Fifth Edition (June 2002)

Before using the information in this book, read the general information in Notices for HACMP Troubleshooting Guide.

This edition applies to HACMP for AIX, version 4.5 and to all subsequent releases of this product until otherwise indicated in new editions.

© Copyright International Business Machines Corporation 1998, 2002. All rights reserved.

Note to U.S. Government Users Restricted Rights--Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
# Contents

## About This Guide

### Chapter 1: Diagnosing the Problem

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Troubleshooting an HACMP Cluster</td>
<td>11</td>
</tr>
<tr>
<td>Becoming Aware of the Problem</td>
<td>11</td>
</tr>
<tr>
<td>Application Services Are Not Available</td>
<td>12</td>
</tr>
<tr>
<td>Messages Displayed on System Console</td>
<td>12</td>
</tr>
<tr>
<td>Determining a Problem Source</td>
<td>12</td>
</tr>
<tr>
<td>Examining Messages and Log Files</td>
<td>13</td>
</tr>
<tr>
<td>Investigating System Components</td>
<td>14</td>
</tr>
<tr>
<td>Tracing System Activity</td>
<td>16</td>
</tr>
<tr>
<td>Using the cldiag Utility to Perform Diagnostic Tasks</td>
<td>17</td>
</tr>
<tr>
<td>Using the Cluster Snapshot Utility to Check Cluster Configuration</td>
<td>17</td>
</tr>
<tr>
<td>Using SMIT Cluster Recovery Aids</td>
<td>18</td>
</tr>
<tr>
<td>Correcting a Script Failure</td>
<td>18</td>
</tr>
<tr>
<td>Verifying Expected Behavior</td>
<td>19</td>
</tr>
</tbody>
</table>

### Chapter 2: Examining Cluster Log Files

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>HACMP Messages and Cluster Log Files</td>
<td>21</td>
</tr>
<tr>
<td>Types of Cluster Messages</td>
<td>21</td>
</tr>
<tr>
<td>Cluster Message Log Files</td>
<td>22</td>
</tr>
<tr>
<td>Understanding the cluster.log File</td>
<td>25</td>
</tr>
<tr>
<td>Format of Messages in the cluster.log File</td>
<td>25</td>
</tr>
<tr>
<td>Viewing the cluster.log File</td>
<td>25</td>
</tr>
<tr>
<td>Understanding the hacmp.out Log File</td>
<td>27</td>
</tr>
<tr>
<td>Format of Messages in the hacmp.out Log File</td>
<td>28</td>
</tr>
<tr>
<td>Viewing the hacmp.out Log File</td>
<td>30</td>
</tr>
<tr>
<td>Changing the Location of the hacmp.out Log File</td>
<td>32</td>
</tr>
<tr>
<td>Resource Group Processing Messages in the hacmp.out File</td>
<td>32</td>
</tr>
<tr>
<td>Understanding the System Error Log</td>
<td>33</td>
</tr>
<tr>
<td>Format of Messages in the System Error Log</td>
<td>33</td>
</tr>
<tr>
<td>Viewing Cluster Messages in the System Error Log</td>
<td>33</td>
</tr>
<tr>
<td>Understanding the Cluster History Log File</td>
<td>35</td>
</tr>
<tr>
<td>Format of Messages in the Cluster History Log File</td>
<td>35</td>
</tr>
<tr>
<td>Viewing the Cluster History Log File</td>
<td>36</td>
</tr>
<tr>
<td>Understanding the /tmp/cm.log File</td>
<td>36</td>
</tr>
<tr>
<td>Viewing the /tmp/cm.log File</td>
<td>36</td>
</tr>
</tbody>
</table>
Contents

Understanding the cspoc.log File ........................................... 37
Format of Messages in the cspoc.log File ................................. 37
Viewing the cspoc.log File .................................................. 38
Understanding the /tmp/emuhacmp.out File .............................. 39
Format of Messages in the /tmp/emuhacmp.out File ..................... 39
Viewing the /tmp/emuhacmp.out File ..................................... 40

Chapter 3: Investigating System Components 41

Overview ................................................................. 41
Checking Highly Available Applications ................................. 41
Checking the HACMP Layer ................................................. 42
  Checking HACMP Components .......................................... 42
  Checking for Cluster Configuration Problems ....................... 46
Checking a Cluster Snapshot File ....................................... 48
Checking the Logical Volume Manager ................................. 53
  Checking Volume Group Definitions .................................. 53
  Checking Physical Volumes .............................................. 55
  Checking Logical Volumes ................................................. 56
  Checking Filesystems ................................................... 57
Checking the TCP/IP Subsystem .......................................... 59
  Checking Point-to-Point Connectivity ................................. 60
  Checking the IP Address and Netmask ............................... 61
  Checking ATM Classic IP Hardware Addresses ...................... 62
Checking the AIX Operating System .................................... 63
Checking Physical Networks ............................................. 63
Checking Disks and Disk Adapters ..................................... 64
  Recovering from PCI Hot Plug Network Adapter Failure ............ 66
Checking System Hardware ............................................... 66

Chapter 4: Solving Common Problems 67

HACMP Installation Issues ................................................ 67
  Cannot Find Filesystem at Boot Time .................................. 67
  cl_convert Does Not Run Due to Failed Installation ................. 68
  Configuration Files Could Not Be Merged During Installation .... 68
  System ID Licensing Issues .............................................. 68
HACMP Startup Issues .................................................... 69
  ODMPATH Environment Variable Not Set Correctly ................ 69
  Cluster Manager Starts but then Hangs ................................ 69
  clinfo Daemon Exits After Starting ................................... 70
  Node Powers Down; Cluster Manager Will Not Start ............... 70
  configchk Command Returns an Unknown Host Message ............. 71
  Cluster Manager Hangs During Reconfiguration ..................... 71
  clsmuxpd Does Not Start or Exits After Starting ................. 71
  Pre- or Post-Event Does Not Exist on a Node After Upgrade ....... 72
About This Guide

Managing an HACMP system involves several distinct tasks. Installation and configuration prepare the system for use, while administration involves making planned changes to the system.

In contrast, troubleshooting deals with the unexpected; it is an important part of maintaining a stable, reliable HACMP environment.

This guide presents a comprehensive strategy for identifying and resolving problems that may affect an HACMP cluster. The guide presents the evaluation criteria, procedures, and tools that help you determine the source of a problem. Although symptoms and causes of common problems are examined in detail, the guide’s overall focus is on developing a general methodology for solving problems at your site.

Who Should Read This Guide

This guide is intended for the system administrator responsible for maintaining an HACMP environment. It helps you identify and solve problems that may occur while using the HACMP software. Even if your site is not experiencing problems with the software, it is still useful to develop the diagnostic skills described in this guide.

If you are running HACMP/ES, see the Enhanced Scalability Installation and Administration Guide for a discussion of troubleshooting in general and the RSCT Services in particular.

Before You Begin

As a prerequisite, you need a basic understanding of the components that make up an HACMP cluster in order to solve problems in the cluster. This guide assumes that you understand:

- HACMP software and concepts
- Communications, including the TCP/IP subsystem
- The AIX operating system, including the Logical Volume Manager subsystem
- The hardware and software installed at your site.

You should also read the following HACMP documentation:

- Concepts and Facilities Guide
- Planning Guide
- Installation Guide
- Administration Guide
- Enhanced Scalability Installation and Administration Guide (if you are running HACMP/ES)
Highlighting

The following highlighting conventions are used in this book:

*Italic* Identifies variables in command syntax, new terms and concepts, or indicates emphasis.

**Bold** Identifies routines, commands, keywords, files, directories, menu items, and other items whose actual names are predefined by the system.

Monospace Identifies examples of specific data values, examples of text similar to what you might see displayed, examples of program code similar to what you might write as a programmer, messages from the system, or information that you should actually type.

ISO 9000

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

Related Publications

The following publications provide additional information about the HACMP software:

- *Release Notes* in `/usr/lpp/cluster/doc/release_notes` contain hardware and software requirements and last-minute information about the current release.
- *Planning Guide* - SC23-4277
- *Installation Guide* - SC23-4278
- *Administration Guide* - SC23-4279
- *Programming Locking Applications* - SC23-4281
- *Programming Client Applications* - SC23-4282
- *Enhanced Scalability Installation and Administration Guide* - SC23-4284
- *Master Glossary* - SC23-4285
- *IBM International Program License Agreement*

Manuals accompanying machine and disk hardware also provide relevant information.

Accessing Publications

On the World Wide Web, enter the following URL to access an online library of documentation covering AIX, RS/6000, and related products:

http://www-1.ibm.com/servers/aix/library/
Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

- AFS
- AIX
- AIX 5L
- DFS
- @server
- Enterprise Storage Server
- IBM
- NetView
- pSeries
- RS/6000
- Scalable POWERParallel Systems
- Shark
- SP
- xSeries

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

Other company, product, and service names may be trademarks or service marks of others.
Chapter 1: Diagnosing the Problem

This chapter presents the recommended strategy for troubleshooting an HACMP cluster. It neither identifies nor addresses specific problems. See Chapter 4: Solving Common Problems, for solutions to common problems that may occur in an HACMP environment.

Note: The default locations of log files are used in this chapter. If you redirected any logs, check the appropriate location.

Troubleshooting an HACMP Cluster

Typically, a functioning HACMP cluster requires minimal intervention. If a problem occurs, however, diagnostic and recovery skills are essential. Thus, troubleshooting requires that you identify the problem quickly and apply your understanding of the HACMP software to restore the cluster to full operation.

In general, troubleshooting an HACMP cluster involves:

• Becoming aware that a problem exists
• Determining the source of the problem
• Correcting the problem.

Becoming Aware of the Problem

When a problem occurs within an HACMP cluster, you will most often be made aware of it through:

• End users’ complaints because they are not able to access an application running on a cluster node
• One or more error messages displayed on the system console.

There are two other ways you can become aware of a cluster problem: through mail notification or pager notification.

• Mail Notification. Although HACMP standard components do not send mail to the system administrator when a problem occurs, you can create pre- or post-event processing scripts that perform mail notification either before or after an event script is executed. In an HACMP cluster environment, mail notification is effective and highly recommended. See the Planning Guide for more information.

• Pager Notification. You can also define a notification method through the SMIT interface to issue a customized page in response to a cluster event. See the chapter on customizing cluster events in the Installation Guide for more information.
Application Services Are Not Available

End-user complaints often provide the first indication of a problem with the system. End users may be locked out of an application, or they may not be able to access a cluster node. Thus when problems occur, you must be able to resolve them and restore your cluster to its full operational status.

When a problem is reported, gather detailed information about exactly what has happened. Find out which application failed. Was an error message displayed? If possible, verify the problem by having the user repeat the steps that led to the initial problem. Try to duplicate the problem on your own system, or ask the end user to re-create the failure.

Note: Being locked out of an application does not always indicate a problem with the HACMP software. Rather, the problem can be with the application itself or with its start and stop scripts. Troubleshooting the applications that run on nodes, therefore, is an integral part of debugging an HACMP cluster.

Messages Displayed on System Console

The HACMP system generates descriptive messages when the scripts it executes (in response to cluster events) start, stop, or encounter error conditions. In addition, the daemons that make up an HACMP cluster generate messages when they start, stop, encounter error conditions, or change state. The HACMP system writes these messages to the system console and to one or more cluster log files. Errors may also be logged to associated system files, such as the snmpd.log file.

For information about how to include additional notification services in your HACMP cluster, see the Administration Guide.

Determining a Problem Source

Once you are aware of a problem, try to locate its source. Be aware, however, that the surface problem is sometimes misleading. To diagnose a problem, follow these general steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>What you do...</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Save associated log files (/tmp/hacmp.out and /tmp/cm.log). It is important to save the log files associated with the problem before they are overwritten or no longer available.</td>
</tr>
<tr>
<td>2</td>
<td>Examine the log files for messages generated by the HACMP system.</td>
</tr>
<tr>
<td>3</td>
<td>Investigate the critical components of an HACMP cluster using a combination of HACMP utilities and AIX commands.</td>
</tr>
<tr>
<td>4</td>
<td>Activate tracing of HACMP subsystems.</td>
</tr>
</tbody>
</table>

Each step lets you obtain more detailed information about HACMP cluster components. You may not, however, need to perform each step. Examining the cluster log files may provide enough information to diagnose a problem. The following sections describe how to perform these diagnostic tasks.
Examining Messages and Log Files

Your first step in investigating a problem should be to look for an error message. Whenever a cluster script or an HACMP daemon encounters an error condition, it generates an error message. This message should provide the best clue to the source of the problem.

For example, the Cluster Manager on the local node generates the following message if the entry in the /etc/services file that defines the keepalive port to the Cluster Manager on another cluster node is missing or was added without updating the file:

Could not find port 'clm_keepalive'.

Appendix A: HACMP Messages, contains a list of messages generated by HACMP components. The list suggests actions you can follow in response to some messages.

When an HACMP script or daemon generates a message, the message is written to the system console and to one or more cluster log files. Messages written to the system console may scroll off screen before you notice them. If no messages are visible on the console, begin your search by examining the cluster log files.

HACMP scripts, daemons, and utilities write messages to the following log files:

/usr/adm/cluster.log Contains time-stamped, formatted messages generated by HACMP scripts and daemons.

/tmp/hacmp.out Contains time-stamped, formatted messages generated by the HACMP scripts. In verbose mode, this log file contains a line-by-line record of each command executed in the scripts, including the values of the arguments passed to the commands. By default, the HACMP software writes verbose information to this log file; however, you can change this default. Verbose mode is recommended.

system error log Contains time-stamped, formatted messages from all AIX subsystems, including the HACMP scripts and daemons.

/usr/sbin/cluster/history/cluster.mmddyyyy Contains time-stamped, formatted messages generated by the HACMP scripts. The system creates a new cluster history log file every day and identifies each day’s copy by the filename extension, where mm indicates the month, dd indicates the day, and yyyy the year.

/tmp/cm.log Contains time-stamped, formatted messages generated by HACMP clstrmgr activity. Information in this file is used by IBM Support personnel when the clstrmgr is in debug mode. Note that this file is overwritten every time cluster services are started, so you should be careful to make a copy of it before restarting cluster services on a failed node.

/tmp/cspoc.log Contains time-stamped, formatted messages generated by HACMP C-SPOC commands. Because the C-SPOC utility lets you start or stop the cluster from a single cluster node, the /tmp/cspoc.log file is stored on the node that initiates a C-SPOC command.
Diagnosing the Problem  
Determining a Problem Source

See Chapter 2: Examining Cluster Log Files, for more information about these files.

Investigating System Components

If no error messages are displayed on the console and if examining the log files proves fruitless, investigate each component of your HACMP environment and eliminate it as the cause of the problem.

Both HACMP and AIX provide utilities you can use to determine the state of an HACMP cluster and the resources within that cluster. Using these commands, for example, you can gather information about volume groups or networks. Again, your knowledge of the HACMP system is essential. You must know beforehand the characteristics of a normal cluster and be on the lookout for deviations from the norm as you examine the cluster components. Often, the surviving cluster nodes can provide an example of the correct setting of a system parameter or other cluster configuration information.

The following sections describe the components of an HACMP cluster and recommend guidelines you should follow when investigating a cluster. See Chapter 3: Investigating System Components, for more information about the HACMP software and AIX utilities you can use for this purpose.
System Component Overview

The following figure shows a model of an HACMP system. In the model, each key component of the system is shown as a distinct layer. These layers identify the components to investigate when troubleshooting an HACMP system.

<table>
<thead>
<tr>
<th>Layer</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application layer</td>
<td>consists of the highly available applications that use HACMP for AIX services</td>
</tr>
<tr>
<td>HACMP for AIX layer</td>
<td>provides highly available services to client applications</td>
</tr>
<tr>
<td>LVM layer</td>
<td>manages disk space at the logical level</td>
</tr>
<tr>
<td>TCP/IP layer</td>
<td>manages communications at the logical level</td>
</tr>
<tr>
<td>AIX layer</td>
<td>provides operating system services</td>
</tr>
<tr>
<td>Physical Network layer</td>
<td>provides data exchange between cluster members</td>
</tr>
<tr>
<td>Physical Disk layer</td>
<td>manages data at the physical layer</td>
</tr>
<tr>
<td>System Hardware layer</td>
<td>provides hardware support</td>
</tr>
</tbody>
</table>

HACMP System Components

For more detailed information about HACMP system components, see the *Concepts and Facilities Guide*. 
Troubleshooting Guidelines

As you investigate HACMP system components, the following guidelines should make the troubleshooting process more productive:

- **Save the log files associated with the problem before they become unavailable.** Make sure you save the `/tmp/hacmp.out` and `/tmp/cm.log` files before you do anything else to try to figure out the cause of the problem.

- **Attempt to duplicate the problem.** Do not rely too heavily on the user’s problem report. The user has only seen the problem from the application level. If necessary, obtain the user’s data files to recreate the problem.

- **Approach the problem methodically.** Allow the information gathered from each test to guide your next test. Do not jump back and forth between tests based on hunches.

- **Keep an open mind.** Do not assume too much about the source of the problem. Test each possibility and base your conclusions on the evidence of the tests.

- **Isolate the problem.** When tracking down a problem within an HACMP cluster, isolate each component of the system that can fail and determine whether it is working. Work from top to bottom, following the progression described in the following section.

- **Go from the simple to the complex.** Make the simple tests first. Do not try anything complex and complicated until you have ruled out the simple and obvious.

- **Make one change at a time.** Do not make more than one change at a time. If you do, and one of the changes corrects the problem, you have no way of knowing which change actually fixed the problem. Make one change, test the change, and then, if necessary, make the next change.

- **Stick to a few simple troubleshooting tools.** For most problems within an HACMP system, the tools discussed in Chapter 3: Investigating System Components, are sufficient.

- **Do not neglect the obvious.** Small things can cause big problems. Check plugs, connectors, cables, and so on.

- **Keep a record of the tests you have completed.** Record your tests and results, and keep an historical record of the problem in case it reappears.

Tracing System Activity

If the log files have no relevant information and the component-by-component investigation does not yield concrete results, you can use the HACMP trace facility to attempt to diagnose the problem. The trace facility provides a detailed look at selected system events. Note that both the HACMP and AIX software must be running in order to use HACMP tracing.

See Appendix B: HACMP Tracing, for more information on using the trace facility. Interpreting the output generated by the trace facility requires extensive knowledge of both the HACMP software and the AIX operating system.
Using the cldiag Utility to Perform Diagnostic Tasks

To help diagnose problems, the HACMP software includes the `/usr/sbin/cluster/diag/cldiag` diagnostic utility that provides a common interface to several HACMP and AIX diagnostic tools. Using this utility, you can perform the following diagnostic tasks:

- View the cluster log files into which the cluster writes error and status messages
- Activate Cluster Manager debug mode
- Obtain a listing of all locks in the Cluster Lock Manager’s lock resource table
- Check volume group definitions
- Activate tracing in the HACMP daemons.

When you invoke the `cldiag` utility, by entering the `cldiag` command, the utility displays a list of available options and the `cldiag` prompt. You select an option by entering it at the `cldiag` prompt. The `cldiag` utility displays additional options, if appropriate, with each selection, until the command syntax is completed. Once you are familiar with the `cldiag` command syntax for a particular function, you can enter it directly at the system prompt by specifying the entire command with all its options. Note that the `cldiag` utility should not be used while the Cluster Manager daemon (`clstrmgr`) is running.

For more information about the syntax of the `cldiag` utility, see the `cldiag` man page. Also, specific functions of the `cldiag` utility are described in other sections of this guide.

Using the Cluster Snapshot Utility to Check Cluster Configuration

The HACMP cluster snapshot facility (`/usr/sbin/cluster/utilities/clsnapshot`) allows you to save in a file a record of all the data that defines a particular cluster configuration. You can use this snapshot for troubleshooting cluster problems.

The cluster snapshot saves the data stored in the HACMP ODM classes. In addition to this ODM data, a cluster snapshot also includes output generated by various HACMP and standard AIX commands and utilities. This data includes the current state of the cluster, node, network, and adapters as viewed by each cluster node, as well as the state of any running HACMP daemons. It may also include additional user-defined information if there are custom snapshot methods in place.

See Chapter 3: Investigating System Components, for more information on using the cluster snapshot utility.
Using SMIT Cluster Recovery Aids

After you have identified a problem, you must correct it and restore access to critical applications. For example, if a script failed because it was unable to set the hostname, the Cluster Manager reports the event failure. Once you correct the problem by setting the hostname from the command line, you must get the Cluster Manager to resume cluster processing. The SMIT Cluster Recovery Aids screen allows you to do so. The Recover From Script Failure menu option invokes the /usr/sbin/cluster/utilities/clruncmd command, which sends a signal to the Cluster Manager daemon (clstrmgr) on the specified node, causing it to stabilize. You must re-run the script manually to continue processing.

Be aware that to fix some cluster problems, you must stop the Cluster Manager on the failed node and have a surviving node take over its shared resources. If the cluster is in reconfiguration, it can only be brought down through a forced stop. The surviving nodes in the cluster will interpret a forced stop as a graceful node down event and will not attempt to take over resources. You can then begin the troubleshooting procedure.

If all else fails, bring down the Cluster Manager on all cluster nodes. Then manually start the application that the HACMP cluster event scripts were attempting to start and run the application without the HACMP software. With the Cluster Manager down on all cluster nodes, correct the conditions that caused the initial problem.

Correcting a Script Failure

On rare occasions, an HACMP script may fail and cause a cluster node to become unstable. If this happens, you may need to execute the Recover From Script Failure option on the SMIT Cluster Recovery Aids menu to stabilize the node. Before using this option to run the /usr/sbin/cluster/utilities/clruncmd command, make sure that you fix the problem that caused the script failure. Then, to resume clustering, complete the following steps:

1. Type `smit hacmp`
2. Select `Cluster Recovery Aids > Recover From Script Failure`.
3. Select the adapter IP label for the node on which you want to run the `clruncmd` command and press Enter. The system next prompts you to confirm the recovery attempt. The adapter IP label is listed in the `/etc/hosts` file and is the name assigned to the service adapter of the node on which the failure occurred.
4. Press Enter to continue. Another SMIT screen appears to confirm the success of the script recovery.
5. Press F10 to exit SMIT.

Note that to run the `clruncmd` command remotely on cluster nodes, each node must list the other cluster nodes in its `/rhosts` file.
Verifying Expected Behavior

When the highly available applications are up and running, verify that end users can access the applications. If not, you may need to look elsewhere to identify problems affecting your cluster. The remaining chapters in this guide describe ways in which you should be able to locate potential problems.

**Note:** To verify the expected behavior of a particular cluster or DARE event, without actually running that event, use the HACMP Event Emulator. For more information about the Event Emulator see the *Concepts and Facilities Guide*. 
Diagnosing the Problem
Verifying Expected Behavior
Chapter 2: Examining Cluster Log Files

This chapter describes how to use cluster log files to understand your cluster’s operation.

Note: The default locations of log files are used in this chapter. If you redirected any logs, check the appropriate location.

HACMP Messages and Cluster Log Files

Your first approach to diagnosing a problem affecting your cluster should be to examine the cluster log files for messages put out by the HACMP subsystems. These messages can provide invaluable information toward understanding the current state of the cluster and possible causes of cluster problems. The following sections describe the types of messages the HACMP system puts out and the log files into which the system writes these messages.

Types of Cluster Messages

The HACMP system generates several types of messages:

Event notification messages

Cluster events cause HACMP scripts to be executed. When scripts start, complete, or encounter error conditions, the HACMP software generates a message. For example, the following fragment from a cluster log file illustrates the start and completion messages for several HACMP scripts. The messages include any parameters passed to the script.

Feb 25 11:02:46 EVENT START: node_up 2
Feb 25 11:02:46 EVENT START: node_up_local
Feb 25 11:02:47 EVENT START: acquire_service_addr
Feb 25 11:02:56 EVENT COMPLETED: acquire_service_addr

Verbose script output messages

In addition to the start, completion, and error messages generated by scripts, the HACMP software can also generate a detailed report of each step of script processing. In verbose mode, the default mode, the shell generates a message for each command executed in the script, including the values of all arguments to these commands. Verbose mode is recommended for troubleshooting your cluster. The following fragment from a cluster log file illustrates the verbose output of the node_up script. The verbose messages are prefixed with a plus (+) sign.

Feb 25 11:02:46 EVENT START: node_up 2
+ set -u
+ [ 2 = 2 ]
+ /usr/sbin/cluster/events/cmd/clcallev node_up_local
Feb 25 11:02:46 EVENT START: node_up_local
+ set -u
+ rm -f /usr/sbin/cluster/server.status
+ /usr/sbin/cluster/events/cmd/clcallev acquire_service_addr

Feb 25 11:02:47 EVENT START: acquire_service_addr
+ set -u
+ +grep : boot + cut -d: -f1
/usr/sbin/cluster/utilities/cllsif -cSi 2
Examine Cluster Log Files
HACMP Messages and Cluster Log Files

Cluster state messages

When an HACMP cluster starts, stops, or goes through other state changes, it generates messages. These messages may be informational, such as a warning message, or they may report a fatal error condition that causes an HACMP subsystem to terminate. In addition to the clstart and clstop commands, the following HACMP subsystems and utilities generate status messages:

- The Cluster Manager daemon (clstrmgr)
- The Cluster Information Program daemon (clinfo)
- The Cluster SMUX Peer daemon (clsmuxpd)
- The Cluster Lock Manager daemon (clclockd)

The following example illustrates cluster state messages that the Cluster Manager, the Clinfo daemon, and several HACMP scripts put out. Script messages are identified by their “HACMP for AIX” subsystem name.

Feb 25 11:02:30 limpet HACMP for AIX: Starting execution of /etc/rc.cluster with parameters: --
Feb 25 11:02:32 limpet HACMP for AIX: clstart: called with flags -sm
Feb 25 11:02:36 limpet clstrmgr[18363]: CLUSTER MANAGER STARTED
Feb 25 11:02:40 limpet HACMP for AIX: Completed execution of /etc/rc.cluster with parameters: --. Exit status = 0
Feb 25 11:02:46 limpet HACMP for AIX: EVENT START: node_up 2
Feb 25 11:02:47 limpet HACMP for AIX: EVENT START: node_up_local
Feb 25 11:02:47 limpet HACMP for AIX: EVENT START: acquire_service_addr
Feb 25 11:02:53 limpet HACMP for AIX: EVENT COMPLETED: acquire_service_addr
Feb 25 11:02:54 limpet HACMP for AIX: EVENT START: get_disk_vg_fs
Feb 25 11:02:55 limpet HACMP for AIX: EVENT COMPLETED: get_disk_vg_fs
Feb 25 11:03:35 limpet clinfo[6543]: read_config: node address too long, ignoring.

Appendix A: HACMP Messages, contains a list of messages generated by HACMP scripts, daemons, and the C-SPOC utility.

All C-SPOC commands generate messages based on their underlying AIX command output. See the Administration Guide for a list of C-SPOC commands, or see the C-SPOC man pages to determine the underlying AIX command.

Cluster Message Log Files

The HACMP software writes the messages it generates to the system console and to several log files. Each log file contains a different subset of messages generated by the HACMP software. When viewed as a group, the log files provide a detailed view of all cluster activity. The
following list describes the log files into which the HACMP software writes messages and the types of cluster messages they contain. The list also provides recommendations for using the different log files.

<table>
<thead>
<tr>
<th>Filename</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/usr/adm/cluster.log</td>
<td>Contains time-stamped, formatted messages generated by HACMP scripts and daemons. For more information, see Understanding the cluster.log File. Recommended Use: This log file provides a high-level view of current cluster status. It is a good place to look first when diagnosing a cluster problem.</td>
</tr>
<tr>
<td>/tmp/hacmp.out</td>
<td>Contains time-stamped, formatted messages generated by HACMP scripts on the current day. The /tmp/hacmp.out log file does not contain cluster state messages. In verbose mode (recommended), this log file contains a line-by-line record of every command executed by scripts, including the values of all arguments to each command. For more information, see Understanding the hacmp.out Log File. In HACMP/ES only, an event summary appears at the end of each set of event details. You can view and save all event summary information pulled from current and past hacmp.out files using the Display Event Summaries option. Recommended Use: This file is the primary source of information when investigating a problem.</td>
</tr>
<tr>
<td>system error log</td>
<td>Contains time-stamped, formatted messages from all AIX subsystems, including HACMP scripts and daemons. For information about viewing this log file and interpreting the messages it contains, see Understanding the System Error Log. Recommended Use: The system error log contains time-stamped messages from many other system components, so it is a good place to match cluster events with system events.</td>
</tr>
<tr>
<td>/usr/sbin/cluster/history/cluster.mmddyyyy</td>
<td>Contains time-stamped, formatted messages generated by HACMP scripts. The system creates a cluster history file every day, identifying each file by its filename extension, where mmm indicates the month, dd indicates the day and yyyy the year. For information about viewing this log file and interpreting its messages, see Understanding the Cluster History Log File. Recommended Use: Use the cluster history log files to get an extended view of cluster behavior over time.</td>
</tr>
</tbody>
</table>
Examining Cluster Log Files

HACMP Messages and Cluster Log Files

The following table summarizes the types of messages contained in each of the log files you might consult on a regular basis.

<table>
<thead>
<tr>
<th>Log File</th>
<th>Event Notification</th>
<th>Cluster State</th>
<th>Verbose Output</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>/usr/adm/cluster.log</code></td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td><code>/tmp/cm.log</code></td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td><code>/tmp/cspoc.log</code></td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td><code>/tmp/hacmp.out</code></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><code>system error log</code></td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td><code>/usr/sbin/cluster/history/cluster.mmddyyyy</code></td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Contains time-stamped, formatted messages generated by HACMP `clstrmgr` activity. By default, the messages are short. Note that this file is overwritten every time cluster services are started, so you should be careful to make a copy of it before restarting cluster services on a failed node.

IBM Support personnel may have you turn on `clstrmgr` debug options (for verbose, detailed information) to help them understand a particular problem. With debugging turned on, this file grows quickly. You should clean up the file and turn off debug options as soon as possible.

**Recommended Use:** Information in this file is for IBM Support personnel.

Contains time-stamped, formatted messages generated by HACMP C-SPOC commands. The `/tmp/cspoc.log` file resides on the node that invokes the C-SPOC command.

**Recommended Use:** Use the C-SPOC log file when tracing a C-SPOC command’s execution on cluster nodes.

For information about starting and stopping a cluster using C-SPOC commands, see the Administration Guide.

Records log messages every time HACMP triggers the deadman switch. Be aware that over time, this file can grow large.

Contains time-stamped, formatted messages generated by the HACMP Event Emulator. The messages are collected from output files on each node of the cluster, and cataloged together into the `/tmp/emuhacmp.out` log file.

In verbose mode (recommended), this log file contains a line-by-line record of every event emulated. Customized scripts within the event are displayed, but commands within those scripts are not executed. For more information, see Understanding the `/tmp/emuhacmp.out` File.
Understanding the cluster.log File

The /usr/adm/cluster.log file is a standard text file. When checking this file, first find the most recent error message associated with your problem. Then read back through the log file to the first message relating to that problem. Many error messages cascade from an initial error that usually indicates the problem source.

Format of Messages in the cluster.log File

The entries in the /usr/adm/cluster.log file use the following format:

```
```

Format of cluster.log File Entries

Each entry contains the following information:

- **Date and Time stamp**  The day and time on which the event occurred.
- **Node**  The node on which the event occurred.
- **Subsystem**  The HACMP subsystem that generated the event. The subsystems are identified by the following abbreviations:
  - clstrmgr—The Cluster Manager daemon
  - clinfo—The Cluster Information Program daemon
  - clsmuxpd—The Cluster SMUX Peer daemon
  - c1lockd—The Cluster Lock Manager daemon
  - HACMP—Startup and reconfiguration scripts.
- **PID**  The process ID of the daemon generating the message. (Not included for messages output by scripts.)
- **Message**  The message text. See Appendix A: HACMP Messages, for a description of each message.

The entry in the previous example indicates that the Cluster Information Program (clinfo) stopped running on the node named *n1* at 5:25 P.M. on March 3.

Viewing the cluster.log File

The /usr/adm/cluster.log file is a standard text file that can be viewed in any of the following ways:

- Using standard AIX file commands, such as the **more** or **tail** commands
- Using the SMIT interface
- Using the HACMP **cldiag** diagnostic utility.
Using Standard AIX File Commands to View the cluster.log file

Standard AIX file commands, such as the `more` or `tail` commands, let you view the contents of the `/usr/adm/cluster.log` file. See the `more` or `tail` man pages for information about using these commands.

Using the SMIT Interface to View the cluster.log File

To view the `/usr/adm/cluster.log` file using SMIT:

1. Type `smit hacmp`
2. Select **RAS Support > View HACMP Log Files > Scan the HACMP System Log**.

   The contents of the `/usr/adm/cluster.log` file are listed at the console.

   **Note:** You can choose to either `scan` the contents of the `/usr/adm/cluster.log` file as it exists, or you can `watch` an active log file as new events are appended to it in real time. Typically, you `scan` the file to try to find a problem that has already occurred; you `watch` the file while duplicating a problem to help determine its cause, or as you test a solution to a problem to determine the results.

Using the cldiag Utility to View the cluster.log File

To view the `/usr/adm/cluster.log` file using the `cldiag` utility, you must include the `/usr/sbin/cluster/diag` directory in your PATH environment variable. Then to run the utility from any directory, perform the following steps.

1. First, type `cldiag`

   The utility returns a list of options and the `cldiag` prompt:

   -----------------------------------------------
   To get help on a specific option, type: help <option>
   To return to previous menu, type: back
   To quit the program, type: quit
   -----------------------------------------------

   **valid options are:**
   debug
   logs
   vgs
   error
   trace

   `cldiag>`

   The `cldiag` utility `help` subcommand provides a brief description of the syntax of the option specified. For more information about the command syntax, see the `cldiag` man page.

2. Enter the `logs` option at the `cldiag` prompt:

   `cldiag>` logs

   The `cldiag` utility displays the following options and prompt. Note that the prompt changes to reflect the last option selection.

   **valid options are:**
   scripts
   syslog
3. To view the /usr/adm/cluster.log file, enter:

```bash
cldiag.logs> syslog
```

By default, the `cldiag` utility displays all messages in the log file for every cluster process on the local node. However, you can optionally view only those messages associated with a specific process or processes.

To view specific messages, quit the `cldiag` utility and use the `lssrc -g cluster` command at the system prompt to obtain the name of cluster processes. Then restart the `cldiag` utility and specify the name of the process whose messages you want to view. If you want to view more than one process, separate multiple names with spaces.

For example, to view only those messages generated by the Cluster Manager and `clinfo`, specify the names as in the following example:

```bash
cldiag.logs> syslog clstrmgr clinfo
```

Using flags associated with the `syslog` option, you can specify the types of messages you want to view, the time period covered by the messages, and the file in which you want the messages stored.

The following table lists the optional command-line flags and their function:

<table>
<thead>
<tr>
<th>Flag</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-h hostname</code></td>
<td>View messages generated by a particular cluster node.</td>
</tr>
<tr>
<td><code>-e</code></td>
<td>View only error-level messages.</td>
</tr>
<tr>
<td><code>-w</code></td>
<td>View only warning-level messages.</td>
</tr>
<tr>
<td><code>-d days</code></td>
<td>View messages logged during a particular time period. You specify the time period in days.</td>
</tr>
<tr>
<td><code>-R filename</code></td>
<td>Store the messages in the file specified. By default, the <code>cldiag</code> utility writes the messages to <code>stdout</code>.</td>
</tr>
</tbody>
</table>

For example, to list all Cluster Manager error-level messages recorded in the last two days and have the listing written to a file named `cm_errors.out`, enter the following:

```bash
cldiag logs syslog -d 2 -e -Rcm_errors.out clstrmgr
```

This example illustrates how to execute a `cldiag` function directly without traversing the menu hierarchy.

---

### Understanding the hacmp.out Log File

The `/tmp/hacmp.out` file is a standard text file. Each night, a cron job cycles this file and creates a new `hacmp.out` log file; it retains the last seven copies. Each copy is identified by a number appended to the filename. The newly created and most recent log file is named `/tmp/hacmp.out`; the oldest version of the file is named `/tmp/hacmp.out.7`.

When checking the `/tmp/hacmp.out` file, search for EVENT FAILED messages. These messages indicate that a failure has occurred. Then, starting from the failure message, read back through the log file to determine exactly what went wrong. The `/tmp/hacmp.out` log file provides the most important source of information when investigating a problem.
In HACMP/ES only, event details are followed by an event summary. These event summaries can also be viewed outside of the **hacmp.out** file using the Display Event Summaries option in the HACMP/ES SMIT menu. For more details on this features, see the *Enhanced Scalability Installation and Administration Guide*. Also see issues relating to event summaries in the section Miscellaneous Issues in Chapter 4: Solving Common Problems.

