

# AlphaServer Management Station

---

## User's Guide

**July 2005**

**Product Version:** AlphaServer Management Station Version 5.0

This manual describes the procedures for setting up and using the AlphaServer Management Station on AlphaServer ES47/ES80/GS1280 and GS80/GS160/GS320 platforms.

---

© Copyright 2003–2005 Hewlett-Packard Development Company, L.P.

The information contained herein is subject to change without notice.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation. UNIX® is a registered trademark of The Open Group in the U.S. and other countries. Java™ is a U.S. trademark of Sun Microsystems, Inc.

---

# Contents

## About This Manual

### 1 AlphaServer Management Station Overview and Startup

1.1	Overview of the AlphaServer Management Station .....	1-1
1.2	AMS's Place in Your Information Technology Infrastructure .....	1-2
1.2.1	The Platform's Management LAN .....	1-3
1.2.2	The NAT Box .....	1-3
1.2.3	The Terminal Server .....	1-3
1.3	The Server Platform Manager .....	1-3
1.4	The AlphaServer Management Utility .....	1-4
1.5	The AlphaServer Partition Wizard .....	1-5
1.6	The Platform Console Manager .....	1-5
1.7	Required Steps for Configuring the AMS .....	1-6
1.7.1	Step 1: Start the Console Management Facility Daemon and the Tomcat Web Server .....	1-6
1.7.2	Step 2: Add Users to the amsuser Group .....	1-7
1.7.3	Step 3: Add and Configure the Platforms to Be Managed .....	1-7

### 2 Using the Server Platform Manager

2.1	Overview .....	2-1
2.2	Logging On and Working with Users .....	2-2
2.2.1	Using the SPM Locally .....	2-2
2.2.2	Accessing the SPM Remotely .....	2-2
2.2.3	Security Certificate .....	2-2
2.2.4	Logging On .....	2-3
2.2.5	Assigning Privileges .....	2-4
2.3	The Main SPM Window .....	2-5
2.3.1	The Monitor Bar .....	2-5
2.3.2	The Left Frame .....	2-6
2.3.3	The Top Right Frame .....	2-7
2.3.4	The Bottom Right Frame .....	2-9
2.3.4.1	Hardware Status .....	2-9
2.3.4.2	Recent Events .....	2-10
2.3.5	Customizing the Main SPM Window .....	2-11
2.4	Adding and Modifying a Platform .....	2-11
2.4.1	Adding or Modifying an ES47, ES80, and GS1280 .....	2-11
2.4.2	Adding or Modifying a GS80, GS160, and GS320 .....	2-12
2.5	Managing Platforms .....	2-13
2.5.1	Connecting to the Platform's Management Port .....	2-14
2.5.1.1	ES47, ES80, and GS1280 Platforms .....	2-14
2.5.1.2	GS80, GS160, and GS320 Platforms .....	2-15
2.5.2	Partitions .....	2-15
2.5.3	Accessing the AMU .....	2-15
2.5.4	Accessing the APW .....	2-16
2.5.5	Viewing a Platform's Properties .....	2-16
2.5.5.1	ES47, ES80, and GS1280 Platform Properties .....	2-16

2.5.5.2	GS80, GS160, and GS320 Platform Properties .....	2-17
2.5.6	Removing a Platform .....	2-19
2.6	Managing Partitions .....	2-19
2.6.1	Configuring a Subpartition .....	2-19
2.6.2	Accessing the HP Insight Management Agents .....	2-20
2.6.3	Enabling and Disabling Events Generated from Console Output .....	2-21
2.6.4	Using the Event Viewer .....	2-22
2.6.5	Viewing ES47, ES80, and GS1280 Subpartition Properties .....	2-23
2.7	Adding a Standalone Console .....	2-23
2.8	Working with Consoles .....	2-24
2.8.1	Telnet Access to Consoles .....	2-24
2.8.2	Identifying, Contacting, and Disconnecting Other Users .....	2-24
2.8.2.1	Displaying and Users .....	2-24
2.8.2.2	Broadcasting a Message .....	2-25
2.8.3	Console Logging .....	2-25
2.8.4	Enabling and Disabling a Console .....	2-26
2.8.5	Port Mapping .....	2-26
2.8.6	Viewing a Console's Properties .....	2-27
2.8.7	Creating and Modifying an Event Definition File .....	2-28
2.8.8	Setting the Archive Period for Log Files .....	2-30

### 3 Using the AlphaServer Management Utility

3.1	Overview .....	3-1
3.2	Accessing and Configuring AMU .....	3-1
3.2.1	Running AMU as a Standalone Application .....	3-2
3.2.2	Running AMU from SPM .....	3-3
3.3	The Main AMU Window .....	3-3
3.3.1	The Left Frame .....	3-3
3.3.2	The Top Right Frame .....	3-4
3.3.2.1	The Hardware View .....	3-4
3.3.2.2	The Logical View .....	3-5
3.3.2.3	Displaying an Icon Legend .....	3-6
3.3.3	Bottom Right Frame .....	3-7
3.3.3.1	Activity Tab .....	3-7
3.3.3.2	Alerts Tab .....	3-7
3.4	Displaying the Platform's I/O and Power Connections .....	3-9
3.5	Monitoring the Platform's Environmental Status .....	3-10
3.6	Connecting to a Console .....	3-10
3.7	Connecting to the Platform's Management Port .....	3-11
3.8	Taking Exclusive Control .....	3-11
3.9	Viewing MBM Error Log Files .....	3-11
3.10	Using CDL File Support .....	3-12
3.11	Working with Firmware .....	3-13
3.12	Working with Partitions .....	3-15
3.12.1	The Partitions Branch .....	3-16
3.12.1.1	The Partitions Drop-Down Menu .....	3-16
3.12.1.2	The Partitions Properties Window .....	3-17
3.12.1.2.1	General Tab .....	3-17
3.12.1.2.2	Free Pool Tab .....	3-18
3.12.1.2.3	IP Connections Tab .....	3-19
3.12.1.2.4	Alerts Tab .....	3-19
3.12.2	The Hard Partitions Branch .....	3-19
3.12.2.1	Hard Partition Drop-Down Menu .....	3-20

3.12.2.2	The Hard Partition Properties Window .....	3-21
3.12.2.3	Alerts Tab .....	3-23
3.12.3	The Sub Partition Branch .....	3-24
3.12.3.1	The Sub Partition Drop-Down Menu .....	3-24
3.12.3.2	The Sub Partition Properties Window .....	3-25
3.12.3.3	Alerts Tab .....	3-26
3.13	Creating and Modifying Partitions .....	3-26
3.13.1	Creating a Partition .....	3-26
3.13.1.1	Preliminary Steps .....	3-27
3.13.1.2	New Hard Partitions Menu .....	3-27
3.13.1.3	Creating the Partition .....	3-28
3.13.2	Modifying an Existing Partition .....	3-28
3.13.2.1	Remove CPUs from a Partition .....	3-28
3.13.2.2	Add CPUs to a Subpartition .....	3-28
3.13.2.3	Assign Memory to a Subpartition .....	3-28
3.13.2.4	Assign Memory to a Community .....	3-28
3.14	Reconfiguring Cable Connections .....	3-29
3.15	Testing All Cable LEDs .....	3-29
3.16	Viewing Detailed Information About Each Component .....	3-29
3.16.1	Viewing Properties of System Drawers .....	3-29
3.16.1.1	Viewing General System Drawer Properties .....	3-29
3.16.1.2	Viewing Environmental Properties .....	3-29
3.16.1.3	Viewing Drawer Indicator Properties .....	3-30
3.16.1.4	Viewing Firmware Properties .....	3-30
3.16.2	Viewing Properties of I/O Drawers .....	3-30
3.16.2.1	Viewing Environmental Properties .....	3-30
3.16.2.2	Viewing Drawer Indicator Properties .....	3-30
3.16.2.3	Viewing Firmware Properties .....	3-31
3.16.3	Viewing Properties of Dual CPU Modules .....	3-31
3.16.3.1	Dual CPU Module Properties: Environment .....	3-31
3.16.3.2	Dual CPU Module Properties: Frequency .....	3-31
3.16.3.3	Dual CPU Module Properties: Firmware .....	3-31
3.16.4	Viewing Properties of CPUs .....	3-31
3.17	Using the Visual Editor .....	3-31
3.17.1	Accessing and Using the Editor .....	3-32
3.17.2	Creating and Modifying a New Template .....	3-32
3.17.3	Adding Platforms to a Standalone AMU .....	3-34
3.17.4	File Locations .....	3-35

## 4 Using the AlphaServer Partition Wizard

4.1	APW Overview and Start Up .....	4-1
4.1.1	Accessing the APW .....	4-1
4.1.2	APW Features .....	4-2
4.1.3	ES47/ES80/GS1280 and GS80/GS160/GS320 Platform Differences .....	4-2
4.2	Working with Partition Maps .....	4-4
4.2.1	The Current Partition Map Window .....	4-4
4.2.2	The Resources Window .....	4-6
4.2.3	The Work with Partition Maps Window .....	4-7
4.2.4	The Create or Modify a Partition Map Window .....	4-8
4.3	Modifying a Partition Map .....	4-9
4.3.1	Adding a Hard Partition .....	4-10
4.3.2	Modifying a Partition .....	4-11

4.3.3	Creating Soft Partitions .....	4-13
4.4	Creating a New Partition Map .....	4-14
4.5	Saving, Validating, and Committing a Partition Map .....	4-15
4.5.1	Saving a Partition Map .....	4-15
4.5.2	Validating a Partition Map .....	4-16
4.5.3	Committing a Partition Map .....	4-16
4.6	Managing APW Files .....	4-18

## 5 Using the Platform Console Manager

5.1	Overview .....	5-1
5.1.1	Starting, Navigating, and Exiting the PCM .....	5-2
5.1.2	Customizing the Telnet Escape Sequence .....	5-2
5.2	The Main PCM Window .....	5-2
5.2.1	System View and Selection Area .....	5-2
5.2.2	Buttons .....	5-3
5.2.3	Console Output .....	5-6
5.3	Adding a Platform or Console .....	5-6
5.3.1	Adding a Platform .....	5-7
5.3.1.1	Add an ES47, ES80, and GS1280 Platform .....	5-7
5.3.1.2	GS80, GS160, and GS320 Platforms .....	5-9
5.3.2	Adding a Console .....	5-10
5.3.2.1	Adding an AMS Platform Console .....	5-11
5.3.2.2	Adding a Standalone Console .....	5-11
5.4	Modifying Platform and Console Properties .....	5-12
5.5	Removing a Platform or Console .....	5-13
5.6	Restarting and Stopping the cmfd .....	5-14
5.6.1	Restarting the cmfd .....	5-14
5.6.2	Stopping the cmfd .....	5-14
5.7	Setting Log Archiving Interval .....	5-15
5.8	Working with Events .....	5-15
5.8.1	The Create Events Definition File Window .....	5-16
5.8.2	Modifying or Deleting an Existing Event Definition File .....	5-17
5.8.3	Generating Events from Console Error Messages .....	5-18
5.8.4	Viewing Events .....	5-20
5.9	Connecting to a Platform's Management Port .....	5-20
5.10	Managing Consoles .....	5-21
5.10.1	Connecting to a Console .....	5-22
5.10.2	Determining a Console's Status .....	5-22
5.10.3	Monitoring a Console's Output .....	5-23
5.10.4	Viewing the Consoles' Logs .....	5-23
5.10.5	Disconnect a Users from a Console .....	5-24
5.10.6	Managing Console Log Files .....	5-25

## A Troubleshooting AMS

## B Firmware Alerts

## C Log File Management

C.1	Console logs .....	C-1
C.2	AMS application logs .....	C-1

## D Using the Event Manager

D.1	Event Manager Overview .....	D-1
D.1.1	Features of the Event Manager .....	D-1
D.1.2	Understanding Event Manager Events .....	D-1
D.1.3	Event Manager Command-Line Utilities .....	D-2
D.1.4	Event Manager System Files .....	D-3
D.2	Administering Event Manager .....	D-5
D.2.1	Starting and Stopping Event Manager .....	D-6
D.2.2	Configuring the Event Manager Logger .....	D-6
D.2.3	Security Considerations .....	D-9
D.2.3.1	User Authentication .....	D-9
D.2.3.2	User Authorization .....	D-9
D.2.4	Managing Log Files .....	D-10
D.3	Using Event Manager in System Administration .....	D-11
D.3.1	Displaying Events Using evmshow .....	D-11
D.3.2	Introducing Event Filters .....	D-13
D.3.3	Retrieving Stored Events Using evmget .....	D-14
D.3.4	Sorting Events Using evmsort .....	D-15
D.3.5	Using the -A Option to Simplify the Command String .....	D-16
D.3.6	Monitoring Events Using evmwatch .....	D-17
D.3.7	Understanding the Event Manager Mark Event .....	D-18
D.3.8	Viewing Events Using the Event Viewer .....	D-18
D.3.9	Advanced Selection and Filtering Techniques .....	D-19
D.3.9.1	Filtering By Time .....	D-19
D.3.9.2	Using the event-id to Select Events for Detailed Display .....	D-20
D.3.9.3	Searching for Reserved Component Names .....	D-21
D.3.9.4	Using Filter Files .....	D-21
D.3.10	Logging and Forwarding Events .....	D-22
D.3.10.1	Logging Events .....	D-23
D.3.10.2	Using Forwarding to Handle Events Automatically .....	D-23
D.4	Troubleshooting Event Manager .....	D-24

## E Sending Selected Events Via E-mail

E.1	Overview .....	E-1
E.2	Sending Selected Events to a Cellular Phone or Pager .....	E-1
E.3	EVM Configuration File .....	E-1
E.4	Using Templates with evmshow .....	E-1
E.5	Editing the EVM Logger Configuration File .....	E-2
E.6	Verifying Success .....	E-3
E.7	Troubleshooting .....	E-4

## F Regular Expressions

## G Navigating the Character Cell Environment

### Glossary

### Index

### Examples

D-1	Sample Event Manager Logger Configuration File Entries .....	D-6
D-2	Sample Event Manager Authorization File Entries .....	D-9

### Figures

1-1	AMS's Place in Your Information Technology Infrastructure .....	1-2
1-2	SPM Main Window .....	1-4
1-3	AMU Main Window .....	1-5
1-4	PCM Main Window .....	1-6
2-1	Security Warning .....	2-3
2-2	Login Dialog Box .....	2-3
2-3	Assign User Access Dialog Box .....	2-4
2-4	Main SPM Window .....	2-5
2-5	Monitor Bar .....	2-6
2-6	Left Frame .....	2-7
2-7	The Top Right Frame (Icon View) .....	2-8
2-8	The Top Right Frame (Details View) .....	2-8
2-9	The Top Right Frame (Specific Console View) .....	2-8
2-10	Add Platform Dialog Box (ES47, ES80, and GS1280) .....	2-11
2-11	Add Platform Dialog Box (GS80, GS160, and GS320) .....	2-12
2-12	Platform Properties Dialog Box (ES47, ES80, and GS1280) .....	2-17
2-13	Platform Properties Dialog Box (GS80, GS160, and GS320) .....	2-18
2-14	Remove Platform Confirmation Dialog Box .....	2-19
2-15	Configure Subpartition Dialog Box .....	2-20
2-16	Insight Management Agents .....	2-21
2-17	View Events Dialog Box .....	2-22
2-18	Subpartition Properties Dialog Box .....	2-23
2-19	Broadcast to All Users Dialog Box .....	2-25
2-20	View Console Log... Window .....	2-26
2-21	Port Mapping Dialog Box .....	2-27
2-22	Console Properties Box .....	2-27
2-23	Create/Modify Event Definition File Dialog Box .....	2-29
2-24	Set Log File Archive Period Dialog Box .....	2-30
3-1	Main AMU Window .....	3-3
3-2	Right Frame with Logical View .....	3-5
3-3	Logical View .....	3-6
3-4	Hardware View Icon Legend .....	3-6
3-5	Partition View Icon Legend .....	3-7
3-6	Alerts Tab in System Drawer Properties Window .....	3-8
3-7	I/O and Power Connections .....	3-9
3-8	Status Lights .....	3-10
3-9	Platform Properties Window Logs Tab .....	3-12



3-10	Save CDL File Dialog Box .....	3-13
3-11	Platform Properties Window Firmware Tab .....	3-14
3-12	Firmware Module Properties Window .....	3-15
3-13	Upgrade Firmware Window .....	3-15
3-14	Partitions Drop-Down Menu .....	3-16
3-15	Partitions Properties Dialog Box — General Tab .....	3-17
3-16	Partitions Properties Dialog Box — Free Pool Tab .....	3-18
3-17	Partitions Properties Dialog Box — IP Connections Tab .....	3-19
3-18	Hard Partitions Drop-Down Menu .....	3-20
3-19	Hard Partition Properties Window .....	3-21
3-20	Hard Partition Properties — Resources Tab .....	3-23
3-21	Subpartitions Drop-Down Menu .....	3-24
3-22	Sub Partition Properties Box .....	3-25
3-23	Sub Partition Properties — Resources Tab .....	3-26
3-24	New Hard Partition Menu .....	3-27
3-25	New Template Dialog Box .....	3-33
3-26	Visual Editor .....	3-34
4-1	QBB Resources Window .....	4-3
4-2	Duo Resources Window .....	4-3
4-3	Current Partition Map .....	4-5
4-4	Work with Partition Maps Window .....	4-8
4-5	Create or Modify a Partition Map Window .....	4-9
4-6	Add a Partition .....	4-10
4-7	Modify a Partition .....	4-12
4-8	Partition Map Creation Criteria Window .....	4-14
4-9	Warning Message .....	4-15
4-10	Commit Status Window .....	4-17
4-11	Committed Partition Map Window .....	4-17
5-1	Main PCM Window .....	5-1
5-2	Connect Dialog Box .....	5-3
5-3	Force Connection Dialog Box .....	5-4
5-4	Tools Dialog Box .....	5-5
5-5	Modify Mapped Port Dialog Box .....	5-6
5-6	Add Platform: Specify Type Window .....	5-7
5-7	Add an ES47, ES80, and GS1280 Platform Window .....	5-8
5-8	Layout Template Selection Window .....	5-8
5-9	Select an Event Definition File Window .....	5-9
5-10	Add a GS80, GS160, and GS320 Platform .....	5-10
5-11	Add a Console Dialog Box .....	5-11
5-12	Add a Standalone Console Dialog Box .....	5-12
5-13	Modify a Platform Dialog Box .....	5-13
5-14	Restarting the cmfd .....	5-14
5-15	Set Log Archive Interval Dialog Box .....	5-15
5-16	Create Events Definition File Window .....	5-16
5-17	Import an Event Pattern .....	5-17
5-18	Events: Add Dialog Box .....	5-18
5-19	View Events Dialog Box .....	5-20
5-20	Connecting to the Platform's Management Port .....	5-21
5-21	Console Status Display .....	5-22
5-22	PCM Console Log .....	5-23
5-23	View a Console Log .....	5-24
5-24	Disconnecting Users from a Console .....	5-24
D-1	Event Model .....	D-2

## Tables

2-1	SPM Privileges .....	2-4
3-1	Types of Alerts .....	3-8
5-1	EVM Event Priorities .....	5-19
B-1	Firmware Alerts — Environmental Group .....	B-1
B-2	Firmware Alerts — Operational Group .....	B-2
B-3	Firmware Alerts — Partition Group .....	B-2
B-4	Firmware Alerts — EV7 Group .....	B-3
D-1	Event Manager Command-Line Utilities .....	D-3
D-2	Event Manager Administrative Utilities .....	D-3
G-1	Character Cell Navigation Key Guide .....	G-1

---

# About This Manual

This manual describes the procedures for setting up and using the AlphaServer Management Station on AlphaServer ES47/ES80/GS1280 and GS80/GS160/GS320 platforms.

Topics include monitoring platforms, monitoring and managing event logs, booting and managing operating systems configured on the platforms, and accessing the AMS remotely.

## Audience

The AlphaServer Management Station *User's Guide* is intended for anyone who administers ES47/ES80/GS1280 and GS80/GS160/GS320 platforms.

## Organization

This manual is organized as follows:

<i>Chapter 1</i>	Provides an overview of the AMS, its components, and what you can accomplish with them. It also describes the steps you take to start up and configure the AMS.
<i>Chapter 2</i>	Describes the Server Platform Manager (SPM) and how you can use it.
<i>Chapter 3</i>	Describes the AlphaServer Management Utility (AMU) and how you can use it.
<i>Chapter 4</i>	Describes how to use the AlphaServer Partition Wizard (APW) to simplify the creation and management of partitions.
<i>Chapter 5</i>	Describes the Platform Console Manager (PCM) and how you can use it.
<i>Appendix A</i>	Lists error messages and provides corrective action for errors that might be encountered while using components of the AMS.
<i>Appendix B</i>	Lists all of the alerts generated by the firmware, the source of each alert, the severity level, and the data that is contained in the alert packet.
<i>Appendix C</i>	Provides information about the log files generated by the AlphaServer Management Station applications and the <code>cmfd</code> daemon.
<i>Appendix D</i>	Describes how to use the Event Manager (EVM).
<i>Appendix E</i>	Describes how to send EVM events via e-mail.
<i>Appendix F</i>	Describes special characters that may be helpful when making changes to event definitions.
<i>Appendix G</i>	Provides a key guide for the character cell environment of the Platform Console Manager (PCM).
<i>Glossary</i>	Provides definitions of AMS-related terms used in this manual.

## Related Documentation

The following documents may be useful references when you are installing and configuring ES47/ES80/GS1280 and GS80/GS160/GS320 platforms for use with the AMS:

- The documentation for your hardware shows how to physically set up the processor and its additional devices, provides a list of supported console variables, and contains troubleshooting guidelines. It is located on the Server Management CD-ROM.
- The documentation for your Network Address Translation (NAT) box or terminal server or router that contains installation and configuration information.

## Conventions

<code>%</code>	A percent sign represents the C shell system prompt. A dollar sign represents the system prompt for the Bourne, Korn, and POSIX shells.
<code>#</code>	A number sign represents the superuser prompt.
<code>% <b>cat</b></code>	Boldface type in interactive examples indicates typed user input.
<code>&gt;&gt;&gt;</code>	The console mode prompt is three right angle brackets.
<i>file</i>	Italic (slanted) type indicates variable values, placeholders, and function argument names.
<code>cat(1)</code>	A cross-reference to a reference page includes the appropriate section number in parentheses. For example, <code>cat(1)</code> indicates that you can find information on the <code>cat</code> command in Section 1 of the reference pages.
<code>Ctrl/x</code>	This symbol indicates that you hold down the first named key while pressing the key or mouse button that follows the slash. In examples, this key combination is enclosed in a box (for example, <code>Ctrl/C</code> ).

---

# AlphaServer Management Station Overview and Startup

This chapter provides a brief overview of the AlphaServer Management Station (AMS) and describes the procedures for starting and configuring it. The following topics are discussed:

- AMS basics (Section 1.1)
- The AMS's place in your company's information technology infrastructure (Section 1.2)
- The Server Platform Manager (Section 1.3)
- The AlphaServer Management Utility (Section 1.4)
- The AlphaServer Partition Wizard (Section 1.5)
- The Platform Console Manager (Section 1.6)
- The steps you need to take to start and configure the AMS (Section 1.7)

## 1.1 Overview of the AlphaServer Management Station

The AlphaServer Management Station (AMS) is a software application running on an AlphaServer or workstation that allows you to manage one or more ES47/ES80/GS1280 and GS80/GS160/GS320 platforms.

Using the AMS, you can monitor platform environmental status, monitor message and event logs, connect to the platform's management port, and boot and manage operating systems configured on subpartitions of the platforms. You can use the AMS either locally on the AlphaServer or access it remotely through either a Web browser or a Telnet session. You must have an account on the AMS machine and log in to it to access its functionality.

The AMS management software is composed of the following:

- The Server Platform Manager (SPM) is a client-server application. The server runs on the AMS and the client is a Web-based graphical user interface (see Chapter 2) that provides remote platform management.
- The AlphaServer Management Utility (AMU) is a client-server application. The server runs on the AMS and the client is a Web-based graphical user interface (see Chapter 3) that allows you to view and monitor a particular platform in greater detail. The AMU is for use with ES47, ES80, and GS1280 systems only.
- The AlphaServer Partition Wizard (APW) is a client-server application. The server runs on the AMS and the client is a graphical application that simplifies the creation and management of partitions on AlphaServer ES47, ES80, and GS1280 and GS80, GS160, and GS320 system platforms. (See Chapter 4.)
- The Platform Console Manager (PCM), a character-cell user interface (see Chapter 5) that allows you to monitor and manage consoles over low bandwidth remote connections.
- Underlying the SPM, AMU, APW and PCM is the Console Management Facility (CMF) daemon, `cmfd`, which controls the connections to consoles configured on the platforms. The `cmfd` monitors and logs the output of any console connections.

The AMS can be used as the single point of access to manage your ES47/ES80/GS1280 and GS80/GS160/GS320 platforms as described in the following section.

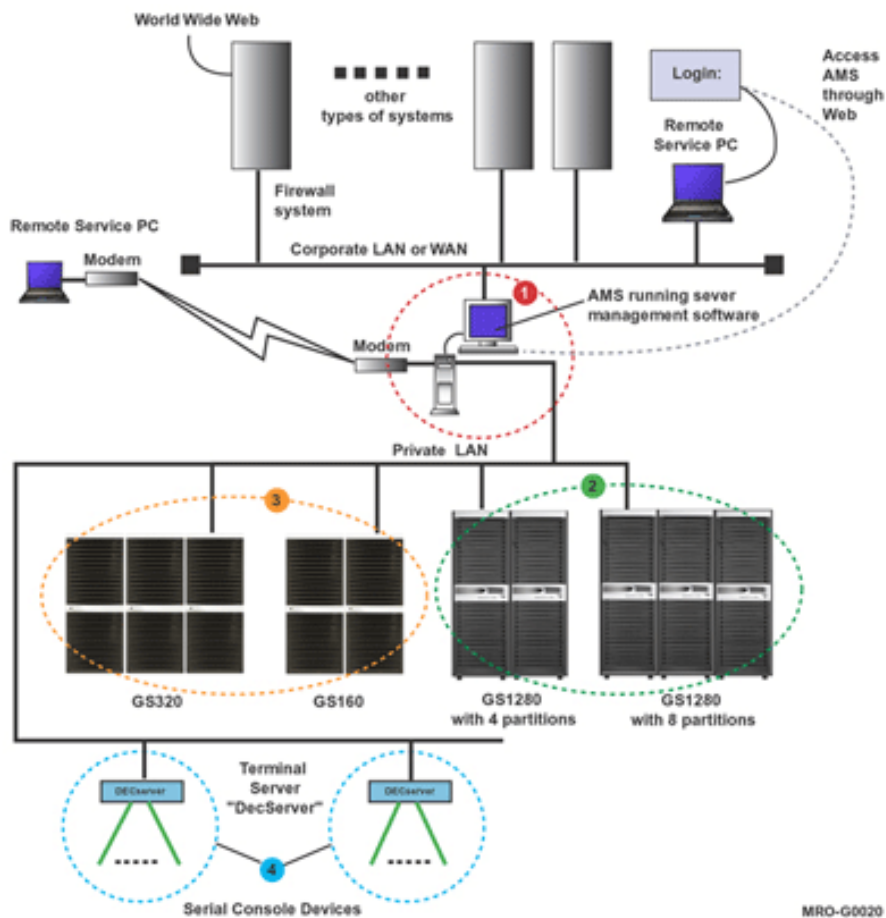
## 1.2 AMS's Place in Your Information Technology Infrastructure

The AlphaServer or workstation running the AMS software can serve as a bridge between the platform's management LAN and your corporate network. See Section 1.2.1 for more information.

Use the AMS machine as a single point of access to the platforms. For additional security, you can install two network interface cards (NIC) in the AMS machine. This allows the AMS machine to connect to the platform's built-in local area network (LAN) through a Network Address Translation (NAT) box, terminal server, or similar device, and to the corporate network. This configuration restricts access to the platforms because you must have an account on the AMS machine to use its components.

Figure 1-1 shows the AMS as the single point of access to the managed AlphaServer platforms connected to the AMS via a private LAN. The figure illustrates that users with the appropriate permissions to the AMS can manage the platforms from a Web browser or Telnet session through an Internet or modem connection, or from a local connection to the corporate network.

**Figure 1-1: AMS's Place in Your Information Technology Infrastructure**



- 1 The AMS machine runs software that controls access to platforms through their management LANs.

- 2 The GS1280 platforms are connected to the AMS management LAN through a NAT box. These platforms have their own internal Server Management LAN.
- 3 The GS160 and GS320 platforms are connected to the AMS management LAN through a terminal server.

### 1.2.1 The Platform's Management LAN

ES47, ES80, and GS1280 platforms are configured with a built-in management local area network (LAN). The LAN connects to the platform's management software, which is controlled by the backplane manager (MBM). The management LAN is used for communication with firmware.

When you connect the AMS to the platform's management LAN, you can connect to the MBM port to perform platform management tasks such as displaying configuration information, status, and error logs, configuring the MBM, or updating the firmware.

See the *Command Line Interface* reference on the Installation and Management CD for more information about managing the platform through the management LAN.

### 1.2.2 The NAT Box

A Network Address Translator device (NAT box) is a device that allows multiple connections from your corporate network to the private local area network (LAN) configured on ES47, ES80, and GS1280 platforms. A router is a type of NAT box.

Every ES47, ES80, and GS1280 platform is configured with its own management LAN using the same IP address, 10.253.X.X. The NAT box is an address translator that enables you to configure a different set of IP addresses for the platform so users on the corporate network can access the platform's management LAN. The NAT box translates the IP addresses you configure into the platform's internal set of IP addresses.

See the Installation and Service CD for information on how to install and configure NAT boxes. Also, see the instructions that came with your NAT box.

### 1.2.3 The Terminal Server

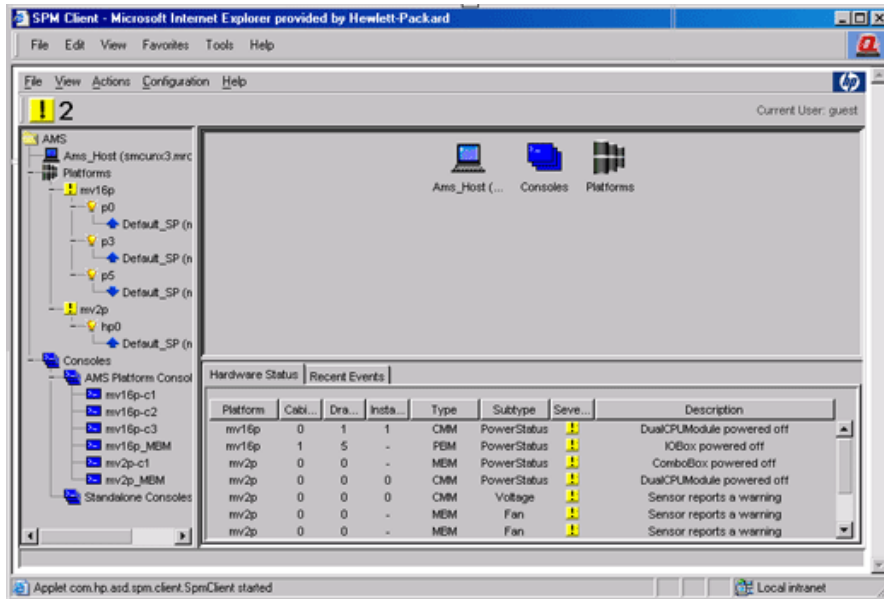
A terminal server is a device that provides terminals (PCs, printers, and other devices) with a common connection point to a local or wide area network. In an AMS environment, the terminal server is connected to the Internal Server Management LAN, which connects to the AMS host. You can connect multiple GS80, GS160, and GS320 platforms to the LAN, with each one having its own terminal server.

## 1.3 The Server Platform Manager

The Server Platform Manager (SPM) is a graphical client-server application. The server runs on the AMS machine and the client is a Web-based graphical user interface that provides local and remote management of ES47/ES80/GS1280 and GS80/GS160/GS320 platforms. It displays a list of managed platforms including the platform's partitions and the systems and consoles associated with those partitions. A system is a subdivision of a platform and runs an operating system.

The SPM displays each platform's hardware status and each partition's and console's operation status. The SPM provides Telnet access to a platform's management port, to a system's SRM console, and to management applications dedicated for managing platforms and systems.

Figure 1-2: SPM Main Window



The SPM allows you to:

- Display all platforms connected to the AMS and configured in the SPM
- Monitor the status of all platforms
- Display environmental errors
- Launch the AlphaServer Management Utility (AMU) and operating system management applications
- Launch the AlphaServer Partition Wizard (APW)
- Connect to the consoles of systems running on the platform to boot, log in, and monitor the operating system through error and event logs
- Display the platform's management port logs and system's console logs
- Display the most recent EVM events that have occurred on AMS-managed platforms and consoles
- Display the event logs of a platform and console
- Launch the HP Insight Management Agents running on a subpartition's operating system and on the AMS system

See Chapter 2 for detailed information.

## 1.4 The AlphaServer Management Utility

The AlphaServer Management Utility (AMU) is a client-server application. The server runs on the AMS machine and the client is a Web-based graphical user interface that allows you to view, configure, and monitor a particular ES47, ES80, and GS1280 platform.

Using the AMU client, you can perform the following tasks:

- View detailed, dynamic information about the configuration and status of platforms, system drawers, hard partitions, subpartitions, I/O drawers, dual CPU modules, and CPUs.
- Monitor a platform's environmental status, I/O connections, and power connections.
- Create partitions and distribute resources between partitions.

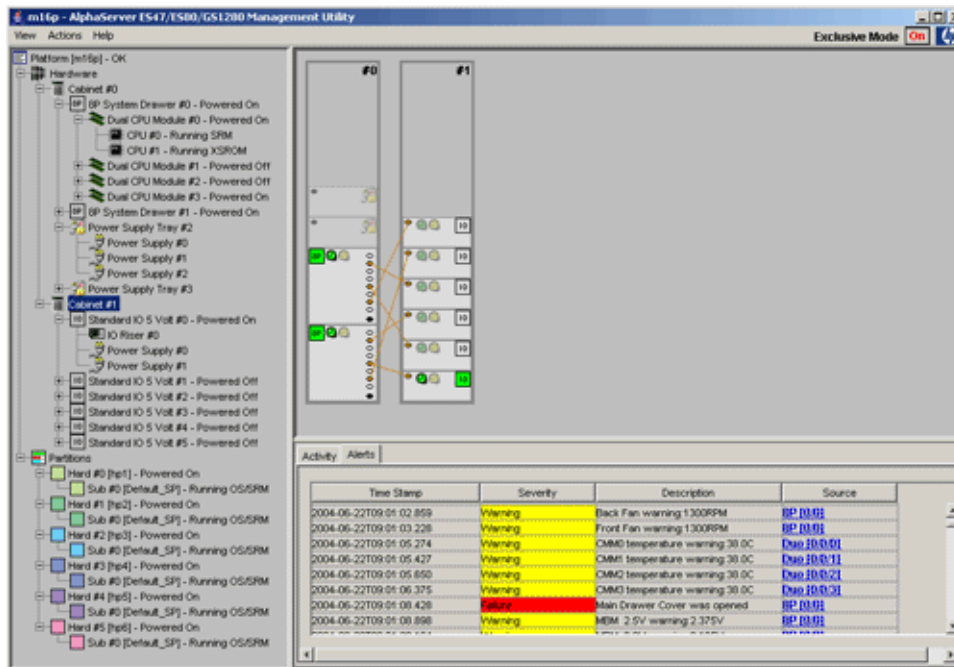


- Display hardware error logs.
- Display hardware alerts.
- Connect to the management port and SRM Console ports of ES47, ES80, and GS1280 systems to load and boot the operating system, log into the operating system running on a subpartition, and issue commands from the command-line interface.
- View the installed firmware version and upgrade the firmware.

The AMU does not recognize GS80, GS160, and GS320 platforms.

Figure 1-3 shows the AMU. The left frame displays a tree view of the managed platform and the right frame displays a graphical representation of the platform.

**Figure 1-3: AMU Main Window**



See Chapter 3 for detailed information.

## 1.5 The AlphaServer Partition Wizard

Through a wizard-like series of screens, the AlphaServer Partition Wizard (APW) enables you to work with partitions without having to know anything about the console commands involved. The APW works with both hard and soft partitions.

As you create and modify partitions, the APW updates AMS configurations by adding, modifying, and removing consoles as needed to match your partition configuration. You can use the APW with both ES47/ES80/GS1280 and GS80/GS160/GS320 platforms.

You can run the APW from the Server Platform Manager (SPM) and from the command line.

See Chapter 4 for detailed information.

## 1.6 The Platform Console Manager

The Platform Console Manager (PCM) is a character-cell application that displays a list of managed systems and their consoles for each platform connected to the AMS. A system is a subdivision of a platform and runs an operating system.

Because the PCM runs in the character cell environment, it is ideal for use when you use Telnet to connect to the AMS machine over a low-bandwidth connection.

The PCM displays each console's status and provides access to each console and to the console's log files. It also displays a continuously updated, timestamped list of the latest console output from the managed systems. The PCM obtains information about each system from a database that is shared between all the components of the AMS application. Figure 1-4 shows the main PCM window.

**Figure 1-4: PCM Main Window**



You can use the PCM as the launch point for all console management activities. With PCM, you can perform the following tasks:

- Add, modify, and delete systems within each platform
- Connect to the platform's management port
- Connect to the console of an operating system
- View a list and status of systems within each platform
- Log console output and view console logs of each system

See Chapter 5 for detailed information.

## 1.7 Required Steps for Configuring the AMS

The following steps describe how to configure the AlphaServer Management Station. You must perform these configuration steps before you try to access the AMS applications to manage your AlphaServer:

### 1.7.1 Step 1: Start the Console Management Facility Daemon and the Tomcat Web Server

The Console Management Facility (CMF) daemon, `cmfd`, allows you to connect to consoles configured on the platforms. It monitors and logs the output of any console connections.

The Tomcat Web server allows you to run the Server Platform Manager (SPM) and AlphaServer Management Utility (AMU) in a Web browser.

The following steps show you the commands you need to run to start the `cmfd` daemon and the Tomcat Web server:

1. To start `cmfd` enter one of the following commands:

For Tru64 UNIX:

```
# /sbin/init.d/cmfd start
```

For Linux:

```
# /etc/init.d/cmfd start
```

The `cmfd` starts automatically during subsequent reboots of the AMS.

2. To start the Tomcat Web server enter one of the following commands:

For Tru64 UNIX:

```
# /sbin/init.d/amstomcat start
```

For Linux:

```
# /etc/init.d/amstomcat start
```

The Tomcat Web server starts automatically during subsequent reboots of the AMS.

See Section 3.2.1 for information about running AMU as a standalone application.

## 1.7.2 Step 2: Add Users to the `amsuser` Group

The `amsuser` group is created on the AMS machine when you install the AMS software. Members of the `amsuser` group, along with root, are allowed to run the SPM and PCM.

To add users to the `amsuser` group, edit the `/etc/group` file located on the AMS machine.

You can secure access to the platforms by installing two network interface cards (NIC) in the AMS machine. This allows the AMS machine to connect to the platform's built-in local area network (LAN) and the corporate network through a Network Address Translator (NAT) box or similar device for ES47, ES80, and GS1280 platforms and through terminal servers for GS80, GS160, and GS320 platforms. This configuration restricts access to the platforms because you must have an account on the AMS machine to use its components.

We recommend that you secure access to the platforms in this way for the following reasons:

- There is no login process to the MBM; therefore, it is not secure.
- Securing access to the platforms also controls conflicting access to the MBM console and subpartition console ports. Only one connection can be made to a console port at a time.

## 1.7.3 Step 3: Add and Configure the Platforms to Be Managed

Before managing platforms with the AMS, you must add and configure them in either the Server Platform Manager (SPM) or the Platform Console Manager (PCM):

- Use the SPM if you want to manage the platforms locally on the AMS machine or remotely using a Web browser. See Section 2.2 for information about logging into the SPM and Section 2.4 for information about adding a platform.
- Use the PCM if you want to manage the platforms remotely over a low-bandwidth connection. See Section 5.1.1 for information about starting PCM and Section 5.3 for information about adding a platform.

SPM and PCM use a common datastore, which means that platforms and consoles configured by SPM can be displayed in PCM and those configured by PCM can be displayed in SPM.



---

## Using the Server Platform Manager

This chapter describes the different tasks you can accomplish using the Server Platform Manager (SPM). Section 2.1 provides a brief overview of the program, after which, the following topics are discussed:

- How to access the program locally and remotely, log on, and assign privileges (Section 2.2)
- The parts of the main SPM window and the icons it uses (Section 2.3)
- How to add and modify a platform (Section 2.4 )
- Managing platforms (Section 2.5)
- Managing subpartitions (Section 2.6)
- Adding a standalone console (Section 2.7)
- Working with consoles (Section 2.8)

### 2.1 Overview

The Server Platform Manager is a graphical client-server application. The server runs on the AMS machine and the client is a Web-based graphical user interface that provides local and remote management of platforms and consoles.

Each console represents a name for a port on a platform or a subpartition that can be connected via the `cmd`. Consoles are logged and monitored for events on all platform management ports and all partition ports.

Each platform has at least one console, the console associated with the platform management port or the terminal-server port, which is always port 23.

A partition that can run an operating system can have a console:

- On ES47, ES80, and GS1280 platforms, the port number associated with a console is always assigned by the firmware.
- On GS80, GS160, and GS320 platforms, the port is assigned through the terminal-server configuration.

Using the SPM's left frame and monitor bar you can monitor the status of platforms and systems. In the right frame's tabbed view you can see detailed status information and EVM events. Both displays are updated dynamically.

The left frame lets you monitor the hardware status of each platform and see the operation status of each partition using the SPM's color-coded status icons.

The monitor bar, located under the menu bar, lets you see the following:

- The status of any platforms that are running in a warning, critical, or unknown state
- The number of platforms with that status
- The user name of the person currently logged in

You can also view and manage the platforms' partitions and the consoles associated with those partitions.

To manage a platform or system, you can launch a Telnet session to a platform's management port or a system's console. You can also access platform and system management applications.

The SPM's online help provides step-by-step information about tasks you can perform with the SPM. To view the SPM online help, select `Help` in the menu bar and then select `Contents`.

## 2.2 Logging On and Working with Users

The following sections describe how access and log onto the SPM, add users, and assign privileges to users.

### 2.2.1 Using the SPM Locally

You can run the SPM locally on an AMS machine either in a Web browser or as a Java application. We recommend running SPM locally on the AMS as a Java application.

To run the SPM locally on an AMS machine using a Web browser:

1. Set the environment variable for the Java 2 plug-in in the `ksh` environment:

On Tru64 UNIX:

```
# NPX_PLUGIN_PATH=/usr/opt/java142/jre/plugin/alpha/ns4
# export NPX_PLUGIN_PATH
```

On Linux:

```
# ln -s /usr/java/j2re1.4.2_08/plugin/i386/ns610-gcc32/libjavaplugin_oji.so \
/usr/lib/mozilla/plugins
```

2. Point your browser to the following URL (where `localhost` is the host name of the AMS machine):

```
http://localhost:8080/spm
```

To run the SPM locally on an AMS machine as a Java application:

```
# /usr/bin/spm
```

### 2.2.2 Accessing the SPM Remotely

To connect to the SPM, enter the following URL in a Web browser, specifying the host name of the AMS machine you want to connect to:

```
http://AMS_hostname:8080/spm
```

### 2.2.3 Security Certificate

The first time you access Version 3.0 of the SPM program or the AMU as a standalone program, you must respond the Java Plug-in Security Certificate (Figure 2-1) that is displayed prior to loading the SPM program.

**Figure 2-1: Security Warning**



The action you take with the security window determines whether you can access the program and whether you will see the certificate again:

- Selecting Grant this session allows SPM to start; however, you will see this window the next time you access SPM.
- Selecting Grant always allows SPM to start. You will not see this window again.
- Selecting Deny prohibits SPM from starting.

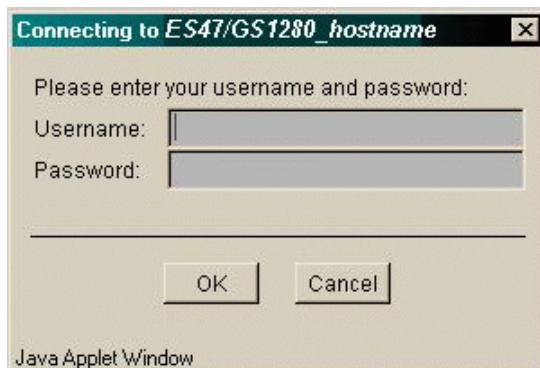
Pressing the View Certificate button opens a new window with information about the certificate.

All applets included in the AMS application are digitally signed by HP with a VeriSign certificate. The signing gives applets permission to access resources and enable copy and paste operations on client machines.

## 2.2.4 Logging On

You must be root on the AMS machine to log into the SPM for the first time. The AMS root user automatically has SPM administrator privileges. Authorization roles can be assigned only to accounts in the `amsuser` group. Figure 2-2 shows the SPM login dialog box.

**Figure 2-2: Login Dialog Box**



## 2.2.5 Assigning Privileges

The AMS root user has administrator privileges to all SPM functions by default. All other amsuser group accounts have limited guest access until the SPM administrator assigns them different privileges.

An administrator can assign or modify privileges to an amsuser group account from the Configuration menu by choosing Security → Assign User Access... (Figure 2-3), selecting the role in the combo box, and selecting Modify.

The SPM access roles are stored in the SPM's server database until the administrator removes them.

**Figure 2-3: Assign User Access Dialog Box**

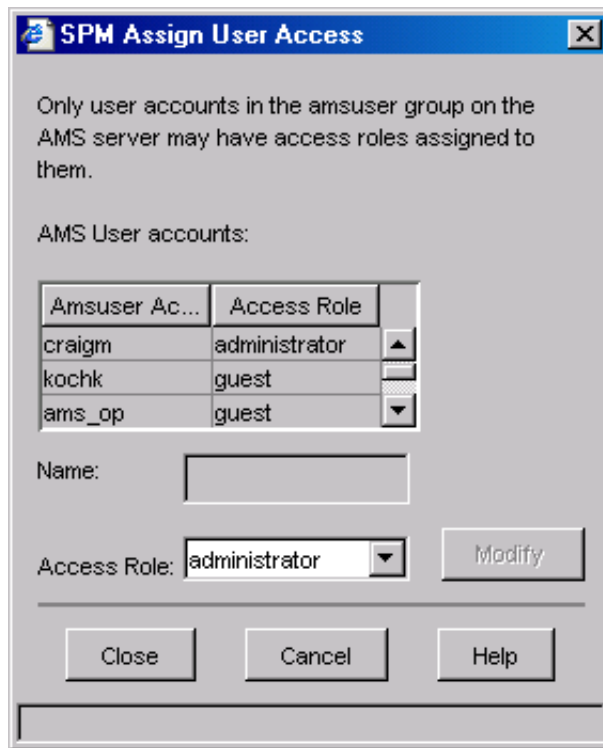


Table 2-1 displays a list of SPM functions and the privileges allowed for each.

**Table 2-1: SPM Privileges**

	Administrator	Operator	Guest
Expand and collapse tree	yes	yes	yes
View discovered servers and their status	yes	yes	yes
View event details (toolbar and tree)	yes	yes	yes
Customize the display of the right frame	yes	yes	yes
View help (all menus)	yes	yes	yes
Set refresh period	yes	yes	
Add platform	yes		
Modify platform	yes		
Remove platform	yes		
Configure console	yes	yes	
Assign access roles	yes		



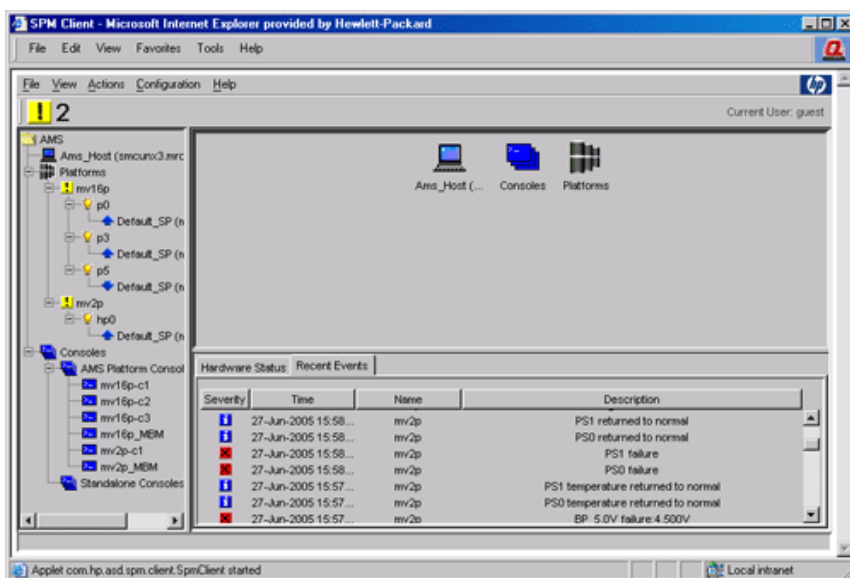
**Table 2-1: SPM Privileges (cont.)**

	Administrator	Operator	Guest
Launch AMU, Event Viewer, Insight Management Agents	yes	yes	
Launch APW	yes		
Telnet to console	yes		
Telnet to MBM	yes		
Turn on or off console output logging	yes		
View console log files	yes	yes	
View properties (all tree notes)	yes	yes	
Show/disconnect users	yes	yes	
Add standalone console	yes	yes	
Map console ports	yes	yes	
Broadcast to connected users	yes	yes	
Enable console	yes	yes	
Show AMS sessions	yes	yes	

## 2.3 The Main SPM Window

The main SPM window displays the platforms and consoles connected to the SPM and lets you interact with them. Figure 2-4 shows the main SPM window, which is described in the following sections.

**Figure 2-4: Main SPM Window**






### 2.3.1 The Monitor Bar

The monitor bar (Figure 2-5), gives you an easy way to see the status of any platforms that are running in a warning, critical, or unknown state; the number of platforms with that status; and the user name of the person currently logged in to the SPM using the monitor bar. You can separate the monitor bar from the main SPM window to save desktop space.

