HP Availability Manager User's Guide

Order Number: AA-RNSJD-TE

January 2005

This guide explains how to use HP Availability Manager software to detect and correct system availability problems.

Revision/Update Information:	This guide supersedes the *HP OpenVMS Availability Manager User's Guide*, Version 2.3-1.
Operating System:	**Data Analyzer:** Windows 2000 SP 4 or higher; Windows XP SP 1; OpenVMS Alpha Version 7.2-1 or later OpenVMS I64 Version 8.2 or later **Data Collector:** OpenVMS Alpha and VAX Version 6.2 or higher, OpenVMS I64 Version 8.2 or higher
Software Version:	HP Availability Manager Version 2.4-1

Hewlett-Packard Company
Palo Alto, California

Printed in the US

ZK6552

The HP OpenVMS documentation set is available on CD-ROM.

This document was prepared using DECdocument, Version 3.3-1b.

Contents

4 Displaying OpenVMS Cluster Data

5 Getting Information About Events

6 Performing Fixes on OpenVMS Nodes

7 Customizing the Availability Manager

Examples

Figures

Tables

Preface

Intended Audience

This guide is intended for system managers who install and use HP Availability Manager software. It is assumed that the system managers who use this product are familiar with Windows terms and functions.

Note

The term Windows as it is used in this manual refers to either Windows 2000 or Windows XP but *not* to any other Windows product.

Document Structure

This guide contains the following chapters and appendixes:

- Chapter 1 provides an overview of Availability Manager software, including security features.
- Chapter 2 tells how to start the Availability Manager, use the main Application window, select a group of nodes and individual nodes, and use online help.
- Chapter 3 tells how to select nodes and display node data; it also explains what that data is.
- Chapter 4 tells how to display OpenVMS Cluster summary and detailed data; it also explains what that data is.
- Chapter 5 tells how to display and interpret events.
- Chapter 6 tells how to take a variety of corrective called **fixes**, to improve system availability.
- Chapter 7 describes the tasks you can perform to filter, select, and customize the display of data and events.
- Appendix A contains a table of CPU process states, which are referred to in Section 3.2.2.4 and in Section 3.3.1.
- Appendix B contains a table of OpenVMS and Windows events that can be displayed in the Events pane discussed in Chapter 5.
- Appendix C describes the events that can be signaled for each type of OpenVMS data that is collected.

Related Documents

The following manuals provide additional information:

- *HP OpenVMS System Manager's Manual* describes tasks for managing an OpenVMS system. It also describes installing a product with the POLYCENTER Software Installation utility.
- *HP OpenVMS System Management Utilities Reference Manual* describes utilities you can use to manage an OpenVMS system.
- *HP OpenVMS Programming Concepts Manual* explains OpenVMS lock management concepts.

For additional information about HP OpenVMS products and services, visit the following World Wide Web address:

`http://www.hp.com/go/openvms`

Reader's Comments

HP welcomes your comments on this manual. Please send comments to either of the following addresses:

Internet	**openvmsdoc@hp.com**
Postal Mail	Hewlett-Packard Company OSSG Documentation Group, ZKO3-4/U08 110 Spit Brook Rd. Nashua, NH 03062-2698

How to Order Additional Documentation

For information about how to order additional documentation, visit the following World Wide Web address:

`http://www.hp.com/go/openvms/doc/order`

Conventions

The following conventions are used in this guide:

Ctrl/*x*	A sequence such as Ctrl/*x* indicates that you must hold down the key labeled Ctrl while you press another key or a pointing device button.
PF1 *x*	A sequence such as PF1 *x* indicates that you must first press and release the key labeled PF1 and then press and release another key or a pointing device button.
Return	In examples, a key name enclosed in a box indicates that you press a key on the keyboard. (In text, a key name is not enclosed in a box.) In the HTML version of this document, this convention appears as brackets, rather than a box.

. . .	A horizontal ellipsis in examples indicates one of the following possibilities: • Additional optional arguments in a statement have been omitted. • The preceding item or items can be repeated one or more times. • Additional parameters, values, or other information can be entered.
. . .	A vertical ellipsis indicates the omission of items from a code example or command format; the items are omitted because they are not important to the topic being discussed.
( )	In command format descriptions, parentheses indicate that you must enclose choices in parentheses if you specify more than one.
[ ]	In command format descriptions, brackets indicate optional choices. You can choose one or more items or no items. Do not type the brackets on the command line. However, you must include the brackets in the syntax for OpenVMS directory specifications and for a substring specification in an assignment statement.
|	In command format descriptions, vertical bars separate choices within brackets or braces. Within brackets, the choices are optional; within braces, at least one choice is required. Do not type the vertical bars on the command line.
{ }	In command format descriptions, braces indicate required choices; you must choose at least one of the items listed. Do not type the braces on the command line.
bold type	Bold type represents the introduction of a new term. It also represents the name of an argument, an attribute, or a reason.
italic type	Italic type indicates important information, complete titles of manuals, or variables. Variables include information that varies in system output (Internal error *number*), in command lines (/PRODUCER=*name*), and in command parameters in text (where *dd* represents the predefined code for the device type).
UPPERCASE TYPE	Uppercase type indicates a command, the name of a routine, the name of a file, or the abbreviation for a system privilege.
`Example`	This typeface indicates code examples, command examples, and interactive screen displays. In text, this type also identifies URLs, UNIX commands and pathnames, PC-based commands and folders, and certain elements of the C programming language.
-	A hyphen at the end of a command format description, command line, or code line indicates that the command or statement continues on the following line.
numbers	All numbers in text are assumed to be decimal unless otherwise noted. Nondecimal radixes—binary, octal, or hexadecimal—are explicitly indicated.

1
Overview

This chapter answers the following questions:

- What is the HP Availability Manager?
- How does the Availability Manager work?
- How does the Availability Manager identify possible performance problems?
- How does the Availability Manager maintain security?

1.1 What Is the HP Availability Manager?

The HP Availability Manager is a system management tool that allows you to monitor, from an OpenVMS or Windows node, one or more OpenVMS nodes on an extended local area network (LAN).

The Availability Manager helps system managers and analysts target a specific node or process for detailed analysis. This tool collects system and process data from multiple OpenVMS nodes simultaneously, analyzes the data, and displays the output using a graphical user interface (GUI).

Features and Benefits

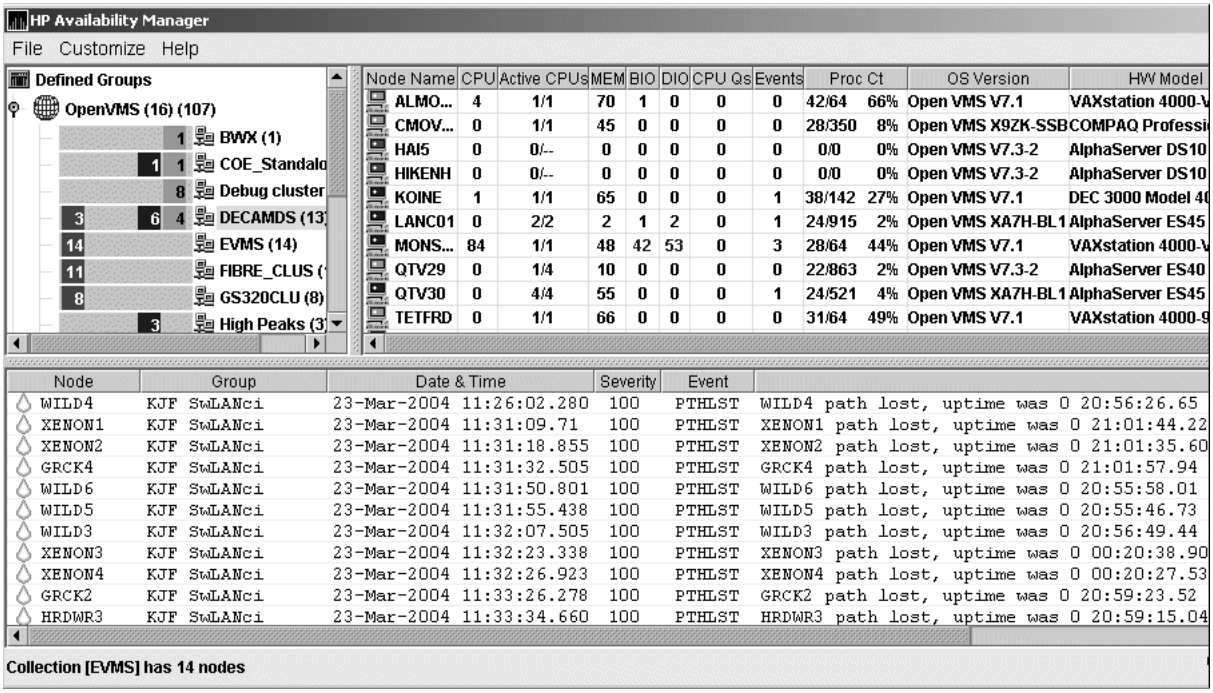
The Availability Manager offers many features that can help system managers improve the availability, accessibility, and performance of OpenVMS nodes and clusters.

Feature	Description
Immediate notification of problems	Based on its analysis of data, the Availability Manager notifies you immediately if any node you are monitoring is experiencing a performance problem, especially one that affects the node's accessibility to users. At a glance, you can see whether a problem is a persistent one that warrants further investigation and correction.
Centralized management	Provides centralized management of remote nodes within an extended local area network (LAN).
Intuitive interface	Provides an easy-to-learn and easy-to-use graphical user interface (GUI). An earlier version of the tool, DECamds, uses a Motif GUI to display information about OpenVMS nodes. The Availability Manager uses a Java GUI to display information about OpenVMS nodes on an OpenVMS or a Windows node.
Correction capability	Allows real-time intervention, including adjustment of node and process parameters, even when remote nodes are hung.

Feature	Description
Uses its own protocol	An important advantage of the Availability Manager is that it uses its own network protocol. Unlike most performance monitors, the Availability Manager does not rely on TCP/IP or any other standard protocol. Therefore, even if a standard protocol is unavailable, the Availability Manager can continue to operate.
Customization	Using a wide range of customization options, you can customize the Availability Manager to meet the requirements of your particular site. For example, you can change the severity levels of the events that are displayed and escalate their importance.
Scalability	Makes it easier to monitor multiple OpenVMS nodes.

Figure 1–1 is an example of the initial Application window of the Availability Manager.

Figure 1–1 Application Window



The Application window is divided into the following sections:

- In the upper left section of the window is a list of user-defined groups of nodes. You can click either the name of a group or the icon in front of it to select a group.
- In the upper right section is a list of the nodes in the group you selected. Double-click a node name or the icon in front of it to display more detailed data for that node. You can also double-click data items in each row to display more detailed data about a specific item.
- In the lower section events are posted, alerting you to possible problems on your system.

1.2 How Does the Availability Manager Work?

The Availability Manager uses two types of nodes to monitor systems:

- One or more OpenVMS Data Collector nodes, which contain the software that collects data.
- An OpenVMS or a Windows Data Analyzer node, which contains the software that analyzes the collected data.

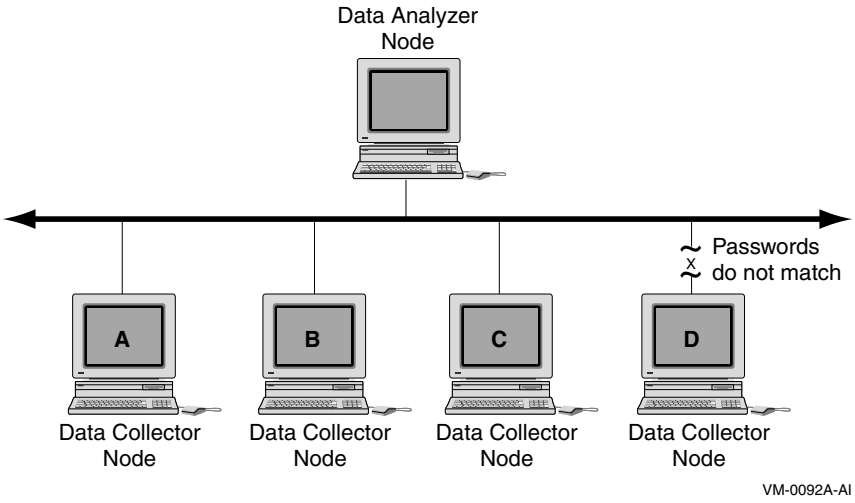
The Data Analyzer and Data Collector nodes communicate over an extended LAN using an IEEE 802.3 Extended Packet format protocol. Once a connection is established, the Data Analyzer instructs the Data Collector to gather specific system and process data.

Although you can run the Data Analyzer as a member of a monitored cluster, it is typically run on a system that is not a member of a monitored cluster. In this way, the Data Analyzer will not hang if the cluster hangs.

Only one Data Analyzer at a time should be running on each node; however, more than one can be running in the LAN at any given time.

Figure 1–2 shows a possible configuration of Data Analyzer and Data Collector nodes.

Figure 1–2 Availability Manager Node Configuration



In Figure 1–2, the Data Analyzer can monitor nodes A, B, and C across the network. The password on node D does not match the password of the Data Analyzer; therefore, the Data Analyzer cannot monitor node D.

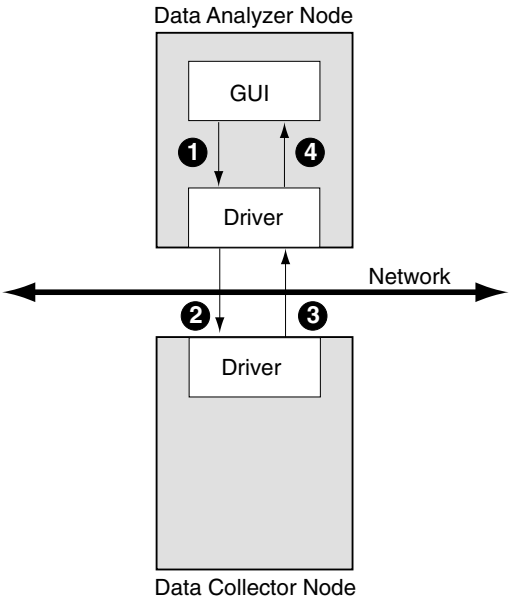
For information about password security, see Section 1.4.

Requesting and Receiving Information

After installing the Availability Manager software, you can begin to request information from one or more Data Collector nodes.

Requesting and receiving information requires the Availability Manager to perform a number of steps, which are shown in Figure 1–3 and explained after the figure.

Figure 1–3 Requesting and Receiving Information



The following steps correspond to the numbers in Figure 1–3.

❶ The GUI communicates users' requests for data to the driver on the Data Analyzer node.

❷ The Data Analyzer driver sends users' requests across the network to a driver on a Data Collector node.

❸ The Data Collector driver transmits the requested information over the network to the driver on the Data Analyzer node.

❹ The Data Analyzer driver passes the requested information to the GUI, which displays the data.

In step 4, the Availability Manager also checks the data for any events that should be posted. The following section explains in more detail how data analysis and event detection work.

1.3 How Does the Availability Manager Identify Performance Problems?

When the Availability Manager detects problems on your system, it uses a combination of methods to bring these problems to the attention of the system manager. If no data display is open for a particular node, the Availability Manager reduces the data collection interval so that data can be analyzed more closely. Performance events are also posted in the Event pane, which is in the lower portion of the Application window (Figure 1–1).

The following topics are related to detecting problems and posting events:

- Collecting and analyzing data
- Posting events

1.3.1 Collecting and Analyzing Data

This section explains how the Availability Manager collects and analyzes data. It also defines terms related to data collection and analysis.

1.3.1.1 Types of Data Collection

You can use the Availability Manager to collect data either as a background activity or as a foreground activity.

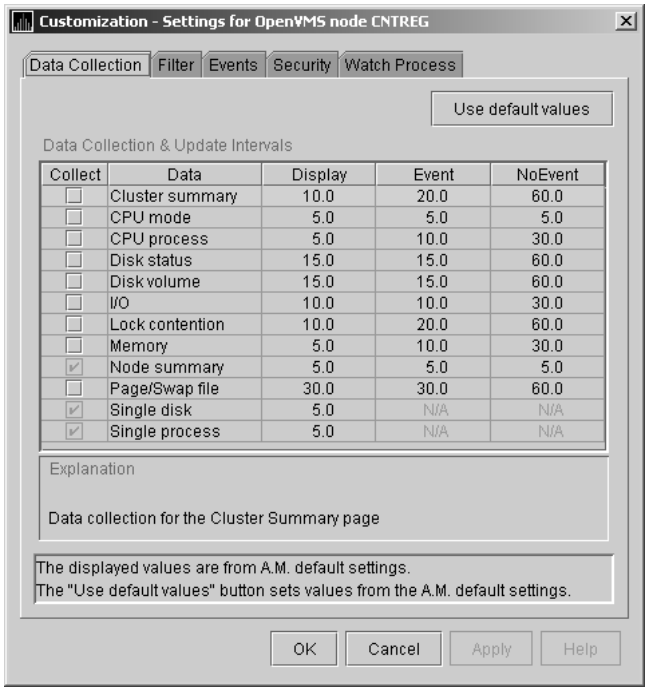
- **Background** data collection

  When you enable background collection of a specific type of data on a specific node, the Availability Manager collects that data whether or not any windows are currently displaying data for that node.

  To enable background data collection, select the check box for a specific type of data on the Data Collection Customization page (Figure 1–4). Note that if the Customize window applies to all OpenVMS nodes, the data collection properties that you set are for all nodes. If the window applies to a specific node, the properties you set apply only to that node.

  Chapter 7 contains instructions for customizing data collection properties.

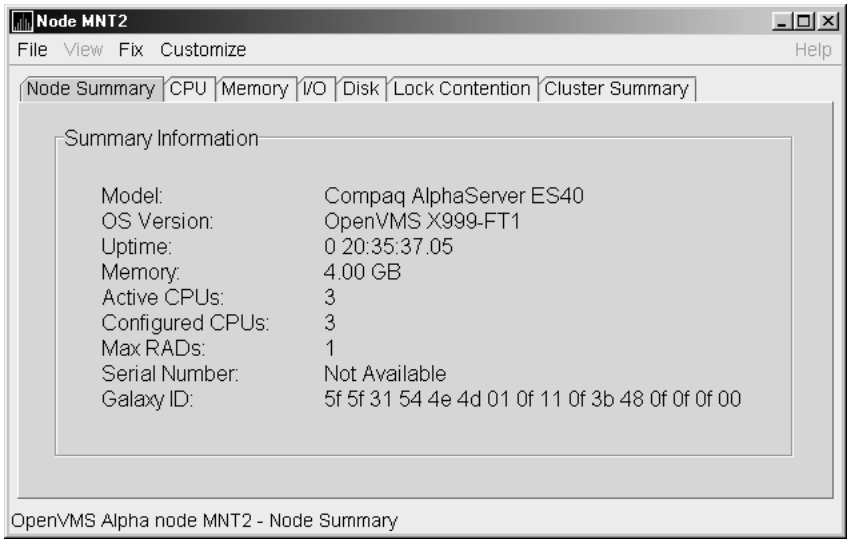
Figure 1–4 Data Collection Customization Page



- **Foreground** data collection

  Foreground data collection occurs automatically when you open any data page for a specific node. To open a node data page, double-click a node name in the Node pane of the Application window (Figure 1–1). The Node Summary page is the first page displayed (by default); Figure 1–5 is an example. At the top of the page are tabs that you can select to display other data pages for that node.

Figure 1–5 Sample Node Summary Page



Foreground data collection for all data types begins automatically when any node data page is displayed. Data collection ends when all node data pages have been closed.

Chapter 3 contains instructions for selecting nodes and displaying node data.

1.3.1.2 Events and Data Collection

An **event** is a problem or potential problem associated with resource availability. Users can customize criteria for events. Events are associated with types of data collected. For example, collection of CPU data is associated with the PRCCUR, PRCMWT, and PRCPWT events. (Appendix B describes events, and Appendix C describes the events that each type of data can signal.)

When the GUI requests one type of data from the Data Collector (for example, CPU data for all the processes on the system), a snapshot is taken of that type of data. This snapshot is considered one **data collection**.

1.3.1.3 Data Collection Intervals

Data collection **intervals**, which are displayed on the Data Collection customization page (Figure 1–4), specify the frequency of data collection. Table 1–1 describes these intervals.

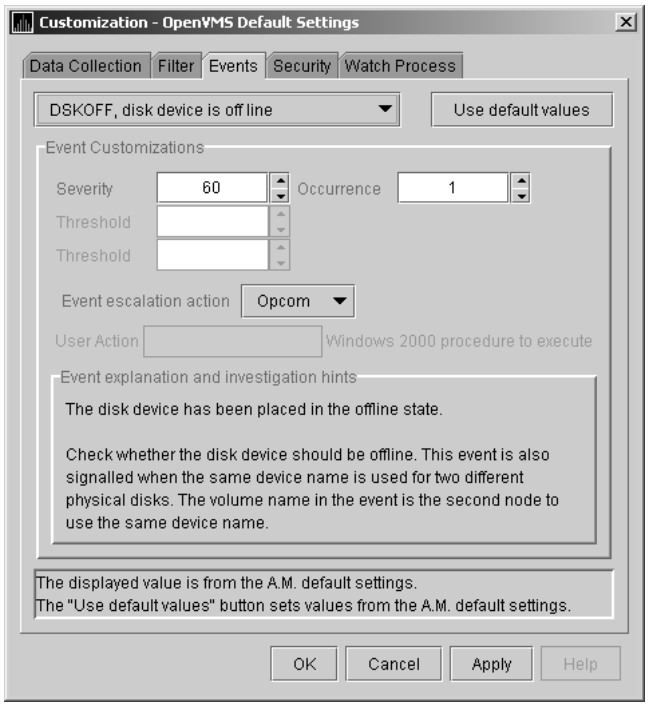
Table 1–1 Data Collection Intervals

Interval (in seconds)	Type of Data Collection	Description
NoEvent	Background	How often data is collected if no events have been posted for that type of data. The Availability Manager starts background data collection at the **NoEvent** interval (for example, every 75 seconds). If no events have been posted for that type of data, the Availability Manager starts a new collection cycle every 75 seconds.
Event	Background	How often data is collected if any events have been posted for that type of data. The Availability Manager continues background data collection at the **Event** interval until all events for that type of data have been removed from the Event pane. Data collection then resumes at the **NoEvent** interval.
Display	Foreground	How often data is collected when the page for a specific node is open. The Availability Manager starts foreground data collection at the **Display** interval and continues this rate of collection until the display is closed. Data collection then resumes as a background activity.

1.3.2 Posting Events

The Availability Manager evaluates each data collection for events. The Availability Manager posts events when data values in a data collection meet or exceed user-defined thresholds and occurrences. Values for thresholds and occurrences are displayed on Event Customization pages similar to the one shown in Figure 1–6. Thresholds and occurrences are described in the next section.

Figure 1–6 Sample Event Customization Page



1.3.2.1 Thresholds and Occurrences

Thresholds and occurrences are criteria that the Availability Manager uses for posting events.

A **threshold** is a value against which data in a data collection is compared. An **occurrence** is a value that represents the number of consecutive data collections that meet or exceed the threshold.

Both thresholds and occurrences are customizable values that you can adjust according to the needs of your system. For details about how to change the values for thresholds and occurrences, see Chapter 7.

Relationship between Thresholds and Occurrences

For a particular event, when the data collected meets or exceeds the threshold, the data collection enters a threshold-exceeded state. When the number of consecutive data collections to enter this state meets or exceeds the value in the Occurrence box (see Figure 1–6), the Availability Manager displays (posts) the event in the Event pane.

A closer look at Figure 1–6 shows the relationship between thresholds and occurrences. For the `DSKRWT, high disk device RWAIT count` event, a threshold of 1 `Rwait` process has been set. A value of 2 in the Occurrence box indicates that the number of `Rwait` errors during 2 consecutive data collections must meet or exceed the threshold of 1 for the `DSKRWT, high disk device RWAIT count` event to be posted.

1.4 How Does the Availability Manager Maintain Security?

The Availability Manager uses passwords to maintain security. These passwords have somewhat different appearances on Windows Data Analyzer nodes and on OpenVMS Data Analyzer and Data Collector nodes. On Windows Data Analyzer nodes, passwords are up to 8 characters long. On OpenVMS Data Analyzer and Data Collector nodes, passwords are part of a three-part security code called a **security triplet**.

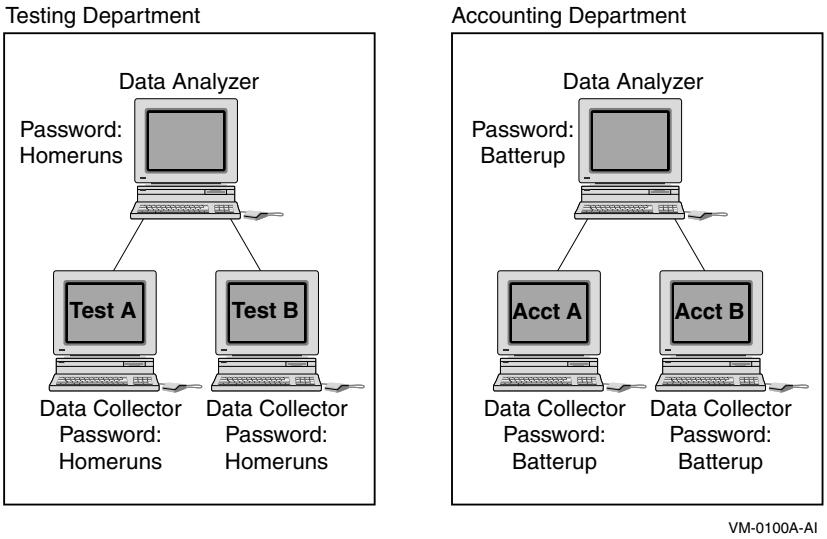
The following sections explain these security methods further.

1.4.1 Data Analyzer Password Security

For monitoring to take place, the password on a Data Analyzer node must match the password section of the security triplet on each OpenVMS Data Collector node. (A Windows Data Analyzer checks only the password part of each OpenVMS Data Collector security triplet. OpenVMS Data Collectors impose other security measures, which are explained in Section 1.4.2.)

Figure 1–7 illustrates how you can use passwords to limit access to node information. The Testing Department's Data Analyzer, whose password is HOMERUNS, can access only OpenVMS Data Collector nodes with the HOMERUNS password as part of their security triplets. The same is true of the Accounting Department Data Analyzer, whose password is BATTERUP; it can access only OpenVMS Data Collector nodes with the BATTERUP password as part of their security triplets.

Figure 1–7 Availability Manager Password Matching



The Availability Manager sets a default password when you install the Data Analyzer. To change that password, you must use a customization option that is explained in Chapter 7.

1.4.2 OpenVMS Data Collector Security Features

OpenVMS Data Collector nodes have the following security features:

- **Private LAN transport**

  The Availability Manager protocol is based on the 802.3 Extended Packet Format (also known as SNAP). The IEEE Availability Manager protocol values are as follows:

  ```
  Protocol ID:        08-00-2B-80-48
  Multicast Address:  09-00-2B-02-01-09
  ```

  If you filter protocols for bridges or routers in your network, you need to add these values to your network protocols.

- **Availability Manager data-transfer security**

  Each OpenVMS node running as a Data Collector has a file containing a list of security triplets. For Data Analyzer and Data Collector nodes to exchange data, the passwords on the nodes must match.

  In addition, note the following:

  – Data Collector nodes that have read access allow Windows Data Analyzer nodes to view system data.

  – Data Collector nodes that have write access also allow a matching Windows Data Analyzer node to perform fixes or modifications to the running system.

  Chapter 7 explains security triplets and how to edit them.

- **OpenVMS file protection and process privileges**

  When the Availability Manager is installed, it creates a directory (SYS$COMMON:[AMDS$AM]) and sets directory and file protections on it so that only the SYSTEM account can read the files in that directory. For additional security on these system-level directories and files, you can create access control lists (ACLs) to restrict and set alarms on write access to the security files.

  For more information about creating ACLs, see the *HP OpenVMS Guide to System Security*.

2
Getting Started

Notes

Before you start this chapter, be sure to read the explanation of data collection, events, thresholds, and occurrences in Chapter 1.

When this manual does not use the terms Windows 2000 or Windows XP, the term "Windows" refers to both Windows 2000 and XP, but *not* to any other Windows product.

This chapter provides the following information:

- How to start the Availability Manager Data Collector
- How to start the Availability Manager Data Analyzer
- How to use the main Application window
- How to display basic node data
- How to get help when you need it
- How to print an Availability Manager page

For information about installing the hp Availability Manager on OpenVMS or Windows systems, see the appropriate installation instructions. You can access these instructions from the Availability Manager web pages at the following URL:

`http://h71000.www7.hp.com/openvms/products/availman/`

The installation instructions for OpenVMS systems also include an explanation of how to install and use both DECamds and the Availability Manager on the same system.

2.1 Starting the Data Collector

Beginning with OpenVMS Version 7.2, the files needed to run the Data Collector on OpenVMS nodes are shipped with the OpenVMS operating system. However, if you want the latest Data Collector software, you need to install it from the Availability Manager Version 2.2 kit. Once the Data Collector is running on a node, you can monitor that node using DECamds or the Availability Manager.

To use the Data Collector on a particular node, do either of the following:

- Run the following command procedure:

```
$ @SYS$STARTUP:AMDS$STARTUP START
```

- Add the following command to the SYSTARTUP_VMS.COM command file in the SYS$MANAGER directory:

```
@SYS$STARTUP:AMDS$STARTUP START
```

2.2 Starting the Data Analyzer

This section describes what you need to do after the Availability Manager Data Analyzer is installed. Starting the Data Analyzer is somewhat different on OpenVMS and on Windows systems. However, on both systems, starting the Data Analyzer automatically starts the Java graphical user interface (GUI) that allows you to view information that is collected from the Data Collector nodes.

The following sections contain the sequence of steps required to start the Data Analyzer on an OpenVMS node and a Windows node.

2.2.1 How to Start the Data Analyzer on an OpenVMS Alpha Node

Make sure the Data Analyzer has been installed on the OpenVMS Alpha node from which you want to monitor other nodes. (Installation instructions are at the web site referred to at the beginning of this chapter.)

To start the Data Analyzer, enter the following command:

```
$ avail/avail
```

The Availability Manager then displays the main Application window, which is shown in Figure 1–1.

See the Installation Instructions for qualifiers you can use with the AVAIL/AVAIL command.

2.2.2 How to Start the Data Analyzer on a Windows Node

Make sure the Data Analyzer has been installed on the Windows node from which you want to monitor other nodes. (Installation instructions are at the web site referred to at the beginning of this chapter.)

Starting the Data Analyzer

To start the Data Analyzer, follow these steps:

1. Choose the following options beginning with the Windows Start menu:

   Start —> Programs

2. Choose **Availability Manager**.
3. Choose **Data Analyzer Startup**.

The Availability Manager then displays the main Application window, which is shown in Figure 2–1.

2.3 Using the Application Window

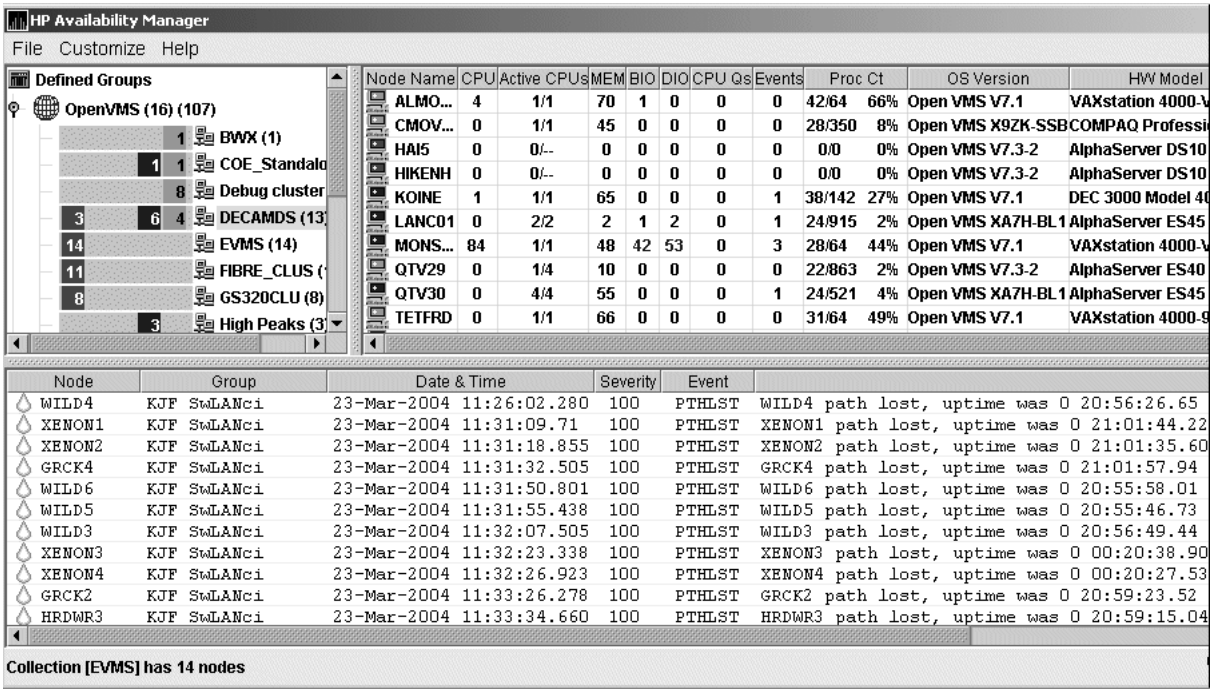
Once it starts, the Availability Manager watches for notifications from nodes running the Data Collector. After receiving notification from the Data Collector, the Availability Manager attempts to connect to a node. This is called the **attempting collection** phase.