### Format of Messages in the hacmp.out Log File

**Non-Verbose Output**

In non-verbose mode, the `/tmp/hacmp.out` log contains the start, completion, and error notification messages output by all HACMP scripts. The following example illustrates the start of the script executed in response to the **node_up** cluster event as it appears in an `/tmp/hacmp.out` file:

```plaintext
<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Message</th>
<th>Return Status</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feb 22</td>
<td>07:31:35</td>
<td>EVENT START: fail_standby 140.186.100.189</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Feb 22</td>
<td>07:31:36</td>
<td>EVENT COMPLETED: fail_standby 140.186.100.189</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Feb 22</td>
<td>07:31:37</td>
<td>EVENT START: release_vg_fs limpetvg</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Feb 22</td>
<td>07:31:39</td>
<td>EVENT FAILED:1: release_vg_fs limpetvg</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

**Format of Non-Verbose hacmp.out Output**

Each entry contains the following information:

- **Date and Time Stamp**: The day and time the event occurred.
- **Message**: Text that describes the cluster activity.
- **Return Status**: Messages that report failures include the status returned from the script. This information is not included for successful scripts.
- **Event Description**: The specific action attempted or completed on a node, file system, or volume group.

In verbose mode, the `/tmp/hacmp.out` file also includes the values of arguments and flag settings passed to the scripts and commands, and the expansion of script statements. These lines are prefixed with a plus sign (+). The following example illustrates the flags and arguments passed to the `release_vg_fs` script in the previous example.

```plaintext
Mar 12 14:06:36 EVENT START: acquire_acconn_service enl ether_rot
rot111:acquire_acconn_service[53] [[ high = high ]]
rot111:acquire_acconn_service[53] version=1.7
rot111:acquire_acconn_service[54] rot111:acquire_acconn_service[54] cl_get_path
HA_DIR=es
rot111:acquire_acconn_service[56] STATUS=0
```

**Verbose Output**

In verbose mode, the `/hacmp.out` file also includes the values of arguments and flag settings passed to the scripts and commands.
Examining Cluster Log Files

Understanding the hacmp.out Log File

Troubleshooting Guide

rot111:acquire_aconn_service[58] [ 2 -ne 2 ]
rot111:acquire_aconn_service[64] set -u
rot111:acquire_aconn_service[66] SERVICE_INTERFACE=en1
rot111:acquire_aconn_service[67] NETWORK=ether_rot
rot111:acquire_aconn_service[70] rot111:acquire_aconn_service[70] cllsif
- i holmes -Sc
rot111:acquire_aconn_service[70] awk -F: { if ( $2 == "standby" && ( $5 == "public" || $5 == "private" )) print $0)
STANDBY_ADAPTERS_INFO=holmes_en2stby:standby:ether_rot:ether:public:holmes:192.168.91.4::en2::255.255.255.0
holmes_en4stby:standby:ether_svc:ether:private:holmes:192.168.93.4::en4::255.255.255.0
rot111:acquire_aconn_service[73] STANDBY_INTERFACES=
rot111:acquire_aconn_service[76] echo
holmes_en2stby:standby:ether_rot:ether:public:holmes:192.168.91.4::en2::255.255.255.0
rot111:acquire_aconn_service[76] cut -d: -f3
rot111:acquire_aconn_service[76] [ ether_rot = ether_rot ]
rot111:acquire_aconn_service[78] rot111:acquire_aconn_service[78] echo
holmes_en2stby:standby:ether_rot:ether:public:holmes:192.168.91.4::en2::255.255.255.0
rot111:acquire_aconn_service[78] cut -d: -f1
standby_adapter=holmes_en2stby
rot111:acquire_aconn_service[79] rot111:acquire_aconn_service[79]
cgetif -a holmes_en2stby
rot111:acquire_aconn_service[79] LANG=C
standby_interface=en2
rot111:acquire_aconn_service[80] [ 0 -eq 0 ]
rot111:acquire_aconn_service[82] STANDBY_INTERFACES= en2
rot111:acquire_aconn_service[76] echo
holmes_en4stby:standby:ether_svc:ether:private:holmes:192.168.93.4::en4::255.255.255.0
rot111:acquire_aconn_service[76] cut -d: -f3
rot111:acquire_aconn_service[76] [ ether_svc = ether_rot ]
rot111:acquire_aconn_service[90] echo Call swap_aconn_protocol en1 en2
Call swap_aconn_protocol en1 en2
rot111:acquire_aconn_service[91] ccall ev swap_aconn_protocols en1 en2
Mar 12 14:06:36 EVENT START: swap_aconn_protocols en1 en2
rot111:swap_aconn_protocols[60] [[ high = high ]]
rot111:swap_aconn_protocols[60] version=1.6
rot111:swap_aconn_protocols[61] rot111:swap_aconn_protocols[61]
cl_get_path
HA_DIR=es
rot111:swap_aconn_protocols[63] STATUS=0
rot111:swap_aconn_protocols[65] [ 2 -ne 2 ]
rot111:swap_aconn_protocols[71] set -u
rot111:swap_aconn_protocols[73] TNETDIR=/etc/totalnet
rot111:swap_aconn_protocols[74] [ ! -d /etc/totalnet ]
rot111:swap_aconn_protocols[75] echo No /etc/totalnet directory found.
No /etc/totalnet directory found.
rot111:swap_aconn_protocols[76] exit 0
Mar 12 14:06:36 EVENT COMPLETED: swap_aconn_protocols en1 en2
rot111:acquire_aconn_service[95] exit 0
Mar 12 14:06:36 EVENT COMPLETED: acquire_aconn_service en1 ether_rot
rot111:acquire_service_addr[386] RC=0
rot111:acquire_service_addr[388] [ 0 -ne 0 ]
rot111:acquire_service_addr[409] [[ UNDEFINED != UNDEFINED ]]
rot111:acquire_service_addr[412] export NSORDER=
rot111:acquire_service_addr[416] [[ false = false ]]
rot111:acquire_service_addr[421] [ true = true ]
rot111:acquire_service_addr[426] [ ! -f /usr/es/sbin/cluster/.telinit ]
rot111:acquire_service_addr[468] exit 0
Examining Cluster Log Files
Understanding the hacmp.out Log File

Setting the Level of Information Recorded in the hacmp.out File
To set the level of information recorded in the /tmp/hacmp.out file:
1. Type smit hacmp
2. Select Cluster Configuration > Cluster Resources > Change/Show Run Time Parameters. SMIT prompts you to specify the node name of the cluster node you want to modify. (Note that run-time parameters are configured on a per-node basis.)
3. Select the node and press Enter.
4. To obtain verbose output, make sure the value of the Debug Level field is high. If necessary, press Enter to record a new value. The Command Status screen appears.
5. Press F10 to exit SMIT.

Viewing the hacmp.out Log File
The /tmp/hacmp.out log file is a standard text file that can be viewed in the following ways:
• Using standard AIX file commands, such as the more or tail commands
• Using the SMIT interface
• Using the HACMP cldiag diagnostic utility.

Using Standard AIX File Commands to View hacmp.out
Standard AIX file commands, such as the more or tail commands, let you view the contents of the /tmp/hacmp.out file. See the more or tail man pages for information on using these commands.

Using the SMIT Interface to View hacmp.out
To view the /tmp/hacmp.out file using SMIT:
1. Type smit hacmp
2. Select RAS Support > View HACMP Log Files. From the menu that appears, you can choose to either scan the contents of the /tmp/hacmp.out file or watch as new events are appended to the log file. Typically, you will scan the file to try to find a problem that has already occurred and then watch the file while duplicating a problem to help determine its cause, or as you test a solution to a problem to determine the results. In the menu, the /tmp/hacmp.out file is referred to as the “HACMP Scripts Log File.”
3. Select Scan the HACMP Scripts Log File and press Enter. SMIT displays the scripts log files available.
4. Select a script log file and press Enter.
5. Press F10 to exit SMIT.
Using the cldiag Utility to View hacmp.out

To view the /tmp/hacmp.out file using the cldiag utility, you must include the /usr/sbin/cluster/diag directory in your PATH environment variable. Then to run the utility from any directory:

1. First, type:

   cldiag

   The utility returns a list of options and the cldiag prompt:

   -------------------------------------------------------
   To get help on a specific option, type: help <option>
   To return to previous menu, type: back
   To quit the program, type: quit
   -------------------------------------------------------

   valid options are:
   debug
   logs
   vgs
   error
   trace

   cldiag>

   The cldiag utility help subcommand provides a brief synopsis of the syntax of the option specified. For more information about the command syntax, see the cldiag man page.

2. Next, enter the logs option at the cldiag prompt:

   cldiag> logs

   The cldiag utility displays the following options and prompt. Note that the prompt changes to reflect the current option selection:

   valid options are:
   scripts
   syslog

   cldiag.logs>

   To view the /tmp/hacmp.out file, enter:

   cldiag.logs> scripts

   By default, the cldiag utility writes the entire contents of /tmp/hacmp.out file to stdout. However, you only can view messages related to one or more specific events, such as node_up or node_up_local. See the Concepts and Facilities Guide for a list of all HACMP events. Separate multiple events by spaces. The following example commands allows you to view only those messages associated with the node_up and node_up_local events:

   cldiag.logs> scripts node_up node_up_local
By using flags associated with the **scripts** options, you can specify the types of messages you want to view, the time period covered by the messages, and the file in which you want the messages stored. The following table lists the optional command-line flags and their functions:

<table>
<thead>
<tr>
<th>Flag</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h hostname</td>
<td>View messages generated by a particular cluster node. By default, the <code>scripts</code> subcommand only displays messages generated by the local node.</td>
</tr>
<tr>
<td>-s</td>
<td>View only start and completion messages.</td>
</tr>
<tr>
<td>-f</td>
<td>View only failure messages.</td>
</tr>
<tr>
<td>-d days</td>
<td>View messages logged during a particular time period. You can specify a time period of up to seven days. (The HACMP software keeps only the latest seven copies of the <code>/tmp/hacmp.out</code> file.) By default, the current day’s log, <code>/tmp/hacmp.out</code>, is displayed.</td>
</tr>
<tr>
<td>-R filename</td>
<td>Store the messages in the file specified. By default, the <code>cldiag</code> utility writes the messages to <code>stdout</code>.</td>
</tr>
</tbody>
</table>

For example, to obtain a listing of all failure messages associated with the `node_up` event recorded in the last two days, and have the listing written to a file named `script_errors.out`, enter the following:

```
cldiag logs scripts -d 2 -f -R script_errors.out node_up
```

### Changing the Location of the hacmp.out Log File

You can redirect logs to new locations using SMIT. See the chapter on customizing events and logs in the *Installation Guide* for instructions.

### Resource Group Processing Messages in the hacmp.out File

For each resource group that has been processed by HACMP, the software sends the following information to the `hacmp.out` file:

- the resource group name
- the script name
- the name of the command that is being executed.

The general pattern of the output is:

```
resource_group_name:script_name [line number] command line
```

In cases where an event script does not process a specific resource group, for instance, in the beginning of a `node_up` event, a resource group’s name cannot be obtained. In this case, the resource group’s name part of the tag is blank.

For example, the `hacmp.out` file may contain either of the following lines:

```
cas2:node_up_local[199] set_resource_status ACQUIRING
:node_up[233] cl_ssa_fence up stan
```
Examining Cluster Log Files

Understanding the System Error Log

In addition, references to the individual resources in the event summaries in the hacmp.out file contain reference tags to the associated resource groups.

For instance:


Understanding the System Error Log

The HACMP software logs messages to the system error log whenever a script starts, stops, or encounters an error condition, or whenever a daemon generates a state message.

Format of Messages in the System Error Log

The HACMP messages in the system error log follow the same format as that used by other AIX subsystems. You can view the messages in the system error log in short or long format.

In short format, also called **summary format**, each message in the system error log occupies a single line. The following figure illustrates the short format of the system error log:

<table>
<thead>
<tr>
<th>ERROR_ID</th>
<th>TIMESTAMP</th>
<th>T</th>
<th>CL</th>
<th>RESOURCE_NAME</th>
<th>ERROR_DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>0B8E3D0F1</td>
<td>0709092293 P</td>
<td>H</td>
<td>ent1</td>
<td>CMSA/CD LAN Commun</td>
<td></td>
</tr>
<tr>
<td>ABB1CD5</td>
<td>0709092293 T</td>
<td>H</td>
<td>ent1</td>
<td>COMMUNICATION PROTOCOL</td>
<td></td>
</tr>
<tr>
<td>OF27A5</td>
<td>07040739993 P</td>
<td>S</td>
<td>SRC</td>
<td>SOFTWARE PROGRAM ERROR</td>
<td></td>
</tr>
<tr>
<td>OF27AA5</td>
<td>08110733993 P</td>
<td>S</td>
<td>SYS/PROC</td>
<td>SOFTWARE PROGRAM ABNORMALLY TERMINATED</td>
<td></td>
</tr>
<tr>
<td>AAB8B5241</td>
<td>0906273935 T</td>
<td>O</td>
<td>cltrmgr</td>
<td>OPERATOR NOTIFICATION</td>
<td></td>
</tr>
<tr>
<td>AAB8B5241</td>
<td>0906273935 T</td>
<td>O</td>
<td>cltrmgr</td>
<td>OPERATOR NOTIFICATION</td>
<td></td>
</tr>
<tr>
<td>AAB8B5241</td>
<td>0906273935 T</td>
<td>O</td>
<td>cltrmgr</td>
<td>OPERATOR NOTIFICATION</td>
<td></td>
</tr>
<tr>
<td>AAB8B5241</td>
<td>0906273935 T</td>
<td>O</td>
<td>cltrmgr</td>
<td>OPERATOR NOTIFICATION</td>
<td></td>
</tr>
<tr>
<td>AAB8B5241</td>
<td>0906273935 T</td>
<td>O</td>
<td>cltrmgr</td>
<td>OPERATOR NOTIFICATION</td>
<td></td>
</tr>
</tbody>
</table>

Format of System Error Log Entries (Short Format)

**Error_ID**  
A unique error identifier.

**Timestamp**  
The day and time the event occurred.

**T**  
Error type: permanent (P), unresolved (U), or temporary (T).

**CL**  
Error class: hardware (H), software (S), or informational (O).

**Resource_name**  
A text string that identifies the AIX resource or subsystem that generated the message. HACMP messages are identified by the name of their daemon or script.

**Error_description**  
A text string that briefly describes the error. In long format, a page of formatted information is displayed for each error.

Viewing Cluster Messages in the System Error Log

Unlike the HACMP log files, the **system error log** is not a text file. You can, however, view this log file in the following ways:
Examining Cluster Log Files
Understanding the System Error Log

- Using the AIX `errpt` command
- Using the SMIT interface
- Using the HACMP `cldiag` diagnostic utility.

Using the AIX Error Report Command to view the System Error Log

The AIX `errpt` command generates an error report from entries in the system error log. See the `errpt` man page for information on using this command.

Using the SMIT Interface to View the System Error Log

To view the system error log using SMIT:

1. Type: `smit`
2. Select `Problem Determination > Error Log > Change / Show Characteristics of the Error Log`. The next screen shows the logfile pathname, maximum log size, and memory buffer size.
3. Press F10 to exit SMIT.

For more information on this log file, refer to your AIX documentation.

Using the cldiag Utility to View the System Error Log

To view the system error log using the `cldiag` utility, you must include the `/usr/sbin/cluster/diag` directory in your PATH environment variable. Then to run the utility from any directory:

1. First, type:
   ```
   cldiag
   ```
   The utility returns a list of options and the `cldiag` prompt:
   ```
   -----------------------------------------------
   To get help on a specific option, type: help <option>
   To return to previous menu, type: back
   To quit the program, type: quit
   -----------------------------------------------
   valid options are:
   debug
   logs
   vgs
   error
   trace
   
   cldiag>
   ```
   The `cldiag` utility `help` subcommand provides a brief synopsis of the syntax of the option specified. For more information about command syntax, see the `cldiag` man page.

To view the system error log, enter the `error` option with the type of error display you want at the `cldiag` prompt. For example, to view a listing of the system error log in short format, enter the following command:

```
cldiag> error short
```
To obtain a listing of system error log messages in long format, enter the `error` option with the `long` type designation. To view only those messages in the system error log generated by the HACMP software, enter the `error cluster` option. When you request a listing of cluster error messages, the `cldiag` utility displays system error log messages in short format.

By default, the `cldiag` utility displays the system error log from the local node. Using flags associated with the `error` option, however, you can choose to view the messages for any other cluster node. In addition, you can specify a file into which the `cldiag` utility writes the error log. The following list describes the optional command-line flags and their functions:

<table>
<thead>
<tr>
<th>Flag</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-h hostname</code></td>
<td>View messages generated by a particular cluster node. By default, only messages on the local node are displayed.</td>
</tr>
<tr>
<td><code>-R filename</code></td>
<td>Store the messages in the file specified. By default, the <code>cldiag</code> utility writes the messages to <code>stdout</code>.</td>
</tr>
</tbody>
</table>

For example, to obtain a listing of all cluster-related messages in the system error log and have the listing written to a file named `system_errors.out`, enter the following:

```
cldiag error cluster -R system_errors.out
```

---

**Understanding the Cluster History Log File**

The cluster history log file is a standard text file with the system-assigned name `/usr/sbin/cluster/history/cluster.mmddyyyy`, where `mm` indicates the month, `dd` indicates the day in the month and `yyyy` is the year. You should decide how many of these log files you want to retain and purge the excess copies on a regular basis to conserve disk storage space. You may also want to include the cluster history file in your regular system backup procedures.

**Format of Messages in the Cluster History Log File**

Entries in the cluster history log file use the following format:

```
Feb 22 07:31:35 EVENT START: fail_standby 140.186.100.189
Feb 22 07:31:35 EVENT COMPLETED: fail_standby 140.186.100.189
Feb 22 07:31:36 EVENT START: join_standby 140.186.100.189
Feb 22 07:31:36 EVENT COMPLETED: join_standby 140.186.100.189
Feb 22 07:31:36 EVENT START: node_up 2
Feb 22 07:31:37 EVENT START: node_up_local
Feb 22 07:31:38 EVENT COMPLETED: acquire_service_addr
Feb 22 07:31:39 EVENT START: get_disk_vg_fs lmpetvg
Feb 22 07:31:39 EVENT COMPLETED: get_disk_vg_fs lmpetvg
```

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feb 22 07:31:35</td>
<td>EVENT</td>
<td>START: fail_standby</td>
<td>140.186.100.189</td>
</tr>
<tr>
<td>Feb 22 07:31:35</td>
<td>EVENT</td>
<td>COMPLETED: fail_standby</td>
<td>140.186.100.189</td>
</tr>
<tr>
<td>Feb 22 07:31:36</td>
<td>EVENT</td>
<td>START: join_standby</td>
<td>140.186.100.189</td>
</tr>
<tr>
<td>Feb 22 07:31:36</td>
<td>EVENT</td>
<td>COMPLETED: join_standby</td>
<td>140.186.100.189</td>
</tr>
<tr>
<td>Feb 22 07:31:36</td>
<td>EVENT</td>
<td>START: node_up</td>
<td>2</td>
</tr>
<tr>
<td>Feb 22 07:31:37</td>
<td>EVENT</td>
<td>START: node_up_local</td>
<td></td>
</tr>
<tr>
<td>Feb 22 07:31:38</td>
<td>EVENT</td>
<td>COMPLETED: acquire_service_addr</td>
<td></td>
</tr>
<tr>
<td>Feb 22 07:31:39</td>
<td>EVENT</td>
<td>START: get_disk_vg_fs lmpetvg</td>
<td></td>
</tr>
<tr>
<td>Feb 22 07:31:39</td>
<td>EVENT</td>
<td>COMPLETED: get_disk_vg_fs lmpetvg</td>
<td></td>
</tr>
</tbody>
</table>

**Format of Cluster History Log Entries**

- **Date and Time Stamp**: The date and time the event occurred.
Examining Cluster Log Files

Understanding the /tmp/cm.log File

Viewing the Cluster History Log File

Because the cluster history log file is a standard text file, you can view its contents using standard AIX file commands, such as `cat`, `more`, and `tail`, or using the HAView utility through the NetView menu bar. For more information about using the HAView utility, see the Administration Guide.

Note that you cannot view the cluster history log file using SMIT or the `cldiag` utility.

Understanding the /tmp/cm.log File

The /tmp/cm.log file is a standard text file. This file is basically used for debugging purposes. As long as the cluster functions normally, you generally do not need to consult this file. But be aware that this file is overwritten every time cluster services are started, so you should be careful to make a copy of it before restarting cluster services on a failed node.

IBM Support personnel may ask you to turn on `clstrmgr` debug options for detailed information to help them understand a particular problem. With debugging turned on, this file may grow quickly. You should clean its contents frequently and turn debugging off in general.

Viewing the /tmp/cm.log File

To view the contents of this file, use standard AIX file commands, such as `cat`, `more`, and `tail`. You cannot view this log file using SMIT or the `cldiag` utility. Messages are formatted as they are for the `hacmp.out` file. (See Understanding the hacmp.out Log File.)

Sample Output of the /tmp/cm.log File Without Debug Options

Here is a sample of /tmp/cm.log output without debug options:

```
CLUSTER MANAGER STARTED
*** ADUP sally 140.186.30.115 (hb4) ***
Oct 12 14:18:48 EVENT START: node_up crusty
Oct 12 14:18:53 EVENT COMPLETED: node_up crusty
Oct 12 14:18:54 EVENT START: node_up_complete crusty
Oct 12 14:18:55 EVENT COMPLETED: node_up_complete crusty
Oct 12 14:18:59 EVENT START: node_up sally
Oct 12 14:19:01 EVENT COMPLETED: node_up sally
Oct 12 14:19:05 EVENT START: node_up_complete sally
Oct 12 14:19:06 EVENT COMPLETED: node_up_complete sally
*** ADDN crusty 140.186.30.164 (noHb214) ***
*** ADDN sally 140.186.38.115 (noHb810) ***
*** ADDN sally 140.186.39.115 (noHb811) ***
*** ADDN sally /dev/tmscsi0 (noHb82) ***
eating ADUP event for crusty_en0
Forwarding (3331 1 0 33554601) SYNCPOINT from navajo to sally
Forwarding (3331 1 0 33554602) NEW EVENT from navajo to sally
```
Sample Output of the /tmp/cm.log File with Debug Options

To enable `clstrmgr` debugging, use the following commands (specifying the options suggested by IBM Support personnel):

```
chssys -s clstrmgr -a"-d'evmgr,time,jil,jil2'"
```

**Empty**, The output contains the following level of detail:
```
handleGood searching for 0x0000019d from crusty
setid: serial = 0x0000019d, same = 0
setid: serial = 0x0000019e, same = 0
sending hb navajo_tr0 -> sally_tr0
SEND 33554847 140.186.38.9 140.186.38.115 121
==><SEND 33554847 140.186.38.9 140.186.38.115 121 000121 000053 3 1 3331 1 2 1
2 33554847 0 0 0 slowhb ARE YOU ALIVE> 1
bad network token1
handleBad searching for 0x0200019f
===<crusty /dev/tmscsi2 000121 000053 3 1 3331 0 1 0 1 16777577 0 0 0 slowhb ARE YOU ALIVE>
got name (crusty) and address (/dev/tmscsi2)
setid: serial = 0x0000019f, same = 0
setid: serial = 0x0000001a0, same = 0
sending hb navajo_tr1 -> sally_tr1
SEND 33554849 140.186.39.9 140.186.39.115 121
==><SEND 33554849 140.186.39.9 140.186.39.115 121 000121 000053 3 1 3331 1 2 1
2 33554849 0 0 0 slowhb I AM ALIVE> 1
setid: serial = 0x0000001a1, same = 0
setid: serial = 0x0000001a2, same = 0
sending hb navajo_tmscsi1 -> crusty_tmscsi2
SEND 419 /dev/tmscsi1 /dev/tmscsi2 116
==><SEND 419 /dev/tmscsi1 /dev/tmscsi2 116 000116 000048 3 1 3331 1 0 1 0 419 0
```

To disable the debug options and return the file to normal output mode, enter:
```
chssys -s clstrmgr -a ""
```

**Note:** You must stop and restart the `clstrmgr` to enable the changed option settings.

Understanding the cspoc.log File

The `/tmp/cspoc.log` file is a standard text file that resides on the source node, the node on which the C-SPOC command is invoked. Many error messages cascade from an underlying AIX error that usually indicates the problem source and success or failure status.

Format of Messages in the cspoc.log File

The entries in the `/tmp/cspoc.log` file use the following format:
Examining Cluster Log Files

Understanding the cspoc.log File

Format of cspoc.log File Entries

Each /tmp/cspoc.log entry contains a command delimiter to separate C-SPOC command output. This delimiter is followed by the first line of the command’s output, which contains arguments (parameters) passed to the command. Additionally, each entry contains the following information:

Date and Time stamp  The date and time the command was issued.

Node  The name of the node on which the command was executed.

Status  Text indicating the command’s success or failure. Command output that reports a failure also includes the command’s return code. No return code is generated for successful command completion. See Appendix A: HACMP Messages, for a description of each C-SPOC message.

Error Message  Text describing the actual error. The message is recorded in the Error message field. See Appendix A: HACMP Messages, for a description of each message.

Note that error messages generated as a result of standard C-SPOC validation are printed to stderr and to the /tmp/cspoc.log file.

Viewing the cspoc.log File

The /tmp/cspoc.log file is a standard text file that can be viewed in either of the following ways:

• Using standard AIX file commands, such as the more or tail commands
• Using the SMIT interface.

You cannot view this log file using the cldiag utility.
Using Standard AIX File Commands to View cspoc.log

Standard AIX file commands, such as the `more` or `tail` commands, let you view the contents of the `/tmp/cspoc.log` file. See the `more` or `tail` man pages for information on using these commands.

Using the SMIT Interface to View cspoc.log

To view the `/tmp/cspoc.log` file using SMIT:

1. Type `smit hacmp`
2. Select `RAS Support > View HACMP Log Files > Scan the C-SPOC System Log File`. This option references the `/tmp/cspoc.log` file.

   Note: You can choose to either `scan` the contents of the `/tmp/cspoc.log` file as it exists, or you can `watch` an active log file as new events are appended to it in real time. Typically, you scan the file to try to find a problem that has already occurred; you watch the file while duplicating a problem to help determine its cause, or as you test a solution to a problem to determine the results.

Understanding the `/tmp/emuhacmp.out` File

The `/tmp/emuhacmp.out` file is a standard text file that resides on the node from which the HACMP Event Emulator was invoked. The file contains information from log files generated by the Event Emulator on all nodes in the cluster. When the emulation is complete, the information in these files is transferred to the `/tmp/emuhacmp.out` file on the node from which the emulation was invoked, and all other files are deleted.

Using the `EMUL_OUTPUT` environment variable, you can specify another name and location for this output file. The format of the file does not change.

Format of Messages in the `/tmp/emuhacmp.out` File

The entries in the `/tmp/emuhacmp.log` file use the following format:

```
**********************************************************************
******************START OF EMULATION FOR NODE buzzcut***************
**********************************************************************

Jul 21 17:17:21 EVENT START: node_down buzzcut graceful
+ [ buzzcut = buzzcut -a graceful = forced ]
+ [ EMUL = EMUL ]
+ cl_echo 3020 NOTICE >>>> The following command was not executed <<<< 

NOTICE >>>> The following command was not executed <<<<
+ echo /usr/sbin/cluster/events/utils/cl_ssa_fence down buzzcut
/usr/sbin/cluster/events/utils/cl_ssa_fence down buzzcut graceful

+ [ 0 -ne 0 ]
+ [ EMUL = EMUL ]
+ cl_echo 3020 NOTICE >>>> The following command was not executed <<<< 

NOTICE >>>> The following command was not executed <<<<
+ echo /usr/sbin/cluster/events/utils/cl_ssa_fence down buzzcut graceful
/usr/sbin/cluster/events/utils/cl_ssa_fence down buzzcut graceful
```
Examining Cluster Log Files
Understanding the /tmp/emuhacmp.out File

The output of emulated events is presented as in the /tmp/hacmp.out file described earlier in this chapter. The /tmp/emuhacmp.out file also contains the following information:

Header
Each node’s output begins with a header that signifies the start of the emulation and the node from which the output is received.

Notice
The Notice field identifies the name and path of commands or scripts that are echoed only. If the command being echoed is a customized script, such as a pre- or post-event script, the contents of the script are displayed. Syntax errors in the script are also listed.

ERROR
The error field contains a statement indicating the type of error and the name of the script in which the error was discovered.

Footer
Each node’s output ends with a footer that signifies the end of the emulation and the node from which the output is received.

Viewing the /tmp/emuhacmp.out File
You can view the /tmp/emuhacmp.out file using standard AIX file commands, such as the more or tail commands. You cannot view this log file using the cldiag utility or the SMIT interface.

Using Standard AIX File Commands
Standard AIX file commands, such as the more or tail commands, let you view the contents of the /tmp/emuhacmp.out file. See the more or tail man pages for information on using these commands.
Chapter 3: Investigating System Components

This chapter describes how to investigate system components using HACMP and AIX utilities and commands.

Overview

If your examination of the cluster log files does not reveal the source of a problem, you must investigate each system component using a top-down strategy to move through the layers. You should investigate the components in the following order:

1. Application layer
2. HACMP layer
3. Logical Volume Manager layer
4. TCP/IP layer
5. AIX layer
6. Physical network layer
7. Physical disk layer
8. System hardware layer.

The following sections describe what you should look for when examining each layer. They also briefly describe the tools you should use to examine the layers. For additional information about a tool described in this chapter, see the appropriate HACMP or AIX documentation.

Keep in mind that effective troubleshooting requires a methodical approach to solving a problem. Be sure to read Chapter 1: Diagnosing the Problem, for a recommended approach to debugging a cluster before using the tools described in this chapter.

Checking Highly Available Applications

As a first step to finding problems affecting a cluster, check each highly available application running on the cluster. Examine any application-specific log files and perform any troubleshooting procedures recommended in the application’s documentation. In addition, check the following:

- Do some simple tests. For a database application, for example, try to add and delete a record.
- Use the `ps` command to check that the necessary processes are running, or to verify that the processes were stopped properly.
- Check the resources that the application expects to be present to ensure that they are available; for example, filesystems and volume groups.
Checking the HACMP Layer

If checking the application layer does not reveal the source of a problem, check the HACMP layer next. The two main areas to investigate are:

- HACMP components and required files
- Cluster topology and configuration.

The following sections describe how to investigate these problems.

Note: These steps assume that you have checked the log files and that they do not point to the problem.

Checking HACMP Components

An HACMP cluster is made up of several required files and daemons. The following sections describe what to check for in the HACMP layer.

Checking HACMP Required Files

Make sure that the HACMP files required for your cluster are in the proper place, have the proper permissions (readable and executable), and are not zero length. The HACMP files and the AIX files modified by the HACMP software are listed in the README file that accompanies the product.

Checking Cluster Services and Processes

Check the status of the following HACMP daemons:

- The Cluster Manager (clstrmgr) daemon
- The Cluster Information Program (clinfo) daemon
- The Cluster SMUX Peer (clsmuxpd) daemon
- The Cluster Lock Manager (cllockd) daemon.

Use the /usr/sbin/cluster/utilities/clm_stats command for current information about the number of locks, resources, and amount of memory usage. See the Administration Guide for more information.

When these components are not responding normally, use the lssrc command or the options on the SMIT Show Cluster Services screen on a cluster node to determine if the daemons are active.

For example, to check on the status of all daemons under the control of the SRC, enter:

```
    lssrc -a | grep active
```

```
infod     infod     5703   active
hcon      system    5963   active
syslogd   ras       6500   active
portmap   portmap   7017   active
clinfo    cluster   8053   active
clstrmgr  cluster   8310   active
cllockd   lock      9354   active
sendmail  mail      5038   active
inetd     tcpip     7605   active
```
To check on the status of all cluster daemons under the control of the SRC, enter:
```
lssrc -g cluster
```

**Note:** When you use the `-g` flag with the `lssrc` command, the status information does not include the status of subsystems if they are inactive. If you need this information, use the `-a` flag instead. For more information on the `lssrc` command, see the man page.

To determine whether the Cluster Manager is running, or if processes started by the Cluster Manager are currently running on a node, use the `ps` command.

For example, to determine whether the `clstrmgr` daemon is running, enter:
```
ps -ef | grep clstrmgr
```
```
root 18363  3346  3 11:02:05    -  10:20 /usr/sbin/cluster/clstrmgr
root 19028  19559 2 16:20:04 pts/10  0:00 grep clstrmgr
```
See the `ps` man page for more information on using this command.

### Obtaining More Detailed Information About Cluster Services

Using the `cldiag` utility, you can obtain low-level information about the following HACMP daemons: Cluster Manager and Cluster Lock Manager.

Using the `debug` option of the `cldiag` utility, you can activate Cluster Manager debug mode. In debug mode, the Cluster Manager reports at a very detailed level on its internal processing. You can determine the level of detail provided. At a minimum, in debug mode the Cluster Manager reports on the keepalive message activity among cluster nodes. At its most detailed, this debug information reports each step of Cluster Manager processing, including system calls.

When you use the `cldiag` utility `debug` option with the Cluster Lock Manager, you are not turning on debug mode. Instead, the debug option causes the Cluster Lock Manager to write the contents of its internal lock resource table and lock table to a file. The information contained in these tables can be useful when a lock that an application expects to receive is not granted. By examining the lock resource and lock tables, you can compare the current state of granted and blocked locks in the Cluster Lock Manager with what the application expects and uncover the source of the mismatch.

To obtain this information using the `cldiag` utility, you must include the `/usr/sbin/cluster/diag` directory in your PATH environment variable. Then to run the utility from any directory:

Start by entering:
```
cldiag
```

The utility returns a list of options and the `cldiag` prompt:
```
-------------------------------------------------------
To get help on a specific option, type: help <option>
To return to previous menu, type: back
To quit the program, type: quit
-------------------------------------------------------
valid options are:
  debug
```
The `cldiag` utility `help` subcommand provides a brief synopsis of the syntax of the option specified. For more information about the command syntax, see the `cldiag` man page.

To access these debug tools, enter the `debug` option at the `cldiag` prompt, as in the following example:
```
cldiag> debug
```

The `cldiag` utility returns a list of options and the prompt. Note that the prompt changes to indicate previous selections.
```
valid options are:
c1strmger
c1lockd
c1diag.debug>
```

To activate Cluster Manager debug mode, see step 3. To obtain a listing of the Cluster Lock Manager’s lock resource table, go to step 4.

To activate Cluster Manager debug mode, enter the `clstrmgr` option.

By default, the `cldiag` utility writes the debug information to `stdout` until you terminate the output by pressing CTRL-C. Using the flags associated with the `clstrmgr` option (as described in the following table), you can specify the level of detail included in the debug output, or whether the debug option should be turned off. You also can specify (optionally) an output filename for storing debug information. If you do not specify a file, the information is written to `/tmp/clstrmgr.debug` by default.

<table>
<thead>
<tr>
<th>Flag</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-l level</code></td>
<td>Specifies the level of detail provided in debug messages. You specify the level as a number between 0 and 9. Each level includes a different subset of Cluster Manager messages. The higher numbers specify greater detail and include all previous levels.</td>
</tr>
<tr>
<td><code>level 0</code></td>
<td>Turns off debug mode. This is the default level. The Cluster Manager still reports all state changes to the console and to all cluster logs.</td>
</tr>
<tr>
<td><code>level 1</code></td>
<td>Includes important information about Cluster Manager activity and provides information about the Event Manager, event interfaces, IPC modules, and timestamps.</td>
</tr>
<tr>
<td><code>level 2</code></td>
<td>Includes membership protocol and syncpoint facility information.</td>
</tr>
<tr>
<td><code>level 3</code></td>
<td>Includes inbound and outbound message information.</td>
</tr>
<tr>
<td><code>level 4</code></td>
<td>Includes network interface module (nim) information.</td>
</tr>
<tr>
<td><code>level 5</code></td>
<td>Includes heartbeat information.</td>
</tr>
<tr>
<td><code>level 6</code></td>
<td>Includes cluster node map and debug module information.</td>
</tr>
</tbody>
</table>
The following `cldiag` entry activates Cluster Manager debugging, requesting level 1 detail and specifying `cm_debug.out` as the output file:

```
clstrmgr
cllockd
cldiag.debug> clstrmgr -l 1 -R cm_debug.out
```

The following example illustrates a fragment of the debug information generated by the Cluster Manager in response to this command.