**Figure 2-5: Monitor Bar**



The monitor bar uses the following icons:

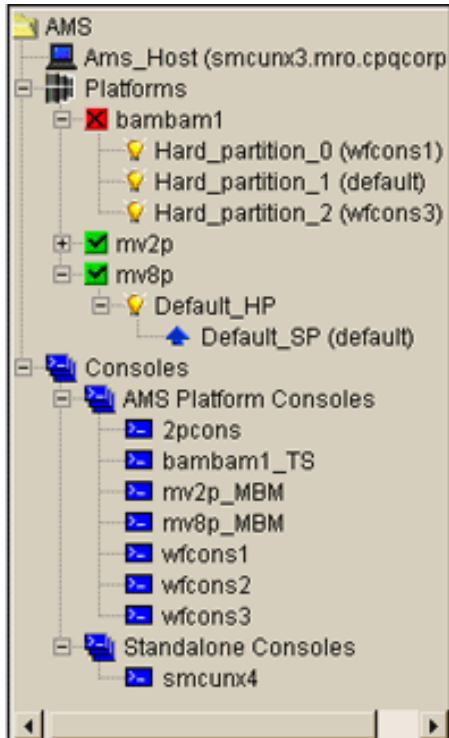
-  The number to the right of this icon indicates how many platforms are running without errors.
-  The number to the right of this icon indicates how many platforms have warning errors. These are not critical yet, but you may want to investigate them further.
-  The number to the right of this icon indicates how many platforms have critical errors calling for your immediate attention.

### 2.3.2 The Left Frame

The left frame (Figure 2-6) displays a tree structure in which you can view and interact with the platforms and consoles managed by the AMS.

- **Platforms Group**  
Displays a hierarchical list of all managed platforms, and their hard partitions and subpartitions. Icons next to each component display their status.
- **Console Group**  
Displays two types of consoles, AMS-managed consoles and standalone consoles:
  - **AMS-managed consoles**  
The consoles in this group are associated with the managed platforms. They consist of platform management consoles, which appear as soon as a platform is added and discovered, and SRM/operating system consoles, which must be configured before their display appears.
  - **Standalone consoles**  
The consoles in this group are any non-AMS-managed consoles that you want to configure, access, and monitor.

**Figure 2-6: Left Frame**



The left frame uses the following icons:



The platform is running without errors.



The platform has one or more warning errors. These are not critical yet, but you may want to investigate them further. For example, this icon displays when the SPM times out during platform discovery.



The platform has critical errors calling for your immediate attention.



The hard partition is powered on.



The hard partition is powered off.



The operating system, SRM console, or XSROM is running on the subpartition.



Nothing is running on the subpartition.



The component is in an unknown state. The SPM could be in the process of discovering this component.

You can perform actions on the components in the left frame. Different actions are available for different components. Select a component and then select the Actions menu to display the list of actions you can perform on that component. You can also press the right mouse button on a component to display a pop-up Actions menu.

See Section 2.5, Section 2.6, Section 2.8, and the online help for information about each of the menu items.

### 2.3.3 The Top Right Frame

The top right frame displays information about disk utilization for the AMS server, icons of the platforms or consoles, the default hard partitions, detailed information about the default subpartitions, and the status of a selected subpartition. Selecting

a component in the left frame displays the component, groups of components, or detailed information in the SPM top right frame.

You can display either the platforms connected to the AMS, the subpartitions configured on a platform, the consoles configured on a subpartition, or the console's status. For example, selecting Platforms in the left frame displays all of the platforms connected to the AMS in the top right frame.

When a branch of the tree in the left frame contains branches below it, you can view icons in the right frame or you can view details about that branch. You choose the view you want by using the View menu.

For example, Figure 2-7 displays the icon view for the AMS Platform Consoles; Figure 2-8 displays the details view.

**Figure 2-7: The Top Right Frame (Icon View)**



**Figure 2-8: The Top Right Frame (Details View)**

Name	Status	Console Port
2pcons	Open	323
bambam1_TS	Open	23
mv2p_MBM	Open	23
mv8p_MBM	Disabled	23
wfcons1	Refused	2001
wfcons2	Open	2002

If the branch in the left frame contains no branches below it, the right frame displays details about that branch. In this case, clicking on the View menu items has no effect on the display. Figure 2-9 shows the right frame display of a specific AMS platform console.

**Figure 2-9: The Top Right Frame (Specific Console View)**

Console Property	Value
Name	2pcons
Status	Open
Operating System Type	Unknown
Port	323
Mapped Port	1501
Logging	Enabled

When you display a platform and default hard partition in the top right frame, you can right-click on its icon to display its Actions menu.

You can customize the console status view by dragging the column headings in the order you want.

## 2.3.4 The Bottom Right Frame

The bottom right frame provides two tabs which you can toggle to view snapshots of hardware issues and recent events.

### 2.3.4.1 Hardware Status

The Hardware Status view displays all managed platform components that report a warning or error state. The information is provided by the AMU/APW services by requesting state information from a platform's firmware. The display is updated dynamically to always show the most recent status. Status information is never logged. Figure 1-2 shows the main SPM window with the Hardware Status tab output displayed.

The following is a summary of the hardware errors that will be displayed if they occur:

#### ES47, ES80, and GS1280 Platforms

- MBM microprocessor status error
- MBM power status warning if power is off
- MBM environmentals (warning or error for each fan, voltage, temperature)
- CMM microprocessor status error
- CMM power status warning if power is off
- EV7 microprocessor status error
- PBM microprocessor status error
- PBM power status warning, if power is off
- PBM environmentals (warning or error for each fan, voltage, temperature)
- PBM power supply status (warning, error for each power supply)

#### GS80, GS160, and GS320 Platforms

- One or more components are powered off: enter "show system" at the SCM prompt for details.
- One or more components have failed: enter "show system" at the SCM prompt for details.
- Some PCI Drawers are disconnected from the QBBs: enter "show system" at the SCM prompt for details.
- This platform is turned off at the OCP power switch.
- The temperature of one or more components is too hot: enter 'show "show system" at the SCM prompt for details.
- Soft partitions and memory size for hard partition 1 unavailable.
- Master SCM Port for this platform not found.
- A console is configured on a port outside the port range configured for this platform.
- There are multiple AlphaServer platforms on the terminal server.
- Two or more ports on the terminal server report different AlphaServer serial numbers.
- PCI Drawer *draw\_number* should be connected to the terminal server: it is a partition's console.
- A console command timeout on port *port\_number* has prevented discovery.

- Couldn't open consoles for this platform.

### 2.3.4.2 Recent Events

The Recent Events view displays the latest events reported to EVM by the console manager (CMFD) and the AlphaServer Management Utility (AMU). The AMU forwards ES47, ES80, GS1280 alerts to EVM and CMFD forwards events when text in console output matches a specified pattern in the console's event definition file. With this display you can easily identify problems that may need immediate attention. Figure 2-4 shows the main SPM window with the Recent Events tab output displayed.

When the SPM client starts, it retrieves from the EVM log up to 500 events that have occurred in the last 24 hours. Thereafter, the display is updated as new events occur. If the 500-event limit is reached, the oldest events are removed as new events are added.

The default setting for the table is to sort the events by date and time. To sort the display using another criteria, select the header of that column.

To view the full EVM log, which may contain additional information, you can open the EVM Viewer by selecting it in the Platforms tree node context menu.

The Recent Events display provides the following information:

- Severity

This column contains an icon that identifies the severity of the event. All ES47, ES80, GS1280 alerts that originate from the firmware have a severity that is assigned by the firmware, as described in the Firmware Alerts table. The severity for CMFD-generated events is determined by the priority number that defines the event in the event definition file. The following icons identify the different severity levels.



Unknown — Indicates an unknown state.



Informational — Provides information about the operating state of a component, partition, or software.



Warning — Alerts you to an error state that requires attention.



Error — Alerts you to an error state that requires immediate attention.

EVM priority numbers are mapped to a severity level by AMS as follows:

- 100-199 - unknown
- 200-299 - informational
- 300-499 - warning
- 500-700 - error

- Time

This column displays the date and time EVM received the event notification.

- Name

This column lists the name of the managed platform, console, or service from which the event originated.

- Description

This column provides a short description of the event.

## 2.3.5 Customizing the Main SPM Window

You can move the shaded bars on the SPM to customize the layout. For example, you can click and drag the shaded bars between frames to make the frames larger or smaller. You can also move the monitor bar within the application window or drag it outside of the application window to create a separate monitor bar.

You can customize the right frame display to display detailed properties for each selected tree node.

You can sort the columns of the hardware errors table and all the tables when in the Details view, or move them to a different position.

---

### Note

---

Window customizations are not persistent between different browser sessions.

---

See the SPM online help for more information.

## 2.4 Adding and Modifying a Platform

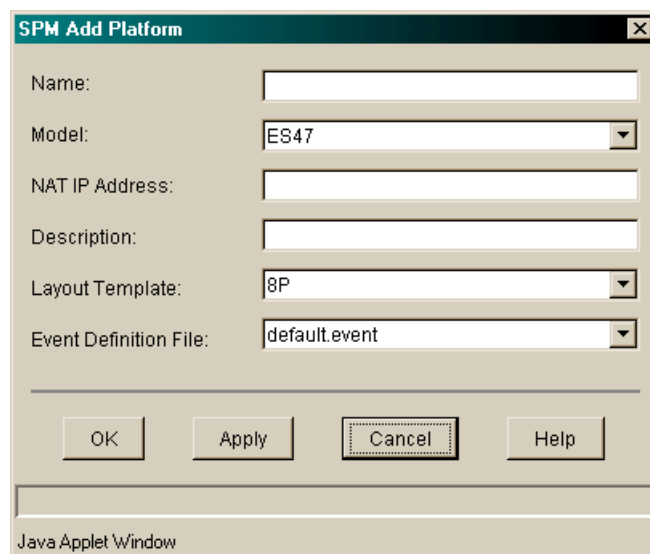
You can add a platform to the SPM by selecting Add Platform... from the Platforms context menu or from the Actions menu when you select Platforms. The process is the same for the ES47/ES80/GS1280 and GS80/GS160/GS320 platforms, with some differences in the information you provide to the Add Platform dialog box.

The same dialog boxes are displayed when you modify an existing platform. You modify a platform by selecting Modify... from the specified platform's context menu or from Actions menu when you highlight the specified platform.

### 2.4.1 Adding or Modifying an ES47, ES80, and GS1280

Figure 2-10 shows the Add Platform dialog box for ES47, ES80, and GS1280 platforms. A description of the fields follows.

**Figure 2-10: Add Platform Dialog Box (ES47, ES80, and GS1280)**



To add a platform or modify an existing one, you need the following information:

- Name of the platform  
A user-specified unique name given to the platform.

- **Model**  
The model number of the system being added. You select the model from a drop-down menu.
- **NAT IP Address**  
The IP address of the platform's NAT box.
- **Description**  
A user-supplied description to help in identify the platform.
- **Layout template**  
A graphical template used by the AlphaServer Management Utility (AMU). It determines how the AMU will graphically represent the cabinet layout and configuration of the system you are adding. The drop-down menu contains the model types. To modify or create a template file, select the AMU Visual Editor from the Configuration menu. (See Section 3.17.)
- **Event Definition File**  
A file to associate with the MBM console that contains event patterns. When console monitoring is enabled, `cmfd` generates an event when console output matches a pattern found in the event file. To modify or create an event definition file, select Create/Modify Event Definition File... from the Console context menu.  
  
The drop-down menu contains the text patterns for each type of console that may exist on a manager platform.

The platform appears in the left frame after you add it to the SPM. The SPM automatically obtains the platform's configuration information. If a platform's configuration is not returned, the SPM cannot access the platform at the specified address.

You can also modify a platform that is managed by the SPM by selecting Modify... from the Actions menu.

After the subpartition icons are displayed, you should configure each subpartition. Configuring the subpartition allows you to connect to its OS/SRM console port. See Section 2.6.1 for more information.

## 2.4.2 Adding or Modifying a GS80, GS160, and GS320

Figure 2-11 shows the Add Platform dialog box for GS80, GS160, and GS320 platforms. A description of the fields follows.

**Figure 2-11: Add Platform Dialog Box (GS80, GS160, and GS320)**

To add a platform or modify an existing one, you need the following information:



- **Name of the platform**  
A user-supplied unique name given to the platform.
- **Model**  
The model number of the system being added. You select the model from a drop-down menu.
- **Terminal Server IP Address**  
The IP address of the platform's terminal server.
- **Description**  
A user-supplied description to help identify the platform.
- **Terminal Server Port Range**  
A user-specified range of port numbers for the terminal server. The default setting is 2001 through 2008.

The platform appears in the left frame after you add it to the SPM. The SPM automatically obtains the platform's configuration information. If a platform's configuration is not returned, the SPM cannot access the platform at the specified address.

You can also modify a platform that is managed by the SPM by selecting **Modify...** from the **Actions** menu.

After the subpartition icons are displayed, you should configure each subpartition. Configuring the subpartition allows you to connect to its OS/SRM console port. See Section 2.6.1 for more information.

## 2.5 Managing Platforms

You can manage platforms with the SPM by:

- Connecting to the ES47, ES80, and GS1280 platform's management (MBM) port or the GS80, GS160, and GS320 platform's master system control manager (SCM)
- Monitoring a platform using a graphical representation of the platform's hardware
- Accessing the AlphaServer Management Utility (AMU) and the AlphaServer Partition Wizard (APW)
- Displaying a platform's properties, and removing a platform from the SPM

Selecting a platform's context menu or clicking on the **Actions** menu when a specific platform is highlighted displays a menu with the following items:

- **Open**  
Expands the platform tree for that platform to display all partitions.
- **Refresh**  
Causes SPM to rediscover the platform.
- **Modify...**  
Brings up the dialog box in which you added the specified platform. See Section 2.4.
- **Remove**  
Removes a platform and its associated consoles. See Section 2.5.6.
- **APW...**  
Invokes the AlphaServer Partition Wizard. See Section 2.5.4.

- AMU... (ES47, ES80, and GS1280 platforms only. )  
Invokes the AlphaServer Management Utility. See Section 2.5.3.
- Warnings and Errors ...  
Displays warnings and errors for the specified platform. See Section 2.3.4.1 for descriptions of the warnings and errors.
- Telnet to MBM ... (ES47, ES80, and GS1280 platforms only)  
Lets you make a Telnet connection with the backplane manager. See Section 2.8.1.
- Telnet to Terminal Server ... (GS80, GS160, and GS320 platforms only)  
Lets you make a Telnet connection with the Platform's terminal server. See Section 2.8.1.
- View Console Log ...  
Displays the console log for the selected platform. See Section 2.8.3.
- Enable Console  
Lets you enable or disable the console. See Section 2.8.4.
- Console Logging  
Lets you select one of the following actions:
  - Do Not Log or Monitor Output
  - Log Console Output
  - Log Console Output and Monitor Events
- Show/Disconnect Users...  
Lets you see who is connected to the MBM or terminal server console and to disconnect all users. See Section 2.8.2.
- Broadcast to Connected Users ...  
Lets you send a message to connected users. See Section 2.8.2.
- Properties ...  
Displays the properties of the selected platform. See Section 2.5.5.

## 2.5.1 Connecting to the Platform's Management Port

You can establish a connection to a platform's management LAN directly from the SPM by connecting to the platform's management port.

### 2.5.1.1 ES47, ES80, and GS1280 Platforms

The management LAN connects to the platform's management software, which is controlled by the backplane manager (MBM). You can view the status and error logs of the platform and manage the MBM using the command-line interface when you connect to the management port.

You access the management port through a Network Address Translator (NAT) box, which provides the platform with a unique IP address for the AMS and the hard partitions configured on the platform with a single point of access to the AMS.

The prompt of the management port is `MBM>`. See the *CLI Reference* manual on the Server Management CD-ROM.

For a list of commands you can perform at the `MBM>` prompt, enter **help**.

The MBM console output is logged to a file named `PlatformName_MBM.log` in the `/usr/opt/ams/logs/cmfd.dated` directory. By default, `cmfd` archives the

console logs every seven days. You can change the archive schedule by selecting the Console Logfile Archiving Period ... item from the Consoles context menu.

### 2.5.1.2 GS80, GS160, and GS320 Platforms

In GS80, GS160, and GS320 platforms, the interface to the firmware is the System Control Manager (SCM). SCM commands allow an administrator to perform tasks such as check detailed hardware status, view error registers, partition the platform, and power partitions on and off. To issue SCM control commands to the firmware you must connect to the Master SCM console.

The Master SCM is the console associated with the lowest port number of the configured terminal server's port range. The SCM runs in two modes, SCM mode and console mode:

- In SCM mode, the prompt in the console window is one of the following (in which *nn* is a number from E0 to EF):
  - `SCM_nn` if a console device is attached to the master CSB
  - `SLV_nn` if a console device is attached to a slave node
- In console mode the prompt in the console window is `P00>>>`.

In SPM, you can determine which partition console is the Master SCM by displaying the Properties dialog box of a GS80, GS160, and GS320 platform.

To access the Master SCM, invoke the Telnet application from the partition associated with the SCM port.

For a list of the available SCM commands type `help` at the SCM prompt. See the *AlphaServer GS80/160/320 Firmware Reference Manual* for additional information.

## 2.5.2 Partitions

The SPM's left frame displays each platform's hard partitions and subpartitions. One hard partition and one subpartition within that hard partition are configured by default on ES47, ES80, and GS1280 platforms.

Hard partitions physically divide computing resources into separate logical systems; in this case the resources are CPUs and their associated memory. You can consider the platform as a whole as one hard partition. Each partition is capable of running an operating system with its own set of applications.

A subpartition is configured on the hard partition by default to enable you to load and run an operating system on the platform.

You can create new partitions using the AlphaServer Partition Wizard (see Chapter 4) and the AlphaServer Management Utility (see Section 3.13) on how to partition a platform.

## 2.5.3 Accessing the AMU

You can access the AlphaServer Management Utility (AMU), a Web-based application with which you can monitor and manage ES47, ES80, and GS1280 platforms from the SPM. The AMU does not recognize GS80, GS160, and GS320 platforms.

With AMU you can:

- Display the hardware components of a platform
- Display detailed hardware properties
- Display the platform's environmental status

- Load firmware
- View firmware error logs
- Partition the platform
- Power on and power off partitions

The AMU window is divided into three frames:

- The left frame displays a tree view of the platform's processor units by cabinet location.
- The top right frame displays a graphical representation of the physical layout of the selected platform or the selected component of the platform.

For example, you can display a graphical representation of the platform's cabinets by clicking on Hardware in the left frame. You can move your mouse over the right frame to display information about each cabinet; for example, the number of processors, the system box it is running on, and the status.

- The bottom right frame displays either a timestamped list of activities that the AMU has performed or a listing of any alerts being sent by system firmware. You click on either the Activities tab or the Alerts tab to choose the list you want to see.

See Chapter 3 and the AMU's online help for more information.

## 2.5.4 Accessing the APW

The AlphaServer Partitioning Wizard (APW) provides an easy-to-use graphical interface for adding or removing partitions from a selected platform.

You can access the APW by selecting a platform and selecting APW from the drop-down menu or the Actions item of the main menu. You can use the APW to partition ES47/ES80/GS1280 and GS80/GS160/GS320 platforms.

For information about using the APW, see Chapter 4.

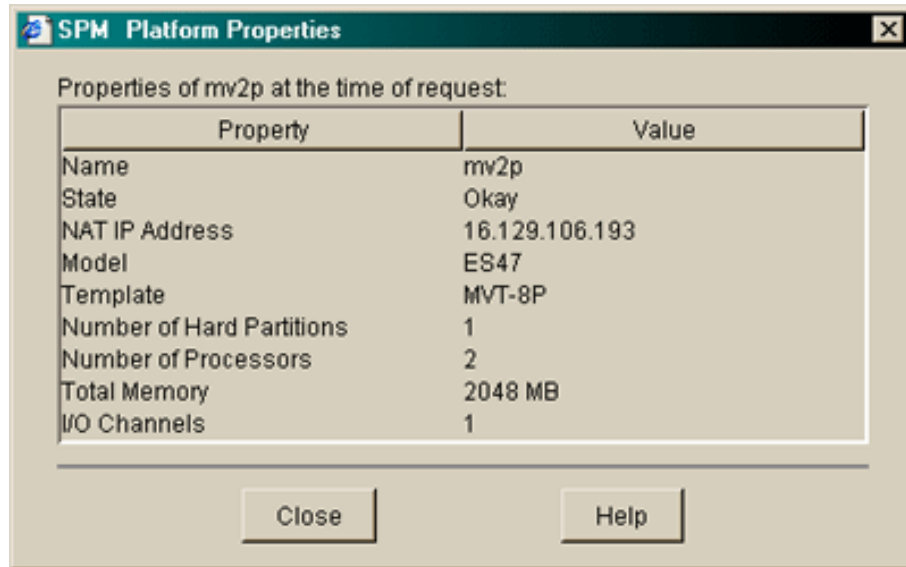
## 2.5.5 Viewing a Platform's Properties

You can view the properties of a selected platform or console using the Properties... item from the selected platform or console's context menu or from the Actions Menu.

### 2.5.5.1 ES47, ES80, and GS1280 Platform Properties

Figure 2-12 shows the Properties dialog box for an ES47, ES80, and GS1280 platform. A description of the fields in that box follows.

**Figure 2-12: Platform Properties Dialog Box (ES47, ES80, and GS1280)**

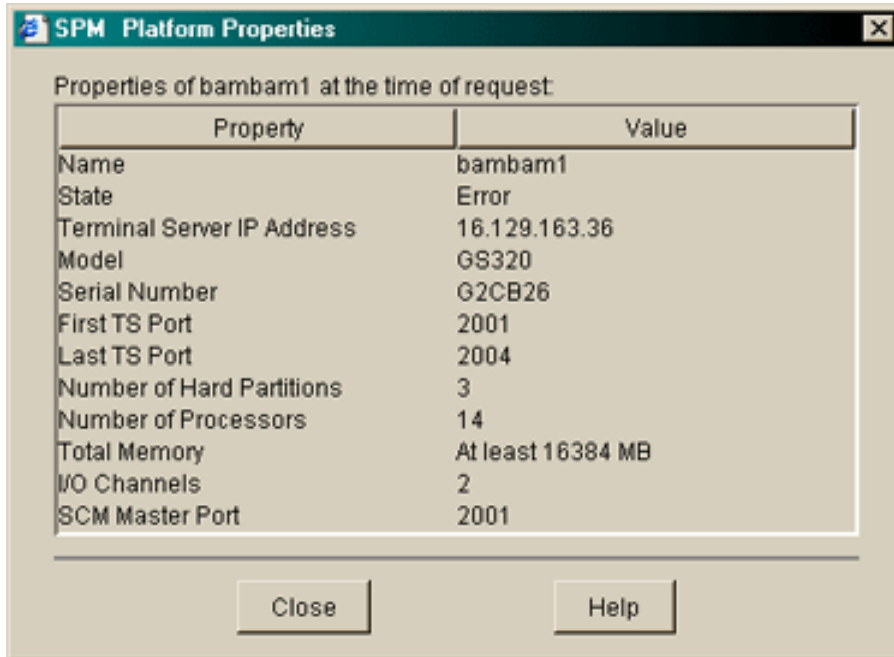


- **Name**  
The user-assigned name for the platform.
- **State**  
A one-word indication on the status of the platform, either Okay or Error.
- **NAT IP Address**  
The IP address for the platform's NAT box.
- **Model**  
The model number of the platform, for example ES47.
- **Template**  
The name of a file that contains the physical location of the hardware components in the cabinets. The template is used by the AMU for display of the graphical physical layout.
- **Number of Hard Partitions**  
All hard partitions are included, regardless of state.
- **Number of Processors**  
All processors that are present are included, regardless of state.
- **Total Memory**  
All reported memory along with units; for example, 7168 MB.
- **I/O Channels**  
All I/O channels are included. Disconnected I/O channels may not be included.

### 2.5.5.2 GS80, GS160, and GS320 Platform Properties

Figure 2-13 shows the Properties dialog box for a GS80, GS160, and GS320 platform. A description of the fields in that box follows.

**Figure 2-13: Platform Properties Dialog Box (GS80, GS160, and GS320)**

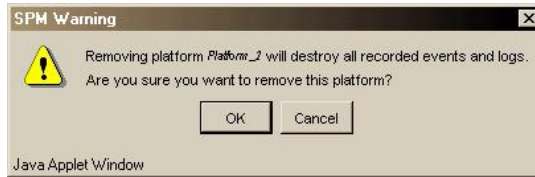


- **Name**  
The user-assigned name for the platform.
- **State**  
A one-word indication on the status of the platform, either Okay or Error.
- **Terminal Server IP Address**  
The IP address for the platform's terminal server.
- **Model**  
The model number of the platform, for example GS80.
- **First TS Port**  
The first port number in the port number range used for accessing the platform's hard partitions.
- **Last TS Port**  
The last port number in the port number range used for accessing the platform's hard partitions.
- **Number of Hard Partitions**  
All hard partitions are included, regardless of state.
- **Number of Processors**  
All processors that are present are included, regardless of state.
- **Total Memory**  
All reported memory along with units; for example, 7168 MB.
- **I/O Channels**  
All I/O channels that are connected with a CMM are included. Disconnected I/O channels may not be included.
- **SCM Master Port**  
The port number of the master SCM.

## 2.5.6 Removing a Platform

You can remove a platform and its associated consoles by selecting Remove from the selected platform's context menu or from the Actions item of the menu bar. You will be asked to confirm the removal (Figure 2-14) before the platform is removed.

**Figure 2-14: Remove Platform Confirmation Dialog Box**



## 2.6 Managing Partitions

ES47/ES80/GS1280 and GS80/GS160/GS320 platforms can be configured into one or more hard partitions that can contain one or more subpartitions. By default, ES47, ES80, and GS1280 platforms are configured with a default hard partition that contains a default subpartition. The subpartition allows an operating system to run on the platform. You can load an operating system onto a subpartition at its SRM prompt. See the *SRM Console Reference* on the Server Management CD-ROM for more details.

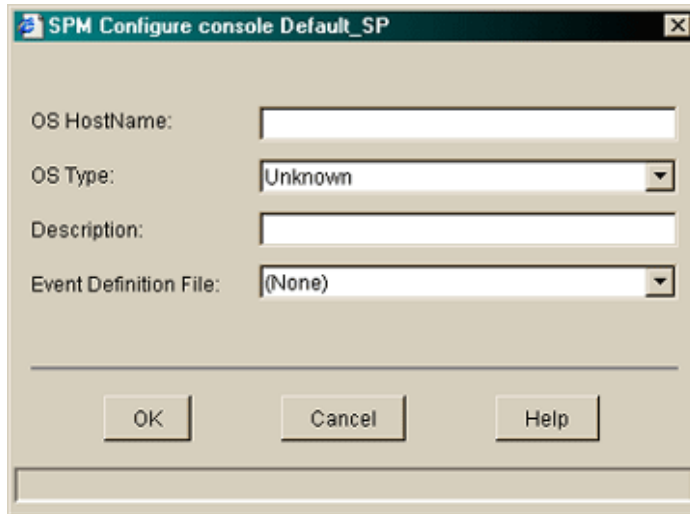
Use the SPM to do the following:

- Configure a console for a partition.
- Connect to a partition's console (See Section 2.8 for information about working with consoles).
- Access the HP Insight Management Agents running on an operating system.
- View a console's log.
- Turn console logging on or off.
- View users connected to a console.
- Broadcast a message to the users connected to the subpartition's console.
- Enable/disable `cmfd` on the subpartition's console.
- Disconnect users connected to the console.
- Enable or disable events generated from console output.
- Use the Event Viewer.
- View subpartition properties.

### 2.6.1 Configuring a Subpartition

You configure a subpartition to be managed by SPM using the Configure dialog box (Figure 2-15). Configuring a subpartition allows you to connect to the subpartition's console.

**Figure 2-15: Configure Subpartition Dialog Box**



To configure the console, you must enter the following information:

- **OS HostName**  
The host name of the operating system running on the platform.

---

**Note**

---

You must use the exact host name of the operating system to enable access to the Insight Management Agents.

---

- **OS Type**  
The type of the operating system running on the subpartition. A drop-down box allows you to select one of the following:
  - Tru64 UNIX
  - OpenVMS
  - OpenVMS Galaxy
  - Linux
  - Unknown
- **Description**  
User-supplied comment, such as “Console for default subpartition.”
- **Event Definition File**  
A file containing event patterns to associate with an operating system/SRM console. By default, this field contains the `default.event` file. A drop-down list provides the available files or lets you select none.  
  
When console monitoring is enabled, `cmfd` generates an event when console output matches a pattern found in the event file. To modify or create an event definition file, select `Create/Modify Event Definition File...` from the Console context menu.

## 2.6.2 Accessing the HP Insight Management Agents

You can use the SPM to access the HP Insight Management Agents running on the Tru64 UNIX or OpenVMS operating system of a selected subpartition.



## Note

To access the Insight Management Agents, the subpartition must be running the operating system.

You cannot access the Insight Management Agents from a subpartition running a Linux environment.

**Figure 2-16: Insight Management Agents**



Figure 2-16 shows the Insight Management Agents Device Home Page.

The Insight Management Agents allow you to look across a heterogeneous computing services environment and access information through a Web browser about any entity connected to the network. The Insight Management Agents can be run on partitions running Tru64 UNIX or on OpenVMS servers. You can view your hardware configuration and monitor the state of the system.

Using the Insight Management Agents for Tru64 UNIX, you can view your AlphaServer hardware configuration and monitor the state of the system. You can access the Tru64 UNIX System Management Home Page, SysMan Menu, SysMan Station, and the Sys\_Check Configuration reports from any browser.

See <http://h30097.www3.hp.com/cma> for documentation of Insight Management Agents for Tru64 UNIX and [http://h71000.www7.hp.com/open-vms/products/mgmt\\_agents/](http://h71000.www7.hp.com/open-vms/products/mgmt_agents/) for documentation of Insight Management Agents for OpenVMS.

### 2.6.3 Enabling and Disabling Events Generated from Console Output

You can enable or disable events generated from console output from the Console Logging submenu of the selected subpartition's Actions menu.

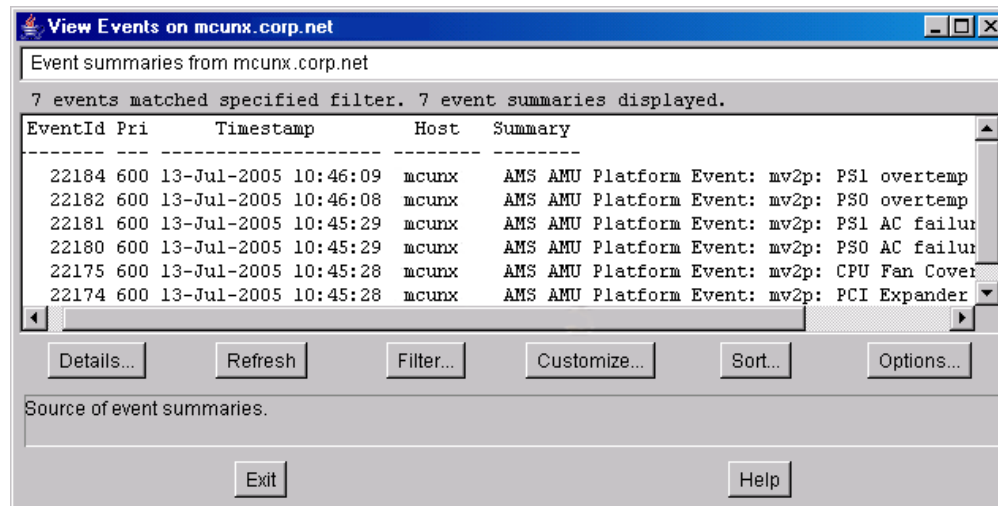
By default, events are generated for each platform management console and OS console connection defined. Messages that are normally echoed to the consoles are parsed; if a match between the output and any entry in the specified event definition file is found an event with the indicated priority is generated.

Be aware, however, that event generation for a given port is disabled when a user is connected to that port.

## 2.6.4 Using the Event Viewer

You can view events that have been generated from operating system console output, from AlphaServer ES47, ES80, and GS1280 alerts, or from AMS components in the Event Viewer. In the main SPM window, open the Event Viewer (Figure 2-17) from the Actions menu of the AMS.

Figure 2-17: View Events Dialog Box



You must choose to log console output and monitor events from the Console Logging option in a subpartition's Actions menu in order to view its events in the Event Viewer. ES47, ES80, and GS1280 alerts are always forwarded to the Event Manager (EVM). Although the Event Viewer does not dynamically display new events, you can update the display using the viewer's Refresh button.

The Event Viewer is part of the Event Manager system. EVM is a comprehensive event management system that, in addition to providing traditional event handling facilities, unifies events from many channels, such as a log file, to provide a systemwide source of information.

An EVM event is a package of information that can be passed among programs and stored in files. You can receive events from either the AMS components or from the operating system running on a subpartition. See the EVM chapters in the *Tru64 UNIX System Administration* guide and *Programmer's Guide* for more information.

Examples of events you can receive from the AMS components include the following:

- ES47, ES80, and GS1280 firmware-generated alerts
- Console output that matches a pattern found in the event definition file associated with the console
- AMS events generated by the `cmfd` daemon

Examples of events you can receive from the operating system include the following:

- AdvFS domain panic
- Hardware connections reduced
- Fan sensor is above the critical threshold
- Power sensor is above the critical threshold
- Hardware state change

You can view events generated by AMS components by selecting the AMS icon with the right mouse button in the SPM's left frame and selecting View Events.

EVM can notify a user via e-mail or a pager about events it receives. EVM sends e-mail messages of events with a priority of 700 or higher to the root user of the AMS, by default. You can configure EVM to let you specify a priority and the name of a user you want notified.

See Appendix D for information about using Event Manager and Appendix E for information about how to send selected events via e-mail.

## 2.6.5 Viewing ES47, ES80, and GS1280 Subpartition Properties

You can view the properties of ES47, ES80, and GS1280 subpartitions configured on the SPM.

**Figure 2-18: Subpartition Properties Dialog Box**

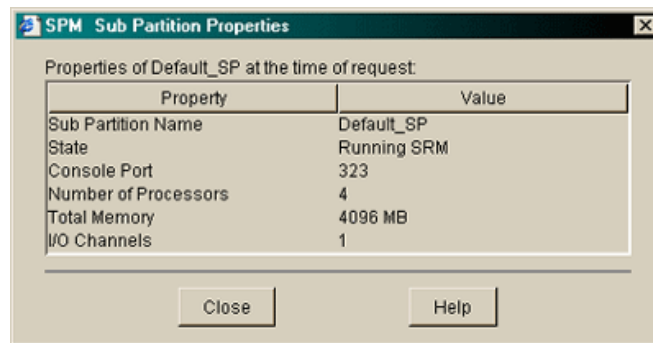


Figure 2-18 shows the SPM's Subpartition Properties dialog box. A description of the fields in this box follows:

- **Sub Partition Name**  
The default or user-assigned name for the partition.
- **State**  
The present status of the system.
- **Console Port**  
The console port number.
- **Number of Processors**  
All processors that are present are included, regardless of state.
- **Total Memory**  
All reported memory along with units; for example, 7168 MB.
- **I/O Channels**  
All I/O channels that are connected with some CMM are included; disconnected I/O channels may not be included.

## 2.7 Adding a Standalone Console

SPM lets you add standalone consoles (also called generic consoles) to the Consoles tree. By doing this, you can access non-AMS consoles through the SPM.

To do this, select the Add Standalone Console ... menu item from the Standalone Console's context menu or from the Actions menu when the Standalone Consoles listing is highlighted. This displays the Add Standalone Console dialog box, in which you provide a name for the console, its IP address and port number, a description, and an event definition file to be identified with this console.

After you have created a standalone console, its context menu is the same as that for AMS platform consoles (see Section 2.8), with the addition of the following items:

- **Modify ...**  
Lets you modify the information you entered when you added the console.
- **Remove**  
Lets you remove the console from the Consoles tree.

## 2.8 Working with Consoles

MBM, master SCM, and SRM/OS consoles are available from their platform and partition and from the Consoles tree node. Standalone consoles are available only from the Consoles tree. From a console's menu you can perform the following tasks:

- Telnet to the consoles (Section 2.8.1)
- Identify, contact, and disconnect other users (Section 2.8.2)
- Control console logging (Section 2.8.3)
- Enable or disable a console (Section 2.8.4)
- View console properties (Section 2.8.6)
- Map console ports for external Telnet access (Section 2.8.5)

### 2.8.1 Telnet Access to Consoles

You can connect to a management or SRM/OS port or subpartition's port using Telnet in one of the following access modes:

- **Read-only mode**  
Allows you to see console output, but not to send input to it.
- **Shared mode**  
Allows you to see console output and send input to it. The input and output of connections is shown in all open console windows.
- **Exclusive mode**  
Allows you to take complete control of the console, preventing other users to connect using share or exclusive modes. Read-only connections are allowed.

To create a Telnet session to an ES47, ES80, and GS1280 backplane manager, select the Telnet to MBM item from the Action menu or context menu of a selected platform or console MBM. To create a Telnet session to a console, select the Telnet to Console item from the Action menu or context menu of the selected platform.

To create a Telnet session to a GS80, GS160, and GS320 terminal server, select the Telnet to Terminal Server ... item from the Action menu or context menu of a selected platform.

To create a Telnet session to a console, select the Telnet to Console item from the Action menu or context menu of the selected console.

### 2.8.2 Identifying, Contacting, and Disconnecting Other Users

The SPM allows you to identify the users connected to the console, broadcast messages to them, and disconnect them from the console.

#### 2.8.2.1 Displaying and Users

You can see which users are connected to AMS-managed consoles and disconnect them from those consoles.

- Selecting Show/Disconnect Users... from a selected console's context menu or the Action menu provides a list of users connected to that console and lets you disconnect them from that console.
- Selecting Show/Disconnect to All Consoles from the Consoles group context menu or the Action menu provides a list of the users connected to all consoles and lets you disconnect them from those consoles.

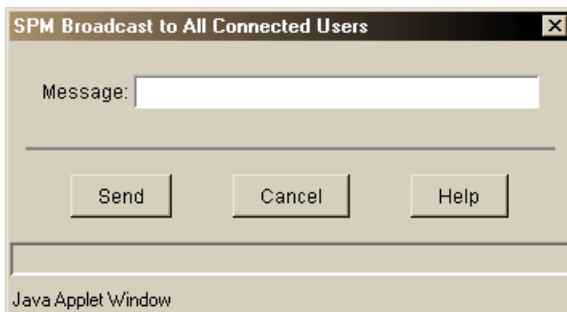
The user names, IP addresses, and connection modes of the connected users are displayed. This feature gives you the means to resolve problems you may have accessing a console that is managed by the AMS.

The user names of users who are connected using a different console manager cannot be displayed.

### 2.8.2.2 Broadcasting a Message

You can send a message to the users connected to a specific console or all consoles managed by AMS.

**Figure 2-19: Broadcast to All Users Dialog Box**



- Selecting the Broadcast to Connected Users... item from a selected console's context menu or the Action menu lets you send a message to the users connected to that console (Figure 2-19).
- Selecting the Show Users Connected to All Consoles item from the Consoles group context menu or the Action menu lets you to send a message to all connected users.

Users who are connected using a different console manager will not receive the broadcast messages.

### 2.8.3 Console Logging

You can turn console logging on or off by selecting Console Logging from the context menu of the selected subpartition or console listing or from the Action menu. From this menu, you can chose one of the following items:

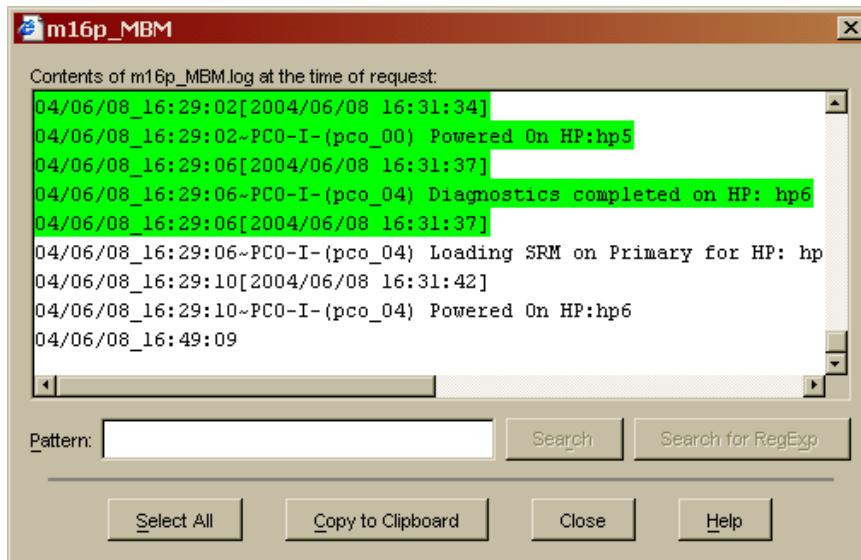
- Do not log or monitor output.  
When you turn console logging off, you cannot monitor events generated from the console.
- Log console output.
- Log console output and monitor events.

You can view a console's log by selecting View Console Log... from the context menu of the selected subpartition or console or from the Action menu.

The View Console Log... window provides a search facility and lets you copy all or selected information to the clipboard to paste it into a text file or another application.

Figure 2-20 shows a View Console Log... window with text selected for copying to the clipboard.

**Figure 2-20: View Console Log... Window**



## 2.8.4 Enabling and Disabling a Console

When a console is enabled, console connections using another console manager cannot be established. To allow another console manager to access a console, you should disable the console.

The `cmfd` establishes connections to all enabled consoles; all consoles are enabled by default.

If you need to disable the `cmfd` connection in order to connect to a console using another console manager, you can do so by selecting Enable Console item from the console's drop-down menu. A checkmark in front of the Enable Console item indicates that the console is enabled. You can also see if a console is enabled by viewing its properties, in which an enabled console has a value of True.

## 2.8.5 Port Mapping

The SPM's port mapping feature lets you configure a console or platform management port to be accessible by other console managers via `cmfd`.

You access this feature from the context menu of the Consoles tree item or from the Actions menu when Consoles is highlighted. Selecting the Map Console Ports for External Access item opens a window (Figure 2-21), which lists the identified consoles, their IP Addresses, and their port numbers.

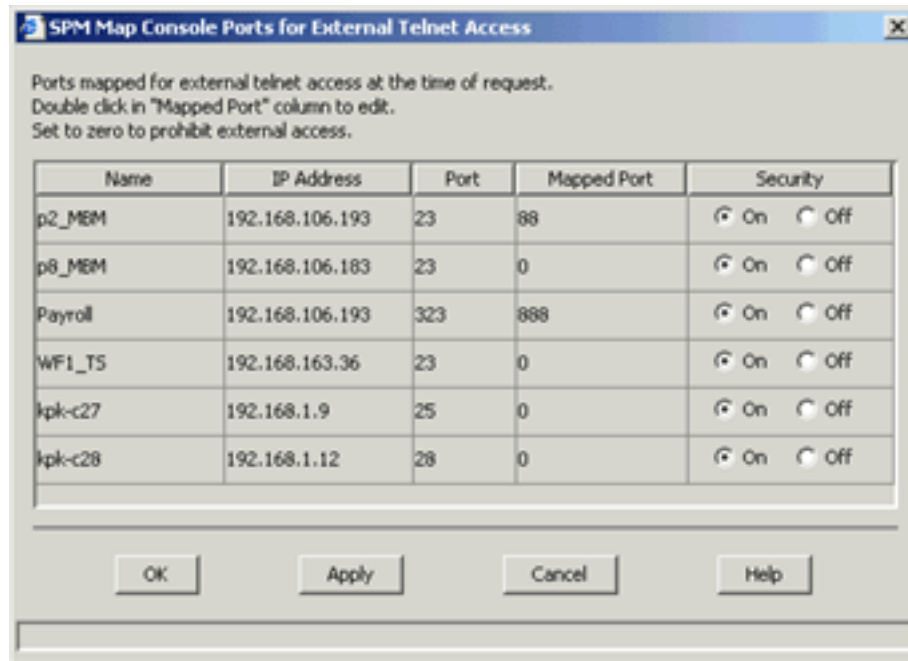
In this dialog box you can specify a port number to be mapped to the actual port. For example, if you map port 323 to port 1501, a user on a remote machine could access the console at port 323 by issuing a command like the following:

```
telnet ams.hostname.customer 1501
```

After entering a user name and password at the prompts, the user will be connected to console corresponding to port 323.

The dialog box also lets you enable or disable security. By enabling security, you require authentication for the clients that connect to this port.

**Figure 2-21: Port Mapping Dialog Box**

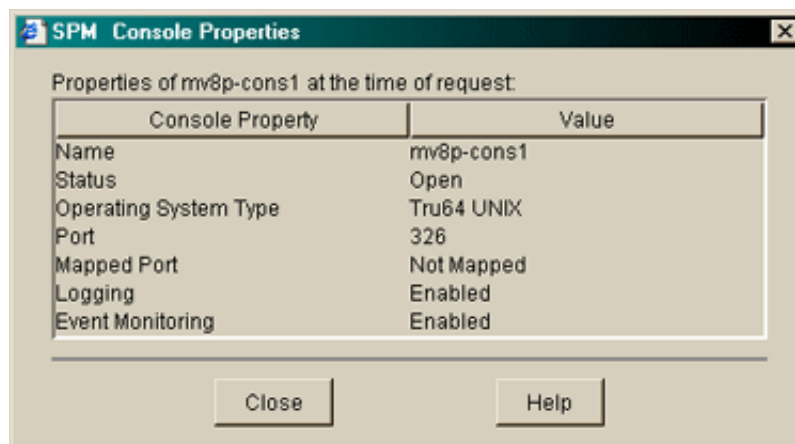


## 2.8.6 Viewing a Console's Properties

You bring up the Console Properties window of a selected console by selecting the Properties... item from the console's context menu or from the Actions Menu. You can also click on the console to view its properties in the right frame.

The properties that are displayed vary according to the type of console you select. For example, the properties for a standalone console include the console's IP address and the properties for a console for a GS80, GS160, and GS320 platform may include the property for a Master SCM. Figure 2-22 shows a console for an ES47, ES80, and GS1280 platform.

**Figure 2-22: Console Properties Box**



The following list describes the console properties you may see.

- Name  
The user-assigned name for the platform.
- IP Address  
The IP address for a standalone console.

- Status
 

The console connect status:

  - Open if a connection has been established to a console and is available to be used for a login session.
  - Busy if a connection has been established and is being used by a user in a login session.
  - Unknown if `cmfd` is stopped or unresponsive.
  - Refused if a connection cannot be made; for example, another application is using the console connection or a terminal is connected directly to the console.
- Operating System Type
 

The operating system running on the platform.
- Port
 

The port number used to open a Telnet connection to the console.
- Mapped Port
 

A user-specified port number that maps to the actual port number.
- Logging
 

Whether the logging of console output is Enabled or Disabled.
- Event Monitoring
 

Whether event monitoring is Enabled or Disabled.
- Master SCM
 

Whether a master SCM is present on the specified GS80, GS160, and GS320 console.

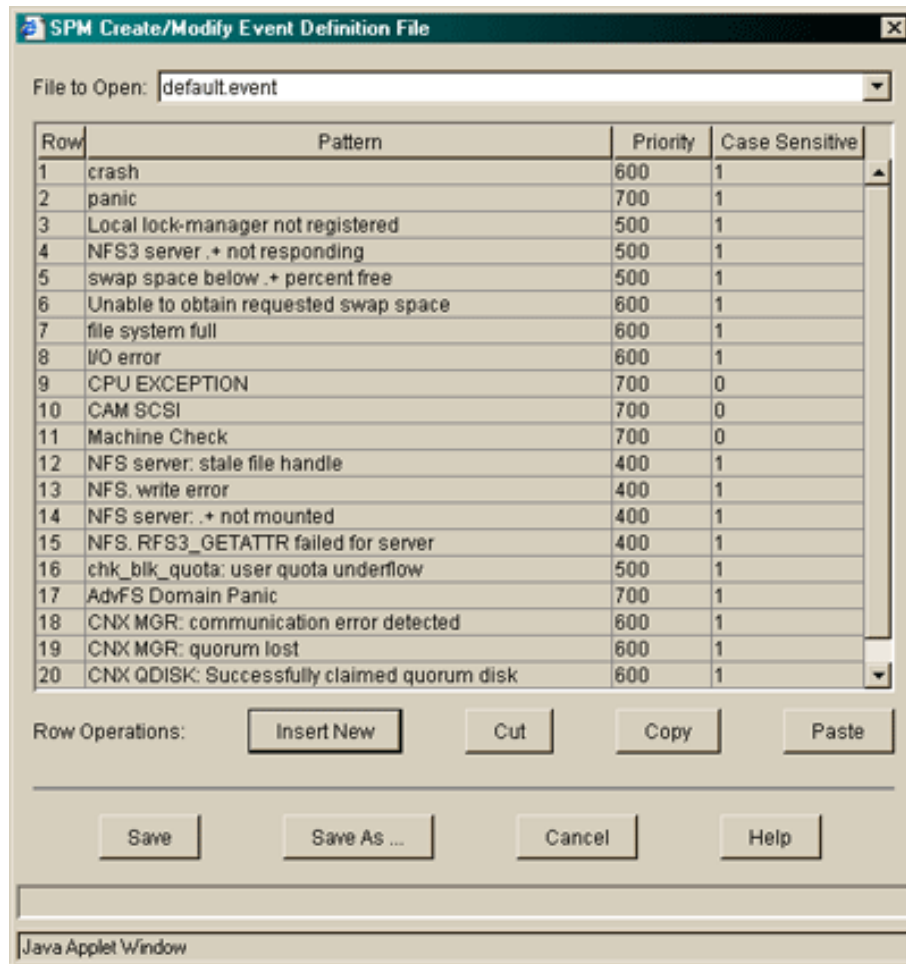
### 2.8.7 Creating and Modifying an Event Definition File

You can create a new event definition file from scratch or by using an existing event definition file as a template. You can also modify an existing file.

You access this feature from the context menu of the Consoles tree item or from the Actions menu when Consoles is highlighted. Selecting the Create/Modify Event Definition File... item opens the Create/Modify Event Definition File window.



Figure 2-23: Create/Modify Event Definition File Dialog Box



When you first open the window, the File to Open field has an entry for a new file. A drop-down menu lets you select one of the existing event definition files. You can, for example, select the `default.event` file, change its patterns and do one of the following:

- Save it with the same name (Save) to modify it.
- Save it with a new name (Save As...) to create a new file.

The text field contains three columns, Patterns, Priority, and Case Sensitive. To add or modify text in each field, click on the field, delete the existing text, and type the new text. In the Case Sensitive column, put a 1 (one) if you want the pattern to be case sensitive, or 0 (zero) if you do not want the pattern to be case sensitive.