If the node passes the security check while the Availability Manager is attempting the connection, the connection succeeds, and data collection starts. This is called the **data collection** phase. If the node fails the security check, it is in the **connection failed** phase.

While collecting data, if a node goes down, or a network connection fails between the graphical user interface and the node, that node is placed in the **path lost** phase.

The Availability Manager notifies you of these phases and other states in the Application window, which is shown in Figure 2–1.

Figure 2–1 Application Window



The Application window is divided into three segments, or **panes**:

- **Group pane**

  The Group pane is at the top left of the window. In this pane, you select the group of nodes that you want to monitor. The first number in parentheses after "OpenVMS" is the number of groups that are listed. The second number is the total number of nodes in the listed groups.

  The number in parentheses after each group name is the total number of nodes in the group. Preceding the name of each group, you might see as many as five color-coded columns of numbers.

  From left to right, the columns display the number of nodes in the group that are in the states described in Table 2–1.

Table 2–1 Node Information Displayed in Group Pane

Column Number	Color	Description
1	Brown	Number of nodes for which attempts to configure the node have failed—for example, because the node is in a connection failed phase.
2	Yellow	Number of nodes that are in the attempting collection phase.

(continued on next page)

Table 2–1 (Cont.) Node Information Displayed in Group Pane

Column Number	Color	Description
3	Black	Number of nodes that are in a path lost phase.
4	Red	Number of nodes that are in the data collection phase but that have exceeded a threshold, causing an event to be posted. Note that if an event causes the output of any message besides an informational one, a node would be displayed in red.
5	Green	Number of nodes that are in the data collection phase.

- **Node pane**

  The Node pane occupies most of the top right of the window. In this pane, the Availability Manager displays a list of the nodes in the group you select in the Group pane, along with summary data for each node. In Figure 2–1, the Debug cluster group has been selected. Chapter 3 contains more information about using the Node pane.

  Figure 2–1 shows the node information that is displayed when you select a group of OpenVMS nodes. Somewhat different information is displayed for a group of Windows nodes. For more information about this, see Chapter 3.

  When you hold the cursor over a node in the Node pane, the Availability Manager displays a tool tip in one of several colors. Each color has a specific meaning attached to it regarding the health of the node. The colors and their meanings are in Table 2–2.

Table 2–2 Colors of Tooltips in the Node Pane

Color	Meaning
Brown	Indicates why the configuration of the node failed.
Yellow	Shows number of RM Driver broadcasts (“Hello”) and the number of attempts to configure the node (“Configuration packets sent”). Nodes that remain in this state more than a few seconds indicate network connectivity problems with the Data Analyzer.
Black	Show one of the following: If the node was successfully configured and then lost, – When the connection to the node was lost (“Path lost at *time*”). – When that node was booted (“Boot time: *time*”). – What the uptime of the node was (“Uptime: *time*”). If the node was never configured, – When the connection to the node was lost (“Path lost at *time*”). – The reason the node was not configured.
Red	Events signalled for the node.
Green	Node uptime.

- **Event pane**

  The Event pane occupies the entire bottom of the window. In this pane, the Availability Manager displays events that occur on all the nodes being monitored on your system. (Events signal potential problems that might require further investigation.)

An event must reach a certain level of severity to be displayed. You can customize the severity levels at which events are displayed (see Chapter 7). For more information about displaying events, see Chapter 5.

You can change the size of the panes as well as the width of specific fields in the Application window and also the borders between the fields by clicking on a border and dragging it. Scroll bars indicate whether you are displaying all or part of a screen. For example, clicking a right arrow on a scroll bar allows you to view the rightmost portion of a screen.

2.3.1 Other Window Components

In addition to panes, the Application window also includes the following components (see Figure 2–1):

Title bar

The title bar runs across the top of the window and contains the product name.

Menu bar

The menu bar, immediately below the title bar, contains the following menu options:

- **File**

  The File menu contains the Exit option, which allows you to stop the Data Analyzer and close the window.

- **Customize**

  The Customize menu contains options that allow you to customize various aspects of the Availability Manager. These options are explained in Chapter 7.

- **Help**

  The Help menu offers different types of online help for the Availability Manager. These options are explained in Section 2.5.

Status bar

The status bar runs across the bottom of the window. It displays the name of the selected group and the number of nodes in that group.

2.3.2 Displaying More Information

In the initial Application window (Figure 2–1), which is displayed by default, you can do the following at any time:

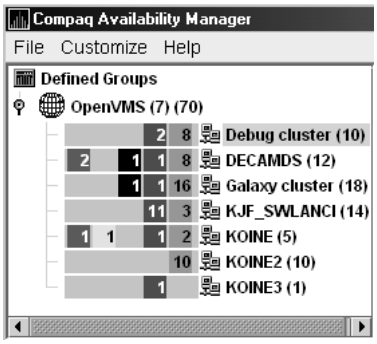
- Click a field to select it.
- Double-click most fields to display a page containing information specific to that field.
- Right-click a field to display a popup menu.

2.3.3 Understanding Groups of Nodes

When you start the Availability Manager, the Group pane lists groups of nodes that the Data Analyzer has found. If the Data Analyzer finds Windows nodes, those are also displayed.

To monitor specific nodes, you must select the group in the Group pane that contains those nodes (see Figure 2–2).

Figure 2–2 Group Pane



Groups are set up during installation on Data Collector nodes and are user definable. You might define groups by function, type of hardware, or geographical location.

For example, if you were to set up groups of nodes by geographical location, you might assign nodes A and B to a group called Dallas and nodes C, D, and E to a group called Denver. When you select a group, the Availability Manager displays only the nodes in that group, as shown in the following table:

Group Selected	Nodes Displayed
Dallas	Node A Node B
Denver	Node C Node D Node E

By default, all nodes are members of one group, DECAMDS, when your system is set up. If you want to change the groups being monitored, you need to to use a customization option to make changes. See Section 7.2 for instructions.

HP recommends that you define a cluster as its own group.

2.4 Displaying More Information about Nodes

The Node pane of the Application window allows you to focus on resource usage activity at a high level and to display more specific data whenever you want. This section explains the basic use of the Node pane. For more detailed information, see Chapter 3.

Within the group of nodes you select, the Availability Manager displays all the nodes with which that group can communicate. Figure 2–3 shows a list of OpenVMS nodes.

Figure 2–3 OpenVMS Node Pane

Node Name	CPU	Active CPUs	MEM	BIO	DIO	CPU Qs	Events	Proc Ct	OS Version	HW Model	HW Arch
AFFC5	0	2/4	44	0	0	0	1	36/2500 1%	Open VMS V7.3-2	AlphaServer ES40	Alpha
AFFC6	0	2/4	54	2	2	0	1	51/792 6%	Open VMS V7.3-2	AlphaServer ES40	Alpha
AFFS10	1	2/2	54	13	4	2	1	73/514 14%	Open VMS V7.3-1	AlphaServer 2100A 5/300	Alpha
AFFS11	0	2/2	45	1	0	0	1	22/153 14%	Open VMS V6.2-1H3	AlphaServer 2000 4/200	Alpha
AFFS12	0	2/2	51	0	0	0	0	26/136 19%	Open VMS V7.2-1	AlphaServer 2000 4/200	Alpha
AFFS21	0	1/1	6	0	0	0	0	22/1500 1%	Open VMS V7.3-2	AlphaServer DS15	Alpha
AFFS22	0	1/1	65	0	0	0	0	15/480 3%	Open VMS V7.1	VAX 4000-600	VAX
AFFS23	0	1/1	21	0	0	0	0	22/150 15%	Open VMS V7.1-1H1	DEC 3000 - M800	Alpha
AFFS5	0	1/1	64	0	0	0	0	24/240 10%	Open VMS V7.1	VAX 4000-300	VAX
AFFS51	67	2/2	65	121	111	0	5	82/1113 7%	Open VMS V7.3-2	AlphaServer 2100 4/275	Alpha
AFFS52	1	2/2	15	3	1	0	1	52/126 41%	Open VMS V7.2-2	AlphaServer 2100 4/275	Alpha
AFFS55	0	1/1	24	0	0	0	0	15/360 4%	Open VMS V6.2	VAX 4000-300	VAX
AFFS6	0	2/2	42	0	0	0	0	20/117 17%	Open VMS V7.1-2	AlphaServer 2000 4/200	Alpha
AFFS7	0	1/1	51	0	0	0	0	33/173 19%	Open VMS V7.2-2	AlphaServer 2000 4/233	Alpha
AFFS8	0	1/1	62	0	0	0	0	42/483 8%	Open VMS V7.3	AlphaStation 600A 5/500	Alpha
AFFS9	1	1/1	64	0	0	0	1	18/90 20%	Open VMS V7.3	VAXstation 4000-60	VAX

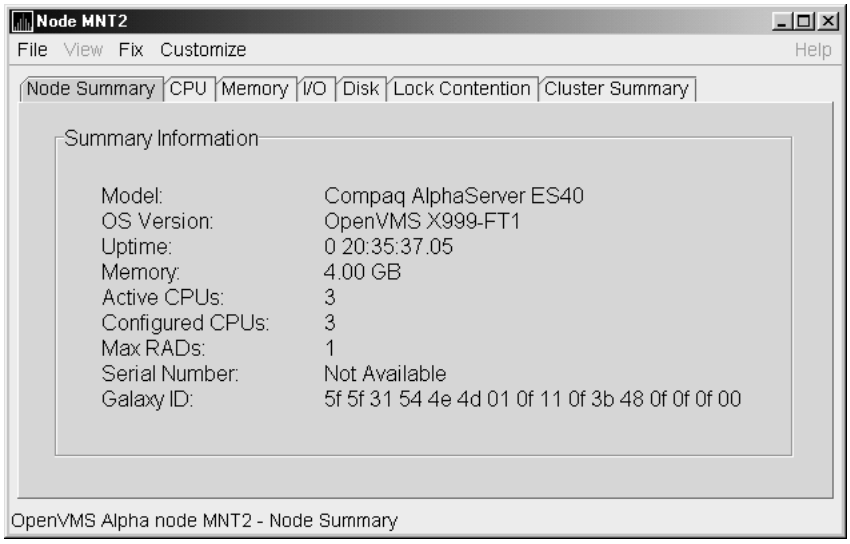
Each node name has an icon next to it. The color of the icon represents a state similar to those described in Table 2–1:

Color	Description
Brown	Attempts to configure the node have failed—for example, because it failed the security check.
Yellow	Node security check is in progress or has failed.
Black	Path to node has been lost.
Red	Security check was successful. However, a threshold has been exceeded, and an event has been posted. Note that if an event causes the output of any message besides an informational one, the node is displayed in red.
Green	Security check was successful; data is being collected.

2.4.1 Choosing a Node

To choose a node on a Windows or an OpenVMS system, double-click a node name in the Node pane to highlight the name of the node and display the Node Summary page (Figure 2–4). Alternatively, you can right-click a node name to display a popup menu. To display the Node Summary page, select the **Display...** option.

Figure 2–4 OpenVMS Node Summary Page



The data displayed on this page is explained in Chapter 3.

At the top of the Node Summary page are tabs that correspond to most of the types of node data displayed in the Node pane. When you click a tab on the Node Summary page, the Availability Manager displays most of the same pages that are displayed when you double-click a data item in the Node pane (see Figure 2–3).

2.4.2 Specifying Data to Collect on OpenVMS Nodes

For OpenVMS nodes, if you want background data collection (and the associated event detection), you must **turn on** data collection for each type of data you want to collect. On Windows nodes, background data collection is always enabled and cannot be turned off.

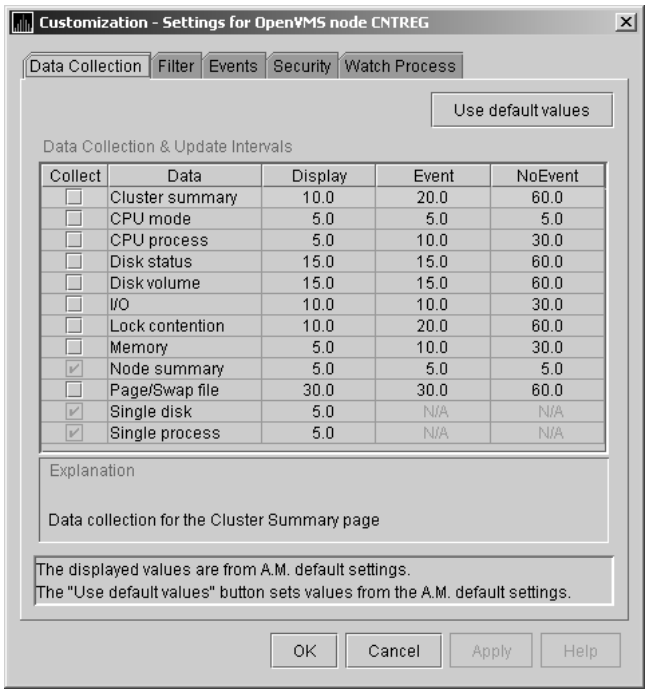
To turn on various types of data to be collected, follow these steps:

1. In the Application window, click the **Customize** menu.
2. Click **Customize OpenVMS...**.
3. Click the **Data Collection** tab.

The Availability Manager displays the Data Collection Customization page (Figure 2–5).

Background and foreground collections are explained in Chapter 1.

Figure 2–5 Data Collection Customization Page



The following types of data are collected by default:

- Node summary
- Single disk
- Single process

To stop collecting Node Summary data, for example, clear the check box for “Node summary” in the “Collect” column. You cannot, however, turn off the collection of single disk and single process data. These types of data are collected by default when you open a Single Disk Summary page or a Process Information page, respectively.

To turn on a type of data to be collected, select the check box for that type in the “Collect” column. Table 7–2 identifies the page where each type of data that is collected appears.

On the Data Collection Customization page, you can also change the intervals at which data is collected. Collection intervals are explained in Chapter 7.

2.4.3 Sorting Data

You can sort data in many OpenVMS displays, for example:

- Event pane of the Application window (Figure 2–1)
- CPU Process Summary pane (Figure 3–8)
- Memory page (Figure 3–10)
- Bottom pane of I/O Summary page (Figure 3–12)
- Disk Status Summary page (Figure 3–14)
- Disk Volume Summary page (Figure 3–16)

Depending on the field, you can sort data alphabetically or numerically. An alphabetical sort is performed using ASCII character values; for example, dollar signs ($) precede letters in the sort order.

To sort the values in a field, double-click the corresponding column heading. To reverse the sort order, double-click the column heading again.

2.5 Getting Help

To obtain online help, click the **Help** menu on the Application window menu bar. Then choose one of the following options:

Menu Option	Description
Availability Manager Help	Information about using the Availability Manager.
Getting Started	A special online version of help for getting started using this tool.
Availability Manager Release Notes	Last-minute information about the software and how it works.
About Availability Manager...	Information about this Availability Manager release (such as the version number).

2.6 Printing an Availability Manager Page

The Availability Manager does not provide a printscreen capability. However, you can capture Availability Manager pages and print them by following these steps:

1. Display the Availability Manager page in your active window.
2. Press the key combination `Alt + PrintScreen`.

   This action copies the image of the page displayed into your copy buffer. (To capture the entire screen, press `Ctrl + PrintScreen`.)
3. Run the Windows Paint program:

   ```
   Start --> Programs --> Accessories --> Paint
   ```
4. Do one of the following:
   - Press the key combination `Ctrl + V`.
   - From Paint's Edit menu, select `Paste`.
5. Then do one of the following:
   - Select an option from Paint's File menu. For example:
     - Save or Save As...: to name the file containing the image and place it in a directory that you specify.
     - Print: to print the image on a printer that you select.
   - Use one of Paint's editing options to edit the image before saving or printing it.

3
Getting Information About Nodes

Note

Before you start this chapter, be sure to read the explanation of data collection, events, thresholds, and occurrences in Chapter 1. HP also recommends completing the getting-started steps described in Chapter 2.

Node summary data is the only data that is collected by default. The Availability Manager looks for events only in data that is being collected.

You can collect additional data in either of the following ways:

- Opening any display page that contains node-specific data (for example, CPU, memory, I/O) automatically starts foreground data collection and event analysis except for Lock Contention and Cluster Summary information. (You must select these tabs individually to start foreground data collection.) Collection and evaluation continue as long as a page with node-specific data is displayed.
- Clicking a check mark on the Data Collection Customization page (which you can select on the Customize OpenVMS menu) enables background collection of that type of data. Data is collected and events are analyzed continuously until you remove the check mark.

See Chapter 1 and Chapter 7 for details.

This chapter describes the node data that the Availability Manager displays by default and more detailed data that you can choose to display. Differences are noted whenever information displayed for OpenVMS nodes differs from that displayed for Windows nodes.

Although Cluster Summary is one of the tabs displayed on the OpenVMS Node Summary page (see Figure 3–4), see Chapter 4 for a detailed discussion of OpenVMS Cluster data.

Note

On many node displays, you can hold the cursor over a data field or column header to display an explanation of that field or header in a little rectangle, called a **tooltip**. Figure 3–2 contains an example.

3.1 Node Panes

After you select a group of nodes in the Group pane, the Availability Manager automatically displays data for each node within that group in the Node pane of the Application window (Figure 3–1).

Figure 3–1 OpenVMS Node Pane

Node Name	CPU	Active CPUs	MEM	BIO	DIO	CPU Qs	Events	Proc Ct		OS Version	HW Model	HW Arch
AFFC5	0	2/4	44	0	0	0	1	36/2500	1%	Open VMS V7.3-2	AlphaServer ES40	Alpha
AFFC6	0	2/4	54	2	2	0	1	51/792	6%	Open VMS V7.3-2	AlphaServer ES40	Alpha
AFFS10	1	2/2	54	13	4	2	1	73/514	14%	Open VMS V7.3-1	AlphaServer 2100A 5/300	Alpha
AFFS11	0	2/2	45	1	0	0	1	22/153	14%	Open VMS V6.2-1H3	AlphaServer 2000 4/200	Alpha
AFFS12	0	2/2	51	0	0	0	0	26/136	19%	Open VMS V7.2-1	AlphaServer 2000 4/200	Alpha
AFFS21	0	1/1	6	0	0	0	0	22/1500	1%	Open VMS V7.3-2	AlphaServer DS15	Alpha
AFFS22	0	1/1	65	0	0	0	0	15/480	3%	Open VMS V7.1	VAX 4000-600	VAX
AFFS23	0	1/1	21	0	0	0	0	22/150	15%	Open VMS V7.1-1H1	DEC 3000 - M800	Alpha
AFFS5	0	1/1	64	0	0	0	0	24/240	10%	Open VMS V7.1	VAX 4000-300	VAX
AFFS51	67	2/2	65	121	111	0	5	82/1113	7%	Open VMS V7.3-2	AlphaServer 2100 4/275	Alpha
AFFS52	1	2/2	15	3	1	0	1	52/126	41%	Open VMS V7.2-2	AlphaServer 2100 4/275	Alpha
AFFS55	0	1/1	24	0	0	0	0	15/360	4%	Open VMS V6.2	VAX 4000-300	VAX
AFFS6	0	2/2	42	0	0	0	0	20/117	17%	Open VMS V7.1-2	AlphaServer 2000 4/200	Alpha
AFFS7	0	1/1	51	0	0	0	0	33/173	19%	Open VMS V7.2-2	AlphaServer 2000 4/233	Alpha
AFFS8	0	1/1	62	0	0	0	0	42/483	8%	Open VMS V7.3	AlphaStation 600A 5/500	Alpha
AFFS9	1	1/1	64	0	0	0	1	18/90	20%	Open VMS V7.3	VAXstation 4000-60	VAX

Recall that the colors of the icons represent the following states:

Color	Description
Brown	Attempts to configure the node have failed—for example, because it failed the security check.
Yellow	Node security check is in progress or has failed.
Black	Path to node has been lost.
Red	Security check was successful. However, a threshold has been exceeded, and an event has been posted.
Green	Security check was successful; data is being collected.

The following sections describe the data displayed for OpenVMS and Windows Node panes.

3.1.1 OpenVMS Node Pane

Node pane data displayed in red on your screen indicates that the amount is above the threshold set for that field. For each OpenVMS node and group it recognizes, the Availability Manager displays the data described in Table 3–1. This table also lists the abbreviation of the event that is related to each type of data, where applicable. See Section 7.6 for information about setting event thresholds. Appendix B describes OpenVMS and Windows events.

Note that you can sort the order in which data is displayed in the Node Pane by clicking a column header. To reverse the sort order of a column of data, click the column header again.

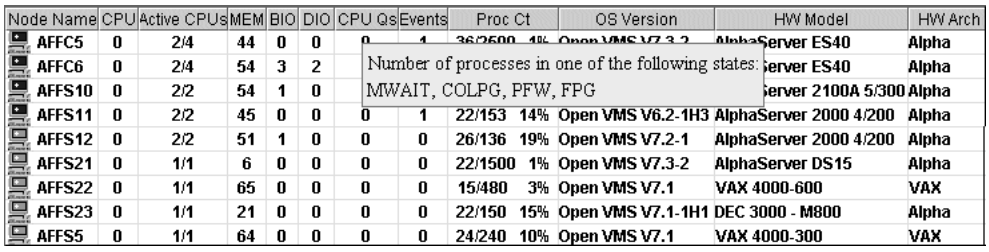
Table 3–1 OpenVMS Node Data

Data	Description of Data	Related Event
Node Name	Name of the node being monitored.	n/a
CPU[1]	Percentage of CPU usage of all processes on the node.	HICOMQ HIMTTO PRCCUR PRCPUL
Active CPUs	The number of active CPUs over the number of CPUs in the potential set of CPUs.	n/a
MEM	Percentage of space in memory that all processes on the node use.	LOMEMY
BIO	Buffered I/O rate of processes on the node.	HIBIOR
DIO	Direct I/O usage of processes on the node.	HIDIOR
CPU Qs	Number of processes in one of the following states: MWAIT, COLPG, PFW, FPG.	HIMWTQ PRCMWT HIPWTQ PRCPUT
Events	Number of triggered events that are associated with this node.	List of relevant events
Proc Ct	Actual count of processes over the maximum number of processes. Percentage of actual to maximum processes.	HIPRCT
OS Version	Version of the operating system on the node.	NOPLIB UNSUPP
HW Model	Hardware model of the node.	NOPLIB UNSUPP
HW Arch	Hardware architecture: Alpha or VAX	n/a

[1]By default, the CPU heading follows Node Name on a line of Node Pane data. You can use the cursor to move a column heading to another location on the line, if you like.

By holding the cursor over many column headers and some data items on Availability Manager screens, you can display a tooltip. Figure 3–2 is an example of a tooltip that explains the CPU Queues column header in the Node Pane.

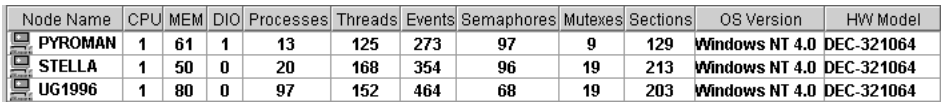
Figure 3–2 Sample Tooltip



3.1.2 Windows Node Pane

Figure 3–3 is an example of a Windows Node pane. From the group you select, the Availability Manager displays all the nodes with which it can communicate.

Figure 3–3 Windows Node Pane



Node Name	CPU	MEM	DIO	Processes	Threads	Events	Semaphores	Mutexes	Sections	OS Version	HW Model
PYROMAN	1	61	1	13	125	273	97	9	129	Windows NT 4.0	DEC-321064
STELLA	1	50	0	20	168	354	96	19	213	Windows NT 4.0	DEC-321064
UG1996	1	80	0	97	152	464	68	19	203	Windows NT 4.0	DEC-321064

For each Windows node in the group, the Availability Manager displays the data shown in Table 3–2.

Table 3–2 Windows Node Data

Data	Description
Node Name	Name of the node being monitored.
CPU	Percentage of CPU usage of all the processes on the node.
MEM	Percentage of memory that is in use.
DIO	Direct I/O usage of processes on the node.
Processes	Number of processes on the node.
Threads	Number of threads on the node. A thread is a basic executable entity that can execute instructions in a processor.
Events	The number of events on the node. An event is used when two or more threads want to synchronize execution.
Semaphores	The number of semaphores on the node. Threads use semaphores to control access to data structures that they share with other threads.
Mutexes	The number of mutexes on the node. Threads use mutexes to ensure that only one thread executes a section of code at a time.
Sections	The number of sections on the node. A section is a portion of virtual memory created by a process for storing data. A process can share sections with other processes.
OS Version	Version of the operating system on the node.
HW Model	Hardware model of the node.

3.2 Node Data Pages

The following sections describe node data pages, which you can display in any of the following ways:

- Double-click a data item in the Node pane to display an associated page.
- Double-click a node name on the Node pane to display the Node Summary page (Figure 3–4). You can then click other tabs on the Node Summary page to display the same detailed data that you display by double-clicking a data item in the Node pane.
- Double-click an event in the Event pane.

The menu bar on each node data page contains the options described in Table 3–3.

Table 3–3 Node Data Page Menu Bar

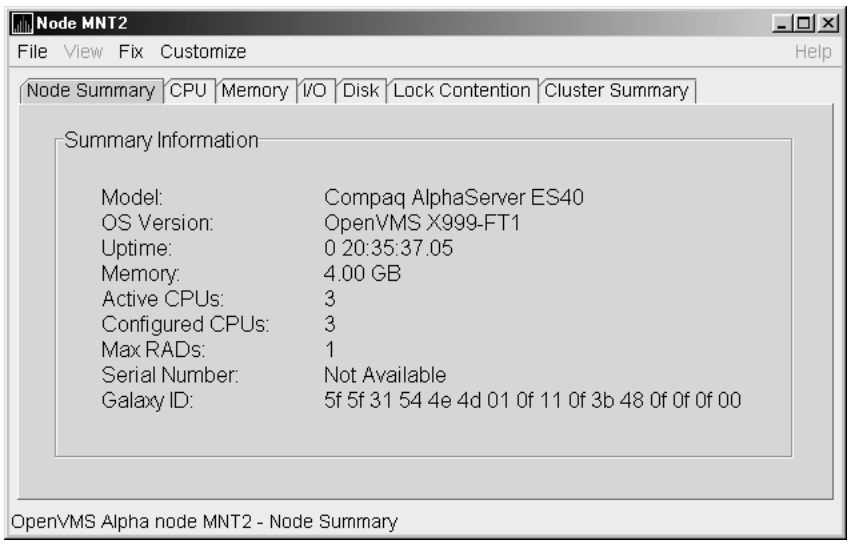
Menu Option	Description	For More Information
File	Contains the Close option, which you can choose to exit from the pages.	n/a
View	Contains options that allow you to view data from another perspective.	See specific pages.
Fix	Contains options that allow you to resolve various resource availability problems and improve system performance.	Chapter 6
Customize	Contains options that allow you to organize data collection and analysis and to display data by filtering and customizing Availability Manager data.	Chapter 7

The following sections describe individual node data pages.

3.2.1 Node Summary

When you double-click a node name, operating system (OS) version, or hardware model in an OpenVMS or Windows Node pane, the Availability Manager displays the Node Summary page (Figure 3–4).

Figure 3–4 Node Summary Page



On this page, the following information is displayed for the node selected:

Data	Description
Model	System hardware model name.
OS Version	Name and version of the operating system.
Uptime	Time (in days, hours, minutes, and seconds) since the last reboot.
Memory	Total amount of physical memory (in megabytes) found on the system.
Active CPUs	Number of CPUs running on the node.

Data	Description
Configured CPUs	Number of CPUs that are configured to run on the node.
Max RADs	Maximum number of resource affinity domains (RADs) for this node.
Serial Number	The system's hardware serial number retrieved from the Hardware Restart Parameter Block (HWRPB).
Galaxy ID	The Galaxy ID uniquely identifies a Galaxy. Instances in the same Galaxy have the same Galaxy ID.

3.2.2 CPU Modes and Process Summaries

By clicking the CPU tab, you can display CPU panes that contain more detailed statistics about CPU mode usage and process summaries than the Node Summary does. You can use the CPU panes to diagnose issues that CPU-intensive users or CPU bottlenecks might cause. For OpenVMS nodes, you can also display information about specific CPU processes.

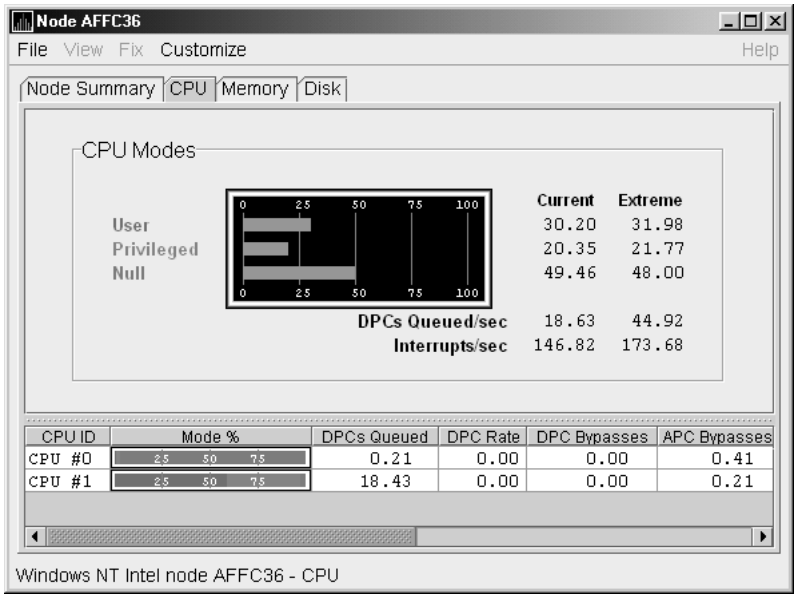
When you double-click a value under the CPU or CPU Qs heading on either an OpenVMS or a Windows Node pane, or when you click the CPU tab, the Availability Manager displays the CPU Modes Summary in the top pane and, by default in the bottom pane, CPU Modes Detail. You can use the View menu to select the CPU Process Summary in the bottom pane (see Section 3.2.2.4).

CPU modes summaries and process summary panes are described in the following sections. Note that there are differences between the pages displayed for OpenVMS and Windows nodes.

3.2.2.1 Windows CPU Modes

Figure 3–5 contains a sample Windows CPU Modes page.

Figure 3–5 Windows CPU Modes Page



The top pane of the Windows CPU Modes page is a summary of Windows CPU usage, listed by type of mode.

On the left, the following CPU modes are listed:

- User
- Privileged
- Null

On the graph, values that exceed thresholds are displayed in red. To the right of the graph are current and extreme amounts for each mode.

