and Red Hat EL 5.3.

Red Hat EL 4 support (AS) includes support for Red Hat EL 4, Red Hat EL 4.5, Red Hat EL 4.6 and Red Hat EL 4.7.

RHEL4 AS (ppc) on BladeCenter JS21 is only supported with Quarterly Update 3 (QU3), or later.
Planning for Cluster-Ready Hardware Server (CRHS)

Cluster Ready Hardware Server (CRHS) software enhances control over HMC-attached System p and OpenPower servers. CRHS enables access to multiple HMCs and other functions that simplify communication across the hardware service network. These include:

- Hardware discovery. See Hardware discovery component of CRHS.
- A central database for cluster hardware information. See Shared repository component of CRHS.
- An updated hardware server daemon. Hardware server daemon component of CRHS.
- Installation and password setup for managed servers. See Password management component of CRHS.

CRHS is required in clusters that use the IBM High Performance Switch (HPS). CRHS is also supported in clusters that do not use an HPS. CRHS provides:

- Consolidation of service networks into a maximum of two subnets for redundancy
- Reduced HMC requirements for recovery
- Automated discovery and database management for System p5 servers and HMCs
- Automated association of System p 575, 590, and 595 servers with their frames
- Ease of movement for System p5 servers across HMCs
- Shared repository of System p cluster hardware information
- Reduced number of DHCP servers for larger clusters.

Note:
HPS is not supported with any POWER 6 servers at this time.

Limitations:
For POWER 5, CRHS is only supported on System p, OpenPower, and HMCs, running system firmware level SF230, or later. POWER5(TM) servers and HMCs, running system firmware levels earlier than SF230, are not supported. Any POWER4(TM) servers must be isolated on HMCs that do not use CRHS.

See the CSM for AIX and Linux: Administration Guide for detailed information on CRHS.

Hardware discovery component of CRHS

From the CSM management server you can use the command line interface to the hardware server discovery agent (HSDA) to discover all of the above hardware that is connected to the management server on the service LAN. This may be used in the initial configuration to find the HMCs and System p servers. Once the HMCs are discovered, you can define the HMCs that will participate in the cluster and will share a single repository containing the information for all of the hardware that has been discovered.

Note that a service VLAN is also called a management VLAN or a service network in CSM documentation.
Shared repository component of CRHS

Once all of the hardware is discovered, you can identify which frames will be supported by HMCs that will be part of the CRHS. A command is used to create a shared repository on each HMC that you select to be included. Once this is done the HSDA begins polling for the hardware, and it automatically adds to the shared repository all of the hardware found. This information is listed and modified from the management server with CLIs.

Hardware server daemon component of CRHS

The hardware server daemon provides the software management of the CRHS. The daemon connects to and communicates with the service processors in the System p servers. It exists on all HMCs and is used by the HMC to connect and communicate with the System p servers. In an HPS environment, a hardware server daemon also runs on the management server to enable the HPS network manager (HPSNM), an interface to the servers' service processors. The hardware server daemon uses the information in the shared repository to determine which servers are managed by the HMC on which the daemon is running. When an HMC is part of the shared repository, the daemon runs in cluster mode. When an HMC is not part of the shared repository, it runs in stand-alone mode.

Password management component of CRHS

The `systemid` command allows you to set the password for the System p service processor. It can also initiate the current password for an existing system. In both cases, the password is encrypted and stored within the repository. This is done so that the hardware service daemon can login and provide other applications, such as the HMC and the HPSNM, access to the hardware.

CRHS network planning

System POWER 6/p5 575, 590, and 595 servers have two network connections for each CEC server service processor (SP) and frame bulk power assembly (BPA). Known as the A and B sides of the SP and BPA, they provide redundant connections in case of failure. The networking configuration requires each side to be on a separate LAN, and to be connected to the HMC and the management server. These two LANs are called the service networks, because the applications that use the networks provide the access required to service the systems. CRHS service networks must connect the A and B sides of the SP to the CSM HMCs and management server.

In previous configurations, the HMC was connected to at least one of the service networks, and provided the DHCP server and addresses for the connected SP and BPA. A second HMC with a DHCP server provided IP addresses for the other side of the SP and BPA on the network. In large clusters, this configuration can require many subnets, each with one or two HMCs for redundant connectivity. With CRHS, the model has been consolidated to only one DHCP server, which can service either a single service network or two service networks when configured for redundancy.

Planning the service network

The service network is the network that connects the servers and frames to the HMC and the management server. In a cluster the HMC and management servers have network interfaces on the service network.
which are used to connect them into the embedded service processors contained in each frame or server. The control or management of frames is accomplished over this network.

The service network must be a single subnet with all elements of the cluster attached. Most frames contain two hubs that allow that frame to be joined to the service networks. Internal to the frame are two networks, and by plugging the A side into the hub you can join the frame to the greater service network with other frames.

The support of Cluster Ready Hardware Server (CRHS) redundancy working with POWER6 575/595 frame and servers requires only one active network connection to be used in the cluster service network that is connected between CSM MS, HMCs, POWER6 575/595 Frame BPA, and POWER6 575/595 server FSP. This change is based on the design modification of the POWER6 Frame Bulk Power Controller (BPC) internal network that is now providing the redundancy support to the Frame BPA and Server FSP. The configuration of having two active network connections from the POWER6 575/595 frame and servers to the HMC and CSM MS may cause SLP network issues working with CRHS.

---

**Using hardware control software**

CSM hardware control software provides remote hardware control functions for cluster nodes and devices from a single point of control. CSM allows you 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, Web-based System Manager graphical user interface (GUI), System Management Interface Tool (SMIT) panels, or the DCEM graphical user interface.

CSM supports hardware control for non-node devices, and provides power control and where applicable, remote console access for a wide range of devices such as hardware control points, external console servers, and remote supervisor adapters. The predefined dynamic device group `AllDevices` includes all defined devices.

CSM hardware control functions depend on specific hardware, software, network, and configuration requirements. The requirements for remote power are separate and distinct from the requirements for remote console. 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 AIX supports remote hardware control for System p, System x nodes from an AIX management server, including BladeCenter JS, and eServer OpenPower 710 and 720.

Hardware control commands can be run on the AIX management server to simultaneously control both AIX and Linux nodes in a mixed cluster. See the *CSM for AIX and Linux: Administration Guide* for a complete description of CSM mixed clusters.

CSM for Linux supports remote hardware control for System x and System p nodes from a Linux management server, including BladeCenter HS and LS, and eServer 325, 326, and 326m.

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

`chbmcconsusr`

*CSM for AIX and Linux: Planning and Installation Guide*
Defines a remote console user name for node BMCs.

**chhwdev**
Changes a device definition in the CSM database.

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

**chsnmp**
Sets the SNMP agent configuration information for System x servers.

**definehwdev**
Defines the devices in a CSM cluster.

**getadapters**
Collects information for LAN adapters.

**hwdevgrp**
Manages device group definitions in the CSM database.

**lsbmcconsusr**
Returns the remote console user names for node BMCs.

**lshwdev**
Lists the device definitions in the CSM database.

**lshwinfo**
Collects node information from one or more hardware control points.

**lshwstat**
Collects environmental and Vital Product Data (VPD) information from System x servers. This command is not supported for CSM for Linux on System p.

**lssnmp**
Collects SNMP agent configuration information from System x servers.

**netboot**
Initiates a network boot and install of an AIX node over the CSM cluster network.

**rconsole**
Opens a remote console for a node.

**rconsolerefresh**
Refreshes the Conserver daemon.

**reventlog**
Collects service processor log information for System x servers.

**rmhwdev**
Removes device definitions from the CSM database.

**rpower**
Boots, resets, powers on and off, and queries nodes, devices and CECs.

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

## Hardware control attributes

To use CSM hardware control, you must define the hardware-related attributes for the applicable nodes and devices. In some cases default values are provided. If these defaults are acceptable, you do not need to provide the attribute values when you define the node or device.

The supported node hardware control attribute values are described in [Hardware control attributes](#).

The supported device hardware control attribute values are described in [Defining devices](#).
Hardware and network requirements

CSM for AIX or Linux hardware control depends on specific hardware and network requirements. 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. For the specific cluster architectures required, see Planning for CSM for AIX nodes. See Hardware configuration for model-specific hardware control configuration requirements.

Note:
To perform hardware control on HMC-attached System p servers, Hardware Management Console (HMC) for System p version 3 release 1.0 or later is required. The HMC can be used to partition physical System p servers into multiple logical partitions (LPARs), or nodes, each containing its own operating system image.

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.

Create one or more VLANs for the CSM management server, managed devices, and hardware control points, and one or more 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 refer to VLANs as defined by IEEE standards - see http://standards.ieee.org/ for details. The management, cluster, and public VLANs, 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. The management VLAN, or network, is also referred to as the service VLAN, or network.

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.

For more information, see Conceptual diagrams.
Hardware control overview

CSM 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 are on the management virtual LAN (VLAN) and connected to the hardware that ultimately controls the power functions.

The supported hardware control points are:

- HMC (Hardware Management Console) for HMC-attached System p nodes
- IVM (Integrated Virtualization Manager) for IVM-managed System p nodes
- Management Module for BladeCenter nodes
- RSA (Remote Supervisor Adapter) for System x nodes
- BMC (Baseboard Management Controller) for System x 336, 346, 3455, 3550, 3650, 3655 and 3755 nodes
- FSP (Flexible Service Processor) for System p5 direct attach nodes
- APC (American Power Conversion) MasterSwitch for devices that do not have another hardware control point such as an RSA and require the APC MasterSwitch

Remote power software and configuration describes the remote power configurations for your cluster when you are using hardware control.

CSM 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. (See Virtual LANs (VLANs).) 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.

For HMC-attached System p servers, the HMC is the remote console server. System x servers can use any of the following console servers:

- MRV IR-8020, IR-8040, LX-4008S, LX-4016S, and LX-4032S
- Avocent CPS1600
- Cyclades AlterPath ACS48

For System p servers that are not attached to an HMC, remote console is supported using the flexible service processor (FSP); no additional console device is required. For IVM-managed System p servers, remote console is supported using the IVM; no additional console device is required.

BladeCenter HS20-8678 blade servers that are part of an IBM 1350 Cluster require the 1350 Serial Port Module (SPM) option in order to support remote console. The SPM must be connected to an MRV IR-8020 or IR-8040 console server. HS20-8678 blade servers that are not part of a 1350 Cluster, or that do not have the SPM option, cannot support remote console. Consoles for these servers may be viewed, one at a time, by accessing the Management Module's Web interface and selecting "Remote Control" from the "Blade Tasks" list.

BladeCenter JS, HS (except for the HS20-8678), and LS blade servers support remote console through the Ethernet Switch Module, using Serial Over LAN (SOL). Refer to your BladeCenter documentation for information on enabling and configuring SOL. To ensure maximum reliability, verify that the most up-to-date firmware is installed for the following components:
• BladeCenter HS20-8677 chassis: Management Module and Ethernet Switch Module
• BladeCenter HS (except for HS20-8678), JS, and LS blade servers: Flash BIOS and Integrated Systems Management Processor (ISMP)

You can view the installed versions of these components in the Management Module's Web Interface by selecting "Firmware VPD" from the "Monitors" navigation panel. For information on the latest versions, see the IBM systems support Web page, at: http://www-304.ibm.com/jct01004c/systems/support/. See your BladeCenter documentation for information on updating firmware levels.

All System x 336/346/e326m and later server nodes also support remote console via SOL. For these servers, remote consoles are opened through the on-board Baseboard Management Controller (BMC). See Remote console configuration. To ensure maximum reliability, ensure that the most up-to-date firmware is installed for the following components:

• Flash BIOS
• Baseboard Management Controller

Remote console software describes the remote console software for your cluster when you are using hardware control while Remote console configuration describes the different kinds of remote console configurations.

Power status mode

CSM can maintain the current power status for each node configured for power control. The status is represented by the PowerStatus attribute value for each node. The PowerStatusMode attribute, which is set globally using the csmconfig command, defines whether CSM maintains power status. The PowerMethod attribute, which is set per node using the definenode or chnode command, determines the CSM method for maintaining power status.

Each node configured for power control is defined with the PowerMethod attribute set for its particular node type. Some power methods support power events. These power methods are automatically notified whenever a node's power state changes. The power method will notify CSM, and the PowerStatus attribute for the node will be updated to reflect the new state. The hmc, lvm, and csp power methods currently support power events.

The apc, bmc, bmc2, blade, fsp, and xseries power methods do not support events. CSM must poll these nodes periodically to obtain their power status. The frequency of the polling is determined by the PowerPollingInterval attribute, which is set globally using the csmconfig command. The apc, bmc, bmc2, blade, fsp, and xseries power methods, along with any user-defined power methods, support polling.

The PowerStatusMode attribute can be set to the following values:

0 | Mixed
   CSM polls nodes that support polling, and monitors power events on nodes that send events.
1 | Events
   This is the default value. CSM monitors power events on nodes that send events. Nodes that support polling are not updated; the PowerStatus attribute for these nodes is always set to 127 (unknown).
2 | Polling
   CSM polls nodes that support polling. Nodes that support events are not updated; the PowerStatus attribute for these nodes is always set to 127 (unknown).
3 | None

CSM for AIX and Linux: Planning and Installation Guide
CSM does not poll or monitor power events. The *PowerStatus* attribute of all nodes is set to 127 (unknown).

**Note:**

1. The default value is 1 (Events).
2. The `csmconfig` command accepts either the number or the text label for the *PowerStatusMode* attribute.

The Hardware Control Resource Manager must be stopped and restarted for any changes to the *PowerStatusMode* to take effect. Use the `stopsrc -s IBM.HWCTRLRM` command to stop the resource manager, and use `startsrc -s IBM.HWCTRLRM` to restart it.

**Conceptual diagrams**

The following diagrams are provided for conceptual explanation only. They are not intended to be literal depictions of how to configure a specific cluster environment. See your eServer Cluster 1350 or 1600 resources for specific cluster hardware configuration details.

**Note:**

Configure System POWER 6 servers using the same connections shown for System p5 servers.

**HMC-attached System p nodes**

*Figure 1* shows the hardware and networking configuration required for using CSM hardware control with HMC-attached POWER4 and System p5 (POWER5) servers. The System p servers in the diagram are individual servers that were partitioned using an HMC into 16 LPARs (nodes) each. The management server connects to the management and cluster VLANs through Ethernet adapters. The controlling HMCs must be attached to the management VLAN. The POWER4 server is attached to an HMC through a direct serial connection. The System p5 server is attached to the management VLAN directly, along with its controlling HMC. POWER4 and System p5 servers cannot share an HMC. HMC-attached System p nodes must be connected to the cluster VLAN. Configuration for a public VLAN is flexible and can be customized.
Figure 1. CSM hardware control configuration for IBM HMC-attached System p nodes

Figure 2 shows the relationship between CSM node attributes and the internal hardware names used in Figure 1. For remote power and remote console to work as expected for HMC-attached System p servers, this matching of node attribute names in the CSM database to the internal hardware values must be correct for all HMCs in the CSM cluster.
The following attribute values for System p nodes correspond to Figure 1 and Figure 2:

Table 7. Hardware control attribute values for System p nodes

<table>
<thead>
<tr>
<th>Hostname</th>
<th>Power Method</th>
<th>HWControlPoint</th>
<th>HWControlNodeId</th>
<th>ConsoleMethod</th>
<th>ConsoleServerName</th>
<th>ConsolePortNum</th>
<th>ConsoleSerial-Device</th>
<th>ConsoleSerial-Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>clsn01.clusters.com</td>
<td>hmc</td>
<td>c01hmc.clusters.com</td>
<td>clsn01</td>
<td>hmc</td>
<td>c01hmc.clusters.com</td>
<td>not applicable</td>
<td>not applicable</td>
<td>not applicable</td>
</tr>
<tr>
<td>clsn02.clusters.com</td>
<td>hmc</td>
<td>c01hmc.clusters.com</td>
<td>clsn02</td>
<td>hmc</td>
<td>c01hmc.clusters.com</td>
<td>not applicable</td>
<td>not applicable</td>
<td>not applicable</td>
</tr>
<tr>
<td>clsn03.clusters.com</td>
<td>hmc</td>
<td>c01hmc.clusters.com</td>
<td>clsn03</td>
<td>hmc</td>
<td>c01hmc.clusters.com</td>
<td>not applicable</td>
<td>not applicable</td>
<td>not applicable</td>
</tr>
<tr>
<td>clsn04.clusters.com</td>
<td>hmc</td>
<td>c01hmc.clusters.com</td>
<td>clsn04</td>
<td>hmc</td>
<td>c01hmc.clusters.com</td>
<td>not applicable</td>
<td>not applicable</td>
<td>not applicable</td>
</tr>
</tbody>
</table>
**IVM-managed System POWER 6/p5 nodes**

*Figure 3* shows the hardware and networking configuration required for using CSM hardware control with IVM-managed System p5 nodes. The System p5 server in the diagram is one physical server partitioned to 16 LPARs (nodes) using Integrated Virtualization Manager (IVM) on VIOS. The management server connects to the management and cluster VLANs through Ethernet adapters. The System p5 server is attached to the management VLAN directly, along with its controlling VIOS.

Note that SSH must be installed, and *cimserver* must be running on VIOS. If not, *rpower* will fail to connect the IVM-managed nodes. To verify *cimserver* is running, enter:

```bash
pss -ef | grep cim
```

If *cimserver* is not running, start it by entering:

```
/usr/ios/sbin/climgr cimserver start
```

---

*CSM for AIX and Linux: Planning and Installation Guide*
IVM-managed System p servers must be connected to the cluster VLAN. Configuration for a public VLAN is flexible and can be customized.

**Figure 3. CSM hardware control configuration for IVM-managed System p5 nodes**

Configure the IVM-managed POWER 6 servers using the same connections as the way for the IVM-managed P5 nodes shown in Figure 3

**Figure 4** shows the relationship between CSM node attributes and the internal hardware names used in **Figure 1**. For remote power and remote console to work as expected for IVM-managed System POWER 6/p5 nodes, this matching of node attribute names in the CSM database to the internal hardware values must be correct for all VIOS hardware in the CSM cluster.

**Figure 4. CSM hardware control attribute values for IVM-managed System p5 nodes**

The following attribute values for IVM-managed System POWER 6/p5 nodes correspond to **Figure 3** and **Figure 4**:

**Table 8. Attribute values for IVM-managed System p5 nodes**
<table>
<thead>
<tr>
<th>Hostname</th>
<th>Power Method</th>
<th>HWControlPoint</th>
<th>HWControl NodeId</th>
<th>Console Method</th>
<th>Console ServerName</th>
<th>Console PortNum</th>
<th>Console Serial-Device</th>
<th>Console Serial-Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>clsn01.clusters.com</td>
<td>ivm</td>
<td>c01ivm.clusters.com</td>
<td>clsn01</td>
<td>ivm</td>
<td>c01ivm.clusters.com</td>
<td>1</td>
<td>not applicable</td>
<td>not applicable</td>
</tr>
<tr>
<td>clsn02.clusters.com</td>
<td>ivm</td>
<td>c02ivm.clusters.com</td>
<td>clsn02</td>
<td>ivm</td>
<td>c02ivm.clusters.com</td>
<td>2</td>
<td>not applicable</td>
<td>not applicable</td>
</tr>
<tr>
<td>clsn16.clusters.com</td>
<td>ivm</td>
<td>c03ivm.clusters.com</td>
<td>clsn16</td>
<td>ivm</td>
<td>c03ivm.clusters.com</td>
<td>16</td>
<td>not applicable</td>
<td>not applicable</td>
</tr>
</tbody>
</table>

**Direct-attach System POWER 6/p5 nodes**

*Figure 5* shows the hardware and networking configuration required for using CSM hardware control with direct-attach System POWER 6/p5 nodes. In this configuration, no HMC is required to control the hardware. The Flexible Service Processor (FSP) is attached to the management VLAN directly, along with its controlling management server. Because there is no HMC in this configuration, the System POWER 6/p5 server cannot be partitioned. Each server is a single CSM node, and must be connected to the cluster VLAN.

*Figure 5. CSM hardware control configuration for direct-attach System POWER 6/p5 nodes*

*Figure 6* shows the relationship between CSM node attributes and the internal hardware names used in Direct-attach System POWER 6/p5 nodes. For remote power and remote console to work as expected for direct-attach System POWER 6/p5 nodes, this matching of node attribute names in the CSM database to the internal hardware values must be correct for all System POWER 6/p5 servers in the cluster.

---

*CSM for AIX and Linux: Planning and Installation Guide* 34
The following attribute values for direct-attach System POWER 6/p5 nodes correspond to Figure 5 and Figure 6:

Table 9. Attribute values for direct-attach System POWER 6/p5 nodes

<table>
<thead>
<tr>
<th>Hostname</th>
<th>Power Method</th>
<th>HWControlPoint</th>
<th>HWControlNodeId</th>
<th>Console Method</th>
<th>Console ServerName</th>
<th>Console PortNum</th>
<th>Console Serial-Device</th>
<th>Console Serial-Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>clsn01.clusters.com</td>
<td>fsp</td>
<td>fsp01.clusters.com</td>
<td>clsn01</td>
<td>fsp</td>
<td>fsp01.clusters.com</td>
<td>not applicable</td>
<td>not applicable</td>
<td>not applicable</td>
</tr>
<tr>
<td>clsn02.clusters.com</td>
<td>fsp</td>
<td>fsp02.clusters.com</td>
<td>clsn02</td>
<td>fsp</td>
<td>fsp02.clusters.com</td>
<td>not applicable</td>
<td>not applicable</td>
<td>not applicable</td>
</tr>
</tbody>
</table>

Note: The IVM version supported is 1.4 or later. You can refer the IVM web site for more details,

http://www-03.ibm.com/systems/power/software/virtualization/editions/ivm/index.html
xSeries nodes and APC devices

Figure 7 shows the hardware and networking configuration required to use CSM hardware control for Linux on xSeries 336 and 346 nodes. An APC MasterSwitch device is also shown.

The management server shown in the diagram connects to the management and cluster VLANs through ethernet adapters. The console server (mr01) connects to the management VLAN through its internal ethernet interface, and to the xSeries 336 and 346 servers through a serial connection. The console server is shown as a managed device, and is controlled by CSM using the APC MasterSwitch. The APC MasterSwitch is connected to the management VLAN through its internal ethernet interface.

The management VLAN connects to the IBM Remote Supervisor Adapter (RSA). The servers must be connected to the cluster VLAN through an available ethernet adapter (eth0), and directly or indirectly to an RSA. An RSA connects to its node Internal Systems Management Processor (ISMP) port; up to 24 node ISMP ports can be daisy-chained from the RSA ISMP port.

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 customized.

Figure 7. CSM hardware control hardware configuration for xSeries 336 and 346 nodes and APC devices
Figure 8 shows the relationship between the CSM node database attributes and the internal hardware names used in the diagram in xSeries nodes and APC devices. 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), APCs, and console servers in the CSM cluster.

Figure 8. CSM hardware control database attribute values for xSeries nodes and APC devices

The following attribute values for xSeries nodes correspond to Figure 7 and Figure 8:

Table 10. Attribute values for xSeries nodes

<table>
<thead>
<tr>
<th>Hostname</th>
<th>Power Method</th>
<th>HWControlPoint</th>
<th>HWControlNodeId</th>
<th>Console Method</th>
<th>Console ServerName</th>
<th>Console PortNum</th>
<th>Console Serial-Device</th>
<th>Console Serial-Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>clsn01.clusters.com</td>
<td>xseries</td>
<td>rsa01.clusters.com</td>
<td>clsn01</td>
<td>mrv</td>
<td>mrv01.clusters.com</td>
<td>1</td>
<td>ttyS0</td>
<td>9600</td>
</tr>
</tbody>
</table>

CSM for AIX and Linux: Planning and Installation Guide
The following attribute values for APC devices correspond to Figure 7 and Figure 8:

**Table 11. Attribute values for APC devices**

<table>
<thead>
<tr>
<th>Hostname</th>
<th>Power Method</th>
<th>HWControlPoint</th>
<th>HWControl DeviceId</th>
<th>Console Method</th>
<th>ConsoleServerName</th>
<th>Console PortNum</th>
</tr>
</thead>
<tbody>
<tr>
<td>mrv01.clusters.com</td>
<td>apc</td>
<td>apc01.clusters.com</td>
<td>1</td>
<td>not applicable</td>
<td>not applicable</td>
<td>not applicable</td>
</tr>
</tbody>
</table>

**BMC and BladeCenter nodes**

Figure 9 shows the hardware and networking configuration required for using CSM hardware control with eServer, xSeries, and System x servers equipped with a Baseboard Management Controller (BMC). The configuration is also shown for BladeCenter blade servers.

The management server in the diagram connects to the management and cluster VLANs through ethernet adapters. The BladeCenter management module connects to the management VLAN through its internal ethernet interface. Each eServer, xSeries, and System x server is equipped with a BMC, which is connected to the cluster VLAN.

The mrv01 and mrv02 console servers connect to the management VLAN through ethernet adapters, to the eServer and BladeCenter HS20-8678 servers through the Cluster 1350 Serial Port Module option. The xSeries, System x, and remaining BladeCenter HS, JS, and LS servers do not require an attached console server; these servers use Serial Over LAN (SOL) for remote console. When using SOL for BladeCenter remote console support, equip each blade server with two Ethernet Switch Modules (ESM). Use the first ESM for SOL, and connect the second ESM to your cluster VLAN.

The IBM Cluster 1350 Serial Port Module is an optional part that must be ordered separately to connect BladeCenter HS20-8678 blade servers to an MRV console server. This connection provides rconsole command function for BladeCenter HS servers; see the CSM for AIX and Linux: Administration Guide for the configuration required for this alternative.
Figure 9. CSM hardware control configuration for BMC and BladeCenter nodes

Figure 10 shows the relationship between the CSM node database attributes and the internal hardware names used in the diagram located in BMC and BladeCenter nodes. 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 modules, BMCs, and console servers in the CSM cluster.
Figure 10. CSM hardware control attribute values for BMC and BladeCenter nodes

Table 12. Attribute values for BMC and BladeCenter nodes

The following attribute values for BMC and BladeCenter nodes correspond to Figure 10:
<table>
<thead>
<tr>
<th>Hostname</th>
<th>Power Method</th>
<th>HWControl Point</th>
<th>Console Method</th>
<th>Console Server Name</th>
<th>Console Port Num</th>
<th>Console Serial-Device</th>
<th>Console Serial-Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>clsn01.clusters.com</td>
<td>bmc</td>
<td>bmc01.clusters.com</td>
<td>clsn01</td>
<td>bmc</td>
<td>bmc01.clusters.com</td>
<td>not applicable</td>
<td>ttyS0 19200</td>
</tr>
<tr>
<td>clsn02.clusters.com</td>
<td>bmc</td>
<td>bmc02.clusters.com</td>
<td>clsn02</td>
<td>bmc</td>
<td>bmc02.clusters.com</td>
<td>not applicable</td>
<td>ttyS0 19200</td>
</tr>
<tr>
<td>clsn03.clusters.com</td>
<td>bmc</td>
<td>bmc03.clusters.com</td>
<td>clsn03</td>
<td>bmc</td>
<td>bmc03.clusters.com</td>
<td>not applicable</td>
<td>ttyS0 19200</td>
</tr>
<tr>
<td>clsn04.clusters.com</td>
<td>bmc</td>
<td>bmc04.clusters.com</td>
<td>clsn04</td>
<td>bmc</td>
<td>bmc41.clusters.com</td>
<td>not applicable</td>
<td>ttyS0 19200</td>
</tr>
<tr>
<td>clsn05.clusters.com</td>
<td>bmc</td>
<td>bmc05.clusters.com</td>
<td>clsn05</td>
<td>mrv</td>
<td>mrv01.clusters.com</td>
<td>12</td>
<td>ttyS0 9600</td>
</tr>
<tr>
<td>clsn06.clusters.com</td>
<td>bmc</td>
<td>bmc06.clusters.com</td>
<td>clsn06</td>
<td>mrv</td>
<td>mrv01.clusters.com</td>
<td>13</td>
<td>ttyS0 9600</td>
</tr>
<tr>
<td>clsn07.clusters.com</td>
<td>bmc</td>
<td>mm01.clusters.com</td>
<td>1</td>
<td>mrv</td>
<td>mrv02.clusters.com</td>
<td>1</td>
<td>ttyS0* 9600</td>
</tr>
<tr>
<td>clsn08.clusters.com</td>
<td>bmc</td>
<td>mm01.clusters.com</td>
<td>2</td>
<td>mrv</td>
<td>mrv02.clusters.com</td>
<td>2</td>
<td>ttyS0* 9600</td>
</tr>
<tr>
<td>clsn09.clusters.com</td>
<td>bmc</td>
<td>mm01.clusters.com</td>
<td>3</td>
<td>mrv</td>
<td>mrv02.clusters.com</td>
<td>3</td>
<td>ttyS0* 9600</td>
</tr>
<tr>
<td>clsn10.clusters.com</td>
<td>bmc</td>
<td>mm01.clusters.com</td>
<td>4</td>
<td>mrv</td>
<td>mrv02.clusters.com</td>
<td>4</td>
<td>ttyS0* 9600</td>
</tr>
<tr>
<td>clsn11.clusters.com</td>
<td>bmc</td>
<td>mm01.clusters.com</td>
<td>5</td>
<td>blade</td>
<td>mm01.clusters.com</td>
<td>5</td>
<td>ttyS1* 19200</td>
</tr>
<tr>
<td>clsn12.clusters.com</td>
<td>bmc</td>
<td>mm01.clusters.com</td>
<td>7</td>
<td>blade</td>
<td>mm01.clusters.com</td>
<td>7</td>
<td>ttyS1* 19200</td>
</tr>
<tr>
<td>clsn13.clusters.com</td>
<td>bmc</td>
<td>mm01.clusters.com</td>
<td>8</td>
<td>blade</td>
<td>mm01.clusters.com</td>
<td>8</td>
<td>ttyS1* 19200</td>
</tr>
</tbody>
</table>

* BladeCenter HS20-8678 blade servers with the 1350 Serial Port Module will recognize the serial interface as the COM1 port on the blade, so the **ConsoleSerialDevice** attribute must be set to **ttyS0**. Blade servers using SOL recognize the serial interface as the COM2 port on the blade, so the **ConsoleSerialDevice** attribute must be set to **ttyS1**.
Chapter 3. Planning for CSM software

CSM is available in three IBM product offerings, which can be ordered separately. Each CSM product is tailored to a specific operating system and hardware type:

- CSM for AIX
- CSM for Linux on POWER
- CSM for Linux Multiplatform

Selecting one or more CSM products depends upon your cluster environment. For example, using both AIX nodes and Linux on POWER nodes requires the CSM for AIX and CSM for Linux on POWER products.

CSM software is available from the following sources:

- CSM product CDs
- AIX product media; CSM for AIX

The CSM product license is only available on the CSM product CDs.

Planning for CSM for AIX

Installing IBM Cluster Systems Management requires installing CSM software and prerequisite non-IBM software. Before installing CSM, gather all the necessary software, including CSM, open source prerequisites, software updates, and optionally, CSM software for Linux nodes. Most of the required software is available from AIX, CSM, or the Linux product media, but you must also download some software.

Details on installing an AIX management server are described in Installing a CSM for AIX management server.

The following prerequisites are required for CSM for AIX:

- The CSM for AIX management server must be installed with either AIX 5.3 Technology Level 7 (5300-07), or later, or AIX 6.1.
- AIX nodes must be installed with AIX for POWER Version 5.3 or AIX for POWER Version 6.1.

Note:
CSM support for node switch and multilink adapters requires the nodes to be installed with AIX V5.3 with Recommended Maintenance Package 5300-07, or later, or AIX V6.1.

- CSM 1.7.1.0 requires RSCT 2.4.11, or later, with the following exception: AIX 6.1 requires RSCT 2.5.3, or later.
See the CSM README file at /opt/csm/README/csm.README for additional service requirements. The README file can be found on the CSM product CD or in the tar file available from the IBM Cluster support Web site.

A management server that runs CSM 1.7.1, or later, can manage nodes that have earlier levels of CSM installed.

**Using AIX 5.3 or AIX 6.1**

The AIX 5.3 and 6.1 operating system product media is available from IBM. You must use the media to install the node that you plan to use as the CSM management server. For information about migrating to the latest release level of AIX, see [Migrating the AIX operating system](#).

**CSM for AIX software**

CSM file sets required for basic CSM support:

- csm.core
- csm.dsh
- csm.diagnostics
- csm.deploy
- csm.server
- csm.hc_utils
- csm.client

CSM optional file sets:

- csm.msg
  This file set contains the non-English CSM message catalogs. They are required for National Language Support (NLS).
- csm.hpsnm
  This file set is required to set up support for a High Performance Switch (HPS) network manager.
- csm.hams
  This file set is required for Highly Available Management Server (HA MS) support.
- csm.gui.dcem
  This file set provides support for the Distributed Command Execution Manager (DCEM) feature. DCEM provides a variety of services for a network of distributed targets. The DCEM graphical user interface (GUI) allows you to create command specifications for running on multiple targets, while providing real-time status as commands are run.
  **Note:**
  A version of csm.gui.dcem is automatically installed with AIX but it is not specifically required for basic CSM support.
- csm.gui.websm
  This file set provides support for the CSM application plug-in for the IBM Web-based System Manager GUI.

**CSM High Performance Computing (HPC) solution packs:**

- csm.ll
- csm.pe
CSM optional solution packs facilitate administration of the IBM High Performance Computing (HPC) product suite. Solution packs include predefined node groups for application administration, and a customization script to install the application on cluster nodes. See the *CSM for AIX and Linux: Administration Guide* for more information.

**IBM System Blue Gene Solution support:**

- **csm.bluegene**

CSM support for IBM System Blue Gene Solution lets you set up monitoring and automated responses for events recorded in the Blue Gene(R) configuration, RAS, and environmental databases.

**CSM for AIX coexistence**

Consider the following restrictions and coexistence considerations in a CSM cluster:

- Starting with CSM 1.4.1, the operating system level on managed nodes can be at a later level than the operating system level on the management server. Note that you must use an install server to install a later level of AIX on the node than is on the management server.
- The following table illustrates how different AIX and CSM levels can coexist in a CSM cluster:

<table>
<thead>
<tr>
<th>Management server AIX operating system</th>
<th>Management server CSM level</th>
<th>Managed node distribution</th>
<th>Managed node CSM level</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIX 5.3</td>
<td>CSM 1.7.1</td>
<td>o  AIX 5.3</td>
<td>o  For AIX 5.3: CSM 1.5, or CSM 1.6, or CSM 1.7</td>
</tr>
<tr>
<td></td>
<td></td>
<td>o  AIX 6.1</td>
<td>o  For AIX 6.1: CSM 1.7</td>
</tr>
<tr>
<td>AIX 6.1</td>
<td>CSM 1.7.1</td>
<td>o  AIX 5.3</td>
<td>o  For AIX 5.3: CSM 1.5, or CSM 1.6, or CSM 1.7</td>
</tr>
<tr>
<td></td>
<td></td>
<td>o  AIX 6.1</td>
<td>o  For AIX 6.1: CSM 1.7</td>
</tr>
</tbody>
</table>

**Required CSM for AIX open source software**

The following required open source RPMs are available on the CSM for AIX Version 5.3, or later, AIX 6.1 product CDs:

- conserver-8.1
- tcl-8.3.3-1
• tk-8.3.3-1
• expect-5.32-1

Note:

The rpm packages of expect/tcl/tk are replaced by new installp packages in AIX 6.1.3 or later.

Optional CSM for AIX open source software

Table 15. Optional AIX open source software

<table>
<thead>
<tr>
<th>Open Source Software</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>autoupdate (required for software maintenance of Linux nodes: installation and upgrades of non-CSM RPMs)</td>
<td><a href="http://freshmeat.net/projects/autoupdate">http://freshmeat.net/projects/autoupdate</a> (Select the link under RPM package, then download the <code>autoupdate-*_noarch.rpm</code>), or <a href="">ftp://linuxpatch.ncsa.uiuc.edu/csm/noarch/</a>.</td>
</tr>
</tbody>
</table>

OpenSSH and prerequisite software

The OpenSSH software is available on the IBM AIX Expansion Pack. Updates to this software are available on the AIX OpenSSH Web site: [http://sourceforge.net/projects/openssh-aix](http://sourceforge.net/projects/openssh-aix). Install the latest updates of OpenSSH from the Web site.

You must install the following minimum prerequisite file sets (for the English language):

- openssh.base
- openssh.license
- openssh.man.en_US
- openssh.msg.en_US
- openssh.msg.EN_US

The OpenSSL software is a prerequisite of OpenSSH software. The RPM package `openssl` is available at: [https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=aixtbx](https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=aixtbx). This site requires registration. OpenSSH requires the AIX Network Authentication (NAS) software to enable Kerberized OpenSSH. If installing OpenSSH3.8 or later, you must install or upgrade to NAS1.4, or later.

**CSM for AIX updates and fixes**

CSM for AIX updates and fixes (APARs) are required to maintain your cluster; see: https://www14.software.ibm.com/webapp/set2/sas/f/csm/home.html.

**CSM for AIX HA MS**

CSM High Availability Management Server (HA MS) is an optional tool that prevents your CSM management server from being a single point of failure. HA MS uses a shared disk to store CSM management server data and Tivoli® System Automation for Multiplatforms to control the failover. (Tivoli System Automation for Multiplatforms is included in the priced feature for HA MS use only).

You can install HA MS at any time. HA MS must be installed on a primary management server and a backup management server. For complete installation information and supported hardware and software, see the *CSM for AIX and Linux: Administration Guide*.

**CSM for AIX Kerberos setup**

CSM for AIX can automatically perform the following optional Kerberos setup:

- Set up a Kerberos Version 5 server on the CSM management server.
- Set up the Kerberos client on the managed nodes.
- Create the CSM principal and host principals for the nodes in the Kerberos database, install the keytab for the host principal on the nodes, and update the .k5login file in the home directory of root with the CSM principal name to enable CSM scripts to run with Kerberos Version 5 enabled rsh or ssh.

**Kerberos server in the cluster:** You can install the Kerberos server required for Kerberos remote command processing on either the CSM management server, or on a node outside of your CSM cluster. If the Kerberos server is installed on a node outside the cluster, the management server must be a Kerberos client in the same realm as the cluster nodes. To install the Kerberos server outside of the cluster, ensure that the required software is installed on the node that is to be the Kerberos server.

**Software for AIX nodes:** You can obtain the Kerberos Version 5 installation packages from the AIX 5.3 or later expansion pack, IBM Network Authentication Service (NAS) Version 1.3 or later. Consider the following requirements for Kerberos Version 5, CSM 1.7, AIX 5.3, and AIX 6.1:

- NAS 1.4 is required.
- If you use OpenSSH with NAS 1.4, OpenSSH 3.8.0.5300 or later is required for AIX 5.3.

For the AIX Kerberos server, obtain the following software, where lang is one or more desired language; for example, EN_US:

- krb5.server
- krb5.msg.lang
- krb5.client
For the AIX Kerberos client nodes, obtain the following software, where lang is one or more desired language; for example, EN_US

- krb5.client
- krb5.msg.lang

**Software for rsh:** The Kerberos packages supply a version of rsh and rshd that are capable of using Kerberos for authentication.

**Software for ssh:** The OpenSSH supplied with AIX is enabled to use Kerberos Version 5 for authentication. If you want to use OpenSSH with Kerberos Version 5, it is your responsibility to build Kerberos Version 5 enabled OpenSSH for your distribution, install OpenSSH, and to verify that the users of ssh can successfully authenticate using Kerberos Version 5. Once you have completed these tasks, you can configure CSM to use Kerberos Version 5 for authentication.

**Restrictions and considerations:** Consider the following for any CSM cluster:

- AIX nodes must have AIX 5.3 or later installed to enable Kerberos to use rsh.
- CSM does not support Kerberos Version 5 with Distributed Computing Environment (DCE).
- If you are setting up Kerberos remote commands through rsh or ssh, you must ensure that the clocks for the server and clients are synchronized. When you install CSM, the Network Time Protocol (NTP) configuration files are available for use in the cluster.
- You must ensure that the domain name service (DNS) is enabled.
- In general, the Kerberos commands work as shown with the implementations of Kerberos Version 5 that is shipped with AIX and with Red Hat EL. The system administrator might need to modify these commands for other Kerberos implementations. CSM has specific requirements for Kerberos setup, and these requirements are the same for all implementations of Kerberos Version 5. These requirements include the format of the name of the CSM principal and the location of its keytab.

**AIX-only cluster:** Consider the following for a CSM cluster that includes an AIX management server and AIX nodes only:

- To use the Kerberos V5 authentication protocol as the only authentication protocol for rsh between the management server and the managed nodes, all nodes must be at AIX 5.3 or later. CSM supports the automatic setup of the Kerberos server using AIX Network Authentication Services (NAS) on the management server and the setup of Kerberos clients on the managed nodes.

---

**Planning for CSM for Linux**

IBM Cluster Systems Management for Linux has requirements for non-IBM software as well as IBM-developed software. As a convenience, some of the required non-IBM software for Linux that is not part of a Linux distribution is included on the CSM CDs. Unless otherwise specified, the software is required on both the management server and the nodes.

See the README file in the root directory on the CD-ROM or in the tar file for additional or service requirements. After installation, the README file resides in /opt/csm/README/csm_README.
Before installing CSM, see Avoiding problems with hardware and network setup for details on avoiding installation problems.

Planning CSM for Linux management server

The following Linux distributions are supported on a CSM for Linux management server:

- Red Hat EL 5, 5.1, 5.2 and 5.3 Client/Server
- Red Hat EL 4 (AS/ES)
- Red Hat EL 4.5, 4.6 and 4.7 (AS/ES)
- SUSE Linux Enterprise Server (SLES) 9
- SUSE Linux Enterprise Server (SLES) 10

Red Hat EL ES 4, 4.5, 4.6 and 4.7 and Red Hat EL 5, 5.1, 5.2 and 5.3 Client are not supported as a CSM for Linux on POWER management server.

For a list of Linux distributions supported on cluster nodes, see Planning CSM for Linux nodes.

CSM for Linux software coexistence

Consider the following CSM for Linux restrictions and coexistence considerations:

- The operating system level on managed nodes can be at a later level than the operating system level on the management server. For example, the management server can run SLES 9 if the nodes run SLES 10.
- The Linux nodes in a CSM cluster must be installed with one of the Linux distributions listed in Planning CSM for Linux nodes.
- For more information on how different Linux distributions and CSM levels can coexist in a CSM cluster, see Table 27.

Hardware Management Console (HMC) for System p hardware

For HMC updates, see the following Web site:

CSM for Linux packages

CSM for Linux Multiplatform software: The following packages are included on the CSM for Linux Multiplatform 1.7.1 CDs.

- csm.bluegene 1.7.1
- csm.client 1.7.1 (required on the managed nodes only)
- csm.core 1.7.1
- csm.deploy 1.7.1 (required on the management server only)
- csm.diagnostics 1.7.1
- csm.dsh 1.7.1
- csm.gpfs 1.7.1
• csm.gui.decem 1.7.1 (installed on the management server)
• csm.ll 1.7.1
• csm.server 1.7.1 (required on the management server only)
• csm.hc_utils 1.7.1 (required on the management server only)
• csm.pe 1.7.1
• rsct.basic 2.5.3
• rsct.core 2.5.3
• rsct.core.cimrm 2.5.3
• rsct.core.utils 2.5.3
• rsct.64bit 2.5.3
• rsct.opt.storagerm 2.5.3
• src 1.3.0

Note:
CSM does not use rsct.opt.storagerm, but if you have an earlier version, CSM automatically updates it to the current level.

CSM for Linux on POWER software: The following packages are included on the CSM for Linux on POWER 1.7.1 CDs:

• csm.bluegene 1.7.1
• csm.client 1.7.1 (required on the managed nodes only)
• csm.core 1.7.1
• csm.deploy 1.7.1 (required on the management server only)
• csm.dsh 1.7.1
• csm.diagnostics 1.7.1
• csm.essl 1.7.1
• csm.gpfs 1.7.1
• csm.gui.decem 1.7.1 (installed on the management server)
• csm.gui.websm 1.7.1 (installed on the management server)
• csm.hc_utils 1.7.1 (required on the management server only)
• csm.ll 1.7.1
• csm.pe 1.7.1
• csm.pessl 1.7.1
• csm.server 1.7.1 (required on the management server only)
• rsct.basic 2.5.3
• rsct.core 2.5.3
• rsct.core.utils 2.5.3
• rsct.core.cimrm 2.5.3
• rsct.64bit 2.5.3
• rsct.opt.storagerm 2.5.3
• rsct.core.gui 2.5.3
• src 1.3.0
• sysmgt.websm.framework 5.0.3
• sysmgt.websm.apps 5.0.3
• sysmgt.websm.help 5.0.3
• sysmgt.websm.webaccess 5.0.3

Note:
1. CSM does not use rsct.64bit 2.5.3, or rsct.opt.storagerm 2.5.3, but if you have an earlier version installed, CSM automatically updates it to the current level.
2. For information on installing these file sets, see the managing cluster applications information in the *CSM for AIX and Linux: Administration Guide*.

**CSM for Linux HA MS**

CSM for Linux High Availability Management Server (HA MS) prevents the CSM management server from being a single point of failure in the CSM cluster. CSM HA MS uses a shared disk to store the CSM management server data and Tivoli System Automation for Multiplatforms to control the failover. (Tivoli System Automation for Multiplatforms is included in the priced feature for HA MS use only).

You can install HA MS at any time. HA MS must be installed on a primary management server and a backup management server. For complete installation information and supported hardware and software, see the *CSM for AIX and Linux: Administration Guide*.

HA MS is included with the following packages on the CSM product CD:

- csm.hams 1.7.1
- sam.core 2.3.0

**CSM for Linux Kerberos setup**

CSM can automatically perform the following optional Kerberos setup on Red Hat EL:

- Set up the Kerberos client on the managed nodes.
- Create the CSM principal and host principals for the nodes in the Kerberos database, install the keytab for the host principal on the nodes, and update the root's `.k5login` file with the CSM principal name to enable CSM scripts to run with Kerberos Version 5 `rsh` or `ssh`.

**Kerberos server:** You can install the Kerberos server on the CSM management server or on a node outside of the CSM cluster. If the Kerberos server is installed on a node outside the cluster, the management server must be a Kerberos client in the same realm as the cluster nodes. To install the Kerberos server outside of the cluster, ensure that the required software is installed on the node that is to be the Kerberos server.

For a Red Hat EL cluster, CSM does not automatically configure the Kerberos server. You must set up the Kerberos server manually. For a SLES cluster CSM cannot perform automatic set up of Kerberos.

**CSM for AIX cluster with Linux nodes:** Consider the following for a CSM for AIX cluster that includes Linux nodes:

- CSM only supports automatic setup of Red Hat EL managed nodes as Kerberos clients.
- In a cluster with an AIX management server and managed nodes running SLES, you must configure the software as Kerberos clients to the Kerberos server. CSM can do the following Kerberos setup for the SLES nodes:
  - Create host principals and keytabs for SLES nodes.
  - Copy the `krb5.conf` file to the nodes.
  - Update the `.k5login` file in the home directory of root on the nodes with the CSM principal.
  - Transfer the keytab for the host principal of the node to a temporary file on the node. CSM is not able to merge the key for the host principal into an existing `krb5.keytab` on a SLES node. If there is no `krb5.keytab` on the node, you can move the temporary file to the
krb5.keytab location in the /etc directory. If there is an existing krb5.keytab on the node, the system administrator must use Kerberos commands to merge the key for the host principal into the existing krb5.keytab. On the managed node, the temporary file that contains the key for the host principal is located as follows:

- /var/ct/IW/sec/krb5/csm/k5keytabs/keytab.tmp

**Software for SLES:** For a SLES node, you can obtain the Kerberos Version 5 RPMs from the SLES CD. You must install the following RPMs on the node that is to function as the Kerberos server or Kerberos client:

- heimdal* (the heimdal RPMs that provide Kerberos server or client function)
- xinetd-* (the RPMs required to start the remote shell)

**Software for rsh:** The Kerberos packages supply a version of rsh and rshd that are capable of using Kerberos for authentication.

**Software for ssh:** If you want to use OpenSSH with Kerberos Version 5, it is your responsibility to build Kerberos Version 5 enabled OpenSSH RPMs for your distribution, install the RPMs, and to verify that the users of ssh can successfully authenticate using Kerberos Version 5. Once you have completed these tasks, you can configure CSM to use Kerberos Version 5 for authentication.

**Restrictions and considerations:** Consider the following for any CSM cluster:

- CSM cannot perform automatic set up of Kerberos for a SLES cluster; to use Kerberos with SLES, you must manually configure Kerberos. You can use several CSM functions; for example, you can use SMS to install the packages. You can also use user-customized installation scripts to provide configuration like copying the krb5.conf file to a client node.
- If you are setting up Kerberos remote commands through rsh or ssh, you must ensure that the clocks for the server and clients are synchronized. When you install CSM, the Network Time Protocol (NTP) configuration files are available for use in the cluster.
- You must ensure that the domain name service (DNS) is enabled.
- In general, the Kerberos commands work as shown with the implementations of Kerberos Version 5 that is shipped with Red Hat EL. The system administrator might need to modify these commands for other Kerberos implementations. CSM has specific requirements for Kerberos setup, and these requirements are the same for all implementations of Kerberos Version 5. These requirements include the format of the name of the CSM principal and the location of its keytab.

**CSM for Linux non-IBM software**

To enable some CSM for Linux functions, including software maintenance and hardware control, you must download non-IBM software prerequisites.

**Optional software for x86 architecture**

**Table 16. Optional software for x86 architecture**

<table>
<thead>
<tr>
<th>Open Source Software</th>
<th>Download</th>
</tr>
</thead>
<tbody>
<tr>
<td>autoupdate 4.8.4, or later, for SMS installation and upgrade of non-CSM RPMs.</td>
<td><a href="http://freshmeat.net/projects/autoupdate">http://freshmeat.net/projects/autoupdate</a>, or <a href="">ftp://linuxpatch.ncsa.uiuc.edu/csm/noarch/</a>.</td>
</tr>
</tbody>
</table>
Optional software for POWER-based architecture

Table 17. Optional software for POWER-based architecture

<table>
<thead>
<tr>
<th>Open Source Software</th>
<th>Download</th>
</tr>
</thead>
<tbody>
<tr>
<td>autoupdate 5.4.1, or later, for SMS installation and upgrade of non-CSM RPMs.</td>
<td><a href="http://freshmeat.net/projects/autoupdate">http://freshmeat.net/projects/autoupdate</a>, or <a href="">ftp://linuxpatch.ncsa.uiuc.edu/csm/noarch/</a>.</td>
</tr>
<tr>
<td>autoupdate 5.4.1-2, or later, for Red Hat EL 5</td>
<td><a href="http://freshmeat.net/projects/autoupdate">http://freshmeat.net/projects/autoupdate</a>, or <a href="">ftp://linuxpatch.ncsa.uiuc.edu/csm/noarch/</a>.</td>
</tr>
</tbody>
</table>

Planning CSM for Linux nodes

To manage Linux nodes, one of the following Linux distribution packages must be installed. For additional hardware information, see [Linux distributions and hardware support](#).

- Red Hat EL 5, 5.1, 5.2 and 5.3 Client/Server
- Red Hat EL 4.5, 4.6 4.7 (AS)
- Red Hat EL 4 (AS/ES/WS)
- SUSE Linux Enterprise Server (SLES) 10
- SUSE Linux Enterprise Server (SLES) 9

Required CSM for Linux software

The following RPMs are included on the CSM for Linux CDs, and are required for managing Linux nodes.

- csm.client 1.7.1
- csm.core 1.7.1
- csm.diagnostics 1.7.1
- csm.dsh 1.7.1
- rsct.core 2.5.3
- rsct.core.utils 2.5.3
- rsct.basic 2.5.3
- src 1.3.0

For optional CSM High Availability Management Server (HA MS) file sets, see [CSM for Linux HA MS](#).
Open source software shipped on Linux product media (required for Linux nodes)

The following software packages are required for Red Hat EL 4 for x86-based architecture nodes:

### Table 18. Red Hat EL 4 for x86-based architecture (AS/ES/WS):

<table>
<thead>
<tr>
<th>Red Hat EL 4 AS for x86-based (32 bit) architecture</th>
<th>Red Hat EL 4 ES for x86-based (32 bit) architecture</th>
<th>Red Hat EL 4 WS for x86-based (32 bit) architecture</th>
</tr>
</thead>
<tbody>
<tr>
<td>compat-libstdc++-296-*</td>
<td>compat-libstdc++-296-*</td>
<td>compat-libstdc++-296-*</td>
</tr>
<tr>
<td>compat-libstdc++-33-*</td>
<td>compat-libstdc++-33-*</td>
<td>compat-libstdc++-33-*</td>
</tr>
<tr>
<td>dhcp-3*</td>
<td>dhcp-3*</td>
<td>dhcp-3*</td>
</tr>
<tr>
<td>expect-5.42*</td>
<td>expect-5.42*</td>
<td>expect-5.42*</td>
</tr>
<tr>
<td>freetype-2.1*</td>
<td>freetype-2.1*</td>
<td>freetype-2.1*</td>
</tr>
<tr>
<td>gdk-pixbuf-0.*</td>
<td>gdk-pixbuf-0.*</td>
<td>gdk-pixbuf-0.*</td>
</tr>
<tr>
<td>gtk+-1.2*</td>
<td>gtk+-1.2*</td>
<td>gtk+-1.2*</td>
</tr>
<tr>
<td>nfs-utils-*</td>
<td>nfs-utils-*</td>
<td>nfs-utils-*</td>
</tr>
<tr>
<td>pdksh-*</td>
<td>pdksh-*</td>
<td>pdksh-*</td>
</tr>
<tr>
<td>perl-5*</td>
<td>perl-5*</td>
<td>perl-5*</td>
</tr>
<tr>
<td>rdist-6*</td>
<td>rdist-6*</td>
<td>rdist-6*</td>
</tr>
<tr>
<td>syslinux-*</td>
<td>syslinux-*</td>
<td>syslinux-*</td>
</tr>
<tr>
<td>tcl-8.4*</td>
<td>tcl-8.4*</td>
<td>tcl-8.4*</td>
</tr>
<tr>
<td>tk-8.4*</td>
<td>tk-8.4*</td>
<td>tk-8.4*</td>
</tr>
<tr>
<td>xorg-x11-*</td>
<td>xorg-x11-*</td>
<td>xorg-x11-*</td>
</tr>
</tbody>
</table>

The following software packages are required for Red Hat EL 4 for x86-64 based architecture nodes:

### Table 19. Red Hat EL 4 for x86-64 (64 bit)-based architecture (AS/ES/WS) software and for POWER-based architecture (AS) software:

<table>
<thead>
<tr>
<th>Red Hat EL 4 (AS) for x86-64 (64 bit) architecture</th>
<th>Red Hat EL 4 (ES) for x86-64 (64 bit) architecture</th>
<th>Red Hat EL 4 (WS) for x86-64 (64 bit) architecture</th>
<th>Red Hat EL 4 (AS) for POWER-based architecture</th>
</tr>
</thead>
<tbody>
<tr>
<td>compat-libstdc++-296-*</td>
<td>compat-libstdc++-296-*</td>
<td>compat-libstdc++-296-*</td>
<td>compat-libstdc++-296-*</td>
</tr>
<tr>
<td>compat-libstdc++-33-*</td>
<td>compat-libstdc++-33-*</td>
<td>compat-libstdc++-33-*</td>
<td>compat-libstdc++-33-*</td>
</tr>
<tr>
<td>dhcp-3*</td>
<td>dhcp-3*</td>
<td>dhcp-3*</td>
<td>dhcp-3*</td>
</tr>
<tr>
<td>expect-5.42*</td>
<td>expect-5.42*</td>
<td>expect-5.42*</td>
<td>expect-5.42*</td>
</tr>
<tr>
<td>freetype-2.1*</td>
<td>freetype-2.1*</td>
<td>freetype-2.1*</td>
<td>freetype-2.1*</td>
</tr>
<tr>
<td>gdk-pixbuf-0.*</td>
<td>gdk-pixbuf-0.*</td>
<td>gdk-pixbuf-0.*</td>
<td>gdk-pixbuf-0.*</td>
</tr>
<tr>
<td>gtk+-1.2*</td>
<td>gtk+-1.2*</td>
<td>gtk+-1.2*</td>
<td>gtk+-1.2*</td>
</tr>
<tr>
<td>nfs-utils-*</td>
<td>nfs-utils-*</td>
<td>nfs-utils-*</td>
<td>nfs-utils-*</td>
</tr>
<tr>
<td>pdksh-*</td>
<td>pdksh-*</td>
<td>pdksh-*</td>
<td>pdksh-*</td>
</tr>
<tr>
<td>perl-5*</td>
<td>perl-5*</td>
<td>perl-5*</td>
<td>perl-5*</td>
</tr>
<tr>
<td>rdist-6*</td>
<td>rdist-6*</td>
<td>rdist-6*</td>
<td>rdist-6*</td>
</tr>
<tr>
<td>syslinux-*</td>
<td>syslinux-*</td>
<td>syslinux-*</td>
<td>syslinux-*</td>
</tr>
<tr>
<td>tcl-8.4*</td>
<td>tcl-8.4*</td>
<td>tcl-8.4*</td>
<td>tcl-8.4*</td>
</tr>
<tr>
<td>tk-8.4*</td>
<td>tk-8.4*</td>
<td>tk-8.4*</td>
<td>tk-8.4*</td>
</tr>
<tr>
<td>xorg-x11-*</td>
<td>xorg-x11-*</td>
<td>xorg-x11-*</td>
<td>xorg-x11-*</td>
</tr>
</tbody>
</table>

The following software packages are required for Red Hat EL 4.5, Red Hat EL 4.6 and Red Hat EL 4.7 for x86-based architecture nodes:
Table 20. Red Hat EL 4.5/4.6/4.7 packages for x86-based architecture (AS/ES/WS):

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>compat-libstdc++-296-*</td>
<td>compat-libstdc++-296-*</td>
<td>compat-libstdc++-296-*</td>
</tr>
<tr>
<td>compat-libstdc++-33-*</td>
<td>compat-libstdc++-33-*</td>
<td>compat-libstdc++-33-*</td>
</tr>
<tr>
<td>dhcp-3*</td>
<td>dhcp-3*</td>
<td>dhcp-3*</td>
</tr>
<tr>
<td>expect-5.42*</td>
<td>expect-5.42*</td>
<td>expect-5.42*</td>
</tr>
<tr>
<td>freetype-2.1*</td>
<td>freetype-2.1*</td>
<td>freetype-2.1*</td>
</tr>
<tr>
<td>gdk-pixbuf-0.*</td>
<td>gdk-pixbuf-0.*</td>
<td>gdk-pixbuf-0.*</td>
</tr>
<tr>
<td>gtk+1.2*</td>
<td>gtk+1.2*</td>
<td>gtk+1.2*</td>
</tr>
<tr>
<td>nfs-utils-*</td>
<td>nfs-utils-*</td>
<td>nfs-utils-*</td>
</tr>
<tr>
<td>pdksh-*</td>
<td>pdksh-*</td>
<td>pdksh-*</td>
</tr>
<tr>
<td>perl-5*</td>
<td>perl-5*</td>
<td>perl-5*</td>
</tr>
<tr>
<td>rdist-6*</td>
<td>rdist-6*</td>
<td>rdist-6*</td>
</tr>
<tr>
<td>syslinux-*</td>
<td>syslinux-*</td>
<td>syslinux-*</td>
</tr>
<tr>
<td>tcl-8.4*</td>
<td>tcl-8.4*</td>
<td>tcl-8.4*</td>
</tr>
<tr>
<td>tk-8.4*</td>
<td>tk-8.4*</td>
<td>tk-8.4*</td>
</tr>
<tr>
<td>xorg-x11-*</td>
<td>xorg-x11-*</td>
<td>xorg-x11-*</td>
</tr>
</tbody>
</table>

The following software packages are required for Red Hat EL 4.5, Red Hat EL 4.6 and Red Hat EL 4.7 for x86-64 and POWER-based architecture nodes:

Table 21. Red Hat EL 4.5/4.6/4.7 packages for x86-64 (64 bit) (AS/ES/WS) and POWER-based architecture (AS):

<table>
<thead>
<tr>
<th>Red Hat EL 4.5/4.6/4.7 AS for x86-64 (64 bit) architecture</th>
<th>Red Hat EL 4.5/4.6/4.7 ES for x86-64 (64 bit) architecture</th>
<th>Red Hat EL 4.5/4.6/4.7 WS for x86-64 (64 bit) architecture</th>
<th>Red Hat EL 4.5/4.6/4.7 AS for POWER-based architecture</th>
</tr>
</thead>
<tbody>
<tr>
<td>compat-libstdc++-296-*</td>
<td>compat-libstdc++-296-*</td>
<td>compat-libstdc++-296-*</td>
<td>compat-libstdc++-296-*</td>
</tr>
<tr>
<td>compat-libstdc++-33-*</td>
<td>compat-libstdc++-33-*</td>
<td>compat-libstdc++-33-*</td>
<td>compat-libstdc++-33-*</td>
</tr>
<tr>
<td>dhcp-3*</td>
<td>dhcp-3*</td>
<td>dhcp-3*</td>
<td>dhcp-3*</td>
</tr>
<tr>
<td>expect-5.42*</td>
<td>expect-5.42*</td>
<td>expect-5.42*</td>
<td>expect-5.42*</td>
</tr>
<tr>
<td>freetype-2.1*</td>
<td>freetype-2.1*</td>
<td>freetype-2.1*</td>
<td>freetype-2.1*</td>
</tr>
<tr>
<td>gdk-pixbuf-0.*</td>
<td>gdk-pixbuf-0.*</td>
<td>gdk-pixbuf-0.*</td>
<td>gdk-pixbuf-0.*</td>
</tr>
<tr>
<td>gtk+1.2*</td>
<td>gtk+1.2*</td>
<td>gtk+1.2*</td>
<td>gtk+1.2*</td>
</tr>
<tr>
<td>nfs-utils-*</td>
<td>nfs-utils-*</td>
<td>nfs-utils-*</td>
<td>nfs-utils-*</td>
</tr>
<tr>
<td>pdksh-*</td>
<td>pdksh-*</td>
<td>pdksh-*</td>
<td>pdksh-*</td>
</tr>
<tr>
<td>perl-5*</td>
<td>perl-5*</td>
<td>perl-5*</td>
<td>perl-5*</td>
</tr>
<tr>
<td>rdist-6*</td>
<td>rdist-6*</td>
<td>rdist-6*</td>
<td>rdist-6*</td>
</tr>
<tr>
<td>syslinux-*</td>
<td>syslinux-*</td>
<td>syslinux-*</td>
<td>syslinux-*</td>
</tr>
<tr>
<td>tcl-8.4*</td>
<td>tcl-8.4*</td>
<td>tcl-8.4*</td>
<td>tcl-8.4*</td>
</tr>
<tr>
<td>tk-8.4*</td>
<td>tk-8.4*</td>
<td>tk-8.4*</td>
<td>tk-8.4*</td>
</tr>
<tr>
<td>xorg-x11-*</td>
<td>xorg-x11-*</td>
<td>xorg-x11-*</td>
<td>xorg-x11-*</td>
</tr>
<tr>
<td>sg3_utils-*</td>
<td>sg3_utils-*</td>
<td>sg3_utils-*</td>
<td>sg3_utils-*</td>
</tr>
</tbody>
</table>

The following software packages are required for Red Hat EL 5, Red Hat EL 5.1, Red Hat EL 5.2 and Red Hat EL 5.3 for x86-based architecture nodes:

Table 22. Red Hat EL 5/5.1/5.2/5.3 packages for x86-based architecture

<table>
<thead>
<tr>
<th>Red Hat EL 5/5.1/5.2/5.3 Server for x86-based (32 bit) architecture</th>
<th>Red Hat EL 5/5.1/5.2/5.3 Client for x86-based (32 bit) architecture</th>
</tr>
</thead>
<tbody>
<tr>
<td>compat-libstdc++-296-*</td>
<td>compat-libstdc++-296-*</td>
</tr>
<tr>
<td>compat-libstdc++-33-*</td>
<td>compat-libstdc++-33-*</td>
</tr>
<tr>
<td>dhcp-3*</td>
<td>dhcp-3*</td>
</tr>
<tr>
<td>expect-5.42*</td>
<td>expect-5.42*</td>
</tr>
<tr>
<td>freetype-2.1*</td>
<td>freetype-2.1*</td>
</tr>
<tr>
<td>gdk-pixbuf-0.*</td>
<td>gdk-pixbuf-0.*</td>
</tr>
<tr>
<td>gtk+1.2*</td>
<td>gtk+1.2*</td>
</tr>
<tr>
<td>nfs-utils-*</td>
<td>nfs-utils-*</td>
</tr>
<tr>
<td>pdksh-*</td>
<td>pdksh-*</td>
</tr>
<tr>
<td>perl-5*</td>
<td>perl-5*</td>
</tr>
<tr>
<td>rdist-6*</td>
<td>rdist-6*</td>
</tr>
<tr>
<td>syslinux-*</td>
<td>syslinux-*</td>
</tr>
<tr>
<td>tcl-8.4*</td>
<td>tcl-8.4*</td>
</tr>
<tr>
<td>tk-8.4*</td>
<td>tk-8.4*</td>
</tr>
<tr>
<td>xorg-x11-*</td>
<td>xorg-x11-*</td>
</tr>
<tr>
<td>sg3_utils-*</td>
<td>sg3_utils-*</td>
</tr>
</tbody>
</table>

CSM for AIX and Linux: Planning and Installation Guide
The following software packages are required for Red Hat EL 5, Red Hat EL 5.1, Red Hat EL 5.2 and Red Hat EL 5.3 for x86-64 and POWER architecture nodes:

Table 23. Red Hat EL 5/5.1/5.2/5.3 packages for x86-64 and POWER

<table>
<thead>
<tr>
<th>Red Hat EL 5/5.1/5.2/5.3 (Server) for x86-64 architecture</th>
<th>Red Hat EL 5/5.1/5.2/5.3 (Client) for x86-64 architecture</th>
<th>Red Hat EL 5/5.1/5.2/5.3 (Server) for POWER architecture</th>
</tr>
</thead>
<tbody>
<tr>
<td>perl-5*</td>
<td>perl-5*</td>
<td>perl-5*</td>
</tr>
<tr>
<td>ksh*</td>
<td>ksh*</td>
<td>ksh*</td>
</tr>
<tr>
<td>nfs-utils*</td>
<td>nfs-utils*</td>
<td>nfs-utils*</td>
</tr>
<tr>
<td>rdist-6*</td>
<td>rdist-6*</td>
<td>rdist-6*</td>
</tr>
<tr>
<td>tcl-8.4*</td>
<td>tcl-8.4*</td>
<td>tcl-8.4*</td>
</tr>
<tr>
<td>tk-8.4*</td>
<td>tk-8.4*</td>
<td>tk-8.4*</td>
</tr>
<tr>
<td>expect-5.42*</td>
<td>expect-5.42*</td>
<td>expect-5.42*</td>
</tr>
<tr>
<td>freetype-2.1*</td>
<td>freetype-2.1*</td>
<td>freetype-2.1*</td>
</tr>
<tr>
<td>compat-libstdc++-296* i386</td>
<td>compat-libstdc++-296* i386</td>
<td>compat-libstdc++-296* ppc</td>
</tr>
<tr>
<td>compat-libstdc++-33* i386</td>
<td>compat-libstdc++-33* i386</td>
<td>compat-libstdc++-33* ppc</td>
</tr>
<tr>
<td>net-snmp*</td>
<td>net-snmp*</td>
<td>net-snmp*</td>
</tr>
<tr>
<td>net-snmp-utils*</td>
<td>net-snmp-utils*</td>
<td>net-snmp-utils*</td>
</tr>
<tr>
<td>syslinux*</td>
<td>syslinux*</td>
<td>syslinux*</td>
</tr>
<tr>
<td>system-config-netboot*</td>
<td>system-config-netboot*</td>
<td>system-config-netboot*</td>
</tr>
<tr>
<td>dhcp-3*</td>
<td>dhcp-3*</td>
<td>dhcp-3*</td>
</tr>
<tr>
<td>yum*</td>
<td>yum*</td>
<td>yum*</td>
</tr>
<tr>
<td>libxml2-python*</td>
<td>libxml2-python*</td>
<td>libxml2-python*</td>
</tr>
<tr>
<td>createrepo*</td>
<td>createrepo*</td>
<td>createrepo*</td>
</tr>
</tbody>
</table>

The following software packages are required for SLES 9 for x86 and POWER architecture nodes:

Table 24. SLES 9 software

<table>
<thead>
<tr>
<th>SLES 9 for x86-based (32 bit) architecture:</th>
<th>SLES 9 for x86_64 (64 bit) architecture:</th>
<th>SLES 9 for POWER-based architecture:</th>
</tr>
</thead>
<tbody>
<tr>
<td>bootsplash-3*</td>
<td>bootsplash-3*</td>
<td>dhcp-3*</td>
</tr>
<tr>
<td>bootsplash-theme-SuSE-SLES-3*</td>
<td>bootsplash-theme-SuSE-SLES-3*</td>
<td>dhcp-server*</td>
</tr>
<tr>
<td>dhcp-3*</td>
<td>dhcp-3*</td>
<td>expat-*</td>
</tr>
<tr>
<td>dhcp-server*</td>
<td>dhcp-server*</td>
<td>expect-5*</td>
</tr>
<tr>
<td>expat-*</td>
<td>expat-*</td>
<td>freetype2-2*</td>
</tr>
<tr>
<td>expect-5.40-*</td>
<td>expect-5.40-*</td>
<td>nfs-utils-*</td>
</tr>
<tr>
<td>freetype2-2*</td>
<td>freetype2-2*</td>
<td>freetype2-2*</td>
</tr>
</tbody>
</table>
The following software packages are required for SLES 10 for x86 and POWER architecture nodes:

Table 25. SLES 10 software

<table>
<thead>
<tr>
<th>SLES 10 for x86-based (32 bit) architecture</th>
<th>SLES 10 for x86_64 (64 bit) architecture</th>
<th>SLES 10 for POWER-based architecture</th>
</tr>
</thead>
<tbody>
<tr>
<td>bootsplash-3*</td>
<td>bootsplash-3*</td>
<td>compat-libstdc++-5*</td>
</tr>
<tr>
<td>bootsplash-theme-SuSE-SLES-3*</td>
<td>bootsplash-theme-SuSE-SLES-3*</td>
<td>dhcp-3*</td>
</tr>
<tr>
<td>compat-readline4-*</td>
<td>compat-readline4-*</td>
<td>dhcp-server*</td>
</tr>
<tr>
<td>dhcp-3*</td>
<td>dhcp-3*</td>
<td>expat-*</td>
</tr>
<tr>
<td>dhcp-server*</td>
<td>dhcp-server*</td>
<td>expect-5*</td>
</tr>
<tr>
<td>expect-5.43-*</td>
<td>expect-5.43-*</td>
<td>expect-5.43-*</td>
</tr>
<tr>
<td>freetype2-*</td>
<td>freetype2-*</td>
<td>freetype2-2*</td>
</tr>
<tr>
<td>ksh-*</td>
<td>ksh-*</td>
<td>ksh-*</td>
</tr>
<tr>
<td>mtools-3*</td>
<td>mtools-3*</td>
<td>nls-utils-*</td>
</tr>
<tr>
<td>nfs-utils-*</td>
<td>nfs-utils-*</td>
<td>perl-5*</td>
</tr>
<tr>
<td>perl-5*</td>
<td>perl-5*</td>
<td>perl-HTML-Parser-*</td>
</tr>
<tr>
<td>perl-HTML-Parser-*</td>
<td>perl-HTML-Parser-*</td>
<td>perl-HTML-Tagset-*</td>
</tr>
<tr>
<td>perl-HTML-Tagset-*</td>
<td>perl-HTML-Tagset-*</td>
<td>perl-libwwwperl-*</td>
</tr>
<tr>
<td>perl-libwwwperl-*</td>
<td>perl-libwwwperl-*</td>
<td>perl-URI-*</td>
</tr>
<tr>
<td>perl-URI-*</td>
<td>perl-URI-*</td>
<td>perl-XM-IDOM-*</td>
</tr>
<tr>
<td>perl-XM-DOM-*</td>
<td>perl-XM-DOM-*</td>
<td>perl-XM-Parser-*</td>
</tr>
<tr>
<td>perl-XM-Parser-*</td>
<td>perl-XM-Parser-*</td>
<td>perl-XM-RegExp-*</td>
</tr>
<tr>
<td>perl-XM-RegExp-*</td>
<td>perl-XM-RegExp-*</td>
<td>ppc64-utils-*</td>
</tr>
<tr>
<td>rdist-6.1.5-*</td>
<td>rdist-6.1.5-*</td>
<td>rdist-6*</td>
</tr>
<tr>
<td>rdist-6.1.5-*</td>
<td>rdist-6*</td>
<td>rsh-server-*</td>
</tr>
<tr>
<td>rsh-server-*</td>
<td>rsh-server-*</td>
<td>rsync-*</td>
</tr>
<tr>
<td>rsh-server-*</td>
<td>rsh-server-*</td>
<td>tcl-8*</td>
</tr>
<tr>
<td>syslinux-3*</td>
<td>syslinux-3*</td>
<td>termcap-*</td>
</tr>
<tr>
<td>tcl-8*</td>
<td>tcl-8*</td>
<td>tk-8*</td>
</tr>
<tr>
<td>termcap-*</td>
<td>termcap-*</td>
<td>xinetd-*</td>
</tr>
<tr>
<td>tk-8*</td>
<td>tk-8*</td>
<td>xinetd-*</td>
</tr>
<tr>
<td>XFree86-*</td>
<td>XFree86-*</td>
<td>xinetd-*</td>
</tr>
</tbody>
</table>

CSM for AIX and Linux: Planning and Installation Guide
Installing minimally-managed Linux nodes

Minimally-managed nodes are Linux nodes with no CSM or RSCT code installed. The CSM minimal installation option installs the Linux operating system only, and provides limited CSM management capability of minimally-managed nodes. To define a minimally-managed node, set the node Mode attribute to MinManaged.

The following CSM functionality is supported on minimally-managed nodes:

- Listing nodes and node information
- Creating node groups
- Using dsh
- Using DCEM
- Automatic setup of rsh using .rhosts for authentication, or automatic setup of ssh using authorized keys for authentication; required for dsh
- Using limited function of updatenode to set up the remote shell environment only
- Monitoring conditions and responses on the management server only
- Running user customization scripts during installation
- Full operating system installation of nodes
- Using probes on the management server only
- Minimal heartbeat through fping
- Mixed clusters of minimally-managed nodes and managed nodes
- Using install servers as minimally-managed nodes
- Using CFM
- Using SMS

CSM functionality not supported on minimally-managed nodes includes:

- Monitoring conditions and responses on the node.
- Installation of CSM and RSCT RPMs.
- Full RMC heartbeat.
- Automatic setup of Kerberos Version 5, as indicated by a non-zero value for csmconfig attribute SetupKRB5. If you manually set up the minimally-managed node as a Kerberos client, CSM can use Kerberos for dsh authentication.

Hardware Management Console (HMC) for System p hardware

For updates to the IBM Hardware Management Console (HMC), see the following Web site: https://www14.software.ibm.com/webapp/set2/sas/f/hmc/home.html.

CSM High Availability Management Server (HA MS) (optional)

You can install CSM High Availability Management Server (HA MS) at any time. Using CSM HA MS requires installing HA MS on a primary management server and a backup management server. For details, see CSM for Linux HA MS and CSM for AIX and Linux: Administration Guide.
Considerations for mixed clusters

If the management server is the cluster install server, the operating system combinations labeled yes can be installed on a node:

Table 26. Supported CSM cross-distribution installation environments

<table>
<thead>
<tr>
<th>Management server operating system</th>
<th>Node operating system</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>AIX</td>
</tr>
<tr>
<td>AIX</td>
<td>yes</td>
</tr>
<tr>
<td>Red Hat EL on System p</td>
<td>no</td>
</tr>
<tr>
<td>Red Hat EL on System x</td>
<td>no</td>
</tr>
<tr>
<td>SLES on System p</td>
<td>no</td>
</tr>
<tr>
<td>SLES on System x</td>
<td>no</td>
</tr>
</tbody>
</table>

Key:

1. The following commands are not supported on Red Hat EL 5 nodes if the install server, or management server if no install server is used, is not also installed with Red Hat EL 5: getadapters -m pxeboot; cmsetuphwmaint.
2. Native PXE services are not available in Linux on System p. You must extract the pxelinux.0 file from the Linux on System x distribution after it is loaded by the copycds command, and place it in the correct directory for CSM.
3. Tools do not exist in this distribution to manipulate the Linux on System p zImage. This means that the zImage shipped with the Linux on System p distribution will need to be used as is. This implies the following limitations:
   a. User-supplied drivers are not supported for these System p distributions. This limits the System p hardware that can be supported if install drivers are not included as part of the base zImage.
   b. Kernel parameters cannot be added to the zImage, therefore installnode with the -noreboot flag is not supported for these Linux on System p distributions.

If separate install servers are used, the operating system combinations labeled yes can be installed on a node:

Table 27. Operating system coexistence between install servers and nodes
Host name resolution

When you define a CSM cluster node the host name that you provide is the network interface that the management server uses to install and manage the node. The Hostname node attribute in the CSM database is the resolved value for the host name that you provide to the `definenode` command.

CSM supports the use of either a short host name or a long host name. A long host name is recommended, especially in an environment that contains multiple networks. It is very important that the host name resolution for a CSM node name be consistent throughout the cluster. For example, if you use the short host name, all host name resolution for that node name on the management server or any cluster node must also use the short host name.

The primary host name of the node (that is, the value returned by the `hostname` command) does not have to be set to the host name of the node that is known by the CSM management server. For example, you can change the primary host name to the name of an interface that is connected to a public network but not used for cluster management.

CSM license requirements

CSM has licensing requirement options. You should use the Full production license.
For installation procedures related to CSM licensing, see Accepting the CSM for Linux license.

For software migration issues when you migrate to a new version and release of AIX, see Migrating the AIX operating system. For CSM software maintenance issues, see Updating CSM for AIX.

**Full production license**

To use CSM for production purposes, you must purchase a full production license and a license key, and you must accept the IPLA license agreement. The license key is a file called `csmlum.full`. Orders can be placed by calling IBM.COM, Americas at 1-800-IBM-CALL (1-800-426-2255).
Chapter 4. Creating a CSM cluster

Follow these steps to create a CSM cluster:

Table 28. Creating a CSM cluster

<table>
<thead>
<tr>
<th>Step</th>
<th>More information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set up the management server (required)</td>
<td>To set up a management server, you must install the management server software, and configure the management server. For setting up an AIX management server, see Installing a CSM for AIX management server. For setting up a Linux management server, see Installing a CSM for Linux management server.</td>
</tr>
<tr>
<td>Set up one or more install servers (optional)</td>
<td>See Setting up install servers.</td>
</tr>
<tr>
<td>Define the nodes (required)</td>
<td>Create node definitions in the CSM database. The information needed for the definitions includes general attributes, hardware control information, and information about installation software. See Defining nodes.</td>
</tr>
<tr>
<td>Define non-node devices to be managed (optional)</td>
<td>If you plan to manage non-node devices, you must create device definitions in the CSM database. See Defining devices.</td>
</tr>
<tr>
<td>Install the nodes (optional)</td>
<td>See Installing AIX on nodes and Installing Linux on nodes.</td>
</tr>
<tr>
<td>Add the nodes to the cluster (required)</td>
<td>Add the AIX or Linux nodes to the cluster. You can add both AIX or Linux nodes to any CSM cluster.</td>
</tr>
</tbody>
</table>

Automating cluster configuration

You can use CSM to automatically perform various configuration tasks when you install or add nodes to the cluster. For example, use the CSM configuration file manager (CFM) support to distribute configuration files across the cluster. For more information on CFM support, see the CSM for AIX and Linux: Administration Guide.

Node provisioning

Node provisioning automatically detects and adds nodes to the cluster; see Provisioning Linux nodes.

Using probes

You can use the following probe scripts to verify that CSM has been configured correctly.
Management server probe (ibm.csm.ms)

The management server probe checks for problems that occur when you install the management server. The probe is part of the csm.diagnostics file set and is installed on the management server when you install CSM.

To run the management server probe, issue the following command:

probemgr -p ibm.csm.ms

Node install probe (ibm.csm.node-install)

Verifies that a node is fully configured and ready to be installed. This probe ensures that all node attributes are correct, installation source files are available, and installation configuration files have been created.

probemgr probemgr options -p ibm.csm.node-install

The probemgr command has options for node lists and nodegroups which get passed to the probe. You can also specify a list of node names in a ibm.csm.node-install.conf file located at the directory defined by STD_PROBE_CONFIGDIR (as documented in the probemgr command).

Install server probe (ibm.csm.install-server)

Verifies that an install server is fully configured. This probe ensures that the required software packages are installed, install services are configured and running, and network connections are correct and active.

probemgr probemgr options -p ibm.csm.install-server

The probemgr command has options for node lists and nodegroups which get passed to the probe. You can also specify a list of node names in a ibm.csm.install-server.conf file located at the directory defined by STD_PROBE_CONFIGDIR (as documented in the probemgr command). The probe will use the specified nodes as install servers that need to be checked. If the -a flag or no parameters are specified, the InstallServer attributes of all nodes will be used to build a list of install servers to run the probe against.

Hardware control probe (ibm.csm.hwctrl)

The hardware control probe verifies that the hardware control points and console servers are available. It generates a list of hardware control point and conservers based on the attributes in the ManagedNode table for the specified set of nodes. The hardware control probe assumes that the configuration for the node might not be ready for an operating system installation. It does not check for installation requirements.

The probe is part of the csm.diagnostics file set or package and is installed on the management server when you install CSM.

To run the hardware control probe, issue the following command:

probemgr -p ibm.csm.hwctrl
Kerberos probe (ibm.csm.security-k5setup)

The Kerberos probe (ibm.csm.security-k5setup) checks to determine if the Kerberos environment is set up to automatically transfer the Kerberos Version 5 host keytab file to the nodes. It checks if the following condition response is active:

NodeFullInstallComplete/GatherKRB5keytabs

The probe is part of the csm.diagnostics file set or package and is installed on the management server when you install CSM.

To run the Kerberos probe, issue the following command:

probemgr -p ibm.csm.security-k5setup

Migrating to a new CSM release

For AIX, Migrating the AIX operating system contains information for migrating from one level of AIX to another. Updating CSM for AIX describes the basic procedures for updating CSM software in a cluster that uses AIX as the management server.

For Linux, Updating CSM for Linux contains information for migrating from one level of CSM to another as well as CSM coexistence.

Getting started: road maps for specific cluster configurations

This section presents several common cluster configurations. For each configuration a road map—a high-level series of steps—is given to help you understand this particular environment. Some configurations refer you to sample installation scenarios documented in Installation scenarios.

Configuration 1: AIX-only cluster

This environment consists of a CSM on AIX management server and CSM on AIX nodes only.

1. Install the management server. See Installing a CSM for AIX management server.
2. Define the nodes. See Defining nodes.
3. Optionally define non-node devices. See Defining devices.
4. Add nodes and install AIX on the nodes. See Adding AIX nodes and Installing AIX on nodes.

See CSM for AIX cluster configuration for a sample installation scenario.
Configuration 2: Red Hat EL on System x cluster

This environment consists of a Red Hat EL for System x management server and Red Hat EL for System x nodes.

1. Install the management server. See Installing a CSM for Linux management server.
2. Define the nodes. See Defining nodes.
3. Optionally define non-node devices. See Defining devices.
4. Add Linux nodes and any diskless Linux nodes, and install Linux on the nodes. See Adding Linux nodes and Installing Linux on nodes. For diskless nodes, see Using Linux diskless nodes.

See Red Hat EL on System x cluster configuration for a sample installation scenario.

Configuration 3: SUSE Linux Enterprise Server (SLES) on System p cluster

This environment consists of a SUSE Linux Enterprise Server (SLES) 9 on System p management server and SLES on System p nodes.

1. Install the management server. See Installing a CSM for Linux management server.
2. Define the nodes. See Defining nodes.
3. Optionally define non-node devices. See Defining devices.
4. Add Linux nodes and any diskless Linux nodes, and install Linux on the nodes. See Adding Linux nodes and Installing Linux on nodes. For diskless nodes, see Using Linux diskless nodes.

See SLES on System p cluster configuration for a sample installation scenario.

Configuration 4: Mixed System p cluster

This environment consists of an AIX management server on System p hardware, AIX nodes, a Red Hat EL on System p install server, and Red Hat EL on System p nodes.

1. Install the management server. See Installing a CSM for AIX management server.
2. Create CSM install servers. See Setting up install servers.
3. Define the nodes. See Defining nodes.
4. Optionally define non-node devices. See Defining devices.
5. Add nodes and install AIX on the nodes. See Adding AIX nodes and Installing AIX on nodes.
6. Add nodes and install Linux on the nodes. See Adding Linux nodes and Installing Linux on nodes.
Configuration 5: Red Hat EL and SLES on System x clusters with an install server

This environment consists of a Red Hat EL on a System x management server, SLES on System x install server, SLES on System x nodes, and Red Hat EL on System x nodes.

1. Install the management server. See Installing a CSM for Linux management server.
2. Create CSM install servers. See Setting up install servers.
3. Define the nodes. See Defining nodes.
4. Optionally define non-node devices. See Defining devices.
5. Add nodes and install Linux on the nodes. See Adding Linux nodes and Installing Linux on nodes.

Configuration 6: SLES on POWER cluster with an install server

This environment consists of a SLES on POWER management server, a SLES on POWER install server, and SLES on POWER nodes.

1. Install the management server. See Installing a CSM for Linux management server.
2. Create CSM install servers. See Setting up install servers.
3. Define the nodes. See Defining nodes.
4. Optionally define non-node devices. See Defining devices.
5. Add nodes and install Linux on the nodes. See Adding Linux nodes and Installing Linux on nodes.
Chapter 5. Installing a CSM for AIX management server

To install a CSM for AIX management server, you must manually install the AIX operating system and the CSM for AIX software. Once you have installed the AIX management server, you can use CSM to install the AIX operating system and CSM on your cluster nodes.

For installation command usage details, see the man pages or the *CSM for AIX and Linux: Command and Technical Reference*.

You can use standard AIX tools and procedures to install CSM and the required open source software. The tools that AIX provides include Web-based System Manager, System Management Interface Tool (SMIT), and a command line interface.

Your CSM management server must be installed with AIX for POWER Version 5.3 (5300-07) or later, or 6.1. For detailed information on management server software requirements, see Planning for CSM for AIX.

Web site access: This procedure describes downloading software products from various Web sites. If your management server does not have internet access, you must download these packages to another server (AIX, Linux, or Windows(R)), and transfer the files to your management server.

Register AIX host names

Register the following AIX host names with the nameserver, or add them to the `/etc/hosts` file on the management server:

- Management server
- Nodes
- Any secondary adapters
- Devices; to monitor the status of a network-connected device, the device Name attribute must be registered with the nameserver, or added to the `/etc/hosts` file.
- For hardware control:
  - HMC hostname for HMC-attached System p hardware
  - Remote Supervisor Adapter (RSA) host name for System x hardware
  - APC MasterSwitch host name
  - Management module host name for BladeCenter
  - Baseboard Management Controller (BMC) host name for eServer 325 and 326, and optionally for xSeries 336 and 346
  - Console server host names
**Update AIX $PATH and $MANPATH variables**

Add `/opt/csm/bin` to the root user's $PATH variable on the management server:

```bash
export PATH=$PATH:/opt/csm/bin
```

**Note:**

MANPATH does not need to be updated to include `/opt/csm/man`.

To verify that this step completed successfully, issue the following commands:

```bash
echo $PATH
echo $MANPATH
```

**Note:**

The examples above only show how to change the $PATH and $MANPATH variables in the current login session. To permanently change them, edit your login environment.

---

**Create AIX /csminstall file system (optional)**

A separate file system called `/csminstall` stores files on the management server that are used with CSM. If you do not create the `/csminstall` file system manually, CSM creates the `/csminstall` directory for you when you install the management server. In this case, however, `/csminstall` is created as a subdirectory of the / (root) file system and might not contain enough space for your intended use.

The size of the `/csminstall` file system depends on your particular cluster requirements. The following list estimates the space required for some basic categories of files that you can store in `/csminstall`:

- Space required for CSM software, configuration files - 120 MB.
- Space required for AIX operating system installation resources - 2.0 GB (per level of AIX). It is not necessary to store these resources in the `/csminstall` file system.
- Additional space required if adding Linux nodes to the cluster - 120 MB in the `/csminstall` file system and 250 MB in the `/var` file system.
- If managing Linux nodes, additional space required to store Linux distribution RPMs - amount of space that is required in `/csminstall` depends on the number of CDs that make up the Linux distribution. Each CD requires about 700 MB, so if you have four CDs, you need about 3 GB.

You can create the `/csminstall` file system as part of the `rootvg` or in its own volume group. The following examples illustrate how to create `/csminstall` using the root volume group. To create a 1 GB file system called `/csminstall`, do the following:

**Table 29. Using the root volume group to create /csminstall**

<table>
<thead>
<tr>
<th>If using:</th>
<th>Do this:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command line</td>
<td>Issue the AIX <code>crfs</code> command: &lt;br&gt;<code>crfs -v jfs2 -g rootvg -m /csminstall -a size=1024M -a bf=true</code>&lt;br&gt;<code>-a bf=true</code> allows the creation of a large file enabled file system. (For example, if you define the <code>mksysb</code> file, it can use a large amount of space.)</td>
</tr>
<tr>
<td>SMIT</td>
<td>Issue the <code>crfs</code> command via SMIT. The fastpath is <code>crfs</code>. For example:</td>
</tr>
</tbody>
</table>
Web-based System Manager
Use the File Systems plug-in to create the new file system.

After you have created /csminstall, you must mount it, as follows:

mount /csminstall

---

### Download open source software for AIX

Open source software is used to support the capabilities of the management server.

**openCIMOM**
- Required to support hardware control on POWER4, System p5 and POWER 6 nodes.

**autoupdate**
- Required to support the CSM Software Maintenance System (SMS).

**perl-RPM2**
- Used to update software on the management server. This is optional.

#### Downloading openCIMOM 0.8 for AIX

You must install version 0.8 of openCIMOM on your management server to use CSM hardware control for HMC-attached POWER4, System p5 (POWER5) and POWER 6 (POWER6) nodes.

You can download openCIMOM from the following Web site:
http://www.ibm.com/servers/aix/products/aixos/linux/download.html, or
ftp://linuxpatch.ncsa.uiuc.edu/csm/noarch/.

Copy the file to a temporary directory on the management server. You can use the `rpm` command to install the file. For example, for RPM package `openCIMOM-0.8-1.aix5.2.noarch.rpm`, issue the following command:

```
rpm -i openCIMOM-0.8-1.aix5.2.noarch.rpm
```

You can also obtain openCIMOM on the IBM AIX Toolbox CD-ROM.

#### Downloading autoupdate for AIX (required for SMS)

The autoupdate software is required to support the CSM Software Maintenance System (SMS) feature that is available for updating software on Linux nodes. You only need the software if you are adding Linux nodes to your CSM cluster.

You can download the autoupdate software from the following Web site:
http://freshmeat.net/projects/autoupdate. To download the software, select the link under "RPM package:"
then download `autoupdate-release.noarch.rpm`; for example, `autoupdate-5.2.5-1.noarch.rpm`. Copy the
RPM to a temporary directory; for example /tmp/csm/RPMS/ppc. You do not have to install the RPM on the management server.

You can also download the autoupdate software from the following Web site:
ftp://linuxpatch.nesa.uiuc.edu/csm/noarch/.

The autoupdate RPM is required only when you add Linux nodes to the cluster. You can postpone downloading the autoupdate RPM until you are ready to follow the procedure to add the Linux node. See Adding Linux nodes. You can also download the autoupdate RPM open source software from other sites on the web.

**Downloading perl-RPM2 for AIX (optional)**

It is time-consuming to use autoupdate for updating software. Using Perl-RPM2 software reduces the amount of time required. You can download the perl-RPM2 software from the following Web site: http://www.mat.univie.ac.at/~gerald/ftp/autoupdate/perl-modules/.

Copy the RPM to a temporary directory. You do not have to install the RPM on the management server. The perl-RPM2 RPM is optional; it is used by autoupdate to improve its performance. You can also download the perl-RPM2 RPM open source software from other sites on the Web.

The available perl-RPM2 is for Red Hat EL on x86 architecture. For SLES or POWER architecture, download the source RPM and build it manually.

**Verify AIX prerequisite software**

Check for the required RSCT software by checking the installed version of rsct.core. The minimum required rsct.core version is 2.4.9.0 for AIX 5.3 and 2.5.1.0 for AIX 6.1. You must run installp to upgrade RSCT to the required level.

To verify the required level of rsct.core, use the lslpp command as follows:

**Table 30. Verify rsct.core**

<table>
<thead>
<tr>
<th>If using:</th>
<th>Do this:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command line</td>
<td>Issue the lslpp command, as follows: and lslpp -L rsct*</td>
</tr>
<tr>
<td>SMIT</td>
<td>Issue the lslpp command using SMIT. The fastpath is list_installed_sw.</td>
</tr>
<tr>
<td>Web-based System</td>
<td>Use the Software plug-in to list installed software.</td>
</tr>
<tr>
<td>Manager</td>
<td></td>
</tr>
</tbody>
</table>

The following sample command output for the lslpp command shows the required rsct.core file sets are installed with the 2.4.9.0 version for the AIX 5.3 operating system:

```
file set                  Level State Type  Description (Uninstaller)
```

CSM for AIX and Linux: Planning and Installation Guide 69
<table>
<thead>
<tr>
<th>Component</th>
<th>Version</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rsct.core.auditim</td>
<td>2.4.9.0</td>
<td>C</td>
<td>RSCT Audit Log Resource Manager</td>
</tr>
<tr>
<td>rsct.core.errm</td>
<td>2.4.9.0</td>
<td>C</td>
<td>RSCT Event Response Resource Manager</td>
</tr>
<tr>
<td>rsct.core.fsrm</td>
<td>2.4.9.0</td>
<td>C</td>
<td>RSCT File System Resource Manager</td>
</tr>
<tr>
<td>rsct.core.gui</td>
<td>2.4.9.0</td>
<td>C</td>
<td>RSCT Graphical User Interface</td>
</tr>
<tr>
<td>rsct.core.lprm</td>
<td>2.4.9.0</td>
<td>C</td>
<td>RSCT Host Resource Manager</td>
</tr>
<tr>
<td>rsct.core.rmc</td>
<td>2.4.9.0</td>
<td>C</td>
<td>RSCT Resource Monitoring and Control</td>
</tr>
<tr>
<td>rsct.core.sec</td>
<td>2.4.9.0</td>
<td>C</td>
<td>RSCT Security</td>
</tr>
<tr>
<td>rsct.core.sensorrm</td>
<td>2.4.9.0</td>
<td>C</td>
<td>RSCT Sensor Resource Manager</td>
</tr>
<tr>
<td>rsct.core.utils</td>
<td>2.4.9.0</td>
<td>C</td>
<td>RSCT Registry</td>
</tr>
</tbody>
</table>

Note: For the support of AIX61 TL1 and AIX 53 TL8, the RSCT 2.5.1 and 2.4.9 are required as part of support with CSM 1.7.0.10 and later levels.

RSCT updates are available from the AIX product update media or by downloading updates from the following Fix Central support Web site: [http://www.ibm.com/eserver/support/fixes](http://www.ibm.com/eserver/support/fixes).

Using the Fix Central Web site

When prompted enter the following information:

- Product Group->System p
- Product->AIX
- Version->5.3
- Fix type->Fix search
- -> Continue
- In the search string box, enter rsct.core

---

**Install CSM for AIX software**

The following file sets and RPM packages must be installed on the management server to support the various CSM features.