The buttons in Row operations fields do the following:

- Insert New  
Adds a new row each time it is pressed.
- Cut  
Deletes a row when any column in that row is selected. To paste the deleted text, click anywhere on the row above where you want the text placed and press Paste.
- Copy  
Copies a row when any column in that row is selected. To paste the deleted text, click anywhere on the row above where you want the text placed and press Paste.

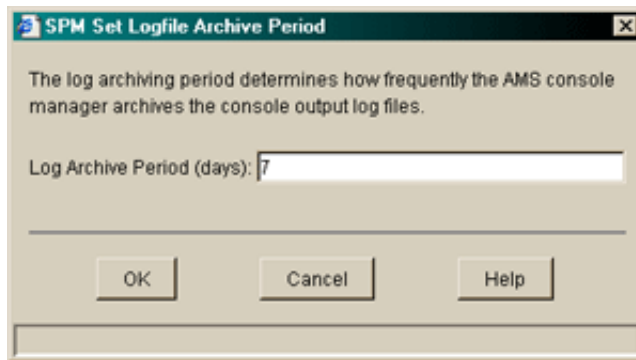
- Paste  
Pastes a copied or deleted row.

## 2.8.8 Setting the Archive Period for Log Files

By default, SPM logs console output for seven days and then archives the file. Using the Console Logfile Archive Period menu item, you can specify the number of days before log files are archived.

You access this feature from the context menu of the Consoles tree item or from the Actions menu when Consoles is highlighted. Selecting Console Logfile Archive Period ... brings up the Set Logfile Archive Period dialog box (Figure 2-24).

**Figure 2-24: Set Log File Archive Period Dialog Box**



You view current console log files by selecting View Console Logs ... from the context menu of a selected platform in the Platforms tree. After a file is archived, you can view them from within a terminal window in the `/usr/opt/ams/logs` directory.

---

## Using the AlphaServer Management Utility

This chapter describes the different tasks you can accomplish using the AlphaServer Management Utility (AMU). Section 3.1 provides a brief overview of the program, after which, the following topics are discussed:

- How to access the AMU as a standalone program or from the SPM and select a platform template (Section 3.2)
- The components of the main AMU window (Section 3.3)
- Viewing a graphical representation of I/O and power connections (Section 3.4)
- Monitoring the platform's environmental status (Section 3.5)
- Connecting to the console of a configured subpartition (Section 3.6)
- Connecting to the platform's management port (Section 3.7)
- Taking exclusive control of the AMU (Section 3.8)
- Viewing log files (Section 3.9)
- Using CDL file support (Section 3.10)
- Working with firmware (Section 3.11)
- Working with partitions (Section 3.12)
- Creating and modify partitions (Section 3.13)
- Reconfiguring cable connections (Section 3.14)
- Testing cable LEDs (Section 3.15)
- Viewing details about system drawers (Section 3.16)
- Creating templates with the AMU Visual Editor (Section 3.17)

### 3.1 Overview

The AlphaServer Management Utility (AMU) is a client-server based application. The server runs on the AMS machine and the client is a Web-based graphical user interface. Use the client to remotely monitor the status of platforms connected to the AMS and the partitions configured on the platforms.

Using the AMU, you can monitor the platform's environmental status, I/O connections, and power connections. You can also connect to the management port of ES47, ES80, and GS1280 platforms, load and boot operating systems by connecting to the console of a configured subpartition, view hardware error logs, and create, modify and configure partitions.

The AMU's online help provides step-by-step information about tasks you can perform with the AMU. To view the AMU online help, select Help in the menu bar and then select Contents.

### 3.2 Accessing and Configuring AMU

You can access the AMU in two ways:

- As a standalone application (Section 3.2.1)

If you installed the AMU kit, you can access it directly.

- From the SPM (Section 3.2.2)  
If you installed the AMS kit, you can access AMU through the Server Platform Manager running on AMS.

### 3.2.1 Running AMU as a Standalone Application

You can install and run AMU as a standalone application on computers running Tru64 UNIX, Linux, OpenVMS, or Windows Operating Systems. The following steps describe the steps you need to perform after you have installed the AMU kit

1. Start the Tomcat Server by entering one of the following commands:

- For Tru64 UNIX:

```
# /sbin/init.d/amutomcat start
```

- For Linux:

```
# /etc/init.d/amutomcat start
```

- For OVMS:

```
$ @sys$startup:apache$jakarta_startup
```

- For Windows:

Tomcat is started by the installation procedure. If you need to restart Tomcat, Select Start->Programs->AMU->Start Tomcat

2. Configure the Java plug-in if you use a Tru64 or Linux machine to access the AMU client:

- On Tru64 UNIX clients, set the environment variable as follows:

```
# NPX_PLUGIN_PATH=/usr/opt/java131/jre/plugin/alpha/ns4
# export NPX_PLUGIN_PATH
```

- On Linux clients, set the environment variable as follows:

```
# ln -s /usr/java/jre1.3.08/plugin/i386/libjavaplugin_obj.so \
/usr/lib/mozilla/plugins
```

Note that this example sets the environmental variable for the ksh shell. The shell you use may have a different syntax. The reference page for your shell provides information about setting environmental variables.

- On Windows clients the Internet Explorer installs the plug-in if it is not installed.

3. Access AMU

To access AMU locally or remotely, specify a URL in the following form:

```
http://amu_server_name:8080/mpmu
```

Before the AMU is displayed, you will see the Java Plug-in Security Warning. Selecting Grant this session or Grant always allows AMU to run. (See Section 2.2.3 for information about the security certificate.)

The first time AMU is launched, you will see a message that says “There are currently no configured platforms. Open the Visual Editor to add your configuration”.

4. Use the AMU Visual Editor to configure ES47/ES80/GS1280 platforms to be managed by AMU:
  - a. Select Open Visual Editor from the File Menu.
  - b. Configure the platforms you want to manage, as described in Section 3.17.
  - c. After the configurations are created and saved, the next time you open AMU it will contain a list of the platforms you have configured.
  - d. Select the platform you want to view.

## 3.2.2 Running AMU from SPM

To access AMU from SPM, you must first configure your ES47, ES80, or GS1280 platforms. See Section 2.4.2 for information about adding a platform.

After the platforms you added have been successfully discovered, you can launch AMU by selecting AMU... from the platform's context menu.

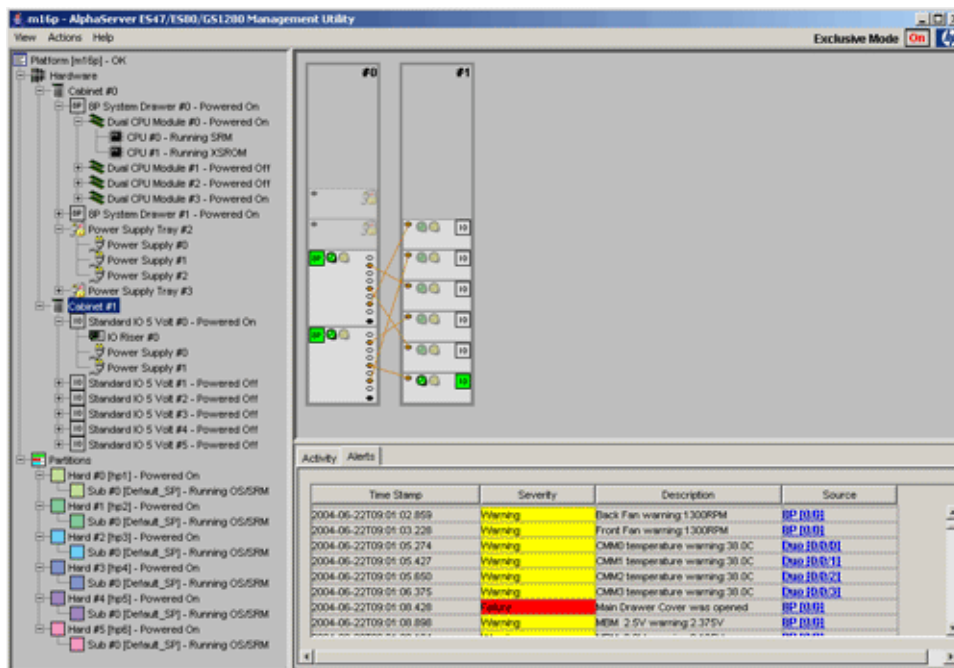
## 3.3 The Main AMU Window

The main AMU window (Figure 3-1) is composed of three frames:

- The left frame displays a tree view of the ES47, ES80, and GS1280 platform managed by the AMU and the components attached to the platform, its IP and I/O information, configured hard partitions, and configured subpartitions.
- The top right frame displays information according to what you select in the left frame; for example, a graphical representation of a selected system.
- The bottom right frame provides two tabs that allow you to view AMU activities and firmware alerts.

The following sections describe the content of these frames.

Figure 3-1: Main AMU Window



### 3.3.1 The Left Frame

Select icons in the left frame of the AMU window to display in the top right frame the physical view of the platform's cabinets and their hardware contents, including IP cable and connection information, I/O cable information, and configured hard partitions and subpartitions. You can also determine the power status of the system drawers and the hard partitions and subpartitions in the left frame.

You can view properties in the top right frame or perform actions depending on the component icon you select in the left frame.

Selecting each icon with the left mouse button displays in the right frame the following information:

- The platform managed by the AMU.

Displays the platform's properties when you select this icon, or right-click on the icon and select Properties from the pop-up menu.

- Hardware

Displays a graphical representation of the platform.

- Cabinet

Highlights the selected cabinets and all I/O and power supply connections to the system drawers and CPUs. When you view a system drawer in zoom mode, you can select the Cabinets icon to zoom out again to view the entire cabinet.

- System Drawers

Highlights the location of a particular system drawer in the hardware view. The power state of the system drawer is displayed next to the number of the drawer. You can view the drawer's properties by pausing the mouse pointer over this icon, or by right-clicking on the icon and selecting Properties from the pop-up menu.

- Dual CPU modules

Shows connection lines if a CPU in the module is connected to an I/O or power supply drawer. The power state of the modules are displayed next to the module's number. You can view the module's properties by pausing the mouse pointer over this icon, or by right-clicking on the icon and selecting Properties from the pop-up menu.

- Power Supply Tray

Highlights its location in the hardware view and shows the power supply connections to CPUs.

- Standard I/O

Highlights the PCI drawer and shows the I/O connection to the CPUs.

- I/O Riser

Displays its configuration information in the right frame.

- I/O Power Supply

Displays the I/O power supply connections in the hardware view.

- Partitions

Displays in the right frame a graphical representation of how the CPUs are partitioned.

- Hard partition

Highlights all the CPUs that belong to the specified partition's subpartitions.

- Subpartition

Highlights the CPUs that belong to the subpartition.

### 3.3.2 The Top Right Frame

The top right frame displays information that depends on what you select in the left frame. For example, you can display a graphical representation of the system by selecting Hardware from the left frame. You can display a graphical representation of how the platform is partitioned by selecting Partitions. You also can display the platform's log files, and IP cable connections, and such.

#### 3.3.2.1 The Hardware View

The hardware view (seen in Figure 3-1) is displayed when you select the Hardware tree node in the left frame. This view displays a graphical representation of a

platform, complete with system, I/O, and power supply drawers. The system lights display a real time status of the components.

You can monitor the power status of a system drawer using the status lights for each drawer. Pause the mouse pointer over a component to display its properties. For example, the system drawer displays the number of processors, the system box it is running on, and its status.

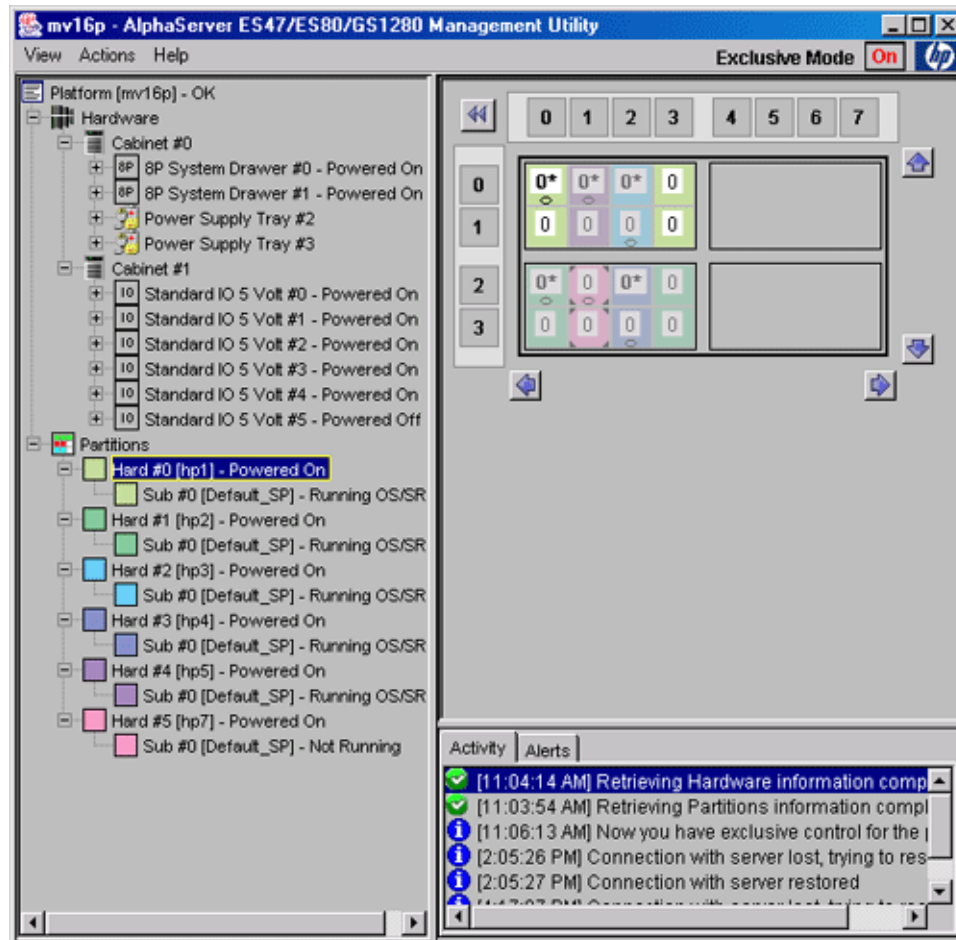
A green light indicates the system drawer is powered on and a yellow light indicates the system drawer is in an abnormal state. If the graphic of the drawer is grayed-out, then it indicates that the drawer is powered off.

You can determine why a system drawer is in an abnormal state by displaying its properties. To display its properties, pause the mouse pointer over the graphic of the system drawer in the hardware view. You can also select the system drawer's icon in the left frame with the right mouse button and then select Properties.

### 3.3.2.2 The Logical View

The logical view (also known as the partitions view) provides a logical representation of the system drawers and the CPUs they contain. Figure 3-2 shows the main AMU window with the logical view displayed.

Figure 3-2: Right Frame with Logical View

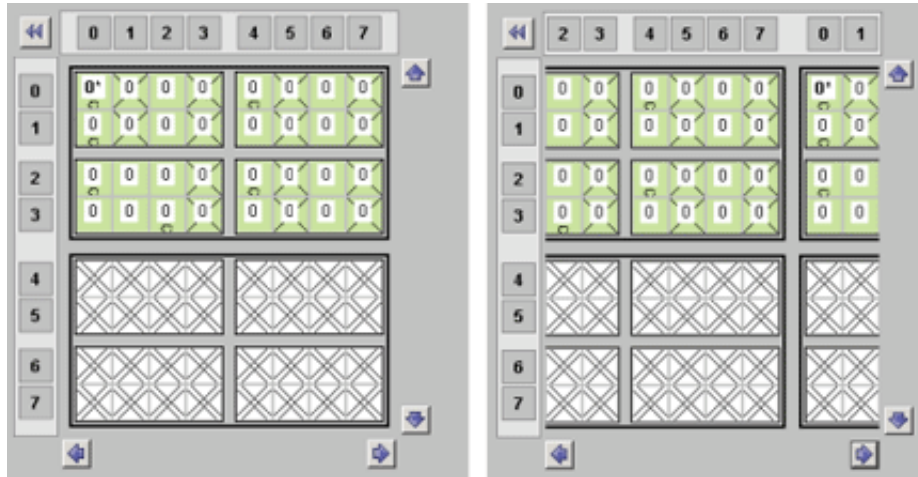


By clicking on the arrows in the display, you rotate the axis and CPUs in a circular fashion simulating the toroidal mesh of ES47, ES80, and GS1280 systems. The logical view uses colors and symbols to show the partitions, the subpartitions they contain, the type of CPUs and the CPUs that are connected to I/Os. Check

the Legend (see Section 3.3.2.3) for a full description of the symbols used in the logical view.

The left-hand side of Figure 3-3 shows the logical view of a four-drawer system that contains 32 CPUs. The x, y axis shown on the top and left of the display highlights a CPU's coordinates when the CPU is selected. The right-hand side shows the same view rotated clockwise.

**Figure 3-3: Logical View**



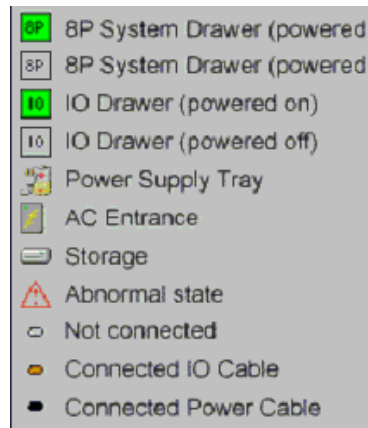
CPUs can be assigned to hard partitions and subpartitions only by selecting them in the logical view. See Section 3.12 for information about adding CPUs to a partition.

You select CPUs by clicking the left mouse button on a CPU square. To select multiple CPUs, select one and move the mouse pointer to consecutive CPUs without releasing the button. Release the button when you have finished selecting.

### 3.3.2.3 Displaying an Icon Legend

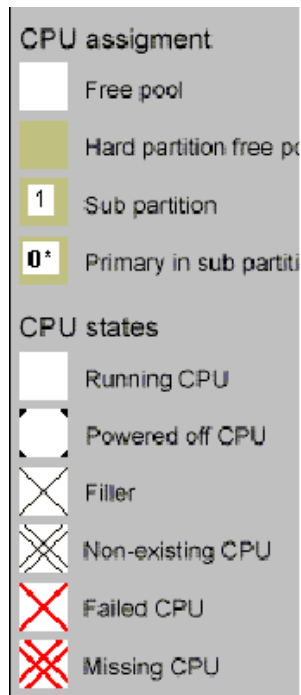
You can display an icon legend in either the hardware view (Figure 3-4) or the partitions view (Figure 3-5) by selecting Legend from the View Menu.

**Figure 3-4: Hardware View Icon Legend**





**Figure 3-5: Partition View Icon Legend**



### 3.3.3 Bottom Right Frame

The bottom right frame displays either a timestamped list of activities that the AMU has performed or a listing of any alerts being sent by system firmware. You click on either the Activities tab or the Alerts tab to choose the list you want to see.

#### 3.3.3.1 Activity Tab

Selecting the Activity tab (see Figure 3-2) displays an ongoing list of AMU activities and the times they occur. For example, a list item might specify the time that the AMU started to retrieve information about hardware, while another list item specifies the time that the task was completed.

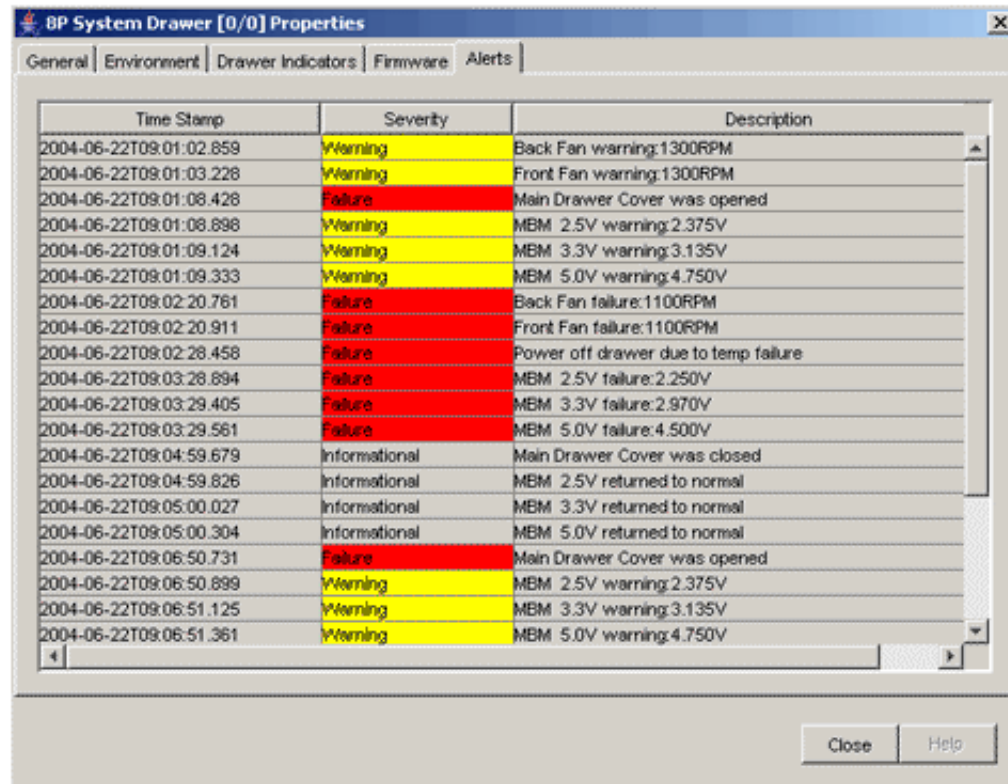
The Activity tab is the default display when you open the AMU.

#### 3.3.3.2 Alerts Tab

Firmware version V2.3-7 and higher for the ES47/ES80/GS1280 MBM supports asynchronous alerts for hardware errors or configuration changes. The alerts are generated by the firmware when hardware components fail, hardware or partition configurations change, and environmental sensors report out of spec values.

To display the firmware alerts, AMU provides an Alert tab at the bottom of its right frame of its main window (see Figure 3-1), as well as a listing in the context menus of most Properties windows. The alerts displayed in the Properties windows are for the specific component. Figure 3-6 shows alerts as they appear in the Properties window for a system drawer.

**Figure 3-6: Alerts Tab in System Drawer Properties Window**



The display includes the time the alert occurred, the severity and description of the alert, and the component that is the source to the alert. For some alerts, clicking on the component will open the component's Properties window, where you may find additional information.

Note that the AMU displays only the alerts that occur while the AMU client is running. Starting with AMS Version 5.0, the AMU service forwards all alerts to EVM, which enables you to see them in the SPM's Recent Events window and with the EVM Event Viewer. See Section 2.3.4.2 for information about the Recent Events window and Section 2.6.4 for information about the Events Viewer.

Appendix B lists all of the alerts generated by the firmware, the source of each alert, the severity level, and the data that is contained in the alert packet.

All the alerts generated by the SMLAN firmware will appear in the Alerts display of the Main window. The Alerts tab window is the same in all Properties windows, but the alerts displayed depend on the component that generated the alert. Table 3-1 lists the dialog boxes that display alerts and the origin of the majority of the alerts that those dialog boxes display.

**Table 3-1: Types of Alerts**

Dialog Box	Origin of Alert
CPU Properties	EV7 alerts
Dual CPU Module Properties - Alert	CMM alerts
Dual CPU Module Properties - Environment	CMM environmental alerts
Hard Partition Properties	Operational alerts originated from that partition
I/O Drawer Properties - Alerts	PBM alerts
I/O Drawer Properties - Environment	PBM environmental alerts

**Table 3-1: Types of Alerts (cont.)**

Dialog Box	Origin of Alert
I/O Power Supply properties	PBM alerts
Main Display	Server Management LAN firmware
Partitions Properties	Operational alerts originated from that partition
Platform Properties	Operational alerts
Power Supply Tray Properties	PBM alerts
SubPartition Properties	Operational alerts originated from that partition
System Drawer Properties - Alerts	MBM alerts
System Drawer Properties - Environment	MBM environmental alerts
System Power Supply Properties	PBM alerts

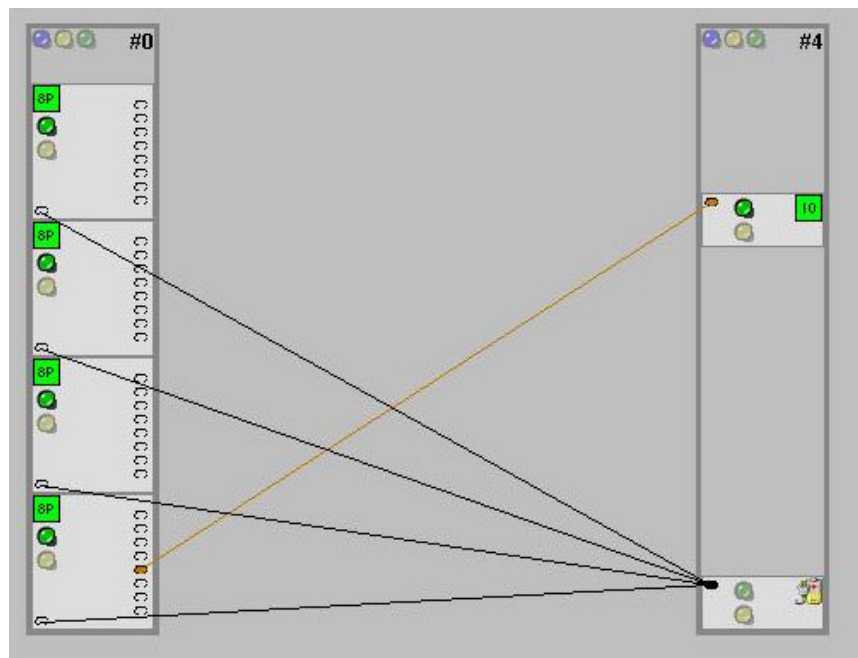
Because environmental readings can fluctuate, with different alerts generated for each different reading, the environmental displays include a Last Alert column and a History button. The Last Alert column displays the reading of the last sent alert, while the History button allows you to see all the readings of the Locator that has the problem.

AMU supports backwards compatibility with firmware versions 2.3-6 and older. You can use the AMS/AMU 4.0 applications to manage AlphaServer ES47, ES80, and GS1280 platforms running MBM firmware V2.3-6 or older.

### 3.4 Displaying the Platform's I/O and Power Connections

You can view a graphical representation of the I/O and power connections of a platform. Display the platform in the hardware view and click on the system or I/O drawer to view its I/O and power connections (Figure 3-7).

**Figure 3-7: I/O and Power Connections**



## 3.5 Monitoring the Platform's Environmental Status

You can monitor the platform's environmental status by viewing the graphic of the system and the properties of each system drawer, I/O drawer, and dual CPU module.

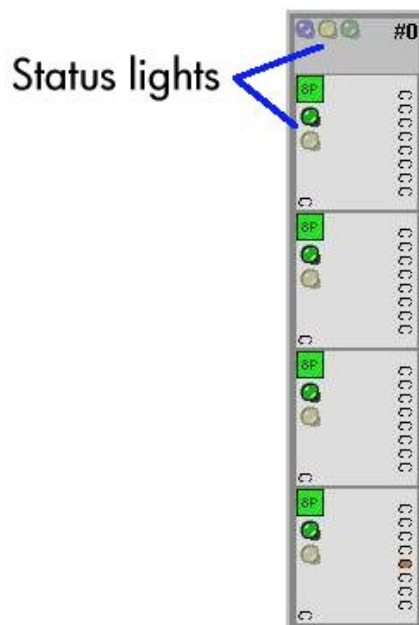
The graphical representation of the platform shown in the AMU's hardware view includes status lights for each system drawer. If the status light is green, then the system drawer is powered on and ready. If the status light is yellow, then the system drawer is in an abnormal state. It may be in an abnormal state because of a problem with its environmentals; that is, its fan, voltage, or power.

You can also monitor the I/O drawer in this way.

To determine why a system or I/O drawer is in an abnormal state, you can view the properties of a system drawer, I/O drawer, or dual CPU modules. See Section 3.16 for more information.

Figure 3-8 shows a close-up of one of the system drawers in the hardware view. The status lights of each drawer are green, which indicates that they are operating in a normal state.

**Figure 3-8: Status Lights**



## 3.6 Connecting to a Console

You can connect to either the SRM console or operating system running on a subpartition using the AMU Java Telnet applet. If no operating system is loaded and running on the subpartition, then you connect to the SRM console. If an operating system is running on the subpartition, then you connect to the console of the operating system.

Connecting to the SRM console allows you to manage the firmware of a partition or boot an operating system that is loaded on a subpartition. The SRM console is firmware on the backplane manager module that provides you with a command-line interface for operator control of the platform or of a partition. The SRM console is responsible for booting the operating system and passing system configuration data, discovered during power-up, to it.

Connecting to an operating system running on a subpartition allows you to log in to and manage the operating system.

### 3.7 Connecting to the Platform's Management Port

You can establish a connection to the management LAN of ES47, ES80, and GS1280 platforms directly from the AMU by connecting to the platform's management port. The management LAN connects to the platform's management software, which is controlled by the backplane manager (MBM). You can view the status and error logs of the platform and manage the MBM when you connect to the management port.

---

#### Note

---

AMU connects to console ports using exclusive connections only.

There can be only one exclusive connection to the management port open at a time. If an exclusive connection to the management port is already established by another user, you will not be able to connect to the management port.

It is important to terminate the Telnet session when you are finished because the port will not be accessible while the session is in progress.

---

You can access the management port of ES47, ES80, and GS1280 platforms through a Network Address Translator (NAT) box. A NAT box provides the platform with a unique IP address for the AMS and the hard partitions configured on the platform with a single point of access to the AMS. It allows you to assign to the hard partitions a set of IP addresses for internal traffic and a single IP address for external traffic.

The prompt of the management port is `MBM>`. See the *CLI Reference* manual on the Server Management CD-ROM for more information.

For a list of commands you can perform at the `MBM>` prompt, enter **help**.

### 3.8 Taking Exclusive Control

To perform certain tasks, you must take exclusive control of the AMU so that no other user can inadvertently perform conflicting critical tasks at the same time when using AMU on another client machine. However, users without exclusive control may still do noncritical tasks and activities by connecting to an MBM directly or through another console manager.

To take or relinquish exclusive control of the AMU system, use the Actions menu or the Exclusive Mode toggle button on the right side of the menu bar.

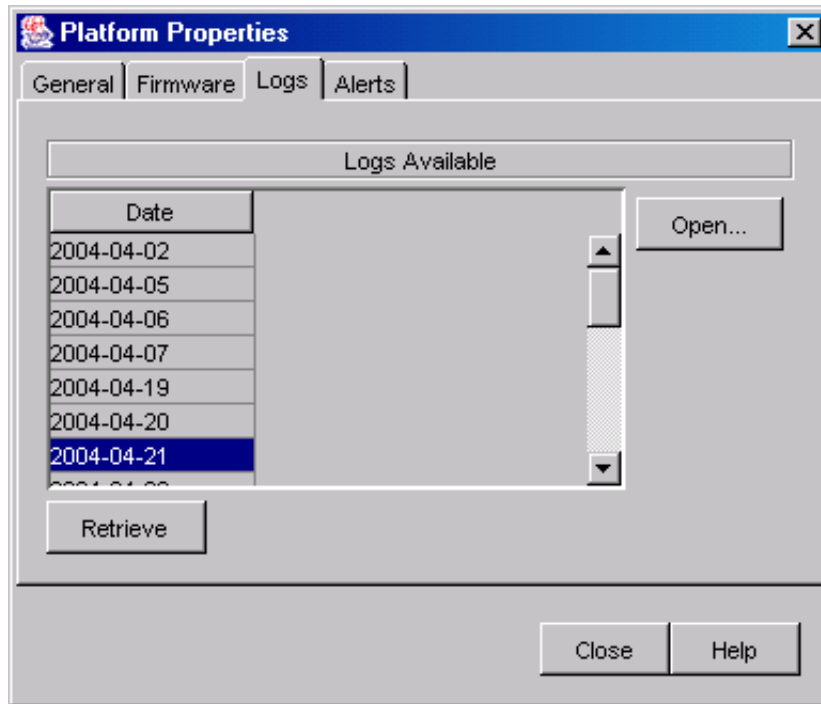
If you have exclusive control, no other user can take exclusive control until you relinquish it. Remember to relinquish exclusive control when you are finished with it.

### 3.9 Viewing MBM Error Log Files

AMU retains daily log files of all MBM errors. To view these log files, proceed as follows:

1. Click on Platform in the left frame to display the platforms properties in the right frame. You can open a separate properties box (Figure 3-9) by right clicking on Platform or opening the Actions menu and selecting Properties.

**Figure 3-9: Platform Properties Window Logs Tab**



2. Click on Retrieve to bring up a list of dates that contain MBM error logs from the server.
3. Highlight the day for which you want to view the logs and click on Open... This displays a Daily Log Properties box, which lists all messages from that day, along with a timestamp and the source of the message.

### 3.10 Using CDL File Support

Console Log Data (CDL) file support provides a way to save an error state when critical errors occur on an AlphaServer. The data saved is retrieved from the MBM and forwarded by the SRM console to the Operating System, which places it into the binary event log. The OS can create and save the file only when it is up and running.

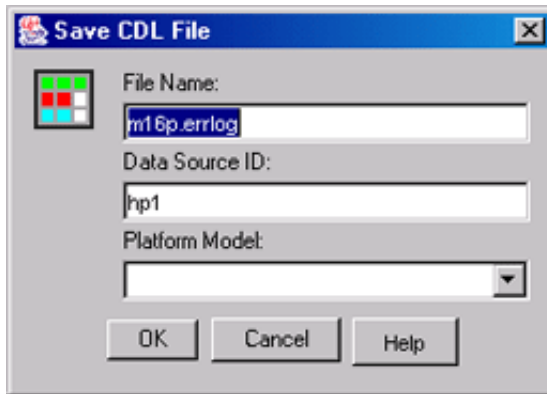
Using AMU, the CDL log can be retrieved and saved no matter the state of the operating system or partition. Only the PMU and associated MBMs need to be active for this error state retrieval to work.

Once CDL files are generated, they can be loaded into the System Event Analyzer (SEA) for error analysis.

When you create a CDL, AMU creates a new file if one does not exist. New CDL data is always appended at the end of the file. All the CDL data returned by the MBM firmware together with an event log header, event log terminator subpacket, and event log trailer are written into the file every time the user asks for CDL data and the response contains at least one entry. Nothing is written into the file if there is no data returned by the PMU.

To create or save a CDL file, select the CDL file ... menu item from a hard partition's drop-down menu (Figure 3-18) to bring up the Save CDL File dialog box (Figure 3-10).

**Figure 3-10: Save CDL File Dialog Box**



This dialog box asks for the following information:

- **File Name**  
Type in a name for the log file. The extension should always be `.errlog`.
- **Name ID**  
Type an identifier name that will subsequently be included in the header to provide information about the origin of the data that follows the header
- **Platform Model**  
Choose model of platform from the drop-down choices.

The file is saved as follows:

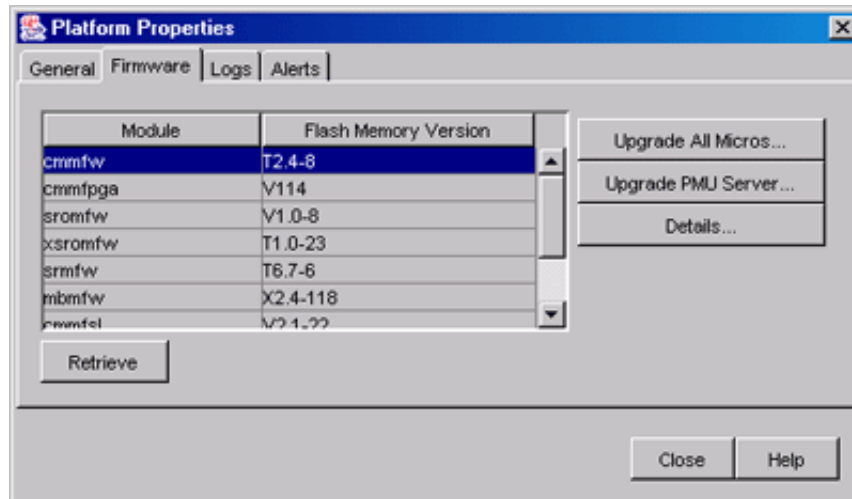
- **AMS installations on Tru64 UNIX and Linux:**  
`/usr/opt/ams/tomcat/webapps/spm/WEB-INF/log`
- **AMU standalone installations on Tru64 UNIX and Linux:**  
`/usr/opt/amu/tomcat/webapps/mpmu/WEB-INF/log`
- **AMU standalone installation in Windows:**  
`c:\amu\tomcat\webapps\mpmu\WEB-INF\log`
- **AMS installations on OpenVMS:**  
`sys$sysdevice:[apache.jakarta.tomcat.webapps.mpmu.WEB-INF.log`

### 3.11 Working with Firmware

You can upgrade the firmware of dual CPU modules, I/O drawers, and system drawers directly from the AMU. You must be in Exclusive Mode to upgrade firmware. The procedure is as follows:

1. Click on Platform in the left frame to display the platforms properties in the right frame. You can open a separate properties box by right clicking on Platform or opening the Actions menu and selecting Properties.

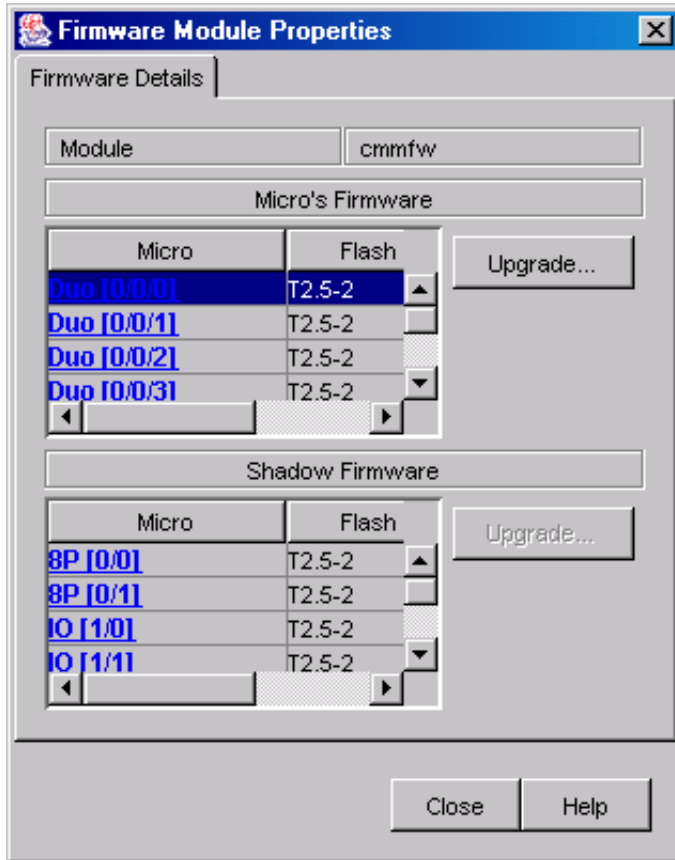
**Figure 3-11: Platform Properties Window Firmware Tab**



2. In the Properties box, select the Firmware tab. This displays a list of the firmware versions (Figure 3-11) for all modules found in the platform. If the list is empty, click on the Retrieve button to generate the list.
3. Highlight the module whose firmware you want to upgrade. You can upgrade the firmware for all module micros, for the PMU server only, or for selected micros.
  - To upgrade the PMU server, specify the TFTP server's address and specify the module you want to upgrade. The default module name is the selected module in the firmware's modules table. Note that you can load firmware from the PMU server to any of the platform's micros.
  - To upgrade the firmware for all micros, specify the PMU server or a TFTP server address as the source and the module you want to upgrade in all micros.
  - To upgrade the firmware for a specific micro, click on Details... in the Firmware window to bring up a list of all micros for the selected module. Highlight the micro whose firmware you want to update and click on Upgrade... (Figure 3-12).



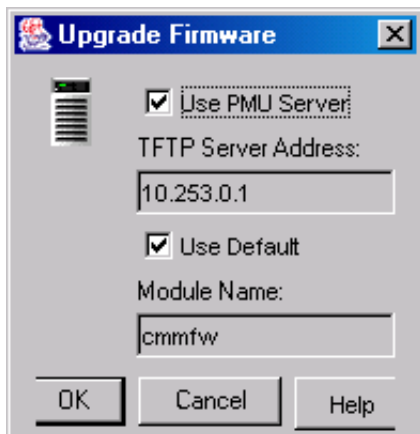
**Figure 3-12: Firmware Module Properties Window**



Specify the PMU server or the TFTP's server address as the source and the module you want to upgrade. Note that only the firmware of the selected micro is updated.

Clicking on any button in the Firmware window or the Firmware Module Properties window opens the Upgrade Firmware window (Figure 3-13).

**Figure 3-13: Upgrade Firmware Window**



## 3.12 Working with Partitions

You can view and modify partitions' properties and create new partitions and subpartitions from the menus available in the Partitions tree.

The following sections describe the drop-down menus available from the Partitions, Hard Partitions, and Sub Partitions branches of the tree structure in the left frame.

You can access these menus by using the branch's context menu or by selecting the branch and clicking on the Action menu.

You must take exclusive control of the AMU to perform many of the tasks in these menus. (See Section 3.8 for information about exclusive control.)

### 3.12.1 The Partitions Branch

The drop-down menu available from the Partitions branch lets you perform actions on all partitions. Figure 3-14 shows the menu. The sections that follow describe the items in that menu and a detailed description of the Partitions Properties window.

**Figure 3-14: Partitions Drop-Down Menu**



#### 3.12.1.1 The Partitions Drop-Down Menu

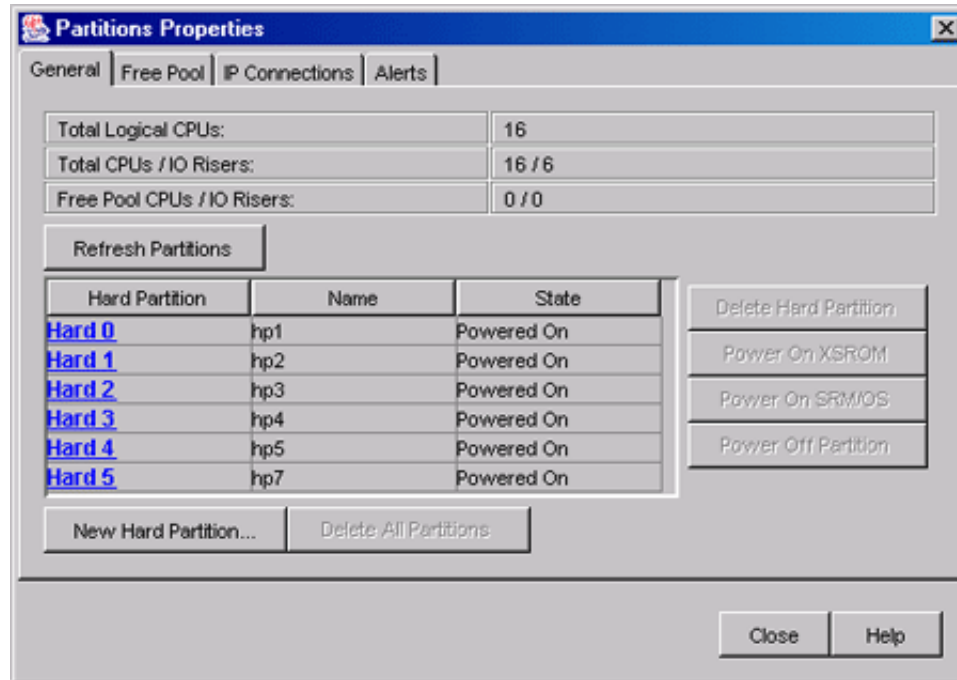
The following list describes the actions you can perform from the Partitions drop-down menu. Section 3.12.1.2 describes the contents of the Partitions Properties window.

- **New Hard Partition...**  
Brings up the New Partition window. See Section 3.13.1.2 for information about the New Partition window.
- **Assign To Platform's Free Pool**  
Moves the selected CPU into the platform's free pool. This is enabled only if a CPU in the logical view is selected. All assignments are saved in volatile storage. Assignments will not be committed to permanent storage (partitions database) until you save them.
- **Power On OS/SRM All Partitions**  
Turns on the power of all hard partitions. The start level is set to OS/SRM. (Requires exclusive control.)
- **Power On XSROM All Partitions**  
Turns on the power of all hard partitions. The start level is set to XSROM. (Requires exclusive control.)
- **Power Off All Partitions**  
Turns off the power on all hard partitions. (Requires exclusive control.)  
Because the CPUs are controlled in pairs, if the Dual CPU Module is split across partitions, the power will not be turned off, but flagged as "available to power off."
- **Refresh Partitions**  
Causes AMU to rediscover all partitions and subpartitions.
- **Properties**  
Invokes the Hard Partition Properties window (Figure 3-19).

### 3.12.1.2 The Partitions Properties Window

Figure 3-15 shows the Partition Properties window when you select Properties from the Partitions drop-down menu. The sections that follow describe the Partitions Properties window.

**Figure 3-15: Partitions Properties Dialog Box — General Tab**



#### 3.12.1.2.1 General Tab

The General tab of the Partitions Properties window provides information about partitions, and buttons to let you work with partitions.

##### Information

The table at the top of the dialog box provides the following information about partitions:

- Total Logical CPUs  
The total number of logical CPUs. This number may contain filler and empty CPU slots.
- Total CPU/IO Risers
- The actual number of CPUs and I/O connections found in the platform
- Free Pool CPUs/IO Risers  
The number of CPUs and I/O connections found in the platform's free pool.

The second table in the dialog box lists all hard partitions and their power status. It contains the following columns:

- Hard Partition  
The number assigned to the hard partition by the firmware.
- Name  
The partition's name.
- State  
The Powered On or Powered Off state of the partition.

Selecting an entry in this table enables the Delete Partition button if the partition's power is off. Delete Partition permanently deletes the hard partition and all its subpartitions. The partition is identified by its hard partition number, its name, and its running status.

### Actions

The buttons of the dialog box let you perform the following actions:

- Refresh Partitions  
Updates the Partitions Properties dialog box with data retrieved from the partition's database.
- New Hard Partition...  
Invokes the New Hard Partition dialog box. (See Section 3.13.1.2 for information about creating a new hard partition.)
- Power Off Partition  
Powers off the selected partition.

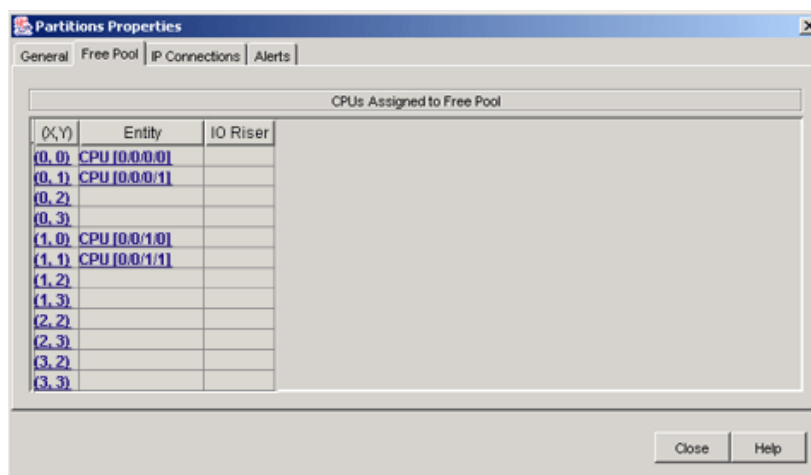
The following buttons are enabled only if a hard partition is powered off:

- Delete All Partitions  
Removes all partitions (and their subpartitions) that are in the Powered Off state.
- Delete Hard Partition  
Removes the selected hard partition and any of its subpartitions if the hard partition is in the Power Off state.
- Power On XSR0M  
Powers on the selected hard partition.
- Power On SRM/OS  
Powers on the selected hard partition. The start level is set to SRM/OS.

### 3.12.1.2.2 Free Pool Tab

The Free Pool Tab of the Partitions Properties dialog box (Figure 3-16) provides information about CPUs assigned to the free pool.

**Figure 3-16: Partitions Properties Dialog Box — Free Pool Tab**



The Free Pool tab provides the following information:

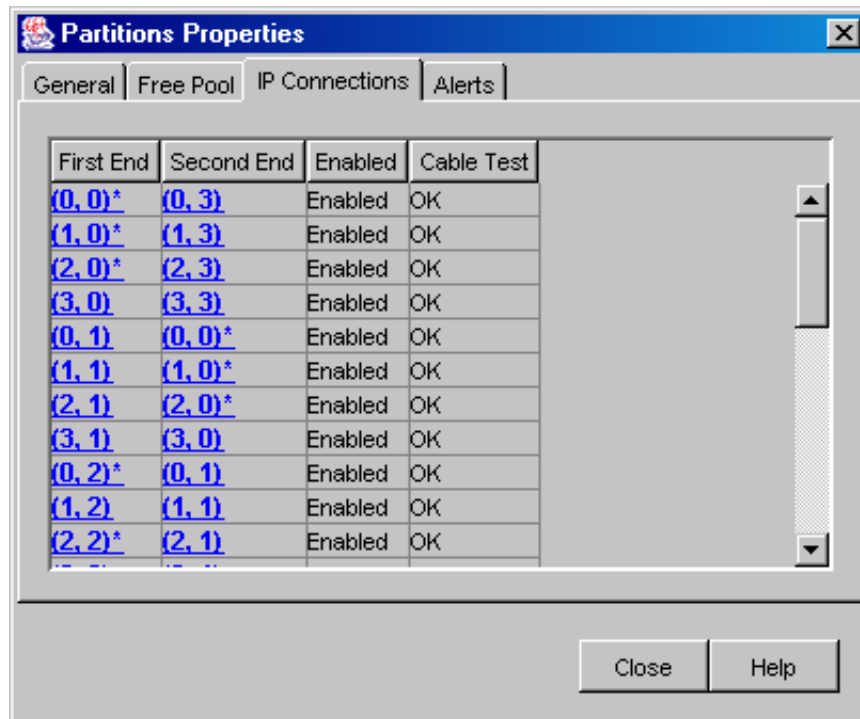
- (X, Y)  
The logical x and y coordinates of the CPU in the free pool.

- Entity  
The cabinet, drawer, x coordinate, and y coordinate of the CPU.
- I/O Riser  
The cabinet, drawer, and instance of the I/O Riser the CPU is connected to.