```
Turning debugging ON (level 1) (Wed Apr 19 11:41:26 1999).
trott: Adding type TE_JOIN_NODE event, node = 0, net = -1
eventize_event: Called with event TE_UNSTABLE.
eventize_event: Logging event (TE_UNSTABLE)
trott: got "node_up bass" event from bass

trott: Adding type TE_JOIN_NODE event, node = 0, net = -1
trott: duplicate event
*** ADUP bass 140.186.38.173 (hb3) ***
*** ADUP bass 140.186.39.229 (hb2) ***
*** ADUP bass 140.186.30.229 (hb2) ***
*** ADUP bass 140.186.31.173 (hb3) ***
*** ADUP bass /dev/tmscsi0 (hb2) ***
Performing event rollup.
trott: Getting type TE_JOIN_NODE event, node = 0, net = -1
>>> type TE_JOIN_NODE, node 0, network -1
trott: casting vote for 7 "node_up bass"
trott: bass votes for 7 "node_up bass"
trott: Adding type TE_JOIN_NODE event, node = 0, net = -1
trott: duplicate event
trott: got "join_adapter bass share_en3" event from bass

trott: Adding type TE_JOIN_ADAPTER event, node = 0, net = 3
trott: got "fail_adapter bass bass_boot" event from bass

trott: Process TE_JOIN_NODE_COMPLETE event, node = 0, net = -1
eventize_event: Called with event TE_JOIN_NODE_COMPLETE.
eventize_event: Submitting event (node_up_complete)
eventize_event: Submitted event (node_up_complete)
eventize_event: Logging event (TE_JOIN_NODE_COMPLETE)
Rollup fail_adapter bass bass_boot

trott: Completed TE_JOIN_NODE_COMPLETE event, node = 0, net = -1
Performing event rollup.
Get event: EM_NO_ACTIVE_EVENT
clearing event queue

eventize_event: Called with event TE_STABLE.
eventize_event: Logging event (TE_STABLE)
eventize_event: Called with event TE_NEW_PRIMARY.
eventize_event: Logging event (TE_NEW_PRIMARY)
*** ADDN bass 140.186.30.229 (noHb25) ***
```
Investigating System Components
Checking the HACMP Layer


Now, to obtain a listing of the Cluster Lock Manager's lock resource table, enter the `clclockd` subcommand.

By default, the `cldiag` utility writes the lock information to `/tmp/lockdump`. Using the `-R` flag, you optionally can redirect the lock information to the specified file.

The following example obtains a listing of the lock resource table and stores the output in the file named `lock_resources.out`:

```
clstrmgr
clclockd

cldiag.debug> clclockd -R lock_resources.out
```

The following fragment illustrates the type of lock information obtained using the `cldiag` utility:

```
DUMPING CLIENT TABLE
DUMPING GROUP TABLE
DUMPING RESOURCE TABLE
Global migration tuning parameters: event queue length=20
        decay rate=3f
TOTAL LOCKS IN RESOURCE TABLE: 0
TOTAL LOCKS IN UNIX FREELIST: 0
TOTAL LOCKS IN VMS FREELIST: 0
TOTAL RESOURCES: 0
TOTAL RESOURCES ON FREELIST: 0
TIMEOUT QUEUE DUMP
REMOTE LOCKID MAP TABLE
TOTAL TRANSACTION BUFFERS ON FREELIST: 0
Allocated transaction dump: 0x0

Total ASTs: 0
RLDB DUMP:
  0 allocated  0 directory 0 free
    0 total in table
Allocated block dump: 0x0
```

Checking for Cluster Configuration Problems

For an HACMP cluster to function properly, all the nodes in the cluster must agree on the cluster topology, network configuration, and ownership and takeover of HACMP resources. This information is stored in the ODM on each cluster node.

To begin checking for configuration problems, ask yourself if you (or others) have made any recent changes that may have disrupted the system? Have components been added or deleted? Has new software been loaded on the machine? Have new PTFs or application updates been
performed? Has a system backup been restored? Then run the `/usr/sbin/cluster/diag/clverify` utility described in the *Administration Guide* to verify that the proper HACMP-specific modifications to AIX software are in place and that the cluster configuration is valid.

The `clverify` utility can check many aspects of a cluster configuration and can report any inconsistencies. Using the `clverify` utility, you can perform the following tasks:

- Verify that all cluster nodes contain the same cluster topology information
- Check that all adapters and tty lines are properly configured, and that shared disks are accessible to all nodes that can own them
- Check each cluster node to determine whether multiple RS232 serial networks exist on the same tty device
- Check for agreement among all nodes on the ownership of defined resources, such as filesystems, log files, volume groups, disks, and application servers
- Check for invalid characters in cluster names, node names, network names, adapter names and resource group names
- Verify takeover information.

The `clverify` utility will also print out diagnostic information about the following:

- Custom snapshot methods
- Custom verification methods
- Custom pre/post events
- Cluster log file redirection.

If you have configured Kerberos on your system, the `clverify` utility also determines that:

- All IP labels listed in the configuration have the appropriate service principals in the `.klogin` file on each node in the cluster
- All nodes have the proper service principals
- Kerberos is installed on all nodes in the cluster
- All nodes have the same security mode setting.

You can use the `clverify` utility from SMIT or from the command line. From the main HACMP SMIT screen, select *Cluster Configuration > Cluster Verification > Verify Cluster Topology, Resources*, or *all*. If you find a configuration problem, you can issue the `clverify cluster topology sync` subcommand from the command line to propagate the correct cluster definitions from the local node to other cluster nodes.

**Note:** The local node should have the correct ODM definitions before you attempt to synchronize the cluster topology. Also, if a shared volume group is set to `autovaryon` or if a stop script is missing, a topology synchronization will not help to resolve the configuration problem.

For more information about using the `clverify` utility, see the *Administration Guide* and the man page.

If you do not want to use the `clverify` utility, you can gather additional information about the cluster configuration using the `ls -lt /etc|head -40` command to list the most recent changes to the `/etc` directory. You also can use this command in the `/usr/sbin/cluster` and application directories.
If using either the `clverify` utility or the `ls -lt /etc|head -40` command does not uncover recent changes that may have disrupted the cluster, check the cluster configuration information on each node.

To check this information, from the main HACMP SMIT screen, select **Cluster Configuration > Cluster Topology > Show Cluster Topology**. From there you can choose to view the cluster topology information, such as the adapters and network connections, in any of several ways. To view the cluster resource configuration information, such as volume group definitions, from the main HACMP SMIT screen, select **Cluster Configuration > Cluster Resources > Show Cluster Resources**.

**Note:** If cluster configuration problems arise after running the `clverify` utility, do not run C-SPOC commands in this environment as they may fail to execute on cluster nodes.

### Checking a Cluster Snapshot File

The HACMP cluster snapshot facility (`/usr/sbin/cluster/utilities/clsnapshots`) allows you to save in a file a record of all the data that defines a particular cluster configuration. It also allows you to create your own custom snapshot methods to save additional information important to your configuration. You can use this snapshot for troubleshooting cluster problems. The default directory path for storage and retrieval of a snapshot is `/usr/sbin/cluster/snapshots`.

Note that you cannot use the cluster snapshot facility in a cluster which is running different versions of HACMP concurrently.

For information on how to create and apply cluster snapshots, see the chapter on saving and restoring cluster configurations in the *Administration Guide*.

### Information Saved in a Cluster Snapshot

The primary information saved in a cluster snapshot is the data stored in the HACMP/ES ODM classes (such as HACMPcluster, HACMPnode, HACMPnetwork, HACMPdaemons). This is the information used to recreate the cluster configuration when a cluster snapshot is applied.

The cluster snapshot does not save any user-customized scripts, applications, or other non-HACMP configuration parameters. For example, the name of an application server and the location of its start and stop scripts are stored in the HACMPserver ODM object class. However, the scripts themselves as well as any applications they may call are not saved.

The cluster snapshot does not save any device- or configuration-specific data that is outside the scope of HACMP. For instance, the facility saves the names of shared filesystems and volume groups; however, other details, such as NFS options or LVM mirroring configuration are not saved.

In addition to this ODM data, a cluster snapshot also includes output generated by various HACMP and standard AIX commands and utilities. This data includes the current state of the cluster, node, network, and adapters as viewed by each cluster node, as well as the state of any running HACMP daemons.

The cluster snapshot includes output from the following commands:

- `cllscf`
- `df`
- `lsfs`
- `netstat`
Because the cluster snapshot facility is a shell script that can be edited, you can add commands to obtain site-specific information. This is not a recommended practice, however, because any local modifications you make may create incompatibilities with future snapshots.

Note: Be aware that sticky location markers specified during earlier dynamic reconfigurations may be present in the snapshot. For information on locating and removing these markers while the cluster is down, see the section on DARE Resource Migration in the Administration Guide.

Cluster Snapshot Files

The cluster snapshot facility stores the data it saves in two separate files, the ODM data file and the Cluster State Information File, each displaying information in three sections

ODM Data File (.odm)
This file contains all the data stored in the HACMP ODM object classes for the cluster. This file is given a user-defined basename with the .odm file extension. Because the ODM information must be largely the same on every cluster node, the cluster snapshot saves the values from only one node. The cluster snapshot ODM data file is an ASCII text file divided into three delimited sections:

Version section
This section identifies the version of the cluster snapshot. The characters <VER identify the start of this section; the characters </VER identify the end of this section. The version number is set by the cluster snapshot software.

Description section
This section contains user-defined text that describes the cluster snapshot. You can specify up to 255 characters of descriptive text. The characters <DSC identify the start of this section; the characters </DSC identify the end of this section.

ODM data section
This section contains the HACMP ODM object classes in generic AIX ODM stanza format. The characters <ODM identify the start of this section; the characters </ODM identify the end of this section.

The following is an excerpt from a sample cluster snapshot ODM data file showing some of the ODM stanzas that are saved:

```xml
<VER
1.0
</VER

<DSC
My Cluster Snapshot
</DSC
```
Investigating System Components
Checking the HACMP Layer

<ODM

HACMPcluster:
  id = 97531
  name = "Breeze1"
  nodename = "mynode"
  sec_level = "Standard"
  last_node_ids = "2,3"
  highest_node_id = 3
  last_network_ids = "3,6"
  highest_network_id = 6
  last_site_ids = 
  highest_site_id = 0
  handle = 3
  cluster_version = 5
  reserved1 = 0
  reserved2 = 0
  wlm_subdir = " "

HACMPnode:
  name = "mynode"
  object = "VERBOSE_LOGGING"
  value = "high"

</ODM

Cluster State Information File (.info)
This file contains the output from standard AIX and HACMP system management commands. This file is given the same user-defined basename with the .info file extension. If you defined custom snapshot methods, the output from them is appended to this file. The Cluster State Information file contains three sections:

Version section
This section identifies the version of the cluster snapshot. The characters <VER identify the start of this section; the characters </VER identify the end of this section. This section is set by the cluster snapshot software.

Description section
This section contains user-defined text that describes the cluster snapshot. You can specify up to 255 characters of descriptive text. The characters <DSC identify the start of this section; the characters </DSC identify the end of this section.

Command output section
This section contains the output generated by AIX and HACMP ODM commands. This section lists the commands executed and their associated output. This section is not delimited in any way.

The following is an excerpt from a sample Cluster State Information (.info) file:

<VER
1.0
</VER

<DSC
My cluster snapshot
</DSC
=========================================
COMMAND: cllscf
Cluster Description of Cluster BVT_Cluster
Cluster ID: 89
Cluster Security Level Standard
There were 2 networks defined: en0, tr0
There are 2 nodes in this cluster

NODE mynode:
    This node has 1 service interface(s):

    Service Interface mynode:
        IP address: 10.50.14.53
        Hardware Address:
        Network: en0
        Attribute: public
        Aliased Address?: Disable

    (INVALID) Service Interface mynode has no boot interfaces
    Service Interface mynode has no standby interfaces

Breakdown of network connections:
Connections to network en0
    Node mynode is connected to network en0 by these interfaces:
        mynode

COMMAND: cllsnw

COMMAND: cllsif

COMMAND: clshowres

Resource Group Name cas1
Node Relationship cascading
Participating Node Name(s) mynode
Node Priority
Service IP Label mynode_trsvc
Filesystems ALL
Filesystems Consistency Check fsck
Filesystems Recovery Method sequential
Filesystems/Directories to be exported
Filesystems to be NFS mounted /jj1
Network For NFS Mount
Volume Groups vg1
Concurrent Volume Groups
Disks
AIX Connections Services
AIX Fast Connect Services
Shared Tape Resources
Application Servers
Highly Available Communication Links
Miscellaneous Data
Auto Discover/Import of Volume Groups false
Inactive Takeover false
Cascading Without Fallback false
SSA Disk Fencing false
Filesystems mounted before IP configured false

The following information is retrieved from a node:

mynode

===============================================

---------- COMMAND: /usr/bin/netstat -i
Name Mtu Network Address Ipkts Ierrs Opkts Oerrs Coll
lo0 16896 <Link> 29125 0 29277 0 0
lo0 16896 127 loopback 29125 0 29277 0 0
en0 1500 <Link> 8.0.5a.d.97.b9 567398 0 85485 0 0
en0 1500 140.186.100 mynode 567398 0 85485 0 0

---------- COMMAND: /usr/bin/netstat -in
Name Mtu Network Address Ipkts Ierrs Opkts Oerrs Coll
lo0 16896 <Link> 29126 0 29278 0 0
lo0 16896 127 8.0.0.0.1 29126 0 29278 0 0
en0 1500 <Link> 8.0.5a.d.97.b9 567398 0 85485 0 0
en0 1500 140.186.100.80 140.186.100.80 567398 0 85485 0 0

---------- COMMAND: /usr/sbin/no -a

---------- thewall = 16384
sb_max = 65536
net_malloc_police = 0
rto_low = 1
rto_high = 64
rto_limit = 7
rto_length = 13
arptab_bsz = 7
arptab_nb = 25
tcp_ndebug = 100
ifsize = 8
subnetsarelocal = 0
maxttl = 255
ipfragttl = 60
ipsendredirects = 1
ipforwarding = 0
udp_ttl = 30
tcp_ttl = 60
arpt_killc = 20
tcp_sendspace = 16384
tcp_recvspace = 16384
udp_sendspace = 9216
udp_recvspace = 41600
rfc1122addrchk = 0
nonlocsrcroute = 0
tcp_keepintvl = 150
tcp_keepid = 14400
bcastping = 0
udpcsum = 1
tcp_mssdfilt = 512
icmpaddressmask = 0
tcp_keepinit = 150
ie5_old_multicast_mapping = 0
rfc1323 = 0
ipqmaxlen = 100
directed_broadcast = 1

---------- COMMAND: /usr/sbin/lsdev -Cc if
en0 Available Standard Ethernet Network Interface
Checking the Logical Volume Manager

When troubleshooting an HACMP cluster, you need to check the following LVM entities:

- Volume groups
- Physical volumes
- Logical volumes
- Filesystems.

Checking Volume Group Definitions

Check to make sure that all shared volume groups in the cluster are active on the correct node. If a volume group is not active, vary it on using the appropriate command for your configuration. The volume group should be running if cluster services are running.

Compare the list of active volume groups with the list of disks specified in the Volume Groups or Concurrent Volume Groups field on the HACMP SMIT Show Cluster Resources screen to see if any discrepancies exist.

Using the lsvg Command to Check Volume Groups

To check for inconsistencies among volume group definitions on cluster nodes, use the lsvg command as follows to display information about the volume groups defined on each node in the cluster:

```
lsvg
```

The system returns volume group information similar to the following:

```
rootvg
datavg
```
To list only the active (varied on) volume groups in the system, use the `lsvg -o` command as follows:

```
lsvg -o
```

The system returns volume group information similar to the following:

```
rootvg
```

To list all logical volumes in the volume group, use the `lsvg -l` command and specify the volume group name as shown in the following example:

```
lsvg -l rootvg
```

If you are running the C-SPOC utility, use the `cl_lsvg` command to display information about shared volume groups in your cluster.

**Using the cldiag Utility to Check Volume Groups**

You can also check for inconsistencies in volume group definitions among the cluster nodes by using the `cldiag` utility. To check for inconsistencies using the `cldiag` utility, you must include the `/usr/sbin/cluster/diag` directory in your PATH environment variable. Then to run the utility from any directory, enter:

```
cldiag
```

The system displays the following:

```
-------------------------------------------------------
To get help on a specific option, type: help <option>
To return to previous menu, type: back
To quit the program, type: quit
-------------------------------------------------------
valid options are:
debug
logs
vgs
error
trace
```

```
cldiag>
```

The `help` option provides a brief synopsis of the syntax of the option specified. For more information about the command syntax, see the `cldiag` man page.

The C-SPOC utility is not supported with the `cldiag` utility.

To check volume definitions, enter the `vgs` option at the `cldiag` prompt, specifying the `-h` flag with the names of at least two nodes, and no more than four nodes, on which you want to compare volume group definitions. Separate the node names by commas. You optionally can use the `-v` flag to specify the names of the volume groups you want checked. If you do not specify volume group names, the `cldiag` utility checks the definitions of only those volume groups that are shared by all the nodes specified.

The following example checks the definition of volume groups named `sharedvg1` and `sharedvg2` on nodes `port`, `starboard`, and `rudder`:

```
cldiag vgs -h port,starboard,rudder -v sharedvg1,sharedvg2
```
Note: vgs Can Cause cldiag to Exit Prematurely
Occasionally, using the vgs option causes the utility to exit prematurely. If you want to check
the consistency of volume group, logical volume, and filesystem information among nodes, and
you encounter this problem, run the clverify routine instead, using SMIT or the command line.
For more information about running clverify, see Checking for Cluster Configuration Problems
and the chapter on verifying cluster configuration in the Administration Guide.

Using the C-SPOC Utility to Check Shared Volume Groups
To check for inconsistencies among volume group definitions on cluster nodes in a two-node
C-SPOC environment:
1. Enter the following fastpath: smitty cl_admin
2. Select the Cluster Logical Volume Manager.
3. Select List All Shared Volume Groups and press Enter to accept the default (no). A list
   of all shared volume groups in the C-SPOC environment appears.
You can also use the C-SPOC cl_lsvg command from the command line to display this
information.

Checking Physical Volumes
To check for discrepancies in the physical volumes defined on each node, obtain a list of all
physical volumes known to the systems and compare this list against the list of disks specified
in the Disks field of the Command Status screen. Access the Command Status screen through
the SMIT Show Cluster Resources screen.
To obtain a list of all the physical volumes known to a node and to find out the volume groups
to which they belong, use the lspv command. If you do not specify the name of a volume group
as an argument, the lspv command displays every known physical volume in the system
assigned to a specific node. For example:

```
lspv
hdisk0      0000914312e971a   rootvg
hdisk1      00000132a78e213   rootvg
hdisk2      00000902a78e21a   datavg
hdisk3      00000321358e354   datavg
```
The first column of the display shows the logical name of the disk. The second column lists the
physical volume identifier of the disk. The third column lists the volume group (if any) to which
it belongs.

Note that on each cluster node, AIX can assign different names to the same physical volume.
To tell which names correspond to the same physical volume, compare the physical volume
identifiers listed on each node.

If you specify the logical device name of a physical volume (hdiskx) as an argument to the lspv
command, it displays information about the physical volume, including whether it is active
(varied on). For example:

```
lspv hdisk2
PHYSICAL VOLUME:   hdisk2              VOLUME GROUP:   abalonevg
PV IDENTIFIER:      0000301919439ba5    VG IDENTIFIER: 00003019460f63c7
PV STATE:           active              VG STATE:      active/complete
STALE PARTITIONS:   0                   ALLOCATABLE:       yes
PP SIZE:            4 megabyte(s)       LOGICAL VOLUMES:   2
```
If a physical volume is inactive (not varied on, as indicated by question marks in the PV STATE field), use the appropriate command for your configuration to vary on the volume group containing the physical volume. Before doing so, however, you may want to check the system error report to determine whether a disk problem exists. Enter the following command to check the system error report:

erpt -a | more

You can also use the `lsdev` command to check the availability or status of all physical volumes known to the system. For example:

`lsdev -Cc disk`

produces the following output:

<table>
<thead>
<tr>
<th>name</th>
<th>status</th>
<th>location</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hdisk0</td>
<td>Available</td>
<td>00-07-00-00</td>
<td>2.0 GB SCSI Disk Drive</td>
</tr>
<tr>
<td>hdisk1</td>
<td>Available</td>
<td>00-07-00-10</td>
<td>2.0 GB SCSI Disk Drive</td>
</tr>
<tr>
<td>hdisk2</td>
<td>Available</td>
<td>00-07-00-20</td>
<td>2.0 GB SCSI Disk Drive</td>
</tr>
</tbody>
</table>

Output of `lsdev -Cc disk`

### Checking Logical Volumes

To check the state of logical volumes defined on the physical volumes, use the `lspv -l` command and specify the logical name of the disk to be checked. As shown in the following example, you can use this command to determine the names of the logical volumes defined on a physical volume:

`lsvg -l rootvg` or `lspv -l hdisk2`

<table>
<thead>
<tr>
<th>LV NAME</th>
<th>LPs</th>
<th>PPs</th>
<th>DISTRIBUTION</th>
<th>MOUNT POINT</th>
</tr>
</thead>
<tbody>
<tr>
<td>lv02</td>
<td>50</td>
<td>50</td>
<td>25..00..00..00..25</td>
<td>/usr</td>
</tr>
<tr>
<td>lv04</td>
<td>44</td>
<td>44</td>
<td>06..00..00..32..06</td>
<td>/clusterfs</td>
</tr>
</tbody>
</table>

Use the `lslv logicalvolume` command to display information about the state (opened or closed) of a specific logical volume, as indicated in the LV STATE field. For example:

`lslv abalonelv`

<table>
<thead>
<tr>
<th>LOGICAL VOLUME:</th>
<th>abalonelv</th>
<th>VOLUME GROUP:</th>
<th>abalonevg</th>
</tr>
</thead>
<tbody>
<tr>
<td>LV IDENTIFIER:</td>
<td>00003019460f63c7.1</td>
<td>PERMISSION:</td>
<td>read/write</td>
</tr>
<tr>
<td>VG STATE:</td>
<td>active/complete</td>
<td>LV STATE:</td>
<td>opened/syncd</td>
</tr>
<tr>
<td>TYPE:</td>
<td>jfs</td>
<td>WRITE VERIFY:</td>
<td>off</td>
</tr>
<tr>
<td>MAX LPs:</td>
<td>128</td>
<td>PP SIZE:</td>
<td>4 megabyte(s)</td>
</tr>
<tr>
<td>COPIES:</td>
<td>1</td>
<td>SCHED POLICY:</td>
<td>parallel</td>
</tr>
<tr>
<td>LPs:</td>
<td>10</td>
<td>PPs:</td>
<td>10</td>
</tr>
<tr>
<td>STALE PPs:</td>
<td>0</td>
<td>BB POLICY:</td>
<td>relocatable</td>
</tr>
<tr>
<td>INTER-POLICY:</td>
<td>minimum</td>
<td>RELOCATABLE:</td>
<td>yes</td>
</tr>
<tr>
<td>INTRA-POLICY:</td>
<td>middle</td>
<td>UPPER BOUND:</td>
<td>32</td>
</tr>
<tr>
<td>MOUNT POINT:</td>
<td>/abalonefs</td>
<td>LABEL:</td>
<td>/abalonefs</td>
</tr>
<tr>
<td>MIRROR WRITE CONSISTENCY:</td>
<td>on</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

TOTAL PPs: 203 (812 megabytes) VG DESCRIPTORS: 2
FREE PPs: 192 (768 megabytes)
USED PPs: 11 (44 megabytes)
FREE DISTRIBUTION: 41..30..40..40..41
USED DISTRIBUTION: 00..11..00..00..00
If a logical volume state is inactive (or closed, as indicated in the LV STATE field), use the appropriate command for your configuration to vary on the volume group containing the logical volume.

### Using the C-SPOC Utility to Check Shared Logical Volumes

To check the state of shared logical volumes on cluster nodes in a two-node C-SPOC environment:

1. Enter the following fastpath: `smitty cl_admin`
2. Select `Cluster Logical Volume Manager > Shared Logical Volumes > List All Shared Logical Volumes by Volume Group`. A list of all shared logical volumes appears.

You can also use the C-SPOC `cl_lsv` command from the command line to display this information.

### Checking Filesystems

Check to see if the necessary filesystems are mounted and where they are mounted. Compare this information against the HACMP definitions for any differences. Check the permissions of the filesystems and the amount of space available on a filesystem.

Use the following commands to obtain this information about filesystems:

- The `mount` command
- The `df` command
- The `lsfs` command.

Use the `cl_lsfs` command to list filesystem information when running the C-SPOC utility.

### Obtaining a List of Filesystems

Use the `mount` command to list all the filesystems, both JFS and NFS, currently mounted on a system and their mount points. For example:

```
mount
```

<table>
<thead>
<tr>
<th>node</th>
<th>mounted</th>
<th>mounted over</th>
<th>vfsdate</th>
<th>options</th>
</tr>
</thead>
<tbody>
<tr>
<td>/dev/hd4</td>
<td>/</td>
<td>jfsOct 06 09:48</td>
<td>rw,log=/dev/hd8</td>
<td></td>
</tr>
<tr>
<td>/dev/hd2</td>
<td>/usr</td>
<td>jfsOct 06 09:48</td>
<td>rw,log=/dev/hd8</td>
<td></td>
</tr>
<tr>
<td>/dev/hd9var</td>
<td>/var</td>
<td>jfsOct 06 09:48</td>
<td>rw,log=/dev/hd8</td>
<td></td>
</tr>
<tr>
<td>/dev/hd3</td>
<td>/tmp</td>
<td>jfsOct 06 09:49</td>
<td>rw,log=/dev/hd8</td>
<td></td>
</tr>
<tr>
<td>/dev/hd1</td>
<td>/home</td>
<td>jfsOct 06 09:50</td>
<td>rw,log=/dev/hd8</td>
<td></td>
</tr>
<tr>
<td>pearl</td>
<td>/home</td>
<td>nfsOct 07 09:59</td>
<td>rw,soft,bg,intr</td>
<td></td>
</tr>
<tr>
<td>jade</td>
<td>/usr/local</td>
<td>nfsOct 07 09:59</td>
<td>rw,soft,bg,intr</td>
<td></td>
</tr>
</tbody>
</table>

Determine whether and where the filesystem is mounted, then compare this information against the HACMP definitions to note any differences.

### Checking Available Filesystem Space

To see the space available on a filesystem, use the `df` command. For example:

```
df
```
Investigating System Components
Checking the Logical Volume Manager

<table>
<thead>
<tr>
<th>Filesystem</th>
<th>Total KB</th>
<th>free</th>
<th>%used</th>
<th>iused</th>
<th>%iused</th>
<th>Mounted on</th>
</tr>
</thead>
<tbody>
<tr>
<td>/dev/hd4</td>
<td>12288</td>
<td>5308</td>
<td>56%</td>
<td>896</td>
<td>21%</td>
<td>/</td>
</tr>
<tr>
<td>/dev/hd2</td>
<td>413696</td>
<td>26768</td>
<td>93%</td>
<td>19179</td>
<td>18%</td>
<td>/usr</td>
</tr>
<tr>
<td>/dev/hd9var</td>
<td>8192</td>
<td>3736</td>
<td>45%</td>
<td>115</td>
<td>5%</td>
<td>/var</td>
</tr>
<tr>
<td>/dev/hd3</td>
<td>4096</td>
<td>3932</td>
<td>4%</td>
<td>17</td>
<td>1%</td>
<td>/home</td>
</tr>
<tr>
<td>/dev/hd1</td>
<td>12288</td>
<td>7904</td>
<td>3%</td>
<td>17</td>
<td>0%</td>
<td>/crabfs</td>
</tr>
<tr>
<td>/dev/crab1lv</td>
<td>12288</td>
<td>11744</td>
<td>4%</td>
<td>16</td>
<td>0%</td>
<td>/crab3fs</td>
</tr>
<tr>
<td>/dev/crab41v</td>
<td>16384</td>
<td>15156</td>
<td>7%</td>
<td>17</td>
<td>0%</td>
<td>/crab4fs</td>
</tr>
<tr>
<td>/dev/crablv</td>
<td>4096</td>
<td>3522</td>
<td>20%</td>
<td>17</td>
<td>1%</td>
<td>/crabfs</td>
</tr>
</tbody>
</table>

Check the %used column for filesystems that are using more than 90% of their available space. Then check the free column to determine the exact amount of free space left.

Checking Mount Points, Permissions, and Other Filesystem Information

Use the lsfs command to display information about mount points, permissions, filesystem size and so on. For example:

```
lsfs
```

<table>
<thead>
<tr>
<th>Name</th>
<th>Nodename</th>
<th>Mount Pt</th>
<th>VFS</th>
<th>Size</th>
<th>Options</th>
<th>Auto</th>
</tr>
</thead>
<tbody>
<tr>
<td>/dev/hd4</td>
<td>--</td>
<td>/</td>
<td>jfs</td>
<td>24576</td>
<td>--</td>
<td>yes</td>
</tr>
<tr>
<td>/dev/hd1</td>
<td>--</td>
<td>/home</td>
<td>jfs</td>
<td>8192</td>
<td>--</td>
<td>yes</td>
</tr>
<tr>
<td>/dev/hd2</td>
<td>--</td>
<td>/usr</td>
<td>jfs</td>
<td>827392</td>
<td>--</td>
<td>yes</td>
</tr>
<tr>
<td>/dev/hd9var</td>
<td>--</td>
<td>/var</td>
<td>jfs</td>
<td>16384</td>
<td>--</td>
<td>yes</td>
</tr>
<tr>
<td>/dev/hd3</td>
<td>--</td>
<td>/tmp</td>
<td>jfs</td>
<td>16384</td>
<td>--</td>
<td>yes</td>
</tr>
<tr>
<td>/dev/hd7</td>
<td>--</td>
<td>/mnt</td>
<td>jfs</td>
<td>--</td>
<td>--</td>
<td>no</td>
</tr>
<tr>
<td>/dev/hd5</td>
<td>--</td>
<td>/blv</td>
<td>jfs</td>
<td>--</td>
<td>--</td>
<td>no</td>
</tr>
<tr>
<td>/dev/crab1lv</td>
<td>--</td>
<td>/crab1fs</td>
<td>jfs</td>
<td>16384</td>
<td>rw</td>
<td>no</td>
</tr>
<tr>
<td>/dev/crab3lv</td>
<td>--</td>
<td>/crab3fs</td>
<td>jfs</td>
<td>24576</td>
<td>rw</td>
<td>no</td>
</tr>
<tr>
<td>/dev/crab41v</td>
<td>--</td>
<td>/crab4fs</td>
<td>jfs</td>
<td>32768</td>
<td>rw</td>
<td>no</td>
</tr>
<tr>
<td>/dev/crablv</td>
<td>--</td>
<td>/crabfs</td>
<td>jfs</td>
<td>8192</td>
<td>rw</td>
<td>no</td>
</tr>
</tbody>
</table>

**Important:** For filesystems to be NFS exported, be sure to verify that logical volume names for these filesystems are consistent throughout the cluster. Also, use the cl_lsfs command to list filesystem information when running the C-SPOC utility.

Using the C-SPOC Utility to Check Shared Filesystems

To check to see whether the necessary shared filesystems are mounted and where they are mounted on cluster nodes in a two-node C-SPOC environment:

1. Enter the following fastpath: smitty cl_admin
2. Select Cluster Logical Volume Manager > Shared Filesystems > List All Shared Filesystems. A list of all shared filesystems appears.

You can also use the C-SPOC cl_lsfs command from the command line to display this information.

Checking the Automount Attribute of Filesystems

At boot time, AIX attempts to check all the filesystems listed in /etc/filesystems with the check=true attribute by running the fsck command. If AIX cannot check a filesystem, it reports the following error:

```
Filesystem helper: 0506-519 Device open failed
```
For filesystems controlled by HACMP, this error message typically does not indicate a problem. The filesystem check fails because the volume group on which the filesystem is defined is not varied on at boot time.

To avoid generating this message, edit the /etc/filesystems file to ensure that the stanzas for the shared filesystems do not include the check=true attribute.

### Checking the TCP/IP Subsystem

Use the following AIX commands to investigate the TCP/IP subsystem:

- Use the **netstat** command to make sure that the adapters are initialized and that a communication path exists between the local node and the target node.
- Use the **ping** command to check the point-to-point connectivity between nodes.
- Use the **ifconfig** command on all adapters to detect bad IP addresses, incorrect subnet masks, and improper broadcast addresses.
- Scan the /tmp/hacmp.out file to confirm that the /etc/rc.net script has run successfully. Look for a zero exit status.
- If IP address takeover is enabled, confirm that the /etc/rc.net script has run and that the service adapter is on its service address and not on its boot address.
- Use the **lssrc -g tcpip** command to make sure that the inetd daemon is running.
- Use the **lssrc -g portmap** command to make sure that the portmapper daemon is running.
- Use the **arp** command to make sure that the cluster nodes are not using the same IP or hardware address.

Use the **netstat** command to:

- Show the status of the network interfaces defined for a node.
- Determine whether a route from the local node to the target node is defined.

The **netstat -in** command displays a list of all initialized interfaces for the node, along with the network to which that interface connects and its IP address. You can use this command to determine whether the service and standby adapters are on separate subnets. (The subnets are displayed in the Network column.)

```
netstat -in

<table>
<thead>
<tr>
<th>Name</th>
<th>Mtu</th>
<th>Network</th>
<th>Address</th>
<th>Ipks</th>
<th>Ierrs</th>
<th>Opks</th>
<th>Oerrs</th>
<th>Coll</th>
</tr>
</thead>
<tbody>
<tr>
<td>lo0</td>
<td>1536</td>
<td>&lt;Link&gt;</td>
<td>18406</td>
<td>0</td>
<td>0</td>
<td>18406</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>lo0</td>
<td>1536</td>
<td>127</td>
<td>127.0.0.1</td>
<td>18406</td>
<td>0</td>
<td>18406</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>en1</td>
<td>1500</td>
<td>&lt;Link&gt;</td>
<td>1111626</td>
<td>0</td>
<td>0</td>
<td>58643</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>en1</td>
<td>1500</td>
<td>100.100.86.100.100.86.136</td>
<td>1111626</td>
<td>0</td>
<td>0</td>
<td>58643</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>en0</td>
<td>1500</td>
<td>&lt;Link&gt;</td>
<td>943656</td>
<td>0</td>
<td>0</td>
<td>52208</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>en0</td>
<td>1500</td>
<td>100.100.83.100.100.83.136</td>
<td>943656</td>
<td>0</td>
<td>0</td>
<td>52208</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>tr1</td>
<td>1492</td>
<td>&lt;Link&gt;</td>
<td>1879</td>
<td>0</td>
<td>0</td>
<td>1656</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>tr1</td>
<td>1492</td>
<td>100.100.84.100.100.84.136</td>
<td>1879</td>
<td>0</td>
<td>0</td>
<td>1656</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>tr0</td>
<td>1492</td>
<td>&lt;Link&gt;</td>
<td>1862</td>
<td>0</td>
<td>0</td>
<td>1647</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>tr0</td>
<td>1492</td>
<td>100.100.85.100.100.85.136</td>
<td>1862</td>
<td>0</td>
<td>0</td>
<td>1647</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```
Look at the first, third, and fourth columns of the output. The **Name** column lists all the interfaces defined and available on this node. Note that an asterisk preceding a name indicates the interface is down (not ready for use). The **Network** column identifies the network to which the interface is connected (its subnet mask). The **Address** column identifies the IP address assigned to the node.

The `netstat -r` command indicates whether a route to the target node is defined. To see all the defined routes, enter:

```
netstat -r
```

Information similar to that shown in the following example is displayed:

```
Routing tables
Destination      Gateway            Flags  Refcnt Use       Interface
```

To test for a specific route to a network (for example 100.100.83), enter:

```
netstat -nr | grep '100\.100\.83'
```

The same test, run on a system that does not have this route in its routing table, returns no response. If the service and standby adapters are separated by a bridge, router, or hub and you experience problems communicating with network devices, the devices may not be set to handle two network segments as one physical network. Try testing the devices independent of the configuration, or contact your system administrator for assistance.

Note that if you have only one adapter active on a network, the Cluster Manager will not generate a failure event for that adapter. (For more information, see the section on network adapter events in the *Installation Guide*.)

See the `netstat` man page for more information on using this command.

### Checking Point-to-Point Connectivity

The `ping` command tests the point-to-point connectivity between two nodes in a cluster. Use the `ping` command to determine whether the target node is attached to the network and whether the network connections between the nodes are reliable. Be sure to test all TCP/IP interfaces configured on the nodes (service and standby).

For example, to test the connection from a local node to a remote node named `clam` enter:
/etc/ping clam

PING chowder.clam.com: (100.100.81.141): 56 data bytes
64 bytes from 100.100.81.141: icmp_seq=0 ttl=255 time=2 ms
64 bytes from 100.100.81.141: icmp_seq=1 ttl=255 time=1 ms
64 bytes from 100.100.81.141: icmp_seq=2 ttl=255 time=2 ms
64 bytes from 100.100.81.141: icmp_seq=3 ttl=255 time=2 ms

Type Control-C to end the display of packets. The following statistics appear:

----chowder.clam.com PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 1/1/2 ms

The ping command sends packets to the specified node, requesting a response. If a correct response arrives, ping prints a message similar to the output shown above indicating no lost packets. This indicates a valid connection between the nodes.

If the ping command hangs, it indicates that there is no valid path between the node issuing the ping command and the node you are trying to reach. It could also indicate that required TCP/IP daemons are not running. Check the physical connection between the two nodes. Use the ifconfig and netstat commands to check the configuration. A “bad value” message indicates problems with the IP addresses or subnet definitions.

Note that if “DUP!” appears at the end of the ping response, that means the ping command has received multiple responses for the same address. This response typically occurs when adapters have been misconfigured, or when a cluster event fails during IP address takeover. Check the configuration of all adapters on the subnet to verify that there is only one adapter per address.

See the ping man page for more information.

In addition, starting with HACMP 4.5, you can assign a persistent IP label to a cluster network on a node.

When for administrative purposes you wish to reach a specific node in the cluster using the ping or telnet commands without worrying whether an IP service label you are using belongs to any of the resource groups present on that node, it is convenient to use a persistent IP label defined on that node.

See chapter 9 in the Installation Guide for more information on how to assign persistent IP labels on the network on the nodes in your cluster.