**CSM for AIX file sets**

**CSM file sets required for basic CSM support:**

- csm.core
- csm.dsh
- csm.diagnostics
- csm.deploy
- csm.server
- csm.hc_utils
Note:
The `csm.client` file set is automatically installed with AIX but is not specifically required for a CSM management server. The `csm.client` file set is required on cluster nodes however.

Optional CSM file sets:

`csm.msg`
Contains the CSM message catalogs.

`csm.hpsnm`
Required to set up support for a High Performance Switch (HPS) network manager.

`csm.gui.decem`
Supports the Distributed Command Execution Manager (DCEM) feature. DCEM provides a variety of services for a network of distributed targets. The DCEM graphical user interface (GUI) allows you to create command specifications for running on multiple targets, while providing real-time status as commands are run. A version of `csm.gui.decem` is automatically installed with AIX, but it is not specifically required for basic CSM support.

`csm.gui.websm`
Supports the CSM plug-in for the IBM Web-based System Manager GUI.

High Performance Computing (HPC) solution packs:

Optional solution packs facilitate administration of the IBM High Performance Computing (HPC) product suite. Solution packs include predefined node groups for application administration, and a customization script to install the application on cluster nodes. See the *CSM for AIX and Linux: Administration Guide* for more information. The HPC solution packs available with CSM are:

- `csm.ll`
- `csm.pe`
- `csm.pessl`
- `csm.essl`
- `csm.gpfs`

IBM System Blue Gene Solution:

CSM's optional Blue Gene support lets you set up monitoring and automated responses for entries of interest in the Blue Gene configuration, RAS and environmental databases.

- `csm.bluegene`

Open source AIX prerequisites

Required open source software that is available on AIX product media:

- `expect`
- `tk`
- `tcl`
- `conserver` - Required if using the CSM hardware control features. This software is needed to support hardware control of System p nodes.

Note:
The rpm packages of expect/tcl/tk are replaced by new installp packages in AIX 6.1.3 or later.

**High Availability Management Server (HA MS) support on AIX**

HA MS is an optional feature of CSM, designed to provide high availability protection for the CSM management server. HA MS improves the reliability, availability, and serviceability of the CSM management server by providing automatic failover and reintegration to a backup management server.

- csm.hams
- sam.core

**Installing CSM for AIX software**

The CSM file sets are available from the following sources:

- The CSM product media.
- The AIX product media.

The open source prerequisites are available on the AIX product media.

The process for installing the CSM file sets on a CSM management server varies slightly, depending on the source of the software and the specific file sets you are installing.

**Using the CSM product media:**

CSM file sets (excluding csm.hams), including the CSM product license, are available on the CSM product media. The open source prerequisites are available on the AIX media.

The required open source software must be installed before the CSM file sets. To install the open source software, insert the AIX media and use either the rpm or geninstall command.

For example, you can use the AIX geninstall command to install selected CSM software as follows:

```
geninstall -IaX -d /dev/cd0 csm.core csm.dsh csm.diagnostics /csm.deploy csm.server csm.hc_utils
```

Or, to install all CSM file sets, issue:

```
geninstall -IaX -d /dev/cd0 all
```

**Using the AIX product media:**

All the CSM file sets (excluding csm.hams) as well as the required open source software are available on the AIX media. However, the AIX product media may not contain the latest version of the CSM file sets and does not contain the CSM license.

Some of the CSM file sets are automatically installed with AIX, the rest are available on the AIX media. The following CSM file sets are automatically installed with AIX:
The remaining software can be installed using the AIX media and the AIX Web-based System Manager, SMIT panels, or command line interface.

For example, you can use the AIX `geninstall` command to install the additional CSM software:

```
geninstall -IaX -d /dev/cd0 csm.server csm.deploy csm.hc_utils R:expect R:tcl R:tk R:conserver
```

**Note:**
The rpm packages of expect/tcl/tk are replaced by new installp packages in AIX 6.1.3 or later. For AIX 6.1.3 or later nodes, please run following commands:

```
geninstall -IaX -d /dev/cd0 csm.server csm.deploy csm.hc_utils expect tcl tk R:conserver
```

The `geninstall` command installs the RPMs before the `installp` file sets. The `csm.server` file set can only be installed if the open source prerequisites have been installed first.

**Using the IBM Cluster support Web site:**


You can download the latest CSM base file sets as well as the latest updates from this site. The CSM product license, however, is not available from this source.

The open source prerequisites are available on the AIX media.

The required open source software must be installed before the CSM file sets. To install the open source software, insert the AIX media and use either the `rpm` or `geninstall` command. For example, you could use AIX CD-ROM #1 and the `geninstall` command as follows:

```
geninstall -d /dev/cd0 R:expect R:tcl R:tk R:conserver
```

**Note:**
The rpm packages of expect/tcl/tk are replaced by new installp packages in AIX 6.1.3 or later. For AIX 6.1.3 or later nodes, please run following commands:

```
geninstall -d /dev/cd0 expect tcl tk R:conserver
```

To install the CSM file sets you can unwrap the CSM tar file that you downloaded and use either the AIX Web-based System Manager, SMIT panels, or an AIX command line interface. For example, if the files were extracted into the `/tmp/csm` directory you could issue the `geninstall` command as follows:

```
geninstall -IaX -d /tmp/csm all
```

**Note:**
The previous step can be combined with [Apply CSM for AIX software updates](#) to install the base file sets and any updates at the same time.

**Errors installing expect and tk:**
Failed dependency errors when installing the `expect` and `tk` RPMs on AIX usually occur because the RPM command does not recognize the shared library. If this type of error occurs, verify that the X11 libraries are installed in the `/usr/lpp/X11/lib` directory. If they are not installed, use the AIX product media to install them. After you have installed the libraries, run the following command to enable the `rpm` command to recognize that the libraries have been installed:

```
/usr/sbin/updtvpkg
```

After running the command, install `expect` and `tk`. For required RPM levels, see Required CSM for AIX open source software.

The remaining optional CSM file sets, including the HPC solution packs and the Blue Gene file set, can be installed using the same procedure described above.

## Apply CSM for AIX software updates

To apply CSM for AIX software updates, you must install them on your management server. The management server must be installed with the most recent version of CSM that is running on your cluster nodes. You can obtain the latest CSM updates from the Fix Central Web site, or from the CSM support Web site, at [http://www14.software.ibm.com/webapp/set2/sas/f/csm/home.html](http://www14.software.ibm.com/webapp/set2/sas/f/csm/home.html).

If you are downloading directly to the management server, place the updates tar file in a temporary directory; for example, `/tmp/csm`. If you download the file to a different server, copy the tar file to the management server before you unwrap it. Use the `tar` command to unwrap the tar file. For example, to unwrap `csm-aix-1.7.1.0.tar.gz` in the `/tmp/csm` directory, run the following commands:

```
gunzip csm-aix-1.7.1.0.tar.gz
tar -xvf csm-aix-1.7.1.0.tar
```

The commands create a set of subdirectories under `/tmp/csm` and locate the files in the appropriate subdirectories. When you apply any updates, check the CSM support Web site for the most current information on required prerequisites, and for information on any special handling that might be required.

After downloading the updates to the `/tmp/csm` directory and unwrapping them, run the `geninstall` command as follows:

```
geninstall -IaX -d /tmp/csm all
```

## Check the CSM for AIX remote shell attribute

A distributed shell program (`dsh`) is used to issue remote commands from the management server to the nodes. It is contained in the `csm.dsh` package. The `dsh` program uses a remote shell of your choice to issue remote commands to the managed nodes. The default remote shell is `/usr/bin/rsh`, but you can specify a different remote shell (`/usr/bin/ssh`) by running the `csmconfig` command with the following attribute value pairs:

**RemoteShell**

Stores the path name of the executable that `dsh` uses to run remote commands.
**SetupRemoteShell**

Directs CSM to automatically configure the remote shell (1 = yes, 0 = no).

CSM can automatically configure `rsh` and **OpenSSH** when a node is being added to the cluster.

To display or change the remote shell values, run the `csmconfig` command. The command displays the current values for the `RemoteShell` and `SetupRemoteShell` attributes. You can then set the `Remote Shell` and `SetupRemoteShell` attributes values. For example, the following command sets the remote shell to `rsh` and instructs CSM to not configure it automatically:

```
csmconfig RemoteShell=/usr/bin/rsh SetupRemoteShell=0
```

You can also temporarily override the remote shell setting with the `DSH_REMOTE_CMD` environment variable. To switch from the default `rsh` shell to `ssh`, specify the `DSH_REMOTE_CMD` environment variable with the full path name of the remote shell command:

```
export DSH_REMOTE_CMD=/usr/bin/ssh
```

For prerequisite software, see [OpenSSH and prerequisite software](#).

---

**Install OpenSSH and OpenSSL for AIX**

This step is required to use **OpenSSH** as your remote shell.

To use `ssh` as your remote shell command, you must install **OpenSSH** and **OpenSSL** on your management server; these files are not part of the basic AIX installation. Install **OpenSSH** and **OpenSSL** during initial installation of an AIX, or when installing CSM on an AIX, as follows.

**Bundle files:** Create two bundle files to use with AIX tools for copying and installing the software. A bundle file contains a list of software file sets or packages. Create one bundle file for **OpenSSL** and one bundle file for **OpenSSH**.

You can also use these bundle files when you install the software on the nodes. If you are using NIM to install the nodes, copy the bundle files to the file system used to store other NIM resources used by the node; for example, `/export/nim`. For details, see [Installing AIX on nodes](#).

Ensure that the **OpenSSL** bundle file contains the following line:

```
R:openssl*
```

Ensure that the **OpenSSH** bundle file contains the following lines:

```
I:openssh.base
I:openssh.license
I:openssh.man.en_US
I:openssh.msg.en_US
```

CSM for AIX and Linux: Planning and Installation Guide
To use additional languages in your cluster, include the language file sets in this list.

To install OpenSSL on the management server, insert the Linux Toolbox CD and issue the `geninstall` command. The following example assumes the name of the OpenSSL bundle file is `openssl.bnd`:

```
geninstall -IaXY -d /dev/cd0 -f openssl.bnd
```

To install OpenSSH on the management server, insert the Expansion Pack CD and issue the `geninstall` command. The following example assumes the name of the OpenSSH bundle file to be `openssh.bnd`:

```
geninstall -IaXY -d /dev/cd0 -f openssh.bnd
```

To install Kerberos Version 5 for CSM for AIX remote commands

This step is required to set up Kerberos for remote commands with `rsh` or `ssh`.

The Kerberos server can be one of the following servers:

- The CSM management server
- A server outside the CSM cluster, with the CSM management server configured as a Kerberos client of the Kerberos server. To set up HA MS, ensure that the Kerberos Server is a node outside the CSM cluster and not the primary or backup management server.

To use the CSM management server as the Kerberos server, ensure that the following files are installed, where `lang` can be any valid language; for example, `en_US`:

```
krb5.server.rte
krb5.client.rte
krb5.msg.lang
krb5.doc.lang - for NAS documentation
```

To install the Kerberos server software on the management server, insert the AIX Expansion Pack CD and issue the following command:

```
geninstall -d /dev/cd0 krb5.server krb5.client krb5.msg.lang krb5.doc.lang
```

To use NAS defaults, consider the following:
To bypass the default NAS setup for your Kerberos server, configure the Kerberos server now. For details, see the AIX security documentation, at http://publib.boulder.ibm.com/infocenter/pseries/v5r3/index.jsp.

To use the NAS defaults for your Kerberos server configuration, you can direct CSM to configure a Kerberos server on your management server later (in Set up Kerberos Version 5 for CSM for AIX remote command processing (optional)), but first continue with this step.

To configure the management server as a client of a separate Kerberos server, do the following:

1. Install the Kerberos client software on the management server.

   To install the Kerberos client software on the management server, insert the AIX Expansion Pack CD and issue the following command, where lang can be any valid language; for example, en_US:

   ```
   geninstall -d /dev/cd0 krb5.client.rte krb5.msg.lang
   ```

2. Configure the Kerberos client by copying the `krb5.conf` file from the Kerberos server to the following location on the management server:

   `/etc/krb5/krb5.conf`

   On the AIX management server, create a link from `/etc/krb5.conf` to `/etc/krb5/krb5.conf`.

Kerberos client and message files: Use the following command to copy the Kerberos client and message files to the management server for use when you add nodes to the cluster. In the example, files are placed in the default `/usr/sys/inst.images/installp/ppc` directory; use the `-t` flag to select another directory. The `lang` value can be any valid language; for example, en_US:

```
gendcopy -d /dev/cd0 krb5.client krb5.msg.lang
```

---

**Accept the CSM for AIX license**

CSM is available with a full production license; see CSM license requirements for details.

**Accepting the CSM for AIX full license agreement**

To accept the CSM for AIX full license agreement:

1. The `csmlum.full` license key is located on the CSM for AIX CD-ROM. Use the key file name as input with the `csmconfig` command, in the next step.
2. Accept the license and activate the license key, using the `mount` and `csmconfig` commands, as follows.

   ```
   mount -v cdrfs -o ro /dev/cd0 /mnt
   csmconfig -L /mnt/csmlum.full
   ```

   At the prompt, follow the directions to accept the CSM license.
3. Run the `csmconfig` command with no flags:
The following is sample command output for the csmconfig command:

AddUnrecognizedNodes = 0 (no)
BMCConsoleEncryptAuth = 1 (yes)
BMCConsoleKeepAlive = 0 (no)
BMCConsolePerMsgAuth = 0 (no)
ClusterSNum =
ClusterTM = 9078-160
DeviceStatusFrequency = 12
DeviceStatusSensitivity = 8
ExpDate =
HAMode = 0
HeartbeatFrequency = 12
HeartbeatSensitivity = 8
MaxNumNodesInDomain = -1 (unlimited)
PowerStatusMode = 0 (Mixed)
Properties =
RegSyncDelay = 1
RemoteCopyCmd = /usr/bin/rcp
RemoteShell = /usr/bin/rsh
SetupKRB5 = 0
SetupRemoteShell = 1 (yes)
TFTPpackage =

Copy CSM for AIX files to /csminstall subdirectories

Issue the following csmconfig command to copy the CSM files into the proper /csminstall subdirectories:

csmconfig -c

These files are primarily used when CSM system management scripts are run on the cluster nodes.

Note:
The -c flag can be combined with the -L flag to accept the license. For example:

csmconfig -c -L

Set the CSM for AIX cluster ID (optional)

You can optionally store the Cluster 1600 serial number. The serial number is on the labels provided with your Cluster 1600 hardware. The labels are part of the group of materials that also includes the IBM Cluster 1600 Planning, Installation, and Service Guide.

To store the serial number, issue the csmconfig command:

csmconfig -s 654BN5011
Store AIX hardware control point user IDs and passwords

If you are using hardware control, you must store the hardware control point user IDs and passwords. The `systemid` command stores the user ID and password required for internal programs to access remote hardware. You must run the command for each hardware control point in the cluster.

BladeCenter JS, HS, and LS blade servers use the Serial Over LAN (SOL) feature to provide remote console access. The System x x336/x346 and later servers can also be configured to use SOL instead of requiring a console server device. See Remote console configuration for more information. The `systemid` command is also used to store the user ID and password for the SOL feature when the `-c` flag is specified.

This is required for hardware control. For complete information about hardware control points for the cluster, see Managing hardware control points.

**USING THE COMMAND LINE:**

See the following descriptions to store hardware control point user IDs and passwords using the command line. The `systemid` command stores the user ID and password for remote hardware.

**HMC-attached System p**

Run the `systemid` command. For example, if the hostname of the HMC is `hmc1` and the user ID is `hscroot`, run the following command:

```
systemid hmc1 hscroot
```

You will be prompted for a password for the user ID you specified.

**IVM-managed System p**

Issue the `systemid` command. For example, if the host name of the IVM is `ivm1` and the user ID is `padmin`, issue the following command:

```
systemid ivm1 padmin
```

You will be prompted for a password for the user ID you specified.

**Direct attach System p**

Run the `systemid` command with the `-f` and `-s` flags for the HMC, admin, and general login IDs. For example, if the IP address of the node FSP is 199.168.1.1, enter the following command to set the HMC login password:

```
systemid -f -s 199.168.1.1 HMC
```

You will be prompted for a password for the user ID you specified. The default passwords are the same as their respective login values.

**System x x336/x346 and later servers with RSA-II SlimLine Adapters**

Change 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-D).

**eServer 325 and 326, and System x x336/x346 without RSA-II SlimLine Adapters**

Issue the `systemid` command. For example, if the BMC name is `bmc01.pok.ibm.com`, issue the following command:

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

You will be prompted for a password for the user ID you specified.
BladeCenter 8677
Change the default hardware control point Login Profile user ID and password using the Management Module Web interface and documentation provided with the hardware. For BladeCenter Management Modules, the default Login Profile user ID is "USERID" and the default password is "PASSW0RD" (P-A-S-S-W-zero-R-D).

BladeCenter and System x x336/x346 and later servers using SOL
With the exception of the BladeCenter HS20-8678, run the `systemid` command with the `-c` flag to store the Login Profile user ID and password required to access the SOL feature. For BladeCenter Management Modules, the default console user ID is `RMTCON` and the default console password is `RMTC0N` (R-M-T-C-zero-N). Change the default console Login Profile user ID and password using the Management Module web interface and documentation provided with the hardware. Do not use a Login Profile with supervisor privileges for console access. If the default console Login Profile user ID is not used, only grant Blade Console remote access privileges to the new Login Profile.

APC MasterSwitch
For devices using the APC MasterSwitch, run the `systemid` command. For example, if the APC MasterSwitch name is `apc01.pok.com`, issue the following command:

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

You will be prompted for a password for the user ID you specified.

**USING SMIT:**

To store hardware control point user IDs and passwords using SMIT:

Issue the `systemid` command via SMIT. The fastpath is `systemid`. For example:

```
smit systemid
```

The `systemid` command stores the user ID and password for remote hardware.

Storing hardware control point user IDs and passwords is not supported using the Web-based System Manager or DCEM GUIs.

For information about remote consoles, see [Remote console attributes](#).

If you are using Cluster-Ready Hardware Server (CRHS), see [Planning for Cluster-Ready Hardware Server (CRHS)](#) and the *CSM for AIX and Linux: Administration Guide* before proceeding to Install user-defined power methods on the CSM for AIX management server (optional).

---

**Install user-defined power methods on the CSM for AIX management server (optional)**

To install a user-defined power method for hardware control, place the power method in the following directory on the management server:

```
/opt/local
```

For details, see [User-defined power methods](#).

_CSM for AIX and Linux: Planning and Installation Guide_
Change CSM for AIX power control attributes (optional)

You can use the `csmconfig` command to change the cluster's `PowerStatusMode` and `PowerPollingInterval` attributes. See `Power status mode` for more information.

Verify the CSM for AIX installation

You can run the `ibm.csm.ms` probe to verify that the management server has been installed correctly and is ready for use. To run the probe, enter:

```
probemgr -p ibm.csm.ms -l 0
```

For information about CSM support for probes, see the *CSM for AIX and Linux: Administration Guide*.

Set up Kerberos Version 5 for CSM for AIX remote command processing (optional)

Ensure that one of the following is true:

- The management server is the Kerberos server
- The management server is configured as a client of a Kerberos server that is not part of the CSM cluster. To use HA MS, ensure that your Kerberos Server is on a node outside the CSM cluster and is not the primary or backup management server.

See `CSM for AIX Kerberos setup`.

CSM can perform one or more of the following configuration steps:

- Create a Kerberos server on the CSM management server
- Create a CSM principal in the Kerberos database.
- Create a host principal in the Kerberos database for each node defined to the CSM cluster
- Place the CSM principal name in the `.k5login file` in the home directory of root on each managed node.
- Transfer the host principal keytab to each managed node.

You can use the `csmconfig` command to set up Kerberos for CSM. The `csmconfig` command provides various options for setting up Kerberos commands to suit your environment. These options determine the extent of CSM set up for Kerberos including the set up of the Kerberos server and client and the creation of principals.

The format of the `csmconfig` command for the Kerberos options is as follows, where `n` is a number from 0 to 15:
The accepted values for $n$ are as follows:

0

No CSM setup of Kerberos (default).

1

CSM configures a Kerberos server on the management server. You are prompted to specify the principal name for the Kerberos Version 5 database administrator. You are also prompted for the database master password, the database administrator password, and the DNS domain name. The domain name is used as the name of the Kerberos realm.

2

CSM sets up the Kerberos client on the managed nodes.

4

CSM creates the required CSM principal in Kerberos. You are prompted to enter the Kerberos Version 5 administrator principal name and password.

8

CSM creates the required host principals in Kerberos. You are prompted to enter the Kerberos Version 5 administrator principal name and password.

You can add any of the values of $n$ to specify one or more actions. For example, to specify CSM to run all of the Kerberos setup options, add the values for each action (1+2+4+8=15) and run the following `csmconfig` command:

```
csmconfig SetupKRB5=15
```

If the management server and managed nodes are added for the first time to a previously established Kerberos realm, a Kerberos server does not need to be configured. However the CSM principal and a host principal for each node must be created and the nodes must be configured as Kerberos clients. Add the values corresponding to each action (2+4+8=14) and specify the following `csmconfig` command:

```
csmconfig SetupKRB5=14
```

If the management server and managed nodes are already part of a Kerberos realm, and you only want to enable CSM to use Kerberos for remote command authentication, specify the following `csmconfig` command:

```
csmconfig SetupKRB5=4
```

For additional information on automatic Kerberos Version 5 client setup of the nodes, see the `updatenode` command in CSM for AIX and Linux: Command and Technical Reference or the man pages.

When you complete the installation process, you need to do the following tasks:

- Set up the nodes as Kerberos clients.
- Enable Kerberos command processing.

For enabling Kerberos, see Enabling remote commands to use Kerberos Version 5 authentication.
Create CSM for AIX hardware service representative login ID

If your cluster uses a High Performance Switch (HPS) Network, this step is required to grant a hardware service representative access to HPSNM (HPS Network Manager) for hardware installation, verification, diagnosis, and repair. You will be given instructions on how to use a script that is included with the csm.hpsnm file set. Read the details to ensure that the script set up meets your local security requirements. The *CSM for AIX and Linux: Administration Guide* describes how to develop your own method for creating the login ID.
Chapter 6. Installing a CSM for Linux management server

To install a CSM for Linux management server, you must manually install the Red Hat EL or SUSE Linux Enterprise Server (SLES) operating system and prerequisite software, and the CSM for Linux software. Once you have installed the Linux management server, you can use CSM to install the Linux operating system and CSM on your cluster nodes.

Complete the following steps to install a CSM for Linux management server:

Prepare for CSM for Linux management server installation

1. For Linux on System x (x86 architecture), ensure that you are running one of the following operating systems on the management server:
   - Red Hat Enterprise Linux (EL) 5 (Server/Client) (includes support for Red Hat EL 5.1 Server/Client, Red Hat EL 5.2 Server/Client and Red Hat EL 5.3 Server/Client)
   - Red Hat EL 4 (AS/ES) (includes support for Red Hat EL 4.5 AS/ES, Red Hat EL 4.6 AS/ES and Red Hat EL 4.7 AS/ES)
   - SUSE Linux Enterprise Server (SLES) 10
   - SLES 9

   See also Linux on System x and Linux on x86 eServer and BladeCenter.

   For Linux on System p (POWER-based architecture), ensure that you are running one of the following operating systems on the management server:

   - Red Hat Enterprise Linux (EL) 5 Server (includes support for Red Hat EL 5.1 Server, Red Hat EL 5.2 Server and Red Hat EL 5.3 Server)
   - Red Hat EL 4 (AS) (includes support for Red Hat EL 4.5 AS, Red Hat EL 4.6 AS and Red Hat EL 4.7 AS)
   - SUSE Linux Enterprise Server (SLES) 10
   - SLES 9

   See also Linux on System p.

2. Ensure that you have read the management server software requirements in Planning for CSM software.

   Note:
   To update Ethernet driver modules on your management server, go to http://techsupport.services.ibm.com/server/cluster2/fixes/csmdriverdownload.html.
Download CSM for Linux open source software

The following open source software is required to support the full capabilities of a CSM for Linux management server.

**openCIMOM**
- Required to support hardware control for POWER4, System p5 and POWER 6 nodes.

**autoupdate**
- Required to support CSM Software Maintenance System (SMS).

**perl-RPM2**
- Used to update software on the management server. This is optional, and for Red Hat EL only.

### Downloading openCIMOM for Linux

You must install version 0.8 of openCIMOM on your management server to use CSM hardware control for HMC-attached POWER4, System p5 (POWER5) and POWER6 nodes.

You can download openCIMOM from the following Web site:

Copy the file to a temporary directory on the management server. You can use the `rpm` command to install the file. For example, assuming the name of the RPM package is `rpmname.rpm`, issue the following command:

```
rpm -i rpmname.rpm
```

You can also obtain openCIMOM from the IBM AIX Toolbox CD. The `cpio` package compatible with the `rpm2cpio` command is available on the IBM AIX Toolbox CD or from http://www.ibm.com/servers/aix/products/aixos/linux/download.html.

### Downloading AutoUpdate for Linux (required for SMS)

AutoUpdate open source software is required to support CSM Software Maintenance System (SMS) for updating software on Linux nodes. You can download AutoUpdate from http://freshmeat.net/projects/autoupdate, or ftp://linuxpatch.ncsa.uiuc.edu/csm/noarch/.

To download the software:

1. Select the link under "RPM package:"
2. Download `autoupdate-release.noarch.rpm`; for example, `autoupdate-5.2.5-1.noarch.rpm`.
3. Copy the RPM to a temporary directory, for example `/tmp/csm/RPMS/ppc`. You do not have to install the RPM on the management server.

You can postpone downloading the `autoupdate` RPM until you are ready to follow the procedure to add the Linux node. See Adding Linux nodes. You can also download the `autoupdate` RPM open source software from other sites on the Web.
**Downloading perl-RPM2 for Linux (optional)**

It is time-consuming to use **autoupdate** for updating software. Using Perl-RPM2 software reduces the amount of time required. You can download the perl-RPM2 software from [http://www.mat.univie.ac.at/~gerald/ftp/autoupdate/perl-modules/](http://www.mat.univie.ac.at/~gerald/ftp/autoupdate/perl-modules/).

Copy the RPM to a temporary directory. You do not have to install the RPM on the management server. The perl-RPM2 RPM is optional; it is used by **autoupdate** to improve its performance. You can also download the perl-RPM2 RPM open source software from other sites on the web.

The available perl-RPM2 is for Red Hat EL on x86 architecture. For SLES or POWER architecture, download the source RPM and build it yourself.

---

**Register Linux host names**

Register the host names for the following hardware with the nameserver, or add the host names to the `/etc/hosts` file on the management server:

- Management server
- Secondary adapters
- Nodes that are being defined to the cluster
- Devices that are being defined to the cluster; to monitor the status of a network-connected device, the device name attribute must be registered with the nameserver, or added to the `/etc/hosts` file.
- Hardware Control:
  - HMC host name for System p hardware
  - tty device specification on the management server for SP Nodes
  - tty device specification on the management server for the p660 server
  - Remote Supervisor Adapter (RSA) host name for System x hardware
  - APC MasterSwitch host name for non-node devices or other devices
  - Management module host name for BladeCenter
  - Baseboard Management Controller (BMC) host name for eServer 325 and 326, and optionally for System x 336 and 346

---

**Create the Linux /csminstall partition**

Create a separate partition called `/csminstall`, on the management server, to hold the required CSM packages. The size of this partition will depend on how you plan to use the cluster and the software it will contain. The elements of your system require approximately the following space:

- CSM-only installation - 250 MB
- Linux operating system - The amount of space that is required in `/csminstall` depends on the number of CDs that make up the Linux distribution. Each CD requires about 700 MB, so if you have four CDs, you need approximately 3 GB.

For examples of how to create partitions, see your Red Hat EL or SLES documentation.
Download CSM for Linux packages

To install CSM from the product CDs, you do not need to download the CSM software from the Web site; skip this step and go directly to Install the Linux csm.core package.

To download and install CSM from the Web, download CSM and required software from the Web site to a local directory.

For Linux on System x CSM packages:

1. Go to the following Web site:
2. Click on Download; click on CSM fixes; click on Linux Multiplatform.
3. Click on the CSM RPM and download the CSM tarballs to a temporary directory; for example, /tmp/csm:
4. Untar the CSM tarballs:

   cd /tmp/csm
   tar -xzvf csm-linux-1.7.1.0.i386.tar.gz

For Linux on System p CSM packages:

2. Click on Download; click on CSM fixes; click on Linux on POWER.
3. Click on the CSM RPM and download the CSM tarballs to a temporary directory; for example, /tmp/csm:
4. Untar the CSM tarball:

   cd /tmp/csm
   tar -xzvf csm-linux-1.7.1.0.ppc64.tar.gz
   tar -xzvf csm.websm-linux-1.7.1.0.ppc64.tar.gz

Install the Linux csm.core package

To install CSM directly from the product CDs:

1. Mount the CSM CD:

   mount /dev/cdrom /media/cdrom

2. Install the csm.core package:

   rpm -i /media/cdrom/csm.core-*

To install CSM from a directory:

1. If you have not already downloaded the CSM packages, follow the instructions in Download CSM for Linux packages.
2. Run the `rpm` command to install the `csm.core` package from the `/tmp/csm` directory, as follows:

```
rpm -i /tmp/csm/csm.core-*
```

When you install `csm.core`, CSM sets the `PATH` and `MANPATH` environment variables. You must start a new shell to pick up these environment variable settings before you run the `installms` command in Install CSM for Linux software.

---

### Install CSM for Linux software

The `installms` command performs the tasks and installs the software required to configure a CSM for Linux management server, including CSM management server packages, RSCT packages and other CSM management server prerequisite packages. If the management server software is not installed, or if the software is at a previous level, the command installs the Linux and IBM prerequisite software on the management server. You can run the `installms` command multiple times after the management server is already set up.

The `installms` command is located in `/opt/csm/bin`. Run the `installms` command on the management server, and insert the Linux operating system CDs or DVDs when prompted. The `installms` command establishes the CSM directories and the required files; see Installation directories and files for details.

For more information about the `installms` command, see the man page or the CSM for AIX and Linux: Command and Technical Reference.

### Setting up the Linux /csminstall partition

Set up the `/csminstall` partition before you run the `installms` command. See Create the Linux /csminstall partition. If you do not set up the `/csminstall` partition before you run the `installms` command, the command creates the `/csminstall` directory in the root (`/`) partition.

### Installing CSM for Linux software

Ensure that `csm.core` is installed on the management server. If you are installing CSM from the CD, ensure that the CD is mounted. See the instructions in Install the Linux csm.core package.

Perform the installation as follows:

1. Log in as root to the server you have selected as your management server.
2. If you are installing CSM from a directory instead of from the product CDs, follow the instructions in Download CSM for Linux packages to download CSM.
3. Run the `installms` command with the `-p pkg_path` flag, specifying a colon-separated list of package paths. Specify the mount point of the CD-ROM or directory in which the CSM packages reside, and the directory containing any downloaded RPM packages. If you have copied the Linux distribution CDs to a directory, that directory is in the path.
Specify the directories containing the newest versions of RPM packages for `-p pkg_path`. For example, first specify the directory containing downloaded packages, then specify the CSM directory. If the contents of the Linux distribution CDs are in a directory, specify that directory last.

If your management server is running Red Hat EL with a Quarterly Update (QU) or SLES with a Service Pack (SP), you might be prompted for the corresponding Quarterly Update or Service Pack CDs when you run the `installms` command.

**Examples:**

1. If the CSM packages are on a CD, and other downloaded RPMs such as `autoupdate` are in the `/tmp/csm` directory, run the `installms` command as follows:

   ```sh
ingstallms -p /tmp/csm:/media/cdrom
   ```

   **Note:**
   - The CSM packages CD must be mounted to `/media/cdrom` manually before running this command.
   - The device drive name (`/media/cdrom`) varies depending on the device drive configuration.
   - If the directory `/media/cdrom` does not exist, it needs to be created manually.

2. If the CSM packages are in a directory called `/tmp/csm`, and other downloaded RPMs such as `autoupdate` are in a directory called `/tmp/csmreqs`, run the `installms` command as follows:

   ```sh
ingstallms -p /tmp/csmreqs:/tmp/csm
   ```

If `installms` is unable to find all required distribution RPMs in the `-p pkg_path`, it prompts you to insert the Linux distribution CDs into the drive. The program automatically mounts and unmports the CDs as necessary, and copies the Linux RPMs that are required to the `/csminstall` directory.

The CSM, Linux distribution, and open source packages are used to install the management server, and some of the packages are used later to install the install servers and the nodes. The `installms` command determines whether the code needs to be installed (if it is missing or back level), and then installs or replaces the required packages, as necessary.

**Note:**
If the CSM packages, open source packages, or Linux distribution packages are in directories, be sure to specify each directory with the `-p` flag.

**Diagnosing Linux installation command errors**

If any of the following errors occur when you run the `installms` command, verify that all required software updates and fixes have been installed. See [Updating CSM for Linux](#) for more information.

**Device busy**
If you get a device-busy message while running the `installms` command, ensure that your current directory is not `/cdrom` or `/media/cdrom`. Running the `installms` command while in these directories causes a device-busy condition because it interferes with the mounting and unmounting of Linux distribution CDs.

**Command not found**
If the `installms` command is not found, make sure your PATH environment variable includes `/opt/csm/bin` and check for the existence of the `installms` command in that directory. If it does not
exist in /opt/csm/bin, make sure that the csm.core package has been installed. If it is not installed, see Install the Linux csm.core package.

Prerequisite software not copied

After running the installms command, if the CSM packages and prerequisite software are not copied to the /csminstall subdirectories, CSM displays an error message. Verify that the files are in the path that you passed to the installms command. If they are not in the path, gather the missing files, put them in a directory with the rest of the files, and run the installms command again. Also, check the command usage to verify that you used the command correctly.

If you get a conflicts error, uninstall the package that the message specifies.

If other errors occur, check the log file for the installms command /var/log/csm/installms.log. The log file contains error and informational messages that are useful when debugging problems.

---

**Choosing a Linux remote shell**

A distributed shell program (dsh) is used to issue remote commands from the management server to the nodes. It is contained in the csm.dsh RPM. The dsh program uses a remote shell of your choice to issue remote commands to the managed nodes. The default remote shell is /usr/bin/ssh, but you can specify a different remote shell (/usr/bin/rsh) by running the csmconfig command with attribute value pairs.

**Attributes for the remote shell:**

Two csmconfig attributes affect the remote shell:

- RemoteShell
  Stores the pathname of the executable that dsh uses to run remote commands.
- SetupRemoteShell
  Indicates to CSM that you want the remote shell to be automatically configured (1 = yes, 0 = no).

CSM can automatically configure OpenSSH during both operating system and CSM-only installations. However, CSM can only configure rsh during an operating system installation or when the root user is able to issue rexec commands to the nodes. In any other situation, you must manually configure rsh.

Run the csmconfig command to display the current values for the RemoteShell and SetupRemoteShell attributes. You can set the RemoteShell and SetupRemoteShell attributes to other values. For example, the following command sets the remote shell to rsh and instructs CSM to not automatically set it up:

```bash
csmconfig RemoteShell=/usr/bin/rsh SetupRemoteShell=0
```

You can also temporarily change the remote shell setting with the DSH_REMOTE_CMD environment variable. To switch from the default ssh shell to rsh, specify the DSH_REMOTE_CMD environment variable with the full path name of the remote shell command:

```bash
export DSH_REMOTE_CMD=/usr/bin/rsh
```

For more information about using the RemoteShell attribute, see the csmconfig and dsh man pages or the CSM for AIX and Linux: Command and Technical Reference.
Choosing NFS or HTTP for Linux installation

If you are using HTTP to install large scale clusters, see Setting up an HTTP server manually for details on configuring Apache for improved scaling.

CSM allows you to choose NFS or HTTP for installing the Linux operating system on cluster nodes. If you choose HTTP for installation, CSM also offers automatic setup of the Apache 2 HTTP server on the install server.

By default, CSM uses NFS to do node installations, but you can specify HTTP as the install protocol, and have Apache 2 setup automatically by running the `csmconfig` command with attribute value pairs.

Attributes for the Network Install Protocol:

Two `csmconfig` attributes are used to indicate how CSM should set up the cluster for network installations:

- **NetworkInstallProtocol**
  - Selects the network protocol that will be used to do the network install. Valid values are **NFS** and **HTTP**. The default is **NFS**.
- **SetupNetworkInstallProtocol**
  - If this attribute is set to **1** and `NetworkInstallProtocol` is also set to **HTTP**, CSM installs and configures the Apache 2 HTTP server. If this attribute is set to **0** and `NetworkInstallProtocol` is set to **HTTP**, you must set up an HTTP server.

If `NetworkInstallProtocol` is set to **NFS**, the `SetupNetworkInstallProtocol` attribute is ignored. CSM sets up an NFS server on the install server regardless of the `NetworkInstallProtocol` or `SetupNetworkInstallProtocol` values, because use of NFS by CSM is not limited to operating system installation.

If `NetworkInstallProtocol` is set to **HTTP** and `SetupNetworkInstallProtocol` is set to **1**, CSM installs and configures the Apache 2 HTTP server on the install server. When the node installations are complete, CSM does not turn the HTTP server off, which allows you to continue to use the HTTP server.

If `NetworkInstallProtocol` is set to **HTTP**, and `SetupNetworkInstallProtocol` is set to **0**, you must manually set up an HTTP server on the install server.

For more information about using these attributes, see the `csmconfig` man page or the CSM for AIX and Linux: Command and Technical Reference.

Install Kerberos Version 5 for remote Linux commands (optional)

This step is required to set up Kerberos for remote commands with `rsh` or `ssh`. The Kerberos server can be one of the following servers:

- The CSM management server
- A server outside the CSM cluster with the CSM management server configured as a Kerberos client of the Kerberos server. To set up HA MS, ensure that the Kerberos server is on a node
outside the CSM cluster and not on the primary management server or the backup management server.

**To use the CSM management server as the Kerberos server**, do the following:

1. Install the Kerberos server packages listed in CSM for AIX Kerberos setup.
2. Configure the Kerberos server by following the directions for your Linux distribution.
3. Verify that the Kerberos server is started, and that you can get a ticket as the Kerberos administrator. Use the following command:

   ```
kinit admin_principal
   ```

   If you receive error messages, review your Kerberos documentation to determine the cause and repair the problem. For Linux management servers, you must set up the Kerberos server and be able to run as the Kerberos administrator before you do Set up Kerberos Version 5 for remote Linux command processing (optional).

**To configure the management server as a client of a separate Kerberos server**, do the following:

1. Install the Kerberos client software on the management server. See CSM for AIX Kerberos setup
2. Configure the Kerberos client by copying the `krb5.conf` file from the Kerberos server to the following location on the management server:

   ```
   /etc/krb5.conf
   ```

   Copy the Kerberos packages to the management server for use when you add nodes to the cluster.

CSM provides the `/etc/opt/csm/csmkrb5.conf.default` configuration file, which provides the location of the Kerberos Version 5 libraries on Linux.

The default configuration file provides search paths for Kerberos API libraries on Linux. Because of the many distributions of Kerberos supported on Linux, this configuration file allows the administrator to customize where the Linux Kerberos API libraries are installed and to supply that information to the CSM Kerberos configuration scripts and executable files.

To specify different locations for the Kerberos libraries, do the following:

1. Copy `/etc/opt/csm/csmkrb5.conf.default` to the following location:

   ```
   /etc/opt/csm/csmkrb5.conf
   ```

2. Make the changes in the `csmkrb5.conf` file.

The routines check for `/etc/opt/csm/csmkrb5.conf` first and if the file exists use the file. Because the file `csmkrb5.conf.default` can be updated during a CSM update, do not modify that file. If a `csmkrb5.conf` file has been created, you must copy the file to the `/etc/opt/csm` directory on the node before the `updatenode` command runs in order for the Kerberos Version 5 setup to succeed on the node. Use a customization script to do the copy during a new node install.
Install ssh for Kerberos Version 5 Linux commands

This step is required to use Kerberos with ssh. The ssh packages installed with your Linux distribution might not be enabled to use Kerberos. Obtain or build the appropriate Kerberos enabled ssh packages for your distribution and install them now.

Accepting the CSM for Linux license

CSM is available with a full production license. For general planning information on these options, see CSM license requirements.

Accepting the CSM for Linux full license agreement

To accept the CSM for Linux full license agreement:

1. The csmlum.full license key is located on the CSM CD-ROM. You will use the key file as input for the csmconfig command, in the next step.
2. Accept the license and activate the license key, using the mount and csmconfig commands. Enter the following commands:

   ```bash
   mount /dev/cdrom /media/cdrom
   csmconfig -L /media/cdrom/csmlum.full
   ```

   At the prompt, follow the directions to accept the CSM license.

3. The csmconfig command returns output similar to the following. Because you accepted the full license, the ExpDate attribute is blank.

   ```bash
   csmconfig
   AddUnrecognizedNodes = 0 (no)
   BMCConsoleEncryptAuth = 1 (yes)
   BMCConsoleKeepAlive = 0 (no)
   BMCConsolePerMsgAuth = 0 (no)
   CFMRootDir = /cfmroot
   ClusterSNum =
   ClusterTM = 9078-160
   CSMAadminID = root
   CSMLogDir = /var/log/csm
   DeviceStatusFrequency = 12
   DeviceStatusSensitivity = 8
   ExpDate =
   HAMode = 0
   HeartbeatFrequency = 12
   HeartbeatSensitivity = 8
   MaxNumNodesInDomain = -1 (unlimited)
   NetworkInstallProtocol = nfs
   PowerPollingInterval = 300
   PowerStatusMode = 1 (Events)
   Properties =
   RegSyncDelay = 1
   ```
The step is required to use hardware control for Linux nodes; see also Managing hardware control points.

System x x336/x346 and later servers with RSA-II SlimLine Adapters installed: You need to define the user IDs and passwords that are required to access each RSA (Remote Supervisor Adapter) and ISMP (IBM Integrated System Management Processor). To configure xSeries servers, change 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).

HMC-attached pSeries hardware: Issue the systemid command. For example, if the host name of the HMC is hmc1 and the user ID is hscroot, issue the following command:

```
systemid hmc1 hscroot
```
You will be prompted for a password for the user ID you specified.

Devices that use the APC MasterSwitch: Issue the systemid command. For example, if the APC MasterSwitch name is apc01.pok.ibm.com, issue the following command:

```
systemid apc01.pok.ibm.com USERID
```
You will be prompted for a password for the user ID you specified.

BladeCenter 8677: To configure BladeCenter Management Modules, change the default hardware control point Login Profile user ID and password using the Management Module web interface and documentation provided with the hardware.

For BladeCenter Management Modules, the default Login Profile user ID is USERID and the default password is PASSW0RD (P-A-S-S-W-zero-R-D).

BladeCenter and System x x336/x346 and later servers using SOL: For BladeCenter (other than HS20-8678) blade servers, and for xSeries 336 and 346 servers using SOL, run the systemid -c command to store the Login Profile user ID and password required to access the SOL feature.

For BladeCenter Management Modules, the default console user ID is RMTCON, and the default console password is RMTCON (R-M-T-C-zero-N). Change the default console Login Profile user ID and password using the Management Module web interface and documentation provided with the hardware. You should not use a Login Profile with supervisor privileges for console access. If the default console Login Profile user ID is not used, the new Login Profile should only be granted Blade Console remote access privileges.

IVM managed System p hardware: Issue the systemid command. For example, if the host name of the IVM is ivm1 and the user ID is padmin, issue the following command:
systemid ivm1 padmin

You will be prompted for a password for the user ID you specified.

eServer 325 and 326 servers, and System x x336/346 and later servers with no RSA-II SlimLine Adapter installed: Issue the systemid command. For example, if the BMC name is bmc01.pok.ibm.com, issue the following command:

systemid bmc01.pok.ibm.com USERID
You will be prompted for a password for the user ID you specified.

The systemid command stores the user ID and password for remote hardware.

If you plan to use Cluster-Ready Hardware Server, before proceeding to Install user-defined power methods on a Linux management server (optional), see Planning for Cluster-Ready Hardware Server (CRHS) and the CSM for AIX and Linux: Administration Guide.

Install user-defined power methods on a Linux management server (optional)

To install a user-defined power method for hardware control, place the power method in the following directory on your Linux management server:

/opt/local

For details, see User-defined power methods.

Change Linux power control attributes (optional)

You can use the csmconfig command to change the cluster PowerStatusMode and PowerPollingInterval attributes. See Power status mode for more information.

Verifying and troubleshooting the CSM for Linux installation

To verify that the management server has installed correctly and is ready for use, you can run the ibm.csm.ms probe, which is shipped with CSM. To run the probe issue the following command.

probemgr -p ibm.csm.ms -l 0

For information about CSM support for probes, see the CSM for AIX and Linux: Administration Guide.
Set up Kerberos Version 5 for remote Linux command processing

(optional)

Ensure that one of the following is true:

- The management server is the Kerberos server
- The management server is configured as a client of a Kerberos server that is not part of the CSM cluster. If you plan to setup HA MS, ensure that the Kerberos Server is on a node outside the CSM cluster and not on the primary management server or the backup management server.

See [CSM for AIX Kerberos setup](#).

CSM can provide some automated setup of Kerberos Version 5 as follows:

- Create a CSM principal in the Kerberos database.
- Create a host principal in the Kerberos database for each node defined to the CSM cluster.
- Place the CSM principal name in the `.k5login` file in the home directory of root on each managed node.
- Transfer the host principal keytab to each managed node.

See [CSM for AIX Kerberos setup](#).

You can use the `csmconfig` command to set up Kerberos for CSM. The `csmconfig` command provides various options for Kerberos that you can specify according to the needs of your environment. These options determine the extent of CSM set up for Kerberos including the set up of the Kerberos client and the creation of principals.

The format of the `csmconfig` command for the Kerberos options is as follows, where `n` is a number from 0 to 14:

```
csmconfig SetupKRB5=n
```

The values for `n` in the `csmconfig` command and the corresponding CSM actions for Kerberos are as follows:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>No CSM setup of Kerberos (default)</td>
</tr>
<tr>
<td>1</td>
<td>CSM is to configure a Kerberos server on an AIX management server. <strong>Unavailable on Linux:</strong> Specifying the value results in an error message.</td>
</tr>
<tr>
<td>2</td>
<td>CSM is to set up the Kerberos client on the managed nodes.</td>
</tr>
<tr>
<td>4</td>
<td>CSM is to create the required CSM principals in Kerberos. You are prompted to enter the Kerberos Version 5 administrator principal name and password.</td>
</tr>
<tr>
<td>8</td>
<td>CSM is to create required host principals in Kerberos. You are prompted to enter the Kerberos Version 5 administrator principal name and password.</td>
</tr>
</tbody>
</table>
You can add any of the values of $n$ to specify one or more actions. For example, if you want CSM to do all the valid Kerberos setup for the cluster, add the corresponding values for each action (2+4+8=14) and specify the following `csmconfig` command to generate the required CSM Kerberos principal:

```
csmconfig SetupKRB5=14
```

If the managed nodes are already part of a Kerberos realm, and you only want to enable CSM to use Kerberos for remote command authentication, specify the following `csmconfig` command:

```
csmconfig SetupKRB5=4
```

You use the `SetupKRB5` attribute to direct processing by the `updatenode` command and during the installation of a node. For information see the `updatenode` command in *CSM for AIX and Linux: Command and Technical Reference* or the man pages.

The only `SetupKRB5` option supported for management servers running SLES is the following:

```
csmconfig SetupKRB5=4
```

In this case, the CSM principal is NOT created; however, CSM displays a message that gives the name of the CSM principal. The system administrator must use Kerberos commands to create the indicated principal and an associated keytab as directed by the message. CSM commands and `cron` jobs use the CSM principal and keytab to authenticate when you set the option SetupKRB5=4.

When you complete the installation process, you need to do the following tasks:

- Set up the nodes as Kerberos clients.
  
  For setting up the client nodes, see [Provide Kerberos client packages for Linux (optional)](#).

- Enable Kerberos command processing.
  
  For enabling Kerberos, see [Enabling remote commands to use Kerberos Version 5 authentication](#).

---

### Enable Web-based client download on Linux (optional)

To enable a download of the IBM Web-based System Manager for AIX client from a CSM for Linux on System p management server, you must run the `setWebSMClientDownload` command. For details on Web-based System Manager, see the *IBM CSM for AIX and Linux: Administration Guide*.

If running Apache 2 webserver, enter:

```
/usr/websm/bin/setWebSMClientDownload
```

If running a webserver other than Apache 2, enter:

```
/usr/websm/bin/setWebSMClientDownload --docroot dir
```

Where `dir` is the document root location for your webserver.
Chapter 7. Setting up install servers

Separate install servers can be used to increase the scalability and performance of CSM cluster node installations, for mixed operating system node installations, and as file servers for node updates. If you do not use separate install servers, your management server is your install server.

A CSM install server is a system that can be used as a file server for node updates or to run the boot service that responds to network boot requests and from which operating system installations are driven. For Linux network installations, this is the system that responds to PXE (System x) and bootp (System p) requests. For AIX network installations, this is the AIX Network Installation Manager (NIM) master that responds to bootp requests. CSM supports the creation of multiple install servers which can all be managed from either a Linux or an AIX management server.

Install servers provide the following functionality:

- Installation capability for operating systems other than the management server operating system.
- Improved installation scaling and performance.
- Install servers may be created at remote locations to help facilitate full install support and provide better installation performance.
- Distributing files to install servers can improve performance when updating nodes with the updatenode command.

The CSM management server or selected cluster nodes may be used as install servers. The decision as to what install servers are needed will depend on the particular cluster environment. For example, if the cluster consists of all AIX nodes, the management server can be used as the install server for the whole cluster. If the cluster is a mix of AIX and Linux systems then at least one install server must be set up for each type of operating system.

When using a cluster node instead of the management server as an install server, the install server node must be defined, installed and added to the cluster before defining or installing the other nodes.

An install server can be used to install different operating system levels but not different operating system distributions. A separate install server is required for each operating system distribution; a Red Hat EL install server is required for Red Hat EL nodes, and a SLES install server is required for SLES nodes.

Install server limitations

The following limitations apply to separate install servers:

- If your CSM management server is running Kerberos, your install servers must also be set up with Kerberos. If your install servers are not set up with Kerberos, your CSM management server must be set up with Kerberos Version 5 and std. If using NIM, std authentication must be enabled for the NIM master. CSM automatically sets up the authentication for an install server if requested.
- Linux install servers are not supported on Red Hat EL WS 4/4.5/4.6/4.7. These distributions do not contain the services required to drive installations.
For clusters with an AIX management server and Linux install servers, the `cpio` RPM on the AIX Linux Toolkit CD must be installed on the CSM management server. The `cpio` function provided with base AIX does not work for extracting files from a Linux rpm, but the open version from the Toolkit CD does work for both AIX and Linux.

- pSeries nodes using the CSP hardware control method are not supported from a Linux management server. CSP nodes can only be attached to an AIX management server.
- If you are using RDM with CSM, see the IBM Director information in the *CSM for AIX and Linux: Administration Guide* for restrictions.
- Install servers must run CSM 1.5.0, or later.

---

**Cluster configurations using install servers**

The management server must have network connectivity to each of its nodes through an Ethernet connection; this connectivity is referred to as the *CSM Cluster Network*. This network is used by the management server to manage the cluster nodes. As a cluster node, the install server must also be connected to the cluster network. An install server must also have network connectivity to each of the nodes it serves. The cluster network connecting the install server to its nodes can be the cluster network or a separate network.

CSM requires that both the install server and the nodes that it serves must be able to do full host name resolution on each other. This information will be provided to the node during full install, but must be manually added to the install server's `/etc/hosts` file or DNS, and added to the nodes' `/etc/hosts` file or DNS if you are doing CSM only installs.

An install server must be network connected to the nodes that it serves, either directly through a local subnet, or indirectly through one or more gateways. An install server for Linux on System p nodes is configured as a DHCP server, and processes `bootp` requests from the nodes. An install server for Linux on System x nodes is configured as a DHCP server, and processes PXE requests from the nodes.

If your Linux nodes are connected across a gateway from the Linux install server, see [Network requirements](#) for the network setup requirements. If the gateway is a Linux node other than the install server, do the following to install nodes across the subnet:

1. Set the `InstallAdapterNetmask` and `InstallAdapterGateway` node attributes to correspond to the gateway server closest to the node.
2. Configure and enable the dhcp-relay daemon on the gateway server closest to the node to allow `bootp` replies from the dhcp server to travel across the subnet.
3. On the gateway server closest to the node, add a permanent `arp` entry for the node. For example:
   ```
   arp -s node1.cluster.com 00:02:55:AF:CE:6E
   ```
4. If the `/etc/dhcpd.conf` generated by CSM does not contain a subnet stanza for the node, the subnet stanza must be added. Use the `mkdhcp` command to add a subnet. For example, if the install server is located within subnet 192.168.0.0 and nodes are within subnet 172.20.0.0, run:
   ```
   mkdhcp --add -s 172.20.0.0 Netmask=255.255.0.0
   ```

   When the `csmsetupinstall` command is run, the nodes across the gateway are added to the correct subnet.
Note:
For some network configurations, CSM does not automatically add node entries to the /etc/dhcpd.conf stanza that you added; in this case, you must add node entries manually. To ensure that CSM does not modify the /etc/dhcpd.conf file once you have edited it, set the CSM_NO_SETUP_DHCP environment variable.

For System x installations, the nodes must be on a local subnet with the install server to properly capture node PXE broadcasts over the network. CSM configures a DHCP server on each install server to provide static IP addresses based on MAC addresses or UUIDs for each node. The DHCP server on the install server processes the broadcast PXE requests, and requires all nodes to be on a local subnet to that install server. This network can be different than the CSM cluster network.

CSM allows multiple Linux install servers to exist on the same subnet. A CSM node group must be created to contain this set of install servers. CSM configures the DHCP and PXE services identically across the group of install servers. CSM configures the DHCP configuration files on each server to have identical static IP address lists, and unique dynamic address ranges so that two servers do not serve the same dynamic address to different target nodes. For targeted requests such as NFS, a server is chosen at random from this group to service a particular node. This improves NFS, tftp, and DHCP scaling for simultaneous installations across the subnet.

CSM does not provide special support for multiple AIX install servers on the same subnet. To set up multiple install servers on a subnet, the set of nodes that are to be serviced by each server must be unique. A node can only have one NIM master defined.

The CSM management server must have remote shell capability (dsh, dcp) to the install server. This may be set up automatically when the install server is added to the cluster as a managed node.

Install server node attributes

When defining install server nodes and the other cluster nodes, certain node attributes must be set depending on the cluster configuration. In the sample configurations described below, the following attributes are described. For a complete list of node attributes, refer to Defining nodes, and the nodeattributes man page.

Hostname

The host name or IP address associated with the node's network interface as known by the management server; IP addresses are not supported for AIX. This is the network interface used to manage the node.

ManagementServer

The host name or IP address of the management server as known by the node. The definenode command automatically sets the ManagementServer attribute value to the IP address; you do not typically have to define or change this attribute. This attribute can be edited.

InstallServer

The host name or IP address of the install server as known by the management server, and an optional directory that will serve the CSM install files to this node. The format is:

install_server[:install_directory]
If not defined, the management server serves as the install server, and the directory that will serve
the CSM install files is /esminstall. If install_server is specified, the install server must be a node
in the cluster. If an install_directory is not specified, it is assumed to be /csmsserver.

For example, to specify only the name of the install server, iserver1.clusters.com, enter:

```text
iserver1.clusters.com
```

To specify the name of the install server, **iserver1.clusters.com**, and a directory called
/mydirectory, enter:

```text
iserver1.clusters.com:/mydirectory
```

To ensure enough space for the CSM repository, you may wish to create the install_directory as a
separate file system. It will have size requirements similar to /esminstall on the management server.
The CSM code will copy the CSM directories and files into the specified install server directory.
You should not store other data in the install server directory.

If you are configuring multiple Linux install servers on the same subnet, you must create an install
server nodegroup and the InstallServer attribute must be set to the value "+" followed by a
nodegroup name, optionally followed by a ":" and directory name.

For example, if the install server node group is ISGroup1 then you could set the InstallServer value
to:

```text
+ISGroup1:/mydirectory
```

**InstallAdapterHostname**
The hostname or IP address of the node as known by the install server. The value is the hostname
used to connect to the node during the installation, and the value assigned to the install adapter
when it is configured on the node during installation. If left blank, the Hostname attribute value is
used by default.

**InstallServerAKBNode**
The hostname or IP address of the install server as known by the node. If there are multiple Linux
install servers on the same subnet, this attribute is ignored, and the network connection on the
install server that is used by the node is dynamically determined. If left blank, CSM determines this
value dynamically during runtime. If there are multiple connections from a Linux install server to
the installation subnet that the node is on, one connection is chosen at random.

**InstallAdapterGateway**
Specifies the hostname or IP address of the network gateway that connects the node's subnet to the
install server's subnet. CSM sets the gateway on the node to the InstallAdapterGateway.

If there is no gateway required between the node and the install sever, the InstallAdapterGateway
attribute may be used to specify the gateway between the node and the management server.

If different gateways are required between the node and the install server, and the node and the
management server, use InstallAdapterGateway to specify the gateway between the node and the
install server. The gateway between the node and the management server must be configured using
the secondary adapter configuration mechanism described in Secondary adapter interface
configuration.
If a single adapter on the node requires different gateways to get to the management server and the install server, the `InstallAdapterGateway` attribute should be set to the gateway to the install server. Configure the gateway to the management server using a pre-reboot customization script.

The following configuration examples illustrate how install servers can be used in a CSM cluster environment.

**Note:**

CSM supports multiple install servers and multiple nodes per install server even though the examples show only one of each.

The following diagrams represent some common network configurations. If your management server, install servers and nodes are connected in a different configuration, you should use an install pre-reboot customization script to configure your adapters.

**Configuration #1A - The management server is the install server**

![Diagram showing CSM Management Server (MSA) and Node A.]

In this case, set this group of node attributes as follows for the cluster node:

**Table 31. Configuration #1A node attributes**

<table>
<thead>
<tr>
<th>Attribute name</th>
<th>Attribute value</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>NodeA</td>
<td>The name of the node as it is known by the management server.</td>
</tr>
<tr>
<td>ManagementServer</td>
<td>MSA</td>
<td>The name of the management server as it is known by this node.</td>
</tr>
<tr>
<td>InstallServer</td>
<td>no value.</td>
<td>Defaults to the <code>ManagementServer</code> attribute value.</td>
</tr>
<tr>
<td>InstallAdapterHostname</td>
<td>no value.</td>
<td>Defaults to the <code>Hostname</code> attribute value.</td>
</tr>
<tr>
<td>InstallServerAKBNode</td>
<td>no value.</td>
<td>None.</td>
</tr>
<tr>
<td>InstallAdapterGateway</td>
<td>no value.</td>
<td>The gateway closest to the node.</td>
</tr>
</tbody>
</table>
**Configuration #1B - The management server is the install server; gateway between management server and node**

This configuration is supported for general CSM use, but for operating system installation, this configuration is only supported for Linux on System p, and AIX.

**Table 32. Configuration #1B node attributes**

<table>
<thead>
<tr>
<th>Attribute name</th>
<th>Attribute value</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>NodeB</td>
<td>The name of the node as it is known by the management server.</td>
</tr>
<tr>
<td>ManagementServer</td>
<td>MSA</td>
<td>The name of the management server as it is known by this node.</td>
</tr>
<tr>
<td>InstallServer</td>
<td>no value</td>
<td>Defaults to the ManagementServer attribute value.</td>
</tr>
<tr>
<td>InstallAdapterHostname</td>
<td>no value</td>
<td>Defaults to the Hostname attribute value.</td>
</tr>
<tr>
<td>InstallServerAKBNode</td>
<td>no value</td>
<td>None.</td>
</tr>
<tr>
<td>InstallAdapterGateway</td>
<td>GWB</td>
<td>None.</td>
</tr>
</tbody>
</table>
Configuration #1C - The management server is the install server; two subnets between management server and node

In this configuration, the management server is acting as the install server. The node is installed through Subnet A, but communicates with the management server through Subnet B after installation. Normally, the InstallServerAKBNode is used to indicate the name of the install server as known by the node, but in this case, the management server is the install server, so InstallServerAKBNode can be used to refer to the hostname of the management server that is on the subnet used for installation. The NodeB adapter must be configured as a secondary adapter. See Secondary adapter interface configuration for details. Setting this secondary adapter attribute causes CSM to configure the adapter on the node, and allows the node to connect to the management server at the end of the install process, when it changes the node's Mode attribute to Managed.

Table 33. Configuration #1C node attributes

<table>
<thead>
<tr>
<th>Attribute name</th>
<th>Attribute value</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>NodeB</td>
<td>The name of the node as it is known by the management server.</td>
</tr>
<tr>
<td>ManagementServer</td>
<td>MSB</td>
<td>The name of the management server as it is known by this node.</td>
</tr>
<tr>
<td>InstallServer</td>
<td>MSB or no value</td>
<td>The name of the management server, or leave it blank.</td>
</tr>
<tr>
<td>InstallAdapterHostname</td>
<td>NodeA</td>
<td>The name of the node, this hostname connects to the installation subnet.</td>
</tr>
<tr>
<td>InstallServerAKBNode</td>
<td>MSA</td>
<td>The name of the install server as known by the node.</td>
</tr>
<tr>
<td>InstallAdapterGateway</td>
<td>no value</td>
<td>The name of gateway from the node to the management server</td>
</tr>
<tr>
<td>InstallAdapter*</td>
<td>various values</td>
<td>InstallAdapterNetmask, InstallAdapterMacaddr, for example</td>
</tr>
</tbody>
</table>
Configuration #2 - The management server, install server, and node are on the same subnet

In this case this group of node attributes set as follows for the install server and the node that it serves:

Table 34. Install server

<table>
<thead>
<tr>
<th>Attribute name</th>
<th>Attribute value</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>ISA</td>
<td>The name of the node as it is known by the management server.</td>
</tr>
<tr>
<td>ManagementServer</td>
<td>MSA</td>
<td>The name of the management server as it is known by this node.</td>
</tr>
<tr>
<td>InstallServer</td>
<td>no value</td>
<td>Defaults to the ManagementServer attribute.</td>
</tr>
<tr>
<td>InstallAdapterHostname</td>
<td>no value</td>
<td>Defaults to the Hostname attribute.</td>
</tr>
<tr>
<td>InstallServerAKBNode</td>
<td>no value</td>
<td>CSM dynamically determines the correct connection to the install server; because InstallServer also has no value, the ManagementServer attribute is used.</td>
</tr>
<tr>
<td>InstallAdapterGateway</td>
<td>no value</td>
<td>None.</td>
</tr>
</tbody>
</table>

Table 35. Configuration #2 node attributes

<table>
<thead>
<tr>
<th>Attribute name</th>
<th>Attribute value</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 36. Configuration #3 install server attributes

<table>
<thead>
<tr>
<th>Attribute name</th>
<th>Attribute value</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>ISA</td>
<td>The name of the node as it is known by the management server.</td>
</tr>
<tr>
<td>ManagementServer</td>
<td>MSA</td>
<td>The name of the management server as it is known by this node.</td>
</tr>
<tr>
<td>InstallServer</td>
<td>ISA</td>
<td>The name of the install server as known by the management server.</td>
</tr>
<tr>
<td>InstallAdapterHostname</td>
<td>no value</td>
<td>Defaults to the Hostname value.</td>
</tr>
<tr>
<td>InstallServerAKBNode</td>
<td>no value</td>
<td>The code will dynamically determine the correct connection to the install server.</td>
</tr>
<tr>
<td>InstallGateway</td>
<td>no value</td>
<td>None.</td>
</tr>
<tr>
<td>InstallAdapter*</td>
<td>various values</td>
<td>InstallAdapterNetmask, InstallAdapterMacaddr, for example.</td>
</tr>
</tbody>
</table>

Configuration #3 - The install server acts as a gateway between management server and node

In this case this group of node attributes set as follows for the install server and the node that it serves:

Table 36. Configuration #3 install server attributes
Table 37. Configuration #3 node attributes

<table>
<thead>
<tr>
<th>Attribute name</th>
<th>Attribute value</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>NodeB</td>
<td>The name of the node as it is known by the management server.</td>
</tr>
<tr>
<td>ManagementServer</td>
<td>MSA</td>
<td>The name of the management server as it is known by this node.</td>
</tr>
<tr>
<td>InstallServer</td>
<td>ISA</td>
<td>The name of the install server as known by the management server.</td>
</tr>
<tr>
<td>InstallAdapterHostname</td>
<td>no value</td>
<td>Defaults to the Hostname value.</td>
</tr>
<tr>
<td>InstallServerAKBNode</td>
<td>ISB</td>
<td>The name of the install server as known by this node.</td>
</tr>
<tr>
<td>InstallAdapterGateway</td>
<td>ISB</td>
<td>The gateway is the install server as known by the node, because the install server is acting as the gateway.</td>
</tr>
</tbody>
</table>
Configuration #4A - The management server communicates to node and install server across different subnets (SubnetA and SubnetB respectively); install server installs node across third subnet (SubnetC)

In this case this group of node attributes set as follows for the install server and the node that it serves:

**Table 38. Configuration #4A install server attributes**

<table>
<thead>
<tr>
<th>Attribute name</th>
<th>Attribute value</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>ISB</td>
<td>The name of the node as it is known by the management server.</td>
</tr>
<tr>
<td>ManagementServer</td>
<td>MSB</td>
<td>The name of the management server as it is known by this node.</td>
</tr>
<tr>
<td>InstallServer</td>
<td>no value</td>
<td>Defaults to the ManagementServer attribute value.</td>
</tr>
<tr>
<td>InstallAdapterHostname</td>
<td>no value</td>
<td>Defaults to the Hostname attribute value.</td>
</tr>
<tr>
<td>InstallServerAKBNode</td>
<td>no value</td>
<td>CSM dynamically determines the correct connection to the install server.</td>
</tr>
<tr>
<td>InstallAdapterGateway</td>
<td>no value</td>
<td>None.</td>
</tr>
</tbody>
</table>

**Table 39. Configuration #4A node attributes**

<table>
<thead>
<tr>
<th>Attribute name</th>
<th>Attribute value</th>
<th>Notes</th>
</tr>
</thead>
</table>
| CSM for AIX and Linux: Planning and Installation Guide 109
<table>
<thead>
<tr>
<th><strong>Hostname</strong></th>
<th><strong>NodeA</strong></th>
<th>The name of the node as it is known by the management server.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ManagementServer</strong></td>
<td><strong>MSA</strong></td>
<td>The name of the management server as it is known by this node.</td>
</tr>
<tr>
<td><strong>InstallServer</strong></td>
<td><strong>ISB</strong></td>
<td>The name of the install server as known by the management server.</td>
</tr>
<tr>
<td><strong>InstallAdapterHostname</strong></td>
<td><strong>NodeC</strong></td>
<td>The name of the node as known by the install server.</td>
</tr>
<tr>
<td><strong>InstallServerAKBNode</strong></td>
<td><strong>ISC</strong></td>
<td>The name of the install server as known by this node.</td>
</tr>
<tr>
<td><strong>InstallAdapterGateway</strong></td>
<td>no value</td>
<td>None.</td>
</tr>
<tr>
<td>*<em>InstallAdapter</em>”</td>
<td>various values</td>
<td>*InstallAdapterNetmask, InstallAdapterMacaddr, for example.</td>
</tr>
</tbody>
</table>

**Note:**

Two adapters on the node in this configuration must be configured; one connected to Subnet C and one connected to subnet A. The Subnet C adapter is automatically configured during the installation process. The Subnet A adapter must be configured for the node to communicate with the management server and become a managed node. For AIX nodes, the adapter can be configured using the AIX NIM support for secondary adapter configuration; see the AIX installation documentation and the nimadapters man page.

For Linux nodes this adapter can be configured using the CSM sample customization script provided. The sample script, adapter_config_Linux and ibAdapterConfig, and the associated README file are located in the /csminstall/csm/scripts and /opt/csm/samples/ib directory on the CSM management server.

See the Optional tools and services in the CSM for AIX and Linux: Administration Guide for other sample scripts.
Configuration #4B - The management server, install server, and nodes are on different networks; node connects to management server and install server via different gateways

This configuration is supported for general CSM use, but for operating system installation, this configuration is only supported for Linux on System p and AIX on System p.

In this complicated network setup, the management server and the install server are on the same subnet, but the node is on a different subnet. The node must go through one gateway (Gateway 1) to get to the install server, and another gateway (Gateway 2) to get to the management server. The install server is not acting as a gateway between the node and the management server.

In this configuration, there are two gateways, but only one InstallAdapterGateway attribute. In this case, you should set the InstallAdapterGateway attribute to the gateway between the node and the install server (Gateway 1). This will allow CSM to install the node from the install server.

The gateway between the node and the management server (Gateway 2) must be added as either a "GATEWAY" attribute or as a static route in the secondary adapter configuration for the node. For AIX, only a static route can be used. In this example, "GWE" would be added as the gateway or static route in the "NodeE" secondary adapter configuration. See Secondary adapter interface configuration for details. Setting this secondary adapter attribute causes CSM to configure the adapter on the node, and allows the node to connect to the management server at the end of the install process, when it changes the node's Mode attribute to Managed.

**Table 40. Configuration #4B install server attributes**

<table>
<thead>
<tr>
<th>Attribute name</th>
<th>Attribute value</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>ISB</td>
<td>The name of the node as it is</td>
</tr>
</tbody>
</table>
known by the management server.

<table>
<thead>
<tr>
<th>Attribute name</th>
<th>Attribute value</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>ManagementServer</td>
<td>MSB</td>
<td>The name of the management server as it is known by this node.</td>
</tr>
<tr>
<td>InstallServer</td>
<td>no value</td>
<td>Defaults to the ManagementServer value.</td>
</tr>
<tr>
<td>InstallAdapterHostname</td>
<td>no value</td>
<td>Defaults to the Hostname value.</td>
</tr>
<tr>
<td>InstallServerAKBNode</td>
<td>no value</td>
<td>CSM dynamically determines the correct connection to the install server; since InstallServer is also blank, the ManagementServer attribute is used.</td>
</tr>
<tr>
<td>InstallAdapterGateway</td>
<td>no value</td>
<td>None.</td>
</tr>
</tbody>
</table>

Table 41. Configuration #4B node attributes

<table>
<thead>
<tr>
<th>Attribute name</th>
<th>Attribute value</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>NodeE</td>
<td>The name of the node as it is known by the management server.</td>
</tr>
<tr>
<td>ManagementServer</td>
<td>MSA</td>
<td>The name of the management server as it is known by this node.</td>
</tr>
<tr>
<td>InstallServer</td>
<td>ISB</td>
<td>The name of the install server as known by the management server.</td>
</tr>
<tr>
<td>InstallAdapterHostname</td>
<td>NodeD</td>
<td>The name of the node as known by the install server.</td>
</tr>
<tr>
<td>InstallServerAKBNode</td>
<td>ISC</td>
<td>The name of the install server as known by this node.</td>
</tr>
<tr>
<td>InstallAdapterGateway</td>
<td>GWD</td>
<td>The name of gateway from the node to the install server (Gateway 1). The other gateway (Gateway 2) will need to be configured in the secondary adapter configuration for the NodeE adapter, so that the node can connect to the management server during installation.</td>
</tr>
<tr>
<td>InstallAdapter*</td>
<td>various values</td>
<td>The other InstallAdapter* attributes (InstallAdapterNetmask, InstallAdapterMacaddr) refer to NodeD.</td>
</tr>
</tbody>
</table>
Configuration #5 - Multiple gateways between node and install server

In this configuration, there are two gateways between the node and the install server, and the install server is a gateway itself to the management server. The gateway closest to the node must be specified as the InstallAdapterGateway. This will allow the node to communicate with both the install server and the management server.

Table 42. Configuration #5 install server attributes

<table>
<thead>
<tr>
<th>Attribute name</th>
<th>Attribute value</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>ISA</td>
<td>The name of the node as it is known by the management server.</td>
</tr>
<tr>
<td>ManagementServer</td>
<td>MSA</td>
<td>The name of the management server as it is known by this node.</td>
</tr>
<tr>
<td>InstallServer</td>
<td>no value</td>
<td>Defaults to the ManagementServer value.</td>
</tr>
<tr>
<td>InstallAdapterHostname</td>
<td>no value</td>
<td>Defaults to the Hostname value.</td>
</tr>
<tr>
<td>InstallServerAKBNode</td>
<td>no value</td>
<td>CSM dynamically determines the correct connection to the install server; because InstallServer is also blank, the ManagementServer attribute is used.</td>
</tr>
<tr>
<td>InstallAdapterGateway</td>
<td>no value</td>
<td>None.</td>
</tr>
</tbody>
</table>

Table 43. Configuration #5 node attributes

CSM for AIX and Linux: Planning and Installation Guide 113
<table>
<thead>
<tr>
<th>Attribute name</th>
<th>Attribute value</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>NodeD</td>
<td>The name of the node as it is known by the management server.</td>
</tr>
<tr>
<td>ManagementServer</td>
<td>MSA</td>
<td>The name of the management server as it is known by this node.</td>
</tr>
<tr>
<td>InstallServer</td>
<td>ISA</td>
<td>The name of the install server as known by the management server.</td>
</tr>
<tr>
<td>InstallAdapterHostname</td>
<td>NodeD</td>
<td>The name of the node as known by the install server.</td>
</tr>
<tr>
<td>InstallServerAKBNode</td>
<td>ISB</td>
<td>The name of the install server as known by this node.</td>
</tr>
<tr>
<td>InstallAdapterGateway</td>
<td>GWD</td>
<td>The name of gateway from the node to the install server (Gateway 2). Here we use the gateway that is closest to the node.</td>
</tr>
<tr>
<td>InstallAdapter*</td>
<td>various values</td>
<td>InstallAdapterNetmask, InstallAdapterMacaddr, for example.</td>
</tr>
</tbody>
</table>

Configuration #6A - Node has gateway to management server and direct connection to install server

In this configuration, the node is on the same subnet as the install server, but the node is not on the same subnet as the management server - it needs to connect to the management server through a gateway. Typically, the InstallAdapterGateway attribute is used to indicate the gateway from the node and the install server, but in this case, there is no gateway to the install server, so InstallAdapterGateway can be used to refer to the gateway to the management server.
### Table 44. Configuration #6A install server attributes

<table>
<thead>
<tr>
<th>Attribute name</th>
<th>Attribute value</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>ISB</td>
<td>The name of the node as it is known by the management server.</td>
</tr>
<tr>
<td>ManagementServer</td>
<td>MSB</td>
<td>The name of the management server as it is known by this node.</td>
</tr>
<tr>
<td>InstallServer</td>
<td>no value</td>
<td>Defaults to the <code>ManagementServer</code> attribute value.</td>
</tr>
<tr>
<td>InstallAdapterHostname</td>
<td>no value</td>
<td>Defaults to the <code>Hostname</code> attribute value.</td>
</tr>
<tr>
<td>InstallServerAKBNode</td>
<td>no value</td>
<td>CSM dynamically determines the correct connection to the install server; since <code>InstallServer</code> is also blank, the <code>ManagementServer</code> attribute is used.</td>
</tr>
<tr>
<td>InstallAdapterGateway</td>
<td>no value</td>
<td>None.</td>
</tr>
</tbody>
</table>

### Table 45. Configuration #6A node attributes

<table>
<thead>
<tr>
<th>Attribute name</th>
<th>Attribute value</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>NodeD</td>
<td>The name of the node as it is known by the management server.</td>
</tr>
<tr>
<td>ManagementServer</td>
<td>MSA</td>
<td>The name of the management server as it is known by this node.</td>
</tr>
<tr>
<td>InstallServer</td>
<td>ISB</td>
<td>The name of the install server as known by the management server.</td>
</tr>
<tr>
<td>InstallAdapterHostname</td>
<td>NodeC</td>
<td>The name of the node as known by the install server.</td>
</tr>
<tr>
<td>InstallServerAKBNode</td>
<td>ISC</td>
<td>The name of the install server as known by this node.</td>
</tr>
<tr>
<td>InstallAdapterGateway</td>
<td>GWD</td>
<td>The name of gateway from the node to the management server.</td>
</tr>
<tr>
<td>InstallAdapter*</td>
<td>various values</td>
<td><em>InstallAdapterNetmask, InstallAdapterMacaddr</em>, for example.</td>
</tr>
</tbody>
</table>
Configuration #6B - Node has gateway to management server, direct connection to install server, and single network interface

In this configuration, the node has a single network interface on the same subnet as the install server, but is not on the same subnet as the management server - it must connect to the management server through a gateway. Typically, the `InstallAdapterGateway` attribute is used to indicate the gateway from the node and the install server, but in this case, there is no gateway to the install server, so `InstallAdapterGateway` can be used to refer to the gateway to the management server.

Table 46. Configuration #6B install server attributes

<table>
<thead>
<tr>
<th>Attribute name</th>
<th>Attribute value</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>ISB</td>
<td>The name of the node as it is known by the management server.</td>
</tr>
<tr>
<td>ManagementServer</td>
<td>MSB</td>
<td>The name of the management server as it is known by this node.</td>
</tr>
<tr>
<td>InstallServer</td>
<td>no value</td>
<td>Defaults to the <code>ManagementServer</code> attribute value.</td>
</tr>
<tr>
<td>InstallAdapterHostname</td>
<td>no value</td>
<td>Defaults to the <code>Hostname</code> attribute value.</td>
</tr>
<tr>
<td>InstallServerAKBNode</td>
<td>no value</td>
<td>CSM dynamically determines the correct connection to the install server; since <code>InstallServer</code> is also blank, the <code>ManagementServer</code> attribute is used.</td>
</tr>
<tr>
<td>InstallAdapterGateway</td>
<td>no value</td>
<td>None.</td>
</tr>
</tbody>
</table>
### Table 47. Configuration #6B node attributes

<table>
<thead>
<tr>
<th>Attribute name</th>
<th>Attribute value</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>NodeC</td>
<td>The name of the node as it is known by the management server.</td>
</tr>
<tr>
<td>ManagementServer</td>
<td>MSA</td>
<td>The name of the management server as it is known by this node.</td>
</tr>
<tr>
<td>InstallServer</td>
<td>ISB</td>
<td>The name of the install server as known by the management server.</td>
</tr>
<tr>
<td>InstallAdapterHostname</td>
<td>NodeC</td>
<td>The name of the node as known by the install server.</td>
</tr>
<tr>
<td>InstallServerAKBNode</td>
<td>ISC</td>
<td>The name of the install server as known by this node.</td>
</tr>
<tr>
<td>InstallAdapterGateway</td>
<td>GWC</td>
<td>The name of gateway from the node to the management server.</td>
</tr>
<tr>
<td>InstallAdapter*</td>
<td>various values</td>
<td>InstallAdapterNetmask, InstallAdapterMacaddr, for example.</td>
</tr>
</tbody>
</table>

### Setting up an AIX install server

Perform the following steps to set up an AIX install server. The install server must be added to the cluster as a managed node before defining or installing the nodes served by the install server.

1. Define the install server as a cluster node.

   When defining install server nodes with the `definenode` command, do not define an `InstallServer` attribute value; the value defaults to the CSM management server value. Refer to Defining nodes for details.

   The `InstallOSName` attribute value must be specified, if it is different from the CSM management server value. When the nodes that use this install server are defined this value will be used as a default for the node definitions.

2. Install AIX on the install server.

   There are several options for installing an AIX install server:

   a. If your management server is running AIX, you can set it up as a NIM master to install other AIX install servers. Refer to Installing AIX on nodes for details. If you use this procedure then the install server node will be automatically added to the cluster so step 3 below will not be necessary.

   b. Use a remote NIM master, outside of the CSM cluster, to install the install server.

   c. Install the install server using the AIX product CDs.

3. Add the install server node to the cluster.
If the install server node was not added to the cluster in the previous step then it is added to the cluster by running the `updatenode` command on the management server. See Adding AIX nodes for details.

4. Verify the install server.

   Run the `ibm.csm.install-server` probe to verify that an install server is fully configured. This probe ensures that the required software packages are installed, install services are configured and running, and network connections are correct and active. For example:

   ```
   probemgr -p ibm.csm.install-server -l 0
   ```

5. Update the install server (optional).

   You can update the install server with the required files and directories by running the `updateisvr` command. The command distributes the required files from the `/csminstall` directory on the management server to the install servers. This step is optional because these install server updates are done automatically when installing or updating the nodes served by the install server; because the install server updates take time to complete, you can run `updateisvr` to avoid delays when installing or updating nodes.

   For example, to update all install servers, enter:

   ```
   updateisvr -a
   ```

To be able to install AIX on cluster nodes, an AIX install server must be set up as an AIX Network Installation Manager (NIM) master. The install server must be at the same or later AIX level as the nodes it serves. Typically, only one NIM master is required to server all AIX nodes in a cluster. To improve installation performance in a large cluster, multiple AIX install servers may be created, or NIM support for resource servers may be used.

If the CSM management server and nodes are both running AIX, use the management server as the install server and NIM master. However, one or more separate systems can be used for the AIX install servers; for example, if using AIX nodes at a later operating system level than the management server.

The procedure for configuring an install server as a NIM master is covered in Installing AIX on nodes.

---

**Setting up a Linux install server**

Perform the following steps to create a Linux install server on a cluster node. The install server must be added to the cluster as a managed node before defining or installing the nodes that will be using it as an install server.

1. Define the install server as a cluster node.

   When defining install server nodes with the `definenode` command, do not define an `InstallServer` attribute value. The value defaults to the CSM management server value. Refer to Defining nodes for details.

   Define the following attribute values, if different from the CSM management server values:
When the nodes that use this install server are defined, these values are used as default node definitions.

2. Install Linux on the install server node.

There are several options for installing a Linux install server:

a. Use your Linux management server to install a Linux install server, including install servers with different Linux distributions than the management server. See Installing Linux on nodes for details; the procedure automatically adds the install server to the cluster, so you can skip step 3.

b. If there are multiple install servers with the same distribution then one can be installed manually and then used to install the other install servers of the same type. Refer to Installing Linux on nodes for details.

c. Install the install server using the Linux product CDs.

3. Add the install server node to the cluster.

If the install server node was not added to the cluster in the previous step then it is added to the cluster by running the updatenode command on the management server. See Adding Linux nodes for details.

4. Verify the install server.

Run the ibm.csm.install-server probe to verify that an install server is fully configured. This probe ensures that the required software packages are installed, install services are configured and running, and network connections are correct and active. For example:

```
probemgr -p ibm.csm.install-server -l 0
```

5. Update the install server (optional)

After you have run the copycds or csmsetupinstall command, you can run the updateisvr command to update the install server files and directories. The updateisvr command distributes required files from the /csminstall directory on the management server to the install servers. This step is optional because these updates are handled automatically when installing or updating an install server; you can run the updateisvr at this point to avoid delays when installing or updating install servers.

For example, to update all of install servers, enter:

```
updateisvr -a
```

A Linux install server can be used to provide boot services (PXE, bootp) for initiating the native Linux operating system install mechanism. In this case, it will contain the configuration files for Red Hat EL Kickstart or SLES AutoYaST installation and be defined as the TFTP and NFS server for the nodes. If
using a Linux install server to install other cluster nodes, the required services are enabled automatically by the CSM commands that are run during the process. The procedure for installing Linux nodes using an install server is described in Installing Linux on nodes.

When defining nodes that are served by an install server, the node InstallServer attribute value must be set to the correct install server name.

If there are multiple System x Linux install servers on the same subnet, there is the potential for interference between them. Any of the install servers in the subnet may respond to a node's DHCP and PXE request that is broadcast across the entire subnet. To avoid interference, CSM will configure each install server in the same subnet to have complementary DHCP and PXE configurations. The DHCP configuration files on each install server will have identical static IP address lists so that no matter which install server responds, the same static address will be returned. The DHCP configuration files on each install server will have unique dynamic ranges so that two servers do not serve the same dynamic address to different target nodes. For targeted requests such as NFS, an install server will be chosen at random from the group to service a particular node.

To ensure that all the install servers on the same subnet get configured as a group, they must be configured as follows:

- The install servers have the same InstallDistributionName, InstallDistributionVersion, InstallServiceLevel, InstallPkgArchitecture, and InstallCSMVersion attributes. The CSM version must also be the same.
- The install servers on the same subnet must be added to a node group.
- The node's InstallServer attribute must be set to the name of the install server node group preceded by the plus character (+). It can optionally be followed by a colon character (:) and a directory name.

For example, to specify a group of install servers on the same subnet, enter:

```
nodegrp -a iserver1.clusters.com,iserver2.clusters.com,iserver3.clusters.com ISGroup1
```

Specify the InstallServer attribute as:

```
+ISGroup1:/mydirectory
```

During the installation process, servers are randomly chosen from this node group to provide the various installation services. If any server in this node group becomes inactive, you must remove it from the node group before continuing with node installations. If the optional directory is specified, each install server in the group will use the same directory that was indicated.

For Linux on System p install servers, including BladeCenter JS, the network install is not initiated by a DHCP broadcast; it is initiated by a directed DHCP request to the specific install server. Therefore, Linux on System p and BladeCenter JS install servers do not have restrictions on how they can be configured. A node group of System p and BladeCenter JS install servers cannot be used as the InstallServer attribute value for Linux nodes.
Chapter 8. Defining nodes

Before you can add, update, or manage a cluster node, you must define the node by defining node attributes in the CSM database.

Note:
To use hardware control, you must also store hardware control point user IDs and passwords; see Store Linux hardware control point user IDs and passwords and .

Complete the following steps to define your cluster nodes.

Determining node attributes

As part of the CSM cluster installation process, you must collect information that is used to define the cluster nodes. The node information that creates a node definition is collectively known as node attributes. The complete list of node attributes and descriptions are documented in the nodeattributes man page.

Defining nodes requires assigning values for the following types of node attributes.

General attributes

**Hostname**
The resolvable host name or IP address of the node, as known by the management server. It represents the network adapter hostname or IP address on the Cluster VLAN. Hostname is always required and must be specified when you define the node. The name must be unique within the cluster and cannot conflict with other devices or cluster nodes. In a pure Linux cluster, this attribute can be an unresolved IP address.

**ManagementServer**
The host name or IP address of the CSM management server. A ManagementServer value is required. It must be set to the host name of the management server as it is known by the node. Because the management server can have multiple interfaces, different nodes might use different interfaces to communicate with the management server. If a route to the node exists at the time that the node is defined, CSM attempts to set the value to the IP address of the management server automatically. If a route to the node does not exist, CSM cannot set the value automatically, so the name must be explicitly set to the host name of the management server on the network that installs the node.

**InstallServer**
The host name or IP address of the install server as known by the management server, and an optional directory that will serve the CSM install files to this node. The host name and directory must be separated by the colon character (:). The install server must be a node in the cluster.

For example, to specify only the name of the install server iserver1.clusters.com, enter:

```
InstallServer=iserver1.clusters.com
```
To specify the name of the install server, `iserver1.clusters.com`, and a directory called `/mydirectory`, enter:

`iserver1.clusters.com:/mydirectory`

If you specify an install server but not a directory, `/csmserver` is used by default. To have enough space for the CSM database, you can create the install server directory in a separate file system. The size requirements are similar to `/csminstall` on the management server. CSM copies the CSM directories and files into the specified install server directory. Do not store other data in the install server directory.

If you do not specify an install server, the management server is used to serve the install files from `/csminstall`.

If you are configuring multiple Linux install servers on the same subnet, you must create an install server nodegroup and the `InstallServer` attribute must be set to the value `+` followed by a node group name, optionally followed by a `:` and directory name.

For example, if the install server node group is `ISGroup1`, set the `InstallServer` value to:

`+ISGroup1:/mydirectory`

**InstallAdapterHostname**

The hostname or IP address of the node as known by the install server. The value is the hostname used to connect to the node during the installation, and the value assigned to the install adapter when it is configured on the node during installation. If left blank, the `Hostname` attribute value is used by default.

**InstallServerAKBNode**

The hostname or IP address of the install server as known by the node. If there are multiple Linux install servers on the same subnet, this attribute is ignored, and the network connection on the install server that is used by the node is dynamically determined. If left blank, CSM determines this value dynamically during runtime. If there are multiple connections from a Linux install server to the installation subnet that the node is on, one connection is chosen at random.

**UserComment**

Any useful information concerning this node. Not required.

**Mode**

The node's current phase in the install process. To define a minimally-managed node, set this attribute to `MinManaged` or run the `definenode` command with the `--minmanaged` option; see **Installing minimally-managed Linux nodes**. If you do not set the node `Mode` attribute, CSM sets it automatically during the installation.

### Hardware control attributes

To configure your nodes for hardware control, you must define the hardware control attributes. In some cases, default values are provided. If the defaults are acceptable, you do not need to provide the attribute values when you define the node.

For a complete description of these attributes, see the *CSM for AIX and Linux: Administration Guide*.

### HMC-attached System p nodes

Set the following hardware control attribute values for HMC-attached System p nodes:
**PowerMethod**
Set this attribute to **hmc**.

**HWControlPoint**
Set this attribute to the host name or IP address of the **HMC**. If you set the **HWControlPoint** attribute to two comma-separated HMC host names or IP addresses, CSM attempts to connect to the second HMC if the connection to the first HMC is lost, and vice versa.

**HWControlNodeId**
Set this attribute to the partition name of the LPAR.

**ConsoleMethod**
Set this attribute to **hmc**. If the **PowerMethod** attribute is set to **hmc**, this value is set by default.

**ConsolePortNum**
Set this attribute to the partition LParID.

**ConsoleServerName**
Set this attribute to the host name of the **HMC**. If the **PowerMethod** attribute is set to **hmc**, this attribute is set by default to the host name of the **HMC**.

**ConsoleSerialDevice**
To enable the console, leave this attribute blank; to disable console support for the node, set this attribute to **NONE**.

### IVM-managed System p nodes

Set the following hardware control attribute values for IVM-managed System p nodes:

**PowerMethod**
Set this value to **ivm**.

**HWControlPoint**
Set this value to the host name of the **IVM**.

**HWControlNodeId**
Set this value to the partition name of the LPAR.

**ConsoleMethod**
Set this value to **ivm**. If the **PowerMethod** attribute is set to **ivm**, this value is set by default.

**ConsolePortNum**
Set this value to the partition LParID.

**ConsoleServerName**
Set this value to the host name of the **IVM**. If the **PowerMethod** attribute is set to **ivm**, this value is set by default to the host name of the **IVM**.

**ConsoleSerialDevice**
To enable the console, leave this field blank; to disable console support for the node, set to **NONE**.

**InstallAdapterDuplex**
Set this value to **auto**. Otherwise, **getadapters** will fail to obtain the MAC address.

**InstallAdapterSpeed**
Set this value to **auto**. Otherwise, **getadapters** will fail to obtain the MAC address.

### System p (**POWER5 and later**) direct attach nodes

Set the following hardware control attribute values for System p direct attach nodes. System p direct attach nodes do not use an HMC for hardware control.

**PowerMethod**
Set this value to **fsp**.

**HWControlPoint**
Set this value to the host name or IP address of the FSP.

**HWControlNodeId**
This attribute is required but its value is not limited. It is recommended that the short host name be used.

**ConsoleMethod**
Set this value to **fsp**.

**ConsoleServerName**
Set this value to the host name or IP address of the FSP.

**System x 3455, 3550, 3650, 3655, and 3755 nodes**

Set the following hardware control attribute values for System x 3455, 3550, 3650, 3655, and 3755 nodes:

**PowerMethod**
Set this value to **bmc2**.

**HWControlPoint**
Set this value to the hostname of the BMC.

**HWControlNodeId**
Set this value to the short hostname of the node.

**System x 3455, 3550, 3650, 3655, and 3755 nodes using Serial-over-LAN (SOL)**

Set the following hardware control attribute values for System x 3455, 3550, 3650, 3655, and 3755 nodes that are using SOL:

**ConsoleMethod**
Set this value to **bmc2**.

**ConsoleSerialDevice**
Valid values are **ttyS0** and **NONE**. If you do not specify a value when the node is created with the **definenode** command, a default value of **ttyS0** is set. If you do not want console output redirected to the serial port, the **ConsoleSerialDevice** attribute must be set to **NONE**. Otherwise, set it to **ttyS0**.

**ConsoleSerialSpeed**
Set this value to 19200.

**ConsoleServerName**
Set this value to the host name for the Baseboard Management Controller (BMC) of the node.

**ConsolePortNum**
This attribute is not used. Leave this field blank.

**xSeries 335, 336, 345, 346, 366 and System x 3455, 3550, 3650, 3655, 3755 using an RSA-II SlimLine adapter**

Set the following hardware control attribute values for xSeries 335, 336, 345, 346, 366 and System x 3455, 3550, 3650, 3655, 3755, that are using an RSA-II SlimLine adapter:

**PowerMethod**
Set this value to **xseries**.

**HWControlPoint**
Set this value to the host name of the IBM Remote Supervisor Adapter (RSA).
**HWControlNodeId**

Use the **TextID** associated with the node's Integrated System Management Processor (ISMP), or the ASM name of the RSA adapter, if the node has an adapter installed.

**Note:**

**BMC** cannot be used for console access in this configuration. This configuration would require the use of a terminal server for remote console.

**System x nodes using a console server**

Set the following hardware control attribute values for System x nodes that are using a console server:

**ConsoleMethod**

Valid values are: **mrv**, **els**, **computone**, **cps**, and **cyclades**.

**ConsoleSerialDevice**

The device name of the console serial port on the node. Valid values are: **ttyS0**, **ttyS1**, and **NONE**. If no value is specified for this attribute when the node is created with the **definenode** command, a default value of **ttyS0** is set. If the system has no serial port defined, or if you do not want console output redirected to the serial port, the **ConsoleSerialDevice** attribute value must be set to **NONE**.

**ConsoleSerialSpeed**

The speed used on the serial line between the node and the console server. This value must match the speed set on the console server port to which the node is connected. If no value is entered, a default value of 9600 is used.

**ConsoleServerName**

Set this value to the host name for the console server.

**ConsolePortNum**

The number associated with the console port for this node. The valid MRV console port numbers range from 1 through 40 depending on the model. The valid CPS and ELS port numbers range from 1 through 16 (decimal). The valid Computone port numbers range from 1 through 8. The valid Cyclades port numbers range from 1 through 48.

**eServer 325, 326 and 326m nodes, and xSeries 336 and 346 without an RSA-II SlimLine adapter**

Set the following hardware control attribute values for eServer 325, 326, and 326m nodes, and xSeries 336, and 346 that do not use an RSA-II SlimLine adapter:

**PowerMethod**

Set this value to **bmc**.

**HWControlPoint**

Set this value to the hostname of the node's Baseboard Management Controller (BMC).

**HWControlNodeId**

Set this value to the short hostname of the node.

**xSeries 336, 346 using Serial-over-LAN (SOL)**

Set the following hardware control attribute values for System x336/x346 nodes that use SOL:

**ConsoleMethod**
Set this value to bmc.

**ConsoleSerialDevice**
Valid values are: *ttyS0*, and *NONE*. If no value is specified for this attribute when the node is created with the `definenode` command, a default value of *ttyS0* is set. If you do not want console output redirected to the serial port, the `ConsoleSerialDevice` attribute value must be set to *NONE*. Otherwise, use *ttyS0*.

**ConsoleSerialSpeed**
Set this value to 19200.

**ConsoleServerName**
Set this value to the host name for the Baseboard Management Controller (BMC) of the node.

**ConsolePortNum**
Not used. Leave this field blank.

### eServer 326m nodes using Serial-over-LAN (SOL)

Set the following hardware control attribute values for eServer 326m nodes that use SOL:

**ConsoleMethod**
Set this value to bmc.

**ConsoleSerialDevice**
Valid values are: *ttyS0*, and *NONE*. If no value is specified for this attribute when the node is created with the `definenode` command, a default value of *ttyS0* is set. If you do not want console output redirected to the serial port, the `ConsoleSerialDevice` attribute value must be set to *NONE*. Otherwise, use *ttyS0*.