Current and extreme amounts are also displayed for the following values:

- Deferred procedure calls (DPCs) queued per second
- Interrupts that occurred per second

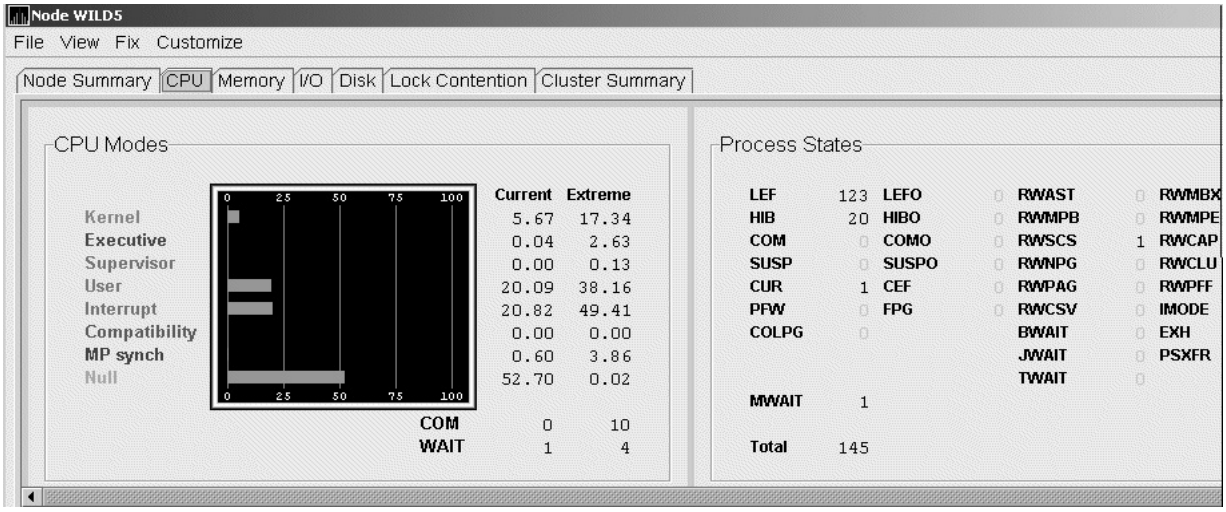
The bottom pane of the Windows CPU Modes contains modes details. The following data is displayed:

Data	Description
CPU ID	Decimal value representing the identity of a processor in a multiprocessing system. On a uniprocessor, this value is always CPU #00.
Mode %	Graphical representation of the percentage of active modes on that CPU. The color displayed matches the mode color on the graph on the top pane.
DPCs Queued	Rate that deferred procedure call (DPC) objects are queued to this processor's DPC queue.
DPC Rate	Average rate that DPC objects are queued to this processor's DPC queue per clock tick.
DPC Bypasses	Rate that dispatch interrupts were short-circuited.
APC Bypasses	Rate that kernel asynchronous procedure call (APC) interrupts were short-circuited.

3.2.2.2 OpenVMS CPU Modes Summary and Process States

Figure 3–6 shows sample OpenVMS CPU Modes summary and CPU Process States, which are the left and right top panes of the CPU Modes page.

Figure 3–6 OpenVMS CPU Modes Summary and Process States Pane



CPU Modes Summary

In the CPU modes section of the pane, percentages are averaged across all the CPUs and are displayed as a single value on symmetric multiprocessing (SMP) nodes.

To the left of the graph is a list of CPU modes. The bars in the graph represent the percentage of CPU cycles used for each mode. Values that are lower than the thresholds are displayed in green; values that exceed thresholds are displayed in red. To the right of the graph are current and extreme percentages of time spent in each mode.

Below the graph, the Availability Manager displays the COM and WAIT process queues:

- COM: The value displayed is the number of processes in the COM and COMO states.
- WAIT: The value displayed is the number of processes in the miscellaneous WAIT, COLPG, CEF, PFW, and FPG states.

CPU Process States

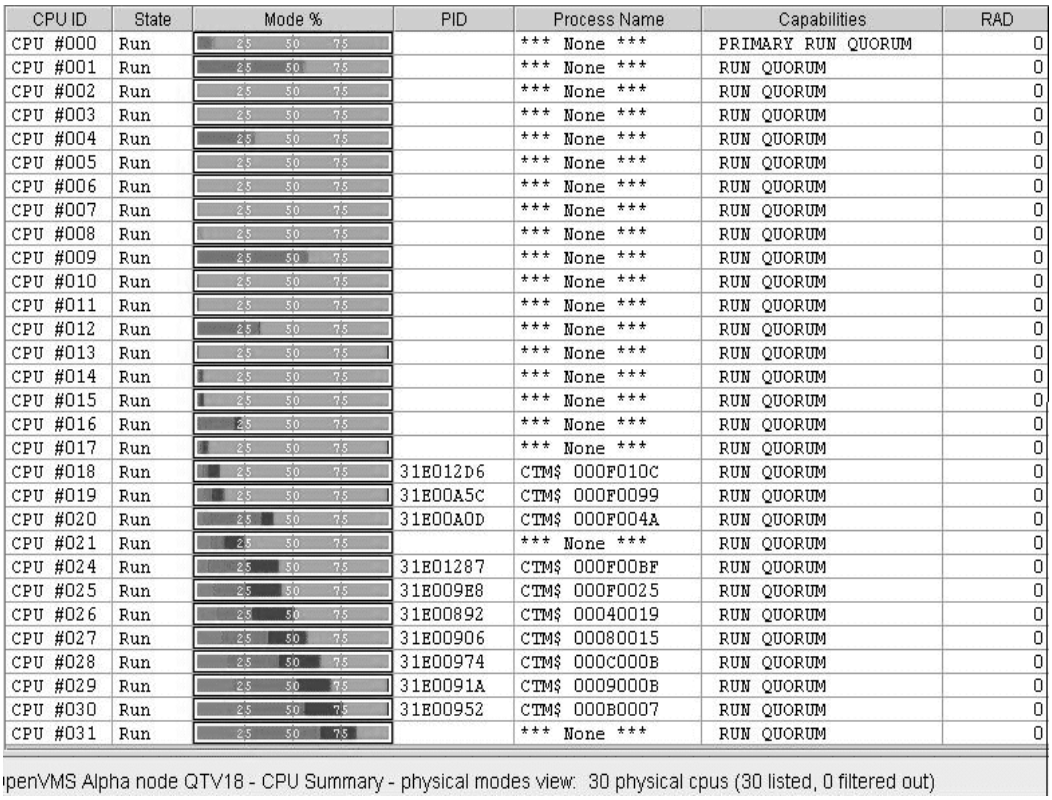
The right side of Figure 3–6 shows a sample CPU Process States display.

Appendix A contains explanations of the CPU process states. Note that the value for MWAIT, in the left column, is the sum of all values for the states in the two right columns.

3.2.2.3 OpenVMS CPU Modes Detail

The bottom pane of the CPU Modes page contains CPU modes details, as shown in Figure 3–7.

Figure 3–7 OpenVMS CPU Modes Detail Pane



CPU ID	State	Mode %	PID	Process Name	Capabilities	RAD
CPU #000	Run			*** None ***	PRIMARY RUN QUORUM	0
CPU #001	Run			*** None ***	RUN QUORUM	0
CPU #002	Run			*** None ***	RUN QUORUM	0
CPU #003	Run			*** None ***	RUN QUORUM	0
CPU #004	Run			*** None ***	RUN QUORUM	0
CPU #005	Run			*** None ***	RUN QUORUM	0
CPU #006	Run			*** None ***	RUN QUORUM	0
CPU #007	Run			*** None ***	RUN QUORUM	0
CPU #008	Run			*** None ***	RUN QUORUM	0
CPU #009	Run			*** None ***	RUN QUORUM	0
CPU #010	Run			*** None ***	RUN QUORUM	0
CPU #011	Run			*** None ***	RUN QUORUM	0
CPU #012	Run			*** None ***	RUN QUORUM	0
CPU #013	Run			*** None ***	RUN QUORUM	0
CPU #014	Run			*** None ***	RUN QUORUM	0
CPU #015	Run			*** None ***	RUN QUORUM	0
CPU #016	Run			*** None ***	RUN QUORUM	0
CPU #017	Run			*** None ***	RUN QUORUM	0
CPU #018	Run		31E012D6	CTM$ 000F010C	RUN QUORUM	0
CPU #019	Run		31E00A5C	CTM$ 000F0099	RUN QUORUM	0
CPU #020	Run		31E00A0D	CTM$ 000F004A	RUN QUORUM	0
CPU #021	Run			*** None ***	RUN QUORUM	0
CPU #024	Run		31E01287	CTM$ 000F00BF	RUN QUORUM	0
CPU #025	Run		31E009E8	CTM$ 000F0025	RUN QUORUM	0
CPU #026	Run		31E00892	CTM$ 00040019	RUN QUORUM	0
CPU #027	Run		31E00906	CTM$ 00080015	RUN QUORUM	0
CPU #028	Run		31E00974	CTM$ 000C000B	RUN QUORUM	0
CPU #029	Run		31E0091A	CTM$ 0009000B	RUN QUORUM	0
CPU #030	Run		31E00952	CTM$ 000B0007	RUN QUORUM	0
CPU #031	Run			*** None ***	RUN QUORUM	0

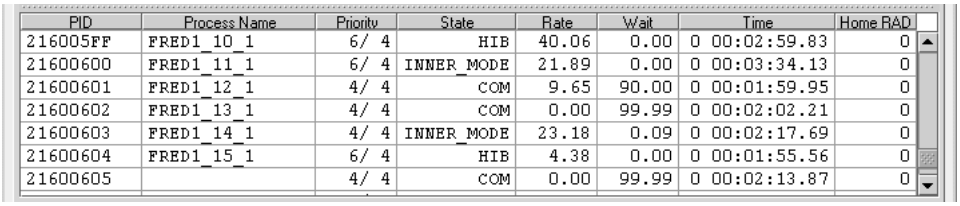
In the OpenVMS CPU Modes Detail pane, the following data is displayed:

Data	Description
CPU ID	Decimal value representing the identity of a processor in a multiprocessing system. On a uniprocessor, this value is always CPU #00.
State	One of the following CPU states: Boot, Booted, Init, Rejected, Reserved, Run, Stopped, Stopping, or Timeout.
Mode %	Graphical representation of the percentage of active modes on that CPU. The color displayed coincides with the mode color in the graph in the top pane.
PID	Process identifier (PID) value of the process that is using the CPU. If the PID is unknown to the console application, the internal PID (IPID) is listed.
Process Name	Name of the process active on the CPU. If no active process is found on the CPU, the name is listed as *** None ***.
Capabilities	One or more of the following CPU capabilities: Primary, Quorum, Run, or Vector.
RAD	Number of the RAD where the CPU exists.

3.2.2.4 OpenVMS CPU Process Summary

To display the OpenVMS CPU Process Summary pane at the bottom of the CPU page, select CPU Process Summary from the View menu. Figure 3–8 shows a sample OpenVMS CPU Process Summary pane.

Figure 3–8 OpenVMS CPU Process Summary Pane



PID	Process Name	Priority	State	Rate	Wait	Time	Home RAD
216005FF	FRED1_10_1	6/ 4	HIB	40.06	0.00	0 00:02:59.83	0
21600600	FRED1_11_1	6/ 4	INNER_MODE	21.89	0.00	0 00:03:34.13	0
21600601	FRED1_12_1	4/ 4	COM	9.65	90.00	0 00:01:59.95	0
21600602	FRED1_13_1	4/ 4	COM	0.00	99.99	0 00:02:02.21	0
21600603	FRED1_14_1	4/ 4	INNER_MODE	23.18	0.09	0 00:02:17.69	0
21600604	FRED1_15_1	6/ 4	HIB	4.38	0.00	0 00:01:55.56	0
21600605		4/ 4	COM	0.00	99.99	0 00:02:13.87	0

The OpenVMS CPU Process Summary pane displays the following data:

Data	Description
PID	Process identifier, a 32-bit value that uniquely identifies a process.
Process Name	Name of the process active on the CPU.
Priority	Computable *(xx)* and base *(yy)* process priority in the format *xx*/*yy*.
State	One of the process states listed in Appendix A.
Rate	Percentage of CPU time used by this process. This is the ratio of CPU time to elapsed time. The CPU rate is also displayed in the bar graph.
Wait	Percentage of time the process is in the COM or COMO state.
Time	Amount of actual CPU time charged to the process.
Home RAD	Where most of the resources of the process reside.

Displaying Single Process Information

When you double-click a PID on the lower part of an OpenVMS CPU Process Summary (Figure 3–8), Memory Summary (Figure 3–10), or I/O Summary (Figure 3–12) page, the Availability Manager displays the first of several OpenVMS Single Process pages. On these pages, you can click tabs to display specific data about one process.

This data includes a combination of data elements from the CPU Process, Memory, and I/O pages, as well as data for specific quota utilization, current image, and queue wait time. These pages are described in more detail in Section 3.3.

3.2.3 Memory Summaries and Details

The Memory Summary and Memory Details pages contain statistics about memory usage on the node you select. The Memory Summary pages displayed for OpenVMS and Windows nodes are somewhat different, as described in the following sections. The Memory Details page exists only for OpenVMS systems.

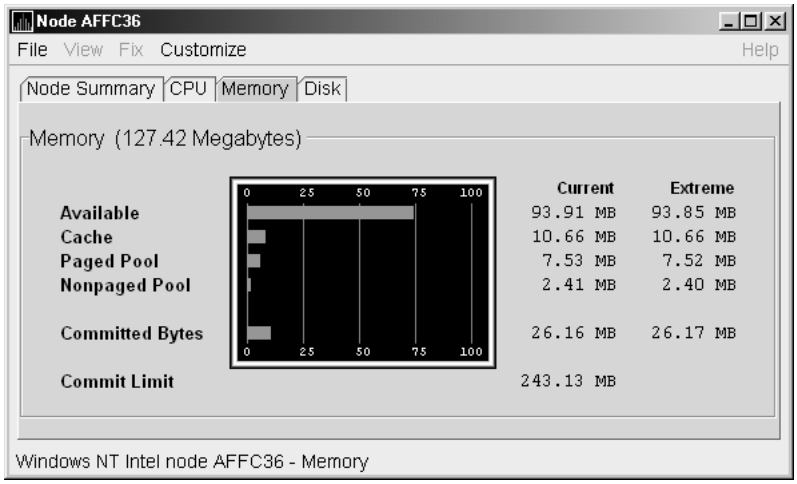
3.2.3.1 Windows Memory Summary

You can display the Windows Memory Summary page in either of the following ways:

- Double-click a node, and then click the Memory tab.
- Double-click a value under the MEM heading.

The Availability Manager displays the Windows Memory page (Figure 3–9).

Figure 3–9 Windows Memory Page



The Current and Extreme amounts on the page display the data shown in the following table. The table also indicates what the graph amounts represent.

Data	Description
Available	Size (in bytes) of the virtual memory currently on the zeroed, free, and standby lists. Zeroed and free memory are ready for use, with zeroed memory cleared to zeros. Standby memory is removed from a process's working set but is still available. The graph shows the percentage of physical memory that is available for use.
Cache	Number of bytes currently in use by the system cache. The system cache is used to buffer data retrieved from disk or LAN. The system cache uses memory not in use by active processes on the computer. The graph shows the percentage of physical memory devoted to the cache.
Paged Pool	Number of bytes in paged pool, a system memory area where operating system components acquire space as they complete their tasks. Paged pool pages can be paged out to the paging file when the system does not access them for long periods of time. The graph shows the percentage of physical memory devoted to paged pool.
Nonpaged Pool	Number of bytes in nonpaged pool, a system memory area where operating system components acquire space as they complete their tasks. Nonpaged pool pages cannot be paged out to the paging file; instead, they remain in memory as long as they are allocated. The graph shows the percentage of physical memory devoted to nonpaged pool.

Data	Description
Committed Bytes	Amount of available virtual memory (the Commit Limit) that is in use. Note that the commit limit can change if the paging file is extended. The graph shows the percentage of the Commit Limit used by the Committed Bytes.
Commit Limit	Size (in bytes) of virtual memory that can be committed without having to extend the paging files. If the paging files can be extended, this limit can be raised.

3.2.3.2 OpenVMS Memory Summary

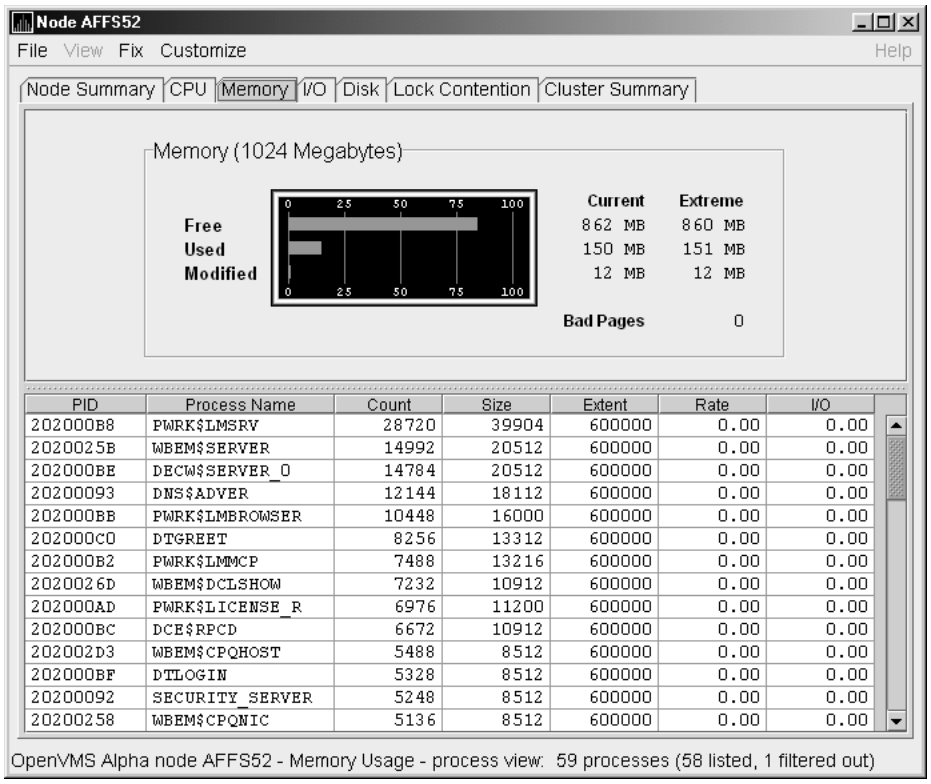
When you double-click a value under the MEM heading in an OpenVMS Node pane, or if you click the Memory tab, the Availability Manager displays the OpenVMS Memory Summary page (Figure 3–10).

Alternatively, if you click the View menu on the OpenVMS Memory Summary page, the following options are displayed in a popup menu:

- Memory Summary View
- Memory Details View

You can click Memory Summary View to select the Memory Summary page.

Figure 3–10 OpenVMS Memory Summary Page



The graph in the top pane shows memory distribution (Free, Used, and Modified) as absolute values, in megabytes of memory. Current and extreme values are also listed for each type of memory distribution. (Free memory uses the lowest seen value as its extreme.) Bad Pages show the number of pages that the operating system has marked as bad. The thresholds that you see in the graph are the ones

set for the LOMEMY event. (The LOMEMY thresholds are also in the display of values for the Mem field in the OpenVMS Node pane shown in Figure 3–1.)

The bottom pane displays the data shown in the following table.

Data	Description
PID	Process identifier. A 32-bit value that uniquely identifies a process.
Process Name	Name of the process.
Count	Number of physical pages or pagelets of memory that the process is using for the working set count.
Size	Number of pages or pagelets of memory the process is allowed to use for the working set size. The operating system periodically adjusts this value based on an analysis of page faults relative to CPU time used.
Extent	Number of pages or pagelets of memory in the process's working set extent (WSEXTENT) quota as defined in the user authorization file (UAF). Number of pages or pagelets cannot exceed the value of the system parameter WSMAX.
Rate	Number of page faults per second for the process.
I/O	Rate of I/O read attempts necessary to satisfy page faults (also known as page read I/O or the hard fault rate).

When you double-click a PID on the lower part of the Memory Summary page (Figure 3–10), the Availability Manager displays an OpenVMS Single Process, where you can click tabs to display pages containing specific data about one process. This data includes a combination of data from the CPU Process, Memory, and I/O pages, as well as data for specific quota utilization, current image, and queue wait time. These pages are described in Section 3.3.

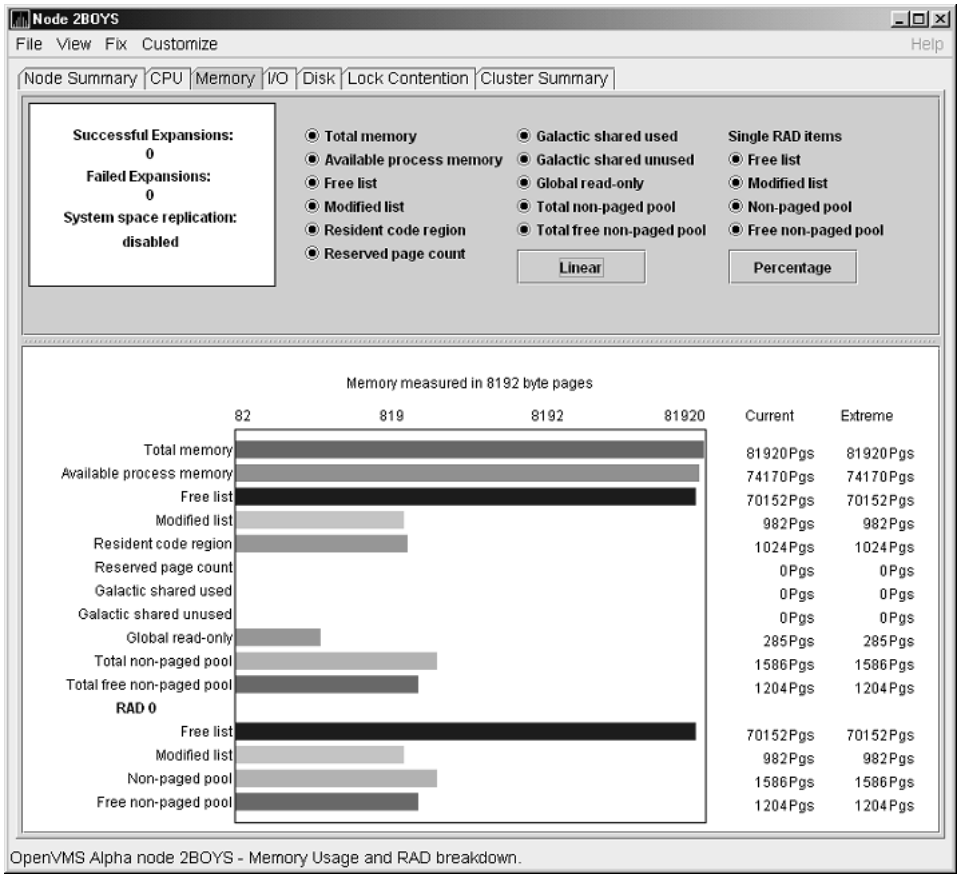
3.2.3.3 OpenVMS Memory Details

When you click the View menu on the OpenVMS Memory Summary page (see Figure 3–10), the following options are displayed in a popup menu:

- Memory Summary View
- Memory Details View

To display memory details, select that option. The Availability Manager displays the OpenVMS Memory Details page (Figure 3–11).

Figure 3–11 OpenVMS Memory Details Page



The following data items are in a box at the top left of the page:

Heading	Description
Successful Expansions	Number of successful nonpaged pool expansions.
Failed Expansions	Number of failed attempts to expand nonpaged pool.
System space replication	Whether system space replication is enabled or disabled.

To the right of the box is a list of system memory data that is displayed in the bar graphs at the bottom of the page. You can toggle these data items on or off (that is, to display them or not to display them as bar graphs). You can also click a small box to choose between Linear and Logarithmic bar graph displays.

The system memory data items are described in Table 3–4.

Table 3–4 System Memory Data

Data	Description
Total memory	Total physical memory size, as seen by OpenVMS.
Available process memory	Amount of total physical memory available to processes. This is the total memory minus memory allocated to OpenVMS.
Free list	Size of the free page list.
Modified list	Size of the modified page list.
Resident code region	Size of the resident image code region.
Reserved page count	Number of reserved memory pages.
Galactic shared used	Galaxy shared memory pages currently in use.
Galactic shared unused	Galaxy shared memory pages currently not in use.
Global read-only	Read-only pages, which are installed as resident when system space replication is enabled, that will also be replicated for improved performance.
Total nonpaged pool	Total size of system nonpaged pool.
Total free nonpaged pool	Amount of nonpaged pool that is currently free.

To the right of the system memory data is a list of single RAD data items, which are described in Table 3–5. You can toggle these items to display them or not in bar graphs.

Table 3–5 Single RAD Data Items

Data	Description
Free list	Size of the free page list.
Modified list	Size of the modified page list.
Nonpaged pool	Total size of system nonpaged pool.
Free nonpaged pool	Amount of nonpaged pool that is currently free.

Below the list of single RAD items is a box where you can toggle between Percentage and Raw Data to display Current and Extreme values to the right of the bar graphs.

3.2.4 OpenVMS I/O Summary and Page/Swap Files

By clicking the I/O tab on any OpenVMS node data page, you can display a page that contains summaries of accumulated I/O rates. In the top pane, the summary covers all processes; in the bottom pane, the summary is for one process.

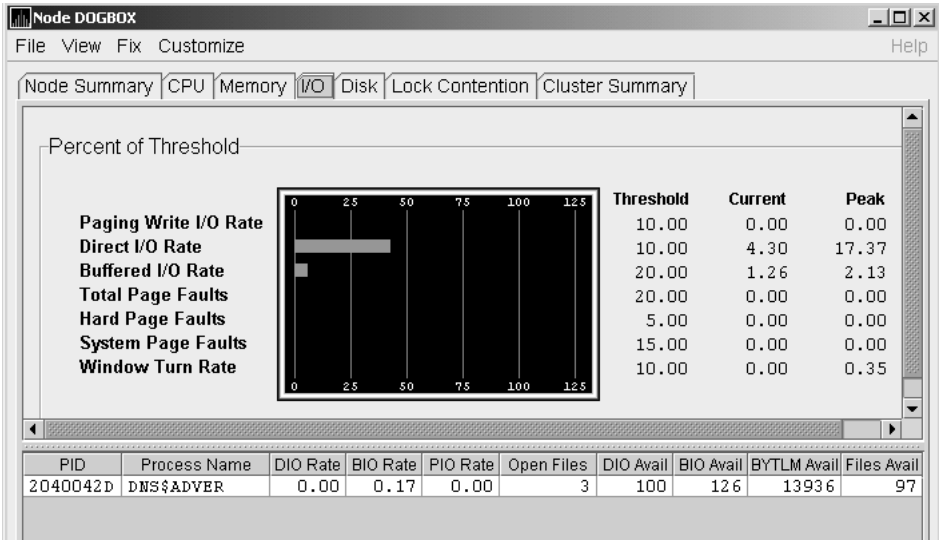
From the View menu, you can also choose to display (in the bottom pane) a list of page and swap files.

3.2.4.1 OpenVMS I/O Summary

The OpenVMS I/O Summary page displays the rate, per second, at which I/O transfers take place, including paging write I/O (WIO), direct I/O (DIO), and buffered I/O (BIO). In the top pane, the summary is for all CPUs; in the bottom pane, the summary is for one process.

When you double-click a data item under the DIO or BIO heading on the Node pane, or if you click the I/O tab, the Availability Manager displays, by default, the OpenVMS I/O Summary (Figure 3–12).

Figure 3–12 OpenVMS I/O Summary Page



The graph in the top pane represents the percentage of thresholds for the types of I/O shown in Table 3–6. The table also shows the event that is related to each data item. (See Section 7.6 for information about setting event thresholds.)

Table 3–6 I/O Data Displayed

Type of I/O	I/O Description	Related Event
Paging Write I/O Rate	Rate of write I/Os to one or more paging files.	HIPWIO
Direct I/O Rate	Transfers are from the pages or pagelets containing the process buffer that the system locks in physical memory to the system devices.	HIDIOR
Buffered I/O Rate	Transfers are for the process buffer from an intermediate buffer from the system buffer pool.	HIBIOR
Total Page Faults	Total of hard and soft page faults on the system, as well as peak values seen during an Availability Manager session.	HITTLP
Hard Page Faults	Total of hard page faults on the system.	HIHRDP
System Page Faults	Page faults generated by OpenVMS itself.	HISYSP
Window Turn Rate	Number of times that the file extent cache had to be refreshed.	WINTRN

Current and peak values are listed for each type of I/O. Values that exceed thresholds set by the events indicated in the table are displayed in red on the screen. Appendix B describes OpenVMS and Windows events.

To the right of the graph, the following values are listed:

Value	Description
Threshold	Defined in Event Properties.
Current	Current value or rate.
Peak	Highest value or rate seen since start of data collection.

The bottom pane displays summary accumulated I/O rates on a per-process basis. The following data is displayed:

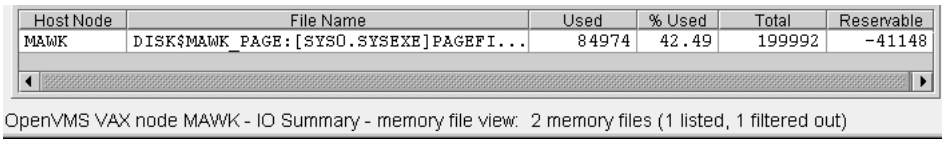
Data	Description
PID	Process identifier. A 32-bit value that uniquely identifies a process.
Process Name	Name of the current process.
DIO Rate	Direct I/O rate. The rate at which I/O transfers occur between the system devices and the pages or pagelets that contain the process buffer that the system locks in physical memory.
BIO Rate	Buffered I/O rate. The rate at which I/O transfers occur between the process buffer and an intermediate buffer from the system buffer pool.
PIO Rate	Paging I/O rate. The rate of read attempts necessary to satisfy page faults (also known as page read I/O or the hard fault rate).
Open Files	Number of open files.
DIO Avail	Direct I/O limit remaining. The number of remaining direct I/O limit operations available before the process reaches its quota. DIOLM quota is the maximum number of direct I/O operations a process can have outstanding at one time.
BIO Avail	Buffered I/O limit remaining. The number of remaining buffered I/O operations available before the process reaches its quota. BIOLM quota is the maximum number of buffered I/O operations a process can have outstanding at one time.
BYTLM	The number of buffered I/O bytes available before the process reaches its quota. BYTLM is the maximum number of bytes of nonpaged system dynamic memory that a process can claim at one time.
Files	Open file limit remaining. The number of additional files the process can open before reaching its quota. The FILLM quota is the maximum number of files that can be opened simultaneously by the process, including active network logical links.

When you double-click a PID on the lower part of the I/O Summary page, the Availability Manager displays an OpenVMS Single Process, where you can click tabs to display specific data about one process. See Section 3.3 for more details.

3.2.4.2 OpenVMS I/O Page/Swap Files

Click I/O Page/Swap Files on the I/O page View menu to select this option. The Availability Manager displays an OpenVMS I/O Page/Swap Files page. The top pane displays the same information as that in the OpenVMS I/O Summary page (Figure 3–12). The bottom pane contains the I/O Page/Swap Files Pane shown in Figure 3–13.

Figure 3–13 OpenVMS I/O Page/Swap Files Pane



The I/O Page/Swap Files Pane displays the following data:

Data	Description
Host Name	Name of the node on which the page or swap file resides.
File Name	Name of the page or swap file. For secondary page or swap files, the file name is obtained by a special AST to the job controller on the remote node. The Availability Manager makes one attempt to retrieve the file name.
Used	Number of used blocks in the file.
% Used	Of the available blocks in each file, the percentage that has been used.
Total	Total number of blocks in the file.
Reservable	The number of reservable blocks in each page or swap file currently installed. Reservable blocks are blocks that might be logially claimed by a process for future physical allocation. A negative value indicates that the file might be overcommitted. Although a negative value is not an immediate concern, it indicates that the file might become overcommitted if physical memory becomes scarce.

Notes

OpenVMS Version 7.3-1 and higher do not have a page or swap file "Reservable" field. The Availability Manager displays N/A in the field for these versions of OpenVMS.

If events for secondary page and swap files are signaled before the Data Analyzer has resolved their file names from the file ID (FID), events such as LOPGSP display the FID instead of file name information. You can determine the file name for the FID by checking the File Name field in the I/O Page Swap Files page. The FID for the file name is displayed after the file name.

3.2.5 Disk Summaries

The Disk tab allows you to display disk pages that contain data about availability, count, and errors of disk devices on the system. OpenVMS disk data displays differ from those for Windows nodes, as described in the following sections.