Checking the IP Address and Netmask

Use the ifconfig command to confirm that the IP address and netmask are correct. Invoke ifconfig with the name of the network interface that you want to examine. For example, to check the first Ethernet interface, enter:

ifconfig en0

en0: flags=2000063<UP,BROADCAST,NOTRAILERS,RUNNING,NOECHO>
in net 100.100.83.136 netmask 0xffffff00 broadcast 100.100.83.255

If the specified interface does not exist, ifconfig replies:
No such device
The `ifconfig` command displays two lines of output. The first line shows the interface’s name and characteristics. Check for these characteristics:

**UP**  
The interface is ready for use. If the interface is down, use the `ifconfig` command to initialize it. For example:
```
ifconfig en0 up
```
If the interface does not come up, replace the interface cable and try again. If it still fails, use the `diag` command to check the interface hardware.

**RUNNING**  
The interface is working. If the interface is not running, the driver for this interface may not be properly installed, or the interface is not properly configured. Review all the steps necessary to install this interface, looking for errors or missed steps.

The second line of output shows the IP address and the subnet mask (written in hexadecimal). Check these fields to make sure the network interface is properly configured.

See the `ifconfig` man page for more information.

**Using the arp Command**

Use the `arp` command to view what is currently held to be the IP addresses associated with nodes listed in a host’s arp cache. For example:
```
arp -a
```

```
flounder (100.50.81.133) at 8:0:4c:0:12:34 [ethernet]
cod (100.50.81.195) at 8:0:5a:7a:2c:85 [ethernet]
seahorse (100.50.161.6) at 42:c:2:4:0:0 [token ring]
pollock (100.50.81.147) at 10:0:5a:5c:36:b9 [ethernet]
```

This output shows what the host node currently believes to be the IP and MAC addresses for nodes flounder, cod, seahorse and pollock. (If IP address takeover occurs without Hardware Address Takeover, the MAC address associated with the IP address in the host’s arp cache may become outdated. You can correct this situation by refreshing the host’s arp cache.)

See the `arp` man page for more information.

**Checking ATM Classic IP Hardware Addresses**

For Classic IP interfaces, the `arp` command is particularly useful to diagnose errors. It can be used to verify the functionality of the ATM network on the ATM protocol layer, and to verify the registration of each Classic IP client with its server.

**Example 1**
The following `arp` command yields the output below:
```
arp -t atm -a
SVC - at0 on device atm2
================================
at0(10.50.111.4) 39.99.99.99.99.99.99.0.0.99.99.1.1.8.0.5a.99.a6.9b.0
IP Addr VPI:VCI Handle ATM Address
stby_1A(10.50.111.2)
server_10_50_111(10.50.111.99)
  0:103 14 39.99.99.99.99.99.99.0.0.99.99.1.1.88.88.88.88.a.11.0
```

```
```
Example 2

If the connection between an ATM device and the switch is not functional on the ATM layer, the output of the `arp` command looks as follows:

```
arp -t atm -a
```

SVC - at0 on device atm2

```
SVC - at0 on device atm2
at0(10.50.111.4) 8.0.5a.99.a6.9b.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0
```

Here the MAC address of ATM device atm2, 8.0.5a.99.a6.9b, appears as the first six bytes of the ATM address for interface at0. The ATM device atm2 has not registered with the switch, since the switch address does not appear as the first part of the ATM address of at0.

See the section HACMP Configuration Requirements for ATM Hardware Address Swapping (Classic IP only) in the Planning Guide for more information on configuring Hardware Address Takeover on an ATM adapter.

Checking the AIX Operating System

To view hardware and software errors that may affect the cluster, use the `errpt` command or use the `error` option to the `/usr/sbin/cluster/diag/cldiag` utility. Be on the lookout for disk and network error messages, especially permanent ones, which indicate real failures.

See the `errpt` man page for more information.

Checking Physical Networks

- Check the serial line between each pair of nodes.
- If you are using Ethernet:
  - Use the `diag` command to verify that the adapter card and cables are good.
• Use the SMIT Minimum Configuration & Startup screen to confirm that all Ethernet adapters are set to either DIX or BNC. If you change this connector type on the Minimum Configuration & Startup screen, you must also set the Apply Change to DATABASE Only field on the SMIT Change/Show Characteristics of an Ethernet Adapter screen to Yes. Then reboot the machine to apply the configuration change.

• Verify that you are using a T-connector plugged directly into the inboard/output transceiver.

• Make sure that you are using Ethernet cable, not EM-78 cable. (Ethernet cable is 50 OHM; EM-78 cable is 96 OHM.)

• Make sure that you are using Ethernet terminators, not EM-78 terminators or diagnostic plugs, which are 25 OHM. (Ethernet terminators are 50 OHM; EM-78 terminators are 96 OHM.)

• Ethernet adapters for the RS/6000 can be used with either the transceiver that is on the card or with an external transceiver. There is a jumper on the adapter to specify which you are using. Verify that your jumper is set correctly.

• If you are using Token-Ring:
  • Use the diag command to verify that the adapter card and cables are good.
  • Make sure that all the nodes in the cluster are on the same ring.
  • Make sure that all adapters are configured for 4 Mbps, or that they are all configured for 16 Mbps.

To review HACMP network requirements, see the Planning Guide.

---

### Checking Disks and Disk Adapters

Use the diag command to verify that the adapter card is functioning properly. If problems arise, be sure to check the jumpers, cables, and terminators along the SCSI bus.

For SCSI disks, including IBM SCSI-2 Differential and SCSI-2 Differential Fast/Wide disks and arrays, make sure that each array controller, adapter, and physical disk on the SCSI bus has a unique SCSI ID. Each SCSI ID on the bus must be an integer value from 0 through 7 (standard SCSI-2 Differential) or from 0 through 15 (SCSI-2 Differential Fast/Wide). A common configuration is to set the SCSI ID of the adapters on the nodes to be higher than the SCSI IDs of the shared devices. (Devices with higher IDs take precedence in SCSI bus contention.)

For example, if the standard SCSI-2 Differential adapters use IDs of 5 and 6, assign values from 0 through 4 to the other devices on the bus. You may want to set the SCSI IDs of the adapters to 5 and 6 to avoid a possible conflict when booting one of the systems in service mode from a mksysb tape of other boot devices, since this will always use an ID of 7 as the default.

If the SCSI-2 Fast/Wide Differential adapters use IDs of 14 and 15, assign values from 3 through 13 to the other devices on the bus. Refer to your worksheet for the values previously assigned to the adapters.

The IBM High Performance SCSI-2 Differential Fast/Wide Adapter is used with the IBM 7135-210 RAIDiant Disk Array and cannot be assigned SCSI IDs 0, 1, or 2; the adapter restricts the use of these IDs. Additionally, although each controller on the IBM 7135-210 RAIDiant Disk Array contains two connectors, each controller requires only one SCSI ID.
You can check the SCSI IDs of adapters and disks using either the `lsattr` or `lsdev` command. For example, to determine the SCSI ID of the adapter `scsi1` or `ascsi1` (SCSI-2 Differential Fast/Wide), use one of the following `lsattr` commands and specify the logical name of the adapter as an argument:

- For SCSI-2 Differential adapters, use:
  ```
  lsattr -E -l scsi1 | grep id
  ```
- For SCSI-2 Differential Fast/Wide adapters, use:
  ```
  lsattr -E -l ascsi1 | grep external_id
  ```

Do not use wildcard characters or full pathnames on the command line for the device name designation.

A display similar to the following appears:

```
<table>
<thead>
<tr>
<th>id</th>
<th>7</th>
<th>Adapter card SCSI ID</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>7</td>
<td></td>
</tr>
</tbody>
</table>
```

**Output of lsattr Command**

The first column lists the attribute names. The integer to the right of the `id` attribute is the adapter SCSI ID.

**Important:** If you restore a backup of your cluster configuration onto an existing system, be sure to recheck or reset the SCSI IDs to avoid possible SCSI ID conflicts on the shared bus. Restoring a system backup causes adapter SCSI IDs to be reset to the default SCSI ID of 7.

If you note a SCSI ID conflict, see the *Installation Guide* for information about setting the SCSI IDs on disks and disk adapters.

To determine the SCSI ID of a disk, enter:
```
lsdev -Cc disk -H
```
A display similar to the following appears:

```
<table>
<thead>
<tr>
<th>name</th>
<th>status</th>
<th>location</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hdisk0</td>
<td>Available</td>
<td>00-07-00-00</td>
<td>2.0 GB SCSI Disk Drive</td>
</tr>
<tr>
<td>hdisk1</td>
<td>Available</td>
<td>00-07-00-10</td>
<td>2.0 GB SCSI Disk Drive</td>
</tr>
<tr>
<td>hdisk2</td>
<td>Available</td>
<td>00-07-00-20</td>
<td>2.0 GB SCSI Disk Drive</td>
</tr>
</tbody>
</table>
```

**Output of lsdev -Cc disk -H**

The third column of the display is the location code of the device in the format AA-BB-CC-DD. The first digit (the first D) of the DD field is the disk’s SCSI ID.
**Recovering from PCI Hot Plug Network Adapter Failure**

If an unrecoverable error causes a PCI hot-replacement process to fail, you may be left in a state where your adapter is unconfigured and still in maintenance mode. The PCI slot holding the adapter and/or the new adapter may be damaged at this point. User intervention is required to get the node back in fully working order.

For more information, refer to your hardware manuals or search for information about devices on IBM’s website, [http://www.ibm.com](http://www.ibm.com).

**Checking System Hardware**

Check the power supplies and the LED displays to see if any error codes are displayed. Run the `diag` command to test the system unit.

Without an argument, `diag` runs as a menu-driven program. You can also run `diag` on a specific piece of hardware. For example:

```
diag -d hdisk0 -c
```

Starting diagnostics.
Ending diagnostics.

This output indicates that `hdisk0` is okay.

See the `diag` man page for more information. Note that the `cldiag` utility should not be used while the Cluster Manager is running.
Chapter 4: Solving Common Problems

This chapter identifies problems that you may encounter as you use HACMP and offers possible solutions.

Problems and solutions are categorized as follows:
- HACMP Installation Issues
- HACMP Startup Issues
- Disk and File System Issues
- Network and Switch Issues
- HACMP Takeover Issues
- Client Issues
- Miscellaneous Issues

HACMP Installation Issues

The following potential installation issues are described here:
- Cannot Find Filesystem at Boot Time
- cl_convert Does Not Run Due to Failed Installation
- Configuration Files Could Not Be Merged During Installation
- System ID Licensing Issues

Cannot Find Filesystem at Boot Time

Problem
At boot-time, AIX tries to check, by running the fsck command, all the file systems listed in /etc/filesystems with the “check=true” attribute. If it cannot check a file system, AIX reports the following error:

```
+----------------------------------------------------------+
Filesystem Helper: 0506-519 Device open failed
+----------------------------------------------------------+
```

Solution
For file systems controlled by HACMP, this error typically does not indicate a problem. The file system check failed because the volume group on which the file system is defined is not varied on at boot-time. To prevent the generation of this message, edit the /etc/filesystems file to ensure that the stanzas for the shared file systems do not include the “check=true” attribute.
cl_convert Does Not Run Due to Failed Installation

**Problem**
When you install HACMP, cl_convert is run automatically. The software checks for an existing HACMP configuration and attempts to update that configuration to the format used by the newer version of the software. However, if installation fails, cl_convert will fail to run as a result. Therefore, conversion from the ODM of a previous HACMP version to the ODM of the current version will also fail.

**Solution**
Run cl_convert from the command line. To gauge conversion success, refer to the /tmp/clconvert.log file, which logs conversion progress.

Root user privilege is required to run cl_convert.

**WARNING:** Before converting from HACMP 4.5 to HACMP ES 4.5, be sure that your ODMDIR environment variable is set to /etc/es/objrepos.

For information on cl_convert flags, refer to the cl_convert man page.

Configuration Files Could Not Be Merged During Installation

**Problem**
During the installation of HACMP client software, the following message is displayed:

```
+----------------------------------------------------------+
| Post-installation Processing...                         |
+----------------------------------------------------------+
```

Some configuration files could not be automatically merged into the system during the installation. The previous versions of these files have been saved in a configuration directory as listed below. Compare the saved files and the newly installed files to determine if you need to recover configuration data. Consult product documentation to determine how to merge the data.

Configuration files which were saved in /usr/lpp/save.config:
/usr/sbin/cluster/utilities/clexit.rc

**Solution**
As part of the HACMP, Version 4.5, installation process, copies of HACMP files that could potentially contain site-specific modifications are saved in the /usr/lpp/save.config directory before they are overwritten. As the message states, users must merge site-specific configuration information into the newly installed files.

System ID Licensing Issues

The Concurrent Resource Manager is licensed to the hardware system identifier of a cluster node. Many of the clvm or concurrent access commands validate the system ID against the license file. A mismatch will cause the command to fail, with an error message indicating the lack of a license.

Restoring a system image from a mksysb tape created on a different node or replacing the planar board on a node will cause this problem. In such cases, you must recreate the license file by removing and reinstalling the cluster.clvm component of the current release from the original installation images.
HACMP Startup Issues

The following potential HACMP startup issues are described here:

- ODMPATH Environment Variable Not Set Correctly
- Cluster Manager Starts but then Hangs
- clinfo Daemon Exits After Starting
- Node Powers Down; Cluster Manager Will Not Start
- configchk Command Returns an Unknown Host Message
- Cluster Manager Hangs During Reconfiguration
- clsmuxpd Does Not Start or Exits After Starting
- Pre- or Post-Event Does Not Exist on a Node After Upgrade
- Node Fails During Configuration with “869” LED Display
- Node Cannot Rejoin the Cluster After Being Dynamically Removed

ODMPATH Environment Variable Not Set Correctly

**Problem**
Queried object not found.

**Solution**
HACMP has a dependency on the location of certain ODM repositories to store configuration data. The ODMPATH environment variable allows ODM commands and subroutines to query locations other than the default location if the queried object does not reside in the default location. You can set this variable, but it must include the default location, `/etc/objrepos`, or the integrity of configuration information may be lost.

Cluster Manager Starts but then Hangs

**Problem**
The Cluster Manager starts but hangs; it generates a message similar to the following:

```
Cannot bind socket UDP keep-alives on adapter-name.
```

An adapter is not configured. A problem may exist with the way that the adapter card is seated in the slot or with cable connections.

**Solution**
First run the `ifconfig` command on the adapter; the Cluster Manager should resume working without having to execute the `clruncmd` command. If this does not work, power down the CPU, open the system unit, and reseat the adapter card. When the node is rebooted, the Cluster Manager should work correctly. You should, however, run diagnostics against the adapter, and check the status of the physical adapters as described in Chapter 3: Investigating System Components.

Note that if you have only one adapter active on a network, the Cluster Manager will not generate a failure event for that adapter. (For more information, see the section on network adapter events in the *Installation Guide.*)
clinfo Daemon Exits After Starting

Problem
The “smux-connect” error occurs after starting the clinfo daemon with the -a option. Another process is using port 162 to receive traps.

Solution
Check to see if another process, such as the trapgend smux subagent of NetView for AIX or the System Monitor for AIX sysmond daemon, is using port 162. If so, restart clinfo without the -a option and configure NetView for AIX to receive the clsmuxpd traps. Note that you will not experience this error if clinfo is started in its normal way using the startsrc command.

Node Powers Down; Cluster Manager Will Not Start

Problem 1
The node powers itself off or appears to hang after starting the Cluster Manager. The configuration information does not appear to be identical on all nodes, causing the cexit.rc script to issue a halt -q to the system.

Solution 1
Use the clverify utility to uncover discrepancies in cluster configuration information on all cluster nodes. See the Administration Guide for more information.

Correct any configuration errors uncovered by the clverify utility. Make the necessary changes using the Cluster Configuration SMIT screens. After correcting the problem, select the Cluster Resources option from the Cluster Configuration SMIT screen, and then choose Synchronize Cluster Resources to synchronize the cluster resources configuration across all nodes. Then select the Start Cluster Services option from the Cluster Services SMIT screen to start the Cluster Manager.

Problem 2
The following error messages appear in the /usr/adm/cluster.log file:

Could not find port clm_lkm
Could not find port clm_smux
Could not find port 'clm_keepalive'

Solution 2
Check that all the ports required by the Cluster Manager are listed in the /etc/services file. The following list describes the ports required by the Cluster Manager. If any of the following ports are missing from the file, add them to the /etc/services file:

# HACMP CLM-specific ports
clm_keepalive 6255/udp# HACMP clstrmgr-to-clstrmgr msgs
cllockd 6100/udp# HACMP CLM CTI
clm_pts 6200/tcp# HACMP CLM PTI
clm_lkm 6150/tcp# HACMP clstrmgr-to-cllockd deadman
clm_smux 6175/tcp# HACMP clinfo deadman port

The following command refreshes TCP/IP and forces a re-read of the /etc/services file:

refresh -s tcpip
configchk Command Returns an Unknown Host Message

Problem
The `/etc/hosts` file on each cluster node does not contain the IP labels of other nodes in the cluster. For example, in a four-node cluster, Node A, Node B, and Node C’s `/etc/hosts` files do not contain the IP labels of the other cluster nodes.

If this situation occurs, the `configchk` command returns the following message to the console: "your hostname not known," "Cannot access node x."

which indicates that the `/etc/hosts` file on Node x does not contain an entry for your node.

Solution
Before starting the HACMP software, ensure that the `/etc/hosts` file on each node includes the service and boot IP labels of each cluster node.

Cluster Manager Hangs During Reconfiguration

Problem 1
The Cluster Manager hangs during reconfiguration and generates messages similar to the following:

The cluster has been in reconfiguration too long; Something may be wrong.

An event script has failed.

Solution 1
Determine why the script failed by examining the `/tmp/hacmp.out` file to see what process exited with a non-zero status. The error messages in the `/usr/adm/cluster.log` file may also be helpful. Fix the problem identified in the log file. Then execute the `clruncmd` command on the command line, or by using the SMIT Cluster Recovery Aids screen. The `clruncmd` command signals the Cluster Manager to resume cluster processing.

Problem 2
The Cluster Manager fails because of duplicate cluster IDs on the same network.

Solution 2
If more than one cluster on the same network has the same cluster ID, the Cluster Manager fails and writes the following message to the System Error Log:

MESSAGE FROM ERRLOGGER COMMAND
ASSERT FAILED: invalid node name in cvtAtoE, file cc_event.c, line 399+

To avoid receiving this message, ensure that all clusters on the same network have unique cluster IDs. See the Administration Guide for more information about assigning cluster IDs.

clsmuxpd Does Not Start or Exits After Starting

Problem
clsmuxpd does not start or exits after starting

Solution
- Verify that there is an `/etc/hosts` entry for loopback by entering:

  127.0.0.1 loopback localhost
- Verify that the proper HACMP entries exist in `/etc/services`.
- Verify that `snmpd` is running by entering:
  
  ```
  lssrc -ls snmpd
  ```

If `clsmuxpd` still does not start or exits after starting, you may wish to check whether the smux port (199) has been locked by another program. First check to see if `snmpd` tracing is enabled by examining the output of the `lssrc -ls snmpd` command. If `snmpd` tracing is enabled, examine the log file listed by `lssrc`. If `snmpd` tracing is not enabled, enable it and examine the specified log file:

```
stopsrc snmpd
startsrc snmpd -a '-d /tmp/snmpd.log'
```

If the log file contains a smux I/O error, it is possible that another program has locked the smux port (199). To determine the offending program:

```
stop snmpd
stopsrc snmpd
```

and run:

```
netstat -a | grep smux
```

If any port is returned, the listed program will need to be changed to access some other port. 199 is reserved for SMUX and should not be used by other programs.

### Pre- or Post-Event Does Not Exist on a Node After Upgrade

**Problem**
The `/usr/sbin/cluster/diag/clverify` utility indicates that a pre- or post-event does not exist on a node after upgrading to a new version of the HACMP software.

**Solution**
Ensure that a script by the defined name exists and is executable on all cluster nodes.

Each node must contain a script associated with the defined pre- or post-event. While the contents of the script do not have to be the same on each node, the name of the script must be consistent across the cluster. If no action is desired on a particular node, a “no-op” script with the same event-script name should be placed on nodes on which no processing should occur.

### Node Fails During Configuration with “869” LED Display

**Problem**
The system appears to be hung. “869” is displayed continuously on the system LED display.

**Solution**
A number of situations can cause this display to occur. Make sure all devices connected to the SCSI bus have unique SCSI IDs to avoid SCSI ID conflicts. In particular, check that the adapters and devices on each cluster node connected to the SCSI bus have a different SCSI ID. By default, AIX assigns an ID of 7 to a SCSI adapter when it configures the adapter. See the *Installation Guide* for more information on checking and setting SCSI IDs.
Node Cannot Rejoin the Cluster After Being Dynamically Removed

**Problem**
A node that has been dynamically removed from a cluster cannot rejoin.

**Solution**
When you remove a node from the cluster, the cluster definition remains in the node’s ODM. If you start cluster services on the removed node, the node reads this cluster configuration data and attempts to rejoin the cluster from which it had been removed. The other nodes no longer recognize this node as a member of the cluster and refuse to allow the node to join. Because the node requesting to join the cluster has the same cluster name and ID as the existing cluster, it can cause the cluster to become unstable or crash the existing nodes.

To ensure that a removed node cannot be restarted with outdated ODM information, complete the following procedure to remove the cluster definition from the node:

1. Use the following command to stop cluster services on the node to be removed:
   ```
   clstop -R
   ```
   **WARNING:** You must stop the node before removing it.
   The -R flag removes the HACMP entry in the `/etc/inittab` file, preventing cluster services from being automatically started when the node is rebooted.

2. Remove the HACMP entry from the `rc.net` file using the following command:
   ```
   clchipat false
   ```

3. Remove the cluster definition from the node’s ODM using the following command:
   ```
   clrmclstr
   ```
   You can also perform this task by selecting **Remove Cluster Definition** from the **Cluster Topology** SMIT screen.

---

**Disk and File System Issues**

The following potential disk and file system issues are described here:

- AIX Volume Group Commands Cause System Error Reports
- `varyonvg` Command Fails on Volume Group
- `cl_nfskill` Command Fails
- `cl_scdiskreset` Command Fails
- `fsck` Command Fails at Boot Time
- System Cannot Mount Specified File Systems
- Cluster Disk Replacement Process Fails
AIX Volume Group Commands Cause System Error Reports

Problem
The `redefinevg`, `varyonvg`, `lqueryvg`, and `syncvg` commands fail and report errors against a shared volume group during system restart. These commands send messages to the console when automatically varying on a shared volume group. When configuring the volume groups for the shared disks, `autovaryon at boot` was not disabled. If a node that is up owns the shared drives, other nodes attempting to vary on the shared volume group will display various varyon error messages.

Solution
When configuring the shared volume group, set the `Activate volume group AUTOMATICALLY at system restart?` field on the SMIT Add a Volume Group screen to no. After importing the shared volume group on the other cluster nodes, use the following command to ensure that the volume group on each node is not set to `autovaryon at boot`:

```
chvg -an vgname
```

varyonvg Command Fails on Volume Group

Problem 1
The HACMP software (the `/tmp/hacmp.out` file) indicates that the `varyonvg` command failed when trying to vary on a volume group.

Solution 1
Ensure that the volume group is not set to `autovaryon` on any node and that the volume group (unless it is in concurrent access mode) is not already varied on by another node.

The `lsvg -o` command can be used to determine whether the shared volume group is active. Enter

```
lsvg volume_group_name
```
on the node that has the volume group activated, and check the `AUTO ON` field to determine whether the volume group is automatically set to be on. If `AUTO ON` is set to yes, correct this by entering

```
chvg -an volume_group_name
```

Problem 2
The volume group information on disk differs from that in the Device Configuration Data Base.

Solution 2
Correct the Device Configuration Data Base on the nodes that have incorrect information:

1. Use the `smit exportvg` fastpath to export the volume group information. This step removes the volume group information from the Device Configuration Data Base.

2. Use the `smit importvg` fastpath to import the volume group. This step creates a new Device Configuration Data Base entry directly from the information on disk. Be sure, however, to change the volume group to not `autovaryon` at the next system boot.

3. Use the SMIT Cluster Recovery Aids screen to issue the `clruncmd` command to signal the Cluster Manager to resume cluster processing.
Problem 3
The HACMP software indicates that the `varyonvg` command failed because the volume group could not be found.

Solution 3
The volume group is not defined to the system. If the volume group has been newly created and exported, or if a `mksysb` system backup has been restored, you must import the volume group. Follow the steps described in Problem 2 to verify that the correct volume group name is being referenced. Also, see the *Administration Guide* for more information on importing a volume group.

**cl_nfskill Command Fails**

**Problem**
The `/tmp/hacmp.out` file shows that the `cl_nfskill` command fails when attempting to perform a forced unmount of an NFS-mounted file system. NFS provides certain levels of locking a file system that resists forced unmounting by the `cl_nfskill` command.

**Solution**
Make a copy of the `/etc/locks` file in a separate directory before executing the `cl_nfskill` command. Then delete the original `/etc/locks` file and run the `cl_nfskill` command. After the command succeeds, re-create a copy of the `/etc/locks` file.

**cl_scdiskreset Command Fails**

**Problem**
The `cl_scdiskreset` command logs error messages to the `/tmp/hacmp.out` file. To break the reserve held by one system on a SCSI device, the HACMP disk utilities issue the `cl_scdiskreset` command. The `cl_scdiskreset` command may fail if back-level hardware exists on the SCSI bus (adapters, cables or devices) or if a SCSI ID conflict exists on the bus.

**Solution**
See the appropriate sections in Chapter 3: Investigating System Components, to check the SCSI adapters, cables, and devices. Make sure that you have the latest adapters and cables. The SCSI IDs for each SCSI device must be different.

**fsck Command Fails at Boot Time**

**Problem**
At boot time, AIX runs the `fsck` command to check all the file systems listed in `/etc/filesystems` with the check=true attribute. If it cannot check a file system, AIX reports the following error:

Filesystem Helper: 0506-519 Device open failed

**Solution**
For file systems controlled by HACMP, this message typically does not indicate a problem. The file system check fails because the volume group defining the file system is not varied on. The boot procedure does not automatically vary on HACMP-controlled volume groups.

To prevent this message, make sure that all the file systems under HACMP control do not have the check=true attribute in their `/etc/filesystems` stanzas. To delete this attribute or change it to check=false, edit the `/etc/filesystems` file.
System Cannot Mount Specified File Systems

**Problem**
The `/etc/filesystems` file has not been updated to reflect changes to log names for a logical volume. If you change the name of a logical volume after the file systems have been created for that logical volume, the `/etc/filesystems` entry for the log does not get updated. Thus when trying to mount the file systems, the HACMP software tries to get the required information about the logical volume name from the old log name. Because this information has not been updated, the file systems cannot be mounted.

**Solution**
Be sure to update the `/etc/filesystems` file after making changes to logical volume names.

Cluster Disk Replacement Process Fails

**Problem 1**
You are unable to complete the disk replacement process due to a node_down event.

**Solution 1**
Once the node is back online, you must export the volume group, then import it again before starting HACMP on this node.

**Problem 2**
The disk replacement process failed while the `replacepv` command was running.

**Solution 2**
Be sure to delete the `/tmp/replacepv` directory, and attempt the replacement process again. You can also try running the process on another disk.

Network and Switch Issues

The following potential network and switch issues are described here:

- Unexpected Adapter Failure in Switched Networks
- Cluster Nodes Cannot Communicate
- Distributed SMIT Causes Unpredictable Results
- Cluster Managers in a FDDI Dual Ring Fail to Communicate
- Token-Ring Network Thrashes
- System Crashes Reconnecting MAU Cables After a Network Failure
- TMSCSI Will Not Properly Reintegrate when Reconnecting Bus
- Lock Manager Communication on FDDI or SOCC Networks Is Slow
- SOCC Network Not Configured after System Reboot
- Unusual Cluster Events Occur in Non-Switched Environments
- Cannot Communicate on ATM Classic IP Network
- Cannot Communicate on ATM LAN Emulation Network
Unexpected Adapter Failure in Switched Networks

**Problem**
Unexpected adapter failures can occur in HACMP configurations using switched networks if the networks and the switches are incorrectly defined/configured.

**Solution**
Take care to configure your switches and networks correctly. See the section on considerations for switched networks in the *Planning Guide* for more information.

Cluster Nodes Cannot Communicate

**Problem**
If your configuration has two or more nodes connected by a single network, you may experience a partitioned cluster. Basically, a partitioned cluster occurs when cluster nodes cannot communicate. In normal circumstances, a service adapter failure on a node causes the Cluster Manager to recognize and handle a swap adapter event, where the service adapter is replaced with its standby adapter. However, if no standby adapter is available, the node becomes isolated from the cluster. Although the Cluster Managers on other nodes are aware of the attempted swap adapter event, they cannot communicate with the now isolated (partitioned) node because no communication path exists.

**Solution**
Make sure your network is configured for no single point of failure.

Distributed SMIT Causes Unpredictable Results

**Problem**
Using the AIX utility DSMIT on operations other than starting or stopping HACMP cluster services can cause unpredictable results.

**Solution**
DSMIT manages the operation of networked RS/6000 processors. It includes the logic necessary to control execution of AIX commands on all networked nodes. Since a conflict with HACMP functionality is possible, use DSMIT only to start and stop HACMP cluster services.

Cluster Managers in a FDDI Dual Ring Fail to Communicate

**Problem**
The Cluster Managers in a FDDI Dual Ring cannot communicate. Broken links in the dual ring seem to have caused the Cluster Managers to lose communications. This situation can occur when the cluster is configured with service and standby mother-daughter adapter pairs in a dual ring or other FDDI configurations. If certain combinations of defective cables, adapters, or hardware exist, the Cluster Managers lose communication and call event scripts that can create unpredictable results.

**Solution**
Check the FDDI Dual Ring configuration thoroughly to ensure that all hardware links are functioning properly before bringing up the cluster. You can test the network’s connections using the *ping* command as described in Chapter 3, Investigating System Components.
Token-Ring Network Thrashes

**Problem**
A Token-Ring network cannot reach steady state unless all stations are configured for the same ring speed. One symptom of the adapters being configured at different speeds is a clicking sound heard at the MAU (multi-station access unit).

**Solution**
Configure all adapters for either 4 or 16 Mbps.

System Crashes Reconnecting MAU Cables After a Network Failure

**Problem**
A global network failure occurs and crashes all nodes in a four-node cluster after reconnecting MAUs. More specifically, if the cables that connect multiple MAUs are disconnected and then reconnected, all cluster nodes begin to crash.

This result happens in a configuration where three nodes are attached to one MAU (MAU1) and a fourth node is attached to a second MAU (MAU2). Both MAUs (1 and 2) are connected together to complete a Token-Ring network. If MAU1 is disconnected from the network, all cluster nodes can continue to communicate; however, if MAU2 is disconnected, node isolation occurs.

**Solution**
To avoid causing the cluster to become unstable, do not disconnect cables connecting multiple MAUs in a Token-Ring configuration.

TMSCSI Will Not Properly Reintegrate when Reconnecting Bus

**Problem**
If the SCSI bus is broken while running as a target mode SCSI network, the network will not properly reintegrate when reconnecting the bus.

**Solution**
The HACMP software may need to be restarted on all nodes attached to that SCSI bus. When target mode SCSI is enabled and the `cfgmgr` command is run on a particular machine, it will go out on the bus and create a target mode initiator for every node that is on the SCSI network.

In a four-node cluster, when all four nodes are using the same SCSI bus, each machine will have three initiator devices (one for each of the other nodes).

In this configuration, use a maximum of four target mode SCSI networks. You would therefore use networks between nodes A and B, B and C, C and D, and D and A.

Target mode SCSI devices are not always properly configured during the AIX boot process. You must ensure that all the tmscsi initiator devices are available on all nodes before bringing up the cluster. This should be done by executing `lsdev -Cc tmscsi`, which returns:

```
tmscsix Available 00-12-00-40 SCSI I/O Controller Initiator Device
```

where `x` identifies the particular tmscsi device. If the status is not “Available,” run the `cfgmgr` command and check again.
Lock Manager Communication on FDDI or SOCC Networks Is Slow

**Problem**
If the Cluster Lock Manager communication on FDDI or SOCC networks seems slow, the TCP/IP protocol may be experiencing a buffering problem.

**Solution**
Change the MTU values for network adapters used by the lock manager to 1500. Use the `smit chif` fastpath to change the MTU value. Select the appropriate FDDI or SOCC adapter and replace the default value for the MTU with 1500. After this change, lock manager communication will pass between nodes at normal speeds over the point-to-point lines.

SOCC Network Not Configured after System Reboot

**Problem**
If the nodes attached to a SOCC line are rebooted at the same time, the cluster comes up without the SOCC line configured.

**Solution**
Complete the following steps simultaneously on both nodes to configure the SOCC line:
1. Enter `smit chinet` to see a list of adapters.
2. Select `so0` to get the SMIT Change/Show a Serial Optical Network Interface screen.
3. Set the current STATE field to **up**.
4. Press Enter.

Unusual Cluster Events Occur in Non-Switched Environments

**Problem**
Some network topologies may not support the use of simple switches. In these cases, you should expect that certain events may occur for no apparent reason. These events may be:
- Cluster unable to form, either all or some of the time
- `swap_adapter` pairs
- A `swap_adapter`, immediately followed by a `join_standby`
- `fail_standby` and `join_standby` pairs.

These events occur when ARP packets are delayed or dropped. This is correct and expected HACMP behavior, as HACMP is designed to depend on core protocols strictly adhering to their related RFCs.

(For a review of basic HACMP network requirements, see the *Planning Guide.*

**Solution**
The following implementations may reduce or circumvent these events:
- Increase the Failure Detection Rate (FDR) to exceed the ARP retransmit time of 15 seconds, where typical values have been calculated as follows:
  \[ FDR = (2^+ \times 15 \text{ seconds}) + >5 = 35+ \text{ seconds} \text{ (usually 45-60 seconds)} \]
“2+” is a number greater than one in order to allow multiple ARP requests to be generated. This is required so that at least one ARP response will be generated and received before the FDR time expires and the adapter is temporarily marked down, then immediately marked back up.

Keep in mind, however, that the “true” failover is delayed for the value of the FDR.

- Increase the ARP queue depth.
  
  If you increase the queue, note that requests which are dropped or delayed will be masked until network congestion or network quiescence (inactivity) makes this problem evident.

- Use a dedicated switch, with all protocol optimizations turned off. Segregate it into a physical LAN segment and bridge it back into the enterprise network.

- Use permanent ARP entries (IP address to MAC address bindings) for all boot, service and standby adapters. These values should be set at boot time, and since none of the ROM MAC addresses are used, replacing adapter cards will be invisible to HACMP.

Note: The above four items simply describe how some customers have customized their unique enterprise network topology to provide the classic protocol environment (strict adherence to RFCs) that HACMP requires. IBM cannot guarantee HACMP will work as expected in these approaches, since none addresses the root cause of the problem. If your network topology requires consideration of any of these approaches please contact the IBM Consult Line for assistance.

Cannot Communicate on ATM Classic IP Network

Problem
If you cannot communicate successfully to a cluster adapter of type atm (a cluster adapter configured over a Classic IP client at#), check the following:

Solution
1. Check the client configuration. Check that the 20 Byte ATM address of the Classic IP server that is specified in the client configuration is correct, and that the interface is configured as a Classic IP client (svc-c) and not as a Classic IP server (svc-s).

2. Check that the ATM TCP/IP layer is functional. Check that the UNI version settings that are configured for the underlying ATM device and for the switch port to which this device is connected are compatible. It is recommended not to use the value auto_detect for either side.

   If the connection between the ATM device# and the switch is not functional on the ATM protocol layer, this can also be due to a hardware failure (adapter, cable, or switch).

   Use the arp command to verify this:

   [bass]/>arp -t atm -a

   SVC - at0 on device atm1 -

   ===========================
   at0(10.50.111.6) 39.99.99.99.99.99.99.0.0.99.99.1.1.8.0.5a.99.98.fc.0
   server_10_50_111(10.50.111.255) 0:888 0:188.88.88.88.a0.11.0
Solving Common Problems
Network and Switch Issues

In the above example the client at0 is operational. It has registered with its server, server_10_50_111.

The client at1 is not operational, since it could not resolve the address of its Classic IP server, which has the hardware address 39.99.99.99.99.99.99.0.0.99.99.1.1.88.88.88.88.a0.11.0. However the ATM layer is functional, since the 20 byte ATM address that has been constructed for the client at1 is correct. The first 13 bytes is the switch address, 39.99.99.99.99.99.99.0.0.99.99.1.1.

For client at3, the connection between the underlying device atm2 and the ATM switch is not functional, as indicated by the failure to construct the 20 Byte ATM address of at3. The first 13 bytes do not correspond to the switch address, but contain the MAC address of the ATM device corresponding to atm2 instead.

**Cannot Communicate on ATM LAN Emulation Network**

**Problem**
If you are having problems communicating with an ATM LANE client, check the following:

**Solution**
Check that the LANE client is registered correctly with its configured LAN Emulation server. A failure of a LANE client to connect with its LAN Emulation server can be due to the configuration of the LAN Emulation server functions on the switch. There are many possible reasons.

1. Correct client configuration: Check that the 20 Byte ATM address of the LAN Emulation server, the assignment to a particular ELAN, and the Maximum Frame Size value are all correct.

2. Correct ATM TCP/IP layer: Check that the UNI version settings that are configured for the underlying ATM device and for the switch port to which this device is connected are compatible. It is recommended not to use the value auto_detect for either side.