**ConsoleSerialSpeed**
Set this value to 9600.

**ConsoleServerName**
Set this value to the host name for the Baseboard Management Controller (BMC) of the node.

**ConsolePortNum**
Not used. Leave this field blank.

### BladeCenter nodes

If the SPM components have not been installed, set the `ConsoleSerialDevice` attribute for all blades to *NONE*, and leave the `ConsoleMethod`, `ConsoleServerName`, and `ConsolePortNum` attributes blank.

The following attributes apply to BladeCenter HS, except for the HS20-8678, and LS blade servers, and are valid only if the Serial Over LAN (SOL) feature has been enabled on the BladeCenter Management Module:

**ConsoleMethod**
Set this value to `blade`.

**ConsoleServerName**
Set this value to host name of the BladeCenter Management Module.

**ConsolePortNum**
Set this value to the slot number where the blade server is located in the BladeCenter chassis.

**ConsoleSerialDevice**
Set this value to *ttyS1*.

**ConsoleSerialSpeed**
Set this value to *19200*.
If Serial Over LAN has not been enabled, set the `ConsoleSerialDevice` attribute for all blades to NONE, and leave the `ConsoleMethod`, `ConsoleServerName`, and `ConsolePortNum` attributes blank.

The following attributes apply to BladeCenter JS blade servers, and are valid only if Serial Over LAN (SOL) has been enabled on the BladeCenter Management Module:

- **ConsoleMethod**
  - This value must be set to `blade`.
- **ConsoleServerName**
  - Use the host name of the BladeCenter Management Module.
- **ConsolePortNum**
  - Use the blade slot number within the BladeCenter chassis.
- **ConsoleSerialDevice**
  - Leave this field blank.

If Serial Over LAN has not been enabled, set the `ConsoleSerialDevice` attribute for all blades to NONE, and leave the `ConsoleMethod`, `ConsoleServerName`, and `ConsolePortNum` attributes blank.

The following attributes apply only to the BladeCenter HS20-8678 blade server, and are only valid if the blade server is part of an eServer Cluster 1350 and the optional Serial Port Module (SPM) components have been installed:

- **ConsoleMethod**
  - Set this value to `mrv`.
- **ConsolePortNum**
  - Set this value to the port number of the MRV console server to which the blade is connected.
- **ConsoleSerialDevice**
  - Set this value to `ttyS0`.
- **ConsoleSerialSpeed**
  - Set this value to match the port speed of the MRV console port (default is 9600).
- **ConsoleServerName**
  - Set this value to the host name of the MRV console server to which the blade is connected.
- **ConsoleRedirectionAfterPOST**
  - The status of console redirection after POST (Power On Self Test). This attribute can be edited. Set this attribute to match the value of the "Console Redirection after POST" BIOS attribute. Setting `ConsoleRedirectionAfterPOST` allows CSM to determine how to configure the serial console settings to display correctly during installation.

**Remote power attribute values**

The following table summarizes the CSM node hardware types and their required remote power attribute values.

**Table 48. Remote power attribute values**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>System x and xSeries&lt;sup&gt;1&lt;/sup&gt;,&lt;sup&gt;2&lt;/sup&gt;</th>
<th>System x and xSeries&lt;sup&gt;1,4&lt;/sup&gt;</th>
<th>System p and pSeries</th>
<th>Blade Center</th>
<th>Devices that require APC MasterSwitch</th>
<th>eServer&lt;sup&gt;3&lt;/sup&gt;</th>
<th>Direct attach System p (POWER5 and later)</th>
</tr>
</thead>
</table>

CSM for AIX and Linux: Planning and Installation Guide
### Remote console attribute values

The following table summarizes the console server models that can be used with CSM node architectures and their required remote console attribute values.

<table>
<thead>
<tr>
<th>Node hardware type</th>
<th>Console server</th>
<th>Console Method</th>
<th>Console PortNum</th>
<th>Console ServerName</th>
<th>Console SerialSpeed</th>
<th>Console SerialDevice</th>
</tr>
</thead>
<tbody>
<tr>
<td>HMC-attached System p and pSeries</td>
<td>none</td>
<td>hmc</td>
<td>not applicable</td>
<td>hostname of controlling HMC</td>
<td>not applicable</td>
<td>not applicable</td>
</tr>
<tr>
<td>IVM-managed System p</td>
<td>none</td>
<td>ivm</td>
<td>LParID attribute value</td>
<td>hostname of controlling IVM</td>
<td>not applicable</td>
<td>not applicable</td>
</tr>
<tr>
<td>BladeCenter JS</td>
<td>none</td>
<td>blade</td>
<td>1-14</td>
<td>hostname of controlling</td>
<td>19200</td>
<td>not applicable</td>
</tr>
<tr>
<td>BladeCenter HS</td>
<td>none</td>
<td>blade</td>
<td>1-14</td>
<td>hostname of controlling</td>
<td>19200</td>
<td>ttyS1</td>
</tr>
</tbody>
</table>

**Note:**

1. 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.
2. Includes xSeries 335, 336, 345, 346 and 366, System x 3455, 3550, 3650, 3655, 3755 with RSA-II SlimLine Adapter.
3. eServer includes eServer 325 326, and 326m, xSeries 336 and 346 without RSA-II SlimLine Adapter.
4. Includes xSeries 366, System x 3455, 3550, 3650, 3655, and 3755 without RSA-II SlimLine Adapter.
and LS, except for HS20-8678

<table>
<thead>
<tr>
<th>BladeCenter HS20-8678 with SPM</th>
<th>MRV IR-820; IR-8040</th>
<th>mrv</th>
<th>1-20; 1-40</th>
<th>console server hostname</th>
<th>varies - default 9600</th>
<th>ttyS0</th>
</tr>
</thead>
<tbody>
<tr>
<td>eServer 325, 326, 326m, xSeries</td>
<td>MRV IR-820; IR-8040; LX-4008; LX-4016; LX-4032</td>
<td>mrv</td>
<td>1-20; 1-40; 1-8; 1-16; 1-32</td>
<td>console server hostname</td>
<td>varies - default 9600</td>
<td>varies - default ttyS0</td>
</tr>
<tr>
<td>Equinox ELS 16II</td>
<td>els</td>
<td>1-16</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Avocent CPS1610</td>
<td>cps</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Computone RCM4; RCM8</td>
<td>computone</td>
<td>1-4; 1-8</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cycldes ACS48</td>
<td>cyclades</td>
<td>1-48</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>xSeries 336, 346 with SOL</td>
<td>none</td>
<td>bmc</td>
<td>not applicable</td>
<td>BMC hostname</td>
<td>19200</td>
<td>ttyS0</td>
</tr>
<tr>
<td>eServer 326m with SOL</td>
<td>none</td>
<td>bmc</td>
<td>not applicable</td>
<td>BMC hostname</td>
<td>9600</td>
<td>ttyS0</td>
</tr>
<tr>
<td>System x 3455, 3550, 3650, 3655, and 3755</td>
<td>none</td>
<td>bmc2</td>
<td>not applicable</td>
<td>BMC hostname</td>
<td>19200</td>
<td>ttyS0</td>
</tr>
<tr>
<td>FSP direct attach System p5/POWER 6</td>
<td>none</td>
<td>fsp</td>
<td>not applicable</td>
<td>HWControl Point</td>
<td>not applicable</td>
<td>not applicable</td>
</tr>
</tbody>
</table>

When the `csm.client` package is installed on Linux nodes on xSeries, eServer 325 and 326, and BladeCenter HS, 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`, CSM automatically adds 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 for details on how to redirect grub output to a remote console.

## Installation attributes

The following CSM attributes are used for node installation:

### InstallAdapterNetmask

The `InstallAdapterNetmask` and `InstallAdapterHostname` attributes are used to determine the node subnet when generating the node DHCP configuration file. If not specified, the default is the netmask of the install server's network adapter used to install the node. If the install server and node are on the same subnet, the attribute can be left blank. If the install server and node are on different subnets, you must define this attribute as the node subnet.

### InstallAdapterGateway

The node gateway is used to define the network path to the node. If not specified, the default is the default gateway on the install server's network adapter used to install the node. If the install server and node are on the same subnet, the attribute can be left blank. If the install server and node are on different subnets, you must define this attribute as the node subnet.
The IP address or hostname of the gateway between the node and its install server. If there are multiple gateway servers between the node and the install server, set this attribute to the gateway closest to the node.

For System x and System p installations when the management server and node are not on the same subnet, an install server can act as a gateway between them. In this case, the InstallAdapterGateway attribute is set to the same values as the InstallServerAKBNode attribute.

**InstallAdapterDuplex**
The duplex value of the network adapter that is used to install the node. Valid values are: auto, half, or full.

**InstallAdapterMacaddr**
The attribute that contains the MAC address of the network adapter named in the InstallAdapterName attribute.

**InstallAdapterSpeed**
The speed of the network adapter that is to install the node. Valid values are: auto, 10, 100, or 1000.

**InstallAdapterType**
The type of the network adapter that is to install the node. Valid value is ent (Ethernet).

**InstallAdapterName**
The name of the node network adapter, for example, eth0, eth1, for performing the installation. The getadapters command obtains the MAC address of the node network adapter and stores it as the InstallAdapterMacaddr value.

**UUID**
The Universal Unique Identifier (UUID) for a Linux node. This value can be set automatically by the getuuid command. This attribute is only used for Linux on System x and BladeCenter HS nodes.

### Defining node installation attributes

You must define software-related attributes before installing cluster nodes. However, these attributes use the management server values as the defaults; if these values are acceptable, you do not need to specify any attribute values when defining a node that runs the same operating system.

Each attribute takes its default value from the management server only if the management server is running the same operating system as the node. If the management server is running AIX and the InstallOSName attribute for the node is Linux, then the default for these attributes is blank. If you are using install servers, and you set the InstallServer attribute for the node, then the attributes listed below take their defaults from the node's install server instead of from the management server.

**For AIX nodes:**

**InstallOSName**
The name of the operating system on the node. When you define a node, the default is the name of the operating system that is installed on the management server. For AIX nodes the value must be AIX.

**For Linux nodes:**

**InstallCSMVersion**
The version of CSM that is to be installed on the node. This value must be in the format 
version.release.modification; for example, 1.7.1. When you define a node, the default is the version 
of CSM that is installed on the management server.

**InstallOSName**
The name of the operating system to install. When you define a node, the default is the name of the 
operating system that is installed on the management server. For Linux nodes the value must be 
Linux.

**InstallDisk**
The specific disk to install. This value is set to /dev/sda, /dev/hda, /dev/hdb, for example. This 
attribute is required if the install disk is not the first hard disk If InstallDisk is set, InstallDiskType 
is ignored.

**InstallDiskType**
Type of disk to be used for node installation. The default value is scsi. Set this value to ide for 
nodes that contain an ide disk. If InstallDisk is defined, the attribute is ignored.

**InstallDistributionName**
The operating system distribution name. The valid values are RedHatEL-Server, 
RedHatEL-Client, RedHatEL-AS, RedHatEL-ES, RedHatEL-WS, and SLES. When defining 
a node, the default value is the distribution name installed on the management server.

**InstallDistributionVersion**
The name of the distribution version to be installed. When you define a node, the default is the 
distribution version installed on the management server. The valid values are:

- Red Hat EL 5.1: 5.1
- Red Hat EL 5.2: 5.2
- Red Hat EL 5.3: 5.3
- Red Hat EL 5: 5
- Red Hat EL 4.5: 4.5
- Red Hat EL 4.6: 4.6
- Red Hat EL 4.7: 4.7
- Red Hat EL 4: 4
- SLES 10: 10
- SLES 9: 9

**InstallMethod**
This attribute is defined automatically by the csmsetupinstall command during kickstart and 
autoyast installations. For diskless nodes, you must explicitly set this attribute to warewulf. To 
upgrade Red Hat EL nodes, set this attribute to kickstart-upgrade. To upgrade SLES nodes, set 
this attribute to you (Yast online update).

**InstallPkgArchitecture**
The machine architecture of the node. For System x and BladeCenter HS nodes, set this attribute to 
i386; this value represents any server with i386, i486, i586, or i686 architecture. For System p, 
including BladeCenter JS, set this attribute to ppc64. For BladeCenter LS and eServer nodes, set 
this attribute to x86_64. When defining a node, this attribute is set by default to the 
InstallPkgArchitecture install server attribute value. If InstallServer is not set, the default is the 
management server package architecture.

**InstallServiceLevel**
The service level installed on the node. This can be set to a predefined value such as SP3 or QU2, 
or to a user-defined value. User-defined values can be used to create custom service levels, or for 
multiple copies of the same service level with slight differences. This value is case-sensitive for 
user-defined values.
The `InstallServiceLevel` value also indicates the subdirectory name where the service level is installed. For example, if `InstallServiceLevel=SP1`, the service level for SLES 9 on xSeries is installed in `/csminstall/Linux/SLES/9/i386/SP1`.

Officially supported service levels are listed in the `pkgdefs` files in the `/opt/csm/install/pkgdefs` directory. The `pkgdefs` file for each supported GA and service level includes the number of CDs and CD identifiers.

If `InstallServiceLevel` is defined in the `pkgdefs` file, the `copycsmpkgs`, `copycds`, and `csmsetupinstall` commands prompt for the correct CDs and validate each CD. If `InstallServiceLevel` is not defined in the `pkgdefs` file, CSM assumes a user-defined service level. No error message is displayed, and there is no prompting for CDs. Use the `copycsmpkgs -p` command to specify all paths to copy.

**Note:** For detailed information on `InstallServiceLevel` attribute values, see Installation directories and files.

**Note:** For Red Hat EL 4.5, Red Hat EL 4.6, Red Hat EL 4.7, Red Hat EL 5.1, Red Hat EL 5.2 and Red Hat EL 5.3, set the `InstallServiceLevel` attribute to `GA` or no value.

---

### Collecting node attribute values

At this point, you have identified what attributes are required for your node definitions. The next step is to collect the actual values you need for the attributes.

You can do this as a manual task. You can make decisions about the hostnames, networks, adapters, and other node attribute values during the planning process, and record the information for use when you define the nodes in the CSM database.

An alternative to creating a hard copy template for each node is to create a node definition stanza file. A stanza file contains information for each node, and you can pass this file directly to the `definenode` command during the CSM installation process. See Creating a node definition file for details.

See Installation scenarios for examples. Some hardware configurations can be automatically detected, and the node attributes can be filled in automatically; see Automatic node detection and definition.

---

### Defining nodes options

Run the `definenode` command on the CSM management server to define all nodes in a CSM cluster. The command creates node definitions in the CSM database. At this point the nodes are in PreManaged Mode; after they are added to the cluster, they become Managed nodes.

The `definenode` command provides several options for creating cluster node definitions:

1. Create one definition at a time; see Defining a single node.
2. Use a node definition file as input to the command to define multiple nodes; see Using a node definition file.
3. Automatically detect and define cluster nodes on the supported hardware configurations only; see Automatic node detection and definition.
4. For Linux nodes, use starting_node and count values to automatically generate a set of node definitions with consecutive IP addresses.
5. Create a node definition file (use the -s flag and redirect the output to a file) that you can modify and use as input to the definenode command; see Creating a node definition file.
6. Automatically detect and add Linux nodes to the cluster based on a predefined node profile; see Node provisioning.

See the man page or the CSM for AIX and Linux: Command and Technical Reference for details on definenode command line syntax.

You can also define CSM nodes using SMIT. The SMIT fastpath is csm_defnodes. SMIT is only available on the AIX management server. To use this interface, issue:

```
smitt csm_defnodes
```

The definenode command and Kerberos Version 5: When the csmconfig SetupKRB5 attribute value is 8 or greater, the definenode command creates Kerberos Version 5 host principals and keys for the nodes. You are prompted to enter the Kerberos Version 5 administrator principal name and password. If you run definenode several times for several groups of nodes, you can defer the creation of Kerberos Version 5 host principals by running definenode with the --nopwd option. After the node definitions are complete, run csmconfig with SetupKRB5 set to 8 or greater. The csmconfig command creates principals and keys for all defined nodes that do not already have Kerberos Version 5 host principals created for them.

Defining a single node

The information required to define a node differs depending on the type of node to be defined, and whether or not hardware control is supported on the node. The host name or IP address of the node is always required. Specific node information is stored in the CSM database as node attribute values. For a complete list of the node attributes defined by the definenode command, see the nodeattributes man page.

Note:
If you are not using hardware control, the only required attribute for a node is the host name.

AIX nodes example

You must set the Hostname attribute to the resolvable host name or IP address of the node. This is the node's network interface as known by the management server. Set the following attributes for hardware control:

**PowerMethod**
Set to hmc for HMC-attached System p, fsp for direct attach System p, ivm for IVM-managed System p, blade for BladeCenter JS.

**HWCcontrolPoint**
Set to the hostname or IP address of the HMC, IVM, FSP or MM.

For attribute requirements, see General attributes, Hardware control attributes, and Defining node installation attributes.
For example, to define an HMC-attached AIX node with host name `clsn01`, issue the `definenode` command:

```
definenode -n clsn01 -H hmc12 PowerMethod=hmc InstallOSName=AIX
```

If values are not provided for some attributes on the command line, default values are set. For example, the default values for the `InstallOSName` attribute is set to the operating system name. Also, for nodes with a `PowerMethod` of `hmc`, the `ConsoleMethod` and `ConsoleServerName` can be set automatically.

To view the values that are set by the `definenode` command, without actually creating the definition, use the `-s` flag. If `-s` is specified on the command line, the `definenode` command displays the list of attributes and values that would be set for the node.

**Note:**
If you are using a Linux management server to define AIX nodes, you must set the `InstallOSName` attribute to `AIX`.

### Linux on System x nodes example

The following Linux node attributes must be set to use hardware control:

- The `Hostname` set to the resolvable host name or IP address of the node. This is the nodes' network interface, as known by the management server.
- The `PowerMethod` attribute set to `xseries` for xSeries and System x nodes, `apc` for devices that use APC MasterSwitch, or `bmc` for eServer 325 nodes.
- The `HWControlPoint` and `HWControlNodeId` attribute values.
- The `ConsoleMethod` attribute set to `mrv`, `bmc`, `bmc2`, `cps`, `computone`, `els`, or `cyclades`.
- The `ConsoleServer`, and `ConsolePortNum`, and `ConsoleSerialDevice` attribute values.
- The `InstallCSMVersion`, `InstallOSName`, `InstallDistributionName`, `InstallDistributionVersion` and `InstallPkgArchitecture` attributes must be set to appropriate values.

For attribute requirements, see [General attributes](#), [Hardware control attributes](#), and [Defining node installation attributes](#).

The following example defines a Linux on xSeries or System x node with an RSA hardware control point and an MRV console server:

```
```

**Note:**
1. The default values that are typically set for AIX cluster nodes are not valid for Linux nodes.
2. If you are using an AIX management server to manage Linux nodes, you must set the `InstallOSName` attribute to `Linux`. You must also set the `InstallDistributionName`, `InstallDistributionVersion`, `InstallPkgArchitecture` and (optionally) `InstallServiceLevel` attributes, because these values default to blank (no value) on an AIX management server.

### System p Linux nodes

Set the following attributes:
The resolvable host name or IP address of the node. This is the node's network interface, as known by the management server.

The `PowerMethod` attribute value is `hmc` for HMC-attached pSeries nodes, `ivm` for IVM managed System p nodes, or `blade` for JS20, JS21, JS22, JS12, JS23 and JS43 blade servers.

The `HWControlPoint` and either the `LPartID` or `HWControlNodeId` attribute values.

The `InstallCSMVersion`, `InstallOSName`, `InstallDistributionName`, `InstallCSMVersion`, `InstallDistributionVersion` and `InstallPkgArchitecture` attributes must be set to appropriate values.

For attribute requirements, see General attributes, Hardware control attributes, and Defining node installation attributes.

To define a node with host name `clsn01`, issue the `definenode` command:

```
definenode -n clsn01  -H hmc12 PowerMethod=hmc
```

For other examples of remote power software definitions, see Managing hardware control points.

**Note:**
If you are using an AIX management server for Linux nodes, be sure to set the `InstallOSName` attribute to `Linux`. You will also need to set the `InstallDistributionName`, `InstallDistributionVersion`, `InstallCSMVersion`, `InstallPkgArchitecture` and (optionally) `InstallServiceLevel` attributes, since these values default to blank on an AIX management server.

**Creating a node definition file**

A node definition file contains a stanza of information for each node to be defined. You can pass this file to the `definenode` command to create the node definitions in the CSM database.

Note that the examples contain attributes that have default values. If the default values are acceptable, you do not have to include them in the stanzas.

For more information, see the CSM `nodedef` man page.

**Node definition file rules**

- A stanza header consists of the node name followed by the colon character (:).
- Attribute lines must take the form of `Attribute=Value`.
- If a line is not blank, a comment, a header, an `Attribute=Value` pair, or specifying a embedded `nodedef` file, the command skips to the next valid header.
- When you submit the file, a warning message is issued for attributes that are not valid, but the processing continues.
- Each line of the file can have only one header, or attribute definition, or can specify a embedded `nodedef` file.
- Only one stanza can exist for each node.
- If the header keyword is `default`, the attribute values in the stanza are considered default values for subsequent node definitions.
- You can specify default stanzas multiple times and at any point in a definition file. The values apply to all definitions following the default stanza. The default values are cumulative; that is, a default attribute value remains set until the value is explicitly unset or changed.
- To turn off a default value, set the attribute to no value (blank).
• When you provide a specific value for an attribute in the node stanza, that value takes priority over any other default value that is set.
• You can add comments to the file. Begin a comment line with the pound sign character (#). Each comment must be on a separate line.
• When parsing the file, CSM ignores the tab characters and spaces.
• When the node definition file is used as input by the `definenode` command, command processing sets some attribute values. This applies to attributes that you do not include in the node definition file; if you do not set attributes in the node definition file, the default value is used.
• A `nodedef` file can embed a second `nodedef` file by specifying the `include` keyword.

**AIX examples without default stanzas**

```
clnode01:
  ManagementServer=csmms.clusters.com
  InstallOSName=AIX
  PowerMethod=hmc
  HWControlPoint=hmc1
  HWControlNodeId=cls01
  ConsoleMethod=hmc
  ConsoleServerName=hmc1
  InstallAdapterMacaddr=0001A2B3C4D5
  InstallAdapterType=ent
  InstallAdapterSpeed=100
  InstallAdapterDuplex=full
  UserComment="First LPAR on CEC #1"

clnode02:
  ManagementServer=csmms.clusters.com
  InstallOSName=AIX
  PowerMethod=hmc
  HWControlPoint=hmc1
  HWControlNodeId=cls02
  ConsoleMethod=hmc
  ConsoleServerName=hmc23
  InstallAdapterMacaddr=0001E6F7A8B9
  InstallAdapterType=ent
  InstallAdapterSpeed=100
  InstallAdapterDuplex=full
  UserComment="Second LPAR on CEC #1"
```

**Linux examples without default stanzas**

```
nfnode11:
  ManagementServer=c5bs.ppd.ibm.com
  InstallCSMVersion=1.7.1
  InstallOSName=Linux
  InstallDistributionName=RedHatEL-AS
  InstallDistributionVersion=4
  InstallPkgArchitecture=i386
  PowerMethod=xseries
  HWControlPoint=rsa05
  HWControlNodeId=nfnode11
  ConsoleMethod=mr
  ConsoleSerialDevice=ttyS0
  ConsoleServerName=mr15
  ConsolePortNum=1

nfnode12:
  ManagementServer=c5bs.ppd.ibm.com
  InstallCSMVersion=1.7.1
  InstallOSName=Linux
```
InstallDistributionName=RedHatEL-AS
InstallDistributionVersion=4
InstallPkgArchitecture=i386
PowerMethod=xseries
HWControlPoint=rsa04
HWControlNodeId=nfnode12
ConsoleMethod=mrv
ConsoleSerialDevice=ttyS0
ConsoleServerName=mrv15
ConsolePortNum=2

**AIX examples with a default stanza**

default:
    ManagementServer=c46cw.ppd.ibm.com
    InstallOSName=AIX
    PowerMethod=hmc
    HWControlPoint=hmc23
    ConsoleMethod=hmc
    ConsoleServerName=hmc23
    InstallAdapterType=ent
    InstallAdapterSpeed=100
    InstallAdapterDuplex=full
clstrnode01:
    InstallAdapterMacaddr=0003AC6E05E1
    HWControlNodeId=clstrnode01
clstrnode02:
    InstallAdapterMacaddr=0003AC6E05E3
    HWControlNodeId=clstrnode02
clstrnode03:
    InstallAdapterMacaddr=0003AC6E05E4
    HWControlNodeId=clstrnode03

**Linux examples with a default stanza**

default:
    PowerMethod=xseries
    ConsoleMethod=esp
    ConsoleServerName=esp15
    ConsolePortNum=0
    InstallOSName=Linux
    InstallCSMVersion=1.7.1
    HWControlPoint=asm03
    ManagementServer=c5bs.ppd.xyz.com
    InstallDistributionVersion=4

nfnode11:
    HWControlNodeId=nfnode11

nfnode12:
    ConsolePortNum=2
    HWControlNodeId=nfnode12

nfnode13:
    HWControlPoint=asm05
    HWControlNodeId=nfnode13
    ConsolePortNum=3
Using a node definition file

You can use a `nodedef` node definition file to define multiple nodes. This file consists of stanzas containing node attribute values for each node to be defined. To use a node definition file, you should start by looking at the sample file provided with CSM. The `/opt/csm/samples/install` file contains information on the format that must be used and also provides examples.

You can create this file manually and pass it to the `definenode` command using the `-f` flag. The `definenode` command uses information in the `nodedef` file to create node definitions. When possible, default values are set for attributes that are not specified in the file. The `definenode` command does not allow you to specify additional attributes on the command line when using the `-f` flag.

You can also use the `definenode -s` flag to create a node definition file. The `-s` flag tells the `definenode` command to send a list of the nodes and their attributes to standard output. The information includes what you provided on the command line in addition to whatever default values would be set. The nodes are not defined in the CSM database if you use the `-s` flag. You can redirect the output of the `definenode -s` command to a file. This file is created in the correct format to be used as a node definition file. Check this file to be sure it is correct and complete, and edit the file, if necessary, before using it to define the nodes.

For details about the node definition file, see the `nodedef` man page or CSM for AIX and Linux: Command and Technical Reference. For an example of a typical node definition file, see Creating a node definition file.

To define a set of cluster nodes, as specified in a node definition file, do the following:

### Table 50. Define cluster node sets

<table>
<thead>
<tr>
<th>If using:</th>
<th>Do this:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command line</td>
<td>Issue the <code>definenode</code> command. For example:</td>
</tr>
<tr>
<td></td>
<td><code>definenode -f /tmp/mynodedefs</code></td>
</tr>
<tr>
<td>Web-based System Manager or DCEM</td>
<td>Not applicable</td>
</tr>
<tr>
<td>SMIT</td>
<td>Issue the <code>definenode</code> command using SMIT. The fastpath is <code>csm_defnodes</code>. For example:</td>
</tr>
<tr>
<td></td>
<td><code>smit csm_defnodes</code></td>
</tr>
</tbody>
</table>

### Automatic node detection and definition

Using the `definenode -M` flag, you can specify a host name mapping file that allows you to define large numbers of CSM cluster nodes. The host name mapping (hostmap) file contains a list of host names and associated hardware control information. The `definenode` command uses the information in the file to create CSM node definitions. Any other required attribute values can be specified on the command line.

Before you create the hostname mapping file, you must run the `systemid` command to define the user IDs and passwords that are required to access remote hardware control points. See Store AIX hardware control point user IDs and passwords.
Note that if the PowerMethod attribute is **hmc**, the default value for the ConsoleMethod attribute is **hmc** and the default for ConsoleServerName is the name of the hardware control point.

A hostmap file can be created by running the **lshwinfo** command, redirecting the output to a file, and editing the file to add the host names for each machine. This command gathers hardware control information for all nodes that are controlled by the specified hardware control point.

**Note:**
If the PowerMethod attribute is **fsp**, use the **hwsda** command instead of **lshwinfo**.

### Linux on POWER-based architecture node example

The following information is required if you are using hardware control:

- The resolvable host name or IP address of the node. This is the node's network interface, as known by the management server.
- The PowerMethod attribute value set to **hmc**.
- The HWControlPoint and either the LParID or HWControlNodeID attribute values. HWControlNodeID must be unique per node.
- The InstallCSMVersion, InstallOSName, InstallDistributionName, InstallDistributionVersion and InstallPkgArchitecture attributes must be set to appropriate values.

The following example shows how to create a host name mapping file that lists the nodes associated with hardware control point **hmc01**, has a PowerMethod of **hmc**, and is redirected to a file called /tmp/mymapfile:

1. Create the hostmap file, by issuing the following command:

   ```bash
   lshwinfo -p hmc -c hmc01 -o /tmp/mymapfile
   ```

   The output file /tmp/mymapfile would look like the following:

   ```
   # Hostname::PowerMethod::HWControlPoint::HWControlNodeID::LParId::HWType: \
   :HWModel::HWSerialNum
   no_hostname::hmc::hmc01.kav.opn.com::lpar01::001::7040::681::7017-S9
   no_hostname::hmc::hmc01.kav.opn.com::lpar02::002::7040::681::7017-S9
   no_hostname::hmc::hmc01.kav.opn.com::lpar03::003::7040::681::7017-S9
   no_hostname::hmc::hmc01.kav.opn.com::lpar04::004::7040::681::7017-S9
   ```

2. Edit the hostmap file to add the host names for each node. For example:

   ```
   # Hostname::PowerMethod::HWControlPoint::HWControlNodeID::LParId::HWType: \
   :HWModel::HWSerialNum
   clstrn01::hmc::hmc01.clusters.com::lpar01::001::7040::681::7017-S9
   clstrn02::hmc::hmc01.clusters.com::lpar02::002::7040::681::7017-S9
   clstrn03::hmc::hmc01.clusters.com::lpar03::003::7040::681::7017-S9
   clstrn04::hmc::hmc01.clusters.com::lpar04::004::7040::681::7017-S9
   ```

Note that if the nodes you are defining are pSeries LPARS, the value of the HWControlNodeID is the name that was assigned to the LPAR when it was defined. If the host name that you intend to use for that LPAR is used as the LPAR name, it is easier to add the host names to the hostmap file. In this case, the host name would be the same as the HWControlNodeID.

For example, the first line in step 2 above would be:
Depending on the hardware control point, the output of the `lshwinfo` command varies and some information is not returned. In most cases, except for the host name, the missing information is not required. You can add missing fields manually, if necessary.

If you use the `lshwinfo -s` flag, and a hostname is not already defined for the node, the command attempts to resolve the `HWControlNodeId`. If successful, it uses the resolved value to fill in the hostname field. If you define your LPAR or ASM names as the short hostname of the node, this command option creates a hostmap file with the correct long hostnames.

For pSeries systems, the file can contain information about the LPARs that have been defined. This information allows you to create CSM node definitions, by issuing the following command:

```
definenode -M /tmp/mymapfile InstallCSMVersion=1.7.1 InstallOSName=Linux
```

### Linux on x86 architecture node example

The following information is required if you are using hardware control:

- Set the `Hostname` attribute to the resolvable host name or IP address of the node. This is the nodes' network interface as known by the management server.
- The `PowerMethod` attribute is set to `bmc2` for System x 3455, 3550, 3650, 3655 and 3755 `xseries` for xSeries and remaining System x models, `blade` for BladeCenter, `apc` for devices that use the APC MasterSwitch, and `bmc` for eServer 325 and 326.
- The `HWControlPoint` and `HWControlNodeId` attribute values. `HWControlNodeId` must be unique per node.
- The `ConsoleMethod` attribute set to `mrv`, `esp`, `computone`, `conserver`, `els`, or `cyclades`.
- The `ConsoleServerName`, and `ConsolePortNum`, and `ConsoleSerialDevice` attribute values.
- The `InstallCSMVersion`, `InstallOSName`, `InstallDistributionName`, `InstallDistributionVersion` and `InstallPkgArchitecture` attributes must be set to appropriate values.

For example, to create a hostmap file that lists the nodes associated with hardware control points `frame10` and `frame11` and a `PowerMethod` of `xseries` to a file called `/tmp/hcp_out`:

1. Issue the `lshwinfo` command, as follows:

```
lshwinfo -p xseries -c frame10,frame11 -o /tmp/hcp_out
```

The output file `/tmp/hcp_out` is similar to:

```
# Hostname::PowerMethod::HWControlPoint::HWControlNodeId::LPARId: \
:HWType::HWModel::HWSerialNum::DeviceType
no_hostname::xseries::frame10.acme.com::node01:::::::
no_hostname::xseries::frame10.acme.com::node02:::::::
no_hostname::xseries::frame10.acme.com::node03:::::::
no_hostname::xseries::frame10.acme.com::node04:::::::
no_hostname::xseries::frame11.acme.com::node01:::::::
no_hostname::xseries::frame11.acme.com::node02:::::::
no_hostname::xseries::frame11.acme.com::node03:::::::
no_hostname::xseries::frame11.acme.com::node04:::::::
```

2. Edit the hostmap file to add the host names for each node. For example:
On System x, the file can contain information about nodes that have been defined. You can use this information to create CSM node definitions using the `definenode` command. For example:

```
definenode -M /mydir/mymapfile -C mrv1:1:0:12 ConsoleMethod=mrv /InstallCSMVersion=1.7.1 InstallOSName=Linux
```

### AIX and Linux on POWER node example

The following example shows how to create a host name mapping file that lists the nodes associated with hardware control point `hmc01`, has a `PowerMethod` of `hmc`, and is redirected to a file called `/tmp/mymapfile`:

1. Create the hostmap file, as follows:

   **Table 51. Create a host name mapping file**

<table>
<thead>
<tr>
<th>If using:</th>
<th>Do this:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command line</td>
<td>Issue the <code>lshwinfo</code> command, as follows:</td>
</tr>
<tr>
<td></td>
<td><code>lshwinfo -p hmc -c hmc01 -o /tmp/mymapfile</code></td>
</tr>
<tr>
<td>Web-based System Manager or</td>
<td>Not applicable.</td>
</tr>
<tr>
<td>DCEM</td>
<td></td>
</tr>
<tr>
<td>SMIT</td>
<td>Issue the <code>lshwinfo</code> command using SMIT. The fastpath is <code>csm_lshwinfo</code>. For example:</td>
</tr>
<tr>
<td></td>
<td><code>smit csm_lshwinfo</code></td>
</tr>
</tbody>
</table>

The output file `/tmp/mymapfile` is similar to:

```
# Hostname::PowerMethod::HWControlPoint::HWControlNodeID::LParId::HWType::HWModel::HWSerialNum::DeviceType::UUID
no_hostname::hmc::hmc01.kav.opn.com::lpar01::001::7040::681::7017-S9:    
no_hostname::hmc::hmc01.kav.opn.com::lpar02::002::7040::681::7017-S9:    
no_hostname::hmc::hmc01.kav.opn.com::lpar03::003::7040::681::7017-S9:    
no_hostname::hmc::hmc01.kav.opn.com::lpar04::004::7040::681::7017-S9:    
```

2. Edit the hostmap file to add the host names for each node. For example:

```
# Hostname::PowerMethod::HWControlPoint::HWControlNodeID::LParId::HWType: \
:HWModel::HWSerialNum::DeviceType::UUID
clstrn01::hmc::hmc01.clusters.com::lpar01::001::7040::681::7017-S9::    
clstrn02::hmc::hmc01.clusters.com::lpar01::002::7040::681::7017-S9::    
clstrn03::hmc::hmc01.clusters.com::lpar03::003::7040::681::7017-S9::    
clstrn04::hmc::hmc01.clusters.com::lpar04::004::7040::681::7017-S9::    
```
If you are defining pSeries or System p nodes, the **HWControlNodeID** value is the name assigned to the LPAR when it was defined. If the host name used for that LPAR is also used as the LPAR name, add the host names to the hostmap file. In this case, the host name is the same as the **HWControlNodeID**.

For example, the first line in step 2 above would be:

```
clstrn01::hmc::hmc10.clusters.com::clstrn01::001::7040::681::7017-S9
```

Depending on the hardware control point, the output of the `lshwinfo` command varies and some information is not returned. In most cases, except for the host name, the missing information is not required. You can add missing fields manually, if necessary.

If you use the `lshwinfo -s` flag, and a hostname is not already defined for the node, the command attempts to resolve the **HWControlNodeID**. If successful, it uses the resolved value to fill in the hostname field. If you define your LPAR or ASM names as the short hostname of the node, this command option creates a hostmap file with the correct long hostnames.

On System p, the file can contain information about the LPARs that have been defined. This information allows you to create CSM node definitions, as follows:

### Table 52. Create CSM node definitions

<table>
<thead>
<tr>
<th>If using:</th>
<th>Do this:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command line</td>
<td>Issue the <code>definenode</code> command, similar to the following example:</td>
</tr>
<tr>
<td></td>
<td><code>definenode -M /tmp/mymapfile InstallOSName=AIX</code></td>
</tr>
<tr>
<td>SMIT</td>
<td>Issue the <code>definenode</code> command via SMIT. The fastpath is <code>csm_lshwinfo</code>, for example:</td>
</tr>
<tr>
<td></td>
<td><code>smit csm_lshwinfo</code></td>
</tr>
<tr>
<td>Web-based System Manager or DCEM</td>
<td>Use DCEM (Distributed Command Execution Manager) to run the <code>definenode</code> command.</td>
</tr>
<tr>
<td></td>
<td>DCEM can be started standalone, or launched from the Nodes, Groups, or Commands plug-in of Web-based System Manager.</td>
</tr>
</tbody>
</table>

### System x node example

The following example shows how to create a hostmap file that writes the nodes associated with hardware control points **frame10** and **frame11**, and a **PowerMethod** of **xseries**, to a `/tmp/mymapfile` file.

### Table 53. Create a hostmap file

<table>
<thead>
<tr>
<th>If using:</th>
<th>Do this:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command line</td>
<td>1. Issue the <code>lshwinfo</code> command:</td>
</tr>
<tr>
<td></td>
<td><code>lshwinfo -p xseries -c frame10,frame11 -o /tmp/mymapfile</code></td>
</tr>
<tr>
<td></td>
<td>The output file <code>/tmp/hcp_out</code> is similar to:</td>
</tr>
<tr>
<td></td>
<td># Hostname::PowerMethod::HWControlPoint::HWControlNodeID: \</td>
</tr>
<tr>
<td></td>
<td>:LParId::HWType::HWModel::HWSerialNum</td>
</tr>
<tr>
<td></td>
<td>no_hostname::xseries::frame10.clusters.com::node01:::::::::::</td>
</tr>
<tr>
<td></td>
<td>no_hostname::xseries::frame10.clusters.com::node02:::::::::::</td>
</tr>
<tr>
<td></td>
<td>no_hostname::xseries::frame10.clusters.com::node03:::::::::::</td>
</tr>
</tbody>
</table>
2. Edit the hostmap file to add the host names for each node. For example:

```bash
# Hostname::PowerMethod::HWControlPoint::HWControlNodeID: 
:LPARId::HWType::HWMModel::HWSerialNum
clsn01::xseries::frame10.acme.com::node01:0101:
clsn02::xseries::frame10.acme.com::node02:0102:
clsn03::xseries::frame10.acme.com::node03:0103:
clsn04::xseries::frame10.acme.com::node04:0104:
clsn05::xseries::frame11.acme.com::node01:0105:
clsn06::xseries::frame11.acme.com::node02:0106:
clsn07::xseries::frame11.acme.com::node03:0107:
clsn08::xseries::frame11.acme.com::node04:0108:
```

**SMIT**

Issue the `lshwinfo` command using SMIT. The fastpath is `lshwinfo`. For example:

```bash
smit lshwinfo
```

**Web-based System Manager**

Not applicable.

The `lshwinfo` command may not always be able to return information for all the columns listed above. In most cases, except for the host name, the omitted information is be required. Missing fields can be added manually, if necessary.

For System x nodes, the file can contain information about the LPARs that have been defined. This information can be used to create CSM node definitions, as follows:

**Table 54. Create CSM node definitions on System x nodes**

<table>
<thead>
<tr>
<th>If using:</th>
<th>Do this:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command line</td>
<td>Issue the <code>definenode</code> command. For example:</td>
</tr>
<tr>
<td></td>
<td><code>definenode -M /mydir/mymapfile -C mrv1:1:0:12 ConsoleMethod=mrv \ InstallCSMVersion=1.7.1 InstallOSName=Linux</code></td>
</tr>
<tr>
<td>SMIT</td>
<td>Issue the <code>definenode</code> command using SMIT. The fastpath is <code>csm_defnodes</code>. For example:</td>
</tr>
<tr>
<td>Web-based System Manager</td>
<td><code>smit csm_defnodes</code></td>
</tr>
<tr>
<td></td>
<td>Not applicable.</td>
</tr>
</tbody>
</table>

**Verifying node information**

To verify your node information before defining any nodes, run the `definenode` command with the `-M` and `-s` flags and redirect the output to a `nodedef` file. You can check the `nodedef` file for accuracy, edit the file if necessary, and specify the file with the `-f` flag to define your nodes.
Direct attach System p5/POWER 6 node example

Direct attach System p nodes are connected directly to the management server; they do not use an HMC. To define direct attach System p5/POWER 6 nodes:

1. Use the hardware server discovery agent to inventory hardware that is configured on the service network. Run the following command to verify that all the hardware are detected by CSM hardware discovery agent:

   hwsda -s SP

<table>
<thead>
<tr>
<th>device</th>
<th>type-model</th>
<th>serial number</th>
<th>IP addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>SP</td>
<td>9123-710</td>
<td>10DCA8F</td>
<td>192.168.1.2 192.168.3.147</td>
</tr>
<tr>
<td>SP</td>
<td>9123-710</td>
<td>10DC2FF</td>
<td>192.168.1.3 192.168.3.147</td>
</tr>
<tr>
<td>SP</td>
<td>9123-710</td>
<td>10DF57F</td>
<td>192.168.1.4 192.168.3.147</td>
</tr>
<tr>
<td>SP</td>
<td>9123-710</td>
<td>10DC72F</td>
<td>192.168.1.5 192.168.3.147</td>
</tr>
<tr>
<td>SP</td>
<td>9123-710</td>
<td>10DC58F</td>
<td>192.168.1.6 192.168.3.147</td>
</tr>
</tbody>
</table>

2. Create the hostmap file, by issuing the following command:

   hwsda -f -o /tmp/mymapfile

   The output file `/tmp/mymapfile` is similar to:

   Hostname::PowerMethod::HWControlPoint::HWControlNodeId::LParID::HWType::HWMode
   l::HWSerialNum::DeviceType
   no_hostname::fsp::192.168.1.2::10DCA8F::1::9123::710::10DCA8F:::;
   no_hostname::fsp::192.168.1.3::10DC2FF::1::9123::710::10DC2FF:::;
   no_hostname::fsp::192.168.1.4::10DF57F::1::9123::710::10DF57F:::;
   no_hostname::fsp::192.168.1.5::10DC72F::1::9123::710::10DC72F:::;
   no_hostname::fsp::192.168.1.6::10DC58F::1::9123::710::10DC58F:::;

3. Edit the hostmap file to add the hostnames for each node. For example:

   clstrn01::fsp::192.168.1.2::10DCA8F::1::9123::710::10DCA8F:::;
   clstrn02::fsp::192.168.1.3::10DC2FF::1::9123::710::10DC2FF:::;
   clstrn03::fsp::192.168.1.4::10DF57F::1::9123::710::10DF57F:::;
   clstrn04::fsp::192.168.1.5::10DC72F::1::9123::710::10DC72F:::;
   clstrn05::fsp::192.168.1.6::10DC58F::1::9123::710::10DC58F:::;

   Note that the value of the HWControlNodeId is the serial number of the server by default. Because this attribute is required but its value is not limited, changing the attribute value is optional. Use the node short hostname for the HWControlNodeId value.

4. Run the `definenode` command, specifying the hostmap file you edited previously:

   definenode -M /tmp/mymapfile

Defining multiple nodes simultaneously

Multiple nodes can be defined simultaneously by specifying `definenode starting_node` and `count` values, or by providing one or more node ranges. Using a starting_node and count defines the starting node and increments the node IP address to determine the value for the next node. IP addresses are incremented up
to the `count`, which is the total number of nodes. The values for node hardware control and remote console attributes must be specified with the `-H` and `-C` flags.

Using a list of node ranges allows greater flexibility in specifying the list of nodes to define. All the nodes in the list of node ranges are defined, and the values for node hardware control, and remote console attributes must be specified with the `-H` and `-C` flags. See the `noderange` man page for details on specifying node ranges.

When defining multiple nodes simultaneously, it is assumed that the hardware has been configured in a way that facilitates the use of this method. The mapping of IP address to node hardware and console servers can range in complexity, depending on the type of hardware being used and the cluster environment. Initial planning is required for cluster installation and configuration to be automated as much as possible.

When defining multiple nodes simultaneously, the following requirements apply:

- Short host names to be assigned to the nodes are resolvable.
- If using a `starting_node` and `count`, there must be a set of valid consecutive IP addresses that can be assigned to a particular set of nodes.
- The hardware text ID on the ISMP must be set to the short host name of the node. The IBM Integrated System Management Processor (ISMP) device provides monitoring and remote power control for System x and BladeCenter HS nodes. ISMPs are also referred to as ASMs.
- A consecutive set of console port numbers must be connected to nodes with consecutive IP addresses. For example, the first port number connects to the first IP address, the second port number connects to the second IP address, and so on.

To define Linux nodes, the `HWControlNodeId` attribute values must be set to the node short host names. The following command defines 30 nodes with consecutive IP addresses as `HWControlNodeId` values `node1` - `node30`:

```
definenode -n node1 -c 30 -s -H rsa1:10,rsa2:10,rsa3:10 -C mrv1::1:20,mrv2::1:20  
PowerMethod=xseries ConsoleMethod=mrv InstallCSMVersion=1.7.1  
InstallDistributionName=RedHatEL-AS InstallDistributionVersion=4
```

The following example uses a node range:

```
definenode -n node1+30 -s -H rsa1:10,rsa2:10,rsa3:10 -C mrv1::1:20,mrv2::1:20  
PowerMethod=xseries ConsoleMethod=mrv InstallCSMVersion=1.7.1  
InstallDistributionName=RedHatEL-AS InstallDistributionVersion=4
```

**Note:**
The difference between the above examples is that the node range increments by host names, while the `starting_node` and `count` increments by IP address. Depending on the host name resolution, this may result in a different list of nodes being defined.

The nodes are assigned to hardware control points in order up to the total number of nodes for each hardware control point. In the example, there are 10 nodes connected to each hardware control point. The first hardware control point (rsa1) is assigned to the first 10 nodes (node1 - node10); the second hardware control point (rsa2) is assigned to the next 10 nodes (node11 - node20); the third hardware control point (rsa3) is assigned to the last 10 nodes (node21 - node30). The `HWControlNodeId` attributes are set to the node's host names, which must be the same as their ISMP hardware text IDs.

The nodes are assigned to the console servers in order up to the number of ports for each console server. In the example, the first console server (mrv1) is assigned to the first 20 nodes (node1 - node20), and the second console server (mrv2) is assigned to the next 10 nodes (node21 - node30). The number of console
ports must be greater than or equal to the number of nodes being defined. In this case there are only 30 nodes being defined so the last console server is left with some unassigned ports.

In the example, the console port numbers are assigned in consecutive order starting with 1. Port 1 is assigned to the node with the first IP address, port 2 to the next IP address, and so on.

When defining multiple nodes at once, it is important to redirect output to a file and check the file for accuracy before actually creating the node definitions. You can do this using the -s flag as described earlier.
Chapter 9. Defining devices

Before you can add, update, or manage a cluster device—which is any cluster hardware other than node, install server, or management server hardware—you must define the device by defining device attributes in the CSM database.

CSM hardware control for devices provides power control and where applicable, remote console access for a wide range of devices such as hardware control points, external console servers, and remote supervisor adapters. The devices are not required to be on the network, and the names you give them do not have to be resolvable. For those devices that are on the network, CSM can provide a network status.

Note:
To use hardware control, you must store hardware control point user IDs and passwords; see Store Linux hardware control point user IDs and passwords and Store AIX hardware control point user IDs and passwords.

Use the following CSM commands to define and manage device definitions. For detailed command usage information, see the man pages or the CSM for AIX and Linux: Command and Technical Reference.

- definehwdev to define devices to CSM
- rmhwdev to remove device definitions
- chhwdev to modify existing device definitions
- lshwdev to list attribute information for existing devices
- hwdevgrp to allow an administrator to create groups of devices

Determining device attributes

CSM installation requires collecting attribute information for any cluster devices. Device attributes and descriptions are documented in the deviceattributes man page. The following information describes the attributes and values to use when defining devices. The information is divided into the following categories:

- General attributes
- Hardware control attributes
- Status attributes
- Dynamic attributes that describe information CSM returns to the administrator.

General attributes

Name
The name associated with the device. This is the only attribute required to define a device. The name must be unique within the cluster and cannot conflict with other devices or cluster nodes. If the given name can be resolved on the network, the device will be defined with the resolved full hostname. Otherwise, the given name will be used.

DeviceType
Optional device type information provided by the administrator to group devices. You can use the attribute to create dynamic device groups by device type. You can edit this attribute.

**HWType**
Optional hardware information provided by the administrator to identify the device. You can edit this attribute.

**HWModel**
Optional hardware information provided by the administrator to identify this device. You can edit this attribute.

**HWSerialNum**
Optional hardware information provided by the administrator to identify this device. You can edit this attribute.

**PhysicalLocation**
Identifies the location of the device in the frame, for informational purposes only. CSM software does not read or write this value. If this value is returned, it can be used to create a dynamic device group for each frame.

**Properties**
A string value that holds user-defined attributes. Individual properties can be set or changed using the `chhwdev -P` command.

**UserComment**
Comments provided by the administrator about the device. You can edit this attribute.

**RemoteShell**
Specifies the path of the remote shell command that CSM should use to run commands on the nodes. The default is `/usr/bin/rsh` on AIX and `/usr/bin/ssh` on Linux.

**RemoteCopyCmd**
Specifies the remote copy command that the dcp command will use when copying files. The default is `/usr/bin/rcp`.

**RemoteShellUser**
Specifies the user ID to use for remote shell and remote copy execution to the device.

**Hardware control attributes**

For CSM hardware control of devices, you must define the following hardware control attributes for each device:

- **HWControlDeviceId**
- **HWControlPoint**
- **PowerMethod**

You must provide, configure, and attach a supported hardware control point to each device. If the device supports console connections, you can also define the following remote console attributes:

- **ConsoleMethod**
- **ConsoleServerName**
- **ConsolePortNum**

For remote console support, you must also provide, configure, and attach a valid console server to the device console port.

**HWControlDeviceId**
Identifier associated with the device power control. You can edit this attribute. You must define the attribute to enable hardware control. The value is dependent on the PowerMethod and can be one of the following:

- APC MasterSwitch outlet port number.

The value is dependent on the PowerMethod and is the APC MasterSwitch outlet port number.

**HWControlPoint**

The host name of the network adapter for the hardware control point. You can edit this attribute. You must define the attribute to enable hardware control.

**PowerMethod**

The power method used to perform hardware control. The valid values for a CSM for AIX management server are `apc` and `esp`. The valid value for Linux is `apc`. You can edit this attribute. This attribute must be defined to enable hardware control.

**ConsoleMethod**

The console method used to open a device console. You can edit this attribute. Enter the value appropriate to access the remote console for the device. Refer to the `nodeattributes` man page or the CSM for AIX and Linux: Command and Technical Reference for more information.

**ConsolePortNum**

The number associated with the console port for this device. You can edit this attribute. Enter the value appropriate to the ConsoleServerName specified for the device. Refer to the `nodeattributes` man page or the CSM for AIX and Linux: Command and Technical Reference for more information.

**ConsoleServerName**

The host name of the network interface for the console server. It is optional when you define a resource.

## StatusMethod attribute

The StatusMethod specifies the status method used to obtain the network status of the device. The valid values are as follows:

- NONE
- ping

If this attribute is set to NONE or is left undefined, CSM does not perform status checking. If this attribute is set to ping, CSM attempts to ping the general attribute Name for the device. The frequency of this ping operation is configurable; see the `csmconfig DeviceStatusFrequency` attribute.

**Note:**

If the StatusMethod is set to ping using the `definehwdev` command, any device name specified must be resolvable on the network. If the device name cannot be resolved, an error is returned and the device is be defined. If the StatusMethod is set to ping using the `definehwdev` command, and an IP address is specified as the device name, the `definehwdev` command attempts to resolve the IP address to a hostname. If the address can be resolved, the device is defined with the resolved full hostname. Otherwise, the device is defined with the specified IP address.

## Dynamic attributes

You can monitor the following dynamic resource attributes for the IBM.DeviceHwCtrl class:
**PowerStatus**

The current power status of the device. The valid states are:

- OFF (0)
- ON (1)
- UNKNOWN (127)
- UNCONFIGURED (128)

**Status**

The current accessibility status of the device. Accessibility is determined by the `StatusMethod` defined for the device. The valid states are:

- UNREACHABLE (0)
- ALIVE (1)
- UNKNOWN (127)
- UNCONFIGURED (128)

**Mode**

The `Mode` is automatically set by CSM to **PreManaged** or **Managed**. When the device is defined initially the `Mode` is set to **PreManaged**. After successful completion of the `addpeer` or `updatehwdev` command, CSM sets the `Mode` attribute to **Managed**.

---

**Naming devices**

Unlike nodes, devices managed by CSM are not required to be on the network, and the device names are not required to be resolvable to IP addresses. In most cases, the device name must only be unique in the cluster; the device `Name` attribute must not conflict with existing device `Name` values or node `Hostname` values.

CSM always attempts to resolve the given device name or IP address to a full hostname. If the given name or address can be resolved, the device will be defined using the resolved full hostname, and the `StatusMethod` of the device is set to `ping` automatically.

If the given name or address cannot be resolved, the result will depend upon the attributes given when the `definehwdev` command was invoked. If the `StatusMethod` attribute was explicitly set to `ping` on the `definehwdev` command line, the command will fail and the device will not be defined. If the `StatusMethod` attribute was defined to a value other than `ping`, or left undefined, the device will be defined with the exact name or address given.

If the device is defined with `StatusMethod` set to no value or a value other than `ping`, the `definehwdev` command attempts to resolve the given name to prevent naming conflicts. For example, if you try to define a device named **1.2.3.4** with `StatusMethod` set to no value or a value other than `ping`, and a device named **device1.cluster.com** already exists, CSM does not create the device **1.2.3.4** because the IP address resolves to a full hostname of a device that is already defined. If you try to define a device named **1.2.3.4** with `StatusMethod` set to no value or a value other than `ping`, and a device named **device1.cluster.com** does not already exist, CSM creates the new device named **1.2.3.4**.
Store hardware control point user IDs and passwords

Storing hardware control point user IDs and passwords is required for hardware control. For more information, see Store Linux hardware control point user IDs and passwords and Store AIX hardware control point user IDs and passwords.

Defining devices

To define CSM devices—which are any cluster hardware other than node, install server, or management server hardware—consider the following.

Defining a single device

You must ensure that each device name is unique within the cluster. Specific device information is stored as device attributes and values in the CSM database. Use the definehwdev command to set the device attributes. For the complete list of device attributes, see the deviceattributes man page. Default values are set for some attributes if they are not provided on the command line. To view the set of values that the definehwdev command sets without actually creating the definitions, use the -s flag. For example:

```
definehwdev -d dev1.clusters.com HWControlPoint=apc03.clusters.com \
HWControlDeviceId=2 PowerMethod=apc ConsoleServerName=mrv02.clusters.com \
ConsolePortNum=3 ConsoleMethod=mrv
```

Using a device definition file

You can use a device definition file to define multiple devices. A devicedef file consists of stanzas containing device attribute values for each device to be defined. For an example see the following sample:

```
/opt/csm/samples/install/devicedef.sample
```

You can create devicedef manually and pass the file to the definehwdev command using the -f flag. The definehwdev command then uses the file to create device definitions. When possible, default values are set for attributes that are not specified in the file.

The definehwdev command does not accept additional attributes specified on the command line when you use the -f flag. You can use the -s flag on the definehwdev to create a device definition and redirect the output of the command to a specific file. You can then modify the file as required and pass it back to the definehwdev command by using the -f flag.

For example, to define a set of devices specified in a file called myservicedefs, issue the following command:

```
definehwdev -f /tmp/myservicedefs
```

For details on the device definition file, see the devicedef man page.
Using a device mapping file

Use the `definehwdev` command with the `-M` flag to define large numbers of CSM cluster devices simultaneously. The flag specifies a file containing a list of host names and associated hardware control information. The `definehwdev` command uses the host names to create CSM device definitions. Values to use for the `HWControlPoint` and `HWControlDeviceId` attributes are retrieved from the associated hardware control information provided in the file. You can specify any other required attribute values on the command line.

You can create a host name mapping file by running the `lshwinfo` command, redirect the output to a file, and edit the file to add the names for each device, provided that the hardware control point to which the device is attached supports the `lshwinfo` command. Before you run the `definehwdev -M` command, you must ensure that these comment characters are removed from the host name mapping file for any I/O units that you want to define.

---

Defining devices scenarios

Common scenarios for defining devices in a CSM cluster include adding network switches, and System p5 I/O server partitions.

Adding network switches

Your cluster might contain one or more network switches to manage network traffic. You can add these switches to the CSM cluster as devices to control them from the CSM management server. The switches can be plugged into an APC MasterSwitch remote control power strip to provide power control. You can connect the serial console port of the switches to a console server device to provide remote console access.

To define the switch, use the `definehwdev` command. Define the following hardware control attributes:

- For power control, set the `HWControlPoint` attribute to the network name of the power strip.
- Set the `PowerMethod` attribute to `apc`.

Once these definitions are complete, you can use the `rpower` command with the `-d` flag to power the switch on or off, or to query the power status.

For remote console access, define the following console attributes:

- Set the `ConsoleServerName` attribute to the network name of the console server.
- Set the `ConsolePortNum` attribute to the port number on the console server to which the console port of the switch is connected.
- Set the `ConsoleMethod` to the appropriate value for the console server that you are using.

Once these definitions are complete, you can use the `rconsole` command with the `-d` flag to open a remote console to the switch. If the switch can be accessed from the network, you can also choose to set the `StatusMethod` attribute to `ping`. Assuming that the `Name` general attribute of the device is set to the network name of the switch, CSM pings the device to determine if it is reachable on the network. CSM updates the status attribute with the appropriate network status of the device.
Adding System p5/POWER 6 I/O server partitions

The Advanced POWER Virtualization feature for IBM System p5/POWER 6 includes support for virtual I/O devices. The virtual I/O option includes virtual SCSI for sharing Fibre Channel and SCSI adapters and the attached disk drives and virtual networking to enable the sharing of Ethernet adapters. Sharing I/O devices and adapters allows multiple partitions to coexist on a System p5/POWER 6 server with fewer disk drives, adapters, cables and other infrastructure.

Virtual I/O devices are owned by a Virtual I/O Server partition, which provides access to the real hardware that the virtual device is based on. A single I/O server partition can provide virtual I/O for many client partitions.

The I/O Server Partition will operate as a self-contained appliance with limited function and limited user access. The virtual I/O Server partition is created using the Hardware Management Console (HMC) and is installed using the new AIX NIMOL support running on the HMC or directly from a CD.

In a CSM cluster environment the I/O Server partition may be managed as a non-node device. Information about the I/O Server partition can be gathered using the `lshwinfo` command. An I/O Server partition can be identified by checking for the string `IOServer` in the `DeviceType` field output from the `lshwinfo` command. The partition may be defined as a non-node device using the `definehwd` command.

CSM supports basic `rpower` (on, off, reboot, and query) hardware control and monitoring of the partition. CSM also supports `rconsole` for the I/O Server partition.

For more information, see *Partitioning Implementations for IBM eServer System p5 Servers, SG24-7039-02.*
Chapter 10. System x hardware inventory and maintenance

CSM hardware inventory and maintenance commands scan, configure, and update x86-based System x servers prior to node installation. Other server types are not supported.

For hardware inventory and maintenance command usage information, see the CSM for AIX and Linux: Command and Technical Reference or the man pages for the csmsetuphwmaint, mkflashfiles, rfwscan, rfwcfg, and rfwflash commands.

Hardware inventory and maintenance on pre-OS nodes

After your management server and install servers are set up and your nodes are defined, you can collect node hardware information before installing the operating system. CSM commands can collect the BIOS level, hardware type, model and serial number, and UUID information from nodes in this pre-operating system (pre-OS) state.

CSM configures pre-OS nodes to boot over the network from the install server. The nodes are configured in much the same way as they are for a node install, although not all the steps are required. In particular, the same scaling considerations that exist for node installations apply to the pre-OS environment as well. Review the scaling considerations information before proceeding. Then, review the information contained in Installing Linux on nodes, and perform the following steps:

1. Check Linux node software requirements
2. Set the node boot order for Linux on System x nodes
3. Verify Linux node hardware control point user IDs and passwords
4. Verify Linux node definitions
5. Validate remote power for Linux nodes
6. Copy SLES service level CDs
7. Configure Linux driver modules

Attention:

BIOS settings control many different aspects of node operation; incorrect settings can render a node inoperable. Use care when making changes to node BIOS settings.

Once these steps are completed, run the csmsetuphwmaint command on the management server to create the network kernel and ramdisk that will be used to boot the node. The Linux distribution and version used for the network kernel and ramdisk will be determined by the InstallDistributionName, InstallDistributionVersion, and InstallServiceLevel attributes defined for the node in the CSM database.

If you have already run copycds, run:

csmsetuphwmaint -n node01,node02 -x

If you have NOT already run copycds, run:

csmsetuphwmaint -n node01,node02 -x

CSM for AIX and Linux: Planning and Installation Guide
You will be prompted for Linux distribution CDs.

If the nodes are configured to use different Linux distributions, it may be necessary to run the command more than one time. For example, if one group of cluster nodes is set up to use Red Hat EL AS 4, and another group is set up to use SLES 9, the `csmsetuphwmaint` command would need to be run twice, once for each distribution. CSM includes some predefined node groups that make this task easier. See the `nodegrp` command man page or the *CSM for AIX and Linux: Command and Technical Reference* for information on listing node groups.

When these nodes are booted from the install server, the desired scan, BIOS update, or BIOS setting operation is performed, the CSM database is updated (if requested), and then the node is reset to boot from local disk on its next boot. Since the node uses an active network connection to the install server, it is powered off once the operation is completed.

---

**Performing hardware inventory and maintenance**

After the network kernels and ramdisks are created, the hardware inventory and maintenance commands can be run. The commands use the `-r` flag to determine pre-OS behavior. By default, the commands always try to use the CSM `dsh` command to run the task. If a target node is managed by CSM and reachable by `dsh`, the task is performed on the running system. If the `-r` flag is specified, the target node is rebooted at the end of the task so the changes can take effect.

If the target node is not managed by CSM or reachable by `dsh`, the `-r` flag determines how the command proceeds. If the `-r` flag is not specified, the command returns an error and exits. If the `-r` flag is specified, the command attempts to reboot the node from the network and perform the task.

**Collecting system information**

The `rfwscan` command is used to collect BIOS levels, hardware type and model numbers, serial numbers, and the UUID from nodes. This information can be written to the CSM database if desired. Use one of the following forms of the `rfwscan` command with the `-r` flag to collect information in a pre-OS environment:

**Note:**

Before running this command, you must complete the steps listed in *Hardware inventory and maintenance on pre-OS nodes*, and run `csmsetuphwmaint`.

1. To scan specific nodes:
   2. `rfwscan -r -n node01,node02`
2. To scan specific node groups:
   4. `rfwscan -r -N SLES9Nodes`
5. Write the results of the scan to the CSM database, add the `-w` flag:
6. `rfwscan -r -w -N SLES9Nodes`

The `rfwscan -w` command sets the following attributes, if available for the node: `HWType`, `HWModel`, `HWSerialNum`, `UUID`, `FWSvcProc`, and `FWSysBIOS`. 
Updating BIOS levels

The `rfwflash` command is used to perform BIOS updates to various hardware components. The command uses Linux update packages to perform these updates. These packages must be downloaded from the IBM Support Web site, at [http://www.ibm.com/support](http://www.ibm.com/support).

**Note:**
Before running this command, you must complete the command prerequisites, including running the `csmsetuphwmaint` command.

To successfully apply BIOS updates, the node definitions in the CSM database must include the correct values for the `HWType` attribute for the target nodes. The `HWType` attribute is defined by the `rfwscan -w` command, or it can be set manually using the `chnode` command. See the information on remote hardware inventory and maintenance in the *CSM for AIX and Linux: Administration Guide* for information about hardware types and Linux update packages.

Perform the following steps:

1. Define the `HWType` attribute in the CSM database for the target nodes.
2. Download the appropriate Linux update packages from the IBM Support Web site. At [http://www.ibm.com/support](http://www.ibm.com/support), select **Drivers and Downloads**, navigate to the pages supporting the target servers, and download the appropriate packages.

   **Note:**
   There are two different styles of Linux Update Packages available on the Web site. Under the `dsh` environment, CSM supports both the newer, more compact `lflash` packages, and the older package style that does not flash the BIOS while Linux is running, but instead queues a DOS-based update to run at the next reboot. One way to tell the difference between the two styles is by file size. The `lflash` packages are generally under 1 MB; the older style packages are 2 MB or greater. *When running in a pre-OS environment, only the lflash package is supported.*

3. Use the `mkflshfiles` command to copy the downloaded packages to the correct CSM directory.
4. Use one of the following `rfwflash -r` commands to update BIOS in a pre-OS environment:
   - To flash the system BIOS for specific nodes:
     ```
     rfwflash -t system -r -n node01, node02
     ```
   - To flash all available components on specific node groups:
     ```
     rfwflash -r -N RedHatELAS4Nodes
     ```

   Occasionally, the existing BIOS on a system may not properly support network booting. In these cases, pre-OS support for BIOS updates cannot be used, because the target nodes are required to boot from the network to perform the task; manually update the BIOS for these nodes.

**Querying and setting BIOS settings**

The `rfwcfg` command queries or sets the BIOS settings on System x and BladeCenter HS and LS nodes.

**Note:**
Before running this command, you must have first followed the steps listed in **Hardware inventory and maintenance on pre-OS nodes**, and have run `csmsetuphwmaint`.
To successfully query or set BIOS settings, the node definitions in the CSM database must include the correct \textit{HWType} attribute values for the target nodes. Set the \textit{HWType} attributes using the \texttt{rfwscan -w} command, or manually using the \texttt{chnode} command. See the remote hardware inventory and maintenance information in the \textit{CSM for AIX and Linux: Administration Guide} for the supported \textit{HWType} values.

Perform the following steps:

1. Populate the \textit{HWType} attribute in the CSM database for the target nodes.
2. Use the one of the following forms of the \texttt{rfwcfg} command with the -r flag to query or set BIOS settings in a pre-OS environment:
   - To show the current values of all BIOS settings on a specific node:
     \begin{verbatim}
     rfwcfg -r -n node01 --show
     \end{verbatim}
   - To show the current values of BIOS settings for a specific node and write those settings to a file:
     \begin{verbatim}
     rfwcfg -r -n node01 --show --o my_settings_file
     \end{verbatim}
   - To use a file to set BIOS settings on a specific node:
     \begin{verbatim}
     rfwcfg -r -n node01 -f my_settings_file
     \end{verbatim}

The settings files created and used by the \texttt{rfwcfg} command reside in directories specific to the hardware type of the target nodes. For information on settings files, see the \texttt{rfwcfg} command man page or the \textit{CSM for AIX and Linux: Command and Technical Reference}, and the remote hardware inventory and maintenance information in the \textit{CSM for AIX and Linux: Administration Guide}.  

---

CSM for AIX and Linux: Planning and Installation Guide
Chapter 11. Adding AIX nodes

Use the following procedure to add a node that is installed with AIX to a CSM cluster.

Prerequisites for adding AIX nodes

Before continuing, ensure that you have completed the following steps:

- Set up an AIX or Linux management server; see Installing a CSM for AIX management server or Installing a CSM for Linux management server.
- Defined the AIX nodes to be added to your CSM cluster; see Defining nodes.
- Installed AIX for POWER Version 5.3 or 6.1 on your nodes. You can set up an install server to install AIX nodes; see Setting up install servers.
- Verified that your AIX node software is supported; see Planning for CSM software.
- Considered upgrading your AIX nodes a new version of CSM for AIX; see Updating CSM for AIX.
- For node hardware control, set up hardware control points and console servers; see CSM for AIX and Linux: Administration Guide.

Once you have met the prerequisites, you can begin adding AIX nodes to your cluster.

Verify AIX node definitions

Before you add your AIX nodes, verify the node definitions and if necessary, update them. At this stage, you can make changes to any AIX node definitions.

Verify AIX node definitions:

Table 55. Verify AIX node definitions

<table>
<thead>
<tr>
<th>If using:</th>
<th>Do this:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command line</td>
<td>Issue the <strong>lsnode</strong> command from the management server, as follows:</td>
</tr>
<tr>
<td></td>
<td><code>lsnode</code></td>
</tr>
<tr>
<td>SMIT</td>
<td>Issue the <strong>lsnode</strong> command through SMIT. The fastpath is <code>csm_</code>lsnode.</td>
</tr>
<tr>
<td></td>
<td>For example: <code>smit csm_</code>lsnode.</td>
</tr>
<tr>
<td>Web-based System Manager or DCEM</td>
<td>Use the <strong>Nodes</strong> plug-in to display node information, or use DCEM to run the <strong>lsnode</strong> command. DCEM can be started standalone, or launched from the <strong>Nodes</strong>, <strong>Groups</strong>, or <strong>Commands</strong> plug-in from Web-based System Manager.</td>
</tr>
</tbody>
</table>

CSM for AIX and Linux: Planning and Installation Guide
The system responds with one line for each node that has been correctly defined. If a node has not been defined, it will not appear in `lsnode` command output.

**Display AIX node attributes:**

<table>
<thead>
<tr>
<th>If using:</th>
<th>Do this:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command line</td>
<td>Issue the <code>lsnode -l</code> (lowercase L) command from the management server:</td>
</tr>
<tr>
<td></td>
<td><code>lsnode -l</code></td>
</tr>
<tr>
<td>SMIT</td>
<td>Issue the <code>lsnode</code> command through SMIT. The fastpath is <code>csm_lsnod</code>. For example:</td>
</tr>
<tr>
<td></td>
<td><code>smit csm_lsnod</code></td>
</tr>
<tr>
<td>Web-based System Manager or DCEM</td>
<td>Use the <code>Nodes</code> plug-in to display node information, or use DCEM to run the <code>lsnode</code> command. DCEM can be started standalone, or launched from the <code>Nodes, Groups</code>, or <code>Commands</code> plug-in of Web-based System Manager.</td>
</tr>
</tbody>
</table>

The system responds with output containing extended information for each node that has been correctly defined. If a node has not been defined, it does not appear in the `lsnode` command output. Note that some of the attributes for a node might have null values at this point.

If you need to make corrections, either remove the node that is not correctly defined and re-define it, or use the `chnode` command to make the necessary changes to the node definition.

**To remove an AIX node before redefining it:**

<table>
<thead>
<tr>
<th>If using:</th>
<th>Do this:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command line</td>
<td>Issue the <code>rmnode</code> command on the management server:</td>
</tr>
<tr>
<td></td>
<td><code>rmnode hostname</code></td>
</tr>
<tr>
<td>SMIT</td>
<td>Issue the <code>rmnode</code> command through SMIT. The fastpath is <code>csm_rmnode</code>. For example:</td>
</tr>
<tr>
<td></td>
<td><code>smit csm_rmnode</code></td>
</tr>
<tr>
<td>Web-based System Manager or DCEM</td>
<td>Use the <code>Nodes</code> plug-in to remove a node, or use DCEM to run the <code>rmnode</code> command. DCEM can be started standalone, or launched from the <code>Nodes, Groups</code>, or <code>Commands</code> plug-in of Web-based System Manager.</td>
</tr>
</tbody>
</table>

To change AIX node attributes:

<table>
<thead>
<tr>
<th>If using:</th>
<th>Do this:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command line</td>
<td>Issue the <code>chnode</code> command from the management server:</td>
</tr>
<tr>
<td></td>
<td><code>chnode hostname attr=value</code></td>
</tr>
<tr>
<td>SMIT</td>
<td>Issue the <code>chnode</code> command through SMIT. The fastpath is <code>csm_chnode</code>. For example:</td>
</tr>
</tbody>
</table>
Use the `Nodes` plug-in to change attributes of a node, or use DCEM to run the `chnode` command. DCEM can be started standalone, or launched from the `Nodes`, `Groups`, or `Commands` plug-in of Web-based System Manager.

To use separate install servers not on the management server, ensure that the install servers installed and defined as CSM Managed nodes. If the nodes you are installing are defined with the `InstallServer` attribute set to blank or a value that does not equal the management server value, you must have already run `updatenode` on each install server and verified that the `Mode` attribute is set to `Managed`.

### Create CSM for AIX node groups (optional)

Creating CSM node groups simplifies the remaining installation process. To create a node group:

**Table 59. Create CSM for AIX node groups**

<table>
<thead>
<tr>
<th>If using:</th>
<th>Do this:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command line</td>
<td>Issue the CSM <code>nodegrp</code> command. For example: <code>nodegrp -a clusternode1,clusternode2 cluster_grp</code></td>
</tr>
<tr>
<td>SMIT</td>
<td>Issue the <code>nodegrp</code> command through SMIT. The fastpath is <code>csm_mknod</code> for example: <code>smit csm_mknod</code></td>
</tr>
<tr>
<td>Web-based System Manager or DCEM</td>
<td>Use the <code>Groups</code> plug-in to create a node group. DCEM can be started standalone, or launched from the <code>Nodes</code>, <code>Groups</code>, or <code>Commands</code> plug-in of Web-based System Manager.</td>
</tr>
</tbody>
</table>

When you use the `nodegrp` command, you supply the node names followed by the name you want to designate for that group. In the example above, `clusternode1,clusternode2` are the nodes and `cluster_grp` is the name of the group that includes those nodes.

See the man pages or the *CSM for AIX and Linux: Command and Technical Reference* for more information about the `lsnode`, `rmnode`, and `chnode` commands.

### Prepare CSM for AIX customization scripts (optional)

Prepare any user-defined customization scripts. These scripts are used in Add AIX nodes to the cluster.
For information on CSM support for user-provided customization scripts, see the CSM for AIX and Linux: Administration Guide.

---

**Install OpenSSH and OpenSSL for AIX**

This step is required if you established `ssh` as your remote shell. Because OpenSSH and its prerequisite OpenSSL are not installed automatically with AIX, you must install the software on the AIX cluster nodes. See Install OpenSSH and OpenSSL for AIX.

---

**Install Kerberos client file sets for AIX (optional)**

To use Kerberos for remote commands, install the Kerberos client file sets on the node. You might have already copied these files to your management server in Install Kerberos Version 5 for CSM for AIX remote commands. Install the following files on the node, where `lang` can be any valid language; for example, `en_US`:

- `krb5.client.rte`
- `krb5.msg.lang`

Assuming that the directory containing the Kerberos files has been exported to the node and mounted, issue the following command:

```
geninstall -IaXY -d /mnt krb5.client.rte krb5.msg.lang```

The directory is mounted on the node and the command is run on the node.

---

**Set up AIX cluster configuration (optional)**

You can use CSM Configuration File Manager (CFM) to automatically perform various configuration tasks when adding a node to the cluster. For example, you can distribute configuration files to the nodes, such as password files. For more information on CFM, see the CSM for AIX and Linux: Administration Guide.

CSM also provides a set of samples that you can use to help configure the cluster. Samples are provided for configuring NTP, automounter, and network tuning. If you plan to use any of the CSM samples provided with this release, do the setup as documented in the appropriate README file in the following directory:

```
/opt/csm/samples/docs```

You can modify the samples to handle different configuration or system requirements.
Prepare for AIX secondary adapter configuration (optional)

Secondary adapters may be configured during the node installation process or when adding a node to the cluster. To use this support there are some additional steps that must be completed. Refer to Secondary adapter interface configuration for a description of how to use this CSM feature.

Add AIX nodes to the cluster

The `updatenode` command adds the AIX nodes to the cluster. Run the `updatenode` command for the AIX nodes that you have defined. The `updatenode` command does the following for an AIX node:

- If remote shell authentication is not already set up, automatically sets up remote shell authentication for OpenSSH or `rsh`. See AIX remote shell attributes.
- Distributes configuration files if configuration file manager (CFM) is set up. Setting up CFM before installing your nodes can save you from needing to customize the nodes later. For information on configuring CFM, see the CSM for AIX and Linux: Administration Guide.
- Runs any user customization scripts. See Prepare CSM for AIX customization scripts (optional).
- Sets up the Kerberos Version 5 options for remote commands if requested on the `csmconfig` command. For information, see Set up Kerberos Version 5 for CSM for AIX remote command processing (optional).

Before you run `updatenode`, ensure the following:

- The management server and any install servers are configured and the AIX nodes are defined.
- The AIX nodes have all the prerequisite AIX software. Ensure that the following CSM software is installed on the AIX nodes:
  - `csm.core`
  - `csm.client`
  - `csm.dsh`

  This software is installed automatically with AIX. If for some reason it has been uninstalled, you must ensure that it is reinstalled.

- To use Kerberos remote command processing, the required software is installed; see CSM for AIX Kerberos setup.
- The AIX nodes are up and running.

For information on prerequisite software, see the CSM README file and Planning for CSM software.

It is not necessary to update the cluster nodes with the latest available CSM software updates unless the updates are specifically required. See the following CSM support Web site for information on any required updates for the nodes: [http://www14.software.ibm.com/webapp/set2/sas/f/csm/download/home.html](http://www14.software.ibm.com/webapp/set2/sas/f/csm/download/home.html). To update the CSM level for your AIX nodes, see Updating CSM for AIX.

When a node has been defined but not added to the cluster, its `Mode` attribute is `PreManaged`. After a node has been defined and added to the cluster with the `updatenode` command, its `Mode` attribute changes to `Managed`, and the node becomes a managed node of the cluster. Note that if the `updatenode` command
is not successful, the node's Mode attribute remains **PreManaged** and the `UpdateNodeFailed` attribute is set to 1 (true).

**Kerberos and standard authentication:** If you have set up Kerberos Version 5 for `rsh` remote command processing with the managed nodes, ensure that standard AIX authentication is enabled so that a common authentication exists between the management server and the nodes; otherwise, command processing might fail. To determine the current authentication setting, use the `lsauthent` command. For information about enabling standard AIX authentication, see Enabling standard AIX remote command authentication.

**AIX remote shell attributes**

For authentication, the `updatenode` command prompts you for the root password for the target nodes. As a result, you must either make the root password common to all the target nodes, or run the `updatenode` command to each node, or group of nodes, and provide the related passwords.

When you set up the management server, you specified the `RemoteShell` and `SetupRemoteShell` attribute values with the `csmconfig` command; see Check the CSM for AIX remote shell attribute. The `updatenode` command behaves differently, depending on the `RemoteShell` and `SetupRemoteShell` attribute values specified with `csmconfig` command, and the Kerberos `SetupKRB5` attribute value specified with the `csmconfig` command, as follows:

- If you specified `RemoteShell=/usr/bin/rsh` and `SetupRemoteShell=1` (yes), the `updatenode` command sets up remote shell access and uses standard AIX authentication to all AIX **PreManaged** nodes. This is also true for all cluster nodes if you used the `-k` flag with the `updatenode` command, which prompts you for the root password.
- If you specified `RemoteShell=/usr/bin/ssh` and `SetupRemoteShell=1` (yes), and OpenSSH is installed on the management server and the nodes, the `updatenode` command sets up secure shell access to all **PreManaged** nodes. This is also true for all cluster nodes if you used the `updatenode -k` command, which prompts you for the root password.
- If you specified `SetupRemoteShell=0` (no), the `updatenode` command does not set up remote access for any of the nodes.
- If `csmconfig SetupKRB5` indicates to set up the Kerberos client, CSM sets up the nodes as Kerberos clients.
- If `csmconfig SetupKRB5` indicates to set up Kerberos principals, when you run `updatenode -k`, or when you run `updatenode` with defaults to a **PreManaged** node, CSM adds the CSM principal to the `.k5login` file in the home directory of root on each node and transfers the host key of the node to the node. To only transfer the keytab for the host node from the management server to the managed node, you can run `updatenode -K krb5 nodename`, where `nodename` is the name of the node.

To add all **PreManaged** AIX nodes to your cluster and make them **Managed** nodes, do the following:

**Table 60. Add AIX nodes to the cluster**

<table>
<thead>
<tr>
<th>If using:</th>
<th>Do this:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command line</td>
<td>Issue the <code>updatenode</code> command, as follows:</td>
</tr>
<tr>
<td></td>
<td><code>updatenode -P</code></td>
</tr>
<tr>
<td></td>
<td>The <code>updatenode</code> command adds the <strong>PreManaged</strong> AIX nodes to the cluster. Note that the command does not update or install any software on the AIX node. For more information, see the man page or the <code>CSM for AIX and Linux: Command and Technical Reference</code>.</td>
</tr>
</tbody>
</table>
**SMIT**

Issue the `updatenode` command through SMIT. The fastpath is `csm_update`. For example:

```
smitt csm_update
```

**Note:**
When you run the `updatenode` command from SMIT, the command does not set up remote shell access to the nodes; set up access manually before running the `updatenode` command with SMIT.

**Web-based System Manager or DCEM**

1. Select the **Nodes** plug-in
2. From the **Nodes** menu, select **Update Nodes**. The **Update Nodes** dialog appears.
3. In the **Nodes to update** area, select **Update all premanaged nodes**.
4. In the **Updates to perform** area, select **Update CSM client code** and **Update configuration files**.
5. Click the OK button to install the nodes.

---

**Verify AIX nodes**

To verify that the AIX nodes have been added to your cluster, do the following:

**Table 61. Verify AIX nodes**

<table>
<thead>
<tr>
<th>If using:</th>
<th>Do this:</th>
</tr>
</thead>
</table>
| Command line    | Issue the `lsnode` command, specifying the name of the node. In this example, the name of the node is `clstrn01`.  
                  | `lsnode -n clstrn01 -a Mode,UpdatenodeFailed`                           |
| SMIT            | Issue the `lsnode` command through SMIT. The fastpath is `csm_lsnode`. For example:  
                  | `smitt csm_lsnode`                                                      |
| Web-based System Manager or DCEM | Use the **Nodes** plug-in to display node information, or use DCEM to run the `lsnode` command. DCEM can be started standalone, or launched from the **Nodes**, **Groups**, or **Commands** plug-in of Web-based System Manager. |

The output of the `lsnode` command should consist of the name of the node, followed by the values for these two attributes. For example:

```
clstrn01: Managed, 0
```

If the **Mode** is not **Managed**, or if the **UpdatenodeFailed** attribute is equal to 1, then the node has not been successfully added to the cluster. Do the following:

- Check the following log files for error and informational messages:
  - `/var/log/csm/updatenode.log` on the management server
  - `/var/log/csm/install.log` on each cluster node
- If the log indicates that the `mgmtsvr` command failed, do the following:

**Table 62. Using updatenode**
If using: | Do this:
---|---
Command line | Run the `updatenode` command with the `-k` flag and the name of the node. For example:
| `updatenode -k -n clstrn01`
SMIT | Run the `updatenode` command through SMIT. The fastpath is `csm_update`. For example:
| `smit csm_update`
Web-based System Manager or DCEM | Use the `Nodes` plug-in to update nodes, or use DCEM to run the `updatenode` command. DCEM can be started standalone, or launched from the `Nodes`, `Groups`, or `Commands` plug-in of Web-based System Manager.

- If you are running the `updatenode` command to a large number of nodes, you might be overloading the NFS server. If errors like `Bad UMNT RPC: RPC: Timed out` occur in the `updatenode.log`, try reducing the `updatenode` fanout. To do this, set the `CSM_FANOUT` environment variable to a low value, such as 16, then run the `updatenode` command again.
- Issue a remote command on the node:

| Table 63. Issuing a remote command on the node |
|---|---|
| **If using:** | **Do this:** |
| Command line | Issue the `dsh` command, specifying the name of the node. For example:
| `dsh -n clstrn01 -s date`
| SMIT | Not applicable.
| Web-based System Manager or DCEM | Use DCEM to run a test command such as the `date` command on a specified node. DCEM can be started standalone, or launched from the `Nodes`, `Groups`, or `Commands` plug-in of Web-based System Manager.

If the `dsh` command returns an error, see the CSM for AIX and Linux: Administration Guide for information on diagnosing `dsh` problems.

To verify that the Remote Management Console (RMC) is working:

| Table 64. Verify RMC for AIX |
|---|---|
| **If using:** | **Do this:** |
| Command line | Run the `lsnode` command with the `-H` flag, as follows:
| `lsnode -H`
| SMIT | Issue the `lsnode` command using SMIT. The fastpath is `csm_lsnodelog`. For example:
| `smit csm_lsnodelog`
| CSM Web-based System Manager | Use the `Nodes` plug-in to display node information, or use DCEM to run the `lsnode` command. DCEM can be started standalone, or launched from the `Nodes`, `Groups`, or `Commands` plug-in of the Web-based System Manager.

The `lsnode` command retrieves information about the attributes from each node.
Enable Kerberos Version 5 remote commands for AIX (optional)

To use Kerberos Version 5 for remote command authentication, see Enabling remote commands to use Kerberos Version 5 authentication.
Chapter 12. Adding Linux nodes

To add Linux nodes to your cluster, the nodes must already be installed with a supported level of the Linux operating system. To install Linux on your nodes, see Installing Linux on nodes.

Prerequisites for adding Linux nodes

Before continuing, ensure that you have completed the following steps:

- Set up an AIX or Linux management server; see Installing a CSM for AIX management server or Installing a CSM for Linux management server.
- Defined the Linux nodes to be added to your CSM cluster; see Defining nodes.
- Installed a supported version of Linux on your nodes. You can set up an install server to install Linux nodes; see Setting up a Linux install server.
- Verified that your Linux node software is supported; see Planning for CSM software.
- Considered upgrading your Linux nodes a new version of CSM for Linux; see Updating CSM for Linux.
- For node hardware control, set up hardware control points and console servers; see the CSM for AIX and Linux: Administration Guide.

Before you begin the procedures, be sure that you have completed the required planning in Planning for CSM software. Run the node installation commands from the management server; for command usage information, see the CSM for AIX and Linux: Command and Technical Reference or the man pages.

If you plan to use CSM Configuration File Manager (CFM) in a mixed cluster environment to synchronize files on the management server with the managed nodes, you must take additional steps and note the format and location of files on both AIX and Linux. For example, the format and content of /etc/passwd file are different on AIX and Linux. See the CSM for AIX and Linux: Administration Guide for more information on CFM.

If you plan to use CSM Configuration Manager (CFM) to distribute /etc/passwd to Linux nodes that are also install servers, be sure to include the tftp and dhcpd userids. When CSM sets up the install servers, these userids are created. If /etc/passwd doesn't contain these userids, and is later distributed to the install server node by CFM, the userids will get removed, which may cause subsequent installs to fail.

Once you have met the prerequisites, you can begin adding Linux nodes to your cluster.

Verify Linux node definitions

Before you add your Linux nodes, verify the node definitions and if necessary, update them. At this stage, you can make changes to any Linux node definitions.
To determine whether the nodes have been defined, issue the **lsnode** command from the management server:

```
lsnode
```

The system responds with a line for each node that was successfully defined. If a node has not been defined, it will not appear in the output for the **lsnode** command.

To display all the information about each node, enter the **lsnode -l** (lowercase L) command, from the management server:

```
lsnode -l
```

The system responds with a list (output) containing extended information for each node that was successfully defined. If a node has not been defined, it will not appear in the output for the **lsnode** command. Note that some of the attributes for a node might have null values at this point.

You can change node attributes by either running the **chnode** command, or by rerunning the **definenode** command with the -m (modify) flag. The **definenode -m** command accepts a new **nodedef** file or a new command line and only modifies the nodes that have changed attributes.

To change node attributes, use the **chnode** command from the management server:

```
chnode hostname attr=value
```

See the man pages or the **CSM for AIX and Linux: Command and Technical Reference** for more information about the **lsnode**, **chnode**, and **definenode** commands.

If you are using separate install servers other than the management server, you must ensure that install servers are installed and defined as CSM Managed nodes. If the nodes you are installing have **InstallServer** attributes set to something other than the management server values, or to no values (blank), make sure you have already run **updatenode** on each install server, and that the install server **Mode** attributes are set to **Managed**.

---

**Set up Linux cluster configuration (optional)**

You can use the CSM Configuration File Manager (CFM) support to automatically perform various configuration tasks when adding a node to the cluster. For example, you could distribute configuration files to the nodes, such as password files. For more information on the CFM support, see the **CSM for AIX and Linux: Administration Guide**.

CSM also provides a set of samples that you can use to help configure the cluster. Samples are provided for configuring NTP and Automounter. If you plan to use any of the CSM samples provided with this release, do the setup as documented in the appropriate README file in the following directory:

```
/opt/csm/samples/docs
```

You can modify the samples to handle different configuration or system requirements.
Set up RPM updates for Linux nodes (optional)

During node updates, CSM Software Maintenance System (SMS) automatically updates other RPMs on the nodes. To take advantage of this feature, you must copy the updated RPMs to the /csminstall directory. To speed up processing on the nodes, you can pre-populate the autoupdate database. For details on configuring SMS, see the CSM for AIX and Linux: Administration Guide.

Prepare Linux customization scripts (optional)

The updatenode command runs any user-provided customization scripts that have been placed in the /csminstall/csm/scripts/update directory. The command checks this directory and runs each script on the node when it is being updated. Subdirectories are not checked. If multiple scripts exist in a directory, they are run in alphabetical order, as determined by the ls command on the management server. The naming convention for the scripts is as follows:

```
scriptname[._target]
```

The _ following the script name is required if the script is to be used only for a specific node or node group. The target value must be a single node name or group name that has been defined in the CSM database. If the target extension is not used, then the script runs on all nodes. If a script exists and additional multiple versions for subsets of nodes (for example, myscript, myscript._groupA, myscript._groupB) also exist, the script with no target extension runs only for those nodes that are not included in one of the specific groups (for example, not in groupA or groupB). For more information on CSM support for user-provided customization scripts, see the CSM for AIX and Linux: Administration Guide.

Provide Kerberos client packages for Linux (optional)

Follow this step if you plan to use Kerberos Version 5 for remote commands. You can use the software maintenance System (SMS) to install the Kerberos client packages when you run the updatenode command. For a list of the required packages, see CSM for AIX Kerberos setup. Place the packages in the following directory:

```
/csminstall/Linux/InstallDistributionName/InstallDistributionVersion/InstallPkgArchitecture/install
```

To use Kerberos with ssh, the Kerberos enabled ssh packages must also be installed on the node. You cannot use SMS to update ssh unless you provide updates to the ssh that is installed with your Linux distribution. If the packages have different names, conflicts can result. In this case, do the following:

1. Uninstall the ssh packages for your distribution.
2. Install the new packages and update the various configuration files.
3. Stop and then restart sshd.
Prepare Linux secondary adapter configuration (optional)

Secondary adapters may be configured during the node installation process or when adding a node to the cluster. To use this support there are some additional steps that must be completed. Refer to Secondary adapter interface configuration for a description of how to use this CSM feature.

Copy CSM for Linux packages

If any values for the following node attributes do not match the management server attribute values, you must use the copycsmpkgs tool to copy the CSM packages to /csminstall:

- InstallDistributionName
- InstallDistributionVersion
- InstallPkgArchitecture
- InstallCSMVersion
- InstallServiceLevel

Consider the following scenarios for running copycsmpkgs:

- The management server is running AIX and a node is running Linux; different InstallOSName values.
- The management server is running a Red Hat EL-AS or Red Hat EL-ES, and a node is running Red Hat EL-WS; different InstallDistributionName values.
- The management server is running a different level of the operating system from that on the nodes. For example, the management server is running SLES 10 and a node is running SLES 9; different InstallDistributionVersion values.
- The management server is an xSeries server (x86 architecture) and the node is a BladeCenter JS server (POWER architecture); different InstallPkgArchitecture values.
- The management server is running a different service level than a node; different InstallServiceLevel values.

In any of the cases above, or any time any of the attributes listed above are different between the management server and a node, run copycsmpkgs as follows, where node is a single node name for which the packages are copied, and path is the path name that contains the CSM RPMs. The command prompts for any required Linux distribution CDs.

    copycsmpkgs -p path -n node

If you have multiple nodes that all have the same installation attributes, run copycsmpkgs for only one of the representative nodes.

Install CSM on Linux nodes

Before you run the updatenode command, ensure that your management server and any install servers are configured, and that the definenode command has been run successfully on the management server.
The `updatenode` command installs and updates the CSM software and files on the cluster nodes, including CSM managed node packages, RSCT packages and other CSM managed node prerequisite packages. The nodes on which you run the `updatenode` command must already have the operating system installed.

The `updatenode` command does the following for a Linux node:

- Installs the CSM software and configures the node so that the management server can manage it; changes the node `Mode` attribute from `PreManaged` to `Managed`.
- If remote shell authentication is not already set up, automatically sets up remote shell authentication for OpenSSH or `rsh`. See Remote shell attributes for Linux.
- Distributes the CFM configuration files if CFM is set up.
- Distributes the SMS RPMs if SMS is set up.
- Runs any user customization scripts. See Prepare Linux customization scripts (optional).
- Sets up the Kerberos options for remote commands if specified on the `csmconfig` command. For information, see Set up Kerberos Version 5 for remote Linux command processing (optional).

If the `Mode` attribute for a node is set to `MinManaged`, the `updatenode` does not install CSM on the node; however, the command does set up the remote shell, runs CFM, SMS and runs customization scripts for the `MinManaged` node.

**Note:** When you use the `updatenode` command, NFS error messages might occur. You can ignore these error messages; see NFS warnings.

### Updating Linux node attributes

**PreManaged and Managed nodes:** When a node has only been defined, but has not been installed with CSM, its `Mode` attribute value is `PreManaged`. After the `updatenode` command installs CSM on the node, its `Mode` attribute value changes to `Managed`. If the `updatenode` command is not successful, the node's `Mode` attribute remains `PreManaged` and the `UpdatenodeFailed` attribute is set to `1` (true) for the node.

**MinManaged nodes:** If the `Mode` attribute is `MinManaged`, `updatenode` does not alter the value. The value remains `MinManaged` after you run the `updatenode` command, and CSM sets the `UpdatenodeFailed` attribute to `1` (true) for the node. Minimally-managed nodes have no CSM or RSCT code installed.

### Remote shell attributes for Linux

For authentication, the `updatenode` command prompts you for the root password for the target nodes. As a result, you must either make the root password common to all the target nodes, or run the `updatenode` command to each node, or group of nodes, and provide the related passwords.

When you set up the management server, you already specified the `RemoteShell` and `SetupRemoteShell` attributes using the `csmconfig` command; see Choosing a Linux remote shell. The `updatenode` command behaves differently, depending on the values you specified with the `RemoteShell` and `SetupRemoteShell` attributes of the `csmconfig` command and the values you specify for `csmconfig` with the `SetupKRB5` Kerberos option:

- If you specified `RemoteShell=/usr/bin/ssh` and `SetupRemoteShell=1` (yes), and OpenSSH is installed on the management server and all of the nodes, the `updatenode` command sets up secure...
shell access to all PreManaged nodes. This is also true for all cluster nodes if you used the updatenode -k command, which prompts you for the root password.

- If you specified RemoteShell=/usr/bin/ssh and SetupRemoteShell=1 (yes) and OpenSSH is not already set up, the updatenode command automatically sets up the remote shell authentication for OpenSSH and prompts you for the root password for the target nodes.
- If you specified SetupRemoteShell=0 (no), the updatenode command does not set up remote access for any of the nodes.
- If you specified RemoteShell=/usr/bin/rsh, you need to set up rsh manually on each node. If the root is able to issue rexec commands to the nodes, you can use updatenode to set up rsh.
- If csmconfig SetupKRB5 indicates to set up Kerberos client, CSM sets up the nodes as Kerberos clients.
- If csmconfig SetupKRB5 indicates to set up Kerberos principals, when you run updatenode -k, or when you run updatenode with defaults to a PreManaged node, CSM adds the CSM principal to the .k5login file in the home directory of root on each node and transfers the host key of the node to the node. To only transfer the keytab for the host node from the management server to the managed node, you can run updatenode -K krb5 nodename, where nodename is the name of the node.