### 3.12.1.2.3 IP Connections Tab

Figure 3-17 shows the contents of IP Connections Tab.

**Figure 3-17: Partitions Properties Dialog Box — IP Connections Tab**



The following information is provided:

- First End  
The CPU coordinates of the first end of the connections.
- Second End  
The CPU coordinates of the second end of the connections.
- Enabled  
The state of the connection, either Enabled or Disabled.
- Cable Test  
The state of the cable test for its connection, either OK or Failed.

### 3.12.1.2.4 Alerts Tab

The Alerts tab displays operational alerts that originated from the selected partition. See Section 3.3.3.2 for information about firmware alerts.

## 3.12.2 The Hard Partitions Branch

The drop-down menu available from the Hard Partition branch lets you perform actions on the selected partition. Figure 3-18 shows the menu. The sections that follow describe the items in that menu and a detailed description of the Hard Partitions Properties window.

**Figure 3-18: Hard Partitions Drop-Down Menu**



### 3.12.2.1 Hard Partition Drop-Down Menu

The following list describes the actions you can perform from the Hard Partitions drop-down menu. Section 3.12.2.2 describes the contents of the Sub Partitions Properties window.

- **Power On OS/SRM**  
Turns on the power of the hard partition; the start level is set to OS/SRM. (Requires exclusive control.)
- **Power On XSROM**  
Turns on the power of the hard partition; the start level is set to XSROM. (Requires exclusive control.)
- **Power Off**  
Turns off a hard partition's power. (Requires exclusive control.)  
Because the CPUs are controlled in pairs, if the Dual CPU Module is split across partitions, the power will not be turned off, but flagged as "available to power off."
- **Reset OS/SRM**  
Resets the hard partition; the start level is set to OS/SRM. (Requires exclusive control.)
- **Reset XSROM**  
Resets the hard partition; the start level is set to XSROM. (Requires exclusive control.)
- **New Sub Partition**  
Enabled only if the hard partition is powered off. Select it to create a new subpartition within the hard partition. The type of subpartitions created are always soft subpartitions.  
You only need to provide a name to create a subpartition. The Sub Partition Name is a case sensitive string of alphanumeric characters including underscores. The maximum length is 20 characters. Partition names must be unique.
- **Delete Hard Partition**  
Enabled only if all subpartitions within the selected hard partition are powered off. When the hard partition is deleted all its subpartitions are also deleted and all the partition's resources are returned to the platform's free pool.
- **Assign to Hard Partition's Free Pool**

Moves the selected CPU into the platform's free pool. This is enabled only if a CPU in the logical view is selected. All assignments are saved in volatile storage. Assignments will not be committed to permanent storage (partitions database) until you save them.

- Save CDL File...

Provides a way to save an error state when critical errors occur on an AlphaServer. You can use the results of the analysis to provide Support and Field Service engineers with a diagnosis of the problem. Section 3.10 describes CDL (Console Log Data) file support.

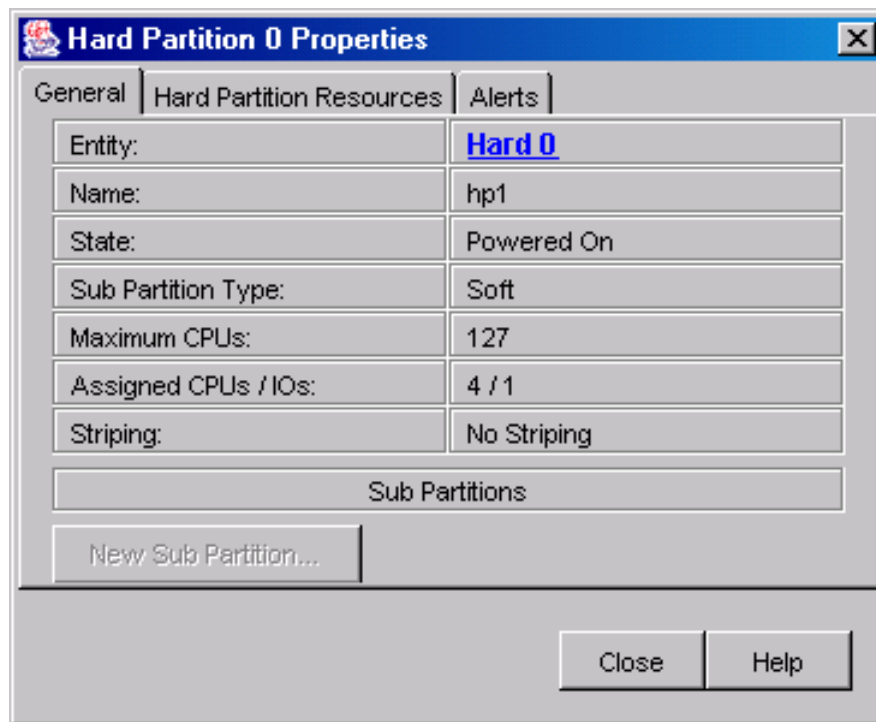
- Properties

Invokes the Hard Partition Properties window (Figure 3-19).

### 3.12.2.2 The Hard Partition Properties Window

Figure 3-19 shows the Hard Partition Properties window when you select Properties from the Hard Partition drop-down menu. A description of the Properties window follows.

**Figure 3-19: Hard Partition Properties Window**



The General tab of the Hard Partition Properties window provides the following information:

- Entity  
The hard partition number, which is 0 to 254.
- Name  
The name assigned to the hard partition at creation. The maximum length is 20 characters.
- State  
Whether the partition is powered on or powered off.
- Sub Partitions Type  
The type of subpartitions found in this hard partition.

- **Maximum CPUs**  
The maximum number of CPUs that can ever be placed in the hard partition. This number is used to determine the proper outing algorithm.
- **Assigned CPUs/IOs**  
The number of CPUs and I/O risers assigned to that partition.
- **Striping**  
Whether striping is enabled or disabled.
- **Delete Sub Partition**  
Deletes the selected subpartition. This button is enabled only if a selected subpartition is not in the Running state.
- **New Sub Partition**  
Invokes the New Sub Partition dialog box.

The Sub Partitions table lists all subpartitions found in the hard partition and displays the following information:

- **SubPartition**  
The name of the subpartition, including the hard partition and subpartition numbers.
- **State**  
The current running state of the subpartition, which is one of the following:
  - Not Running XSROM
  - Running OS/SRM
  - Unknown
- **CPUs/IOs**  
The number of CPUs and IO connections.

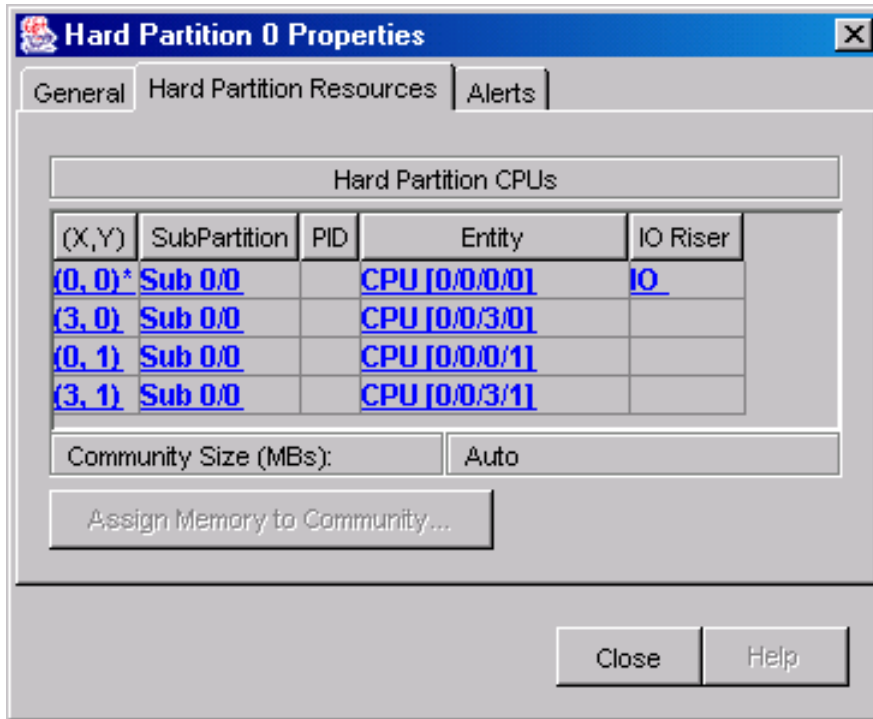
A subpartition can be deleted by selecting it and clicking on the Delete Sub Partition button.

When the hard partition's power is off, you can select the New Sub Partition button to create a new subpartition.

You can delete a subpartition by selecting it and clicking on the Delete Sub Partition button.



**Figure 3-20: Hard Partition Properties — Resources Tab**



The Hard Partition Resources tab (Figure 3-20) lists all the CPUs assigned to the hard partition and displays the following information for each CPU:

- (X,Y)  
The logical coordinates of the CPU.
- SubPartition  
The name and hard partition and subpartition number the CPU has been assigned.
- PID  
The processor ID.
- Entity  
The cabinet/drawer/dual module/instance coordinates of the CPU.
- IO Riser  
The cabinet/drawer/instance of the IO riser the CPU is connected to.
- Community Size (MBs)  
The memory allocated to the hard partitions community. `Auto` is displayed if memory is assigned by the firmware.
- Assigns memory to the community. This button is enable only if you have exclusive control, the hard partition is powered off, and the hard partition has more than one subpartition.

### 3.12.2.3 Alerts Tab

The Alerts tab displays operational alerts that originated from the selected partition. See Section 3.3.3.2 for information about firmware alerts.

### 3.12.3 The Sub Partition Branch

The drop-down menu available from the Sub Partition branch lets you perform actions on the selected subpartition. Figure 3-21 shows the menu. The sections that follow describe the items in that menu and a detailed description of the Partitions Properties window.

**Figure 3-21: Subpartitions Drop-Down Menu**

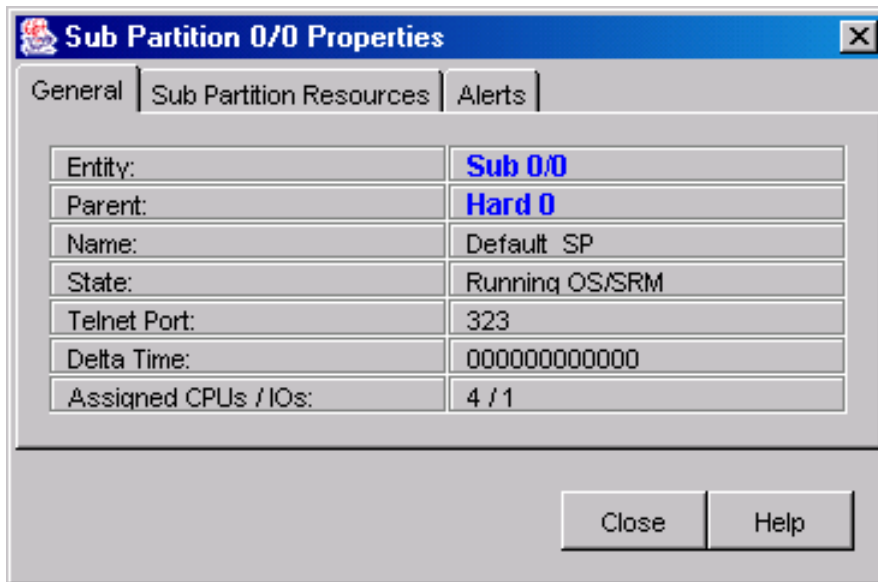


#### 3.12.3.1 The Sub Partition Drop-Down Menu

The following list describes the actions you can perform from the Sub Partitions drop-down menu. Section 3.12.3.2 describes the contents of the Sub Partitions Properties window.

- **Open Telnet**  
Opens a Telnet session using the subpartition's Telnet port.
- **Halt In**  
Halts the subpartition.
- **Halt Out**  
Brings the subpartition out of the halt state.
- **Delete Sub Partition**  
Deletes the selected subpartition, returning the subpartition resources to the hard partition's free pool. This menu is enabled only if the subpartition is in the Not Running state.
- **Assign To Sub Partition**  
Lets you assign the selected CPU to the subpartition. This menu is enabled only if the subpartition is in the Not Running state and one or more CPUs are selected in the logical view.
- **Properties**  
Invokes the Sub Partition Properties window (Figure 3-22).

**Figure 3-22: Sub Partition Properties Box**

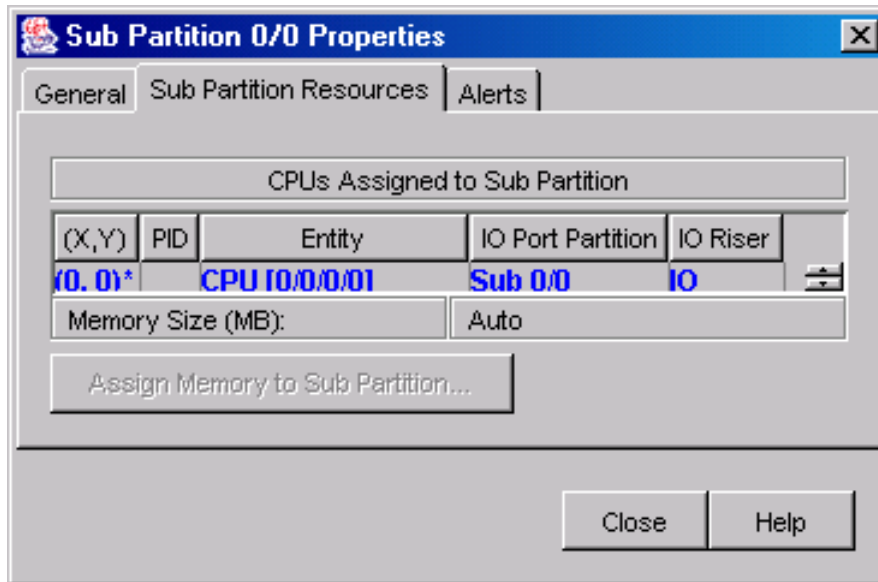


### 3.12.3.2 The Sub Partition Properties Window

The Sub Partition Properties window (Figure 3-22) provides the following information:

- Entity  
The subpartition itself.
- Parent  
The hard partition the subpartition belongs to.
- Name  
The name assigned to the subpartition.
- State  
The status of the subpartition, which can be Not Running, Running SRM, or Unknown.
- Telnet Port  
The port assigned to the subpartition for a Telnet connection.
- Delta Time  
Six bytes of Delta Time. All 1's indicate Invalid data. Delta Time is applied to the base time to provide the BB-watch value.
- Assigned CPUs/IOs  
Total number of CPUs and I/O connections assigned to this subpartition.
- The Close button closes the properties box.

**Figure 3-23: Sub Partition Properties — Resources Tab**



The Sub Partition Resources tab (Figure 3-23) displays the following information:

- (X, Y)  
The x, y coordinates of the CPU.
- PID  
The processor ID.
- Entity  
The cabinet/drawer/duel module/instance of the CPU.
- IO Port Partition  
Indicates which subpartition has the I/O port for this CPU.
- IO Riser  
The cabinet/drawer/instance coordinates of the I/O Riser to which the CPU is connected.
- Memory Size (MB):  
The total memory allocated to the subpartition. `Auto` is displayed if memory is assigned by the firmware.

To assign memory to a subpartition, select the `Assign Memory to Sub Partition` button. This button is enabled when the hard partition's power is off.

### 3.12.3.3 Alerts Tab

The Alerts tab displays operational alerts that originated from the selected partition. See Section 3.3.3.2 for information about firmware alerts.

## 3.13 Creating and Modifying Partitions

You can create and modify partitions using the AMU. The following sections tell you how.

### 3.13.1 Creating a Partition

The following sections describe how to create a new partition.

### 3.13.1.1 Preliminary Steps

Before you begin the process of creating or modifying a partition, make sure that your partition meets the following criteria:

- You must have at least one PCI box for each subpartition you need to create.
- Partitions must contain at least one Dual Processor Module (duo). Each duo contains two processors.
- Duos cannot be split among hard partitions.
- The set of processors to be assigned to a partition should form a continuous rectangle on the mesh. The AMU's partition view can help you locate the processors on the mesh.
- At least one of the processors in a subpartition must be connected to an I/O Riser.

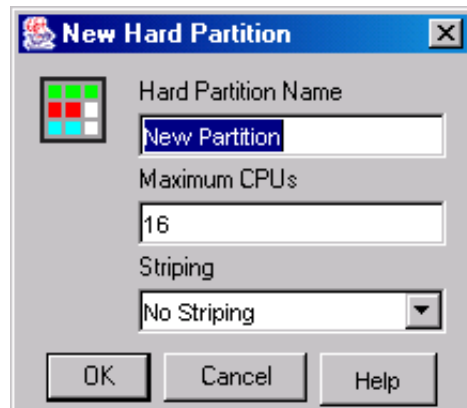
Decide ahead of time on the following items:

- The names for your partitions
- The names for the subpartitions
- The number of processors and the location of the processors on the mesh
- Memory assignments if other than the default 64 MB per processor
- Whether you want to enable striping — the splitting of physical memory across a set of RIMMS

### 3.13.1.2 New Hard Partitions Menu

Choosing New Hard Partition from the Partitions main menu or the Actions menu opens the New Hard Partition menu Figure 3-24.

**Figure 3-24: New Hard Partition Menu**



This menu asks for the following information:

- **Hard Partition Name**  
A case-sensitive string of alphanumeric characters including underscores. The maximum length is 20 characters. Partitions names must be unique.
- **Maximum CPUs**  
The maximum number of CPUs that can be placed in the hard partition. The default is the total number of CPUs present in the platform.
- **Striping**  
Select Striping to enable the splitting of physical memory across a set of RIMMS. The default is No Striping.

### 3.13.1.3 Creating the Partition

The following steps provide an overview of how to create a new hard partition:

1. In the left frame, highlight Partitions and choose New Hard Partition from the Partitions menu.
2. Fill in the requested data in the New Hard Partition menu and click OK. A new hard partition will appear in the AMU tree. The new hard partition has a default subpartition named Default\_SP.
3. Optionally, you can create a new subpartition by right clicking on the partition you created and choosing New Subpartition. Give the subpartition a name.
4. Select the CPUs you want to assign to the partition. In the partitions logical view displayed in the right frame, select one or more CPUs by moving the cursor over the CPUs and selecting with the left mouse button pressed.
5. Assign the selected CPUs to the partition by right clicking on the subpartition and choosing the Assign to Sub Partition subpartition menu
6. Boot the partition.

### 3.13.2 Modifying an Existing Partition

You must power a partition off before you try to modify it. Menu items related to partition modifications are disabled when the partition is in power on state. The following is the list of some of the operations that modify the configuration of a partition:

- Remove CPUs from a partition
- Add CPUs to a partition
- Assign memory to a partition

#### 3.13.2.1 Remove CPUs from a Partition

To remove CPUs from a partition, select the CPUs in the logical view and assign them to the platform's free pool or the hard partition's free pool using the Partitions and Hard Partitions drop-down menus.

#### 3.13.2.2 Add CPUs to a Subpartition

You can only add CPUs from the platform's free pool or the hard partition's free pool to a subpartition. To add CPUs:

1. Move the CPUs to the free pool.
2. Reselect the CPUs and assign them to the subpartition.

#### 3.13.2.3 Assign Memory to a Subpartition

To assign memory to a subpartition perform the following steps:

1. Select the subpartition's properties menu.
2. In the properties dialog box, select the Assign Memory To Sub Partition button and enter the amount of memory you want to assign.

#### 3.13.2.4 Assign Memory to a Community

You can assign memory to a Community only if a hard partition has more than one subpartition. To do this:

1. Select the hard partition's Properties menu.

2. In the hard partition properties dialog box, select the Assign Memory To Community button and enter the memory you want to assign.

## 3.14 Reconfiguring Cable Connections

When you make changes to the platform's cabling, you must update the firmware cabling database.

To reconfigure the cabling, you must first take exclusive control of the AMU. See Section 3.8 for more information.

Next, right-click on the Hardware icon in the left frame and then select Reconfigure Cabling. A message in the bottom frame of the main display confirms your action.

## 3.15 Testing All Cable LEDs

You can test the LEDs of all IP and I/O cable ports from the AMU. When you test the LEDs, they blink on and off until the interval timer elapses.

To test the LEDs, you must take exclusive control of the AMU. See Section 3.8 for more information.

After you take exclusive control, right-click the Hardware icon in the left frame and select Turn On All Cable LEDs from the pop-up menu. Then enter the amount of time in seconds you want the LEDs to blink. The maximum value is 3600 (1 hour).

You can also turn on the LEDs of either the IP Cables Connections Properties or I/O Cables Connections Properties dialog boxes.

To stop the blinking, right-click the Hardware icon in the left frame and select Turn Off All Cable LEDs from the pop-up menu.

## 3.16 Viewing Detailed Information About Each Component

You can view detailed information about:

- System drawers
- Hard partitions
- Subpartitions
- I/O drawers
- Dual CPU modules
- CPUs

### 3.16.1 Viewing Properties of System Drawers

You can view detailed information about each system drawer of the platform; such as general information, environmental, drawer indicators, and firmware, by viewing their properties. To display the Properties dialog box of a system drawer, select the system drawer icon in the left frame with the right mouse button, and then select Properties.

#### 3.16.1.1 Viewing General System Drawer Properties

You can view the system drawer's general properties by selecting the General tab in the System Drawer Properties dialog box.

#### 3.16.1.2 Viewing Environmental Properties

You can monitor the system drawer's environmental in the System Drawer Properties: Environment dialog box. This dialog box displays a warning limit and a

failure limit for the fan, voltage, and temperature sensors of the system drawer. The warning limits are not user-configurable.

When a sensor receives a reading that meets or exceeds a limit, the system drawer is placed into the appropriate state. For example, if the system drawer's temperature sensor has a warning limit of 25 degrees Celsius, then the yellow status light on the system drawer will light when the temperature of the system drawer reaches 25 degrees Celsius.

You can view the system drawer's environmental properties by selecting the Environment tab in the System Drawer Properties dialog box.

### **3.16.1.3 Viewing Drawer Indicator Properties**

You can view the settings of the system drawer's status lights in the Drawer Indicators tab of the System Drawer Properties dialog box. The status lights are either enabled (true) or disabled (false).

You can view the system drawer's indicator properties by selecting the Drawer Indicators tab in the System Drawer Properties dialog box.

### **3.16.1.4 Viewing Firmware Properties**

You can view detailed information about the firmware running on the system drawer in the Firmware tab of the System Drawer Properties dialog box.

Select the Firmware tab in the System Drawer Properties dialog box. To fill in the dialog box, select Retrieve.

## **3.16.2 Viewing Properties of I/O Drawers**

You can view the properties of the platform's I/O drawers. The I/O drawer properties display the I/O drawer's backplane type, power status, and the status of its PCI backplane manager (PBM).

To display the properties of an I/O drawer, select the I/O drawer's icon in the left frame with the right mouse button, and then select Properties. You can view the general properties by selecting the General tab in the I/O Properties dialog box.

### **3.16.2.1 Viewing Environmental Properties**

You can view an I/O drawer's environmental properties in the I/O Drawer Properties: Environment dialog box. It displays a warning limit and a failure limit for the fan, voltage, and temperature sensors of the I/O drawer. When a sensor receives a reading that meets or exceeds a limit, the I/O drawer is placed into the appropriate state. For example, if the I/O drawer's temperature sensor has a warning limit of 25 degrees Celsius, then the yellow status light on the I/O drawer will light when the temperature of the system drawer reaches 25 degrees Celsius.

You can view the environmental properties of the I/O drawer by selecting the Environment tab in the I/O Properties dialog box.

### **3.16.2.2 Viewing Drawer Indicator Properties**

You can view the settings of the I/O drawer's status lights in the Drawer Indicators tab of the I/O Drawer Properties dialog box. The status lights are either enabled (true) or disabled (false).

You can view the indicator properties of the I/O drawer by selecting the Drawer Indicators tab in the I/O Properties dialog box.



### 3.16.2.3 Viewing Firmware Properties

You can view detailed information about the firmware running on an I/O drawer in the Firmware tab of the I/O Drawer Properties dialog box.

Select the Firmware tab in the I/O Drawer Properties dialog box. To fill in the dialog box, select Retrieve.

### 3.16.3 Viewing Properties of Dual CPU Modules

You can view detailed information about each dual CPU module including the status of its CPU management module (CMM), its environmentals, frequency, and firmware.

The General properties tab of the Dual CPU Module Properties dialog box displays the module's coordinates, CMM IP address, CMM power state, CMM status, and CMM POST code.

To view the general properties of a dual CPU module, select its icon in the left frame with the right mouse button, and then select Properties. You can view the dual CPU module's general properties by selecting the General tab in the Dual CPU Module Properties dialog box.

#### 3.16.3.1 Dual CPU Module Properties: Environment

You can view a dual CPU module's environmental properties in the Dual CPU Module Properties: Environment dialog box. This dialog box displays a warning limit and a failure limit for the fan, voltage, and temperature sensors of the dual CPU module. When a sensor receives a reading that meets or exceeds a limit, the dual CPU module is placed into the appropriate state. For example, if the module's temperature sensor has a warning limit of 25 degrees Celsius, then the yellow status light on the I/O drawer will light when the temperature of the module reaches 25 degrees Celsius.

You can view the environmental properties of the dual CPU module by selecting the Environment tab in the Dual CPU Module dialog box.

#### 3.16.3.2 Dual CPU Module Properties: Frequency

You can view the CPU frequency of the dual CPU module by selecting the Frequency tab in the Dual CPU Module dialog box.

#### 3.16.3.3 Dual CPU Module Properties: Firmware

You can view detailed information about the firmware running on a dual CPU module in the Firmware tab of the Dual CPU Module Properties dialog box.

Select the Firmware tab in the Dual CPU Module Properties dialog box. To fill in the dialog box, select Retrieve.

### 3.16.4 Viewing Properties of CPUs

You can view detailed information about a CPU such as its coordinates, status, its memory modules, and their number and capacity in the CPU Properties dialog box.

To view the CPU's properties, select the CPU in the left frame using the right mouse button and then select Properties.

## 3.17 Using the Visual Editor

AMU uses hardware configuration templates and information provided by the SMLAN firmware to draw the hardware displays of managed platforms.

Included with the AMU are a number of standard templates that represent the manufacturing layout of supported configurations. The Visual Editor integrated with SPM and AMU let you move beyond these standard templates.

The AMU Visual Editor lets you:

- Create and modify ES47, ES80, and GS1280 hardware configuration templates
- Configure platforms to be managed by AMU in standalone mode

### 3.17.1 Accessing and Using the Editor

The Visual Editor allows you to design a new configuration (called a template) or modify an existing one by dropping and dragging a collection of graphics and moving those components within the template. You access the editor as follows:

- In SPM, by selecting the AMU Visual Editor from the Configuration menu.
- From AMU in standalone mode, by selecting Visual Editor from AMU's File menu

When you first invoke the Visual Editor, its left frame contains all the standard hardware configurations of ES47, ES80, and GS1280 platforms. Selecting a template displays its hardware layout in the right frame, similar to what one sees in the AMU's hardware display in the right frame.

The cabinets, their contents, the position and size of each components, and the IDs from the thumbwheel settings are all included in the template. You can see a template's contents graphically in the right frame or as nodes of the platform's tree structure in the left frame.

Clicking on a template causes a graphical representation of that cabinet to appear in the right frame. By expanding the template's tree structure, you cause the cabinet's components to be displayed. You can then click on a component to see it highlighted in the graphical representation.

You cannot modify the default templates, but you can copy them and then modify the copy to create a new template configuration. After you save a newly created template, it is available in SPM.

To assign a new template to a configured platform in SPM select Modify in the platform's context menu and then select the template from the Template drop-down box.

### 3.17.2 Creating and Modifying a New Template

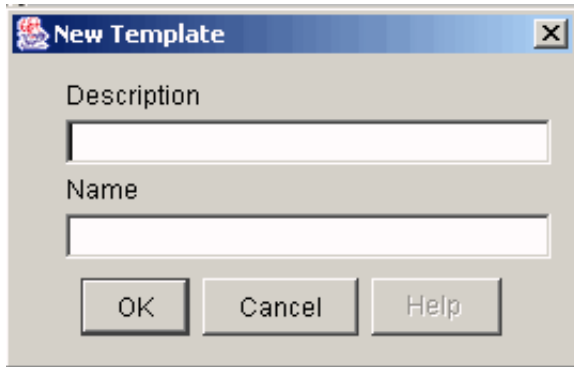
You can create a template from scratch or from an existing template. You can also modify and delete any template you create:

- To create a new template based on an existing template, right click on your preferred machine model and select Duplicate Template. For example, right click on the template GS1280 Model 8 (standard 8p) to create a new template based on the existing template's configuration.

This opens the New Template dialog box (Figure 3-25), which provides a default Description and Name. You can accept the default or provide a description and name of your choosing.

- To create a template from scratch, right click Templates in the left frame to open the New Template dialog box (Figure 3-25). Enter a name and description.
- To modify a template you created, right click on the template you want to modify and select Edit Template.
- To delete a template you created, right click on the template you want to remove and select Delete Template.

**Figure 3-25: New Template Dialog Box**

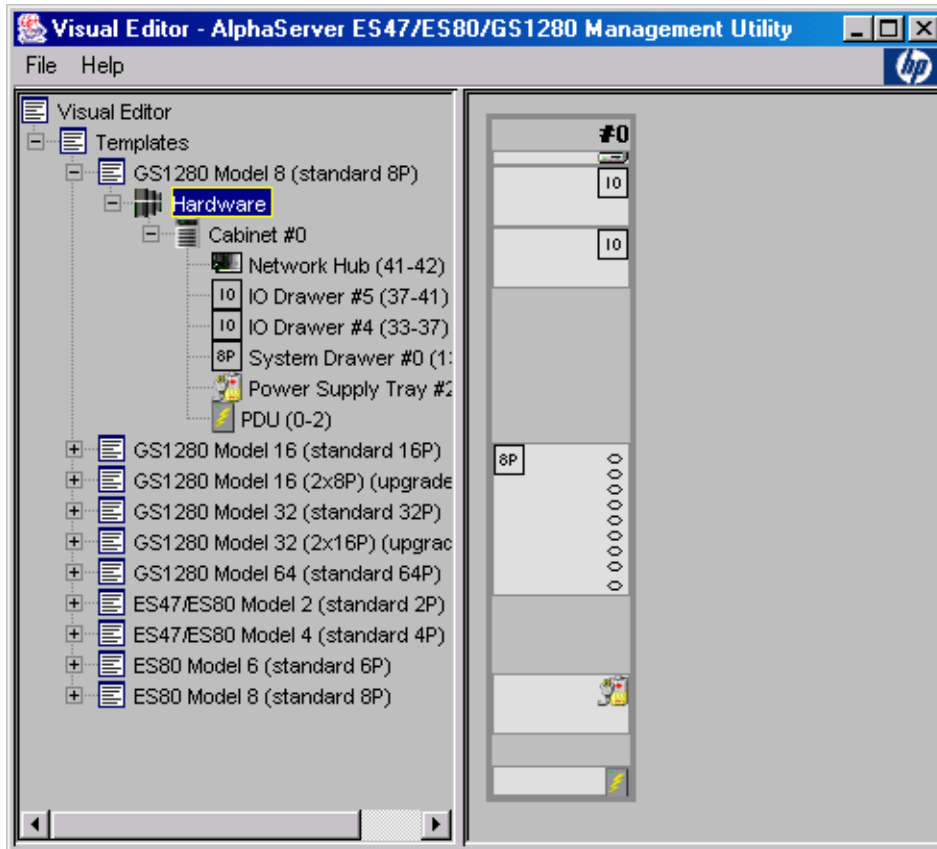


When you click OK in the New Template dialog box, the name you selected appears at the bottom of the Templates list in the left frame. To save the new template, right click on the template name and select save.

If you are creating a new template from an existing template or modifying a template, the right frame displays the layout of the existing template (Figure 3-26). If you are building a template from scratch, you must click on Add Cabinet to add a cabinet box for your template. The following list describes contents of the right frame:

- **Components box**  
This box contains components that you can add to your template. To do so, click on the selected component and drag it to its position in the cabinet. You will use this feature as you add components to your ES47, ES80, and GS1280 platform and want them represented in the graphical representation. Clicking the Add Cabinet button adds a new cabinet box to the graphical display and a new cabinet listing to the Templates tree.
- **Properties box**  
The Number, Position, and Size fields of the Properties box display numbers when you access any components in the cabinet box. The numbers change as you add, remove, move, and resize components in the cabinet box.
- **Cabinet box**  
This box provides a representation of the selected model cabinet's original configuration if you use an existing template, or it is empty if you clicked on Add Cabinet when building a template from scratch. In this box you create the configuration that represents your platform.

**Figure 3-26: Visual Editor**



The following list describes the basics for creating a template:

- You add components by dragging them from the components box to the cabinet box.
- You move components by dragging the selected component to a new location or by using the arrows in the Position field of the Properties box.
- You resize components by clicking on the component and using the arrows in the Size field of the Properties box.
- You remove components by dragging them to the Components box or by right clicking on them and clicking Delete Element. You are prompted on whether you want to complete the removal.
- A red border around a component indicates that two components overlap.

To save the template or discard changes, use the editor's File menu or the context menu of the template you are working on.

After you have saved a template, you can remove it (Destroy Template) or edit it using the File menu or the template's context menu.

You cannot remove or edit the pre-existing templates.

### **3.17.3 Adding Platforms to a Standalone AMU**

You can use the Visual Editor to configure platforms to be managed by AMU in standalone mode. When you launch the editor from within AMU, the tree in the left frame contains a Platform Configurations node. To configure a new platform, do the following:

1. Right click Platform Configurations and select New Configuration.

2. In the New Configuration dialog box, enter a description and the NAT box IP address.
3. Select the check box to enable the Templates drop-down box and select a template from the available list of templates.
4. Click OK. The new configuration appears under the platform configurations node.
5. Select Save from the context menu to save the configuration.

To manage a newly configured platform:

1. Exit the editor.
2. Select Open Platform from the AMU file menu.
3. Select the platform you want from the list of available platforms in the dialog box.

To modify a configuration:

1. Select Edit from the configuration's context menu.
2. Select Properties
3. Modify the property you want to change and click OK.
4. Save the configuration.

### 3.17.4 File Locations

Templates created by the Visual editor are saved in a file named `Templates.xml` and configurations are saved in a file named `Configuration.xml`. The directory locations for these files are as follows:

- AMS Tru64 UNIX and Linux  
`/usr/opt/ams/tomcat/webapps/spm/WEB-INF/data`
- AMU Tru64 UNIX and Linux  
`/usr/opt/amu/tomcat/webapps/mpmu/WEB-INF/data`
- AMU Windows  
`C:\amu\tomcat\webapps\mpmu\WEB-INF\data`



---

## Using the AlphaServer Partition Wizard

The AlphaServer Partition Wizard (APW) is a graphical application that simplifies the creation and management of partitions on AlphaServer ES47/ES80/GS1280 and GS80/GS160/GS320 platforms. The following topics are discussed:

- An overview and how to run the application, including differences between how APW works with ES47/ES80/GS1280 and GS80/GS160/GS320 platforms (Section 4.1)
- The processes involved in working with partition maps (Section 4.2)
- Modifying partition maps (Section 4.3)
- Creating new partition maps (Section 4.4)
- Saving partition map files, validating maps, and applying a map to the system (Section 4.5)
- Managing APW files (Section 4.6)

### 4.1 APW Overview and Start Up

The APW runs on the AMS and, through a series of windows, enables you to work with partitions without having to know anything about the console commands involved. The APW works with both hard and soft partitions:

- Hard partitions do not share CPU, memory, or I/O resources; the boundaries of these partitions are “hard.” An instance of an operating system can run in each hard partition. These instances run independently of each other.
- Each hard partition can have a soft partition, also called a subpartition. Soft partitions share the CPU, memory, and I/O of the hard partition. Partitions running the OpenVMS Galaxy operating system can have multiple soft partitions.

By default, each hard partition on an ES47, ES80, and GS1280 has one default soft partition.

Whenever APW changes your hardware’s configuration, it also changes the AMS configuration by adding, modifying and removing consoles as needed to match your partition configuration.

Before attempting to run the APW, make sure your system meets the installation requirements described in installation instructions.

#### 4.1.1 Accessing the APW

You can run APW in two ways:

- From the Server Platform Manager (SPM)

You must run APW as root or while logged in as a user in the `amsuser` group with the Administrator role within SPM.

From the SPM, select the platform you want to partition by highlighting it, and select APW from the platform’s context menu or from the Actions menu.

When running APW from the SPM, you can resize columns in APW windows by clicking on a divider between columns and dragging. The pointer changes to indicate that a column can be expanded or contracted.

Moving the pointer over a button displays a tool tip for using that button.

- From the command line

To run APW from the command line, you must be logged on as root on a system running AMS. Type the `apw` command at the command prompt, providing the name of a platform as an argument. For example:

```
# /usr/opt/ams/bin/apw rhnat1
```

### 4.1.2 APW Features

The following list describes a few APW features. Detailed information is provided later in this chapter.

- You can create new partition maps or modify existing ones.
- You can run the APW while a partition is running an operating system. Although you cannot commit a partition map that reassigns hardware to or from a hard partition that is running an operating system, you can commit changes that affect other partitions and you can create and save any partitions maps.
- The Validate button causes the APW to review the proposed changes and then lets you know of any problems such changes could cause.
- The Commit button makes the desired changes. Prior to clicking the commit button, you can rearrange resources to find the configuration that meets your needs. Once satisfied, you can commit the changes or save them to a file for later use.

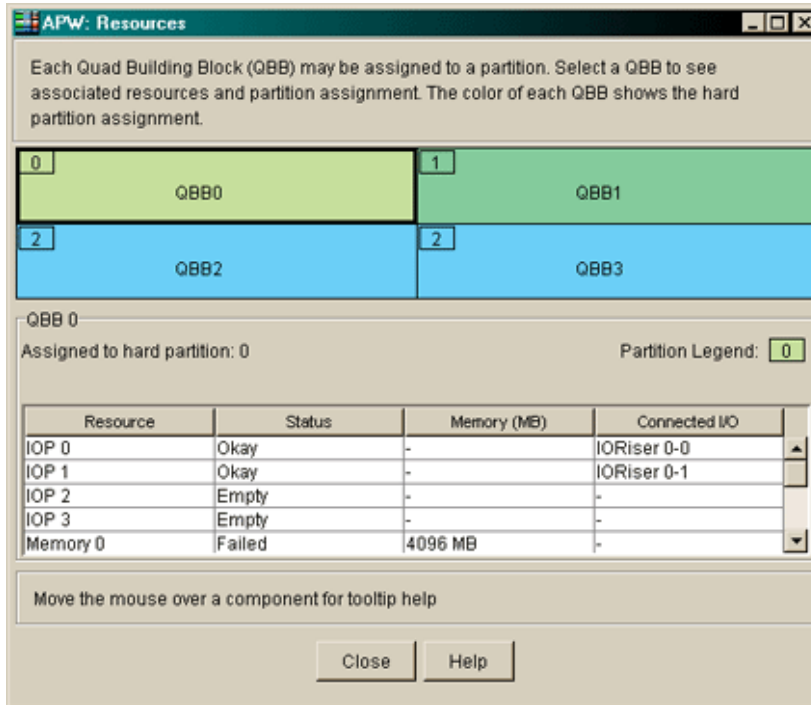
### 4.1.3 ES47/ES80/GS1280 and GS80/GS160/GS320 Platform Differences

You can use APW to create or modify partition maps for ES47/ES80/GS1280 and GS80/GS160/GS320 platforms. Although the process for doing so is similar, you will see some differences.

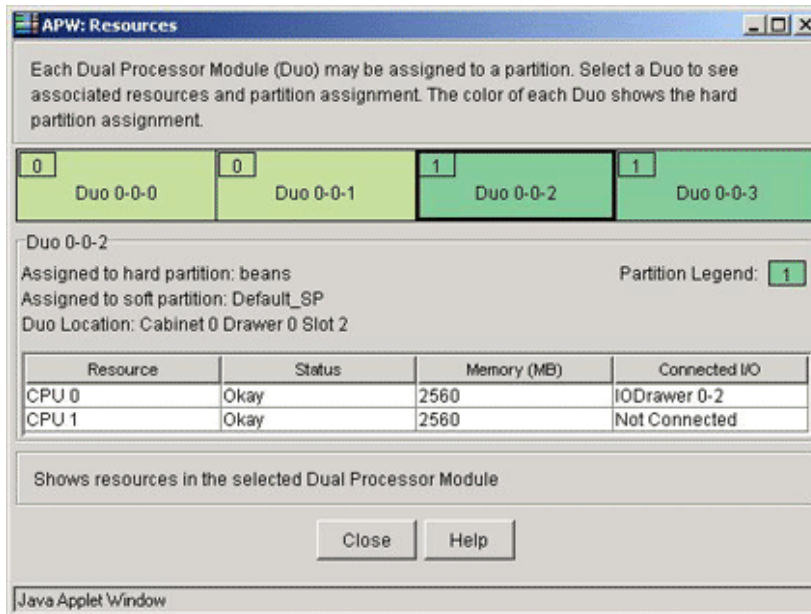
The principal difference is that on ES47, ES80, and GS1280 platforms, the partition map assigns each of the platform's Dual processor Module (Duo) to a partition. On GS80, GS160, and GS320 platforms, the partition map assigns Quad Building Blocks (QBBs) to a partition. Figure 4-1 shows the Resources window for GS80, GS160, and GS320 platforms and Figure 4-2 shows the Resources window for ES47, ES80, and GS1280 platforms. See Section 4.2.2 for information about the Resources window and the differences between to two platform series.



**Figure 4-1: QBB Resources Window**



**Figure 4-2: Duo Resources Window**



In this chapter, when the text and figures refer to duos and ES47, ES80, and GS1280 platforms, those references also pertain to QBBs and GS80, GS160, and GS320 platforms unless otherwise indicated.

The following list describes other differences you need to be aware of when working with the two different series of platforms:

- Partitions and soft partitions on GS80, GS160, and GS320 platforms do not have names, although each partition and soft partition can have a console name
- Unlike duos, QBBs have no “striping” attribute. QBB partitions do use memory striping, but the striping is automatically determined by what memory is installed in a QBB. Consult your platform documentation for more information.

- GS80, GS160, and GS320 platforms are switch based, allowing any QBB to be put into a hard partition with any other QBB. ES47, ES80, and GS1280 platforms are mesh based, and so the mesh governs what duos can be part of a hard partition. There are no error messages about “the mesh” for GS80, GS160, and GS320 platforms.
- Only ES47, ES80, and GS1280 platforms have a default partition. If there are no other hard partitions, there is a special partition called Default\_HP. If a hard partition has no other soft partitions, there is a special soft partition called Default\_SP. These platforms have unique circumstances when adding hard partitions and soft partitions, which the user interface reproduces for consistency with the MBM console interface. For example:
  - In the Create or Modify a Partition Map window, whenever you add a hard partition, if the only other hard partition is called Default\_HP, the default hard partition is automatically removed.
  - In the Soft Partitions and Memory Assignments window, whenever you add a soft partition, if the only other soft partition is called Default\_SP, the default soft partition is automatically removed.
- Before you can upgrade an ES47, ES80, and GS1280 platform’s firmware, you must unpartition the platform. To do this, you modify the partition map to assign all QBBs to a single partition. When you commit the partition map, APW unpartitions the platform.

## 4.2 Working with Partition Maps

When you invoke APW, the Current Partition Map for the selected platform is displayed (Figure 4-3). A warning message alerts you if the console for the selected platform is in use.

Selecting Resources... from the Current Partition Map brings up a new window that provides a graphical view of the Dual Processor Modules (duos) or Quad Building Blocks (QBB) assigned to each partition and displays information about them. In some cases, the duo shown may contain a duo filler module or may represent an empty duo slot. Figure 4-2 and Figure 4-1 show the Resource window for both platforms.

You move from the Current Partition Map window to the Work with Partition Maps (Figure 4-4) window, where you chose whether to modify an existing map or create a new one.

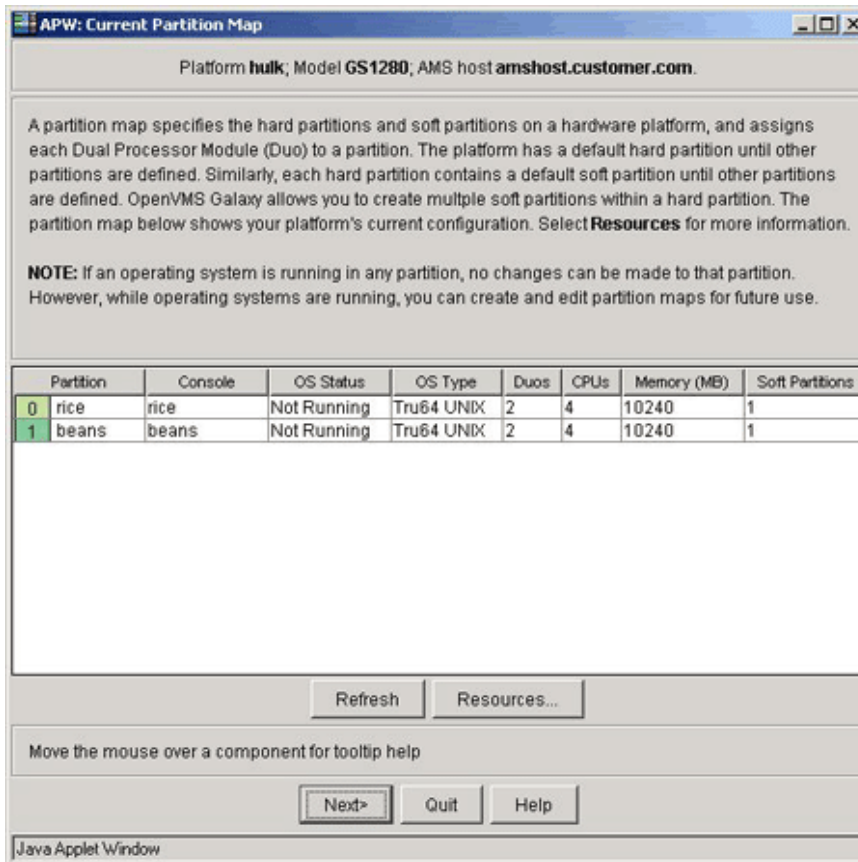
From within the Create or Modify a Partition Map (Figure 4-5) you can validate the configuration you selected, save your partition map to a file, and apply the map to your system.

The following sections describe the Current Partition Map window, the Resources window, the Work with Partition Maps window, and the Create or Modify a Partition Map.

### 4.2.1 The Current Partition Map Window

The Current Partition Map window (Figure 4-3) provides information about the partitions on the platform you selected. It is the starting point for using the AlphaServer Partition Wizard.

**Figure 4-3: Current Partition Map**



The display fields for partitions in the Current Partition Map window are as follows:

- **Partition**  
Lists the number assigned to the platform, with number 0 assigned to the first partition. A U indicates that the partition is unassigned. It also contains a color legend to correlate with the graphical representation of the platform.  
For ES47, ES80, and GS1280 platforms, the name of the partition appears here. (GS80, GS160, and GS320GS80, GS160, and GS320 platforms do not have names.)
- **Console**  
Lists the console for the partition.
- **OS Status**  
The operating system status in this column can be one of the following:
  - **Running**  
An operating system is running in this partition.
  - **Not Running**  
The SRM firmware is running.
  - **Powered Off**  
The partition is powered off.
  - **Faulted**  
There is a fault.
  - **Unknown**

The firmware reports the partition is powered on and has no faults, but APW was unable to discover whether the OS is running for one of the following reasons:

- The console name for one of the soft partitions within the partition is not configured.
  - The console daemon, `cmfd`, is not running.
  - The console is in use or inaccessible
  - The console is not responding
- OS Type  
Shows the operating system for this partition. This is set in the Add or Modify Hard Partition screen and can be Tru64 UNIX, OpenVMS, OpenVMS Galaxy, Linux, or Unknown.
  - Duos or QBBs  
Shows the number of Dual Processor Modules or Quad Building Blocks in the hard partition.
  - CPUs  
Shows the number of CPUs. This number may include faulted CPUs.
  - Memory (MB)  
Shows the amount of memory (in megabytes).  
For GS80, GS160, and GS320 platforms, this field may be listed as Unknown if the SPM firmware is not running and the data is not cached.
  - Soft Partitions  
The number of soft partitions in this hard partition.

You can cause the APW to rediscover the partitions and update platform information by selecting the Refresh Button.

## 4.2.2 The Resources Window

The Resources window (Figure 4-2 and Figure 4-1) provides a graphical view of the Dual Processor Module (duo) or Quad Building Block (QBB) assigned to each partition and displays information about them. You launch this window from the Current Partition Map and can keep it on your desktop as you move through the partition wizard. As you modify a partition map, the changes are reflected in the Resources window.

Each box at the top of the Resources window represents a duo or QBB, with a color representing the hard partition for that slot. The duo slot may contain a duo or a filler module, or it may be empty. A smaller box in the upper left corner displays the number assigned to the partition, with number 0 assigned to the first partition. A U indicates that the duo is unassigned.

The area below the duo grid displays information about the selected duo slot. You select a duo or QBB by moving to it via the mouse, the tab key, or the arrow keys and clicking on it. Selecting a duo or QBB shows the following information:

- The names of the hard partition and soft partition
- The location of the duo by cabinet, drawer, and slot
- A Partition Legend, which displays the number and color assigned to the partition

The columns of the Resources area of the window contain the following fields:

- Resource

Shows the CPUs physically located on that duo.

- Status

Shows the status of the CPU, which can be one of the following:

- Okay

The CPU is present and functioning.

- Powered Off

The CPU is present but powered off.

- Failed

The CPU is present, but is returning an error status. It may be powered on or off.

- Empty

The duo slot is empty.

- Filler

The slot contains a filler module.

- Memory

The amount of memory (in megabytes) physically located with that CPU on the duo.