If the connection between the ATM device# and the switch is not functional on the ATM protocol layer, this can also be due to a hardware failure (adapter, cable, or switch).

Use the `enstat` and `tokstat` commands to determine the state of ATM LANE clients.

```bash
bass[/]>
entstat -d ent3
```

The output will contain the following:

**General Statistics:**
--

No mbuf Errors: 0
Adapter Reset Count: 3
Driver Flags: Up Broadcast Running
Simplex AlternateAddress

ATM LAN Emulation Specific Statistics:

--------------------------------------
Emulated LAN Name: ETHER3
Local ATM Device Name: atm1
Local LAN MAC Address: 42.0c.01.03.00.00
Local ATM Address: 39.99.99.99.99.99.00.00.00.5a.99.98.fc.04
Auto Config With LECS: No
LECS ATM Address: 00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00
LES ATM Address: 39.99.99.99.99.99.99.00.00.99.99.01.01.88.88.88.88.00.03.00

In the above example the client is operational, as indicated by the Running flag.

If the client had failed to register with its configured LAN Emulation Server, the Running flag would not appear, instead the flag Limbo would be set.

If the connection of the underlying device atm# was not functional on the ATM layer, then the local ATM address would not contain as the first 13 Bytes the Address of the ATM switch.

3. Switch-specific configuration limitations: Some ATM switches do not allow more than one client belonging to the same ELAN and configured over the same ATM device to register with the LAN Emulation Server at the same time. If this limitation holds and two clients are configured, the following are typical symptoms.

- Cyclic occurrence of events indicating adapter failures, such as fail_standby, join_standby, and swap_adapter
  This is a typical symptom if two such clients are configured as cluster adapters. The client which first succeeds in registering with the LES will hold the connection for a specified, configuration-dependent duration. After it times out the other client succeeds in establishing a connection with the server, hence the cluster adapter configured on it will be detected as alive, and the former as down.

- Sporadic events indicating an adapter failure (fail_standby, join_standby, and swap_adapter)
  If one client is configured as a cluster adapter and the other outside, this configuration error may go unnoticed if the client on which the cluster adapter is configured manages to register with the switch, and the other client remains inactive. The second client may succeed at registering with the server at a later moment, and a failure would be detected for the cluster adapter configured over the first client.

HACMP Takeover Issues

The following potential takeover issues are described here:

- varyonvg Command Fails during Takeover
- Highly Available Applications Fail
- Node Failure Detection Takes Too Long
- Cluster Manager Sends a DGSP Message
- cfgmgr Command Causes Unwanted Behavior in Cluster
- Deadman Switch Causes a Node Failure
- Releasing Large Amounts of TCP Traffic Causes DMS Timeout
- A “device busy” Message Appears After node_up_local Fails
- Adapters Swap Fails Due to an rmdev “device busy” Error
- MAC Address Is Not Communicated to the Ethernet Switch

**varyonvg Command Fails during Takeover**

**Problem**
The HACMP software failed to vary on a shared volume group. The volume group name is either missing or is incorrect in the HACMP ODM object class.

**Solution**
- Check the `/tmp/hacmp.out` file to find the error associated with the varyonvg failure.
- List all the volume groups known to the system using the `lsvg` command; then check that the volume group names used in the HACMPresource ODM object class are correct. To change a volume group name in the ODM, from the main HACMP SMIT screen select `Cluster Configuration > Cluster Resources > Change/Show Resource Groups`, and choose the resource group where you want the volume group to be included. Use the `Volume Groups` or `Concurrent Volume Groups` fields on the `Configure Resources for a Resource Group` screen to set the volume group names. After you correct the problem, use the SMIT Cluster Recovery Aids screen to issue the `clruncmd` command to signal the Cluster Manager to resume cluster processing.
- Run `clverify` to verify cluster resources.

**Highly Available Applications Fail**

**Problem 1**
Highly available applications fail to start on a fallover node after an IP address takeover. The hostname may not be set.

**Solution 1**
Some software applications require an exact hostname match before they start. If your HACMP environment uses IP address takeover and starts any of these applications, add the following lines to the script you use to start the application servers:

```
mkdev -t inet
chdev -l inet0 -a hostname=nnn
```

where `nnn` is the hostname of the machine the fallover node is masquerading as.

**Problem 2**
An application which a user has manually stopped following a `forced` stop of cluster services does not restart with reintegration of the node.
Solution 2
Check that the relevant application entry in the `/usr/sbin/cluster/server.status` file has been removed prior to node reintegration.

Since an application entry in the `/usr/sbin/cluster/server.status` file lists all applications already running on the node, HACMP will not restart the applications with entries in the `server.status` file.

Deleting the relevant application `server.status` entry before reintegration, allows HACMP to recognize that the highly available application is not running, and that it must be restarted on the node.

Node Failure Detection Takes Too Long

Problem
The Cluster Manager fails to recognize a node failure in a cluster configured with a Token-Ring network. The Token-Ring network cannot become stable after a node failure unless the Cluster Manager allows extra time for failure detection.

In general, a buffer time of 14 seconds is used before determining failures on a Token-Ring network. This means that all Cluster Manager failure modes will take an extra 14 seconds if the Cluster Manager is dealing with Token-Ring networks. This time, however, does not matter if the Cluster Manager is using both Token-Ring and Ethernet. If Cluster Manager traffic is using a Token-Ring adapter, the 14 extra seconds for failures applies.

Solution
If the extra time is not acceptable, you can switch to an alternative network. The alternative could be an Ethernet. The RS232 line recommended for all clusters should prevent this problem.

For some configurations, it is possible to run all the cluster network traffic on a separate network (Ethernet), even though a Token-Ring network also exists in the cluster. When you configure the Cluster Manager, describe only the interfaces used on this separate network. Do not include the Token-Ring interfaces.

Since the Cluster Manager has no knowledge of the Token-Ring network, the 14-second buffer does not apply; thus failure detection occurs faster. Since the Cluster Manager does not know about the Token-Ring adapters, it cannot monitor them, nor can it swap adapters if one of the adapters fails or if the cables are unplugged.

Cluster Manager Sends a DGSP Message

Problem
A Diagnostic Group Shutdown Partition (DGSP) message is displayed and the node receiving the DGSP message shuts itself down. A message indicating that a DGSP message was sent will be logged in the `/usr/adm/cluster.log` file on the associated cluster nodes.

A DGSP message is sent when a node loses communication with the cluster and then tries to reestablish communication.
Solution
Because it may be difficult to determine the state of the missing node and its resources (and to avoid a possible data divergence if the node rejoins the cluster), you should shut down the node and successfully complete the takeover of its resources.

For example, if a cluster node becomes unable to communicate with other nodes, yet it continues to work through its process table, the other nodes conclude that the “missing” node has failed because they no longer are receiving keepalive messages from the “missing” node. The remaining nodes then process the necessary events to acquire the disks, IP addresses, and other resources from the “missing” node. This attempt to take over resources results in the dual-attached disks receiving resets to release them from the “missing” node and to start IP address takeover scripts.

As the disks are being acquired by the takeover node (or after the disks have been acquired and applications are running), the “missing” node completes its process table (or clears an application problem) and attempts to resend keepalive messages and rejoin the cluster. Since the disks and IP address have been successfully taken over, it becomes possible to have a duplicate IP address on the network and the disks may start to experience extraneous traffic on the data bus.

Because the reason for the “missing” node remains undetermined, you can assume that the problem may repeat itself later, causing additional down time of not only the node but also the cluster and its applications. Thus, to ensure the highest cluster availability, DGSP messages should be sent to any “missing” cluster node to identify node isolation, to permit the successful takeover of resources, and to eliminate the possibility of data corruption that can occur if both the takeover node and the rejoining “missing” node attempt to write to the disks. Also, if two nodes exist on the network with the same IP address, transactions may be missed and applications may hang.

When you have a partitioned cluster, the node(s) on each side of the partition detect this and run a node_down for the node(s) on the opposite side of the partition. If while running this, or afterwards, communication is restored, the two sides of the partition do not agree on which nodes are still members of the cluster, so a decision is made as to which partition should remain up, and the other partition is shutdown by a DGSP from nodes in the other partition or by a node sending a DGSP to itself.

In clusters consisting of more than two nodes the decision is based on which partition has the most nodes left in it, and that partition stays up. With an equal number of nodes in each partition (as is always the case in a two-node cluster) the node(s) that remain(s) up is determined by the node number (lowest node number in cluster remains) which is also generally the first in alphabetical order.

DGSP messages indicate that a node isolation problem was handled to keep the resources as highly available as possible, giving you time to later investigate the problem and its cause.

cfgmgr Command Causes Unwanted Behavior in Cluster

Problem
SMIT commands like Configure Devices Added After IPL use the cfgmgr command. Sometimes this command can cause unwanted behavior in a cluster. For instance, if there has been an adapter swap, the cfgmgr command tries to reswap the adapters, causing the Cluster Manager to fail.
Solution
See the Installation Guide for information about modifying rc.net, thereby bypassing the issue. You can use this technique at all times, not just for IP address takeover, but it adds to the overall takeover time, so it is not recommended.

Deadman Switch Causes a Node Failure

Problem
The node experienced an extreme performance problem, such as a large I/O transfer, excessive error logging, or running out of memory, and the Cluster Manager was starved for CPU time. It could not reset the deadman switch within the time allotted. Misbehaved applications running at a priority higher than the cluster manager can also cause this problem.

Solutions
The term “deadman switch” describes the AIX kernel extension that causes a system panic and dump under certain cluster conditions if it is not reset. The deadman switch halts a node when it enters a hung state that extends beyond a certain time limit. This enables another node in the cluster to acquire the hung node’s resources in an orderly fashion, avoiding possible contention problems. Solutions related to performance problems should be performed in the following order:

1. Tune the system using I/O pacing.
2. Increase the syncd frequency.
3. If needed, increase the amount of memory available for the communications subsystem.
4. Tune virtual memory management (VMM)
5. Change the Failure Detection Rate.

Tuning the System Using I/O Pacing
In some cases, I/O pacing can be used to tune the system so that system resources are distributed more equitably during large disk-writing operations. However, the results of tuning I/O pacing are highly dependent on each system’s specific configuration and I/O access characteristics.

I/O pacing can help ensure that the HACMP cluster manager continues to run even during large disk-writing operations. In some situations, it can help prevent DMS timeouts. You should be cautious when considering tuning I/O pacing for your cluster configuration, since this is not an absolute solution for DMS timeouts for all types of cluster configurations. Remember, tuning I/O pacing can significantly reduce system performance and throughput. I/O pacing and other tuning parameters should only be set to values other than defaults after a system performance analysis indicates that doing so will lead to both the desired results and acceptable side effects.

If you experience workloads that generate large disk-writing operations or intense amounts of disk traffic, contact IBM for recommendations on choices of tuning parameters that will both allow HACMP to function, and provide acceptable performance. To contact IBM, open a Program Management Report (PMR) requesting performance assistance, or follow other established procedures for contacting IBM.

To change the I/O pacing settings:

1. Enter smitty hacmp > Cluster Configuration > Advanced Performance Tuning Parameters > Change/Show I/O Pacing
2. Configure the entry fields with the recommended HIGH and LOW watermarks:

**HIGH** water mark for pending write **33** is recommended for most clusters. Possible values are 0 to 32767.

**LOW** watermark for pending write **24** is recommended for most clusters. Possible values are 0 to 32766.

While the most efficient high- and low-water marks vary from system to system, an initial high-water mark of 33 and a low-water mark of 24 provide a good starting point. These settings only slightly reduce write times, and consistently generate correct failover behavior from HACMP. If a process tries to write to a file at the high-water mark, it must wait until enough I/O operations have finished to make the low-water mark. See the *AIX Performance Monitoring & Tuning Guide* for more information on I/O pacing.

**Extending the syncd Frequency**
Increase the **syncd** frequency from its default value of 60 seconds to either 30, 20, or 10 seconds. Increasing the frequency forces more frequent I/O flushes and reduces the likelihood of triggering the deadman switch due to heavy I/O traffic. The SMIT utility updates `/sbin/rc.boot`, kills the old **syncd** process, then starts the new one with the new value.

To change the **syncd** frequency setting:
1. Enter `smitty hacmp > Cluster Configuration > Advanced Performance Tuning Parameters > Change/Show syncd frequency`
2. Configure the entry fields with the recommended **syncd** frequency:

   **syncd frequency in seconds** **10** is recommended for most clusters. Possible values are 0 to 32767.

**Increase Amount of Memory Available for Communications Subsystem**
If the output of `netstat -m` reports that requests for mbufs are being denied, or if errors indicating **LOW_MBUFS** are being logged to the AIX error report, increase the value associated with “thewall” network option. The default value is 25% of the real memory. This can be increased to as much as 50% of the real memory.

To change this value, add a line similar to the following at the end of the `/etc/rc.net` file:

```
no -o thewall=xxxx
```

where `xxxx` is the value you want to be available for use by the communications subsystem. For example,

```
no -o thewall=10240
```

**Tuning Virtual Memory Management**
For most customers, increasing **minfree/maxfree** whenever the freelist gets below **minfree** by more than 10 x the number of memory pools is necessary to allow a system to maintain consistent response times. To determine the current size of the freelist, use the **vmstat** command. The size of the freelist is the value labeled **fre**. The number of memory pools in a system is the maximum of the number of CPUs/8 or memory size in GB/16, but never more than the number of CPUs and always at least one. The value of **minfree** is shown by the **vmtune** command.
In systems with multiple memory pools, it may also be important to increase minfree/maxfree even though minfree will not show as 120, since the default minfree is 120 times the number of memory pools. If raising minfree/maxfree is going to be done, it should be done with care, that is, not setting it too high since this may mean too many pages on the freelist for no real reason. One suggestion is to increase minfree and maxfree by 10 times the number of memory pools, then observe the freelist again. In specific application environments, such as multiple processes (three or more) each reading or writing a very large sequential file (at least 1GB in size each) it may be best to set minfree relatively high, e.g. 120 times the number of CPUs, so that maximum throughput can be achieved.

This suggestion is specific to a multi-process large sequential access environment. Maxfree, in such high sequential I/O environments, should also be set more than just 8 times the number of CPUs higher than minfree, e.g. maxfree = minfree + (maxpgahead x the number of CPUs), where minfree has already been determined using the above formula. The default for maxpgahead is 8, but in many high sequential activity environments, best performance is achieved with maxpgahead set to 32 or 64. This suggestion applies to all pSeries models still being marketed, regardless of memory size. Without these changes, the chances of a DMS timeout can be high in these specific environments, especially those with minimum memory size.

For database environments, these suggestions should be modified. If JFS files are being used for database tables, then watching minfree still applies, but maxfree could be just minfree + (8 x the number of memory pools). If raw logical volumes are being used, the concerns about minfree/maxfree don't apply, but the following suggestion about maxperm does.

In any environment (HA or otherwise) that is seeing non-zero paging rates, it is recommended that maxperm be set lower than the default of ~80%. Use the avm column of vmstat as an estimate of the number of working storage pages in use (should be observed at full load on the system’s real memory, as shown by vmtune (number of valid memory pages) to determine the percentage of real memory occupied by working storage pages. For example, if avm shows as 70% of real memory size, then maxperm should be set to 25% (vmtune -P 25). The basic formula used here is maxperm = 95 - avm/memsize in pages. If avm is less than or equal to 95% of memory, then this system is memory constrained. The options at this point are to set maxperm to 5% and incur some paging activity, add additional memory to this system, or to reduce the total workload run simultaneously on the system so that avm is lowered.

**Changing the Failure Detection Rate to Predefined Values Using SMIT**

Use the SMIT Change/Show a Cluster Network Module > Change a Cluster Network Module Using Predefined Values screen to change the Failure Detection Rate for your network module only if enabling I/O pacing or extending the syncd frequency did not resolve deadman problems in your cluster. By changing the Failure Detection Rate to Slow, you can extend the time required before the deadman switch is invoked on a hung node and before a takeover node detects a node failure and acquires a hung node’s resources.

**WARNING:** Keep in mind that the Slow setting for the Failure Detection Rate is network specific, and may vary.
Note: The formula for calculating the heartbeat rate is different in HACMP and in HACMP/ES. The sections below describe the formula which is used in HACMP. For information on how to change the heartbeat rate of a network module in HACMP/ES see Chapter 24 in the Enhanced Scalability Installation and Administration Guide.

Changing the Failure Detection Rate Beyond Fast/Normal/Slow Settings

If your system needs to withstand a performance hit or outage longer than that achieved by setting all associated NIMs to Slow, you can specify a slower Failure Detection Rate by altering the HACMPnim ODM class. To do this, select custom settings for Heartbeat Rate and Failure Cycle in the Change a Cluster Network Module Using Custom Values SMIT panel.

The Failure Detection Rate is made up of two components:

- cycles to fail (cycle): the number of heartbeats that must be missed before detecting a failure
- heartbeat rate (hbrate): the number of seconds between heartbeats.

Together, these two values determine the Failure Detection Rate. Before altering the Failure Detection Rate, note the following:

- Before altering the NIM, you should give careful thought to how much time you want to elapse before a real node failure is detected by the other nodes and the subsequent takeover is initiated.
- The Failure Detection Rate should be set equally for every NIM used by the cluster. The change must be synchronized across cluster nodes. The new values will become active the next time cluster services are started. To alter the Failure Detection Rate:
  - Identify the NIMs to be modified. All NIMs used in the cluster should be included.
  - To determine the NIMs in use, check the output from the \texttt{/usr/sbin/cluster/utilities/cllsif} command. For example:

```
cllsif -cS | cut -d':' -f4 | sort -u
ether
rs232
```

To Change the Attributes of a Network Module to Predefined Values:

If you are running standard HACMP, stop cluster services on all cluster nodes. If you are running HACMP/ES, you can use the DARE Resource Migration utility to change the attributes without stopping cluster services.

1. Enter \texttt{smitty hacmp}.
2. Select Cluster Configuration > Advanced Performance Tuning Parameters > Change/Show Network Modules > Change a Cluster Network Module Using Predefined Values and press Enter. SMIT displays a list of defined network modules.
3. Select the network module you want to change and press Enter. SMIT displays the attributes of the network module, with their current values.

<table>
<thead>
<tr>
<th>Network Module Name</th>
<th>Name of network type, for example, ether.</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Network Module Name</td>
<td>[]</td>
</tr>
<tr>
<td>Description</td>
<td>For example, Ethernet Protocol</td>
</tr>
</tbody>
</table>

Troubleshooting Guide
Failure Detection Rate  The default is Normal. Other options are Fast, and Slow. The failure cycle and the heartbeat rate determine how soon a failure can be detected. The time needed to detect a failure is calculated using this formula: (heartbeat rate) * (failure cycle).

Note: Whenever a change is made to any of the values that affect the failure detection time—failure cycle (FC), heartbeat rate (HB) or failure detection rate—the new value of these parameters is sent as an output to the screen in the following message:

SUCCESS: Adapter Failure Detection time is now FC * HB* 1 or SS seconds

Note: For HACMP/ES, the console message shows this formula:

SUCCESS: Adapter Failure Detection time is now FC * HB* 2 or SS seconds

4. Make the selections you need for your configuration and press Enter. If you set the Failure Detection Rate to Slow, Normal or Fast, the Heartbeat Rate and the Failure Cycle values will be set accordingly to Slow, Normal or Fast. SMIT executes the command to modify the values of these attributes in the ODM.

Although HACMP will detect an adapter failure in the time specified by the formula: Failure Detection Rate = Failure Cycle * Heartbeat Rate (or FC * HB* 2 for HACMP/ES), or very close to it, the software may not take action on this event for another few seconds.

5. Synchronize the Cluster Topology and resources from the node on which the change occurred to the other nodes in the cluster.

6. Run clverify to ensure that the change was propagated.

7. Restart the cluster services on all nodes to make the changes active.

Network Grace Period is the time period in which, after a network failure was detected, further network failures of the same type would be ignored. Network Grace Period is network specific and may also be set in SMIT. See the Administration Guide for the default values for each network type.

To Change the Attributes of a Network Module to Custom Values:
If setting the tuning parameters to one of the predefined values does not provide sufficient tuning, or if you wish to customize any other attribute of a network module, you may also change the Failure Detection Rate of a network module to a custom value by changing the Heartbeat Rate and the Failure Cycle from their predefined values to custom values.

Remember that after you customize the tuning parameters, you can always return to the original settings by using the SMIT panel for setting the tuning parameters to predefined values.

Note: The failure detection rate of the network module affects the deadman switch timeout. The deadman switch timeout is triggered one second before the failure is detected on the slowest network in your cluster.

To change the tuning parameters of a network module to custom values:
1. Stop cluster services on all cluster nodes.
2. Enter `smitty hacmp`
   SMIT displays a list of defined network modules.
4. Select the network module for which you want to change parameters and press Enter.
   SMIT displays the attributes of the network module, with their current values.

<table>
<thead>
<tr>
<th><strong>Network Module Name</strong></th>
<th>Name of network type, for example, ether.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>For example, Ethernet Protocol</td>
</tr>
<tr>
<td><strong>Address Type</strong></td>
<td>Toggle between two options in this field: Device and Address.</td>
</tr>
<tr>
<td></td>
<td>Address option specifies that the adapter which is associated with this network module uses an IP-typed address.</td>
</tr>
<tr>
<td></td>
<td>Device option specifies that the adapter which is associated with this network module uses a device file.</td>
</tr>
<tr>
<td><strong>Path</strong></td>
<td>This field specifies the path to the network executable file.</td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
<td>Enter any additional parameters below.</td>
</tr>
<tr>
<td><strong>Grace Period</strong></td>
<td>The current setting is the default for the network module selected. This is the time period in which, after a network failure was detected, further network failures of the same type would be ignored.</td>
</tr>
<tr>
<td><strong>Supports Gratuitous ARP</strong></td>
<td>Set this field to <strong>true</strong> if this network supports gratuitous ARP. Setting this field to <strong>true</strong> enables HACMP/ES to use the IPAT through IP Aliasing in the case of an adapter failure.</td>
</tr>
<tr>
<td><strong>Entry Type</strong></td>
<td>This field specifies the type of the adapter - either an adapter card (for a NIM specific to an adapter card), or an adapter type (for a NIM to use with a specific type of adapter).</td>
</tr>
<tr>
<td><strong>Next Generic Type</strong></td>
<td>This field specifies the next generic type of NIM to try to use if a more suitable NIM cannot be found.</td>
</tr>
<tr>
<td><strong>Next Generic Name</strong></td>
<td>This field specifies the next generic type of NIM to try to use if a more suitable NIM cannot be found.</td>
</tr>
<tr>
<td><strong>Supports Source Routing</strong></td>
<td>Set this field to <strong>true</strong> if this network supports source routing.</td>
</tr>
<tr>
<td><strong>Failure Cycle</strong></td>
<td>The current setting is the default for the network module selected. (Default for Ethernet is 10). This is the number of successive heartbeats that can be missed before the interface is considered to have failed. You can enter a number from 1 to 21474.</td>
</tr>
</tbody>
</table>
Releasing Large Amounts of TCP Traffic Causes DMS Timeout

Large amounts of TCP traffic over an HACMP-CONTROLLED service interface may cause AIX to experience problems when queuing and later releasing this traffic. When traffic is released, it generates a large CPU load on the system and prevents timing-critical threads from running, thus causing the Cluster Manager to issue a DMS timeout.

To reduce performance problems caused by releasing large amounts of TCP traffic into a cluster environment, consider increasing the Failure Detection Rate beyond Slow to a time that can handle the additional delay before a takeover. See the Administration Guide for more information and instructions on changing the Failure Detection Rate.

Also, to lessen the probability of a DMS timeout, complete the following steps before issuing a node_down:

1. Use the netstat command to identify the ports using an HACMP-controlled service adapter.
2. Use the ps command to identify all remote processes logged to those ports.
3. Use the kill command to terminate these processes.

A “device busy” Message Appears After node_up_local Fails

Problem
A device busy message in the /tmp/hacmp.out file appears when swapping hardware addresses between the boot and service address. Another process is keeping the device open.
Solution
Check to see if **sysinfod**, the SMUX peer daemon, or another process is keeping the device open. If it is **sysinfod**, restart it using the `-H` option.

Adapters Swap Fails Due to an `rmdev` “device busy” Error

**Problem**
Adapters swap fails due to an `rmdev device busy` error. For example, `/tmp/hacmp.out` shows a message similar to the following:

```
Method error (/etc/methods/ucfgdevice):
0514-062 Cannot perform the requested function because the specified device is busy.
```

**Solution**
Check to see whether the following applications are being run on the system. These applications may keep the device busy:

- **SNA**
  Use the following commands to see if SNA is running:
  ```
  lssrc -g sna
  ```

  Use the following command to stop SNA:
  ```
  stopsrc -g sna
  ```

  If that doesn’t work, use the following command:
  ```
  stopsrc -f -s sna
  ```

  If that doesn’t work, use the following command:
  ```
  /usr/bin/sna -stop sna -t forced
  ```

  If that doesn’t work, use the following command:
  ```
  /usr/bin/sna -stop sna -t cancel
  ```

- **Netview / Netmon**
  Ensure that the **sysmond** daemon has been started with a `-H` flag. This will result in opening and closing the adapter each time SM/6000 goes out to read the status, and allows the `cl_swap_HW_address` script to be successful when executing the `rmdev` command after the `ifconfig detach` before swapping the hardware address.

  Use the following command to stop all Netview daemons:
  ```
  /usr/OV/bin/nv6000_smit stopdaemons
  ```

- **IPX**
  Use the following commands to see if IPX is running:
  ```
  ps -ef | grep npsd
  ps -ef | grep sapd
  ```

  Use the following command to stop IPX:
  ```
  /usr/lpp/netware/bin/stopnps
  ```

- **Netbios**
  Use the following commands to see if Netbios is running:
  ```
  ps -ef | grep netbios
  ```
Use the following commands to stop Netbios and unload Netbios streams:

```
mcsadm stop; mcs0 unload
```

- Unload various streams if applicable (that is, if the file exists):

```
cd /etc
strload -uf /etc/dlpi.conf
strload -uf /etc/pse.conf
strload -uf /etc/netware.conf
strload -uf /etc/xtiso.conf
```

- Some customer applications will keep a device busy. Ensure that the shared applications have been stopped properly.

### MAC Address Is Not Communicated to the Ethernet Switch

**Problem**

With switched Ethernet networks, MAC address takeover sometimes appears to not function correctly. Even though HACMP has changed the MAC address of the adapter, the switch is not informed of the new MAC address. The switch does not then route the appropriate packets to the adapter.

**Solution**

Do the following to ensure that the new MAC address is communicated to the switch:

1. Modify the line in `/usr/sbin/cluster/etc/clinfo.rc` that currently reads:

   ```
   PING_CLIENT_LIST=" 
   ```

2. Include on this line the names or IP addresses of at least one client on each subnet on the switched Ethernet.

3. Run `clinfo` on all nodes in the HACMP cluster that are attached to the switched Ethernet.

   If you normally start HACMP cluster services using the `/usr/sbin/cluster/etc/rc.cluster` shell script, specify the `-i` option. If you normally start HACMP cluster services through SMIT, specify `yes` in the **Start Cluster Information Daemon?** field

### Client Issues

The following potential HACMP client issues are described here:

- Adapter Swap Causes Client Connectivity Problem
- Clients Cannot Find Clusters
- Clients Cannot Access Applications
- Clinfo Does Not Appear to Be Running
- Clinfo Does Not Report that a Node Is Down

### Adapter Swap Causes Client Connectivity Problem

**Problem**

The client cannot connect to the cluster. The ARP cache on the client node still contains the address of the failed node, not the fallover node.
Solution
Issue a `ping` command to the client from a cluster node to update the client’s ARP cache. Be sure to include the client name as the argument to this command. The `ping` command will update a client’s ARP cache even if the client is not running `clinfo`. You may need to add a call to the `ping` command in your applications’ pre- or post-event processing scripts to automate this update on specific clients. Also consider using hardware address swapping, since it will maintain configured hardware-to-IP address mapping within your cluster.

Clients Cannot Find Clusters

Problem
The `clstat` utility running on a client cannot find any clusters. The `clinfo` daemon has not properly managed the shared memory segment it created for its clients (like `clstat`) because it has not located a `clsmuxpd` with which it can communicate. Because `clinfo` gets its cluster status information from `clsmuxpd`, it will not be able to populate the HACMP MIB if it cannot communicate with this daemon. As a result, a variety of intermittent problems can occur between `clsmuxpd` and `clinfo`.

Solution
Update the `/usr/sbin/cluster/etc/clhosts` file to include the IP labels or addresses of cluster nodes. Ensure that the format for this information is just like that in the `/etc/hosts` file; for example, `beavis-trsvc` for labels and `140.186.152.117` for IP addresses. Also check the `/etc/hosts` file on the node on which `clsmuxpd` is running and on the node having problems with `clstat` or other `clinfo` API programs to ensure that localhosts are included.

The `clhosts` file on an HACMP client node should contain all boot and service names (or addresses) of HACMP servers accessible through logical connections to this client node. Upon startup, `clinfo` uses these names to attempt communication with a `clsmuxpd` process executing on an HACMP server.

**WARNING:** Do not include standby addresses in the `clhosts` file.

An example `/usr/sbin/cluster/etc/clhosts` file follows:

```bash
cowrie-en0-cl83# cowrie service
140.186.91.189 # limpet service
```

Clients Cannot Access Applications

Problem
The `clsmuxpd` utility failed.

Solution
Check the `/etc/hosts` file on the node on which `clsmuxpd` failed to ensure that it contains IP labels or addresses of cluster nodes. Also see Clients Cannot Find Clusters.

Clinfo Does Not Appear to Be Running

Problem
The service and boot addresses of the cluster node from which `clinfo` was started do not exist in the `/usr/sbin/cluster/etc/clhosts` file on the client.
Solving Common Problems

Solution
Include the cluster node service and boot addresses in the */usr/sbin/cluster/etc/hosts* file on the client before running the `clstat` command. Do not include other addresses because `clinfo` will take longer to start.

Clinfo Does Not Report that a Node Is Down

Problem
Even though the node is down, the `clsmuxpd` daemon and `clinfo` report that the node is up. All the node’s interfaces are listed as down.

Solution
When one or more nodes are active and another node tries to join the cluster, the current cluster nodes send information to the `clsmuxpd` daemon that the joining node is up. If for some reason, the node fails to join the cluster, `clinfo` does not send another message to the `clsmuxpd` daemon the report that the node is down.

To correct the cluster status information, restart the `clsmuxpd` daemon, using the options on the HACMP Cluster Services SMIT screen.

Miscellaneous Issues

The following non-categorized HACMP issues are described here:

- Limited Output when Running the `tail -f` Command on */tmp/hacmp.out*
- CDE Hangs After IPAT on HACMP Startup
- `cl_verify` Utility Gives Unnecessary Message
- `config_too_long` Message Appears
- Console Displays `clsmuxpd` Messages
- Device LEDs Flash “888” (System Panic)
- Resource Group Down though Highest Priority Node Up
- Unplanned System Reboots Cause Fallover Attempt to Fail
- Deleted or Extraneous Objects Appear in NetView Map
- F1 Doesn’t Display Help in SMIT Screens
- */usr/es/sbin/cluster/cl_event_summary.txt* File (Event Summaries Display) Grows Too Large
- Display Event Summaries does not Display Resource Group Information as Expected

Limited Output when Running the `tail -f` Command on */tmp/hacmp.out*

Problem
Only script start messages appear in the */tmp/hacmp.out* file. The script specified in the message is not executable, or the DEBUG level is set to low.

Solution
Add executable permission to the script using the `chmod` command, and make sure the DEBUG level is set to high.
CDE Hangs After IPAT on HACMP Startup

Problem
If CDE is started before HACMP is started, it binds to the boot address. When HACMP is started it swaps the IP address to the service address. If CDE has already been started this change in the IP address causes it to hang.

Solution
- The output of `hostname` and the `uname -n` must be the same. If the output is different, use `uname -S hostname` to make the `uname` match the output from `hostname`.
- Define an alias for the `hostname` on the loopback address. This can be done by editing `/etc/hosts` to include an entry for:
  
  ```
  127.0.0.1   loopback localhost hostname
  ```

  where `hostname` is the name of your host. If name serving is being used on the system edit the `/etc/netsvc.conf` file such that the local file is checked first when resolving names.
- Ensure that the `hostname` and the service IP label resolve to different addresses. This can be determined by viewing the output of the `/bin/host` command for both the `hostname` and the service IP label.

cl_verify Utility Gives Unnecessary Message

Problem
You get the following message in `cl_verify` regardless of whether or not you have configured Auto Error Notification:

“Remember to redo automatic error notification if configuration has changed.”

Solution
Ignore this message if you have not configured Auto Error Notification.

config_too_long Message Appears

This message appears each time a cluster event takes more time to complete than a specified time-out period.

In versions prior to 4.5, the time-out period was fixed for all cluster events and set to 360 seconds by default. If a cluster event, such as a node_up or a node_down event, lasted longer than 360 seconds, then every 30 seconds HACMP issued a config_too_long warning message that was logged in the `hacmp.out` file.

In HACMP and HACMP/ES 4.5, you can customize the time period allowed for a cluster event to complete before HACMP issues a system warning for it.

If this message appears, in the hacmp.out Event Start you see:

`config_too_long $sec $event_name $argument`

- `$event_name` is the reconfig event that failed
- `$argument` is the parameter(s) used by the event
- `$sec` is the number of seconds before the message was sent out
In versions prior to HACMP and HACMP/ES 4.5, `config_too_long` messages continued to be appended to the `hacmp.out` file every 30 seconds until action was taken.

Starting with version 4.5, for each cluster event that does not complete within the specified event duration time, `config_too_long` messages are logged in the `hacmp.out` file and sent to the console according to the following pattern:

- the first five `config_too_long` messages appear in the `hacmp.out` file at 30 second intervals
- the next set of five messages appears at interval that is double the previous interval until the interval reaches one hour
- then these messages are logged every hour until the event is complete or is terminated on that node.

This message could appear in response to the following problems:

**Problem**
Activities that the script is performing take longer than the specified time to complete; for example, this could happen with events involving many disks or complex scripts.

**Solution**
- Determine what is taking so long to execute, and correct or streamline that process if possible.
- Increase the time to wait before calling `config_too_long`.

You can customize Event Duration Time using the Change/Show Time Until Warning panel in SMIT. You access this panel through two different pathways: Cluster Resources > Cluster Events, or Cluster Configuration > Advanced Performance Tuning Parameters.

For complete information on tuning event duration time, see Chapter 9 in the Administration Guide, or Chapter 18 in the Enhanced Scalability Installation and Administration Guide.

**Problem**
A command is hung and event script is waiting before resuming execution. If so, you can probably see the command in the AIX process table (`ps -ef`). It is most likely the last command in the `/tmp/hacmp.out` file, above the `config_too_long` script output.

**Solution**
May need to kill the hung command.

**Console Displays clsmuxpd Messages**

**Problem**
The `/etc/syslogd` file has been changed to send the `daemon.notice` output to `/dev/console`.

**Solution**
Edit the `/etc/syslogd` file to redirect the `daemon.notice` output to `/usr/tmp/snmpd.log`. The `snmpd.log` file is the default location for logging messages.
Device LEDs Flash “888” (System Panic)

Problem
The crash system dump device with stat subcommand indicates the panic was caused by the HACMP deadman switch. The Cluster Manager cannot obtain sufficient time to process CPU cycles during intensive operations (df, find, for example) and may be required to wait too long for a chance at the kernel lock. Often, more than five seconds will elapse before HACMP can get a lock. The results are the invocation of the deadman switch and a system panic.

Solution
Determine what process is hogging CPU cycles on the system that panicked. Then attempt (in order) each of the following solutions that address this problem:

1. Tune the system using I/O pacing.
2. Increase the syncd frequency.
3. Change the Failure Detection Rate.

Tuning the System Using I/O Pacing
Use I/O pacing to tune the system so that system resources are distributed more equitably during large disk writes. Enabling I/O pacing is required for an HACMP cluster to behave correctly during large disk writes, and it is strongly recommended if you anticipate large blocks of disk writes on your HACMP cluster.

To change the I/O pacing settings:

1. Enter smitty hacmp > Cluster Configuration > Advanced Performance Tuning Parameters > Change/Show I/O Pacing
2. Configure the entry fields with the recommended HIGH and LOW watermarks:

   HIGH water mark for pending write 33 is recommended for most clusters. Possible values are 0 to 32767.
   LOW watermark for pending write 24 is recommended for most clusters. Possible values are 0 to 32766.

While the most efficient high- and low-water marks vary from system to system, an initial high-water mark of 33 and a low-water mark of 24 provide a good starting point. These settings only slightly reduce write times, and consistently generate correct fallover behavior from HACMP. If a process tries to write to a file at the high-water mark, it must wait until enough I/O operations have finished to make the low-water mark. See the AIX Performance Monitoring & Tuning Guide for more information on I/O pacing.

Extending the syncd Frequency
Increase the syncd frequency from its default value of 60 seconds to either 30, 20, or 10 seconds. Increasing the frequency forces more frequent I/O flushes and reduces the likelihood of triggering the deadman switch due to heavy I/O traffic.