On OpenVMS pages, the View menu lets you choose the following disk summaries:

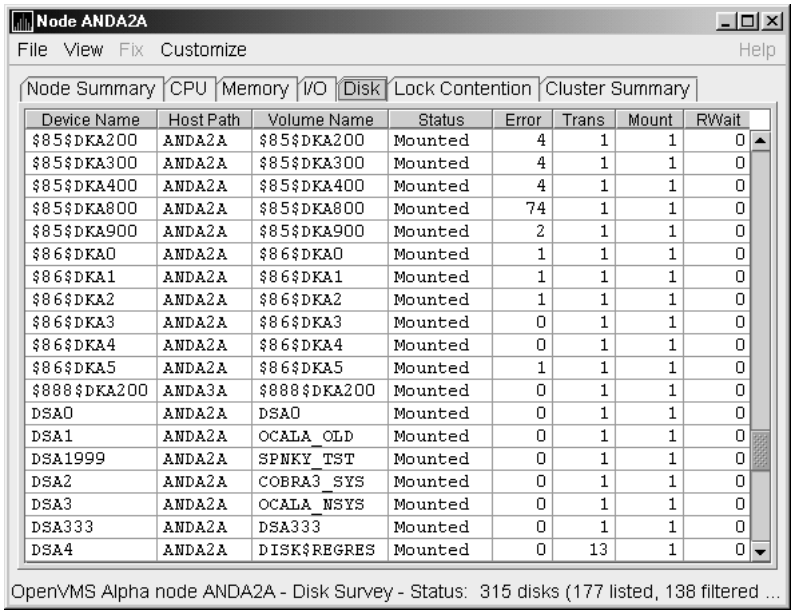
- Status Summary
- Volume Summary

Also, on the Disk Status Summary, you can double-click a device name to display a Single Disk Summary page.

3.2.5.1 OpenVMS Disk Status Summary

To display the default disk page, the OpenVMS Disk Status Summary (Figure 3–14), click the Disk tab on the OpenVMS Node Summary page. The Disk Status Summary page displays disk device data, including path, volume name, status, and mount, transaction, error, and resource wait counts.

Figure 3–14 OpenVMS Disk Status Summary



This summary displays the following data:

Heading	Description
Device Name	Standard OpenVMS device name that indicates where the device is located, as well as a controller or unit designation.
Host Path	Primary path (node) from which the device receives commands.
Volume Name	Name of the mounted media.

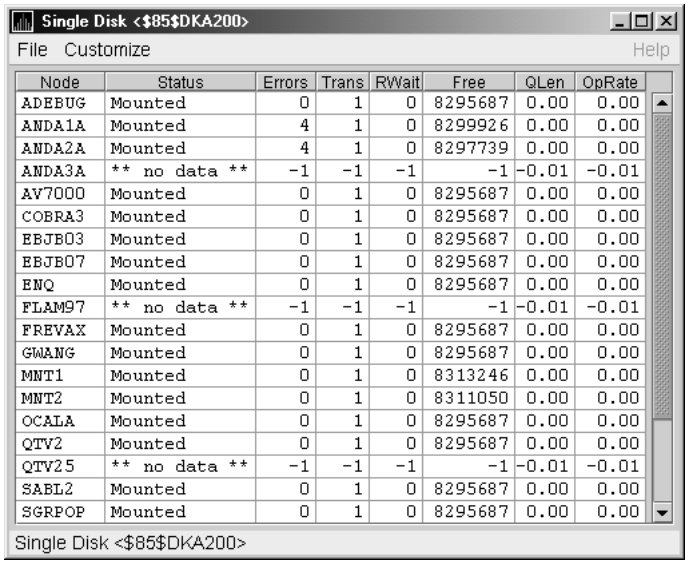
Heading	Description	
Status	One or more of the following disk status values:	
	Alloc	Disk is allocated to a specific user.
	CluTran	Disk status is uncertain because of a cluster state transition in progress.
	Dismount	Disk in process of dismounting; may be waiting for a file to close.
	Foreign	Disk is mounted with the /FOREIGN qualifier.
	Invalid	Disk is in an invalid state (most likely Mount Verify Timeout).
	MntVerify	Disk is waiting for a mount verification.
	Mounted	Disk is logically mounted by a MOUNT command.
	Offline	Disk is no longer physically mounted in device drive.
	Online	Disk is physically mounted in device drive.
	Shadow Set Member	Disk is a member of a shadow set.
	Unavailable	Disk is set to unavailable.
	Wrong Volume	Disk was mounted with the wrong volume name.
	Wrtlck	Disk is mounted and write locked.
Error	Number of errors generated by the disk (a quick indicator of device problems).	
Trans	Number of in-progress file system operations for the disk.	
Mount	Number of nodes that have the specified disk mounted. (These nodes must have the Data Collector installed and running to be participate in the mount count.)	
Rwait	Indicator that a system I/O operation is stalled, usually during normal recovery from a connection failure or during volume processing of host-based shadowing.	

3.2.5.2 OpenVMS Single Disk Summary

To collect single disk data and display the data on the Single Disk Summary, double-click a device name on the Disk Status Summary. Figure 3–15 is an example of a Single Disk Summary page. The display interval of the data collected is 5 seconds.

Note that you can sort the order in which data is displayed in the Single Disk Summary page by clicking a column header. To reverse the sort order of a column of data, click the column header again.

Figure 3–15 OpenVMS Single Disk Summary Page



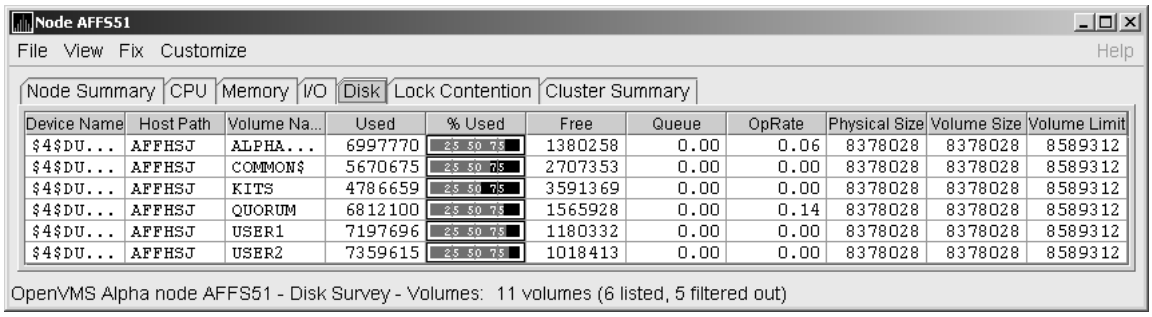
This summary displays the following data:

Data	Description
Node	Name of the node.
Status	Status of the disk: mounted, online, offline, and so on.
Errors	Number of errors on the disk.
Trans	Number of in-progress file system operations on the disk (number of open files on the volume).
Rwait	Indication of an I/O stalled on the disk.
Free	Number of free disk blocks on the volume.
QLen	Average number of operations in the I/O queue for the volume.
OpRate	Each node's contribution to the total operation rate (number of I/Os per second) for the disk.

3.2.5.3 OpenVMS Disk Volume Summary

By using the View option on the Disk Status Summary page (Figure 3–14), you can select the Volume Summary option to display the OpenVMS Disk Volume Summary (Figure 3–16). This page displays disk volume data, including path, volume name, disk block utilization, queue length, and operation rate.

Figure 3–16 OpenVMS Disk Volume Summary Page



The disk volume summary displays the data described in the following table. (The last two columns, Volume Size and Volume Limit, are displayed only on OpenVMS Version 7.3-2 and later systems.)

Data	Description
Device Name	Standard OpenVMS device name that indicates where the device is located, as well as a controller or unit designation.
Host Path	Primary path (node) from which the device receives commands.
Volume Name	Name of the mounted media.
Used	Number of blocks on the volume that are in use.
% Used	Percentage of the number of volume blocks in use in relation to the total volume blocks available.
Free	Number of blocks of volume space available for new data from the perspective of the node that is mounted.
Queue	Average number of I/O operations pending for the volume (an indicator of performance; less than 1.00 is optimal).
OpRate	Operation rate for the most recent sampling interval. The rate measures the amount of activity on a volume. The optimal load is device specific.
Physical Size	Total number of blocks on the current physical disk device. This is the "Total Blocks" field of the $SHOW DEVICE/FULL display
Volume Size	Current number of blocks available for file allocation. This is the "Logical Volume Size" field of the $SHOW DEVICE/FULL display. (See $SET VOLUME/SIZE for more information.) This column is displayed only on OpenVMS Version 7.3-2 and later systems.
Volume Limit	Maximum number of blocks the volume can reach using Dynamic Volume Expansion. This is the "Expansion Size Limit" of $SHOW DEVICE/FULL display. (See $SET VOLUME/LIMIT for more information.) This column is displayed only on OpenVMS Version 7.3-2 and later systems.

If the Availability Manager detects that a disk volume size has increased, an VLSZCH event is signalled:

```
AFFS55 Volume size of device $8$DKA200 (OPAL-X9U6) has changed
  ^                              ^          ^
  Node                         Device     Volume
  name                          name       name
```

Windows Logical and Physical Disk Summaries

On Windows nodes, the View menu lets you choose the following summaries:

- Logical Disk Summary
- Physical Disk Summary

3.2.5.4 Windows Logical Disk Summary

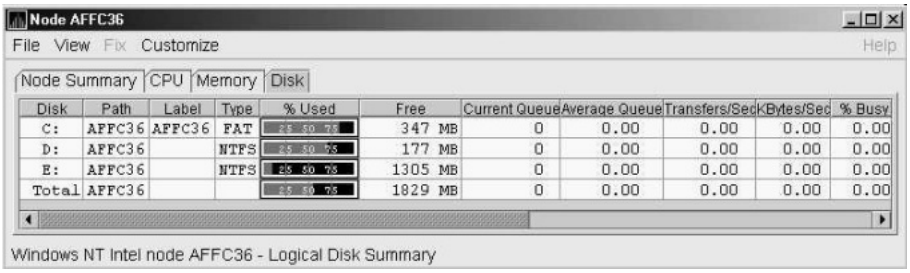
A **logical disk** is the user-definable set of partitions under a drive letter. The Windows Logical Disk Summary displays logical disk device data, including path, label, percentage used, free space, and queue statistics.

To display the Logical Disk Summary page, follow these steps:

1. Double-click a node name in the Node pane to display the Windows Node Summary.
2. Click the Disk tab on the Windows Node Summary.

The Availability Manager displays the Windows Logical Disk Summary page (Figure 3–17).

Figure 3–17 Windows Logical Disk Summary Page



This summary displays the following data:

Data	Description
Disk	Drive letter, for example, *c:*, or *Total*, which is the summation of statistics for all the disks.
Path	Primary path (node) from which the device receives commands.
Label	Identifying label of a volume.
Type	File system type; for example, FAT or NTFS.
% Used	Percentage of disk space used.
Free	Amount of free space available on the logical disk unit.
Current Queue	Number of requests outstanding on the disk at the time the performance data is collected. It includes requests in progress at the time of data collection.
Average Queue	Average number of both read and write requests that were queued for the selected disk during the sample interval.
Transfers/Sec	Rate of read and write operations on the disk.
KBytes/Sec	Rate data is transferred to or from the disk during write or read operations. The rate is displayed in kilobytes per second.
% Busy	Percentage of elapsed time that the selected disk drive is busy servicing read and write requests.

3.2.5.5 Windows Physical Disk Summary

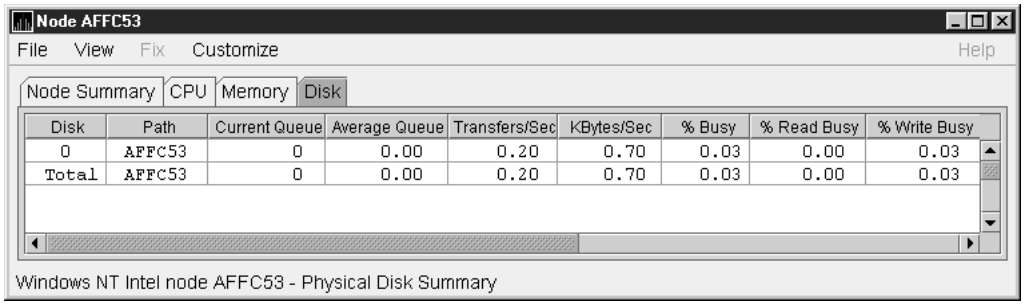
A **physical disk** is hardware used on your computer system. The Windows Physical Disk Summary displays disk volume data, including path, label, queue statistics, transfers, and bytes per second.

To display the Windows Physical Disk Summary, follow these steps:

1. Click the View menu on the Windows Logical Disk Summary.
2. Click the Physical Disk Summary menu option.

The Availability Manager displays the Windows Physical Disk Summary page (Figure 3–18).

Figure 3–18 Windows Physical Disk Summary Page



This page displays the following data:

Data	Description
Disk	Drive number, for example, 0, 1, 2 or *Total*, which is the summation of statistics for all the disks.
Path	Primary path (node) from which the device receives commands.
Current Queue	Number of requests outstanding on the disk at the time the performance data is collected; it includes requests in service at the time of data collection.
Average Queue	Average number of read and write requests that were queued for the selected disk during the sample interval.
Transfers/Sec	Rate of read and write operations on the disk. The rate is displayed in kilobytes per second.
KBytes/Sec	Rate bytes are transferred to or from the disk during read or write operations. The rate is displayed in kilobytes per second.
% Busy	Percentage of elapsed time the selected disk drive is busy servicing read and write requests.
% Read Busy	Percentage of elapsed time the selected disk drive is busy servicing read requests.
% Write Busy	Percentage of elapsed time the selected disk drive is busy servicing write requests.

3.2.6 OpenVMS Lock Contention

To display the OpenVMS Lock Contention page, click the Lock Contention tab on the OpenVMS Node Summary page (Figure 3–4). For all the nodes in the group you have selected, the Lock Contention page displays each resource for which a lock contention problem might exist.

Note

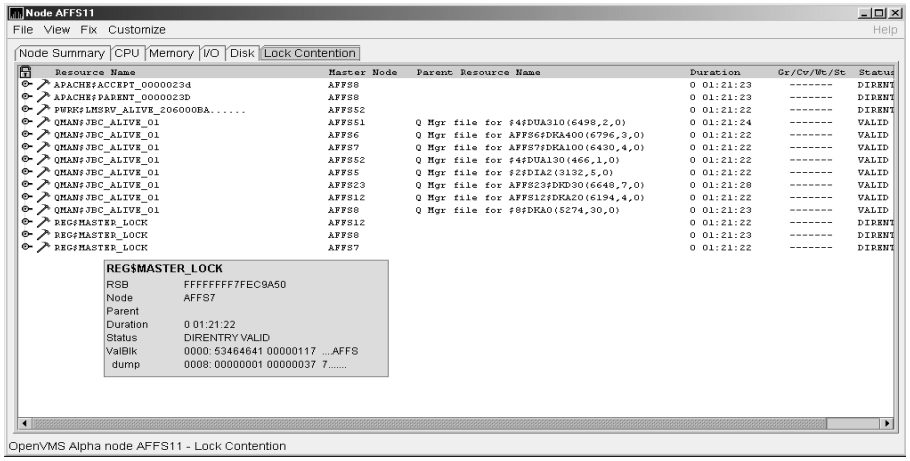
Lock contention data is accurate only if every node in an OpenVMS Cluster environment is in the same group. You might lose accuracy if you do not have all the nodes of a cluster in one group.

Example 3–1 shows a sample Lock Contention Log file, accompanied by an explanation of its contents.

3.2.6.1 Lock Contention Page in Decoded Format

Figure 3–19 shows a sample Lock Contention page containing resource names in decoded format, which is the default.

Figure 3–19 OpenVMS Lock Contention Page (Decoded Format)



(You can display a tooltip similar to the one shown in Figure 3–19 by holding the cursor on a resource line. See the Note in the introduction to this chapter for further details.)

By selecting the View menu (on the Lock Contention page), followed by the Resource names menu item, you can choose to display the resource name and parent resource name in either of two formats:

- Raw format (the format that SDA uses)
- Decoded format (the default format)

Figure 3–19 displays the resource names in decoded format. (The Availability Manager decodes all common resource names.)

The Lock Contention page displays the data described in Table 3–7. Numbered lines correspond to lines or items of data in the Lock Contention Log (see Example 3–1).

Table 3–7 Data on the OpenVMS Lock Contention Page

Reference Number	Data	Description
1	Resource Name	Resource name associated with the $ENQ system service call.
2	Master Node	Node on which the resource is mastered.
3	Parent Resource	Name of the parent resource. No name is displayed when a parent resource does not exist.
4	Duration	Time elapsed since the Availability Manager first detected the contention situation.
5	Gr/Cv/Wt/St	Total number of locks in each of four states. Numbers for these states appear only when you are collecting lock data. The states are: • Granted • Converting • Waiting • Stalled *Stalled* indicates one of several states whenever a lock is waiting for a response from another node in the cluster.
6	Status	Status of the lock. See the $ENQW description of flags in the *HP OpenVMS System Services Reference Manual*.

The tooltip that is displayed when you hold the cursor over a line of data in Figure 3–19 contains the data described in Table 3–7, as well as the information described in Table 3–8.

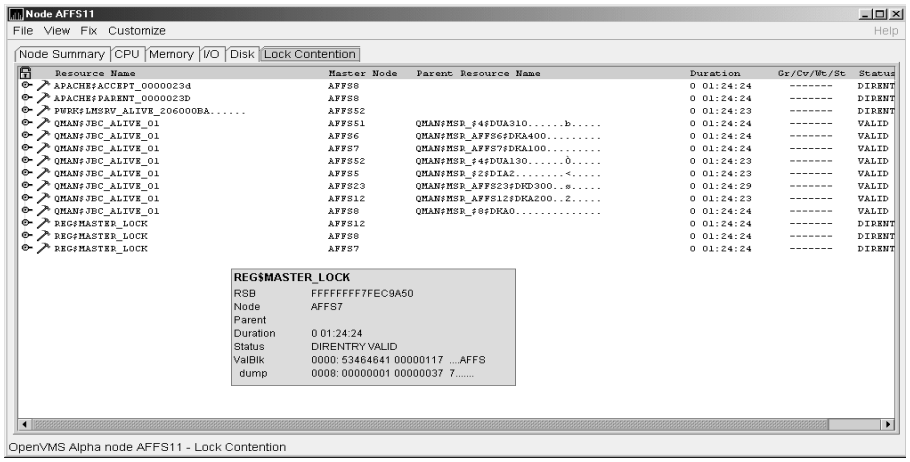
Table 3–8 Lock Contention Tooltip Data

Reference Number	Data	Description
7	RSB	Address of the Resource Block
8	ValBlk dump	Resource Value Block dump in standard OpenVMS dump format

3.2.6.2 Lock Contention Page in Raw Format

Figure 3–20 shows the Lock Contention page with resource name data displayed in raw format. It also shows the tooltip that is displayed when you hold the cursor over a line of data.

Figure 3–20 OpenVMS Lock Contention Page (Raw Format)



In Figure 3–20, notice that a period is substituted for each unprintable character in the Resource Name and Parent Resource Name fields.

3.2.6.3 Lock Block Data

When you click the handle preceding any line of resource data, the Availability Manager displays the lock block data shown in Figure 3–21 and Figure 3–22.

Figure 3–21 OpenVMS Lock Block Data

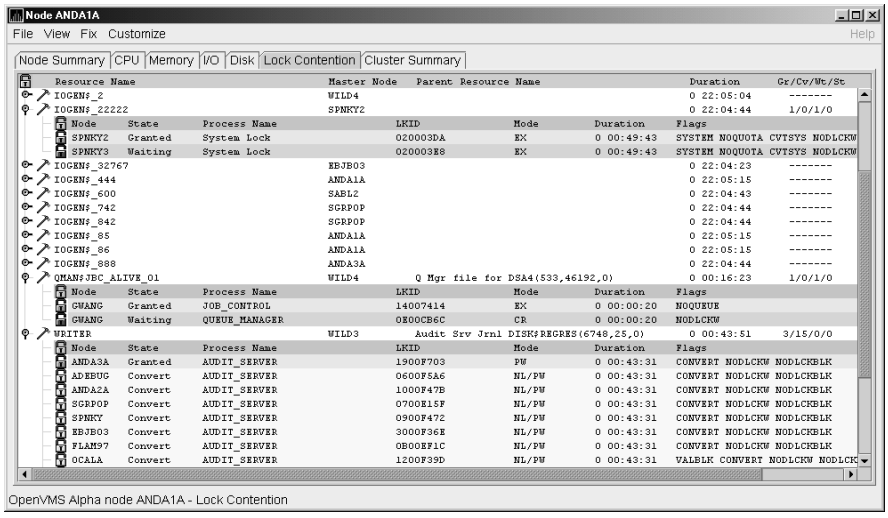
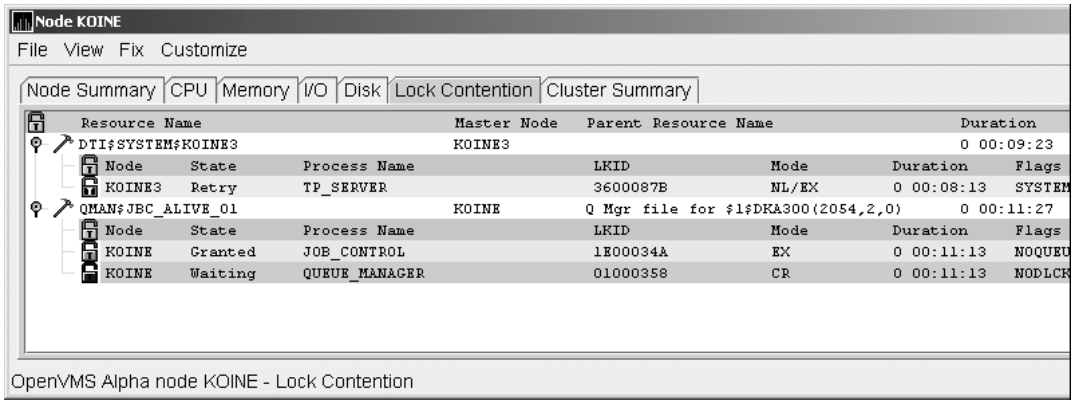


Figure 3–22 OpenVMS Lock Block Data (Retry Stalled State)



The lock block data in these two figures includes additional lock information under the headings shown in Table 3–9. Numbered lines correspond to lines or items of data in the Lock Contention Log (see Example 3–1).

Table 3–9 Lock Block Data

Reference Number	Data	Description
9	Node	Node name on which the lock is granted.
10	State	One of the following:

Color	Meaning
Green	Granted
Yellow	Converting
Pink	Waiting
Pale grey	Stalled states that are visible:
	SCSWAIT: A transient state indicating that a lock message has been sent to the node with the master lock and a response is awaited.
	RETRY: A transient state seen only under error conditions that require that a lock message be resent. This can occur if the node to which a lock message was sent goes down before a response from it is received or if resources for sending a message cannot be allocated.

11	Process Name	Name of the process that owns the blocking lock.
12	LKID	Lock ID value (which is useful with SDA).

(continued on next page)

Table 3–9 (Cont.) Lock Block Data

Reference Number	Data	Description		
13	Mode	One of the following modes in which the lock is granted or requested:[1]		
		CR	Concurrent read	Grants read access and allows resource sharing with other readers and writers.
		CW	Concurrent write	Grants write access and allows resource sharing with other groups.
		EX	Exclusive	Grants write access and prevents resource sharing with any other readers or writers.
		NL	Null	Grants no access; used as an indicator of interest or a placeholder for future lock conversion.
		PR	Protected read	Grants read access and allows resource sharing with other readers, but not writers.
		PW	Protected write	Grants write access and prevents resource sharing with any other readers or writers.
		If one mode is displayed, it is the Granted mode; if two modes are displayed, the first is the Granted mode and the second is the Converting mode.		
14	Duration	Length of time the lock has been in the current queue since the console application found the lock.		
15	Flags	Flags specified with the $ENQW request. See the $ENQW entry in *HP OpenVMS System Services Reference Manual*.		

[1]Descriptions are from Goldenberg, Ruth, and Saravanan, Saro, *OpenVMS AXP Internals and Data Structures*, Version 1.5, Digital Press, 1994.

To interpret the information displayed on the OpenVMS Lock Contention page, you need to understand OpenVMS lock management services. For more information, see the *HP OpenVMS System Services Reference Manual*.

3.2.6.4 Lock Block Log File

Example 3–1 contains an excerpt of a lock block log file. You can find a lock block log file in either of the following locations:

System	File Name	Location
Windows	AvailManLock.log	Installation directory
OpenVMS	Log prefaced by AMDS$AM_LOG	Directory to which AMDS$AM_LOG logical points

Numbers preceding lines or items of data in Example 3–1 correspond to numbered lines in Table 3–7, Table 3–8, and Section 3.2.6.3. Table 3–10 contains lines or items of data in a lock block log file that are not described in the other tables in this section.

Table 3–10 Additional Data in the Lock Block Log File

Reference Number	Data from Example	Description
16	Reason for logging	In the example, the reason for logging is "the number of locks has changed." Other reasons include the "initial discovery of resource contention" or "lock data collection has been turned on."
17	GGMODE/CGMODE	Lock has been Granted/Lock is Converting
18	Resource Name Dump	OpenVMS style of Resource Name dump
19	Rdb global database name resource	Decoded Resource Name
20	Parent Resource Name Dump	OpenVMS style of Parent Resource Name dump
21	Rdb global database name resource	Decoded Parent Resource Name
22	Lock data is being collected	The handle preceding a line of lock data has been turned.
23	Master copy info. Remote Node	Remote node that contains the master copy of the lock. If “Local Copy”, only one node is interested in the lock.
24	Master copy info. Remote Lock ID	Lock ID of remote node that contains the master copy of the lock.

Example 3–1 Lock Block Log File

```
************************************************
Time:  11-Nov-2003 14:54:13.656

16)Reason for logging:    Number of locks has changed

2) Master Lock Node:      ALTOS

1) Resource Name:         I.....
17)    GGMODE/CGMODE:     EX/EX
6)     Status:            VALID
7)     RSB Address:       FFFFFFFE.889F1580
18)    Resource Name Dump (includes initial count byte):
          0000:   000200 00004906  .I.....

8)     Value Block Dump:
          0000: 00000000 00000000  ........
          0008: 00000000 00000000  ........

19) Rdb Remote monitor resource
          #:                2

3) Parent Resource Name:  Ý...D....VDEROOT     . 7....
7)     RSB Address:       FFFFFFFE.8847DB80
20)    Resource Name Dump (includes initial count byte):
          0000: 00004400 0000DD1C  .....D..
          0008: 4F4F5245 44560200  ..VDEROO
          0010: A0002020 20202054  T     ..
          0018:       00 00000237  7....

8)     Value Block Dump:
          0000: 00000000 00000000  ........
          0008: 00000000 00000000  ........
```

(continued on next page)

Example 3–1 (Cont.) Lock Block Log File

```
21)    Rdb global database name resource
          Disk volume name:  VDEROOT
          FID for file:      (14240,2,0)

22) Lock data is being collected

5)     Granted lock count:       1
5)     Conversion lock count:    0
5)     Waiting lock count:       4
5)     Stalled lock count:       0

       10)      9)              11)           12)      13) Master copy info:   15)
      Lock     Node   Process  Process         Lock    Gr/Cv Remote Remote   Flags
      State           PID      Name            ID       Mode Node   Lock ID
                                                             23)    24)
      Granted  ALTOS  28E00441 RDMS_MONITOR70  04014B37 EX    (Local copy)      NQUE SYNC SYS
      Waiting  ALTOS  2880023F RDMS_MONITOR70  4C0065B5 PR   TSAVO  32005001      SYNC SYS  NDLW
      Waiting  ALTOS  00000000 (EPID=28A0023D) 4C0144C4 PR   ETOSHA 74005E36      SYNC SYS  NDLW
      Waiting  ALTOS  28C00448 RDMS_MONITOR70  1D0144A3 PR   CHOBE  77005906      SYNC SYS  NDLW
      Waiting  ALTOS  28E026C3 VDE$KEPT126A3   01014B2D PR    (Local copy)             SYS  NDLW

**********************************************
```

3.3 OpenVMS Single Process

When you double-click a PID on the lower part of an OpenVMS CPU Process (Figure 3–8), Memory (Figure 3–10), or I/O (Figure 3–12) page, the Availability Manager displays the first of several OpenVMS Single Process pages. On these pages, you can click tabs to display specific data about one process. The following sections describe these pages.

Note About ENQ Values on Single Process Pages

In versions of Availability Manager prior to Version 2.0, whenever an ENQ value in the Single Process page was higher than 32,767, the Availability Manager assigned it a large default value (4,294,967,295, for example) and displayed that large value. This problem has been corrected so that any value up to 32 bits is displayed correctly.

3.3.1 Single Process Information

To display the Single Process Information page (Figure 3–23), click the Process Information tab. The data on this page is displayed at the default intervals shown for Single Process Data on the Data Collection Customization page.

Figure 3–23 Single Process Information Page

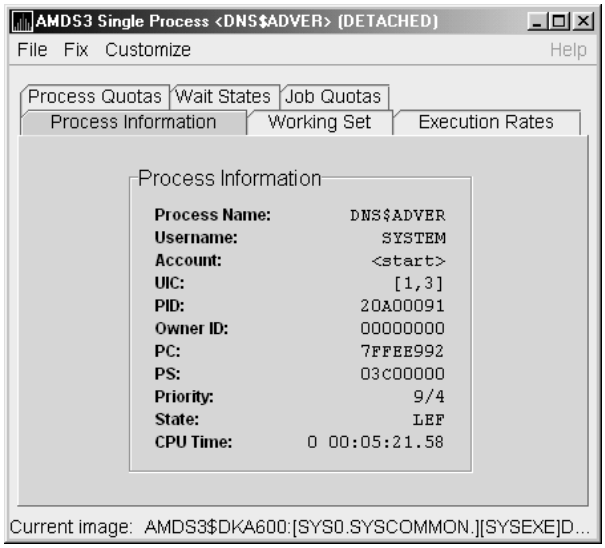


Table 3–11 describes the data in Figure 3–23.

Table 3–11 Single Process Information

Data	Description
Process name	Name of the process.
Username	User name of the user who owns the process.
Account	Account string that the system manager assigns to the user.
UIC	User identification code (UIC). A pair of numbers or character strings that designate the group and user.
PID	Process identifier. A 32-bit value that uniquely identifies a process.
Owner ID	Process identifier of the process that created the process displayed on the page. If the PID is 0, then the process is a parent process.
PC	Program counter. On OpenVMS Alpha systems, this value is displayed as 0 because the data is not readily available to the Data Collector node.
PS	Processor status longword (PSL). This value is displayed on VAX systems only.
Priority	Computable and base priority of the process. Priority is an integer between 0 and 31. Processes with higher priority are given more CPU time.
State	One of the process states listed in Appendix A.
CPU Time	CPU time used by the process.

3.3.2 Single Process Working Set

To display the Single Process Working Set page (Figure 3–24), click the Working Set tab.

Figure 3–24 Single Process Working Set Page

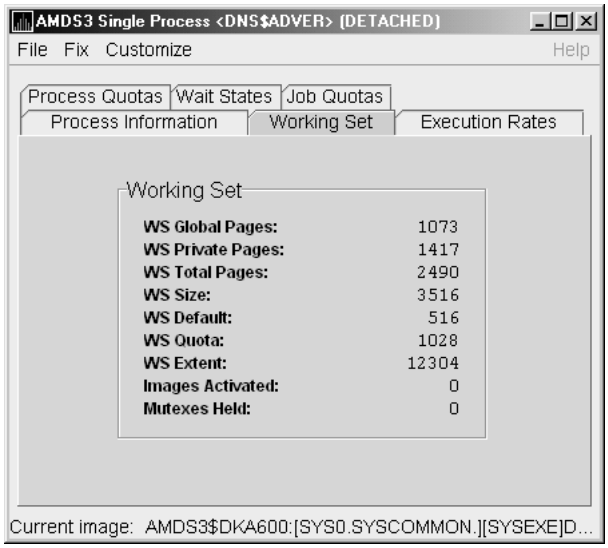


Table 3–12 describes the data in Figure 3–24.

Table 3–12 Single Process Working Set

Data	Description
WS Global Pages	Shared data or code between processes, listed in pages (measured in pagelets).
WS Private Pages	Amount of accessible memory, listed in pages (measured in pagelets).
WS Total Pages	Sum of global and private pages (measured in pagelets).
WS Size	Working set size. The number of pages (measured in pagelets) of memory the process is allowed to use. This value is periodically adjusted by the operating system based on analysis of page faults relative to CPU time used. Increases in large units indicates that a process is taking many page faults, and its memory allocation is increasing.
WS Default	Working set default. The initial limit of the number of physical pages (measured in pagelets) of memory the process can use. This parameter is listed in the user authorization file (UAF); discrepancies between the UAF value and the displayed value are due to page/longword boundary rounding or other adjustments made by the operating system.
WS Quota	Working set quota. The maximum amount of physical pages (measured in pagelets) of memory the process can lock into its working set. This parameter is listed in the UAF; discrepancies between the UAF value and the displayed value are due to page/longword boundary rounding or other adjustments made by the operating system.