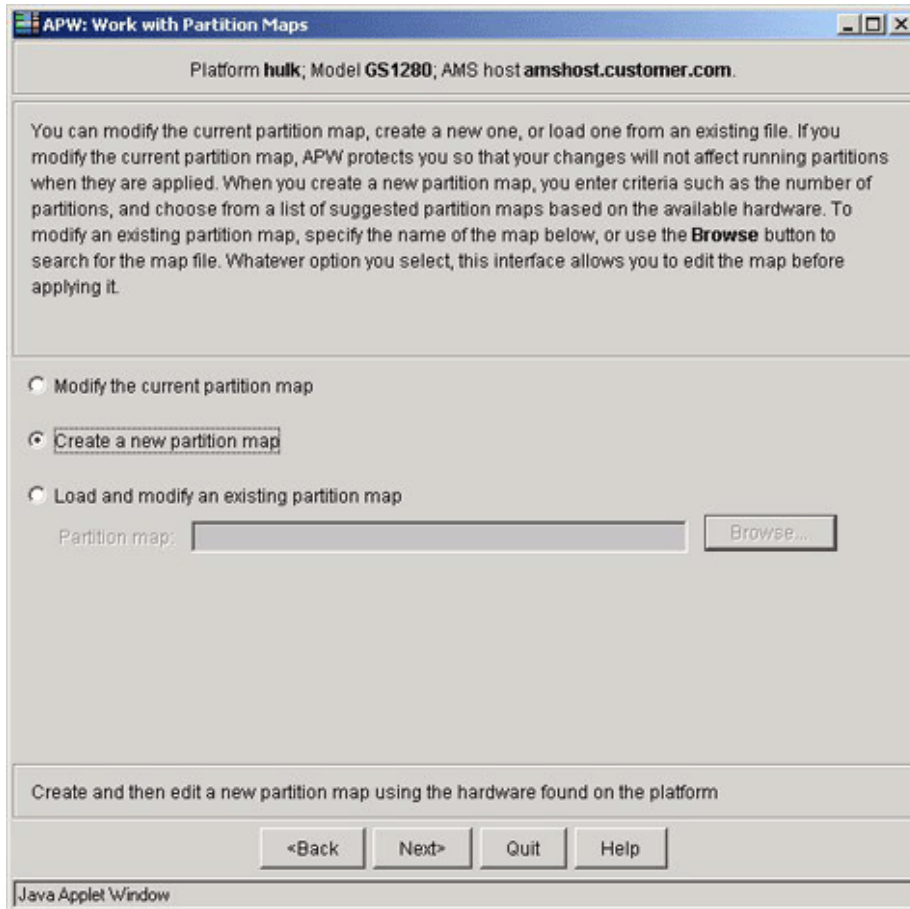
- Connected I/O

Shows the I/O drawer connected to that partition or show that no I/O drawer is connected.

### **4.2.3 The Work with Partition Maps Window**

From the Current Partition Map window, select Next to bring up the Work with Partition Maps window (Figure 4-4).

**Figure 4-4: Work with Partition Maps Window**



In this window, you can perform one of the following actions:

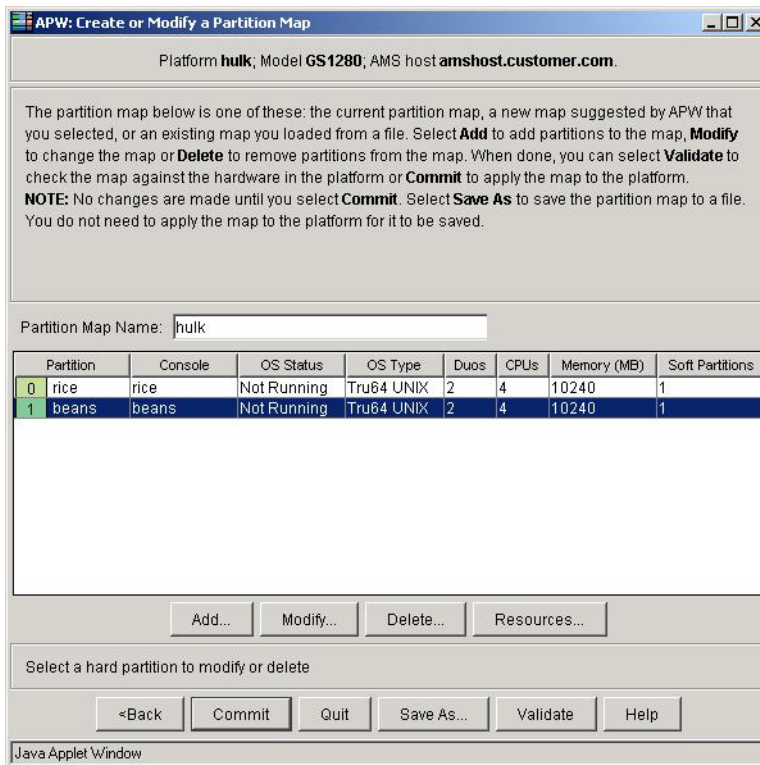
- Modify the current partition map.
- Create a new partition map  
Lets you set certain parameters, such as number of hard partitions and distribution of CPUs. The APW creates a map based on those parameters. You can then accept the suggested map or modify it. The create a new map option is most often used with new platforms.
- Load and modify an existing partition map. You can do this by typing in the name of an existing map or by selecting the Browse button to search for one. You can create multiple partition maps in order to meet different needs in your computing environment.

After choosing the task you want to perform, press Next. The next window you see depends upon whether you selected to modify the current partition window or create a new one.

#### **4.2.4 The Create or Modify a Partition Map Window**

You see the Create or Modify a Partition Map window (Figure 4-5) when you modify the current partition map or load an existing one.

**Figure 4-5: Create or Modify a Partition Map Window**



From this window, you can add, modify, or delete a partition, and bring up the Resources window. The following buttons are also on this window:

- **Back**  
Returns you to the previous window.
- **Commit**  
Applies the partition map to the platform. (See Section 4.5.3.)
- **Validate**  
Validates the partition map. (See Section 4.5.2.)
- **Quit**  
Leaves the APW program, discarding any information you provided.
- **Save As...**  
Allows you to save the partition map. (See Section 4.5.1.)
- **Help**  
Provides online help for the APW program.

### 4.3 Modifying a Partition Map

If you choose to modify the current partition, click on the Modify the current partition map radio button and click Next. This will bring up the Create or Modify a Partition window (see Section 4.2.4), which contains a list of your current partitions.

Partitions running an operating system are disabled if you choose to modify the current partition map. Choose Modify the current partition map if:

- You want to start with the present configuration of the hardware.
- You want APW to protect you from making changes that cannot be committed because of a running operating system.

From this window you can choose to add new partitions, modify existing partitions, or delete partitions.

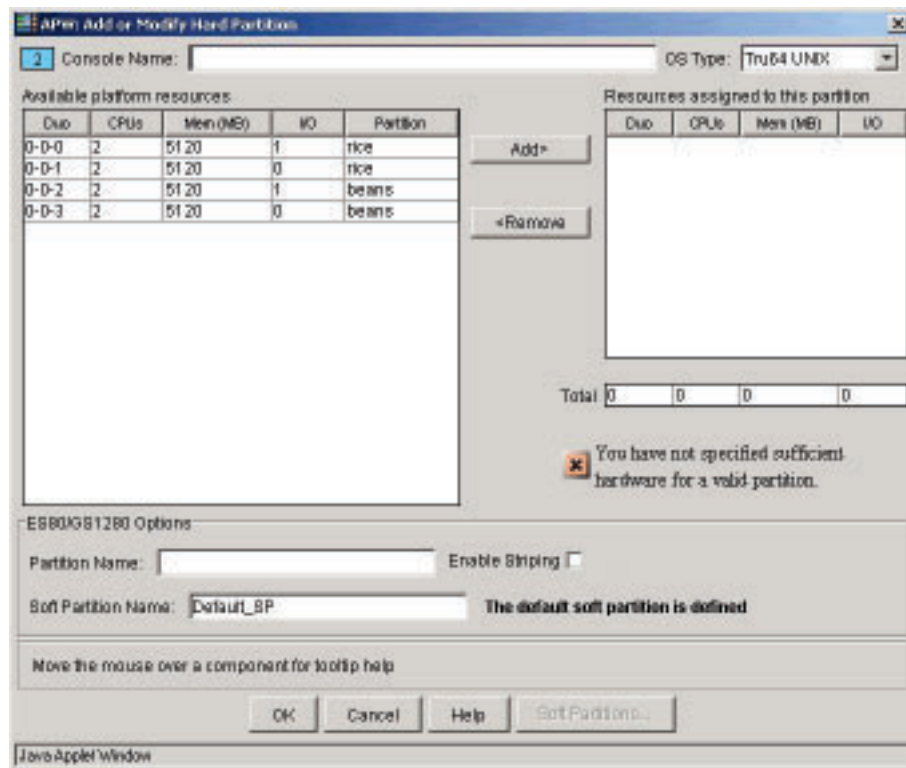
- To add a partition, select Add... This brings up the Add or Modify Hard Partition window, with the existing hard partitions listed in the box on the left (Figure 4-6).
- To modify a partition, select the partition you want to modify by highlighting it and then select Modify... This brings up the Add or Modify Hard Partition window, with the resources of the partition you want to modify listed in the box on the right (Figure 4-7), and the resources for all other partitions on this platform listed in the box on the left.
- To delete a partition, select the partition you want to delete by highlighting it and then select Delete... You will be asked to confirm this action.

None of the changes you make take effect until you commit them. (See Section 4.5.)

### 4.3.1 Adding a Hard Partition

When you add a hard partition, you must select the duos or QBBs that will be assigned to the partition. You can select a duo or duo filler even if it is currently assigned to another partition. (Figure 4-6).

**Figure 4-6: Add a Partition**



You add a partition as follows:

1. In the box on the left, select the resources that you want to move to a new partition. You do this by highlighting a duo or QBB and clicking on Add.
2. Continue moving duos or QBBs from the left box to the right until you have the configuration you want.
3. Look at the icon below the right-hand box. An X icon indicates a problem with your proposed partition. The problem is described as follows:
  - This partition is not valid in the mesh.



Tells you that the duos or QBBs you selected do not conform to the configuration requirements of your ES47, ES80, and GS1280.

- You have not specified sufficient hardware for a valid partition.

Tells you that you need to select additional duos or QBBs to meet the minimum hardware requirements for a partition. Each partition needs at least one CPU (duos contain two CPUs by default) and a connection to an I/O Drawer.

Select different duos or QBBs by using the Add and Remove buttons until the icon turns to a check mark and says “The hardware requirements for a valid partition have been met.”

4. Type in a console name for the partition.
5. Select the operating system that will run on the partition.

For ES47, ES80, and GS1280 platforms only:

6. Type in a name for the partition. This will enable the firmware to identify the partition.
7. Depending upon your system needs, you can use the following optional characteristics:
  - Click in the Enable Striping box to stripe memory access across each CPU within a duo. This helps smooth out Nonuniform Memory Access (NUMA) memory latency differences.
  - Provide a name for the first soft partition. This will enable the firmware to identify the soft partition. The default name is Default\_SP.

If the operating system running on this partition is OpenVMS Galaxy, the Soft Partitions... button at the bottom of the window is active. You can click on it to create additional soft partitions. See Section 4.3.3 for more information.

For ES47/ES80/GS1280 and GS80/GS160/GS320 platforms:

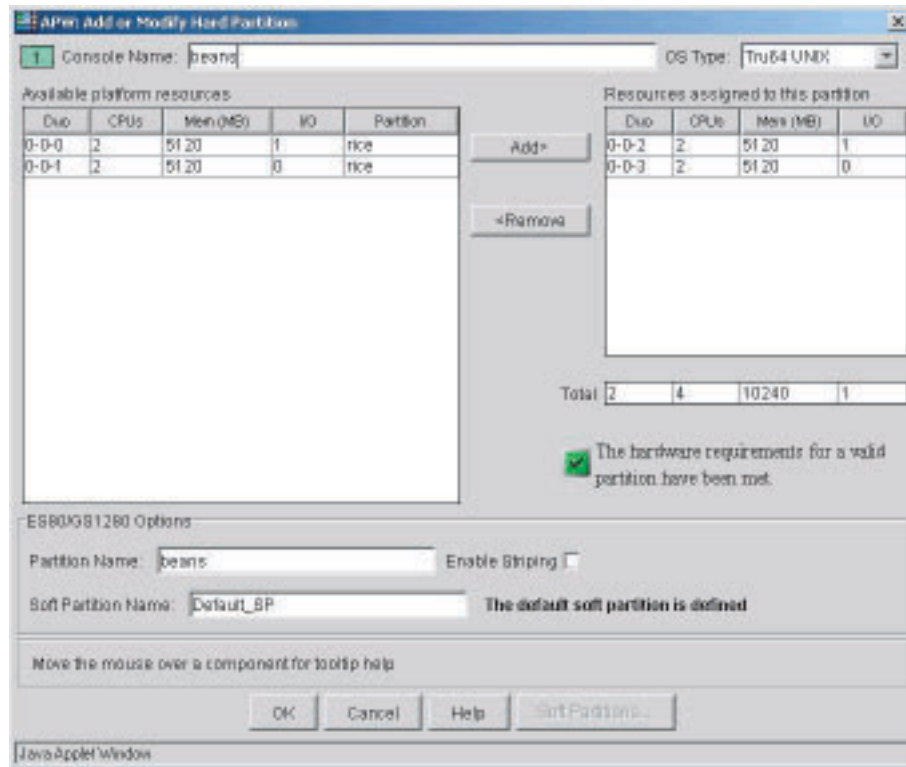
8. Select OK to return to the Add or Modify a Partition Map window.
9. See Section 4.5 for information about validating, saving, and committing a partition map. See Section 4.3.2 if you want to make changes to the partition you added.

Remember that when you are moving resources out of and into the left-hand box, you are modifying the platform's other partitions. You can see those changes in the Resources window, but they are not reflected by the use of the X and check mark icons below the right-hand box.

### 4.3.2 Modifying a Partition

To modify a partition, select the partition you want to modify by highlighting it and then click on the Modify... button to bring up the Add or Modify Hard Partition window (Figure 4-7). In this window, the resources of the partition you want to modify are listed in the box on the right, and the resources for all other partitions on this platform are listed in the box on the left.

**Figure 4-7: Modify a Partition**



Proceed as follows:

1. Using the Add and Remove buttons, move the duos or QBBs into or out of the box on the right until the resources of the selected partition meet your needs.
2. Look at the icon below the right-hand box. An X icon indicates a problem with your proposed partition. The problem is described as follows:

- This partition is not valid in the mesh.

Tells you that the duos or QBBs you selected do not conform to the configuration requirements of your ES47, ES80, and GS1280 platform.

- You have not specified sufficient hardware for a valid partition.

Tells you that the duos or QBBs you selected are missing required components, such as sufficient memory or I/O.

Select different duos or QBBs by using the Add and Remove buttons until the icon turns to a check mark and says “The hardware requirements for a valid partition have been met.”

Remember that when you are moving resources out of and into the left-hand box, you are modifying the platform’s other partitions. You can see those changes in the Resources window, but they are not reflected by the use of the X and check mark icons below the right-hand box.

3. Depending upon your system needs, you can use the following optional characteristics when modifying a ES47, ES80, or GS1280 platform:
  - Click in the Enable Striping box to stripe memory access across each duo in the partition.
  - Provide a name for the first soft partition, which will enable the firmware to identify it. The default name is Default\_SP.  
If the operating system running on this partition is OpenVMS Galaxy, the Soft Partitions... button at the bottom of the window is active. You can

click on it to create additional soft partitions. See Section 4.3.3 for more information.

4. Press OK to return to the Add or Modify a Partition Map window.

See Section 4.5 for information about validating, saving, and committing a partition map. See Section 4.3.2 if you want to make changes to the partition you added.

### 4.3.3 Creating Soft Partitions

Each ES47, ES80, and GS1280 partition has a default soft partition on which the operating system runs. GS80, GS160, and GS320 do not have a default soft partition.

If you are running OpenVMS Galaxy, your partitions can have multiple soft partitions. The procedures for creating and modifying soft partitions are similar to the procedures you follow to create or modify hard partitions.

When you add a soft partition to an ES47, ES80, or GS1280, the default soft partition (Default\_SP) is automatically removed.

The following steps show you how to create two soft partitions from the default soft partition. The steps are similar if the soft partition is not Default\_SP.

1. Highlight the platform you want to work with and open the APW.
2. After APW finishes its discovery stage, the Current Partition Map window is displayed. Click Next. This brings up the Work with Partitions Maps window.
3. Select Modify the current partition map and click Next. This brings up the Create or Modify a Partition Map window.
4. Highlight the hard partition for which you want to create a soft partition and click Modify. This brings up the Add or Modify Hard Partition box.
5. Change OS type to OpenVMS Galaxy. The Soft Partitions... button is made active.
6. Click on the Soft Partitions... button. This brings up the Soft Partitions and Memory Assignment window.
7. Click Add... This brings up the Add or Modify Soft Partition window.
8. Highlight the duos or QBBs you want in the new soft partition and click on Add to move those duos or QBBs to the right-hand box. Continue until you have the resources you want in your soft partition.
9. If the platform is an ES47, ES80, or GS1280, provide a name for the soft partition and for its console.
10. Select OK. This returns you to the Soft Partitions and Memory Assignment window. Notice that you have only one partition. On ES47, ES80, or GS1280 platforms, the Default\_SP is automatically removed.
11. You can assign memory to this partition as follows:
  - a. To assign shared memory to all soft partitions, specify an amount of memory and click on Apply.
  - b. To assign memory to this partition, specify the amount of memory and click on Apply.

The shared and total memory you assign are displayed in the slider bar. The full width of the slider represents the amount of memory available in the hard partition. You can leave some memory unassigned if any soft partition is set to Automatic memory assignment.

---

### Note

---

On the Soft Partitions and Assigned Memory window, the Mem (MB) column shows the amount of memory that is local to duos or QBBs assigned to the soft partition. This amount of memory is available to the soft partition without Non-Uniform Memory Access (NUMA) delays.

The Assigned (MB) column shows the amount of memory assigned to the soft partition. When the column's value is listed as Automatic, the firmware calculates the amount of memory assigned to the soft partition.

For ES47, ES80, and GS1280 platforms, partitions with Automatic assignment display assigned memory as unspecified when viewed at the firmware's MBM command-line interface.

---

12. To add the second soft partition, click on the Add button. Repeat the process, utilizing the hard partition's remaining resources.

## 4.4 Creating a New Partition Map

By choosing to create a new partition map in the Work with Partitions Maps window, you let the APW create a map based on criteria you specify (Figure 4-8).

**Figure 4-8: Partition Map Creation Criteria Window**

APW: Partition Map Creation Criteria

Platform **hulk**; Model **GS1280**; AMS host **amshost.customer.com**.

Enable and disable the creation criteria below to specify the partition map parameters you want in the new map. When you have selected the parameters you want, press the **Next>** button. If the current platform can be partitioned to match your parameters, you will see a suggested partition map. If not, you will see an error message.

There must be  hard partition(s).

Each partition must have at least  CPU(s).

Count slots as well as current CPUs.

Each partition must have at least  MB of memory.

Move the mouse over a component for tooltip help

Java Applet Window

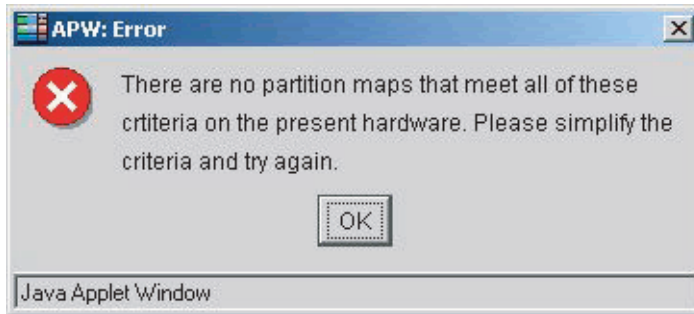
To enable a field in the Partition Map Creation Criteria window, click in that field's check box. The first check box is enabled by default. Specify your criteria as follows:

1. Select the number of partitions you want to create.
2. Specify the minimum number of CPUs that each partition must contain.
3. Specify if you want to count slots as well as current CPUs.

4. Specify the minimum amount of memory in megabytes that each partition must have.

After you have enter the required information and click the Next button, you will either be taken to the Create or Modify a Partition Map window (Figure 4-5) or receive a warning message (Figure 4-9).

**Figure 4-9: Warning Message**



If you receive a warning message, click the Back button to change the criteria you selected.

If a new map was created, you will receive a message alerting you to the need to modify it in order to provide a name for the partition and its console. The Create or Modify a Partition Map window is displayed. Continue as follows:

1. Highlight the first partition and click on Modify... This brings you to the Add or Modify Hard Partition window.
2. Type in a console name where indicated.
3. Type in a partition name where indicated.
4. Save or commit the map for that partition as described in Section 4.5.
5. Repeat the procedure for any other partitions you created.

## 4.5 Saving, Validating, and Committing a Partition Map

You save, validate, and commit a partition map from the Create or Modify a Partition Map window (See Figure 4-5). The following sections describe these operations.

### 4.5.1 Saving a Partition Map

You can have multiple partition maps for the same platforms, thereby providing an easy way to configure your system to meet specific needs.

To save a partition map, do the following:

1. In the Create or Modify a Partition Map screen, click the Save As... button. An information box is displayed.
2. Supply a file name and, optionally, change the location to which the file is saved. Click Save. A message confirms that the file was saved successfully.

The default file extension is `.pmf` (partition management file). The default (and recommended) location is `/usr/opt/ams/maps`. When APW is launched from the AMS Web page, `/usr/opt/ams/maps` is the only location available for saving or loading a partition management file.

## 4.5.2 Validating a Partition Map

Before committing or saving a partition map, you can have it checked for any problems by clicking the Validate button. If the map is problem free, you will see the following message:

- The partition map is valid for this system.

Otherwise, you will see one or more of the following messages:

---

### Note

---

In the following list, *name* represents the name assigned to the partition on ES47, ES80, and GS1280 platforms. Because GS80, GS160, and GS320 platforms do not have names, the number of the platform will appear where *name* is represented.

---

- Warning: Some duos are unassigned.
- Warning: Some QBBs are unassigned.
- Warning: Partition *name* is not valid in the mesh.
- Warning: Partition *name* needs more CPUs, Memory, or I/O.
- Warning: Some resources within partition *name* are unassigned.
- Warning: Soft partition *name* in partition *name* needs more CPUs, Memory, or I/O.
- Warning: This commit affects partitions that could be running an operating system.
- Error: This commit affects running operating systems
- Error: Each partition must have a unique partition name.
- Error: Supply a unique console name for partition *name*.
- Error: Supply a unique console name for soft partition *name* in partition *name*.

The messages you see when validating a partition map will also be displayed when committing a map if you did not fix the problem or if you did not validate the map.

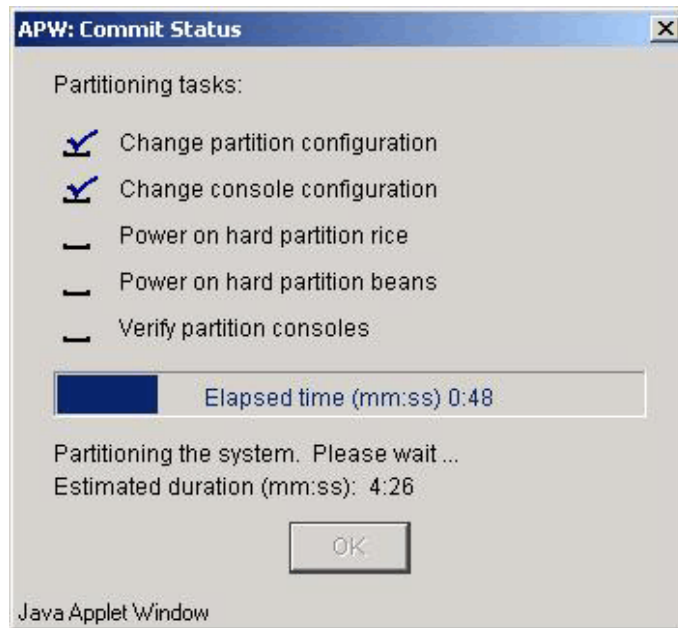
## 4.5.3 Committing a Partition Map

Committing a partition map applies the map to the system. To do so, click the Commit button. If the map has not been saved to a file, a message is displayed asking you to do so.

Before committing the map, APW first validates the configuration. If it finds any of the warnings listed in Section 4.5.2, you are prompted to respond Yes or No on whether you want to commit. If it finds any of the errors, you will be prevented from committing a map.

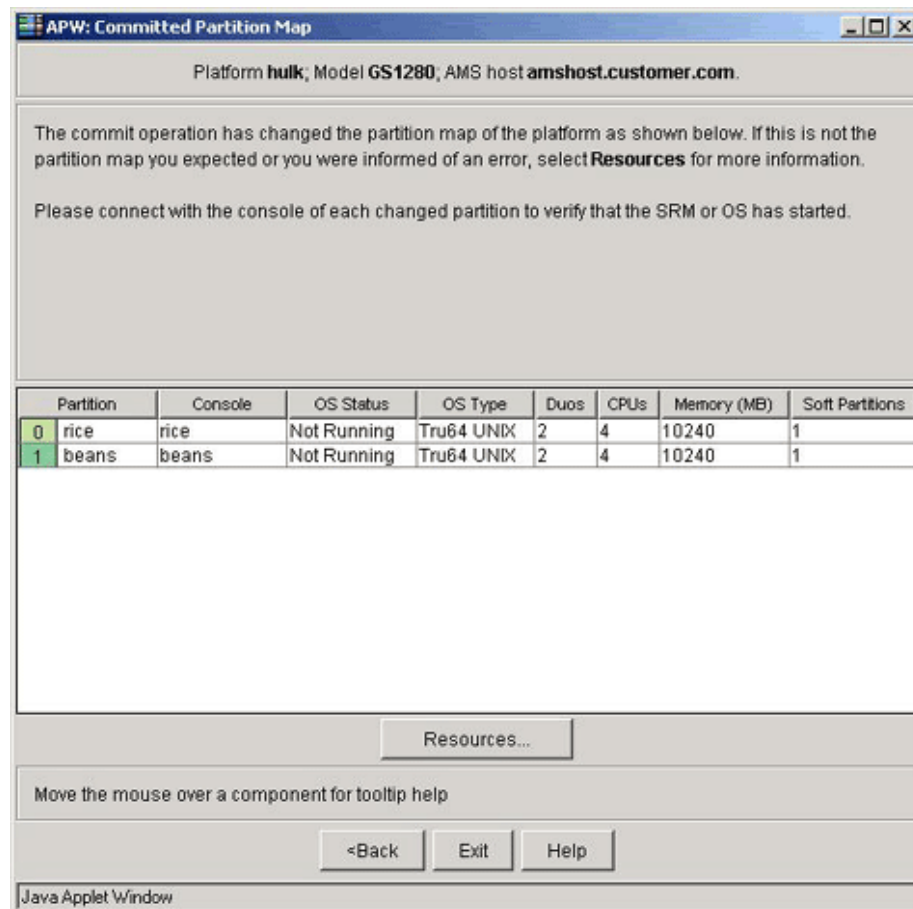
When the commit is accepted, it applies the map to the system and restarts the system. A status box shows the progress of the commit (Figure 4-10) and the commit status is written to the log file. (See Section 4.6.)

**Figure 4-10: Commit Status Window**



After the map is committed, the commit is confirmed with the display of the Committed Partition Map window (Figure 4-11.)

**Figure 4-11: Committed Partition Map Window**



## 4.6 Managing APW Files

APW creates log files and partition map files.

The APW log file contains a record of the transaction information and any errors that occur as the application runs. The file is saved to the folder `/usr/opt/ams/logs`. It creates a new log file for every session, but keeps only the 10 most recent files.

The naming convention for log files is `apwlog-yyyy.mm.dd-s.txt`, where *yyyy* is the year, *mm* the month, *dd* the day of the month, and *s* is the session. For example, if you use APW twice on May 21, 2003, the name of the log file for the second session is `apwlog-2003.05.21-2.txt`.

The information type for each entry is listed in brackets. This is for ease of sorting and processing.

APW partition map files are written to `/usr/opt/ams/maps`. This is done when you select the Save As... button and provide a file name. The default extension is `.pmf`.



## Using the Platform Console Manager

Following a brief overview of the Platform Console Manager (PCM) and the main PCM window in Section 5.1 and Section 5.2, the following topics are discussed:

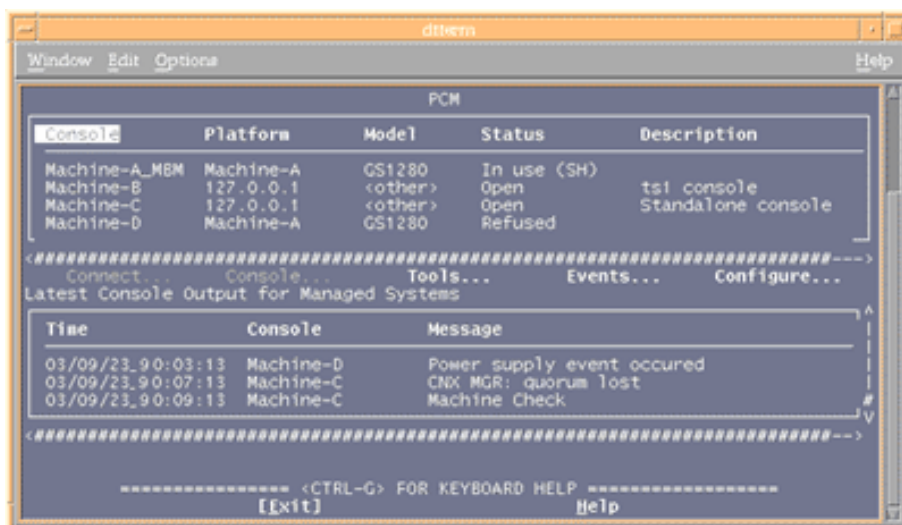
- Adding platforms and consoles to the PCM (Section 5.3).
- Modifying the properties of platforms and consoles managed by PCM (Section 5.4)
- Removing platforms and consoles from the list of managed items (Section 5.5)
- Stopping and restarting the `cmfd` daemon from the PCM (Section 5.6)
- Viewing and modifying the number of days that the `cmfd` daemon logs console output before archiving the log file (Section 5.7)
- Working with events (Section 5.8)
- Connecting to the ES47/ES80/GS1280 and GS80/GS160/GS320 platform management port (Section 5.9)
- Managing consoles Connecting to a system's console (Section 5.10)

### 5.1 Overview

The Platform Console Manager (PCM) is a character-cell application that provides access to the consoles of subpartitions and systems configured in the PCM.

You can use the PCM to connect to the platform's management port, connect to consoles, view the status of each console, and view the console's log files. You can also monitor the latest console output from the managed systems in a continuously updated, timestamped list located in the main PCM window (Figure 5-1).

**Figure 5-1: Main PCM Window**



The Console Management Facility (CMF) daemon `cmfd` provides the PCM access to the consoles and logs console output; it logs all console sessions by default. See `cmfd(8)` for more information.

## 5.1.1 Starting, Navigating, and Exiting the PCM

You must be `root` or a member of the `amsuser` group on the AMS machine to use the PCM.

To start the PCM:

1. Unset your display:

```
# unset DISPLAY
```

2. Start the PCM:

```
# /usr/bin/pcm
```

Press `Ctrl/g` for keyboard navigation help.

Select `Exit` from the main PCM window or press `Ctrl/c` to exit PCM.

## 5.1.2 Customizing the Telnet Escape Sequence

The default Telnet escape sequence is `Ctrl/x`. You can customize the escape sequence of Telnet sessions you launch from the PCM. You can ensure that you choose a unique escape sequence that does not conflict with escape sequences of other applications.

When using the Bourne and Korn shells, configure the Telnet escape sequence and add the following line to the `.profile` file:

```
AMS_SESSION_ESC=^G; export AMS_SESSION_ESC
```

In this example, the Telnet escape sequence is changed to `^G`.

When using the C shell, add the following line to the `.login` file:

```
setenv AMS_SESSION_ESC ^G
```

In this example, the Telnet escape sequence is changed to `^G`.

The PCM displays the configured escape sequence in the top of the Telnet window.

## 5.2 The Main PCM Window

The Main window is launched when you start up PCM. It has three principal sections: a systems view and selection area, buttons to perform various actions, and console message area.

For a guide to navigating the character cell environment, see Appendix G.

### 5.2.1 System View and Selection Area

The system view and selection area displays information you specified when you added a platform or console (see Section 5.3). This information includes the console's name, the name of the platform on which the console is running, the model number of the platform, and a description of the system. Also included is a status column, which displays one of the following:

- **Open** — `cmfd` has a connection to the console.
- **In use (RO)** — All the users connected to the console are in Read-Only mode.
- **In use (SH)** — At least one user is connected in Shared mode. Other users may be connected in Shared or Read-Only modes.

In this mode, users with shared connections can all make changes that affect the work of other shared-connection users.

- **In Use (EX)** — One user is connected in Exclusive mode. Other users may be connected in Read-Only mode. A connection as Shared is not possible.

- Inaccessible — The platform or network is down.
- Refused — The port is in use, external to `cmfd`.
- Disabled — The console is disabled.
- Unknown — An internal error has occurred. Often, this status occurs because the `cmfd` daemon is not running.

Select any column heading to sort by that field. For instance, to sort the systems by platform, select the Platform column heading, and the managed systems will be sorted alphabetically by platform.

## 5.2.2 Buttons

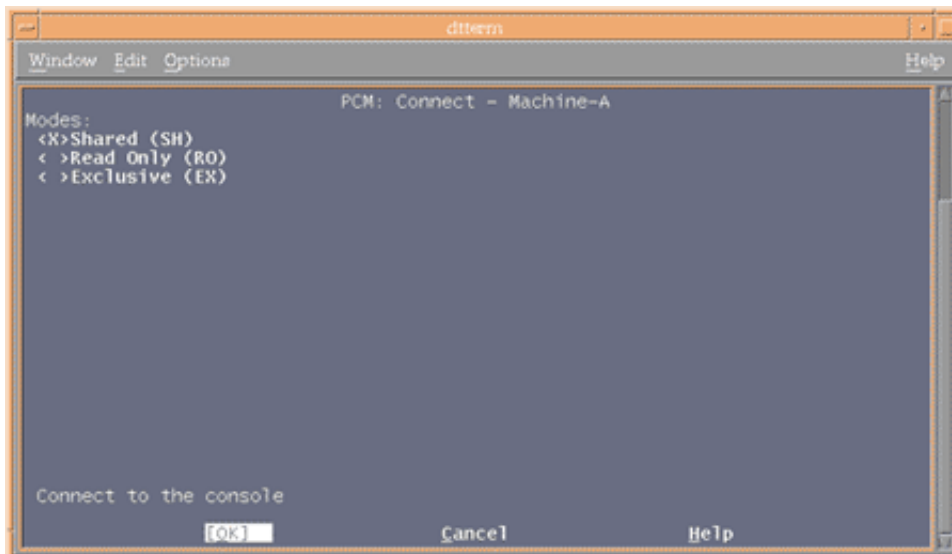
When you select the Connect..., Console..., Tools..., Events..., or Configure... buttons in the Main window, you open a new window in which you can perform various actions. Selecting OK in any of those windows returns you to the Main window. A description of the button actions follows.

### Connect...

Selecting Connect... lets you choose the type of connection you want to make to the selected system:

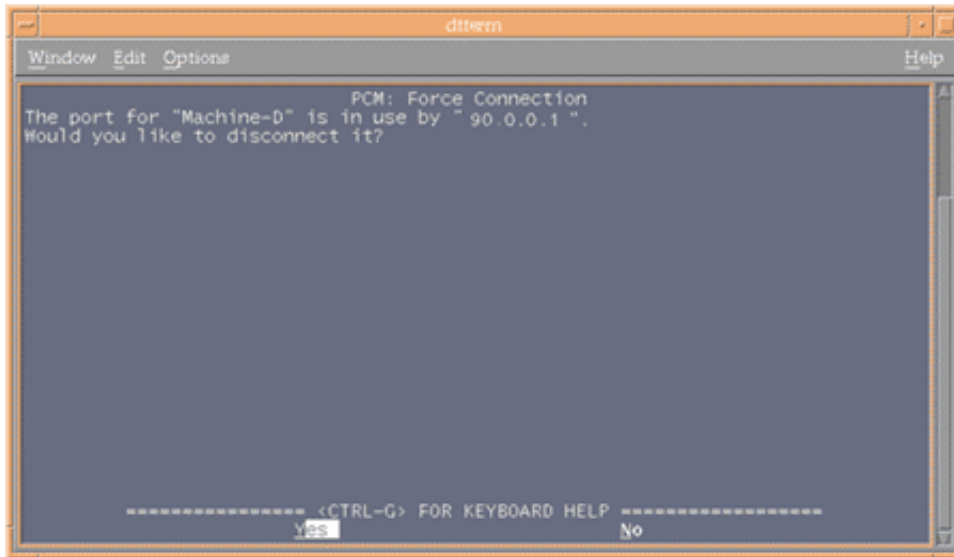
- Read-only mode  
Allows you to see console output, but not to send input to it.
- Shared mode (the default)  
Allows you to see console output and send input to it. The input and output of connections is shown in all open console windows.
- Exclusive mode  
Allows you to take complete control of the console, preventing other users to connect using share or exclusive modes. Read-only connections are allowed.

**Figure 5-2: Connect Dialog Box**



If the selected system is on an ES47, ES80, and GS1280 series platform and its status is REFUSED, a force connection dialog box will appear. Force connection allows you to disconnect the external user connected to the port. To disconnect the external user select Yes, otherwise, select No to terminate the connection attempt.

**Figure 5-3: Force Connection Dialog Box**



Select the type of connection you want and then press OK.

If an error occurs, for example, you request a shared connection when a user is connected in exclusive mode, a new window displays the error.

### **Console...**

Selecting Console... lets you do one of the following:

- View the console log (the default action).
- View/Disconnect Users

Selecting this option (see Figure 5-24) brings up a window that lists the users, their IP addresses, and their connection mode. This window is refreshed every 30 seconds.

The Disconnect All option disconnects all the users connected to the console. Once the users are disconnected, the window is refreshed to show any connected user. Selecting OK closes this window and returns you to the main window.

- Send a message to users on the console. The message is limited to 160 characters.

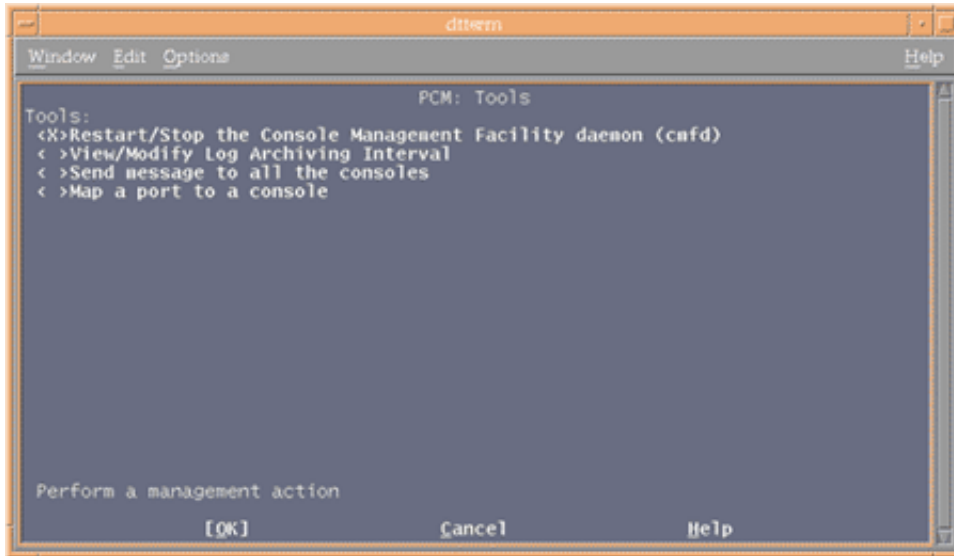
Selecting this option brings up a new window in which you can send a message to users. Selecting OK in that window brings up a window that displays a success message or an error message (for example, a message that exceeds the 160 character limit). Selecting OK returns you to the Send Message window, where selecting OK returns you to the Main window. The Send Message window is also available from the Tools... menu.

- Disconnect users from the console.

Selecting this window brings up a new window in which you can disconnect all or specific users from the console. This includes users who are connected in Exclusive mode.

## Tools...

Figure 5-4: Tools Dialog Box



Selecting Tools... lets you do one of the following:

- Restart/Stop `cmfd` (see Section 5.6.1 for more details).
- View/Modify log archiving interval

Selecting this option lets you specify the number of days before log files are archived. By default, the `cmfd` daemon logs console output for seven days and then archives the file.

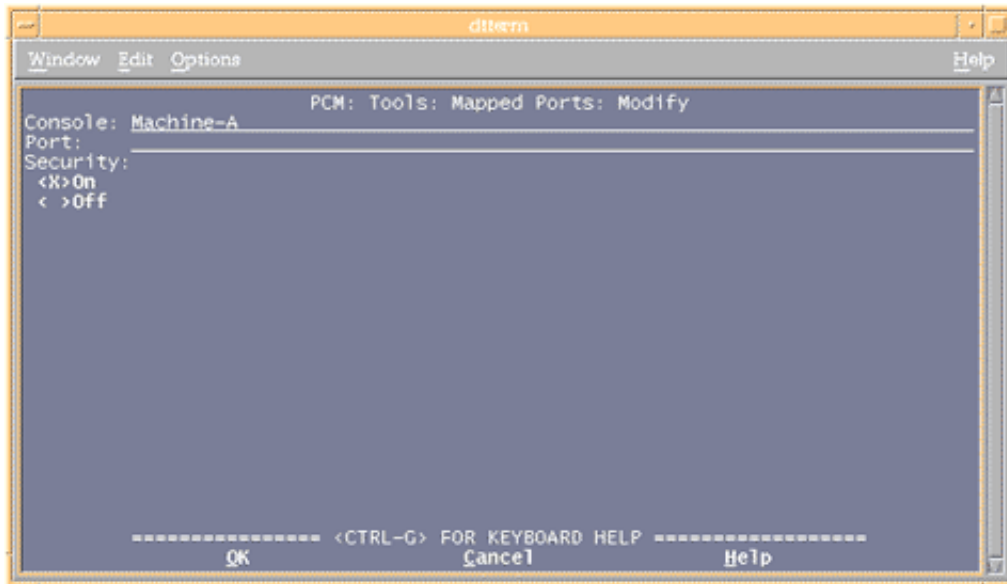
- Send a message to all consoles.

This option acts the same as the Send Message option in the Console... menu.

- Map a console to a port on the local host.

Selecting this option brings up a window that lists all the configured consoles and the port on the local host that are mapped to them. To assign or modify a port on the local host to a console, select the console in the list and press Modify button. This brings up a new window in which you can assign a port on the local host to that console and also specify whether authentication is required for the clients that connect to this port. You select OK to complete the process.

**Figure 5-5: Modify Mapped Port Dialog Box**



### Events...

Selecting Events... lets you do the following:

- View events.
- Create a new event file.
- Modify an existing event file.
- Delete an event file.

See Section 5.8 for more details.

### Configure...

Selecting Configure... lets you do the following:

- Add a platform or console (see Section 5.3).
- Modify a selected item (see Section 5.4).
- Delete a selected item from the list of managed systems (see Section 5.5).

## 5.2.3 Console Output

In the bottom of the Main window, you can view a consolidated log file for all managed systems. The time stamp uses the format *yy/mm/dd\_hh:mm:ss* (Year/Month/Day\_Hours:Minutes:Seconds). Select any column heading (Time, System, or Message) to sort by that field.

The PCM displays the console log files that were generated during the past seven days. To view older log files, you must view them in the `/usr/opt/ams/logs` directory within a terminal window.

## 5.3 Adding a Platform or Console

The steps for adding a platform or a console to the PCM are similar. The main difference is in the data you supply to the Add Platform and Add Console dialog boxes.

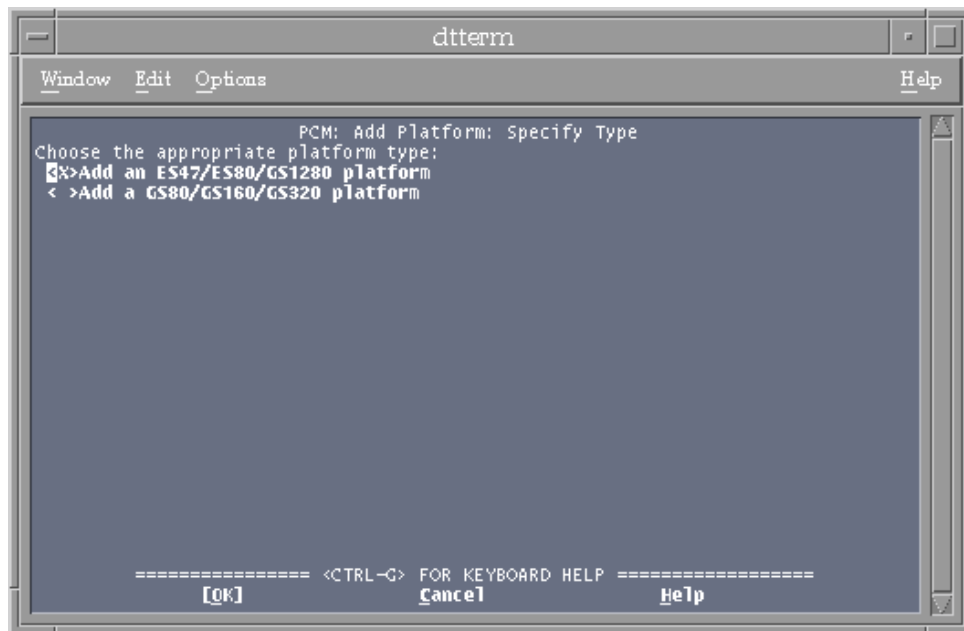
### 5.3.1 Adding a Platform

To manage a platform from the PCM, you add it to the PCM's list of managed systems. When you add a platform, the changes are dynamically updated in the PCM's main window. Once you add a platform, you can connect to the management port of the platform and view the console's log.

To add a platform to the PCM:

1. Select Configure....
2. Select Add Platform.
3. Select OK. The Add Platform: Specify Type dialog box is displayed (Figure 5-6).

**Figure 5-6: Add Platform: Specify Type Window**

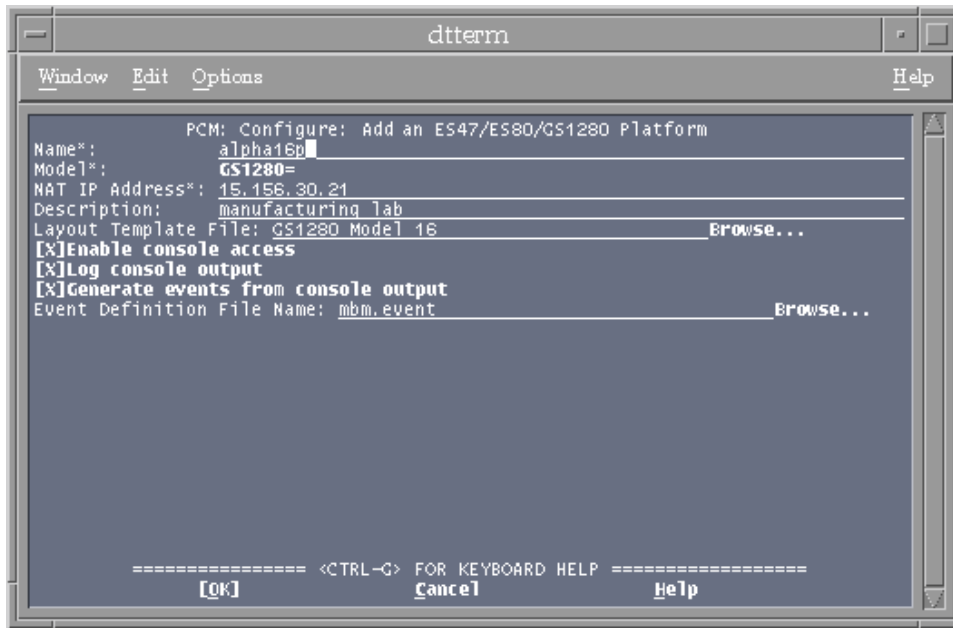


4. Choose your platform type, either ES47, ES80, and GS1280 or GS80, GS160, and GS320. The next dialog box you see depends on the platform you chose.

#### 5.3.1.1 Add an ES47, ES80, and GS1280 Platform

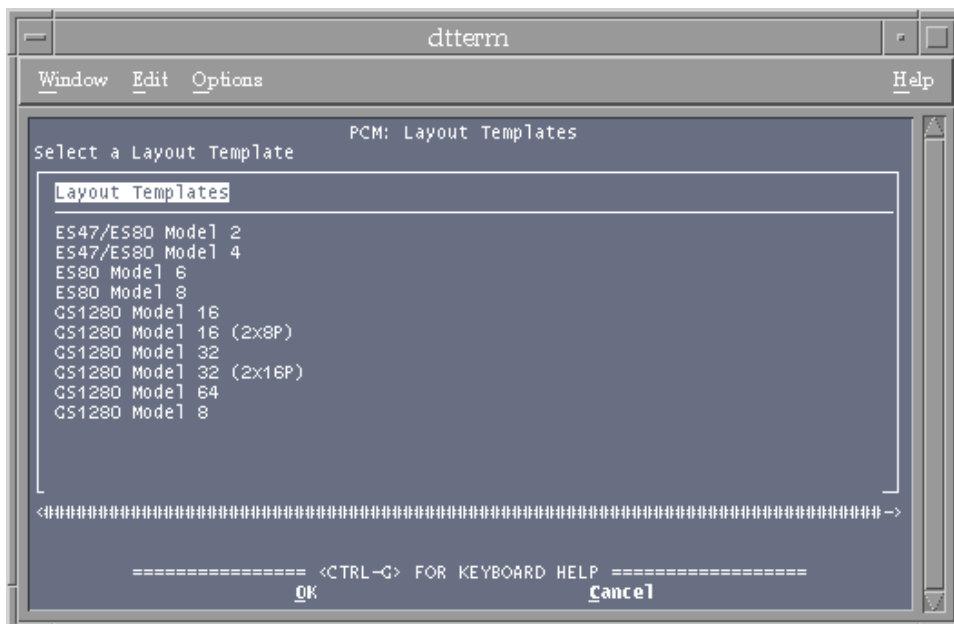
Figure 5-7 shows the dialog box for adding an ES47, ES80, or GS1280 platform. A description of the fields in that dialog box follows.

**Figure 5-7: Add an ES47, ES80, and GS1280 Platform Window**



1. Enter the name of the platform to be managed.
2. Select the model from the dropdown list.
3. Enter the IP address of the Nat box to which the system's console is connected.
4. Provide a description of the platform.
5. Select a Layout Template File by typing one in the field or by selecting one from the Select a Layout Template window (Figure 5-8) that you bring up by selecting the Browse... button.