To change the syncd frequency setting:

1. Enter smitty hacmp > Cluster Configuration > Advanced Performance Tuning Parameters > Change/Show syncd frequency
2. Configure the entry fields with the recommended `syncd` frequency:

   syncd frequency in seconds  10  is recommended for most clusters. Possible values are 0 to 32767.

**Increase Amount of Memory Available for Communications Subsystem**

If the output of `netstat -m` reports that requests for mbufs are being denied, or if errors indicating `LOW_MBUFS` are being logged to the AIX error report, increase the value associated with “thewall” network option. The default value is 25% of the real memory. This can be increased to as much as 50% of the real memory.

To change this value, add a line similar to the following at the end of the `/etc/rc.net` file:

```
no -o thewall=xxxxx
```

where `xxxxx` is the value you want to be available for use by the communications subsystem. For example,

```
no -o thewall=10240
```

**Changing the Failure Detection Rate to Predefined Values Using SMIT**

Use the SMIT Change/Show a Cluster Network Module > Change a Cluster Network Module Using Predefined Values screen to change the Failure Detection Rate for your network module only if enabling I/O pacing or extending the `syncd` frequency did not resolve deadman problems in your cluster. By changing the Failure Detection Rate to `Slow`, you can extend the time required before the deadman switch is invoked on a hung node and before a takeover node detects a node failure and acquires a hung node’s resources.

**WARNING:** Keep in mind that the `Slow` setting for the Failure Detection Rate is network specific, and may vary.

**Changing the Failure Detection Rate Beyond Fast/Normal/Slow Settings**

If your system needs to withstand a performance hit or outage longer than that achieved by setting all associated NIMs to `Slow`, you can specify a slower Failure Detection Rate by altering the HACMPnim ODM class. To do this, select custom settings for Heartbeat Rate and Failure Cycle in the Change a Cluster Network Module Using Custom Values SMIT panel.

The Failure Detection Rate is made up of two components:

- `cycles to fail (cycle)`: the number of heartbeats that must be missed before detecting a failure
- `heartbeat rate (hbrate)`: the number of microseconds between heartbeats.

Together, these two values determine the Failure Detection Rate. For example, for a NIM with an `hbrate` of 1,000,000 microseconds and a cycle value of 12, the Failure Detection Rate would be 12 (1 second x 12 cycles).

Before altering the Failure Detection Rate, note the following:

- Before altering the NIM, you should give careful thought to how much time you want to elapse before a real node failure is detected by the other nodes and the subsequent takeover is initiated.
- The Failure Detection Rate should be set equally for every NIM used by the cluster. The change must be synchronized across cluster nodes. The new values will become active the next time cluster services are started. To alter the Failure Detection Rate:
- Identify the NIMs to be modified. All NIMs used in the cluster should be included.
To determine the NIMs in use, check the output from the `/usr/sbin/cluster/utilities/cllsif` command. For example:

```bash
cllsif -cS | cut -d':' -f4 | sort -u
ether
rs232
```

**To Change the Attributes of a Network Module to Predefined Values:**

If you are running standard HACMP, stop cluster services on all cluster nodes. If you are running HACMP/ES, you can use the DARE Resource Migration utility to change the attributes without stopping cluster services.

1. Enter `smitty hacmp`.
2. Select `Cluster Configuration > Advanced Performance Tuning Parameters > Change/Show Network Modules > Change a Cluster Network Module Using Predefined Values` and press Enter. SMIT displays a list of defined network modules.
3. Select the network module you want to change and press Enter. SMIT displays the attributes of the network module, with their current values.

   **Network Module Name**  Name of network type, for example, ether.

   **New Network Module Name**  

   **Description**  For example, Ethernet Protocol

   **Failure Detection Rate**  The default is Normal. Other options are Fast, and Slow. The failure cycle and the heartbeat rate determine how soon a failure can be detected. The time needed to detect a failure is calculated using this formula: (heartbeat rate) * (failure cycle).

   **Note:**  For HACMP, whenever a change is made to any of the values that affect the failure detection time - failure cycle (FC), heartbeat rate (HB) or failure detection rate - the new value of these parameters is sent as an output to the screen in the following message:

   SUCCESS: Adapter Failure Detection time is now FC * HB* 1 or SS seconds

   **Note:**  For HACMP/ES, the following message is sent as an output to the screen:

   SUCCESS: Adapter Failure Detection time is now FC * HB* 2 or SS seconds

4. Make the selections you need for your configuration and press Enter. If you set the Failure Detection Rate to Slow, Normal or Fast, the Heartbeat Rate and the Failure Cycle values will be set accordingly to Slow, Normal or Fast. SMIT executes the command to modify the values of these attributes in the ODM.
Although HACMP will detect an adapter failure in the time specified by the formula:
\[ \text{Failure Detection Rate} = \text{Failure Cycle} \times \text{Heartbeat Rate} \] (or \( FC \times HB \times 2 \) for HACMP/ES), or very close to it, the software may not take action on this event for another few seconds.

5. Synchronize the Cluster Topology and resources from the node on which the change occurred to the other nodes in the cluster.

6. Run `clverify` to ensure that the change was propagated.

7. Restart the cluster services on all nodes to make the changes active.

Network Grace Period is the time period in which, after a network failure was detected, further network failures of the same type would be ignored. Network Grace Period is network specific and may also be set in SMIT. See the *Administration Guide* for the default values for each network type.

**To Change the Attributes of a Network Module to Custom Values:**

If setting the tuning parameters to one of the predefined values does not provide sufficient tuning, or if you wish to customize any other attribute of a network module, you may also change the Failure Detection Rate of a network module to a custom value by changing the Heartbeat Rate and the Failure Cycle from their predefined values to custom values.

Remember that after you customize the tuning parameters, you can always return to the original settings by using the SMIT panel for setting the tuning parameters to predefined values.

**Note:** The failure detection rate of the network module affects the deadman switch timeout. The deadman switch timeout is triggered one second before the failure is detected on the slowest network in your cluster.

To change the tuning parameters of a network module to custom values:

1. Stop cluster services on all cluster nodes.
2. Enter `smitty hacmp`
3. Select **Cluster Topology > Configure Network Modules > Change a Cluster Network Module Using Custom Values**.
   SMIT displays a list of defined network modules.
4. Select the network module for which you want to change parameters and press Enter.
   SMIT displays the attributes of the network module, with their current values.

<table>
<thead>
<tr>
<th>Network Module Name</th>
<th>Name of network type, for example, ether.</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Network Module Name</td>
<td>[]</td>
</tr>
<tr>
<td>Description</td>
<td>For example, Ethernet Protocol</td>
</tr>
<tr>
<td>Address Type</td>
<td><strong>Address</strong> or <strong>Device</strong>. Toggle to select the correct type.</td>
</tr>
<tr>
<td>Path</td>
<td>Actual pathname of the network module, for example <code>/usr/sbin/cluster/nims/nim_ether</code></td>
</tr>
</tbody>
</table>
Solving Common Problems

Miscellaneous Issues

Parameters
Any optional parameters passed to the network module executable. This field is typically empty.

Grace Period
The current setting is the default for the network module selected. This is the time period in which, after a network failure was detected, further network failures of the same type would be ignored.

Failure Cycle
The current setting is the default for the network module selected. (Default for Ethernet is 20). This is the number of successive heartbeats that can be missed before the interface is considered to have failed. You can enter a number from 1 to 21474.

Heartbeat Rate
The current setting is the default for the network module selected. This parameter tunes the interval (in seconds) between heartbeats for the selected network module. You can enter a number from 1 to 21474.

Note: Whenever a change is made to any of the values that affect the failure detection time - failure cycle (FC), heartbeat rate (HB) or failure detection rate - the new value of these parameters is sent as output to the screen in the following message:

SUCCESS: Adapter Failure Detection time is now FC * HB* 1 or SS seconds

5. Make the changes you want for your configuration.

Although HACMP will detect an adapter failure in the time specified by the formula:
Failure Detection Rate = Failure Cycle * Heartbeat Rate (or FC * HB * 2 for HACMP/ES), or very close to it, the software may not take action on this event for another few seconds.

6. Changes made in this panel must be propagated to the other nodes by synchronizing topology. On the local node, synchronize the cluster topology. Return to the SMIT Cluster Topology menu and select the Synchronize Cluster Topology option.

The configuration data stored in the DCD on each cluster node is updated and the changed configuration becomes the active configuration when cluster services are started.

Contact your IBM Support representative for help with any of the preceding solutions.

Resource Group Down though Highest Priority Node Up

Problem
You may encounter situations when a resource group which is down is dependent on the highest priority node to bring it online, but the highest priority node is already up. Since no subsequent node which comes up will acquire the resource group, the resource group will remain in an inactive state.

This situation occurs:
• If a cascading resource group with cascading without fallback set to true, is placed on a non-highest priority node, and that node is brought down with a graceful shutdown or a cldare stop
• If you use cldare stop to bring down a cascading resource group which is assigned an inactive takeover value of false and resides on the highest priority node.

Solution
Unless you bring the resource group up manually, it will remain in an inactive state.

To bring the resource group back up:
1. Enter smitty hacmp at the command line.
2. Choose Cluster System Management > Cluster Resource Group Management > Bring a Resource Group Online
3. Select the appropriate resource group.

Unplanned System Reboots Cause Fallover Attempt to Fail

Problem
Cluster nodes did not fallover after rebooting the system.

Solution
To prevent unplanned system reboots from disrupting a fallover in your cluster environment, all nodes in the cluster should either have the Automatically REBOOT a system after a crash field on the Change/Show Characteristics of Operating System SMIT screen set to false, or you should keep the RS/6000 key in Secure mode during normal operation.

Both measures prevent a system from rebooting if the shutdown command is issued inadvertently. If neither measure is used and an unplanned reboot occurs, the activity against the disks on the rebooting node can prevent other nodes from successfully acquiring the disks.

Deleted or Extraneous Objects Appear in NetView Map

Problem
Previously deleted or extraneous object symbols appeared in the NetView map.

Solution
Rebuild the NetView database.

Perform the following steps on the NetView server:
1. Stop all NetView daemons: /usr/OV/bin/ovstop -a
2. Remove the database from the NetView server: rm -rf /usr/OV/database/*
3. Start the NetView object database: /usr/OV/bin/ovstart ovwdb
4. Restore the NetView/HAView fields: /usr/OV/bin/ovw -fields
5. Start all NetView daemons: /usr/OV/bin/ovstart -a
F1 Doesn’t Display Help in SMIT Screens

Problem
Pressing F1 in SMIT screen doesn’t display help.

Solution
Help can be displayed only if the LANG variable is set to one of the languages supported by HACMP, and if the associated HACMP message catalogs are installed. The languages supported by HACMP Version 4.5 are:

en_US ja_JP
En_US Ja_JP

To list the installed locales (the bsl LPPs), type:
locale -a
To list the active locale, type:
locale
Since the LANG environment variable determines the active locale, if LANG=en_US, the locale is en_US.

/usr/es/sbin/cluster/cl_event_summary.txt File (Event Summaries Display) Grows Too Large

Problem
In HACMP/ES, event summaries are pulled from the hacmp.out file and stored in the cl_event_summary.txt file. This file continues to accumulate as hacmp.out cycles, and is not automatically truncated or replaced. Consequently, it can grow too large and crowd your /usr directory.

Solution
HACMP/ES users should clear event summaries periodically, using the Clear Event Summary History option in SMIT.

Display Event Summaries does not Display Resource Group Information as Expected

Problem
In HACMP/ES, event summaries are pulled from the hacmp.out file and can be viewed using the Display Event Summaries option in SMIT. This display includes resource group status and location information at the end. The resource group information is gathered by clfindres, and may take extra time if the cluster is not running when the Display Event Summaries option is run.

Solution
clfindres displays resource group information much more quickly when the cluster is running. If the cluster is not running, wait a few minutes and the resource group information will eventually appear.
Appendix A: HACMP Messages

The HACMP daemons, scripts, Cluster Single Point of Control (C-SPOC), DARE, and Event Emulator commands, and HAView browser generate messages that are displayed on the system console and written to various log files. This appendix explains the messages that appear. See Chapter 2: Examining Cluster Log Files, for more information about the general content and purpose of the log files.

Overview

This appendix first identifies the HACMP components and C-SPOC commands that generate messages, and then lists the messages. The messages are organized by subsystem, and listed alphabetically within each subsystem. Each listing includes information about the meaning of the message, possible causes, and, where possible, provides suggestions for resolving a problem.

HACMP Daemons

The HACMP software includes the following daemons that generate messages:

- Cluster Manager (clstrmgr)
- Cluster Information Program (clinfo)
- Cluster Lock Manager (cllockd)
- Cluster SMUX Peer (clsmuxpd).

Use the /usr/sbin/cluster/utilities/clm_stats command to check for current information about the number of locks, resources, and amount of memory usage. See the Administration Guide for more information.

HACMP Scripts

The HACMP software includes many scripts that generate messages. The following sections list these scripts by category.

Startup Scripts

The following HACMP startup and stop scripts generate messages:

- clexit.rc
- clstart.sh
- clstop.sh

Utility Scripts

The HACMP software includes many utility scripts that are called by the event scripts:

General Disk Utilities

cl_disk_available
## SCSI Disk Subsystem Utilities

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>cl_scdiskreset</code></td>
<td></td>
</tr>
<tr>
<td><code>cl_scdiskrsrv</code></td>
<td></td>
</tr>
<tr>
<td><code>cl_is_scsidisk</code></td>
<td></td>
</tr>
<tr>
<td><code>cl_pscsilunreset</code></td>
<td></td>
</tr>
<tr>
<td><code>cl_scsi_convaryonvg</code></td>
<td></td>
</tr>
<tr>
<td><code>cl_fscsilghost</code></td>
<td></td>
</tr>
<tr>
<td><code>cl_fscsilunreset</code></td>
<td></td>
</tr>
</tbody>
</table>

## RAIDiant Disk Array Subsystem Utilities

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>cl_array_mode3</code></td>
<td></td>
</tr>
<tr>
<td><code>cl_is_array</code></td>
<td></td>
</tr>
<tr>
<td><code>cl_is_fcparray</code></td>
<td></td>
</tr>
<tr>
<td><code>cl_mode3</code></td>
<td></td>
</tr>
</tbody>
</table>

## File System Utilities

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>cl_activate_fs</code></td>
<td></td>
</tr>
<tr>
<td><code>cl_activate_nfs</code></td>
<td></td>
</tr>
<tr>
<td><code>cl_deactivate_fs</code></td>
<td></td>
</tr>
<tr>
<td><code>cl_deactivate_nfs</code></td>
<td></td>
</tr>
<tr>
<td><code>cl_get_disk_vg_fs_pvids</code></td>
<td></td>
</tr>
<tr>
<td><code>cl_nfskill</code></td>
<td></td>
</tr>
<tr>
<td><code>cl_export_fs</code></td>
<td></td>
</tr>
<tr>
<td><code>cl_fs2disk</code></td>
<td></td>
</tr>
</tbody>
</table>

## Volume Group Utilities

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>cl_activate_vgs</code></td>
<td></td>
</tr>
<tr>
<td><code>cl_deactivate_vgs</code></td>
<td></td>
</tr>
<tr>
<td><code>convaryonvg</code></td>
<td></td>
</tr>
<tr>
<td><code>cl_sync_vgs</code></td>
<td></td>
</tr>
</tbody>
</table>

## Network Utilities

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>cl_hats_adapter</code></td>
<td></td>
</tr>
<tr>
<td><code>cl_swap_ATM_HW_address</code></td>
<td></td>
</tr>
<tr>
<td><code>cl_swap_ATMLE_HW_address</code></td>
<td></td>
</tr>
<tr>
<td><code>cl_swap_HW_address</code></td>
<td></td>
</tr>
<tr>
<td><code>cl_swap_ATM_IP_address</code></td>
<td></td>
</tr>
<tr>
<td><code>cl_swap_IP_address</code></td>
<td></td>
</tr>
<tr>
<td><code>cl_unswap_HW_address</code></td>
<td></td>
</tr>
</tbody>
</table>

## Startup Utilities

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>start_clmarketdemo</code></td>
<td></td>
</tr>
<tr>
<td><code>stop_clmarketdemo</code></td>
<td></td>
</tr>
<tr>
<td><code>start_imagedemo</code></td>
<td></td>
</tr>
<tr>
<td><code>stop_imagedemo</code></td>
<td></td>
</tr>
</tbody>
</table>

## SP Utilities

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>cl_Eprimary_HPS_app</code></td>
<td></td>
</tr>
<tr>
<td><code>cl_HPS_init</code></td>
<td></td>
</tr>
</tbody>
</table>
The HACMP software includes many utilities, some of which generate messages. Messages for the following utilities are described in the following sections:

- Cluster Single Point of Control (C-SPOC)
- Dynamic Reconfiguration (DARE)
- Event Emulator
- HAView

**HACMP C-SPOC Messages**

C-SPOC messages are generated by the C-SPOC initialization and verification routine, `cl_init.cel`, the Command Execution Language (CEL) preprocessor (`celpp`), and C-SPOC commands. This section describes only the C-SPOC commands that generate messages.

**C-SPOC Commands**

All C-SPOC commands generate messages. Most messages, however, are based on an underlying AIX command’s output. To identify the underlying AIX command, see the man page for each command in the `/usr/man/cat1` directory. To see examples of command usage, see the Administration Guide.

**C-SPOC User and Group Commands**

The following C-SPOC commands generate messages specific to user and group tasks:

- `cl_chuser`
- `cl_lsuser`
- `cl_rmgp`  
- `cl_chgroup`  
- `cl_mkgroup`  
- `cl_rmuser`  
- `cl_lsgroup`  
- `cl_mkuser`  

**C-SPOC Logical Volume Manager and File System Commands**

The following C-SPOC commands generate messages specific to logical volume and file system tasks:

- `cl_chfs`
- `cl_lslv`  
- `cl_rmlv`
HACMP Messages

The following messages are generated by HACMP scripts and utilities:

cl_activate_fs: Failed fsck -p of file system_name.

The fsck -p command failed while checking the named file system. Possible reasons include an incorrect file system name in the ODM, or the file system no longer exists.

cl_activate_nfs: Backgrounding attempted mount of host_name:file system_name.

The attempt to mount the named file system is being performed in the background.

cl_activate_nfs: Failed mount of host_name:file system_name.

The named file system could not be mounted. Make sure the local node can communicate with the NFS server and that the NFS server is exporting the file system correctly.

cl_activate_nfs: Failed mount of host_name:file system_name after 1 attempts.

The named file system could not be mounted.

cl_activate_nfs: Mount of host_name:file system_name failed again, still re-trying.

The mount of the named file system failed but the system is retrying it.

cl_activate_vgs: Failed varyonvg of volumegroup_name.

The varyonvg command was unable to vary on (make active) the named volume group. Possible reasons include loss of quorum, or the volume group could already be active on this or another system. See Chapter 3: Investigating System Components, for more information.

cl_activate_vgs: Unable to varyon concurrent RAID volume group volumegroup_name.

The attempt to vary on the named volume group failed. The volume group is a concurrent volume group defined on an IBM Disk Array. You must use the convaryonvg command to vary on a concurrent volume group on a disk array.

cl_array_mode3: Failed convaryonvg of volume group volumegroup_name.

The convaryonvg command was unable to vary on (make active) the named volume group. Possible reasons include loss of quorum, or the volume group could already be active on this or another system.

cl_deactivate_fs: Failed obtaining logical volume for file system_name from ODM.

The system was unable to determine the logical volume on which the file system is mounted. See Chapter 3: Investigating System Components, to determine if logical volume and file system name mismatches exist.

cl_deactivate_fs: Failed umount of file system_name.
The **unmount** command was unable to unmount the named file system. The device is probably busy. Use the **fuser -k** command to force the unmount, or see Chapter 3: Investigating System Components, to determine if logical volume and file system name mismatches exist.

```
cl_deactivate_vgs: Failed varyoff of volumegroup_name.
```

The **varyoffvg** command was unable to vary off (deactivate) the named volume group. The logical volumes must first be closed. For example, if the volume group contains a file system, the file system must be unmounted. Another possibility is that the file system was never varied on. See Chapter 3: Investigating System Components, for more information.

```
cl_deactivate_vgs: Volume group volumegroup_name already varied off.
```

The named volume group is already varied off.

```
cl_disk_available: Concurrent disk array is reserved, unable to use disk_name.
```

The disk specified is part of a concurrent disk array that is reserved. The specified disk cannot be accessed.

```
cl_disk_available: Failed reset/reserve for device: disk_name.
```

The SCSI device on which the named disk is defined and available could not be reset, or it could not be reserved and reset, if it was already reserved.

```
cl_disk_available: Failed reset for device: disk_name.
```

The IBM SSA device on which the named disk is defined could not be reset.

```
cl_disk_available: Undefined disk device: disk_name.
```

The system tried to reset the disk subsystem but the named device was not defined. See Chapter 3: Investigating System Components, to determine whether the named hdisk is listed.

```
cl_disk_available: Unable to make device disk_name available. Check hardware connections.
```

The **mkdev** command was unable to make a physical disk available. A hardware problem is the most likely source of the error. Another possibility is that there are duplicate entries for the same disk. See Chapter 3: Investigating System Components, to determine if the named hdisk is listed.

```
clexit: Unexpected termination of ${SSYS}
```

The **clexit** script is called when any element of a lock or cluster group exits abnormally. The hacmp6000 initab entry may have been removed. See Chapter 2: Examining Cluster Log Files, for information on determining the source of a system error.

```
clexit: Halting system immediately!!!
```

The **clexit** script generates this message just before it executes the **clstop** script.

```
cl_export_fs: Unable to export file system_name.
```

The **exportfs** command was unable to export the file system named in the command. Possible reasons include an incorrect file system name passed as an argument, the file system does not exist, or the file system is not mounted locally. See Chapter 3: Investigating System Components, to determine whether the file system exists.

```
cl_export_fs: Unable to start rpc.mountd via SRC.
```

The System Resource Controller was unable to start the **rpc.mountd** daemon. Use the **lssrc -a** command to make sure that the subsystem is listed in the subsystem object class and is inoperative before using the **cl_export_fs** command.
cl_fs2disk: ODMErrNo: err_number; Retrieval of ODM error message failed.

An error was encountered while the system was attempting to retrieve the text of an ODM error message.

cl_fs2disk: Unable to find classname object with criteria.

The system was unable to retrieve information of type specified by criteria from the ODM entries for class indicated by classname.

cl_fs2disk: ODM failure getting classname object(s).

The system was unable to retrieve information about the class specified.

cl_fs2disk: ODMErrNo: err_number: error_message.

The system was unable to retrieve information about the class specified.

cl_is_array: Device disk_name not configured.

The system is attempting to determine whether a disk is an IBM 7135-210 RAIDiant Disk Array but the lsparent command could not find the device in the ODM.

cl_is_scsidisk: Device disk_name not configured.

The system is attempting to determine whether a disk is a SCSI disk, but the lsparent command could not find the device in the ODM.

cl_nm_nis_on: Unable to turn name serving ON.

The system attempted to turn on name serving using the /usr/bin/namerslv command and it failed.

cl_nm_nis_on: Unable to turn ypbind (NIS) ON.

The system attempted to turn on Network Information Systems using the /usr/bin/startsrc command and it failed.

cl_nm_nis_off: Unable to turn name serving OFF.

The system attempted to turn off name serving using the /usr/bin/namerslv command and it failed.

cl_nm_nis_on: Unable to turn ypbind (NIS) OFF.

The system attempted to turn off NIS using the /usr/bin/stopsrc command and it failed.

cl_raid_vg: Invalid volume group volume_group_name.

There is no physical volume information in the ODM for the volume group specified. See Chapter 3: Investigating System Components, to determine that the named volume group exists.

clstart: called with flags arguments

The clstart script, which starts the cluster daemons, has been called. The arguments passed to clstart specify which daemons to start. Here are the flags and the daemons they represent:

<table>
<thead>
<tr>
<th>Flag</th>
<th>Daemon</th>
</tr>
</thead>
<tbody>
<tr>
<td>-i</td>
<td>clinfo</td>
</tr>
</tbody>
</table>
clstart: Unable to start Cluster Information Program (clinfo) via SRC.  

The **clstart** script could not start the **clinfo** daemon using the **startsrc** command.

clstart: Unable to start Cluster Lock Manager (clclockd) via SRC.  

The **clstart** script could not start the **clclockd** daemon using the **startsrc** command.

clstart: Unable to start Cluster Manager (clstrmgr) via SRC.  

The **clstart** script could not start the Cluster Manager daemon. See Chapter 4: Solving Common Problems, for information on starting the cluster manager.

clstart: Unable to start Cluster SMUX Peer Daemon (clsmuxpd) without snmpd.  

The **clstart** script could not start the clsmuxpd daemon without the SNMP daemon.

clstart: Unable to start Cluster SMUX Peer Daemon (clsmuxpd) via SRC.  

The **clstart** script could not start the **clsmuxpd** daemon using the **startsrc** command.

clstop: called with flags command arguments

The **clstop** script stops the cluster daemons. The arguments passed to **clstart** specify the manner of cluster shutdown:

<table>
<thead>
<tr>
<th>Argument</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>-f</td>
<td>Forced stop</td>
</tr>
<tr>
<td>-g</td>
<td>Graceful down, no takeover by other node</td>
</tr>
<tr>
<td>-g[r]</td>
<td>Graceful down, release resources</td>
</tr>
<tr>
<td>-s</td>
<td>Do not broadcast the shutdown via <code>/bin/wall</code></td>
</tr>
<tr>
<td>-y</td>
<td>Do not ask for confirmation of process-shutdown</td>
</tr>
<tr>
<td>-N</td>
<td>Stop now</td>
</tr>
<tr>
<td>-R</td>
<td>Stop on subsequent system restart (remove <code>inittab</code>)</td>
</tr>
<tr>
<td>-B</td>
<td>Stop now and on subsequent system restart.</td>
</tr>
</tbody>
</table>

clstop: Ignoring obsolete -i option

The -i option, which caused the **clstop** command to stop the cluster immediately, is obsolete and ignored.

clstop: Ignoring obsolete -t option

The -t option, which specified a wait time, is obsolete and ignored.

clstop: Shutting down Cluster Group. Continue [y/n]?  

The confirmation message generated by the **clstop** script before shutdown.

clstop: Shutdown not confirmed by operator.
The `clstop` script received negative confirmation of the shutdown message it displays before shutdown.

`cl_swap_HW_address: failed chdev on device_name`.  
The `chdev` command failed trying to change the specified device. Use the `lsdev` command to make sure that the identified interface is available.

`cl_swap_HW_address: failed mkdev on device_name`.  
The `ifconfig` command failed. Use the `lsdev` command to make sure that the interface identified in the message is available.

`cl_swap_HW_address: failed rmdev on device_name`.  
The `rmdev` command failed when trying to remove the device specified. Use the `lsdev` command to make sure that the interface identified in the message is available.

`cl_swap_HW_address: Invalid interface name`.  
The interface name specified does not contain an integer between 0 and 9.

`cl_swap_HW_address: Invalid interface type`.  
The interface type specified is not a supported device type. The supported interface types are:

```
en     Ethernet
et     Ethernet
tr      Token-Ring
fi      FDDI
```

`cl_swap_HW_address: Unable to make device name for interface interface_name`.  
The `mkdev` command failed for the interface name specified in the message. Use the `lsdev -Cc interface` command to make sure that the interface identified in the message is available.

`cl_swap_IP_address: Failed ifconfig interface_name inet address netmask netmask up`.  
The `ifconfig` command failed. Use the `lsdev` command to make sure that the interface identified in the message is available.

`cl_sync_vgs: Failed syncvg of volumegroup_name`.  
The volume group specified could not be synchronized.

`cl_sync_vgs: Volume group volumegroup_name not varied on. Syncvg not attempted`.  
The volume group specified could not be synchronized because it was not varied on.

`clvaryonvg: Device disk_name is not available for concurrent use`.  
The disk on which the volume group is defined is reserved.

`convaryonvg: Unable to varyon volume group volumegroup_name for concurrent use`.  
The `convaryonvg` command failed.

`nodeA: Couldn’t obtain information from LVM for logical volume, id=000472486e119e8a`.  

Automatic Error Notification could not add an error notify method on `nodeA` because the cluster was running. Cluster must be down when configuring Automatic Error Notification.

`missing node mapping`
This is an internal error that should be reported to IBM support.

\texttt{name needs root privileges to run}

The following programs can be run only by a system administrator or someone with root privileges: \texttt{genodm, fence, getbit, clear}.

\texttt{no fence bit set on device_name}.

This is an internal error that should be reported to IBM support.

\texttt{PVID device_name is not on a serial DASD}.

This is an internal error that should be reported to IBM support. The message only occurs during configuration or reconfiguration.

\texttt{start_clmarketdemo: Database file database_file does not exist}.

The \texttt{clmarket} demo program requires a database file and the database file specified does not exist.

\texttt{start_clmarketdemo: Logfile logfile does not exist}.

The \texttt{clmarket} demo program requires a log file and the log file specified does not exist.

\texttt{start_clmarketdemo: clclockd must be running for demo}.

The Cluster Lock Manager daemon must be running to run the \texttt{clmarket} demo program.

\texttt{start_clmarketdemo: marserv already running}.

The server program, named \texttt{marserv}, associated with the \texttt{clmarket} demo program is already running. If it is not running, the \texttt{start_clmarketdemo} script starts it.

\texttt{start_imagedemo: clclockd must be running for demo}.

The Cluster Lock Manager daemon must be running to run the image demo program.

\texttt{start_imagedemo: imserv_image_location does not exist}.

The location of the image files is incorrect.

\texttt{stop_clmarketdemo: Sending sigkill to marserv PID: process_ID}.

The \texttt{stop_clmarketdemo} script is attempting to stop the server program associated with the \texttt{clmarket} demo program by using the \texttt{kill -9} command.

\texttt{stop_clmarketdemo: marserv PID not found}.

The \texttt{stop_clmarketdemo} script could not find the PID of the server program, named \texttt{marserv}, that is associated with the \texttt{clmarket} demo program.

\section*{Cluster Manager Messages}

This section describes the error messages generated by the \texttt{clstrmgr} daemon.

\section*{Types of Cluster Manager Error Messages}

Cluster Manager messages may be fatal or non-fatal:

- \textit{Fatal errors} are serious errors that cause the Cluster Manager to stop so that the integrity of shared resources is not compromised. A fatal error must be corrected before the Cluster Manager can continue.
• Non-fatal errors indicate that a problem exists in the HACMP environment, but does not stop the Cluster Manager. While a non-fatal error does not stop the Cluster Manager, you should still investigate the cause of the error and correct the condition so that it does not evolve into a more serious problem.

Fatal Messages

The fatal Cluster Manager messages are:

accept failed for deadman: sys_err

The Cluster Lock Manager or the Cluster SMUX Peer attempted to connect to the deadman port and failed. The Cluster Manager prints the reason why and dies. See the accept man page for additional information.

An error was detected in the cluster configuration

A problem exists with the cluster configuration. The Cluster Manager dies. Correct the problem and restart the Cluster Manager.

Cluster Manager: Permission denied, must be root to run this command.

The program you are attempting to run can be run only by a system administrator or someone with root privilege.

Cluster Manager: Unrecognized argument argument.

The Cluster Manager could not recognize the argument passed.

Could not find port port_name

The Cluster Manager could not find the deadman port to the Cluster Lock Manager (clm_lkm) or the port to the Cluster SMUX Peer daemon (clm_smux) and died. To register the ports, add the following entries to the /etc/services file:

```
clm_lkm     6150/tcp   # HACMP for AIX clstrmgr-to-cllockd deadman
clm_smux    6175/tcp   # HACMP for AIX clstrmgr-to-clsmuxpd deadman
```

Fatal error received from select: sys_err.

The Cluster Manager experienced a fatal error.

listen failed on port_name socket: sys_err.

The Cluster Manager was unable to listen to either the Cluster Lock Manager socket (clm_lkm) or the Cluster SMUX Peer socket (clm_smux). The Cluster Manager prints the reason why and dies. See the listen man page for additional information.

Memory error trying to add Topology Event to list.

A memory allocation error occurred while attempting to add a topology event to the event list. Ensure that enough memory exists; otherwise, contact IBM support.

The local node is undefined: Check for a configuration error or an inactive interface.

There is a problem with the cluster configuration. The Cluster Manager died. Correct the problem and restart the Cluster Manager.

unable to open socket for port_name: sys_err.

The Cluster Manager encountered an error on a socket call to the Cluster Lock Manager port (clm_lkm) or the Cluster SMUX Peer daemon port (clm_smux). The Cluster Manager prints the reason why and dies. See the socket man page for possible reasons.
Unable to bind port for **port_name**: **sys_err**.

The Cluster Manager was unable to bind to the Cluster Lock Manager port (clm_lkm) or the Cluster SMUX Peer daemon (clm_smux). The Cluster Manager prints the reason why and dies. See the **bind** man page for additional information.

**Non-Fatal Messages**

The non-fatal Cluster Manager error messages are:

**cluster controller initialized twice.**

A second attempt to start the cluster controller caused an error.

**cc_hb: addAdapter failed.**

An attempt to add an adapter to the cluster configuration failed.

**cc_hb: node node_name seems to have died.**

The Cluster Manager thinks that a node has left the cluster; it has not received a heartbeat response.

**cc_hb: malloc failed in startHB; slow heartbeats disabled.**

Slow heartbeats have been disabled because of a memory allocation error. Ensure that enough memory exists; otherwise, contact IBM support.

**cc_join: suspects a partitioned cluster.**

The Cluster Manager identified a node with a different membership; it will start partition detection.

**cc_sync: bad script status status for node_name.**

The specified script on a node failed.

**Cluster has been in reconfiguration too long.**

The Cluster Manager has detected that an event has been in process for more than the specified time.

In HACMP and HACMP/ES versions prior to 4.5, the time-out period is fixed for all cluster events and set to 360 seconds by default. If a cluster event, such as a node_up or a node_down event, lasts longer than 360 seconds, then every 30 seconds HACMP issues a **config_too_long** warning message that is logged in the **hacmp.out** file.

In HACMP and HACMP/ES 4.5, you can customize in SMIT the time period allowed for a cluster event to complete before HACMP issues a system warning for it.

See Chapter 9 in the *Administration Guide* for information on how to customize event duration time before receiving a **config_too_long** message.

See the section in this book on the **config_too_long** message and its possible causes and solutions in Chapter 4: Solving Common Problems.

**Cluster Manager caught UNKNOWN signal signal_number.**

The Cluster Manager caught a signal that it did not recognize.

**Cluster Manager for nodename nodename is exiting with code code.**
The message printed by a Cluster Manager before it dies. The codes are:

0  Success
1  Memory problem
2  System error
3  Configuration error.

FSM: unknown transition state_name/event_name.

The Cluster Manager received an event but could not determine the next state.

get_msgslot: message list full.

The Cluster Manager communications module can transmit messages but the messages may not be acknowledged.

INCO message without terminating newline.

The Cluster Manager communications module received a message with an unrecognized format.

interrupted system call.

The Cluster Manager received a signal that interrupted a system call.

invoked new JIM, pid=process_id

The specified network interface module process died and was restarted.

jil_multicast: non-existent dest (node_number).

An attempt was made to send a message to a nonexistent node in the cluster.

jil message message should start with length.

The Cluster Manager communications module received a message with an unrecognized format. The first 10 characters of the message are displayed.

JIM pid process_id on net network_name has died.

The Cluster Manager communications module recognized that a network interface module died.

malloc failed.

Memory allocation failed. Ensure that enough memory exists; otherwise, contact IBM support.

malloc failed in doHeartBeat.

A memory allocation error occurred as doHeartBeat attempted to issue a slow heartbeat.

malloc failed in startSync.

A memory allocation error occurred while initializing a sync point.

mitadd: callout table full.

The Cluster Controller cannot set new interval timers because the callout table is full.

mq_send failed in externalized_event.

The Cluster Manager could not write to the message; it could not communicate with other HACMP daemons.

Multiple events found in mark_event_complete.
The Cluster Manager tried to process two events simultaneously.

Received unknown message type = \texttt{message\_type}.

The Cluster Manager does not recognize the message received.

script startup failed.

An attempt to start a script failed.

short INCO packet from jim (\texttt{number} < \texttt{number}).

The Cluster Manager communications module received a message with an unrecognized format.

\texttt{WARNING: Cluster has been running event <xxxx> for <nnn> seconds. Please check event status.}

The Cluster Manager has detected that an event has been in process for more than the specified time.

See the section on the \texttt{config\_too\_long} message and its causes and solutions in Chapter 4: Solving Common Problems.

---

\textbf{Clinfo Messages}

This section lists the error messages generated by the \texttt{clinfo} daemon.

\texttt{add\_event\_notify: system\_error\_message}

Clinfo could not allocate an application event notification request structure. See the \texttt{malloc} man page for more information.

\texttt{check\_event\_notify: Invalid event id \texttt{number}}

Clinfo has received notification of an event but cannot identify an event with this ID number.

\texttt{check\_for\_en\_registration: Invalid set of requests.}

Clinfo has received a request to register zero events.

\texttt{check\_for\_en\_registration: system\_error\_message}

Clinfo has encountered a system error.

\texttt{check\_for\_events: An invalid base\_type was received for EventId.}

Clinfo has received a MIB object response with an incorrect datatype.

\texttt{check\_for\_events: An invalid base\_type was received for EventNetId}

Clinfo has received a MIB object response with an incorrect datatype.