(continued on next page)

Table 3–12 (Cont.) Single Process Working Set

Data	Description
WS Extent	Working set extent. The maximum number of physical pages (measured in pagelets) of memory the system will allocate for the process. The system provides memory to a process beyond its quota only when it has an excess of free pages and can be recalled if necessary. This parameter is listed in the UAF; any discrepancies between the UAF value and the displayed value are due to page/longword boundary rounding or other adjustments made by the operating system.
Images Activated	Number of times an image is activated.
Mutexes Held	Number of mutual exclusions (mutexes) held. Persistent values other than zero (0) require analysis. A mutex is similar to a lock but is restricted to one CPU. When a process holds a mutex, its priority is temporarily increased to 16.

3.3.3 Single Process Execution Rates

To display the Single Process Execution Rates page (Figure 3–25), click the Execution Rates tab.

Figure 3–25 Single Process Execution Rates Page

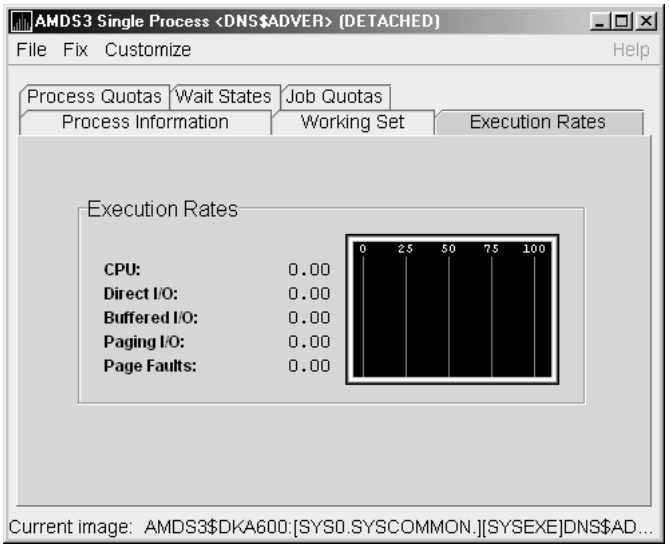


Table 3–13 describes the data in Figure 3–25.

Table 3–13 Single Process Execution Rates

Data	Description
CPU	Percent of CPU time used by this process. The ratio of CPU time to elapsed time.

(continued on next page)

Table 3–13 (Cont.) Single Process Execution Rates

Data	Description
Direct I/O	Rate at which I/O transfers take place from the pages or pagelets containing the process buffer that the system locks in physical memory to the system devices.
Buffered I/O	Rate at which I/O transfers take place for the process buffer from an intermediate buffer from the system buffer pool.
Paging I/O	Rate of read attempts necessary to satisfy page faults. This is also known as page read I/O or the hard fault rate.
Page Faults	Page faults per second for the process.

3.3.4 Single Process Quotas

To display the Single Process Quotas page (Figure 3–26), click the Process Quotas tab.

Figure 3–26 Single Process Quotas Page

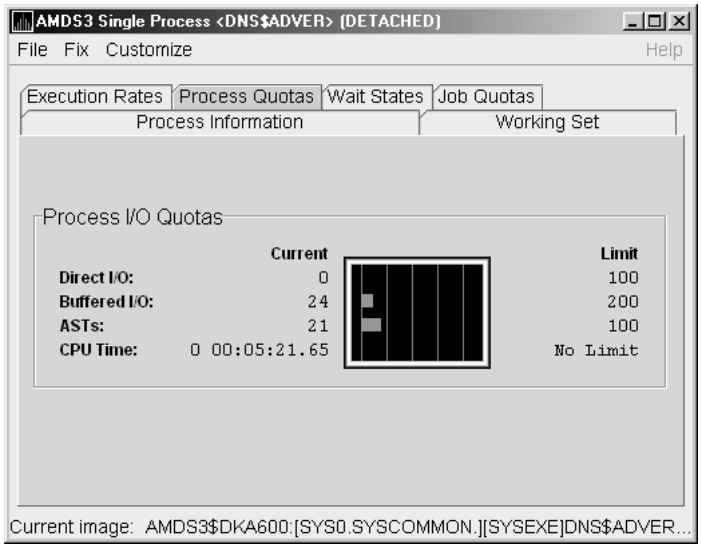


Table 3–14 describes the data displayed in Figure 3–26. When you display the SWAPPER process, however, no values are listed in this section. The SWAPPER process does not have quotas defined in the same way as other system and user processes do.

Table 3–14 Single Process Quotas

Data	Description
Direct I/O	The current number of direct I/Os used compared with the limit possible.
Buffered I/O	The current number of buffered I/Os used compared with the possible limit.

(continued on next page)

Table 3–14 (Cont.) Single Process Quotas

Data	Description
ASTs	Asynchronous system traps. The current number of ASTs used compared with the possible limit.
CPU Time	Amount of time used compared with the possible limit (in ms). "No Limit" is displayed if the limit is 0.

3.3.5 Single Process Wait States

To display the Single Process Wait States page (Figure 3–27), click the Wait States tab.

Figure 3–27 Single Process Wait States Page

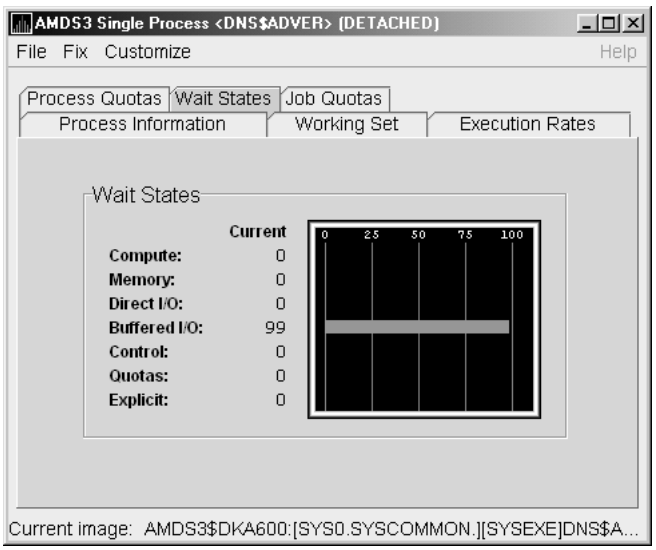


Table 3–15 describes the data in Figure 3–27. In the graph, “Current” refers to the percentage of elapsed time each process spends in one of the computed wait states. If a process spends all its time waiting in one state, the total gradually reaches 100%.

How Wait States are Calculated

The wait state specifies why a process cannot execute, based on calculations made on collected data. Each value is calculated over an entire data collection period of approximately 2 minutes. The graph shows, over this period of time, the percentage of time a process spends in each wait state. Each value is an exponential average that approximates a moving average. A more detailed explanation follows.

When monitoring of a single process starts, all wait state values are zero. When the system periodically checks the process, the system first subtracts 10% from each value. It then adds a value of 10 to the wait state the process is currently in, if any.

For example, at the start, if a process is found to be in the Control wait state, the graph immediately registers 10 for Control. If the process is still in the Control wait state the next time it is checked, the graph shows Control at 19. This value is 90% of the original 10 (or 9), plus 10 (the value currently being added).

The next time the process is checked, if it is found to be in the Buffered I/O wait state, Buffered I/O is set to 10 and Control is set to 17 (approximately 90% of the previous value of 19).

The following time the process is checked, if it is not in a wait state at all, Buffered I/O is set to 9 (90% of 10), and Control is set to 15 (90% of 17).

Appendix A contains descriptions of process wait states.

Table 3–15 Single Process Wait States

Data	Description
Compute	Average percentage of time that the process is waiting for CPU time. Possible states are COM, COMO, or RWCAP.
Memory	Average percentage of time that the process is waiting for a page fault that requires data to be read from disk; this is common during image activation. Possible states are PFW, COLPG, FPG, RWPAG, RWNPG, RWMPE, or RWMPB.
Direct I/O	Average percentage of time that the process waits for data to be read from or written to a disk or tape. The possible state is DIO.
Buffered I/O	Average percentage of time that the process waits for data to be read from or written to a slower device such as a terminal, line printer, mailbox, or network traffic. The possible state is BIO.
Control	Average percentage of time that the process is waiting for another process to release control of some resource. Possible states are CEF, MWAIT, LEF, LEFO, RWAST, RWMBX, RWSCS, RWCLU, RWCSV, RWUNK, or LEF waiting for an ENQ.
Quotas	Average percentage of time that the process is waiting because the process has exceeded some quota. Possible states are QUOTA or RWAST_QUOTA.
Explicit	Average percentage of time that the process is waiting because the process asked to wait, such as a hibernate system service. Possible states are HIB, HIBO, SUSP, SUSPO, or LEF waiting for a TQE.

3.3.6 Single Process Job Quotas

To display the Single Process Job Quotas page (Figure 3–28), click the Job Quotas tab.

Figure 3–28 Single Process Job Quotas Page

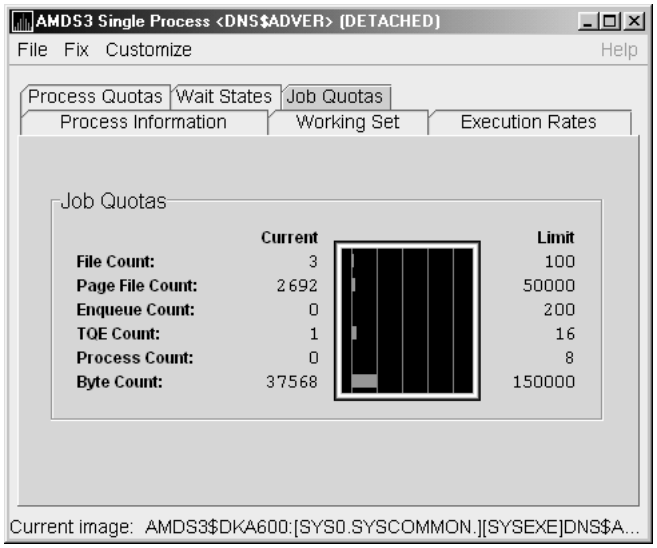


Table 3–16 describes the data in Figure 3–28.

Table 3–16 Single Process Job Quotas

Data	Description
File Count	Current number of open files compared with the possible limit.
Page File Count	Current number of disk blocks in the page file that the process can use compared with the possible limit.
Enqueue Count	Current number of resources (lock blocks) queued compared with the possible limit.
TQE Count	Current number of timer queue entry (TQE) requests compared with the possible limit.
Process Count	Current number of subprocesses created compared with the possible limit.
Byte Count	Current number of bytes used for buffered I/O transfers compared with the possible limit.

4
Displaying OpenVMS Cluster Data

The Availability Manager displays a great deal of OpenVMS Cluster data. The amount of cluster information has increased in each successive version of the product and will probably continue to do so. In order to accommodate future growth in this area, beginning with Availability Manager Version 2.2, OpenVMS Cluster information is documented in a separate chapter of this manual.

By clicking a series of "handles" on the cluster node tree in the Cluster Members pane of the Cluster Summary page, you can open up lines of data to display progressively more detailed cluster data. This chapter describes the data you can display.

Support for Managed Objects

New support has been added to the OpenVMS Data Collector, RMDRIVER, for OpenVMS managed objects. These are operating system components with characteristics that allow the Availability Manager to manage them. Managed objects, which register themselves with the Data Collector at system startup, not only provide data but also implement fixes in response to client requests.

In OpenVMS Version 7.3 and later, cluster data and fixes are available for LAN virtual circuits through the managed object interface. When the Availability Manager Version 2.2 Data Analyzer connects to a Data Collector node, it retrieves a list of the managed objects on that node, if any. For such a node, the Availability Manager can provide additional details and new data that would otherwise be unavailable.

Note

To enable managed object data collection on nodes running OpenVMS Version 7.3 and later, the system manager must take steps so that the Data Collector driver, RMDRIVER, is loaded early in the boot process. See the postinstallation steps in the *Installation Instructions for OpenVMS Systems* for more details on how to enable collection of managed object data.

LAN Displays

When you monitor OpenVMS Version 7.3 and later nodes with managed objects enabled, additional cluster data and fixes are available for LAN virtual circuits. This includes enhanced LAN virtual circuit summary data in the Cluster Summary window and the LAN Virtual Circuit Details (NISCA) window. In addition, the Cluster Summary now includes virtual circuit, channel, and device fixes. If managed object support is not enabled for a Data Collector node, then only basic virtual circuit data is available.

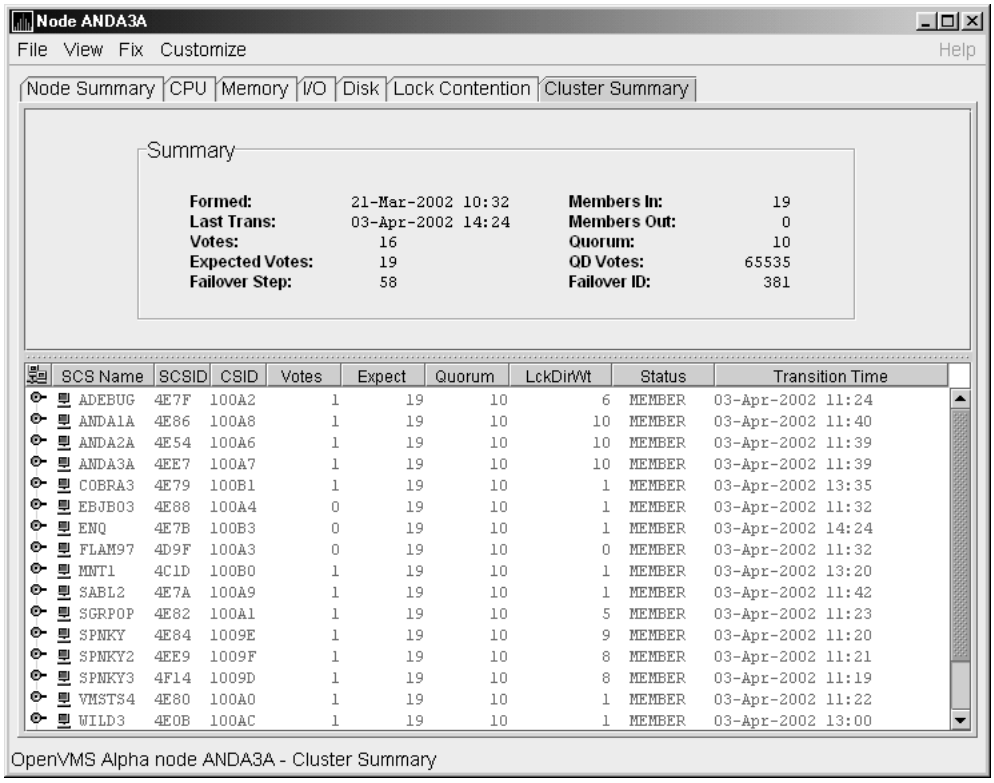
4.1 OpenVMS Cluster Summary Page

To display the OpenVMS Cluster Summary page (Figure 4–1), click the Cluster Summary tab on an OpenVMS Node Summary page.

The Cluster Summary page contains cluster interconnect information for an entire cluster as well as detailed information about each node in the cluster, including System Communications Services (SCS) circuits and connections for individual nodes. You can also display details about PEdriver LAN virtual circuits.

The data items shown on the page correspond to data that the Show Cluster utility (SHOW CLUSTER) displays for the SYSTEMS, MEMBERS, CONNECTIONS, and CIRCUITS classes. No SHOW CLUSTER counterpart exists for the PEdriver LAN virtual circuit, channel, and device detail displays. The data items shown on the page also correspond to data that the SCACP utility displays for SHOW commands that display PORT, CIRCUIT, VC, CHANNEL, and LAN DEVICE information.

Figure 4–1 OpenVMS Cluster Summary



The two panes in the Cluster Summary page display the following information:

- The Summary pane (top) displays summary information about the entire cluster.
- The Cluster Members pane (bottom) displays detailed information about each node in the cluster, including its System Communication Architecture (SCA) connections with other nodes.

Notes About Pane Displays

Following are notes about the display of data in the panes:

- The Availability Manager signals the LOVOTE event when cluster votes minus cluster quorum *is less than* the threshold value for the event:

  ```
  LOVOTE, 'node' VOTES count is close to or below QUORUM
  ```

  The default threshold for the LOVOTE event is 1.

- You can change collection intervals by using the Customize menu on the main Application window. Choose the Customize OpenVMS... option, and then click the Data Collection tab. On the page displayed, you can select the data that you want to collect and also change default collection intervals.

4.1.1 OpenVMS Cluster Summary Pane

Table 4–1 describes the data in the OpenVMS Cluster Summary pane (see Figure 4–1).

Table 4–1 Summary Pane Data

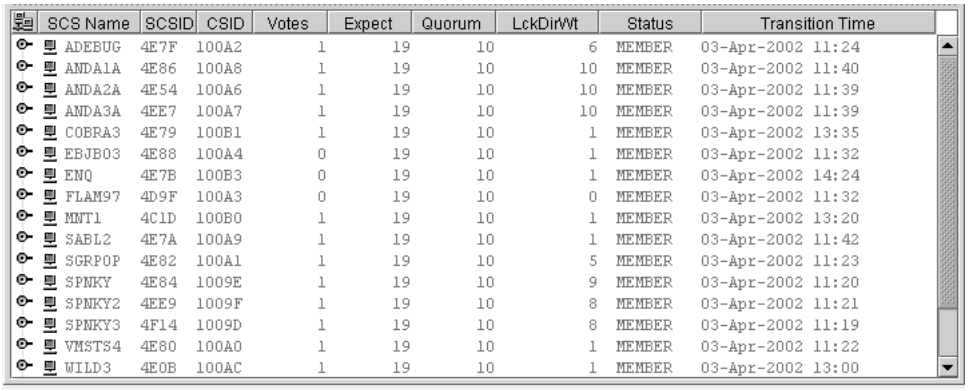
Data	Description
Formed	Date and time the cluster was formed.
Last Trans	Date and time of the most recent cluster state transition.
Votes	Total number of quorum votes being contributed by all cluster members and by the quorum disk.
Expected Votes	The expected votes contribution by all members of the cluster. This value is calculated from the maximum EXPECTED_VOTES system parameter and the maximized value of the VOTES system parameter.
Failover Step	Current failover step index. Shows which step in the sequence of failover steps the failover is currently executing.
Members In	Number of cluster members to which the Availability Manager has a connection.
Members Out	Number of cluster members to which the Availability Manager either has no connection or has lost its connection.
Quorum[1]	Number of votes that must be present for the cluster to function and to permit user activity, that is, to "maintain cluster quorum."
QD Votes	Number of votes given to the quorum disk. A value of 65535 means no quorum disk exists.
Failover ID	Failover instance identification. Unique ID of a failover sequence that indicates to system managers whether a failover has occurred since the last time they checked.

[1]You can adjust the quorum value by using the Adjust Quorum fix described in Section 6.2.2.

4.1.2 OpenVMS Cluster Members Pane

The Cluster Members pane (the lower pane on the Cluster Summary page shown in Figure 4–1) lists all the nodes in the cluster and provides detailed information about each one. Figure 4–2 shows only the Cluster Members pane.

Figure 4–2 OpenVMS Cluster Members Pane



SCS Name	SCSID	CSID	Votes	Expect	Quorum	LckDirWt	Status	Transition Time
ADEBUG	4E7F	100A2	1	19	10	6	MEMBER	03-Apr-2002 11:24
ANDA1A	4E86	100A8	1	19	10	10	MEMBER	03-Apr-2002 11:40
ANDA2A	4E54	100A6	1	19	10	10	MEMBER	03-Apr-2002 11:39
ANDA3A	4EE7	100A7	1	19	10	10	MEMBER	03-Apr-2002 11:39
COBRA3	4E79	100B1	1	19	10	1	MEMBER	03-Apr-2002 13:35
EBJBO3	4E88	100A4	0	19	10	1	MEMBER	03-Apr-2002 11:32
ENQ	4E7B	100B3	0	19	10	1	MEMBER	03-Apr-2002 14:24
FLAM97	4D9F	100A3	0	19	10	0	MEMBER	03-Apr-2002 11:32
MNT1	4C1D	100B0	1	19	10	1	MEMBER	03-Apr-2002 13:20
SABL2	4E7A	100A9	1	19	10	1	MEMBER	03-Apr-2002 11:42
SGRPOP	4E82	100A1	1	19	10	5	MEMBER	03-Apr-2002 11:23
SPNKY	4E84	1009E	1	19	10	9	MEMBER	03-Apr-2002 11:20
SPNKY2	4EE9	1009F	1	19	10	8	MEMBER	03-Apr-2002 11:21
SPNKY3	4F14	1009D	1	19	10	8	MEMBER	03-Apr-2002 11:19
VMSTS4	4E80	100A0	1	19	10	1	MEMBER	03-Apr-2002 11:22
WILD3	4E0B	100AC	1	19	10	1	MEMBER	03-Apr-2002 13:00

The first level of information in the Cluster Members pane contains cluster member data, which is described in Table 4–2.

Table 4–2 Cluster Member Data

Data	Description
SCS Name	System Communications Services (SCS) name for the node (system parameter SCSNODE).
SCSID	SCS identification for the node (system parameter SCSYSTEMID).
CSID	Cluster system identification.
Votes	Number of votes the member contributes.
Expect	Member's expected votes as set by the EXPECTED_VOTES system parameter.
Quorum	Number of votes that must be present for the cluster to function and permit user activity, that is, to "maintain cluster quorum".
LckDirWt	Lock manager distributed directory weight as determined by the LCKDIRWT system parameter.
Status	Current cluster member status:

Status Value	Description
NEW	New system in cluster.
BRK_NEW	New system; there has been a break in the connection.
MEMBER	System is a member of the cluster.
BRK_MEM	Member; there has been a break in the connection.
NON	System is not a member of the cluster.
BRK_NON	Nonmember; there has been a break in the connection.
REMOVED	System has been removed from the cluster.
BRK_REM	System has been removed from the cluster, and there has also been a break in the connection.

(continued on next page)

Table 4–2 (Cont.) Cluster Member Data

Data	Description
Transition Time	The time of the system's last change in cluster membership status.

4.2 Summary Data in the Cluster Members Pane

The following sections contain descriptions of the categories of summary data displayed in the Cluster Members pane shown in Figure 4–2.

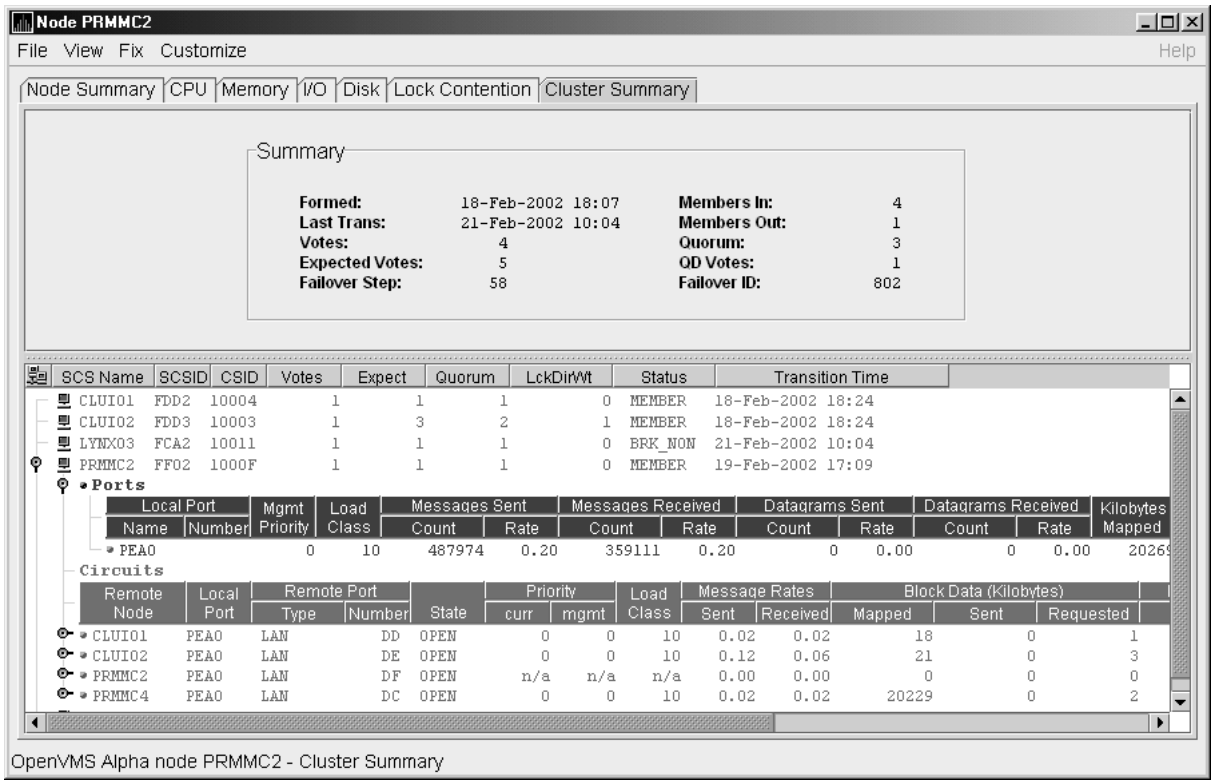
When you click the handle in front of an SCS (System Communications Services) Name, the Availability Manager first displays a Ports heading, if ports are configured on your system.

A **port** is an OpenVMS device that provide SCA (System Communications Architecture) services. Port summary data is discussed in Section 4.2.1. Below the Ports heading is the Circuits heading, which precedes a line of SCA headings. (SCA data are discussed in Section 4.2.2.)

4.2.1 Port Summary Data

When you initially click the handle in front of Ports in the Cluster Members pane (Figure 4–1), Ports headings are displayed, with information about port interfaces on the local system, as shown in Figure 4–3.

Figure 4–3 Port Summary Data



The port summary data shown in Figure 4–3 is described in Table 4–3. Data items in this table are related to the SCACP utility SHOW PORTS display and the SHOW CLUSTER utility LOCAL_PORT CLASS display.

Table 4–3 Local Port Data

Data	Description
Local Port:	
Name	Device name of the port.
Number	The local port's interconnect address or other interconnect-specific identifier.
Mgmt Priority	Management priority assigned to the port.
Load Class	Hard-coded capacity value of the port, based on the rate (in megabits/second) of the interconnect of the port.
Messages Sent:	
Count	Total number of messages sent since the port was initialized.
Rate	Rate at which messages are sent (per second).
Messages Received:	
Count	Total number of messages sent since the port was initialized.
Rate	Rate at which SCS messages are received (per second).
Datagrams Sent:	
Count	Total number of SCS datagrams sent since the port was initialized.
Rate	Rate at which SCS datagrams are sent (per second).
Datagrams Received:	
Count	Total number of SCS datagrams sent since the port was initialized.
Rate	Rate at which SCS datagrams are sent (per second).
Kilobytes Mapped	Number of kilobytes mapped for block transfer.

4.2.2 SCA (System Communications Architecture) Summary Data

Below the heading Circuits in Figure 4–4 is a line of SCA summary headings that include information about a node's SCS circuits between local SCA ports and remote SCA ports on other nodes in the cluster. More than one circuit indicates more than one communications path to the other node.

The data displayed in Figure 4–4 is similar to the information that the Show Cluster utility (SHOW CLUSTER) displays for the CIRCUITS, CONNECTIONS, and COUNTERS classes and that the SCACP utility's SHOW CIRCUITS command displays. Note that circuit count is the total number of events since the the state of the circuit changed to OPEN.

Starting with Availability Manager Version 2.2, the circuits display shows circuits to non-OpenVMS nodes, such as storage controllers.

Figure 4–4 SCA Summary Data

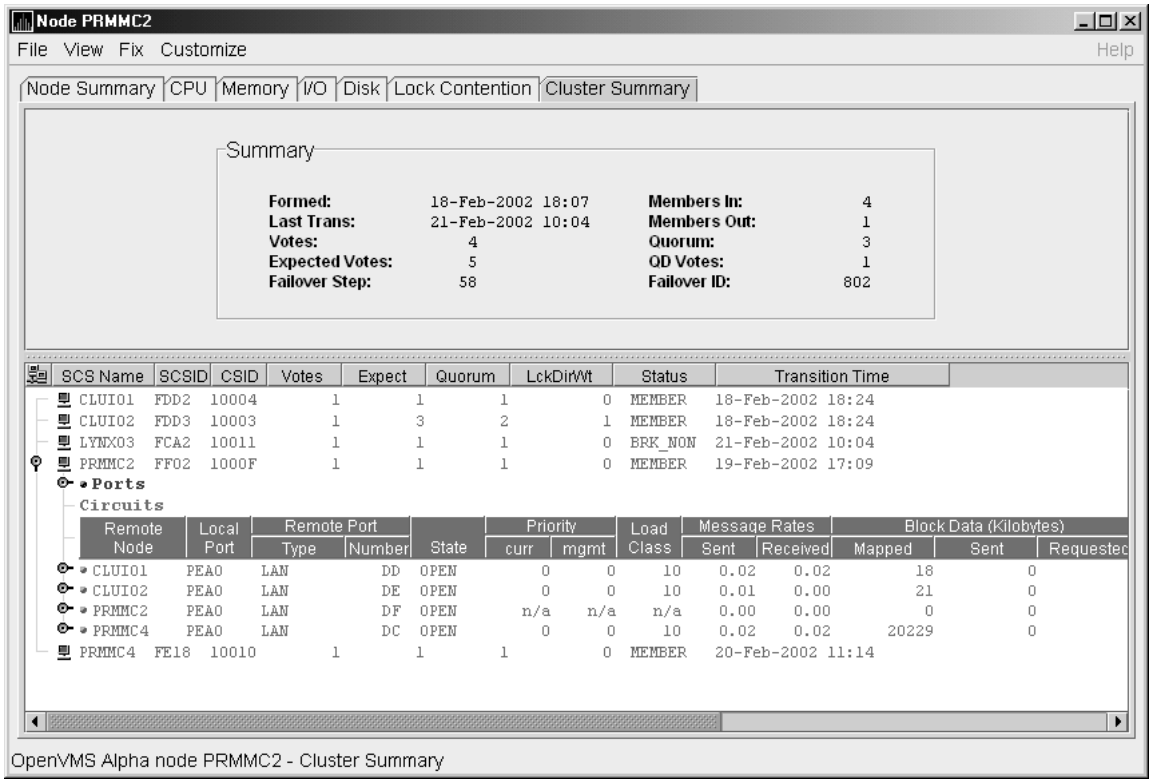


Table 4–4 describes the SCA summary data displayed in Figure 4–4. Each line of data shows either a summary of an SCS connection between a local system connection of an application (or SYSAP) to a remote SYSAP that uses the circuit, or a summary of interconnect-specific information about the operation of the circuit.

Some of the data described in Table 4–4 is not displayed in Figure 4–4 because the screen display is wider than the page. You can scroll to the right on your terminal screen to display the remaining fields described in the table.

Note

Each rate referred to in Figure 4–4 is in messages per second. The "Message Rates" data are rates; the remaining data items are counts.

Table 4–4 SCA Summary Data

Data	Description
Remote Node	SCS name of the remote node containing the remote port of the circuit.
Local Port	The device name of the local port associated with the circuit.

(continued on next page)

Table 4–4 (Cont.) SCA Summary Data

Remote Port:		
	Type	The remote port's device or interconnect type associated with the circuit (for example, LAN, CIPCA, DSSI).
	Number	The remote port's interconnect address, or another other interconnect-specific unique identifier.
State		The state of the virtual circuit connection.
Priority:		
	Curr	Circuit's current priority, which is the sum of the management priorities assigned to the circuit and associated local port.
	Mgmt	Priority value assigned to the circuit by management action.
Load Class		The circuit's current capacity rating, derived from the current ECS member's load class values.
Message Rates:		
	Sent	Count/rate of SCS messages sent over the circuit.
	Received	Count/rate that SCS messages are received on the circuit.
Block Data (Kilobytes):		
	Mapped	Count/rate of kilobytes mapped for block data transfers over the circuit.
	Sent	Count/rate of kilobytes sent over the circuit using transfers.
	Requested	Count/rate of kilobytes requested from the remote port over the circuit using request block data transfers.
Block Data (Count):		
	Sent	Count/rate of send block data transfers over the circuit.
	Requested	Count/rate of block data transfer requests sent over the circuit.
Datagrams:		
	Sent	Count/rate of SCS datagrams sent over the circuit.
	Received	Count/rate of SCS datagrams received on the circuit.
Credit Wait		Count/rate any connection on the circuit had to wait for a send credit.
Buff Desc Wait		Count/rate any connection over the circuit had to wait for a buffer descriptor.