## Installing CSM on Linux nodes

The updatenode command installs CSM packages, distributes configuration files to the nodes, and updates other software that is installed on the nodes. For more information, see the man page or the CSM for AIX and Linux: Command and Technical Reference.

To install all PreManaged nodes, which changes them to Managed nodes, run the updatenode command as follows:

```
updatenode -P
```

## Reboot CSM for Linux nodes

If your node hardware does not support remote console—for example, BladeCenter HS20-8678 nodes without Serial Port Module (SPM) installed—or if you are not using remote console, this step is not required.

If you are using remote console, this step is required.

To enable the remote console for the node, you must reboot the nodes after installing CSM. You can perform this step now, or you can do it later, when you want to use the remote console.

To reboot System x, IntelliStation(R), BladeCenter, or eServer nodes, run the rpower command for the specified nodes. For example:

```
rpower -n nodename reboot
```

If you just installed HMC-attached System p nodes, you cannot reboot them. Instead, use the rpower command as follows to power off and on the HMCs for the specified nodes:

```
rpower -n nodename off
rpower -n nodename on
```
Verify the CSM for Linux installation

To verify CSM for Linux installation, run the `lsnode` command with the node hostnames. In this example, the name of the node is `clsn01`.

```bash
lsnode -n clsn01 -a Mode,UpdatenodeFailed
```

The `lsnode` command output displays the node name and the attribute values. For example:

```
clsn01: Managed, 0
```

If the `Mode` is not **Managed** or **MinManaged**, or if the `UpdatenodeFailed` attribute is equal to 1, then the node was not successfully updated; do the following in response:

- Check the log files for error and informational messages. Check `/var/log/csm/updatenode.log` on the management server and `/var/log/csm/install.log` on the cluster node.
- If the log indicates that the `mgmtsvr` command failed, issue the `updatenode` command, specifying the `-k` flag and the name of the node. For example:
  ```bash
  updatenode -k -n clsn01
  ```
- If you are running the `updatenode` command on a large number of nodes, you can overload the NFS server. If errors similar to `Bad UMNT RPC: RPC: Timed out` are written to the `updatenode.log`, reduce the `updatenode` fanout; set the `CSM_FANOUT` environment variable to a low value, such as 16, and run the `updatenode` command again.
- Issue a remote command on the node. For example, issue the `dsh` command, specifying the name of the node:
  ```bash
  dsh -n clsn01 -s date
  ```
  If the `dsh` command returns an error, see the *CSM for AIX and Linux: Administration Guide* for information on diagnosing `dsh` problems.

---

Enable Kerberos Version 5 remote commands for Linux (optional)

To use Kerberos Version 5 for remote command authentication, see [Enabling remote commands to use Kerberos Version 5 authentication](#).
Chapter 13. Installing AIX on nodes

You must install one of the following AIX versions on your CSM for AIX nodes:

- AIX for POWER Version 5.3 (5300-07 or later)
- AIX for POWER Version 6.1

When installing the AIX operating system, you can automatically add the installed nodes to a CSM cluster. You can also set up an install server to install AIX nodes; see Setting up install servers.

Using AIX Network Installation Manager (NIM) and CSM: Use AIX Network Installation Manager (NIM), CSM, and hardware commands to install AIX on your cluster nodes. NIM enables centralized management of AIX installation and configuration, and optional software on servers within a network environment. You can install and configure NIM on an AIX management server, or on one or more AIX install servers. If using a Linux management server, you must configure at least one AIX install server to use as your NIM master.

CSM for AIX installation commands automatically perform tasks on the management server, or on an install server. The required NIM commands must be run on the NIM master. The examples assume that the NIM master is on the management server. If the NIM master is on an install server, NIM commands can be run from the management server using `dsh`. For example, to run the `lsnim` command on the management server, enter:

```
lsnim
```

To run the same command on an install server named `isserver01` enter:

```
dsh -n isserver01 lsnim
```

This procedure does not describe all of the NIM commands or functions that are available. Depending on your CSM cluster configuration, you might need to perform other steps that are not described. For example, if your nodes are connected to different subnets, or to use a `mksysb` image to install the nodes, you must perform additional steps. For a scenario on using `mksysb`, see Using mksysb for AIX nodes.

Using NIM and Kerberos: NIM requires standard authentication to be enabled when you perform the installation. If you are setting up Kerberos for remote commands, follow Add Kerberos client software for AIX. After installation is complete, change to Kerberos authentication as part of the process to enable Kerberos remote command processing. For information, see Enabling remote commands to use Kerberos Version 5 authentication.

For a complete description of NIM commands and functions, see the IBM AIX Installation Guide and Reference for your version of AIX.

Before you can begin the installation steps, ensure that you have completed the following steps:

- You have set up the management server; see Installing a CSM for AIX management server.
- You have defined the nodes to be added to the cluster; see Defining nodes.
Verify CSM for AIX node definitions

Before you add the nodes, verify the node definitions and if necessary, update them. At this stage, you can make changes to any of the definitions.

To determine whether the nodes have been defined:

Table 65. Verify the nodes have been defined.

<table>
<thead>
<tr>
<th>If using:</th>
<th>Do this:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command line</td>
<td>Issue the <code>lsnode</code> command from the management server, as follows: <code>lsnode</code></td>
</tr>
<tr>
<td>SMIT</td>
<td>Issue the <code>lsnode</code> command through SMIT. The fastpath is <code>csm_lsnod</code>. For example: <code>smit csm_lsnod</code></td>
</tr>
<tr>
<td>Web-based System Manager or DCEM</td>
<td>Use the <code>Nodes</code> plug-in to display node information, or use DCEM to run the <code>lsnode</code> command. DCEM can be started standalone, or launched from the <code>Nodes</code>, <code>Groups</code>, or <code>Commands</code> plug-in of Web-based System Manager.</td>
</tr>
</tbody>
</table>

The system responds with one line for each node that has been correctly defined. If a node has not been defined, it will not appear in the output for the `lsnode` command.

To display information about each node:

Table 66. Verifying node information

<table>
<thead>
<tr>
<th>If using:</th>
<th>Do this:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command line</td>
<td>Issue the <code>lsnode</code> command, from the management server, with the <code>-l</code> (lowercase L, not uppercase i) option: <code>lsnode -l</code></td>
</tr>
<tr>
<td>SMIT</td>
<td>Issue the <code>lsnode</code> command through SMIT. The fastpath is <code>csm_lsnod</code>. For example: <code>smit csm_lsnod</code></td>
</tr>
<tr>
<td>Web-based System Manager or DCEM</td>
<td>Use the <code>Nodes</code> plug-in to display node information, or use DCEM to run the <code>lsnode</code> command. DCEM can be started standalone, or launched from the Web-based System Manager <code>Nodes</code>, <code>Groups</code>, or <code>Commands</code> plug-in.</td>
</tr>
</tbody>
</table>
The system responds with output that contains extended information for each node. If a node has not been defined, it does not appear in the `lsnode` command output. Note that some of the attributes for a node might have null values at this point.

If you need to make corrections, either remove the node that was not correctly defined, make the corrections, and run the `definenode` command, or use the `chnode` command to make the necessary changes to the attributes of the node.

**To remove a node before redefining it:**

<table>
<thead>
<tr>
<th>Table 67. Removing a node</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>If using:</strong></td>
</tr>
</tbody>
</table>
| Command line              | Issue the `rmnode` command on the management server:  
                          | `rmnode hostname` |
| SMIT                      | Issue the `rmnode` command through SMIT. The fastpath is `csm_rmnode`. For example:  
                          | `smit csm_rmnode` |
| Web-based System Manager or DCEM | Use the `Nodes` plug-in to remove a node, or use DCEM to run the `rmnode` command.  
                          | DCEM can be started standalone, or launched from the `Nodes, Groups, or Commands` plug-in of Web-based System Manager. |

**To change the attributes of a node:**

<table>
<thead>
<tr>
<th>Table 68. Changing node attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>If using:</strong></td>
</tr>
</tbody>
</table>
| Command line                      | Issue the `chnode` command from the management server:  
                          | `chnode hostname attr=value` |
| SMIT                              | Issue the `chnode` command through SMIT. The fastpath is `csm_chnode`. For example:  
                          | `smit csm_chnode` |
| Web-based System Manager or DCEM  | Use the `Nodes` plug-in to change attributes of a node, or use DCEM to run the `chnode` command.  
                          | DCEM can be started standalone, or launched from the `Nodes, Groups, or Commands` plug-in of Web-based System Manager. |

See the man pages or the *CSM for AIX and Linux: Command and Technical Reference* for more information about the `lsnode`, `rmnode`, and `chnode` commands.

---

**Create CSM for AIX node groups (optional)**

Creating CSM node groups simplifies the remainder of the installation process. To create a node group:

<table>
<thead>
<tr>
<th>Table 69. Create CSM node groups</th>
</tr>
</thead>
</table>

CSM for AIX and Linux: Planning and Installation Guide
If using:  Do this:

Command line  Issue the CSM nodegrp command. For example:
nodegrp -a clusternode1,clusternode2 cluster_grp

When you use the nodegrp command, you supply the node names followed by the name you want to designate for that group. In the example, clusternode1,clusternode2 are the nodes and cluster_grp is the name of the group that includes those nodes.

SMIT  Issue the nodegrp command through SMIT. The fastpath is csm_mknodegrp. For example:
smit csm_mknodegrp

Web-based System Manager or DCEM  Use the Groups plug-in to create a node group. DCEM can be started standalone, or launched from the Nodes, Groups, or Commands plug-in of Web-based System Manager.

See the man page or the CSM for AIX and Linux: Command and Technical Reference for more information about the nodegrp command.

---

**Validate CSM for AIX remote power**

Before installing CSM on your AIX nodes, validate remote power configuration, as follows:

**Table 70. Validate remote power control**

<table>
<thead>
<tr>
<th>If using:</th>
<th>Do this:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command line</td>
<td>Issue the rpower command, as follows: rpower -a query</td>
</tr>
<tr>
<td>SMIT</td>
<td>Issue the rpower command through SMIT. The fastpath is csminst_rp. For example: smit csminst_rp</td>
</tr>
<tr>
<td>Web-based System Manager or DCEM</td>
<td>Use DCEM to run the rpower command. DCEM can be started standalone, or launched from the Nodes, Groups, or Commands plug-in of Web-based System Manager.</td>
</tr>
</tbody>
</table>

The following is sample output from the rpower command:

root@c5n71:/u/build # rpower -a query
c5n72.ppd.pok.ibm.com on
c5n73.ppd.pok.ibm.com on
c5n74.ppd.pok.ibm.com off

c5n75.ppd.pok.ibm.com off

If any of the nodes do not return either on or off, see the CSM for AIX and Linux: Administration Guide for information on diagnosing rpower problems.

---

CSM for AIX and Linux: Planning and Installation Guide
Collect AIX network adapter information

To install a cluster node on a network, you must collect information about the Ethernet adapter that installs and manages the node, and store that information in the CSM database. Each node must have at least one network adapter that can reach the management server for this purpose. You store the information for this adapter in the CSM database as node installation adapter attributes.

AIX Virtual IP Addresses (VIPA) cannot be used for CSM network communications. VIPA interfaces can be set up on cluster nodes for purposes other than cluster management.

You can collect the adapter information manually, or by using the `getadapters` command. The `getadapters` command can collect information about all adapters assigned to a node, or for adapters that satisfy certain criteria. There is no restriction on the number of HMC-based nodes that you can run the command on simultaneously; however, problems can occur when running the command on many nodes simultaneously. In these cases, you can issue the command with the `-l` flag to limit the execution of the command to one node at a time per HMC. This increases the time required to complete the command, but reduces the load on the HMC and management server. The `CSM_LIMIT_OFW_SESSIONS` environment variable can also be set to enable this same limit. The value of the variable is not significant; only whether it is defined or not. In a `ksh` environment, you can use the following command to set the variable:

```
export CSM_LIMIT_OFW_SESSIONS=1
```

In a `ksh` environment, use the following command to clear the variable:

```
unset CSM_LIMIT_OFW_SESSIONS
```

The command can automatically choose an adapter and add the information to the database, or a specific adapter can be chosen manually. See the `getadapters` man page or the *IBM CSM for AIX: Command and Technical Reference*.

Using `getadapters` to choose an installation adapter for a node: The following examples illustrate using the `getadapters` command to automatically select an appropriate install adapter, and how that information is added to the CSM database.

1. Run the `getadapters -D` command to choose an install adapter. Specify that the information is to be written to an adapter stanza file.

   The examples in this step pertain only to HMC-attached System p nodes.

   **Table 71. Using getadapters**

<table>
<thead>
<tr>
<th>If using:</th>
<th>Do this:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command line</td>
<td>Issue the <code>getadapters</code> command. For example: <code>getadapters -a -D -t ent -s 100 -d full -z mystanzafile</code></td>
</tr>
<tr>
<td></td>
<td>In this example, the command requests information for all nodes. It specifies that the adapter is to be Ethernet (<code>ent</code>), the speed is to be 100, and the duplex value is to be <code>full</code>. This version of the <code>getadapters</code> command checks each Ethernet adapter on the node until it finds the first adapter that can be used to ping the management server. This adapter information is returned for each node, and is written to an</td>
</tr>
</tbody>
</table>
adapter stanza file called mystanzafile.

### SMIT

Run the `getadapters` command through SMIT. The fastpath is `csm_getadapters` or `csm_getadap`. For example:
```
smit csm_getadapters
```

### Web-based System Manager or DCEM

Not applicable.

2. Verify that the `getadapters` command returns the information you expect and make any changes by editing the stanza file.

The stanza file must have only one stanza marked as the installation adapter for each node. If the `getadapters` command does not automatically choose the right adapter, edit the stanza file to specify the desired adapter. For more information on the use of the stanza file and the its required format, see the `getadapters` man page and the *CSM for AIX and Linux: Administration Guide*.

**Note:**
During the installation process this adapter is configured with the *Hostname* or IP address used to define the node in CSM. This is the interface that CSM uses for all cluster system management communications.

3. Save the node installation adapter information in the CSM database.

You can use the `getadapters` command with the `-w` flag to write information into the CSM database. The following example of the command uses the flag with the adapter stanza file `myadapters` that you created in the previous example.

**Table 72. Using getadapters to write information to the CSM database**

<table>
<thead>
<tr>
<th>If using:</th>
<th>Do this:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command line</td>
<td>Issue the <code>getadapters</code> command. For example: <code>getadapters -w -f mystanzafile</code></td>
</tr>
</tbody>
</table>
| SMIT                          | Run the `getadapters` command through SMIT. The fastpath is `csm_getadapters` or `csm_getadap`. For example:  
  `smit csm_getadapters`      |
| Web-based System Manager or DCEM | Not applicable.                                                           |

If you experience a problem while using `getadapters`, consult the following error log:

```
/var/log/csm/getadapters
```

This directory contains a single log file per node.

For setting up NIM resources and using NIM, see [Set up Network Installation Manager (NIM) for AIX](Set up Network Installation Manager (NIM) for AIX).
Methods for collecting AIX MAC addresses

The **getadapters** command provides two additional methods for collecting node MAC addresses: **arp** and **snmp**. Both methods collect adapter information for AIX and Linux nodes, regardless of the hardware type.

Use the **arp** method when the nodes are reachable, and on the same subnet as the management server or install server. The **arp** method for **getadapters** collects Ethernet adapter information.

Use the **snmp** method under the following conditions:

- The switch inside the cluster is SNMP enabled. This is the default setting.
- Only one MAC address is associated with one combination of module, port, and VLAN. This is true for cluster 1350. The **snmp** method fails if another switch is attached to the 1350 switch, with multiple nodes attached to the second switch.
- Know which switch, module, port, and VLAN each node connects to; this information is supplied by the manufacturer.

To use **arp** run:

```
getadapters -m arp -n node_name
```

To use **snmp** run:

```
getadapters -m snmp -i switch_info_filename -n node_name
```

Using the **-m** flag, the **getadapters** command attempts to get the MAC address from the `InstallAdapterHostname` attribute value. If this attribute value is null, the **getadapters** command attempts to get the MAC address from the interface host name. If the **-w** flag is used, **getadapters** sets `InstallAdapterMacaddr` to the MAC address, but does not update `InstallAdapterName`.

**Note:**

If you defined `InstallAdapterName`, it is not changed by **getadapters** **-w**. If the `InstallAdapterName` attribute value is null, CSM assumes **eth0** for the attribute value.

Only one MAC address for each node will be returned; the **arp** and **snmp** methods will not distinguish which MAC address belongs to `InstallAdapterName`. You must verify that the attribute value for `InstallAdapterMacaddr` matches the attribute value for `InstallAdapterName`.

See the **getadapters** man page for command details.

---

Set up Network Installation Manager (NIM) for AIX

NIM enables a cluster administrator to centrally manage the installation and configuration of AIX and optional software on machines within a network environment. Setting up NIM includes the following tasks:

- Installing NIM file sets
- Configuring basic resources
Creating machine and network definitions
Creating resources that are used to install the nodes.

The specific tasks depend on which features of NIM that you plan to use. For more information about NIM, see the *IBM AIX Installation Guide and Reference* for your version of AIX.

To simplify the NIM setup process, you can use the `nim_master_setup` command. This command automatically performs basic NIM tasks. It installs NIM file sets, configures NIM, creates basic resources and creates a resource group with the resources that are created. You must use AIX CD #1.

**Note:**
This command must be run on the server that will be the NIM master. If you are using an install server, use the `dsh` command to run it on that server.

If you are using CSM High Availability Management Server (HA MS), see the HA MS information in the *CSM for AIX and Linux: Administration Guide* for NIM setup considerations. This is valid only when the NIM master is the management server.

The command supports several options and indicates which resources have been created when it completes. If the default resources created by this script are not adequate, you can use individual NIM commands. For a preview of the commands, issue `nim_master_setup` with the `-h` flag:

```
nim_master_setup -h
```

The resources created by this command are stored in the `/export/nim` directory by default. The file system is automatically created with the correct size for storing the required resources. You can specify an alternate file system name. The command creates a new file system with the name that you provide.

**Note:**
This command automatically creates a `mksysb` (system backup image) resource on the management server. Do not use this `mksysb` image to install the cluster nodes. Instead, use the `-B` flag on the command to indicate that a `mksysb` image is not to be created. If you need a `mksysb` image, create it on a node that has been installed and configured as desired. See *Using mksysb for AIX nodes*.

To use the `nim_master_setup` command to set up NIM, do the following:

**Table 73. Setting up NIM**

<table>
<thead>
<tr>
<th>If using:</th>
<th>Do this:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command line</td>
<td>Issue the <code>installp</code> command. For example:</td>
</tr>
<tr>
<td></td>
<td><code>nim_master_setup -B</code></td>
</tr>
<tr>
<td></td>
<td><code>-B</code> indicates that the command is not to create a <code>mksysb</code> resource. This command creates a default resource group that you can use later with the <code>nim -o bos_inst</code> command in Add CSM for AIX nodes to the cluster.</td>
</tr>
<tr>
<td>SMIT</td>
<td>Not available.</td>
</tr>
<tr>
<td>Web-based System Manager</td>
<td>Not applicable.</td>
</tr>
</tbody>
</table>

CSM for AIX and Linux: Planning and Installation Guide 181
To make sure that NIM is correctly set up, issue the `lsnim` command on the NIM master as follows:

```
lsnim
```

If NIM is correctly set up, the `lsnim` command displays information about the NIM environment. The following sample output varies depending on your cluster setup:

```
master           machines   master
boot             resources  boot
nim_script       resources  nim_script
master_net       networks   ent
master_net_conf  resources  resolv_conf
bid_ow           resources  bosinst_data
530lpp_res       resources  lpp_source
530spot_res      resources  spot
basic_res_grp    groups     res_group
```

For more information about using the `nim_master_setup` and `lsnim` commands, see the *IBM AIX Installation Guide and Reference* for your version of AIX.

As described in the NIM documentation, you must define the following resources:

- `spot`
- `lpp_source`
- `bosinst_data`
- `resolv_conf`

You can use the `bosinst_data` sample file that is included with AIX 5.3 and 6.1; ensure that the `CONSOLE` attribute in the file is set to `/dev/tty0`.

Note:

For JS22, JS23 and JS43 nodes, you have to set the `CONSOLE` attribute to `/dev/vty0` in the `bosinst_data` resource script.

---

**Tuning NIM for large AIX installations**

If you are installing a large number of AIX nodes, you can make additional NIM settings to improve NIM scalability and performance:

1. Enable the multithread option on the NIM `nimesis` daemon using the `max_nimesis_threads` value. Setting the value improves NIM performance when working with a large number of nodes. Specify a value from 20 to 150. Set the value to approximately half the number of nodes you are using simultaneously. For example, to install 100 nodes, set the value to 50.

   Issue the following command on the NIM master to set the value:

   ```
   nim -o change -a max_nimesis_threads=50 master
   ```

2. Set the `global_export` attribute to `yes` on the management server (NIM master). Always set the attribute when you are simultaneously running NIM operations to many nodes.
Issue the following command on the NIM master to set the value:

```
nim -o change -a global_export=yes master
```

If you have a large number of nodes defined, make sure the `arptab` values are increased from their default values to at least the minimum values listed below. Use the AIX `no -a` command to check them, and use `no -o` command to change them. See the `no` man page for more information.

```
arptab_nb=149
arptab_bsiz=73
```

See the *IBM AIX Installation Guide and Reference* for details.

### Create additional AIX NIM network definitions and routes

NIM network definitions represent the networks used in the NIM environment. During the procedure *Set up Network Installation Manager (NIM) for AIX*, the network associated with the NIM master is automatically defined. The NIM master is the same as the management server in the CSM cluster.

Defining additional networks is only required if nodes reside on other local area networks or subnets. If the physical network is changed in any way, you must modify the NIM network definitions, as follows:

**Table 74. Creating network definitions for an Ethernet subnet**

<table>
<thead>
<tr>
<th>If using:</th>
<th>Do this:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command line</td>
<td>Issue the <strong>nim</strong> command on the NIM master. For example:</td>
</tr>
<tr>
<td></td>
<td>`nim -o define -t ent -a snm=255.255.255.0 -a net_addr=129.35.101.0 \</td>
</tr>
<tr>
<td></td>
<td>sbnet2</td>
</tr>
<tr>
<td>SMIT</td>
<td>Issue the <strong>nim</strong> command through SMIT. The fastpath is <strong>nim_mknet</strong>.</td>
</tr>
<tr>
<td></td>
<td><code>smit nim_mknet</code></td>
</tr>
<tr>
<td>Web-based System Manager or</td>
<td>Not applicable.</td>
</tr>
<tr>
<td>DCEM</td>
<td></td>
</tr>
</tbody>
</table>

NIM uses route definitions to ensure that a client on one network can communicate with a server on another network. It defines the gateway to use to go from one network to the other. You must provide routing information for each additional network that has been defined.

**Note:**

See the *IBM AIX Installation Guide and Reference* for information on automatically creating additional network and route definitions when a client machine is defined.

In a CSM environment, create a route for the NIM masters primary network interface (`master_net`) that is created when you complete *Set up Network Installation Manager (NIM) for AIX*.

To create a route for `master_net`, you must know the default gateway; do the following on the NIM master to retrieve the default gateway:
### Table 75. To retrieve the default gateway

<table>
<thead>
<tr>
<th>If using:</th>
<th>Do this:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command line</td>
<td>Issue the <strong>netstat</strong> command, as follows:</td>
</tr>
<tr>
<td></td>
<td><code>netstat -rn</code></td>
</tr>
<tr>
<td>SMIT</td>
<td>Issue the <strong>netstat</strong> command through SMIT. The fastpath is <strong>netstat</strong>. For example:</td>
</tr>
<tr>
<td></td>
<td><code>smit netstat</code></td>
</tr>
<tr>
<td>Web-based System Manager or DCEM</td>
<td>Not applicable.</td>
</tr>
</tbody>
</table>

Output is similar to:

```bash
netstat -nr
Routing tables
Destination Gateway Flags Refs Use If PMTU Exp Groups

Route Tree for Protocol Family 2 (Internet):
    default          9.114.67.62       UGc       0        0  en0     -   -
    9.56.216.89      9.114.67.62       UGHW      1     4577  en0     -   -
    9.114.67/26      9.114.67.3        U         4  5157696  en0     -   -
    9.114.67.3       127.0.0.1         UGHS     30   540947  lo0     -   -
    9.117.6.195      9.114.67.62       UGHW      2     5053  en0  1500   -
    9.117.14.183     9.114.67.62       UGHW      2      414  en0  1500   -
    127/8            127.0.0.1         U         8    13031  lo0     -   -
    192.168.67/27    192.168.67.1      U         0      108  en2     -   -
    192.168.67.1     127.0.0.1         UGHS      0     433  lo0     -   -

Route Tree for Protocol Family 24 (Internet v6):
    ::1              ::1               UH        0        0  lo0 16896   -
```

In the example, the default gateway IP address is 9.114.67.62.

To create the route, do the following on the NIM master:

### Table 76. Using the nim command

<table>
<thead>
<tr>
<th>If using:</th>
<th>Do this:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command line</td>
<td>Issue the <strong>nim</strong> command. The following example assumes that the <strong>routing</strong> with a sequence number of <code>l</code> had not been used.</td>
</tr>
<tr>
<td></td>
<td><code>nim -o change -a routing1=&quot;default default_gateway_address&quot; master_net</code></td>
</tr>
<tr>
<td>SMIT</td>
<td>Issue the <strong>nim</strong> command through SMIT. The fastpath is <strong>nim_mkdroute</strong>. For example:</td>
</tr>
<tr>
<td></td>
<td><code>smit nim_mkdroute</code></td>
</tr>
<tr>
<td>Web-based System Manager or DCEM</td>
<td>Not applicable.</td>
</tr>
</tbody>
</table>
Create AIX NIM machine definitions

You must define CSM nodes that you are installing using NIM as NIM client machines. Because you have already defined the nodes in CSM, you must use the CSM `csm2nimnodes` command. This command takes the information stored in CSM with information provided on the command line and creates corresponding NIM client definitions.

Whether using a NIM command or a CSM command, a node has the same name. NIM commands use the client (node) definition in the NIM database and the CSM commands use the node definitions in the CSM database. If a definition is added, removed, or modified in one database, the other database is not updated automatically.

Internally, the `csm2nimnodes` command calls the appropriate NIM command. It automatically runs the appropriate NIM commands on the install server if one is being used as the NIM master.

To define a NIM client machine that corresponds to the CSM cluster node `clstrn14`, do the following. In the example, some defaults are shown.

Table 77. Defining a NIM client machine

<table>
<thead>
<tr>
<th>If using:</th>
<th>Do this:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command line</td>
<td>Issue the <code>csm2nimnodes</code> command as follows:</td>
</tr>
<tr>
<td></td>
<td><code>csm2nimnodes -n clstrn14 type=standalone platform=chrp netboot_kernel=mp network_name=master_net cable_type=&quot;N/A&quot;</code></td>
</tr>
<tr>
<td>SMIT</td>
<td>Issue the <code>nim</code> command through SMIT. The fastpath is <code>csm_nimnodes</code>. For example:</td>
</tr>
<tr>
<td></td>
<td><code>smit csm_nimnodes</code></td>
</tr>
<tr>
<td>Web-based</td>
<td>Not applicable.</td>
</tr>
<tr>
<td>System</td>
<td></td>
</tr>
<tr>
<td>Manager or</td>
<td></td>
</tr>
<tr>
<td>DCEM</td>
<td></td>
</tr>
</tbody>
</table>

The `csm2nimnodes` command provides default values, so only some arguments are required when defining many NIM clients. For example, if you use the node group `AIXNodes`, which includes all AIX nodes with the same attributes, you can create all NIM client definitions as follows:

```
csm2nimnodes -N AIXNodes
```

For more information on using the `csm2nimnodes` command, see the man page or the `CSM for AIX and Linux: Command and Technical Reference`.

Create AIX NIM machine groups (optional)

You can create NIM machine groups to represent collections of client machines. You can then use the machine group names with NIM commands to specify a set of machines to act on. For example, using machine groups is convenient if you have a set of machines that all used the same set of resources.
In a CSM cluster environment, it is also useful to create NIM machine groups that correspond to CSM node groups.

The `csm2nimgrps` command automatically runs the appropriate NIM commands on the install server if one is being used as the NIM master. For example, to create a NIM machine group that corresponds to the `AIXNodes` predefined CSM node group, do the following:

**Table 78. Creating a NIM machine group**

<table>
<thead>
<tr>
<th>If using:</th>
<th>Do this:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command line</td>
<td>Issue the <code>csm2nimgrps</code> command, as follows:</td>
</tr>
<tr>
<td></td>
<td><code>csm2nimgrps -N AIXNodes</code></td>
</tr>
<tr>
<td>SMIT</td>
<td>Issue the <code>csm2nimgrps</code> command through SMIT. The fastpath is <code>csm_nimgrps</code>. For example:</td>
</tr>
<tr>
<td></td>
<td><code>smit csm_nimgrps</code></td>
</tr>
<tr>
<td>Web-based System Manager or DCEM</td>
<td>Not applicable.</td>
</tr>
</tbody>
</table>

The `csm2nimgrps` command takes a snapshot of the members of the CSM group and calls the NIM command to create the machine group. There are no automatic updates after this command has run. For example, if the group member list changes in CSM, that change is not automatically reflected in the NIM definition. In this case, you should run the `csm2nimgrps` command again to update the NIM group.

The NIM machine group definitions that you create have the same names as the corresponding CSM cluster node definitions.

---

**Prepare AIX customization scripts (optional)**

Prepare any user-defined customization scripts. These scripts are used in [Add CSM for AIX nodes to the cluster](#) when you add the AIX nodes to the cluster.

For information on CSM support for user-provided customization scripts, see the [CSM for AIX and Linux: Administration Guide](#).

---

**Prepare for AIX secondary adapter configuration (optional)**

Secondary adapters can be configured during node installation, or when adding a node to the cluster. To use this support there are some additional steps that must be completed. Refer to [Secondary adapter interface configuration](#) for a description of how to use this CSM feature.
Set up AIX cluster configuration (optional)

You can use the CSM Configuration File Manager (CFM) support to automatically perform various configuration tasks when installing a node. For example, you could distribute configuration files to the nodes, such as password files. For more information on the CFM support, see *CSM for AIX and Linux: Administration Guide*.

Verify AIX authentication methods for NIM (optional)

Skip this step if your management server is not configured to use Kerberos for remote command authentication.

NIM uses standard AIX authentication for remote commands during an installation. The management server must be enabled to use standard authentication. If you plan not to use the CSM `netboot` command to add the node, you must configure the node to allow remote commands to use standard authentication from the management server.

On the management server issue the following command:

`lsauthent`

If the response does not include **Standard AIX**, you must add standard authentication to the list of authentication methods.

For example, issue the following command to change the authentication:

`chauthent -k5 -std`

If you plan to add the node using the CSM `netboot` command, go to **Prepare NIM to add the AIX nodes**. Otherwise, use `lsauthent` to check the authentication methods on the node and `chauthent` to change them. You must also ensure the `.rhosts` file exists in root's home directory and contains the name of the NIM master.

Prepare NIM to add the AIX nodes

To configure the system as a managed node for **Initiate a network installation of CSM for AIX nodes**, run the `csmsetupnim` command in this step. The `csmsetupnim` command creates node configuration files and defines CSM customization scripts as NIM script resources. NIM then runs scripts on the node during installation. The `csmsetupnim` command creates and allocates the NIM script resource to the client machine.

The command will automatically run the appropriate NIM commands on the install server if one is being used as the NIM master.

**Note:**
Each time you reinstall a node, you must run this command.

For example, to prepare NIM for installing all AIX nodes in the AIXNodes node group, do the following:

### Table 79. Preparing NIM

<table>
<thead>
<tr>
<th>If using:</th>
<th>Do this:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command line</td>
<td>Issue the <strong>csmsetupnim</strong> command, as follows:</td>
</tr>
<tr>
<td></td>
<td><code>csmsetupnim -N AIXNodes</code></td>
</tr>
<tr>
<td>SMIT</td>
<td>Issue the <strong>csmsetupnim</strong> command through SMIT. The fastpath is <code>csm_setupnim</code>. For example:</td>
</tr>
<tr>
<td></td>
<td><code>smit csm_setupnim</code></td>
</tr>
<tr>
<td>Web-based System Manager or DCEM</td>
<td>Not applicable.</td>
</tr>
</tbody>
</table>

---

## Add OpenSSH and OpenSSL software for AIX

This step is required to use OpenSSH as your remote shell. CSM only sets up OpenSSH remote shell authentication to AIX nodes during a full installation when the full installation is kicked off using the `netboot` command. If you do not use the `netboot` command for your full installations of AIX nodes, run the following command on the management server before installing them to ensure that OpenSSH remote shell authentication will be set up:

```bash
chnode -n node_list Mode=Installing
```

Because OpenSSH and its prerequisite OpenSSL are not installed with AIX, you must install the software on the management server and the AIX cluster nodes. See [OpenSSH and prerequisite software](#). To install the software on the nodes, you must copy the files to the correct NIM `lpp_source` resource directory on the NIM master and include the files for installation when you issue the NIM `bos_inst` operation.

**Bundle files:** To facilitate the installation, use the bundle files that you created when you installed the software on the management server. For example, you can create an OpenSSL bundle file called `openssl.bnd`, which contains the following line:

```
R:openssl*
```

You can create an OpenSSH bundle file called `openssh.bnd`, which contains the following lines:

```
I:openssh.base
I:openssh.license
I:openssh.man.en_US
I:openssh.msg.en_US
I:openssh.msg.EN_US
```

See [Install OpenSSH and OpenSSL for AIX](#).
Copying the software: You must copy the software to the NIM lpp_source resource directory that the nodes are to use. Use the gencopy command. You can find the software at the following locations:

- OpenSSL on the AIX Toolbox for Linux Applications for POWER Systems
- OpenSSH on the IBM AIX Expansion Pack - AIX for POWER 5.3 or 6.1

For example, assuming the lpp_source directory is the following:

/export/nim/lpp_source/530lpp_res

use the gencopy command to copy the OpenSSL package as follows:

gencopy -d /dev/cd0 -t /export/nim/lpp_source/530lpp_res -f openssl.bnd

Use the gencopy command to copy the OpenSSH file sets to the correct directory as follows:

gencopy -d /dev/cd0 -t /export/nim/lpp_source/530lpp_res -f openssh.bnd

Using bundle files with bos_inst: To have NIM install this software for you automatically during the node installation, you need to include these files when you issue the NIM bos_inst operation. Use the bundle files openssl.bnd and openssh.bnd to create NIM installp_bundle resources to use with the bos_inst operation. Create the bundle files on the same filesystem (or copy them to the same file system) that is used to store the other NIM resources (for example, /export/nim).

Assuming that the bundle files are in the directory /export/nim directory, create the two resources with the following commands:

nim -o define -t installp_bundle -a server=master -a location=/export/nim/openssl.bnd openssl

nim -o define -t installp_bundle -a server=master -a location=/export/nim/openssh.bnd openssh

You can now include the bundle resources in the bos_inst operation. For example, to include the installp_bundle resources in the bos_inst in Add CSM for AIX nodes to the cluster, modify it as follows. Note that you need to specify openssl before openssh:

nim -o bos_inst -a source=rte -a boot_client=no -a group=basic_res_grp -a
installp_bundle=openssl -a installp_bundle=openssh
accept_licenses=yes AIXNodes

Add Kerberos client software for AIX

This step is required if you are setting up Kerberos for remote commands with rsh or ssh. Because Kerberos software for remote commands is not installed with AIX, you must install the software on the management server and the AIX cluster nodes.

To facilitate the installation create a Kerberos client bundle file. A bundle file is a text file defined to NIM as a resource. During an installation or maintenance operation, NIM mounts the installp_bundle file on the client machine so it can be used by the local installp command. NIM automatically unmounts the
resource from the client when the operation has completed. For example, create a bundle file located in
/export/nim/krb5client.bnd, with the following lines:

```
I:krb5.client
I:krb5.msg.en_US
I:krb5.msg.EN_US
```

**Copying the software:** You must copy the software to the NIM lpp_source resource directory that the
nodes are to use. Use the gencopy command. You can find the software at the following location:

- AIX Expansion Pack CD

For example, assuming that the bundle file is called /export/nim/krb5client.bnd and the lpp_source
directory is /export/nim/lpp_source/530lpp_res, use the following command to copy the Kerberos client
file sets to the NIM lpp_source resource directory:

```
gencopy -d /dev/cd0 -t /export/nim/lpp_source/530lpp_res -f /export/nim/krb5client.bnd
```

**Using the bundle file with bos_inst:** To have NIM install this software for you automatically during the
node installation, you need to include krb5client.bnd when you issue the NIM bos_inst operation. Use the
bundle file krb5client.bnd to create the NIM installp_bundle resource to use with the bos_inst operation.

Assuming that the bundle file is in the directory /export/nim, directory, create the NIM installp_bundle
resource with the following command:

```
nim -o define -t installp_bundle -a server=master -a \\
    location=/export/nim/krb5client.bnd krb5client
```

You can now include the bundle resources in the bos_inst operation. For example, to include the
installp_bundle resources in the bos_inst in the next step, modify it as follows.

```
nim -o bos_inst -a source=rte -a boot_client=no -a group=basic_res_grp -a \\
    installp_bundle=krb5client AIXNodes
```

**Adding a node without hardware control:** If the csmconfig -d SetupKRB5 command indicates a value
greater than 7 for SetupKRB5 and you are not using the CSM netboot command to install the node, do
the following:

1. Issue the following command where nodename is the name of the node that you are adding:

   ```
   chnode -n nodename Mode=Installing
   ```

   Every time you add a node with Kerberos and do not use the CSM netboot command, you must
   issue the chnode command.

2. Initiate a network install of the nodes as follows:

   ```
   nim -o bos_inst -a source=rte -a boot_client=yes -a group=basic_res_grp -a \\
   installp_bundle=krb5client AIXNodes
   ```

3. Go to Monitor and verify CSM and AIX installations.

When the addition of the node is complete, CSM transfers the keytab for the host principal to the node.
Add CSM for AIX nodes to the cluster

To set up NIM to install the nodes run the `nim bos_inst` command on the NIM master as shown below.

**Note:**
Each time you reinstall a node, you must run this command.

For example, assume that you want to do an initial installation of all nodes in the `AIXNodes` node group. Also, assume that you are doing an `rte` type installation, and that the required resources have been added to the resource group `basic_res_grp` that is created when you complete the set up of NIM. Do the following:

**Table 80. Add nodes to the NIM cluster**

<table>
<thead>
<tr>
<th>If using:</th>
<th>Do this:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command line</td>
<td>Issue the <code>nim</code> command, as follows:</td>
</tr>
<tr>
<td></td>
<td>`nim -o bos_inst -a source=rte -a boot_client=no -a \</td>
</tr>
<tr>
<td></td>
<td>group=basic_res_grp AIXNodes</td>
</tr>
<tr>
<td>SMIT</td>
<td>Issue the following <code>nim</code> commands through SMIT. The first <code>nim</code> command</td>
</tr>
<tr>
<td></td>
<td>allocates the NIM install resources. The fastpath for the command is</td>
</tr>
<tr>
<td></td>
<td><code>smit nim_mac_res</code>. For example:</td>
</tr>
<tr>
<td></td>
<td><code>smit nim_mac_res</code></td>
</tr>
<tr>
<td></td>
<td>The second <code>nim</code> command sets up the <code>bos_inst</code> operation with the other</td>
</tr>
<tr>
<td></td>
<td>source, <code>boot_client</code>, and so forth. The fastpath for the second command</td>
</tr>
<tr>
<td></td>
<td>is <code>smit nim_mac_op</code>. For example:</td>
</tr>
<tr>
<td></td>
<td><code>smit nim_mac_op</code></td>
</tr>
<tr>
<td></td>
<td>When you use SMIT, you can only enable one node at a time.</td>
</tr>
<tr>
<td>Web-based System Manager or</td>
<td>Not applicable.</td>
</tr>
<tr>
<td>DCEM</td>
<td></td>
</tr>
</tbody>
</table>

To verify that you have allocated all the NIM resources that you need, before you do the network boot, you can check a single node. In the example, `node01` by issuing the following command on the NIM master:

```
lsnim -l node01
```

Because this is the initial installation of the node, NIM is not able to initiate the network boot; the `boot_client` attribute is set to `no`. In this case, you must either initiate the network boot manually on the client machine, or use the `netboot` command as described in [Initiate a network installation of CSM for AIX nodes](#).
Initiate a network installation of CSM for AIX nodes

This step assumes you are using hardware control.

Before performing this step, close all virtual terminal connections to the Hardware Management Console (HMC). Also close any `rconsole` sessions running on the nodes.

The CSM `netboot` command can be used to power on or restart a node over the cluster network. It uses adapter information for the node that is stored in the CSM database. The `netboot` command must be run on the management server.

For example, to initiate a network installation of all AIX nodes from the example in Add CSM for AIX nodes to the cluster, do the following:

**Table 81. Initiate network installation of all AIX nodes**

<table>
<thead>
<tr>
<th>If using:</th>
<th>Do this:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command line</td>
<td>Issue the <code>netboot</code> command, as follows:</td>
</tr>
<tr>
<td></td>
<td><code>netboot -N AIXNodes</code></td>
</tr>
<tr>
<td>SMIT</td>
<td>Issue the <code>netboot</code> command through SMIT. The fastpath is <code>netboot</code>. For example:</td>
</tr>
<tr>
<td></td>
<td><code>smit netboot</code></td>
</tr>
<tr>
<td>Web-based System Manager or DCEM</td>
<td>Not applicable.</td>
</tr>
</tbody>
</table>

There is no restriction for the number of HMC-attached nodes. However, running the command on many nodes at one time can result in errors. In this case, you can issue the command with the `-l` flag to limit the command to one node at a time per HMC. This increases the time to complete the command but reduces the load on the HMC and management server. You can also set the `CSM_LIMIT_OFW_SESSIONS` environment variable to enable the same limit.

By default, the `netboot` command assumes that the nodes to be installed reside on the same network segment as the management server. If the nodes reside on a different segment, you must provide the `netboot` command with the host names or IP addresses of the management server and the network gateway on the segment that is used to route LAN traffic to the management server.

For more information about the `netboot` command, see the man page or the *CSM for AIX and Linux: Command and Technical Reference*.

If you have not configured hardware control, you must initiate the network boot manually; see the *IBM AIX Installation Guide and Reference*.

Monitor and verify CSM and AIX installations

This step assumes you are using hardware control.
After the `netboot` command has completed, you can monitor and verify the installation. For a full installation, you can use the `rconsole` command to view the progress on a sample node, only after the `netboot` command has completed. For example:

```sh
rconsole -r -t -n node1
```

The `rconsole` command displays a console for the node you specified.

**Note:**
For help with `rconsole`, press the keys `Ctrl + E`, then `c`, and then `?`. To exit the `rconsole` command, press the keys `Ctrl + E`, then `c`, and then `.` (period).

You can also use the `lsnim` command to see the state of the NIM installation for a particular node, by running the following command on the NIM master:

```sh
lsnim -l clientname
```

For more information about using the `lsnim` command, see the *AIX Commands Reference*.

To check the node installations:

**Table 82. Verify node installation**

<table>
<thead>
<tr>
<th>If using:</th>
<th>Do this:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command line</td>
<td>Issue the <code>lsnode</code> command, as follows:</td>
</tr>
<tr>
<td></td>
<td><code>lsnode -a Mode</code></td>
</tr>
<tr>
<td>SMIT</td>
<td>Issue the <code>lsnode</code> command through SMIT. The fastpath is <code>csm_lsnode</code>.</td>
</tr>
<tr>
<td></td>
<td>For example:</td>
</tr>
<tr>
<td></td>
<td><code>smit csm_lsnode</code></td>
</tr>
<tr>
<td>Web-based System Manager or</td>
<td>Use the Nodes plug-in to display node information, or use DCEM to run</td>
</tr>
<tr>
<td>DCEM</td>
<td>the <code>lsnode</code> command. DCEM can be started standalone, or launched from</td>
</tr>
<tr>
<td></td>
<td>the Nodes, Groups, or Commands plug-in of the Web-based System Manager.</td>
</tr>
</tbody>
</table>

`lsnode` returns a list of all the active cluster nodes, along with their *Mode* attributes. Nodes that were successfully installed are set to *Managed*.

To check that `dsh` is working:

**Table 83. Verify dsh**

<table>
<thead>
<tr>
<th>If using:</th>
<th>Do this:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command line</td>
<td>Issue the <code>dsh</code> command. For example:</td>
</tr>
<tr>
<td></td>
<td><code>dsh -a date</code></td>
</tr>
<tr>
<td>SMIT</td>
<td>Not applicable.</td>
</tr>
<tr>
<td>Web-based System Manager or</td>
<td>DCEM can send the <code>date</code> command using <code>dsh</code>. Not applicable for Web-based System Manager.</td>
</tr>
<tr>
<td>DCEM</td>
<td></td>
</tr>
</tbody>
</table>
A list of the cluster nodes is returned, with a date for each node.

If there is a problem, see `/var/log/csm/install.log` on the managed node for information on what happened on each node during installation. Also see `/var/log/csm/netboot/*.log` on the management server.

You can also view the logs for NIM. To do this:

**Table 84. View NIM logs**

<table>
<thead>
<tr>
<th>If using:</th>
<th>Do this:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command line</td>
<td>Issue the <code>nim</code> command. For example:</td>
</tr>
<tr>
<td></td>
<td><code>nim -o showlog -a log_type=niminst lparn03</code></td>
</tr>
<tr>
<td>SMIT</td>
<td>Issue the <code>nim</code> command through SMIT. The fastpath is <code>nim_mac_op</code>. For example:</td>
</tr>
<tr>
<td></td>
<td><code>smit nim_mac_op</code></td>
</tr>
<tr>
<td>Web-based System Manager or DCEM</td>
<td>In Web-based System Manager, select Network Installation Management and Machines; right-click on a node and choose Troubleshooting -&gt; Show NIM logs; select The installp output from a NIM operation (niminst) and click OK. Not applicable on DCEM.</td>
</tr>
</tbody>
</table>

You can view one of several log types by using the `log_type` attribute with the `showlog` operation. Some of the valid `log_type` attribute values are:

- niminst
- bosinst
- boot
- script

For a complete list of these logs and their corresponding `log_type` attribute values, see the *IBM Network Installation Management Guide and Reference*.

---

**Enable Kerberos Version 5 remote commands for AIX (optional)**

To use Kerberos Version 5 for remote command authentication, see *Enabling remote commands to use Kerberos Version 5 authentication*. 

---

194
Chapter 14. Installing Linux on nodes

Use the following sections to install the Linux operating system on your cluster nodes. If your nodes already have a supported version of Red Hat Enterprise Linux (Red Hat EL) or SUSE Linux Enterprise Server (SLES) installed, see Upgrading Linux nodes, Upgrading a Linux install server, or Adding Linux nodes.

Before you perform the Linux installation

Before you begin installing the Linux operating system, verify the following prerequisites:

- The operating system and CSM is installed on the management server.
- The operating system and CSM is installed on any install servers, and the install servers are CSM Managed nodes.
- Node attributes are defined; see Defining nodes.
- To use hardware control, hardware control points and console servers are set up; see the CSM for AIX and Linux: Administration Guide.
- Optionally, remote hardware inventory and maintenance is set up, and the rfwscan command has been run as described in System x hardware inventory and maintenance.

To upgrade a Linux node instead of reinstalling the operating system, see Upgrading Linux on nodes.

Avoiding problems with Linux node hardware and network setup

To avoid problems you might encounter during installation, see Avoiding problems with hardware and network setup.

Continue with the following procedures to install CSM and Linux on nodes.

Installing Linux nodes without using hardware control

For details, see:

- Installing Linux nodes without hardware control
- Installing Linux on System p and BladeCenter JS nodes
- Provisioning Linux nodes
Configuring your switch for multiple VLANs on Linux

If you have multiple network interfaces on a management server that are attached to the same VLAN, you may see some unexpected side effects due to the fact that broadcast traffic on the VLAN is seen on multiple interfaces.

Avoiding problems with externally attached SCSI devices on Linux

If your system has external storage attached to either a secondary SCSI device or FiberChannel PCI adapter, it must be powered off or disconnected when you install the operating system.

Check Linux node software requirements

Before continuing with the installation, see Planning for CSM software for information about cluster node software requirements.

Set the node boot order for Linux on System x nodes

System x and xSeries nodes: You must set the boot order for each Linux on System x node in your cluster, in the node BIOS (Basic Input/Output System). During node boot, press the F1 key when you are prompted. Set the boot order as follows:

1. Diskette
2. CD-ROM
3. Network
4. Hard disk

BladeCenter JS nodes: To set the boot order for the BladeCenter JS nodes, launch the Management Module Web interface, and do the following:

1. Click on Blade Tasks --> Configurations.
2. Change boot sequence to "Hard drive 0".

Disable Virus Detection for x360 nodes (optional)

To avoid a Virus Warning message that can occur during the first boot after the full Linux installation on x360 nodes, change the Virus Detection from "Enabled" to "Disabled".
Update Linux node BIOS to support non-eth0 installation (optional)

For xSeries 335 and 345 servers, the default BIOS only supports booting from eth0. To support the installation through a non-eth0 adapter, you must update the BIOS; high-level BIOS version for these servers is available at http://www.ibm.com/support.

For x335, update BIOS to 1.10 or above to support PXE boot from BOTH Ethernet.

For x345, update BIOS to 1.15 or above to support PXE boot from BOTH Ethernet.

Verify Linux node hardware control point user IDs and passwords

Verify that the user IDs and passwords required for remote hardware control points have been set; see Store Linux hardware control point user IDs and passwords. The step is required for hardware control. For detailed information about hardware control points, see Managing hardware control points.

System x, including xSeries 336 and 346 servers with RSA-II SlimLine adapters installed: You must define the user IDs and passwords required to access each RSA (Remote Supervisor Adapter) and ISMP (IBM Integrated System Management Processor). To configure System x servers, change the default hardware control point user IDs and passwords using the utility disks and documentation provided with the hardware. For System x RSAs the default user ID is USERID and the default password is PASSWORD (P-A-S-S-W-zero-R-D).

HMC-attached System p: Issue the systemid command. For example, if the host name of the HMC is hmc1 and the user ID is hscroot, issue the following command:

```
systemid hmc1 hscroot
```

You will be prompted for a password for the user ID you specified.

Servers that require the APC MasterSwitch: Issue the systemid command. For example, if the APC MasterSwitch name is apc01.pok.com, issue the following command:

```
systemid apc01.pok.ibm.com apc
```

You will be prompted for a password for the specified user ID.

Direct attach System p: Change the default hardware control point password using the systemid command. Run systemid with the -f and -s flags for the HMC, admin, and general login IDs. For example, if the IP address of the node's FSP is 192.168.1.1 and the password for the HMC login is being set:

```
systemid -f -s 192.168.1.1 HMC
```

You will be prompted for a password for the user ID you specified. The default passwords are the same as their respective login.

Note:
Change the "System power off policy" to "Stay on". This setting is required for installation and can be changed in the FSP Web ASM GUI, or by running the `rpower -o option cec_setting` command. See the man page or the CSM for AIX and Linux: Command and Technical Reference for `rpower` command usage.

**BladeCenter**: To configure BladeCenter Management Modules, change the default hardware control point Login Profile user ID and password using the Management Module web interface and documentation provided with the hardware.

For BladeCenter JS and HS (except for the HS20-8678) blade servers, run the `systemid -o` command to store the Login Profile user ID and password required to access the Serial Over LAN feature.

For xSeries 336 and 346 servers using SOL to access the remote console, you must run the `systemid -c` command. For more information, refer to Remote console configuration.

For information on BladeCenter HS servers, see Configuring the BladeCenter Management Module; for BladeCenter JS servers, see Authentication and console requirements.

**IVM-managed System p**: Issue the `systemid` command. For example, if the host name of the IVM is `ivm1` and the user ID is `padmin`, issue the following command:

```
systemid ivm1 padmin
```

You will be prompted for a password for the user ID you specified.

**eServer 325 and 326 and xSeries 336 and 346 without an RSA-II SlimLine adapter installed**: Issue the `systemid` command. For example, if the BMC name is `bmc01.ibm.com`, issue the following command:

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

You will be prompted for a password for the user ID you specified. The `systemid` command stores the user ID and password for remote hardware.

### Verify Linux node definitions

After `definenode` has run, the management server has been set up with node information for CSM, and any install servers have been set up, you are ready to verify the node definitions. Verify and customize your cluster node definitions before the nodes are installed. Because nodes have not been installed, you can make changes to node definitions.

To determine whether the nodes have been defined, issue the `lsnode` command from the management server:

```
lsnode
```

The system responds with a line for each node that was successfully defined. If a node has not been defined, it will not appear in the output for the `lsnode` command.

To display all the information about each node, use the `lsnode` command, from the management server, with the `-l` (lowercase L) flag:

```
lsnode
```
lsnode -l

The system responds with a list (output) containing extended information for each node that was successfully defined. If a node has not been defined, it will not appear in the output for the lsnode command. Note that some of the attributes for a node might have null values at this point.

Note:
If a node has not been defined, it will not be installed.

If you must correct information, you can change the attributes of the nodes either by running the chnode command, or by rerunning the definenode command with the -m (modify) flag. The definenode -m command accepts a new nodedef file or a new command line and only modifies nodes that have changed attributes.

To change attribute values of a node, issue the chnode command from the management server:

chnode hostname attr=value

See the man pages or the CSM for AIX and Linux: Command and Technical Reference for more information about the lsnode, chnode, and definenode commands.

---

**Validate remote power for Linux nodes**

Before installing Linux nodes, test remote power (rpower) and remote console (rconsole) to make sure they are configured. Remote power network boots the nodes to collect the MAC addresses and install the nodes. To test rpower, issue the following:

rpower -a query

The rpower command output lists node power status. For example:

```
# rpower -a query
c5n72.clusters.com on
c5n73.clusters.com on
c5n74.clusters.com off
c5n75.clusters.com off
```

To perform the installation, node power can be in either the on or off state. If you get errors from running the rpower command, see the CSM for AIX and Linux: Administration Guide to diagnose the problem. Nodes with errors will not be installed.

Remote console is required to obtain MAC addresses. To test rconsole, issue the following:

rconsole -a

The rconsole -a command opens console windows for all nodes. If there are a large number of nodes in your cluster, you can test only a subset of the nodes.

Note:
1. For BladeCenter, the MAC addresses are obtained from the vital product data (VPD) of the node. Remote console is not required.
2. If you use an incorrect MAC address dhcp errors can occur when a node boots during the installnode process.

Copy CSM packages for Linux nodes

If any of your Linux nodes have different installation attribute values than the management server values, you must run the copycsmpkgs command to copy the CSM packages to the correct locations in /csminstall before you can install the nodes. If you have multiple nodes that all have the same installation attributes, you can run copycsmpkgs only once for a representative node.

Consider the following scenarios for running the copycsmpkgs command:

- The management server is running AIX and a node is running Linux - different InstallOSName values.
- The management server is running Red Hat EL AS or Red Hat EL ES, and a node is running Red Hat EL WS - different InstallDistributionName values.
- The management server is running a different level of the operating system than the nodes. For example, the management server is running SLES 10, and a node is running SLES 9 - different InstallDistributionVersion values.
- The management server is an xSeries server (x86 architecture) and the node is a BladeCenter JS blade server (POWER architecture) - different InstallPkgArchitecture values.
- The management server is running a different Service level than a node - different InstallServiceLevel values.

In any of these cases, or any time any of the attributes listed above are different between the management server and a node, run copycsmpkgs as follows, where node is a single node name for which the packages might be copied, and path is the path name that contains the CSM RPMs. The command prompts for any required Linux distribution CDs.

```
copycsmpkgs -p path -n node
```

If you have multiple nodes that all have the same installation attributes, run copycsmpkgs for only one of the representative nodes.

Copy SLES service level CDs

If you are installing nodes with a SLES 9 service level-the InstallServiceLevel attribute is set to a value other than GA or blank—you must copy both the GA and service level CDs. For example, if you are installing SLES 9, service pack 1 (SP1), run the following command, where PATH is the directory path to the SLES 9 GA CDs:

```
copycds -p PATH InstallDistributionName=SLES InstallDistributionVersion=9 \
InstallServiceLevel=GA
```

The service level CDs are copied when you run csmsetupinstall, in Configure a SLES installation.
Attention:
If you are installing a SLES 10 service level, you do not have to copy the SLES 10 GA CDs.

Modify Linux node configuration templates (optional)

If necessary, you can modify node configuration templates before proceeding with Linux node installations. For Red Hat EL nodes, use the Kickstart configuration template. For SLES nodes, use the AutoYaST configuration template. See Using the Kickstart node configuration template and Using the AutoYaST node configuration template.

Using the Kickstart node configuration template

The Red Hat EL Kickstart node configuration template file is as follows, where
InstallDistributionNameInstallDistributionVersion is the concatenation of the InstallDistributionName and InstallDistributionVersion attribute values. Some template files also have an appended -Arch extension, which matches the InstallPkgArchitecture attribute value:

/opt/csm/install/kscfg.tmpl.InstallDistributionNameInstallDistributionVersion-Arch

For example, the template name for Red Hat EL AS 4 POWER nodes is:

/opt/csm/install/kscfg.tmpl.RedHatEL-AS4-ppc64

The Kickstart configuration template file contains the following information:

- Initial root password (defaults to cluster), plus an additional user ID called admin with a password of cluster.
- Disk partition table
  
  A sample disk partition table is provided, which can be modified.

- RPMs to install

  A standard list is provided; you can modify the list, or you can use your own list.

- Language and time zone
- Post-install script

  This script does standard set up and CSM-specific set up. The script may be modified to suit your installation, provided the marked sections are not altered.

Note:
Kickstart chooses a default disk type and size based on the located hardware. To specify a specific disk type and size, you can modify the kickstart configuration file. The Red Hat EL Kickstart node configuration template includes kickstart configuration file details. Red Hat EL 5 installation requires an Installation Number, which configures the installer package set. However, CSM default Kickstart templates are not permitted to specify a Red Hat EL 5 Installation Number; CSM Kickstart templates use key --skip by default. To specify an Installation Number, change key --skip to key InstallationNumber before running the csmsetupinstall or csmsetupks command.
You can create your own version of the configuration template by copying, modifying, and renaming the Kickstart template. You can use the `csmsetupinstall -k` command (in a later step) to specify that the template you created might be used for each node in your cluster, or you can set the `InstallTemplate` attribute of each node to the path name of the Kickstart template file. The default configuration template is the original `/opt/csm/install/kscfg.tmpl.RedHatVersion`.

See the annotations in the `kscfg.tmpl` file for instructions on how to modify the template. Instead of adding to the scripts in the configuration template file, consider using a customization script. For information, see Setting up Linux customization scripts.

**Using the AutoYaST node configuration template**

The SLES AutoYaST node configuration template file is as follows, where `InstallDistributionNameInstallDistributionVersion` matches the `InstallDistributionName` and `InstallDistributionVersion` node attributes. Some template files also have an appended `-Arch` extension which matches the `InstallPkgArchitecture` attribute:

```
/opt/csm/install/yastcfg.InstallDistributionNameInstallDistributionVersion-Arch.xml
```

For example, the template name for SLES 9 on x86 architecture (32-bit) is as follows:

```
/opt/csm/install/yastcfg.SLES9-i386.xml
```

The AutoYaST configuration template file contains the following information:

- Initial root password, which defaults to `cluster`, plus an additional user ID called `admin` with a password of `cluster`.
- RPMs to install. A standard list is provided; you can modify the list, or use your own list.
- Language and time zone.

**Disk partition table:** The AutoYaST template file that is shipped with CSM does not contain a disk partition table. Instead, CSM automatically determines the disk partitioning. It chooses the install device based on the attributes `InstallDisk` and `InstallDiskType` for the node, then creates the partition table based on the disk type and size. You can add your own disk partition table to the template to suit your configuration needs.

**Post-install scripts:** The `csmsetupinstall` command adds post-install scripts to each AutoYaST template file that it generates. Templates for the scripts are in the following directories:

```
/opt/csm/install/autoyast.postscript.tmpl.architecture
/opt/csm/install/autoyast.chrootscript.tmpl.architecture
```

You can modify the scripts to suit your installation needs; however, consider using a customization script. For information, see Setting up Linux customization scripts.

You can create your own version of the configuration template by copying the AutoYaST template, modifying it, and giving it a new name (make sure you keep the original template under its original name).
If you do not want CSM to parse the contents of your configuration template, the name of the template must end with "-DC.xml". For example, "my.SLES10-ppc64-DC.xml".

There are a number of variables that you can add to your template in the format of #CSMVAR:XXX#, such as "#CSMVAR:DNSDOMAIN#". CSM will substitute the appropriate values for these variables.

The list of variables is:

- **DNSDOMAIN**: the node's DNS domain name.
- **NODE_SHORTNAME**: the node's short hostname.
- **ROUTING**: the routing related information.
- **PRESOURCE**: CSM pre-install scripts.
- **POSTSOURCE**: CSM post-install scripts.
- **CHROOTSOURCE**: CSM chroot scripts.
- **TIMEZONE**: the timezone setting, such as UTC or PRC.
- **INSTALLPROTOCOL**: the network protocol used to install the node, such as nfs or http.
- **NFS_IP**: the NFS server's IP address.
- **NFS_DIR**: the node's repository location on NFS server.
- **PROFILELOCATION**: the node's profile location on Install Server.
- **NODE_IP**: the node's IP address.
- **NODE_NETDEV**: the node's network adapter name.
- **NODE_MASK**: the node's netmask.

To run the CSM pre-install, post-install or chroot scripts during installation you must use the #CSMVAR:PRESOURCE#, #CSMVAR:POSTSOURCE# and #CSMVAR:CHROOTSOURCE# variables in your <script> stanzas. For example:

```xml
<scripts>
  <pre-scripts config:type="list">
    <script>
      <filename>csmprescript</filename>
      <interpreter>shell</interpreter>
      <![CDATA[#CSMVAR:PRESOURCE#]]>
    </script>
  </pre-scripts>
  <post-scripts config:type="list">
    <script>
      <filename>csmpostscript</filename>
      <interpreter>shell</interpreter>
      <![CDATA[#CSMVAR:POSTSOURCE#]]>
    </script>
  </post-scripts>
  <chroot-scripts config:type="list">
    <script>
      <filename>csmchrootscript</filename>
      <interpreter>shell</interpreter>
      <![CDATA[#CSMVAR:CHROOTSOURCE#]]>
    </script>
  </chroot-scripts>
</scripts>
```
Sample "*-DC.xml" template files are available in /opt/csm/install/

You can use the **csmsetupinstall -k** command to specify that the created template is to be used for each node in your cluster, or you can set the **InstallTemplate** attribute of each node to the path name of the AutoYaST template file.

For AutoYaST information, see:


**Kickstart and AutoYaST node configuration scripts**

CSM includes install templates for AutoYaST and Kickstart in the /opt/csm/install directory. The templates only include basic elements for the node configuration such as base packages to install, disk partitioning schemes and root passwords. You can include additional configuration in the respective post--installation sections for Kickstart (%post, %pre) and AutoYaST (chroot script and post script).

In CSM these parts of the configuration file are separated into several scripts that the template merges with the final install image that it creates in each node. The scripts that perform the basic CSM functions and set variables are in the following location, where **distribution** is the **InstallDistributionName** attribute:

```
/opt/csm/install/templatescripts/[pre|post|chroot].distribution.
```

These scripts are appended to the Kickstart or AutoYaST template files when you run the **csmsetupinstall** command. You do not need to change anything in these scripts. Instead, use the customization scripts described in Setting up Linux customization scripts to make changes.

---

**Configure Linux driver modules**

To update drivers used during Linux installation, or drivers installed with the Linux operating system, follow this procedure. This driver update procedure is supported for SLES and Red Hat EL on System p and System x.

For example, on a SLES 9 SP1 system:

1. Check the level of your operating system using the **uname -r** command.

   ```
   uname -r
   2.6.5-7.139-default
   ```

2. Under /csminstall/csm/drivers, create the directory **2.6.5-7.139-default/i386**.

3. Download the appropriate driver tar file with the corresponding kernel version from:
Note:
If you are using a service level, you may also need drivers for the base operating system, in this case for SLES 9: CSM1.7.1.0_dvrs-2.6.5-7.97.tar.

Use the following procedure to update a driver:

1. Place a copy of the driver in the /csminstall/csm/drivers/kernel version/arch directory on the management server; for example /csminstall/csm/drivers/2.6.9-5.EL/x86_64. CSM recognizes the drivers by the suffix *\.ko in the corresponding directories. The kernel used for the installation process and the kernel installed as part of the runtime operating system may be different. For example, in RHEL4 GA, the installation kernel is 2.6.9-5.EL, but on the installed system the kernel may be 2.6.9-5.ELsmp.

2. For installation drivers, if the kernel version matches the installation kernel - 2.6.9-5.EL for example - the driver under this directory is copied into the /tftpboot/csm/distro_version.gz ramdisk image file. The driver is used later only during full installation. Typically, Red Hat EL requires the pcitable and module-info files for installation drivers.

3. For runtime operating system drivers, if the kernel version matches the kernel to be installed, the driver is copied to the node during full installation by CSM scripts as follows:
   o If a driver already exists in the system, it is overwritten.
   o For drivers such as bcm5700, ips, and megaide, which were previously supported through driver updates, the drivers are put in their specific directories under /lib/modules/. For example, the bcm5700.ko driver is put into /lib/modules/kernel version/kernel/drivers/addon/bcm5700.
   o All other drivers by default are copied to /lib/modules/kernel version/kernel/addon.
   o If there are pcitable, module-info, or modules-dep files, they are automatically used in the Red Hat EL system. These files are ignored in SLES.

For information on using customized Perl modules to extend driver-related functions, see Customizing kernel module installation on Linux (optional).

Prepare for Linux secondary adapter configuration (optional)

Secondary adapters may be configured during the node installation process or when adding a node to the cluster. To use this support there are some additional steps that must be completed. Refer to Secondary adapter interface configuration for a description of how to use this CSM feature.

Configure a Red Hat EL installation

After you have prepared your Kickstart configuration template, use the csmsetupinstall command to create a Kickstart configuration file for each of the nodes in your cluster. The csmsetupinstall command uses the information from your Kickstart node configuration template to create the Kickstart configuration files. The csmsetupinstall command does the following:

- Copies the required CDs to the /csminstall directory on the management server.
- Synchronize the install servers by copying everything in /csminstall from the management server to the install servers.
- Creates and populates the /tftpboot directory on the install servers.
- Installs the dhcp, tftp, syslinux, and nfs packages to the install server. If NetworkInstallProtocol=http and SetupNetworkInstallProtocol=1, the HTTP package is also installed.
- Creates or updates the /etc/dhcpd.conf file on the install servers.
- Checks the network and starts the DHCP, NFS, and TFTP daemons on the install servers. If NetworkInstallProtocol=http and SetupNetworkInstallProtocol=1, the HTTP daemon is also checked.
- Collects and sets MAC addresses (InstallAdapterMacaddr) or UUIDs (UUID) for nodes, if the attributes are not already set
- Creates a Kickstart configuration file for each node in on the install servers.
- Sets the InstallMethod attribute to kickstart.

For more details, see the csmsetupinstall man page or the CSM for AIX and Linux: Command and Technical Reference.

If you are not using remote power or a remote console for your nodes, see Installing Linux nodes without hardware control.

To automatically collect MAC addresses on x445 nodes, using csmsetupinstall or getadapters, the updated summit kernel must be installed on the CSM management server. To collect a MAC address, run the getadapters command. For more information, see Methods for collecting AIX MAC addresses and the getadapters man page.

Note:

1. To install eServer 325 or 326 nodes with Red Hat EL 4 (GA) i386, you must set the node HWType attributes to e325 or e326.
2. To install Red Hat EL 4 (GA) i386 on x345 hardware type 8676-61x, you must set the node HWType attribute to 8676-61x. Otherwise the system will report "kernel panic" when installing.

Before you run csmsetupinstall:

- Set the InstallServiceLevel attribute to the correct value - the service level being installed on the node. If you are installing the base operating system, set the InstallServiceLevel attribute to GA. If you are installing a service level, set the attribute to a predefined value such as QU2, or a user defined value such as compute or test.
- If your install server, or management server if it is acting as the install server, is connected to multiple VLANs, you might need to configure DHCP to only listen to requests on specific interfaces.
- For Red Hat EL on POWER-based architecture nodes, if the InstallAdapterMacaddr is not set, make sure that the remote console for that node is closed before running csmsetupinstall; otherwise, the open remote console interferes with MAC address collection.
- For Red Hat EL 4, on e325 and e326 servers, run the chnode command to set the HWType attribute to e325 or e326.
- For Red Hat EL 4 64 bit system on x346 nodes, run the chnode command to set the HWType attribute to x346 or 8840.
- If you want to install from a non-eth0 NIC, ensure that you set the following hardware attribute (see Hardware control attributes):
  - InstallAdapterName
Running csmsetupinstall: To run the csmsetupinstall command for all PreManaged nodes, enter the following commands. The lsnode command indicates if the node is valid for installation.

lsnode -a Hostname,InstallStatus

csmsetupinstall -P

You are prompted to insert the Red Hat EL CD-ROMs if they have not already been copied. The copy progress is indicated through a percentage (%) value. If the InstallServiceLevel attribute is set to a user defined value such as compute, use the -p flag to specify the pathname that contains your custom RPMs.

The csmsetupinstall command saves output to /var/log/csm/csmsetupinstall.log.

Large clusters of HMC-attached pSeries nodes running Linux on POWER: Large clusters of HMC-attached pSeries nodes that run Linux on POWER can see hmc_nodecond errors when collecting the MAC addresses for large numbers of nodes at the same time. In these cases, try to limit MAC address collection to one node at a time per HMC by setting the CSM_LIMIT_OFW_SESSIONS environment variable, then re-running the command. This will increase the time to complete the command, but will reduce the load on the HMC and management server. The value of the variable is not significant; only whether it is defined or not. In a ksh environment, you can use the following command to set the variable:

export CSM_LIMIT_OFW_SESSIONS=1

In a ksh environment, use the following command to clear the variable:

unset CSM_LIMIT_OFW_SESSIONS

Red Hat EL Kickstart installations and upgrades

During a Red Hat EL Kickstart installation or upgrade, the installnode command completes the following steps. For Red Hat EL on System x nodes:

1. Sets up the /tftpboot/pxelinux.cfg/node-ip-addr-in-hex on each node's install server, so that a node reboot runs a Kickstart installation or upgrade.
2. Reboots the node. At this point, installnode command execution is complete, and the remainder of the process proceeds on the node.
3. As the node reboots, broadcasts its MAC address.
4. The dhcp server on the install server accepts the node's dhcp request, and pxelinu initiates a Kickstart installation or upgrade.
5. Kickstart installs or upgrades the operating system on each node using the kickstart configuration file in /csminstall/csm/InstallCSMVersion/kickstart_installDistributionNameInstallDistributionVersion/node-ipaddr-kickstart. After some additional configuration, any user scripts in /csminstall/csm/scripts/installprereboot or /csminstall/csm/scripts/osupgradepreboot are run. Then the Kickstart post-installation script adds the csmfirstboot script /csminstall/csm/InstallCSMVersion/csmfirstboot to /etc/inittab. Then the Kickstart post-installation or upgrade script adds the csmfirstboot script /csminstall/csm/InstallCSMVersion/csmfirstboot to /etc/inittab. It then modifies the pxelinu configuration file /csminstall/pxelinu.cfg/node-ip-addr-in-hex on the install server so that the next reboot of the node reboots from the local hard drive.
6. The node reboots to the local hard drive.
7. As the reboot completes, the csmfirstboot script, which was listed in /etc/inittab, is run on the node.
8. The csmfirstboot script installs or upgrades CSM and its dependencies, defines the management server, transfers CFM files, installs SMS packages, and runs any user scripts in /csminstall/csm/scripts/installpostreboot or /csminstall/csm/scripts/osupgradepostreboot. Then csmfirstboot removes itself from /etc/inittab. If the node's Mode is MinManaged, CSM is not installed on the node.

9. When the node Mode attribute value is Managed, the node is ready for use in the cluster. For MinManaged nodes, the Mode does not change to Managed. Run the monitorinstall command from the management server to see the installation or upgrade status of MinManaged nodes.

For Red Hat EL on System p, including BladeCenter JS nodes:

1. An arp entry is made for the node on the install server and the node is rebooted to start in firmware mode. The installnode command communicates with the node's firmware to initiate a directed BOOTP request to the install server, which retrieves the kernel and initial ramdisk and reboots the node.

2. At this point, installnode command execution is complete, and the rest of the process proceeds on the node.

3. Kickstart installs or upgrades the operating system on each node.

4. After the Kickstart installation or upgrade of the operating system is complete, the Kickstart post-installation script, /csminstall/csm/InstallCSMVersion/kickstart.InstallDistributionNameInstallDistributionVersion/node-ipaddr-kickstart, is run on the node. After some additional configuration, scripts in /csminstall/csm/scripts/installprereboot or /csminstall/csm/scripts/osupgradepreboot are run. Then the Kickstart post-installation or upgrade script adds the csmfirstboot script /csminstall/csm/InstallCSMVersion/csmfirstboot to /etc/inittab.

5. The node reboots to the local hard drive.

6. As the reboot completes, the csmfirstboot script, which was listed in /etc/inittab, is run on the node.

7. The csmfirstboot script installs or upgrades CSM and its dependencies, defines the management server, transfers CFM files, installs SMS packages, and runs any user scripts in /csminstall/csm/scripts/installpostreboot or /csminstall/csm/scripts/osupgradepostreboot. Then csmfirstboot removes itself from /etc/inittab. If the node's Mode is MinManaged, CSM is not installed on the node.

8. When the node Mode attribute changes to Managed, the node is installed and ready for use in the cluster. For MinManaged nodes, the Mode does not change to Managed. Run the monitorinstall command from the management server to see the installation or upgrade status of MinManaged nodes.

Configure a SLES installation

After you have prepared your AutoYaST configuration template, use the csmsetupinstall command to create a AutoYaST configuration file for each of the nodes in your cluster. The csmsetupinstall command uses the information from your AutoYaST node configuration template to create the AutoYaST configuration files. The csmsetupinstall command does the following:

- Copies SLES CDs to the /csminstall directory on the management server
- Synchronize the install servers by copying everything in /csminstall from the management server to the install servers
- Creates and populates the /tftpboot directory on the install server
• Installs the dhcp, tftp, syslinux, and nfs packages to the install server. If "NetworkInstallProtocol=http" and "SetupNetworkInstallProtocol=1", the http package is also installed.
• Creates or updates the /etc/dhcpd.conf file on the install server
• Checks the network and starts the DHCP, NFS, and TFTP daemons on the install servers. If "NetworkInstallProtocol=http" and "SetupNetworkInstallProtocol=1", the HTTP daemon is also checked.
• Collects and sets MAC addresses (InstallAdapterMacaddr) or UUIDs (UUID) for nodes, if the attributes are not already set.
• Creates a AutoYaST configuration file for each node on the install server.
• Sets the InstallMethod attribute to autoyast.

For details, see the csmsetupinstall man page or the CSM for AIX and Linux: Command and Technical Reference.

**Before you run csmsetupinstall:** If your management server is connected to multiple VLANs, configure DHCP to only listen to requests on specific interfaces.

For SLES 9 GA on System x 346 nodes, run the chnode command to set the HWType attribute to x346. Use the aic79xx.ko driver for the SCSI hard disk controller in the x346 server.

For SLES on System p nodes, if the InstallAdapterMacaddr is not set, make sure that the console for that node is closed before running csmsetupinstall; otherwise, the open remote console interferes with MAC address collection.

Before running csmsetupinstall, set the InstallServiceLevel attribute to the service level being installed on the node. If you are installing the base operating system, set the InstallServiceLevel attribute to GA. If you are installing a service level, set the attribute to a predefined value such as SP1 or SP3, or a user defined value such as compute or test.

**Running csmsetupinstall:** To run the csmsetupinstall command for all the PreManaged nodes of your cluster, enter the following command:

csmsetupinstall -P

You are prompted to insert the SLES CD-ROMs if they have not already been copied.

If the InstallServiceLevel node attribute is set to GA or blank, you will be prompted to insert the base CDs. If the InstallServiceLevel is set to a supported service level such as QU3, you will be prompted to insert both the base CDs and the service level CD-ROMs. If the InstallServiceLevel attribute is set to a user defined value such as compute, use the -p flag to specify the pathname that contains your custom RPMs.

The csmsetupinstall command saves the output to the following log file:

/var/log/csm/csmsetupinstall.log

**Note:**

dhcp sometimes holds on to the IP lease, resulting in installation problems. This problem can be detected by looking for NOACKS, or "no free leases" entries in the /var/log/messages file. Erase the/var/lib/dhcp/dhcpd.leases file and restart dhcp as follows:

/etc/init.d/dhcpd restart

**Large numbers of Linux on HMC-attached System p nodes:** hmc_nodecond errors can occur when simultaneously collecting MAC addresses for large numbers of Linux on HMC-attached System p nodes.
You can limit MAC address collection to one node at a time per HMC by setting the `CSM_LIMIT_OFW_SESSIONS` environment variable, then re-running the command. This increases the time required to complete the command, but reduces the load on the HMC and management server. The value of the variable is not significant; only whether it is defined or not. In a ksh environment, you can use the following command to set the variable:

```
export CSM_LIMIT_OFW_SESSIONS=1
```

In a ksh environment, use the following command to clear the variable:

```
unset CSM_LIMIT_OFW_SESSIONS
```

### SLES AutoYaST installation

SLES uses AutoYaST to install the operating system. The `installnode` command completes the following steps for Linux on System x nodes:

1. Sets up the `/tftpboot/pxelinux.cfg/node-ip-addr-in-hex` file on your install servers so that a node reboot runs an AutoYaST installation.
2. Reboots the node.
3. As the node reboots, broadcasts its MAC address.
4. The `dhcp` server on the install server accepts the node's dhcp request, and `pxelinux` initiates an AutoYaST installation.
5. AutoYaST installs the operating system on each node.
6. After the AutoYaST installation of the operating system is complete, the AutoYaST post-installation script `/csminstall/csm/InstallCSMVersion/InstallDistributionName InstallDistributionVersion/nodeipaddr-autoyast.xml` is run on the node. After some additional configuration, scripts in `/csminstall/csm/scripts/INSTALLPREREBOOT` are run. The AutoYaST post-installation script adds the `/opt/csm/install/csmfirstboot` script to `/etc/inittab`. It then modifies the `pxelinux` configuration file `/tftboot/pxelinux.cfg/node-ip-addr-in-hex` on the management server so the next node reboot is from the local hard drive.
7. The node reboots to the local hard drive.
8. As the reboot completes, the `csmfirstboot` script listed in `/etc/inittab` runs on the node.
9. The `csmfirstboot` script installs or upgrades CSM and its dependencies, defines the management server, transfers CFM files, installs SMS packages, and runs any user scripts in `/csminstall/csm/scripts/INSTALLOSTBOOT` or `/csminstall/csm/scripts/OSSUPPORTPROCESS`. Then `csmfirstboot` removes itself from `/etc/inittab`. If the node's `Mode` is MinManaged, CSM is not installed on the node.
10. When the node `Mode` attribute changes to Managed, the node is installed and ready for use in the cluster. For MinManaged nodes, the `Mode` is not changed to Managed. Run the `monitorinstall` command from the management server to see the installation status of MinManaged nodes.

The `installnode` command completes the following steps for Linux on POWER (System p and BladeCenter JS) nodes:

1. An `arp` entry is made for the node on the install server and the node is rebooted to start in firmware mode. The `installnode` command communicates with the node's firmware to initiate a directed BOOTP request to the install server, which retrieves the kernel and initial ramdisk and reboots the node.
2. At this point, `installnode` command execution is complete, and the rest of the process proceeds on the node.
3. AutoYaST installs the operating system on each node.
4. After the AutoYaST installation of the operating system is complete, the AutoYaST post-installation script `/csminstall/csm/InstallCSMVersion/autoyast/InstallDistributionName
InstallDistributionVersion/nodeipaddr-autoyast.xml` is run on the node. After some additional configuration, any user scripts in `/csminstall/csm/scripts/installprereboot` are run. The AutoYaST post-installation script then adds the `csmfirstboot` script, `/opt/csm/install/csmfirstboot`, to `/etc/inittab`. The script then modifies the `/tftboot/pxelinux.cfg/node-ip-addr-in-hex` configuration file on the management server so the next node reboot is from the local hard drive.

5. The node reboots to the local hard drive.

6. As the reboot completes, the `csmfirstboot` script, which was listed in `/etc/inittab`, is run on the node.

7. The `csmfirstboot` script installs or upgrades CSM and its dependencies, defines the management server, transfers CFM files, installs SMS packages, and runs any user scripts in `/csminstall/csm/scripts/installpostreboot` or `/csminstall/csm/scripts/osupgradepostreboot`. Then `csmfirstboot` removes itself from `/etc/inittab`. If the node's `Mode` is `MinManaged`, CSM is not installed on the node.

8. When the `Mode` attribute for this node is changed to `Managed`, the node is installed and ready for use in the cluster. For `MinManaged` nodes, the `Mode` is not changed to `Managed`. Run the `monitorinstall` command from the management server to see the installation status of `MinManaged` nodes.

---

### Verify and update Linux node configuration

Run the `ibm.csm.node-install` probe to verify that the nodes are correctly configured and ready to be installed. This probe ensures that all node attributes are correct, installation source files are available, and installation configuration files have been created. For example:

```
probemgr -p ibm.csm.node-install -l 0
```

For details, see [Using probes](#) in the *CSM for AIX and Linux: Administration Guide*.

### Update Linux DHCP configuration

After the `csmsetupinstall` command runs the first time, you can customize the `/etc/dhcpd.conf` file. Take care to not remove or modify any CSM entries when making modifications to the new `/etc/dhcpd.conf` file, or use the `mkdhcp` tool to safely add or delete your own entries in the `/etc/dhcpd.conf` file.

### Update Kickstart configuration

The `csmsetupinstall` command generates a Kickstart configuration file for each Red Hat Enterprise Linux (EL) node. You can modify these Kickstart files, which are stored on your install server. If your management server is the install server, the file names are:

```
/csminstall/csm/CSMVersion/kickstart.InstallDistributionName\
InstallDistributionVersion/node-ip-address-kickstart
```

For example, a Kickstart configuration file for a Red Hat EL AS 4 node is similar to:
If a separate install server is used for Red Hat EL nodes, the Kickstart configuration file names use
/cmserver by default, or the value specified by the InstallServer attribute. For example:

Modify your Kickstart configuration files after running the cmsetupinstall command. Modifying a file
affects only the settings on the specific node. Rerunning cmsetupinstall overwrites the file, so use
cautions when modifying a generated file.

**Update AutoYaST configuration**

If you are using SLES, you can modify the AutoYaST configuration file that the cmsetupinstall
command generates for each node. The AutoYaST configuration file is generated on the management
server. If the management server is acting as the install server, or on the install servers, for example. If it is
on the management server, the filename is:
/cminstall/cm/cmserver/cm/1.7.1/autoyast.DistributionNameDistributionVersion \
/node-ip-address-autoyast.xml

For example, the file for SLES 9 is the following:
/cminstall/cm/1.7.1/autoyast.SLES9/9.114.113.130-autoyast.xml

If the install server is not on the management server, then the first part of the filename is either /cmserver,
by default, or whatever value was specified in the InstallServer attribute:
/cminstall/cm/1.7.1/autoyast.SLES9/9.114.113.130-autoyast.xml

Modify this file after running the cmsetupinstall command. Modifying the file affects only the settings
on the specific node. If you rerun cmsetupinstall, you overwrite the file, so use care when you modify a
generated file.

---

**Create configuration files and RPM updates for Linux nodes**

*(optional)*

During the operating system installation, CSM can automatically transfer system configuration files and do
additional RPM updates on the nodes. These tasks can be accomplished by setting up the Configuration
File Manager (CFM) and Software Maintenance System (SMS) utilities before installing your nodes. For
information on configuring CFM and SMS, see the *CSM for AIX and Linux: Administration Guide*.

The CFM configuration files are distributed to the node when the Mode changes to Managed or when a
MinManaged node finishes installation.

After the node becomes Managed, or when a MinManaged node finishes installation, the SMS RPMs are
also updated and installed on the node. First SMS installs any RPMs stored in the following directory:
Then SMS updates any RPMs in the following directory:

```
/csminstall/Linux/InstallDistributionName/InstallDistributionVersion/ \
InstallPkgArchitecture/install
```

For example, to install IB packages to CSM Managed Nodes after the basic SLES10SP2 OS is installed, the user needs to copy all the IB related rpms from suse/ directory in SLES10SP2 Advanced Server CD to /csminstall/Linux/SLES/10/ppc64/SP2/install/ directory.

---

**Setting up Linux customization scripts**

The `installnode` command runs any user-defined customization scripts that have been placed in the following two directories:

- These scripts are executed after the node has been installed, but prior to the node reboot:
  `installprereboot`
- These scripts are executed after the first node reboot, after CSM has been installed:
  `installpostreboot`

This command checks these directories and runs each script on the node at the appropriate time. Subdirectories are not checked. If there are multiple scripts in a directory, they are run in alphabetical order, as determined by the `ls` command on the management server.

**Note:**

See also the `/csminstall/csm/scripts` directories in *Installation directories and files*.

The naming convention for the scripts is:

```
scriptname[._target]
```

The `_` following the script name is required if the script is to only be used for a specific node or node group. The target value must be a single node name or group name that has been defined in the CSM database. If the target extension is not used, then the script will be run on all nodes. If there is a script and additional multiple versions for subsets of nodes (for example, `myscript`, `myscript_groupA`, `myscript_groupB`), the script with no target extension is run only for those nodes that are not included in one of the specific groups (for example, not in `groupA` or `groupB`). For more information on CSM support for user-provided customization scripts, see the *CSM for AIX and Linux: Administration Guide*.

If you are using Kerberos with remote commands, you can use customization scripts to automate some post installation tasks for enabling remote commands to authenticate with Kerberos. See *Enabling remote commands to use Kerberos Version 5 authentication*.

**Modifying and deleting Linux customization scripts**

Because subsequent installations and updates of CSM cause CSM to update the `install|pre|post|reboot` scripts, do not change them in the `/csminstall/csm/scripts/install|pre|post|reboot` directory. Instead, copy
the script to the /esminstall/esm/scripts/data directory and modify the script there. In this way, you can override the CSM install[pre|post]reboot scripts.

All CSM install[pre|post]reboot scripts contain a flag in the beginning of the script to check if a script of the same name exists in the /esminstall/esm/scripts/data directory. If a script with the same name exists, CSM runs the override script instead of the standard script.

To list the post-installation scripts (preboot or postboot) to be used during installation, enter the following command:

```
nodegrp -s nodename | xargs -i find \
/esminstall/esm/scripts/installprereboot \
/esminstall/esm/scripts/installpostreboot -name *{}\{}
```

### Modifying a Linux customization script

For example, to modify the Linux customization script `006CSM_adduser._LinuxNodes`:

1. Copy the file:
   
   `/csminstall/csm/scripts/installprereboot/006CSM_adduser._LinuxNodes`

   to the following directory:

   `/csminstall/csm/scripts/data`

2. Edit the script.

   When you perform the installation of the node, CSM checks if a modified `006CSM_adduser._LinuxNodes` script exists in the `/csminstall/csm/scripts/data` directory and runs the modified script instead of the standard script.

### Deleting a Linux customization script

For example, to stop running the Linux customization script `001CSM_updateDrivers._LinuxNodes`, which updates the drivers on the server and is located in `/csminstall/csm/scripts/installprereboot/001CSM_updateDrivers._LinuxNodes`:

1. Copy the following:

   `/csminstall/csm/scripts/installprereboot/006CSM_adduser._LinuxNodes`

   to the following directory:

   `/csminstall/csm/scripts/data`

2. Remove the contents of the following script so that it is blank:

   `/csminstall/csm/scripts/installprereboot/001CSM_updateDrivers._LinuxNodes`

   When you perform the installation of the node, CSM calls the blank script and does not update the drivers. The original script remains in the following location:
Update Linux kernels during installation (optional)

To use a kernel other than the default kernel for your Linux nodes, use the `updateKernel` sample script. The script installs the kernel after the operating system has been installed, but before the node has been rebooted. This allows the node to reboot into the new kernel. Copy the `/opt/csm/samples/install/updateKernel` script to `/csminstall/csm/scripts/installprereboot` before installing the node. See the `/opt/csm/samples/install/updateKernel.README` file for details.

Provide Kerberos client packages for Linux (optional)

If you plan to use Kerberos Version 5 for remote commands, ensure that the Kerberos client packages are available for installation. See CSM for Linux Kerberos setup.

Place the required Kerberos packages in the following directory, where `InstallDistributionName` is the Linux distribution, `InstallDistributionVersion` is the Linux version, and `InstallPkgArchitecture` is the Linux architecture:

```
csminstall/Linux/InstallDistributionName/InstallDistributionVersion /InstallPkgArchitecture/install
```

SMS installs the Kerberos packages when you run the `installnode` command as described in Install CSM and Linux on nodes.

Use README files to perform Linux NTP or Automounter setup (optional)

CSM provides sample files to help you configure your cluster, including samples for configuring NTP and the Automounter. To use any CSM samples, do the setup now as documented in the README files in `/opt/csm/samples/docs`. You can modify the samples to handle different configurations or system requirements.

Install CSM and Linux on nodes

When a node has been defined but not installed, its `Mode` attribute value is `PreManaged`. By installing the node using the `installnode` command, the `Mode` attribute value is changed to `Managed`. If the `Mode` attribute value is `MinManaged`, after running the `installnode` command the value remains `MinManaged`.  

CSM for AIX and Linux: Planning and Installation Guide
You must run the `definenode` and `csmsetupinstall` commands before running the `installnode` command. If the `installnode` command fails for a PreManaged node, the `Mode` value is PreManaged or Installing. If the `installnode` command fails for a MinManged node, the `Mode` value is MinManaged or MinManaged-Installing.

To install all PreManaged nodes, issue the following command:

```
installnode -P
```

The PreManaged nodes are rebooted and installed with the operating system and CSM. See Installing Linux nodes without hardware control for more information.

The installation runs asynchronously. Immediately after the installation process is initiated-when the node is rebooted-the `installnode` command exits, even though the installation might not be complete.

Use the `installnode -t` command to provide a timeout value, where `timeout` is the timeout value in minutes. If you do not specify a value for `timeout`, the default is 60 minutes:

```
installnode -P -t timeout
```

If the installation process does not complete within the timeout period specified, CSM considers the installation process to have failed. Use the `monitorinstall` command to provide output information for the installation process. See Monitor and verify CSM and Linux installations.

After the operating system is installed, the following occurs on the node:

1. The `installprereboot` customization scripts are run.
2. The node reboots to its local hard disk.
3. CSM is installed, along with the software listed in Planning for CSM for Linux nodes.
4. The node `Mode` attribute changes to Managed.
5. `ssh` or `rsh` is set up on the node to grant access to the management server.
6. Any CFM files are transferred to the node.
7. If configured, SMS is run to install or update software.
8. The `installpostreboot` customization scripts are run.

If you defined Kerberos options on `csmconfig` when you defined the management server, the `installnode` command sets up the Kerberos options for the cluster. See Set up Kerberos Version 5 for remote Linux command processing (optional).

After a full installation, the boot order in the BIOS for System x nodes can remain:

1. diskette
2. CD-ROM
3. network
4. hard disk

Each time the node boots, it uses Dynamic Host Configuration Protocol (`dhcp`) to contact the management server or the install server, which uses `pxelinux` to boot the node from its hard drive. Alternately, after full installation you can change the boot order in the BIOS for System x nodes to:

1. diskette
2. CD-ROM
3. hard disk
4. network

Note:
When you run the **installnode** command on SLES nodes, NFS error messages can occur. You can ignore these error messages; see [NFS warnings](#).

**Large numbers of Linux on HMC-attached System p nodes:** Reboot errors can occur when simultaneously installing large numbers of Linux on HMC-attached System p nodes. In this case, limit the installations to one node at a time per HMC by setting the `CSM_LIMIT_OFW_SESSIONS` environment variable, and re-running the command. This increases the time to complete the command, but reduces the load on the HMC and management server. The value of the variable is not significant; only whether it is defined or not. In a **ksh** environment, you can use the following command to set the variable:

```bash
export CSM_LIMIT_OFW_SESSIONS=1
```

In a **ksh** environment, use the following command to clear the variable:

```bash
unset CSM_LIMIT_OFW_SESSIONS
```

To install SLES 9 x86_64 GA on System x 336, 346, or BladeCenter HS20-8843, see [Installing SLES 9 x86_64 GA on x336, x346, and BladeCenter HS20-8843](#).

---

### Monitor and verify CSM and Linux installations

**Note:**
If a System x 360 node previously had an operating system installed, you might see a Virus Warning when installing a new operating system. If a Virus Warning appears on your console, select **Change is expected**. To avoid the warning, see [Disable Virus Detection for x360 nodes](#) (optional).

For full node installations, use the **rconsole** command to view installation progress. To run the **rconsole** command on all the nodes, enter:

```bash
rconsole -a
```

The **rconsole** command displays a console for each node in the cluster.

You can monitor the messages when you boot the node to help identify problems. For example, you might receive the following message that indicates a problem with the MAC address:

```plaintext
Receiving PXE-E51 No dhcp or bootp offers received
```

To check the results of the operating system upgrade, use the **monitorinstall** command, which displays the status of the upgrade for each node. The command displays upgrade progress messages, including one of the following:

- installed
- not installed
- failed install
- install-timedout
- Starting makenode to install CSM RPMs

To run the `monitorinstall` command, enter:

```
monitorinstall
```

The `monitorinstall` command output is similar to:

<table>
<thead>
<tr>
<th>Node</th>
<th>Mode</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>clsn02.cluster.com</td>
<td>Managed</td>
<td>Installed</td>
</tr>
<tr>
<td>clsn03.cluster.com</td>
<td>Managed</td>
<td>Installed</td>
</tr>
<tr>
<td>clsn04.cluster.com</td>
<td>MinManaged</td>
<td>Installed</td>
</tr>
<tr>
<td>clsn05.cluster.com</td>
<td>MinManaged</td>
<td>Installed</td>
</tr>
<tr>
<td>clsn06.cluster.com</td>
<td>MinManaged</td>
<td>Installed</td>
</tr>
<tr>
<td>clsn07.cluster.com</td>
<td>Managed</td>
<td>Installed</td>
</tr>
<tr>
<td>clsn08.cluster.com</td>
<td>PreManaged</td>
<td>Not Installed</td>
</tr>
</tbody>
</table>

All nodes are listed as **Installed** when their installation is complete. Any other status values that appear in the output represent the progress of the installation. Installation errors are indicated with a status code. The nodes will eventually reach the **Installed** state. If the installation times out as a result of using the `installnode -t` command, the status message reads **Install - timedout**.

You can use the `monitorinstall -r` or `-R` flag to get the nodes' installation real time status such as the installation percentage and the RPM name that is being installed. Please see the *CSM Command and Technical Reference Guide* for details.

To continuously display the output of the `monitorinstall` command, enter:

```
watch monitorinstall
```

If there is a problem, see `/var/log/csm/installnode.log` on the management server or `/var/log/csm/install.log` on the managed node for the installation log file.

To check the installation of the managed nodes, you can also use the `lsnode` command, as follows:

```
lsnode -a Mode
```

The `lsnode` command returns a list of the active cluster nodes, along with their `Mode` attributes values. Nodes that were successfully installed are set to **Managed** or **MinManaged**.