\texttt{check\_for\_events: An invalid base\_type was received for Event Node}

Clinfo has received a MIB object response with an incorrect datatype.

\texttt{check\_for\_events: An invalid base\_type was received for EventTime}

Clinfo has received a MIB object response with an incorrect datatype.

\texttt{check\_for\_events: group-name received, event group expected.}

Clinfo has received a response from SNMP that does not match the request made.

\texttt{check\_for\_events: Invalid value for eventPtr received - value}

Clinfo has received a MIB object with an invalid value.
check_for_events: Unexpected base_type type-name for cluster group received.

Clinfo has received a MIB object response with an incorrect data type.

check_for_events: Unexpected base_type type-name for event group received.

Clinfo has received a MIB object response with an incorrect datatype.

check_for_events: Unexpected type type-name for cluster group received.

Clinfo has received a response from SNMP that does not match the request made.

check_for_events: Unexpected type type-name for event group received.

Clinfo has received a response from SNMP that does not match the request made.

check_for_events: Unexpected group number received.

Clinfo has received a response from SNMP that does not match the request made.

check_missed_events: Invalid event id number

Clinfo has received notification of an event but cannot identify an event with this ID number.

cleanup_apps_notify: system_error_message

Clinfo sent a signal to a process using the kill command and received a status other than success (0) or process-not-found (ESRCH). See the kill command for more information.

clinfo[<clinfo PID>]: send_snmp_req: Messages in queue got = 4 read = 1 not read

This message indicates how many messages are on the request/response socket, and how many have been read.

clinfo exiting.

The clinfo daemon is shutting down, most likely at the request of the System Resource Controller.

clinfo_main: cl_model_touch error number.

clinfo encountered a system error with the ID provided.

clinfo_main: system_error_message

clinfo encountered an error in the system call noted in the message.

Debug level must be a number in the range [0,10].

An invalid debug level was specified with the -d flag when clinfo was started.

delete_event_notify: Unexpected event id number received.

clinfo cannot delete event notification registrations for the event specified.

find_new_clusters: Can’t get local host entry.

A call to lookup_host for the local host failed.

find_new_clusters: Communication has occurred with all clusters.

clinfo is now communicating with the maximum number of clusters.

find_new_clusters: make_SNMP_request failed.

A call to make_SNMP_request in the indicated routine failed.

find_new_clusters: number addresses were never communicated with.

Remaining addresses in the clhosts file are being ignored because clinfo is already communicating with the maximum number of clusters.
find_new_clusters: Search ended, though at least 1 new cluster found.

   clinfo ended the search for clusters after finding only one cluster.

find_new_clusters: sys_err

   The find_new_clusters routine encountered the system error specified.

find_new_clusters: Unable to create traps socket for cluster number.

   clinfo failed to create a socket for trap data for the indicated cluster.

get_cl_map: cl_model_lock_write: string

   The error indicated was encountered by the cl_model_lock_write routine.

get_cl_map: cl_model_lock_write: string

   The error indicated was encountered by the cl_model_lock_write routine.

get_intfc_type: Invalid NetAttribute basetype received.

   clinfo has received a MIB object response with an incorrect datatype.

get_intfc_type: Invalid NetAttribute received.

   clinfo has received a response from SNMP that does not match the request made.

get_intfc_type: Invalid NetAttribute basetype received.

   clinfo has received a response from SNMP that does not match the request made.

get_intfc_type: Incorrect NetAttribute received.

   clinfo has received a response from SNMP that does not match the request made.

get_intfc_indx: Too many interfaces.

   clinfo is attempting to initialize the cluster map and there are too many interfaces for a particular node.

get_response: All responses have been read.

   clinfo tries to access the message received queue but all messages have already been accessed.

get_response: No responses have been received.

   clinfo expects to have received a message, but has not.

initialize_map: cl_model_lock_write: cluster model error

   Error returned from cl_model_lock_write call in the function initialize_map.

init_cl_ev: EventPtr expected, number group number type received.

   clinfo has received a response from SNMP that does not match the request made.

init_cl_ev: invalid event pointer basetype received.

   clinfo has received a MIB object response with an incorrect datatype.

init_cl_nodes: An invalid node index number was encountered.

   The SNMP MIB string for a node group MIB object contained an invalid node index.

init_cl_nodes: cl_model_retr_cluster error number.

   A call to cl_model_retr_cluster failed with the error specified.

init_cl_nodes: cl_model_retr_interface error number

   The call to cl_model_retr_interface failed with the error specified.

init_cl_nodes: inet_addr failed for host host-name

   A call to inet_addr failed.

init_cl_nodes: invalid AddrLabel.

   The MIB object instance for an AddrLabel type was invalid.

init_cl_nodes: Invalid number of interfaces for node number cluster number
An invalid number of interfaces was counted in the address group of the given cluster.

init_cl_nodes: Invalid number of nodes for cluster number - number

An invalid number of nodes was counted in the node group of the MIB for the given cluster.

init_cl_nodes: Network group expected, number group number received.

clinfo has received a response from SNMP that does not match the request made.

init_cl_nodes: Unexpected type number received in Address group.

clinfo has received a response from SNMP that does not match the request made.

init_cl_nodes: Unexpected type number received in node group.

clinfo has received a response from SNMP that does not match the request made.

init_cluster: number group received, cluster group expected.

clinfo has received a response from SNMP that does not match the request made.

init_cluster: Unexpected type received number.

clinfo has received a response from SNMP that does not match the request made.

init_msgq: msgget failed with error number.

A call to the msgget routine failed with the error specified.

init_msgq: sys_err

The init_msgq routine encountered the system error specified.

notify_apps: system_error_message

clinfo sent a signal to a process using the kill command and received a status other than success (0) or process-not-found (ESRCH). See the kill command for more information.

parse_snmp_traps: parse_SNMP_packet

clinfo could not decode an SNMP packet.

parse_snmp_traps: sys_err

The parse_snmp_trap routine encountered a system error while attempting to decode an SNMP packet.

parse_snmp_var: An unexpected group number was received with type number.

clinfo has received a response from SNMP that does not match the request made.

parse_snmp_var: header mismatch in var name string.

The MIB string variable received by clinfo is invalid. The MIB string variable does not contain the expected header.

parse_snmp_var: inet_addr failed for host message.

The MIB string variable received by clinfo is invalid.

parse_snmp_var: Invalid object instance for address group.

The MIB string variable received by clinfo is invalid.

parse_snmp_var: Invalid object instance for event group.

The MIB string variable received by clinfo is invalid.

parse_snmp_var: Invalid object instance for network group.

The MIB string variable received by clinfo is invalid.
parse_snmp_var: Invalid object instance for node group.

The MIB string variable received by clinfo is invalid.

parse_snmp_var: no type found in var name string.

The MIB string variable received by clinfo does not contain a type index.

parse_snmp_var: variable name string too short.

The MIB string variable received by clinfo is invalid.

ping: sys_err

The ping routine encountered the system error specified.

read_config: clhosts files contains no HACMP server addresses.

The /usr/sbin/cluster/clhosts file contains no HACMP server addresses.

read_config: node address too long, ignoring

An address in the /usr/sbin/cluster/clhosts file was more than 50 characters.

read_config: Too many addresses in clhosts - ignoring excess.

The /usr/sbin/cluster/clhosts file contains more than 256 addresses. Clinfo ignores the excess.

read_config: sys_err

clinfo encountered the system error when attempting to open or read the Clinfo configuration file /usr/sbin/cluster/clhosts.

record_event: cl_model_retr_interface error number

clinfo encountered the specified error while accessing information from (or while storing it into) shared memory.

record_event: cluster_unstable error number

clinfo encountered the specified error while accessing information about the cluster’s state from (or while storing it into) shared memory.

record_event: cluster_stable error number

clinfo encountered the specified error while accessing information about the cluster’s state from (or while storing it into) shared memory.

record_event: cluster_error error number

clinfo encountered the specified error while accessing information about a cluster from (or while storing it into) shared memory.

record_event: fail_network error number

clinfo encountered the specified error while accessing information about a failed network from (or while storing it into) shared memory.

record_event: failed_node error number

clinfo encountered the specified error while accessing information about a failed node from (or while storing it into) shared memory.

record_event: failing_node error number

clinfo encountered the specified error while accessing information about a failing node from (or while storing it into) shared memory.

record_event: joined_node error number
**HACMP Messages**

**Clinfo Messages**

- **clinfo** encountered the specified error while accessing information about a node that has joined the cluster from (or while storing it into) shared memory.

  record_event: joining_node error number

- **clinfo** encountered the specified error while accessing information about a joining node from (or while storing it into) shared memory.

  record_event: new_primary error number

- **clinfo** encountered the specified error while accessing information about a new primary node from (or while storing it into) shared memory.

  record_event: Nonexistent event number

- **clinfo** encountered the specified error while accessing or storing information in shared memory.

  refresh_intfcs: inet_addr failed for host name.

  **clinfo** did not receive the inet_addr it requested thus requiring the ARP cache be refreshed.

  refresh_intfcs: invalid AddrLabel

  **clinfo** received an address label of zero length.

  refresh_intfcs: Unexpected type number received in Address group.

  **clinfo** encountered an unknown type while processing an address group response.

  refresh_intfcs: Address group expected, number group encountered.

  **clinfo** sent an address group request but received a different type in the response.

  refresh_intfcs: cl_model_retr_interface error number.

  An error occurred while accessing shared memory.

  save_SNMP_trap: alloc_tvar_mem failed

  **clinfo** failed to allocate a linked list of a specified size of trap variable structures; the variable could not be stored into shared memory.

  save_SNMP_var: sys_err

  **clinfo** encountered a system error when attempting to store an SNMP variable into shared memory.

  save_SNMP_var: receive buffer is full.

  **clinfo**’s internal message receive buffer is full. The incoming message is dropped.

  send_event_notify_msg: msgsnd failed with error number.

  A call to the **msgsnd** routine failed with the indicated error code.

  send_event_notify_msg: Process id PID is invalid.

  The ID of the process to which **clinfo** must send an event notification is invalid.

  send_snmp_req: make_SNMP_request failed.

  A call to the **make_SNMP_request** in the indicated routine failed.

  smux_connect: Can’t get host-name host entry.

  A call to the **lookup_host** routine to retrieve the address of the indicated host name failed.

  smux_connect: Can’t get localhost entry.

  A call to the **lookup_host** routine to retrieve the address of the local host failed.

  smux_connect: number group number type received, ClusterId expected.
clinfo has received a response from SNMP that does not match the request made.

smux_connect: sys_err

The indicated system error was encountered in the smux_connect routine.

Timeout must be a positive value greater than number.

The timeout value for receiving responses must be greater than the specified number.

**Cluster Lock Manager Messages**

This section lists the error messages generated by the clclockd daemon. To view these messages on the system console, add the following line to the /etc/syslog.conf file:

```
kern.debug /tmp/syslog
```

where /tmp/syslog is a file in the system that will be filled with the output. Be sure to touch the file to ensure that it exists, then refresh the syslog daemon.

add_client_reclock: couldn’t add client.

The add_client_reclock function is unable to add a reclock for the specified client because the client record could not be found.

add_queue: Corrupt Queue.

The pointer to the tail of the linked list is incorrectly pointing to NULL. This occurred in the add_queue function.

add_queue: duplicate reclock.

The pointer to the tail of the linked list has something in next when it should be NULL. When the reclock is added to the end it will be added over existing reclock. This occurred in the add_queue function.

addmap: can’t malloc hash table.

Unable to allocate another hash table entry. The get_hashent call or malloc call returned an error in the addmap function. See the malloc man page for more information.

allocate_resource: bad length (name_length).

The length of the name was less or equal to zero.

allocate_resource: malloc error getting resource name.

Unable to allocate a resource name using malloc. See the malloc man page for more information.

allocate_resource: non-empty resref list for resource_name.

The resref list for the specified resource is not empty.

allocate_resource: resource table overflow.

The reference count is greater than or equal to the maximum number of resources allowed.

Allocation failed in purge_list.

Unable to allocate transaction buffer in the purge_list function. The clm_alloc_trans call indicates that no buffers are available.

bad direction specifier in PTI request.
A bad Cluster Manager direction was specified in a PTI (primary transaction interface) request. Good directions are PTI_RESPONSE, PTI_STAT, or PTI_ASYNC.

Bad arg passed to rl_enum.

This is an internal error that should be reported to IBM support.

Bad return from clmm_ctrl.

This is an internal error that should be reported to IBM support.

begin_lock_clm: can’t get resource for converting lock lock_type.

The Cluster Lock Manager could not find the resource for a convert operation. This is an internal error that should be reported to IBM support.

begin_scn_op: can’t find handle for address.

The Cluster Lock Manager could not find the resource for an scn operation. This is an internal error that should be reported to IBM support.

begin_register: failed call to PTI.

The begin_register function failed to pass the request to the master node for the resource. This is an internal error that should be reported to IBM support.

begin_scn_op: NULL resource handle for address.

The lock record for the SCN operation has an invalid resource handle. This is an internal error that should be reported to IBM support.

Can’t determine directory node.

The Cluster Lock Manager cannot determine which node holds directory information for the resource. This is an internal error that should be reported to IBM support.

Can’t establish deadman socket to clstrmgr.

Unable to establish a deadman socket to the Cluster Manager. The clstr_connect call returned an error.

Can’t find resource in local_lock_unix.

This is an internal error that should be reported to IBM support.

clm_alloc_trans: malloc failed.

Note that whenever there’s a malloc failure, the system in question is likely to be short on memory—this applies to most or all malloc messages. This is an internal error that should be reported to IBM support.

clmdd_analyze: can’t get resource handle.

This is an internal error that should be reported to IBM support.

clmdd_pushr: can’t look up resource.

This is an internal error that should be reported to IBM support.

clmdd_message: can’t look up resource.

This is an internal error that should be reported to IBM support.

clm_convert: NULL resource handle for resourceid.

The resource handle is NULL in the function clm_convert. This is an internal error that should be reported to IBM support.

clm_convert: clm_direct ( ) returned NULL.
Unable to determine the directory for this resource. This is an internal error that should be reported to IBM support.

clm_convert: lock but no resource on non-master.

Lock exists on the local node, but the resource is gone. This is an internal error that should be reported to IBM support.

clm_direct ( ) returned NULL.

Unable to determine the directory for this resource. This is an internal error that should be reported to IBM support.

clm_lock: clm_direct ( ) returned NULL.

Unable to determine the directory for this resource. This is an internal error that should be reported to IBM support.

clm_process: Unrecognized client pid.

The client is not recognized. The checkclient call returned false in the clm_process function.

clm_reply: response and request NULL.

Both the response and the request are NULL in clm_reply function.

clm_request: bad request type type.

The request to clm_request function has a bad type.

CLM_VOID in sendudp.

The transaction to send in the function sendudp has no status. This is not an error.

cllockd: unable to init comm layer.

The call to initialize the communications layer returned an error. This is an internal error that should be reported to IBM support.

cllockd: unable to init PTI request port.

The call to initialize a communications port returned an error. This is an internal error that should be reported to IBM support.

cllockd: unable to init directory port.

The call to initialize a communications port returned an error. This is an internal error that should be reported to IBM support.

cllockd: unable to init PTI response port.

The call to initialize a communications port returned an error. This is an internal error that should be reported to IBM support.

cllockd: unable to init RLDB.

The call to initialize the Resource Location Database subsystem returned an error. This is an internal error that should be reported to IBM support.

cllockd: unable to init CLMM.

The call to initialize the resource migration subsystem returned an error. This is an internal error that should be reported to IBM support.

cllockd: unable to init deadlock detection.

The call to initialize the distributed deadlock detection subsystem returned an error. This is an internal error that should be reported to IBM support.
Cluster Manager has died, exiting.

The Cluster Manager has died. The Cluster Lock Manager is exiting.

cont_lock_clm: ERROR: can’t find relock for blocked lock id=address.

This is an internal error that should be reported to IBM support.

cont_lock_clm: NULL resource handle for address.

This is an internal error that should be reported to IBM support.

cont_lock_clm: can’t get resource for converting lock lock_type.

This is an internal error that should be reported to IBM support.

cont_lock_clm: can’t get resource for new lock lock_type.

This is an internal error that should be reported to IBM support.

cont_remote_register: too many resources.

There were too many resources. This occurred in the cont_remote_register function.

cont_remote_register: resource failure.

Unable to allocate a resource. This occurred in the cont_remote_register function.

Copyin failed.

This is an internal error that should be reported to IBM support.

Copyout failed.

This is an internal error that should be reported to IBM support.

Could not find service clm_pts.

Unable to find service clm_pts. The pts_port was less than zero.

dir_proc_request: rl_create failed.

This is an internal error that should be reported to IBM support.

dir_proc_request: rl_modify failed.

This is an internal error that should be reported to IBM support.

Error detected in clm_response_complete.

This is an internal error that should be reported to IBM support.

Error detected in pti_call_complete.

This is an internal error that should be reported to IBM support.

Error detected in send_glob_params_complete.

This is an internal error that should be reported to IBM support.

ERROR: lost a reply from the primary. Aborting.

A request is found that never received a reply.

Error, no cluster manager running.

Unable to connect two sockets, no Cluster Manager is running. See the connect man page for more information.

ERROR: remoteid remote_id already hashed.

The remote id was already hashed.

Error responding to resend transaction.
This is an internal error that should be reported to IBM support.

Error returned from pti_princ_request.

This is an internal error that should be reported to IBM support.

Exiting on signal signal.

Exiting out of Cluster Lock Manager’s server loop on signal. A signal other than SIGUSR1, SIGUSR2, or SIGPIPE was received.

find_reclock: got wrong reclock.

The lock has invalid ownership. This occurred in find_reclock function. This is an internal error that should be reported to IBM support.

find_reclock: index index out of range.

The lockidtoindex call returns an index value greater than the maximum number of locks allowed. This occurred in the find_reclock function.

find_reclock: segment segment_id out of range boundary for type lock_type.

This is an internal error that should be reported to IBM support.

find_rehash: can’t allocate rehash.

Unable to allocate a resource hash structure in the find_rehash function. See the malloc man page for more information.

find_rehash: can’t find/delete resource_name.

Unable to find resource to delete from hash. This occurred in the find_rehash function.

find_rehash: found existing hash for new resource.

An existing hash already existed for new resource; possible error. This occurred in the find_rehash function.

free_dead: found dptr from outside pool address.

Unable to find a map for the remote ID in the freemap function.

freemap: can’t find map for remoteid id remote_id.

Unable to find a map for the remote ID in the freemap function.

freemap: not allocated.

The idhash equals NULL. The hash table was not allocated yet in the freemap function.

get_le: negative lockid lockid.

A lock ID has a negative value in get_le function.

get_le: NO MORE LOCKS.

There are no more locks. This occurred in the get_le function.

Got stray response!

Incoming response does not match with the associated request. The match_request call returns that the associated request is NULL. The response went astray.

Incomplete send in pti_flisht_responses( ).

This is an internal error that should be reported to IBM support.

inflight queue exceeds 500 entries.

This is a debug message and is likely to be disabled in production-level code.
insert_le: can’t allocate lock entry.
Unable to allocate the lock entry in the insert_le function. The get_le call returned NULL.

Invalid trans type for directory create.
This is an internal error that should be reported to IBM support.

kern_main: server loop error.
There was an error (other than EINTR) in the Cluster Lock Manager’s server loop. This occurred in the kern_main function. See the getuerror man page for more information.

local_lock_unix: can’t allocate lock entry.
Unable to allocate the lock entry in the local_lock_unix function. The get_le call returned NULL.

local_scn_op: can’t find handle for address.
This is an internal error that should be reported to IBM support.

local_scn_op: NULL resource handle for address.
This is an internal error that should be reported to IBM support.

local_unlock_clm: can’t find handle for lock_id.
Unable to find resource handle in the local_unlock_clm function. This is an internal error that should be reported to IBM support.

local_unlock_clm: can’t find reclock for lock_id.
The find_reclock function could not find reclock because the ID was out of range. This occurred in the local_unlock_clm function. This is an internal error that should be reported to IBM support.

local_unlock_clm: NULL resource handle for lock_id.
The resource handle was NULL in the local_unlock_clm function. This is an internal error that should be reported to IBM support.

Lock daemon cannot be restarted.
The Cluster Lock Manager was already initialized and needs to be reinitialized. Therefore, the cllockd daemon cannot be restarted.

malloc: can’t malloc locks.
Memory allocation failed while trying to allocate space for more locks. For more information see the man pages on malloc and realloc.

malloc error in clm_queue_response.
Memory allocation failed. Ensure that enough memory exists; otherwise, contact IBM support.

malloc failed in pti_cal ( ).
Memory allocation failed. Ensure that enough memory exists; otherwise, contact IBM support.

malloc failed in pti_call_reg ( ).
Memory allocation failed. Ensure that enough memory exists; otherwise, contact IBM support.

malloc failed in pti_call_purge ( ).
Memory allocation failed. Ensure that enough memory exists; otherwise, contact IBM support.

malloc failed in pti_call_unix ( ).
Memory allocation failed. Ensure that enough memory exists; otherwise, contact IBM support.

Malloc error in clmdd_startstart ( ).

Memory allocation failed. Ensure that enough memory exists; otherwise, contact IBM support.

Malloc error in clmdd_encode ( ).

Memory allocation failed. Ensure that enough memory exists; otherwise, contact IBM support.

Malloc error in clmdd_dostart ( ).

Memory allocation failed. Ensure that enough memory exists; otherwise, contact IBM support.

Malloc error in clmdd_pushr ( ).

Memory allocation failed. Ensure that enough memory exists; otherwise, contact IBM support.

Malloc error in clmdd_processddx ( ).

Memory allocation failed. Ensure that enough memory exists; otherwise, contact IBM support.

Malloc error in ddx_alloc ( )

Memory allocation failed. Ensure that enough memory exists; otherwise, contact IBM support.

Malloc error in ddx_expand ( )

Memory allocation failed. Ensure that enough memory exists; otherwise, contact IBM support.

Malloc error in update_directory ( )

Memory allocation failed. Ensure that enough memory exists; otherwise, contact IBM support.

Malloc failed in rl_expand_freelist

Memory allocation failed. Ensure that enough memory exists; otherwise, contact IBM support.

Malformed QUEUE. ABORTING

The linked list is not formed correctly. The head of the linked list previous pointer does not point to NULL or the tail of the linked list next pointer does not point to NULL.

mapid: can’t find map for remoteid remote_id

Unable to find a map for the remote ID in mapid function.

mapid: not allocated

The idhash equals NULL. The hash table was not allocated in the mapid function.

master_lock_unix: can’t allocate lock entry

Lock segments may have bad custom values. Locks apparently no longer exist.

master_unlock_clm: can’t find handle for address

This is an internal error that should be reported to IBM support.

master_unlock_clm: clm_direct ( ) returned NULL

Unable to determine the directory for this resource. This is an internal error that should be reported to IBM support.

master_unlock_clm: NULL resource handle for address

This is an internal error that should be reported to IBM support.

Master convert request for length:name not found by directory server

This is an internal error that should be reported to IBM support.

Master unlock request for length:name not found by directory server
This is an internal error that should be reported to IBM support.

Master purge request for length:name not found by directory server

This is an internal error that should be reported to IBM support.

match_request interrupted

The **match_request** call was interrupted.

msg_initialize: can’t get message queue id

Unable to get a message queue identifier. The **msgget** call returned an error in the **msg_initialize** function. See the **msgget** man page for more information.

notify: bad HOW parameter

The method of notification parameter to the notify function is bad. This is an internal error that should be reported to IBM support.

notify: bad resptr, rh=address

This is an internal error that should be reported to IBM support.

notify: NULL resource handle

The resource handle is NULL in the notify function. This is an internal error that should be reported to IBM support.

pre_proc_unlock_clm: can’t find handle for address

This is an internal error that should be reported to IBM support.

pre_proc_unlock_clm: NULL resource handle for address

This is an internal error that should be reported to IBM support.

pti_prog_p: illegal request type type seq seq_number

This is an internal error that should be reported to IBM support.

purge_deadlock: bad resptr, rh=address

This is an internal error that should be reported to IBM support.

receive_resource: couldn’t allocate resource slot

This is an internal error that should be reported to IBM support.

receive_lock: invalid resource handle

This is an internal error that should be reported to IBM support.

receive_lock: map remote lockid

This is an internal error that should be reported to IBM support.

receive_lock: unable to alloc reclock

This is an internal error that should be reported to IBM support.

Remote function failed

The function that handles requests on the secondary and forwards the transaction to the primary has returned with an error condition. This can be caused by invalid actions of a lock client.

remove_queue: Corrupt Queue

The pointer to the head of the linked list is pointing incorrectly. This occurred in the **remove_queue** function.

removeclient: no such client: pid
The **removeclient** function is unable to remove a client because the **bsearch** call returned that the client does not exist. See the **bsearch** man page for more information.

**rl_init**: unable to allocate memory for RLDB

Memory allocation failed. Ensure that enough memory exists; otherwise, contact IBM support.

**clm_main**: can’t allocate dead pid structs

This is an internal error that should be reported to IBM support.

**clm_resource**: segment memory segment already allocated

This is an internal error that should be reported to IBM support.

**clm_resource**: all resource segments full

Resource space is full. Custom segment sizes may be too small.

**clm_resource**: failed to find res segment

This is an internal error that should be reported to IBM support.

**clm_resource**: failed to allocate resource segment

Memory allocation failed. Ensure that enough memory exists; otherwise, contact IBM support.

**clm_resource**: couldn’t find empty resource slot

This is an internal error that should be reported to IBM support.

**clm_resource**: Queue type out of range

This is an internal error that should be reported to IBM support.

**clm_resource**: malloc error expanding restab

Memory allocation failed. Ensure that enough memory exists; otherwise, contact IBM support.

**clm_tune**: malloc failed

Memory allocation failed. Ensure that enough memory exists; otherwise, contact IBM support.

**clm_tune**: cccp_send returned %d

This is an internal error that should be reported to IBM support.

**clm_unixlock**: can’t get lock entry

This is an internal error that should be reported to IBM support.

**search_lock**: bad resptr, rh=0x%x

This is an internal error that should be reported to IBM support.

**send_timeouts**: could not allocate transaction

Unable to allocate a transaction buffer in **send_timeouts** function. The **clm_alloc_trans** returned that no buffers are available.

**sendudp**: could not find client **pid**

Unable to find client. The **findclient** call returned NULL in the **sendudp** function.

**sendudp**: could not allocate buffer

Unable to allocate a transaction buffer in the **sendudp** function. The **clm_alloc_trans** call returned that no buffers are available.

**sendast**: send failed AST

The **ASTcall** call fails in the **sendast** function while trying to respond by AST.
**HACMP Messages**  
Cluster SMUX Peer Messages

sendast: send failed for BAST

The ASTcall call fails in the sendast function while trying to respond by blocking AST.

send_ast: no valid handle

No valid AST handle in sendast function.

send timeouts: bad resptr, rh=0x%x

This is an internal error that should be reported to IBM support.

sent number of number from address

This message may come up during reconfiguration. It is not an error as long as it stops.

string: Error error

The string and the current value of the process’s u_error field are printed in the perror function. See the perror man page for more information.

send failed for 0xbase_memory_address

The getuerror call returned an error other than bad address and interrupt system call. See the send man page for more information.

Unable to allocate resource tables of size max_resources

Unable to allocate resource tables. See the malloc man page for more information.

Unable to determine directory node

Unable to determine the directory for this resource. This is an internal error that should be reported to IBM support.

Unable to determine local site info

Unable to determine cluster configuration information. This is an internal error that should be reported to IBM support.

Unknown directory request type in dir_proc_request

This is an internal error that should be reported to IBM support.

---

**Cluster SMUX Peer Messages**

This section lists the error messages generated by the clsmuxpd daemon.

app_accept: accept: sys_err

The accept call failed while reading from an application socket. See the accept man page for more information.

app_accept: read: sys_err

The read call failed while reading from an application socket. See the read man page for possible reasons.

app_accept: select: sys_err

The select system call returned with an error other than EINTR. See the select man page for possible reasons.

app_accept: Select timeout deny request

The select call timed out while waiting for an application to register. See the select man page for more information.
app_createPort: getservbyname: sys_err

The getservbyname call failed. There is no clsmuxpd entry in the /etc/services file.

app_createPort: socket: sys_err

The socket call failed while creating the application listen socket. See the socket man page for possible reasons.

app_createPort: setsockopt: sys_err

The setsockopt call to allow reuse of local addresses failed. See the setsockopt man page for possible reasons.

app_createPort: bind: sys_err

The bind call failed while creating the application listen socket. See the bind man page for possible reasons.

app_createPort: listen: sys_err

The listen call failed while creating the application listen socket. See the listen man page for possible reasons.

childWait: sigaction: sys_err

The sigaction call failed. See the sigaction call for possible reasons.

childWait: setitimer: sys_err

The setitimer call failed. See the setitimer man page for possible reasons.

clsmuxpd_main: fork: sys_err

Unable to create child process. This is a fatal error. See the fork man page for possible reasons.

clsmuxpd_main: Error in smuxp_init()

Make sure smuxpd is running and refreshed, and an entry exists in /etc/snmpd.conf and /etc/snmpd.peers for risc6000clsmuxpd.

clsmuxpd_main: Error in app_createPort()

Make sure another clsmuxpd is not already running.

clsmuxpd_main: Error in config_init()

Use the clverify utility to make sure the HACMP cluster is properly configured.

cls_createDeadman: connect

The connect call failed while attempting to connect to the clstrmgr TCP/IP deadman socket. See the connect man page for possible reasons.

cls_createDeadman: getservbyname

The getservbyname call failed. There is no clm_smux entry in /etc/services.

cls_createDeadman: setsockopt

The setsockopt call failed while attempting to connect to the clstrmgr TCP/IP deadman socket. See the setsockopt man page for possible reasons.

cls_createDeadman: socket

The socket call failed while attempting to connect to the clstrmgr TCP/IP deadman socket. See the socket man page for possible reasons.

config_init: Error in get_clusterConfig
Make sure another `clusmuxpd` is properly configured.

`getStat: fork: sys_err`

Unable to create child process. See the `fork` man page for possible reasons.

`hacmp_handler: Error in cls_createDeadman( )`

Make sure another `clusmuxpd` is not already running.

`hacmp_handler: Duplicate key encountered.`

Received a duplicated application request.

`hacmp_handler: lnInsert: sys_err`

Unable to add entry into linked list. The `malloc` call probably failed. See the `malloc` man page for possible reasons.

`hacmp_handler: malloc message queue`

The `malloc` call failed while allocating memory for message queue. See the `malloc` man page for possible reasons.

`rcv_eventMap: Unknown event`

`clusmuxpd` received unknown event. Ignored.

`rcv_topologyMap: malloc`

The `malloc` call failed while attempting to receive data from the `clstrmgr`. See the `malloc` man page for possible reasons.

`rcv_topologyMap: realloc`

The `realloc` call failed. See the `realloc` man page for possible reasons.

`refresh_addrGroup: lnOpen: sys_err`

Unable to create linked list. The `malloc` call probably failed. See the `malloc` man page for possible reasons.

`refresh_addrGroup: lnInsert: sys_err`

Unable to add entry into linked list. The `malloc` call probably failed. See the `malloc` man page for possible reasons.

`refresh_addrGroup: switch on MAXIFSTYPES sys_err`

Unable to add entry into linked list. The `malloc` call probably failed. See the `malloc` man page for possible reasons.

`refresh_appGroup: lnOpen: sys_err`

Unable to create linked list. The `malloc` call probably failed. See the `malloc` man page for possible reasons.

`refresh_appGroup: xselect: sys_err`

The `select` system call returned with an error other than EINTR. See the `select` man page for possible reasons.

`refresh_clinfoGroup: lnInsert: sys_err`

Unable to add entry into linked list. The `malloc` call probably failed. See the `malloc` man page for possible reasons.

`refresh_clinfoGroup: lnOpen: sys_err`
Unable to create linked list. The `malloc` call probably failed. See the `malloc` man page for possible reasons.

refresh_clclockdGroup: lnInsert: `sys_err`
Unable to add entry into linked list. The `malloc` call probably failed. See the `malloc` man page for possible reasons.

refresh_clclockdGroup: lnOpen: `sys_err`
Unable to create linked list. The `malloc` call probably failed. See the `malloc` man page for possible reasons.

refresh_clstrmgrGroup: lnInsert: `sys_err`
Unable to add entry into linked list. The `malloc` call probably failed. See the `malloc` man page for possible reasons.

refresh_clstrmgrGroup: lnOpen: `sys_err`
Unable to create linked list. The `malloc` call probably failed. See the `malloc` man page for possible reasons.

refresh_clsmuxpdGroup: malloc: `sys_err`
Unable to allocate memory. See the `malloc` man page for possible reasons.

refresh_clusterGroup: malloc: `sys_err`
Unable to allocate memory. See the `malloc` man page for possible reasons.

refresh_eventGroup: lnInsert `sys_err`
Unable to allocate memory. See the `malloc` man page for possible reasons.

refresh_eventGroup: lnOpen `sys_err`
Unable to allocate memory. See the `malloc` man page for possible reasons.

refresh_netGroup: lnOpen: `sys_err`
Unable to create linked list. The `malloc` call probably failed. See the `malloc` man page for possible reasons.

refresh_netGroup: lnInsert: `sys_err`
Unable to add entry into linked list. The `malloc` call probably failed. See the `malloc` man page for possible reasons.

refresh_nodeGroup: lnInsert: `sys_err`
Unable to add entry into linked list. The `malloc` call probably failed. See the `malloc` man page for possible reasons.

refresh_nodeGroup: lnOpen: `sys_err`
Unable to create linked list. The `malloc` call probably failed. See the `malloc` man page for possible reasons.

src_handler: Error: link_listInit( )
May be low on memory.

startSubsys: fork: `sys_err`
Unable to create child process. See the `fork` man page for possible reasons.

stopSubsys: fork: `sys_err`
Unable to create child process. See the `fork` man page for possible reasons.
HACMP C-SPOC Messages

C-SPOC messages are generated by the C-SPOC initialization and verification routine, cl_init.cel, the CEL preprocessor, and C-SPOC commands. This section lists messages you may experience when using the C-SPOC utility.

CELPP Messages

The Command Execution Language (CEL) preprocessor (celpp) generates the following messages:

celpp: Cannot open input file filename.
Either the file permissions are set incorrectly, or the file may not exist.
celpp: Unable to open output file filename.
Directory permissions may be set incorrectly.
celpp: Unrecognized argument argument.
Check the celpp usage statement.
celpp: No include path specified.
Specify an include path after the -I option.
celpp: No input file specified.
Specify an input filename.
celpp: Bad option Value.
Specify a valid argument. Check the celpp usage statement.
celpp: Cannot allocate space for include path.
celpp: Debug level set to level.
celpp: Input file is filename.
celpp: Output file will be filename.
celpp: No output file specified.
celpp: No debug level specified.

Initialization and Verification Messages

The C-SPOC initialization and verification routine, cl_init.cel, generates the following messages. This routine is included in each C-SPOC command’s execution plan; it executes when you invoke a C-SPOC command.

cl_init: Unable to determine node list for the cluster.
Check your HACMP configuration.
cl_init: Unable to determine target node list!
Check your HACMP configuration.
cl_init: _get_rgnodes:
A resource group must be specified.
cl_init: Invalid C-SPOC flag flag specified.
Check the C-SPOC command’s usage statement.

cl_init: Option option requires an argument.

cl_init: Option option does not take an argument.

cl_init: Invalid option option.

cl_init: Mandatory option option not specified.

cl_init: C-SPOC options 'option' and 'option' are mutually exclusive.

cl_init: Unable to open file: filename.

cl_init: The node nodename is not a part of this cluster.

cl_init: Unable to verify HACMP Version on node node_name.

   The specified node may be down or inaccessible. Check your network configuration and the
   cluster node.

cl_init: Node_name is not running HACMP Version 4.5 or higher.

   Ensure that the correct version of HACMP is installed.

cl_init: Resource group groupname not found.

cl_init: Unable to connect to node nodename.

cl_init: Must be root to execute this command.

cl_init: Two nodes have the same serial number, probably due to IPAT.

**User and Group Command Messages**

cl_chuser: User user_name does not exists on node node_name.

cl_chgroup: Group group_name does not exist on node node_name.

cl_lsgroup: Error messages generated by this command rely on the underlying AIX command output. See the lsgroup man page for more information.

cl_lsuser: Error messages generated by this command rely on the underlying AIX command output. See the lsuser man page for more information.

cl_mkgroup: Group group_name already exists on node node_name.

cl_mkuser: User user_name already exists on node node_name.

cl_rmgrp: Error messages generated by this command rely on the underlying AIX command output. See the rmgroup man page for more information.

cl_rmuser: Error messages generated by this command rely on the underlying AIX command output. See the rmuser man page for more information.
Logical Volume Manager and File System Command Messages

cl_chfs: No file system given.

cl_chfs: Filesystem is not a valid file system name.

cl_chfs: Error executing chfs filesystem on node node_name.

cl_chlv: No logical volume given.

cl_chlv: Error executing chlv logical_volume on node node_name.

cl_lsfs: Error executing clfiltlsfs filesystem on node node_name.

cl_lsfs: No filesystems found.

cl_lsfs: An error occurred running cllsfs.

cl_lsfs: Can’t locate filesystem filesystem.

cl_lslv: No logical volume given.

cl_lslv: Error executing lslv logical_volume on node node_name.

cl_lslv: Error attempting to locate lv logical_volume on node node_name.

cl_lsvg: Error executing clfiltlsvg volume_group on node node_name.

cl_lsvg: No volume groups found.

cl_lsvg: An error occurred running cllsvg.

cl_lsvg: Can’t locate volume group vgname.

cl_rmfs: Filesystem filesystem is configured as an HACMP resource.

cl_rmfs: Error executing rmlv filesystem on node node_name.

cl_rmlv: Error executing lsfs /dev/logical_volume on node node_name.

cl_rmlv: Filesystem filesystem (contained within logical volume logical_volume) is configured as an HACMP resource.

cl_rmlv: Warning, all data contained on logical volume logical_volume will be destroyed.

cl_rmlv: Error executing rmlv logical_volume on node node_name. Do you wish to continue? y(es) n(no)?

cl_updatevg: Error attempting to locate volume group vgname on nodename.

cl_updatevg: Can’t reach nodename, continuing anyway.

cl_updatevg: Volume group vgname found active on nodename.

cl_updatevg: Error executing clvaryonvg vgname on nodename.