4.2.3 SCS (System Communications Services) Connections Summary Data

You can click the handle at the beginning of a Virtual Circuit Data (green) row to display the following headings, when they apply to a particular node:

- SCS Connections
- LAN Virtual Circuit Summary

To display SCS connections summary data, click the handle at the beginning of the SCS Connections data row on the Cluster Summary pane shown in Figure 4–1. Figure 4–5 displays SCS Connections Data information.

Figure 4–5 SCS Connections Data

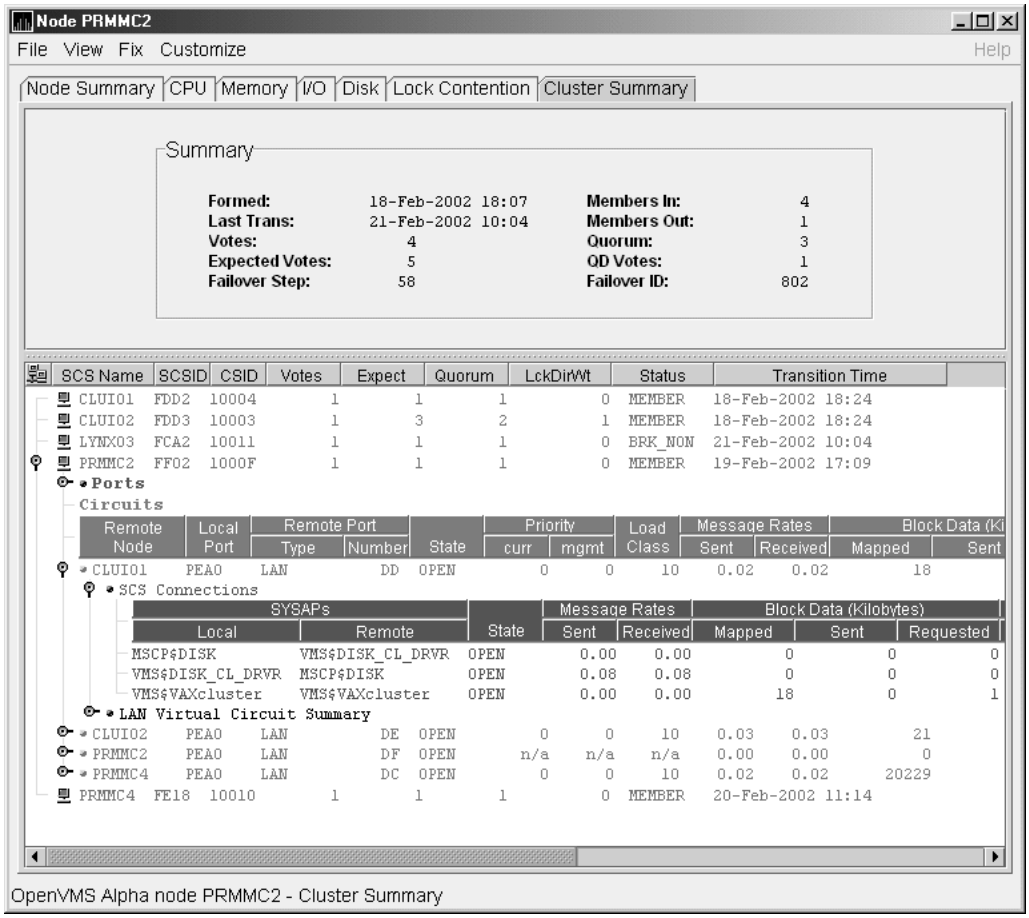


Table 4–5 describes the SCS connections data shown in Figure 4–5. Some of the data described in Table 4–5 is not displayed in Figure 4–5 because the screen display is wider than the page. You can scroll to the right on your terminal screen to display the remaining fields described in the table.

Note that connection count is the total number of events since the state of the connection changed to OPEN.

Table 4–5 SCS Connections Data

Data	Description
SYSAPs:	
Local	Name of the SYSAP (system application) on the local system associated with the connection.
Remote	Name of the SYSAP on the remote system associated with the connection.

(continued on next page)

Table 4–5 (Cont.) SCS Connections Data

Data	Description
State	The connection's current state. The possible displays are: • ACCP_SENT—An accept request has been sent. • CLOSED—The connection is closed. • CON_ACK—A connect request has been sent and acknowledged. • CON_REC— A connect request has been received. • CON_SENT— A connect request has been sent. • DISC_ACK—A disconnect is acknowledged. • DISC_MTCH—A disconnect request has matched. • DISC_REC— A disconnect request has been received. • DISC_SENT—A disconnect request has been sent. • LISTEN— The connection is in the listen state. • OPEN—The connection is open. • REJ_SENT— A rejection has been sent. • VC_FAI—The virtual circuit has failed.
Message Rates:	
Sent	Count/rate that SCS messages are sent over the connection.
Received	Count/rate that SCS messages are being received on the connection.
Block Data (Kilobytes):	
Mapped	Count/rate of kilobytes mapped for block data transfers by the local SYSAP using the connection. Note: This field is available only in raw data format.
Sent	Number of kilobytes sent over the SCS connection by the local SYSAP using send block data transfers.
Requested	Number of kilobytes requested over the SCS connection by the local SYSAP using request block data transfers.
Block Data (Number):	
Sent	Count/Rate of send block data transfers by this node over the SCS connection.
Requested	Count/Rate of request block data transfers sent to the remote port over the SCS connection.
Datagrams:	
Sent	Count/Rate of datagrams sent on the SCS connection.
Received	Count/Rate of datagrams received on the SCS connection.
Credit Wait	Count/Rate of times the connection had to wait for a send credit.

(continued on next page)

Table 4–5 (Cont.) SCS Connections Data

Data	Description
Buff Desc Wait	Count/Rate of times the connection had to wait for a buffer descriptor.

4.2.4 LAN Virtual Circuit Summary Data

You can display interconnect-specific virtual circuit summary data by clicking the handle at the beginning of a Virtual Circuit Summary (black) data row. The screen expands to display the interconnect-specific VC summary data shown in Figure 4–6.

Much of the data in this display corresponds to the information displayed by the SCACP command SHOW VC. The SHOW CLUSTER command does not provide a corresponding display. Which data items are displayed depends on the type of interconnect the virtual circuit is using. Currently, this feature is available only for LAN virtual circuits. VC Summary displays for other cluster interconnects such as CI might be available in the future. When other interconnects are supported, the interconnect type will be displayed at the beginning of the line—for example, CI Virtual Circuit Summary—and the associated heading will have interconnect-specific data items.

Note that LAN Virtual Circuit counters are initialized when PEDRIVER detects the existence of a PEDRIVER on a remote system. All of a LAN VC's counters are cumulative from that time.

Some of the data described in Table 4–6 is not displayed in Figure 4–6 because the screen display is wider than the page. You can scroll to the right on your terminal screen to display the remaining fields described in the table.

Figure 4–6 LAN Virtual Circuit Summary Data

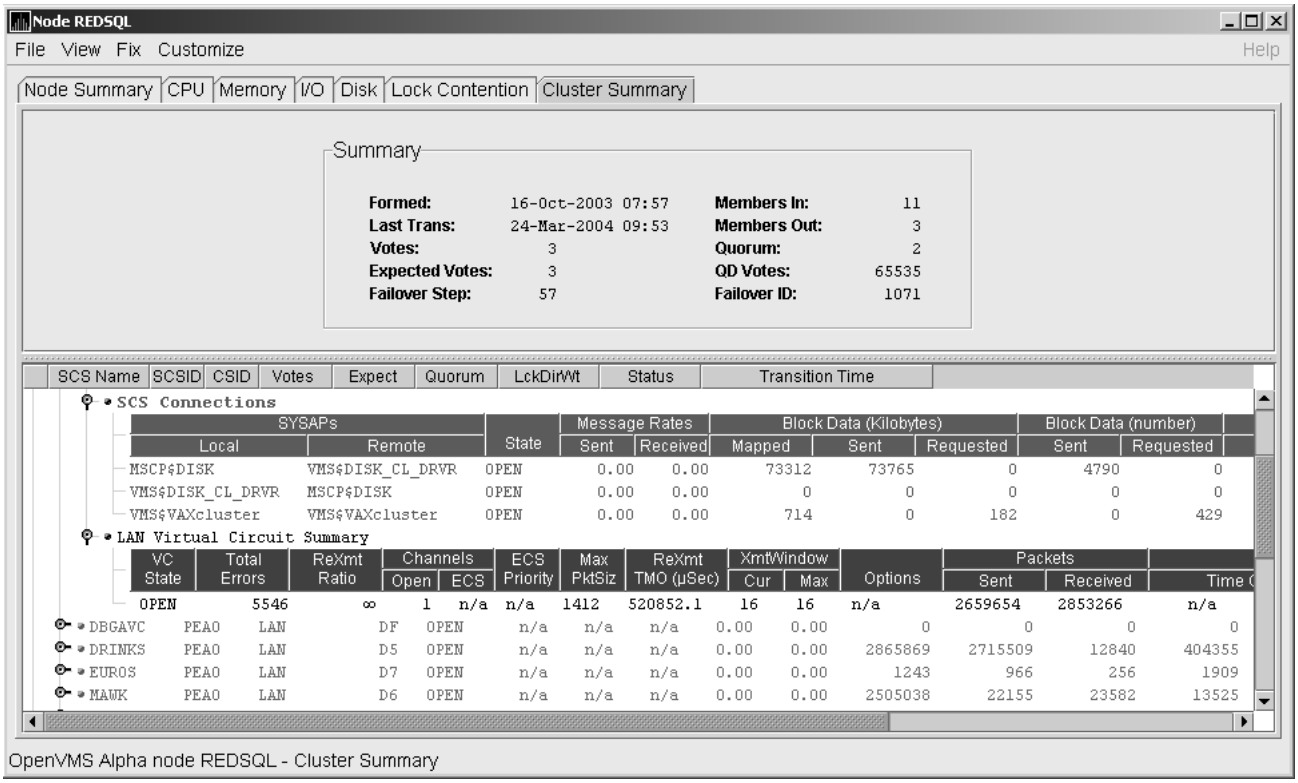


Table 4–6 describes the LAN virtual circuit summary data shown in Figure 4–6.

Table 4–6 LAN Virtual Circuit Summary Data

Data	Description
VC State	Current internal state of the virtual circuit: • OPEN—Virtual Circuit is open and usable. • PATH—At least one open channel has been established, but the Virtual Circuit has not yet transitioned to OPEN. • CLOSED—The Virtual Circuit has been closed or has become unusable.
Total Errors	Number of times the virtual circuit has been closed or has had other errors.
ReXmt Ratio	Ratio of total numbers of transmitted to retransmitted packets during the most recent data collection interval.
Channels:	
Open	Number of currently open channels available to the virtual circuit.
ECS	Number of equivalent channel set (ECS) channels currently in use by the LAN virtual circuit.

(continued on next page)

Table 4–6 (Cont.) LAN Virtual Circuit Summary Data

Data	Description
ECS Priority	Priority a channel must have in order to be included in the Equivalent channel set (ECS). It is the highest priority any open and tight channel has.
MaxPktSiz	Maximum data buffer size in use by this LAN virtual circuit.
ReXmt TMO (µsec)	Retransmission timeout, in microseconds. The length of time the virtual circuit is currently using to wait for an acknowledgment of the receipt of a packet before retransmitting that packet.
XmtWindow:	
Cur	Current value of the transmit window (or pipe quota). Maximum number of packets that are sent before stopping to await an acknowledgment. After a timeout, the transmit window is reset to 1 to decrease congestion; it is allowed to increase as acknowledgments are received.
Max	Maximum transmit window size currently allowed for the virtual circuit.
Options	Virtual circuit options enabled: CKSUM—packet checksumming CMPR—compression
Packets:	
Sent	Number of packets sent over this virtual circuit.
Received	Number of packets received over this virtual circuit.
Most recent:	
Time Opened	Most recent time the virtual circuit was opened.
Time Closed	Most recent time the virtual circuit was closed.

4.2.5 LAN Channel Summary Data

A LAN path or **channel** is a logical communication path between two LAN devices. Channels between nodes are determined by a local device, a remote device, and the connecting network. For example, two nodes, each having two devices, might establish four channels between the nodes. The packets that a particular LAN virtual circuit carries can be sent over any open channel connecting the two nodes.

The difference between channels and virtual circuits is that channels provide datagram service. **Virtual circuits**, layered on channels, provide error-free paths between nodes. Multiple channels can exist between nodes in an OpenVMS Cluster system, but only one LAN-based virtual circuit can exist between any two nodes at a time.

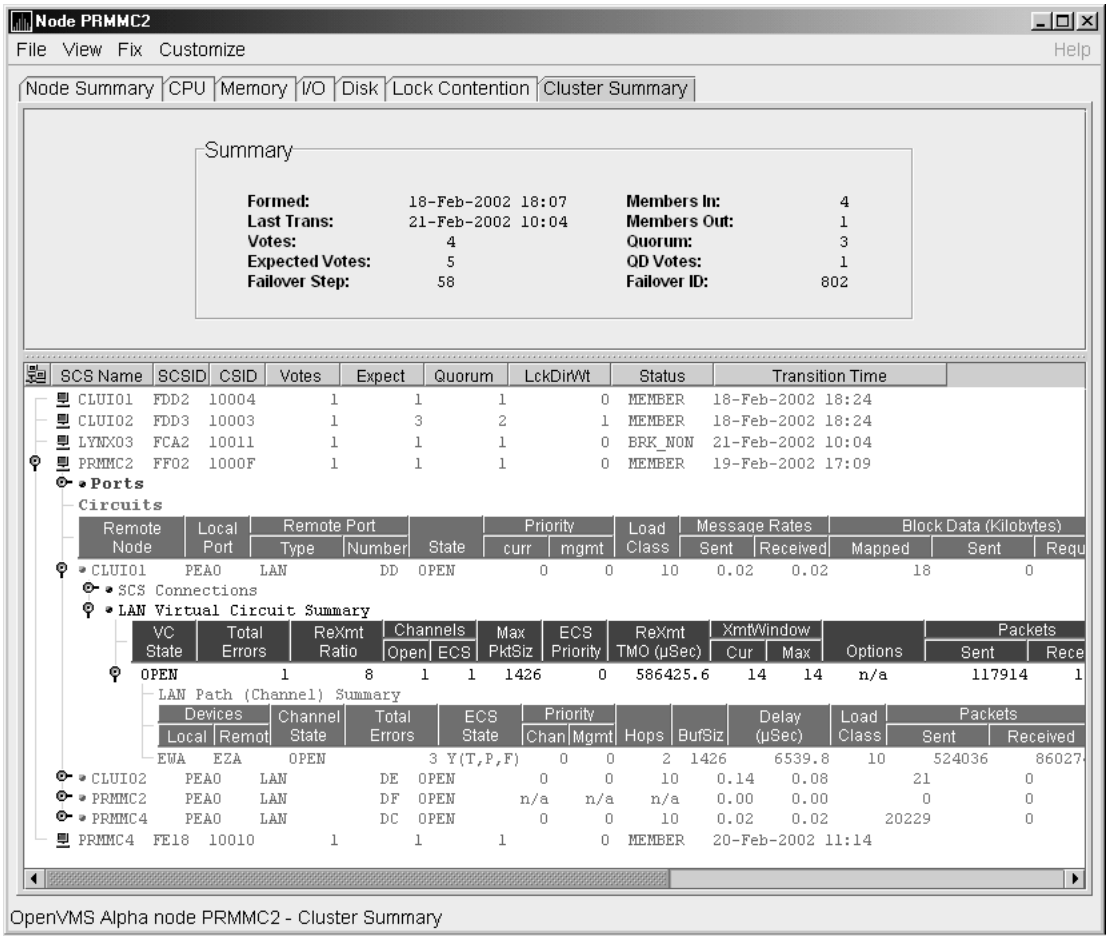
LAN channel **counters** are initialized when PEdriver detects the existence of a LAN device on a remote system. All of a LAN channel counters are cumulative from that time. For more information about channels and virtual circuits, see the *HP OpenVMS Cluster Systems* manual.

Displaying Data

You can display LAN channel summary data by clicking the handle in front of the data item OPEN, PATH, or CLOSED under "VC State" for LAN virtual circuit summary data (see Figure 4–6), or by right-clicking a data item and choosing the Channel Summary item from the popup menu. The screen expands to display the LAN channel summary data shown in Figure 4–7.

The data items displayed depend on the type of virtual circuit. Currently, this feature is available only for LAN virtual circuits.

Figure 4–7 LAN Channel Summary Data



Some of the data described in Table 4–7 is not displayed in Figure 4–7 because the screen display is wider than the page. You can scroll to the right on your terminal screen to display the remaining fields described in the table.

Table 4–7 LAN Channel Data

Data	Description
Devices:	
Local	Local LAN device associated with the channel.
Remote	Remote LAN device associated with the channel.
Channel State	One of the following states: • OPEN—Channel is usable. • PATH—Channel handshake has been completed and, if usable, will transition to OPEN. • CLOSED—Channel has been shut down or is unusable.
Total Errors	Total of various error counters for this channel (see channel details for breakdown).
ECS State	Channel ECS membership information: • Y—Member • N—Nonmember Losses—one of the following: • T (tight)—Packet loss history is acceptable. • L (lossy)—Recent history of packet losses makes channel unusable. Capacity—one of the following: • P (peer)—Priority and Buffer size both match the highest corresponding values of the set of tight channels, entitling the channel to be an ECS member. • I (inferior)—Priority or buffer size does not match the corresponding values of the set of tight channels. • S (superior)—Priority or buffer size is better than those of the current corresponding values of the set ECS member channels. This is a short-lived, transient state because it exists only while the ECS membership criteria are being re-evaluated. • U (unevaluated)—Priority or buffer size, or both, have not been evaluated against the ECS criteria, usually because the channel is lossy. Speed—one of the following: • F (fast)—Channel delay is among the best for tight and peer channels. • S (slow)—Channel delay makes channel too slow to be usable because it would limit the virtual circuit's average delay. **Note:** If a channel is lossy, its capacity and speed are not always kept current. Therefore, displayed values might be those that the channel had at the time it become lossy.

(continued on next page)

Table 4–7 (Cont.) LAN Channel Data

Data	Description
Priority:	
Cur	Current priority used to evaluate the channel for ECS membership. This is the sum of management priority values assigned to the LAN device.
Mgmt	Dynamic management-assigned priority.
Hops	Number of switches or bridges in this channel's network path to the remote LAN device.
BufSiz	Current maximum amount of SCS data that can be contained in a packet sent over the channel. It is the smallest of the following values: • Local LAN device buffer sizes • Remote LAN device buffer sizes • Local NISCS_MAX_PKTSZ system (SYSGEN) parameter values • Remote NISCS_MAX_PKTSZ system (SYSGEN) parameter values • Largest packet size determined by the NISCA Channel Packet Size probing algorithm that the intervening network can deliver
Delay (µsec)	Running average of measured round-trip time, in microseconds, for packets sent over the channel.
Load Class	Load class initialized from local and remote LAN device bit rates.
Packets:	
Sent	Number of packets sent on this channel, including control packets.
Received	Number of packets received by this channel.
Most recent:	
Time Opened	Last time this channel had a verified usable path to a remote system.
Time Closed	Time that this channel was last closed.

4.3 Detailed Data in the Cluster Members Pane

The following sections describe detailed data that appears on lines that you can open in the Cluster Members Pane shown in Figure 4–1.

4.3.1 LAN Device Data

You can display device data by first right-clicking a node name on the Cluster Members pane shown in Figure 4–1. On Version 7.3 or later nodes on which managed objects are enabled, the Availability Manager displays a menu with the following choices:

- SCA Summary
- LAN Device Summary
- Fix *node-name*

Click LAN Device Summary... to display the Device Summary Data page shown in Figure 4–8.

Figure 4–8 LAN Device Summary Data

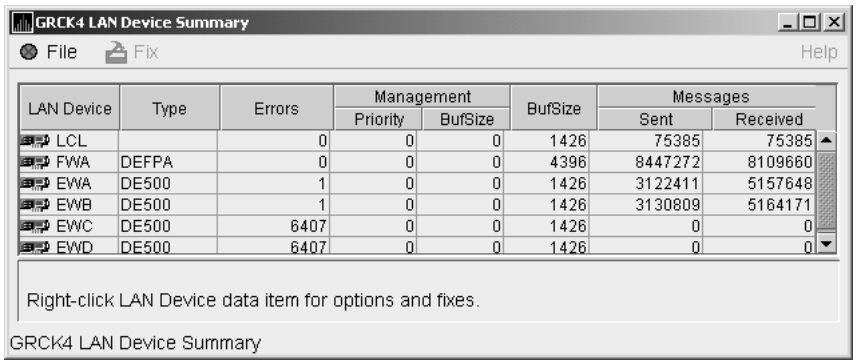


Table 4–8 describes the LAN device summary data displayed in Figure 4–8. This data is also displayed with SCACP command SHOW LAN_DEVICE.

Table 4–8 LAN Device Summary Data

Data	Description
LAN Device	Name of the LAN device used for cluster communications between local and remote nodes.
Type	Type of LAN device used for the cluster.
Errors	Number of errors reported by the device since cluster communications began using it.
Management:	
Priority	Current management-assigned priority of the device.
BufSize	Current management-assigned maximum buffer size of the device
BufSize	Smaller of interconnect specific buffer size of the device and its current management-assigned buffer size.
Messages:	
Sent	Number of LAN packets sent by the device.
Received	Number of packets received from remote LAN device.

4.3.2 LAN Virtual Circuit Details Data

The Network Interconnect for System Communications Architecture (NISCA) is the transport protocol responsible for carrying packets such as disk I/Os and lock packets across Ethernet and FDDI LANs to other nodes in the cluster.

The LAN virtual circuit details (NISCA) pages show detailed information about the LAN Ethernet or FDDI connection between two nodes. The Availability Manager displays one window for each LAN virtual circuit. This page is intended primarily to provide real-time aids for diagnosing LAN-related cluster communications problems. *HP OpenVMS Cluster Systems* describes the parameters shown on these pages and tells how to diagnose LAN-related cluster problems.

The LAN Virtual Circuit Details pages provide the same information as the SCACP command SHOW VC and as the following OpenVMS System Dump Analyzer (SDA) commands: PE VC and SHOW PORTS/VC=VC_ *remote-node-name*. In these commands, *remote-node-name* is the SCS name of another node in the cluster.

SDA defines VC_*remote-node-name* and performs the first SHOW PORTS action after SDA is started. Thus, the /CH and /VC options are valid only with the second and subsequent SHOW PORT commands.

You can display LAN virtual circuit details data by double-clicking OPEN or CLOSED under "VC State" for LAN Virtual Circuit Summary on the Cluster Summary page (see Figure 4–7). After a brief delay, a LAN VC Transmit Data page (shown in Figure 4–9) is displayed. The tabs at the top of the page indicate additional pages that you can display.

The data items displayed depend on the type of virtual circuit. Currently, this feature is available only for LAN virtual circuits.

4.3.2.1 LAN VC Transmit Data

Transmit data is information about data packet transmission. Figure 4–9 is an example of a LAN VC Transmit Data page.

Figure 4–9 LAN VC Transmit Data Page

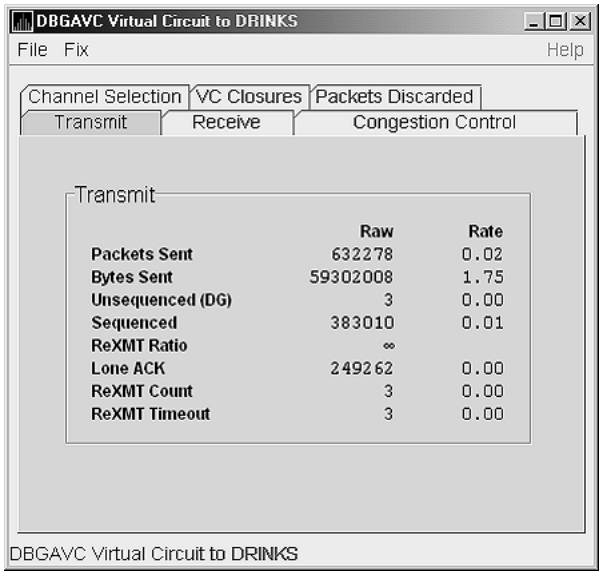


Table 4–9 describes the data displayed in Figure 4–9.

Table 4–9 LAN VC Transmit Data

Data	Description
Packets Sent	(Raw) count and rate of packets transmitted through the virtual circuit to the remote node, including both sequenced and unsequenced (channel control) packets and lone acknowledgments.
Bytes Sent	(Raw) count and rate of bytes transmitted through the virtual circuit.
Unsequenced (DG)	(Raw) count and rate of the number of unsequenced packets that are transmitted.

(continued on next page)

Table 4–9 (Cont.) LAN VC Transmit Data

Data	Description
Sequenced	(Raw) count and rate of sequenced packets transmitted. Sequenced packets are guaranteed to be delivered.
ReXMT Ratio	Ratio of the total number of sequenced packets sent to the current retransmission count.
Lone ACK	(Raw) count and rate of packets sent solely for the purpose of acknowledging receipt of one or more packets.
ReXMT Count	Number of packets retransmitted. Retransmission occurs when the local node does not receive an acknowledgment for a transmitted packet within a predetermined timeout interval.
ReXMT Timeout	Number of retransmission timeouts that have occurred.

4.3.2.2 LAN VC Receive Data

Receive data is information about the receipt of data packets. Figure 4–10 is an example of a LAN VC Receive Data page.

Figure 4–10 LAN VC Receive Data Page

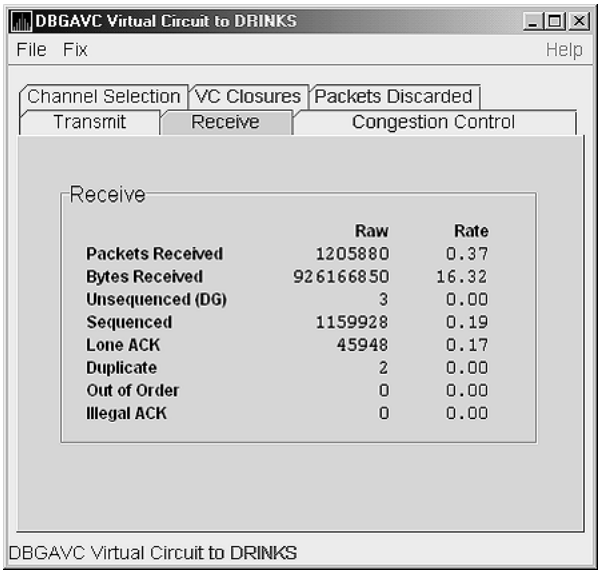


Table 4–10 describes the data displayed in Figure 4–10.

Table 4–10 LAN VC Receive Data

Data	Description
Packets Received	(Raw) count and rate of packets received on the virtual circuit from the remote node, including both sequenced and unsequenced—that is, datagram packets and lone acknowledgments.
Bytes Received	(Raw) count and rate of bytes received in packets over the virtual circuit.

(continued on next page)

Table 4–10 (Cont.) LAN VC Receive Data

Data	Description
Unsequenced (DG)	(Raw) count and rate of unsequenced—datagram—packets received.
Sequenced	(Raw) count and rate of sequenced packets received.
Lone ACK	(Raw) count and rate of lone acknowledgments received.
Duplicate	Number of duplicated packets received by this system. Duplicates occur when the sending node retransmits a packet, and both the original and the retransmitted packets are received.
Out of Order	Number of packets received out of order by this system.
Illegal ACK	Number of illegal acknowledgments received—that is, acknowledgments of an out-of-range sequence number.

4.3.2.3 LAN VC Congestion Control Data

LAN VC congestion control data is information about LAN traffic. The values indicate the number of packets that can be sent to the remote node before receiving an acknowledgment and the retransmission timeout.

Figure 4–11 is an example of a LAN VC Congestion Control Data page.

Figure 4–11 LAN VC Congestion Control Data Page

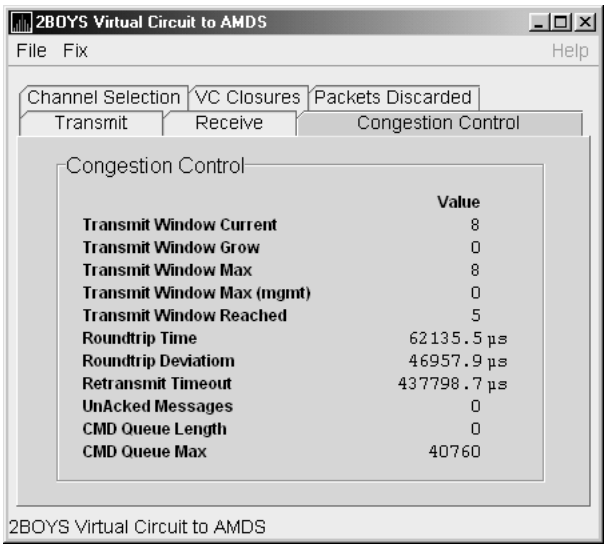


Table 4–11 describes the data displayed in Figure 4–11.

Table 4–11 LAN VC Congestion Control Data

Data	Description
Transmit Window Current	Current value of the transmit window (or pipe quota). After a timeout, the pipe quota is reset to 1 to decrease network path congestion. The pipe quota is allowed to increase as quickly as acknowledgments are received.

(continued on next page)

Table 4–11 (Cont.) LAN VC Congestion Control Data

Data	Description
Transmit Window Grow	The slow growth threshold. The size at which the increase rate of the window is slowed to avoid congestion on the network again.
Transmit Window Max	Maximum transmit window size currently allowed for the virtual circuit based on channel and remote PEdriver receive cache limitations.
Transmit Window Max (mgmt)	Management override to calculated value for Maximum Transmit Window size. N/A on systems prior to Version 2.0.
Transmit Window Reached	Number of times the entire transmit window was full. If this number is small compared with the number of sequenced packets transmitted, then either the local node is not sending large bursts of data to the remote node, or acknowledging packets are being received so promptly that the window limit is never reached.
Roundtrip Time	Average round-trip time, in microseconds, for a packet to be sent and acknowledged.
Roundtrip Deviation	Average deviation, in microseconds, of the round-trip time.
Retransmit Timeout	Value, in microseconds, used to determine packet retransmission timeout. If a packet does not receive either an acknowledging or a responding packet, the packet is assumed to be lost and will be resent.
UnAcked Packets	Current number of unacknowledged packets.
CMD Queue Length	Current length of the virtual circuit's command queue.
CMD Queue Max	Maximum number of commands in the virtual circuit's command queue so far.

4.3.2.4 LAN VC Channel Selection Data (Pre-Version 2.0)

Systems running versions prior to Version 2.0 Availability Manager software collect and display information about LAN VC channel selection, but this information does not include managed objects, which were implemented beginning with Version 2.0 (See the introduction to this chapter for more information about managed objects.)

Figure 4–12 is an example of a pre-Version 2.0 LAN VC Channel Selection Data page.

Figure 4–12 LAN VC Channel Selection Data Page (Pre-Version 2.0)

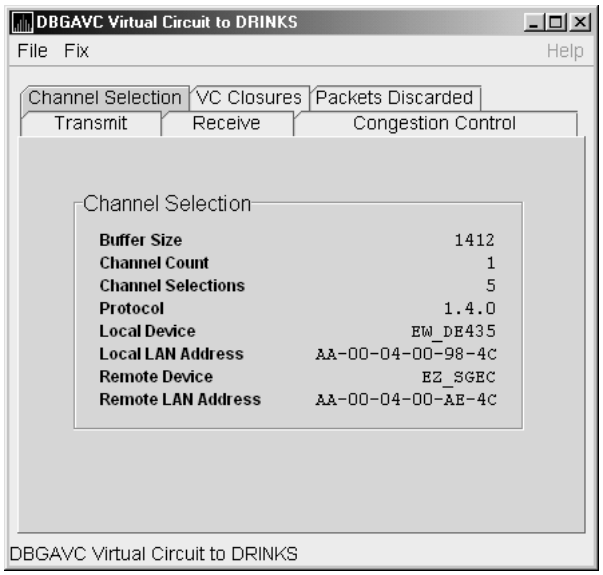


Table 4–12 describes the data displayed in Figure 4–12.