To verify that Remote Monitoring and Control (RMC) is working, use the `lsnode` command with the `-H` flag, as follows:

```
lsnode -H -l
```

**Note:**

The `lsnode -H -l` command can only be used for nodes with `Mode` attributes defined as **Managed**. The `lsnode` command retrieves information about the attributes from each node.

To check that `dsh` is working, issue a `dsh` command. For example:

```
dsh -as date
```

A list of the cluster nodes is returned, with a date for each node.
Enable Kerberos Version 5 remote commands for Linux (optional)

To use Kerberos Version 5 for remote command authentication, see Enabling remote commands to use Kerberos Version 5 authentication.

Installing Linux nodes without hardware control

To use CSM to install Linux nodes that will not be configured for hardware control, you must collect the MAC addresses manually, and reboot the nodes manually to do the installation.

The `csmsetupinstall` command cannot automatically collect the node MAC addresses from nodes that are not configured for hardware control. As a result, if you are not using hardware control, you need to manually set the `InstallAdapterMacaddr` and `InstallAdapterName` attributes for each node before you run the `csmsetupinstall` command. Use the `chnode` command to set the attributes. In the following example, `eth1` is the node adapter name, and `00:00:00:00:00:00` is the node MAC address. Ensure that the `InstallAdapterMacaddr` applies to the `InstallAdapterName`, that the adapter is connected to the management server, and that the node can boot from the adapter:

```
chnode hostname InstallAdapterName=eth1 InstallAdapterMacaddr=00:00:00:00:00:00
```

If you are running SLES on a System x (x86) or System p (ppc64) management server, any SOL-enabled BladeCenter nodes (except for the HS20-8678) must be defined with `InstallAdapterName=eth1`.

Finding the MAC address manually: You can find a node adapter name and MAC address by running the `ifconfig` command on the node. If the node is not installed, the MAC address is displayed on the node console when it does a network boot. The adapter name can be any Ethernet adapter that is connected to the management server, but the adapter name must be the name that the system uses, and the MAC address must be the adapter's MAC address. You can also check the BIOS (basic input/output system) for the MAC address. For information about the `ifconfig` command, see the man page. To automatically collect MAC addresses on x445 nodes, with `csmsetupinstall` or `getadapters`, the updated summit kernel must be installed on the CSM management server.

Before running the `installnode` command, set the `PowerMethod` attribute to no value; or run the command with the `--noreboot` flag. The `installnode` command prompts you to manually reboot the nodes after configuring the installation.

Installing Linux on System p and BladeCenter JS nodes

CSM can install Linux on System p and BladeCenter JS (POWER architecture) nodes using two methods. One method is for CSM to use remote console and an `expect` script to direct node open firmware to do a "directed network boot" using the install server. The install server's DHCP server accepts the BOOTP request, and initiates the node installation. The directed boot method is the standard method for System p nodes; use this method if remote console is available. The nodes can be on subnets that are not directly attached to the install server.
The second method of installation does not use remote console. The node does a broadcast network boot that broadcasts its BOOTP request on the entire subnet. The install server's DHCP server on that subnet accepts the BOOTP request for that node, and initiates the node installation. Use the "broadcast boot" method when remote console or remote power is not available on your nodes, or when you want to reboot the System p nodes manually. For this method, the nodes must be on the same subnet as their install server. The "broadcast boot" method of installing BladeCenter JS nodes is only available when using a System p or BladeCenter JS install server, which can be the management server.

Run the following sequence of commands when doing a broadcast boot network installation:

1. Set the InstallAdapterName attribute. For example:
   
   ```bash
   chnode -n nodelist InstallAdapterName=eth0
   ```

2. Set up the node installation, but do not reboot the node yet:
   
   ```bash
   installnode -n nodelist --noreboot
   ```

3. Change the boot order of the nodes to boot from the network. If the node is already managed, run:
   
   ```bash
   rfwcfg -n nodelist --bootseq
   ```

   If the node is not already managed, use SMS menus for System p nodes or the management module for BladeCenter JS nodes to manually set the boot order to network.

4. Reboot the nodes manually, or by running:
   
   ```bash
   rpower -n nodelist reboot
   ```

---

**Customizing kernel module installation on Linux (optional)**

You can override or extend the functions of a kernel driver module by creating a new kernel module. The modules must be placed in `/csminstall/csm/drivers/pm/custom`. They can be backed up using the `csmbackup` command, and restored using the `csmrestore` command. All user provided kernel modules are retained when CSM is updated to a new version. If you create a module with the same name as the file in `/csminstall/csm/drivers/pm`, CSM uses the new module rather than the CSM module.

Three types of kernel driver modules are supported:

1. Individual kernel driver module: the individual kernel driver module is designed to add a driver onto the ramdisk. To use this type of module, you must place the driver in `/csminstall/csm/drivers`. The file name of these kernel modules indicates the driver's name, kernel version and the architecture. The file name must follow this format:

   ```
   drivername [.kernellevel [.arch]].pm
   ```

   Where:

   ```
   drivername
   ```
is the name of the target driver (without suffix). This is a required field. A kernel driver module will be ignored by CSM when CSM cannot find any driver whose name is same as this driver name.

_kernellevel

is the kernel level of this driver. This field begins with an underscore, and is an optional field. If the kernel level is not provided, this kernel driver module will handle this driver for all kernel levels. If the kernel level is provided, the full kernel information is required.

_arch

the architecture of this driver. This field begins with an underscore and is optional. If this field is not provided, this kernel driver module will handle this driver for all architectures.

Naming Examples:

To use the driver bcm5700 with SLES 9 GA, create a kernel module called bcm5700._2.6.5-7.97-default.pm.

To use the driver aic79xx when you install a SLES9 GA i386 node, create a kernel driver module called aic79xx._2.6.5-7.97._i386.pm.

To use the driver a320raid with Red Hat EL 4 GA (32bit and 64bit), create a kernel driver module called a320raid._2.6.9-11.EL.pm.

To use the driver bcm5700 with all systems, create a kernel driver module called bcm5700.pm.

A kernel driver module with more detailed kernel level or architecture information has a higher priority than one with less information. For example, when installing Red Hat EL 4 GA system on a node, if both a320raid._2.6.9-11.EL.pm and a320raid.pm are found, CSM uses a320raid._2.6.9-11.EL.pm.

CSM automatically invokes the post_copy() subroutine in these modules. If the post_copy() subroutine is defined, it runs after the driver has been copied. The following parameters are passed to this subroutine:

- Distribution name
- Distribution version
- Distribution service level
- Distribution architecture
- Source driver directory
- Destination driver directory

The post_copy subroutine must return a 1 when the subroutine runs successfully, it must return a 0 when CSM fails to execute the subroutine. CSM reports an error and exits when the subroutines returns a 0.

2. Final post kernel driver module: CSM provides one post kernel driver module called drivers_post.pm. In this kernel module, the final_post() subroutine is invoked by CSM after CSM handles all drivers. The parameters passed to this subroutine are the same as those passed to the post_copy() subroutine.

You can also create a final post kernel driver module called drivers_post.pm in /csminstall/csm/drivers/pm/custom, containing a final_post() subroutine. If this subroutine exists, it is run after all drivers_post.pm that CSM provides. This allows a user to handle special cases that do not apply to adding a specific driver.
3. AutoYast kernel driver module: You can add drivers to the AutoYast configuration file to force the installation program to load drivers. CSM provides one AutoYast driver module, called `AutoYast_drivers.pm`. In this file, the subroutine, `get_initrd_modules()` is run by CSM when it creates the AutoYast configuration file. The following parameters are passed to this subroutine:
   - Distribution name
   - Distribution version
   - Distribution service level
   - Distribution architecture
   - Hardware type `HWTypeSource` attribute value
   - Model type `HWModel` attribute value

   This subroutine returns a list of comma-separated driver names that are inserted into the AutoYast configuration file.

   You can also create a AutoYast kernel driver module called `AutoYast_drivers.pm` in `/csminstall/csm/drivers/pm/custom` containing a `get_initrd_modules()` subroutine. If this subroutine exists, CSM uses the driver list in `/csminstall/csm/drivers/pm/AutoYast_drivers.pm` and uses this file to get more drivers to insert into `initrd` for the running system.

---

### Provisioning Linux nodes

CSM node provisioning automates the process of detecting, defining, and installing CSM nodes. The `provisionnode` sample script is an example of how to provision a node based on a predefined node profile. The `provisionnode` sample script and README are located in `/opt/csm/samples/install`. You can customize the script for your cluster requirements.

The `provisionnode` script runs on the CSM management server to automatically detect and add nodes to the cluster. The script does the following:

1. Analyzes command parameters and expands node ranges to node names list.
2. Runs `lshwinfo` to query the specified hardware control point to detect new nodes and collect hardware control attributes. For all new nodes returned by `lshwinfo`, the script takes input for the `-n` flag and tries to match a node name to the returned `HWControlNodeId` value; if found, the script uses the attribute values for the node definition. If there is no match, the script assigns node names to the new nodes in order until there are no input node names left. For example, if only one node name is given, and the name does not match any `HWControlNodeId` value, the script only provisions the first new node returned by `lshwinfo`.
3. Creates a `nodedef` file, which includes the default `nodedef` file specified on the command line.
4. Runs `definenode` to define all nodes based on the `nodedef` file created previously.
5. Runs `csmsetupinstall`.
6. Runs `installnode` to install the OS on all nodes.

The `provisionnode` sample script only supports nodes with a `bmc`, `hmc`, or `blade` power method. Before running this sample script, you must create a `nodedef` file containing a default stanza for the `definenode` command. One method is to use the `lsnode` command with the `-F` or `-l` (lowercase L) flags, and redirect the output to a file. For example:

```bash
lsnode -F nodel > node_definition_file
```

---

CSM for AIX and Linux: Planning and Installation Guide
Edit this file to create a generic, default stanza for the type of node to be provisioned, and remove any node-specific attributes. For example:

```plaintext
#---------Example of a nodedef file with default stanza-----------
default:
  InstallAdapterDuplex = half
  InstallAdapterType = ent
  InstallCSMVersion = 1.7.1
  InstallDistributionName = RedHatEL-AS
  InstallDistributionVersion = 4
  InstallMethod = kickstart
  InstallOSName = Linux
  InstallPkgArchitecture = ppc64
  InstallServiceLevel = GA
#-----------------------End of file--------------------------------
```

You can then use this stanza file as input to the `provisionnode` sample script:

```plaintext
provisionnode -f node_definition_file -H hmc1 -p hmc -n node[2-100]
```

Here, the `node_definition_file` is the file name of the `nodedef` file you prepared.

The following syntax and flags are supported by this sample script:

- **Syntax:**
  
  provisionnode [-h] -n node_list -f nodedef_file \n  -H hardware_control_point[,...] -p PowerMethod

- **Flags:**
  
  - **-h**
    Writes the commands' usage statement to standard output.

  - **-n node_list**
    Specifies a comma or space-separated list of node host names, IP addresses, or node ranges to assign to new nodes. Space-separated lists must be inside double quotation marks (" "). For information about specifying node ranges, see the `noderange` man page.

  - **-f nodedef_file**
    Specifies a `nodedef_file` containing default attribute values for defining provisioned nodes.

  - **-H hardware_control_point**
    Specifies a comma-separated list of hardware control points that are queried to detect new nodes.

  - **-p PowerMethod**
    Specifies the power method used to contact the hardware control point. Valid values are: `hmc`, `bmc`, and `blade`.  

---

CSM for AIX and Linux: Planning and Installation Guide
Chapter 15. Secondary adapter interface configuration

CSM supports the configuration of secondary network adapter interfaces during a node installation or when updating a node with the CSM `updatenode -c` command. Secondary adapters are any additional adapters other than those used for remote network node installation.

CSM adapter interface configuration is available for AIX and Linux nodes. On AIX nodes, CSM supports the configuration of Ethernet, IBM High Performance Switch (HPS), InfiniBand, and Multilink adapter interfaces. On Linux nodes, CSM supports the configuration of Ethernet and InfiniBand adapter interfaces.

Configuring secondary adapter interfaces for Linux diskless nodes must be done in the Virtual Node File System. After you have collected the adapter information, see Using Linux diskless nodes.

Support for HPS and Multilink adapters for AIX nodes requires that the nodes be installed with a minimum operating system level of AIX V5.3 with Recommended Maintenance Package 5300-07. Currently HPS is not supported in AIX 6.1.

Configure secondary adapter interfaces

To configure secondary adapter interfaces:

1. **Collect adapter information:**

   The information required to configure adapters must be collected and made available to the configuration scripts that run on the nodes. This information must be provided in an adapter stanza file. Each stanza in the file must contain the information required for a particular adapter. The stanza begins with the name of the node and is followed by a series of lines in `Attribute=value` format. For details on stanza file format, see the `adapterdef` man page or the CSM for AIX and Linux: Command and Technical Reference.

   The `getadapters` command can be used to collect some of the required information and to create an initial version of the stanza file. The `getadapters` command has a number of options, described in the man page and the CSM for AIX and Linux: Command and Technical Reference. For more information on obtaining MAC addresses using the `getadapters` command, see Methods for collecting AIX MAC addresses.

   For example, to get all adapter information from the cluster node `clstrn01` and create a stanza file called `mystanzafile`, issue the following command:

   ```
   getadapters -z /csminstall/tmp/mystanzafile -n clstrn01
   ```

   You must edit the stanza file to add the remaining required information, such as the IP address. If the file contains stanzas for adapters that are used to install the nodes, the files must have the `machine_type` attribute set to `install`. Secondary adapters must have a `machine_type` of `secondary`.
Additional information is required for each adapter stanza; the required attributes for each adapter type are described below.

**Note:**
This information for the install adapter is not used to configure or update the adapter. Install adapters are skipped in the adapter stanza file.

For Linux nodes, you must provide the actual values to add to the network configuration files on each node. This information must be included in the stanza between the `#START_IFCFG` and `#END_IFCFG` tags. These attributes and values must be provided exactly as they should appear in the network configuration files. For example, you might add the following information to the stanza for Red Hat EL nodes:

- `# START_IFCFG`
- `TYPE=Ethernet`
- `BOOTPROTO=static`
- `ONBOOT=yes`
- `DEVICE=eth1`
- `IPADDR=176.60.50.201`
- `NETMASK=255.255.255.0`
- `HWADDR=00:0D:60:14:00:DE`
- `# END_IFCFG`

See [Configuring Ethernet adapters on AIX nodes](#) for more details. For information on required attributes for the network configuration file, see your Linux documentation.

You can also add stanzas for adapter types that are not currently supported by CSM. These stanzas are used by a user-provided configuration method. See [CSM support for user-provided configuration methods](#) for details.

You can create multiple stanza files for different sets of nodes or different types of adapters.

**Note:**
When using the `pxeboot` method to collect adapter information from Linux nodes, set the `GETADAPTERS_TIMEOUT` environmental variable. The value depends on how many types of adapters are installed on the target nodes. For two adapter types, set the variable to a minimum of 120. Add 70 seconds for each additional adapter type; otherwise, the `getadapters` command might not collect all adapter MAC addresses.

For example, before running the `getadapters` command, set this environmental variable to 120:

```
export GETADAPTERS_TIMEOUT=120
```

2. **Store the name of the stanza file in the node definition:**

   The full path name of the stanza file containing secondary adapter information must be saved in the node definition for CSM configuration scripts to access the information. To save the path name, run the `getadapters -W` command to write the full path name of the stanza file to the `AdapterStanzaFile` attribute for each node. If the stanza file contains information for several nodes, each node definition is updated. The command also checks the stanza file for accuracy and completeness. See the `getadapters` man page or the [CSM for AIX and Linux: Command and Technical Reference](#) for details.
For example, to store the full path name of the stanza file created above, issue the following command:

```
getadapters -W -f /csminstall/tmp/mystanzafile
```

To use a different stanza file or change its location, you must run the `getadapters` command again with the new name or location. If you are using HA MS, consider locating the stanza files in a directory that is automatically backed up during a failover.

3. **Configure the adapters:**

After defining the `AdapterStanzaFile` attribute, configure the adapters by either installing the node or by running the `updatenode -c` command.

In either case, the configuration methods that run on the node use the information in the stanza file to configure the adapters. CSM provides default methods for all supported adapter types. CSM also supports user-provided configuration methods, which can be used to override the default CSM method for a particular adapter type, or to support an adapter type that is not currently supported by CSM; see **CSM support for user-provided configuration methods**.

To stop adapter configuration when installing nodes, set the `AdapterStanzaFile` attribute to no value:

```
AdapterStanzaFile=
```

---

**CSM support for user-provided configuration methods**

CSM supports user-provided configuration methods, which can be used to override the default CSM method for a particular adapter type, or to support an adapter type that is not currently supported by CSM. The user-provided method must be created in the `/csminstall/csm/scripts/data` directory on the CSM management server.

The naming convention must be `config_adapters_adapter_type._group`. For example, `config_adapters_ent._LinuxNodes`. The `adapter type` value must match the `adapter_type` attribute value in the stanza. The `adapter_type` can be `ent` (Ethernet), `sni` (switch), `mlt` (multilink), `tok` (token ring), `vi` (VIPA), `iba` (InfiniBand), or a user-provided value for a user-provided method. The `_group` extension is optional.

User-provided scripts must support the `-n node name` and `-f stanza file` flags. The `stanza file` value is the full path name of the stanza file. The `node name` value corresponds to the node name used in the stanza file. The script must parse the stanza file to extract just the adapter information for this node name and the adapter type supported by the script. All other stanzas must be ignored.

The user-provided method is called by the `CSM 001CSM_adapter_config._AllNodes` customization script that runs on the node during a node installation or update. If a user-provided method is provided for a particular adapter type, it is run; if not, the default CSM methods are used. User methods can also be provided for adapter types not currently supported by CSM.

The CSM method for configuring Ethernet adapters on Linux nodes is `/csminstall/csm/scripts/data/CSM_config_adapters_ent._LinuxNodes`. The script can be used as an example for creating user-provided methods.
Setting static routes

CSM provides support for creating simple static routes when configuring the secondary adapters. This may be especially useful if you need to communicate with a remote host either during or immediately after a node installation.

To have the static routes created you must provide the required information with the stanza file "route" attribute. The values for the destination IP address, the destination netmask, and the gateway for individual routes may be specified. They must be in this order and have two colon characters (::) separating them. The syntax for the route attribute is:

route="destination::dest_netmask::gateway, destination::dest_netmask::gateway, ..."

For example, the information for two static routes can be specified as follows:

route="9.1.2.11::255.255.255.0::9.1.2.1, 9.1.2.12::255.255.255.0::9.1.2.1"

To specify values for the destination and dest_netmask only, you could use the colon delimiters as follows: route="9.1.2.11:::9.1.2.1"

Static routes are created whenever the CSM support for secondary adapter configuration is used. This feature is supported for both AIX and Linux nodes. AIX support requires a minimum operating system level of AIX V5.3 with Recommended Maintenance Package 5300-07.

The routes are preserved if the system is rebooted.

On Linux nodes, route configuration files are created. To remove the route, remove the appropriate file. See the Linux network documentation for details on the route files. To remove the route on AIX nodes, use SMIT or the appropriate chdev command.

Additional route setup may be done after the initial installation of the node by using the CSM CFM and dsh support.

Updating the /etc/hosts file with secondary adapter information

If a hostname is provided for the adapter interface then the /etc/hosts file will be automatically updated. The hostname may be specified using the secondary_hostname attribute. For AIX systems the IP address is provided with the netaddr attribute. For Linux systems it is provided by the IPADDR attribute.

When updating /etc/hosts, if the IP address is not already contained in the file then the IP address and hostname will be added. If the IP address already exists in the file, and the hostname is not part of the entry, then the hostname will be added as an alias.

This feature is supported for both AIX and Linux nodes.
Configuration details

The following examples describe how to configure specific types of adapters on AIX and Linux nodes. These examples assume that the secondary adapter configuration will be done after the nodes have already been installed. This is the preferred method in most cluster environments. If you need to do the configuration as part of a node installation, do all the setup before installing the node to do the configuration automatically during the installation process; you would not do the `updatenode` step.

The examples assume you are only configuring one type of adapter at a time; but this is not a requirement. You could, for example, create a stanza file containing Ethernet, HPS, and Multilink adapter information for an AIX node and configure all the adapters in one operation.

Note:
The adapter configuration is done before running any user-provided customization scripts. Therefore, the adapters are available for the user scripts if necessary. The only exception is the switch adapters which require a reboot before the configuration takes effect.

We also provide another method to configure InfiniBand adapters and Multilink adapters on AIX nodes and configure InfiniBand adapters on Linux nodes. It is a sample script, `ibAdapterConfig`, located in `/opt/csm/samples/ib` directory. This method is recommended for the configurations on AIX 5.3.9 or later, AIX6.1.2 or later, Red Hat EL 5.3 and SLES10 SP2.

**Configuring Ethernet adapters on AIX nodes**

To configure Ethernet adapters on AIX nodes:

1. **Run the `getadapters` command to get adapter information and create the stanza file.**

   For example:

   ```
   getadapters -t ent -z /csminstall/tmp/mystanzafile -n .
   ```

   The command searches for Ethernet adapters on node `clstrn01` and puts the results in the stanza file `/csminstall/tmp/mystanzafile`. The contents of the stanza file is similar to:

   ```
   clstr01:  
   machine_type=  
   interface_type=en  
   adapter_type=ent  
   MAC_address=0002556AB19F  
   cable_type=N/A  
   location=U1.9-P2-I2/E1  
   interface_name=  
   netaddr=  
   subnet_mask=  
   ```

   ```
   clstr01:  
   machine_type=  
   interface_type=en  
   adapter_type=ent  
   MAC_address=0002446AB16D  
   cable_type=N/A  
   location= U1.9-P4-I2/E1  
   interface_name=  
   ```

   CSM for AIX and Linux: Planning and Installation Guide
2. Edit the stanza file

Each stanza is required to have the following attributes and values: machine_type, adapter_type, netaddr, subnet_mask, interface_type, location (or interface_name).

For example, after editing the stanza file in the previous step it might contain the following information. Note that the secondary adapter configuration support will only configure the adapter if the machine_type is set to secondary.

```
clstrn01:
    # this is the install adapter
    machine_type=install
    interface_type=en
    adapter_type=ent
    MAC_address=0002556AB19F
    cable_type=N/A
    location=01.9-P2-I2/E1
    interface_name=en0
    netaddr=9.114.113.11
    subnet_mask=255.255.255.0

clstrn01:
    machine_type=secondary
    interface_type=en
    adapter_type=ent
    MAC_address=0002446AB16d
    cable_type=N/A
    location=01.9-P4-I2/E1
    interface_name=en1
    netaddr=9.114.113.9
    secondary_hostname=clstrn01_en1
    subnet_mask=255.255.255.0
```

3. Save the full path name of the stanza file in the node definition

Run the `getadapters` command with the `-W` flag:

```
getadapters -W -f mystanzafile
```

CSM calculates the full path name and store it in the `AdapterStanzaFile` attribute of the node definitions. It also checks the stanza file for errors.

4. Configure the adapters.

Run the `updatenode` command with the `-c` option:

```
updatenode -c -n clstrn01
```

The CSM code that runs on the node calls a configuration method, which is provided by AIX, to configure the adapters. It is not necessary to reboot the node for the adapter configuration to take effect.
Configuring HPS and Multilink adapters on AIX nodes

IBM High Performance Switch (HPS) and Multilink adapter configuration is limited to the `updatenode -c` flag only. You cannot configure these adapters during a node installation. To configure an HPS switch and Multilink adapters on AIX nodes:

1. **Run the getadapters command to collect adapter information and create the stanza file.**

   For example:
   
   ```
   getadapters -t sni -z /csminstall/tmp/mystanzafile -n clstrn01
   ```

   This will look for HPS adapters on node `clstrn01` and put the results in the stanza file `/csminstall/tmp/mystanzafile`. If a switch adapter is found then a Multilink adapter stanza will also be created.

   The contents of the stanza file would look like the following:

   ```
   clstrn01:
   
machine_type=secondary
interface_type=sn
adapter_type=sni
interface_name=
location=UP8.23-P3-H3/W4
netaddr=
subnet_mask=
   
   clstrn01:
   
machine_type=secondary
interface_type=mlt
adapter_type=mlt
netaddr=
subnet_mask=
   ```

2. **Edit the stanza file.**

   Each stanza is required to have the following attributes and values:

   - **HPS (sni):** `machine_type`, `adapter_type`, `interface_type`, `netaddr`, `subnet_mask`, `location` (or `interface_name`). If the system tunables are not set appropriately then add the `cust_preconfig` and/or `bos_preconfig` attributes. The critical tunable values are indicated in the example below.

   - **Multilink (ml):** `machine_type`, `adapter_type`, `interface_type`, `netaddr`, `subnet_mask`.

   For example, after editing the stanza file, the file is similar to:

   ```
   clstrn01:
   
machine_type=secondary
interface_type=sn
adapter_type=sni
interface_name=sn0
location=UP8.23-P3-H3/W4
netaddr=9.53.153.235
subnet_mask=255.255.255.0
   #both cust_preconfig and bos_preconfig can be included in one stanza
   #cust_preconfig is used when updating the node
   ```
#bos_preconfig is used when installing the node
cust_preconfig="vmo -r -o v_pinshm=1 -o lgpg_size=16777216 -o
lgpg_regions=64"
bos_preconfig="tunchange -f nextboot -t vmo -o lgpg_size=16777216 -o
lgpg_regions=64"
clstrn01:
    machine_type=secondary
    interface_type=ml
    adapter_type=mlt
    interface_name=ml0
    netaddr=9.53.154.135
    subnet_mask=255.255.255.0

3. **Save the full path name of the stanza file in the node definition.**

    Run the **getadapters** command with the **-W** flag:

    ```
    getadapters -W -f mystanzafile
    ```

    CSM calculates the full path name and store it in the *AdapterStanzaFile* attribute of the node definitions. It also checks the stanza file for errors.

4. **Configure the adapters.**

    Run the **updatenode** command with the **-c** flag:

    ```
    updatenode -c -n clstrn01
    ```

    The CSM code that runs on the node calls a configuration method which is provided by AIX.

5. **Reboot the nodes.**

    Run the **rpower** command. The nodes must be rebooted for the configuration to complete:

    ```
    rpower -n clstrn01 reboot
    ```

**Configuring Ethernet adapters on Linux nodes**

To configure Ethernet adapters on Linux nodes:

1. **Run getadapters to get the adapter information and create the stanza file.**

    For example:

    ```
    getadapters -t ent -z /csminstall/tmp/mystanzafile -n clstrn01
    ```

2. **This command looks for Ethernet adapters on node clstrn01 and puts the results in the stanza file.**

    ```
    /csminstall/tmp/mystanzafile
    ```

    Stanzas in the file are similar to:

    ```
    clstrn01:
        machine_type=
    ```
3. **Edit the stanza file**

Each stanza is required to have the following attributes and values: machine_type, adapter_type, MAC_address, and interface_name.

In addition the attributes and values to use in the Linux ifcfg* network adapter configuration file on the node must be included. The actual attributes that are needed vary depending on the distribution, the distribution version and the configuration options you choose. Refer to the appropriate Linux distribution documentation for details. For Red Hat EL nodes, the attributes shown in the example below provide basic adapter configuration. For SLES nodes, use BOOTPROTO, BROADCAST, IPADDR, NETMASK, and STARTMODE.

Optionally, route and device driver information may be included.

**Note:**
CSM creates an ifcfg-interface and optionally an ifcfg-interface file for each adapter interface and then run the ifup command. It would be advisable to manually create these files for one adapter on a single node and test the configuration to make sure it works as desired before doing the adapter configuration for multiple nodes and adapters.

For example, an edited Red Hat EL stanza file is similar to:

```bash
clstrn01.clusters.com:
  machine_type=install
  MAC_address=00:0D:60:14:00:DF
  interface_name=eth0
  adapter_type=ent
  # START_IFCFG
  # END_IFCFG

clstrn01.clusters.com:
  machine_type=secondary
  MAC_address=00:0D:60:14:00:DE
  interface_name=eth1
  adapter_type=ent
  route=9.1.2.11::255.255.255.0::9.1.2.1
  secondary_hostname=clstrn01-net2.clusters.com
  # START_IFCFG
  TYPE=Ethernet
  BOOTPROTO=static
  ONBOOT=yes
  DEVICE=eth1
  IPADDR=176.60.50.201
```

CSM for AIX and Linux: Planning and Installation Guide
4. **Save the full path name of the stanza file in the node definition.**

Run the `getadapters` command with the `-W` flag:

```
getadapters -W -f mystanzafile
```

CSM calculates the full path name and stores it in the `AdapterStanzaFile` attribute of the node definitions. CSM also checks the stanza file for errors.

5. **Configure the adapters.**

Run the `updatenode` command with the `-c` flag:

```
updatenode -c -n clstrn01
```

It is not necessary to reboot the node. CSM automatically runs the `ifup` command on the node to configure the adapters.

### Configuring InfiniBand adapters on AIX nodes

The `getadapters` support for gathering InfiniBand adapter information on AIX nodes is only provided through the `dsh` collection method. Also, the configuration of InfiniBand adapters on AIX systems is only supported by using the `updatenode` command with the `-c` flag. It is not supported as part of a node operating system installation.

1. **Run the `getadapters` command to get the adapter information and create the stanza file.** For example, to get all the InfiniBand adapter information from the AIX node `clstrn01` and create a stanza file called `mystanzafile`, issue the following command:

```
getadapters -m dsh -t iba -z /csminstall/tmp/mystanzafile -n clstrn01
```

In this example the `dsh` method and the adapter type (`iba`) are specified. The contents of a stanza could look like the following.

```
clstrn01.clusters.com:
  machine_type=secondary
  adapter_type=iba
  interface_name=ib0
  netaddr=
  subnet_mask=
  ib_adapter=
  ib_port=
  mtu=
  p_key=
  srq_size =
```

2. **Edit the stanza file.** Each stanza is required to have the following attributes and values: `machine_type`, `adapter_type`, `interface_name`, `netaddr`, `subnet_mask`, `ib_adapter`, and `ib_port`. For example, your edited stanza file could contain the following information:
To define additional interfaces for an InfiniBand adapter, just add additional stanzas. For example, to define a second interface for adapter iba0 using port 2 you could create the following stanza:

```
clstrn01.clusters.com:
    machine_type=secondary
    adapter_type=iba
    interface_name=ib1
    netaddr=9.53.153.237
    subnet_mask=255.255.255.0
    ib_adapter=iba0
    ib_port=2
    mtu=
    p_key=
    srq_size =
```

3. **Save the full path name of the stanza file in the node definition.** Run the `getadapters` command with the `-W` flag:

   ```bash
   getadapters -W -f mystanzafile
   ```

   CSM calculates the full path name and stores it in the `AdapterStanzaFile` attribute of the node definitions. CSM also checks the stanza file for errors.

4. **Configure the adapters.** Run the `updatenode` command with the `-c` flag:

   ```bash
   updatenode -c -n clstrn01
   ```

5. **Check the status of the InfiniBand interfaces.** For example:

   ```bash
   csmstat -s Status,Network-Interfaces -n clstrn01
   ```

### Configuring InfiniBand adapters on Linux

The following procedure for configuring InfiniBand adapters on Linux is supported for SUSE Linux Enterprise Server (SLES) 9, Service Pack 3 nodes only. This CSM support automates the procedure documented in the IBM clusters with the InfiniBand switch README, which is available at [http://www14.software.ibm.com/webapp/set2/sas/f/networkmanager/home.html](http://www14.software.ibm.com/webapp/set2/sas/f/networkmanager/home.html). The README includes the latest information pertaining to InfiniBand configuration and software and hardware requirements; review the README file before using the CSM procedure documented below.

CSM provides the `/csminstall/esm/scripts/data/CSM_config_adapters_iba_LINUXNodes` adapter configuration method for configuring InfiniBand interfaces in the supported environment. If your
environment is not supported, you can modify the method to meet your requirements, or use it as model for a user-provided method. See CSM support for user-provided configuration methods for details.

To configure InfiniBand adapters on SLES 9, you must use the `updatenode -c` command; you cannot configure InfiniBand adapters during node installation.

**Note:**

In the following procedure, **Step 4** creates an adapter stanza file containing the information required to configure adapter interfaces. This step is time consuming, particularly if you are configuring a large number of interfaces. However, if you can use a specific naming convention and accept some basic assumptions, you can automate this step using the `mkLinuxIBstanzas` sample script. The `mkLinuxIBstanzas` script is provided for creating an adapter stanza file that is typical of some large cluster environments. Before beginning the procedure described below, read the `mkLinuxIBstanzas.README` to see if you can use the sample script for your environment. The script and the README are located in `/opt/csm/samples/install` on your CSM management server. You can also modify the `mkLinuxIBstanzas` sample script to meet your requirements.

To configure InfiniBand adapters on your SLES 9 nodes:

1. **Check SLES version:**

   Check the version of SLES running on the nodes; it must be SLES 9, Service Pack 3. The kernel level for Service Pack 3 is 2.6.5-7.244-pseries64. Run the following command to return the kernel level installed on your SLES nodes:

   ```
dsh -N ppcSLES9Nodes uname -r
   ```

   Any nodes not installed with kernel level 2.6.5-7.244-pseries64 are not supported.

2. **Download SLES 9 prerequisites:**

   Download SLES prerequisites from the Novell Web site, at https://you.novell.com/update/ppc/update/SUSE-SLES/9/PTF. You must register for a login ID and password for the Novell Web site, at http://support.novell.com/linux/registration/. After logging in, download the following packages:

   - glibc version 2.3.3-98.66
   - glibc PTFkey-install.sh patch
   - openib package openib-0058-gen2.sles9sp3.ppc.tar.gz.

3. **Install SLES 9 prerequisites:**

   Install the glibc and openib packages using CSM Software Maintenance System (SMS), and install the glibc PTFkey-install.sh patch using `dcp` and `dsh`, as follows:

   a. Follow the directions on the Novell Web site to prepare the `PTFkey-install.sh` patch.
   b. Copy the `PTFkey-install.sh` patch and the new glibc RPMs to the SMS subdirectory `/csminstall/Linux/SLES/9/ppc64/updates`.
   c. Copy the openib tar file to the SMS subdirectory `/csminstall/Linux/SLES/9/ppc64/install`.
   d. Extract the openib RPMs from the tar file:

   ```
gzip -d openib-0058-gen2.sles9sp3.ppc.tar.gz
tar -xvf openib-0058-gen2.sles9sp3.ppc.tar
   ```
e. Copy the **glibc** patch to the nodes:

   dcp -N ppcSLES9Nodes /csminstall/Linux/SLES/9/ppc64/updates\
   /PTFkey-install.sh /tmp

f. Run the **glibc** patch script on the nodes:

   dsh -N ppcSLES9Nodes /tmp/PTFkey-install.sh

g. Run the **smsupdatenode** command to upgrade the node software:

   smsupdatenode -N ppcSLES9Nodes

h. Reboot the nodes using the **rpower** command:

   rpower -N ppcSLES9Nodes reboot

4. Create InfiniBand adapter stanza file:

Create an adapter stanza file for InfiniBand adapter configuration. This stanza file is used by a CSM method (script) that runs on the nodes to configure InfiniBand adapters.

**Note:**
See the /opt/csm/samples/install/mkLinuxIBstanzas.README file for details on automating this step. If your environment is set up using conventions assumed by the mkLinuxIBstanzas script, you can create the stanza file by running the mkLinuxIBstanzas -N ppcSLES9Nodes -z IBstanzafile command. You can also modify the mkLinuxIBstanzas script to meet your requirements.

Configuring InfiniBand interfaces requires completing the following tasks on each node:

- Setting TCP/IP tunable values
- Performing device driver module configuration
- Creating an IP configuration file for each InfiniBand interface.

You can add the information required to complete these tasks to a stanza file, using three sets of tags to mark the beginning and end of each section:

- Add TCP/IP setting information between the #START_TCPIP and #END_TCPIP tags; any information placed between these tags is used to update the /etc/sysctl.conf file on SLES 9 nodes.
- Add device driver module configuration information between the #START_MOD and #END_MOD tags; this information is used to update the /etc/modprobe.conf.local file on SLES 9 nodes.
- Add IP configuration information between the #START_IFCFG and #END_IFCFG tags; this information is used to create a new /etc/sysconfig/network/ifcfg-interface_name file on SLES 9 nodes.

Each adapter interface must also have values defined for the **machine_type**, **adapter_type** and **interface_name** attributes. For InfiniBand interfaces, set **machine_type** to **secondary** and **adapter_type** to **iba**. Each unique interface, **ib0** and **ib1** for example, must be represented by its own stanza.
If you have common values for multiple adapter interfaces, you can add these values to a default stanza at the beginning of the file. If the value is unique for a specific interface, it must be added to the interface-specific stanza. See the `adapterdef` man page for details on creating an adapter stanza file.

For example, to configure `ib0` on nodes `clsn01` and `clsn02`, create a stanza file similar to:

```plaintext
default:
  # required CSM attributes
  machine_type=secondary
  adapter_type=iba
  #ipoib tuning
  # START_TCPIP
  net.ipv4.conf.default.arp_ignore = 2
  net.ipv4.conf.default.arp_filter = 1
  net.ipv4.tcp_wmem = 32768 131072 524288
  net.ipv4.tcp_rmem = 32768 131072 524288
  net.core.wmem_max = 1048576
  net.core.rmem_max = 1048576
  # END_TCPIP
  # device driver module configuration
  # START_MOD
  options hcad_mod nr_ports=2 port_act_time=120
  options ib_ipoib send_queue_size=1024 recv_queue_size=1024
  # END_MOD
  # Configuration file information
  #START_IFCFG
  BOOTPROTO='static'
  STARTMODE='onboot'
  #END_IFCFG
  clsn01:
    interface_name=ib0
    # START_IFCFG
    BROADCAST='102.168.8.255'
    IPADDR='102.168.8.1'
    NETMASK='255.255.255.0'
    NETWORK='102.168.8.0'
    # END_IFCFG
  clsn02:
    interface_name=ib0
    # START_IFCFG
    BROADCAST='102.168.8.255'
    IPADDR='102.168.8.2'
    NETMASK='255.255.255.0'
    NETWORK='102.168.8.0'
    # END_IFCFG

Note: To check if the values listed in this example are correct for your environment, see the IBM clusters with the InfiniBand switch README, which is available at http://www14.software.ibm.com/webapp/set2/sas/f/networkmanager/home.html. For example, if your cluster has more than 32 nodes, set the `send_queue_size` and `recv_queue_size` values to 2048.

5. Define the `AdapterStanzaFile` attribute:

Save the stanza file name by setting the `AdapterStanzaFile` attribute to the full path name of the adapter stanza file. The attribute value is defined for each node in the stanza file. For example:
getadapters -W -f mystanzafie

The command stores the full path name in each node definition, and also checks the stanza file for the required attribute values.

6. Configure InfiniBand adapter interfaces:

Configure the InfiniBand adapter interfaces by running the updatenode -c command. For example:

updatenode -c -N ppcSLES9Nodes

7. Reboot the nodes:

Reboot the nodes using the rpower command. For example:

rpower -N ppcSLES9Nodes reboot

8. Check interface status:

Check the status of your InfiniBand interfaces using the csmstat command. For example:

csmstat -s Status,Network-Interfaces -N ppcSLES9Nodes

You can take additional steps to verify the configuration; see the IBM clusters with the InfiniBand switch README for details, at http://www14.software.ibm.com/webapp/set2/sas/f/networkmanager/home.html.

Configuring InfiniBand adapters using script ibAdapterConfig

The ibAdapterConfig script is used to do secondary adapter configuration for InfiniBand interfaces (ibX) and ml0 on AIX and InfiniBand interfaces (ibX) on Linux MNs. It should be run on CSM Managed Nodes, so the user needs to use dcp/scp/rcp to copy this sample script to the target nodes before running it by dsh.

1. Edit the /etc/hosts file. To use this script, the IP address entries for IB interfaces in /etc/hosts on CSM MNs should have the node hostname and the unique IB interface name in them. The format should be <ip_address_for_this_ib_interface node_hostname-ib_interfacename >.

For example:
192.168.8.165    c890f11ec05-ib0

One IB adapter has two ports, we will use the first port to the first interface, and second port to the second interface. Please see the detail relationship in below table:

<table>
<thead>
<tr>
<th>Interface Name</th>
<th>Adapter Name</th>
<th>Port Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>ib0</td>
<td>iba0/ehca0</td>
<td>1</td>
</tr>
<tr>
<td>ib1</td>
<td>iba0/ehca0</td>
<td>2</td>
</tr>
<tr>
<td>ib2</td>
<td>iba1/ehca1</td>
<td>1</td>
</tr>
<tr>
<td>ib3</td>
<td>iba1/ehca1</td>
<td>2</td>
</tr>
<tr>
<td>......</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
2. **Run the ibAdapterConfig script.** ibAdapterConfig script could get its hostname and greps for that string in /etc/hosts file to get the corresponding ibX interfaces and its IP addresses. Since the netmask could be not found in /etc/hosts file, so the user needs to specify the netmask value in command line with -m flag.
Chapter 16. CSM post-installation tasks

CSM post-installation tasks include verifying the CSM installation, setting up nodes for Kerberos Version 5, and using installation and configuration log files. For additional CSM administration tasks, see the CSM for AIX and Linux: Administration Guide.

Verifying CSM installation

After CSM installation is completed, remote RMC and CSM commands are enabled. To verify that the installation was successful, follow the directions in this task. You can use `telnet` to access the nodes, or you can use `ssh` or `rsh` depending on the remote shell settings of the cluster; see Automatic setup of rsh and OpenSSH for more information.

Logging onto Linux nodes

You can use `telnet` to access the nodes, or you can use `ssh` or `rsh` depending on the remote shell settings of the cluster. See Automatic setup of rsh and OpenSSH.

To log on to your Linux nodes using `ssh` or `rsh`:

1. Log in as `root`.
2. Enter `cluster` as the password. This password is set by default.

To log on to your Linux nodes using `telnet`:

1. Log in as `admin`.
2. Enter `cluster` as the password. This password is set by default for both the `admin` and `root` user.
3. Switch user to `root` (`su - root`).

The example shows the CSM defaults for userid and password. For security, your administrator needs to change the defaults. The user IDs and passwords are set in the Kickstart configuration file or the AutoYaST configuration file.

Verifying that dsh is working on the nodes

To verify that `dsh` is working on all of the nodes, run the `dsh` command with the `date` option, as follows:

```
dsh -as date
```

A list of nodes with the date on each node is returned. To interpret alternate output, see the diagnostics information in the CSM for AIX and Linux: Administration Guide.
Checking the status of the nodes

To see the status of all the Linux nodes, you can use the `monitorinstall`, `lsnode`, or `nodegrp` command. To use the `monitorinstall` command, enter:

```
monitorinstall
```

The `monitorinstall` command writes output similar to:

<table>
<thead>
<tr>
<th>Node</th>
<th>Mode</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>clsn02.cluster.com</td>
<td>Managed</td>
<td>Installed</td>
</tr>
<tr>
<td>clsn03.cluster.com</td>
<td>Managed</td>
<td>Installed</td>
</tr>
<tr>
<td>clsn04.cluster.com</td>
<td>MinManaged</td>
<td>Installed</td>
</tr>
<tr>
<td>clsn05.cluster.com</td>
<td>MinManaged</td>
<td>Installed</td>
</tr>
<tr>
<td>clsn06.cluster.com</td>
<td>MinManaged</td>
<td>Installed</td>
</tr>
<tr>
<td>clsn07.cluster.com</td>
<td>Managed</td>
<td>Installed</td>
</tr>
<tr>
<td>clsn08.cluster.com</td>
<td>PreManaged</td>
<td>Not Installed</td>
</tr>
</tbody>
</table>

All nodes are listed as *Installed* when their installation is complete. Any other status values that appear in the output represent the progress of the installation. Installation errors are indicated with a status code. The nodes will eventually reach the *Installed* state.

For AIX or Linux nodes, if the installation hangs for a long time, the node's status changes to *Install - timedout*. If this change occurs, look at the node's console to see why it is hanging. Then fix the problem and reinstall.

To see the installation status of any of the nodes in your cluster using the `lsnode` command, enter:

```
lsnode -a Mode
```

The result shows you the *Mode* of each node. The mode for all the nodes is *Managed* or *Premanaged*.

To return the managed nodes using the `nodegrp` command, enter:

```
nodegrp ManagedNodes
```

The command displays a list of all the cluster nodes that are set to *Mode=Managed*; the defined and installed nodes.

Verifying the power status of the nodes

This step should only be performed if you have hardware control enabled on your system. To verify the power status of the nodes (whether they are on or off), enter:

```
rpower -a query
```

A list of nodes with their associated power state is returned.

Verifying reachability of the nodes

To verify whether the nodes are reachable, enter:
The current accessibility status of the node is returned. Accessibility is defined as the ability to successfully communicate with the RMC subsystem on the node.

**Listing predefined conditions, responses, and dynamic node groups**

CSM provides a set of predefined conditions, responses, and dynamic node groups. To see a list of the predefined conditions, use the RSCT `lscondition` command as follows:

```
lscondition
```

To see a list of the predefined responses, use the RSCT `lsresponse` command as follows:

```
lsresponse
```

To see a list of the predefined condition/response pairs, use the `lscondresp` command, as follows:

```
lscondresp
```

To see a list of the predefined dynamic node groups use the `nodegrp` command, as follows:

```
odegrp
```

---

**Enabling remote commands to use Kerberos Version 5 authentication**

Ensure that you have set up Kerberos and have specified the necessary Kerberos options for the managed nodes. For AIX, see Install Kerberos Version 5 for CSM for AIX remote commands and Set up Kerberos Version 5 for CSM for AIX remote command processing (optional). For Linux, see Set up Kerberos Version 5 for remote Linux command processing (optional).

**Enabling rsh for Kerberos authentication on AIX**

To enable `rsh` for authentication using Kerberos 5 authentication, run the `chauthent` command on the AIX management server and AIX managed nodes.

Do not issue `chauthent` without any flags; this disables remote command authentication and processing such as `telnet`. For information about the AIX `chauthent` command, see the `AIX Version 5.2 Security Guide` or the command man page.

To display AIX authentication options, run the `lsauthent` command. The command returns information to indicate if standard AIX authentication (`-std`), Kerberos authentication (`-k5`), or both, are being used.

CSM only sets up the CSM principal that is required by the CSM scripts to run remote commands in a Kerberos environment. You must set up all other users, including `root`, and ensure the following conditions before removing standard authentication and changing to Kerberos-only authentication:

- All users running remote commands on the node, including `root`, have a valid Kerberos principal.
- The principal name is in the `.k5login` file, in the user's home directory on the node.
To obtain valid Kerberos credentials, users can run the Kerberos `kinit` command. Once users are authenticated, they can issue the `klist` command to check their Kerberos credentials; see the *AIX Commands Reference* or the man page for details.

**To enable Kerberos Version 5 and AIX standard authentication:**

1. Issue the following command on the management server and the managed nodes to set the remote command to both Kerberos Version 5 and standard authentication:

   ```
   chauthent -k5 -std
   ```

   This command allows CSM to authenticate first with Kerberos Version 5. If that fails, CSM uses standard authentication (through the `.rhosts` file).

2. To test that the user is set up properly, run the following command to a managed node:

   ```
   dsh -n nodename date
   ```

   If you do not receive a Kerberos warning message, Kerberos remote commands processing is set up properly for the user.

**To set up only for Kerberos Version 5 remote command authentication (optional)**

1. On both the management server and the managed node, run the following command to set up only for Kerberos Version 5 remote command authentication:

   ```
   chauthent -k5
   ```

2. Remove the `.rhosts` file on each managed node. If you are running `rsh/rcp`, to ensure that CSM does not recreate the `.rhosts` file, issue the following command on the management server:

   ```
   csmconfig SetupRemoteShell=0
   ```

At this point, the management server is set to use both Kerberos Version 5 and standard authentication for remote commands. Remote command processing attempts first to use Kerberos 5 authentication and if that fails, standard AIX authentication. If a managed node is set to use Kerberos Version 5 authentication only and the attempt to use Kerberos Version 5 authentication fails, the remote command fails.

**Considerations:** Situations exist where standard authentication must be enabled on the management server. For example, when you use NIM for AIX installation, you must have standard authentication enabled on both the management server and on the node that NIM is installing. You can enable standard authentication to the management server and the managed node for the duration of the NIM work and remove the standard authentication when the NIM work is complete.

Consider the following when you enable then disable standard authentication:

- If the root `.rhosts` file on the managed node is removed, you must recreate it.
- If you have some managed nodes that have not been setup to use Kerberos, they continue to use standard authentication. In this case, do not remove standard authentication from the management server.
- When a new node is being added to the cluster, the `updatenode` command uses standard authentication for processing. You must ensure that standard authentication is enabled so that `updatenode` can perform the Kerberos setup.
- If standard authentication is temporarily required to use NIM or while `updatenode` completes Kerberos setup, you can enable the management server for Kerberos Version 5 and standard authentication. To use NIM when the root `.rhosts` file on the managed node has been removed, or if `csmconfig SetupRemoteShell=0`, you must also create the root `.rhosts` file on the managed node.
- To set the management server to use only Kerberos Version 5 authentication, enter:

  ```
  chauthent -k5
  ```

**Enabling rsh for Kerberos Version 5 authentication on Red Hat EL nodes**

You can enable `rsh` remote command usage of Kerberos authentication for Red Hat EL. Perform the following steps on the Red Hat EL management server and managed nodes as follows:

1. On the managed node, locate the `kshell` configuration file in the following directory:

   ```
   /etc/xinetd.d/
   ```

2. Edit the file as follows:

   ```
   service kshell
   {
     flags       = REUSE
     socket_type = stream
     wait        = no
     user        = root
     server      = /usr/kerberos/sbin/kshd
     server_args = -5
     disable     = no
   }
   ```

   For CSM use of Kerberos authorization to work, ensure that `-e` is deleted from `server_args` in the file; this option requires encryption, which is not supported by CSM.

3. Run the following command on the managed node:

   ```
   /sbin/service xinetd restart
   ```

4. To direct CSM to use the Kerberos enabled version of `rsh` for Linux nodes, run the following command on the management server:

   ```
   csmconfig RemoteShell=/usr/kerberos/bin/rsh
   ```

5. To enable root use of `dsh` using Kerberos, add the root user's principal to the `.k5login` file in the root user's home directory.

**Disabling standard authentication:** To remove standard authentication for a Linux node, you need to remove the `.rhosts` file in the home directory of all users. If you are running `rsh/rcp`, ensure that CSM does not recreate the `.rhosts` file of root, issue the following command on the management server:

```
csmconfig SetupRemoteShell=0
```
Enabling rsh for Kerberos Version 5 authentication on SLES nodes

You can enable rsh usage of Kerberos authentication for distributions using the heimdal Kerberos implementation on the management server and managed nodes as follows:

1. On the managed node, ensure that the xinetd RPM is installed.
2. Create a kshell configuration file in the /etc/xinetd.d directory with the following contents:

   ```
   service kshell
   {
   flags=EUSE
   socket_type=stream
   wait=no
   user=root
   server=/usr/lib/heimdal/sbin/rshd
   server_args=-k
   disable=no
   }
   ```

3. Run the following command on the managed node to start rshd:

   ```
   /etc/init.d/xinetd restart
   ```

4. On the Linux management server, direct CSM to use the Kerberos version of rsh:

   ```
   csmconfig RemoteShell=/usr/lib/heimdal/bin/rsh )
   ```

5. Optional: enable root use of dsh using Kerberos, add the root user's principal to the .k5login file in the root user's home directory.

Disabling standard authentication: To remove standard authentication for a Linux node, you need to remove the .rhosts file in the home directory of all users. If you are running rsh/rcp, to ensure that CSM does not recreate the .rhosts file of root, issue the following command on the management server:

   ```
   csmconfig SetupRemoteShell=0
   ```

Enabling ssh for Kerberos Version 5 authentication

AIX includes Kerberos-enabled OpenSSH. By default, if Kerberos is configured in the sshd_conf file, the ssh command attempts to use Kerberos for authentication. If authentication fails, ssh attempts to use other methods of authentication.

To configure ssh to use Kerberos on each managed node, do the following:

1. Stop the ssh server.

   ```
   stopsrc -g ssh
   ```

2. On each managed node, edit the /etc/ssh/sshd_conf file to contain the following lines:

   ```
   KerberosAuthentication yes
   KerberosTicketCleanup yes
   GSSAPIAuthentication yes
   ```
3. To start the ssh server daemon, on the SSH server, run the `startsrc -g ssh` command.

4. (Optional) To enable root use of dsh using Kerberos, add the root user's principal to the `.k5login` file in the root user's home directory.

To enable ssh usage of Kerberos authentication on Linux nodes, you must obtain or build Kerberos enabled ssh packages for your distribution.

To disable authentication methods other than Kerberos, remove the associated configuration files from the managed nodes. Check for the following methods that CSM sets up. You might have others in your configuration that you need to consider:

- The authorized keys files in the `.ssh` subdirectory of the home directory of the root. These files are automatically created when you add a node to the cluster through the `updatenode` command and the general CSM installation process.
- To ensure that CSM does not transfer the authorized key files, issue the following command on the management server:

  ```
csmconfig SetupRemoteShell=0
  ```

### Enabling standard AIX remote command authentication

On AIX, after you disable std authentication and enable only Kerberos authentication, you might need to reenable standard authentication. For example, the following tasks require subsequently reenabling standard authentication:

- Using NIM to perform software maintenance.
- Changing the management server hostname.
- Changing the host principal password for a managed node.

On both the management server and the nodes, perform the following steps. For Linux nodes, follow the directions for setting up the `.rhosts` files, but do not use `lsauthent` or `chauthent`.

1. Issue the `lsauthent` command to determine the current authentication setting for the AIX nodes.
2. On the target nodes, examine the `.rhosts` file of the root. If the authentication methods contain standard AIX authentication, and the `.rhosts` file allows access by root, standard authentication is set up. If the response does not include Standard AIX, continue with the following steps to add standard authentication.
3. On the management server and on the target AIX nodes, issue the `chauthent` command to add standard authentication to the available authentication methods as follows

  ```
  chauthent -k5 -std
  ```

4. On the target nodes, create or update the `.rhosts` file in the home directory of the root user. The file must allow access by root.
5. To test the setup, use the `kdestroy` command to remove any Kerberos tickets.
6. Issue the following, where `target_node` is the target node in the cluster:

  ```
dsh -n target_node date
  ```
Using installation and configuration log files

Several installation commands create log files, which are placed in the `/var/log/csm` directory. These log files contain extended error and informational messages.

The following log files are created:

### Table 85. Installation log files on the management server

<table>
<thead>
<tr>
<th>Command</th>
<th>Log file</th>
</tr>
</thead>
<tbody>
<tr>
<td>copycds</td>
<td>/var/log/csm/copycds.log</td>
</tr>
<tr>
<td>copycsmpkgs</td>
<td>/var/log/csm/copycsmpkgs.log</td>
</tr>
<tr>
<td>csm2nimgrps</td>
<td>/var/log/csm/csm2nimgrps.log</td>
</tr>
<tr>
<td>csm2nimnodes</td>
<td>/var/log/csm/csm2nimnodes.log</td>
</tr>
<tr>
<td>csmsetupinstall</td>
<td>/var/log/csm/csmsetupinstall.log</td>
</tr>
<tr>
<td>csmsetupnim</td>
<td>/var/log/csm/csmsetupnim.log</td>
</tr>
<tr>
<td>getadapters</td>
<td>/var/log/csm/getadapters/getadapters.log and, for openfirmware mac method only, /var/log/csm/getadapters/getadapters.node_hostname.log, julian_date</td>
</tr>
<tr>
<td>getuuid</td>
<td>/var/log/csm/getuuid.log</td>
</tr>
<tr>
<td>installms</td>
<td>/var/log/csm/installms.log</td>
</tr>
<tr>
<td>installnode</td>
<td>/var/log/csm/installnode.log, /var/log/csm/nodestatusd.log and, for System p and BladeCenter JS nodes only, /var/log/csm/installnode.node_hostname.log, julian_date</td>
</tr>
<tr>
<td>netboot</td>
<td>/var/log/csm/netboot/node_hostname.log, julian_date (AIX nodes only)</td>
</tr>
<tr>
<td>nodeset</td>
<td>/var/log/csm/nodeset.log</td>
</tr>
<tr>
<td>updateisvr</td>
<td>/var/log/csm/updateisvr.log</td>
</tr>
<tr>
<td>updatenode</td>
<td>/var/log/csm/updatenode.log</td>
</tr>
</tbody>
</table>

### Table 86. Installation log files on install servers

<table>
<thead>
<tr>
<th>Command</th>
<th>Log file</th>
</tr>
</thead>
<tbody>
<tr>
<td>csmsetupinstall</td>
<td>/var/log/csm/nodeset.log, /var/log/csm/install.log</td>
</tr>
<tr>
<td>getadapters</td>
<td>/var/log/csm/nodeset.log</td>
</tr>
<tr>
<td>getuuid</td>
<td>/var/log/csm/nodeset.log</td>
</tr>
<tr>
<td>installnode</td>
<td>/var/log/csm/installnode.log, /var/log/csm/nodestatusd.log, /var/log/csm/nodeset.log</td>
</tr>
<tr>
<td>nodeset</td>
<td>/var/log/csm/nodeset.log</td>
</tr>
<tr>
<td>updatenode</td>
<td>/var/log/csm/install.log, /var/log/csm/nodestatusd.log</td>
</tr>
</tbody>
</table>

### Table 87. Installation log files on nodes
<table>
<thead>
<tr>
<th>Command</th>
<th>Log file</th>
</tr>
</thead>
<tbody>
<tr>
<td>The <strong>updatenode</strong> and <strong>installnode</strong> commands and the NIM install result in data being written to this log</td>
<td>/var/log/csm/install.log</td>
</tr>
</tbody>
</table>

**Remote console log and trace files:** By default, the `rconsole` command uses the conserver tool to open remote console sessions. The conserver tool maintains log files in two directories, depending on whether the daemon or client writes the log file:

- The daemon writes a log file to `var/log/conserver`
- The client writes its log files to `var/log/consoles`

The `/var/log/consoles directory` directory contains one file for each node that opened a remote console session. The file name matches the node name, and contains a date/time stamp for when the console was opened and closed, as well as the console traffic. Because console traffic can contain sensitive data, you must ensure that these log files are secure. The conserver package installed by CSM creates the `/var/log/consoles directory` as owned by root, with read/write permissions granted only to the directory owner. Consult your site's policies regarding securing console log files.
Chapter 17. Using Linux diskless nodes

Linux diskless nodes can be managed as part of your CSM cluster environment. Diskless nodes are nodes that do not use a disk for the runtime operating system image. The operating system can be fully loaded in the node's local memory, or partially serviced by an external file system. CSM uses the Warewulf open source software to set up a diskless boot environment for Linux nodes; Warewulf version 2.6.3 is required. Warewulf does not depend on Linux kernel minor versions, patches, or configuration. For Warewulf solution details, see http://warewulf.lbl.gov/cgi-bin/trac.cgi.

CSM supports diskless nodes running RedHat Enterprise Linux AS 4, RedHat Enterprise Linux ES 4, RedHat Enterprise Linux 5 server/client and SUSE Linux Enterprise Server (SLES) 9 and 10. Standard nodes and diskless nodes can be mixed in the same cluster. The install server for diskless nodes must run Linux, but cannot itself be a diskless node. The management server can run any supported operating system, such as AIX and Linux. Diskless nodes boot an operating system image stored on the install server. In some case, install server runs on management server.

Linux diskless node terminology

Standard Linux node
A CSM node with a disk.

VNFS
A Virtual Node File System (VNFS) contains all the files required to build a diskless boot image for a diskless node or Warewulf node group.

Diskless node
A node that does not use a local disk for the runtime operating system image. The operating system may either be fully loaded in the node's local memory, or partially serviced by an external file system. A diskless node can have RPMs installed into a shared VNFS stored on the install server.

Warewulf node group
Warewulf uses node groups to manage diskless nodes. One VNFS and one diskless boot image are created for each Warewulf node group. CSM maps all nodes with the same Warewulf template to a Warewulf node group. CSM creates Warewulf node groups and names them based on the Warewulf template name. There is no relation between a CSM node group and a Warewulf node group. Warewulf node group names cannot be used to specify target nodes for CSM commands.

Warewulf template
A Warewulf template is a directory containing files to configure and control Warewulf node and node group definitions, and to define and manage the diskless boot image to be used by that Warewulf node group. Default templates are provided with CSM for each operating system distribution version that is supported. You can create a custom template by copying, renaming, and modifying a default template and setting the managed node attribute InstallTemplate to your customized template directory. CSM will use this template to create a Warewulf node group.

Diskless boot image
An operating system boot image built from a VNFS.

Hybrid image
A type of diskless boot image that when booted to the node, has part of its file system in the RAM, and part of its file system on its VNFS mounted through NFS. A hybrid image is created using Warewulf, and requires less RAM space on the node than a RAM-Disk image.

RAM-Disk image
CSM for AIX and Linux: Planning and Installation Guide 249
Planning for Linux diskless nodes

Diskless nodes provide simplified management and maintenance compared to nodes that run individual disks and operating system images. Diskless nodes share a common boot image that is loaded across the network from the CSM install server and executed from the local memory on the node. Optionally, less frequently used portions of the root file system and additional file systems can be network mounted during normal diskless node operation. Simultaneous updates can be made on a large group of nodes by updating or by rebuilding the VNFS and the common boot image on the install server and rebooting the nodes. Provisioning nodes is much easier in a diskless cluster.

Diskless nodes may not be appropriate for all clusters. If each of the nodes in your cluster have unique individual application requirements, it may be easier to manage the different software packages directly on each node instead of trying to build different VNFS and boot images for each of the nodes. Since many diskless nodes can share a common boot image, if there are problems with an image, a large number of nodes may be impacted at the same time.

Diskless node images are used to compensate for hardware servers that may have disk failure rates that exceed acceptable tolerances for a customer environment. The image can be stored on other hardware and networked to the individual nodes and loaded into memory for runtime operation.

Linux diskless nodes and CSM

CSM interfaces with the Warewulf open source software to provide a Linux diskless node solution. CSM works with diskless nodes in the same way it works with standard nodes for most CSM operations. However, due to specific characteristics of diskless nodes or the Warewulf open source software, some CSM features are not supported or may work differently with diskless nodes. The following list describes some of these differences:

Hardware control
Setting up the hardware control point and using CSM hardware control and remote console features work the same for diskless nodes. You must use the installnode command every time you wish to boot your diskless nodes. The installnode command will set up all boot files and pass the kernel parameters to the node in order to correctly load and run the configured diskless boot image.

Note:

1. The installnode --noreboot command does not support diskless nodes.
2. The nodeset command does not support diskless nodes.

CSM node installation functions
HTTP network installation protocol
Standard nodes can be installed using an optional NetworkInstallProtocol of HTTP. This option is not supported for diskless nodes. This is a cluster-wide option; the HTTP network install protocol cannot be used in a CSM cluster that has diskless nodes.

MAC address and UUID installations
System x diskless nodes can be installed using the node UUID or the install adapter's MAC address.
System p diskless nodes must be installed using their install adapter's MAC address.

Configure driver modules
For standard Linux nodes, updates can be provided for drivers that are used during the Linux installation process or that are installed as part of the Linux operating system. For diskless nodes, new and updated drivers will automatically be copied into the VNFS from the same /csminstall/csm/drivers directories that are used for standard Linux nodes.

**Customization scripts**

For standard Linux nodes, you can provide custom scripts that are run on a node during the Linux installation process. For diskless nodes, a customization script directory, /csminstall/csm/scripts/disklessboot, has been created. Your custom scripts should follow the same naming conventions used for standard Linux nodes. The scripts will be run on the diskless node during the node boot process. You can also provide scripts in the /csminstall/csm/scripts/disklessprebuild directory for customizing the VNFS that CSM creates for building diskless boot images.

**Secondary adapter configuration**

Secondary adapters can be configured on the diskless node using the same procedures that are used for standard nodes.

**Install servers**

Same as standard nodes, diskless nodes can only be installed directly from a management server or install server if one is used.

**CFM**

Configuration File Management (CFM) is supported for diskless nodes. CFM will distribute files to diskless nodes following the same rules for standard nodes. However, if you are using a hybrid image, remotely mounted files on the node will be read-only. CFM will return errors for any updates that are attempted on read-only file systems. On the diskless nodes, CFM will distribute files every time when the nodes boot or reboot, while for standard nodes, CFM only distribute files once unless these files are deleted on the nodes.

**SMS**

Software Maintenance System (SMS) is not supported for diskless nodes. SMS adds and updates RPMs on standard Linux nodes after the operating system has been installed. For diskless nodes, additional RPMs should be added to the VNFS and built into the diskless boot images.

**dsh**

The dsh command can be used to run remote shell commands on diskless nodes with no restrictions.

**Predefined node groups**

CSM provides many predefined node groups. The node group WarewulfNodes is created when CSM is installed on the management server. This is a dynamic node group that contains all nodes whose InstallMethod attribute is set to warewulf.

**Monitoring**

Some CSM monitoring features are not operational for diskless nodes. Most conditions can be monitored on a diskless node with the exception of conditions that:

- Require the file systems to be on the nodes for checking disk space, such as AnyNodeFileSystemSpaceUsed.
- Check updates to files, such as ProbeSensorIsActive.

**Backup and restore**

The csmbackup command will back up any custom Warewulf templates on the management server that are referenced by node InstallTemplate attributes. The csmrestore command will restore all saved template files.

**MinManaged nodes**

A CSM minimally-managed (Mode=MinManaged) node does not have any client CSM or RSCT code installed. Diskless nodes can be MinManaged nodes, but Managed and MinManaged diskless nodes cannot coexist in the same Warewulf node group. Instead, they can coexist in the same cluster by using different VNFS(different Warewulf node groups). CSM includes additional
boot scripts in the diskless boot image to correctly boot and configure the node. No CSM or RSCT RPMs are installed in the diskless boot image.

**Heterogeneous clusters**

CSM supports heterogeneous clusters of diskless and standard nodes. For diskless nodes, heterogeneous cluster is supported by using install servers. The diskless nodes can use any supported Linux operating system in a heterogeneous cluster. If diskless nodes use more than one kind of Linux distribution, version and package architecture, each such Linux operating system need at least one install server to support. An install server can only support one Linux operating system for diskless nodes, but multiple install servers can be used in a heterogeneous cluster. For standard nodes, an install server can install any supported Linux operating system and distribution in a heterogeneous CSM cluster.

**HA MS**

High Availability Management Server (HA MS) function is not supported for clusters with diskless nodes.

**Install Server Group**

Install Server Group function is not supported for clusters with diskless nodes.

## Planning the management server

A CSM for Linux management server provides services for installing CSM standard nodes and diskless nodes in the same cluster. See [Planning for cluster hardware](#) for planning for management servers for CSM nodes. Management servers for diskless nodes have additional software requirements. See [Software prerequisites for the install server](#) for more details.

New in CSM 1.7 is the ability to use separate install servers to install diskless Linux nodes. This adds the flexibility to have different operating systems or operating system versions on different diskless nodes in the cluster. You can use a separate install server for each different type of operating system.

## Planning the install server

The install server and the nodes must have the same `InstallDistributionName`, `InstallDistributionVersion`, and `InstallPkgArchitecture`. The exception is Red Hat EL 5 install servers and nodes, which do not require the same `InstallDistributionName`. For example, you could have RedHatEL-Server on the install server and RedHatEL-Client on the nodes. Supported Linux operating systems for diskless nodes are:

1. Red Hat EL AS 4
2. Red Hat EL ES 4
3. Red Hat EL 5 Server/Client
4. SLES 9
5. SLES 10

An install server cannot be diskless. Linux install servers provide diskless boot image build services to diskless nodes. Linux install servers also provide DHCP, PXE or BOOTP, TFTP, HTTP and NFS services for CSM diskless nodes when they boot with their diskless boot image.

The requirements for a Linux install server for diskless nodes are:

- The Linux install server must be running CSM 1.7.0, or later.
- A sufficient number of network adapters are required to accommodate the network installation of all nodes served by this management server. See [Network requirements](#).
For Linux on System p installations, the nodes to be served must be network connected to the management server either directly through a local subnet or indirectly through a gateway.

For Linux on System x installations, the diskless nodes must be network connected to this install server directly through a local subnet.

Disk space on the install server

Additional disk space on the install server, beyond the standard node requirements, is required for:

- Installing diskless support software
- Installing each distribution of Linux in a VNFS. 1 GB is required for the default VNFS that CSM creates.
- Saving diskless boot images for the Linux distribution. CSM supports only one distribution for the install server and the nodes, but you can use templates to create multiple boot images for the same distribution. CSM creates the boot images, which require 500 M each.
- SELinux (Secure Enterprise Linux) must be disabled on the CSM install server. Errors occur when Warewulf and Yum try to build the VNFS and diskless boot images if this Linux feature is enabled.

Software prerequisites for the install server

These are the additional software prerequisites for a diskless node install server. Warewulf and Yum are required for the install server to support diskless nodes:

**Warewulf**

A Linux cluster solution that manages and distributes Linux diskless boot images to any number of diskless nodes. It facilitates the process of installing and long term administration of a cluster. It builds an *initrd* and boot image for diskless nodes.

**Yum**

An automatic updating tool and package installer and remover for Linux systems. It automatically computes dependencies and determines what needs to occur to successfully install packages. Using the *yum* command makes package installation easier than when using the *rpm* command. The *yum* command is used to install Warewulf and to create the VNFS on the install server.

Required software for the Linux install server to support diskless nodes

The following open source software is required on the install server:

**Table 88. Software required for an install server to support diskless nodes**

<table>
<thead>
<tr>
<th>Open source software</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Warewulf 2.6.3, and Warewulf 2.6.3 dependencies: <a href="">ftp://linuxpatch.ncsa.uiuc.edu/csm/</a> or <a href="http://warewulf.lbl.gov/cgi-bin/trac.cgi">http://warewulf.lbl.gov/cgi-bin/trac.cgi</a></td>
<td>CSM install server support of diskless nodes.</td>
</tr>
<tr>
<td>Yum 2.6.1 or later and Yum 2.6.1 dependencies: <a href="">ftp://linuxpatch.ncsa.uiuc.edu/csm/</a> or <a href="http://www.linux.duke.edu/projects/yum/">http://www.linux.duke.edu/projects/yum/</a></td>
<td>Install Warewulf and create the VNFS</td>
</tr>
</tbody>
</table>

Refer to the Yum documentation for the operating system dependencies for your Linux distribution. Required dependency versions may vary depending upon your
Yum version.

You can download RPMs from:

- ftp://linuxpatch.ncsa.uiuc.edu/csm/

For an example installation and more information, see the CSM FAQs: http://www.ibm.com/developerworks/forums/dw_thread.jsp?forum=907&thread=128386&cat=53&treeDisplayType=threadmode1

**Planning for Linux diskless nodes**

To plan for Linux diskless nodes, you need to understand the basic architecture of Warewulf open source software and how it creates and manages the VNFS and diskless boot images. see http://warewulf.lbl.gov/cgi-bin/trac.cgi.

**Hardware requirements**

Hardware requirements for diskless nodes are the same as the node hardware requirements listed in Planning for cluster hardware. Diskless nodes have the following additional requirements.

CSM supports two types of diskless boot images: hybrid images and RAM disk images. Each of these have different memory requirements. The following table shows the details of minimum memory requirement for diskless nodes using default VNFS provided by CSM.

<table>
<thead>
<tr>
<th>Platform</th>
<th>Minimum Memory Required for Hybrid Image</th>
<th>Minimum Memory Required for Ramdisk Image</th>
</tr>
</thead>
<tbody>
<tr>
<td>SLES9 ppc64</td>
<td>512 MB</td>
<td>600MB</td>
</tr>
<tr>
<td>SLES9 x86_64</td>
<td>300 MB</td>
<td>500MB</td>
</tr>
<tr>
<td>SLES9 i386</td>
<td>400MB</td>
<td>500MB</td>
</tr>
<tr>
<td>SLES10 ppc64</td>
<td>512MB</td>
<td>600MB</td>
</tr>
<tr>
<td>SLES10 x86_64</td>
<td>600MB</td>
<td>700MB</td>
</tr>
<tr>
<td>SLES10 i386</td>
<td>512MB</td>
<td>600MB</td>
</tr>
<tr>
<td>RHEL-AS4 ppc64</td>
<td>512MB</td>
<td>600MB</td>
</tr>
<tr>
<td>RHEL-AS4 x86_64</td>
<td>300MB</td>
<td>700MB</td>
</tr>
<tr>
<td>RHEL-AS4 i386</td>
<td>500MB</td>
<td>600MB</td>
</tr>
<tr>
<td>RHEL-ES4 x86_64</td>
<td>300MB</td>
<td>700MB</td>
</tr>
<tr>
<td>RHEL-ES4 i386</td>
<td>400MB</td>
<td>700MB</td>
</tr>
</tbody>
</table>
Configuring Warewulf

Configure Warewulf on the install server

Warewulf needs to be configured on the install server for supporting diskless nodes. CSM provides several default Warewulf configuration files in `/opt/csm/install/warewulf` directory on management server. The `csmsetupinstall` command will customize some variables in these configuration files for a particular install server, then put them in `/etc/warewulf` directory on the install server. You can further customize these configuration files in `/etc/warewulf` on install server after `csmsetupinstall` set them up. These Warewulf configuration are:

- **master.conf**
  The master Warewulf configuration file specifying information for the Warewulf server. The install server is the Warewulf server in a CSM cluster.

- **client.conf**
  The configuration file specifying information that Warewulf clients use to connect to the Warewulf server.

Warewulf templates

A Warewulf template is a directory that contains files to configure and control a Warewulf node group definitions, and to define and manage the diskless boot image for the Warewulf node group. Default templates are provided with CSM for each operating system distribution version and architecture that is supported. You can create a custom template by copying, renaming, and modifying a default template and setting the managed node attribute `InstallTemplate` to your customized template directory. CSM will use this template to create a Warewulf node group. All CSM nodes that use the same Warewulf template will be included in one Warewulf node group.

CSM uses Warewulf tools to create one diskless boot image for each Warewulf node group. Warewulf templates allow customization of the diskless boot image that is installed on the nodes. The following files are included in the Warewulf template:

- **config**
  Update this file for changing:
  
  - The users and user groups allowed access to this node image
  - The type of image: Hybrid image or RAM disk image.
  - The user supplied diskless boot image, kernel, initrd and zimage.

  The `group desc` field can also be updated. Do not edit the remainder of this file.
includes
Update this file to include files in the boot image that are not in the VNFS. Files listed in the
includes file are taken from the install server and built in the boot image.

excludes
Update this file to define which files are included in the RAM disk image, and which files are
excluded. This rule is similar to the rsync -exclude-from option. For more information, see the
rsync man page.

excludes-aggressive
Update this file to specify files to be linked back to the VNFS in a hybrid type node image. Files
not excluded remain in RAM.

wwinitrd.config
The configuration file used to create the Warewulf initial RAM-disk image (initrd) used for all the
diskless nodes in the cluster. It includes lists of kernel modules, load modules, and devices that are
to be included in the initrd.

vnfsrpm
This is a configuration file for csmsetupinstall to build a VNFS. It contains a list of RPM names
that need be installed into the VNFS.

yum.conf
The Yum configuration files.

Here is a table to show which file in template is used to generate which file on the CSM install server:

<table>
<thead>
<tr>
<th>Files in a template</th>
<th>Files on CSM install server</th>
</tr>
</thead>
<tbody>
<tr>
<td>config</td>
<td>/etc/warewulf/nodes/&lt;WarewulfNodeGroupName&gt;/config</td>
</tr>
<tr>
<td>disklessnodecfg</td>
<td>/etc/warewulf/nodes/&lt;WarewulfNodeGroupName&gt;/NodeName</td>
</tr>
<tr>
<td>includes</td>
<td>/etc/warewulf/vnfs/includes.&lt;WarewulfNodeGroupName&gt;</td>
</tr>
<tr>
<td>excludes</td>
<td>/etc/warewulf/vnfs/excludes.&lt;WarewulfNodeGroupName&gt;</td>
</tr>
<tr>
<td>excludes-aggressive</td>
<td>/etc/warewulf/vnfs/includes-aggressive.&lt;WarewulfNodeGroupName&gt;</td>
</tr>
<tr>
<td>Wwinitrd.config</td>
<td>/etc/warewulf/wwinitrd.config.&lt;WarewulfNodeGroupName&gt;</td>
</tr>
<tr>
<td>vnfsrpm</td>
<td>This file stays in the template.</td>
</tr>
<tr>
<td>yum.conf</td>
<td>/&lt;vnfs dir&gt;/&lt;WarewulfNodeGroupName&gt;/var/opt/csm/yum/yum.conf</td>
</tr>
</tbody>
</table>

Note:
The vnfs dir is set in the /etc/warewulf/master.conf. By CSM default, the vnfs dir is set to
/csminstall/diskless/vnfs on management server, and is set to /csmserver/diskless/vnfs on install
server. You can change the settings of vnfs dir by change the template.

All default Warewulf template files reside under
/opt/csm/install/warewulf-tmpl.<InstallDistributionName><InstallDistributionVersion>-<InstallServiceLevel>-<InstallPkgArchitecture> directory.

For more information, see the warewulf-tmpl man page.

Virtual node file system (VNFS)

A VNFS contains all the files required to build a diskless boot image for a diskless node or a Warewulf
node group. A Warewulf node group is defined by a Warewulf template. The csmsetupinstall command
creates one VNFS for each Warewulf node groups. CSM requires that the same operating system
distribution, version, and architecture be used for all diskless nodes that are built from the VNFS that is
located on the install server. Diskless nodes that have different Linux distribution, version, and architecture
must use different install servers. The `csmsetupinstall` command creates the VNFS from the operating system distribution files located in the `/csminstall/Linux` directories. These directories are the same ones CSM uses to install a Linux operating system on standard nodes. By default, the VNFS is created in the `/csminstall/diskless/vnfs` directory, but this can be changed by changing the "vnfs dir" attribute in `/etc/warewulf/master.conf`. CSM names the VNFS based on the name of Warewulf template. The default template is named based on the operating system distribution, version, and architecture. You can create your own VNFS and Warewulf node group by creating your own Warewulf template with your unique name.

The `vnfsrpm` file in a Warewulf template is used to configure and manage the contents of a VNFS. It contains the list of RPMs to be installed in the VNFS.

CSM provides a default `vnfsrpm` file in each default Warewulf template. If you want customize the contents of the `vnfsrpm`, you must create your own Warewulf template and customize the `vnfsrpm` in your Warewulf template, and then you can use your own Warewulf template to build your VNFS and diskless build image.

To further customize your VNFS, CSM lets you provide scripts that can be run against the VNFS right after it is created. Place these scripts in the `/csminstall/csm/scripts/disklessprebuild` directory. The following environment variables are set while running the scripts in this directory, so you can query them in your scripts:

- **SCRIPTDATAPATH**: A full path to "`CSM-CLIENT-MNT-DIR/csm/scripts/data`". E.g. `/var/opt/csm/mnt/csm/scripts/data`.
- **VNFSPATH**: A full path to VNFS. E.g. `/csminstall/diskless/vnfs/RedHatEL-AS4-QU3-i386`.
- **VNFSOSNAME**: The operating system name is installed in VNFS. E.g. Linux.
- **VNFSDISTRIBUTIONNAME**: The operating system distribution name is installed in VNFS. E.g. RedHatEL-AS.
- **VNFSDISTRIBUTIONVERSION**: The operating system version is installed in VNFS. E.g. 4.
- **VNFSSERVICELEVEL**: The operating system service level is installed in VNFS. E.g. QU3.
- **VNFSPKGARCHITECTURE**: The operation system package architecture is installed in VNFS. E.g. i386.

You can use these variables to access the VNFS and your data in the `csm/scripts/data`.

CSM supports multiple VNFSes on an install server, CSM creates one VNFS and one Warewulf node group for each Warewulf template. All CSM nodes with the same Warewulf template are mapped to a Warewulf node group. CSM uses Warewulf tools to create one diskless boot image for each Warewulf node group based on its VNFS. The CSM `InstallTemplate` attribute specifies the Warewulf template to be used for a node. The Warewulf template can specify which files from the VNFS are included or excluded when the diskless boot image is built. A unique diskless boot image is built for each Warewulf template (or for each VNFS) and is named based on the Warewulf template name.
Diskless boot image, initrd, kernel and zimage

CSM builds a diskless boot image for each Warewulf node group based on its VNFS. A Warewulf node group is defined by a Warewulf template.

The config file in the template provides a way to control what kind of diskless boot image you want to build. CSM can build two types of diskless boot images, hybrid diskless boot images and RAM-Disk diskless boot images. By default, CSM will build a hybrid diskless boot image. If you want to build a RAM-Disk diskless boot image, you have to create your own Warewulf template and change the DisklessType setting in the config file of your template. To create your own Warewulf template, you can copy the default template and edit it for your need.

There are three files in the template that control which files on the install server need to be included in the diskless boot image, and which files in the VNFS need to be excluded from the diskless build image. These files are includes, excludes and excludes-aggressive. The includes and excludes files are used to build the RAM-Disk diskless boot image. The includes and excludes-aggressive files are used to build the hybrid diskless boot image. CSM provides default includes, excludes and excludes-aggressive files for each default Warewulf template. If you want to customize these files, you need to create your own Warewulf template, and then edit these files in your template.

System x diskless nodes, require a kernel and an initrd to work with the diskless boot image. CSM uses the kernel in the VNFS for the diskless node. The initrd is created when csmsetupinstall is run. The default wwinitrdf.config file in the template provides a way to control what needs to be in the initrd. To change the default contents of initrd, create your own Warewulf template, and then edit the wwinitrdf.config file in your template.

System p diskless nodes, require a zimage to work with the diskless node boot image. The zimage is created by csmsetupinstall based on the initrd and kernel. Therefore, you can control the zimage by controlling the initrd.

User supplied diskless boot image, initrd, kernel and zimage

You can also provide your own diskless boot image. The supplied diskless boot image must be a RAM-Disk diskless boot image. The csmsetupinstall command accepts a user supplied RAM-Disk diskless node boot image. You can use the DisklessKernel, DisklessInitrd, DisklessZimage and DisklessImage attributes in the Warewulf template config file to define the diskless image to use. The csmsetupinstall command will to set up the system for diskless nodes to boot from the user supplied kernel, initrd and diskless boot image. If you want to supply a diskless boot image, you must supply the zimage or kernel and initrd together with the diskless boot image. The zimage is used for System p and initrd and kernel are used for System x.

Notice: You can only supply a RAM-Disk diskless node boot image. You can not supply a Hybrid diskless node boot image since this kind of diskless boot image needs a VNFS at run time.

You can obtain the kernel, initrd and diskless boot image from an off site CSM install server after running csmsetupinstall on a CSM management server. Sometime, CSM management server can also be used as an install server. You can obtain the initrd, kernel, zimage and diskless boot image from a CSM install server in the locations shown in the table below.

<table>
<thead>
<tr>
<th>Name</th>
<th>Location</th>
<th>System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Location</td>
<td>System</td>
</tr>
</tbody>
</table>

CSM for AIX and Linux: Planning and Installation Guide
When you supply a diskless boot image, you must to supply a kernel and an initrd for a System x diskless node, and you must supply a zimage for a System p diskless node. You must make sure the kernel and the initrd or the zimage works with the diskless image that you supplied. The `csmsetupinstall` command assumes that all necessary drivers are already in initrd or zimage. You can not add any drivers at this time.

To supply a kernel and an initrd or a zimage, create your own template and modify the config file in the template. In the config file, you will see the following lines.