This command can only be executed through the SMIT interface.

The <hdisk/PVID> is not concurrent capable.

The disk cannot be imported to cluster node <node name> for import into the volume group.
Cluster Management Command Messages

cl_clstop:

Error messages generated by this command rely on the underlying HACMP command output. See the clstop man page for more information.

cl_rc.cluster:

Error messages generated by this command rely on the underlying HACMP command output. See the rc.cluster man page for more information.

HACMP DARE Messages

This section lists error messages generated by the cldare utility.

cldare: Unable to rsh a command to node node_name or node_name is not running a Version of HACMP which supports this functionality.

cldare: Node node_name is currently seen by a Cluster Manager to be running a clstrmgr process. Please check for an entry for node_name in the /.rhosts file on node node_name and/or check the Version of HACMP installed.

cldare: Failed removing DARE lock from node: node_name. Please check /.rhosts permissions.

cldare: Detected that node: node_name has an active Cluster Manager process.

cldare: Unable to synchronize the HACMP ODMs to the Active Configuration Directory on node node_name.

cldare: Unable to synchronize the HACMP ODMs to the Stage Configuration Directory on node node_name.

cldare: Failed removing one or more DARE locks.

cldare: Succeeded removing all DARE locks.

cldare: No nodes are configured.

cldare: Verification failed.

cldare: Error detected during synchronization.

cldare: An active Cluster Manager was detected elsewhere in the cluster. This command must be run from a node with an active Cluster Manager process in order for the Dynamic Reconfiguration to proceed. The new configuration has been propagated to all nodes for your convenience.

cldare: A change has been detected in both the Topology and Resource HACMP ODMs. Only changes in one at a time are supported in an active cluster environment.

cldare: A change has been detected with the Cluster ID or Cluster Name. Such changes are not supported in an active cluster environment.

cldare: A node (node_name) which has been removed from the new cluster configuration is currently active. The Cluster Manager on the node must be stopped before the topology change can be applied.
HACMP Messages
HACMP DARE Messages

cldare: A lock for a Dynamic Reconfiguration event has been detected. Another such event cannot be run until the lock has been released. If no Dynamic Reconfiguration event is currently taking place, and the lock persists, it may be forcefully unlocked via the SMIT HACMP Cluster Recovery Aids.

cldare: Unable to set local lock for Dynamic Reconfiguration event.

cldare: Unable to create a cluster snapshot of the current running cluster configuration. Aborting.

cldare: Unable to copy the configuration data from the System Default ODM directory to /usr/sbin/cluster/etc/objrepos/stage. Aborting.

cldare: Unable to synchronize the configuration data to all active remote nodes. Aborting.

cldare: Requesting a refresh of the Cluster Manager.

cldare: This command must be run from a node with an active Cluster Manager.

cldare: Unable to create a DARE lock on a remote node with an active Cluster Manager process.

cldare: Unable to copy the HACMP ODMs from the System Default Configuration Directory to the Stage Configuration Directory on node node_name.

cldare: Detected that node node_name has an active Cluster Manager process, but the configuration was not successfully synchronized to the node.

cldare: Verifying additional pre-requisites for Dynamic Reconfiguration completed.

cldare: No changes detected in Cluster Topology or Resources requiring further processing.

cldare: Detected changes to Network Interface Module (NIM) nim_name. Please note that, other than the Failure Detection Rate, changing NIM parameters via a DARE is not supported.

cldare: Detected changes to network adapter adapter_name. Please note that changing network adapter parameters via a DARE is not supported.

cldare: Detected changes to network network_name. Please note that changing network parameters via a DARE is not supported.

cldare: Resource group ‘resgrp_name’ specified more than once for migration.

cldare: Attempt to migrate unknown resource group ‘resgrp_name’.

cldare: Attempt to migrate concurrent resource group ‘resgrp_name’.

cldare: Attempt to migrate resource group ‘resgrp_name’ to non-member node ‘node_name’.

cldare: Attempt to migrate resource group ‘resgrp_name’ to inactive node ‘node_name’.

cldare: Attempt to use non-sticky migration for cascading resource group ‘resgrp_name’.

cldare: Cannot mix “default” or “stop” requests with other migration requests.

cldare: Bad resource group ‘resgrp_name’ in specifier: -M “resgrp_name:node_name”.

cldare: Bad node name “cru+ty” in specifier: -M “resgrp_name:cru+ty:sticky”.
cldare: Invalid keyword “stickyfoo” at end of specifier: -M “resgrp_name:crusty:stickyfoo”.

cldare: Use of invalid combination “default:sticky” for resource group ‘resgrp_name’.

cldare: Attempt to migrate rotating/cascading resource ‘resgrp_name’ to node ‘node_name’ which is not up on boot address.

cldare: Attempt to migrate rotating resource ‘resgrp_name’ to node ‘node_name’ conflicts with resource ‘resgrp_name2’.

cldare: Attempt to migrate rotating resource group ‘resgrp_name’ to node ‘node_name’ conflicts with rotating resource group ‘resgrp_name’.

cldare: Attempt to migrate rotating resource groups ‘resgrp_name’ and ‘resgrp_name2’ to same node and to network.

cldare: Attempt to migrate cascading resource group to node ‘crusty’ which has insufficient free standby adapters.

cldare: Attempt to migrate cascading resources ‘res1’ and ‘res2’ to node ‘node_name’ which has insufficient free standby adapters.

cldare: Resource group ‘resgrp_name’ failed to migrate. Failure most likely occurred because of an intervening cluster event; check the /tmp/hacmp.out log file.

clfindres: bad resource group ‘resgrp_name’

clfindres: problems discovering active node set

clfindres: ODM error setting path /etc/objrepos: no such file or directory.

clfindres: problem using GODM to find location of group ‘resgrp_name’ (addr 128.4.5.129).

clfindres: Error reading cluster configuration from ODM in /etc/objrepos.
clfindres: memory allocation error while resizing resource array.

cldare: resource group ‘resgrp_name’ failed to migrate to node ‘crusty’.

cldare: resource group ‘resgrp_name’ failed to stop.

cldare: Failure occurred during resource group migration. Check above for the final location(s) of specified groups. Also, look in the log file (/tmp/hacmp.out) to see more information about the failure.

cldare: Attempt to perform resource group migration with pending changes in either the Topology or Resource HACMP ODMs. Must perform normal dare (without group migration) first then return migration.

cldare: resource group ‘resgrp_name’ failed to activate as requested.

**Note:** If errors occur during the initial check for migration consistency, the dynamic reconfiguration process is immediately aborted.

### HACMP Event Emulator Messages

This section lists error messages generated by the HACMP Event Emulator utility.

getfiles: Error in reading local node name. Ensure that your cluster topology and cluster resources are synchronized.
getfiles: Error in trying to read the IP address of this node. Unable to obtain an active address for this node. Ensure that the node is UP.


getfiles: No active nodes exist in the cluster.

getfiles: Unable to connect to node node_name. Check passwords, permissions, and the ~/.rhosts file.

getversions: To run the emulator HACMP, all nodes must be Version 4.2.2 or higher.

getversions: Unable to rsh to node node_name. Check passwords, permissions, and the ~/.rhosts file.

**HAView Messages**

This section lists error messages generated by HAView.

HAVIEW: Could not get list of symbols on root map. Create a new map.

HAVIEW: Cannot create symbol for the top level clusters object. Check to see if the map is read-only.

HAVIEW: Cannot create submap for clusters symbol. Check to see if the map is read-only.

HAVIEW: Cannot create symbol for the cluster. Check to see if the map is read-only.

HAVIEW: Cannot create symbol for the node. Check to see if the map is read-only.

HAVIEW: Cannot create symbol for the address. Check to see if the map is read-only.

HAVIEW: Cannot create submap for address. Check to see if the map is read-only.

HAVIEW: Cannot create node symbol (in connection). Check to see if the map is read-only.

HAVIEW: Cannot create connection symbol. Check to see if the map is read-only.

HAVIEW: Cannot create submap for addresses. Check to see if the map is read-only.

HAVIEW: Cannot get addresses. Create a new map.

HAVIEW: Could not get symbols for cluster object. Create a new map.

HAVIEW: Unable to get nodes from cluster object. Create a new map.

HAVIEW: Unable to create node object. Your database is not accessible and may be corrupted. See your NetView documentation for information on rebuilding your database.

HAVIEW: Unable to create address object. Your database is not accessible and may be corrupted. See your NetView documentation for information on rebuilding your database.

HAVIEW: Unable to create network elements for network. Your database is not accessible and may be corrupted. See your NetView documentation for information on rebuilding your database.

HAVIEW: Cannot create object for connection. Your database is not accessible and may be corrupted. See your NetView documentation for information on rebuilding your database.
HAVIEW: Unable to create address object. Your database is not accessible and may be corrupted. See your NetView documentation for information on rebuilding your database.

HAVIEW: Could not delete address, object not found for address. Your database is not accessible and may be corrupted. See your NetView documentation for information on rebuilding your database.

HAVIEW: Could not find a SERVICE address for this node with UP status. Wait until the cluster is stabilized and the service address is available; try again.

HAVIEW: Cannot update object status. Your database is not accessible and may be corrupted. See your NetView documentation for information on rebuilding your database.

HAVIEW: Cannot change field value for cluster state. Your database is not accessible and may be corrupted. See your NetView documentation for information on rebuilding your database.

HAVIEW: Cannot change field value for cluster substate. Your database is not accessible and may be corrupted. See your NetView documentation for information on rebuilding your database.

HAVIEW: Cannot change field value for node state. Your database is not accessible and may be corrupted. See your NetView documentation for information on rebuilding your database.

HAVIEW: Cannot change field value for connection state. Your database is not accessible and may be corrupted. See your NetView documentation for information on rebuilding your database.

HAVIEW: Cannot change field value for address state. Your database is not accessible and may be corrupted. See your NetView documentation for information on rebuilding your database.
Appendix B: HACMP Tracing

This appendix describes how to trace HACMP-related events.

Overview of HACMP Tracing

The trace facility helps you isolate a problem within an HACMP system by allowing you to monitor selected events. Using the trace facility, you can capture a sequential flow of time-stamped system events that provide a fine level of detail on the activity within an HACMP cluster.

The trace facility is a low-level debugging tool that augments the troubleshooting facilities described earlier in this book. While tracing is extremely useful for problem determination and analysis, interpreting a trace report typically requires IBM support.

The trace facility generates large amounts of data. The most practical way to use the trace facility is for short periods of time—from a few seconds to a few minutes. This should be ample time to gather sufficient information about the event you are tracking and to limit use of space on your storage device.

The trace facility has a negligible impact on system performance because of its efficiency.

The Trace Facility for HACMP Daemons

Use the trace facility to track the operation of the following HACMP daemons:

- The Cluster Manager daemon (`clstrmgr`)
- The Cluster Information Program daemon (`clinfo`)
- The Cluster SMUX Peer daemon (`clsmuxpd`)
- The Cluster Lock Manager daemon (`cllockd`).

The `clstrmgr`, `clinfo`, and `clsmuxpd` daemons are controlled by the System Resource Controller (SRC), while the `cllockd` daemon is implemented as a kernel extension. This distinction is important and is explained below.

Daemons Under the Control of the System Resource Controller

The `clstrmgr`, `clinfo`, and `clsmuxpd` daemons are user-level applications under the control of the SRC. Before you can start a trace on one of these daemons, you must first enable tracing for that daemon. Enabling tracing on a daemon adds that daemon to the master list of daemons for which you want to record trace data.

Daemons that are Kernel Extensions

The `cllockd` daemon is implemented as a kernel extension. You do not need to enable tracing on a kernel extension.
The Trace Session

You can initiate a trace session using either SMIT or the HACMP /usr/sbin/cluster/diag/cldiag utility. Using SMIT, you can enable tracing in the HACMP SRC-controlled daemons, start and stop a trace session in the daemons, and generate a trace report. Using the cldiag utility, you can activate tracing in any HACMP daemon without having to perform the enabling step. The cldiag utility performs the enabling procedure, if necessary, and generates the trace report automatically. The following sections describe how to initiate a trace session using either SMIT or the cldiag utility.

Using SMIT to Obtain Trace Information

To initiate a trace session using the SMIT interface:

1. Enable tracing on the SRC-controlled daemon or daemons you specify.
   Use the SMIT Enable/Disable Tracing of HACMP Daemons screen to indicate that the selected daemons should have trace data recorded for them.

2. Start the trace session.
   Use the SMIT Start/Stop/Report Tracing of HACMP Services screen to trigger the collection of data.

3. Stop the trace session.
   You must stop the trace session before you can generate a report. The tracing session stops either when either you use the SMIT Start/Stop/Report Tracing of HACMP Services screen to stop the tracing session or when the log file becomes full.

4. Generate a trace report.
   Once the trace session is stopped, use the SMIT Start/Stop/Report Tracing of HACMP Services screen to generate a report.

Each step is described in the following sections.

Enabling Tracing on SRC-controlled Daemons

To enable tracing on the following SRC-controlled daemons (clstrmgr, clinfo, or clsmuxpd):

1. Enter: smit hacmp

2. Select Trace Facility and press Enter.


4. Select Start Trace and press Enter. SMIT displays the Start Trace screen. Note that you only use this screen to enable tracing, not to actually start a trace session. It indicates that you want events related to this particular daemon captured the next time you start a trace session. See Starting a Trace Session for more information.

5. Enter the PID of the daemon whose trace data you want to capture in the Subsystem PROCESS ID field. Press F4 to see a list of all processes and their PIDs. Select the daemon and press Enter. Note that you can select only one daemon at a time. Repeat these steps for each additional daemon that you want to trace.
6. Indicate whether you want a short or long trace event in the **Trace Type** field. A short trace contains terse information. For the **clstrmgr** daemon, a short trace produces messages only when topology events occur. A long trace contains detailed information on time-stamped events.

7. Press Enter to enable the trace. SMIT displays a screen that indicates that tracing for the specified process is enabled.

### Disabling Tracing on SRC-controlled Daemons

To disable tracing on the **clstrmgr**, **clinfo**, or **clsmuxpd** daemons:

1. Enter: `smit hacmp`

2. Select **RAS Support > Trace Facility > Enable/Disable Tracing of HACMP Daemons > Stop Trace**. SMIT displays the Start Trace screen. Note that you only use this screen to *enable* tracing, not to actually start a trace session. It indicates that you want events related to this particular daemon captured the next time you start a trace session. See Starting a Trace Session for more information.

3. Enter the PID of the process for which you want to disable tracing in the **Subsystem PROCESS ID** field. Press F4 to see a list of all processes and their PIDs. Select the process for which you want to disable tracing and press Enter. Note that you can disable only one daemon at a time. To disable more than one daemon, repeat these steps.

4. Press Enter to disable the trace. SMIT displays a screen that indicates that tracing for the specified daemon has been disabled.

### Starting a Trace Session

Starting a trace session triggers the actual recording of data on system events into the system trace log from which you can later generate a report.

Remember, you can start a trace on the **clstrmgr**, **clinfo**, and **clsmuxpd** daemons only if you have previously enabled tracing for them. You do not need to enable tracing on the **clclockd** daemon; it is a kernel extension.

To start a trace session:

1. Enter: `smit hacmp`

2. Select **RAS Support > Trace Facility > Start/Stop/Report Tracing of HACMP Services > Start Trace**. SMIT displays the Start Trace screen.

3. Enter the trace IDs of the daemons that you want to trace in the **ADDITIONAL event IDs to trace** field.

4. Press F4 to see a list of the trace IDs. (Press Ctrl-v to scroll through the list.) Move the cursor to the first daemon whose events you want to trace and press F7 to select it. Repeat this process for each event that you want to trace. When you are done, press Enter. The values that you selected are displayed in the **ADDITIONAL event IDs to trace** field. The HACMP daemons have the following trace IDs:

```
clstrmgr     910
clinfo       911
```
Using SMIT to Obtain Trace Information

5. Enter values as necessary into the remaining fields and press Enter.
SMIT displays a screen that indicates that the trace session has started.

Stopping a Trace Session

You need to stop a trace session before you can generate a trace report. A trace session ends when you actively stop it or when the log file is full.

To stop a trace session:
1. Enter: `smit hacmp`
2. Select RAS Support > Trace Facility > Start/Stop/Report Tracing of HACMP Services > Stop Trace. SMIT displays the Command Status screen, indicating that the trace session has stopped.

Generating a Trace Report

A trace report formats the information stored in the trace log file and displays it in a readable form. The report displays text and data for each event according to the rules provided in the trace format file.

When you generate a report, you can specify:
- Events to include (or omit)
- The format of the report.

To generate a trace report:
1. Enter: `smit hacmp`
2. Select RAS Support > Trace Facility > Start/Stop/Report Tracing of HACMP Services > Generate a Trace Report. A dialog box prompts you for a destination, either a filename or a printer.
3. Indicate the destination and press Enter. SMIT displays the Generate a Trace Report screen.
4. Enter the trace IDs of the daemons whose events you want to include in the report in the IDs of events to INCLUDE in Report field.
5. Press F4 to see a list of the trace IDs. (Press Ctrl-v to scroll through the list.) Move the cursor to the first daemon whose events you want to include in the report and press F7 to select it. Repeat this procedure for each event that you want to include in the report. When you are done, press Enter. The values that you selected are displayed in the IDs of events to INCLUDE in Report field. The HACMP daemons have the following trace IDs:

```
  cldmr
  clinfo
  cldmr
```
6. Enter values as necessary in the remaining fields and press Enter.
7. When the information is complete, press Enter to generate the report. The output is sent to the specified destination. For an example of a trace report, see Sample Trace Report.

Using the cldiag Utility to Obtain Trace Information

When using the cldiag utility, you must include the /usr/sbin/cluster/diag directory in your PATH environment variable. Then you can run the utility from any directory. You do not need to enable tracing on any of the HACMP daemons before starting a trace session.

To start a trace session using the cldiag utility:

1. Start by entering:
   ```
   cldiag
   ```
   The utility returns a list of options and the cldiag prompt:
   ```
   -------------------------------------------------------
   To get help on a specific option, type: help <option>
   To return to previous menu, type: back
   To quit the program, type: quit
   -------------------------------------------------------
   Valid options are:
   debug
   logs
   vgs
   error
   trace
   cldiag>
   ```
   The cldiag utility help subcommand provides a brief synopsis of the syntax of the option specified. For more information about the command syntax, see the cldiag man page.

2. To activate tracing, enter the trace option at the cldiag prompt. You must specify (as an argument to the trace option) the name of the HACMP daemons for which you want tracing activated. Use spaces to separate the names of the daemons. For example, to activate tracing in the Cluster Manager and Clinfo daemons, enter the following:
   ```
   cldiag> trace clstrmgr clinfo
   ```
   For a complete list of the HACMP daemons, see The Trace Facility for HACMP Daemons.

Note: A trace of clclockd provides only a list of current locks; it does not produce a full trace report.
By using flags associated with the `trace` option, you can specify the duration of the trace session, the level of detail included in the trace (short or long), and the name of a file in which you want the trace report stored. The following table describes the optional command line flags and their functions:

<table>
<thead>
<tr>
<th>Flag</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-l</code></td>
<td>Obtains a long trace. A long trace contains detailed information about specific time-stamped events. By default, the <code>cldiag</code> utility performs a short trace. A short trace contains terse information. For example, a short trace of the <code>clstrmgr</code> daemon generates messages only when topology events occur.</td>
</tr>
<tr>
<td><code>-t time</code></td>
<td>Specifies the duration of the trace session. You specify the time period in seconds. By default, the trace session lasts 30 seconds.</td>
</tr>
<tr>
<td><code>-R filename</code></td>
<td>Stores the messages in the file specified. By default, the <code>cldiag</code> utility writes the messages to <code>stdout</code>.</td>
</tr>
</tbody>
</table>

For example, to obtain a 15-second trace of the Cluster Manager daemon and have the trace report written to the file `cm_trace.rpt`, enter:

```
cldiag trace -t 15 -R cm_trace.rpt clstrmgr
```

For an example of the default trace report, see Sample Trace Report.

### Sample Trace Report

You can obtain the following sample trace report by entering:

```
cldiag trace -R clinfo_trace.rpt clinfo
```

```
Wed Mar 10 13:01:37 1998
System: AIX steamer Node: 3
Machine: 000040542000
Internet Address: 00000000 0.0.0.0

trace -j 011  -s -a

ID   PROCESS NAME I SYSTEM CALL ELAPSED APPL SYSCALL KERNEL INTERRUPT
001   trace                          0.000000 TRACE ON channel 0
Fri Mar 10 13:01:38 1995
011   trace                          19.569326 HACMP for AIX:clinfo Exiting Function:
      broadcast_map_request
111   trace                          19.569336 HACMP for AIX:clinfo Entering Function:
      skew_delay
111   trace                          19.569351 HACMP for AIX:clinfo Exiting Function:
      skew_delay, amount: 718650720
111   trace                          19.569360 HACMP for AIX:clinfo Exiting Function:
      service_context
111   trace                          19.569368 HACMP for AIX:clinfo Entering Function:
      dump_valid_nodes
111   trace                          19.569380 HACMP for AIX:clinfo Entering Function:
      dump_valid_nodes
111   trace                          19.569387 HACMP for AIX:clinfo Entering Function:
      dump_valid_nodes
111   trace                          19.569394 HACMP for AIX:clinfo Entering Function:
      dump_valid_nodes
```
011 trace 19.569402 HACMP for AIX:clinfo Waiting for event
011 trace 22.569933 HACMP for AIX:clinfo Entering Function: service_context
011 trace 22.569995 HACMP for AIX:clinfo Cluster ID: -1
011 trace 22.570075 HACMP for AIX:clinfo Cluster ID: -1
011 trace 22.570087 HACMP for AIX:clinfo Cluster ID: -1
011 trace 22.570097 HACMP for AIX:clinfo Time Expired: -1
011 trace 22.570106 HACMP for AIX:clinfo Entering Function: broadcast_map_request
002 trace 23.575955 TRACE OFF channel 0
               Wed Nov 15 13:02:01 1999
Notices for HACMP Troubleshooting Guide

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 product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user’s responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

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

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

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

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

The following paragraph does not apply to the United Kingdom or any country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions; therefore, this statement may not apply to you.

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

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

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

IBM Corporation
Dept. LRAS / Bldg. 003
11400 Burnet Road
Austin, TX 78758-3493
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.
### Index

| +-*|  
|---|---|
| /rhosts file | running clruncmd remotely 18 |
| /etc/hosts file | check before starting cluster 71 |
| | listing adapter IP labels 18 |
| | loopback and localhosts as aliases 95 |
| /etc/locks file | 75 |
| /etc/netsvc.conf file | editing for nameserving 97 |
| /etc/rc.net script | checking the status of 59 |
| /etc/services file | checking port listing 70 |
| /etc/syslog.conf file | obtaining clockd daemon messages 125 |
| /etc/syslogd file | redirecting output 98 |
| /sbin/rc.boot file | 87, 99 |
| /tmp/cm.log file | viewing 36 |
| | viewing its contents 40 |
| | changing its location 32 |
| | correcting sparse content 96 |
| | message formats 28 |
| | recommended use 23 |
| | selecting verbose script output 30 |
| | troubleshooting TCP/IP 59 |
| | understanding messages 27 |
| | viewing its contents 30 |
| /usr | becomes too full 105 |
| | /usr/es/sbin/cluster/cl_event_summary.txt 105 |
| | /usr/sbin/cluster/clinfo daemon |
| | Clinfo 42, 119 |
| | /usr/sbin/cluster/clockd daemon |
| | clockd daemon 147 |
| | Cluster Lock Manager 147 |
| | /usr/sbin/cluster/clsmuxpd daemon |
| | Cluster SMUX Peer 147 |
| | /usr/sbin/cluster/clstrmgr daemon |
| | Cluster Manager 147 |
| | /usr/sbin/cluster/etc/clhosts file |
| | invalid hostnames/addresses 95 |
| | on client 95 |
| | updating IP labels and addresses 95 |
| | /usr/sbin/cluster/server.status 84 |
| | /usr/sbin/cluster/utilities/clruncmd command 18 |
| | /usr/sbin/cluster/utilities/clsnapshot utility |
| | clsnapshot 17 |

### A

adapter failure
- switched networks 77

adapters
- troubleshooting 69

applications
- fail on takeover node 83
- identifying problems 12
- inaccessible to clients 95
- troubleshooting 41

ARP cache
- flushing 94

arp command 62
- checking IP address conflicts 59
- assigning persistent IP labels 61

ATM
- arp command 62
- LAN emulation troubleshooting 81
- troubleshooting 80

### C

CDE
- hangs after IPAT on HACMP startup 97

CEL preprocessor (CELPP)
- messages 138
- CELPP see CEL preprocessor

cfgmgr command
- unwanted behavior in cluster 85
- Diagnostic Group Shutdown Partition 85

checking
- cluster snapshot file 48
- HACMP cluster 42
- logical volume definitions 57
- shared file system definitions 58
- shared volume group definitions 55
- volume group definitions 53

cl_convert
- not run due to failed installation 68

cl_convert utility 68

cl_lsf command
- checking shared file system definitions 58

cl_lsv command
- checking logical volume definitions 57

cl_lsvg command
- checking shared volume group definitions 55

cl_nfskill command
- unmounting NFS filesystems 75

cl_scisdiskreset command
- fails and writes errors to /tmp/hacmp.out file 75
Index
C – C

cldiag utility
  checking volume group definitions 54
  cluster diagnostic tool 17
Cluster Manager debugging 43
  customizing /tmp/hacmp.out file output 32
  customizing output 27
  debug levels and output files 45
  initiating a trace session 148
  listing lock database contents 43
  obtaining trace information 151
  options and flags 26
  troubleshooting AIX 63
  viewing the /tmp/hacmp.out file 31
  viewing the cluster.log file 26
  viewing the system error log 34
clhosts file
  editing on client nodes 95
clients
  cannot access applications 95
  connectivity problems 94
  not able to find clusters 95
Clinfo
  checking the status of 42
  exits after starting 70
  messages 119
  not reporting that a node is down 96
  not running 95
  restarting to receive traps 70
  trace ID 149
  tracing 147
clinfo daemon
  messages 119
cllockd daemon
  exits after starting 70
  messages 125
clsmuxpd daemon
  /usr/sbin/cluster/cllockd daemon 42
  messages 134
clsnapshot utility 17, 48
clstat utility
  finding clusters 95
clstrmgr daemon
  messages 115
cluster configuration
  checking with cluster snapshot utility 17
cluster history log file
  message format and content 35
cluster IDs
  duplicate 71
Cluster Information Program
  Clinfo 147

Cluster Lock Manager
  checking the status of 42
  communicates slowly over FDDI or SOCC networks 79
  messages 125
  obtaining low-level information 43
  trace ID 149
  tracing 147
Cluster Manager
  activating debug mode 43
  cannot communicate in FDDI Dual Ring Network 77
  cannot process CPU cycles 99
  checking the status of 42
  fails to communicate in FDDI Dual Ring 77
  hangs during reconfiguration 71
  messages 115
  starts then hangs with message 69
  trace ID 149
  tracing 147
  troubleshooting common problems 69, 70, 71
  will not start 70
Cluster Message Log Files 22
Cluster Recovery Aids screen
  running clruncmd 74
cluster services
  starting on a node after a DARE 73
Cluster SMUX Peer
  checking the status of 42
  failure 95
  messages 134
  trace ID 149
  tracing 147
cluster snapshot
  checking during troubleshooting 48
  files 49
  information saved 48
  ODM data file 49
  using to check configuration 17
cluster topology
  defining cluster IDs 71
cluster.log file 25
  customizing output 27
  message formats 25
  recommended use 23
  viewing 25
cluster.mmddyyyy file
  recommended use 23
clverify utility
  checking a cluster configuration 47
  tasks performed 47
  troubleshooting a cluster configuration 70
commands
  arp  59, 62
  cl_convert  68
  cl_nfskill  75
  cl_scсидискreset  75
  cldiag  54
  crunmc  18, 74
  configchk  71
  df  57
  diag  63, 64, 66
  erpt  63
  fsck  75
  ifconfig  59, 61, 69
  lsattr  64
  lsdev  65
  lsfs  58
  lsv  56
  lsvp  55, 56
  lsrc  59
  lsvg  53
  mount  57
  netstat  59
  ping  59, 60
  varyonvg  83
config_too_long message  97, 117
configchk command
  returns an Unknown Host message  71
configuration files
  merging during installation  67, 68
configuring
  checking with snapshot utility  17
  run-time parameters  30
configuring clusters
  restoring saved configurations  68
conversion issues
  failed installation  68
C-SPOC utility
  checking shared file systems  58
  checking shared logical volumes  57
  checking shared volume groups  55
  commands  109
  messages  109, 138
cspoc.log file
  message format  37
  viewing its contents  38

d
  daemon.notice output
    redirecting to /usr/tmp/snmpd.log  98
daemons
  clinfo
    exits after starting  70
    messages
      Clinfo  119
  cllockd
    messages  125
  clsmuxpd
    messages  134
  clstrmgr
    messages  115
    cluster messages  22
    monitoring  42
    trace IDs  149
    tracing  147
DARE Resource Migration
  error messages  141
deadman switch
  avoiding  86
  fails due to TCP traffic  92
  releasing TCP traffic
    Deadman Switch  92
    tuning virtual memory management  87
df command  57
  checking filesystem space  57
DGSP
  handling node isolation
    Diagnostic Group Shutdown Partition  84
diag command
  checking disks and adapters  64
  testing the system unit  66
diagnosing problems
  recommended procedures  11
  using cldiag  17
Diagnostic Group Shutdown Partition
  error message displayed  84
disk adapters
  troubleshooting  64
disks
  troubleshooting  64
Distributed SMIT (DSMIT)
  unpredictable results  77

E
  enabling
    I/O pacing  86
  error messages
    console display of  12
    generated by scripts or daemons  13
    list of HACMP messages  107
  errors
    mail notification of  11
  erpt command  63
  event duration time
    customizing  98
  event emulator
    log file  14, 24
    messages  143
event summaries
  cl_event_summary.txt file too large 105
resource group information does not display 105
events
  changing custom events processing 72
  messages relating to unusual events 79
  examining log files 21
exporting
  volume group information 74

F
F1 help fails to display 105
failure detection rate
  as a factor in deadman switch problems 88, 100
  changing beyond SMIT settings 89, 100
  changing to avoid DMS timeout 92
  changing with SMIT 88, 100
  setting for network modules 90, 101
filesystems
  troubleshooting 57
flushing
  ARP cache 94
fsck command
  fails with Device open failed message 75

G
generating
  trace report 150

H
HACMP scripts log file See hacmp.out log file
hacmp.out log file
  brief summary 23
detailed description 27
hardware address swapping
  message appears after node_up_local fails 92
hardware system identifier
  licensing issues 68
HAView
  messages 144
  heartbeat rate 92, 103
  highest priority node
    not acquiring resource group 103
  high-water mark
    I/O pacing 87, 99

I
I/O pacing
  enabling 86
tuning 86
tuning the system 86
  identifying problems 34
ifconfig command 59, 61
  configuring an adapter 69
  initiating a trace session 148
installation issues
  cannot find filesystem at boot-time 67
  installing
    unmerged configuration files 67, 68
IP address takeover
  applications fail on takeover node 83
IP addresses
  in arp cache 62

L
LANG variable 105
license file
  clvm 68
listing
  lock database contents 43
locks
  comparing states 43
log files
  /tmp/cm.log 24
  /tmp/dms_logs.out 24
  /tmp/emuacmp.out 14, 24, 39
  /tmp/hacmp.out 23, 27
  cluster message 22
  cluster.log 23
  cluster.log file 25
  cluster.mmdd 23
  examining 21
  recommended use 23
  system error log 23, 33
types of
  with script and daemon error messages 13
logical volume manager (LVM) 53
logical volumes
  troubleshooting 56
low-water mark (I/O pacing)
  recommended settings 87, 99
lsattr command 64
lsdev command
  for SCSI disk IDs 64
lsfs command 57, 58
lslv command
  for logical volume definitions 56
lspv command 55
  checking physical volumes 55
  for logical volume names 56
lsrsc command
  checking the inetd daemon status 59
  checking the portmapper daemon status 59
lsvg command 53
  checking volume group definitions 53
LVM
  troubleshooting 53
M
mail
used for event notification 11
maxfree 87
mbufs
increase memory available 87, 100
messages
about resource group processing 32
cluster state 22
event notification 21
from clinfo daemon 119
from the Cluster Lock Manager 125
from the Cluster Manager 115
from the Cluster SMUX Peer 134
generated by HACMP C-SPOC commands 138
generated by HACMP DARE utility 141
generated by HACMP scripts 110
generated by HAView 144
generated by the Event Emulator 143
in verbose mode 21
minfree 87
mount command 57

N
netstat command
adapter and node status 59
NetView
deleted or extraneous objects in map 104
network
troubleshooting
network failure after MAU reconnect 78
will not reintegrate when reconnecting bus 78
network grace period 90, 102
network modules
changing parameters 91, 102
networks
Ethernet 63
reintegration problem 78
SOCC 79
Token-Ring 64, 84
troubleshooting 63
cannot communicate on ATM Classic IP 80
cannot communicate on ATM LANE 81
lock manager slow on FDDI or SOCC networks 79
SOCC network not configured after reboot 79
Token-Ring thrashes 78
unusual events when simple switch not supported 79
nodes
troubleshooting
cannot communicate with other nodes 77
configuration problems 72
dynamic node removal affects rejoining 73

O
Object Data Manager (ODM) 74
updating 74
obtaining trace information using cldiag 151
ODM see Object Data Manager

P
pci network adapter
recovering from failure 66
persistent IP label 61
ping command 60
checking node connectivity 59
flushing the ARP cache 95
ports
required by Cluster Manager 70
rebooting
fallover attempt fails 104
resource groups
down with highest priority node up 103
scripts
activating verbose mode 30
messages 21, 110
recovering from failures 18
verbose output 21
SCSI devices
troubleshooting 64
server.status file (see /usr/sbin/cluster/server.status) 84
service adapters
listed in /etc/hosts file 18
S
SMIT help fails to display with F1 105
snapshot
checking cluster snapshot file 48
stabilizing a node 18
starting
cluster services on a node after a DARE 73
switched networks
adapter failure 77
syncd daemon
changing frequency 87, 99
system components
checking 14, 41
system error log file
customizing output 35
message formats 33
recommended use 23
understanding its contents 33
viewing its contents 33
system ID
Concurrent Resource Manager 68
System Panic
invoked by deadman switch 99

T

target mode SCSI
failure to reintegrate 78
TCP/IP
troubleshooting 59
Token-Ring
network thrashes 78
node failure detection takes too long 84
tracing HACMP for AIX daemons
disabling using SMIT 149
enabling tracing using SMIT 148
generating a trace report using SMIT 150
initiating a trace session 148
overview 147
sample trace report 152
specifying a trace report format 149
specifying a trace report output file 150
specifying content of trace report 150
starting a trace session using SMIT 149
stopping a trace session using SMIT 150
trace IDs 149
using cldiag 151
using SMIT 148
troubleshooting
AIX operating system 63
applications 41
Ethernet networks 63
file systems 57
guidelines for 16
HACMP components 42
investigating system components 16, 41
LVM entities 53
networks 63
recommended procedures 11
SCSI disks and adapters 64
solving common problems 67
system hardware 66
TCP/IP subsystem 59
Token-Ring networks 64
volume groups 53
tuning
virtual memory management 87
tuning system
I/O pacing 86, 99
syncd frequency 87, 99

U
unmerged configuration files
installing 67
upgrading
pre- and post-event scripts 72

utilities
cldiag 26
clsnapshot 17, 48
clstat 95
clverify 47
C-SPOC (see also C-SPOC utility)
  checking shared filesystems 58
  checking shared logical volumes 57
  checking shared vgs 55

V
varyonvg command
fails during takeover 83
fails if volume group varied on 74
troubleshooting 83
verbose script output
activating 30
viewing
cluster.log file 25
cspoc.log file 38
emuhacmp.out log file 40
system error log file 33
virtual memory management
tuning deadman switch 87
vmstat command 87
vmtune command 87
volume groups
  checking definitions 54
  disabling autovaryon at boot 74
troubleshooting 53