**Figure 5-8: Layout Template Selection Window**



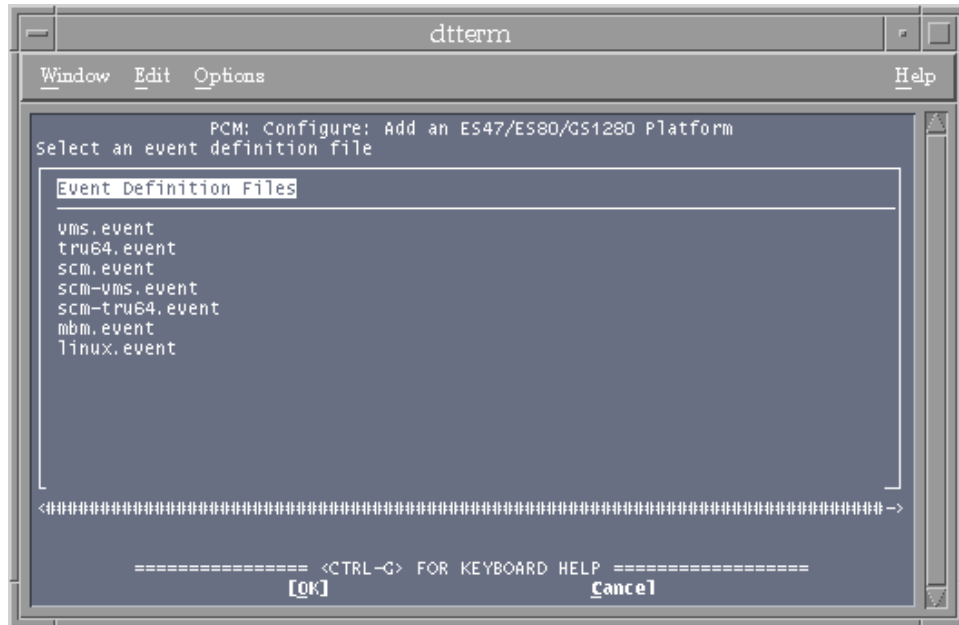
6. Enable or disable Console access.  
If you disable console access, the logging of console output and generation of events from the console output will also be disabled.
7. Enable or disable Log console output.



If you disable the logging of console output, the generation of events from the console output will also be disabled.

8. Enable or disable Generate events from the console output.
9. Enter a name for an event definition file or select the Browse... button to bring up a selection of names to choose from in the Select an event definition file window (Figure 5-9).

**Figure 5-9: Select an Event Definition File Window**



10. Select OK.

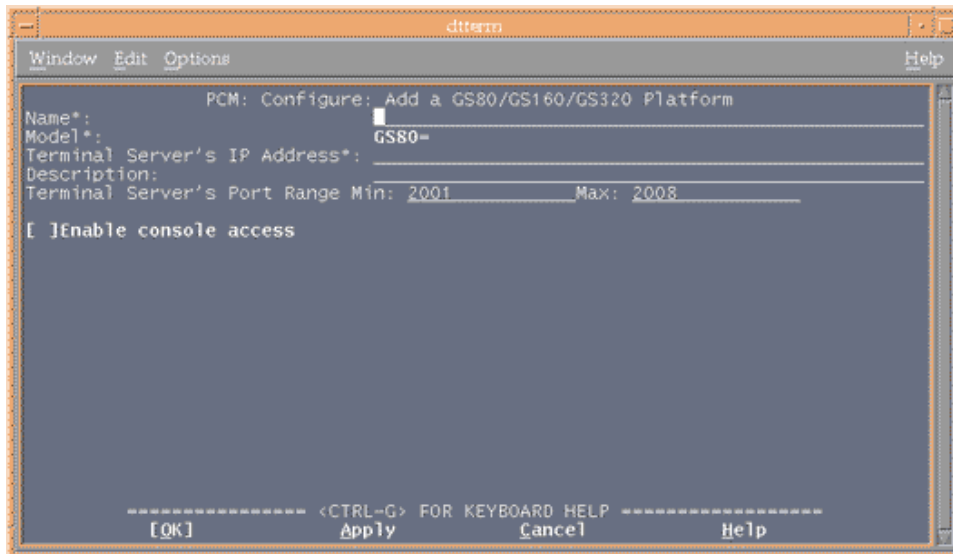
The PCM's main window is displayed and the new platform is now included in the list of managed systems. The MBM console output of the new platform is included in the consolidated console log displayed in the PCM's main window.

If the change does not register in the PCM's display within a few minutes, there may be a problem with the `cmfd` daemon. Restart the `cmfd` daemon from the PCM Tools menu. See Section 5.6.1 for more information.

### 5.3.1.2 GS80, GS160, and GS320 Platforms

Figure 5-10 shows the dialog box for adding an GS80, GS160, or GS320 platform. A description of the fields in that dialog box follows.

**Figure 5-10: Add a GS80, GS160, and GS320 Platform**



1. Enter the name of the platform to be managed.
2. Select the model from the dropdown list.
3. Enter the IP address of the terminal server.
4. Provide a description of the platform.
5. Specify a port range by entering a minimum port number and a maximum port number.
6. Enable or disable Console access.  
If you disable console access, users will be unable to Telnet to the terminal server.
7. Select OK.

The PCM's main window is displayed and the new platform is now included in the list of managed platforms.

If the change does not register in the PCM's display within a few minutes, there may be a problem with the `cmfd` daemon. Restart the `cmfd` daemon from the PCM Tools menu. See Section 5.6.1 for more information.

### 5.3.2 Adding a Console

To manage a console from the PCM, you add it to the PCM's list of managed systems. You can add a console that is on an AlphaServer Management Station (AMS) platform or add a standalone console. Each console represents a name for a port on a subpartition to which you can connect via `cmfd`, which logs the console's output and scans the output for events.

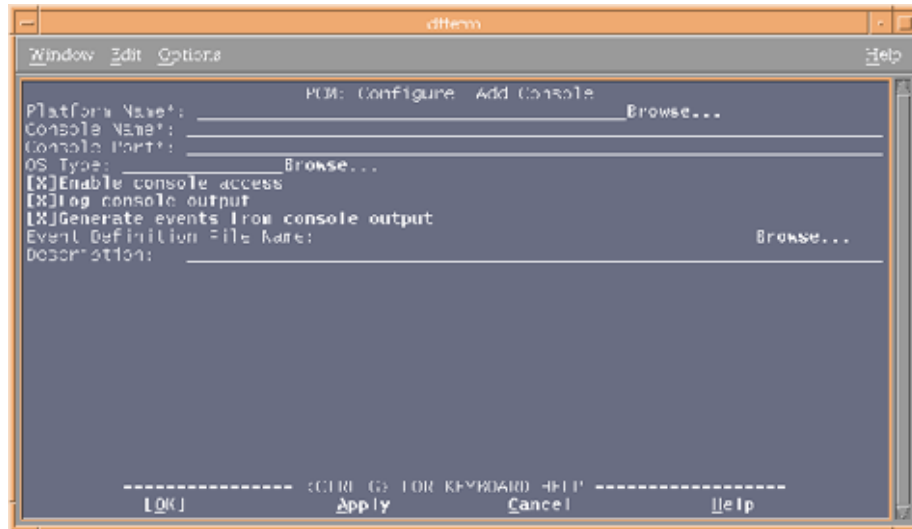
To add a console to the PCM:

1. Select Configure....
2. In the Configure dialog box, select Add Console.
3. Select OK. The Specify Type dialog box is displayed.
4. Select the type of console you want to add — an AMS platform console or a standalone console.
5. Select OK and continue with the procedure for adding the AMS platform console or a standalone console, as applicable.

### 5.3.2.1 Adding an AMS Platform Console

Figure 5-11 shows the dialog box for adding a platform console. The steps that follow describe the fields in that dialog box.

**Figure 5-11: Add a Console Dialog Box**



1. Enter the name of the platform or browse from the list of available platforms.
2. Enter a name for the console.
3. Enter the port number for the console.
4. Enter the operating system (OS) type that will run on the console or browse from the list of supported OS types.
5. Enable or disable the following options. By default, these options are enabled:
  - a. Enable console access.  
If you disable console access, you will not be able to connect to the console. The logging of console output and generation of events from the console output will also be disabled.
  - b. Log console output.  
If you disable the logging of console output, the generation of events from the console output will also be disabled.
  - c. Generate events from the console output.
6. Enter a name for an event definition file or browse from a selection of names.
7. Enter a description (for example, production system).
8. Select OK

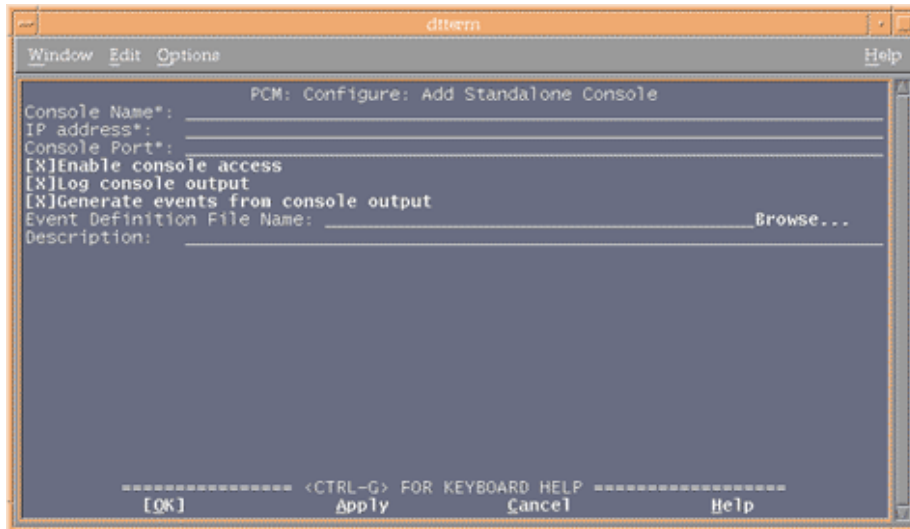
The PCM's main window is displayed and the new console is now included in the list of managed systems.

If the change does not register in the PCM's display within a few minutes, there may be a problem with the `cmfd` daemon. Restart the `cmfd` daemon from the PCM Tools menu. See Section 5.6.1 for more information.

### 5.3.2.2 Adding a Standalone Console

Figure 5-12 shows the dialog box for adding a standalone console. The steps that follow describe the fields in that dialog box.

**Figure 5-12: Add a Standalone Console Dialog Box**



1. Enter a name for the console.
2. Enter the IP Address for the terminal server (or other device) to which the console is connected.
3. Enter the port number for the console.
4. Enable or disable the following options. By default, these options are enabled:
  - a. Enable console access.  
If you disable console access, you will not be able to connect to the console. The logging of console output and generation of events from the console output will also be disabled.
  - b. Log console output.  
If you disable the logging of console output, the generation of events from the console output will also be disabled.
  - c. Generate events from the console output.
5. Enter a name for an event definition file or browse from a selection of names.
6. Enter a description (for example, production system).
7. Select OK

The PCM's main window is displayed and the new console is now included in the list of managed systems.

If the change does not register in the PCM's display within a few minutes, there may be a problem with the `cmfd` daemon. Restart the `cmfd` daemon from the PCM Tools menu. See Section 5.6.1 for more information.

## 5.4 Modifying Platform and Console Properties

When you modify a platform or console (either an AMS platform console or a standalone console), the `cmfd` daemon restarts automatically and the changes are dynamically updated in the PCM's main window.

The modification process is the same for platforms and consoles and the dialog boxes are similar to those for adding platforms and consoles.

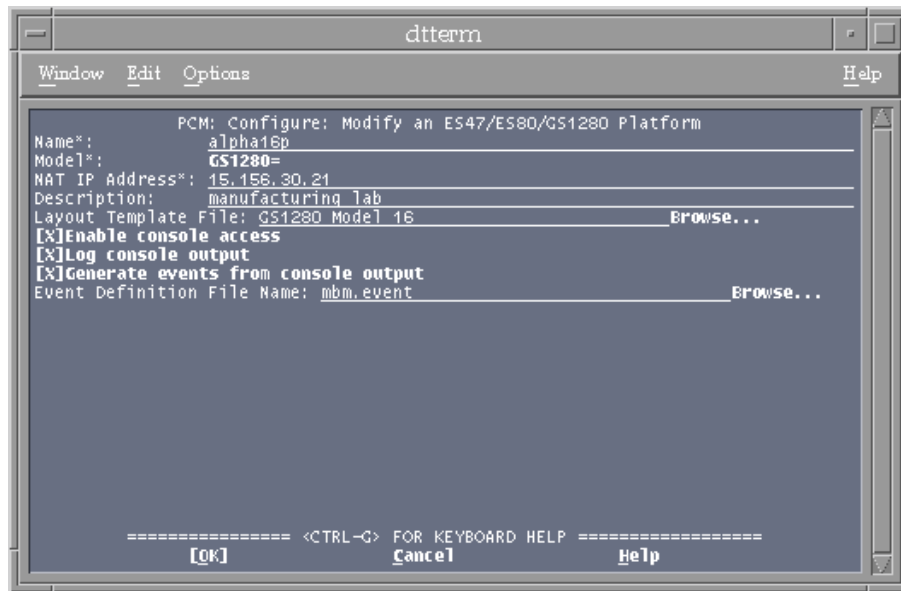
To modify a platform or console configured in the PCM:

1. Select the platform or console you want to modify.

2. Select Configure....
3. Select Modify the selected item.
4. Select OK.

The Modify Platform or Modify Console dialog box is displayed. This dialog box displays the same information you entered when you created the platform or console. For example, the Modify an ES47, ES80, and GS1280 Platform dialog box in Figure 5-13 contains the same information that was entered in Figure 5-7.

**Figure 5-13: Modify a Platform Dialog Box**



5. Modify the data you want (all fields must remain filled). See Section 5.3.1 and Section 5.3.2 for descriptions of the data fields you can modify.
6. Select OK.

The PCM applies the new properties to the system and the PCM's main window is displayed.

If the change does not register in the PCM's display within a few minutes, there may be a problem with the `cmfd` daemon. Restart the `cmfd` daemon from the PCM Tools menu. See Section 5.6.1 for more information.

## 5.5 Removing a Platform or Console

When you remove a platform or console, the `cmfd` daemon restarts automatically and the changes are dynamically updated in the PCM's main window.

To remove a platform or console from the PCM:

1. Select the platform or console you want to delete.
2. Select Configure....
3. Select Delete the selected item.
4. Select OK.

A dialog box with the properties of the platform and console is displayed.

5. Select OK to remove the selected platform or console.

The PCM's main window is displayed, with the removed platform or console no longer included in the list of managed systems.

If the change does not register in the PCM's display within a few minutes, there may be a problem with the `cmfd` daemon. Restart the `cmfd` daemon from the PCM Tools menu. See Section 5.6.1 for more information.

## 5.6 Restarting and Stopping the `cmfd`

You can restart and stop the `cmfd` directly from the PCM, as described in the following sections.

### 5.6.1 Restarting the `cmfd`

Sometimes a console's status is Unknown or the console is unresponsive. You may be able to correct this problem by restarting the `cmfd` daemon.

Restarting the `cmfd` closes all connections to all consoles. Any unsaved work being done on a console will be lost when that console closes. You should ensure that no one is connected to the consoles before stopping the `cmfd`.

**Figure 5-14: Restarting the `cmfd`**

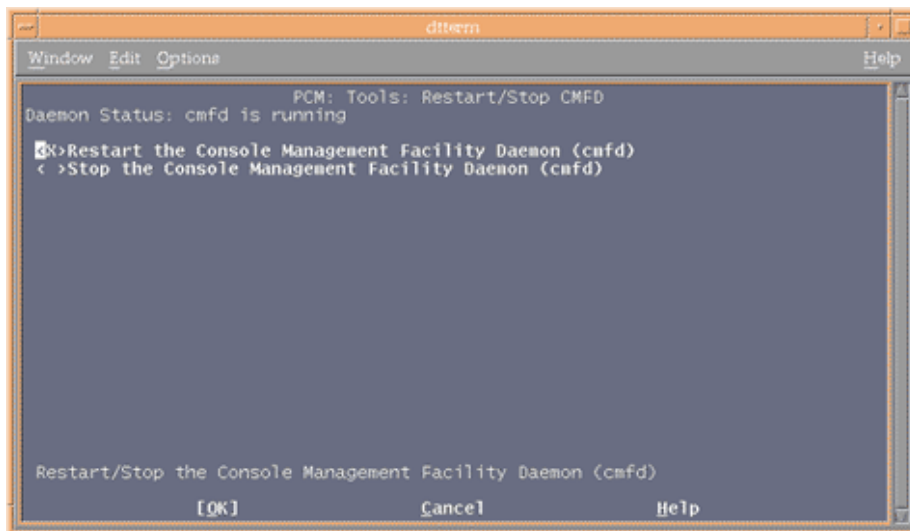


Figure 5-14 shows the PCM Tools menu with the Restart the Console Management Facility daemon (`cmfd`) option displayed.

To restart the `cmfd`:

1. Select Tools...
2. Select Restart/Stop the Console Management Facility daemon (`cmfd`).
3. Select OK.  
This opens the Restart/Stop CMFD dialog box.
4. Select Restart the Console Management Facility Daemon (`cmfd`).
5. Select OK.  
This opens a confirmation dialog box.
6. Select OK.  
The `cmfd` restarts and the PCM's main window is displayed.

### 5.6.2 Stopping the `cmfd`

Stopping the `cmfd` closes all connections to and stops the logging of all consoles. Any unsaved work being done on a console will be lost when that console closes. You should ensure that no one is connected to the consoles before stopping the `cmfd`.

To stop the `cmfd`:

1. Select Tools...
2. Select Reset/Stop the Console Management Facility daemon (`cmfd`).
3. Select OK.

This opens the Restart/Stop CMFD dialog box.

4. Select Stop the Console Management Facility Daemon (`cmfd`).
5. Select OK.

This opens a confirmation dialog box.

6. Select OK.

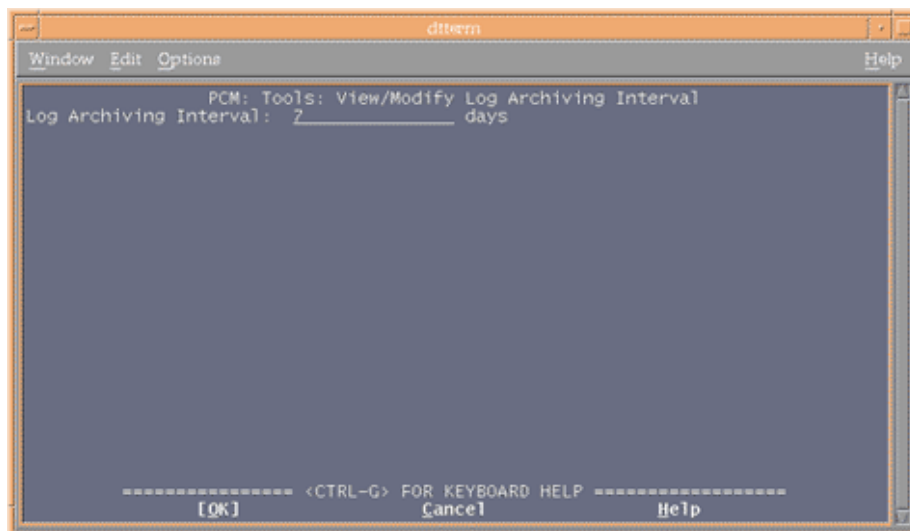
The `cmfd` daemon stops and the PCM's main window is displayed.

The status for all managed consoles changes to Inaccessible.

## 5.7 Setting Log Archiving Interval

The `cmfd` daemon logs console output for specified number of days and then archives the file. You can view the specified archiving interval (which by default is seven days) or modify it as follows:

**Figure 5-15: Set Log Archive Interval Dialog Box**



1. Select Tools...
2. Select View/Modify Log Archiving Interval
3. Select OK.
4. Enter the log archiving interval (in days).
5. Select OK.

The new archiving interval is established and the PCM main window is displayed.

## 5.8 Working with Events

AMS provides event definition files for each supported platform type and its associated console. The files are located in the events directory, `/usr/opt/ams/events`. You can use these files as provided, modify them, or create new files. The following sections describe the actions you can take when you select the Events... option from the Main window.

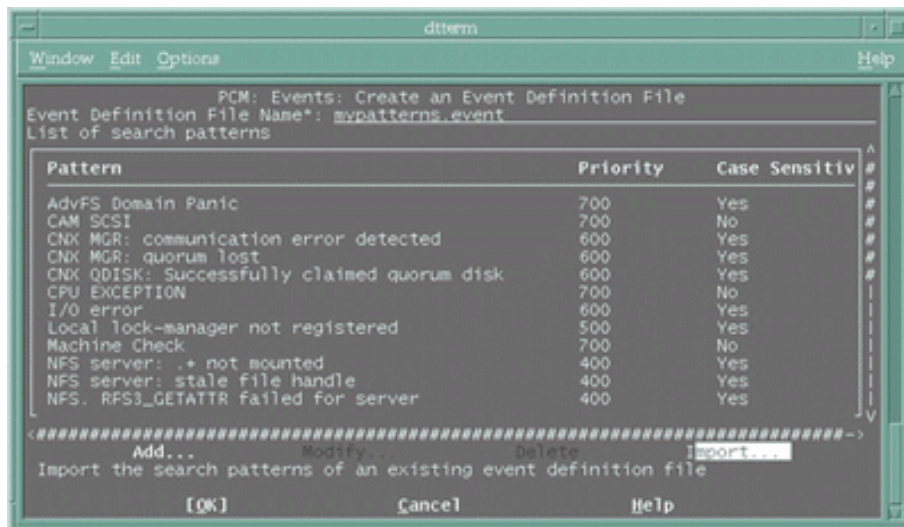
By default, events are generated for each MBM and OS console connection defined. Messages that are normally echoed to the MBM or OS console are parsed; if a match between the output and any entry in the specified event definition file is found, an event with the indicated priority is generated.

Be aware, however, that event generation for a given port is disabled when a user is connected to that port.

### 5.8.1 The Create Events Definition File Window

Selecting the Create Events File option from the Events window brings up a Create Events Definition File window (Figure 5-16). From this window you can add a new event, modify or delete an event, and import event patterns from existing files.

**Figure 5-16: Create Events Definition File Window**



#### Create a File

To create a new file, do the following:

1. Type in a name. An event definition file name can contain only alphanumeric characters, in addition to the hyphen (-), underscore (\_), and period (.). The use of the .event file extension is a common convention, but is not necessary. You cannot specify an existing event name.
2. Select Add... or Import... to bring up a new window:
  - The Add... dialog box (Figure 5-18) lets you specify patterns, priorities, and whether you want the pattern to be searched in a case-sensitive manner.
  - The Import... dialog box lets you replicate the patterns, priorities, and case-sensitivity specified in an existing event definition file.

#### Add Patterns

To add a pattern:

1. In the Add... dialog box (Figure 5-18), type in the pattern you want to monitor and a priority from 100 to 700. You can change the default case sensitivity by pressing the Return Key while positioned in that field. Notice that the Modify... and Delete menus are inactive during this action. When you are satisfied, select OK.
2. To add additional patterns, reselect Add... and repeat the steps.



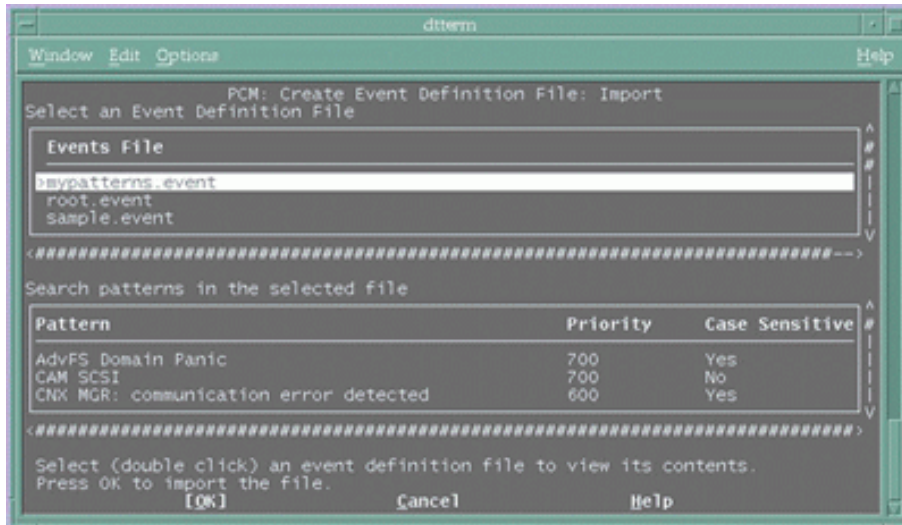
## Import Patterns

When you import patterns from an existing event definition file, the Pattern list box of the Create an Event Definition File window must be empty.

In the Import... dialog box:

1. Select an existing event definition file.  
A new window will open that lists existing event definition files (Figure 5-17).

**Figure 5-17: Import an Event Pattern**



2. Highlight an event definition file and press Return to see its pattern list.
3. When you determine which file's pattern list you want to import, highlight that event definition file and select OK. You will be returned to the Create an Event Definition File window, where the new patterns will be listed.  
From this point you can add additional patterns and can modify or delete existing patterns.
4. When you are finished, select OK in the Create an Event Definition File window to return to the Main window.

You cannot create an empty event definition file.

## Modify or Delete Patterns

After you have named your new event definition file and added at least one pattern, you can modify or delete any patterns listed.

1. Select the pattern you want to modify or delete and select the Modify... or Delete... option.
  - Selecting Modify... opens a window in which you can change the existing pattern. After making changes, select OK. You can continue to add patterns.
  - Selecting Delete... removes the pattern from the pattern list. If the list is empty, the Import... option becomes available.
2. Select OK in the Create an Event Definition File window to return to the Main window.

### 5.8.2 Modifying or Deleting an Existing Event Definition File

You can modify or delete any existing file from the Event Definition File window.

Selecting Modify... or Delete... opens a window that lists the existing event definition files. Highlight the file you want to modify or delete.

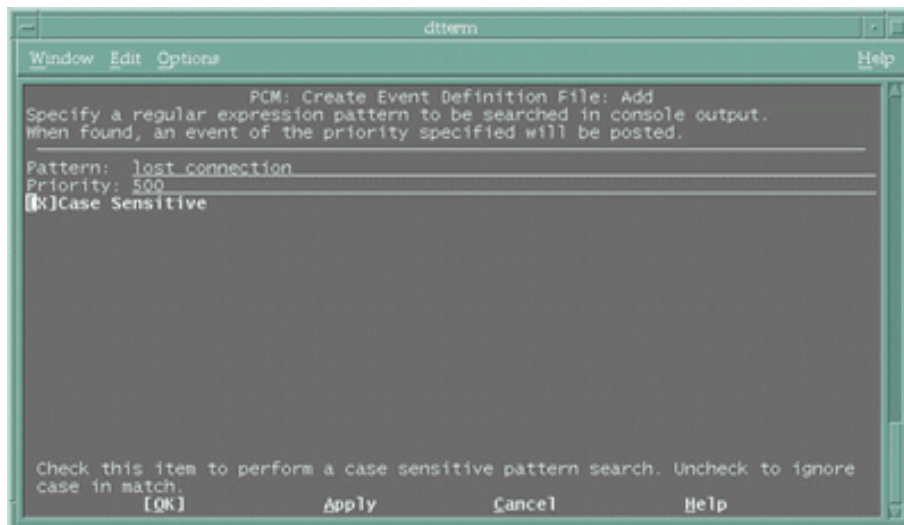
- If you selected the Modify... option, the file you highlight opens in a window that allows you to modify the properties. The window you see and the steps you take are similar to those when you create a new event definition file.
- If you selected the Delete... option, the file you highlight is deleted from the events directory. You can not delete an event definition file that is being used by a console.

### 5.8.3 Generating Events from Console Error Messages

Use the Create Event Definition File: Add dialog box (Figure 5-18) to generate Event Manager events from console error messages.

To generate events from console error messages, first choose a type of console error message you want to generate into an event. For example, you may want to be notified when a system crash has occurred.

**Figure 5-18: Events: Add Dialog Box**



Then enter a regular expression in the PCM Events dialog box that matches the error message you want and the priority you want to assign to the event. For example, to generate system crash error messages into events, enter **crash** and enter a priority of 700. Any console error message that contains the string **crash** is generated into an event with a priority of 700.

After you configure the PCM to generate events, you can view the events that match your filter by opening the Event Viewer from the PCM's Events dialog box. See `evm(5)` and the Event Viewer's online help for more information.

You also can use EVM to notify you when interesting events occur. EVM can display notifications on screen, in e-mail messages, or in pager messages. See Appendix E and the EVM chapters in the *Tru64 UNIX System Administration* guide and *Programmer's Guide* for more information.

To generate events:

1. Select Events in the PCM's main window.
2. Select the Specify Search Patterns checkbox in the Events dialog box.
3. Select Add.

The Events: Add dialog box displays.

4. Enter a search pattern using regular expressions. The PCM will search the console error logs for this pattern and, if found, generate an EVM event for that error.

For example, enter the regular expression **crash**. The PCM will generate events for error messages containing the string `crash`.

See `grep(1)` for more information.

5. Enter the priority of the event you want to generate.

You can use the priority levels to select the events EVM will notify you of or to sort the display in the Event Viewer.

By default, EVM notifies you of events with a high priority level of 500 to 700. The high priority levels range from critical to alert to emergency. See Table 5-1 for more information.

6. Select OK.

The PCM's Events dialog box displays. The regular expression and the priority you entered are displayed in the list of events in the PCM Events dialog box.

7. Select OK to return to the PCM main window.

**Table 5-1: EVM Event Priorities**

EVM Priority/Name	Default Notification	Description
700 Emergency	Log, mail to root	A dangerous situation has been detected and immediate action either is required or has been taken.
600 - 699 Alert	Log, mail to root	A dangerous situation is imminent and immediate action either is required or has been taken.
500 - 599 Critical	Log, mail to root	A failure has been detected that renders some part of the system inoperable.
400 - 499 Error	Log	A noncritical failure has been detected in or by some component of the system or application.
300 - 399 Warning	Log	Some aspect of the system or application requires attention.
200 - 299 Notice	Log	Notification of an expected operational event that the component is designed to deal with.
100 - 199 Information	None	A normal operational event — for example, an application has started or terminated normally. Events in this range typically will not be saved in the system EVM log file.
1 - 99 Debug	None	Program debug information. Events in this range may be monitored for informational purposes, but typically will not be saved in the system EVM log file.
0 None	Application	Priority 0 should be used for events that are specifically intended to be subscribed to by programs, and are not expected to be interesting to administrators.

## 5.8.4 Viewing Events

Use the PCM to launch the Event Viewer to display Event Manager (EVM) events generated from console error messages.

**Figure 5-19: View Events Dialog Box**

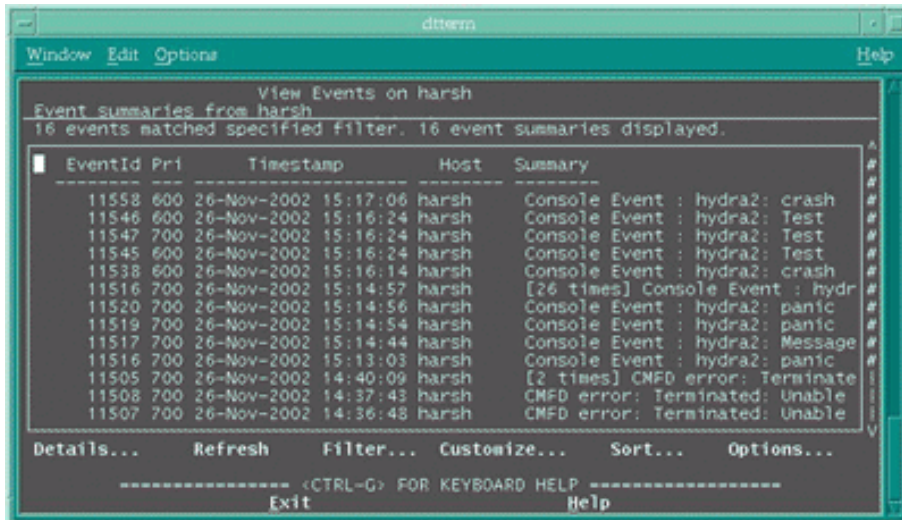


Figure 5-19 shows the summary of events received from the platform harsh.

To view events generated from console error messages:

1. Select Events in the PCM's main window.
2. Ensure that View Events is selected.
3. Select OK.

The EVM Event Viewer launches.

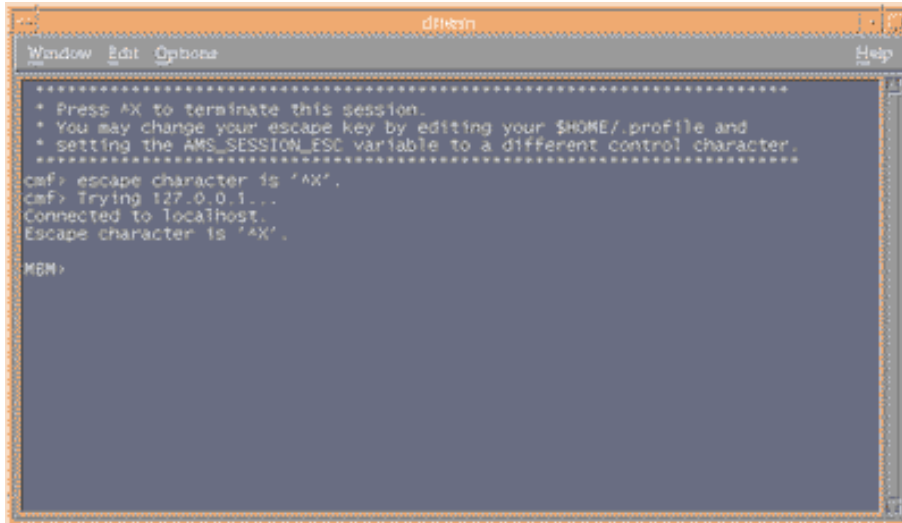
EVM can notify a user via e-mail or a pager about events it receives. EVM sends e-mail messages of events with a priority of 700 or higher to the root user of the AMS, by default. You can configure EVM to let you specify a priority and the name of a user you want notified.

See Appendix D for information about using Event Manager and Appendix E for information about how to send selected events via e-mail.

## 5.9 Connecting to a Platform's Management Port

You can establish a connection to the management LAN of ES47, ES80, and GS1280 platforms directly from the PCM by connecting to the platform's management port.

**Figure 5-20: Connecting to the Platform's Management Port**



```
dflman
Window Edit Options Help
*****
* Press ^X to terminate this session.
* You may change your escape key by editing your $HOME/.profile and
* setting the AMS_SESSION_ESC variable to a different control character.
*****
cmf> escape character is '^X'.
cmf> Trying 127.0.0.1...
Connected to localhost.
Escape character is '^X'.

MBM>
```

Figure 5-20 shows the prompt of the platform's management port displayed after you connect to it from the PCM.

The management LAN connects to the platform's management software, which is controlled by the backplane manager (MBM) of ES47, ES80, and GS1280 platforms. You can view the status and error logs of the platform and manage the MBM when you connect to the management port.

For ES47, ES80, and GS1280 platforms, you access the MBM through a Network Address Translator (NAT) box. A NAT box provides the platform with a unique IP address for the AMS and the hard partitions configured on the platform with a single point of access to the AMS. It allows you to assign to the hard partitions one set of IP addresses for internal traffic and a second set for external traffic.

The MBM prompt is `MBM>`. See the *CLI Reference* manual on the Server Management CD-ROM.

To connect to a platform's management port:

1. Select the platform or console MBM to which you want to connect.
2. Select Console...
3. Select Connect to the platform's management port.
4. The Telnet session starts.

To exit the Telnet session and return to the PCM's main window:

1. Press `Ctrl/x`, which exits from the console's prompt.  
See Section 5.1.2 for information on customizing the Telnet escape sequence.
2. Press `Return` to return to the PCM.

For a list of commands you can perform on the MBM, enter `help` at the MBM prompt.

## 5.10 Managing Consoles

You can manage the consoles of systems created on a platform by using the PCM to:

- Connect to the console (Section 5.10.1)
- Determine a console's status (Section 5.10.2)
- Monitor a console's output (Section 5.10.3)

- Disconnect users from the console (Section 5.10.5)
- View console log files (Section 5.10.6)

### 5.10.1 Connecting to a Console

You can connect to the console of a managed system in the main PCM window.

The Telnet session connects through the `cmfd` daemon to a specific system's console. The `cmfd` logs each Telnet session.

---

#### Note

---

There can be only one connection to a console open at a time. If a connection to a console is already established by another user, you will not be able to connect to the console.

You can clear a console from the PCM, but you should do this with caution and only as a last resort. Clearing the console closes the Telnet connection to it and closes any applications that may be running by a user, which could result in the loss of unsaved data.

It is important to terminate the Telnet session when you are finished since the port will not be accessible while the session is in progress.

---

To connect to a console:

1. Move the cursor to the system to which you want to connect and press Enter.
2. Select Connect to the console.
3. Select OK.

The Telnet session starts. Press Return until you see the console prompt.

Either the firmware prompt (`>>>`) displays if no operating system is installed, or the operating system's login prompt displays.

Enter `help` for a list of commands at the firmware prompt.

To exit the Telnet session and return to the PCM's main window:

1. Press `Ctrl/x`, which exits from the console's prompt and goes to the CMF prompt (`cmf>`).  
See Section 5.1.2 for information on customizing the Telnet escape sequence.
2. Press Return to return to the PCM.

### 5.10.2 Determining a Console's Status

You can determine a console's status in the List of Managed Systems located in the top of the main PCM window. For example, if a console has a status of `In Use`, you can find which user is connected to it and ask that user to disconnect.

**Figure 5-21: Console Status Display**

Console	Platform	Model	Status	Description
<TS_CTRL_PORT>	ts1	M90	Open	Terminal server
Machine-A	ts1	M90	Open	Labmachine #1

Figure 5-21 shows the list of managed systems and their status.

The different status labels indicate the following:

- Open — `cmfd` has a connection to the console.
- In use (RO) — All the users connected to the console are in Read-Only mode.
- In use (SH) — At least one user is connected in Shared mode. Other users may be connected in Read-Only mode.

In this mode, users with shared connections can all make changes that affect the work of other shared-connection users.

- In Use (EX) — One user is connected in Exclusive mode. Other users may be connected in Read-Only mode. A connection as Shared is not possible.
- Inaccessible — The platform or network is down.
- Refused — The port is in use, external to `cmfd`.
- Disabled — The console is disabled.
- Unknown — An internal error has occurred.

The list of systems is sorted by `System` by default. To sort by either `Platform`, `Model`, `Console`, or `Description`, select the heading by which you want to sort.

### 5.10.3 Monitoring a Console's Output

You can monitor a list of consolidated error messages produced by all consoles managed by the PCM. The PCM provides a real-time display of all console output received from all configured systems. It displays the output in a sortable list at the bottom of its main window. Each new line of console output is appended to the list, which scrolls automatically to keep each new line visible.

To view log files of individual systems, either sort the list by `System`, or view the system's log file in the `/usr/opt/ams/logs` directory.

**Figure 5-22: PCM Console Log**

Latest Console Output for Managed Systems

Time	Console	Message
03/04/15_17:48:09	Machine-A	CPU EXCEPTION
03/04/15_17:48:23	Machine-A	AdvFS Domain Panic
03/04/15_17:48:34	Machine-A	Machine Check
03/04/15_17:48:45	Machine-A	CNX MGR: quorum lost

Figure 5-22 shows the latest console output from the managed systems sorted by the time each message was received.

You can customize the console log display by selecting a column heading to sort the output list. For example, to sort by system, select the `System` column heading.

The PCM displays the console log files that were generated during the past seven days. To view older log files, you must view them in the `/usr/opt/ams/logs/cmfd.dated` directory within a terminal window.

### 5.10.4 Viewing the Consoles' Logs

Use the PCM to view console error messages generated during the past seven days.

**Figure 5-23: View a Console Log**

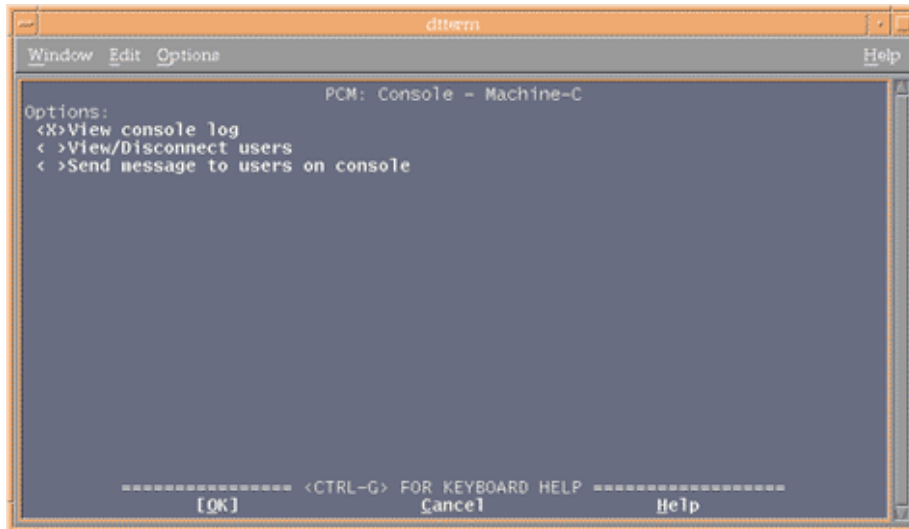


Figure 5-23 shows the PCM Console menu with the View console log option selected.

To view older log files, you must view them in the `/usr/opt/ams/logs/cmfdated` directory within a terminal window.

To view a console's log:

1. Select the system to which you want to connect in the PCM's main window.
2. Select Console...
3. Select View console logs.
4. A dialog box opens displaying the logs.
5. Press `q` to return to the main PCM window.

### 5.10.5 Disconnect a Users from a Console

There can be only one connection to a console open at a time. If a connection to a console is already established by another user, you will not be able to connect to the console without disconnecting that user.

**Figure 5-24: Disconnecting Users from a Console**

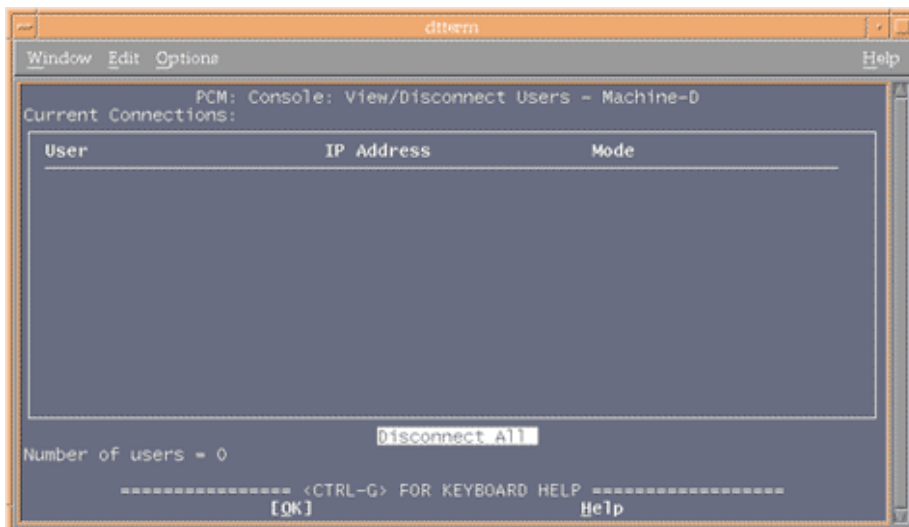




Figure 5-24 shows the PCM Console menu with Disconnect users from console selected.

Although you can disconnect another user from the PCM, you should do so with caution and only as a last resort. Disconnecting a user closes that Telnet connection, thereby closing any applications the user may be running. This could result in the loss of unsaved data.

To disconnect a user from a console managed by the PCM:

1. Select the system whose console you want to clear.
2. Select Console...
3. Select View/Disconnect users.
4. Select OK.

This brings up the View/Disconnect Users dialog box, which lists all connected users.

5. Select Disconnect All.  
The PCM closes all connections to the console.
6. Press Return to return to the main PCM window.

### 5.10.6 Managing Console Log Files

The PCM displays the console log files that were generated during the past seven days. To view older log files, you must view them in the `/usr/opt/ams/logs/cmfdated` directory within a terminal window.



---

## Troubleshooting AMS

This appendix lists errors you may encounter while using components of the AlphaServer Management Station (AMS). (See Section D.4 for advice on troubleshooting Event Manager problems.)

- **Problem:** *SPM displays “platform communication error” in the Hardware Warnings and Errors display when discovering a newly added platform or when refreshing an existing platform.*

The IP address of the NAT box or terminal server may be incorrect or the NAT box or terminal server may have not been configured correctly. Check the configurations, correct any errors you may find and make sure that you can successfully send a ping command to the platforms before you try SPM again.

- **Problem:** *The AMS software intermittently shows one or more platforms with a “Platform not responding” status. The AMU message pane may also show request time-out errors and a partially drawn tree display.*

Version 1.03x of the NAT box’s firmware has tightened up access through its firewall (specifically in the Stateful Packet Inspection (SPI) parameters), and may shut down or limit communication via the UDP protocol used by the AMS server to access the ES47/ES80/GS1280 SMLAN.

When the UDP packets are blocked, AMS times out waiting for a response from the AlphaServer. To resolve this problem, disable the SPI within the firewall function in the SMC7008ABR NAT box (8-port only) with firmware v1.03x.

- **Problem:** *On a Linux Red Hat AMS, the SPM client is launched successfully locally as an application as well as an applet using the web browser, but remote access using the browser on a remote client machine fails.*

You may have enabled the firewall when you installed or configured Red Hat. Reconfigure the firewall setting to No Firewall and try again.

- **Problem:** *On a Linux Red Hat 7.3 workstation, starting the smauth daemon results in the following message:*

```
missing shared library: /usr/lib/libpam.so
```

You need to install the following rpm from the Development/Libraries group of the Red Hat 7.3 installation CD 2:

```
/RedHat/RPMS/pam-devel-0.75-32.i836.rpm
```

- **Problem:** *On a Linux Red Hat 7.3 server, starting amstomcat displays the following error:*

```
missing shared library: libstdc++lib6.1.-1.so2
```

You need to install the following rpm from the System Environment/Libraries group of the Red Hat 7.3 installation CD 2:

```
/RedHat/RPMS/compat-libstdc++-6.2-2.9.0.16.i386.rpm
```

- **Problem:** *In SPM, a partition’s context menu does not contain a Telnet menu item*

When a platform is added, the consoles that correspond to each partition need to be configured before they can be accessed using Telnet. After a console is successfully configured, the console’s context menu will contain “Telnet.”

- **Problem:** *When trying to Telnet to a console using SPM or PCM, the console window displays the message “012 - Console is disabled.”*

Console access has been disabled by a user. In SPM, select the Enable Console menu of the console and make sure that it displays checked. In PCM, select the Enable check box in the console's configuration window.

- **Problem:** *While using SPM a dialog with the message "The AMS server has stopped responding..." is displayed. Closing this dialog causes the SPM display to be cleared.*

You may have had a network interruption and the SPM client could not communicate with the server. If your network is working and you can successfully send a ping command to the server, then the Tomcat server may have stopped running. Log into your AMS server and determine if the Tomcat process is still running by entering one of the following commands

On Tru64 UNIX systems:

```
# /sbin/init.d/amstomcat status
```

On Linux systems:

```
# /etc/init.d/amstomcat status
```

If the catalina process is not running, make sure that Tomcat was not stopped from the command line by checking the last line in `/usr/opt/ams/tomcat/catalina.out`. If that line is "Stopping service Tomcat-Apache", it means that Tomcat was stopped by a user. To restart Tomcat, enter one of the following commands:

On Tru64 UNIX systems:

```
# /sbin/init.d/amstomcat start
```

On Linux systems:

```
# /etc/init.d/amstomcat start
```

If Tomcat was not stopped by a user, Tomcat and the JVM may have crashed. The following steps will help you collect debug information before you contact AMS support

1. Stop Tomcat if it is running.
2. Collect and save current log files from the following directories :

```
/usr/opt/ams/tomcat/logs
/usr/opt/ams/tomcat/webapps/spm/WEB-INF/log
/usr/opt/ams/logs (all files, including subdirectories)
```

3. Enter the following commands to enable the SPM and AMU server debug:

```
# cd /usr/opt/ams/tomcat/webapps/spm/WEB-INF
# cp debug.SPMSLog4J.xml SPMSLog4J.xml
# cd data
# cp debug.ServerConfiguration.xml ServerConfiguration.xml
```

4. Start Tomcat and try to reproduce the problem.
5. When the problem is reproduced, collect the log files as in step 2.
6. Send the log files from steps 2 and 5 to AMS support with a description of the problem.
7. Stop Tomcat.
8. Copy the non-debug files back to stop collecting debug information:

```
# cd /usr/opt/ams/tomcat/webapps/spm/WEB-INF
# cp default.SPMSLog4J.xml SPMSLog4J.xml
# cd data
# cp default.ServerConfiguration.xml ServerConfiguration.xml
```

9. Start Tomcat

- **Problem:** *PCM exits after entering a regular expression in the Events Add dialog box.*  
You may have entered double-quotes in the regular expression. Double-quotes cause the PCM to exit.
- **Problem:** *A blank screen displays when attempting to run the SPM.*  
The AMS machine may not have enough memory to run the SPM. See the installation instructions for more information.
- **Problem:** *Updating the platform's firmware is unsuccessful.*
  1. Stop the Tomcat server before attempting to update the firmware by using one of the following commands:  
For Tru64 UNIX:  

```
# /sbin/init.d/amstomcat stop
```

  
For Linux:  

```
# /etc/init.d/amstomcat stop
```
  2. Use the command line interface to the platform's management port by connecting to it from either the SPM or the PCM. See either Chapter 2 or Chapter 5 for more information.
- **Problem:** *The Console Management Facility daemon, cmfd, keeps writing to console logs in /usr/opt/ams/logs/cmfd.current and /usr/opt/ams/logs/cmfd.dated until the disk is full.*  
Copy the contents of the log files to a separate location and empty the contents of the log directories.
- **Problem:** *The PCM cannot connect to the console daemon, cmfd, and the console status is unknown. The PCM displays this error message in a dialog box and in the list of managed systems.*  
Restart the cmfd daemon.
- **Problem:** *When using the PCM, you attempt to connect to a console but the connection is closed by a foreign host and you are asked to press Return to return to the PCM main window.*  
This may be caused by another user or application being connected to the console. Ask the user to disconnect from the console or clear the console line.
- **Problem:** *A console has a status of Inaccessible.*  
This may be caused by another application using the console connection or by a VT100 terminal that is connected directly to the port. Ask the user to disconnect the terminal from the console or clear the console line.
- **Problem:** *A console has a status of Unknown.*  
This may occur if the cmfd daemon has stopped or unresponsive. To check the status of the cmfd daemon, enter one of the following commands:  
On Tru64 UNIX systems:  

```
# /sbin/init.d/cmfd status
```

  
On Linux systems:  

```
# /etc/init.d/cmfd status
```

  
If the cmfd daemon is not running, enter one of the following commands to start it:  
On Tru64 UNIX systems:  

```
# /sbin/init.d/cmfd start
```

  
On Linux systems:

```
# /etc/init.d/cmfd start
```

## Firmware Alerts

The tables in this appendix list all of the alerts generated by the firmware, the source of each alert, the severity level, and the data that is contained in the alert packet. Section 3.3.3.2 describes firmware alerts.