```
# DisklessType = hybrid
# DisklessKernel = Default
# DisklessInitrd = Default
# DisklessZimage = Default
# DisklessBootImage = Default
```

Read the instructions in the config file about these lines and replace the "Default" value with the full path and name of your kernel and initrd or your zimage. Here are examples of how to set these attributes for a user supplied kernel and initrd or zimage.

On System x

```
# DisklessType = user-ramdisk
# DisklessKernel = /full/path/kernel/name
# DisklessInitrd = /full/path/initrd/name  # DisklessZimage = Default
# DisklessBootImage = /full/path/diskless-boot-image/name
```

On System p

```
# DisklessType = user-ramdisk
# DisklessKernel = Default
# DisklessInitrd = Default
# DisklessZimage = /full/path/zimage/name
# DisklessBootImage = /full/path/diskless-boot-image/name
```

**Notice:** Do not delete the "#" in front of these lines when you set these values.

User supplied diskless node boot image, kernel, initrd and zimage will be saved in `/csminstall/Linux/<InstallDistributionName>/<InstallDistributionVersion>/<InstallPkgArchitecture>/installimages/<WarewulfNodeGroupName>` directory. This will allow the install server to use them.

**User management with diskless nodes**

By default, the diskless boot image created by CSM includes the user management `/etc/password`, `/etc/shadow`, and `/etc/group` files shipped with the Linux distribution. The management server `/home` directory is exported by Warewulf and is controlled by the Warewulf `master.conf` file. Typically, you will want your `/home` directory to reside in persistent storage so that user files will be available when a diskless node is re-installed.

You can change or customize some of the defaults to follow user management procedures established for your cluster environment. Some possible things to do:
- Use CFM to distribute user management files to all nodes when the diskless nodes are installed. You must ensure that corresponding /home directories are created for users listed in these files.
- Provide disklessboot customization scripts that CSM runs when the node is installed. These scripts can mount a /home directory from another server, or run local user management commands.

**Diskless and MinManaged nodes**

On a standard MinManaged node, CSM is not installed and no CSM files are found. However, some CSM files are copied to diskless nodes to allow them to become Managed nodes. No RPMs are installed on such node.

---

**Installing diskless nodes**

CSM uses Warewulf and Yum tools to build diskless boot images for nodes from a VNFS. CSM provides a set of default configuration files for Warewulf and VNFS. Yum is used to install Warewulf and manage the VNFS. Warewulf is used to update and manage the diskless boot images.

For more information on Warewulf software, see the Warewulf documentation at [http://warewulf.lbl.gov/cgi-bin/trac.cgi](http://warewulf.lbl.gov/cgi-bin/trac.cgi).

For more information on Yum software, see the Yum documentation at [http://www.linux.duke.edu/projects/yum/](http://www.linux.duke.edu/projects/yum/).

**Before you perform the installation**

Before you perform the installation, ensure that you have completed the following:

- The operating system and CSM is installed on the management server.
- Diskless node attributes are defined; see Defining nodes.
- For hardware control, hardware control points and console servers are set up and defined; see the CSM for AIX and Linux: Administration Guide.
- Optionally, remote hardware inventory and maintenance is set up and the rfwscan have been run, as described in System x hardware inventory and maintenance.

If you want to upgrade an existing diskless node, see Managing and upgrading Linux diskless nodes.

**Avoiding problems with hardware and network setup**

To avoid problems that can occur during installation, see Avoiding problems with hardware and network setup.
Configuring your switch for multiple VLANs

If you have multiple network interfaces on a management server that are attached to the same VLAN, you may see some unexpected results due to the fact that broadcast traffic on the VLAN is seen on multiple interfaces.

Steps for installing Linux diskless nodes

The following steps describe how to use CSM, Yum, and Warewulf to set up CSM Linux diskless nodes. Each of these steps is described in the following sections, and must be done in order.

1. Check node hardware requirements
2. Check node software requirements
3. Set the node boot order (for Linux on System x or BladeCenter JS)
4. Verify hardware control point user IDs and passwords
5. Verify the node definitions
6. Validate rpower and rconsole
7. Run copycds for the Linux distribution
8. Install Yum and Warewulf on the install server
9. Modify the Warewulf configuration files (optional)
10. Verify the Warewulf configuration
11. Configure the VNFS
12. Modify the Warewulf templates (optional)
13. Configure driver modules (optional)
14. Prepare for secondary adapter configuration (optional)
15. Configure a Linux diskless node installation
16. Register host names
17. Create configuration files for the nodes (optional)
18. Set up with user-provided customization scripts
19. Install the diskless boot image on the nodes
20. Monitor and verify the installation

Check node hardware requirements

Hardware requirements depend on the type of image used - Hybrid image or RAM disk image. Before continuing with the installation, see Hardware prerequisites for more information.

Check node software requirements

Before continuing with the installation, see Software prerequisites for the install server for information about software for Linux diskless nodes. For additional information about general cluster node software requirements, see Planning for CSM software.

Set the node boot order for Linux on System x and BladeCenter JS

Note:
If you have a Cluster 1350 system, you must check the boot order. If the boot order is correct, you may skip this step. If you do not have a Cluster 1350 system, or if the boot order is incorrect, you need to complete this step.
Linux on x86 architecture: You must set the boot order in the BIOS (Basic Input/Output System) for each cluster node. During the node boot, press the F1 key when you are prompted. Set the boot order as follows:

1. Diskette
2. CD-ROM
3. Network
4. Hard disk

Linux on BladeCenter JS: To set the boot order for BladeCenter JS blade servers, open the Management Module Web interface, and do the following:

1. Click on Blade Tasks --> Configurations.
2. Change boot sequence to Hard drive 0.

Update BIOS to support non-eth0 installation (optional)

For System x 335 and 345 servers, the default BIOS only supports booting from eth0. To support the installation through a non-eth0 adapter, you must update the BIOS. You can find the high-level BIOS version for the servers at: http://www.ibm.com/support.

For x330, update BIOS to 1.06 or above to support PXE boot from the adapter.

For x335, update BIOS to 1.10 or above to support PXE boot from BOTH Ethernet.

For x345, update BIOS to 1.15 or above to support PXE boot from BOTH Ethernet.

Verify hardware control point user IDs and passwords

Verify that the user IDs and passwords that are required for remote hardware control points have been set using the systemid command. See Store Linux hardware control point user IDs and passwords.

You must store the user IDs and passwords that are required for remote hardware control points.

The step is required for hardware control. For complete information about hardware control points for the cluster, see Managing hardware control points.

Verify node definitions

After running the definenode command, and setting up the management server with all CSM node information, you are ready to verify the node definitions. Verify and customize the cluster node definitions before the nodes are installed. Because the actual node installation has not happened yet, you can make changes to node definitions at this time.

To determine whether the nodes have been defined, issue the lsnode command from the management server:

lsnode
The system responds with a line for each node that was successfully defined. If a node has not been defined, it will not appear in the output for the `lsnode` command.

To display information about each node, run the `lsnode` command with the `-l` (lowercase L) flag:

```
lsnode -l | more
```

The system responds with output containing extended information for each node that was successfully defined. Some node attributes might have null values at this point. For diskless nodes, the `InstallMethod` attribute must be set to `warewulf`.

**Note:**

If a node has not been defined, it will not be installed. To install Linux diskless nodes, the `InstallAdapterName` attribute must be set before running the `csmsetupinstall` command. The Warewulf diskless node install process requires this information to configure the install adapter device on the node.

If necessary, you can change node attributes by running the `chnode` command, or by rerunning the `definenode` command with the `-m` flag. Use the `definenode -m` command to specify an updated `nodedef` file or updated attribute values; the command only modifies nodes that have changed attribute values.

To change node attribute values, issue the `chnode` command from the management server:

```
chnode -n hostname attr=value
```

See the man pages or the *CSM for AIX and Linux: Command and Technical Reference* for more information about the `lsnode`, `chnode`, and `definenode` commands.

**Validate rpower and rconsole**

Before installing the diskless nodes, test remote power (`rpower`) and remote console (`rconsole`) to make sure they are configured.

Remote power is used to network boot the nodes in order to collect the MAC addresses and install the nodes. To test `rpower`, issue the following:

```
rpower -a query
```

The output from the `rpower` command lists all of the nodes and their status. For example:

```
# rpower -a query
c5n72.clusters.com on
c5n73.clusters.com on
c5n74.clusters.com off
c5n75.clusters.com off
```

To perform the installation, nodes may be in either the `on` or `off` state. If you get errors as a result of running the `rpower` command, see the *CSM for AIX and Linux: Administration Guide* to diagnose the problem. Nodes with errors will not be installed.

Remote console is required to obtain MAC addresses. To test `rconsole`, issue the following:

```
rconsole -a
```

263
The `rconsole -a` command opens console windows for all the nodes. If there are a large number of nodes in your cluster, you might want to test only a subset of the nodes.

**Note:**

1. For BladeCenter, the MAC addresses are obtained from node vital product data (VPD). Remote console is not required.
2. If you use an incorrect MAC address, `dhcp` errors can occur when a node boots during the `installnode` process.

### Run copycds for the Linux distribution

Run the `copycds -A` command to copy the Linux distribution CDs to the `/csminstall/Linux` directory on your management server. The RPMs on the CDs are required to resolve dependencies for installing Yum and Warewulf on your management server. Because diskless nodes are installed with the management server operating system, the RPMs are also used when running the `csmsetupinstall` command and building the VNFS.

If your management server is running the SUSE Linux Enterprise Server (SLES) operating system with a service level applied-the `InstallServiceLevel` attribute value is other than GA or no value-you must copy both the GA and the service level CDs.

**Note:**

To install SLES 10 diskless nodes with a service level, you do not have to copy the SLES 10 GA CDs.

For example, if you are installing SLES 9, service pack 1 (SP1), run the following command, where `PATH` is the path containing the SLES 9 GA CDs:

```
copycds -A -p PATH InstallDistributionName=SLES InstallDistributionVersion=9 \ InstallServiceLevel=GA
```

Then run the following command, where `PATH` is the path containing the SLES 9 SP1 CDs:

```
copycds -A -p PATH InstallDistributionName=SLES InstallDistributionVersion=9 \ InstallServiceLevel=SP1
```

For Red Hat EL distributions, the service level CDs contain the full operating system distribution, so you only need to run a single `copycds` command for the service level.

### Install Yum and Warewulf on the install server

To enable the management server to support diskless nodes, Warewulf and Yum (and their dependencies) need to be copied into `csm_addon` directory on the management server. Because Warewulf and Yum are open source solutions, this software must be downloaded first. See [Software prerequisites for the install server](#) for where to find this software.

Additional RPMs might be needed during installation of Warewulf and Yum. Some of these RPMs are included with the Linux distribution. You should have copied all of the Linux distribution CDs to the `/csminstall/Linux` directory on your management server in the previous step. RPMs that are not included in the Linux distribution need to be downloaded from the internet.
All Yum, Warewulf and their dependences RPMs that do not come with the Linux distribution needs to be copied to CSM designated csm_addon directory. Once you downloaded or compiled these RPMs, you can use the copycsmpkgs -p command to copy them to csm_addon directories. Yum and Warewulf packages will be copied and installed on install server automatically by running csmsetupinstall command later. If the management server is used as an install server, the Yum and Warewulf will be installed on the management server. On Red Hat Enterprise Linux 5, you do not need to copy Yum since it comes with the Linux distribution.

In case you can not get compiled RPMs, you need to download its source code and compile them yourself. Open source RPM dependencies and installation instructions change frequently. Visit the Warewulf and Yum Web sites for the most current instructions. Use the instructions at the CSM FAQ Web site to install Warewulf and Yum on your management server: http://www.ibm.com/developerworks/forums/dw_thread.jsp?forum=907&thread=128386&cat=53&treeDisplayType=threadmode1.

**Modify Warewulf configuration files (optional)**

Before proceeding with your Linux diskless node installation configuration, you can modify the default CSM Warewulf configuration files. CSM provides the following files in /opt/csm/install/warewulf:

- **master.conf**
  The master Warewulf configuration file specifying information for the Warewulf server. The install server is the Warewulf server in a CSM cluster. Sometime, the install server is running on the management server.

- **client.conf**
  The configuration file specifying information that Warewulf clients use to connect to the Warewulf server.

CSM copies these files to the /etc/warewulf directory the first time you run the csmsetupinstall command for diskless nodes.

To customize any of these files before running csmsetupinstall command, copy the default file from the /opt/csm/install/warewulf directory on management server to the /etc/warewulf directory on install server.

Edit the file in the /etc/warewulf directory on install server. When you run csmsetupinstall for your diskless nodes, CSM and Warewulf will use your customized files from the /etc/warewulf directory.

When modifying the files, consider the following information:

- Do not remove or modify the following lines:
  
  "######################## DO NOT ERASE THIS SECTION (begin)########################
  
  "######################## DO NOT ERASE THIS SECTION (end) ########################

  Do not edit any lines that appear in this section of the file. CSM could overwrite your customization changes to the file if these lines are not present.

- CSM has included substitution variables in the file. These variables use the format #CSMVAR:variable#. CSM will replace these variables with the correct values the first time you run the csmsetupinstall command for diskless nodes. You may replace these variables with your own data to not have CSM automatically set these values.
• To restore #CSMVAR:variable# substitution variables that you have replaced, you must copy a new version of the file from /opt/csm/install/warewulf to the /etc/warewulf directory and re-do your customizations. CSM will perform the variable substitution the next time you run csmsetupinstall for a diskless node.
• To replace your customizations with the CSM default files, remove the /etc/warewulf file and run the csmsetupinstall command again for a diskless node. CSM will create a new copy of the file.
• Do not edit the file directly in the /opt/csm/install/warewulf directory. Your changes will be lost if you update CSM on your management server.

Verify the Warewulf configuration

Verify that the information in the Warewulf configuration files is correct. Check the following files in the /etc/warewulf directory:

• master.conf
• client.conf

These files may not exist on the install server if you have not run the csmsetupinstall for the diskless nodes yet. If this is the case, come back here to verify the Warewulf Configuration after you run the csmsetupinstall later in this procedure. If you copied these two files to install server yourself, then continue do the following verification.

If you see values in the form #CSMVAR:variable#, CSM will replace these with the correct data the next time you run the csmsetupinstall command for diskless nodes. CSM will only replace these variables once. If any of the data written by CSM changes in the future, these files can become outdated; you must force CSM to refresh them.

The following changes could impact the data in these files:

• Changing the hostname, alias, or IP address of the management server
• Changing the management server interface that is used to contact the nodes
• Changing the remote shell used with the nodes
• Changing the location of the Virtual Node File System to match an existing Warewulf configuration.

If you find that any of this data is incorrect in the Warewulf configuration files, do the following to force CSM to refresh the data:

1. Save a backup copy of the configuration files.
2. Copy new versions of the default configuration files from /opt/csm/install/warewulf to /etc/warewulf.
3. Apply any local customizations to the files that you may have made. Refer to your saved backup copies for these changes.
4. Do not modify or delete any lines that CSM may have placed in the following sections of the files:

   # DO NOT ERASE THIS SECTION (begin)
   # DO NOT ERASE THIS SECTION (end)

5. The next time you run the csmsetupinstall command for diskless nodes, use the attr=value pair BuildDisklessVNFS=build to force CSM to process these configuration files and rebuild the VNFS and diskless boot images with the new data.
Configure the VNFS

The `csmsetupinstall` command builds a default Virtual Node File System (VNFS) for the Linux operating system installed on your install server. The VNFS contains all the files required to build a diskless boot image for a diskless node or Warewulf node group. You can customize the file used to configure this VNFS in template before proceeding with configuring your Linux diskless node installation and building the VNFS. You can also provide customization scripts that will be run for the VNFS to further customize the VNFS.

CSM provides a default VNFS configuration file in the Warewulf template. This file is `vnfsrpm`. It contains a list of RPMs that will be installed in the VNFS. To customize this file, you need to create your own Warewulf template by copying the default Warewulf template, and then customizing the vnfsrpm file in your Warewulf template. For example, to create your own Warewulf template:

```bash
cp -R /opt/csm/install/warewulf/warewulf-tmpl.RedHatEL-AS4-QU3-ppc64 /mydir/warewulf-tmpl.ComputeNodes
```

When modifying the file, consider the following information:

- CSM has added some lines to the file that should not be modified or removed:

  `################# DO NOT ERASE THIS SECTION (begin)#################`
  `################# DO NOT ERASE THIS SECTION (end)#################`

  Do not edit any lines that appear in these sections of the file. CSM could overwrite your customization changes to the file if these lines are not present.

- The `vnfsrpm` file contains a list of packages that will be installed in the VNFS. You may add additional RPMs to the list if you choose. CSM will build the VNFS when you first run the `csmsetupinstall` command for diskless nodes or if you force a build by specifying the `attr=value` pair `BuildDisklessVNFS=build` the next time you run the `csmsetupinstall` command. The `csmsetupinstall` will use one of the following directories to locate the RPMs:

  - `/csminstall/Linux/<InstallDistributionName>/<InstallDistributionVersion>/<InstallPlatformArchitecture>/<InstallServiceLevel>/RPMS` directory, e.g., `/csminstall/Linux/SLES/9/i386/SP3/RPMS`. This directory contains all packages from Linux distribution.
  - `/csminstall/Linux/<InstallDistributionName>/csm/<InstallCSMVersion>/packages` directory, e.g., `/csminstall/Linux/SLES/csm/1.7.1/packages`. This directory contains packages for CSM, RSCT, and some other open source software and their dependences that not in the Linux distribution.
  - `/csminstall/Linux/<InstallDistributionName>/<InstallDistributionVersion>/csm_addon` and `/csminstall/Linux/<InstallDistributionName>/<InstallDistributionVersion>/csm_addon` directories, e.g., `/csminstall/Linux/SLES/9/i386/csm_addon` and `/csminstall/Linux/SLES/9/i386/SP3/csm_addon`. These directories contain Yum, Warewulf and all additional packages supplied by you. You need to make sure that the dependencies for your additional packages are in one of above three directories. Warewulf client package `warewulf-wulfd` is required for all diskless nodes and should be copied to one of above three directories, which will be installed in VNFS and provide communication function between install server and diskless nodes.
You can use the `copycsmpkgs` command to copy Yum, Warewulf and their dependences to these directories. You must copy other additional packages manually to these directories if they are needed. The specific `csm_addon` directories depend on your additional packages. If the packages are not sensitive to the Linux distribution's service level, copy them into the `/csminstall/Linux/<InstallDistributionName>/<InstallDistributionVersion>/<InstallPkgArchitecture>/csm_addon` directory. If the packages are sensitive to Linux distribution service level, copy them into the `/csminstall/Linux/<InstallDistributionName>/<InstallDistributionVersion>/<InstallPkgArchitecture>/<InstallServiceLevel>/csm_addon` directory.

- When adding packages to the `vnfsrpm` file, you do not need to include all subsequent RPM dependencies. CSM uses the Yum utility to install the RPMs into the VNFS. Yum will automatically resolve all dependencies as long as the dependencies are in one of the above directories.
- CSM builds the VNFS automatically the first time you run the `csmsetupinstall` command for diskless nodes. If you change the `vnfsrpm` file later, you must rerun the `csmsetupinstall` command with `BuildDisklessVNFS=build` to force a rebuild of the VNFS and the diskless boot images created from that VNFS.
- Do not edit the `vnfsrpm` file of default Warewulf template in the `/opt/csm/install/warewulf` directory; your changes will be lost if you update CSM on the management server.

In addition to modifying the `vnfsrpm` file in your own template, you can also provide customization scripts in the `/csminstall/csm/scripts/disklessprebuild` directory to configure your VNFS. When you run the `csmsetupinstall` command with `BuildDisklessVNFS=build` after the new VNFS is rebuilt, all scripts in the `disklessprebuild` directory are run to modify files in the VNFS.

After a new VNFS is built, the `csmsetupinstall` command checks the `/csminstall/csm/scripts/disklessprebuild` directory and run each script on the management server to modify VNFS. Subdirectories in `/csminstall/csm/scripts/disklessprebuild` are not checked. If there are multiple scripts in `/csminstall/csm/scripts/disklessprebuild` directory, they are run in alphabetical order, as determined by the `ls` command.

The naming convention for the scripts is:

```
scriptname[._target]
```

The "._" characters following the script name are used if the script is called when running `csmsetupinstall` on a specific Warewulf node group. The target value is a Warewulf node group name. If the target extension is not used, then the script will be run for all Warewulf node groups when csmsetupinstall build their VNFS. If there is a script and additional multiple versions for subsets of Warewulf node groups (for example, `myscript`, `myscript._groupA`, `myscript._groupB`), then the script with no target extension is run only for those nodes that are not included in one of the specific groups (for example, not in `groupA` or `groupB`). For more information on CSM support for user-provided customization scripts, see the `CSM for AIX and Linux: Administration Guide`.

**Modify the Warewulf templates (optional)**

Before you proceed with the installation, you can alter the Warewulf templates for your diskless nodes, or provide additional data.

A Warewulf template is a directory containing files to configure and control Warewulf node and node group definitions, and to define and manage the VNFS and diskless boot image to be used by that

CSM for AIX and Linux: Planning and Installation Guide
Warewulf node group. Default templates are provided with CSM for each Linux operating system distribution version, service level, and architecture supported by CSM.

You can create a custom template by copying, renaming, and modifying a default template and setting the InstallTemplate attribute to your customized template directory. CSM will use this template to create a Warewulf node group with the same name as the template directory. All CSM nodes that use the same Warewulf template will be included in this Warewulf node group.

CSM uses Warewulf tools to create one VNFS and one diskless boot image for each Warewulf node group. Warewulf templates allow customization of the VNFS and the diskless boot image that is installed on the nodes.

The default template directory is as follows, where 
InstallDistributionName-InstallDistributionVersion-InstallServiceLevel-InstallPkgArchitecture matches the node attribute values:

```
/opt/csm/install/warewulf/warewulf-tmpl.
```

For example, the template name for Red Hat EL AS 4 QU3 POWER-based architecture is as follows:

```
/opt/csm/install/warewulf/warewulf-tmpl.RedHatEL-AS4-QU3-ppc64
```

The Warewulf configuration template is a directory that contains the following files:

- **config**
  Update this file for changing the users and user groups allowed access to this node image or this type of image: hybrid image versus RAM-Disk image. You can also use this file to configure user supplied diskless boot image, kernel, initrd or zimage for the Warewulf node group.

- **includes**
  Update this file to include files that are not in the VNFS. Files listed in the includes file are taken from the management server and built in the node image.

- **excludes**
  Update this file to exclude files in the VNFS from a RAM-Disk image. Update this file to define which files are included in the RAM-Disk image, and which files are excluded. This rule is similar to the rsync -exclude-from option. For more information, see the rsync man page.

- **excludes-aggressive**
  Update this file to specify files to be linked back to the VNFS in a hybrid type node image. Files not excluded remain in the RAM-Disk image.

- **wwinitrd.config**
  This is a configuration file for generating initrd. It is use to configure the modules needed in the initrd.

- **vnfrpm**
  This is a configuration file for csmsetupinstall to build a VNFS. It contains a list of RPM names that need be installed into the VNFS.

- **yum.conf**
  The Yum configuration files. The csmsetupinstall will use this file to generate a Yum configuration file for each VNFS on install server.

To create a custom version of the configuration template, copy the Warewulf template to another directory, modify the files, and give the directory a new name beginning with warewulf-tmpl. Keep the original template under its original name in the /opt/csm/install/warewulf directory. For example, to create a new template to modify for diskless compute nodes, enter:

```
269
```
When modifying template files, consider the following:

- Do not remove or modify the following lines:

```
################# DO NOT ERASE THIS SECTION (begin)#################
################# DO NOT ERASE THIS SECTION (end) #################
```

Do not edit any lines that appear in this section of the file. CSM may overwrite your customization changes to the file if these lines are not present.

- To use the default Warewulf template file instead of your custom template, set the `InstallTemplate` attribute to null for your diskless nodes. The next time you run `csmsetupinstall` for those diskless nodes, CSM will copy the correct default template from `/opt/csm/install/warewulf`.

- Do not edit the template files directly in the `/opt/csm/install/warewulf` directory; changes will be lost if you update CSM on your management server.

- See the `warewulf-tmpl` man page for information on Warewulf templates.

Run the `csmsetupinstall -k InstallTemplate` command to use the template for all diskless nodes processed by the command; or set the `InstallTemplate` attribute for each node to the path name of the new Warewulf template directory. The default configuration template is the original template in the `/opt/csm/install/warewulf` directory.

**Configure driver modules (optional)**

Use the following procedure to update a driver in the diskless boot image:

1. Place a copy of the driver in the `/csminstall/csm/drivers/kernel_version/arch` directory on the management server; for example `/csminstall/csm/drivers/2.6.9-5.EL/x86_64`. CSM recognizes the drivers by the suffix `*.ko` in the corresponding directories. The kernel used for the installation process and the kernel installed as part of the runtime operating system may be different. For example, in RHEL4 GA, the installation kernel is `2.6.9-5.EL`, but on the installed system the kernel may be `2.6.9-5.ELsmp`.

2. For diskless nodes, if the `kernel_version` matches the kernel running on the management server (which is the kernel that will be installed on the node), for example `2.4.21-15.ELBOOT`, then the driver also added into the VNFS and is used after the diskless node has been installed. For diskless nodes, the same kernel is used to boot the node, install the node, and run the node. The drivers are added to both the RAM-Disk image to be used for the diskless node installation and to the VNFS for diskless node runtime.

**Prepare for secondary adapter configuration (optional)**

Secondary adapters may be configured during the diskless node installation process. To use this support there are some additional steps that must be completed. Refer to [Secondary adapter interface configuration](#) for a description of how to use this CSM feature.
Configure a Linux diskless node installation

After you have prepared your Warewulf and VNFS configuration files and your Warewulf node templates, use the `csmsetupinstall` command to create the Warewulf configuration for your diskless nodes. The `csmsetupinstall` command does the following when run for diskless nodes:

- Optionally copies the required CDs to the `/csminstall` directory on the management server using the `csmsetupinstall -p PATH` option if it was specified. This action is only performed if you did not run the `copycds` command in a previous step.
- Initializes the Warewulf server on your install server.
- Uses the node install templates from the `csmsetupinstall -k InstallTemplate` option if specified or the node `InstallTemplate` attributes to create Warewulf node groups.
- Creates a VNFS if no VNFS exists, or if `csmsetupinstall BuildDisklessVNFS=build` is specified.
- Runs the user customization scripts in `/csminstall/csm/scripts/disklessprebuild` for the VNFS after a new VNFS has been built.
- Creates an initial RAM disk (`initrd`) from the VNFS.
- Builds a diskless boot image for each Warewulf node group.
- Creates and populates the `/tftpboot` directory.
- Creates or updates the `/etc/dhcpd.conf` file on the install server.
- Checks the network and starts the DHCP, NFS, and TFTP daemons on the install server.
- Collects and sets MAC addresses (`InstallAdapterMacaddr`) or UUIDs (`UUID`) for nodes, if the attributes are not already set.
- Sets the `InstallMethod` attribute to `warewulf` if the `-m` flag is specified.

For more details, see the `csmsetupinstall` man page or the CSM for AIX and Linux: Command and Technical Reference.

To automatically gather MAC addresses on System x 445 nodes, using `csmsetupinstall` or `getadapters`, the updated summit kernel needs to be installed on the CSM management server. To collect a MAC address, run the `getadapters` command. For more information, see Methods for collecting AIX MAC addresses. Also, see the `getadapters` man page.

Before you run `csmsetupinstall`:

- Set the `InstallServiceLevel` attribute to the correct value - the service level being installed on the node. If you are installing the base operating system, set the `InstallServiceLevel` attribute to `GA`. If you are installing a service level, set the attribute to a predefined value, such as `QU2`.
- If your install server is connected to multiple VLANs, you might need to configure DHCP to only listen to requests on specific interfaces.
- For Red Hat EL nodes on POWER-based architecture, if the `InstallAdapterMacaddress` is not set, you must close remote consoles for nodes before running `csmsetupinstall`; otherwise, the open remote consoles interfere with MAC address collection.
- For Red Hat EL 4 nodes on eServer 325 and 326 servers, run the `chnode` command to set the `HWType` attribute to `e325` or `e326`.
- For Red Hat EL 4 nodes on System x 346 64-bit architecture, run the `chnode` command to set the `HWType` attribute to `x346` or `8840`.
- To install from a non-eth0 NIC, ensure that you set the `InstallAdapterName` hardware attribute; see Hardware control attributes.
- If the Warewulf configuration files `/etc/warewulf/master.conf` and `/etc/warewulf/client.conf`, and `/etc/warewulf/wwinitrd.config` are not copies of the files provided by CSM, `csmsetupinstall` will save these files with a `.precsm` extension and create new files using the defaults provided with CSM in `/opt/csm/install/warewulf`. 
When `csmsetupinstall` builds the diskless boot images, their path name is
/srv/vnfs/WarewulfNodegroup. The following corresponding files are also created, in /tftpboot:
- /tftpboot/csm/ww-<WarewulfNodegroupName>gz
- /tftpboot/csm/ww-zimage-<WarewulfNodegroupName>
- /tftpboot/kernel
- /tftpboot/kernel-KernelVersion-Architecture
- /tftpboot/csm/ww-<WarewulfNodegroupName>z
- /tftpboot/wwinitrd.img
- /tftpboot/wwinitrd-KernelVersion-Architecture.img
- /srv/vnfs/<WarewulfNodegroupName>/vnfs.tar.gz

Some of these files are identical. Do not remove any of these files. They are checked by Warewulf and the nodes will not boot correctly if any of these files are removed from /tftpboot.

Running `csmsetupinstall`:

If you have already set the InstallMethod attribute to warewulf for all of your diskless nodes, you can run the `csmsetupinstall` command for these nodes by typing the following:

```
csmsetupinstall -N WarewulfNodes
```

You are prompted to insert the Linux operating system CDs if they have not already been copied.

The `csmsetupinstall` command saves the output to /var/log/csm/csmsetupinstall.log.

**Note:**

You can use the `csmsetupinstall` command with the "BuildDisklessVNFS=build" flag to force the rebuild of the VNFS if your existing VNFS is broken. By default, CSM does not rebuild the VNFS if it already exists. Also, you can use the "BuildDisklessImage=no" flag to not rebuild diskless boot images, which will save time if the boot images have already been created. By default, CSM always builds diskless boot images.

Also, you can use `csmsetupinstall` command with "BuildDisklessImage=no" flag to not build diskless boot images, which will save your time. In default, CSM always builds diskless boot images.

**Register host names**

Warewulf requires three hostname aliases for the install server and each diskless node:

- hostname-admin
- hostname-cluster
- hostname-sharedfs

Add these aliases to your nameserver or to the /etc/hosts file on your management server.

If you are using /etc/hosts for your cluster name service, Warewulf provides a tool to automatically add the correct aliases to your /etc/hosts file. If you already have an entry for your node, Warewulf will add additional alias entries. If you previously ran the Warewulf tool, the old Warewulf entries will be deleted and replaced with new entries. You can use the following command:

```
wwinit --hosts
```
Notice that this command has to be run on install server where the Warewulf node groups are configured. If you prefer, you can manually edit your `/etc/hosts` file to add the correct entries. This is a sample of the `/etc/hosts` file for your management server:

```
# Do not remove the following line, or various programs
# that require network functionality will fail.
196.0.0.1 localhost.localdomain localhost
# CSM Cluster network
184.20.20.1 ms06.clusters.com ms06 ms06-admin ms06-cluster ms06-sharedfs
184.20.20.2 node1.clusters.com node1
184.20.20.3 node2.clusters.com node2
184.20.20.4 node11.clusters.com node11 node11-admin node11-cluster node11-sharedfs
```

In this example, `ms06` is your management server, and `node11` is a diskless node. `node1` and `node2` are standard nodes.

**Note:**

The `/etc/hosts` file on your diskless node is generated by Warewulf. CSM does not use or modify this file unless secondary adapter support is configured and uses the `secondary_hostname` attribute. If you want a different `/etc/hosts` file on your diskless node, you can add the necessary Warewulf entries to the file and use CFM to distribute the host file from the CSM management server to the diskless node. If you are using CSM to configure secondary adapters for the node, CSM will add an entry to the `/etc/hosts` file on the node for each `secondary_hostname` attribute after CFM has updated the file during the diskless node installation.

**Create configuration files for nodes (optional)**

During the diskless boot image installation, CSM can automatically transfer system configuration files to the nodes. This task can be accomplished by setting up the Configuration File Manager (CFM) utility before installing your nodes. For information on configuring CFM, see the *CSM for AIX and Linux: Administration Guide*.

The CFM configuration files are distributed to the node when the `Mode` changes to `Managed` or when a `MinManaged` node finishes installation.

If you are using a hybrid diskless boot image, remotely mounted files on the node will be read-only. CFM will give errors for any file updates that are attempted to read-only filesystems. If files in the hybrid image are linked back to the VNFS, when CFM updates the file, the link will be removed and the file will be written to the RAM in the node. No updates will be made to the VNFS on the management server.

For diskless nodes, files updated by CFM will not be part of the diskless boot image the next time the node is booted and installed. CSM will run CFM to re-copy the files every time the diskless node is installed.

**Set up with user-provided customization scripts**

The `installnode` command will run any user-defined customization scripts that have been placed in the following directory:

```
/csminstall/csm/scripts/disklessboot
```

These scripts will be executed after the diskless boot image has been loaded on the node and is running.
This command checks this directory and runs each script on the node at the appropriate time. Subdirectories are not checked. If there are multiple scripts in a directory, they are run in alphabetical order, as determined by the `ls` command on the management server.

The naming convention for the scripts is:

```
scriptname[._target]
```

The `_` following the script name is required if the script is to only be used for a specific node or node group. The target value must be a single node name or group name that has been defined in the CSM database. If the target extension is not used, then the script will be run on all nodes. If there is a script and additional multiple versions for subsets of nodes (for example, `myscript`, `myscript_groupA`, `myscript_groupB`), then the script with no target extension is run only for those nodes that are not included in one of the specific groups (for example, not in `groupA` or `groupB`). For more information on CSM support for user-provided customization scripts, see the CSM for AIX and Linux: Administration Guide.

### Install the diskless boot image on the nodes

When a node is only defined, but not installed, its `Mode` attribute value is **PreManaged**. After you install the node through the `installnode` command, the `Mode` attribute value is changed to **Managed**. Before you run `installnode`, if a `Mode` attribute value of the node is **MinManaged**, after the node completes the installation, the attribute value of the node remains **MinManaged**.

You must run the `definenode` and `csmsetupinstall` commands before running the `installnode` command. If the `installnode` command fails for a **PreManaged** node, the `Mode` value is **PreManaged** or **Installing**. If the `installnode` command fails for a **MinManaged** node, the `Mode` value is **MinManaged** or **MinManaged-Installing**.

**Note:**

If a node has not been defined, it will not be installed. To install Linux diskless nodes, the `InstallAdapterName` attribute must be set before running the `csmsetupinstall` command. The Warewulf diskless node install process requires this information to configure the install adapter device on the node.

To install all Warewulf nodes, run the following command using the predefined nodegroup `WarewulfNodes`:

```
installnode -N WarewulfNodes
```

The nodes are rebooted and installed with the diskless boot image.

The installation runs asynchronously. Immediately after the installation process is initiated-when the node is rebooted-the `installnode` command exits, even though the installation might not be complete.

Use the `-t` flag on the `installnode` command to provide a timeout value, where `timeout` is the timeout value in minutes. If you do not specify a value for timeout, the default is 60 minutes:

```
installnode -N WarewulfNodes -t timeout
```
If the installation process does not complete within the timeout period specified, CSM considers the installation process as failed. You can use the `monitorinstall` command to provide output information for the installation process. See Monitor and verify the Linux diskless node installation.

After the diskless boot image is installed, the following activities happen on the node:

1. The node is joined to the CSM cluster.
2. The node's Mode attribute changes to Managed.
3. SSH is set up on the node so it can be accessed by the management server.
4. Any CFM files are transferred to the node.
5. The disklessboot customization scripts are run, including any secondary adapter configuration.

After a diskless node installation, the boot order in the BIOS of the node (non-pSeries) can remain in this order:

1. diskette
2. CD-ROM
3. network
4. hard disk

Every time the node needs to be booted, you must use the `installnode` command to start another diskless node installation for the node. Do not use the CSM `rpower` command or manually power the node, or it may not be correctly installed with the diskless boot image.

**Monitor and verify the installation**

For a Linux diskless node installation, you can use the `rconsole` command to view the progress of the installation on each node. To run the `rconsole` command on all the nodes, type the following:

```
rconsole -a
```

The `rconsole` command displays a console for each node in the cluster.

You can monitor the messages in `/var/log/messages` when you boot the node to help identify problems. For example, you might receive the following message that indicates a problem with the MAC address:

```
Receiving PXE-E51 No dhcp or bootp offers received
```

To check the results of the installation, you can use the `monitorinstall` command. The `monitorinstall` command starts the installation monitor tool, which displays the status of the installation on each of the nodes.

To run the `monitorinstall` command, type the following:

```
monitorinstall
```

The `monitorinstall` command writes output like the following:

```
<table>
<thead>
<tr>
<th>Node</th>
<th>Mode</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>clsn02.cluster.com</td>
<td>Managed</td>
<td>Installed</td>
</tr>
<tr>
<td>clsn03.cluster.com</td>
<td>Managed</td>
<td>Installed</td>
</tr>
<tr>
<td>clsn04.cluster.com</td>
<td>MinManaged</td>
<td>Installed</td>
</tr>
</tbody>
</table>
```
All nodes should be listed as Installed when their installation is complete. Any other status values that appear in the output represent the progress of the installation. Installation errors are indicated with a status code. The nodes will eventually reach the Installed state. If the installation times out as a result of using the `installnode` command, the status message reads **Install - timedout**.

To continuously display the output of the **monitorinstall** command, enter:

```
watch monitorinstall
```

To continuously display the install status for a single node in long format, enter:

```
watch monitorinstall -l node
```

For example:

```
watch monitorinstall -l f2x335n02.clusters.com
```

Output is similar to:

```
Every 2.0s: monitorinstall -l f2x335n02.clusters.com    Wed Aug 23 11:38:01 2006
Node f2x335n02.clusters.com
-----------------------------------
Wed Aug 23 11:31:19 EDT 2006: Configuring remote shell /usr/bin/ssh
Wed Aug 23 11:31:19 EDT 2006: Starting makenode to install CSM
```

If there is a problem, see **/var/log/csm/installnode.log** on the management server or **/var/log/csm/install.log** on the managed node for the installation log file.

To check the installation of the managed nodes, you can also use the **lsnode** command, as follows:

```
lsnode -a Mode
```

The **lsnode** command returns a list of the active cluster nodes, along with their **Mode** attributes values. Nodes that were successfully installed are set to **Managed** or **MinManaged**.

To verify that Remote Monitoring and Control (RMC) is working, use the **lsnode** command with the **-H** flag, as follows:

```
lsnode -H -l
```

**Note:**
The `lsnode -H -l` command can only be run on nodes with the *Mode* attribute set to **Managed**.

The `lsnode` command retrieves attribute values for each node.

To verify that `dsh` is working, run a `dsh` command. For example:

```
dsh -as date
```

A list of the cluster nodes is returned, with a date for each node.

---

**Managing and upgrading Linux diskless nodes**

To manage software on a diskless node, see the tasks under [Installing Linux diskless nodes](#). Note the following exceptions:

1. CSM does not support SMS on diskless nodes for software updates.
2. The `updatenode` command will not install packages on diskless nodes.
3. If using hybrid diskless boot images, excluded files listed in `excludes-aggressive.WarewulfNodeGroupName` are later linked to the mounted VNFS of the node. These files are read-only. If you are using a RAM-Disk diskless boot image, you are able to edit any files on a node. The changes made to a file on diskless nodes will be lost after the diskless nodes reboot.

Upgrading diskless nodes is like installing new diskless nodes, except that an upgrade just upgrades the CSM version level instead of the operating system version level of diskless nodes. In order to not disrupt the current operation of diskless nodes, you must create a new Warewulf template for upgrading nodes. Test your new template on a few nodes first, and then apply it to all nodes that need to be upgraded. Here are the steps for upgrading diskless nodes:

1. Run `copycds -A` on your management server to get new Linux distributions if needed.
2. Run `chnode -n test_node InstallCSMVersion=1.7.1` for target nodes.
3. Run `copycsmpkgs` to update the Yum and Warewulf software.
4. Update additional software packages if needed.
5. Update the install server if it is used.
6. Create a new Warewulf template for upgrade.
7. Change the node definitions. See Verify the node definitions. Set InstallTemplate of test nodes to use new Warewulf template.
8. Run `csmsetupinstall` with "BuildDisklessVNFS=build" flag to rebuild VNFS and diskless boot images for the target nodes.
9. Run `installnode` for the test nodes.
10. Test if the upgraded nodes are running as required.
11. Set InstallTemplate to new Warewulf template for all nodes that need to be upgraded.
12. Run `chnode -n test_node InstallCSMVersion=1.7.1` for the upgraded diskless nodes.
13. Run `csmsetupinstall` again for all upgrade nodes
14. Run `installnode` to install the upgraded diskless nodes.

**Note:**

- Regarding step 6, if you were using a customized VNFS configuration file(`vnfsrpmpm`), you need to copy this file into new Warewulf template. For example, if you customized

---
'/csminstall/diskless/vnfs/vnfsrpm.RedHatEL-AS4-QU4-i386', you need to run command below to copy it to the new Warewulf template.

cp /csminstall/diskless/vnfs/vnfsrpm.RedHatEL-AS4-QU4-i386 
/path/to/new_warewulf_template/vnfsrpm

If you were using a customized Warewulf initial ramdisk configuration file, You need to copy this file into the new Warewulf template. For example, if you customized '/etc/warewulf/wwinitrd.config.RedHatEL-AS4-QU4-i386', you need to run the following command to copy it to the new Warewulf template.

cp /etc/warewulf/wwinitrd.config.RedHatEL-AS4-QU4-i386 
/path/to/template/warewulf-tmpl.your_new_template_name/wwinitrd.config

- Regarding step 8, csmsetupinstall command will migrate the old customized template(e.g. CSM 1.6.0.x) to the current Warewulf template (e.g. CSM 1.7.1) automatically.
- Please don't try to restart network on running diskless nodes with SLES ditribution. Otherwise, it will hang, which is a known problem.


Below is an example on how to upgrade diskless nodes (RedHatEL-AS4-QU4-i386 distribution) from CSM 1.6 to CSM 1.7.

1. Upgrade CSM Management Server from 1.6 to 1.7. Please reference to Updating CSM for AIX and Updating CSM for Linux for more details.
2. Select a test diskless node, then update CSM version of the test node.
   
   chnode -n test_node InstallCSMVersion=1.7.1

3. Copy Yum and Warewulf software into csminstall.

   copycsmpkgs -p /path/to/warewulf_yum_packages

4. Create a new Warewulf template for upgrade. If you were using a customized Warewulf template before, run the following command to create your new customized Warewulf template.

   cp -r /path/to/template/warewulf-tmpl.your_old_template_name 
   /path/to/template/warewulf-tmpl.your_new_template_name

   **Note:** The csmsetupinstall command, which will be run later, will convert your old style template to a new style template automatically. If you were using a default Warewulf template before, we recommend that you continue use the new default Warewulf template provided by this release, unless you find some needed software or kenerl modules are missing. Missing software and kenerl modules may caused by:
a. The new default template uses minimum Linux operating system in this release, so some of the softwares are not installed by default.
b. You were using a customized vnfsrpm in the /csminstall/diskless/vnfs, so some of software are not installed by default.
c. You were using a customized wwinitrd.config in /etc/warewulf, so some of kernel modules are not installed by default.
d. You were using a customized yum.conf in /csminstall/diskless/vnfs/RedHatEL-AS4-QU4-i386/etc/, so some of package repositories are missing by default Warewulf template.

to get these missing software and modules back, you need to create an new Warewulf template as following:

e. Create a new Warewulf template

   $ cp -r /opt/csm/install/warewulf/warewulf-tmpl.RedHatEL-AS4-QU4-i386/ /path/to/template/warewulf-tmpl.your_new_template_name

f. Run the following command if you have customized vnfsrpm configuration file in /csminstall/diskless/vnfs.

   $ cp /csminstall/diskless/vnfs/vnfsrpm.RedHatEL-AS4-QU4-i386 /path/to/template/warewulf-tmpl.your_new_template_name/vnfsrpm

   $ cp /etc/warewulf/wwinitrd.config.RedHatEL-AS4-QU4-i386 /path/to/template/warewulf-tmpl.your_new_template_name/wwinitrd.config

   $ cp /csminstall/diskless/vnfs/RedHatEL-AS4-QU4-i386/etc/yum.conf /path/to/template/warewulf-tmpl.your_new_template_name/yum.conf

5. Set the InstallTemplate. If you had created a new Warewulf template.

   $ chnode -n test_node
   InstallTemplate=/path/to/template/warewulf-tmpl.your_new_template_name

   If you are going to use a default template, let the InstallTemplate blank.

   $ chnode -n test_node InstallTemplate=""

6. Rebuild VNFS and diskless boot images.

   $ csmsetupinstall -n test_node BuildDisklessVNFS=build

7. Boot test diskless node.

   $ installnode -n test_node

8. Test if the upgraded nodes are running as required. If it works as expected, you can use the new Warewulf template for all target diskless nodes.
Coexistence

CSM supports both standard nodes and diskless nodes in the same cluster. CSM 1.7.0 will not support CSM 1.6.0 diskless nodes, user must migrate their diskless node to CSM 1.7.0's level. For more information, please see Managing and upgrading Linux diskless nodes section above.
Chapter 18. Uninstalling CSM

To uninstall CSM management server software and remove CSM cluster definitions and log files, run the `uninstallms` command. The command performs the following tasks when run on the CSM management server:

- Uninstalls CSM management server software
- Removes node group definitions.
- Removes cluster node definitions using the `rmnode` command
- If the `-u` flag is specified, the command performs clean up on the node by running the `rmnode -u` command. This clean up includes removing CSM log files and uninstalling CSM packages from Linux nodes. See the `rmnode` command for details.
- Removes predefined conditions.
- Removes CSM log files.
- Removes `csm.bluegene` and related predefined resources, if present, from the management server.

The `rmnode` command also cleans up all traces of the node, including the following entries. If the node has an install server, the `rmnode` command also cleans up traces of the node on the install server.

- PXE configuration file
- Kickstart or AutoYaST configuration file
- Node entry in `/etc/dhcpd.conf` file
- Node entry in RDM database
- Node entry in `/csminstall/csm/config/sms.info` file
- The node's configuration information (`config_info`) file
- Node customization scripts
- All files for the node in the `/cfmroot` directory
- The node status file in the `/csminstall/csm/status` directory
- All log files for the node in the `/var/log/csm` and `/var/log/consoles` directories

On an AIX management server, the `uninstallms` command removes CSM management server software such as `csm.server`, `csm.deploy`, and `csm.gui`. It does not uninstall any CSM file sets that were installed as part of base AIX; for example, `csm.core`, `csm.client`, `csm.dsh`, and `csm.diagnostics`. HPC application file sets, including `csm.gpfs` and `csm.loadl`, are uninstalled.

Note:

Running the `installp -u` command on an AIX management server to remove CSM file sets does not remove the CSM database definitions or log files.

On a Linux management server the `uninstallms` command removes all the CSM and RSCT packages, however it will not uninstall `csm.core`, or any open source packages that were automatically installed with the Linux operating system, or any open source prerequisites that may have been installed. The command will not remove any of the `/csminstall` directories since they may contain data not pertaining to CSM. If the Linux management server is also a CSM node (has `csm.client` installed), `uninstallms` does uninstall `csm.client`, `csm.core`, `rsct.core`, `rsct.core.utils` or `src`. If `rsct.basic` is installed, `uninstallms` does not uninstall `rsct.basic`, `rsct.core`, `rsct.core.utils` or `src`.

For example, to remove the nodes and uninstall the management server, enter:

```
uninstallms -u
```
Chapter 19. Installation scenarios

The following installation scenarios for AIX and Linux are provided as general examples only. Specific environments may require more detailed configuration.

CSM for AIX cluster configuration

This scenario describes basic steps for setting up a CSM management server, and using CSM to install AIX on cluster nodes. It assumes the following:

- The systems to be used as the management server and nodes are supported hardware.
- You have the latest AIX CDs and the CSM CD containing the CSM license.
- The system to be used as the management server has been installed with AIX.
- You have internet access so that you can download required software.
- You want to use the CSM hardware control support.
- The CSM management server and all the nodes are on the same subnet.
- You will be using `rsh` for the remote shell.
- No additional configuration or customization will be needed on the nodes.

Install the CSM for AIX management server

To install a CSM for AIX management server:

1. Update the $PATH and $MANPATH variables:
   ```bash
   export PATH=$PATH:/opt/csm/bin
   export MANPATH=$MANPATH:/opt/csm/man
   ```

2. Create the `/csminstall` file system:
   ```bash
   crfs -v jfs2 -g rootvg -m /csminstall -a size=1024M -a bf=true
   mount /csminstall
   ```

3. Download CSM updates:
   - Copy the tar file to `/tmp/csm`
   - Unwrap the file. For example:
     ```bash
     gunzip csm-aix-1.7.1.0.tar.gz
     tar -xvf csm-aix-1.7.1.0.tar
     ```

4. Download and install `openCIMOM 0.8` from:
   - `ftp://linuxpatch.ncsa.uiuc.edu/csm/noarch/`. Use the `rpm` command to install it. For example:
5. Install CSM management server software. Insert AIX CD Number 1 and issue the following command:

```
geninstall -IaX -d /dev/cd0 csm.server csm.deploy csm.gui.dcem csm.gui.websm \  R:expect R:tcl R:tk R:conserver
```

**Note:**
The rpm packages of expect/tcl/tk are replaced by new installp packages in AIX 6.1.3 or later. For AIX 6.1.3 or later nodes, please run following commands:

```
geninstall -IaX -d /dev/cd0 expect tcl tk csm.server csm.deploy csm.gui.dcem csm.gui.websm \R:conserver
```

6. Apply management server software updates:

```
geninstall -IaX -d/tmp/csm all
```

7. Accept the CSM license. Insert the license CD, then accept the license and activate the license key, using the `mount` and `csmconfig` commands, as follows:

```
mount -v cdrfs -o ro /dev/cd0 /mnt
csmconfig -c -L /media/csmlum.full
```

The `-c` flag also copies various CSM files to `/csminstall` subdirectories.

8. Store hardware control point user IDs and passwords using the `systemid` command. For example, if the host name of a Hardware Management Console (HMC) is `hmc01` and the user ID is `hscroot`, issue the following command:

```
systemid hmc01 hscroot
```

9. Verify that the CSM management server has been set up correctly:

```
probemgr -p ibm.csm.ms -l 0
```

**Define CSM for AIX nodes**

To define CSM for AIX nodes:

1. Use the `lshwinfo` command to gather hardware control information about the nodes. For example, if the HMC is `hmc01`, issue the following command:

```
lshwinfo -p hmc -c hmc01
```

2. Use the `definenode` command to define the cluster nodes. In the following example the name of the node to define is `clstrn12`, the name of the HMC is `hmc01`, the `PowerMethod` is `hmc`, and the `HWControlNodeId` is `lpar12`. In this example default values will be set for the other required node attributes:

```
definenode -n clstrn12 -H hmc01 HWControlNodeId=lpar12 PowerMethod=hmc
```
Install CSM for AIX nodes

To install CSM for AIX nodes:

1. Get the install adapter information:
   - Get the install adapter information: and create an adapter stanza file. For example, for each node gather information about an ethernet adapter that can be used as the install adapter.
     
     ```
     getadapters -a -D -t ent -s 100 -d full -z mystanzafile
     ```
   
   - Check the stanza file and make any necessary modifications.
   
   - Save the install adapter information in the database.
     
     ```
     getadapters -w -f mystanzafile
     ```

2. Set up the AIX Network Installation Manager (NIM):

   ```
   nim_master_setup -B
   ```
   (This command creates the basic NIM resources and the `basic_res_grp` resource group.)

3. Create NIM machine definitions. To create NIM machine definitions for all AIX nodes using the CSM node definitions issue the following:

   ```
   csm2nimnodes -N AIXNodes
   ```

4. Set up NIM to add the nodes to the CSM cluster during the node installation:

   ```
   csmsetupnim -N AIXNodes
   ```

5. Prepare NIM for the installation.

   ```
   nim -o bos_inst -a source=rte -a boot_client=no -a group=basic_res_grp AIXNodes
   ```

6. Initiate a network boot.

   ```
   netboot -N AIXNodes
   ```

Using `alt_disk_install` for AIX nodes

The AIX `alt_disk_install` feature provides a method for applying software updates to an alternate system image while the node remains running and available. Once the alternate system image has been updated, you can use the alternate disk to reboot the node. As a result, you can reduce maintenance down time to the time it takes to reboot the node. In addition, if you discover a problem with the updates, you can reboot the original system image.

NIM support for `alt_disk_install` allows you to manage the installation of alternate disks on remote nodes. In a CSM cluster environment, you can use the `alt_disk_install` features that are supported by NIM.

For a complete description of the AIX `alt_disk_install` support, see the `AIX Installation Guide and Reference`.

CSM for AIX and Linux: Planning and Installation Guide
The following scenario illustrates how to use `alt_disk_install` to apply software updates and emergency fixes (efixes) to the nodes of a CSM cluster. Follow these basic steps:

- Copy the running system image (rootvg) to an alternate disk.
- Apply the updates to the alternate disk image.
- Use the alternate disk to reboot the node.

**Assumptions for the scenario:** Consider the following assumptions for this scenario:

- Both software updates and efixes are to be applied to the nodes. You might receive efix packages from IBM with commands, library archive files, or scripts. AIX provides efix packaging `epkg` and efix manager `emgr` commands to support the tracking and management of efixes on a system. NIM also supports the updating of nodes with efixes.
- The CSM management server, which also serves as the NIM master, has been installed and updated. This scenario focuses on updating the nodes.
- All the nodes are receiving the same updates; however, you can also apply different updates to different nodes or sets of nodes if needed.
- You can follow the steps in this scenario for any number of nodes up to the documented CSM scaling limit.
- Before you start, NIM has been set up, including installation, configuration, and resource creation.
- The `alt_disk_install` updates are done 20 nodes at a time. You can install and update the alternate disks while the nodes are fully operational; however, the installations can result in increased network usage, and you might need to adjust the fanout value (20). You can use NIM resource servers to speed up the process, but this complicates the procedure and as a result might not be worthwhile.
- Before you can use any of the AIX `alt_disk_install` support, you must install the `bos.alt_disk_install` file set.
- Some of the commands use `AIXNodes` as the name of a NIM machine group. This group is initially created automatically as a CSM node group. The corresponding NIM machine group is created when the `csm2nimgrps` command is run as part of the initial installation of the CSM cluster. See Create AIX NIM machine groups (optional).
- An additional disk must be available with sufficient space to hold a rootvg system image.

After you reboot, consider running the CSM `updatenode` command to update the cluster nodes. The `updatenode` command distributes configuration files, runs user-provided customization scripts, and sets up authentication. If you do not need to perform these updates, you do not need to run the command.

To update all of the AIX cluster nodes, issue the following command:

```
updatenode -N AIXNodes
```

Note: It is important to have the CSM MS database properly have the Node attributes InstallCSMVersion, InstallDistributionVersion in sync with the target CSM and AIX levels when working with alternate disk environments.

**Installing bos.alt_disk_install**

Before you can use the `alt_disk_install` feature for the first time, you must ensure that the `bos.alt_disk_install` file set is installed on both the CSM management server (NIM master) and the cluster nodes. Follow these steps:
1. Add the `bos.alt_disk_install` file set to your `lpp_source`. The `bos.alt_disk_install` file set is located on the AIX installation media volume 2. For example, if you place the volume 2 CD into the directory `/dev/cd0` and your `lpp_source` is named `530lpp_res`, issue the following command:

   ```nim -o update -a source=/dev/cd0 -a packages=bos.alt_disk_install 530lpp_res```

2. To install `bos.alt_disk_install` on the CSM management server (NIM master), issue the following command.

   ```installp -acgXd /dev/cd0 bos.alt_disk_install```

3. To install `bos.alt_disk_install` on each AIX node, issue the following command:

   ```nim -o cust -a lpp_source=610lpp_res -a file sets=bos.alt_disk_install -a concurrent=20 AIXNodes```

**Using alt_disk_install**

When you have ensured that the `bos.alt_disk_install` file set is installed, follow these steps to copy the updates and use `alt_disk_install`.

1. Set the `global_exports` attribute to `yes` on the management server (NIM master). Always set this attribute when you are simultaneously running NIM operations to many nodes.

   ```nim -o change -a global_export=yes master```

2. Copy the updates to the `lpp_source` directory. For example, if the `lpp_source` resource is named `530lpp_res`, the updates are on the directory `/dev/cd0`, and you want to copy all the updates for csm.core and csm.client, issue the following command:

   ```nim -o update -a source=/dev/cd0 -a packages="csm.core csm.client" 530lpp_res```

3. Create `emgr/ppc` subdirectories in the `lpp_source` directory. The `lpp_source` directory is the directory that you have used when you created the NIM `lpp_source` resource. For example, if your `lpp_source` directory is `/export/nim/lppsrc`, issue the following command to create the required subdirectories:

   ```mkdir -p /export/nim/lppsrc/emgr/ppc```

4. Copy the `efixes` to the `lpp_source` directory. For example, if the `efix IY47618.081803.epkg.Z` is in the directory `/tmp`, issue the following command to copy the `efix` to the `lpp_source` directory:

   ```cp /tmp/IY47618.081803.epkg.Z /export/nim/lppsrc/emgr/ppc```

5. Perform the `alt_disk_install` operation on each node. In this example, the `rootvg` of the running system is to be cloned on to `hdisk1`. All the updates that are in the `lpp_source` directory are to be installed on the alternate image and the bootlist is to be set to `boot` from `hdisk1`. The `AIXNodes` group contains all AIX nodes and the concurrent attribute is set so that a maximum of 20 nodes are to be installed at one time.

   ```nim -o alt_disk_install -a disk=hdisk1 -a source=rootvg -a \ set_bootlist=yes -a boot_client=no -a file sets=ALL -a \ lpp_source=530lpp_res -a concurrent=20 AIXNodes```
6. Check the NIM Cstate value to ensure that the `alt_disk_install` operation completes on the nodes. Issue the `lsnim` command as follows:

   `lsnim -a Cstate`

Note:
To check the nodes that belong to a NIM machine group, issue the following `lsnim` command, where `AIXNodes` is the name of a group:

   `lsnim -g AIXNodes`

When the system indicates that the values for the nodes are ready for a NIM operation, continue to the next step.

**Booting the nodes**

When the alternate disk installations have completed, issue the following command to simultaneously boot all the nodes to their alternate disks:

   `nim -o reboot AIXNodes`

When the nodes have completed rebooting, verify the software that is affected by the updates. If any problems occur, reboot the nodes back to the original image. To reboot the original image, run the following two commands. This example assumes that all the clients have the original `rootvg` installed on `hdisk0`:

   `dsh -N AIXNodes bootlist -m normal hdisk0`
   `nim -o reboot AIXNodes`

**Using mksysb for AIX nodes**

A `mksysb` image is the system backup image created by the AIX `mksysb` command. You can use this image to install other servers, or to restore the server that was the source of the `mksysb`.

NIM supports the use of `mksysb` images. Performing a NIM `mksysb` installation is faster than performing a NIM `rte` installation, and with `mksysb`, you can optionally include other installed software. You can use a `mksysb` image to install the nodes of a CSM cluster.

For a complete description of the AIX `mksysb` support, see the *AIX Installation Guide and Reference*.

When a `mksysb` is installed, code in RSCT determines if the `mksysb` is being restored to the source node or cloned to a new node. If the `mksysb` is installed on a new node, RSCT removes and reinitializes certain node specific data contained in the directory `/var/ct/cfg`. This data includes the RSCT node ID and the Host Based Authentication (HBA) Trusted Host List. If the `mksysb` is restored to the source node, the cleanup and initialization is not done.

When creating a `mksysb` of a node in a CSM cluster that uses Kerberos Version 5 for remote commands, you must determine whether to exclude the Kerberos key table file from the image. By default the file is in `/etc/krb5/krb5.keytab`. If the purpose of the `mksysb` is to create new cluster nodes, exclude the `krb5.keytab` file. If you do not exclude the Kerberos keytab, after the `mksysb` is restored to the new node, use the Kerberos `kadmin` command with option `ktremove` to remove the host key of the source node from the `krb5.keytab` on the new node.
The basic process to create a \texttt{mksysb} image and use it to install new cluster nodes is as follows:

1. Create NIM resources for all nodes to be installed.
2. Complete the installation of a single node by doing a NIM \texttt{rte} install.
3. Install any optional software.
4. Create a \texttt{mksysb} image from the installed node.
5. Use the \texttt{mksysb} image to install the other cluster nodes.

\textbf{Note:}

Do not use a \texttt{mksysb} image that is created on the management server to install the nodes.

This scenario describes how to use a \texttt{mksysb} image to perform an initial installation of the nodes. It assumes that the CSM management server is installed and that you have defined the cluster nodes.

1. For all the cluster nodes, in \textbf{Installing AIX on nodes} perform \textbf{Verify CSM for AIX node definitions} through \textbf{Prepare for AIX secondary adapter configuration (optional)}. These steps allow you to define the NIM resources that you need to install all the nodes but do not install the nodes.
2. Continue the installation process for a single node. This node is to be the source of the \texttt{mksysb} image. For this node, in \textbf{Installing AIX on nodes} perform \textbf{Add OpenSSH and OpenSSL software for AIX} through \textbf{Enable Kerberos Version 5 remote commands for AIX (optional)}.
3. Working with this single node, perform the installation verification tasks and any other applicable procedures in \textbf{CSM post-installation tasks}.
4. Use the NIM \texttt{cust} operation to install additional software as needed.
5. Use the installed node to create a NIM \texttt{mksysb} resource and a \texttt{mksysb} image as follows:

\begin{verbatim}
nim -o define -t mksysb -a server=master -a \location=/export/nim/mksysb/610_mksysb -a mk_image=yes -a \source=clstrn05 clstr_mksysb
\end{verbatim}

In the example, the name of the NIM \texttt{mksysb} resource that is created is \texttt{clstr_mksysb} and the name of the \texttt{mksysb} images is \texttt{610_mksysb}.

If this CSM cluster uses Kerberos Version 5 for remote commands, exclude the Kerberos key table file from the image. By default the file is in \texttt{/etc/krb5/krb5.keytab}.

\textbf{Notes:}

- The \texttt{mksysb} file created from the node may be larger than the maximum file size on your management server. You can change the file size limit by editing \texttt{/etc/security/limits} (set it to -1 for unlimited), and rebooting your machine.

6. Define the CSM for AIX nodes:

Use the \texttt{lshwinfo} command to gather hardware control information about the nodes. For example, if the HMC is hmc01, issue the following command:

\begin{verbatim}
lshwinfo -p hmc -c hmc01
\end{verbatim}

Use the \texttt{definenode} command to define the remaining nodes in the cluster. In the following example, the name of the node to define is clstrm12, the name of the HMC is hymc01, the PowerMethod is hmc, and the HWControlNodeId is lpar12. In this example, default values will be set for the other required node attributes:
7. Get the install adapter information:
   o Get the install adapter information and create an adapter stanza file. For example, for each
     node, gather information about an ethernet adapter that can be used as the install adapter.
     
     ```
     getadapters -a -D -t ent -s 100 -d full -z mystanzafile
     ```
   o Check the stanza file and make any necessary modification.
   o Save the install adapter information in the CSM database
     
     ```
     getadapters -w -f mystanzafile
     ```

8. Create the NIM machine definitions.
   o First create a CSM node group containing all the nodes that will be installed using the
     `mksysb` image. For example, if all the nodes in the cluster will be installed using the
     `mksysb` image except clstrn01.clusters.com, run the following command to create the
     clstr_nodes group:
     
     ```
     nodegrp -w "Hostname not like 'clstrn01.clusters.com'" clstr_nodes
     ```
   o Next, create NIM machine definitions for all AIX nodes using the CSM node definitions:
     
     ```
     csm2nimnodes -N clstr_nodes
     ```

9. Set up NIM to add the nodes to the CSM cluster during the node installation:

     ```
     csmsetupnim -N clstr_nodes
     ```

10. If you are installing a large number of nodes, enable the multithreaded option on the NIM `nimesis`
    daemon by setting the `max_nimesis_threads` value. Setting this value improves the performance
    of NIM when you are working with large numbers of nodes. You can specify a value from 20 to
    150. The general rule is to set it for approximately half the number of nodes on which you are
    operating simultaneously. For example, to install 100 nodes, set the value to 50. Issue the following
    command to set the `max_nimesis_threads` value:

     ```
     nim -o change -a max_nimesis_threads=50 master
     ```

11. If you are installing a large number of nodes, set the `global_exports` attribute to `yes` on the
    management server (NIM master). Always set this attribute when you are simultaneously running
    NIM operations to many nodes.

     ```
     nim -o change -a global_export=yes master
     ```

12. Issue the `bos_inst` operation for the rest of the nodes:

     ```
     nim -o bos_inst -a source=mksysb -a mksysb=clstr_mksysb -a spot=610spot_res \
         -a boot_client=no clstr_nodes
     ```

    In the example, `clstr_nodes` is a node group that contains the rest of the AIX cluster nodes. Because
    the Shared Product Object Tree (SPOT) resource `610spot_res` has been used to install the node
    `clstrn05`, which in a previous step has been used to create the `mksysb` image, both are at the same
    level. The `mksysb` image must be at the same level as the SPOT, a fundamental NIM resource that
    provides network boot support for client machines.
13. Initiate a network boot

```
netboot -N clstr_nodes
```

14. If Kerberos Version 5 is being used for CSM remote commands and your remote shell is `rsh`,
examine your security settings using the `lsauthent` command. If necessary, enable `rsh` usage of
Kerberos Version 5 authentication by running the `chauthent` command with the appropriate
arguments.

---

**Red Hat EL on System x cluster configuration**

This scenario describes the basic steps for setting up a Red Hat EL on System x management server, and
using CSM to install Red Hat EL on System x nodes. It assumes the following:

- The management server and node servers are all supported System x hardware.
- You have the Red Hat EL product CDs.
- You have the CSM for Linux Multiplatform CDs containing the CSM license.
- You are installing the same version of Red Hat EL on the management server and nodes.
- You are using CSM to install Red Hat EL on the nodes.
- You have internet access for downloading the required additional software.
- You plan to use CSM hardware control.
- The CSM management server and all nodes are on the same subnet.
- You are using `ssh` for the remote shell.
- You are not doing any optional node configuration or customization.

The following `/tmp/nodedef` node definition file is used in this example, which configures Red Hat EL AS 4:

```
nodel.clusters.com:
    ConsoleMethod = mrv
    ConsoleServerName = cs01.clusters.com
    ConsolePortNum = 14
    ConsoleSerialDevice = ttyS0
    ConsoleSerialSpeed = 9600
    PowerMethod = xseries
    HWControlPoint = hcp01.clusters.com
    HWControlNodeId = nodel
    InstallAdapterName = eth0
    InstallCSMVersion = 1.7.1
    InstallDistributionName = RedHatEL-AS
    InstallDistributionVersion = 4
    InstallMethod = kickstart
    InstallOSName = Linux
    InstallPkgArchitecture = i386
```

**Install a Red Hat EL management server**

To install a Red Hat EL management server:

1. Download the latest version of CSM:
o Download the System x Linux tarball from:

o Copy the tarball to /tmp/csm

o Unzip and untar the file. For example:

   cd /tmp/csm
   tar -xzvf csm-linux-1.7.1.0.i386.tar.gz

2. Install csm.core:

   rpm -U csm.core-*.rpm

   Logoff and log back in to pick up changes to $PATH and $MANPATH.

3. Install and configure the rest of CSM on the management server:

   installms -p /tmp/csm

   installms prompts you for the Red Hat EL CDs.

4. To accept the CSM license, insert the CSM license CD, accept the license, and activate the license key:

   mount -o ro /dev/cdrom /media/cdrom
   csmconfig -L /media/cdrom/csmlum.full

5. Store hardware control point user IDs and passwords using the systemid command:

   systemid hcp01.clusters.com myuserid

6. Verify that the CSM management server has been set up correctly:

   probemgr -p ibm.csm.ms -l 0

For additional steps to perform once you are up and running in this environment, see Configuration 2: Red Hat EL on System x cluster.

**Define and install Red Hat EL nodes**

To define and install Red Hat EL nodes:

1. Create the nodedef file.

2. Define the nodes:

   definenode -f /tmp/nodedef

3. Test remote console and remote power; both are required for step 4. The rconsole opens an xterm window, so you must have an X server running before running this command:

   rpower -n node1 query
   rconsole -n node1

4. Gather MAC addresses, and configure the node installation:
csmsetupinstall -n node1

After **csmsetupinstall** collects the node's MAC address, it prompts you for the Red Hat EL CDs.

5. Install the node:

installnode -n node1

6. Watch the progress of the install using one of these two methods:
   o Run **monitorinstall** every two seconds:

        watch monitorinstall

   o Open a remote console window on the node:

        rconsole -n node1

---

**SLES on System p cluster configuration**

This scenario describes the basic steps for setting up a SLES 9 on System p management server, and using CSM to install SLES 9 on the cluster nodes. It assumes the following:

- The management server and node servers are all supported System p hardware; for example, System p5 550 servers.
- You are using CSM to install SUSE Linux Enterprise Server (SLES) 9 service pack 1 (SP1) on your nodes; and you have the SLES 9 and SLES 9 SP1 CDs.
- You have the CSM for Linux on POWER CD containing the CSM license.
- The management server has been installed with SLES 9.
- You have internet access for downloading required software.
- You are using CSM hardware control.
- The CSM management server and all nodes are on the same subnet.
- You are using **ssh** for the remote shell.
- No additional node configuration or customization is required.

The following /tmp/nodedef node definition file containing one node is used in this scenario:

```
node1.clusters.com:  
ConsoleMethod = hmc  
ConsoleServerName = hmc01.clusters.com  
HWControlNodeId = node1  
HWControlPoint = hmc01.clusters.com  
InstallCSMVersion = 1.7.1  
InstallDistributionName = SLES  
InstallDistributionVersion = 9  
InstallOSName = Linux  
InstallPkgArchitecture = ppc64  
InstallServiceLevel = SP1  
PowerMethod = hmc
```

For additional steps to perform once you are up and running in this environment, see **Configuration 3: SUSE Linux Enterprise Server (SLES) on System p cluster**.
**Install the SLES management server**

To install a SLES 9 management server:

1. Download the latest version of CSM and unzip and untar the file:
   - Download the CSM for Linux on POWER tarball from
   - Copy the tarball to `/tmp/csm`
   - Unzip and untar the file. For example:
     ```
     cd /tmp/csm
     tar -xzvf csm-linux-1.7.1.0.ppc64.tar.gz
     ```

2. Install `csm.core`:

   ```
   rpm -U csm.core-*.rpm
   ```

3. Log off and log back in to pick up changes to `$PATH` and `$MANPATH`.

4. Install and configure the rest of CSM on the management server:

   ```
   installms -p /tmp/csm
   ```

   The `installms` command prompts for the SLES 9 and SLES 9 SP1 CDs.

5. Store hardware control point user IDs and passwords using the `systemid` command:

   ```
   systemid hmc01.clusters.com hscroot
   ```

6. Accept the CSM license. Insert the CSM license CD, accept the license, and activate the license key:

   ```
   mount -o ro /dev/cdrom /media/cdrom
   csmconfig -L /media/cdrom/csmlum.full
   ```

7. Verify that the SLES management server has been set up correctly:

   ```
   probemgr -p ibm.csm.ms -l 0
   ```

**Define and install SLES nodes**

To define and install SLES nodes:

1. Create the `nodedef` file as shown previously.

2. Define the node:

   ```
   definenode -f /tmp/nodedef
   ```

3. Test remote console and remote power (both are required for step 4). The `rconsole` opens an xterm, so be sure to have an X server running before you issue this command:

   ```
   rpower -n node1 query
   rconsole -n node1
   ```
4. Configure the node installation:

   First copy the SLES 9 GA CDs:

   ```bash
   copycds InstallDistributionName=SLES InstallDistributionVersion=9 \
   InstallServiceLevel=GA
   ```

   You will be prompted for the SLES 9 GA CDs.

   Run `csmsetupinstall` to copy the SP1 disks and set up for the install:

   ```bash
   csmsetupinstall -n node
   ```

   You will be prompted for the SLES 9, service pack 1 (SP1) CDs.

5. Install the node:

   ```bash
   installnode -n node1
   ```

6. Watch the progress of the install using one of these two methods:
   - Run `monitorinstall` every two seconds:
     ```bash
     watch monitorinstall
     ```
   - Open a remote console window on the node:
     ```bash
     rconsole -n node1
     ```

---

### Updating the service level of CSM for Linux

Use the following steps to update CSM for Linux to a new service level; for example, to update CSM for Linux 1.6.0.0 to CSM for Linux 1.7.0.0. For detailed information on updates, see [Updating CSM on Linux nodes](#).

1. Download the latest CSM service level from
   ```bash
   ```
2. Untar the service package to `/tmp/csm` using the `tar -xzvf filename` command.
3. Run the `rpm -U /tmp/csm/csm.core-*` command.
4. Run the `installms -p /tmp/csm` command.
5. Accept the CSM license, if necessary. Run the `lsnode` command to verify the license.
6. Merge changes in Kickstart or AutoYaST template files, if necessary.
7. Run the `updatenode -a` command.
Chapter 20. Migrating the AIX operating system

You can use the migration installation method to upgrade your CSM for AIX cluster to a later version of AIX. A migration installation attempts to update rather than overwrite file systems, and to preserve all user configuration while installing a later level of the AIX operating system. During a migration, the installation process determines which optional software products are installed, and updates them to the new versions. Resources that can be updated but not overwritten include directories, such as /home, /var, and /usr, the root volume group, logical volumes, system configurations, and previously installed software. After migration, the only completely overwritten file system is /tmp. To avoid losing information stored in /tmp, copy the files to another directory before the migration.

Before you perform a migration, back up your data and any customized applications or volume groups. For instructions on how to create a system backup, see "Creating System Backups" in the AIX Installation Guide and Reference.

To perform a migration, you must have the AIX product CDs for the target version.

Migrating an AIX management server

During the migration of the CSM for AIX management server, any cluster applications or production jobs that do not specifically depend on the management server continue running without interference. However, any system management functions that run from the management server are not available.

Backing up CSM for AIX data

Though AIX migration preserves most of your CSM data, you can also back up your CSM database before migrating. To back up your CSM database, issue the following command:

```
csmbackup
```

If necessary, you can restore CSM data after migration using the csmrestore command.

Update CSM for AIX prerequisites

You may need to update the following prerequisite open source RPM packages for CSM for AIX. They are not automatically installed during the migration, but are available on the AIX product media:

- conserver
- expect
- tcl
- tk

Note:
The rpm packages of expect/tcl/tk are replaced by new installp packages in base CD of AIX 6.1.3 or later. CSM can work together with either rpm packages or installp packages. If you want to migrate from AIX 6.1.2 or earlier to AIX 6.1.3 or later, you can choose keep those rpms. Otherwise, you need uninstall the rpm packages of expect/tcl/tk, then install the new installp packages which are available on AIX product media of base CD.

See Optional CSM for AIX open source software for details on required open source software.

For example, to install a new level of conserver you could copy the new RPM package from AIX CD-ROM #1 and use the rpm command to install it. If the name of the new conserver package is conserver-8.1.aix5.2.ppc.rpm, you could issue the following command:

```
rpm -U conserver-8.1.aix5.2.ppc.rpm
```

**Note:**

conserver-8.1.aix5.2.ppc.rpm installs conserver-8.1.7-2 on the system.

The following open source software is required for certain CSM features, and may also have to be updated:

- openCIMOM
- autoupdate
- sg3-utils

The openCIMOM software is installed on the management server; if you have Linux nodes, you must install autoupdate and sg3-utils on the nodes.

**Perform the AIX system migration**

Migrate your CSM for AIX management server to a later level of AIX using the Migrating AIX procedure described in the AIX Installation Guide and Reference, at http://publib.boulder.ibm.com/infocenter/pseries/v5r3/index.jsp. The migration process updates all of the CSM for AIX file sets. If you have NIM configured, the process preserves all NIM data and definitions.

**Accept the CSM for AIX license agreement**

You must accept the license agreement for the new CSM release to function properly. If the license agreement is not accepted, the CSM commands fail with a message that indicates that the license agreement has not been accepted and that you must run the csmconfig -L command. On the management server, run the following command to view the license agreement:

```
csmconfig -L
```

After you view the license agreement, the command gives you the option of accepting or rejecting the terms and conditions of the license. A new license key file does not have to be provided with the -L flag when you migrate CSM. CSM copies the key to the following directory:

```
/var/opt/csm/lic
```
Check the success of the license acceptance by running the **csmconfig** command again with no flags. In the output of the command the *ExpDate* and *MaxNumNodesInDomain* values indicate the status of the license acceptance. See the **csmconfig** man page for a description of these attributes.

**Note:**

When running the **csmconfig** command, the *LicenseProductVersion* attribute describes the version of the license key used with the **csmconfig** -L command, not the version of CSM running on the management server. A new version of CSM does not require you to purchase a new full license key, so the version of CSM on the system and the value of the *LicenseProductVersion* attribute may differ. For example, if you purchased a full license key for CSM 1.5 and passed the key to CSM using the **csmconfig** -L *license_key* command, the *LicenseProductVersion* attribute displayed is **1.5**. If you then migrated to CSM 1.6, which accepts CSM 1.5 license keys, you will have full access to CSM 1.6 without having to purchase a new license key. The version of CSM on the management server is **1.6**, but the version defined using the *LicenseProductVersion* attribute by **csmconfig** is **1.5**, because that is the version of the license key provided to CSM.

To check the *LicenseProductVersion* attribute value, run:

```
lsrc -p0 IBM.DmsCtrl | grep LicenseProductVersion
```

CSM 1.7.0 accepts CSM 1.5, CSM 1.6, and CSM 1.7 license keys.

**Copy the files to /csminstall**

Issue the **csmconfig** command to copy updated CSM files into the /csminstall subdirectories:

```
csmconfig -c
```

CSM uses the files when the CSM system management scripts are run on the cluster nodes.

**Using a NIM server**

If your CSM management server is also the NIM server, see the *AIX Installation Guide and Reference* to create new AIX NIM resources for installing or migrating CSM nodes to a later version of AIX.

**Verifying the AIX installation (optional)**

To verify that the management server is installed correctly and ready for use, you can run the **ibm.csm.ms** probe, as follows:

```
probemgr -p ibm.csm.ms -l 0
```

For information on CSM support for probes, see the *CSM for AIX and Linux: Administration Guide*.
Migrating an AIX install server

If you are using AIX install servers, you can update the install server operating system in one of two ways:

- If the install server was installed using a NIM master server, you can migrate using the standard NIM support for migrating AIX clients.
- If NIM cannot be used to migrate the install server, use the standard AIX migration procedures for a standalone server. This process is described in the AIX: Commands Reference.

When you have completed the migration, update the InstallCSMVersion and InstallDistributionVersion attributes for the install server nodes. Then run the updatenode command for the install server to make sure any additional CSM updates are applied. After AIX install server is migrated, new NIM resources need to be added. For example, if the install server is migrated from AIX 5.2 to 5.3, AIX 5.3 lpp_source and spot must be created to install or migrate other nodes to AIX 5.3.

Migrating AIX nodes

Migrate your AIX node operating systems using the standard AIX support. This support includes the AIX Network Installation Manager (NIM) for conventional remote migration installations and remote alternate disk migration installations. These procedures are described in the AIX: Installation Guide and Reference, at http://www.ibm.com/servers/aix/library.

Attention:

If an install server is the NIM master for a node, NIM commands must be run on the install server. These commands can be issued from the management server using the dsh command.

Remote AIX migration

For remote AIX migration installation, do the following:

1. Create the following required resources for AIX nodes:
   - SPOT
   - lpp_source
   - resolv_conf
   - bosinst_data
2. Modify the NIM node's bosinst_data to indicate that you want to perform the migration.
3. Perform the NIM bos_inst operation using the rte source to complete the migration process.

Note:

Run the csmsetupnim command before doing the installation, to execute CSM scripts during the installation and automatically return the nodes to Managed Mode. Alternatively, you can run the updatenode command after the installation is complete.
Using the remote alternate disk to perform AIX migration

NIM remote alternate disk migration installation support uses the AIX `alt_disk_install` feature to copy a node `rootvg` to an alternate disk, and simultaneously migrate it to a new AIX version or release. The migration is performed while the system is up and functioning normally. When the migration on the alternate disk is complete the node can be rebooted to that image. This method can reduce downtime and provides a quick way to revert to the previous operating system level, without requiring an additional disk. See the documentation for the `nimadm` command in the *AIX Installation Guide and Reference.*

**Note:**

Migrating the CSM management server does not require that you also migrate the cluster nodes.

When you complete the migration, update the following attributes for the updated nodes:

- `InstallCSMVersion`
- `InstallDistributionVersion`

For example, to update all the node definitions to CSM Version 1.7.1 and AIX 5.3.0, enter the following command:

```
chnode -a InstallCSMVersion=1.7.1 InstallDistributionVersion=5.3.0
```

After you reboot, you can run the CSM `updatenode` command to update the cluster nodes. The `updatenode` command distributes configuration files, runs user-provided customization scripts, and sets up authentication.

To update all of AIX cluster nodes, enter:

```
updatenode -N AIXNodes
```
Chapter 21. Upgrading the Linux operating system

To upgrade your Linux management server and nodes with a later version of the Linux operating system, you can either perform the CSM for Linux upgrade procedure, or reinstall Linux. Upgrading Linux preserves your existing configuration, including CSM configuration. Reinstalling Linux replaces your existing configuration. Your decision can also depend on the type of upgrade and the Linux distribution and version.

Attention: If you choose to reinstall Linux on your management server, to preserve your CSM configuration you must back up your data before reinstalling by running the `csmbackup` command. After reinstalling, restore your CSM data using the `csmrestore` command.

Before you perform an upgrade or reinstallation, ensure that you have reliable backups of your data and any customized applications. For instructions on how to create a system backup, refer to the instructions provided with your Linux distribution.

Upgrading the Linux management server

During the upgrade or reinstallation of the CSM management server, any applications or production jobs that do not specifically depend on the management server continue running normally. System management functions that must be run from the management server are not available.

Note: Before upgrading to Red Hat EL 5, increase the `/usr` partition size.

You can upgrade Linux on your management server in two ways:

1. Reinstall the Linux operating system with a later version of the Linux distribution. This method requires you to back up the CSM data before the reinstallation (using `csmbackup`), and restore the CSM data after the reinstallation (using `csmrestore`).
2. Upgrade the operating system without overwriting user data. This is only supported for upgrading to a new SLES service level. With this method, you are not required to back up and restore your CSM data.

Backing up CSM for Linux data

Before reinstalling Linux on your management server, you must back up your CSM data so that it can be restored after the reinstall. It is also important to back up your data before doing an operating system upgrade, in case something goes wrong during the upgrade. The back up and restore procedures assume that you are restoring data on a machine that has the same host name as the hardware on which you backed up the data. Ensure that your data is stored safely on remote hardware. See the *CSM for AIX and Linux: Administration Guide* for details on backing up and restoring CSM and ERRM data.
Performing the Linux upgrade or reinstallation

Upgrading the Linux management server by reinstalling:

Use the upgrade or installation procedures provided in your Linux operating system documentation:

- Red Hat EL: http://www.redhat.com/docs/manuals/enterprise/

Upgrading the Linux management server without reinstalling:

This procedure is only supported for upgrading the management server to a SLES 9 service level:

1. Run the `copycds` command to copy the new service level files from the CDs or ISOs to the `/csminstall` tree.
2. Run `online_update`, pointing to the path in `/csminstall` containing the SLES 9 distribution. For example:
   
   ```
   online_update -u /csminstall/Linux/SLES/9/i386/SP3/unitedlinux-sp3
   ```
3. Reboot the management server.

Restoring your CSM for Linux data

If you upgraded your Linux management server by reinstalling, you must reinstall CSM; see Installing a CSM for Linux management server. You must also replace your CSM data on the management server by copying the saved data file from the remote server, and running the `csmrestore` command to restore your data. See the CSM for AIX and Linux: Administration Guide for details on backing up and restoring CSM and ERRM data.

Upgrading a Linux install server

Perform the following steps to upgrade the Linux operating system on an install server. To upgrade, the install server must already be a Managed node; see Setting up install servers.

Important:

- You must upgrade an install server before upgrading the cluster nodes that it serves.

There are several options for upgrading a Linux install server:

- If the management server is installed with the same Linux distribution as the install server, you can use it to upgrade the install server; see Upgrading Linux nodes for details.
- For multiple install servers installed with the same Linux distribution, you can upgrade one install server manually and use it to upgrade the other install servers; see Installing Linux on nodes for details.
- Upgrade the install server using the Linux product CDs.
To use the management server to reinstall an install server, follow the procedures in *Upgrading Linux nodes* to upgrade your install server. To reinstall an install server manually or from another install server, do the following:

1. Install the operating system
2. Update the install server's node attributes
3. Run `updatenode` on the install server to reinstall CSM and add the install server to the cluster.

---

**Upgrading Linux nodes**

Upgrading the Linux operating system on Linux nodes can be done in two ways:

- Upgrade the node operating system; this preserves configuration data including CSM; see *Upgrading Linux on nodes*.
- Reinstall the node operating system with a later release. Reinstalling the operating system replaces all configuration data and CSM, so you must back up all node data on a remote server. Perform the following steps to reinstall the operating system on a node:
  1. Update the following node attributes, using the `chnode` command, to match the characteristics of the new operating system level:
     - `InstallOSName`
     - `InstallDistributionName`
     - `InstallDistributionVersion`
     - `InstallPkgArchitecture`
     - `InstallServiceLevel`
  2. Run the `copycsmpkgs` or the `copycds` command, or both; see *Copy CSM packages for Linux nodes* and *Copy CDs for SLES nodes*.
  3. Install the operating system on the nodes. Run the `csmsetupinstall` and `installnode` commands. For example:

        csmsetupinstall -n nodename
        installnode -n nodename

  4. Monitor and verify the install. Refer to *Installing Linux on nodes*.

**Upgrading Linux on nodes**

**Attention:** This upgrade procedure is only supported for Linux operating systems that were installed using CSM, as described in *Installing Linux on nodes*.

As an alternative to reinstalling Linux on your nodes, you can upgrade your Linux nodes with a later Linux release or service level. Upgrading your Linux nodes preserves your existing configuration and CSM, which includes: setup services, paths, `/etc/hosts`, `resolv.conf`, and user IDs.

**Note:**

Optionally, during the operating system upgrade, you can also upgrade CSM to the latest level.

You can perform the following types of Linux operating system upgrades on Managed and MinManaged CSM nodes:
1. Upgrade the SUSE Linux Enterprise Server (SLES) operating system on nodes from a base release to a later service level; for example, from SLES 9 GA to SLES 9 SP3.

**Note:**
SLES9 SP4 and SLES 10 service level upgrades are not supported.

2. Upgrade the SLES operating system on nodes from one service level to a later service level; for example, from SLES 9 SP1 to SLES 9 SP3.
3. Upgrade the Red Hat EL operating system on nodes from one Red Hat EL release to another; for example, from RHEL4 to RHEL5.
4. Upgrade Red Hat EL from a service level or GA to Red Hat EL 5 or Red Hat EL 5.1, Red Hat EL 5.2 or Red Hat EL 5.3.


CSM upgrades the SLES operating system by running the YaST online update tool on the specified nodes.

CSM uses Kickstart to upgrade the Red Hat EL operating system. The Kickstart configuration file is provided by CSM.

New directories are provided for customization scripts specific to operating system upgrades. The scripts in these directories are run during the operating system upgrade process.

**Note:**
1. You can upgrade MinManaged nodes using the managed node upgrade procedure.
2. To upgrade diskless nodes, add the RPMs to the diskless image and reboot with that new image. For more on diskless nodes, see [Using Linux diskless nodes](#).

**Linux node upgrade prerequisites**

**Before upgrading SLES 9 nodes, you must meet the following upgrade prerequisites:**

- CSM 1.7.1 is installed on the management server and any install servers.
- The `updatenode` or `installnode` commands have been run on the node, and the node *Mode* attribute value is *Managed* or *MinManaged*.
- CSM was used to install the node operating system. If CSM was not used to install the Linux operating system, some configuration must be done manually. Configuration scripts run during a CSM installation, but not during an upgrade, are located in `/csminstall/csm/scripts/installprereboot` and `/csminstall/csm/scripts/installpostreboot`. If CSM was not used to install Linux on the nodes, review these scripts and manually perform the equivalent actions before using CSM to upgrade the nodes.

**Before upgrading Red Hat EL nodes, you must meet the following upgrade prerequisites:**

- CSM 1.7.1 is installed on the management server and any install servers.
- CSM was used to install the node operating system. If CSM was not used to install the Linux operating system, some configuration must be done manually. Configuration scripts run during a CSM installation are located in `/csminstall/csm/scripts/installprereboot` and `/csminstall/csm/scripts/installpostreboot`. If CSM was not used to install Linux on the nodes,
review these scripts and manually perform the equivalent actions before using CSM to upgrade the nodes. For upgrades, Red Hat EL nodes are not required to be Managed or MinManaged.

- If a Red Hat EL node has external storage attached to a secondary SCSI device or FiberChannel PCI adapter, it must be powered off or disconnected before you upgrade the operating system. Upgrading SLES nodes does not require disabling these devices.

**Check Linux node software requirements**

See Planning for CSM software to verify that you are upgrading to supported node software.

**Set the Linux node boot order**

The node boot order required for upgrades is the same as the boot order required for installation. If you used CSM to install the operating system on your nodes, do not change the boot order for these nodes. If you did not use CSM to change the boot order, see Install CSM and Linux on nodes.

**Set Linux node attributes**

To upgrade Linux nodes, define the node attributes as follows, using the chnode command as required:

1. Set the InstallMethod attribute to you for SLES node upgrades.
2. Set the InstallMethod attribute to kickstart-upgrade for Red Hat EL node upgrades.
3. Copy the SLES GA CDs, if you have not already copied them.
4. For SLES nodes, verify that the InstallDistributionVersion attribute value is the version currently installed on the nodes. Change the attribute value if necessary.
5. For SLES nodes, set the InstallServiceLevel attribute value to the service level you are upgrading to.
6. For Red Hat EL nodes, set the InstallDistributionVersion attribute value to the version you are upgrading to.
7. For Red Hat EL nodes, optionally set the InstallServiceLevel attribute value to the service level you are upgrading to.

**Copy CSM packages for Linux nodes**

If any of the following node attribute values are different than the management server attribute values, you must run the copycsmpkgs command before upgrading:

- InstallOSName
- InstallDistributionName
- InstallDistributionVersion
- InstallPkgArchitecture
- InstallServiceLevel
- InstallCSMVersion

Run the copycsmpkgs command for each node being upgraded. In the following example, node is the node hostname for which packages are copied, and path is the path name to the CSM RPMs. If any RPM packages are missing, you are prompted to insert the distribution CD.

```
copycsmpkgs -p path -n node
```
If you are upgrading multiple nodes that all have the same upgrade attribute values, run `copycsmpkgs` for only one of the representative nodes.

**Copy CDs for SLES nodes**

When upgrading SUSE Linux Enterprise Server (SLES) 9 nodes to a service level, you must copy both the GA CDs and the service level CDs. Copy the SLES 9 GA CDs if you have not already copied them. Later, when you run `csmsetupinstall` in Configure a SLES installation, the service level CDs are copied.

For example, if you are upgrading nodes from SLES 9 GA to SLES 9 SP1, run the following command, where `PATH` is the path containing the SLES 9 GA CDs:

```
copycds -p PATH InstallDistributionName=SLES InstallDistributionVersion=9 InstallServiceLevel=GA
```

**Modify Red Hat EL configuration templates (optional)**

Red Hat EL Kickstart configuration templates include basic elements for node configuration such as base packages to upgrade, disk partitioning schemes and root passwords. You can add additional configuration information in the post-installation sections for Kickstart.

**Note:** This step is only required for Red Hat EL nodes; SLES node upgrades do not use the AutoYaST node configuration template.

**Red Hat EL Kickstart node configuration template**

The default Red Hat Enterprise Linux (EL) Kickstart node configuration template for upgrades is as follows, where `InstallDistributionName` and `InstallDistributionVersion` matches the `InstallDistributionName` and `InstallDistributionVersion` node attribute values. Some template files also have an appended `-Arch` extension, which matches the `InstallPkgArchitecture` attribute value:

```
/opt/csm/install/kscfg.tmpl.InstallDistributionNameInstallDistributionVersion\ [-Arch].upgrade
```

For example, the node upgrade configuration template for Red Hat EL AS 4 i386 architecture is:

```
/opt/csm/install/kscfg.tmpl.RedHatEL-AS4.upgrade
```

For example, the upgrade template name for Red Hat EL AS 4 POWER-based architecture is:

```
/opt/csm/install/kscfg.tmpl.RedHatEL-AS4-ppc64.upgrade
```

To create a customized Red Hat EL Kickstart upgrade configuration template, copy the `.upgrade` version of the CSM Kickstart configuration template file and rename the copy, preserving the `.upgrade` extension. Set the `InstallTemplate` node attribute to the custom file name. If you use the same base file name for your install and upgrade Kickstart configuration templates, set your `InstallTemplate` attribute to the base file name; the `csmsetupinstall` command automatically finds the upgrade Kickstart configuration template. If an upgrade Kickstart configuration template with the same base name as the install Kickstart configuration template does not exist, CSM uses the default upgrade Kickstart configuration template file. If you do not set the `InstallTemplate` attribute, CSM uses the default upgrade Kickstart configuration template file.
Kickstart node configuration scripts

CSM includes Kickstart configuration templates for Kickstart upgrades in the /opt/csm/install directory. The Kickstart configuration templates only include basic elements for the node configuration such as base packages to upgrade, disk partitioning schemes and root passwords. You can include additional configuration in the respective post-installation sections for Kickstart; the %pre and %post keywords identify the pre-configuration and post-configuration sections of the Kickstart configuration file:

[%pre]
#CSMVAR:STTYCRTSCTS#
#INCLUDE:#ENV:TEMPLATESCRIPTS#/pre.#ENV:EFFECTIVE_DISTRO_NAME#.ENV:ARCH#
[%post]
#INCLUDE:#ENV:TEMPLATESCRIPTS#/post.#ENV:EFFECTIVE_DISTRO_NAME#.ENV:ARCH#

These parts of the configuration file are separated into several scripts that the Kickstart configuration template merges with the final install image created on each node. The scripts that perform the basic CSM functions and set variables are in the following location, where distribution is the InstallDistributionName attribute value:

/opt/csm/install/templatescripts/[pre|post].distribution[.arch]

These scripts are appended to the Kickstart configuration template files when you run the csmsetupinstall command. Do not edit the scripts included in the %pre and %post sections, and do not remove the #INCLUDE lines. To make changes, use the customization scripts described in Setting up Linux customization scripts.

Recompile Linux driver modules

An operating system upgrade changes the kernel level. If you used CSM to install driver modules for the original kernel level, and have driver modules in /csminstall/csm/drivers/old-kernel-level, you must recompile your driver modules and copy them to /csminstall/csm/drivers/new-kernel-level. See Configure Linux driver modules for details.

Linux secondary adapter configuration (optional)

Secondary adapters can be configured during a node upgrade or when adding a node to the cluster. To use this support, see Secondary adapter interface configuration.

Configure Red Hat EL upgrades

After preparing any custom Kickstart configuration templates, run the csmsetupinstall command to create a Kickstart configuration file for each node you are upgrading. The csmsetupinstall command uses the information from your Kickstart template to create a Kickstart configuration file for each node on the install server. For Red Hat EL upgrades, set the InstallMethod attribute to kickstart-upgrade before running csmsetupinstall. The csmsetupinstall command does the following:

- Copies the required CD-ROMs to the /csminstall directory on the management server.
- Synchronizes the install servers by copying the applicable files in /csminstall from the management server to the install servers.
- Creates and populates the /tftpboot directory on the install servers.
- Installs the **dhcp**, **tftp**, **syslinux**, and **nfs** packages on the install server. If `NetworkInstallProtocol=http` and `SetupNetworkInstallProtocol=1`, the HTTP package is also installed.
- Creates or updates the `/etc/dhcpd.conf` file on the install servers.
- Checks the network and starts the DHCP, NFS, and TFTP daemons on the install servers. If `NetworkInstallProtocol=http` and `SetupNetworkInstallProtocol=1`, the HTTP daemon is also checked.
- Collects and sets MAC addresses (InstallAdapterMacaddr) or UUIDs (UUID) for nodes, if the attributes are not already set.
- Creates a Kickstart configuration file for each node on the install servers.

For command usage details, see the `csmsetupinstall` man page or the *CSM for AIX and Linux: Command and Technical Reference*.

If you are not using remote power or remote console, use the [Installing Linux nodes without hardware control](#) procedure to upgrade your cluster.

To upgrade Red Hat EL, run the `csmsetupinstall` command. For example:

```
csmsetupinstall -N -p RedHatELAS4Nodes
```

If the `/csminstall/Linux` directories are not already populated with the contents of the Red Hat EL CDs, you are prompted to insert the CDs. The copy progress is indicated by a percentage (%) value.

The `csmsetupinstall` command saves the output to the following log file:

```
/var/log/csm/csmsetupinstall.log
```

### Configure SLES upgrades

Once you have set the `InstallMethod` attribute to **you** for all the SLES nodes to upgrade, use the `csmsetupinstall` command to copy the SLES files. The `csmsetupinstall` command does the following for SLES upgrades:

1. Copies SLES images to the `/csminstall` directory on the management server
2. Synchronizes applicable `/csminstall` contents from the management server to the install servers
3. Checks the network and starts the NFS daemons on the install servers.

For details, see the `csmsetupinstall` man page or the *CSM for AIX and Linux: Command and Technical Reference*.

To upgrade SLES nodes, run the `csmsetupinstall` command. For example, to upgrade all SLES 9 nodes, enter:

```
csmsetupinstall -N -p SLES9Nodes
```

If the `/csminstall/Linux` directories are not already populated with the contents of the SLES CDs, you are prompted to insert the CDs. The copy progress is indicated through a percentage (%) value.

The `csmsetupinstall` command saves the output to the following log file:

```
/var/log/csm/csmsetupinstall.log
```
Running csmsetupinstall for SLES upgrades

To upgrade SLES on the nodes, run the `csmsetupinstall` command. For example, to upgrade all the SLES 9 nodes, run the following command:

```
csmsetupinstall -N -p SLES9Nodes
```

If the `/csminstall/Linux` directories are not already populated with the contents of the SLES CD-ROMs, you are prompted to insert the SLES CD-ROMs. The copy progress is indicated through a percentage (%) value.

The `csmsetupinstall` command saves the output to the following log file:

```
/var/log/csm/csmsetupinstall.log
```

Configure a Linux on HMC-attached System p upgrade

Collecting MAC addresses concurrently for a large number of Linux on HMC-attached System p nodes can return `hmc_nodecond` errors. In this case, limit MAC address collection to one node at a time per HMC by setting the `CSM_LIMIT_OFW_SESSIONS` environment variable, and rerunning the `export` command. This increases the time to complete the command, but reduces the load on the HMC and management server. The value of the variable is not significant; only whether it is defined or not. In a `ksh` environment, use the following command to set the variable:

```
export CSM_LIMIT_OFW_SESSIONS=1
```

In a `ksh` environment, use the following command to clear the variable:

```
unset CSM_LIMIT_OFW_SESSIONS
```

Verify Linux node upgrade configuration

Run the `ibm.csm.node-install` probe to verify that the nodes are correctly configured and ready to be upgraded. This probe ensures that all node attributes are correct, installation source files are available, and installation configuration files have been created. For example:

```
probemgr -p ibm.csm.node-install -l 0
```

For more details, see Using probes, the CSM for AIX and Linux: Administration Guide, and the `probemgr` command in the CSM for AIX and Linux: Command and Technical Reference.

Update Linux DHCP configuration

After the `csmsetupinstall` runs the first time, you can customize the `/etc/dhcpd.conf` file. Do not remove or modify any CSM entries when modifying the new `/etc/dhcpd.conf` file. Use the `mkdhcp` tool to add or delete your own entries in the `/etc/dhcpd.conf` file.
Update Kickstart configuration

You can modify the Kickstart configuration file that the `csmsetupinstall` command generates on the install server for each node. The file name is:

```
/csminstall/csm/CSMVersion/kickstart.InstallDistributionName/
InstallDistributionVersion/node-ip-address-kickstart
```

For example, a file for Red Hat EL AS 4 is similar to:

```
```

If the install server is not on the management server, then the first part of the path name is either `/csmserver`, by default, or if set, the `InstallServer` attribute value. For example:

```
```

Modify this file after running the `csmsetupinstall` command. Modifying the file affects only the settings on the specific node. If you rerun `csmsetupinstall`, you overwrite the file, so use care when you modify a generated file.

**Note:**

There is no SLES configuration file for upgrades.

Create configuration files and RPM updates for the Linux nodes (optional)

During a node operating system upgrade, CSM installs both the configuration file manager (CFM) configuration files and Software Maintenance System (SMS) RPMs on the nodes.

Though Kickstart and YaST online updates will upgrade RPMs, SMS can be used in addition to these tools in order to upgrade individual RPMs that are not part of the Red Hat EL or SLES distribution.

Configure Linux customization scripts

When upgrading node operating systems, the `installnode` command runs any customization scripts that have been placed in the following two directories:

1. The scripts in this directory are run after the node has been upgraded, but prior to node reboot:
   2. `/csminstall/csm/scripts/osupgradeprereboot`
2. The scripts in this directory are run after the first node reboot, and after CSM has been installed:
   3. `/csminstall/csm/scripts/osupgradepostreboot`

The `installnode` command checks these directories and runs each script on the node at the appropriate time. Subdirectories are not checked. If there are multiple scripts in a directory, they are run in alphabetical order, as determined by the `ls` command on the management server.

The naming convention for the scripts is:

```
scriptname._target
```
The _ following the script name is required to use the script for a specific node or node group only. The target value must be a single node name or group name that has been defined in the CSM database. If the target extension is not used, then the script will be run on all nodes. If there is a script and additional multiple versions for subsets of nodes (for example, myscript, myscript._groupA, myscript._groupB), then the script with no target extension is run only for those nodes that are not included in one of the specific groups (for example, not in groupA or groupB). For more information on CSM support for customization scripts, see the CSM for AIX and Linux: Administration Guide.

To use Kerberos with remote commands, you can use customization scripts for enabling remote commands to authenticate with Kerberos. See Enabling remote commands to use Kerberos Version 5 authentication.

Modifying or deleting CSM for Linux scripts

Because subsequent installations and updates of CSM also update the osupgrade[pre|post]reboot scripts, do not change them in the /csminstall/csm/scripts/osupgrade[pre|post]reboot directory. Instead, copy the script to the following directory and modify the script there:

/csminstall/csm/scripts/data

In this way, you can override the CSM osupgrade[pre|post]reboot scripts.

All CSM osupgrade[pre|post]reboot scripts contain a flag in the beginning of the script to check if a script of the same name exists in the /csminstall/csm/scripts/data directory. If a script with the same name exists, CSM runs the override script instead of the standard script.

To list the post-installation prereboot or postreboot scripts to be used during operating system upgrade, enter the following command:

    nodegrp -s nodename | xargs -i find /csminstall/csm/scripts/osupgradeprereboot\ /csminstall/csm/scripts/osupgradepostreboot -name *\{\}\.

Example - modifying a Linux script

To modify the script 006CSM_adduser._LinuxNodes:

1. Copy the following:
   2. /csminstall/csm/scripts/osupgradeprereboot/006CSM_adduser._LinuxNodes

   to the following directory:

   /csminstall/csm/scripts/data

3. Edit the script.

   When you perform the node upgrade, if a modified 006CSM_adduser._LinuxNodes script exists in the /csminstall/csm/scripts/data directory, CSM runs the modified script instead of the standard script.
Example - deleting a Linux script

To not run the
/csminstall/csm/scripts/osupgradeprereboot/001CSM_updateDrivers._LinuxNodes script, which updates the drivers on the server:

1. Copy the following:

    /csminstall/csm/scripts/osupgradeprereboot/006CSM_adduser._LinuxNodes

    to the following directory:

    /csminstall/csm/scripts/data

2. Remove the contents of the following script so that it is blank:

    /csminstall/csm/scripts/osupgradeprereboot/001CSM_updateDrivers._LinuxNodes

When you perform the upgrade on the node, CSM calls the blank script and does not update the drivers. The original script remains in the following location:

    /csminstall/csm/scripts/osupgradeprereboot/001CSM_updateDrivers._LinuxNodes

Set up Linux node kernel updates (optional)

To use a kernel other than the default kernel, you can use the updateKernel script to install the kernel after the Linux upgrade, but before the node reboot. This allows the node to reboot with the new kernel. Copy the /opt/csm/samples/install/updateKernel script to /csminstall/csm/scripts/osupgradeprereboot before installing the node. See the /opt/csm/samples/install/updateKernel.README file for more information.

Provide Linux Kerberos client packages (optional)

If you plan to use Kerberos Version 5 for remote commands, ensure that the Kerberos client packages are available for installation. See CSM for Linux Kerberos setup.

Place the required Kerberos packages in the following directory, where InstallDistributionName is the Linux distribution, InstallDistributionVersion is the Linux version, and InstallPkgArchitecture is the Linux architecture. SMS is then able to install the packages when you use installnode in Install CSM and Linux on nodes.

    /csminstall/Linux/InstallDistributionName/InstallDistributionVersion/InstallPkgArchitecture/install

Upgrade the Linux operating system and CSM

Before you can upgrade the SLES operating system on a node, its Mode attribute must be Managed or MinManaged. That is, you must have previously run installnode or updatenode for the node. This is because the management server must be able to dsh to the node so that it can run the YaST online_update tool. Updating the Red Hat EL operating system on a node does not require the node to be in Managed or MinManaged mode.
When updating the Red Hat EL or SLES operating system on nodes, if the Mode attribute is PreManaged, then after the operating system upgrade, the Mode attribute value is changed to Managed. If the Mode attribute is Managed, then it is not changed. If the Mode attribute is MinManaged before the operating system upgrade, then the Mode attribute value remains MinManaged.

If the installnode command fails for a PreManaged node, the attribute value of the node is PreManaged or Installing. If the installnode command fails for a MinManaged node, the attribute value of the node is MinManaged or MinManaged-Installing.

If hardware control is not configured, see Installing Linux nodes without hardware control for more information.

To upgrade the operating system and CSM on all the nodes, issue the following command:

```
installnode -a
```

The Red Hat EL nodes with the InstallMethod attribute set to kickstart-upgrade are rebooted and upgraded with the new level of the operating system, rebooted, and then CSM is updated if necessary. The Red Hat EL operating system upgrade runs asynchronously. Immediately after the operating system upgrade process is initiated (that is, when the node is rebooted), the installnode command exits, even though the operating system upgrade is not complete.

The SLES nodes with the InstallMethod attribute set to you are updated with the new level of the operating system, rebooted to pick up the new kernel, and then CSM is upgraded if necessary. The installnode command continues to run as the SLES operating system is updated. This may take a while to run. Then, installnode reboots the node, and exits. The rest of the upgrade process (CFM, SMS, osupgradepostreboot scripts, upgrading CSM) continues asynchronously.

You can use the -t flag on the installnode command to provide a timeout value in minutes. If you do not specify a value for timeout, the default is 60 minutes:

```
installnode -P -t timeout
```

If the operating system upgrade process does not complete within the timeout period specified, CSM considers the operating system upgrade process as failed. You can use the monitorinstall command to provide output information for the installation process. See Monitor and verify CSM and Linux installations.

After the operating system is updated, the following jobs run on the node:

1. The osupgradeprereboot customization scripts are run.
2. The node reboots to its local hard disk.
3. CSM is installed, along with the software listed in Planning for CSM for Linux.
4. The node's Mode attribute changes to Managed, or remains MinManaged.
5. SSH or RSH are set up on the node so that the node is accessible from the management server.
6. Any CFM files are transferred to the node.
7. SMS is run to install or update software, if it is configured.
8. The osupgradepostreboot customization scripts are run.

If you defined Kerberos options with the csmconfig command when you defined the management server, the installnode command sets up the Kerberos options for the cluster. See Set up Kerberos Version 5 for remote Linux command processing (optional).
After an operating system upgrade on System x, the node BIOS boot order can remain:

1. diskette
2. CD-ROM
3. network
4. hard disk

Every time the on System x node boots, it uses Dynamic Host Configuration Protocol (DHCP) to contact the management server or install server, which uses pxelinux to boot the node from its hard drive. Alternately, after the operating system upgrade is complete, you can change the boot order in the BIOS to the following:

1. diskette
2. CD-ROM
3. hard disk
4. network

Note:
When you run the installnode command on SLES nodes, NFS error messages can occur. You can ignore these error messages; see NFS warnings.

Linux on HMC-attached System p nodes

Linux on HMC-attached System p nodes can return reboot errors while concurrently upgrading large numbers of nodes. In these cases, limit the installations to one node at a time per HMC by setting the CSM_LIMIT_OFW_SESSIONS environment variable, and rerunning the installnode command. This increases the time to complete the command, but reduces the load on the HMC and management server. The value of the variable is not significant; only whether it is defined or not. In a ksh environment, you can use the following command to set the variable:

```bash
export CSM_LIMIT_OFW_SESSIONS=1
```

In a ksh environment, use the following command to clear the variable:

```bash
unset CSM_LIMIT_OFW_SESSIONS
```

Monitor and verify the Linux operating system upgrade

During a Red Hat EL operating system upgrade, you can use the rconsole command to view the progress of the upgrade on each node. To run the rconsole command on all nodes, enter the following:

```bash
rconsole -a
```

The rconsole command displays a console for each cluster node configured for hardware control.

You can monitor the messages when you boot the node to help identify problems. For example, the following message indicates a MAC address problem:

```
Receiving PXE-E51 No dhcp or bootp offers received
```

During a SLES operating system upgrade, the installnode command shows the output of the upgrade on the node's console. You can specify the -v (verbose) flag to see detailed information, or look at the
/var/log/csm/installnode.log. After the operating system has been upgraded, the node reboots, and you can use the rconsole command as described above to view the remainder of the upgrade process.

To check the results of the operating system upgrade, you can use the monitorinstall command, which displays the status of the upgrade of each of the nodes. It displays messages indicating the progress of the upgrade, and eventually displays one of the following messages at the completion of the upgrade process:

- installed
- not installed
- failed install
- install-timedout

To run the monitorinstall command, enter the following:

```
monitorinstall
```

The monitorinstall command returns output similar to:

```
Node               Mode              Status
-----------------------------------------------
clsn01.ibm.com     Managed          Installed
clsn02.ibm.com     Managed          Installed
clsn03.ibm.com     MinManaged       Installed
clsn04.ibm.com     MinManaged       Installed
clsn05.ibm.com     MinManaged       Installed
clsn06.ibm.com     Managed          Installed
clsn07.ibm.com     PreManaged       Not Installed
```

All nodes are listed as Installed when their operating system upgrade is complete. Any other status values that appear in the output represent the progress of the operating system upgrade. Errors are indicated with a status code. If the operating system upgrade times out as a result of using the installnode -t command, the status message reads Install - timedout.

From a Linux management server, to continuously display the output of the monitorinstall command, enter:

```
watch monitorinstall
```

If there is a problem, see /var/log/csm/installnode.log on the management server or /var/log/csm/install.log on the managed node for the installation log file.

To verify that Remote Monitoring and Control (RMC) is working, use the lsnode command with the -H and -l flags, as follows:

```
lsnode -H -l
```

**Note:**

The `lsnode -H -l` command can only be used on Managed nodes. The `lsnode` command retrieves information about the attributes from each node.

To check that dsh is working, issue a simple dsh command. The date command, for example:

```
dsh -as date
```

A list of the cluster nodes is returned.
Red Hat EL Kickstart installations and upgrades

During a Red Hat EL Kickstart installation or upgrade, the `installnode` command completes the following steps. For Red Hat EL on System x nodes:

1. Sets up the `/tftpboot/pxelinux.cfg/node-ip-addr-in-hex` on each node's install server, so that a node reboot runs a Kickstart installation or upgrade.
2. Reboots the node. At this point, `installnode` command execution is complete, and the remainder of the process proceeds on the node.
3. As the node reboots, broadcasts its MAC address.
4. The `dhcp` server on the install server accepts the node's `dhcp` request, and `pxelinux` initiates a Kickstart installation or upgrade.
5. Kickstart installs or upgrades the operating system on each node using the kickstart configuration file in
   `/csminstall/csm/InstallCSMVersion/kickstart.InstallDistributionNameInstallDistributionVersion/n/node-ipaddr-kickstart`. After some additional configuration, any user scripts in `/csminstall/csm/scripts/installprereboot` or `/csminstall/csm/scripts/osupgradeprereboot` are run. Then the Kickstart post-installation script adds the `csmfirstboot` script `/csminstall/csm/InstallCSMVersion/csmfirstboot` to `/etc/inittab`. Then the Kickstart post-installation or upgrade script adds the `csmfirstboot` script `/csminstall/csm/InstallCSMVersion/csmfirstboot` to `/etc/inittab`. It then modifies the `pxelinux` configuration file `/csminstall/pxelinux.cfg/node-ip-addr-in-hex` on the install server so that the next reboot of the node reboots from the local hard drive.
6. The node reboots to the local hard drive.
7. As the reboot completes, the `csmfirstboot` script, which was listed in `/etc/inittab`, is run on the node.
8. The `csmfirstboot` script installs or upgrades CSM and its dependencies, defines the management server, transfers CMF files, installs SMS packages, and runs any user scripts in `/csminstall/csm/scripts/installprereboot` or `/csminstall/csm/scripts/osupgradeprereboot`. Then `csmfirstboot` removes itself from `/etc/inittab`. If the node's `Mode` is `MinManaged`, CSM is not installed on the node.
9. When the node `Mode` attribute value is `Managed`, the node is ready for use in the cluster. For `MinManaged` nodes, the `Mode` does not change to `Managed`. Run the `monitorinstall` command from the management server to see the installation or upgrade status of `MinManaged` nodes.

For Red Hat EL on System p, including BladeCenter JS nodes:

1. An `arp` entry is made for the node on the install server and the node is rebooted to start in firmware mode. The `installnode` command communicates with the node's firmware to initiate a directed `BOOTP` request to the install server, which retrieves the kernel and initial ramdisk and reboots the node.
2. At this point, `installnode` command execution is complete, and the rest of the process proceeds on the node.
3. Kickstart installs or upgrades the operating system on each node.
4. After the Kickstart installation or upgrade of the operating system is complete, the Kickstart post-installation script,
   `/csminstall/csm/InstallCSMVersion/kickstart.InstallDistributionNameInstallDistributionVersion/n ode-ipaddr-kickstart`, is run on the node. After some additional configuration, scripts in `/csminstall/csm/scripts/installprereboot` or `/csminstall/csm/scripts/osupgradeprereboot` are run. Then the Kickstart post-installation or upgrade script adds the `csmfirstboot` script `/csminstall/csm/InstallCSMVersion/csmfirstboot` to `/etc/inittab`.
5. The node reboots to the local hard drive.
6. As the reboot completes, the `csmfirstboot` script, which was listed in `/etc/inittab`, is run on the node.
7. The `csmfirstboot` script installs or upgrades CSM and its dependencies, defines the management server, transfers CFM files, installs SMS packages, and runs any user scripts in `/csminstall/csm/scripts/installpostreboot` or `/csminstall/csm/scripts/osupgradepostreboot`. Then `csmfirstboot` removes itself from `/etc/inittab`. If the node's `Mode` is `MinManaged`, CSM is not installed on the node.
8. When the node `Mode` attribute changes to `Managed`, the node is installed and ready for use in the cluster. For `MinManaged` nodes, the `Mode` does not change to `Managed`. Run the `monitorinstall` command from the management server to see the installation or upgrade status of `MinManaged` nodes.

**SLES AutoYaST upgrades**

During a SLES 9 upgrade, the `installnode` command completes the following steps for System x and System p nodes:

1. Sets the `InstallServiceLevel` attribute to the new service level; for example, SP2.
2. Sets the `InstallMethod` attribute to `you`.
3. Runs the `csmssetupinstall -c` command to copy the new service level CDs or ISOs to the disk.
4. Runs the `installnode` command, which does the following:
   a. Runs `dsh online_update` on the nodes to upgrade the operating system RPMs.
   b. NFS mounts the `/csminstall/csm` directory on the nodes, using `dsh`.
   c. Runs `dsh osprereboot` on the nodes, which adds `csmfirstboot` to `/etc/inittab`, and runs the scripts in the `/csminstall/csm/scripts/osupgradepreboot` directory.
   d. Reboots the nodes to disk.
   e. As the nodes reboot to disk, they run `csmfirstboot`, which runs the scripts in `/csminstall/csm/osupgradepostreboot`, and removes `csmfirstboot` from `/etc/inittab`. It also runs `makenode`, which installs or upgrades CSM and its dependencies on the nodes and defines the management server to the node.
Chapter 22. Updating CSM for AIX

Maintaining your CSM for AIX cluster requires periodically updating CSM software on your AIX management server, install servers, and nodes. For information on updating AIX, see "Optional software product and service updates" in the AIX Installation Guide and Reference. For information about migrating to new releases of AIX, see Migrating the AIX operating system. AIX publications are available at http://publib.boulder.ibm.com/infocenter/pseries/v5r3/index.jsp.

To maintain your CSM for AIX cluster, you must also periodically update CSM for AIX prerequisites.

Obtaining CSM updates


Note:
If your management server does not have internet access, download the updates to another server and transfer them to the management server.

The updates are contained in a tar file that you can download or copy to a temporary directory on the management server; for example, /tmp/csm.

Attention: The CSM support Web site does not include all non-CSM prerequisites. If there are any required prerequisites, they must be installed before or with the CSM updates. For example, if a new level of RSCT is required, you must get the updates and make sure they are applied before the CSM updates are applied. Prerequisite information and any special handling required for the updates are described on the CSM support Web site.

Before installing CSM software updates, the base file sets must be installed. The base CSM file sets are available on AIX product media. You may also have to install base file sets when updating to a new release of CSM.

Updating the CSM for AIX management server

When you apply updates to a CSM cluster, the management server must always be installed with the latest level of CSM in the cluster. The version.release.mod.fix (VRMF) level of the CSM file sets installed on the management server must always be greater than or equal to the levels installed on the nodes.

Backing up CSM data

Before you updating CSM software, back up your CSM data using the csmbackup command as follows:
Commit previous levels of software

Before you install new levels of installp file sets, you can commit the current levels. Then, if any problem with the updates arises, you can reject them and return the software to the previously committed level. For example, issue the following command to commit the latest updates to the csm.server and csm.deploy file sets:

installp -cgX csm.server csm.deploy

Update CSM Blue Gene support

If you are using CSM Blue Gene support software, go to the Pre-update steps under Full CSM plus Blue Gene monitoring support. You will be directed back to this section at the appropriate step.

Gather updates

Updates are available for one or more of the following required CSM file sets and RPM packages. These updates are available from the AIX fix distribution Web site, or the CSM support Web site. See Installing a CSM for AIX management server for details on downloading the required updates from the CSM support Web site, and for a list of the CSM file sets.

Updates might be available for one or more these required RPM packages:

- conserver
- expect
- tcl
- tk

Note:
The rpm packages of expect/tcl/tk are replaced by new installp packages in AIX 6.1.3 or later.

The following optional open source software is not available on the update CDs or from the CSM support Web site, but may be required for certain CSM features. See Optional CSM for AIX open source software for details.

- openCIMOM
- autoupdate
- sg3_utils

The openCIMOM software is installed on the management server. If you are using Linux nodes, autoupdate and sg3_utils RPM packages are copied to the management server but will actually be installed on the Linux nodes.

Before continuing to the next step, make sure you have enough disk space in the /opt directory.
Install the software

Use the following procedure to update CSM versions:

1. **Install RPM updates**

   Install any new versions of required RPM prerequisites. For example, CSM 1.7.1 requires:

   conserver-8.1.aix52.ppc.rpm

   **Note:**
   conserver-8.1.aix52.ppc.rpm installs conserver-8.1.7-2 on the system.

   The following command installs packages is in the `/tmp/csm` directory:

   ```
   rpm -U /tmp/csm/conserver-8.1.aix52.ppc.rpm
   ```

2. **Install the base CSM file sets**

   The base file sets are available on AIX product media only. The base file sets for CSM 1.7.0 are available on the AIX for POWER Version 6.1 base installation CDs or the AIX for POWER Version 5.3 base installation CDs.

   **Note:**
   To update CSM file sets only, you must also update the prerequisite RSCT file sets.

3. **Install RSCT prerequisites**

   Using an AIX maintenance package CD to update CSM enables you to update both CSM and RSCT software in one step, by applying all updates contained on the CD. To install CSM updates only using the CD, you must install any RSCT updates first.

   To apply CSM updates that you downloaded from the CSM support Web site, you must get any required RSCT prerequisites and install them before installing the CSM updates.

   For example, assuming all new RSCT file sets are contained in the `/tmp/rsct` directory, the following command installs the CSM prerequisites:

   ```
   installp -aX -d /tmp/csm rsct.core
   ```

   See [Planning for CSM software](#), for details on CSM prerequisites.

4. **Install CSM updates**

   If you are using the tar file downloaded from the CSM support Web site, you can use the `installp` command to apply the updates. The device that you specify is the name of the directory used to unwrap the tar file. For example, if you downloaded and unwrapped the tar file in the `/tmp/csm` directory, you can install all CSM updates by running:

   ```
   installp -aX -d /tmp/csm all
   ```
**Accept the new CSM license if required**

If the updated software is a new release level of CSM - for example, if the previous level of CSM was 1.5.1 and the updated CSM level is 1.7.0 - you must accept a new CSM license. If the license agreement is not accepted, CSM commands will fail and an error message will indicate that you must run `csmconfig -L`.

Run the following command to view the license agreement:

```
csmconfig -L
```

The command gives you the option of accepting or rejecting the terms and conditions of the license agreement. For details, see **Accept the CSM for AIX license agreement**.

**Copy the files to /csminstall**

Issue the `csmconfig` command to copy certain updated CSM files into the `/csminstall` subdirectories:

```
csmconfig -c
```

**Verify the installation (optional)**

To verify that the management server is installed correctly and ready for use, you can run the `ibm.csm.ms` probe, which is shipped with CSM. To run the probe issue the following command.