Table 4–12 LAN VC Channel Selection Data (Pre-Version 2.0)

Data	Description
Buffer Size	Maximum data buffer size for this virtual circuit.
Channel Count	Number of channels available for use by this virtual circuit.
Channel Selections	Number of channel selections performed.
Protocol	NISCA protocol version.
Local Device	Name of the local LAN device that the channel uses to send and receive packets.
Local LAN Address	Address of the local LAN device that performs sends and receives.
Remote Device	Name of the remote LAN device that the channel uses to send and receive packets.
Remote LAN Address	Address of the remote LAN device performing the sends and receives.

4.3.2.5 LAN VC Channel Selection Data (Version 2.0 and Later)

Systems running Availability Manager Version 2.0 or later collect and display the following information about LAN VC Channel Selection. This information includes managed objects, which were implemented beginning with Version 2.0 (See the introduction to this chapter for more information about managed objects.)

Note

An additional requirement for displaying this data page is that managed objects be enabled on your system. See the postinstallation tasks described in the Installation Guide for OpenVMS Systems.

Figure 4–13 is an example of a Channel Selection Data page on a Version 2.0 or later system.

Figure 4–13 LAN VC Channel Selection Data Page (Version 2.0 and Later)

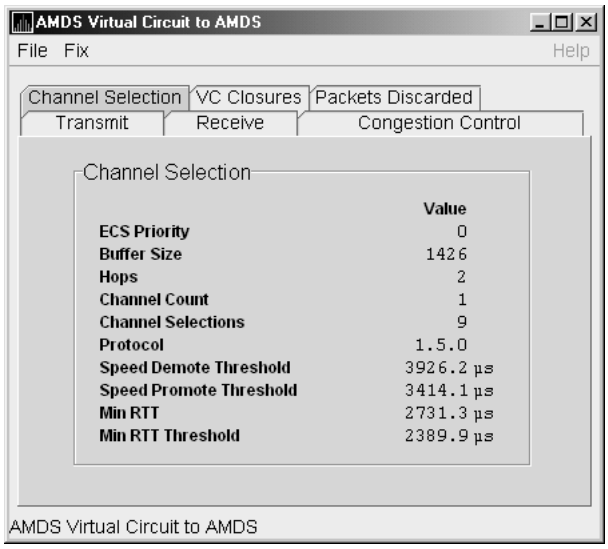


Table 4–13 describes the data displayed in Figure 4–13.

Table 4–13 Channel Selection Data (Version 2.0 and Later)

Data	Description
ECS Priority	Current minimum priority a tight channel must have in order to be an ECS member.
Buffer Size	Maximum data buffer size for this virtual circuit. A channel must have this buffer size in order to be an ECS member.
Hops	Current minimum management hops a channel must have in order to be included in the ECS.
Channel Count	Number of channels currently available for use by this virtual circuit.
Channel Selections	Number of channel selections performed.
Protocol	Remote node's NISCA protocol version.
Speed Demote Threshold	Current threshold for reclassifying a FAST channel to SLOW.
Speed Promote Threshold	Current threshold for reclassifying a SLOW channel to FAST.
Min RTT	Current minimum average delay of any current ECS members.
Min RTT Threshold	Current threshold for reclassifying a channel as FASTER than the current set of ECS channels.

4.3.2.6 LAN VC Closures Data

LAN VC closures data is information about the number of times a virtual circuit has closed for a particular reason. Figure 4–14 is an example of a LAN VC Closures Data page.

Figure 4–14 LAN VC Closures Data Page

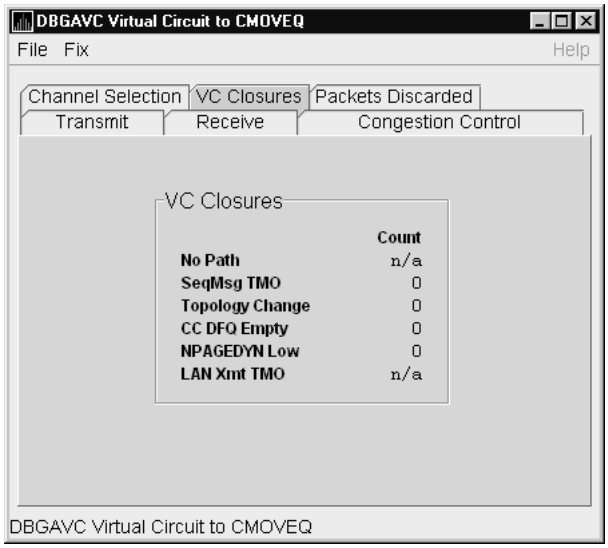


Table 4–14 describes the data displayed in Figure 4–14.

Table 4–14 LAN VC Closures Data

Data	Description
No Path	Number of times the virtual circuit was closed because no usable LAN path was available. N/A on systems prior to Version 2.0.
SeqPkt TMO	Number of times the VC was closed because a sequenced packet's retransmit timeout count limit was exceeded.
Topology Change	Number of times the VC was closed because PEdriver performed a failover from a LAN path (or paths) with a large packet size to a LAN path with a smaller packet size.
CC DFQ Empty	Number of times the VC was closed because the channel control data-free queue (DFQ) was empty.
LAN XmtTMO	Number of times the VC was closed because a sequenced packet was not transmitted by the LAN device within an acceptable amount of time.
NPAGEDYN Low	Number of times the virtual circuit was lost because of a nonpaged pool allocation failure in the local node.

4.3.2.7 LAN VC Packets Discarded Data

LAN VC packets discarded data is information about the number of times packets were discarded for a particular reason. Figure 4–15 is an example of a LAN VC Packets Discarded Data page.

Figure 4–15 LAN VC Packets Discarded Data Page

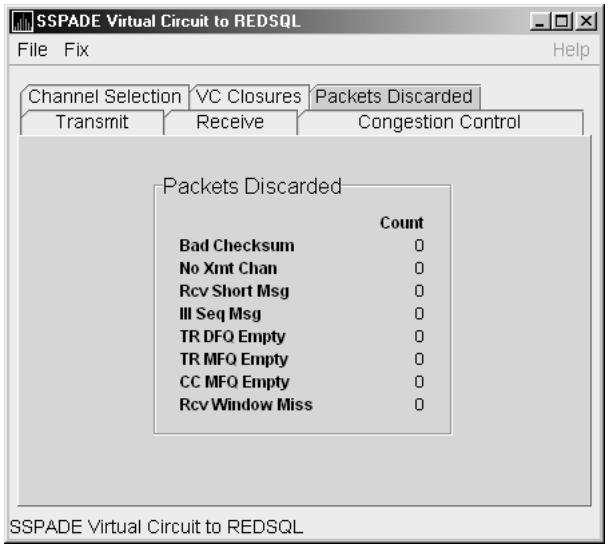


Table 4–15 describes the data displayed in Figure 4–15.

Table 4–15 LAN VC Packets Discarded Data

Data	Description
Bad Checksum	Number of times there was a checksum failure on a received packet.
No Xmt Chan	Number of times no transmit channel was available.
Rcv Short Pkt	Number of times an undersized transport packet was received.
Ill Seq Pkt	Number of times an out-of-range sequence numbered packet was received.
TR DFQ Empty	Number of times the transmit data-free queue (DFQ) was empty.
TR MFQ Empty	Number of times the TR layer message-free queue (MFQ) was empty.
CC MFQ Empty	Number of times the channel control MFQ was empty.
Rcv Window Miss	Number of packets that could not be placed in the virtual circuit's receive cache because the cache was full.

4.3.3 LAN Channel Details Data

To display LAN channel details data, right-click a LAN channel summary data item on the Cluster Summary page (Figure 4–7). The Availability Manager displays a popup menu with the following options:

- Channel Details...
- LAN Device Details...
- Fixes...

To display LAN channel details, select the Channel Details... item on the menu. After a brief delay, a LAN Channel Overview Data Page, shown in Figure 4–16, is displayed. A series of tabs at the top of the Overview Data Page indicate additional channel pages you can display.

4.3.3.1 LAN Channel Overview Data Page

The LAN Channel Overview Data page, shown in Figure 4–16, displays general channel data.

Figure 4–16 LAN Channel Overview Data Page

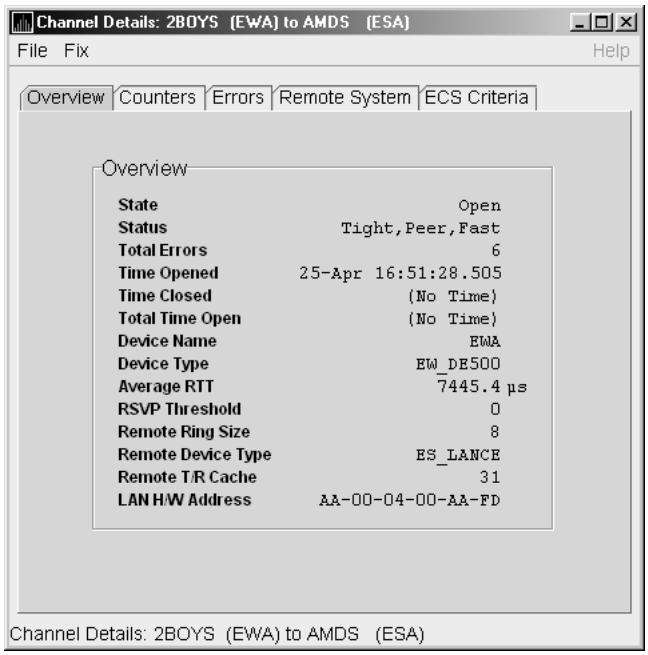


Table 4–16 describes the data displayed in Figure 4–16.

Table 4–16 LAN Channel Overview Data

Data	Description
State	Channel's current state: OPEN, PATH, or CLOSED.
Status	Channel status.
Total Errors	Sum of channel's error counters.
Time Opened	Last time that this channel had a path to a remote system.
Time Closed	Last time that this channel was closed.
Total Time Open	Total time that this channel has been open.
Device Name	Local LAN device name.
Device Type	Local LAN device type.
Average RTT	Average of measured round-trip time.
RSVP Threshold	Number of packets before requesting that the remote node immediately return an acknowledgment.
Remote Ring Size	Number of entries in the remote LAN device.
Remote Device Type	Remote LAN device type.
Remote T/R Cache	Number of out-of-order packets that the remote transmit/receive resequencing cache can buffer.

(continued on next page)

Table 4–16 (Cont.) LAN Channel Overview Data

Data	Description
LAN H/W Address	LAN device's hardware address.

4.3.3.2 LAN Channel Counters Data Page

The LAN Channel Counters Data page, shown in Figure 4–17, displays path counters data.

Figure 4–17 LAN Channel Counters Data Page

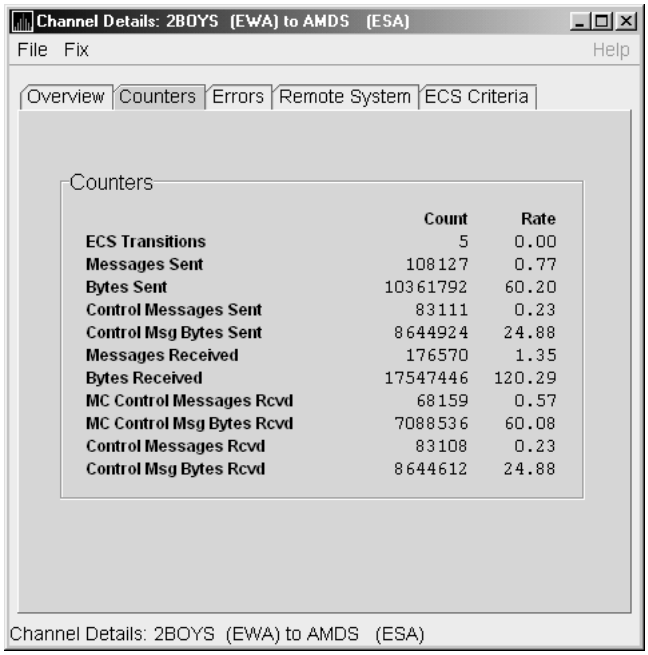


Table 4–17 describes the data displayed in Figure 4–17.

Table 4–17 LAN Channel Counters Data

Data	Description
ECS Transitions	Number of times this channel has been in and out of the equivalent channel set (ECS).
Messages Sent	Number of packets sent over this channel, including control packets.
Bytes Sent	Number of bytes transmitted on this channel, including control packets.
Control Messages Sent	Number of control packets sent, not including multicast packets.
Control Msg Bytes Sent	Number of control packet bytes sent, not including multicast packets.
Messages Received	Number of packets received by this channel.

(continued on next page)

Table 4–17 (Cont.) LAN Channel Counters Data

Data	Description
Bytes Received	Number of bytes in packets received by this channel.
MC Control Messages Rcvd	Number of multicast control packets received.
MC Control Msg Bytes Rcvd	Number of multicast control packets bytes received.
Control Messages Rcvd	Number of control packets received.
Control Msg Bytes Rcvd	Number of control packet bytes received.

4.3.3.3 LAN Channel Errors Data Page

The LAN Channel Errors Data page, shown in Figure 4–18, displays LAN channel errors data.

Figure 4–18 LAN Channel Errors Data Page

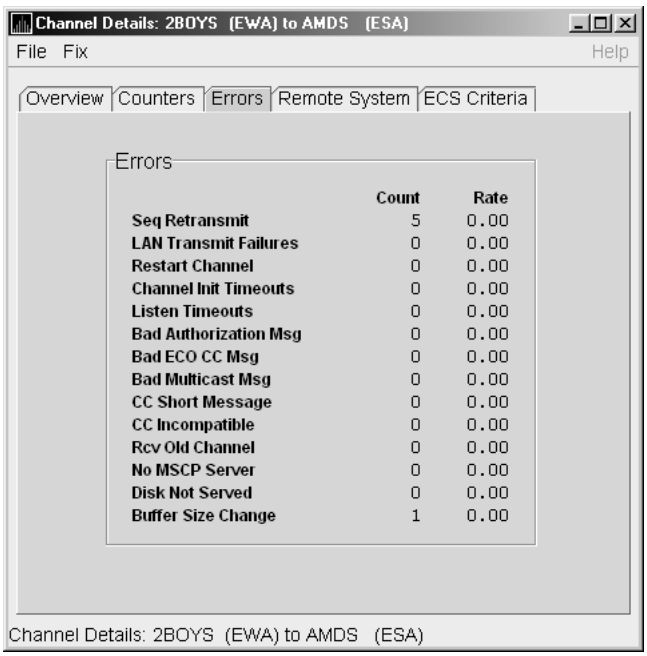


Table 4–18 describes the data displayed in Figure 4–18.

Table 4–18 LAN Channel Errors Data

Data	Description
Seq Retransmit	Number of times a sequenced VC packet sent on this channel was retransmitted, and the channel was penalized for the lost packet.
LAN Transmit Failures	Number of times the local LAN device reported a failure to transmit a packet, and channel was penalized for the lost packet.

(continued on next page)

Table 4–18 (Cont.) LAN Channel Errors Data

Data	Description
Restart Channel	Close/restart because of channel control packet was received indicating the other end closed the channel and is restarting the channel handshake.
Channel Init Timeouts	Channel initialization handshake timeout.
Listen Timeouts	No packets of any kind, including HELLOs, were received in LISTEN_TIMEOUT seconds.
Bad Authorization Msg	Received a CC (channel control) packet with a bad authorization field.
Bad ECO CC Msg	Received a CC packet with an incompatible NISCA protocol ECO rev. field value.
Bad Multicast Msg	Received a bad multicast CC packet.
CC Short Packet	Received a CC packet that was too short.
CC Incompatible	Received a CC packet that was incompatible with existing channels for this virtual circuit.
Rcv Old Channel	Received a packet from an old instance of a channel.
No MSCP Server	No MSCP server available to respond to a received channel control solicit service packet asking this node to boot serve another node.
Disk Not Served	Disk is not served by this system.
Buffer Size Change	Change in buffer size.

4.3.3.4 LAN Channel Remote System Data Page

The LAN Channel Remote System Data page, shown in Figure 4–19, displays LAN path remote system data.

Figure 4–19 LAN Channel Remote System Data Page

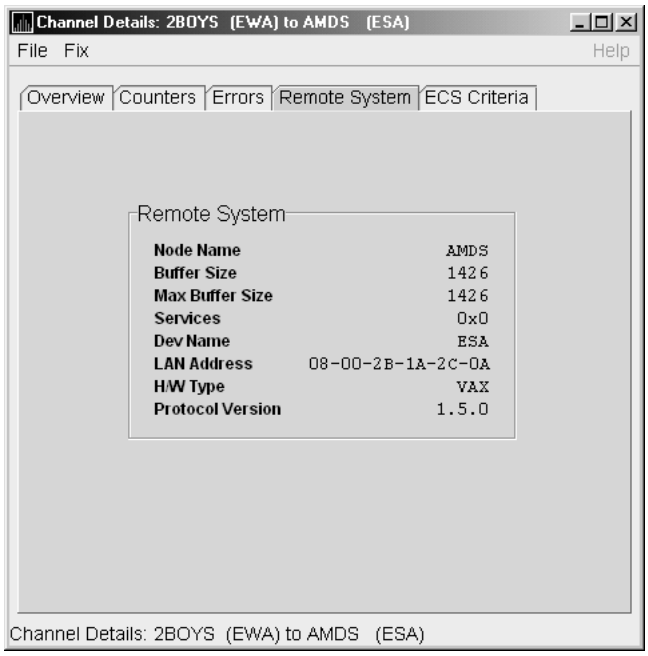


Table 4–19 describes the data displayed in Figure 4–19.

Table 4–19 LAN Channel Remote System Data

Data	Description
Node Name	Node name of remote system.
Buffer Size	Buffer size (largest possible buffer size) of remote system.
Max Buffer Size	Current upper bound on buffer size usable on this channel.
Services	NISCA services supported on this channel.
Dev Name	Name of the remote LAN device.
LAN Address	Remote hardware address.
H/W Type	Hardware type of remote node.
Protocol Version	NISCA protocol version of remote system.

4.3.3.5 LAN Channel ECS (Equivalent Channel Set) Criteria Data Page

The LAN Channel ECS Criteria Data page, shown in Figure 4–20, displays equivalent channel set criteria data.

Figure 4–20 LAN Channel ECS Criteria Data Page

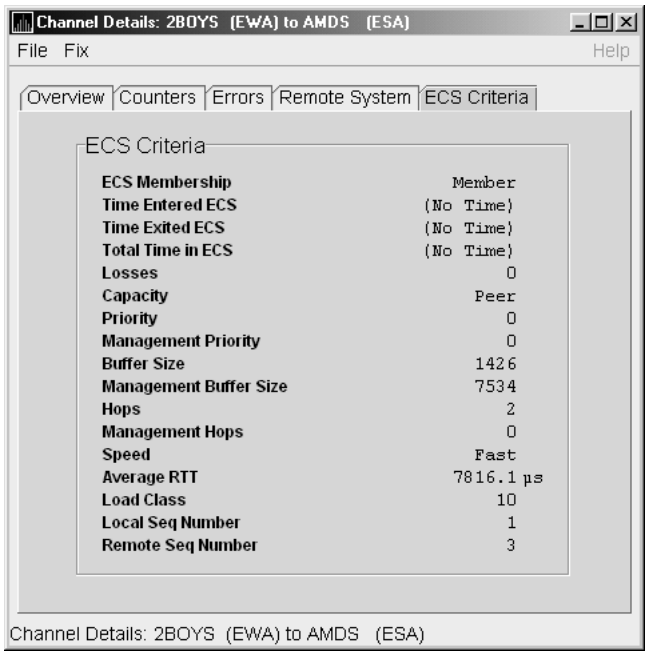


Table 4–20 describes the data displayed in Figure 4–20.

Table 4–20 LAN Channel ECS Criteria Data

Data	Description
ECS Membership	ECS membership status; that is, Member or Nonmember.
Time Entered ECS	Last time this channel entered the ECS.
Time Exited ECS	Last time this channel exited the ECS.
Total Time in ECS	Total time this channel was in the ECS.
Losses	Value representing channel's recent packet loss history.
Capacity	Channel's capacity rating based on evaluating its priority, buffer size, and hops values relative to the current ECS criteria. Values are: Ungraded, Peer, Inferior, Superior.
Priority	Channel's current priority for ECS calculations; it is the sum of the management priorities assigned to the local LAN device and to the channel.
Management Priority	Dynamic management-assigned priority.
Buffer Size	Negotiated maximum common buffer size: the smaller of local and remote BUS$ limits on block data field sizes.
Management Buffer Size	Maximum block data field size assigned by dynamic management.
Hops	Number of switches or bridges for this channel.
Management Hops	Management-supplied hops or media packet storage equivalent.
Speed	Classification of channel's delay relative to that of the lowest delay of any ECS member.

(continued on next page)

Table 4–20 (Cont.) LAN Channel ECS Criteria Data

Data	Description
Average RTT	Average measured round-trip time.
Load Class	Lesser of the local and remote LAN device load class values.
Local Seq Number	Sequence number of the local channel.
Remote Seq Number	Sequence number of the remote channel.

4.3.4 LAN Device Detail Data

To display LAN devices details data, right-click a LAN path (channel) summary data item on the Cluster Summary page (see Figure 4–6). The Availability Manager then displays a popup menu with the following options:

- Channel Details...
- LAN Device Details...
- Fixes...

To display device details, select the LAN Device Details... item on the menu. After a brief delay, a LAN Device Overview Data page (shown in Figure 4–21) is displayed.

A series of tabs at the top of the LAN Device Overview Data page indicate additional LAN device pages that you can display. Much of the LAN device detail data corresponds to data displayed by the SCACP command SHOW LAN_DEVICE.

4.3.4.1 LAN Device Overview Data Page

The LAN Device Overview Data page, shown in Figure 4–21, displays LAN device summary data.

Figure 4–21 LAN Device Overview Data Page

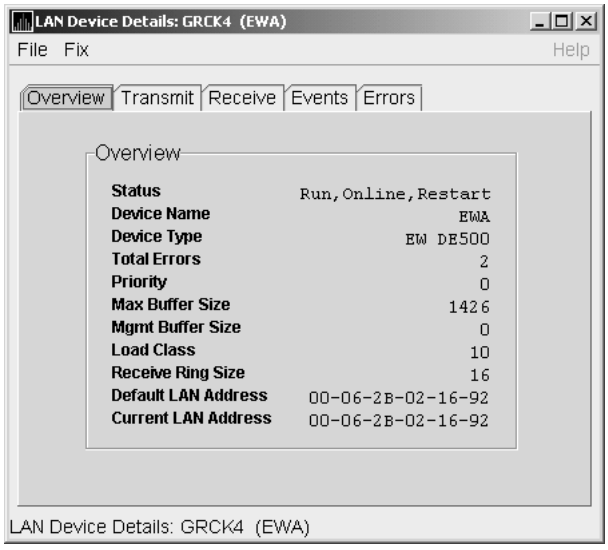


Table 4–21 describes the data displayed in Figure 4–21.

Table 4–21 LAN Device Overview Data

Data	Description
Status	Device status: Run, Online, Restart; or Not in use by SCA.
Device Name	Name of the LAN device.
Device Type	OpenVMS device type value.
Total Errors	Total number of errors listed on the Errors page.
Priority	Dynamic management-assigned priority.
Max Buffer Size	Maximum data buffer size for this LAN device.
Mgmt Buffer Size	Dynamic management-assigned maximum block data field size.
Load Class	Load class. The rate in MBs currently being reported by the LAN device.
Receive Ring Size	Number of packets the LAN device can buffer before it discards incoming packets.
Default LAN Address	LAN device's hardware LAN address.
Current LAN Address	Current LAN address being used by this LAN device.

4.3.4.2 LAN Device Transmit Data Page

The LAN Device Transmit Data page, shown in Figure 4–22, displays LAN device transmit data.

Figure 4–22 LAN Device Transmit Data Page

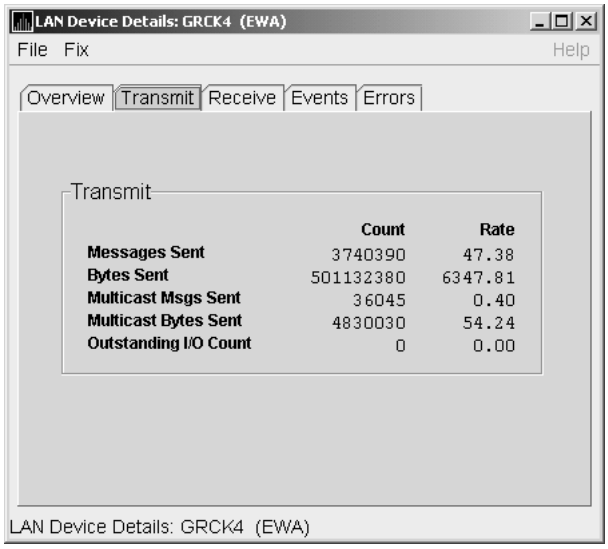


Table 4–22 describes the data displayed in Figure 4–22.

Table 4–22 LAN Device Transmit Data

Data	Description
Messages Sent	Number of packets sent by this bus, including multicast packets.
Bytes Sent	Number of bytes in packets sent by this LAN device, including multicast packets.
Multicast Msgs Sent	Number of multicast packets sent by this LAN device.
Multicast Bytes Sent	Number of multicast bytes in packets sent by this LAN device.
Outstanding I/O Count	Number of transmit requests being processed by LAN driver.

4.3.4.3 LAN Device Receive Data Page

The LAN Device Receive Data page, shown in Figure 4–23, displays LAN device receive data.

Figure 4–23 LAN Device Receive Data Page

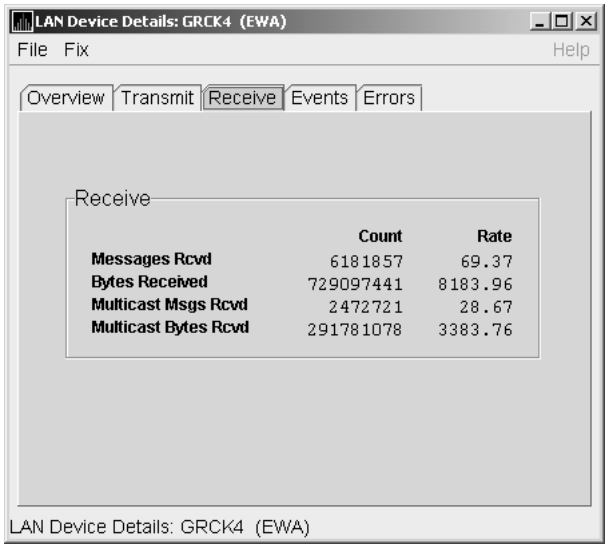


Table 4–23 describes the data displayed in Figure 4–23.

Table 4–23 LAN Device Receive Data

Data	Description
Messages Rcvd	Number of packets received by this LAN device, including multicast packets.
Bytes Received	Number of bytes in packets received by this LAN device, including multicast packets.
Multicast Msgs Rcvd	Number of multicast NISCA packets received by this LAN device.
Multicast Bytes Rcvd	Number of multicast bytes received by this LAN device.

4.3.4.4 LAN Device Events Data Page

The LAN Device Events Data page, shown in Figure 4–24, displays LAN device events data.

Figure 4–24 LAN Device Events Data Page

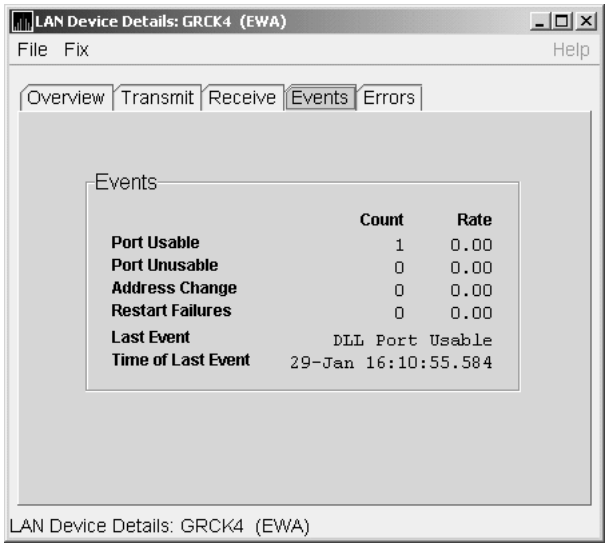


Table 4–24 describes the data displayed in Figure 4–24.

Table 4–24 LAN Device Events Data

Data	Description
Port Usable	Number of times the LAN device became usable.
Port Unusable	Number of times the LAN device became unusable.
Address Change	Number of times the LAN device's LAN address changed.
Restart Failures	Number of times the LAN device failed to restart.
Last Event	Event type of the last LAN device event (for example, LAN address change, an error, and so on).
Time of Last Event	Time the last event occurred.

4.3.4.5 LAN Device Errors Data Page

The LAN Device Errors Data page, shown in Figure 4–25, displays LAN device errors data.

Figure 4–25 LAN Device Errors Data Page

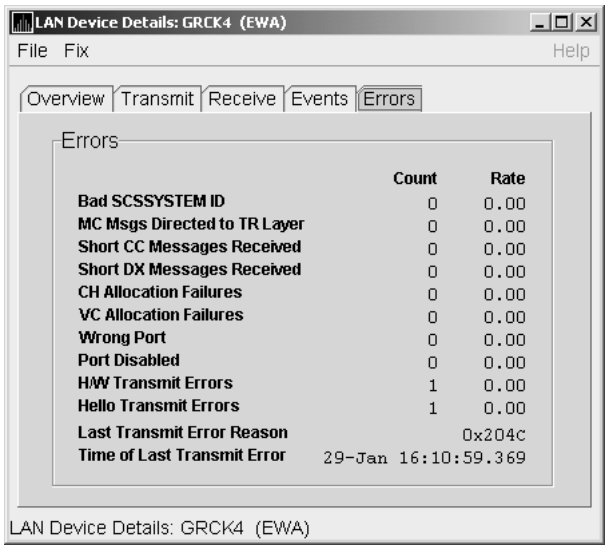


Table 4–25 describes the data displayed in Figure 4–25.

Table 4–25 LAN Device Errors Data

Data	Description
Bad SCSSYSTEM ID	Received a packet with the wrong SCSSYSTEM ID in it.
MC Msgs Directed to TR Layer	Number of multicast packets directed to the NISCA Transport layer.
Short CC Messages Received	Number of packets received that were too short to contain a NISCA channel control header.
Short DX Messages Received	Number of packets received that were too short to contain a NISCA DX header.
CH Allocation Failures	Number of times the system failed to allocate memory for use as a channel structure in response to a packet received by this LAN device.
VC Allocation Failures	Number of times the system failed to allocate memory for use as a VC structure in response to a packet received by this LAN device.
Wrong Port	Number of packets addressed to the wrong NISCA address.
Port Disabled	Number of packets discarded because the LAN device was disabled.
H/W Transmit Errors	Number of local hardware transmit errors.
Hello Transmit Errors	Number of transmit errors during HELLOs.
Last Transmit Error Reason	Reason for last transmit error.
Time of Last Transmit Error	Time of last transmit error: date and time.

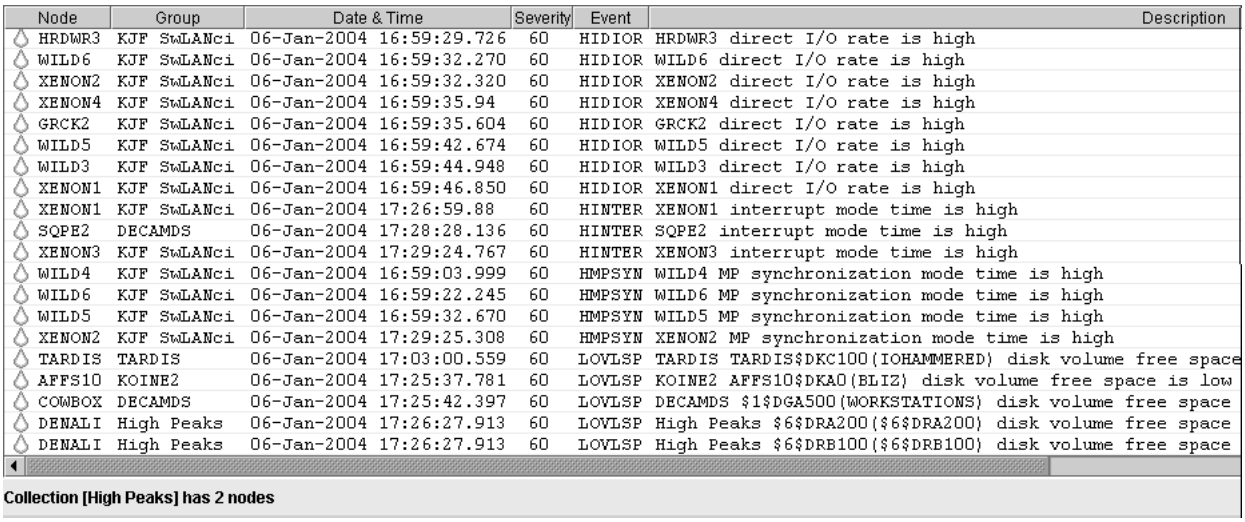
5
Getting Information About Events

Note

Before you start this chapter, be sure to read the explanations of data collection, events, thresholds, and occurrences in Chapter 1.