**Table B-1: Firmware Alerts — Environmental Group**

Event Description	Source	Severity	Supplied Data
Voltage	MBM, PBM, CMMn	OK, Warning, Failure, Non-Present, Unknown	Locator, Voltage reading
Temperature	MBM, PBM, CMMn	OK, Warning, Failure, Non-Present, Unknown	Locator, Temperature reading
Fan	MBM, PBM	OK, Warning, Failure, Non-Present, Unknown	Locator, Fan RPM value
Intrusion	MBM, PBM	OK(close), Warning(open)	Locator
PS	MBM, PBM	OK, Failure, Non-Present, Unknown	Locator, Specific Error: 0=PS type; 1=AC; 2=POK; 3=PSFail; 4=PFRL; 5=overtemp; 6=AC RMS or AC1; 7=Fan
WPI/SDI	MBM	OK, Failure, Unknown	Locator, Specific Error: 0=PS Type; 1=VAUX or 9V_A; 2=Vcc or 9V_B
IOR	PBM	OK, Failure, Non-Present, Unknown	Locator, Specific Error: 1=Converter failure; 2=BP short; 3=1.8V; 4=2.5V; 5=3.3V; 6=IO7 1.5V; 7=BP 1.5V
EEPROM	MBM, PBM, CMMn	OK, Warning, Failure, Non-Present, Unknown	Locator, Temperature reading
EEPROM	MBM, PBM, CMMn	OK, Warning, Failure, Non-Present, Unknown	Locator
VRM	CMMn	OK, Warning, Failure, Non-Present, Unknown	Locator
Power off drawer due to temp failure	MBM, PBM	Failure	
Power off drawer due to insufficient running fans	MBM, PBM	Failure	

**Table B-1: Firmware Alerts — Environmental Group (cont.)**

Event Description	Source	Severity	Supplied Data
Power off drawer due to unknown failure	MBM, PBM	Failure	
Component has been added	CMMn, PS, IORn	OK	
Component has been removed	CMMn, PS, IORn	OK	
Insufficient running PS	PS	Warning	

**Table B-2: Firmware Alerts — Operational Group**

Event Description	Source	Severity	Supplied Data
SYS_SERIAL_NUM is not set	Operational	Warning	
Running with mixed firmware revisions	Operational	Warning	
%s test failure	MBM, PBM	Failure	POST test that failed
Last reset due to watchdog timeout	MBM, PBM, CMMn	Warning	
Server management group is transitioning	Operational	Warning	
Server management group is stable.	Operational	OK	
Power switch state changed	Operational	OK	New state
Error log entry	MBM, PBM	Warning	

**Table B-3: Firmware Alerts — Partition Group**

Event Description	Source	Severity	Supplied Data
IP Cable missing between cab:%d drw:%d port:%s and cab:%d drw:%d port:%s	MBM	Warning	Cabinet, drawer, port
Logging PAL EV7 Logout	EV7	Failure	
Test %02X [%s] failed on cpu [NS: %d EW: %d]	EV7	Failure	test number, test name, cpu ns, cpu ew
Unable to disable Zbox	EV7	Failure	
Disabled CPU/IO	EV7, IORn	Failure	
Disabled Zbox1	EV7	Failure	
Disabled RAID (remap)	EV7	Failure	
Disabled Memory	EV7	Failure	
Disabled: IP Cable cab:%02X drw:%X CPU:%x %s wrap:%d; (%x,%x) to (%x,%x)	EV7	Failure	cab, drawer, cpu, string, wrap, ns1, ew1, ns2, ew2
Other end of IP Cable not found - cab:%02X drw:%X CPU:%x %s wrap:%d; (%x,%x)	EV7	Failure	cab, drawer, cpu, string, wrap, ns1, ew1
IO Configured without CPU Memory	EV7	Warning	



**Table B-3: Firmware Alerts — Partition Group (cont.)**

Event Description	Source	Severity	Supplied Data
Adjusting maximum EV7 CPU count to match assigned PIDs. HP:%d, max PIDs: %d	Operational	Warning	HP number, new max cpus
Partition is unroutable. Fallback Rectangle (%d,%d) (%d,%d) num_RboxReqs: %d	Operational	Failure	ns1, ew1, ns2, ew2, numRboxRegqs
Halt on error. HP:%d	Operational	Failure	HP number
Can't power on: OCP Switch is off.	Operational	Failure	
Can't power on: Drawer will exceed 4 EV7s for ES47	Operational	Failure	
Preparing to power on partition. HP: %s	Operational	OK	HP number
No eligible CPUs have memory required to be a primary.	Operational	Failure	
Preparing to power off partition. HP: %s	Operational	OK	HP number
Resetting partition. HP: %s	Operational	OK	HP number
FPGA Load fault	PBM	Failure	HP number
Time update distribution failed for hp: %d sp:%d	Operational	Failure	hp number, sp number
Partition powered on. HP: %s	Operational	OK	HP number
Partition powered off. HP: %s	Operational	OK	HP number
Partition reset. HP: %s	Operational	OK	HP number
Partition configuration changed.	Operational	OK	
CPU Speeds are mixed.	Operational	Failure	HP number
Memory range check is disabled	Operational	OK	HP number

**Table B-4: Firmware Alerts — EV7 Group**

Event Description	Source	Severity	Supplied Data
CPU Clock Power Fault	EV7	Failure	
%s %s has faulted (VRM failure)	CMMn, EV7?	Failure	cpu_id, vrm name
RIMM SPD Checksum failed for RIMM #%d	CMMn	Warning	failed RIMM number
Error writing the PLL clock ratio registers.	CMMn	Failure	
Too many %s VRMs (%d) have failed	CMMn	Failure	vrm type, number failed
Can't reset EV7 with power off	EV7	Failure	
CPU has timed out during SROM load.\n	EV7	Failure	cpu number
CPU failed SROM/XSROM load	EV7	Failure	
CPU has timed out during tepid reset, continuing	EV7	Failure	

**Table B-4: Firmware Alerts — EV7 Group (cont.)**

<b>Event Description</b>	<b>Source</b>	<b>Severity</b>	<b>Supplied Data</b>
Can't halt EV7 with power off	EV7	Failure	
SROM port is stuck busy	EV7	Failure	cpu number
Scan dump on CPU timed out waiting for busy	EV7	Failure	
Scan dump on CPU timed out	EV7	Failure	
Can't read CPU EEPROM	EV7	Failure	
Can't write CPU EEPROM	EV7	Failure	
srom_check_status: CPU timed out waiting for SROM load status	EV7	Failure	cpu number
srom_check_status: CPU cannot accept the load image command.	EV7	Failure	
srom_check_status: CPU timed out waiting for SROM load image status	EV7	Failure	
srom_check_status: CPU timed out on XSROM version command.	EV7	Failure	
Error in load image to EV7	EV7	Failure	
OCLA %d was found running. Clearing RUN	EV7	Failure	ocla
OCLA %d was found disabled. Setting Enable	EV7	Failure	ocla

---

## Log File Management

This appendix provides information about the log files generated by the AlphaServer Management Station applications and the `cmfd` daemon.

### C.1 Console logs

The console logs are located in the following directory, which contains the current and archived console logs generated by the `cmfd` daemon.

- `/usr/opt/ams/logs/cmfd.dated`

The following directory is a link to the current logs.

- `/usr/opt/ams/logs/cmfd.dated/current`

All other directories contain archived logs. The current and archived logs are preserved during AMS upgrade installations. You may move or delete the archived logs at any time.

### C.2 AMS application logs

AMS components generate many logs that are used mainly for debugging purposes. The following list describes those files:

- The directory `/usr/opt/ams/logs` contains the following:
  - `amsmgr.log`

This file is from the `amsmgr` component. It contains all of the commands sent to `amsmgr` for updating the AMS data store with new or modified configurations.

This file is automatically archived by `amsmgr` when the file size reaches 1 MB. When this happens the `amsmgr` process renames `amsmgr.log` to `amsmgr.log.old` and creates a new log file. If an `amsmgr.log.old` file already exists, it is overwritten. Therefore, it is not necessary to manage this log file.
  - `apw -date-#.txt`

This file is from the APW, which creates one log per APW session. The logs contain mostly platform data that is retrieved during an APW session. These files are never archived and can be removed at any time. The current session's file should be removed after the APW session has ended.
  - `cmfd.log`

This file is from the `cmfd` daemon. Normally `cmfd` is run with no debugging options, so this file will not accumulate data. Should debugging be turned on, the file can be safely managed only when the `cmfd` daemon has been stopped.
- The directory `/usr/opt/ams/tomcat/logs` contains files generated by the Tomcat Web Server.
  - `catalina.out`

This file, created when Tomcat starts, contains all the Java exceptions and error messages sent to `System.out` or `System.err` by Tomcat and the AMS Java server components (SPM/AMU/APW servers).

When the file becomes large you can move it or delete it after you stop Tomcat. If the file is deleted while Tomcat is running, it will not be re-created until the next time you restart Tomcat.

- catalina\_log.date.txt
- localhost\_access\_log.date.txt
- localhost\_log.date.txt

These files contain mainly http session request information. Archived files can be removed at any time. For current files, follow same guideline as for catalina.out.

- The directory `/usr/opt/ams/tomcat/webapps/spm/WEB-INF/log` holds all of the log files generated by the AMU application. These files are as follows:

- `ServerCore.date.log`

This file contains AMU server errors

- `SMLANLib.errors.date.log`

This file contains errors generated by the interface library to the ES47, ES80, and GS1280 AlphaServer SMLAN

- `SMLANLib.events.date.log`

This file contains all the events received by the SMLAN

- `Logs.MV-(hex)IPaddress.data.log`

This file contains MBM log entries for ES47, ES80, and GS1280 systems configured with a NAT box with the IP address that is included in the log name.

- `platformName.errlog`

This file is generated only if you select to generated a CDL file for the platform. One file will contain all the CDL entries for each platform partition.

These log files should be managed after the Tomcat Web server has been stopped. If you delete some or all files, new files will be created when the Tomcat server is restarted.

---

## Using the Event Manager

The Event Manager is a comprehensive event management system providing traditional event handling facilities. The Event Manager includes an event viewer and a full set of command line tools. It is integrated into the AlphaServer Management Station application.

The following topics are covered in this chapter:

- An overview of Event Manager (Section D.1)
- How to set up and customize Event Manager (Section D.2)
- How to use Event Manager to assist in the administration of your system (Section D.3)
- Troubleshooting common Event Manager problems (Section D.4)

### D.1 Event Manager Overview

A critical function of the AlphaServer Management Station is to monitor the state of the platforms and systems being managed, and to inform the administrator when certain unusual conditions occur. Examples include errors like those reported by the platform firmware (fan failure) and by the operating system console (disk full). Such conditions are known as system events.

#### D.1.1 Features of the Event Manager

Event Manager provides the following features:

- Facilities for users and applications to post and monitor events
- Integration of an event viewer with the SPM and PCM user interfaces
- A choice of summary or detailed event data
- A full set of command-line utilities that you can use to monitor and manage events from shell scripts and from the command line
- Configurable event logger that allows full control over which events are logged and optimizes storage space used by identical events
- Configurable event forwarding that enables you to automatically notify other system entities of selected events
- Log file management that automatically archives and purges log files daily
- Centralized access to event information

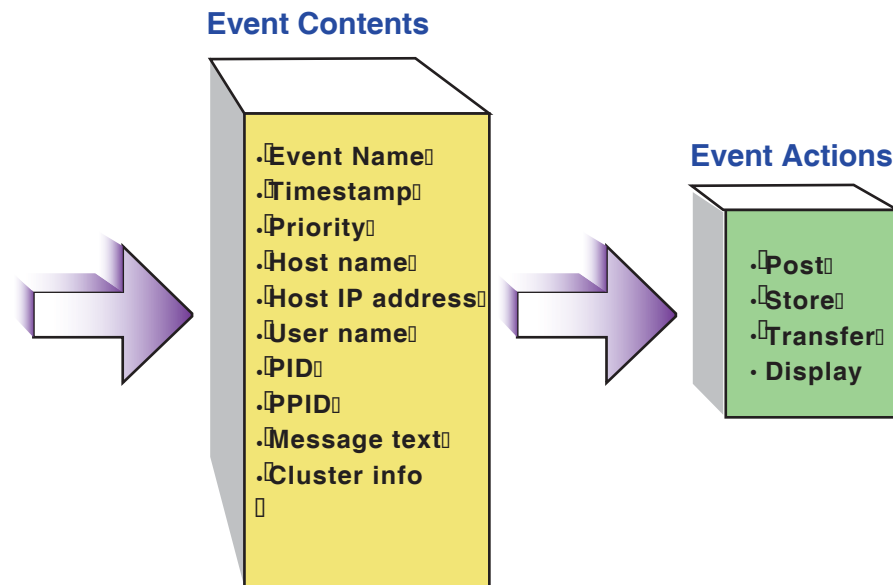
#### D.1.2 Understanding Event Manager Events

An Event Manager event is a binary package of data that contains a set of standard data items, including a name, a timestamp, and information about the poster. An event may contain variable data, which is named and supplied by the poster. For example, an event reporting the failure of a device may hold variables containing the path name and type of the device.

Events are created and posted by an Event Manager posting client, and distributed to other clients by the Event Manager daemon. Then, a receiving process can extract and process the information contained in the event.

Figure D-1 shows a graphical representation of an event. The Event Contents box shows items, such as the process identifier (PID) and the name of the host system on which the event was generated, that may be included in the event. The Event Actions box shows some of the possible actions performed on any event.

**Figure D-1: Event Model**



ZK-1549U-AI

The Event Manager includes command-line utilities that understand the format of the event, and which you use to perform basic operations at the command prompt or in shell scripts; you cannot view an event directly with a text viewer (for example, `more`) because an event is a package of binary data. You can use Event Manager commands to:

- Retrieve events from storage, sort them into a preferred order, and format them for display
- Watch for new events being posted

The Event Manager command-line utilities are designed to be used together in pipelines. For example, you may pipe a set of events from a file into the sort utility, pipe the output into the formatting utility, then pipe the output of that command into the `more` command, or redirect it to a file. Section D.3 provides examples of using Event Manager commands to monitor and review event activity.

After the event file is converted to text form, you can use other standard utilities to analyze it. For example, you may display just the event names, and then pipe the display into the `sort -u` and `wc -l` commands to determine how many different types of events are in the file.

### D.1.3 Event Manager Command-Line Utilities

Event Manager provides a number of command-line utilities both for administering the Event Manager system itself and for obtaining events. Table D-1 describes the general user commands. Detailed information is available from the reference pages. See Section D.3 for examples of how to use these commands to monitor and review event activity.

**Table D-1: Event Manager Command-Line Utilities**

Command	Description
<code>evmget</code>	Retrieves stored events from a configured set of log files and event channels, using channel-specific retrieval functions
<code>evmshow</code>	Accepts one or more Event Manager events and outputs them in the requested format
<code>evmsort</code>	Reads a stream of events and sorts them according to supplied criteria
<code>evmwatch</code>	Subscribes to events specified and outputs them as they arrive

Table D-2 lists the Event Manager administrative commands, which are usually invoked during system initialization. The individual command reference pages discuss other conditions under which the command is used.

**Table D-2: Event Manager Administrative Utilities**

Command	Description
<code>evmchmgr</code>	The Event Manager daemon automatically starts the Event Manager channel manager. It executes the periodic functions defined for any channel.
<code>evmd</code>	The Event Manager daemon receives events from posting clients and distributes them to subscribing clients, that is, clients that have indicated they want to receive the events. The daemon is a critical system facility that starts automatically at system boot. Do not terminate it.
<code>evmlogger</code>	The Event Manager daemon automatically starts the Event Manager logger. The logger receives events from the daemon and writes them to each of the logs whose filter string they match. The <code>evmlogger</code> also serves as an event forwarding agent that you can configure to take an action when required.
<code>evmreload</code>	This command posts control events, which instruct the Event Manager components to reload their configuration files. When you modify an Event Manager configuration file you must use this command to load the new configuration.
<code>evmstart</code>	This command starts the Event Manager daemon. It is intended for use by the system startup scripts, but you can also use it to restart Event Manager should it terminate for any reason.
<code>evmstop</code>	This command stops the Event Manager daemon, preventing entities from posting or subscribing for events. It is intended for use by the system shutdown scripts. Do not use this command under normal circumstances, because Event Manager is required for many system functions to operate correctly.

## D.1.4 Event Manager System Files

Event Manager creates or uses the system files described in the following sections.

### Executable Files

Executable files for Event Manager administrative commands are located in the `/usr/sbin` directory.

General (that is, user) command executable files are located in the `/usr/bin` directory.

Initialization files are located as follows:

- In `/sbin/init.d` for Tru64 UNIX.

- In `/etc/init.d` for Linux

## Configuration Files

Base Event Manager configuration files are located in the `/etc` directory; they are listed here.

`/etc/evmdaemon.conf`

This file is a text file that contains commands used to configure and start the Event Manager.

`/etc/evmchannel.conf`

The event channel configuration file, which is read by the channel manager, `evmchmgr`, and the `evmshow` command. This file describes all the channels through which events can be posted and retrieved.

`/etc/evmlogger.conf`

The configuration file for the logger, `evmlogger`. It contains commands used to direct the display, forwarding, or storage of events. See Section D.2.2 and `evmlogger.conf(4)` for a complete description of this file.

`/etc/evm.auth`

This file is used to control access to events and event services. See Section D.2.3.2 and `evm.auth(4)` for a complete description of this file.

## Log Files, Working Files, and Local Installation Files

Log files, working files, and local installation files are located in the following subdirectories of `/var/evm`.

`/var/evm/sockets`

This directory contains a domain socket node, `evmd`, and a related lock file, `evmd.lock`. Local clients use this socket for connection.

`/var/evm/evmlog`

This directory contains the event logs created by the default Event Manager logger configuration. Log files in this directory have names in the format `evmlog.yyyymmdd[_nn]`, where `yyymmdd` is the date of the log, and `_nn` is a sequential generation number. A new log generation starts if the log reaches its configured maximum size during the course of the day, or if the logger finds an error in the current file. The day's first log file has no generation number. A new log file is started automatically when it receives the first event after midnight, system time.

This directory also contains a lock file, `evmlog.dated.lock`, and a generation control file, `evmlog.dated.gen`, the latter containing information about the current generation number. See Section D.2.4 for more information on managing log files.

`/var/evm/adm/logfiles`

This directory contains output message logs created by the resident components of Event Manager: the daemon, logger, and channel manager. New files are created each time Event Manager starts. Old files are renamed by appending the suffix `".old"` to their names, overwriting any previous old files. These message logs are encapsulated by Event Manager's `misclog` event channel, so their contents are visible through `evmget` and the event viewer.



`/var/evm/shared`

This directory is a work directory that holds temporary files required for client authentication.

`/var/evm/adm/templates`

The directory is provided for installation of local and third-party event template subdirectories. This directory is connected to the system template directory by a symbolic link.

`/var/evm/config`

This directory and its subdirectories contain secondary configuration files for various Event Manager components. In this release, only the logger supports secondary configuration files; see `evmllogger.conf(4)` for more information.

`/var/evm/adm/filters`

The directory is provided for installation of local event filter files.

`/var/run/evmd.pid`

This file contains the daemon process identifier (PID), that is saved by the `evmd` daemon for future actions, such as stopping Event Manager.

`/var/run/evmllogger.info`

This file contains the logger's PID and information about the log files being managed. The `evmlog` channel retrieval and daily cleanup functions use this information.

### System-Supplied Definition Files

System-supplied definition files for templates, channels, and filters are located in the following subdirectories of the `/usr/share/evm` directory.

Do not modify these files.

`/usr/share/evm/channels`

This directory contains a subdirectory for event channels such as `evmlog`. Each subdirectory contains scripts that define the services available for that channel.

`/usr/share/evm/filters`

This directory contains system filter files.

`/usr/share/evm/templates`

This directory contains system event template files and subdirectories.

## D.2 Administering Event Manager

The role of the administrator in running Event Manager involves the following principal activities:

- Starting and stopping Event Manager, described in Section D.2.1
- Configuring the `evmllogger` files, described in Section D.2.2
- Controlling who is allowed to post or access events, described in Section D.2.3
- Managing log files, described in Section D.2.4

For information on using the Event Manager, see Section D.3.

## D.2.1 Starting and Stopping Event Manager

The Event Manager is started automatically at system startup and is stopped when the system is shut down.

Use the `evmstop` command to stop Event Manager:

```
# /usr/sbin/evmstop
```

Use the `evmstart` command to start Event Manager:

```
# /usr/sbin/evmstart
```

You do not need to stop and start Event Manager when you want to change the Event Manager configuration. In this instance, change the configuration, then issue the `evmreload` command. See `evmreload(8)` for more information.

## D.2.2 Configuring the Event Manager Logger

The Event Manager logger handles storage and forwarding of events, according to entries in the `/etc/evmlogger.conf` configuration file. For a complete description of the contents and syntax of this file, see `evmlogger.conf(4)`.

Example D-1 shows sample entries in a logger configuration file — an example of possible customization of the logger is to have events e-mailed to specific users.

---

### Note

---

The `syslog` templates referenced in the following examples are not included in the AMS software kit and are used only for example purposes.

---

Note that

---

### Example D-1: Sample Event Manager Logger Configuration File Entries

---

```
# Main log file:
eventlog { 1
    name          evmlog 2
    logfile       /var/evm/evmlog/evmlog.dated 3
    type          binary 4
    maxsize       512 # Kbytes 5

    # Uncomment the following "alternate" line and set the
    # logfile path to specify an alternate logfile in case
    # of write failures.
    # The path must specify an existing directory.
    #alternate    /your_alterate_fs/evmlog/evmlog.dated 6

    # Log all events with priority >= 200, except syslog events:
    filter        "[prio >= 200] & (! [name @SYS_VP@.syslog])" 7

    # Suppress logging of duplicate events:
    suppress      8
    {
        filter    "[name *]"
        period    30 # minutes
        threshold 3 # No. of duplicates before suppression
    }
}

# Forward details of high-priority events to root:
forward { 9
    name          priority_alert 10
```

## Example D-1: Sample Event Manager Logger Configuration File Entries (cont.)

---

```
maxqueue 200 11

# Don't forward mail events through mail
filter "[prio >= 600] & ![name @SYS_VP@.syslog.mail]" 12

suppress 13
{
  filter "[name *]"
  period 120 # minutes
  threshold 1 # No. of duplicates before suppression
}

# This evmshow command writes a subject line as the first
# line of output, followed by a detailed display of the
# contents of the event.
# The resulting message is distributed by mail(1).
command "evmshow -d -t 'Subject: EVM ALERT [@priority]: @@" |
mail root" 14

# Limit the number of events that can be queued for this
# command:
maxqueue 100
}

# Secondary configuration files can be placed in the following
# directory. See the evmlogger.conf(5) reference page for
# information about secondary configuration files.
configdir /var/evm/adm/config/logger
```

- 
- 1** This line begins an event log configuration group.
  - 2** This line provides a name for the event log. Other portions of the configuration file may reference this name.
  - 3** This line specifies that the log files are stored in the `/var/evm/evmlog` directory. Each day, when the log for that day is first written, the dated suffix is replaced by the date in the format `yyyymmdd`.
  - 4** This line specifies that the type of events written to this log are binary Event Manager events, rather than formatted (ASCII text) events.
  - 5** This line specifies the maximum size of the log file in kilobytes (KB). In this case, if the size of the current log file exceeds 512 KB the logger closes it and begins a new log file, with a sequentially numbered suffix (for example, `_2`) appended to the file name.
  - 6** If this line is not commented out (by #) and the sample path is replaced by the path name of an existing write-enabled directory, an alternate log file is opened in this directory if the primary directory becomes write-disabled.
  - 7** This line establishes the filtering conditions for events, determining which events are logged by this event log. See `EvmFilter(5)` for details of Event Manager filter syntax. The `@SYS_VP@` entry is a macro that is replaced with `sys.unix` when the file is read.
  - 8** These statements define the suppression parameters for this event log. In this case, suppression of a particular event begins if three or more duplicate events are received within 30 minutes. Suppression of duplicate events saves space in the log file. See `evmlogger.conf(4)` for a detailed description of event suppression.
  - 9** This line establishes conditions for forwarding events to the root user. An event forwarder executes a specified command string when selected events

occur. It is useful for notifying the system administrator when a significant error occurs.

- 10** In this line, `name` identifies the forwarder.
- 11** The `maxqueue` `queue_limit` keyword limits the number of events that a forwarder can queue while a previous event is being handled. If the maximum number of events is already queued when a new event arrives, the new event is ignored by this forwarder. If not specified, this keyword has a default value of 100 events. If you specify a value greater than 1000 events, the logger automatically limits it to 1000 events.
- 12** This line establishes filtering for the events. As with an event log definition, the filter string specifies the set of events that are handled by this forwarder. To prevent an event loop from occurring if the mailer posts high-priority events, signifying a possible problem in the mail subsystem, mail events are explicitly excluded from this forwarder.
- 13** These lines suppress multiple forwarding of events. The suppression mechanism for a forwarder is similar to that for an event log. Here, the purpose is to prevent the command from being sent multiple times in a short period because of the same event being posted repeatedly. In the example, a particular event is forwarded once every two hours at most.
- 14** This line defines the command that executes when an event is handled by the forwarder. The event is piped into the command's `stdin` stream. The result of this command is shown in the comments preceding the command line.

If you make any changes to the logger configuration file you must run the `evmreload` command to make the changes known to the logger; see `evmreload(8)` for more information.

## Secondary Logger Configuration Files

Secondary logger configuration files enable you to add event logs or forwarders without modifying the primary configuration file, `/etc/evmlogger.conf`. This feature ensures that any problems with secondary files do not affect the primary configuration. It enables you to safely experiment with different logger configurations.

Should the logger encounter a syntax error in a secondary configuration file, it displays an error message and rejects the file. The primary configuration file and any additional (and correct) secondary files are processed and Event Manager functions correctly.

The secondary configuration directory feature also allows individual system components, products and applications to install or change log files and forwarders by installing or replacing files, rather than having to insert or maintain lines in the primary configuration file. You can uninstall entries by removing the file.

The default and recommended location of secondary configuration files is the `/var/evm/adm/config/logger` directory, or a subdirectory of that directory. Your secondary configuration files must have file name suffix `.conf` and the file syntax must follow the rules described in Example D-1.

It is important that you give appropriate permissions to the secondary logger configuration files and directories. The logger runs with superuser privileges and can execute commands specified in any secondary configuration file. For this reason, the logger rejects any configuration files that do not have the correct permissions and posts a warning event. See `evmlogger.conf(4)` for the correct file permissions.

## D.2.3 Security Considerations

Security is an important consideration when dealing with events, for the following reasons:

- Uncontrolled access to certain event information may provide an unauthorized user with sensitive information about system operation.
- Posting certain events may cause critical system actions, for example, application failover or system shut down, to occur.

Traditionally, event information security is maintained by restricting read access to log files and limiting certain operations to the root user. Because the Event Manager daemon and event retrieval facilities provide alternate means of access to all events, both as they are posted and after they are logged, the daemons also provide a way to limit access, so that events are seen only by authorized users. You can enable access control by providing authorization facilities and using authentication techniques.

### D.2.3.1 User Authentication

The Event Manager daemon authenticates the identities of all local system users before accepting any connection request.

### D.2.3.2 User Authorization

Access to events is controlled by the Event Manager authorization file, `/etc/evm.auth`.

When AMS is installed, members of the `amsuser` group are automatically provided EVM access rights. It is critical to the proper operation of AMS that these privileges remain intact. In addition, the root user can authorize additional individual users or groups of users to do the following:

- Access (subscribe to or retrieve from storage) selected events
- Execute selected services

Event rights are granted by supplying, for each event class, a list of users who have the specified right or who are explicitly denied rights.

A plus sign (+) that is not followed by a user list implicitly grants the right to all users. A minus sign (-) that is not followed by a user list implicitly denies the right to all users.

The root user has implicit posting and access rights to all events unless explicitly denied them. Example D-2 shows sample entries in an authorization file. See `evm.auth(4)` for more information.

#### Example D-2: Sample Event Manager Authorization File Entries

---

```
# =====
#      EVENTS
# =====

event_rights { 1
    class      @SYS_VP@.evm.control    # EVM control events
    post       root
    access     +
}

event_rights { 2
    class      @SYS_VP@.evm.msg.admin  # EVM admin message
    post       root
    access     "root, group=adm"
```

## Example D-2: Sample Event Manager Authorization File Entries (cont.)

---

```
}

event_rights {   3
  class          @SYS_VP@.evm.msg.user    # EVM user message
  post           +
  access         +
}

# =====
#     SERVICES
# =====

service_rights { 4
  service        event_get
  execute        +
}

}
```

---

- 1 Only the root user can post the class of events that have names beginning with `sys.unix.evm.control`. Such events are accessible by all users. The `@SYS_VP@` entry is a macro that is replaced with `sys.unix` when the file is read.
- 2 Only the root user can post the class of events that have names beginning with `sys.unix.evm.msg.admin`. Such events can be accessed by root or other users in the `admin` group.
- 3 All users can post or access the class of events that have names beginning with `sys.unix.evm.msg.user`.
- 4 All users can execute the `event_get` service.

If you make any changes to the authorization file you must run the `evmreload` command to make the Event Manager daemon aware of the changes.

### D.2.4 Managing Log Files

The Event Manager channel manager, `evmchmgr`, provides log management capability through the channel `fn_cleanup` function. You can define this capability for any channel through the channel configuration file, `evmchannel.conf`.

By default, channel cleanup functions run when Event Manager starts. You can change the time of day by editing the `cleanup_time` value in the channel configuration file. When a cleanup is scheduled, the channel manager scans the event channel list, and executes the `fn_cleanup` command for each channel identified in the file.

The `evmlog` cleanup function, `evmlog_cleanup`, takes two arguments:

- The archive period, which has a default value of 7 days.
- The delete period, which has a default value of 31 days.

The function uses the `find` utility to locate and compress (zip) all logs older than the archive period, and to delete any archived files older than the delete period. You can change the period values by editing the function definition in the channel configuration file. Setting either of these values to zero disables the corresponding function.

The `evmget` command does not retrieve `evmlog` events that are stored in archived (zipped) logs. To retrieve events from archived logs you must first uncompress

them with the `gunzip` command; see `gunzip(1)` for information on unzipping archive files.

## D.3 Using Event Manager in System Administration

The following sections illustrate the commands you can use to monitor and review event activity. As you become familiar with the Event Manager command set, you build up a set of favorite commands, shell scripts, and filters that help you to keep track of what is happening on your system.

### D.3.1 Displaying Events Using `evmshow`

Because an Event Manager event is a binary data package, it must be converted to text before you can display it on a terminal. The `evmshow` command reads binary Event Manager events from its `stdin` stream or from a named file, and outputs the same events in text form to `stdout`. For example, you can display the contents of a file containing Event Manager events by using the following command:

```
# cat my_events | evmshow | more
```

This command displays the events from the log file in the default manner, that is, it takes the format data item from each event, expands it with the values of any variables it references, and displays it. References to variables are identified by a dollar sign (`$`). Therefore, if the `my_events` file contains an event with a format data item of `ext3: ext3 domain $domain is full`, and the event also contains a variable named `domain` with a value of `root_domain`, the corresponding line of the output is:

```
ext3: ext3 domain root_domain is full
```

This information tells you what happened, but not when it happened, or the importance of the event. You can modify the output of the `evmshow` command to include any data items in the event, including its timestamp and priority, by using the `-t` option to specify a show-template. A show-template is a text string that indicates which data items you want to be displayed for an event, and how you want them to be displayed.

The following example illustrates the use of a show-template to display an event with a timestamp, a priority, and the formatted event message. In the show-template, the names of the items to be displayed are each preceded by an at sign (`@`). Two at signs (`@@`) indicate that the event's format item should be expanded and displayed. The second line shows the output for the domain full event. In the output, the event priority is surrounded by brackets, and there are two spaces before the message text, exactly as specified in the show-template:

```
# cat my_events | evmshow -t "@timestamp [@priority] @@" | more
22-Jun-2000 11:22:27 [600] ext3: ext3 domain root_domain is full
```

You can set up your own show-template to display the items that are important to you, in any format you want. See `EvmEvent(5)` for a list of all the data items. After you determine your preferred style you can set a default show-template in the environment variable `EVM_SHOW_TEMPLATE` and use fewer keystrokes at the command line. The following Korn shell (`ksh`) commands are equivalent to those in the previous example:

```
# export EVM_SHOW_TEMPLATE="@timestamp [@priority] @@"
# cat my_events | evmshow | more
```

If you want more information about an event, you can request a detailed display, including an explanation and a full dump of its contents, by using the `evmshow` command with the `-d` option. The following example shows a detailed display of the domain full event:

```

# cat my_events | evmshow -d | more
===== EVM Log event =====
EVM event name: sys.unix.fs.ext3.fdmn.full

    This event is posted by the ext3 filesystem to provide
    notification that the specified ext3 domain is full.
    No more space is available for writing. [1]=
=====
Formatted Message:
    ext3: ext3 domain root_domain is full [2]

Event Data Items: [3]
    Event Name      : sys.unix.fs.ext3.fdmn.full
    Cluster Event   : True
    Priority        : 600
    PID            : 1177
    PPID           : 724
    Timestamp       : 22-Jun-2000 11:22:27
    Host IP address : 0.0.0.0
    Host Name       : x.x.example.com
    User Name       : root
    Format          : ext3: ext3 domain $domain is full [4]
    Reference       : cat:evmexp.cat:450

Variable Items: [5]
    domain (STRING) = "root_domain"
=====

```

- [1] The explanation of the event. In some cases, this data field contains a recommended action to rectify a problem.
- [2] The Formatted Message section.
- [3] The Event Data Items section, which lists all the standard data items contained in the event. See `EvmEvent(5)` for a description of each of these items.  
The items shown here are typical of many events, but sometimes some of these are missing, and occasionally you may see additional items.
- [4] The Format data item is almost the same as the content of the Formatted Message data item, but it includes a reference to a variable called *domain*, indicated by the \$ symbol preceding it.
- [5] The Variable Items section, which contains the value of the domain variable.

See Section D.3.9.2 for information on how to select events for detailed display.

You can use the `evmshow -x` command to display the explanation alone. Alternatively, use the `-x` and `-t` options together to provide a summary of the event followed immediately by its explanation. For example:

```

#cat my_events | evmshow -x -t "@timestamp [@priority] @@" | more \
21-Jun-2002 11:22:27 [600] ext3: ext3 domain root_domain is full
    This event is posted by the ext3 filesystem to provide
    notification that the specified ext3 domain is full.
    No more space is available for writing.

```

The examples in this section show how to display Event Manager events that are contained in a single log file. You can display events that are stored in the various system log files, or monitor them as they occur by using the `evmget` and `evmwatch` commands, which are introduced in Section D.3.3 and Section D.3.6.

Some systems produce a large number of events, many of which report normal operation. Use event filters to limit the display to a set of events that you consider interesting. Section D.3.2 introduces the Event Manager filtering facilities.

Regardless where the events come from, you use the `evmshow` command to format them for display. See `evmshow(1)` for more details of the show-template.



## D.3.2 Introducing Event Filters

This section introduces event filters and relates them to the `evmshow` command examples from the previous section. Filtering is used more extensively in later sections, which describe event retrieval and monitoring techniques. The full filter syntax is defined in `EvmFilter(5)`.

An Event Manager event filter is a text string that tells Event Manager which events you want to retrieve. For example, the filter string `[priority >= 600]` selects events that have a priority of 600 or higher. A filter can be very simple, but the filter language is powerful, and with some practice you can easily build and store a filter expression that defines precisely the set of events that you want to monitor. Filters are used by several of the Event Manager command line utilities, by the Event Manager logger, and by system daemons and client applications.

The `evmshow`, `evmget` and `evmwatch` commands support the `-f` option which you use to specify a filter string. You can select the events to be displayed from the `my_events` file, as shown in the following example:

```
# export EVM_SHOW_TEMPLATE="@timestamp [@priority] @@"
# cat my_events | evmshow -f "[priority >= 600]" | more
```

(The preceding example was introduced in Section D.3.1.) In this example, the `-f` option specifies the filter, and selects events that have a priority of 600 or higher. The command reads all events from the file, but returns only those events that match the filter string.

If you know the names of the events you want to retrieve, you can specify them in a filter, as shown in the following example:

```
# cat my_events | evmshow -f "[name sys.unix.fs.ext3.fdmn.full1]" | more
```

You can use wildcard characters in place of name components as follows:

- An asterisk (\*) character matches zero or more complete components
- A question mark (?) matches exactly one complete component

For example, use the following command to shorten the preceding example command:

```
# cat my_events | evmshow -f '[name *.ext3.fdmn.full1]' | more
```

The wildcard asterisk matches the components `sys.unix.fs`. To avoid any possibility that the shell expand the wildcard character with file names, enclose the filter string in single quotes instead of the double quotes. This is always a wise precaution when special characters are used in shell commands.

When you filter by name, Event Manager assumes that there is a wildcard `.*` at the end of the name string, even if it is not included in the command. Therefore, you may receive events with more name components than you specify. The following two commands are equivalent to each other, but the final wildcard (`.*`) in the first command is unnecessary:

```
# cat my_events | evmshow -f '[name *.ext3.*]'
```

```
# cat my_events | evmshow -f '[name *.ext3]'
```

You can find the names of events by specifying `@name` as one of the items in your show-template when you run the `evmshow` command.

Use the filter syntax to combine multiple conditions into a single filter with the AND, OR and NOT keywords, and you can use parentheses to group conditions. The following example command selects all events whose names include the component `ext3`, and that have a priority of 600 or higher:

```
# cat my_events | evmshow -f '[name *.ext3] and [priority >= 600]'
```

The following command also selects events with the name component `syslog`, regardless of their priority. In the following example, the keyword `priority` is

abbreviated to `pri`, and `name` is abbreviated to `na`. Most filter keywords can be abbreviated as described in `EvmFilter(5)`.

```
# cat my_events | evmshow -f '([na *.ext3] and [pri >= 600]) or [na *.syslog]'
```

The examples in this section illustrate the most commonly used filter keywords. When you are familiar with applying filters to the `evmshow` command and the Event Manager commands described in the following sections, you can use the more advanced filter features to create and save useful filters, and to increase your ability to select the events that are most interesting. Advanced filter techniques are described in Section D.3.9, and the full syntax is given in `EvmFilter(5)`.

### D.3.3 Retrieving Stored Events Using `evmget`

System log files store events in many different formats and with different levels of detail, making it difficult to produce an ordered view of all events by using traditional system utilities.

You can use the `evmget` command to produce an ordered view by retrieving events from each of the various log files, converting them to Event Manager events if they are not already in that form, and returning a single stream of Event Manager events. Using the `evmshow` command, you can then turn the Event Manager event stream into a display format.

The following command pipeline uses the `evmget` command to retrieve all system events, and passes them to the `evmshow` command for display:

```
# evmget | evmshow -t "@timestamp [@priority] @@" | more
```

The `evmget` command makes a service connection to the Event Manager daemon, which starts a new copy of the `get-server` program, `/usr/sbin/evm_getsrv`. The `get-server` program reads the channel configuration file, and runs the `get` function, usually a shell script, for each channel configured in the channel configuration file, `/etc/evmchannel.conf`.

The `get` function does the following:

- Reads the channel's log file
- Converts the events into EVM format
- Feeds events back to the `evmget` command which writes them to its `stdout` stream

After all the channel `get` functions run and all the events are returned, the `get-server` daemon and the `evmget` command both terminate.

---

#### Note

---

Even though events may be stored in log files as lines of text, or in a special binary format, the `evmget` command returns all events in the form of binary Event Manager events, which can be passed to `evmshow` for display. If you send the output of `evmget` directly to your terminal, the command displays an error message because the binary output cannot be displayed properly and could affect the settings of your terminal. If you pipe the output into another command, such as `more` or `less`, the `evmget` command is unable to detect the error, and random characters are displayed.

---

Like the `evmshow` command, the `evmget` command supports a filter option to allow you to limit the events it returns. For example, the following command displays only high-priority events:

```
# evmget -f '[pri >= 600]' | evmshow | more
```

It is more efficient to specify a filter with the `evmget` command than with the `evmshow` command. This is because the `evmget` command passes its filter string to the event channel's `get` function, which only returns events that match the filter. Fewer events are passed back through the `get-server` daemon to the `evmget` command, and the commands operate faster because they transfer and process fewer events.

If you want to save retrieved events for later analysis, or to copy them to another system, you can redirect the output of the `evmget` command into a file. For example:

```
# evmget -f '[pri >= 600]' > my_events
```

Saving the binary output of the `evmget` command provides greater flexibility than saving the text output of the `evmshow` command. At a later time you can sort and filter the binary file and pass it to the `evmshow` command to view it in any format you like.

As you experiment with `evmget`, you will see that the events appear in batches, usually ordered chronologically. Each `get` function feeds its events back to the `evmget` command, which then outputs them in the order in which it received them. Because you usually want to see events in some order (often, but not always, chronological), you need to pipe the events through the `evmsort` command, which is described in Section D.3.4. Section D.3.5 introduces using the `evmget -A` command, which lets you retrieve, sort, and display events without building a pipeline.

Depending on the size and type of your system and the number of events being logged, event retrieval may take a noticeably long time. This is because each retrieval operation requires every channel's `get` function to read through its log files, convert its events to Event Manager events, and then apply the filter string (if any) to determine whether the event is passed back to the `evmget` command. The larger the log files, the longer this process takes.

Careful log file management helps to speed up the process. If you know that you want to display events that belong to a particular event channel, you can shorten the process by using the `evmget -C` command to display only the specified channel. For example:

```
# evmget -f '[pri >= 600]' -C syslog | evmshow | more
```

In this example, the `get` function runs only on the `syslog` channel, so the command completes its task quickly. A filter string is specified to return events that have a priority greater than 600. You can determine what channels are configured by using the `evminfo -lc` command, or by examining the channel configuration file. See `evminfo(1)` for more information.

### D.3.4 Sorting Events Using `evmsort`

The `evmsort` command takes a stream of Event Manager events as input, sorts them into the requested order, and writes them to its `stdout` stream. The command is most useful in sorting the output from the `evmget` command, but it can be used to sort Event Manager events from any source. See `evmsort(1)` for more information.

Section D.3.3 explained that the events retrieved by the `evmget` command are output in batches, corresponding to the event channel configuration. You can use the `evmsort` command to sort the events into a preferred order, before passing them to the `evmshow` command for display. The following example shows a typical command sequence:

```
# export EVM_SHOW_TEMPLATE="@timestamp [priority] @@"
# evmget -f '[pri >= 600]' | evmsort | evmshow | more
```

By default, the `evmsort` command sorts events into chronological order, so the previous command is suitable for most cases. You can use the `-s` option to declare a sort specification if you want the events sorted differently. A sort specification is a text string that defines one or more sort keys, which are the data items on which you want to sort the events. The specification is a list of data item names, separated by colons (:). For example:

```
priority:timestamp
```

The preceding specification sorts events by timestamp within priority, so the first group of events that are returned are those with the lowest priority, sorted in their order of occurrence. You may use this specification as follows:

```
# evmget -f '[pri >= 600]' | evmsort -s "priority:timestamp" | evmshow | more
```

The default sort order is ascending, but you can change it to descending for an individual item specifier by appending a minus sign (-). You can explicitly request ascending order by specifying a plus sign (+). For example, the following command displays the highest priority events first (descending order), but within each priority range the events are sorted oldest first (ascending order):

```
# evmget -f '[pri >= 600]' | evmsort -s "priority-:timestamp+" | evmshow | more
```

For consistency with the `show-template` syntax, the `evmsort` command allows you to precede each item specifier with an at (@) character, as described in Section D.3.1. There is no requirement to do this, and it does not affect the operation.

When you establish your sorting preferences, you can create a new default sort sequence by setting the environment variable `EVM_SORT_SPEC`. The following Korn shell (`ksh`) commands are equivalent to the previous example:

```
# export EVM_SORT_SPEC="priority-:timestamp+"
# evmget -f '[pri >= 600]' | evmsort | evmshow | more
```

You can override the value of the `EVM_SORT_SPEC` variable at any time by supplying a different sort specification with the `-s` option.

### D.3.5 Using the `-A` Option to Simplify the Command String

The Event Manager commands are designed to be building blocks, with each command doing one specific operation. This gives you great flexibility in developing shell scripts to manipulate event information. When you enter commands from the command line you may prefer to simplify the command.

The most common command sequence for event retrieval is the `evmget` command, piped into the `evmsort` command, piped into the `evmshow` command. You can then pipe the text output into the `more` command to display the output. Consider the following example:

```
# evmget -f '[pri >= 600]' | evmsort -s "priority-:timestamp+" |
evmshow | more
```

You can simplify the preceding command by using the `evmget -A` command option, which automatically pipes the command output to other Event Manager commands. For example, you can use the `-A` option to simplify the previous command example as follows:

```
# evmget -A -f '[pri >= 600]' -s "priority-:timestamp+" | more
```

When the `evmget -A` command starts, it automatically runs the `evmsort -A` command, and pipes its output into that command. When the `evmsort` command starts, the `-A` option causes it to start the `evmshow` command, piping events into it for display. You can supply a sort specification with the `-s` option and a show-template with the `-t` option. These options are passed along to the `evmsort` command and `evmget` commands respectively.

The `evmwatch` command supports the `-A` described in Section D.3.6.

### D.3.6 Monitoring Events Using `evmwatch`

You can use the `evmwatch` command to monitor event activity through a terminal window. This command is an Event Manager subscribing client. It makes a connection to the Event Manager daemon, sends it a subscription request, and waits to receive events. As events arrive, the `evmwatch` command writes them to the standard out stream (`stdout`) as binary Event Manager events.

You cannot display the output of the `evmwatch` command because it is a stream of binary events. You must use the `evmshow` command to format the events. The following example monitors all events, and displays them on your terminal as they occur:

```
evmwatch | evmshow -t "@timestamp [priority] @"
```

Depending on your system type, and the level of event activity, this command may run for a while before any events are displayed. The command continues to run until you terminate it to regain control of your terminal, usually by pressing `Ctrl/C`.

When a system is operating correctly, many of the events posted are low-priority informational events. You may want to filter these events out, particularly if your system has a high level of event activity. You can do this by supplying a filter to the `evmwatch` command:

```
# evmwatch -f "[priority >= 400]" |  
evmshow -t "@timestamp [priority] @"
```

This example watches for events with a priority of error or higher. You can change the filter string to exclude any set of events that occur regularly and are uninteresting. Alternatively, you may need to watch for a particular set of events.

The preceding examples do not show the output of `evmshow` piped into `more` for display, because `evmwatch` is a realtime monitor. The `evmwatch` command displays events as they occur, rather than displaying them from a file. A command like `pg` or `more` may wait for the operator to intervene before reading more data from its input pipe; over time, this could lead to congestion in the pipeline. The Event Manager daemon cannot wait for its client (the `evmwatch` command) to clear its backlog; this results in the `evmwatch` command missing events. You should display the output from the `evmwatch` command directly on a terminal window, instead of using of piping commands to `more` or `pg`; also use the scroll bar to review the event list.

Avoid piping the output of the `evmwatch` command into the `evmsort` command because the `evmsort` command cannot sort events until it reads to the end of its input. As a monitoring program, the `evmwatch` command usually waits for input until it is killed explicitly. As a result, if you pipe the output of the `evmwatch` command directly into the `evmsort` command, there is no output from the `evmsort` command.

The `-A` option simplifies the command string by running the `evmsort` command and the `evmshow` command automatically. The `evmwatch` command also supports the `-A` option and automatically runs the `evmshow` command when you use it. You can specify a show-template as an option to the `evmwatch` command as follows:

```
# evmwatch -A -f "[priority >= 400]" -t \@timestamp \  
[priority] @"
```

As with the `evmget` command, you can capture a set of interesting events in a file, to review later. It is more useful to store events in binary form than in text form, so you should send the output of the `evmwatch` command directly to a file, as shown in the following example, rather than piping it into the `evmshow` command first.

```
# evmwatch -f "[priority >= 400]" > my_events
```

The `evmwatch` command supports additional options that are useful for monitoring events from within a shell script. See `evmwatch(1)` for more information.

### D.3.7 Understanding the Event Manager Mark Event

When you review or monitor event activity, you observe the following event that occurs every 15 minutes:

```
26-Jun-2000 08:57:45 [200] EVM: Mark event
```

The `evmlog` event channel posts this event to ensure that there is periodic event activity. If your system has a problem and you need to determine when it was last operational, you can look for mark commands in the system log by using the following command:

```
# evmget -f "[name *.evm.mark]" | evmshow -t "@timestamp @last_timestamp @@"
26-Jun-2000 00:57:35 26-Jun-2000 04:42:40 [16 times] EVM: Mark event
26-Jun-2000 04:57:41 - EVM: Mark event
26-Jun-2000 05:12:41 - EVM: Mark event
26-Jun-2000 05:27:41 - EVM: Mark event
26-Jun-2000 05:42:41 26-Jun-2000 09:12:45 [15 times] EVM: Mark event
```

If the default logger configuration file is in use, you usually see three individual mark events, followed by a single event preceded by `[n times]`, where `n` is a number up to 16. This is the result of the logger's suppression facility, which minimizes wasted space by combining multiple events over a period of up to four hours. The normal timestamp value shows the first occurrence of a combined event, and the `last_timestamp` data item shows the time of the last occurrence. The example includes the `last_timestamp` data item in the show-template, which displays the last mark event, posted at `09:12:45`. This mark event tells you that the system was operational at that time.