```
probemgr -p ibm.csm.ms -l 0
```

For information about CSM support for probes, see the **CSM for AIX and Linux: Administration Guide**.

---

**Updating AIX nodes and install servers**

For nodes or install servers that are installed with AIX, use the `dsh` command to apply software updates. The basic procedure is:

- Gather the updates to be installed and put them in a mountable directory on the management server.
- Use `dsh` to mount the directory on the remote node or install server.
- Use `dsh` to run the appropriate AIX command to apply the updates; `installp` or `geninstall`.

If you used NIM to initially install the node, you can also use NIM support to apply updates. The process for updating the nodes is to copy the updates into the NIM `lpp_source` resource directory for the nodes and perform a NIM `cust` operation. See the **AIX: Installation Guide** for information on the NIM `cust` operation.

It is not necessary to update the cluster nodes with the latest available updates unless the updates are specifically required. See the following CSM support Web site for information on any required updates for the nodes: [http://www14.software.ibm.com/webapp/set2/sas/f/cluster/home.html](http://www14.software.ibm.com/webapp/set2/sas/f/cluster/home.html).
Gather updates

The base file sets for all of the CSM software that is required on the nodes are automatically installed with AIX, but they may not be the most recent version. The latest versions must be installed using the CSM product CDs. If these file sets are uninstalled, they must be reinstalled before you can apply the updates.

For AIX 5.3 or AIX 6.1 nodes, you might have to apply updates for the following file sets:

- csm.core
- csm.client
- csm.dsh
- csm.diagnostics

Commit previous levels of CSM software (optional)

Before you install new levels of code, make sure that the current levels are committed. If any problem with the updates exist, they can be rejected and the software will be returned to the previously committed level. To commit the software use dsh and the installp command.

For example, to commit the current levels of csm.core, csm.client, csm.diagnostics, and csm.dsh, you can issue the following command. AIXNodes is the node group containing all AIX nodes.

dsh -N AIXNodes installp -cgX csm.core csm.client csm.dsh csm.diagnostics

Export the directory containing the updates

For example, if you copied your update files to /tmp/csm and the hostname of your management server is clstrms01, you can export the directory with the following command:

exportfs -i /tmp/csm

Mount the directory on the AIX nodes

Use the dsh command to mount the updates directory on the AIX nodes.

dsh -N AIXNodes mount clstrms01:/tmp/csm /mnt

Apply the updates

Use the dsh command to apply the updates to the nodes.

dsh -N AIXNodes installp -aX -d /mnt all

Unmount and unexport the directory

dsh -N AIXNodes umount /mnt
Run the updatenode command (Optional)

It might be necessary to run the `updatenode` command to complete additional updates on the cluster nodes. The `updatenode` command distributes configuration files, runs user-provided customization scripts, exchange RSCT public keys, and performs other update functions. If you do not need to perform these or other updates, you do not need to run the command, but it is suggested.

To update all of the AIX cluster nodes, issue the following command:

```
updatenode -N AIXNodes
```

Backing out updates

To back out updates, you have to undo your updates and then redo the steps using the prior level of code. The details for backing out installed updates depend on the steps that you have performed. For example, if you have applied an update to the management server and a problem occurs, you can simply reject the update. However, if you have completed additional tasks, backing out the changes is more involved.

To avoid having to back out updates, test all updates on a separate system, and back up your CSM data using the `csmbackup` command, before applying updates to your production environment.

Backing out updates to the management server

If software updates have been applied to your AIX management server, but not yet committed, use the standard AIX tools to reject the updates. If the updates have been committed, you must uninstall the software and reinstall it at a previous level. To reinstall a prior level of CSM on the management server, see the *CSM for AIX and Linux: Planning and Installation Guide*. You also need the base CSM file sets and any updates that were previously installed.

Depending on your situation, you might need to restore the database to the previous state by issuing the `csmrestore` command. Also run the `updatenode` command to ensure that the cluster is properly configured. If any new required open source RPM packages were installed for these updates, uninstall them and replace them with the previous versions.

When you have returned the software to the previous level, consider the following:

To verify that the management server is installed correctly and ready for use, run the CSM `ibm.csm.ms` probe. To run the probe, enter:

```
probemgr -p ibm.csm.ms -l 0
```

For information about CSM support for probes, see the *CSM for AIX and Linux: Administration Guide*.
Back out changes on AIX nodes

If software updates have been applied but not yet committed, use NIM to reject the updates. For example, to reject the updates applied to the `csm.core` and `csm.client` file sets on node `clstrn04`, issue the following command:

```
nim -o maint -a installp_flags="-r" -a file sets="csm.core csm.client" clstrn04
```

This command returns the versions of the file sets to the previously committed levels.

If the updates have been committed, you must uninstall the software and reinstall it at a previous level. When you reinstall, you must include both the base file sets and any updates. The NIM `cust` operation can be used to reinstall the file sets.

Remove the updates that were rejected or uninstalled from the `lpp_source` directory, so they are not inadvertently reapplied. If the `InstallCSMVersion` attribute has changed, use the `chnode` command to change the attribute of the nodes to the correct version. Run the `updatenode` command to ensure the node is configured properly.
Chapter 23. Updating CSM for Linux

Updating CSM for Linux requires installing a later level of CSM on your Linux management server, install servers, or nodes. Before updating CSM, note the following:

- Your CSM for Linux management server must be at the same level of CSM, or later, than your Linux nodes and install servers.
- Any separate Linux install servers must be at the same level of CSM, or later, than the Linux nodes they update.
- To update CSM on Linux diskless nodes, see Using Linux diskless nodes.

Updating CSM on a Linux management server

Updating CSM on a Linux management server requires preparing the management server and applying CSM updates. To prepare your Linux management server for updates:

- Back up your management server data using the `csmbackup` command.
- If you are using CSM Blue Gene support software, go to the Pre-update steps under Full CSM plus Blue Gene monitoring support before proceeding here.

To apply CSM updates to a Linux management server:

1. **Remove CSM Linux Cluster Support (LCS) extension:**

   If you are using CSM with IBM Director and have the CSM Linux Cluster Support (LCS) extension installed, you must remove the extension prior to updating CSM. The procedure is as follows:

   a. In the IBM Director Console, do the following:
      - If you have Event Action Plans based on Linux Cluster event types, delete them from the managed objects they are associated with, if any, and delete the Event Action Plans and corresponding Event Filters themselves.
      - If you have any Dynamic Groups based on CSM Node inventory data, delete them.
      - If you have any Custom Queries based on CSM Node inventory data, delete them.
   b. Run the `rmlcsexxt` command on your management server to remove the LCS extension components.
   c. If your IBM Director Server is separate from your management server, run the `rmlcsexxt` command on a Linux Director Server to remove the LCS extension components. On a Windows Director Server, use the Add/Remove Programs interface to remove the LCS extension components.

2. **Obtain the new CSM packages and non-IBM software:**

   If you are updating to a new release or modification level of CSM for Linux, obtain a CSM CD or download the CSM packages from IBM. If you are updating to a new service level of CSM, download the CSM packages from IBM.
If you are updating CSM using the CSM CD, skip to the next step. Otherwise, do the following on your management server:

a. Download the CSM packages from the CSM support Web site at http://www14.software.ibm.com/webapp/set2/sas/f/csm/download/home.html and place them in a directory such as /tmp/csm. After downloading the packages, use the following command to extract the files, where filename is the name of the CSM package:

   tar -zxvf filename

b. Download any packages that are listed in CSM for Linux non-IBM software and put them in a directory such as /tmp/csmreqs.

3. Update the csm.core package on the management server:

   If you are updating CSM from the CSM CDs, do the following:

   a. Mount the CSM CD as follows:

      mount /dev/cdrom /media/cdrom

   b. Update the csm.core package as follows:

      rpm -U /media/cdrom/csm.core-*

   If you are updating CSM from a directory, run the rpm command as follows; the example assumes the CSM packages are in the /tmp/csm directory:

      rpm -U /tmp/csm/csm.core-*

4. Update the other CSM software on the management server:

   Run the installms command with the -p flag specifying the appropriate package path. In addition to updating CSM software packages, the installms command also updates RSCT packages and other CSM management server prerequisite software packages. For example, if the CSM packages are on the CD-ROM and the other downloaded RPMs, such as Autoupdate, are in /tmp/csmreqs, run the installms command as follows:

   installms -p /tmp/csmreqs:/media/cdrom

   If the CSM packages are in /tmp/csm, and the other downloaded RPMs, such as Autoupdate, are in /tmp/csmreqs, run the installms command as follows:

   installms -p /tmp/csmreqs:/tmp/csm

5. Merge new file and script changes into your customized files and scripts, if applicable:

   If you have modified any of the CSM Kickstart or AutoYaST configuration template files, or created your own from the template file shipped in a previous version of CSM, you need to merge the changes from CSM's new template file into the modified template file. If you have customized the post-installation scripts in the template file, move these customizations into new scripts in /csminstall/csm/scripts/installprereboot or /csminstall/csm/scripts/installpostreboot. For details, see Modify Linux node configuration templates (optional).

Complete your CSM for Linux updates as follows:

1. **Accept the new CSM license agreement.**

   You must accept the new license agreement for the new CSM level to function properly. On the management server, run the following command to view and accept the new license agreement:

   ```
   csmconfig -L
   ```

   Check the success of the license acceptance by running the `csmconfig` command again with no flags. In the output of the command the `ExpDate` and `MaxNumNodesInDomain` values indicate the status of the license acceptance. See the man page for the `csmconfig` command for a description of these attributes.

2. **Update CSM on your install servers if applicable.**

   To update AIX install servers, see [Updating AIX nodes and install servers](#). To update Linux install servers, see [Updating CSM on Linux install servers](#).

3. **Update CSM on your Blue Gene Service Node if applicable:**

   If you are using CSM's Blue Gene support software, you must update your Blue Gene Service Node to the same new level of CSM on your management server. See [Updating CSM on Linux nodes](#) to update CSM on your Service Node.

4. **Update CSM on your other nodes:**

   To update AIX nodes, see [Updating AIX nodes and install servers](#). To update Linux nodes, see [Updating CSM on Linux nodes](#).

---

### Updating CSM on Linux install servers

Before updating CSM on any Linux nodes that are served by install servers, you must first update CSM on the install servers. In addition to enabling your install servers for node updates, the latest CSM features and fixes are also applied. To update CSM on your Linux install servers, follow the [Updating CSM on Linux nodes](#) procedure.

---

### Updating CSM on Linux nodes

The level of CSM installed on your nodes cannot be later than your CSM management server level, or CSM install server level, if applicable. Ensure that your management server and install servers are installed with a supported level of CSM. Before continuing, see [Updating CSM for AIX](#) or [Updating CSM on a Linux management server](#), [Updating AIX nodes and install servers](#), and [Updating CSM on Linux install servers](#), as required.

**Note:**

CSM for AIX and Linux: Planning and Installation Guide
The CSM level is the CSM Version, Release, Modification, Fix (VRMF) level. For example, a CSM 1.6.0.0 management server cannot manage a CSM 1.6.0.10 node.

Updating CSM on your nodes is optional; you can update your management server without updating CSM on your nodes. The few exceptions to this general rule are described below. Updating CSM on your nodes, however, installs new CSM features, fixes, and improvements.

If you are using CSM support for Blue Gene, you must update CSM on at least your Blue Gene Service Node if you have updated CSM on your management server.

To update CSM on Linux nodes, do the following:

1. **Change InstallCSMVersion, if necessary:**
   
   If you are updating to a new release or modification level of CSM, change the InstallCSMVersion attribute of the nodes that you want to update. If you are updating to a new service or fix level of CSM, InstallCSMVersion is already set correctly.
   
   For example, to update all nodes from CSM 1.5.x.x to CSM 1.7.1.x, run the following command on your management server:

   ```
   chnode -a InstallCSMVersion=1.7.1
   ```

   Note that the value of InstallCSMVersion must have the form v.r.m, where v is the CSM version number, r is the release number, and m is the modification number. The service or fix number is not used.

   To update only a subset of your nodes from CSM 1.5.x.x to CSM 1.7.1.x, run the chnode command with the -n or -N flag to specify the nodes to update.

2. **Run csmcopypkgs, if necessary.**
   
   Ensure that all packages required to update CSM on the target Linux nodes are available on your management server, or on the nodes' Linux install servers, if used. If your nodes have the same attribute values as your management server or install server, no copying is required; the required packages were copied to the /csminstall directory on your management server when you ran installms, or when you updated CSM on the install server. If the Linux nodes that you want to update are served by Linux install servers, no copying is required - the required packages were copied to the install servers when you updated CSM. However, if you have any Linux nodes that are not served by Linux install servers and are different than the management server, you must obtain the required update packages and run copycsmpkgs to copy them to the management server /csminstall directory. A node is different than its management server if any of the following IBM.ManagedNode attribute values are not the same for the node and the management server:

   - InstallOSName
   - InstallDistributionName
   - InstallDistributionVersion
   - InstallServiceLevel
   - InstallPkgArchitecture
   - InstallCSMVersion

   For example, if your management server is running System p SLES 9 and managing System p SLES 10 nodes, the node InstallDistributionVersion values are different than the management server.
server value. In this case, you must obtain the packages required to update CSM on System p SLES 10 nodes. If you are updating the nodes to the latest release or modification level of CSM, you can obtain a CSM CD or download the CSM packages from IBM. If you are updating to a new service level of CSM, you must download the CSM packages from IBM; see http://www14.software.ibm.com/webapp/set2/sas/f/cluster/home.html.

Once you have the required packages, run the `copycsmpkgs` command. For example, if you downloaded the required packages and placed them in `/tmp/csm/plinux`, enter:

```
copycsmpkgs -N ppcSLES10Nodes -p /tmp/csm/plinux
```

Repeat this process for each type of Linux node being updated.

3. **Run bgsetupms, if applicable:**

   If you are using CSM support for Blue Gene, and you are updating CSM on the Blue Gene Service Node, run the `bgsetupms` command on your management server.

4. **Run updatenode to update your nodes:**

   If all of your nodes are Linux nodes, run the `updatenode -a` command to update CSM on all of them. To update only a subset of your Linux nodes, run `updatenode` using the `-n` or `-N` flag to specify the nodes. In addition to updating CSM software packages, the updatenode command also updates RSCT packages and other CSM managed node prerequisite software packages.

5. **Recover DHCP leases if updating CSM:**

   When the DHCP server starts, it removes all existing leases from `/var/lib/dhcp/dhcpd.leases` if the corresponding IP entry can no longer be found in `/etc/dhcpd.conf`. When CSM is updated, it regenerates the `dhcpd.conf` file with a new format; thus, the existing leases can be lost during migration. CSM helps recover from lost leases, as follows.

   When CSM recreates the `/etc/dhcpd.conf` file, it saves the original file to `/etc/dhcpd.conf.precsm1.5`, and the original lease file is renamed to `dhcpd.leases.precsm1.5`. To keep your existing lease, obtain the previously added dynamic entries from the `dhcpd.conf.precsm1.5` file and use the `mkdhcp` command to add them to the file. Then use `/var/lib/dhcp/dhcpd.leases.precsm1.5` to overwrite `/var/lib/dhcp/dhcpd.leases` and preserve your leases.

   **Note:**
   On SLES, `/var/lib/dhcp/dhcpd.leases` is a symbolic link. The actual file is `/var/lib/dhcp/db/dhcpd.leases`, which is saved to `/var/lib/dhcp/db/dhcpd.leases.precsm1.5`.

6. **Do post-update steps for CSM support for Blue Gene, if applicable.**

   If you are using CSM support for Blue Gene, see the Post-update steps under Full CSM plus Blue Gene monitoring support.
Chapter 24. Hardware configuration

Your cluster environment must meet the following hardware configuration prerequisites, depending on your cluster hardware models.

**eServer configuration**

To use IBM eServer 325, 326, and 326m servers in your CSM cluster, each Baseboard Management Controller (BMC) must be configured with an IP address, network mask, and network gateway. Use the **lancfg** utility included with the BMC DOS updates, which can be downloaded from the IBM support Web site at [http://www.ibm.com/servers/eserver/support/](http://www.ibm.com/servers/eserver/support/).

Follow the instructions in the text file accompanying the update image to transfer the image to a storage device. Once the image is transferred, perform the following steps:

1. Disable the **AUTOEXEC.BAT** file to prevent the BMC firmware from being flashed automatically.
2. Boot the server from the storage device.
3. Enter or confirm the system date and time if prompted.
4. At the A:\> prompt, enter **lancfg**.
5. Press the **F10** key to activate the menu bar, then highlight **LanCfg** and press the **Enter** key.
6. Follow the prompts to enter the BMC network information and save the configuration to the BMC.
7. Remove the storage device and reboot the server.

**System x configuration**

See the following topics to configure IBM System x servers for use in a CSM cluster. For System x server details, see [http://www.ibm.com/servers/eserver/xseries/](http://www.ibm.com/servers/eserver/xseries/).

**System x360 configuration**

IBM System x 360 servers can be configured as a CSM for Linux management server and managed nodes. See [Linux distributions and hardware support](http://www.ibm.com/support/docview.wss?uid=ssg1S1000261) and [Linux on System x](http://www.ibm.com/support/docview.wss?uid=ssg1S1000261) for the specific software supported on x360 hardware. To use remote console with x360 servers, 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.
System x BMC configuration

The following configuration procedure applies to all System x servers using a use a Baseboard Management Controller (BMC) as the hardware control point, with the exception of eServer 32* servers. This includes xSeries 336 and 346 servers without an RSA-II SlimLine adapter installed, and System x 3455, 3550, 3650, 3655, and 3755 servers. You must configure the BMC IP address, network mask, and network gateway, as follows:

1. Reboot the server and press the F1 key when prompted to enter Setup.
2. From the Configuration/Setup Utility menu, select "Advanced Setup".
3. From the Advanced Setup menu, select "Baseboard Management Controller (BMC) Settings".
4. From the Baseboard Management Controller (BMC) Settings menu, select "BMC Network Configuration".
5. Enter the network parameters, save, and exit the Setup utility.

System x440 configuration

IBM System x 440 (x440) servers can be used in CSM clusters as the Linux management server or as Linux managed nodes. See the [Linux distributions and hardware support](#) and [Linux on System x](#) for the specific software supported on x440 hardware. CSM remote console function, MAC address collection, and remote installation is not supported on the x440.

BladeCenter configuration

IBM BladeCenter JS, HS, and LS blade servers can be used as CSM for Linux management servers and managed nodes. BladeCenter JS blade servers can also run CSM for AIX. See the [Linux distributions and hardware support](#) for the specific software supported on BladeCenter hardware. For details on BladeCenter, including product documentation, see [http://www.ibm.com/servers/eserver/bladecenter/index.html](http://www.ibm.com/servers/eserver/bladecenter/index.html).

BladeCenter JS blade servers require a BladeCenter chassis power supply of 220V and 1800W. To use CSM in a mixed blade server environment, check the power supply on the chassis before installing BladeCenter JS blade servers.

Configuring the BladeCenter 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)](#). 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 is 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 later 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)
   o 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 broadcasts 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.
   o Using the default static IP address from the Management Module
      a. The default BladeCenter Management Module 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 is 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/dhcpcd.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.

BladeCenter Management Module firmware updates

The BladeCenter Management Module (MM) firmware level must be later than BRET36A. To check the firmware level, log in to the Management Module using a Web browser and check the Firmware VPD page. To update firmware on the Management Module using a Web browser, do the following:

2. Select "BladeCenter" and search for Management Module updates for type 8677. Update the Management Module using the instructions packaged with the update.
Configuring the BladeCenter switch module

The BladeCenter Ethernet switch module is a hot-swappable module plugged into Module Bay 1 or 2 in the BladeCenter chassis. This switch module connects all blade servers in the BladeCenter chassis to either Ethernet Link 1 (eth0) or Ethernet Link 2, depending on the bay the switch is installed in. See the *IBM BladeCenter Planning and Installation Guide* for detailed BladeCenter configuration information.

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 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 must 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.

Ethernet switch configuration with mixed blade servers

The following information applies to a mixed BladeCenter environment only, where the BladeCenter chassis contains one or more BladeCenter HS20-8678 blade servers and one or more BladeCenter LS or HS (other than HS20-8678) blade servers. IBM does not support BladeCenter JS and HS20-8678 blade servers in the same chassis.

BladeCenter LS and HS (other than HS20-8678) blade servers use the switch module in Module Bay 1 to access the blade server's eth0 interface, and the switch module in Module Bay 2 to access the blade server's eth1 interface.

BladeCenter HS20-8678 blade servers map the switch modules in the opposite way: the switch module in Module Bay 1 accesses the blade server's eth1 interface, while the switch module in Module Bay 2 accesses the blade server's eth0 interface.
To use HS20-8678 blade servers in the same chassis as other BladeCenter HS blade servers, you must upgrade the HS20-8678 blade server BIOS to level 1.05 or later, and then modify the BIOS settings for each HS20-8678 blade server as follows:

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

*Note:* BladeCenter HS models all have unique BIOS versions. Upgrade and reconfiguration of the HS20-8678 blade server is only required in a mixed chassis, to configure the HS20-8678 blade server with the same switch-to-blade ethernet interface relationship as the other BladeCenter HS and LS blade servers.

### Configuring blade servers

A BladeCenter 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, DVD, 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. The following table shows the user-configured names for all blade servers in the chassis. The table includes rows for the 14 blade server bays. To change a blade server name, enter the name in the corresponding text box. You can enter a maximum of 15 alphanumeric characters.
4. Click on **Save**.

### BladeCenter firmware updates

To update BladeCenter blade server firmware:

2. Select the appropriate blade server and download the required update packages.
3. Update the blade server using the instructions packaged with the update.

You can also use CSM to update blade server firmware; see the remote hardware inventory and maintenance topics in the *CSM for AIX and Linux: Administration Guide* for details.

### Setting up CSM for BladeCenter

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

*PowerMethod=blade*

*HWControlPoint=management module host name or IP address*

*HWControlNodeId=blade server text ID*

*Note:* Each blade server requires a unique IP address associated with its Ethernet MAC address.
Configuring BladeCenter HS40 blade servers

Ethernet interface configuration for the BladeCenter HS40 blade server differs from HS20 and HS21 configuration. These interfaces must be configured to work properly with CSM.

Before performing any of the following configuration steps, ensure that your BladeCenter HS40 blade servers have the latest BIOS updates installed. You can download the latest BIOS from the following IBM support Web site: http://www-304.ibm.com/jct01004c/systems/support/. Once the HS40 has been updated with the latest BIOS:

1. Reboot the blade server and press the F1 key when prompted to enter Setup.
2. From the Configuration/Setup Utility menu, select "Devices and I/O Ports."
3. From the Devices and I/O Ports menu, set the following attributes as shown:

   - Dual GigaBit NIC 1 [Enabled]
   - GigaBit NIC 2 [Enabled]
   - GigaBit NIC 3 [Enabled]
   - Dual GigaBit NIC 1a PXE Boot [Disabled]
   - Dual GigaBit NIC 1b PXE Boot [Disabled]
   - GigaBit NIC 2 PXE Boot [Enabled]
   - GigaBit NIC 3 PXE Boot [Enabled]

4. From the Startup Sequence options menu, set the following boot order:

   - First Startup Device [TEAC FD-05PUB]
   - Second Startup Device [LG CD-ROM CRN-8245]
   - Third Startup Device [IBA GE Slot 0110 v]
   - Fourth Startup Device [PM-TOSHIBA MK4019G]
   - 5th Boot Device [IBA GE Slot 0108 v]

5. Save and exit the Setup utility, then reboot the server.

Verifying BladeCenter attribute values

Verify the following BladeCenter hardware attribute values:

For BladeCenter HS, other than the HS20-8678:

- PowerMethod=blade
- ConsoleMethod=blade
- ConsoleSerialDevice=ttys1
- ConsoleSerialSpeed=19200
- InstallAdapterName=eth0 if one ESM is installed; use eth1 if two ESMs are installed.
- InstallDiskType=ide

For BladeCenter JS:

- PowerMethod=blade
- ConsoleMethod=blade
- InstallAdapterName=eth1
- InstallDiskType=ide
The following example shows hardware attribute values for a BladeCenter JS20 blade server:

```plaintext
js20blade01.clusters.com:
ConsoleMethod = blade
ConsolePortNum = 1
ConsoleServerName = bc1mm01
HWControlNodeId = js20n01
HWControlPoint = bc1mm01
InstallAdapterDuplex = full
InstallAdapterName = eth1
InstallAdapterSpeed = 1000
InstallAdapterType = ent
InstallCSMVersion = 1.7.1
InstallDiskType = ide
InstallDistributionName = SLES
InstallDistributionVersion = 9
InstallPkgArchitecture = ppc64
PowerMethod = blade
```

**Setting the BladeCenter JS boot order**

Before you perform a network installation for BladeCenter JS nodes, you must set the boot sequence to boot from the hard disk instead of from the network. To set the boot order, start the BladeCenter Management Module Web interface and do the following:

1. Click on **Blade Tasks --> Configurations**.
2. Change boot sequence to "Hard drive 0".

---

**Supported HMC Models**

CSM support the following HMC models:

- HMC 7315-CR2 and 7315-C02 models with P4 servers
- HMC 7310-CR3 and 7310-C04 and later models with P5 servers
- HMC 7310-CR4 and 7310-C06 and later models with POWER 6 570 servers
- HMC 7042-CR4 and later models with POWER 6 servers

HMC can be controlled remotely using CSM. Complete the following steps to configure the HMC and CSM for this support.

- HMC BMC configuration
- CSM remote shell support for HMC

To set up SSH, see the information on managing hardware devices in the *CSM for AIX and Linux: Administration Guide*.

To set up SSL, see [Configuring CSM to use Secure Socket Layer (SSL)](#).
Chapter 25. Remote power software and configuration

CSM remote power functionality enables you to control power functions for cluster nodes from your management server. To enable your CSM cluster for remote power, you must configure your hardware and define remote power attributes in the CSM database.

Managing hardware control points

For remote power functionality, the CSM management server must have access to the node hardware control point, which is the device that controls node hardware. A user ID and password are generally required to access hardware control points.

You must run the `systemid` command on the management server to define or change 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 System x hardware, you do not need to run the `systemid` command. See Hardware control attributes for the hardware control point attribute values required for each hardware type.

Whenever an ID or password is changed on the hardware control point, the corresponding CSM user ID and password must be changed in the password files, using the `systemid` command. User IDs and encrypted passwords are stored in files in the `/etc/opt/csm/system_config` directory. The file names are the IP addresses of the node, or the hardware control points if the host names 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/efg/ctrmc.acls` file. If this file does not exist, a sample `ctrmc.acls` file can be copied from the `/usr/sbin/rsct/cfg` directory to `/var/ct/efg` and modified.

By default, only a root user on the CSM management server can perform actions such as `rpower` and `lshwinfo`, which call actions on the `IBM.NodeHwCtrl`, `IBM.HwCtrlPoint`, `IBM.DeviceHwCtrl`, and `IBM.DeviceGroup` resource classes. 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 grant read and write access to the user IDs `root` and `user` on the local host-the CSM management server-and grant read-only access to all other users on the management server:
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: Administration Guide.

## Configuring SNIA on a Version 7 HMC

In order for CSM to manage system p servers connected to a version 7 HMC, the HMC must be configured to use SNIA. To configure the Version 7 HMC(s) to allow SNIA communication:

1. Install the following Version 7 HMC APARs to provide SNIA support:
   - APAR # MB02095: REQUIRED FIX FOR CSM FOR HMC V7R3.1.0
   - APAR # MB02111: ADDITIONAL CSM FIXES FOR HMC V7R3.1.0

2. Open the SNIA port for communication. This can be accomplished on the Version 7 HMC either using the command-line interface or the GUI.
   - **Using the Version 7 HMC command-line interface:**
     a. Issue the following command (where `<HMC_IP_ADDRESS>` is the HMC public ip address):

   ```
   chhmc -c CSM_SNIA.name -s add <HMC_IP_ADDRESS>
   ```

   - **Using the Version 7 HMC GUI:**
     a. Start a session on the Version 7 HMC GUI using a supported web browser
     b. In the left pane, select *HMC Management*.
     c. In the right pane, select *Change Network Settings*.
     d. In the *Change Network Settings* window, select the *LAN Adapter* tab. Select the entry for the adapter associated with public network, and then click on *Details*.
     e. In the *Firewall Settings* tab, select the *CSM SNIA* entry in the *Available Applications* table, and then click on *Allow Incoming*. You should now see an entry for CSM SNIA in the *Allowed Hosts* table.

3. Reboot the HMC to have these settings take effect.

## Configuring a Version 7 HMC to use SSL for SNIA communication

To configure the Version 7 HMC(s) to allow SNIA communication through SSL:

1. Log in to the HMC, and become the *root* user. Then issue the following command:
   a. `chomsec -s ssl`
   b. `reboot the hmc`

2. After the HMC completes the reboot check the HMC to verify that SSL is setup by running `lsomsec`, the result should be similar to this:
   ```
   hmc01:/opt/ccfw/data # lsomsec
   curr_security=ssl,pend_security=ssl
   ```
Configuring SSL on a Version 6 HMC

For information on setting up SSL on Version 6 HMCs, see System Manager Security in the IBM Hardware Management Console for pSeries Installation and Operations Guide. HMC documentation is available at the following Web sites:

IBM Hardware Information Center

HMC-attached System p5
http://publib.boulder.ibm.com/infocenter/eserver/v1r3s/index.jsp

HMC-attached POWER4

---

Configuring SSL communication between Version 6 and Version 7 HMCs and the CSM management server

The following procedure describes how to configure CSM to use Secure Socket Layer (SSL) for hardware control from the CSM management server to an IBM(R) Hardware Management Console (HMC). This process includes generation and distribution of key files for both the Version 6 and Version 7 HMCs:

The general flow for Version 7 HMCs is as follows:

1. Install this Version 7 HMC APAR to provide SSL support:
   - o APAR # MB02122 REQUIRED SSL ENABLED CSM FIX FOR HMC V7R3.1.0
2. The Version 7 HMC defaults to supporting SSL and already has a key generated. You can regenerate the key if needed by following instructions in the "Managing Certificates" section of the Version 7 HMC guide Operations Guide for the Hardware Management Console and Managed Systems Version 7 Release 3.1.0 at http://www-01.ibm.com/servers/resourcelink/lib03030.nsf/web+search/FD5F73852A0C46638525F2E3002FFC5F/$file/sa76-0085.pdf
3. Transfer the public key ring file from each Version 7 HMC to the CSM management server. Details on the location of the file and methods to transfer it are documented below. Unlike Version 6 with a single CA HMC where all of the Version 6 public keys have been consolidated into a common file, the Version 7 HMCs each have their own public key file which needs to be copied to the CSM MS

The general flow for Version 6 HMCs is as follows:

1. Designate one HMC as Certificate Authority (CA).
2. Create private key ring files and the public key ring file on the CA HMC.
3. Transfer public and private key ring files to the HMCs.
4. Configure the HMCs as secure servers.
5. Transfer the public key ring file to the CSM management server. Details on transferring the key and location of the file are documented below.
Configuring the CSM management server to use SSL for communication to HMCs

Perform the following tasks on the CSM MS:

1. Create a single Public Key Ring file with key information for all associated HMCs in the cluster:

   This step involves copying the Public Key Ring file from one or more HMCs to the CSM management server. The files can be copied using either of the following methods:

   **Using external media:** If you are using an external media device, like a floppy drive, save the files to the device in HMC/AIX format using the `tar` command. More details can be found in the HMC documentation, at http://publib.boulder.ibm.com/infocenter/eserver/v1r3s/index.jsp?topic=/iphai/hmc.htm.

   **Using ftp or scp:** Issue the `ftp` or `scp` command from the HMC to copy the Public Key Ring file to CSM MS. Depending on which of these commands that you planned on using, ensure that they have been enabled on the HMC as well as the CSM MS.

   The steps to generate a single Public Key Ring file differ between clusters with a single Version 7 HMC and with multiple HMCs:

   - For a configuration where all nodes in the cluster are managed by a single Version 7 HMC:
     a. Copy the Public Key Ring file `/opt/ccfw/data/SM.pubkr` on the Version 7 HMC to the `/usr/websm/codebase` directory on the CSM MS. Ensure that the permission for this file are set to 600.

   - For a configuration where management of the nodes in the cluster is spread across multiple HMCs:

     If there are multiple HMCs in the cluster, it is necessary to merge the contents of the Public Key Ring file from each of the HMCs into a single key file on the CSM MS. The steps to do so are as follows:

     a. Create a directory to hold the copies of the Public Key Ring files:

        Create a temporary directory to hold the copies of the Public Key Ring files from the HMCs. This directory must contain only these Public Key Ring files. For your security protection you should set the permission of this directory to read/write only by root. The `MergeKeyStores.jar` command will verify and if necessary change the permission in this directory to 600.

        The `MergeKeyStores.jar` will create a global new public key file `/usr/websm/codebase/SM.pubkr` on the CSM MS. If a public key file already exists, the `MergeKeyStores.jar` program will backup the current file into `/usr/websm/codebase/SM.pubkr.bak` before it generates the new file.

     b. Copy the Public Key Ring file from the HMCs to the temporary directory on the CSM MS:

        - For Version 6 HMCs:
For Version 6 HMCs the key ring file must be obtained from the Certificate Authority HMC. Copy the public key ring file
/var/websm/security/tmp/SM.pubkr from the Version 6 CA HMC to the temporary directory that you created on the CSM MS in the previous step. The name of the copy should be unique, to avoid overwriting other Public Key Ring files that have already been copied to this directory.

- For Version 7 HMCs:

Copy the public key ring file /opt/ccfw/data/SM.pubkr from each Version 7 HMC in the cluster to the temporary directory that you created on the CSM MS in the previous step. The name of each copy should be unique, to avoid overwriting the other Public Key Ring files that have already been copied to this directory.

c. Add /opt/freeware/bin to the root user's $PATH variable on the management server:

    export PATH=$PATH:/opt/freeware/bin

    To verify that this step completed successfully, issue the following commands:
    echo $PATH

d. Create a single Public Key Ring file with entries for all HMCs in the cluster:

    As root, run java with the MergeKeyStores.jar script file to consolidate the key entries from all the Public Key Ring files into a single public key file. This script takes the directory location of the key files from the HMCs as the only parameter and creates a new global public key file /usr/websm/codebase/SM.pubkr on the CSM MS. The specified directory must only have key ring files. If there are any other types of files in this directory, the command will fail. If a SM.pubkr public key file already exists in /usr/websm/codebase, the MergeKeyStores.jar script will create a backup of this file in the same directory called SM.pubkr.bak before it generates the new file. Additionally, this script will also set the permission of the the directory containing the HMC key files to 600. The following illustrates how to invoke java and use the MergeKeyStores.jar script to create a single public key ring file from the individual HMC key files located in the /tmp/keyfiles directory;

    java /opt/csm/codebase/MergeKeyStores.jar /tmp/keyfiles

2. Enable SSL on the CSM MS:

    Edit the /opt/hsc/data/cim.properties file as follows:

    a. Disable the use of plain sockets. Comment this line in the file by adding the # character at the beginning:

       SocketProvider=org.snia.wbemcmd.xml.PlainSocketProvider

    b. Enable the use of SSL. Uncomment the following line by deleting the # character for this line in the file:
3. Stop and restart the hardware control resource manager by issuing the following commands:
   a. `stopsrc -s IBM.HWCTRLRM`
   b. `lssrc -s IBM.HWCTRLRM`

   This command ensures that the IBM.HWCTRLRM resource manager is "inoperative." If the state is "stopping" for more than two minutes, run `kill -9 pid`.

c. `startsrc -s IBM.HWCTRLRM`

   **Note:** If you change or recreate the /usr/websm/codebase/SM.pubkr file, you have to stop and restart IBM.HWCTRLRM on the CSM MS

   The IBM.HWCTRLRM is now using SSL to communicate to all configured HMCs in this cluster.

SSL must be configured on the CSM management server and on all HMCs that are managing nodes in the cluster; otherwise, hardware control commands such as `rpower` and `lshwinfo` will fail. Nodes attached to unconfigured HMCs have a `PowerStatus` attribute value of 127 (unknown), and actions such as `rpower` and `lshwinfo` take several minutes before returning the message 2651-627 [host_name] Daemon socket read/write timeout.

---

**Remote power and hardware configurations**

All CSM-supported hardware must be configured correctly to enable CSM functionality. For detailed information on defining node hardware attributes, see [Defining nodes](#).

**HMC-attached System p server configuration**

To configure remote power for HMC-attached System p 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*; HMC documentation is available at [http://publib.boulder.ibm.com/infocenter/eserver/v1r3s/index.jsp?topic=/iphai/hmc.htm](http://publib.boulder.ibm.com/infocenter/eserver/v1r3s/index.jsp?topic=/iphai/hmc.htm). 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 System p configuration examples**

The following examples show how to create system IDs for HMC-attached System p nodes. The commands prompt for a valid password. In the examples, the node being defined has the following hardware control attributes:

```
Hostname = clsn01.pok.ibm.com
HWCpoint = c01hmc.pok.ibm.com
HWNodeld = clsn01
PowerMethod = hmc
```

[1]: 342
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, rerun the **systemid** command to define them. See [Creating and testing system IDs](#) 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. There are several options for the **definenode** command. This example shows the specification of all information required for node hardware control. See the **definenode** man page or the *CSM for AIX and Linux: 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 is similar to:

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

   If there was a problem determining the query value, a message is returned. See the appropriate diagnostics information in *CSM for AIX and Linux: Administration Guide* for help determining the problem and resolution.

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

1. If the HMC IP address or hostname has changed:
   a. Run the **systemid** command with the new IP address or hostname and the HMC user ID. Enter the HMC password when prompted.
   b. Run the **chnode** command for all the nodes using this HMC as the 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 hostname 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 your defined LPAR name changed to `clsaixn01.pok.ibm.com`

```
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 required.
   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 system-defined CEC name, and to remove the `LParID` entry. For example, if the node was defined in the CSM database with host name `CEC01.pok.ibm.com` and the system-defined CEC name changed to `7039-651*020D47A`, run the following two commands:

```
chnode CEC01.pok.ibm.com HWControlNodeId=7039-651*020D47A
chnode CEC01.pok.ibm.com LParID=
```

**IVM-managed System p server configuration**

IBM Integrated Virtualization Manager (IVM) provides LPAR configuration and management for IBM System p5 and POWER 6 servers without requiring dedicated hardware such as the IBM Hardware Management Console (HMC). IVM's browser-based interface facilitates virtual device and partition management. Because the IVM and HMC both provide management capabilities, they cannot manage the same server. See the following URLs for detailed IVM information:

**IBM Integrated Virtualization Manager**

**Virtual I/O Server Integrated Virtualization Manager: Redbook**
http://www.redbooks.ibm.com/abstracts/redp4061.html

**IVM white paper**

To configure remote power for IVM-managed System p5 and POWER 6 servers and define the user ID and passwords required to access IVM, run the `systemid` command on the management server. If you change the user ID for an IVM, you must subsequently run the `systemid` command to set the new configuration for the management server.

CSM supports IVM on Linux and AIX management servers. To configure your cluster for IVM:

1. Install CSM & RSCT packages, and set up a CSM management server.
2. Install IVM using the CSM FSP Direct Attach method. The following conditions must be checked:
   a. The target System p5 hardware must be in manufacturing mode.
   b. The target System p5 hardware is never managed by the HMC.
   c. The VIO license is applied.
d. The server firmware level must be SF235 or later.
e. The FSP IP address must be reachable from the CSM management server on the network.

Define hardware nodes, preparing for installation:

f. The hostname must be entered in `/etc/hosts` or the DNS.
g. Define a node using the `FSP_IP` as `HWControlPoint` and `ConsoleServerName`:

```
definenode -n node1 PowerMethod=fsp HWControlPoint=FSP_IP \ ConsoleMethod=FSP_IP
```

h. Authenticate FSP by running the following commands:

```
systemid -f FSP_IP HMC (default password is abc123)
systemid -f -s FSP_IP admin  (default password is admin)
systemid -f -s FSP_IP general (default password is general)
```

i. Verify the FSP authenticated successfully:

```
lshwconn
Hardware server Pid = 14931
--------------------------------------
node1:   192.168.1.1   Status = LINE_UP
```

j. Run the following command to export `CSM_OFW_PSWD`:

```
export CSM_OFW_PSWD=admin
```

k. Enable the virtual serial connection on FSP:

```
rpower -n node1 fsp_vty
```

l. Power on the server to partition standby mode:

```
rpower -n node1 -m standby cec_on
```

m. Set the server power policy to `stayon`:

```
rpower -n node1 -o stayon cec_setting
```

n. Query the power status of the server and partition:

```
rpower -n node1 cec_state
rpower -n node1 state
```

When the partition is in power off mode, and `cec_state` is in standby mode, then you are ready to install IVM using the installation CDs.

Install IVM:

o. Open a console window:

```
rconsole -n node1
```
p. Power on the node. Press "1" at the SMS window, and select the boot device to the CD drive.
q. Insert the IVM 1.3.0 or later CD and start the installation.

After installing IVM:

r. Login as **padmin**.
s. Accept the license.

```
license -accept
```
t. Start up CIMOM:

```
ioscli startnetsvc cimserver
```

3. Create Logical partitions using IVM. Refer to the IVM User Guide for more information.
4. Define and install nodes:
   a. Set the remote user ID and password:

```
systemid IVM_IP padmin
```
   b. Set the console ID for IVM nodes:

```
systemid -c IVM_IP padmin
```
   c. Collect node hardware information from the IVM server:

```
 lshwinfo -p ivm -c vioserverip
```

The output is similar to:

```
#Hostname::PowerMethod::HWControlPoint::HWControlNodeId::LParID::HWType:: HWModel::HWSerialNum:: DeviceType::UUID
no_hostname::ivm::15.16.52.86::15-B7D1G::1::9133::55A::10000XX::IOServer::
no_hostname::ivm::15.16.52.86::lp2::2::9133::55A::10000XX:::
no_hostname::ivm::15.16.52.86::lp3::3::9133::55A::10000XX:::
```

d. Create a map file:

```
 lshwinfo -p ivm -c vioserverip -o mapfile
```

e. Edit the map file to include the hostnames.
f. Define the nodes:

```
definenode -M mapfile
```

g. Verify the node definition:

```
lsnode -F ivmlpar01
ivmlp1.cl.com:
 ConsoleMethod = ivm
 ConsoleSerialSpeed = 9600
 ConsoleServerName = 15.16.52.166
 HWControlNodeId = lp2
```
h. Get the ethernet adapter information:

```bash
getadapters -t ent -D -s auto -n ivmlpar01.clusters.com -w
```

i. Define nodes in AIX NIM database:

```bash
csm2nimnodes -n ivmlpar01.clusters.com
```

j. Prepare nodes for CSM full installation:

```bash
csmsetupnim -n ivmlpar01.clusters.com
```

k. Allocate NIM resources for `ivmlpar01`.

l. Enable BOS installation.

m. Start CSM full installation:

```bash
netboot -n ivmlpar01.clusters.com
```

**IVM-managed System p configuration examples**

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

```
Hostname = clsn01.pok.ibm.com
HWControlPoint = c01ivm.pok.ibm.com
HWControlNodeId = clsn01
PowerMethod = ivm
```

**Note:**

To change attribute values 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](#) for detailed examples.
2. Run the `systemid` command to define the user ID and password required to access the IVM that controls the node:

```bash
systemid c01ivm.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. For hardware control of the node, this example shows the details for all information required. See the `definenode` man page or the *CSM for AIX and Linux: Administration Guide* for detailed command usage information.
definenode -n clsaixn01.pok.ibm.com -H c01ivm.pok.ibm.com \\
HWControlNodeId=clsaixn01 PowerMethod=ivm

4. Verify that the node attribute values 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 is 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 the appropriate diagnostics information in the CSM for AIX and Linux: Administration Guide 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 IVM IP address or host name has changed:
   a. Run the systemid command with the new IP address or host name and the IVM user ID. Enter the IVM password when prompted.
   b. Run the chnode command for all the nodes using this IVM as their hardware control point. Modify the HWControlPoint and ConsoleServerName attribute values to match the new IVM host name. For example, if the IVM host name changed to:

      c01ivm.pok.ibm.com

      run

      chnode clsaixn01.pok.ibm.com HWControlPoint=c01ivm.pok.ibm.com \\
      ConsoleServerName=c01ivm.pok.ibm.com

2. If the IVM user ID or password has changed:
   a. Run the systemid command with the IP address or host name of the IVM and the IVM user ID. Enter the IVM password when prompted.

3. If the IVM user-defined LPAR name has changed:
   a. Run the chnode command for the node corresponding to the changed LPAR. Modify the HWControlNodeId attribute value to match the new user-defined LPAR name. For example, if the user-defined LPAR name changed to

      clsaixn01

      run:

      chnode clsaixn01.pok.ibm.com HWControlNodeId=clsaixn01
Direct attach FSP configuration

For hardware control of FSP nodes, SSL must be installed. To install SSL, download and install the SSL RPM from https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=aixtbx.

For direct remote console to FSP nodes, the hardware control point (FSP) of the nodes must have a system firmware level of SF234 or above.

1. Hardware inventory using CSM hardware discovery agent
   a. Use the hardware server discovery agent to inventory hardware that is configured on the service network. Run the following command to verify that all the hardware are detected by CSM hardware discovery agent:

      hwsda -s SP

      device   type-model   serial number   IP addresses
      SP       9123-710     10DCA8F         192.168.1.2  192.168.3.147
      SP       9123-710     10DC2FF         192.168.1.3  192.168.3.147
      SP       9123-710     10DF57F         192.168.1.4  192.168.3.147
      SP       9123-710     10DC72F         192.168.1.5  192.168.3.147
      SP       9123-710     10DC58F         192.168.1.6  192.168.3.147

   b. Create the hostmap file, by issuing the following command:

      hwsda -f -o /tmp/mymapfile

      The /tmp/mymapfile output file is similar to:

      Hostname::PowerMethod::HWControlPoint::HWControlNodeId::LPaID::HWType::HWModel::HWSerialNum::DeviceType

      no_hostname::fsp::192.168.1.2::10DCA8F::1::9123::710::10DCA8F:::
      no_hostname::fsp::192.168.1.3::10DC2FF::1::9123::710::10DC2FF:::
      no_hostname::fsp::192.168.1.4::10DF57F::1::9123::710::10DF57F:::
      no_hostname::fsp::192.168.1.5::10DC72F::1::9123::710::10DC72F:::
      no_hostname::fsp::192.168.1.6::10DC58F::1::9123::710::10DC58F:::

   c. Edit the hostmap file to add the host names for each node. For example:

      clstrn01::fsp::192.168.1.2::10DCA8F::1::9123::710::10DCA8F:::
      clstrn02::fsp::192.168.1.3::10DC2FF::1::9123::710::10DC2FF:::
      clstrn03::fsp::192.168.1.4::10DF57F::1::9123::710::10DF57F:::
      clstrn04::fsp::192.168.1.5::10DC72F::1::9123::710::10DC72F:::
      clstrn05::fsp::192.168.1.6::10DC58F::1::9123::710::10DC58F:::

      Note that the value of the HWControlNodeId is the serial number of the machine by default. Since this attribute is required but its value is not limited, it is optional to change this attribute to a desired value. It is recommended that the short host name be used for HWControlNodeId.

2. Define the node in the CSM database
   a. Run the following command with the mapfile you edited above:
If defining nodes without a map file, run the following command:

```
definenode -n clsn01.pok.ibm.com HWControlPoint=192.168.1.1
HWControlNodeId=clsn01 \nPowerMethod=fsp ConsoleMethod=fsp
```

**Note:**
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 CSM for AIX and Linux: Administration Guide for detailed command usage information.

3. **Verify that the node attributes are correct**
   a. Run the following command to list the node attributes:

```
lsnode -l clsn01.pok.ibm.com
```

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

4. **Set hardware control point user IDs and passwords**

To configure remote power for direct attach System p servers, run the `systemid` command with the `-f -s` flags on the management server to define the user ID and passwords required to access the FSP. If you change the password for the "HMC" login, you must subsequently run the `systemid` command with the `-f` flag to set the new information for the management server.

   a. Run the `systemid` command with the `-f` flag to define the HMC user ID - the user ID CSM uses to authenticate to the FSP - and to define the password required to access the FSP on the node:

```
systemid -f 192.168.1.1 HMC
```

   b. If you have not changed the default user IDs and passwords, run the `systemid` command with the `-fs` flags to define them:

```
systemid -fs 192.168.1.1 admin
systemid -fs 192.168.1.1 general
systemid -fs 192.168.1.1 HMC
```

To subsequently change the password that CSM uses to authenticate to the FSP, use the `systemid` command with only the `-f` flag and the HMC login ID.

5. **Test remote power control**
   a. Run the following command to test remote power control:

```
rpower -n clsn01.ibm.com cec_query
```

Output from this command is similar to:

```
Server-9115-505-SN1087B2F off clsn01.ibm.com
```
If there was a problem determining the query value, then a message is returned indicating the problem. First check to make sure the correct password is used for the HMC login ID. Use the `systemid` command as in Step 6 and enter the correct password. If there is still a problem, see the appropriate diagnostics information in the *CSM for AIX and Linux: Administration Guide* for help determining the problem and resolution.

The following examples require rerunning the `systemid` command, and possibly changing node configuration information in the CSM database:

- **If the FSP IP address or host name has changed**: Run the `systemid` command with the new IP address or host name and the HMC user ID. Enter the password for HMC when prompted. Modify the `HWControlPoint` and `ConsoleServerName` attribute values to match the new FSP IP address/host name. For example, if the FSP IP address changed to 192.168.2.1, enter:

  ```
  chnode clsn01.pok.ibm.com HWControlPoint=192.168.2.1
  ConsoleServerName=192.168.2.1
  ```

- **If the HMC user ID or password has changed**: Run the `systemid` command with the IP address of the FSP and the HMC user ID. Enter the password when prompted.

6. **Enable remote console**
   a. To enable remote console on the FSP, run the `rpower` command with the `fsp_vty` option to use direct, virtual serial console; this powers on the CEC to a standby state unless the console is already set to virtual serial, in which case the CEC power state remains unchanged.

   **Attention**: This command reboots and powers on the CEC; ensure that the partition is not running prior to running this command to prevent possible data loss. For example:

   ```
   rpower -n clsn01.pok.ibm.com fsp_vty
   ```

7. **Verify that the CEC is powered on**
   a. Run the following command to test remote power control:

   ```
   rpower -n clsn01.pok.ibm.com cec_query
   ```

   b. If the system is not powered on, issue the following command to power it on:

   ```
   rpower -n clsn01.pok.ibm.com -m standby cec_on
   ```

8. **Verify that the system is not set to automatically power off**

   When installing a node, if the system is set to automatically power off when the partitions are powered off, the install process will fail. Therefore, prior to node installation, make sure the "System power off policy" on the FSP is set to "Stay on". This setting can be changed in the FSP Web ASM (Advanced System Management) GUI, or alternatively:

   a. Issue the `rpower` command to change the CEC's power off policy to stay on:

   ```
   rpower -n clsn01.pok.ibm.com -o stayon cec_setting
   ```
Note that this command can only be issued when the CEC is powered on to a stable state: `standby`. See the man pages or the *CSM for AIX and Linux: Command and Technical Reference* for `rpower` command information.

b. To check the power state of the CEC, issue the following command:

```bash
rpower -n clsn01.pok.ibm.com cec_state
```

Note that if you use a terminal server, you must redirect the console to the physical side. Run the command in step 6 with `fsp_pty` (physical terminal) instead of `fsp_vty` (virtual terminal).

When you use a terminal server, you must set the `CSM_OFW_PSWD` environment variable called when installing nodes. The value of the environment variable is used as the FSP Service Processor `admin` account login password, and is provided to the Open Firmware session when it prompts for the account password. You must define this environment variable before invoking any of the following commands:

- `getadapters`
- `netboot`
- `installnode`
- `csmsetupinstall`

To keep the password secure, the environment variable must be `unset` as soon as the command has completed. One way to accomplish this is to specify the following command:

```bash
export CSM_OFW_PSWD=password;installnode -n node01;unset CSM_OFW_PSWD
```

Once the command has completed, remove any command history files, so the password cannot be retrieved from the history.

For full installation of the node, refer to [Installing AIX on nodes](#) and [Installing Linux on nodes](#).

**xSeries 335, 345, 336, 346, 366 and System x 3455, 3550, 3650, 3655, 3755**

**with RSA-II SlimLine adapter**

To configure remote power for System x servers, change the default hardware control point user IDs and passwords using the utility disks and documentation provided with the hardware. For System x 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.


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.
Note: In this configuration, if you want to use the BMC/BMC2 as PowerMethod, you should disable the RSA-II login.

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

- **HWControlPoint**
  The host name or IP address of the System x RSA adapter.

- **HWControlNodeId**
  The text ID associated with the System x ISMP.

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

### System x configuration examples

The following examples show how to create system IDs for System x servers on the management server. The commands 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 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
   ```

   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 CSM for AIX and Linux: Administration Guide for detailed command usage information.

   ```
   definenode -n clsn05.pok.ibm.com -H rsa01.pok.ibm.com\n   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
   ```

**Note:**

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 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
   ```

   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 CSM for AIX and Linux: Administration Guide for detailed command usage information.

   ```
   definenode -n clsn05.pok.ibm.com -H rsa01.pok.ibm.com\n   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 is 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 the appropriate diagnostics information in *CSM for AIX and Linux: Administration Guide* 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.apc.com/products/family/index.cfm?id=70](http://www.apc.com/products/family/index.cfm?id=70).

### APC configuration examples

The following examples show how to create system IDs for devices using an APC MasterSwitch, in a mixed cluster with an AIX management server. In the examples, the node being defined has the following hardware control attributes:

- **Hostname** = Dclsn24.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 Dclsn24.pok.ibm.com -H apc01.pok.ibm.com \ 
   HWControlNodeId=3 PowerMethod=apc
   ```

3. Verify that the node attributes are correct:

   ```
   lsnode -l Dclsn24.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 Dclsn24.pok.ibm.com query

Output from this command is similar to:

Dclsn24.pok.ibm.com on

If there was a problem determining the query value then a message will be returned indicating the problem. See the appropriate diagnostics information in the *CSM for AIX and Linux: Administration Guide* 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.

   **Attention:** Only use this step under the direction of IBM service, for APC power control problems. Start the hardware control resource manager **IBM.HWCTRLRM** as follows:

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

   The command writes an `apc.debug_trace` trace file to the `/var/log/csm` directory. This file can become large over time, so only enable tracing when required. 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` flag, double quotation marks (""") are required.

---

**eServer 325, 326, 326m, xSeries 336, 346, 366 without RSA-II SlimLine adapter, System x 3455, 3550, 3650, 3655, 3755, without RSA-II Slim-Line adapter**

The following examples show how to create system IDs for System x nodes. The commands 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:

1. For xSeries 366, and System x 3455, 3550, 3650, 3655, and 3755, the PowerMethod attribute is set to bmc2.
2. To change attributes for nodes that have already been defined, use the chnode command.

Examples

The following examples demonstrate running the systemid command on System x nodes:

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 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 CSM for AIX and Linux: 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 is 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 the appropriate diagnostics information in Defining nodes for help determining the problem and resolution.
BladeCenter remote power configuration

To configure remote power for BladeCenter blade servers, change the default hardware control point user IDs and passwords using the BladeCenter Management Module Web interface. For BladeCenter Management Modules, the default user ID is **USERID** and the default password is **PASSWORD** (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. Management Module user IDs and passwords stored on the management server must match the blades' Login Profile and password on the Management Module. The `systemid` command must be run once for each BladeCenter HS20-8677 chassis 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 BladeCenter management module.

**HWControlNodeId**
The name associated with the blade server in the BladeCenter Management Module. The name may be viewed or changed in the Management Module Web Interface. Select "Blade Tasks", then "Configuration" to view or change the name.

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

BladeCenter configuration examples

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

```
Hostname = clsn05.pok.ibm.com
HWControlPoint = mm01.pok.ibm.com
HWControlNodeId = clsn05
PowerMethod = blade
```

**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](#) for detailed examples.
2. Run the `systemid` command to define the user ID and password required to access the Management Module that controls the blade:

   ```
   systemid mm01.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 *CSM for AIX and Linux: Administration Guide* for detailed command usage information.

   ```
   definenode -n clsn05.pok.ibm.com -H mm01.pok.ibm.com \ 
   HWControlNodeId=clsn05 PowerMethod=blade
   ```
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 is 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 the appropriate diagnostics information in the CSM for AIX and Linux: Administration Guide for help determining the problem and resolution.

Testing remote power hardware control

To ensure that your CSM cluster is configured correctly for remote power hardware control, all remote power functions must 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 and the CSM for AIX and Linux: Administration Guide for examples.

Note:

1. The resetsp_host option is not supported for the APC MasterSwitch.
2. The resetsp_host and resetsp_hcp options are not supported on Linux on System p nodes.
3. The resetsp_hcp option is supported for IVM.

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, IVM, and HMCs: on, off, or unknown. Polling is used to determine power status for System x, BladeCenter, and eServer servers, 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.

Event notification is used to determine power status for System x 330 and 342, HMC-attached System p. The power status update frequency can 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 AIX node is similar to:
Hostname = clsaixn02.pok.ibm.com
HWControlPoint = c01hmc.pok.ibm.com
HWControlNodeId = clsaixn02
PowerMethod = hmc

Output for each Linux node is similar to:

Hostname = clslnxn18.pok.ibm.com
HWControlPoint = rsa01.pok.ibm.com
HWControlNodeId = clslnxn18
ConsoleServerName = mrv01.pok.ibm.com
PowerMethod = xseries

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

rpower -n clsn01,clsn07,clsn13,clsn16 on

---

System ID attributes

The following table shows the internal hardware attributes that 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, to write the change to the CSM database.

The servers listed in the following table are shipped with default user IDs and passwords. Change these default user IDs and passwords before defining your nodes.

Table 91. System IDs

<table>
<thead>
<tr>
<th>Hardware Model</th>
<th>User ID</th>
<th>Password</th>
<th>Host specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>HMC-attached System</td>
<td>HMC User ID</td>
<td>HMC password</td>
<td>HMC IP address or host name</td>
</tr>
<tr>
<td>IVM-managed System</td>
<td>IVM User ID</td>
<td>IVM password</td>
<td>IVM IP address or host name</td>
</tr>
<tr>
<td>System x, including xSeries 336 and 346, System x 3455, 3550, 3650, 3655, 3755 with RSA-II SlimLine adapter installed</td>
<td>RSA User ID</td>
<td>RSA password</td>
<td>RSA IP address or host name, or ISMP name</td>
</tr>
<tr>
<td>Direct attach System</td>
<td>FSP UserID (For &quot;HMC&quot; login)</td>
<td>FSP password (For &quot;HMC&quot; login)</td>
<td>FSP IP address or host name</td>
</tr>
<tr>
<td>BladeCenter JS 12, 20, 21, 22, 23, 43; BladeCenter HS 20, 21, 40; BladeCenter LS 20, 21, 41</td>
<td>MM User ID</td>
<td>MM ID</td>
<td>MM IP address or host name</td>
</tr>
<tr>
<td>eServer 325, 326 and 326m, xSeries 336, 346, 366, System x 3455, 3550, 3650, 3655, 3755</td>
<td>BMC Administrator-level User ID</td>
<td>BMC password</td>
<td>BMC IP address or host name</td>
</tr>
</tbody>
</table>
Creating and testing system IDs

The following example shows how to create a system ID for a System x 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 System x 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 is 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 the appropriate diagnostics information in CSM for AIX and Linux: Administration Guide 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 a System x 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
   ```

**User-defined power methods**

CSM can integrate user-defined power methods into the power control architecture. You can define hardware control devices for CSM that have not been enabled by IBM provided that you also supply a custom power method to control the devices. CSM passes a list of arguments to your power method. Your power method performs the requested action, and passes response strings that contain the result of the action back to CSM.

**Requirements and options**

The user-defined power method must be a file executable by the root user and can be either a compiled binary file or a script. The power method must properly process the arguments that CSM passes, handle all interactions with the hardware control device, and send properly formatted responses back to CSM.

Consider the following:
Because user-defined power methods must be executable by CSM as the root user, ensure that the file is owned by root.

- Ensure that the file has a minimum of 500-level permissions (read/execute by owner).
- Ensure any required authentication for the power method to access the hardware control point. Note that you cannot use CSM commands (like `systemid`) for this authentication.
- If more than one hardware control point is defined with your power method, CSM is able to call it several times in parallel for each hardware control point. Ensure that the power method can handle these parallel invocations.
- CSM support of user-defined power methods is limited to passing properly ordered and formatted arguments to the power method and processing response strings sent back by the power method.

### Required power actions

CSM invokes the user-defined power method with a power control action. These actions tell the power method which action needs to be performed on the node or device controlled by the power method. Each user-defined power method must support the following power control actions:

- **on**
  - Request to power on a node or device
- **off**
  - Request to power off a node or device
- **query**
  - Request for the power status of a node or device

These actions allow the power method to be integrated with the `rpower` command. CSM is also able to automatically update the `PowerStatus` attribute in the CSM database for any nodes or devices that the power method controls.

### Optional power control actions

In addition to the required power control actions, the user-defined power method can support the following actions if the hardware control device also supports the functions:

- **reboot**
  - Requests that the node or device be rebooted. If the target node or device is already powered off, this action should cause it to be powered on.
- **reset_hcp**
  - Requests that the hardware control device itself be reset.
- **getlist**
  - Returns information about all the hardware that is being controlled by the hardware control device.

The `rpower` command invokes the `reboot` and `reset_hcp` actions. The `lshwinfo` command invokes the `getlist` action.

### Installation of nodes with user-defined power methods

You must configure the hardware control configuration in order to install cluster nodes with the operating system and CSM. If any of the cluster nodes to be installed require a user-defined power method, you must provide the power method after the CSM software has been installed on the management server, but before you define and add the nodes.
**PowerStatusMode**

CSM does not support events when updating the power status of nodes and devices that are controlled by user-defined power methods. If the cluster **PowerStatusMode** attribute is set to **none** or **events**, CSM does not perform power status checking for nodes or devices controlled by the user-defined power methods. If the **PowerStatusMode** is set to **mixed** or **polling**, CSM performs power status checking.

See the **csmconfig** man pages or the *CSM for AIX and Linux: Command and Technical Reference* for information on setting **PowerStatusMode**.

**Power method location and naming**

You must place a user-defined power method in the following directory on the management server:

/opt/local

The name of the power method must be in the form **method_power**. Nodes and devices defined with this power method must have their **PowerMethod** attribute set to **method**, where **method** is the user-provided name.

For example, if your user-defined power method is called **usermethod_power** and is copied to the /opt/local directory, any nodes or devices that use this power method have their **PowerMethod** attribute in the CSM database set to **usermethod**. CSM recognizes the name as a user-defined power method and attempts to invoke /opt/local/usermethod_power when it needs to invoke power actions for these nodes or devices.

The following power methods are reserved for IBM use and must not be used for user-defined power methods:

- apc
- blade
- bmc
- bmc2
- csp
- fsp
- hmc
- ivm
- xseries

**Writing a user-defined power method**

All user-defined power methods must include error handling and logging. Ensure that any log messages are written to a log file in the /var/log/csm directory.

**Command input**

CSM invokes a user-defined method with the following list of arguments:
• Name of the power method
• Action to be performed
• HWControlPoint attribute defined in the CSM database for the target nodes or devices
• -n.Hostname:HWControlNodeId pairs of the target nodes, where -n is the name of the host. For devices, use the Name:HWControlDeviceId pair to specify a target device.

The power method uses the HWControlPoint value to connect to the device that controls the target nodes. The Hostname:HWControlNodeId pair or Name:HWControlDeviceId pair identifies the target of the requested action. These values can be repeated to specify multiple nodes or devices on the given hardware control point. If CSM receives a command intended for nodes or devices on multiple hardware control points, CSM invokes your power method multiple times.

In the topics and examples that follow, the term Hostname:HWControlNodeId represents the target of the action. If the target is a device, assume that the pair is Name:HWControlDeviceId.

Command output

When the user-defined power method is invoked, the results must be written in a response string to STDOUT. CSM intercepts STDOUT and parses the results. Ensure that the format of the response string is as follows:

Hostname:HWControlNodeId:Action_String

The value Action_String is formatted as follows where Action_Result is an action value, Action_Info is information in the form of an error message, and ETX is the ASCII End-Of-Text character (0x03):

Action_Result:Action_InfoETX

Ensure that ETX ends each response string sent to CSM and that one response string exists for each Hostname:HWControlNodeId pair that the power method invokes.

The Action_Result field returns the completion status of the action for a target node or device, and must contain one of the following ASCII values:

0 Action successful
1 Action failed

If the action fails (Action_Result = 1), the Action_Info field must contain an error message. CSM packages Action_Info and returns the information in CSM error message 2655-228 to the caller.

If the action is successful (Action_Result = 0), Action_Info contains information for the given action as follows:

Table 92. Power actions and Action_info

<table>
<thead>
<tr>
<th>Power actions</th>
<th>Action_info</th>
</tr>
</thead>
<tbody>
<tr>
<td>on</td>
<td>No Action_Info string required</td>
</tr>
<tr>
<td>off</td>
<td>No Action_Info string required</td>
</tr>
</tbody>
</table>
| query | 0 for power off  
|       | 1 for power on  
|       | 127 for unknown (power status cannot be determined) |

| reboot | No Action_Info string required |
| reset_hcp | No Action_Info string required |
| getlist | One string for each node or device on the given hardware control point, in the following format: Hostname|HWControlNodeId|HWType|HWModel|HWSerialNum |

These strings are concatenated for all the nodes or devices on the hardware control point and returned in a single Action_Info string.

Ensure that your power method is able to handle any power actions that are passed to it. If your power method receives a power action that it does not support, it must return an Action_Result of 1 along with an error message in the Action_Info string.

**Scenarios**

The following scenarios illustrate how a user-provided power method might operate for specific power actions:

"Action on" scenario: The following assumptions apply to this scenario:

- A user-defined power method called usermethod is defined, with a hardware control point of usr_hcp.cluster.com.
- Two nodes node1 with hardware control node id of 1 and node2 with hardware control node id of 2 are defined in the CSM database with power method usermethod

The following action occurs when the rpower command is given to power on node1 and node2:

1. CSM invokes the usermethod with the following command:

   `/opt/local/usermethod_power on usr_hcp.cluster.com node1:1 node2:2`

2. In this example, the power method writes the following responses (one for each node) to STDOUT:

   - node1:1:0:ETX
   - node2:2:0:ETX

   Each response string shows that the power on request is successful (Action_Result is 0). Because the on action requires no Action_Info, the Action_Info field is empty. The ETX character terminates each response.

If one of the nodes encounters an error the power method might write the following response string to STDOUT:

- node1:1:1:Unable to complete request.ETX
- node2:2:0:ETX
There are still two response strings, but they show that the power on request failed for node1 (Action_Result is 1). The power method must write an error message to the Action_Info field (in this example, Unable to complete request).

CSM passes this message back to the caller. In this example, rpower returns the following CSM error message for node1:

2655-228 [node1] Power method "usermethod" error: Unable to complete request

"Action off", "reboot", "reset_hcp": Because these three actions return an empty Action_Info field when successful, see "Action on" scenario for examples of the kinds of arguments for the power action and how to format the response strings.

"Action query" scenario: The following assumptions apply to this scenario:

- A user-defined power method called usermethod is defined with a hardware control point of \texttt{usrhcp.cluster.com}.
- Two nodes node1 with hardware control node id of 1 and node2 with hardware control node id of 2 are defined in the CSM database with power method usermethod.

The following action occurs when the rpower command is given to request the power status node1 and node2:

1. CSM invokes the usermethod with the following command:

   /opt/local/usermethod_power query usrhcp.cluster.com node1:1 node2:2

2. If node1 is powered on, and an error occurs for node2, the power method might write the following responses (one for each node) to STDOUT:

   node1:1:0:1ETX
   node2:2:1:Error occurred during operationETX

   The response string shows that the query request is successful for node1 (Action_Result is 0). Because Action_Info is 1, the node is powered on. However, the query request for node2 has failed (Action_Result is 1), and Action_Info contains an error message (Error occurred during operation).

   CSM passes the error message back to the caller. In this example, rpower returns the following CSM error message for node2:

   2655-228 [node1] Power method "usermethod" error: Error occurred during operation

"Action getlist" scenarios: The getlist action is sent by the lshwinfo command to obtain a list of all the hardware that a device controls. Not all devices return this information, and those that do might return only a subset of the information that the action can pass back to CSM.

In CSM, every node or device is defined by an identifier that is unique to the hardware control point that controls it. When CSM calls the getlist action, it passes any Hostname:HWControlNodeId pairs for all the nodes or devices defined for that hardware control point. The power method stores this data, and attempts to match the stored hardware control node id with the ids received from the hardware control point.
As a result, the power method can supply hostnames in the response strings as part of the output displayed by the `lshwinfo` command. If the power method does not perform this action, the `lshwinfo` command can only return `no_hostname` for all the nodes or devices.

"Action getlist" example 1: The following assumptions apply to this scenario:

- A user-defined power method called `usermethod` is defined with a hardware control point of `usrhcp.cluster.com`.
- Two nodes `node1` with hardware control node id of 1 and `node2` with hardware control node id of 2 are defined in the CSM database with power method `usermethod`.
- The hardware control point itself is controlling three nodes with hardware control node ids of 1, 2, and 3.

The following action occurs when the `lshwinfo` command is given for the hardware control point:

1. CSM invokes the power method with the following command:
   ```
   /opt/local/usermethod_power getlist usrhcp.cluster.com node1:1 node2:2
   ```
2. In this example, if the power method supports the `getlist` command, it might write the following response string to STDOUT:
   ```
   ::0:node1|1||||node2|2|||||3|||
   ```

   This is a single response string that contains all the required information and can be understood as follows:

   - The first two fields of the response string `Hostname` and `HWControlNodeId`, are left blank. They are not needed because the results of this command are not node specific. If they are included, CSM ignores them.
   - The command is successful (`Action Result` is 0).
   - The `Action_Info` field contains a formatted string with results of the action for hardware control node ids 1, 2, and 3. The power method has used the `Hostname:HWControlNodeId` pairs to match a hostname with the hardware control node id of which the hardware control point is aware. The unknown hardware control node id of 3 has no hostname associated with it, so no information is in the `Hostname` field.
   - The power method does not return information on `HWType`, `HWMethod`, or `HWSerialNum`, so nothing is returned in those fields.

In this example, if the power method does not support the `getlist` action, it might write the following response string to STDOUT:

```
::1:The "getlist" action is not recognized
```

CSM passes this error message back to the caller.

"Action getlist" example 2: The following assumptions apply to this scenario:

- A user-defined power method called `usermethod` is defined, with two hardware control points `usrhcp1.cluster.com` and `usrhcp2.cluster.com`. There are no nodes defined in the registry for either of these hardware control points.
- The hardware control point `usrhcp1` is controlling two nodes with hardware control node ids of `xyz` and `abc`, while the hardware control point `usrhcp2` does not have any nodes associated with it.
The following action occurs when the `lshwinfo` command that specifies `usermethod` and both hardware control points is issued:

1. CSM invokes the power method `usermethod` twice, once for each hardware control point, as follows:

   ```
   /opt/local/usermethod_power getlist usr_hcp1.cluster.com
   /opt/local/usermethod_power getlist usr_hcp2.cluster.com
   ```

2. The response to the first call is as follows:

   ```
   ::0:n|xyz|||abc|||ETX
   ```

   The response to the second call is as follows:

   ```
   ::0:ETX
   ```

   In this case, an **Action_String** is not included because nodes do not exist on the second hardware control point.

### Sample power method

The following code sample fragment is intended to show the interaction between CSM and the user-defined power method. It is not intended to be executable in this form:

```perl
#!/usr/bin/perl
#
# This sample code fragment is intended to show how a user-defined power method may be built using PERL. The functions in this fragment, get_hcp_hw, query_hw and power_hw are implementation-specific and are not defined here.
#
# Initialize a hash to hold the Hostname:HWControlNodeId pairs
#
# Start by collecting command line arguments. CSM will pass at least three arguments to the method, in the following sequence:
# 1. Action to be performed
# 2. Hardware Control Point name
# 3. Target Hostname:HWControlNodeId pairs (there may be more than one)
#
# Get the number of arguments
#$num_arg = @ARGV;

if( $num_arg < 2 ) {
    # This is the first example of the method returning information to CSM. CSM is expecting the response string to be in the following format:
    # Hostname:HWControlNodeId:Action_Result:Action_Info
    # The action and hardware control point must be supplied.
    # The target pairs must also be supplied if the action to be
```
# performed requires them.
#
# In our example, CSM did not pass enough arguments to our power
# method. Since we can't be sure what we were passed, we will
# leave the Hostname and HardwareControlNodeId fields blank. The
# Action_Result is set to 1 to indicate the failure, and the
# Action_Info is a string that will be sent back to CSM
# and returned to the end user. We use the "print" statement to
# send the string to CSM, which has redirected STDOUT.
#
# Each string sent to CSM must be terminated with an End-Of-Text
# (ETX) character, 0x03
#
# print ":::1:Insufficient arguments to power method\x03";
exit 1;
}

$action = shift @ARGV; # ARGV[0]
$hcp = shift @ARGV;    # ARGV[1]

# Build a hash to hold the target pairs
#
while( <ARGV> ){
    ( $hostname, $target ) = split /:/;
    $hostnames{ $target } = $hostname;
    push @targets, $_
}

# Initialize the Action_Info string
#
$action_info = "";

# This example method will process the "getlist" command, which will
# not have any Hostname:HWControlNodeId pairs associated with it.
#
if( $action eq "getlist" ) {
    # Call the user-written function that returns the list of
    # HWControlNodeIds for this hardware control point
    #
    $rc = get_hcp_hw( $hcp, @hcp_hw );

    if( $rc != 0 ) {
        # An error occurred in the function, which is reported
        # in the response string.
        #
        print ":::1:Error in get_hcp_hw function, return code $rc\x03";
        exit 1;
    }
}

# CSM requires the Action_Info portion of the response string to be
# in the following format:
#
# Hostname|HWControlNodeId|HWType|HWModel|HWSerialNum|
#
# This sequence is repeated for each target returned by the
# hardware control point.
#
# This function returns the hardware id and serial number
# of the devices on the hardware control point, separated by a
# colon.
#
foreach $hw_string( @hcp_hw ) {
    ( $hw_id, $hw_serial ) = split /:/, $hw_string;
# Try and match up the hw_id received back from the function
# to one of the target ids passed to us from CSM. If we can
# match it, we can supply a hostname to go with the id.
# if( exists( $hostnames{ $hw_id } ) ) {
#   $hw_host = $hostnames{ $hw_id };
# } else {
#   $hw_host = "";
# }
#
# Since the function doesn't return hardware type or hardware
# model, leave those blank.
# $hw_type = "";
# $hw_model = "";
#
# Append the data to the Action_Info string
# $action_info = "$action_info"."$hw_host|$hw_id|$hw_type|$hw_model|$hw_serial|";
#
# Once we exit the loop, all the hardware returned by the function
# has been processed. Print the response string to STDOUT and
# exit.
# print "::0:$action_info\x03";
# exit 0;
#
# All the remaining actions processed by this method require the target
# pairs passed at the command line. Process them now.
# foreach $dest( @targets ) {
#   ($hname, $trgt ) = split /:/, $dest;
#
#   # Check for the query action.
#   if( $action eq "query" ) {
#     $rc = query_hw( $hcp, $trgt, $state );
#
#     if( $rc != 0 ) {
#       # An error occurred in the function, which is reported
#       # in the response string.
#       # print "$hname:$trgt:1:Error in query_hw function, return code $rc\x03";
#       exit 1;
#     } else {
#       # CSM expects the query result to be one of three values:
#       # "0" (for "off")
#       # "1" (for "on")
#       # "127" (for "unknown")
#       # The method needs to map the state returned by the
#       # hardware to one of these three values
#       if( $state eq "off" ) {
#         $hw_state = "0";
#       } elsif( $state eq "on" ) {
#         $hw_state = "1";
#       } else {
#         $hw_state = "127";
#     }
# Build and return the response string
#
print "$hname:$trgt:0:$hw_state\x03";
exit 0;
}

# Check for a power on or off action
#
elsif( ( $action eq "off" ) || ( $action eq "on" ) ) {
    $rc = power_hw( $hcp, $trgt, $action );

    if( $rc != 0 ) {
        # An error occurred in the function, which is reported
        # in the response string.
        #
        print "$hname:$trgt:1:Error in power_hw function, return code $rc\x03";
        exit 1;
    } else {
        # Build and return the response string. No
        # Action_Info is needed for a power on or off,
        # so leave the last field blank.
        #
        print "$hname:$trgt:0:\x03";
        exit 0;
    }
} else {
    # The power action is not one the user method supports.
    #
    print "$hname:$trgt:1:Action $action not supported by this method\x03";
    exit 1;
}
Chapter 26. Remote console configuration

To enable your CSM cluster for remote console, you must set up and configure your hardware and networking, and define the remote console attributes in the CSM database.

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 Remote console attribute values 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 method used by CSM to open a remote console on the given node. 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. For some console methods (blade, bmc, bmc2, csp, hmc, fsp, ivm), the attribute value identifies the hardware control point that provides remote console access.

**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. This attribute is also not used for BMC; the value of the `ConsoleServerName` attribute identifies the BMC used to open a remote console. For IVM, set `ConsolePortNum` to `LParID`.

**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 `reconsole` 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.

**ConsoleSerialSpeed**
Contains the serial speed used to communicate with the node. The default value for this attribute is 9600, so you only need to set it if your console server speed is set to a value other than 9600 bps. For nodes using Serial Over LAN for remote console access, this attribute must be set to 19200. This attribute is not used for System p nodes that use the `hmc` `ConsoleMethod`.

When the `csm.client` package is installed on Linux nodes on xSeries, pSeries, or BladeCenter 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, CSM automatically adds 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 for details on how to redirect grub output to a remote console.

---

### Remote console software

Once your cluster hardware and networking have been configured, you must install and configure CSM software to enable remote console functions. For detailed CSM installation instructions, see Installing AIX on nodes, Installing Linux on nodes, Adding AIX nodes, and Adding Linux nodes. For detailed command usage information, see the rconsole and definènode man pages or the CSM for AIX and Linux: Command and Technical Reference.

**Note:**

1. Remote console function is not supported on System x 440 servers.
2. Using the rconsole command with BladeCenter HS20-8678 blade servers requires that you order and install additional serial port module parts. Alternatively, you can point your Web browser to the IP address or host name of the BladeCenter management module. See BladeCenter remote power configuration for detailed information on using remote console for BladeCenter hardware.

For examples of different remote console hardware configurations, see Remote console configuration.

To use remote console for a System x 360 node, configure the Serial Port Cable. System x support is available at http://www.ibm.com/servers/eserver/support/xseries/index.html.

### conserver read-only consoles

The rconsole command uses the conserver open source package to support 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 can 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.

The conserver software is packaged with CSM and installed with CSM on the management server. The conserver configuration file is located in /etc/opt/conserver/conserver.cf. The CSM rconsole command invokes the conserver software by default, allowing 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 definènode to refresh the conserver daemon.

**Note:**
Defining or removing large numbers of nodes simultaneously can degrade system performance. To avoid this consequence, 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
```

This condition and response pair is locked by default. These resources must be unlocked in order to perform these steps. For more information, see the information on locked conditions and responses in the *CSM for AIX and Linux: Administration Guide*.

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` flags are not available when `rconsole` is run with the `-c` flag, because `rconsole -c` bypasses the conserver daemon. The conserver software is required for read-only or force write functionality.

### Upgrading to conserver 8.1

CSM includes a version of the conserver open source software based on conserver 8.1, which offers a more secure console environment by disabling remote access to the conserver daemon from other systems on the network. The updated conserver RPM is available on the CSM installation or upgrade media. For AIX, conserver software is installed prior to installing CSM. For Linux, conserver software is updated automatically. If a prior version of conserver is installed on the management server, it is overwritten by the new version. The prior configuration file is saved in the `/etc/opt/conserver` directory, and a new configuration file is generated containing nodes currently defined in the cluster.

### Console server 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, IntelliStation, and eServer 325 servers only. For HMC-attached System p servers, the HMC provides the remote console function. For IVM-managed System p servers, the IVM provides remote console support.

**Attention:** The following console server hardware configuration tips 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. Read your hardware documentation before attempting to configure your console servers.

The default behavior of some console server devices keeps the RS-232 Data Terminal Ready (DTR) signal high at all times. As a result, a node console session can remain active even after closing the `rconsole` window. To change this default, you must change the console server serial port configuration. See the configuration documentation for the console server device to configure the serial port to drop the DTR signal when the session is closed. Also consult your site policy for securing remote console sessions.
MRV IR-8000 series configuration

To configure MRV IR-8000 series consoles for CSM remote console functionality:

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

To configure MRV LX-4000 series consoles for CSM remote console functionality:

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**

To configure the ELS for remote console functionality:

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.

**Computone configuration**

The Computone console device requires a BIOS level of 1.6.002 or later 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 later 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. To optimize security, change the default user IDs and passwords shipped with external devices.

3. For initial configuration, the CPS prompts 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:

```plaintext
SERVER SET IP=CPS_IP_Address MASK= subnet_mask GATEWAY=Default_gateway
```

5. For CSM remote console to work properly with the CPS console device, you must disable user authentication for the device by entering the following:

```plaintext
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:

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:

   ```plaintext
   port 1 set cli=off
   ```

4. Press the **Enter** key, and allow the console device to be rebooted when prompted.

### Cyclades configuration

To configure the Cyclades AlterPath ACS48 console server:

1. Connect a serial terminal or terminal emulator to the console port of the device. Configure the terminal settings for 9600 bps, 8 data bits, no parity, and 1 stop bit (9600 8-N-1).
2. Power on the AlterPath ACS48. When the device boots to a login prompt, login as **root**. The default root password is **tslinux**. To optimize cluster security, change the default root password shipped with external devices.
3. At the command prompt, enter:

   ```plaintext
   wiz
   ```

   This command starts the network configuration wizard and allows you to complete the network configuration, activate the changes, and save the changes to flash memory. If you do not select the DHCP configuration option, you are prompted to provide an IP address, domain name, DNS server, a gateway IP address, and a network mask.
Using remote console on BladeCenter

Using CSM remote console functionality, you can open a remote console session to any BladeCenter node from your management server. The specific procedure depends on your BladeCenter models and cluster environment.

Most BladeCenter blade servers use Serial Over LAN (SOL) to provide access to the serial consoles. Various BladeCenter components implement SOL, including the chassis Management Module and Ethernet Switch Module, BIOS, Advanced System Management Processor, and ethernet interface firmware. Ensure that the latest levels of firmware are installed across these components before configuring and using SOL.

Using remote console on BladeCenter HS20-8678

Remote console function for BladeCenter HS20-8678 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 at a time can own the KVM.

Ethernet Switch Module

The Serial Over LAN (SOL) connection requires an Ethernet Switch Module (ESM) to be installed in Module Bay 1. An ESM installed in this bay enables the SOL connection as well as the blade server interface to the eth0 ethernet. SOL and the blade server eth0 interface can coexist for most functions, with the exception of BladeCenter JS network boot and installation.

To network boot and install a BladeCenter JS blade server, you must install a second ESM in Module Bay 2 to enable the blade server eth1 interface. Then configure the JS20-8842 or JS21-8844 blade server to network boot and install over the eth1 interface.

A second ESM is not required to network boot and install a BladeCenter HS (other than HS20-8678) blade server. If only one ESM is installed in Module Bay 1 (enabling only the eth0 interface), temporarily disable the Serial Over LAN feature on the blade servers you are installing. Serial Over LAN can be enabled once the installation is complete.

Authentication and console requirements

To establish an SOL session, the CSM **rconsole** command must authenticate with the BladeCenter management module. Authentication requires credentials on the CSM management server that match login profiles stored on the management module. CSM uses the **RMTCON** management module user profile by default. This profile must be created on the management module for the **rconsole** command to work with the default authentication credentials. The profile can be added to the management module as follows:
1. From the management module Web interface navigation panel, select "Login Profiles" under "MM Control".
2. Under "Login Profiles", select an unused profile. On the following screen, add a profile named "RMTCON", with the following password:

   "RMTCON" (R-M-T-C-zero-N)

3. Under "Authority Level", select "Custom", then check the "Blade Server Remote Console Access" box. After you make the changes, save the profile.

**systemid command:** Authentication credentials used by CSM to access remote hardware are created using the `systemid` command. The `systemid -c` command creates credentials for the `rconsole` command. If you do not create credentials, the `rconsole` command attempts to use the default RMTCON profile and password to authenticate to the management module.

**Changing the password:** If the password for the RMTCON profile is changed, or another profile is used for remote console access, you must run the `systemid -c` command to create the credentials for the `rconsole` command.

**Using other profiles:** Do not use the default supervisor profile, or any other profile with supervisor authority level, as the console profile because supervisor authority can allow users access to commands that change the configuration or power state of the BladeCenter chassis and blade servers. Use a dedicated profile that allows only remote console access.


### Configuring SOL settings on the management module

The CSM `rconsole` command invokes SOL function through the management module. Complete the following steps to configure the SOL settings on the Management module:

1. On the navigation panel for the management module, click Blade Tasks ---> Serial Over LAN.
2. Under Serial Over LAN Configuration, set the following values:
   - **Serial Over LAN**: Enabled.
   - **BSMP IP address range**: x.x.x.x (BSMP IP range is not exposed to external changes)
   - **Accumulate timeout**: Use the default value of 5, or set another value.
   - **Send threshold**: Use the default value of 250, or set another value.
   - **Set Retry count**: Use the default value of 3, or set another value.
3. Save the changes.

### Enabling SOL on BladeCenter

Before running the `rconsole` command on BladeCenter blade servers, verify that the blade SOL status is ready. Complete the following steps to enable SOL on the blade servers:

- On the navigation panel of the management module, click Blade Tasks ---> Serial Over LAN;
- Scroll to Serial Over LAN Status.
- Check that the SOL column of the table indicates "Enabled".
• Check that the SOL Session column of the table indicates "Ready".
• If SOL is not enabled on the blade, select that blade server
• Click on Enable Serial Over LAN.

Verify the following console attributes for BladeCenter LS and HS (except for HS20-8678) blade servers:

```
ConsoleServerName = hostname or IP address of management module
ConsoleMethod = blade
ConsolePortNum = blade slot number
ConsoleSerialSpeed = 19200
ConsoleSerialDevice = ttyS1
```

Verify the following attributes for BladeCenter JS blade servers:

```
ConsoleServerName = hostname or IP address of management module
ConsoleMethod = blade
ConsolePortNum = blade slot number
```

**System x Serial Over LAN**

System x servers can be configured to use Serial Over LAN (SOL), including the eServer 326m, xSeries 336, 346, and System x 3455, 3550, 3650, 3655, and 3755 servers. Both CSM and the System x servers must be configured to use SOL, and you must open an SOL session to the Baseboard Management Controller (BMC). In an SOL session, serial data is redirected by the BMC to the management VLAN.

**Configuring CSM for SOL**

To configure CSM for SOL on eServer 326m and xSeries 336 and 346 nodes, the Baseboard Management Controller (BMC) requires a new user name dedicated to console access. CSM provides two utilities to assist in configuring this user name.

The `lsbmcconsusr` command queries the BMC on the target nodes and returns the user name (if any) assigned for remote console access. The `chbmcconsusr` command sets the specified name on the BMC. To avoid conflicts with remote power, the `chbmcconsusr` command does not configure user names on the BMC that already exist. Once the console user name is set, run the `systemid` command with the `-c` and `-s` flags to write the password for the console user to the BMC, and create an encrypted password file on the management server. See the man pages or the *CSM for AIX and Linux: Command and Technical Reference Guide* command usage information.

**Note:**

These steps are not required for System x 3455, 3550, 3650, 3655, or 3755 servers.

1. Run the `lsbmcconsusr` command to determine the current console user name for the BMC. If none has been set, the command returns the string "null".
2. Run the `chbmcconsusr` command to set a new user name on the BMC for console access. The command does not allow duplicate user names to be defined on the BMC.
3. Run the `systemid` command with the `-c` and `-s` flags to write the password to the BMC and create the encrypted password file.
4. Define the node console attributes as follows:

```
ConsoleServerName = IP address or hostname of node's BMC
ConsoleMethod = bmc
```
Configuring System x servers

To configure SOL on System x servers, you must change the BIOS settings. To change BIOS settings, reboot the server and press the F1 key when prompted to enter the Setup utility.

Important:
By setting the BMC Serial Port Access Mode to "Dedicated" the COM port on the server will not carry serial console data. Setting the value to "Shared" will allow serial data on both the COM port and the BMC. However, in this mode the COM port takes precedence over SOL until the Linux login prompt is displayed. This means when the value is set to "Shared", the POST BIOS screens and initial Linux boot messages will not be available to SOL.

Important:
Do not attempt to run ROM Diagnostics through the Serial Over LAN console session. Diagnostics will reset the BMC and NIC while loading, causing the SOL session to hang. ROM Diagnostics are run through the COM port only.

To configure SOL on xSeries 336, 346, and System x 3550, 3650, 3655, ad 3755 servers:

1. From the Configuration/Setup Utility menu, select "Advanced Setup".
2. From the Advanced Setup menu, choose "Baseboard Management Controller (BMC) Settings".
3. Set the following options:

   System-BMC Serial Port Sharing [ Enabled ]
   BMC Serial Port Access Mode [ Dedicated ]

4. Save the changes, exit Setup, and reboot the server.

To configure SOL on eServer 326m servers:

1. From the Configuration/Setup Utility menu, select "Advanced Setup".
2. From the Advanced Setup menu, choose "Baseboard Management Controller (BMC) Settings".
3. Set the following option:

   COM Port on BMC [ CLI ]

4. Save the changes, exit Setup, and reboot the server.

To configure SOL on System x 3455 servers:

1. From the Configuration/Setup Utility menu, select "Advanced Setup".
2. From the Advanced Setup menu, choose "Baseboard Management Controller (BMC) Settings".
3. From the BMC Settings menu, select "BMC COM Port Sharing/Configuration".
4. Set the following options:

   Serial Port Sharing [ Enabled ]
   Serial Port Access Mode [ BMC Serial Access Always Available ]

5. Save the changes, exit Setup, and reboot the server.
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 EL nodes, send Linux boot console output to the local console and an *rconsole* window as follows:

- Set `SAFE=YES` in */etc/sysconfig/kudzu*
- Add the following text 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
```

Console redirection on xSeries

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
To enable remote console redirection for xSeries servers, you must change the BIOS settings. 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.

**Note:**

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.

### Console redirection using Serial Over LAN on System x

Remote console redirection using Serial Over LAN is supported on xSeries 336 and 346, and System x 3550, 3650, 3655, and 3755 servers. 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 COM1
3. Remote Console Baud Rate - Select 19200
4. Remote Console Data Bits - Select 8
5. Remote Console Parity - Select None
6. Remote Console Stop Bits - Select 1
7. Remote Console Text Emulation - Select VT100/VT220
8. Remote Console Keyboard Emulation - Select VT100/VT220
9. Remote Console Active After Boot - Select Enabled
10. Remote Console Flow Control - Select Hardware

If the server is using a console server device, follow the instructions in [Console redirection on xSeries](http://www.ibm.com/developerworks/forums/dw_thread.jsp?forum=907&thread=128386&cat=53&treeDisplayType=threadmode1).

---

Console redirection using Serial Over LAN on System x 3455

Remote console redirection using Serial Over LAN is supported on System x 3455 servers. 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:

- Remote Console Serial Port [ Enabled ]
- Baud Rate [ 19200 ]
- Console Type [ vt100-8 bit ]
- Flow Control [ CTS/RTS ]
- Console Connection [ Direct ]
- Continue C.R. after POST [ On ]

Console redirection on BladeCenter

Remote console redirection is supported on BladeCenter HS (other than HS20-8678) blade servers. To enable remote console redirection for HS20 (other than HS20-8678) and HS21 servers, you must change the BIOS settings. 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 COM2
3. Remote Console Baud Rate - Select "19200"
4. Remote Console Data Bits - Select "8"
5. Remote Console Parity - Select "None"
6. Remote Console Stop Bits - Select "1"
7. Remote Console Text Emulation - Select "VT100/VT220"
8. Remote Console Keyboard Emulation - Select "VT100/VT220"
9. Remote Console Active After Boot - Select "Enabled"
10. Remote Console Flow Control - Select "Hardware"

Remote console redirection is supported by default on BladeCenter JS blade servers. No additional configuration is required.

Remote console redirection is supported on BladeCenter HS40 blade servers. To enable remote console redirection for HS40 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. Console Redirection - Select Serial Over LAN
2. Baud Rate - Select 19.2K
3. Flow Control - Select CTS/RTS
4. Terminal Type - Select VT100+

Remote console redirection is not supported for BladeCenter HS20-8678 blade servers; for remote console functionality, use a Web browser to connect to the BladeCenter management module.
Remote console redirection is supported on eServer 325, 326, and 326m servers. To enable remote console redirection, you must change the BIOS settings. Use the BIOS Configuration/Setup Utility to enable and configure remote console redirection. Select **Console Redirection** located under **Advanced Setup**. Configure remote console redirection by selecting the following menu options:

1. **Console Redirection** - Select the port that is connected to the terminal server. This port should correspond to the port defined as the node's `ConsoleSerialDevice` attribute value.
2. **Baud Rate** - Select the speed that matches the terminal server connected to this port. This speed also needs to match the node's `ConsoleSerialSpeed` attribute value. For e326m servers using Serial over LAN, set this value to 9600.
3. **FIFO Level** - Select Level 14
4. **Console Type** - Select vt100 plus
5. **Flow Control** - Select None
6. **Console Connection** - Select Direct
7. **Continue C.R. after POST** - Select **Save the settings and exit the Configuration/Setup Utility**.
Chapter 27. Installation directories and files

CSM directories store software packages, configuration information, scripts, and other files. Directories shown in the diagram below are examples and may not reflect your actual environment.

Create the /csminstall directory as an independent file system before installing CSM on your management server. Space requirements for /csminstall depend upon your cluster environment. If you are not using CSM to install the AIX or Linux operating system on your cluster nodes, and if you are installing the same version of CSM on all nodes, /csminstall requires 120 MB. The /csminstall directory requires and additional 120 MB for each additional version of CSM you are installing, and an additional 120 MB for each additional operating system and architecture. To install the AIX operating system on nodes using /csminstall to store NIM resources, add approximately 2 GB of space for each version of AIX. You are not required to store NIM resources in the /csminstall subdirectories. To install the Linux operating system on nodes, add approximately 2 GB of space for each version of Linux.

If you have not created the /csminstall directory manually, the installms or csmconfig -c command creates it when you install the management server. In this case, however, it will simply be created as a subdirectory of the / (root) file system and might not contain enough space for your intended use.

Portions of the /csminstall directory are replicated on each install server as either /csmserver or the InstallServer node attribute value. The distributions copied to /csmserver on the install server are used by the install server to install nodes. You may want to create /csmserver as its own file system on the install server before running csmsetupinstall, csmsetupnim, or updateisvr.

The /csminstall directory on the management server contains a copy of all the files that are distributed to all the install server.

The following diagram illustrates some of the directory locations that are used by CSM. The installms command establishes the CSM directories and the required packages when it is run from the management server. The diagram illustrates the overall directory structure of CSM after it has been installed on your system.

Note:

1. Not all directories listed below are created on all systems. Directories are only created for the operating system types that CSM is installing.
2. In the figure, xx for Red Hat EL or SLES represents the version number for the release. For valid distributions, see Linux on System x, Linux on x86 eServer and BladeCenter, and Linux on System p.
3. In Figure 13, version is the latest CSM version and release; for example, 1.7.1.
4. In Figure 13, arch is one of the following Linux architectures:
   - i386
   - x86_64
   - ppc64
5. In Figure 13, rh_service_level is InstallDistributionNameInstallDistributionVersion-InstallServiceLevel; rh_service_level can have the following values:

Table 93. rh_service_level values
### Table 94. sles_service_level values

<table>
<thead>
<tr>
<th>Node InstallServiceLevel value</th>
<th>Management server InstallService Level value</th>
<th>Same InstallDistributionName, InstallDistributionVersion and InstallPkgArchitecture values for node and management server</th>
<th>sles_service_level</th>
</tr>
</thead>
<tbody>
<tr>
<td>blank</td>
<td>any value</td>
<td>not applicable</td>
<td>InstallServiceLevel; for example, GA</td>
</tr>
<tr>
<td>specific service level; for example, QU2</td>
<td>any value</td>
<td>not applicable</td>
<td>InstallServiceLevel; for example, SP3</td>
</tr>
<tr>
<td>blank</td>
<td>GA</td>
<td>Yes</td>
<td>GA</td>
</tr>
<tr>
<td>blank</td>
<td>GA</td>
<td>No</td>
<td>GA</td>
</tr>
<tr>
<td>blank</td>
<td>specific service level; for example, QU2</td>
<td>Yes</td>
<td>GA</td>
</tr>
<tr>
<td>blank</td>
<td>specific service level; for example, QU2</td>
<td>No</td>
<td>GA</td>
</tr>
</tbody>
</table>

6. In **Figure 13** and in **Table 95**, sles_service_level is only the InstallServiceLevel attribute. sles_service_level can have the following values:
The following table describes some of the CSM directories. Directory names can contain the following variables, which correspond to node attribute values and must have the same values used during node definition.

**InstallOSName**

CSM for AIX and Linux: Planning and Installation Guide
Represents the operating system type. The supported values are Linux and AIX. For example, /csminstall/Linux.

InstallDistributionName

Represents the operating system distribution, RedHatEL-ES, RedHatEL-AS, RedHatEL-WS, RedHatEL-Server, RedHatEL-Client, and SLES are the valid values. This attribute is for Linux nodes only. For example, /csminstall/Linux/RedHatEL-AS.

InstallCSMVersion

Represents the version, release, and modification of CSM, specified as version.release.modification. This attribute is not required for AIX nodes. The valid values for Linux are 1.5.1, 1.6.0, 1.7.0 and 1.7.1. For example, /csminstall/Linux/RedHatEL-AS/csm/1.7.1.

InstallDistributionVersion

Represents the operating system version. Valid values for Red Hat EL are 4, 4.5, 4.6, 4.7, 5.1, 5.2 and 5.3. Valid values for SLES are 9 and 10. Valid values for AIX are 5.3.0 and 6.1.0. For example /csminstall/Linux/SLES/9.

InstallPkgArchitecture

Represents the machine architecture on Linux nodes. For xSeries, System x, and BladeCenter, the variable and the directory name are i386. The InstallPkgArchitecture value for machine architectures i486, i586, and i686, is also i386. For eServer 325 and 326, the variable and directory name are x86_64. For System p on Linux, the variable and directory name are ppc64. For example, /csminstall/Linux/SLES/9/i386.

InstallServiceLevel

Represents the operating system service pack. For SLES the value can be GA or SP3, for example. For Red Hat EL, the value can be GA, QU2, or QU3, for example. This value can also be user-defined value, such as test. For example, /csminstall/Linux/SLES/9/i386/QU3.

Table 95. CSM installation directories

<table>
<thead>
<tr>
<th>Directories/Files</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/csminstall</td>
<td>Main (parent) CSM install directory. /csminstall is mounted on the cluster nodes during both CSM-only and full installations. On the install server, the /csmserver directory is used by default. Everything in /csminstall is copied to /csmserver on the install servers. The /csmserver directory can be customized by changing the directory part of the InstallServer node attribute. On the install server, look for these files under /csmserver instead of /csminstall.</td>
</tr>
<tr>
<td>/csminstall/csm</td>
<td>Contains tools and libraries required for CSM (for files that are not specific to a particular version of CSM).</td>
</tr>
<tr>
<td>/csminstall/csm/config</td>
<td>Contains temporary node configuration files. Do not modify the contents of this directory.</td>
</tr>
<tr>
<td>/csminstall/csm/status</td>
<td>Status files of node installation.</td>
</tr>
<tr>
<td>/csminstall/csm/scripts</td>
<td>The directory in which the user can place configuration scripts that are run during the installation. This directory contains the following subdirectories: installprereboot, installpostreboot, osupgradeprereboot,</td>
</tr>
<tr>
<td>Directory</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>/csminstall/csm/scripts/installprereboot</td>
<td>Scripts run before the reboot during an operating system installation.</td>
</tr>
<tr>
<td>/csminstall/csm/scripts/installpostreboot</td>
<td>Scripts run after the reboot during an operating system installation. These scripts are run after CSM has been installed, after CFM files have been copied, and after SMS packages have been installed.</td>
</tr>
<tr>
<td>/csminstall/csm/scripts/osupgradeprereboot</td>
<td>Scripts run before the reboot during an operating system upgrade.</td>
</tr>
<tr>
<td>/csminstall/csm/scripts/osupgradepostreboot</td>
<td>Scripts run after the reboot during an operating system upgrade. These scripts are run after CSM has been upgraded, after CFM files have been copied, and after SMS packages have been installed.</td>
</tr>
<tr>
<td>/csminstall/csm/scripts/disklessprebuild</td>
<td>Scripts run during the building of the diskless image.</td>
</tr>
<tr>
<td>/csminstall/csm/scripts/disklessboot</td>
<td>Scripts run during the diskless node boot.</td>
</tr>
<tr>
<td>/csminstall/csm/scripts/update</td>
<td>Scripts run on the node by the <code>updatenode</code> command. These scripts are run after CSM is installed, but before CFM files are copied and before SMS packages are installed.</td>
</tr>
<tr>
<td>/csminstall/csm/scripts/data</td>
<td>User data files can be stored in this directory, and used by any of the user scripts in the <code>/scripts</code> directory.</td>
</tr>
<tr>
<td>/csminstall/csm/InstallCSMVersion</td>
<td>Contains tools and libraries required for CSM (for files that are specific to a particular version of CSM).</td>
</tr>
<tr>
<td>/csminstall/csm/InstallCSMVersion/kickstart.InstallDistributionName</td>
<td>The Kickstart configuration file for each node.</td>
</tr>
<tr>
<td>/csminstall/csm/InstallCSMVersion/autoyast.InstallDistributionName</td>
<td>The AutoYaST configuration file for each node.</td>
</tr>
<tr>
<td>/csminstall/diskless</td>
<td>Holds the VNFS for diskless nodes, and holds the configuration files (vnfsrpm) for the VNFS.</td>
</tr>
<tr>
<td>/csminstall/InstallOSName</td>
<td>Contains files needed to install and configure.</td>
</tr>
<tr>
<td>Path</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>/csminstall/InstallOSName/InstallDistributionName/</td>
<td>The directory in which the RPM packages, that will be installed on the management server and the nodes, are stored. installms copies the CSM RPMs from the CSM CD to this directory. RPMs of open source and IBM Java2 programs also get stored here.</td>
</tr>
<tr>
<td>csm/InstallCSMVersion/packages/*.rpm</td>
<td></td>
</tr>
<tr>
<td>/csminstall/InstallOSName/InstallDistributionName/</td>
<td>The directory in which the RPM packages of the same service level as management server are stored.</td>
</tr>
<tr>
<td>InstallDistributionVersion/InstallPkgArchitecture/RPMS</td>
<td></td>
</tr>
<tr>
<td>/csminstall/InstallOSName/InstallDistributionName/</td>
<td>The directory that contains software packages to be installed on the nodes. When you place RPMs in this directory, they are installed on the nodes by the smsupdatenode and updatenode commands. See the smsupdatenode and updatenode man pages for more information.</td>
</tr>
<tr>
<td>InstallDistributionVersion/InstallPkgArchitecture/install/*.rpm</td>
<td></td>
</tr>
<tr>
<td>/csminstall/InstallOSName/InstallDistributionName/</td>
<td>The directory that contains software updates to be installed on the nodes. When you place RPMs in this directory, they are updated/installed on the nodes by the smsupdatenode and updatenode commands. See the smsupdatenode and updatenode man pages for more information.</td>
</tr>
<tr>
<td>InstallPkgArchitecture/updates</td>
<td></td>
</tr>
<tr>
<td>/csminstall/InstallOSName/InstallDistributionName/</td>
<td>The directory in which the RPM packages, that will be installed on the nodes, are stored. installms or copycsmpkgs copies the RPMs that are needed to install CSM on the nodes to this directory. csmsetupinstall, copycds and smsupdatenode -copy are all commands that copy the RPMs to this directory that are needed to install the operating system and perform software maintenance.</td>
</tr>
<tr>
<td>InstallDistributionVersion/InstallPkgArchitecture/rh_service_level</td>
<td></td>
</tr>
<tr>
<td>or sles_service_level/RPMS</td>
<td></td>
</tr>
<tr>
<td>/etc/dhcpd.conf</td>
<td>The system configuration file for the dhcp server.</td>
</tr>
<tr>
<td>/opt/csm/install/kscfg.tmpl.</td>
<td>The default Kickstart configuration template file.</td>
</tr>
<tr>
<td>InstallDistNameInstallDistributionVersion</td>
<td></td>
</tr>
<tr>
<td>/opt/csm/install/yastcfg.</td>
<td>The default AutoYaST configuration template file.</td>
</tr>
<tr>
<td>InstallDistNameInstallDistributionVersion.xml</td>
<td></td>
</tr>
<tr>
<td>/csminstall/InstallOSName/InstallDistributionName/</td>
<td>Contains the directories and files in each CD.</td>
</tr>
<tr>
<td>InstallDistributionVersion/InstallPkgArchitecture/sles_service_level</td>
<td></td>
</tr>
<tr>
<td>CD*</td>
<td></td>
</tr>
<tr>
<td>/csminstall/Linux/InstallDistributionName/</td>
<td>This directory is used to install additional packages is not InstallServiceLevel sensitive to diskless nodes.</td>
</tr>
<tr>
<td>csm_addon</td>
<td></td>
</tr>
<tr>
<td>/csminstall/Linux/InstallDistributionName/InstallServiceLevel/csm_addon</td>
<td>This directory is used to install additional packages is InstallServiceLevel sensitive to diskless nodes.</td>
</tr>
<tr>
<td>/csmserver/Linux/InstallDistributionName/InstallDistributionVersion/</td>
<td>New Directory for Yum Repository. This</td>
</tr>
<tr>
<td>InstallPkgArchitecture/InstallServiceLevel/Server/csmrepo</td>
<td>change only affects the RHEL 5 or later.</td>
</tr>
</tbody>
</table>
Chapter 28. CSM support for Blue Gene

The IBM System Blue Gene Solution is described at http://www.ibm.com/servers/deepcomputing/bluegene.html. The software included with a Blue Gene Solution lets you manage your racks and jobs efficiently. CSM complements the Blue Gene Solution software by providing capabilities to help you manage your Service Node, Front End Nodes, and File Servers. Additionally, CSM includes optionally-installable Blue Gene-specific monitoring capabilities.

Within your Blue Gene environment, you can install, configure and use all of CSM, including the Blue Gene-specific monitoring capabilities, or install and configure just enough CSM to use the Blue Gene-specific monitoring capabilities alone. If you choose to use all of CSM, you install CSM in the usual manner, setting up a management server on a supported platform, defining cluster nodes, etc. This is called Full CSM plus Blue Gene monitoring support. If you choose to use the Blue Gene monitoring capabilities of CSM only, you install a subset of CSM, setting up a simple management server on your Blue Gene Service Node, but skipping the definition of cluster nodes and other tasks. This is called Stand-alone CSM Blue Gene monitoring support. You can start with Stand-alone support to keep things simple and exploit just the Blue Gene-specific capabilities of CSM. It is easy to install and set this up, and it may turn out to be all you ever want or need. Of course, you can always migrate to Full support later if you want to take advantage of all that CSM has to offer. On the other hand, you can install and set up Full support at the outset if you wish, but it is more involved and will take more time.

Stand-alone CSM Blue Gene monitoring support

The following diagram depicts a Blue Gene environment with Stand-alone CSM Blue Gene monitoring support:
To use Stand-alone CSM Blue Gene monitoring support your Service Node must be set up as a CSM management server as shown in the diagram. Additionally, you install CSM's Blue Gene-specific monitoring support on your Service Node. CSM is installed nowhere else, and no nodes are defined.

With this Stand-alone support installed, you can monitor the Blue Gene database for configuration, RAS, and environmental events that occur in the Blue Gene core.

Installation and Setup

To install and set up the Stand-alone CSM Blue Gene monitoring support, do the following on your Service Node:

Notes:
These steps assume that you have already installed and configured your Service Node as described in the Blue Gene documentation. For full details on the CSM commands mentioned below see the man pages or the CSM for AIX and Linux: Command and Technical Reference.

1. Obtain the CSM for Linux ppc64 CD or tarball. If using the CD, insert it into the CD drive on your Service Node. If using the tarball, unzip and extract its contents to a directory of your choice on your Service Node.
2. Change directory to the CD mount point, or the unzipped and extracted tarball directory.
3. Run: \texttt{rpm -i csm.core* csm.bluegene*}
4. Add \texttt{/opt/csm/bin} to your PATH.
5. Run: \texttt{installms -p package_path}
6. Run: \texttt{csmconfig -L license_key_file}
7. Run: `bgsetupmon`

Once you have installed and setup *Stand-alone CSM Blue Gene monitoring support* on your Service Node, a number of Blue Gene-specific resources have been defined for you, and a new command, *bgmksensor*, has been installed on your Service Node.

To verify your installation and setup, perform these checks on your Service Node:

- `lscondition | grep BG`
  This command should return a list of Blue Gene-related predefined IBM.Condition resources.
- `lssensor | grep BG`
  This command should return a list of Blue Gene-related predefined IBM.Sensor resources.
- `bgmksensor -h`
  This should show the usage information for the *bgmksensor* command.

So what's next? Information on using CSM's Blue Gene-specific monitoring capabilities can be found in the *CSM for AIX and Linux: Administration Guide*.

### Updating

To update your *Stand-alone CSM Blue Gene monitoring support* when a new level of CSM becomes available, complete the following steps on your Service Node:

#### Pre-update

1. Run `lscondresp >/tmp/associations`
2. Examine `/tmp/associations`, and for each association built on a predefined or user-defined Blue Gene-related condition run `rmcondresp condition_name`
4. Run `lscondition >/tmp/conditions`
5. Examine `/tmp/conditions`, and for each user-defined Blue Gene-related condition:
   a. Run `lsrsrc -i -s 'Name=="condition_name"' IBM.Condition >/tmp/condition_name.condition`
   b. Save `/tmp/condition_name.condition` for Post-update.
   c. Run `rmcondition condition_name`
6. Run `lssensor >/tmp/sensors`
7. Examine `/tmp/sensors`, and for each user-defined Blue Gene-related sensor:
   a. Run `lsrsrc -i -s 'Name=="sensor_name"' IBM.Sensor >/tmp/sensor_name.sensor`
   b. Save `/tmp/sensor_name.sensor` for Post-update.
   c. Run `rmsensor sensor_name`
8. If you are migrating from *Stand-alone* to *Full* support, return now to the next step in the migration procedure. Otherwise, proceed to the Update steps below.

#### Update

1. Obtain the CSM for Linux ppc64 CD or tarball. If using the CD, insert it into the CD drive on your Service Node. If using the tarball, unzip and extract its contents to a directory of your choice on your Service Node.
2. Change directory to the CD mount point, or the unzipped and extracted tarball directory.
3. Run: `rpm -U csm.core* csm.bluegene*`
4. Make sure `/opt/csm/bin` is in your PATH.
5. Run: `installms -p package_path`
6. Run: `csmconfig -L license_key_file`
7. Run: `bgsetupmon`

**Post-update**

1. Recycle DB2(R) on your Service Node to discard the old `bgregfresh_sensor.so` and ensure that the new one is loaded and used. Do the following for BG/L (or similar for BG/P):
   a. `sudo /usr/bin/bglmaster stop`
   b. `su - bglsysdb -c "db2 force application all ; db2 terminate ; db2stop"`
   c. `su - bglsysdb -c "db2start"`
   d. `sudo /usr/bin/bglmaster start`
2. If you have `/tmp/sensor_name.sensor` files on your Service Node (from Pre-update) do the following for each file:
   a. Run `mkrsrc -f /tmp/sensor_name.sensor IBM.Sensor`
3. If you have `/tmp/condition_name.condition` files on your Service Node (from Pre-update) do the following for each file:
   a. If you are migrating from Stand-alone to Full support, and if you have installed and set up a CSM management server on a system that is not your Service Node, copy the file to your new management server and complete the following steps on that management server. Otherwise, complete the following steps on your Service Node (which, of course, is also your management server).
   b. Run `mkrsrc -f /tmp/condition_name.condition IBM.Condition`
4. If you have a `/tmp/associations` file on your Service Node (from Pre-update) do the following for each Blue Gene-related condition response association listed in the file:
   a. Run `mkcondresp` with appropriate flags and operands to redefine the association.
   b. If the State of the association is Event Monitored in your `/tmp/associations` file, use `startcondresp` with appropriate flags and operands to restart Blue Gene monitoring on that association.

---

**Full CSM plus Blue Gene monitoring support**

The following diagram depicts a Blue Gene environment with *Full CSM plus Blue Gene monitoring support*: 

---

CSM for AIX and Linux: Planning and Installation Guide 397
To use Full CSM plus Blue Gene monitoring support, you must set up a CSM management server, and your Service Node, Front End Nodes, and File Servers must be set up as managed nodes as shown in the diagram. The CSM management server can be a distinct system as shown, or it can be installed on a Blue Gene system; typically the Service Node. (Note that the Blue Gene core, which consists of I/O and Compute Nodes, is not directly managed by CSM.) For simplicity, the diagram depicts the Blue Gene systems as the only cluster nodes, but the CSM cluster can be much larger and include other managed nodes as well.

You can use basic CSM function to install, update, manage, and monitor the Blue Gene Service Node, Front End Nodes, and File Servers. Additionally, by installing the CSM Blue Gene-specific monitoring support, you can also monitor the Blue Gene database on the Service Node for configuration, RAS, and environmental events that occur in the Blue Gene core.

**Installation and Setup**

To install and set up Full CSM plus Blue Gene monitoring support, or to migrate from Stand-alone CSM Blue Gene monitoring support to Full CSM plus Blue Gene monitoring support, follow the steps below. (For details on the CSM commands mentioned see their man pages or the *CSM for AIX and Linux: Command and Technical Reference*.)

1. This first step depends on your current environment. Do **ONE** of the following:
   a. Install and set up a CSM management server on a supported platform. You can do this on your Blue Gene Service Node (or the system destined to become your Blue
Gene Service Node), or on a distinct system. Please see Installing a CSM for AIX management server or Installing a CSM for Linux management server.

b. If you have not already done so, install and set up your Blue Gene systems as per the Blue Gene documentation. Specifically, install and set up your Service Node, Front End Nodes, and File Servers. (If you need to do this step now, consider using your CSM management server to deploy these Blue Gene systems.)
   o If you have Stand-alone CSM Blue Gene monitoring support installed already and you want to migrate to Full CSM plus Blue Gene monitoring support, do the following:
      a. Follow the Pre-update steps in the Stand-alone CSM Blue Gene monitoring support section. You will be directed back here when you have completed those steps.
      b. If you plan to continue using your Service Node as your CSM management server, you can proceed to the steps below. If you plan to install and set up a CSM management server on a different system, do so now using the instructions in the Installing a CSM for AIX management server or Installing a CSM for Linux management server section, as appropriate.

2. If you have an AIX CSM management server, use the geninstall or installp command to install the csm.bluegene package from the CSM for AIX CD or from the expanded tarball. If you have a Linux CSM management server, change directory to /csminstall/Linux/distro/csm/1.7.1/packages, where distro is the Linux distribution installed on the management server - for example, SLES or RedHatEL-AS - and run: rpm -i csm.bluegene*

3. Create or modify your node definitions file and include the appropriate Blue Gene attributes:

Your Service Node must have:

Properties=BlueGeneNodeType::ServiceNode

Your Front End Node or Nodes must have:

Properties=BlueGeneNodeType::FrontEndNode

Your File Server or Servers must have:

Properties=BlueGeneNodeType::FileServer

If your Blue Gene systems are combined, specify the Properties as follows:

Properties=BlueGeneNodeType::ServiceNode,FrontEndNode

Node definition files are described in Defining nodes.

4. Run the definenode [-m] -f nodedef_file command. Use the -m flag if you modified your nodedef file, omit it if your nodedef file is new and CSM node definitions do not yet exist for your Blue Gene systems.

5. If your management server is not also your Service Node, and has a different operating system than your Service Node, run the copycsmpkgs -n service_node command to copy the CSM SLES ppc64 packages from the CSM for Linux on POWER CD, or from the expanded tarball, to the /csminstall directory.

6. Run the bgsetupms [-t P] command. (-t P must be used for Blue Gene/P, -t L (or no flag) must be used for Blue Gene/L.)

7. Run the updatenode -n service_node command.

8. If you are migrating from Stand-alone to Full support, Follow the Post-update steps in the Stand-alone CSM Blue Gene monitoring support section. When you have finished those steps, your migration from Stand-alone to Full support will be completed.
Once you have installed and set up Full CSM plus Blue Gene monitoring support, a number of Blue Gene-specific resources have been defined for you, and a new command, bgmksensor, has been installed on your Service Node. For information on using these, see CSM for AIX and Linux: Administration Guide.

To verify your installation and setup, perform these checks on your management server (except as noted):

- **nodegrp | grep BlueGene**
  This command should return three dynamic node group names:
  - BlueGeneServiceNodes
  - BlueGeneFrontEndNodes
  - BlueGeneFileServers
- **nodegrp BlueGeneServiceNode**
  This command should return the hostname of your Blue Gene Service Node. Run similar commands to check the membership of BlueGeneFrontEndNodes and BlueGeneFileServers.
- **lscondition | grep BG**
  This command should return a list of Blue Gene-related predefined IBM.Condition resources.
- **On your Service Node, run: bgmksensor -h**
  This should show the usage information for the bgmksensor command.
- **On your Service Node, run: lssensor | grep BG**
  This command should return a list of Blue Gene-related predefined IBM.Sensor resources.

So what's next? Information on using CSM's Blue Gene support can be found in the CSM for AIX and Linux: Administration Guide.

Migration from Stand-alone CSM Blue Gene monitoring support

To migrate from Stand-alone CSM Blue Gene monitoring support to Full CSM plus Blue Gene monitoring support, follow the Full CSM plus Blue Gene monitoring support Installation and Setup procedure. It contains the migration steps.

**Updating**

To update your Full CSM plus Blue Gene monitoring support when a new level of CSM becomes available, you must complete the following steps at the appropriate points in the overall CSM update procedure.

**Pre-update**

Use these steps in the context of updating your management server; so begin with the steps in Updating the CSM for AIX management server or Updating CSM on a Linux management server. You will be directed back here at the appropriate point.

1. Do the following on your management server:
   a. Run lscondresp >/tmp/associations
   b. Examine /tmp/associations, and for each association built on a predefined and user-defined Blue Gene-related condition run rmcondresp condition_name.
   c. Save /tmp/associations for Post-update.
2. Do the following on your management server:
   a. Run lscondition >/tmp/conditions.
   b. Examine /tmp/conditions, and for each user-defined Blue Gene-related condition:
Do the following on your Blue Gene Service Node:

a. Run `lsensor >/tmp/sensors`.

b. Examine `/tmp/sensors`, and for each user-defined Blue Gene-related sensor:
   i. Run `lsrsrc -i -s 'Name=="sensor_name"' IBM.Sensor >/tmp/sensor_name.sensor`
   ii. Save `/tmp/sensor_name.sensor` for Post-update.
   iii. Run `rmsensor sensor_name`.

3. Do the following on your Blue Gene Service Node:

   a. Run `lsrsrc -i -s 'Name=="condition_name"' IBM.Condition`.
      >/tmp/condition_name.condition
   ii. Save `/tmp/condition_name.condition` for Post-update.
   iii. Run `rmcondition condition_name`.

4. Return to Updating the CSM for AIX management server or Updating CSM on a Linux management server, and continue with the procedure.

**Post-update**

Use these steps in the context of updating CSM on your Blue Gene Service Node; so begin with the steps in Updating CSM on Linux nodes. You will be directed back here at the appropriate point.

1. On the Service Node, recycle DB2(R) to discard the old `bgrefresh_sensor.so` and ensure that the new one is loaded and used. Do the following for BG/L (or similar for BG/P):
   a. `sudo /usr/bin/bglmaster stop`
   b. `su - bglsysdb -c "db2 force application all ; db2 terminate ; db2stop"`
   c. `su - bglsysdb -c "db2start"`
   d. `sudo /usr/bin/bglmaster start`

2. If you have `/tmp/sensor_name.sensor` files on your Service Node (from Pre-update) do the following for each file:
   a. Edit the file and delete the `ActivePeerDomain` line, if present. Also, examine the `Command` line. If a `-C` flag appears in the `bgmanage_trigger` command, change it to `-w`.
   b. Run `mkrsrc -f /tmp/sensor_name.sensor IBM.Sensor`

3. On the management server, if you have `/tmp/condition_name.condition` files (from Pre-update) do the following for each file:
   a. Edit the file and delete the `ActivePeerDomain` line, if present. Also, ensure that the `EventExpression` value is `SD.Uint32>0 && SD.Int32==1`, and that the line `NoToggleExprFlag = 1` is present.
   b. Run `mkrsrc -f /tmp/condition_name.condition IBM.Condition`

4. On the management server, if you have a `/tmp/associations` file (from Pre-update) do the following for each Blue Gene-related condition response association listed in the file:
   a. Run `mkcondresp` with appropriate flags and operands to redefine the association.
   b. If the `State` of the association is `Event Monitored` in your `/tmp/associations` file, use `startcondresp` with appropriate flags and operands to restart Blue Gene monitoring on that association.

5. Return to Updating CSM on Linux nodes and complete any remaining procedures there.
Chapter 29. Avoiding problems with hardware and network setup

Use the following information to avoid problems with your CSM cluster hardware and network setup.

**DHCP errors**

A Dynamic Host Configuration Protocol (DHCP) problem can cause Linux node installation to fail. A DHCP failure can be caused by Ethernet switch Spanning-Tree protocol settings. To avoid this problem, either turn off Spanning-Tree or preferably, enable the portFast setting for the ports. For more information about potential Spanning-Tree problems, refer to the following CSM FAQs:


The CSM management server must be the only DHCP server running on the subnet. If you have another DHCP server running on the same subnet as the CSM management server and the nodes, it can intercept the DHCP broadcasts from the nodes. As a result, the install process will not start.

**Before you run csmsetupinstall:** Before you run the `csmsetupinstall` command on Red Hat EL or SLES, modify the `/etc/sysconfig/dhcpd` file to only listen for dhcp requests on specific interfaces. For example, if eth0 connects to the management VLAN, eth1 connects to the cluster VLAN, and eth2 connects to the public VLAN, you probably do not want the public VLAN (eth2) to accept dhcp requests; to listen to eth0 and eth1 only, you must modify the `/etc/sysconfig/dhcpd` file, as follows:

1. To prevent `csmsetupinstall` from modifying the interface information in `/etc/sysconfig/dchpd`, add the following to `/etc/sysconfig/dchpd`:
   ```
   #CSM_NO_CHANGE
   ```

2. For Red Hat EL, ensure that `/etc/sysconfig/dchpd` contains the following line:
   ```
   DHCPDARGS="eth0 eth1"
   ```

   For SLES, ensure that `/etc/sysconfig/dchpd` contains the following line:
   ```
   DHCPD_INTERFACE="eth0 eth1"
   ```

---

**Configuring a switch for multiple VLANs**

Attaching multiple network interfaces on a management server to the same VLAN can produce unexpected results, because broadcast traffic on the VLAN is seen on multiple interfaces. One potential problem is that...
ARP requests for the IP address assigned to one interface can be seen by another interface first. This causes the second interface to send its MAC address back in a form of automatic proxy ARPing. This can cause inbound and outbound traffic for a given network to be split between the interfaces, with inbound traffic coming in on the wrong interface. In addition, protocols that rely on broadcast traffic, such as DHCP, can get confused by the multiple queries and responses that are seen on the network.

To avoid these problems, connect the various cluster networks to separate VLANs.

The following example shows switch configuration for multiple VLANs. The first 16 ports are part of cluster-VLAN, and the remaining ports are part of the default VLAN1, and the Gbps ports trunk.

```
# Connect to the Cisco switch
> telnet cisco
> enable

# Create the new VLAN
> vlan database
> vlan 2 name cluster-VLAN
> exit
# Confirm that the VLAN has been created
> show vlan brief

# Add ports to the VLAN
# Note that we also set each port with "spanning-tree portfast".
# Without this option, DHCP may fail because it takes too long
# for a port to come online after a node powers up.
> configure terminal

# The following needs to be done for each port being added to the VLAN
# For example "interface Fa0/3" for port 3.
> interface Fa0/{port number}
> switchport mode access
> switchport access vlan 2
> spanning-tree portfast
> exit

# When done, exit the configuration mode
> exit

# Verify that the ports are now part of the new VLAN
> show vlan brief

# Make the Fiber ports trunk all VLANS
> configure terminal
> interface Gi0/1
> switchport mode trunk
> switchport trunk encapsulation is1
> exit
> interface Gi0/2
> switchport mode trunk
> switchport trunk encapsulation is1
> exit
> exit

# Save the config
> copy running-config startup-config
> exit
```
Using external SCSI devices

The method for assigning SCSI device names can cause device name problems when installing the Linux operating system on System x servers. During the installation process, SCSI device names are assigned according to the order in which they are found. Therefore, for systems that put their onboard SCSI controllers last in the PCI probe order, any add-on SCSI controllers are found first, and have their attached drives mapped first. This is a common problem for systems that have external storage attached to either a secondary SCSI or FiberChannel PCI adapter.

Note the following output from the /proc/pci file on an xSeries 345 system with optional QLogic fibre adapters:

Bus 6, device 1, function 0:
  Fibre Channel: QLogic Corp. QLA2300 (rev 1).
    IRQ 16.
    Master Capable. Latency=64. Min Gnt=64.
    I/O at 0x2400 [0x24ff].
    Non-prefetchable 64 bit memory at 0xfbfff000 [0xfbffffff].
Bus 8, device 2, function 0:
  Fibre Channel: QLogic Corp. QLA2300 (#2) (rev 1).
    IRQ 18.
    Master Capable. Latency=64. Min Gnt=64.
    I/O at 0x2600 [0x26ff].
    Non-prefetchable 64 bit memory at 0xf9fff000 [0xf9ffffff].

Bus 6, device 8, function 0:
  Ethernet controller: PCI device 8086:1010 (Intel Corp.) (rev 1).
    IRQ 29.
    Master Capable. Latency=64. Min Gnt=255.
    Non-prefetchable 64 bit memory at 0xfbfc0000 [0xfbfdffff].
    I/O at 0x2500 [0x253f].
Bus 6, device 8, function 1:
  Ethernet controller: PCI device 8086:1010 (Intel Corp.) (rev 1).
    IRQ 30.
    Master Capable. Latency=64. Min Gnt=255.
    Non-prefetchable 64 bit memory at 0xfbfa0000 [0xfbfbffff].
    I/O at 0x2540 [0x257f].
Bus 8, device 7, function 0:
  SCSI storage controller: LSI Logic / (...) 53c1030 (rev 7).
    IRQ 27.
    I/O at 0x2700 [0x27ff].
    Non-prefetchable 64 bit memory at 0x9fe0000 [0x9fefe000].
    Non-prefetchable 64 bit memory at 0x9f00000 [0x9f00000].
Bus 8, device 7, function 1:
  SCSI storage controller: LSI Logic / (...) 53c1030 (#2) (rev 7).
    IRQ 28.
    I/O at 0x28000 [0x28ff].
    Non-prefetchable 64 bit memory at 0x9fc00000 [0x9fc00000].
    Non-prefetchable 64 bit memory at 0x9f00000 [0x9f00000].

With this PCI bus arrangement, the first drive or LUN in a storage controller attached to one of the QLogic adapters is mapped by the install kernel as /dev/sda. This causes the installation to overwrite any existing data on that drive or LUN, and creates boot problems because the bootstrap code is written to a drive that is not bootable using the system BIOS.

To avoid this problem, any externally attached SCSI devices or controllers must be powered off or disconnected when you install the operating system. This forces the installation to occur on the native
system drives. After the operating system has been installed, verify that the /etc/modules.conf file lists the modules for add-on controllers with the highest scsi_hostadapter numbers, and that any special SCSI options have been set for those controller types. For example, the following /etc/modules.conf file is for an xSeries 345 server with a FAStT controller attached using Qlogic adapter cards:

```
alias parport_lowlevel parport_pc
alias eth0 e1000
alias eth1 e1000
alias usb-controller usb-ohci
alias scsi_hostadapter mptbase
alias scsi_hostadapter1 mptscsih
alias scsi_hostadapter2 mptscsih
alias scsi_hostadapter3 mptscsih
alias scsi_hostadapter4 qla2300
options scsi_mod max_scsi_luns=128
```

If you change the modules.conf file, you must run the mkinitrd utility to rebuild the boot initrd image.

---

**Installing multiple Linux nodes simultaneously**

To install more than eight Linux nodes simultaneously using the installnode command, you must do the following:

1. For SLES, update the following file:

   `/etc/sysconfig/nfs`

   Set `USE_KERNEL_NFSD_NUMBER` to a higher value than the default of 8. Based on the number of nodes you are installing, consider setting the value to 16 or 32. If you have a large number of nodes, set the value to 32.

   For Red Hat EL, update `/etc/init.d/nfs` and change `RPCNFSDCOUNT` to a higher value than the default value of 8.

2. On SLES and Red Hat EL, restart the nfs server to ensure that the values take effect.

3. On SLES and Red Hat EL, use multiple install servers to increase the number of concurrent CSM and Linux operating system installations.

4. Before you run installnode to install a large number of nodes simultaneously, use the following commands to set the `CSM_FANOUT` to 4 and `CSMFANOUT_DELAY` to 2400:

   ```
   export CSM_FANOUT=4
   export CSM_FANOUT_DELAY=2400
   ```

5. For Red Hat EL, update `/etc/init.d/nfs` and change `RPCNFSDCOUNT` to a higher value than the default value of 8.

---
Installing Red Hat EL 4 on x336 and x346 nodes

If you are installing Red Hat EL 4 (AS, ES, or WS) on x336 or x346 nodes, make sure the BIOS version is one of the following. Otherwise, after all the images have been installed you cannot reboot the nodes from hard disk.

- For x336, the BIOS version is 30A, or later.
- For x346, the BIOS version is 37C, or later.

HMC power status errors


If the `rpower` command does not return a valid power status from the HMC, restart IBM.HWCTRLRM, as follows:

1. Issue the following command:
   
   `lssrc -a`

2. If the IBM.HWCTRLRM daemon is not active, go to step 5.
3. If the daemon is active, issue the following command:
   
   `stopsrc -s IBM.HWCTRLRM`

4. Check to determine that the daemon is stopped:
   
   `lssrc -a`

   If the daemon is not stopped, repeat step 3.

5. If the daemon is stopped, issue the following command:
   
   `ps -ef|grep HWCTRL`

6. To restart the daemon, issue the following command:
   
   `startsrc -s IBM.HWCTRLRM`

Installing Linux on BladeCenter JS nodes

When you are using the `installnode` command to install Red Hat EL or SLES on BladeCenter JS nodes, the installation may not complete on some of the nodes because of a hang during RPM installation. This is especially prevalent when you are installing more than eight nodes at a time. To prevent this, ensure you are running a correct firmware level:
Updating System p firmware


Installing Linux after uninstalling AIX

When installing Red Hat EL on a System p server that was previously installed with AIX, timeouts and prompts related to disk partitioning can occur. For example, you could see the following prompt:

```
+---------------+ Warning +---------------+
|               | The partition table on device sdb was |               |
| unreadable. To create new partitions | it must be initialized, causing the |               |
| loss of ALL DATA on this drive.      |               |
| +---------------+ This operation will override any | previous installation choices about | which drives to ignore. |
| Would you like to initialize this | drive, erasing ALL DATA? |               |
| drive, erasing ALL DATA? |               |
| +-----+             +----+        |
| | Yes |             | No |        |
| +-----+             +----+        |
+-----------------------------------------+
```

To correct the problem, modify the Red Hat EL Kickstart configuration template file. The default file for Red Hat EL AS 4 is /opt/csm/install/kscfg.tmpl.RedHatEL-AS4-ppc64.

To erase all data on the disk, change the following line in the Kickstart file:

```
clearpart --all --initlabel --drives=#CSMVAR:INSTALL_DRIVER#
```

to:

```
clearpart --all --initlabel
```
This change causes all node hard disks - local, and possibly external - to be reformatted, not just the one that is being installed. To prevent Kickstart from reformatting all node hard disks, you must press Enter in a remote console window when the prompts occur.

On Red Hat EL 5, you can specify to ignore certain node disks by adding the following line to your Kickstart file, before the subsequent clearpart line:

```
ignoredisk --drives=drive1,drive2,...
```

where driveN can be sda, sdb, or hda, for example.

---

**Installing SLES 9 x86_64 GA on x336, x346, and BladeCenter HS20-8843**

If you experience problems installing SLES 9 x86_64 GA on System x 336, 346, or BladeCenter HS20-8843 servers, use the following procedure to allow the operating system installation to complete successfully:

**Note:**
As an alternative to this procedure, you can install SLES 9 SP1, or later.

- After setting up the SLES 9 x86_64 GA installation source by running the csmsetupinstall or copycds command, loop mount the following file as follows:

  ```
  mount -o loop -r /csminstall/Linux/SLES/9/x86_64/GA/boot/root mount_point
  ```

- Copy the files into a temporary directory:

  ```
  mkdir /root/tempdir
  cp -a mount_point /* /root/tempdir
  ```

  The cp -a command returns the following messages:

  ```
e326n03:~ # cp -a /mnt/d1/* /root/tmpdir/
cp: will not create hard link `/root/tmpdir/etc/init.d/rc4.d' to directory `/root/tmpdir/root'
cp: will not create hard link `/root/tmpdir/etc/slp.reg.d' to directory `/root/tmpdir/root'
cp: will not create hard link `/root/tmpdir/usr/X11R6/include/X11' to directory `/root/tmpdir/root'
cp: will not create hard link `/root/tmpdir/usr/share/autoinstall/modules' to directory `/root/tmpdir/root'
cp: will not create hard link `/root/tmpdir/usr/share/doc/packages' to directory `/root/tmpdir/root'
```

- Unmount the installation root file system:

  ```
  umount mount_point
  ```

- Edit the Display.ycp file in the /root/tempdir/usr/share/YaST2/modules directory as follows:
Comment out lines 373 to 375 in this file:

```c
<       if ( ! ( Mode::cont && Restore() ) && ! Mode::config ) {
<       probe_settings();
<   }
<---
>       //if ( ! ( Mode::cont && Restore() ) && ! Mode::config ) {
>       //    probe_settings();
>   //}
```

- From a SLES 9 x86_64 system, compile the new version of `Display.ycp`, overwriting the previous `Display.ybc` file, as follows. You might have to install `yast2-core.rpm` before running the following command:

  ```bash
cd /root/tempdir/usr/share/YaST2/modules/
ycpc -c Display.ycp
```

- Create a new install root file system. You must install the `util-linux-2.12-72.20` RPM before running the following command:

  ```bash
cd /root
mkfs -t cramfs /root/tempdir/root.new
```

- Copy this new root file system into the SLES 9 x86_64 CSM install source directory as follows:

  ```bash
cp root.new /csminstall/Linux/SLES/9/x86_64/GA/boot/
```

- Back up the original installation root file system:

  ```bash
cd /csminstall/Linux/SLES/9/x86_64/GA/boot/
cp root root.bak
```

- Replace the root file with the `root.new` file that you just created:

  ```bash
cp /root/root.new ./root
cp root.new root
```

The installation of SLES 9 x86_64 GA on System x 336, 346, and BladeCenter HS20-8843 should now complete successfully. Use the `aic79xx.ko` driver for the SCSI hard disk controller in the x346.

---

**NFS warnings**

The `installnode` and `updatenode` commands can return NFS warnings. NFS `invalid argument` warnings can also be returned by the `exportfs` command:

172.60.3.11:/csminstall/csm: Invalid argument
172.60.3.17:/csminstall/csm: Invalid argument

You can ignore these warnings. The warnings can occur if you have exported the `/csminstall` directory in the `/etc/exports` file or through the `exportfs` command. To eliminate the warnings, unexport the `/csminstall` directory, and then stop and restart the NFS daemon. Stopping and starting the NFS daemon can flush the problems out of the NFS table in the kernel.
Chapter 30. Automatic setup of rsh and OpenSSH

CSM can automatically configure remote shell authentication during full node installation or during node updates. CSM can also set up OpenSSH authentication for root users between all cluster nodes. This is useful for software that requires a remote shell setup between all the nodes, but is not required for CSM. For details on automatic Kerberos setup, see the updatenode man page or the CSM for AIX and Linux: Command and Technical Reference.

Configuring rsh authentication

If you have the following values stored in csmconfig, CSM automatically sets up rsh.

RemoteShell=/usr/bin/rsh  
SetupRemoteShell=1

Configuring rsh authentication during node OS installation

All configuration of rsh setup is done on the node. The steps that CSM uses to automatically configure rsh authentication are as follows:

1. CSM enables rsh on Linux nodes. On AIX nodes, rsh is enabled by default.
2. CSM adds the management server hostname followed by root to the root $HOME/.rhosts file. The file is created if it does not exist.

Configuring rsh authentication during node updates

The configuration of rsh is done on PreManaged nodes, or when updatenode is run with the -k or -K rsh flags. The updatenode command steps are as follows:

1. The updatenode command attempts to issue the dsh command to the node. If dsh is successful, updatenode does not attempt remote shell setup for the node.
2. If dsh fails, updatenode prompts for the root password of the node.
3. Using the root password, updatenode attempts to issue the rexec command to the node to do the following. If rexec is not enabled on the node, rsh setup fails:
   a. CSM enables rsh on Linux nodes.
   b. CSM adds the management server's hostname followed by root to the root user's $HOME/.rhosts file. The file is created if it does not exist.

Configuring OpenSSH authentication

If you have the following values stored in csmconfig, CSM automatically sets up OpenSSH:

CSM for AIX and Linux: Planning and Installation Guide
Configuring OpenSSH authentication during node OS installation

CSM automatically configures OpenSSH authentication when installing the operating system; the following steps are run on the management server:

1. If they are not already created, CSM generates all three types of OpenSSH public/private keys in the root user's $HOME/.ssh directory with no passphrase: rsa1, rsa, and dsa.
2. CSM copies the public half of these keys to a location in /csminstall so that they can be added to authorized_keys on the nodes.
3. When the node's Mode attribute changes to Managed, indicating that CSM has been installed on the node, the GatherSSHHostKeys response runs to append the node's OpenSSH sshd host key to $HOME/.ssh/known_hosts on the management server.

On the node, CSM appends the management server's public keys from /csminstall to the root user's $HOME/.ssh/authorized_keys and $HOME/.ssh/authorized_keys2 files.

Configuring OpenSSH authentication during node updates

OpenSSH configuration is done to PreManaged nodes, or when the updatenode command is run with the -k or -K ssh flags. The updatenode steps are as follows:

1. The updatenode command attempts to issue the dsh command to the node. If dsh is successful, updatenode does not attempt remote shell setup for the node.
2. If dsh fails, updatenode does the following:
   a. If they are not already created, updatenode generates all three types of OpenSSH public/private keys in root's $HOME/.ssh directory with no passphrase: rsa1, rsa, and dsa.
   b. updatenode copies the public half of these keys to temporary files. The updatenode command prompts for the root password of the node.
   c. With the root's password, updatenode copies the temporary files to the node using the secure copy command scp and appends the management server's public keys from the temporary files to root's $HOME/.ssh/authorized_keys and $HOME/.ssh/authorized_keys2 files.

Setting up OpenSSH between all nodes

CSM can set up unprompted OpenSSH authentication for root users between all cluster nodes. This allows root at node1 to ssh to root at node2 and is useful for setting up many cluster applications, although is not required for any CSM functionality. The following procedure is only supported for versions of OpenSSH without Kerberos.

Attention: The following procedure sets up the same root user public/private ssh key pairs and authorization files on all cluster nodes. The root user's entire .ssh directory is copied from the management server to the nodes, allowing a root user on any node to obtain root access to the management server and any other target node. To avoid this scenario, use a unique public/private key pair for each node and
exchange the keys between all nodes. Always ensure that you are using a ssh configuration that complies with your site security policy.

To have CSM set up OpenSSH between all nodes, complete the following steps before remotely installing the operating system, or before running the updatenode command:

1. If the root user's $HOME/.ssh directory - typically /root/.ssh on Linux, and /.ssh on AIX - does not exist on the management server, create it by entering:

   ```bash
   mkdir -m700 $HOME/.ssh
   ```

2. Symbolically link $HOME/.ssh to /cfmroot/$HOME/.ssh on the management server. For example, on Linux:

   ```bash
   mkdir /cfmroot/root
   ln -s /root/.ssh /cfmroot/root/.ssh
   ```

   On AIX:

   ```bash
   ln -s /.ssh /cfmroot/.ssh
   ```

3. Complete a remote installation of your nodes, or run the updatenode command on all nodes. This sets up OpenSSH authentication between all the nodes by pushing the root user's .ssh directory. During a full installation, this push is distributed and runs to groups of nodes as they finish installing, instead of pushing the files to each node serially.

   **Note:**

   Pushing ssh files and the known_hosts list to a large number of nodes each time a node is installed can decrease cluster performance. To minimize any performance impact, first install a number of new nodes. Then link the .ssh directory to /cfmroot on your management server, and run the cfmupdatenode -a command to transfer the files simultaneously to all nodes. After the file transfer completes, remove the link between .ssh and /cfmroot.
Chapter 31. CSM port usage

The tables below provide port information for the services required for CSM to manage a cluster through a firewall. The assumed configuration is the management server, HA MS, HMCs, install servers, and one or more managed nodes behind a firewall, and at least one managed node in front of the firewall. The Trusted side is behind the firewall; the Non-trusted side is in front of the firewall.

A service (or protocol) applies to both AIX and Linux, unless stated otherwise. Service names are typical strings that can appear in an /etc/services file, or in firewall or IP filtering logs. Local customization of the /etc/services files, daemon configuration options such as overriding the default port number, and differences in software source implementations, can yield other service information results.

If your cluster management server is also the install server, the ports used by the management server are as follows:

Table 96. CSM port usage - by management server/install server

<table>
<thead>
<tr>
<th>Service name</th>
<th>Port number</th>
<th>Protocol</th>
<th>Source port range</th>
<th>Required or optional</th>
</tr>
</thead>
<tbody>
<tr>
<td>echo-udp</td>
<td>7</td>
<td>udp</td>
<td>not applicable</td>
<td>required</td>
</tr>
<tr>
<td>ssh-tcp</td>
<td>22</td>
<td>tcp</td>
<td>not applicable</td>
<td>optional</td>
</tr>
<tr>
<td>ssh-upd</td>
<td>22</td>
<td>udp</td>
<td>not applicable</td>
<td>optional</td>
</tr>
<tr>
<td>domain-tcp</td>
<td>53</td>
<td>tcp</td>
<td>not applicable</td>
<td>optional</td>
</tr>
<tr>
<td>domain-udp</td>
<td>53</td>
<td>udp</td>
<td>not applicable</td>
<td>optional</td>
</tr>
<tr>
<td>bootps</td>
<td>67</td>
<td>udp</td>
<td>not applicable</td>
<td>optional</td>
</tr>
<tr>
<td>dhcp</td>
<td>67</td>
<td>tcp</td>
<td>not applicable</td>
<td>optional</td>
</tr>
<tr>
<td>dhcpc</td>
<td>68</td>
<td>tcp</td>
<td>not applicable</td>
<td>optional</td>
</tr>
<tr>
<td>bootpc</td>
<td>68</td>
<td>udp</td>
<td>not applicable</td>
<td>optional</td>
</tr>
<tr>
<td>tftp-tcp</td>
<td>69</td>
<td>tcp</td>
<td>not applicable</td>
<td>optional</td>
</tr>
<tr>
<td>tftp-udp</td>
<td>69</td>
<td>udp</td>
<td>not applicable</td>
<td>optional</td>
</tr>
<tr>
<td>www-tcp</td>
<td>80</td>
<td>tcp</td>
<td>not applicable</td>
<td>optional</td>
</tr>
<tr>
<td>www-udp</td>
<td>80</td>
<td>udp</td>
<td>not applicable</td>
<td>optional</td>
</tr>
<tr>
<td>kerberos</td>
<td>88</td>
<td>tcp</td>
<td>not applicable</td>
<td>optional</td>
</tr>
<tr>
<td>kerberos</td>
<td>88</td>
<td>udp</td>
<td>not applicable</td>
<td>optional</td>
</tr>
<tr>
<td>sunrpc-udp</td>
<td>111</td>
<td>udp</td>
<td>not applicable</td>
<td>optional</td>
</tr>
<tr>
<td>shell</td>
<td>514</td>
<td>tcp</td>
<td>1-1023</td>
<td>optional</td>
</tr>
<tr>
<td>kshell</td>
<td>544</td>
<td>tcp</td>
<td>1-1023</td>
<td>optional</td>
</tr>
<tr>
<td>rmc-tcp</td>
<td>657</td>
<td>tcp</td>
<td>not applicable</td>
<td>required</td>
</tr>
<tr>
<td>rmc-udp</td>
<td>657</td>
<td>udp</td>
<td>not applicable</td>
<td>required</td>
</tr>
<tr>
<td>conserver</td>
<td>782</td>
<td>tcp</td>
<td>not applicable</td>
<td>optional</td>
</tr>
<tr>
<td>nim</td>
<td>1058</td>
<td>tcp</td>
<td>1-1023</td>
<td>optional</td>
</tr>
<tr>
<td>nfsd-tcp</td>
<td>2049</td>
<td>tcp</td>
<td>not applicable</td>
<td>optional</td>
</tr>
</tbody>
</table>
If your cluster uses one or more separate install servers, and there is a firewall between the management server and the install servers, the ports used by the management server are as follows:

Table 97. CSM port usage - by management server using separate install servers

<table>
<thead>
<tr>
<th>Service name</th>
<th>Port number</th>
<th>Protocol</th>
<th>Source port range</th>
<th>Required or optional</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>ssh-tcp</td>
<td>22</td>
<td>tcp</td>
<td>not applicable</td>
<td>optional</td>
<td>ssh is used for dsh remote commands.</td>
</tr>
<tr>
<td>ssh-upd</td>
<td>22</td>
<td>upd</td>
<td>not applicable</td>
<td>optional</td>
<td>none</td>
</tr>
<tr>
<td>sunrpc-udp</td>
<td>111</td>
<td>upd</td>
<td>not applicable</td>
<td>optional</td>
<td>Used by portmap/NFS.</td>
</tr>
<tr>
<td>nfsd-tcp</td>
<td>2049</td>
<td>tcp</td>
<td>not applicable</td>
<td>optional</td>
<td>none</td>
</tr>
<tr>
<td>nfsd-udp</td>
<td>2049</td>
<td>udp</td>
<td>not applicable</td>
<td>optional</td>
<td>none</td>
</tr>
<tr>
<td>csm-nodemsgs</td>
<td>3101</td>
<td>none</td>
<td>not applicable</td>
<td>optional</td>
<td>Default. If in use, value is incremented until available port is found.</td>
</tr>
<tr>
<td>rpc-mount</td>
<td>100005</td>
<td>none</td>
<td>See note 2.</td>
<td>optional</td>
<td>none</td>
</tr>
<tr>
<td>mount-tcp</td>
<td>See note 1.</td>
<td>tcp</td>
<td>not applicable</td>
<td>optional</td>
<td>none</td>
</tr>
<tr>
<td>mount-udp</td>
<td>See note 1.</td>
<td>udp</td>
<td>not applicable</td>
<td>optional</td>
<td>none</td>
</tr>
</tbody>
</table>

If your cluster uses one or more separate install servers, and there is a firewall between the management server and the install servers, the ports used by the install servers are as follows:

Table 98. CSM port usage - by separate install servers

<table>
<thead>
<tr>
<th>Service name</th>
<th>Port number</th>
<th>Protocol</th>
<th>Source port range</th>
<th>Required or optional</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>bootps</td>
<td>67</td>
<td>udp</td>
<td>not applicable</td>
<td>optional</td>
<td>none</td>
</tr>
<tr>
<td>dhcp</td>
<td>67</td>
<td>tcp</td>
<td>not applicable</td>
<td>optional</td>
<td>none</td>
</tr>
<tr>
<td>bootpc</td>
<td>68</td>
<td>udp</td>
<td>not applicable</td>
<td>optional</td>
<td>none</td>
</tr>
<tr>
<td>tftp-tcp</td>
<td>69</td>
<td>tcp</td>
<td>not applicable</td>
<td>optional</td>
<td>none</td>
</tr>
<tr>
<td>tftp-udp</td>
<td>69</td>
<td>udp</td>
<td>not applicable</td>
<td>optional</td>
<td>none</td>
</tr>
<tr>
<td>www-tcp</td>
<td>80</td>
<td>tcp</td>
<td>not applicable</td>
<td>optional</td>
<td>Required for HTTP</td>
</tr>
<tr>
<td>Service</td>
<td>Port</td>
<td>Protocol</td>
<td>Applicable</td>
<td>Requirements</td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>------</td>
<td>----------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>www-udp</td>
<td>80</td>
<td>udp</td>
<td>not applicable</td>
<td>optional none</td>
<td></td>
</tr>
<tr>
<td>sunrpc-udp</td>
<td>111</td>
<td>udp</td>
<td>not applicable</td>
<td>optional Required for portmap/NFS.</td>
<td></td>
</tr>
<tr>
<td>nfsd-tcp</td>
<td>2049</td>
<td>tcp</td>
<td>not applicable</td>
<td>optional none</td>
<td></td>
</tr>
<tr>
<td>nfsd-udp</td>
<td>2049</td>
<td>udp</td>
<td>not applicable</td>
<td>optional none</td>
<td></td>
</tr>
<tr>
<td>csm-nodemsgs</td>
<td>3101</td>
<td>none</td>
<td>not applicable</td>
<td>optional Default. If in use, value is incremented until available port is found.</td>
<td></td>
</tr>
<tr>
<td>pxe</td>
<td>4011</td>
<td>none</td>
<td>not applicable</td>
<td>optional For xSeries nodes.</td>
<td></td>
</tr>
<tr>
<td>rpc-mount</td>
<td>100005</td>
<td>none</td>
<td>See note 2.</td>
<td>optional none</td>
<td></td>
</tr>
<tr>
<td>mount-tcp</td>
<td>See note 1.</td>
<td>tcp</td>
<td>not applicable</td>
<td>optional none</td>
<td></td>
</tr>
<tr>
<td>mount-udp</td>
<td>See note 1.</td>
<td>udp</td>
<td>not applicable</td>
<td>optional none</td>
<td></td>
</tr>
<tr>
<td>rmc-tcp</td>
<td></td>
<td></td>
<td></td>
<td>Resource Monitoring and Control (RMC) used by CSM for hardware monitoring, key exchange. This is for tcp protocol.</td>
<td></td>
</tr>
<tr>
<td>rmc-udp</td>
<td></td>
<td></td>
<td></td>
<td>Resource Monitoring and Control (RMC) used by CSM for hardware monitoring, key exchange. This is for udp protocol.</td>
<td></td>
</tr>
<tr>
<td>echo-udp</td>
<td></td>
<td></td>
<td></td>
<td>Required by RSCT Topology Services.</td>
<td></td>
</tr>
<tr>
<td>domain-tcp</td>
<td></td>
<td></td>
<td></td>
<td>Used when Domain Name Services (DNS) traffic from the Non-trusted nodes and the firewall node to a DNS server is explicitly handled by the firewall. Some firewall applications can be configured to explicitly handle all DNS traffic. This for udp DNS traffic.</td>
<td></td>
</tr>
<tr>
<td>domain-udp</td>
<td></td>
<td></td>
<td></td>
<td>Used when Domain Name Services (DNS) traffic from the Non-trusted nodes and the firewall node to a DNS server is explicitly handled by the firewall. Some firewall applications can be configured to explicitly handle all DNS traffic. This for udp DNS traffic.</td>
<td></td>
</tr>
<tr>
<td>kerberos</td>
<td></td>
<td></td>
<td></td>
<td>Kerberos Version 5 KDC. Needed if running Kerberos Version 5 remote command authentication in CSM. This service defines the protocol for tcp.</td>
<td></td>
</tr>
<tr>
<td>kerberos</td>
<td></td>
<td></td>
<td></td>
<td>Kerberos Version 5 KDC. Needed if running Kerberos Version 5 remote command authentication in CSM. This service defines the protocol for udp.</td>
<td></td>
</tr>
<tr>
<td>sunrpc-udp</td>
<td></td>
<td></td>
<td></td>
<td>The portmapper service. Required when installing a Non-trusted node through the firewall. Specifically required mount request that takes place during node install.</td>
<td></td>
</tr>
<tr>
<td>shell</td>
<td></td>
<td></td>
<td></td>
<td>Used when rsh/rcp is enabled for Standard (std) authentication protocol. Required for CSM dsh operations when using rsh for remote commands.</td>
<td></td>
</tr>
<tr>
<td>kshell</td>
<td></td>
<td></td>
<td></td>
<td>Used when AIX rsh or rcp is enabled for Kerberos Version 5 authentication protocol. It is required for CSM dsh operations when using kerberized rsh for remote commands.</td>
<td></td>
</tr>
<tr>
<td>nim</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Network Installation Management client traffic generated by an Non-trusted node during node boot/shutdown. Required if using NIM. AIX only.

**bootps**
bootp server port needed when installing an Non-trusted AIX or System p node through the firewall. This service is issued by the client to the management server, for an install request. It is not required to install the Non-trusted nodes through the firewall or to apply maintenance, and therefore, is optional.

**bootpc**
bootp client port needed when installing an Non-trusted AIX or System p node through the firewall. This service is issued by the management server back to the client, in response to an install request from the client. It is not required to install the Non-trusted nodes through the firewall or to apply maintenance, and therefore, is optional.

**nfsd-tcp**
Required to use the AIX mount command. This service defines the protocol for tcp. Required when installing an Non-trusted node through the firewall. It is required when an `installp` is issued on an Non-trusted node and the resource exists on the Trusted side.

**nfsd-udp**
Required to run the AIX `mount` command. This service defines the protocol for udp. Required when installing an Non-trusted node through the firewall. Required when an `installp` is issued on an Non-trusted node and the resource exists on the Trusted side.

**mount-tcp**
Required to run the AIX `mount` command. This service defines the protocol for tcp. Required when installing an Non-trusted node through the firewall. Required when `installp` is issued on an Non-trusted node and the resource exists on the Trusted side. Required to run the CSM `updatenode` command. See note 1.

**mount-udp**
Required to use the AIX `mount` command. This service defines the protocol for udp. Required when `installp` is issued on an Non-trusted node and the resource exists on the Trusted side. Required to run CSM `updatenode` command. See note 1.

**rpc-mount**
Remote Procedure Call (RPM) used in conjunction with NFS mount request. See note 2.

**ssh-tcp**
Required to use ssh. This service defines the protocol for tcp. This is required when installing or running `updatenode` through the firewall and CSM is using ssh for remote commands.

**ssh-upd**
Required to use ssh. This service defines the protocol for udp. This is required when installing or running `updatenode` through the firewall and CSM is using ssh for remote commands.

**www-tcp**
Required to use Web http. Required to download the required non-IBM software and the latest CSM support packages for the CSM support Web site. This service defines the protocol for tcp.

**www-udp**
Needed to use Web http. Required to download the required non-IBM software and the latest CSM support packages for the CSM support Web site. This service defines the protocol for udp.

**tftp-tcp**
Required to install Linux nodes. This service defines the protocol for tcp.

**tftp-udp**
Required to install Linux nodes. This service defines the protocol for udp.

**dhcpc**
Required to install System p nodes through the firewall. This is the port for the dhcp client. This service defines the protocol for tcp.

**dhepc**
Required to install System p nodes through the firewall. This is the port for the dhcp client. This service defines the protocol for tcp.
**conserver**

Required when one of the following is true:

- There is a firewall on the management server and the CSM PTF that puts conserver in UDP mode is not being used.
- There is a requirement outside of CSM to connect to conserver from remote locations, and those remote locations pass through a firewall.

This service defines the protocol for tcp.

**pxe**

Required to install System x nodes through the firewall. This is the port for the PXE boot server. This service defines the protocol for tcp.

**csm-nodemsgs**

Port used by CSM to send messages from Linux nodes to the management server during installation. If this port is blocked, the installation fails to reboot after the operating system is installed.

**Note:**

1. On AIX, the `mountd` port range is usually determined at the time of the mount request. Part of the communication flow within a mount command is to query the remote `mountd` server and find out what ports it is using. The `mountd` ports are selected dynamically each time the `mountd` server is initialized. Therefore, the port numbers will vary from one boot to another, or when `mountd` is stopped and restarted.

This causes a problem when used through a firewall, as no rule can be defined to handle traffic with a variable primary port. To create a service for `mountd` (server) traffic that has a fixed port, and one that can be trapped by a rule, you will need to update the `/etc/services` file on the host that is the target of the mount with new `mountd` entries for TCP and UDP, where the port numbers are known to be unused (free). The `mountd` TCP and UDP ports must be different. Any free port number is valid. The `mountd` must be stopped and started to pick up the new port values.

For example, issuing a mount request on Non-trusted node X, whose target is the management server, that is,

```
mount ms2112:/images /images
```

would require that the `/etc/services` file on `ms2112` be updated with something similar to the following:

```
mountd 33333/tcp
mountd 33334/udp
```

For `mountd` to detect its new port values you must stop and start `rpc.mountd`. The stopping and starting of `mountd` takes place on the same host where the `/etc/services` file `mountd` updates were made. In the above example, `ms2112`'s `mountd` is stopped and started. You can verify that `mountd` is using the new port definitions by issuing the `rpcinfo` command.

This procedure shows how to change ports used by `mountd`:

```
lssrc -s rpc.mountd
```
a. Produces output similar to:

<table>
<thead>
<tr>
<th>Subsystem Group PID Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>rpc.mountd nfs 12404 active</td>
</tr>
<tr>
<td>rpcinfo -p ms2112</td>
</tr>
</tbody>
</table>

b. Produces output similar to:

```
100005 1 udp 37395 mountd
100005 2 udp 37395 mountd
100005 3 udp 37395 mountd
100005 1 tcp 34095 mountd
100005 2 tcp 34095 mountd
100005 3 tcp 34095 mountd
```

```
stopsrc -s rpc.mount
```

c. Produces output similar to:

```
0513-044 The rpc.mountd Subsystem was requested to stop.
```

d. Update `/etc/services` with new `mountd` entries.

**Note:**

Make a backup copy of `/etc/services` before making changes.

```
grep mountd /etc/services
```

e. Produces output similar to:

```
mountd 33333/tcp
mountd 33334/udp
```

```
startsrc -s rpc.mountd
```

f. Produces output similar to:

```
0513-059 The rpc.mountd Subsystem has been started. Subsystem PID is 19536.
```

```
rpcinfo -p ms2112 | grep mount
```

g. Produces output similar to:

```
100005 1 udp 33334 mountd
100005 2 udp 33334 mountd
100005 3 udp 33334 mountd
100005 1 tcp 33333 mountd
100005 2 tcp 33333 mountd
100005 3 tcp 33333 mountd
```

2. The rpc-mount service differs from the other service definitions in the following way. There is no associated protocol, because by definition it is UDP-based. There is no source port range.
Chapter 32. Setting up an HTTP server manually

You can set up an Apache HTTP server manually to work for CSM installations. This manual setup is also supported for additional HTTP server models. If the NetworkInstallProtocol csmconfig attribute is set to HTTP, and the SetupNetworkInstallProtocol csmconfig attribute is set to 0 (no), you must install and configure an HTTP server on each install server.

Install Apache RPMs

Red Hat EL and SLES distribution CDs contain Apache RPM packages. The RPMs vary depending upon the Linux distribution and version of Apache.

To install Apache on Red Hat EL, run an `rpm` command similar to:

```
rpm -i apr-0.9.4-24.3.ppc.rpm apr-util-0.9.4-17.ppc.rpm 
httpd-2.0.52-12.ent.ppc.rpm httpd-suexec-2.0.52-12.ent.ppc.rpm
```

To install Apache on SLES, run an `rpm` command similar to:

```
rpm -i libapr0-2.0.49-27.8.i586.rpm apache2-2.0.49-27.8.i586.rpm 
apache2-worker-2.0.49-27.8.i586.rpm
```

**Note:**
For Apache on SLES, all three RPMs must be installed simultaneously, because they are dependent on each other.

Configure Apache to recognize the /csminstall directory

You must add a directory entry for the Apache configuration so the /csminstall directory is recognized. Either edit the `httpd.conf` file directly, or create a separate configuration file in `/etc/httpd/conf.d` (Red Hat EL) or `/etc/apache2/conf.d` (SLES).

CSM provides a configuration template that can be used for this purpose. Copy `/opt/csm/install/csminstall_http.conf.tmpl` to `/etc/httpd/conf.d/csminstall.conf` (for Red Hat EL) or to `/etc/apache2/conf.d/csminstall.conf` (for SLES), and edit it to refer to `/csminstall` if your install server is the management server, `/csmserver` if your install server is not the management server, or the user-defined directory specified in the `InstallServer` attribute.

Set SELinux security context for /csminstall (Red Hat EL only)

On Red Hat EL, SELinux (Secure Enterprise Linux) is enabled by default. If SELinux is enabled on your install server, you must set the correct context for the /csminstall directory so the HTTP server can serve files from that directory. To check if SELinux is active in the current kernel, run:
ls --context

If SELinux is active, run the following command to recursively set the security context of all files and directories under the /csminstall directory:

/usr/bin/chcon -R -t httpd_sys_content_t /csminstall

Note:
If you are configuring the HTTP server for an install server that is not the management server, you should set the SELinux context for /csmserver, or the user-defined directory specified in the InstallServer attribute, instead of for the /csminstall directory.

Configure Apache for better scaling (optional)

The default settings for Apache 2 on Red Hat EL and SLES do not allow enough simultaneous HTTP client connections to install more than 50 nodes at a time. To enable greater scaling, increase the MaxClients and ServerLimit directives from 150 to 1000. On Red Hat EL, change or add these directives in /etc/httpd/conf/httpd.conf. On SLES (with Apache2), change or add these directives in /etc/apache2/server-tuning.conf.

Start Apache

Once Apache has been configured, you can start it by running the following command:

For Red Hat EL:
apachectl start
For SLES:
rcapache2 start

See http://httpd.apache.org for more information on Apache.
Chapter 33. Using HPSNM set programs

Set programs are required by csm.hpsnm switch management software for High Performance Switch Network Management (HPSNM). The set programs give non-root users, including GUI users, the ability to run commands that are owned by root. The commands specific to CSM are /opt/csm/hpsnm/bin/chswelamast, /opt/csm/hpsnm/bin/chswlogtop, and /opt/csm/hpsnm/bin/chswnm. See the IBM CSM for AIX and Linux: Command and Technical Reference for details on these commands, including set uid implementation.

The three set programs are intended for basic setup and operation of the Switch Network Manager software. Unless absolutely necessary, do not remove their set uid capability; doing so can have a drastic impact on clusters that use the IBM High Performance Switch. If the set uid bit is removed, root users are not affected; non-root users will not be able to run HPSNM GUI commands.
Appendix. Accessibility features for CSM

Accessibility features help users who have a disability, such as restricted mobility or limited vision, to use information technology products successfully.

Accessibility features

The following list includes the major accessibility features in IBM Cluster Systems Management (CSM):

- Keyboard-only operation
- Interfaces that are commonly used by screen readers
- Keys that are discernible by touch but do not activate just by touching them
- Industry-standard devices for ports and connectors
- The attachment of alternative input and output devices

The IBM Cluster Information Center, and its related publications, are accessibility-enabled. The accessibility feature of the information center are described at:


Keyboard navigation

This product uses standard Microsoft(R) Windows(R) navigation keys.

IBM and accessibility

See the IBM Human Ability and Accessibility Center for more information about the commitment that IBM has to accessibility at:

http://www.ibm.com/able
Notices

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

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 grant 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 character set (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 106-0032, 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.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

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*
*Intellectual Property Law*
*2455 South Road, P386*
*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.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

---

**Trademarks**

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at http://www.ibm.com/legal/copytrade.shtml.

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

CSM includes Linux software that is publicly available, including:

Conserver 8.1 (CSM for Linux on System x and System p)
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.

This book discusses the use of these products only as they apply specifically to the CSM product.

The following non-IBM software is required for remote hardware control of IBM System p servers attached to a POWER4, System p5 or POWER 6 IBM Hardware Management Console (HMC):

- openCIMOM Version 0.8, or later.

You can download openCIMOM software from:
http://www-03.ibm.com/servers/aix/products/aixos/linux/download.html, or
ftp://linuxpatch.ncsa.uiuc.edu/csm/noarch/.

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

- AutoUpdate V5.4.1-2, or later levels that maintain full backward compatibility.

You can download AutoUpdate software from: http://freshmeat.net/projects/autoupdate, or
ftp://linuxpatch.ncsa.uiuc.edu/csm/noarch/.

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: conserver 8.1.

CSM includes Linux 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.

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
AIX operating system
IBM's implementation of the UNIX operating system. AIX is particularly suited to support technical computing applications, including high function graphics and floating point computations.

ASM
See ISMP.

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

authentication
In computer security, a process that ensures that the identities of both the sender and the receiver of a network transaction are true.

authorization
The process of granting a user, system, or process either complete or restricted access to an object, resource, or function.

Baseboard Management Controller
Firmware on a network interface card (NIC) that handles all network traffic. If the Baseboard Management Controller detects a hardware control command, it accepts and processes the command; otherwise, it forwards the command to the node.

Basic Input/Output System (BIOS)
The code that controls basic hardware operations, such as interactions with diskette drives, hard disk drives, and the keyboard.

Basic Operating System (BOS)
The collection of programs that controls the resources and the operations of the computer system.

BIOS
See Basic Input/Output System.

blade server
A high-throughput, two-way, Intel Xeon-based server on a card that supports symmetric multiprocessors (SMPs).

Blue Gene core
The IBM System Blue Gene I/O nodes, compute nodes, and interconnects.

Blue Gene Solution
IBM's supercomputer product consisting of Blue Gene systems and the Blue Gene core.

Blue Gene system
A Blue Gene service node, front end node, or file server.

BOS
See Basic Operating System.

CEC
See central processor complex.

central electronic complex (CEC)
See central processor complex.

central processor complex (CPC)
A physical collection of hardware that consists of main storage, one or more central processors, timers, and channels.

cluster
A group of application servers that collaborates for the purposes of workload balancing and failover.

cluster VLAN
The virtual LAN that connects nodes to each other and to the management server through an Ethernet connection. Installation and administration tasks are done on the cluster VLAN.

do
coeexistence

The ability of two or more entities to function in the same system or network.

compute node

A Blue Gene core node on which user applications run.

Configuration File Manager (CFM)

A file repository that synchronizes and maintains file consistency across nodes in a cluster.

console server

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

Converged Service Processor (CSP)

A common card in both iSeries and RS/6000 systems. The primary function of a converged service processor is to start the system and diagnose hardware failures.

CSM database

A repository of cluster, node, and node group information that is created and used by Cluster Systems Management (CSM).

CSM graphical user interfaces (GUIs)

The following GUIs that are available for running Cluster Systems Management (CSM) functions: IBM Web-based System Manager, System Management Interface Tool (SMIT), and Distributed Command Execution Manager (DCEM).

CSM-only installation

The process of installing only Cluster Systems Management (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 graphical user interface (GUI) plug-ins, which provide an interface for monitoring and managing one or more Cluster Systems Management (CSM) clusters.

CSP

See Converged Service Processor.

DCEM

See Distributed Command Execution Manager.

device driver

A program that provides an interface between a specific device and the application program that uses the device.

diskless node

A Linux node with no disk or a Linux node that does not use its disk to store the operating system or packages.

Distributed Command Execution Manager (DCEM)

A graphical user interface (GUI) that can run commands on multiple cluster nodes simultaneously.

distributed shell (dsh)

A program that can issue commands to all systems in a network, in parallel.

distribution

A software package that is ready to install. A distribution often refers to a Linux package that contains the Linux operating system, an installation program, utilities, and documentation.

domain

1) A set of systems that allocate shared network resources within a single logical system. 2) A logical grouping of resources in a network for the purpose of common management and administration. 3) In TCP/IP, a named set of hosts. Each domain has authority for the machines within that domain, but not for machines in other domains.

dsh

See distributed shell.

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.

**Ethernet**
A packet-based networking technology for local area networks (LANs) that supports multiple access and handles contention by using Carrier Sense Multiple Access with Collision Detection (CSMA/CD) as the access method. Ethernet is standardized in the IEEE 802.3 specification.

**event**
An occurrence of significance to a task or system. Events can include completion or failure of an operation, a user action, or the change in state of a process.

**expansion I/O unit**
Additional hardware units used to provide additional disk and I/O capacity. Expansion I/O units are located in SP frames, attached to specific SP Nodes, and controlled by a frame supervisor. Expansion I/O units are not CSM nodes.

**fanout**
The number of systems or processors that are to receive software updates or communications simultaneously.

**file server node**
An IBM System Blue Gene node used to serve files to other Blue Gene systems and to I/O nodes.

**file set**
An individually installable option or update. Options provide specific function and updates correct an error in, or enhance, a previously installed option.

**file system**
The collection of files and file management structures on a physical or logical mass storage device, such as a diskette or minidisk.

**fix**
A software maintenance package, such as an interim fix, test fix, or program temporary fix, that solves a customer problem.

**front end node**
An IBM System Blue Gene node on which users compile applications and submit them to be run.

**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.

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

**Hardware Management Console (HMC)**
A system that controls managed systems, including the management of logical partitions and use of Capacity Upgrade on Demand. Using service applications, the HMC communicates with managed systems to detect, consolidate, and send information to IBM for analysis.

**hierarchical CSM**
A tiered Cluster Systems Management (CSM) environment in which a top-level executive management server (EMS) manages mid-level first-line management servers (FMS).

**HMC**
See *Hardware Management Console*.

**hostname file**
See *host name mapping file*.

**host name**
In Internet communication, the name given to a computer. Sometimes, hostname is used to mean the fully qualified domain name; other times, it is used to mean the most specific subname of a fully qualified domain name. For example, if mycomputer.city.company.com is the fully qualified domain name, either of the following host names can be used: mycomputer.city.company.com or mycomputer.

**host name mapping file**

---

CSM for AIX and Linux: Planning and Installation Guide 434
A file containing a list of host names and associated hardware control information.

**HPS network**
The network that interconnects the High Performance Switch (HPS) adapters.

**integrated system management processor (ISMP)**
A service processor built into some System x servers. ISMP is the successor to the Advanced System Management (ASM) processor.

**Integrated Virtualization Manager (IVM)**
A browser-based management interface that is used to manage a System p server. The IVM can be used to create logical partitions, manage virtual storage, and view service information related to the server.

**I/O node**
A Blue Gene core node that is responsible, in part, for providing I/O services to compute nodes.

**IVM**
See Integrated Virtualization Manager.

**Kerberos**
A network authentication protocol that is based on symmetric key cryptography. Kerberos assigns a unique key, called a ticket, to each user who logs on to the network. The ticket is embedded in messages that are sent over the network. The receiver of a message uses the ticket to authenticate the sender.

**kernel**
The part of an operating system that contains programs for such tasks as input/output, management and control of hardware, and the scheduling of user tasks.

**Korn shell (ksh)**
An interactive command interpreter and a command programming language.

**ksh**
See Korn shell.

**license key file**
A file containing keys (passwords) required to run Cluster Systems Management.

**license use key**
A key (password) that is required to run Cluster Systems Management. 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 hardware.

**logical partition (LPAR)**
A subset of a single system that contains resources (processors, memory, and input/output devices). A logical partition operates as an independent system. If hardware requirements are met, multiple logical partitions can exist within a system.

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

**logical partition (LPAR)**
A subset of a single system that contains resources (processors, memory, and input/output devices). A logical partition operates as an independent system. If hardware requirements are met, multiple logical partitions can exist within a system.

**LPAR**
See logical partition.

**MAC address**
A hardware address that uniquely identifies each node of a network. On a local area network (LAN), the MAC address is the computer's unique hardware number; on an Ethernet LAN, it is the same as the computer's Ethernet address.

**managed device**
A non-node device for which CSM supports power control and remote console access.

**managed node**
In Internet communications, a workstation, server, or router that contains a network management agent. In the Internet Protocol (IP), the managed node usually contains a Simple Network Management Protocol (SNMP) agent.

**management control point**
See management server.

**management domain**
A set of nodes that are configured for management by Cluster Systems Management. Such a domain has a management server that is used to administer a number of managed nodes. Only management servers have knowledge of the domain. Managed nodes only know about the servers managing them.

**management module**
The BladeCenter component that handles system-management functions. It configures the chassis and switch modules, communicates with the blade servers and all I/O modules, multiplexes the keyboard/video/mouse (KVM), and monitors critical information about the chassis and blade servers.

**management server**
The server and logical partition (LPAR) that are configured to manage Cluster Systems Management nodes.

**management VLAN**
See service network.

**migration**
Installation of a new version or release of a program to replace an earlier version or release.

**minimally-managed node**
A Linux node with no Cluster Systems Management (CSM) or Reliable Scalable Cluster Technology (RSCT) code installed.

**mixed cluster**
A cluster with both AIX and Linux nodes managed by a single management server.

**Network File System (NFS)**
A protocol, developed by Sun Microsystems, Incorporated, that allows a computer to access files over a network as if they were on its local disks.

**NIM master**
An AIX system that can install one or more Network Installation Manager (NIM) clients. An AIX system must be defined as a NIM master before any NIM clients can be defined on that system. A NIM master manages the configuration database, which contains information for the NIM clients. In CSM, the NIM master is the management server.

**NIM object**
For AIX, a representation of information about the Network Installation Manager (NIM) environment. NIM stores this information as objects in the NIM database.

**NIM resources**
For AIX, the files and directories that the Network Installation Manager (NIM) uses to install a node.

**node**
One operating system image. See also managed node.

**nodedef file**
See node definition file.

**node definition (nodedef) file**
A file containing a stanza of information for defining each node in a cluster.

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

**null value**
A parameter position for which no value is specified.

**open source**
Pertaining to software whose source code is publicly available for use or modification. Open source software is usually developed as a public collaboration and made freely available, although its use and redistribution might be subject to licensing restrictions. Linux is a well known example of open source software.

**package**
An installable unit of a software product. Software product packages are separately installable units that can operate independently from other packages of that software product.

**PAM**
See *Pluggable Authentication Module*.

**partition**
A logical division of storage on a fixed disk.

**Pluggable Authentication Module (PAM)**
In UNIX and AIX, a programming interface that enables third-party security methods to be used. PAM enables multiple types of authentication, such as Kerberos and the Rivest-Shamir-Adleman (RSA) algorithm, to be used without changing login services.

**port number**
In Internet communications, the identifier for a logical connector between an application entity and the transport service.

**predefined dynamic node group**
A node group whose members all have a certain attribute set to a certain value.

**probe**
A monitor that tests a transaction and then detects and reports any errors that were generated during that test.

**public VLAN**
The virtual local area network (VLAN) that 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.

**reduced instruction set computer (RISC)**
A computer that uses a small, simplified set of frequently used instructions for rapid processing.

**remote console**
The display device that qualifies as a system console but is not directly attached to a system.

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

**Remote Shell (rsh)**
In the distributed shell (dsh) program, the shell in which the remote command will run. Also, the shell set up on each node during installation.

**Remote Supervisor Adapter (RSA)**
An IBM service processor built into some System x servers and available as an optional adapter for use with others. When used as a gateway service processor, the RSA can communicate with all service processors on the Advanced System Management (ASM) interconnect.

**resource**
A hardware, software, or data entity.

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

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

**RISC**
See *reduced instruction set computer*.

**RSA**
See *Remote Supervisor Adapter*.

**rsh**
See *Remote Supervisor Adapter*. 
See Remote Shell.

server
In a network, hardware or software that provides facilities to clients. Examples of a server are a file server, a printer server, or a mail server.

service network
The Ethernet network that connects the management server, the Hardware Management Console (HMC), the POWER5 Service Processors, and Bulk Power Assemblies (BPA).

service node
A Blue Gene system which is responsible for management and control of a Blue Gene solution.

service processor
The interface to the Hardware Management Console (HMC) that provides hardware control and logical partition (LPAR) support for System p5 servers.

service VLAN
See service network.

shell
A software interface between users and an operating system. Shells generally fall into one of two categories: a command line shell, which provides a command line interface to the operating system; and a graphical shell, which provides a graphical user interface (GUI).

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

Simple Network Management Protocol (SNMP)
A set of protocols for monitoring systems and devices in complex networks. Information about managed devices is defined and stored in a Management Information Base (MIB).

SNMP

stanza
A group of lines in a file that together have a common function or define a part of the system. Stanzas are usually separated by blank lines or colons, and each stanza has a name.

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

update
Software maintenance such as a manufacturing refresh, refresh pack, or fix pack that changes the modification level of a product.

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

virtual local area network (VLAN)
A logical association of switch ports based upon a set of rules or criteria, such as Medium Access Control (MAC) addresses, protocols, network address, or multicast address. This concept permits the LAN to be segmented again without requiring physical rearrangement.

Web-based System Manager
A graphical user interface (GUI) tool for managing AIX systems. Based on the OO (Object Oriented) model, Web-based System Manager enables users to perform administration tasks by manipulating icons representing objects in the system, as an alternative to learning and remembering complex AIX commands.