To disable mark event posting, edit the channel configuration file to make either of the following changes:

- Comment out the `evmlog` channel's `fn_monitor` entry to disable it completely
- Change the `mon_period` value for the channel to change the frequency with which the event is posted

See Section D.2.2 and `evmlogger.conf(4)` for more information about event suppression.

### D.3.8 Viewing Events Using the Event Viewer

The graphical event viewer provides a simple and convenient interface to the system event logs. The event viewer is an integral part of the AMS system management suite; you can use it in a character cell terminal or from a Web browser.

To launch the event viewer from SPM refer to Section 2.6.4; to launch from PCM see Section 5.8.4.

When you run the event viewer for the first time a warning message may indicate that events are filtered to show only high priority events. If your system is operating normally it is likely that no events are displayed in the event summary window.

To choose the events you want to see, select `Filter...` at the bottom of the window, and change the filter criteria in the Filter window. If you want to see all stored events, make sure that all the check boxes at the left side of the window are in the unchecked state, and select `OK`.

If your system produces a high level of event activity you can reduce the number of events shown, and the time taken to display them, by checking the `Priority` box and adjusting the priority range. Setting the range to `400-700` displays all events with

a priority of `error` and higher. Setting the low end of the range to 300 includes warning events in the display.

You can check any of the buttons at the left of the Filter window to include additional criteria in the display filter. Each time you make a change you must select `Apply` to apply the change to the event list, or select `OK` to apply the change and return to the main viewer window.

The Filter dialog window offers an intuitive and convenient way for you to build an event filter string without having to type it. If you are familiar with the filter syntax and you want to make better use of its power, you can enter a filter string through the Advanced Filter dialog box, which you access by selecting `Options...` at the bottom of the main event window. You can also save a filter string and reuse it later. For more information about the filter syntax, see `EvmFilter(5)`.

One of the most important features of the viewer is the ease with which you can display a detailed view of any event. Simply select the event in the summary window and select `Details...` to see all the information available. From the Event Details window you can browse through the event list without returning to the main window.

You can change the viewer display by selecting `Customize...` and `Options...`. To change the order in which events are displayed, select `Sort...`. Select `Help...` from any window for detailed information about the viewer and its facilities.

---

#### Note

---

The event viewer does not monitor event activity in real time. To display an updated view of the event list, select `Refresh` from the main window.

---

### D.3.9 Advanced Selection and Filtering Techniques

The following section describes some additional filtering techniques that you can use to further improve event selection, so that you receive only the events in which you are interested.

- How to filter events according to their time of posting (Section D.3.9.1)
- How to filter using the `event-id` identifier (Section D.3.9.2)
- How to filter using reserved component names (Section D.3.9.3)
- How to use filter files (Section D.3.9.4)

#### D.3.9.1 Filtering By Time

You can filter for events according to the time at which they were posted by using the `timestamp`, `before`, `since`, and `age` keywords. You may find that the `age` keyword is the easiest of these keywords to use, and the most useful for everyday operation.

When you use the `timestamp` keyword, you must supply a string that defines a time range in the following way:

```
year:month-of-year:day-of-month:day-of-week:hours:minutes:seconds
```

You can use an asterisk (\*) as a wildcard character for any of the components, so to select events that occurred on July 6, 2002 you may use the following commands:

```
# export EVM_SHOW_TEMPLATE="@timestamp [@priority] @@"  
# evmget -A -f '[timestamp 2002:7:6:*:*:*:]' | more
```

The asterisks (\*) in the final four components indicate that you are interested in all events that occurred on that day, no matter what time they occurred. Also, you can specify one or more ranges in any position, as shown in the following command:

```
# evmget -A -f '[timestamp 2002:*:*:1-3,5:*:*:]' | more
```

The fourth component specifies the day of the week. Searching for events with posting times in the range 1-3 or 5 yields all events that were posted on a Monday, Tuesday, Wednesday or Friday in the year 2002.

The `before` and `since` keywords use similar specifier strings, but you cannot use wildcard characters and there is no day of the week indicator. For example, the following command finds events that were posted after 3:00p.m. on July 6, 2002:

```
# evmget -A -f '[since 2002:7:6:15:0:0]' | more
```

The `age` keyword provides a more convenient and intuitive way to select events according to their timestamps. As a system administrator you may be most interested in recent events that indicate a system problem. You can combine the event filter's `priority` and `age` keywords to find such events. For example, the following command sequence shows all events with a priority of error (400) or higher, that occurred either yesterday or today (the age of the event is less than 2 days):

```
# evmget -A -f '[pri >= 400] and [age < 2d]' | more
```

In the preceding example, `2d` specifies events that are less than 2 days old. You can specify an age in seconds (`s`), minutes (`m`), hours (`h`), days (`d`), or weeks (`w`). See `EvmFilter(5)` for information about how each specifier is used in calculating an event's age.

You can use a more complex filter to return events that occurred within a more specific period. The following example finds error events that occurred more than 3 days ago, but less than 6 days:

```
# evmget -A -f '[pri >= 400] and ([age < 6d] and [age > 3d])' | more
```

See `EvmFilter(5)` for detailed information on selecting events according to their timestamps, and the full filter syntax.

### D.3.9.2 Using the event-id to Select Events for Detailed Display

Using the `evmshow -d` command option to display events can result in a large amount of output and you may want to limit the number of displayed events. Events that are posted through Event Manager contain a sequential identifier known as the `event-id`. You can use the `event-id` to select a specific event or a range of events for detailed display.

The `event-id` is not guaranteed to be unique within any particular set of events because the daemon's counter is set to zero each time it is restarted. To ensure that an event is unique, you must also use the timestamp when selecting events as shown in the following example:

```
# evmget -A -f '[age < 1d]' -t "@timestamp @event_id @" | more
15-Apr-1999 14:19:06 0 EVM daemon: Configuration completed
15-Apr-1999 14:19:06 1 EVM daemon: Initialization completed
15-Apr-1999 14:19:06 2 EVM logger: Logger started
15-Apr-1999 14:19:06 3 EVM: Mark event - initial
15-Apr-1999 14:19:06 5 EVM logger: Started eventlog /var/evm/evmlog/evmlog.19990415
1
2
.
.
.
```

**1** The `age` filter keyword selects all events that have occurred today, as indicated by the timestamp in the first column of data.

**2** The `@event_id` specifier in the show template instructs the `evmshow` command to display the `event-id` for each retrieved event, which is shown in the second column of data.



When the `event-ids` are displayed, you can select the interesting events. For example, use the following command to display details of the initial mark event, which has an `event-id` of 3 in the preceding example output:

```
# evmget -f '[age < 1d] and [event_id = 3]' | evmshow -d | more
```

You can select a range of events by using a more complex filter as shown in the following example:

```
# evmget -f '[age < 1d] and [event_id >= 1] and [event_id <= 3]' |
  evmshow -d | more
```

Choose the time range carefully to select the right set of events. If you recently rebooted your system, specify a filter of `[age < 2h]` to select events occurring within the preceding 2 hours.

The most convenient way to select events for detailed display is to use the event viewer described in Section D.3.8.

### D.3.9.3 Searching for Reserved Component Names

Some event names include reserved component names as name extensions. These components begin with an underscore character (`_`), and usually are followed by a component that identifies the item for which the event is being posted. For example, the names of many hardware-related events include the component `_hwid`, followed by the numeric hardware identifier of the item. Reserved component names are appended automatically as an extension to the event name. The name is appended, followed by the value for the named variable. This is done for every reserved component name. For example, an event with the name `@SYS_VP@.temperature_high` and the variable `_degrees` with the value 212 would be observed as an event with the name `@SYS_VP@.temperature_high._degrees.212`.

You can search for all such events by using the following command:

```
# evmget -A -f '[name *._hwid]' | more
```

If you know the hardware identifier of a specific device, you can narrow the search for events related to that device by using a command similar to the following:

```
# evmget -A -f '[name *._hwid.4]' | more
```

### D.3.9.4 Using Filter Files

You can save a useful filter in a file and recall it by using the Event Manager's indirect filter facility. Filter files have names with the suffix `.evf`, and can contain any number of named filters. For example, the following filter file entry selects all `syslog` events that refer to SCSI devices:

```
filter {
  name "scsi"
  value "[name @SYS_VP@.syslog.hw.scsi]"
  title "Syslog SCSI events"
}
```

In this example, the `@SYS_VP@` is a standard Event Manager macro that is replaced by `sys.unix` when the filter is used.

To use indirect filtering, specify the at sign (`@`), followed by the name of the file containing the filter instead of a filter string, as shown in the following example:

```
# evmget -A -f @syslog
```

You do not need to include the `.evf` suffix when you specify a filter file name in such commands.

The previous example uses the first filter in the file, but you can choose a different filter by specifying its name as follows:

```
# evmget -A -f @syslog:scsi
```

You can include as many filters as you like in a single file, or you can keep each filter in its own file. The preceding example specifies the `syslog` filter, which is included in Event Manager. Other filters are provided in the `/usr/share/evm/filters` directory. Use these files as examples for establishing your own filter library.

The `evmshow -F` command option provides an easy way for you to see the contents of a stored filter. The `-F` option causes the `evmshow` command to display the filter string and then exit without reading any events. In the following example, the `evmshow` command displays the contents of the filter named `scsi`, stored in the `syslog.evf` file:

```
# evmshow -f @syslog:scsi -F
( [name sys.unix.syslog.hw.scsi] )
```

See `evmfilterfile(4)` for complete information about the syntax of filter files, and where to locate your files.

---

#### Note

---

Do not edit the filter files provided in the `/usr/share/evm/filters` directory. Your changes may be overwritten without warning by a future installation update.

---

### D.3.10 Logging and Forwarding Events

The response to an event is any action determined by your site-specific needs and conditions. This response can range from activating alarms or paging responsible personnel, to making a log entry or ignoring an expected occurrence of a regular activity.

You can configure the event processing sequence to perform a series of dependent tasks, by using an event output by one task as the trigger to activate the next process. Event Manager provides an interface to the response activity through the logging facility. The available options are event storage and event forwarding.

The Event Manager logger, `evmlogger`, started automatically by the Event Manager daemon, is responsible for the following:

- Displaying selected events on the system console or other device  
If a terminal device is indicated as the `logfile` in the configuration file, all events meeting the filter specifications of an `eventlog` statement are formatted for display on the terminal. (See Section D.2.2 for a discussion of the configuration file.)
- Storing selected events in one or more log files
- Forwarding selected events to interested parties in some other form

By default, the logger handles events posted through its local daemon, but you can also configure it to handle events posted on remote systems.

The logger is an ordinary Event Manager client that is controlled through a configuration file. The default is the `/etc/evmlogger.conf` file, described in Section D.2.2. See `evmlogger.conf(4)` for more information on this file and `evmlogger(8)` for more information on the command.

### D.3.10.1 Logging Events

All events meeting the specifications of an `eventlog` group in the configuration file are written to the event log. See Section D.1.4 for the default location of this file and the naming conventions.

As shown in Example D-1, you can include a `suppress` group specification in an `eventlog` statement in the configuration file. When you include such a statement, events meeting the suppression criteria are not entered in the log. One instance of the event is stored, with additional data indicating the number of events and the time of the first and last occurrence of the event. See `evmlogger.conf(4)` for the explanation of this criterion.

### D.3.10.2 Using Forwarding to Handle Events Automatically

If you want to automate the handling of selected events, you can configure the Event Manager logger to forward the event by executing a command. For example, you can mail the event information to a paging service, or invoke an event-handling application program.

By default, the logger is configured to mail high priority events to the root user. You can use that default forwarding command as an example for developing your own actions. See Section D.2.2 and `evmlogger.conf(4)` for more information.

All events meeting the filter specifications of a `forward` statement in the configuration file are written to the standard input (`stdin`) of the command specified in the statement. The command is the name of a shell script, a single command, a series of commands (pipeline), or any other executable statement. The following operations are typically specified as a forwarding action:

- Specifying the `mail` command or `mailx` command, or another command line mail processor, to send a mail message to a responsible person or paging service
- Invoking additional software that causes emergency shutdown procedures to commence
- Invoking a dependent process that is waiting for the event to occur

When configuring the logger to forward an event, note the following:

- The event selected for forwarding is piped into the configured forwarding command. If your commands need to deal with text information, the `evmshow` command must be the first command in the pipeline so that the event is converted to text form.
- The logger executes the forwarding command asynchronously, meaning that it starts the command and then continues with its normal operation without waiting for the command to finish. The following behaviors are normal:
  - If multiple forwarders are specified in the logger's configuration file, and the same event is to be handled by more than one forwarder, the logger starts each forwarding command without waiting for the others to finish, so the commands may execute simultaneously.
  - If the logger receives another event to be processed by a forwarding command, and the command is still processing the previous event, the logger queues the new event. When the command finishes, the logger restarts it, passing it the new event. By default, the logger queues up to 100 events for each forwarding command. You can increase this limit by specifying a `MAXQUEUE` keyword in the forwarder's configuration.

See `evmlogger.conf(4)` for more information.

- Event text may include characters such as quotes, which have special meaning to the shell. Be sure to post test versions of the event to verify that your command executes correctly under realistic conditions.

- You must take care that the forwarding command does not itself result in the posting of events which would cause an event loop. For example, if you use mail to forward events, the forwarder's filter must exclude mail events.

Use the logger's secondary configuration file facility for adding forwarders or other configuration items as described in REFERENCE.

## D.4 Troubleshooting Event Manager

The following list describes actions you can take if you encounter specific problems:

- A subscribing application fails to receive expected events  
Verify that the user is a member of `amsgroup` by checking that the user's name is present in `/etc/group`.

```
# more /etc/evm.auth
```

Verify that the event is registered by using the following command:

```
# evmwatch -i -f '[name event_name]' |
  evmshow -t "@name"
```

If the events are still not shown, run `evmreload` and examine it again. If they are still not visible, verify that the template files are correctly installed.

Verify that the subscriber is authorized to access these events, by using the following command:

```
# more /etc/evm.auth
```

Verify that the expected events are actually being posted by using the following command:

```
# evmwatch | evmshow -t "@name @@"
```

Run the program that posts the event, and verify that the preceding `evmwatch` command displays them correctly.

- Event retrieval through `evmget` or the event viewer is slow

Examine the sizes of all log files, particularly the `evmlog` files (`/var/evm/evmlog`).

Use the `ls -l` command when listing file sizes to ensure that you see the file itself and not a symbolic link.

- Expected events are not being logged

Examine the event priority from the PCM user interface. Only events with a priority of 200 or higher are logged by the Event Manager logger.

- `evmlogger`: Missed receipt of *number* events

This error occurs when events overflow the receive buffer, whose size is set to the default system socket buffer maximum. You can alter this value by following the Linux kernel tuning instructions provided with your Linux distribution.

---

## Sending Selected Events Via E-mail

### E.1 Overview

This appendix describes how to send selected Event Manager (EVM) events via e-mail.

After you configure the Server Platform Manager (SPM) or Platform Console Manager (PCM) to generate events from console error messages (Section 5.8.3), you can perform the steps outlined in this procedure to send those events via e-mail. You can also send events to a cellular phone or pager that is capable of receiving alphanumeric messages. See Section E.2 for more information.

EVM provides a means for system components or applications to indicate when something of interest has happened, such as a disk failure or a task completion. These indications are called events. You can configure EVM to monitor events on your system and to notify you as soon as interesting events occur. Using this procedure, you can configure EVM to notify you by forwarding the event information through e-mail.

EVM sends e-mail messages of events with a priority of 700 or higher to the root user of the AMS, by default. This procedure shows you how to specify the user name and priority you want.

See Appendix D and the EVM chapters in the *Tru64 UNIX System Administration manual* and *Programmer's Guide* for more information.

### E.2 Sending Selected Events to a Cellular Phone or Pager

When you configure EVM to send events to a cellular phone or pager, you can use the e-mail address of the device to send events to it. Use the procedure outlined in Section E.5 and substitute the example e-mail address with the device's e-mail address.

Read the literature that came with your device to determine that it is capable of receiving alphanumeric messages, determine its e-mail address, and to learn how to use its messaging capability.

### E.3 EVM Configuration File

To specify the user name and event priority you want, edit the EVM logger's configuration file `/etc/evmlogger.conf`. The `/etc/evmlogger.conf` file is a text file that configures the display, forwarding, or storage of events for the EVM logger. All events meeting the specifications of an `eventlog` statement in the configuration file are written to the specified event log or device. This appendix describes how to add entries to the `/etc/evmlogger.conf` file to forward these events as formatted text.

### E.4 Using Templates with `evmshow`

You can use templates with the `evmshow` command to select the information you want to see about each event and to format the display of the information.

```
evmshow -t "@timestamp [@priority] @@"
```

In this example, `evmshow` replaces `@timestamp` with the time at which the event took place, `@priority` with the priority level of the event, and `@@` with the event's formatted text as specified in the `format_specifier` of the event template file. The example output appears as follows:

```
evmshow -t "@timestamp [@priority] @@"
```

## E.5 Editing the EVM Logger Configuration File

To specify the user name and event priority you want to e-mail:

1. Log into the AMS machine as root.
2. Create a Bourne shell script similar to the following that can receive a single EVM event from its `stdin` stream, format it, and mail it to the e-mail address you want. The following examples use `email_me` as the file name.

The script uses a template with the `evmshow` command and the `mail` command, which uses the e-mail address you specify.

```
#!/bin/sh

string=`evmshow -t "EVM alert [@host_name]: @@" `
(echo Subject: $string
 echo $string
) | mail jr_admin@company.com
```

This example executes the `evmshow` command, formats the information using a template, and assigns the result to the variable `string`. The definition of the `string` variable uses back quotes (```).

The `evmshow` command replaces the data item specifier, `@host_name`, with the literal host name of the system on which the event takes place. It also replaces `@@` with the event's formatted text.

The Bourne shell script then executes two `echo` commands. The first creates a Subject line using the information assigned to the `string` variable for the text of the subject. The second repeats the `string` variable for the message body text.

The script pipes the resulting message through the `mail` command, which sends it to the e-mail address you specify. You must replace the example electronic mail address, `jr_admin@company.com`. You can use your own electronic mail address for testing purposes.

3. Change the permission of the Bourne shell script you created with the `chmod` command so that it is executable.

```
# chmod 744 email_me
```

4. Check the contents of the `/etc/evmlogger.conf` file to see if there is an existing forward entry. If there is, we recommend that you copy it and edit the copied entry rather than edit the original.

```
forward {
    name     email_me1

    # Don't forward mail events through mail
    filter   "[prio >= 600] & ![name @SYS_VP@.syslog.mail]"2

    suppress3
    {
        filter   "[name *]"
        period   120 # minutes
        threshold 1 # No. of duplicates before suppression
    }
    command   "full_directory_path/email_me"4
}
```

<sup>1</sup> Any name can be supplied.

- 2 This line posts any event that has a priority equal to or greater than 600 and is not a mail event. An event with a priority of 600–699 is an Alert and an event with a priority of 700 is an Emergency.  
You must filter out mail events because the forwarding command makes use of the mail system. If the mail system encounters a problem, it might post a high priority event. This can cause an endless event loop if you continue to forward high priority mail events through the mail system.
- 3 You can suppress duplicate events to prevent unnecessary duplicate notifications. This example suppresses any event that has occurred twice within 120 minutes.
- 4 You must provide the full pathname of the Bourne shell script you created in step 2.  
You can specify a person's e-mail address or the e-mail address of a cellular phone or pager.

5. Instruct the logger to reload the `/etc/evmlogger.conf` file:

```
# evmreload -l
```

Reloading the logger configuration file causes EVM to begin using the new configuration. You must enter `evmreload -l` every time you modify the `/etc/evmlogger.conf` file.

## E.6 Verifying Success

After you apply this procedure, you can verify whether it was successful.

1. In step 2, use an electronic mail address with which you can test the notification.
2. Create an event with a priority higher than the minimum priority entered in `/etc/evmlogger.conf`.  
# `evmpost -a "Test Message" -p 700`  
This example posts an administrator's quick message and assigns it a priority of 700. Since the example filter used in the procedure selects events with a priority of 600 or greater, this test event meets the selection criteria and a mail notification is sent.
3. Create an event that matches the minimum priority entered in `/etc/evmlogger.conf`.  
# `evmpost -a "Test Message" -p 600`  
This example posts an administrator's quick message and assigns it a priority of 600. Since the example filter used in the procedure selects events with a priority of 600 or greater, this test event meets the selection criteria and a mail notification is sent.
4. Create an event with a priority that is less than the minimum priority entered in `/etc/evmlogger.conf`. This verifies whether it successfully filters out events that do not match.  
# `evmpost -a "Test Message" -p 599`  
This example posts an administrator's quick message and assigns it a priority of 599. Since the example filter used in the procedure selects events with a priority of 600 or greater, this test event does not meet the selection criteria; therefore, a mail message is not sent.
5. Check your mail program for notifications of the two events that match the filter criteria.

## E.7 Troubleshooting

If you determine that this procedure was not successful, as described in Verifying Success, use the following table to identify and solve problems:

Problem	Possible Solutions
The event neither appeared on the system console nor sent mail.	<ul style="list-style-type: none"><li>• Enter the <code>evmreload -l</code> command to reload the logger file.</li><li>• Check to see if the event matches the filter parameters in <code>/etc/evmlogger.conf</code>.</li><li>• Check the values entered in the suppress entry in the <code>/etc/evmlogger.conf</code> file to ensure that the event has not been repeated within the given time period.  For testing purposes, temporarily comment out the suppress entry by entering a pound sign (#) at the beginning of each suppress line and then enter <code>evmreload -l</code> to reload the logger file.</li></ul>
The event appeared on the console but no mail was sent.	<ul style="list-style-type: none"><li>• Ensure that the Bourne shell script file is executable.</li><li>• Select the option to retrieve new messages in your mail viewer.</li><li>• Ensure that the command entry in <code>/etc/evmlogger.conf</code> calls out the correct name of the shell script.</li><li>• Ensure that the Bourne shell script includes the correct electronic mail address.</li><li>• Enter the <code>evmreload -l</code> command to reload the logger file.</li></ul>
The event message was not received.	<ul style="list-style-type: none"><li>• There may be a delay before the device receives the notification. Wait for a few minutes for the notification to be received.</li><li>• Enter the <code>evmreload -l</code> command to reload the logger file.</li></ul>



---

## Regular Expressions

The event definition files use regular expression rules to determine whether there is a match between a given expression and the console output. Regular expressions are described in the `grep(1)` reference page. Regular expression symbols should not be confused with glob symbols `*` and `?`.

The following special characters may be helpful when making changes to event definitions:

- `^` (circumflex)

When used as the first character of an expression, it anchors an expression to the beginning of a line. For example, `^Unable to obtain requested swap space` indicates that the expression must be at the beginning of a line.

- `$` (dollar sign)

At the end of a pattern, it causes that pattern to match only if the last matched character is the last character (not including the newline character) on a line. For example, `Unable to obtain requested swap space$` indicates that the phrase must be at the end of a line.

- `^$` (circumflex and dollar sign)

The construction `^pattern$` restricts the pattern to matching only an entire line. For example, the regular expression `^abcd$` matches lines containing the string `abcd`, where `a` is the first character on the line and `d` the last.

- `.` (period)

When used outside a bracket expression, matches any single character.

- `+` (plus sign)

Matches one or more occurrences of a character. For example, `hel+o` matches "hello" and "hellllo".

- `.+` (period and plus sign)

Match any and all characters. It is similar to glob symbol `*`. For example, `NFS3 server .+ not responding` will produce a match with any characters substituted for `.+` — provided that they are preceded by "NFS3 server" and succeeded by "not responding".



## Navigating the Character Cell Environment

This appendix contains a key guide for use with the character cell environment. Refer to it when using the Platform Console Manager (PCM).

To make selections, open dialog boxes, enter text, and scroll through console logs, you should be familiar with navigating the character cell environment. The following table describes the keys that are used for each task.

**Table G-1: Character Cell Navigation Key Guide**

<b>General Navigation Tasks</b>	<b>Keys</b>
Display the character cell keyboard online help.	Ctrl-g
Move to the next selectable section of the dialog box. For example, move from the Description column header to the selectable list of systems.	Ctrl-n or Tab
Move to the previously selectable section of the dialog box. For example, move from the Configure... selection to the Events... selection.	Ctrl-p
Activate the selection.	Enter or Space
<b>Single Line Entry Tasks</b>	<b>Keys</b>
Scroll right or left.	Right arrow or left arrow
Jump to the end of the line.	Ctrl-e
Jump to the start of the line.	Ctrl-a
<b>Multi-Line Entry Tasks</b>	<b>Keys</b>
Scroll list up or down.	Up arrow or down arrow
Scroll list right or left.	Right arrow or left arrow
Scroll up one page.	Ctrl-u or Page Up
Scroll down one page.	Ctrl-d or Page Down
Jump to the start of the line.	Ctrl-a
Jump to the end of the text.	Ctrl-e
<b>List Tasks</b>	<b>Keys</b>
Double-click the selection.	Enter
Single-click or select the highlighted list item.	Space
Scroll the list up or down.	Up arrow or down arrow
Scroll the list right or left.	Right arrow or left arrow
Scroll up one page.	Ctrl-u or Page Up
Scroll down one page.	Ctrl-d or Page Down

---

<b>List Tasks</b>	<b>Keys</b>
Jump to the start of the line.	Ctrl-a
Jump to the end of the text.	Ctrl-e

---

This glossary provides definitions for many of the terms you will see while using the AlphaServer Management Station (AMS) documentation. Although the majority of terms are related to the AMS, other terms related to platform management are included.

## Special Characters

/  
See *root*

## 1

### **2p drawer**

A chassis with backplane that supports one dual processor module, five PCI/PCI-X slots, and one AGP slot.

### **8p drawer**

A chassis with backplane that supports four dual processor modules.

## A

### **available swap space**

The amount of swap space not reserved by processes. In contrast, free swap space is everything except for the space actually in use. Available swap space is smaller than free swap space because it takes into account both the space that is in use and any reservations that processes may have made. Free swap space does not take reservations into account.

See also *swap space*

## B

### **backplane manager**

See *MBM*

### **base operating system**

The operating system without any additional third-party or layered products installed. All software subsets that are located on the first CD-ROM comprise the base operating system.

### **boot time**

The time when the operating system is initializing. In the case of a cold boot, the hardware also is initialized.

### **bootable**

Having the ability to load and initialize the operating system.

### **Bourne shell**

The command interpreter and interpreted programming language originally developed by Steve Bourne.

See also *shell*

## C

### **character device**

A data storage or transfer device that manipulates data in increments of a single character; for example, a terminal.

### **client**

A computer system that uses resources provided by another computer system called a server.

### **CMM**

CPU management module. A plug-in card on the dual processor module that provides local module power and initialization control.

### **console**

A port number assigned to a platform or system that allows you to connect to and monitor the platform or system.

### **console mode**

When the system is halted, the operating system is no longer running, and the console subsystem is started. This state is also known as console mode and is recognizable by the console mode prompt, which is represented by three right arrow characters (>>>). The console mode prompt is sometimes called triple arrows or chevron prompt.

### **corporate LAN**

A conventional local area network (LAN), or wide area network (WAN), used for remote management by connecting to the multi-server LAN.

### **CPU module**

See *dual processor module*

## D

### **default**

Any value that is set automatically by an application or process.

### **default partition**

1. The partition used by a system as the default boot partition.
2. The physical portion of a disk that usually is assigned by the installation process to hold a specific file system.

See also *partition*

### **default partition table**

The disk partitions that are defined in the `/etc/disktab` file or, in the absence of an entry in that file, the disk driver itself. The default partition table varies with disk type because it depends upon the size of the disk itself. The `disklabel -p` command is used to view a disk's default partition table.

See also *partition table*

### **device**

1. The general name for any peripheral hardware connected to the processor that is capable of receiving, storing, or transmitting data. For example, card readers, line printers, and terminals are record-oriented devices. Magnetic tape devices and disks are examples of mass storage devices. Terminal line interfaces and interprocessor links are examples of communication devices.
2. The files in the `/dev` directory that are used to access physical devices are themselves sometimes called devices.

**device name**

The name or address used to access a physical disk. Device names are located in the `/dev` directory.

**domain**

1. Any single element of a domain name. Using `host1.nyc.bigcorp.com` as an example: `nyc.bigcorp.com` is the domain and `host1` is the unique host name.
2. Any qualified portion of a domain name. Qualified means that the domain name is fully specified all the way to the root domain. Using `host1.nyc.bigcorp.com` as an example: `nyc.bigcorp.com`, `bigcorp.com`, and `.com` are qualified domains.
3. The domain, and all the subdomains beneath it, down to the leaf nodes of the domain space tree. Using `nyc.bigcorp.com` as an example: `nyc.bigcorp.com` is the name of the domain, and the domain encompasses all the hosts located in `nyc` (New York City).

**dual processor module**

A module containing two processor chips, memory modules, voltage regulator modules (VRMs), and a CPU management module (CMM).

See also *CMM*

**E****external LAN**

See *corporate LAN*

**F****firmware**

The software stored in silicon (for example, ROM or EPROM) on a system's CPU board. Firmware is also known as console code. Firmware is the first software that runs when a system is turned on, and it directly controls all hardware. Each hardware platform uses a different set of firmware. The firmware on a platform is the same regardless of the operating system installed on the platform. Thus, firmware is platform dependent, but is not operating system independent.

**fully qualified host name**

A host name containing one or more labels separated by a period that uniquely defines a computer. A label is a string which begins with a letter and contains letters, digits, and hyphens and ends with a letter or a digit. A label can have between 2 and 63 characters, inclusive. A fully qualified host name can have a maximum of 254 characters. For example, `host1.nyc.bigcorp.com` is a fully qualified host name.

See also *domain*

**H****hard partition**

A subset of a system's computing resources that cannot exchange information or resources with any other partition on the system. The boundaries are maintained by a switch in the system chip. Faults are not propagated across hard partition boundaries.

**high performance I/O drawer**

An enclosure that has 8 high-speed (133 MHz) PCI-X buses, with four I/O riser modules.

**host**

1. The primary or controlling computer in a communications network.
2. Any computer system attached to a network.

**host name**

The name given to a computer. Lowercase and uppercase letters (a-z and A-Z), numbers (0-9), periods, and dashes are permitted in host names. Valid host names contain from 2 to 63 characters with the first character being a letter.

**HTML**

HyperText Markup Language. The coding (markup) inserted in a file intended for display on a World Wide Web browser that tells the browser how to display the words on a web page. The markup is done with *tags*, which are command words enclosed in angle brackets. For example, the tag **<P>** creates a new paragraph; the tag **<TABLE>** begins the formatting of a table. Although the World Wide Web Consortium (W3C) promotes the standardization of HTML, both Netscape and Microsoft browsers currently implement some features differently and provide nonstandard extensions.

**HyperText Markup Language**

See *HTML*

**I****I/O drawer**

See high performance I/O drawer and standard I/O drawer.

**I/O expander module**

A module in the 2P drawer used to provide backplane manager logic and controllers for CD-ROM, SCSI disks, LAN, keyboard, mouse, and modem.

**I/O port**

Logic that provides an interface from the system chip to the I/O chip on I/O riser modules.

See also *I/O riser module*

**I/O riser module**

Module containing the I/O chip that functions as the interconnect between the system chip and PCI, PCI-X, and AGP buses. The standard I/O drawer has one I/O riser module; the high-performance I/O drawer can have up to four I/O riser modules.

**init**

A command that initializes the system by creating and controlling processes. This command also polls the hardware so that it is known to the Full Installation process. The processes run by the *init* command at each run level are defined in the */etc/inittab* file.

**init process**

The root process created by the system that performs system administration tasks, such as spawning login processes and handling the orderly shutdown from multiuser to single-user mode.

**instance**

An operating system running in a partition.

**internal LAN**

A local network that connects the microprocessors used to manage a single ES47, ES80, and GS1280 platform at the lowest level by plugging into the system hub.



**internet address**

A unique 32-bit number that identifies a host's connection to an internet network. An internet address consists of a network number and a host number.

**Internet Protocol**

See *IP*

**IP**

Internet Protocol. The network layer protocol for the Internet protocol suite that provides the basis for the connectionless, best-effort packet delivery service. IP includes the Internet Control Message Protocol (ICMP) as an integral part. The Internet protocol suite is referred to as TCP/IP because IP is one of the two most fundamental protocols.

**IP address**

A 32-bit quantity used to represent a point of attachment in an Internet. Periods (.) delineate each portion of the address.

See also *IP*

**K****kernel**

The core part of the operating system that controls processes, system scheduling, memory management, input and output services, device management, network communications, and the organization of the file systems.

**Korn shell**

A command interpreter and interpreted programming language developed by David Korn. The Korn shell (*ksh*) is semantically an extended version of the Bourne shell, with constructs and commands to implement enhanced features, including job control and command history recall. The POSIX shell is a superset of the Korn shell.

See also *shell*

**ksh**

The command that invokes the Korn shell; the name of the executable file that is the shell.

See also *Korn shell, shell*

**L****LAN**

Local Area Network. A group of two or more computer systems (hosts) connected by a transmission medium, such as an Ethernet cable, token ring, or FDDI. Each host is connected to the transmission medium by a hardware interface. A LAN is a data communications network that spans a physically limited area, such as a single office building. It usually is owned by the organization it services and provides high-bandwidth communication over inexpensive media.

See also *network*

**LED**

Light Emitting Diode. Diodes that emit visible light when electricity is applied. They are similar to light bulbs, but use much less electricity and respond much faster.

**local area network**

See *LAN*

**log in**

To begin using a computer system, usually by entering a login name and password to gain access to and communicate with the operating system as an authorized user.

**M****MBM**

backplane manager. A module on the backplanes of both the 2P and 8P drawers that controls the CPU management modules (CMMs) and has logic to monitor and control environmental conditions in the drawer.

See also *base operating system*

**mount**

To attach a file system to an existing directory to make the file system available for use. File systems are mounted by the `mount` command.

See also *unmount*

**mount point**

A directory that is the name of a mounted file system.

**multiprocessor**

A system with two or more processors sharing common physical memory.

**multi-server LAN**

Used to manage one or more AlphaServers from the AlphaServer Management Station (AMS) using high-level tools including Server Platform Manager (SPM) and AlphaServer Management Utility (AMU). Connects to each server's router (NAT) box.

**N****NAT box**

See *Network Address Translator box*.

**network**

Two or more computing systems that are linked for the purpose of exchanging information and sharing resources.

**Network Address Translator box**

The Network Address Translator box. Found on ES47, ES80, and GS1280 platforms, the NAT box is not part of the internal LAN. It is programmed to have a unique address on the multi-server LAN, and translate requests to this address to specific components within the internal LAN via the LAN management hub.

**NFS**

Network File System. A service that allows a system (the server) to make file systems available across a network for mounting by other systems (clients). When a client mounts an NFS file system, the client's users see the file system as if it were local to the client.

**NFS mounted**

Refers to a file system that is mounted over a network by NFS rather than being physically connected (local) to the system on which it is mounted.

See also *NFS*

## P

### **partition**

The physical portions of a disk that are named a through h. Disks are divided into sections that are then assigned to hold various file systems. By convention, the / (root) file system is always located on the first partition, named a. The /usr file system is on a different partition, often the g partition. The c partition usually represents the entire disk. Each partition may differ in size and can overlap other partitions. Two overlapping partitions cannot be used at the same time. Disks can have up to eight partitions. Partitions are sometimes known as *slices*.

### **partition table**

The component of a disk label that specifies how a physical disk is divided or partitioned.

### **password**

A string of characters that in conjunction with other information, such as the login name, uniquely confirms a user's identity to the system. Passwords should contain a combination of upper and lower case letters, numbers, and special characters and must be a minimum of six to a maximum of 16 characters in length.

### **path**

An ordered list of the directories in which the shell searches for the executable files named by commands that are not entered with a pathname and are not shell built-in commands.

### **pathname**

The name of a file, concatenated onto a list of the directories through which access to that file is achieved; hence, the complete name of the file. Absolute pathnames begin at the root directory and are written with an initial slash (for example, /usr/users/rolf/myfile.txt). Relative pathnames begin at the user's working directory and are written without the initial slash (for example, rolf/myfile.txt).

### **PBM**

PCI backplane manager. Monitors and controls the activity and environment in the I/O drawers.

### **PCI backplane manager**

See *PBM*

### **private LAN**

See *multi-server LAN*

## R

### **reboot**

To bring the system down to console mode and restart the operating system.

### **reference page**

One of a collection of files containing documentation on all commands, system calls, library routines, and so forth. Reference pages are often called manual pages or man pages.

### **regular expression**

A pattern of one or more characters used to find text information and formed according to a set of rules that define how the characters are to be interpreted. For example, a period is interpreted as a valid match for any character in the input. The regular expression a.c matches any string containing the letter a and the letter c separated by a single intervening character, such as abc, a?c, a9c, and so on.

**root**

1. The login name for the superuser (system administrator).

See also *superuser*

2. The name applied to the topmost directory in the UNIX system's tree-like file structure; hence, the beginning of an absolute pathname. The root directory is represented in pathnames by an initial slash (/); a reference to the root directory itself consists of a single slash.

See also *pathname*

**root directory**

See *root*

**root file system**

The topmost file system under which all other file systems are mounted. The root file system contains the operating system files that get the rest of the system running.

**root login**

See *root*

**S****script**

1. A nonbinary program that is interpreted and executed by a specified shell.
2. In the *sed* editor, a list of editing commands to be applied to the input file.

**server**

A computer system that provides software or services to one or more other computers called clients.

See also *client*

**setld**

A command that is used to install, manage, and remove software subsets on a system that is already running the operating system.

**sh**

The command that invokes the Bourne shell.

**shell**

A program that interprets commands entered by the user, invoking programs and calling for system resources as needed.

See also *Korn shell*

**single-user mode**

An operating system mode that prohibits user logins, stops system services and daemons (for networking and graphical windowing environments), stops any running processes, and unmounts file systems.

**soft partition**

A subset of a hard partition's computing resources. There are no hardware boundaries between soft partitions. Hardware faults are propagated throughout the mesh of soft partitions.

**SRM console**

Firmware on the backplane manager module that provides a command-line interface for operator control of the system or of a partition. The SRM console is responsible for booting the operating system and passing system configuration data, discovered during power-up, to it.

**standard I/O drawer**

An enclosure, with eleven PCI/PCI-X slots and one AGP slot, that contains a single I/O riser module. An optional standard I/O module may be present to control an optional CD-ROM drive and SCSI storage drives.

**su**

A command that substitutes another user's login for that of the user who invoked the command, logging in the invoking user under the substituted login. The invoking user must know the login password for the user whose login is being substituted. If no other user's login is specified, the command substitutes the root login.

**superuser**

A user possessing privileges to override the normal restrictions on file access, process control, and so forth. A user who possesses these privileges becomes a superuser by issuing the `su` command, or by logging into the system as the user `root`.

**swap space**

Disk space used to hold modified memory from an idle or low priority process in order to reclaim the physical memory that the process is using.

**symbolic link**

A file that contains the pathname of another file or directory and acts as a pointer to that file or directory. The symbolic link can occur within the same file system or across file systems; also called a soft link or sym link.

**SysMan Menu**

A menu of system management tasks organized in a tree-like hierarchy with branches of general functionality and leaves for actual tasks. Selecting a leaf opens a dialog for performing the task. Depending on the user's display device, the SysMan Menu provides either a graphical or text-based interface. The SysMan Menu is invoked from the command line by entering `/usr/sbin/sysman` or from the CDE Application Manager if your system is running the CDE desktop.

**system**

A subdivision of a platform that runs an operating system.

**U****unmount**

The process that announces to the system that a file system previously mounted on a specified directory is to be removed. Only the person who mounted the particular file system or a superuser can unmount it. A file system is unmounted with the `umount` command.

See also *mount*

**URL (Uniform Resource Locator)**

The address of a file or other resource accessible on the Internet. The type of file or resource depends on the Internet application protocol. For example, using the HyperText Transfer Protocol (HTTP), the file can be an HTML page, an image file, or a program such as a CGI application or Java applet. Such an address would look like this: `http://www.hp.com`, which is the URL for the HP corporate web site.

**V****version**

The number assigned to a particular release of the base operating system or to layered software products.

See also *base operating system*

## A

---

### **Add and configuring a platform**

for the AMU, 3-2

### **AlphaServer Management Station**

( *See* AMS )

### **AlphaServer Management Utility**

( *See* AMU )

### **AlphaServer Partition Wizard**

( *See* APW )

### **AMS**

configure, 1-6

overview, 1-1

### **AMU**

accessing, 2-15

bottom right frame, 3-7

Activity tab, 3-7

Alerts tab, 3-7

configuring a platform, 3-2

connecting to a console, 3-10

connecting to platform's management port, 3-11

creating and modifying partitions with, 3-26

description of, 1-4

displaying a graphical representation of the platform, 3-5

displaying the platform's I/O and power connections, 3-9

left frame, 3-3

main window, 3-3

monitoring a platform's environmental status, 3-10

overview of, 3-1

refreshing the graphical display of cable connections, 3-29

running as standalone application, 3-2

running from SPM, 3-3

starting, 3-1

top right frame, 3-4

hardware view, 3-4

logical view, 3-5

upgrading firmware with, 3-13

viewing with AMU, 3-11

Visual Editor, 3-31

working with partitions, 3-15

### **APW**

accessing from SPM, 2-16

adding hard partition with, 4-10

committing a partition map, 4-16

creating new partition map with, 4-14

creating soft partition with, 4-13

description of, 1-5

managing APW files, 4-18

modifying a partition map with, 4-9

modifying hard partition with, 4-11

overview of, 4-1

Resources Window, 4-6

running from command line, 4-2

running from SPM, 4-1

saving a partition map, 4-15

validating a partition map, 4-16

### **Archived logs**

access with Event Manager, D-10

### **Authorization file**

Event Manager, D-9

## B

---

### **Backplane Manager**

( *See* MBM )

## C

---

### **Cable connections**

refreshing AMU graphical display of, 3-29

### **Character cell environment**

navigating, G-1

### **CMF**

see cmfd, 5-1

### **cmfd**

restarting from the PCM, 5-14

starting, 1-6

stopping from the PCM, 5-14

### **Configuring the AMS, 1-6**

### **Console**

adding a standalone console, 2-23

adding with PCM, 5-10

broadcasting to users in SPM, 2-25

connecting from AMU, 3-10

connecting using PCM, 5-22

determining status in PCM, 5-22

disconnecting users, 5-24

enabling and disabling in SPM, 2-26

identifying users in SPM, 2-24

log files

managing in PCM, 5-25

viewing and archiving in SPM, 2-30

logging output from, 2-25

- managing using PCM, 5-21
- modifying properties with PCM, 5-12
- monitoring output in PCM, 5-23
- removing with PCM, 5-13
- Telnet to from SPM, 2-24
- viewing logs in the PCM, 5-23
- viewing output with PCM, 5-6
- viewing properties in SPM, 2-27
- working with in SPM, 2-24

**Console Management Facility**  
( See cmfd )

**CPU**

- viewing properties of, 3-31

**Cut and paste operations, 2-3**

---

## D

**Drawers**

- ( See I/O Drawers, System Drawers )

**Dual Processor Modules**

- ( See Duo )

**Duo, 4-4**

- ( See also APW; Partition )

- assigning in partition maps, 4-4
- viewing in APW Resources Window, 4-6
- viewing number of in hard partition, 4-6
- viewing properties of in AMU, 3-31

---

## E

**/etc/evmlogger.conf**

- ( See evmlogger.conf file )

**Event**

- enabling and disabling in SPM, 2-21
- generating from console error messages in the PCM, 5-18
- model of, D-1
- sending via e-mail, E-1
- suppression of, D-23
- viewing in SPM, 2-22
- working with in PCM, 5-15

**Event definition file**

- creating and modifying in SPM, 2-28

**Event Manager**

- administration, D-5
- administrative utilities, D-3
- archived (zipped) logs, D-10
- authorization file, D-9
- channel manager, D-10
- command line utilities, D-2
- configuration files, D-4
- description of, D-1
- event logging, D-23
- event suppression, D-23
- evmchmgr command, D-10

- evmviewer, D-18
- evmwatch, D-1
- features, D-1
- initialization files, D-3
- log file management, D-10
- logger configuration, D-6
- processing events automatically, D-23
- responding to events, D-22
- reviewing logged events, D-18
- security considerations, D-9
- system files, D-3
- troubleshooting, D-24
- user authentication, D-9
- using in administration, D-11
- utilities, D-2

**Event Viewer**

- accessing in SPM, 2-22

**Events**

- viewing with Recent Events tab, 2-10

**evm.auth file, D-9**

**evmchmgr command, D-3, D-10**

**evmd daemon, D-3**

**evmget command, D-3**

**evmlogger command, D-3, D-22**

**evmlogger.conf file, D-22**

**evmreload command, D-3**

**evmshow command, D-3**

**evmsort command, D-3**

**evmstart command, D-3**

**evmstop command, D-3**

**evmviewer utility, D-18**

**evmwatch command, D-1, D-3**

---

## F

**firmware**

- alerts for environmental group, B-1t
- alerts for EV7 group, B-3t
- alerts for operational group, B-2t
- alerts for partition group, B-2t
- alerts generated by in AMU, 3-7

**Firmware**

- upgrading with AMU, 3-13

**Frequency**

- viewing dual CPU module, 3-31

---

## G

**Generic console**

- ( See Console, adding a standalone console )

---

## H

**HP Insight Management Agents**

- accessing with SPM, 2-20



## I

---

### I/O

displaying in AMU, 3-9

### I/O Drawers

viewing properties of in AMU, 3-30

### Icons

displaying a legend, 3-6

## J

---

**Java Security Certificate**, 2-2

## L

---

### LED

testing with AMU, 3-29

### log files

( *See Console* )

### Log files

viewing with AMU, 3-11

### Logged events

reviewing, D-18

### Logical view

graphical display in AMU, 3-5

## M

---

### Management Port

( *See MBM* )

### Master SCM

( *See SCM* )

### MBM

connecting to using AMU, 3-11

connecting to using PCM, 5-20

connecting to with SPM, 2-14

errors and warnings, 2-9

prompt for, 5-21

recent events, 2-10

## N

---

### NAT box

overview, 1-3

### Network Address Translator

( *See NAT box* )

## O

---

### OpenVMS Galaxy

multiple subpartitions, 4-1

## P

---

### Partition, 2-19

( *See also Subpartition* )

adding with APW, 4-10

creating and modifying with AMU,  
3-26

creating new partition map with APW,  
4-14

modifying with APW, 4-11

platform differences in APW, 4-2

viewing with SPM, 2-15

working with in AMU, 3-15

working with partition maps, 4-4

### Partition Maps

( *See Partition* )

### Partition Wizard

( *See APW* )

### PCM

adding a console, 5-10

adding a platform, 5-7

connecting to a console, 5-22

connecting to platform's management  
port, 5-20

customizing Telnet escape sequence,  
5-2

description of, 1-5

determining console status, 5-22

disconnecting users from a console,  
5-24

exiting, 5-2

generating events from console error  
messages, 5-18

main window, 5-2

managing console log files, 5-25

managing consoles, 5-21

modifying console properties, 5-12

modifying platform properties, 5-12

monitoring console output, 5-23

overview, 5-1

removing a console from, 5-13

removing a platform from, 5-13

starting, 5-2

working with events, 5-15

### Platform

adding or modifying with SPM, 2-11

adding with PCM, 5-7

displaying I/O and power connections  
in the AMU, 3-9

hardware status, 2-9

management LAN, 1-3

management port

connecting using the AMU, 3-11

connecting using the PCM, 5-20

connecting using the SPM, 2-14

managing with SPM, 2-13

modifying properties with PCM, 5-12

monitoring environmental status in the  
AMU, 3-10

NAT box, 1-3

removing with PCM, 5-13

- removing with SPM, 2-19
- required template for use in AMU, 3-2

**Platform Console Manager**  
( *See* PCM )

**Port mapping**, 2-26

**Power Connections**  
displaying in AMU, 3-9

## Q

---

### QBB

- assignment in APW, 4-2
- viewing in APW Resources Window, 4-6

## R

---

### Resources Window

( *See* APW )

### Restarting the cmfd

, 5-14

### Router

( *See* NAT box )

## S

---

### SCM

, 2-15

### Security

- event management, D-9

### Security Certificate

( *See* Java Security Certificate )

### Sending events via e-mail

, E-1

### Server Platform Manager

( *See* SPM )

### soft partition

( *See* subpartition )

### Soft Partition

- creating with APW, 4-13

### SPM

- accessing HP Insight Management Agents, 2-20
- accessing the AMU, 2-15
- adding a standalone console, 2-23
- adding or modifying a platform, 2-11
- assigning privileges, 2-4
- broadcasting to users, 2-25
- configuring a subpartition, 2-19
- connecting to platform's MBM, 2-14
- customizing the main window, 2-11
- default partitions, 2-15
- description of, 1-3
- disconnecting users, 2-24
- enabling and disabling events
  - generated from console output, 2-21
- hardware warnings and errors for all platforms, 2-9
- identifying users, 2-24
- left frame, 2-6

- log files
  - viewing and archiving, 2-30
- logging in, 2-3
- main window, 2-5
- managing platforms, 2-13
- managing subpartitions, 2-19
- mapping a port, 2-26
- monitor bar, 2-5
- overview of, 2-1
- removing a platform, 2-19
- running APW from, 4-1
- top right frame, 2-7
- turning console logging off, 2-25
- using locally, 2-2
- using remotely, 2-2
- using the Event Viewer, 2-22
- viewing a console's properties, 2-27
- viewing a platform's properties, 2-16
- viewing console log, 2-25
- viewing online help, 2-2
- viewing recent events, 2-10
- viewing subpartition properties, 2-23

**standalone application**  
running AMU as, 3-2

**Starting the cmfd**, 1-6

**Starting the Tomcat Web Server**, 1-6

**Stopping the cmfd**, 5-14

**Subpartition**  
configuring with SPM, 2-19  
managing with SPM, 2-19  
viewing properties with SPM, 2-23

**System Control Manager**  
( *See* SCM )

**System drawers**  
viewing properties of with AMU, 3-29

**System files**  
Event Manager, D-3

**System logs**  
reviewing using event viewer, D-18

## T

---

### Telnet

- customizing escape sequence in PCM, 5-2
- to consoles from SPM, 2-24

### Tomcat Web Server

- starting, 1-6

### Troubleshooting

- AMS components, A-1
- event management (Event Manager), D-24

## V

---

### Viewing console logs

, 5-23

### Visual Editor

, 3-31

## **W**

---

### **Web Server**

( *See Tomcat Web Server* )

### **Windows**

changing appearance, 4-1

displaying button usage, 4-2

### **Wizard**

( *See APW* )

## **Z**

---

### **Zipped log files**

( *See Archived logs* )