The Availability Manager indicates resource availability problems in the Event pane Figure 5–1 of the main Application window (see Figure 1–1).

Figure 5–1 OpenVMS Event Pane



Node	Group	Date & Time	Severity	Event	Description
HRDWR3	KJF SwLANci	06-Jan-2004 16:59:29.726	60	HIDIOR	HRDWR3 direct I/O rate is high
WILD6	KJF SwLANci	06-Jan-2004 16:59:32.270	60	HIDIOR	WILD6 direct I/O rate is high
XENON2	KJF SwLANci	06-Jan-2004 16:59:32.320	60	HIDIOR	XENON2 direct I/O rate is high
XENON4	KJF SwLANci	06-Jan-2004 16:59:35.94	60	HIDIOR	XENON4 direct I/O rate is high
GRCK2	KJF SwLANci	06-Jan-2004 16:59:35.604	60	HIDIOR	GRCK2 direct I/O rate is high
WILD5	KJF SwLANci	06-Jan-2004 16:59:42.674	60	HIDIOR	WILD5 direct I/O rate is high
WILD3	KJF SwLANci	06-Jan-2004 16:59:44.948	60	HIDIOR	WILD3 direct I/O rate is high
XENON1	KJF SwLANci	06-Jan-2004 16:59:46.850	60	HIDIOR	XENON1 direct I/O rate is high
XENON1	KJF SwLANci	06-Jan-2004 17:26:59.88	60	HINTER	XENON1 interrupt mode time is high
SQPE2	DECAMDS	06-Jan-2004 17:28:28.136	60	HINTER	SQPE2 interrupt mode time is high
XENON3	KJF SwLANci	06-Jan-2004 17:29:24.767	60	HINTER	XENON3 interrupt mode time is high
WILD4	KJF SwLANci	06-Jan-2004 16:59:03.999	60	HMPSYN	WILD4 MP synchronization mode time is high
WILD6	KJF SwLANci	06-Jan-2004 16:59:22.245	60	HMPSYN	WILD6 MP synchronization mode time is high
WILD5	KJF SwLANci	06-Jan-2004 16:59:32.670	60	HMPSYN	WILD5 MP synchronization mode time is high
XENON2	KJF SwLANci	06-Jan-2004 17:29:25.308	60	HMPSYN	XENON2 MP synchronization mode time is high
TARDIS	TARDIS	06-Jan-2004 17:03:00.559	60	LOVLSP	TARDIS TARDIS$DKC100(IOHAMMERED) disk volume free space
AFFS10	KOINE2	06-Jan-2004 17:25:37.781	60	LOVLSP	KOINE2 AFFS10$DKA0(BLIZ) disk volume free space is low
COWBOX	DECAMDS	06-Jan-2004 17:25:42.397	60	LOVLSP	DECAMDS 1DGA500(WORKSTATIONS) disk volume free space
DENALI	High Peaks	06-Jan-2004 17:26:27.913	60	LOVLSP	High Peaks 6DRA200(6DRA200) disk volume free space
DENALI	High Peaks	06-Jan-2004 17:26:27.913	60	LOVLSP	High Peaks 6DRB100(6DRB100) disk volume free space

Collection [High Peaks] has 2 nodes

The Event pane helps you identify system problems. In many cases, you can apply fixes to correct these problems as well, as explained in Chapter 6.

The Availability Manager displays a warning message in the Event pane whenever it detects a resource availability problem. If logging is enabled (the default), the Availability Manager also logs each event in the Events Log file, which you can display or print. (See Section 5.2 for the location of this file and a cautionary note about it.)

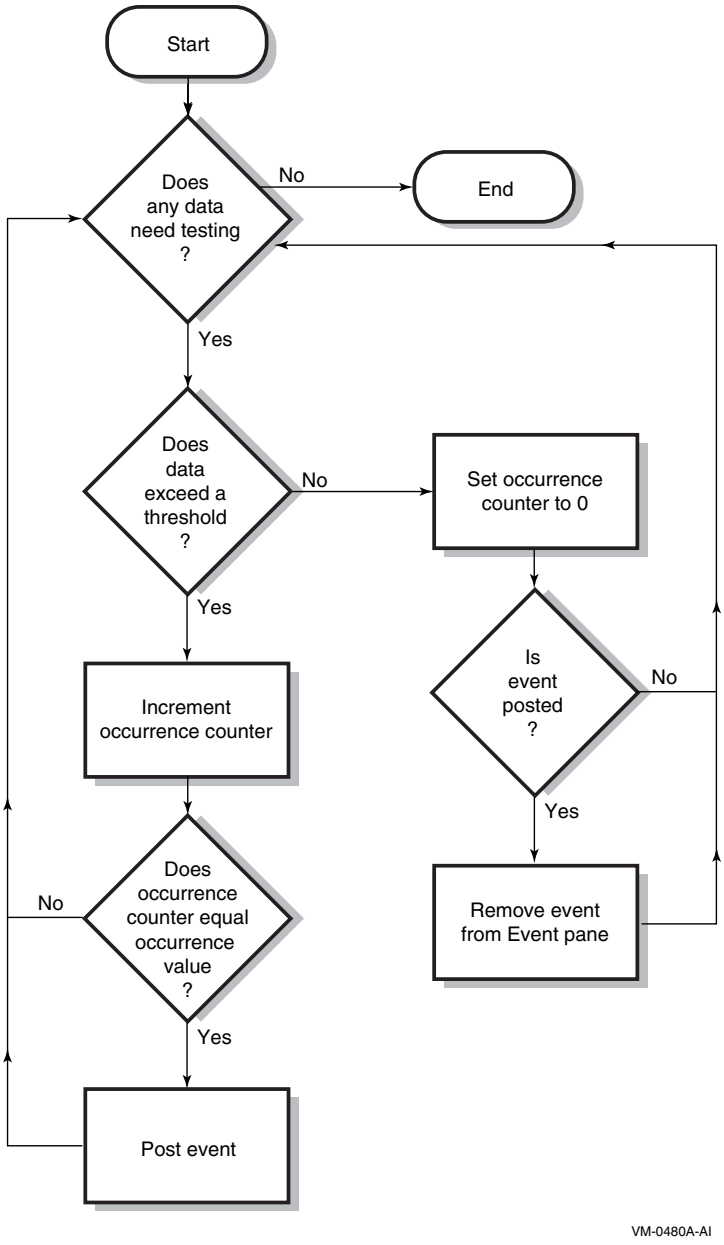
Occurrence Counters

During data collection, any time data meets or exceeds the threshold for an event, an **occurrence counter** is incremented. When the incremented value matches the value in the Occurrence box on the Event Customization page (Figure 1–6), the event is posted in the Event pane of the Application window (see Figure 1–1).

Note that some events are triggered when data is lower than the threshold; other events are triggered when data is higher than the threshold.

If, at any time during data collection, the data does *not* meet or exceed the threshold, the occurrence counter is set to 0, and the event is removed from the Event pane. Figure 5–2 depicts this sequence.

Figure 5–2 Testing for Events



5.1 Event Information That Is Displayed in the Event Pane

The Availability Manager can display events for all nodes that are currently in communication with the Data Analyzer. When an event of a certain severity occurs, the Availability Manager adds the event to a list in the Event pane.

The length of time an event is displayed depends on the severity of the event. Less severe events are displayed for a short period of time (30 seconds); more severe events are displayed until you explicitly remove the event from the Event pane (explained in Section 5.1.2).

5.1.1 Data in the Event Pane

Table 5–1 identifies the data items displayed in the Event pane.

Table 5–1 Event Pane Data

Data Item	Description
Node	Name of the node causing the event
Group	Group of the node causing the event
Date	Date the event occurred
Time	Time that an event was detected
Sev	Severity: a value from 0 to 100
Event	Alphanumeric identifier of the type of event
Description	Short description of the resource availability problem

Appendix B contains tables of events that are displayed in the Event pane. In addition, these tables contain an explanation of each event and the recommended remedial action.

5.1.2 Event Pane Menu Options

When you right-click a node name or data item in the Event pane, the Availability Manager displays a popup menu with the following options:

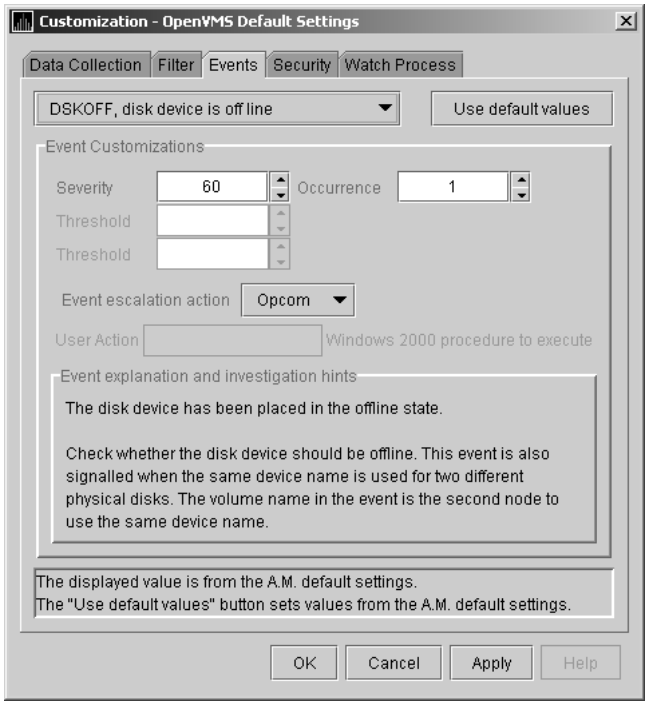
Menu Option	Description
Display	Displays the Node Summary page associated with that event.
Remove	Removes an event from the display.
Freeze/Unfreeze	Freezes a value in the display until you “unfreeze” it; a snowflake icon is displayed to the left of an event that is frozen.
Customize	Allows you to customize events.

5.2 Criteria for Posting and Displaying an Event

The Availability Manager uses the following criteria to determine whether to post an event and display it in the Event pane:

- Data collection posts an event if the event condition exists for the number of data collections specified in the Occurrence value on the Event Customization page (Figure 5–3).

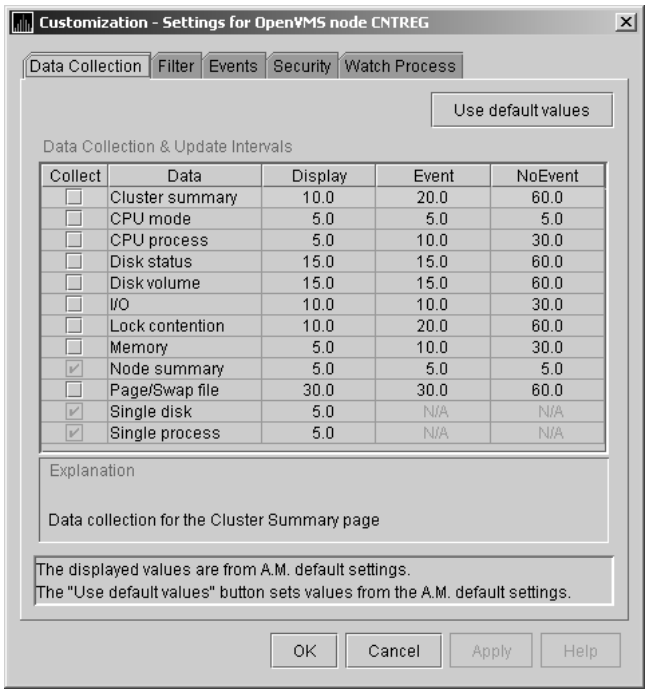
Figure 5–3 Sample Event Customization Page



The sample Event Customization page indicates an Occurrence value of 2. This means that if the DSKERR event exceeds its threshold of 15 for two consecutive data collections, the DSKERR event is posted in the Event pane.

- When an event is posted, data is collected at the **Event** interval shown on the Data Collection Customization page (Figure 5–4).

Figure 5–4 OpenVMS Data Collection Customization Page



On the Data Collection Customization page, for example, the Event interval for Disk Status is every 15 seconds.

- The data value displayed in the Node pane that is associated with the event turns red when an event is posted (see Figure 5–5).

Figure 5–5 OpenVMS Node Pane

Node Name	CPU	Active CPUs	MEM	BIO	DIO	CPU Qs	Events	Proc Ct	OS Version	HW Model	HW Arch
AFFC5	0	2/4	44	0	0	0	1	36/2500 1%	Open VMS V7.3-2	AlphaServer ES40	Alpha
AFFC6	0	2/4	54	2	2	0	1	51/792 6%	Open VMS V7.3-2	AlphaServer ES40	Alpha
AFFS10	1	2/2	54	13	4	2	1	73/514 14%	Open VMS V7.3-1	AlphaServer 2100A 5/300	Alpha
AFFS11	0	2/2	45	1	0	0	1	22/153 14%	Open VMS V6.2-1H3	AlphaServer 2000 4/200	Alpha
AFFS12	0	2/2	51	0	0	0	0	26/136 19%	Open VMS V7.2-1	AlphaServer 2000 4/200	Alpha
AFFS21	0	1/1	6	0	0	0	0	22/1500 1%	Open VMS V7.3-2	AlphaServer DS15	Alpha
AFFS22	0	1/1	65	0	0	0	0	15/480 3%	Open VMS V7.1	VAX 4000-600	VAX
AFFS23	0	1/1	21	0	0	0	0	22/150 15%	Open VMS V7.1-1H1	DEC 3000 - M800	Alpha
AFFS5	0	1/1	64	0	0	0	0	24/240 10%	Open VMS V7.1	VAX 4000-300	VAX
AFFS51	67	2/2	65	121	111	0	5	82/1113 7%	Open VMS V7.3-2	AlphaServer 2100 4/275	Alpha
AFFS52	1	2/2	15	3	1	0	1	52/126 41%	Open VMS V7.2-2	AlphaServer 2100 4/275	Alpha
AFFS55	0	1/1	24	0	0	0	0	15/360 4%	Open VMS V6.2	VAX 4000-300	VAX
AFFS6	0	2/2	42	0	0	0	0	20/117 17%	Open VMS V7.1-2	AlphaServer 2000 4/200	Alpha
AFFS7	0	1/1	51	0	0	0	0	33/173 19%	Open VMS V7.2-2	AlphaServer 2000 4/233	Alpha
AFFS8	0	1/1	62	0	0	0	0	42/483 8%	Open VMS V7.3	AlphaStation 600A 5/500	Alpha
AFFS9	1	1/1	64	0	0	0	1	18/90 20%	Open VMS V7.3	VAXstation 4000-60	VAX

- When an event is posted, it is added to the Events Log file by default:
  - On OpenVMS systems, the Events Log file is:

    ```
    AMDS$AM_LOG:ANALYZEREVENTS.LOG
    ```

    A new version of this file is created each time you access the Availability Manager.
  - On Windows systems, the Events Log file is:

    ```
    AnalyzerEvents.log
    ```

This file, which is in the installation directory, is overwritten each time you access the Availability Manager.

The following example shows a partial events log file:

```
VAXJET 01-22-2004 11:24:50.67 0  CFGDON  VAXJET configuration done
DBGAVC 01-22-2004 11:25:12.41 0  CFGDON  DBGAVC configuration done
AFFS5  01-22-2004 11:25:13.23 0  CFGDON  AFFS5 configuration done
DBGAVC 01-22-2004 11:25:18.31 80 LCKCNT  DBGAVC possible contention for resource REG$MASTER_LOCK
VAXJET 01-22-2004 11:25:27.47 40 LOBIOQ  VAXJET LES$ACP_V30 has used most of
                                         its BIOLM process quota
PEROIT 01-22-2004 11:25:27.16 0  CFGDON  PEROIT configuration done
KOINE  01-22-2004 11:25:33.05 99 NOSWFL  KOINE has no swap file
MAWK   01-22-2004 11:26:20.15 99 FXTIMO  MAWK Fix timeout for FID to Filename Fix
MAWK   01-22-2004 11:26:24.48 60 HIDIOR  MAWK direct I/O rate is high
REDSQL 01-22-2004 11:26:30.61 10 PRPGFL  REDSQL _FTA2: high page fault rate
REDSQL 01-22-2004 11:26:31.18 60 PRPIOR  REDSQL _FTA7: paging I/O rate is high
MAWK   01-22-2004 11:26:24.48 60 HIDIOR  MAWK direct I/O rate is high
AFFS52 01-22-2004 11:25:33.64 60 DSKMNV  AFFS52 $4$DUA320(OMTV4) disk mount verify in progress
VAXJET 01-22-2004 11:38:46.23 90 DPGERR  VAXJET error executing driver program, ...
REDSQL 01-22-2004 11:39:18.73 60 PRCPWT  REDSQL _FTA2: waiting in PWAIT
REDSQL 01-22-2004 11:44:37.19 75 PRCCUR  REDSQL _FTA7: has a high CPU rate
```

Caution About Events Logs

If you collect data on many nodes, running the Availability Manager for a long period of time can result in a large events log. For example, in a run that monitors more than 50 nodes with most of the background data collection enabled, the events log can grow by up to 30 MB per day. At this rate, systems with small disks might fill up the disk on which the events log resides.

Closing the Availability Manager application will enable you to access the events log for tasks such as archiving. Starting the Availability Manager starts a new events log.

5.3 Displaying Additional Event Information

For more detailed information about a specific event, double-click any event data item in the Event pane. The Availability Manager first displays a data page that most closely corresponds to the cause of the event. You can choose other tabs for additional detailed information.

For a description of data pages and the information they contain, see Chapter 3.

6
Performing Fixes on OpenVMS Nodes

You can perform **fixes** on OpenVMS nodes to resolve resource availability problems and improve system availability.

This chapter discusses the following topics:

- Understanding fixes
- Performing fixes

Caution

Performing certain fixes can have serious repercussions, including possible system failure. Therefore, only experienced system managers should perform fixes.

6.1 Understanding Fixes

When you suspect or detect a resource availability problem, in many cases you can use the Availability Manager to analyze the problem and to perform a fix to improve the situation.

Availability Manager fixes fall into these categories:

- Node fixes
- Process fixes
- Cluster interconnect fixes

You can access fixes, by category, from the pages listed in Table 6–1.

Table 6–1 Accessing Availability Manager Fixes

Fix Category and Name	Available from This Page
Node fixes:	Node Summary CPU
Crash Node Adjust Quorum	Memory I/O

(continued on next page)

Table 6–1 (Cont.) Accessing Availability Manager Fixes

Fix Category and Name	Available from This Page
Process fixes: General process fixes: Delete Process Exit Image Suspend Process Resume Process Process Priority Process memory fixes: Purge Working Set (WS) Adjust Working Set (WS) Process limits fixes: Direct I/O Buffered I/O AST Open file Lock Timer Subprocess I/O Byte Pagefile Quota	All of the process fixes are available from the following pages: Memory I/O CPU Process Single Process
Cluster interconnect fixes:	These fixes are available from the following lines of data on the Cluster Summary page (Figure 4–7):
– Port Adjust Priority	Right-click a data item on the local port data display line to display a menu containing the Adjust Priority option.
– Circuit Adjust Priority	Right-click a data item on the circuits data display line to display a menu containing the Adjust Priority option.
LAN Virtual Circuit summary: Maximum Transmit Window Size Maximum Receive Window Size Checksumming Compression	Right-click a data item in the LAN Virtual Circuit Summary category to display a menu. Then click the Fixes... menu item.
LAN Path (Channel) Summary: Adjust Priority Hops Maximum Packet Size	Right-click a data item in the LAN Path (Channel) Summary category to display a menu. Then click the VC LAN Fix... menu item.

(continued on next page)

Table 6–1 (Cont.) Accessing Availability Manager Fixes

Fix Category and Name	Available from This Page
LAN Device Details: Adjust Priority Maximum Buffer Size Start Device Stop Device	Right-click a data item in the LAN Path (Channel) Summary category to display a menu. Then click the LAN Device Details menu item to display pages containing Fix options.

Table 6–2 summarizes various problems, recommended fixes, and the expected results of fixes.

Table 6–2 Summary of Problems and Matching Fixes

Problem	Fix	Result
Node resource hanging cluster	Crash Node	Node fails with operator-requested shutdown.
Cluster hung	Adjust Quorum	Quorum for cluster is adjusted.
Process looping, intruder	Delete Process	Process no longer exists.
Endless process loop in same PC range	Exit Image	Exits from current image.
Runaway process, unwelcome intruder	Suspend Process	Process is suspended from execution.
Process previously suspended	Resume Process	Process starts from point it was suspended.
Runaway process or process that is overconsuming	Process Priority	Base priority changes to selected setting.
Low node memory	Purge Working Set (WS)	Frees memory on node; page faulting might occur for process affected.
Working set too high or low	Adjust Working Set (WS)	Removes unused pages from working set; page faulting might occur.
Process quota has reached its limit and has entered RWAIT state	Adjust Process Limits	Process limit is increased, which in many cases frees the process to continue execution.
Process has exhausted its pagefile quota	Adjust Pagefile Quota	Pagefile quota limit of the process is adjusted.

Most process fixes correspond to an OpenVMS system service call, as shown in the following table:

Process Fix	System Service Call
Delete Process	$DELPRC
Exit Image	$FORCEX
Suspend Process	$SUSPND
Resume Process	$RESUME
Process Priority	$SETPRI
Purge Working Set (WS)	$PURGWS
Adjust Working Set (WS)	$ADJWSL

Process Fix	System Service Call
Adjust process limits of the following: Direct I/O (DIO) Buffered I/O (BIO) Asynchronous system trap (AST) Open file (FIL) Lock queue (ENQ) Timer queue entry (TQE) Subprocess (PRC) I/O byte (BYT)	None

Note

Each fix that uses a system service call requires that the process execute the system service. A hung process will have the fix queued to it, where the fix will remain until the process is operational again.

Be aware of the following facts before you perform a fix:

- You must have write access to perform a fix. To perform LAN fixes, you must have control access.
- You cannot undo many fixes. For example, after using the Crash Node fix, the node must be rebooted (either by the node if the node reboots automatically, or by a person performing a manual boot).
- Do not apply the Exit Image, Delete Process, or Suspend Process fix to system processes. Doing so might require you to reboot the node.
- Whenever you exit an image, you cannot return to that image.
- You cannot delete processes that have exceeded their job or process quota.
- The Availability Manager ignores fixes applied to the SWAPPER process.

How to Perform Fixes

Standard OpenVMS privileges restrict users' write access. When you run the Data Analyzer, you must have the CMKRNL privilege to send a write (fix) instruction to a node with a problem.

The following options are displayed at the bottom of all fix pages:

Option	Description
OK	Applies the fix and then exits the page. Any message associated with the fix is displayed in the Event pane.
Cancel	Cancels the fix.
Apply	Applies the fix and does not exit the page. Any message associated with the fix is displayed in the Return Status section of the page and in the Event pane.

The following sections explain how to perform node fixes and process fixes.

6.2 Performing Node Fixes

The Availability Manager node fixes allow you to deliberately fail (crash) a node or to adjust cluster quorum.

To perform a node fix, follow these steps:

1. On the Node Summary, CPU, Memory, or I/O page, click the Fix menu.
2. Click Fix Options.

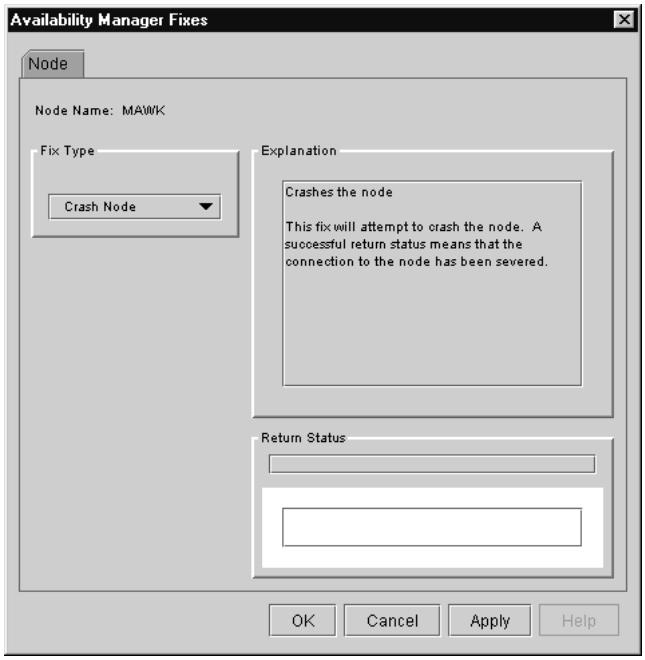
6.2.1 Crash Node

Caution

The crash node fix is an operator-requested bugcheck from the driver. It takes place as soon as you click **OK** in the Crash Node page. After you perform this fix, the node cannot be restored to its previous state. After a crash, the node must be rebooted.

When you select the Crash Node option, the Availability Manager displays the Crash Node page, shown in Figure 6–1.

Figure 6–1 Crash Node Page



Note

Because the node cannot report a confirmation when a node crash fix is successful, the crash success message is displayed after the timeout period for the fix confirmation has expired.

Recognizing a System Failure Forced by the Availability Manager

Because a user with suitable privileges can force a node to fail from the Data Analyzer by using the "Crash Node" fix, system managers have requested a method for recognizing these particular failure footprints so that they can distinguish them from other failures. These failures all have identical footprints: they are operator-induced system failures in kernel mode at IPL 8. The top of the kernel stack is similar the following display:

```
SP => Quadword system address
      Quadword data
      1BE0DEAD.00000000
      00000000.00000000
      Quadword data            TRAP$CRASH
      Quadword data            SYS$RMDRIVER + offset
```

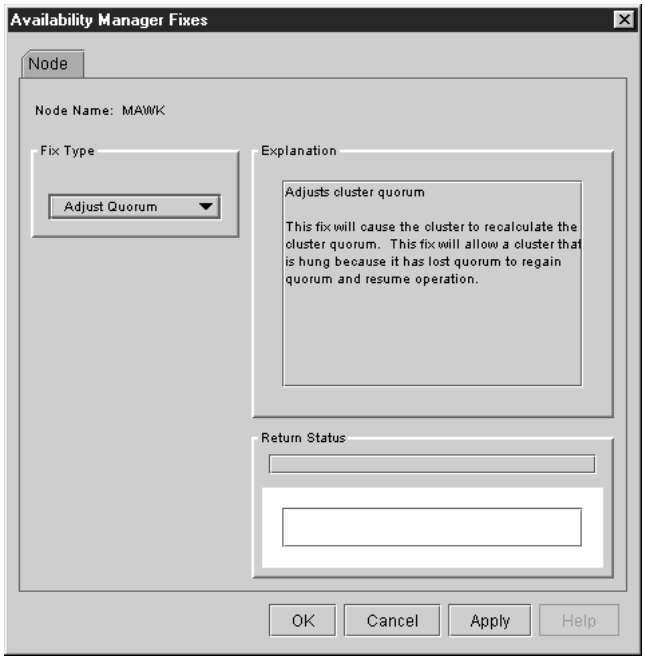
6.2.2 Adjust Quorum

The Adjust Quorum fix forces the node to refigure the quorum value. This fix is the equivalent of the Interrupt Priority C (IPC) mechanism used at system consoles for the same purpose. The fix forces the adjustment for the entire cluster so that each node in the cluster will have the same new quorum value.

The Adjust Quorum fix is useful when the number of votes in a cluster falls below the quorum set for that cluster. This fix allows you to readjust the quorum so that it corresponds to the current number of votes in the cluster.

When you select the Adjust Quorum option, the Availability Manager displays the page shown in Figure 6–2.

Figure 6–2 Adjust Quorum Page



6.3 Performing Process Fixes

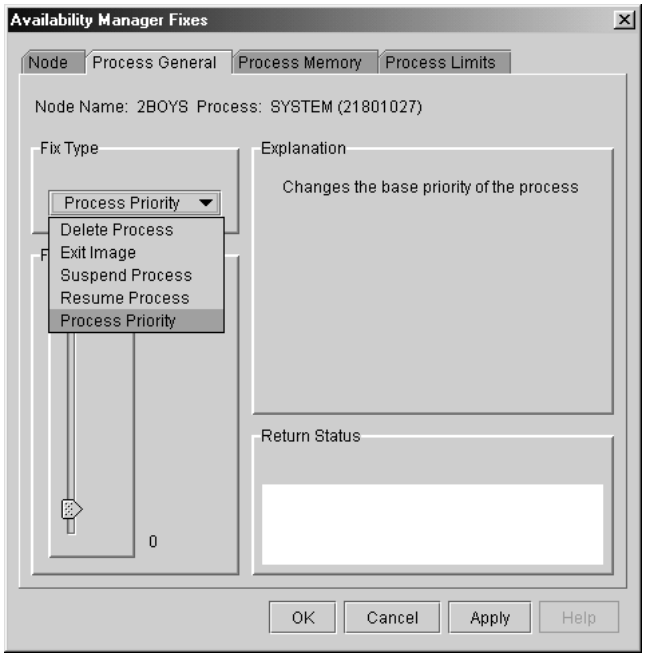
To perform a process fix, follow these steps:

1. On the Memory or I/O page, right-click a process name.
2. Click Fix Options.

   The Availability Manager displays these Process tabs:

   Process General
   Process Memory
   Process Limits
3. Click one of these tabs to bring it to the front.
4. Click the down arrow to display the process fixes in this group, as shown in Figure 6–3, where the Process General tab has been chosen.

Figure 6–3 Process General Options



5. Select a process fix (for example, Process Priority, as shown in Figure 6–3,) to display a fix page.

Some of the fixes, such as Process Priority, require you to use a slider to change the default value. When you finish setting a new process priority, click **Apply** at the bottom of the page to apply that fix.

6.3.1 General Process Fixes

The following sections describe Availability Manager general process fixes.

6.3.1.1 Delete Process

In most cases, a Delete Process fix deletes a process. However, if a process is waiting for disk I/O or is in a resource wait state (RWAST), this fix might not delete the process. In this situation, it is useless to repeat the fix. Instead, depending on the resource the process is waiting for, a Process Limit fix might free the process. As a last resort, reboot the node to delete the process.

Caution

Deleting a system process could cause the system to hang or become unstable.

When you select the Delete Process option, the Availability Manager displays the page shown in Figure 6–4.

Figure 6–4 Delete Process Page

After reading the explanation, click **Apply** at the bottom of the page to apply the fix. A message displayed on the page indicates that the fix has been successful.

6.3.1.2 Exit Image

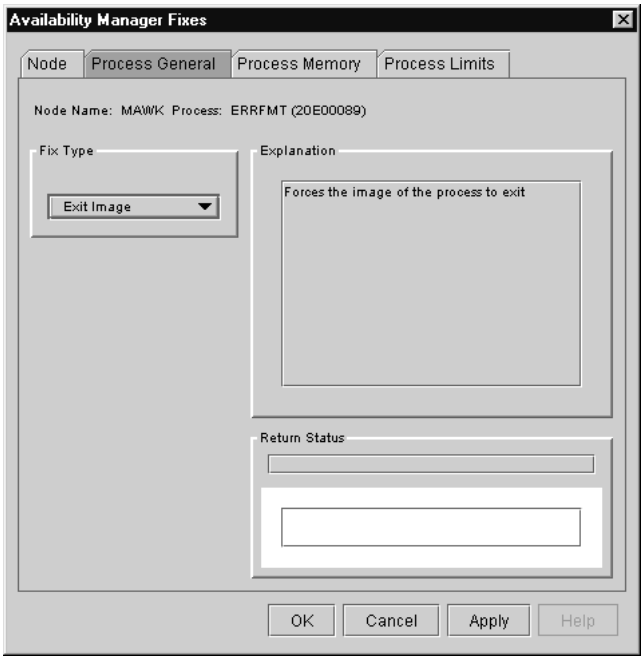
Exiting an image on a node can stop an application that a user requires. Check the Single Process page first to determine which image is running on the node.

Caution

Exiting an image on a system process could cause the system to hang or become unstable.

When you select the Exit Image option, the Availability Manager displays the page shown in Figure 6–5.

Figure 6–5 Exit Image Page



After reading the explanation in the page, click **Apply** at the bottom of the page to apply the fix. A message displayed on the page indicates that the fix has been successful.

6.3.1.3 Suspend Process

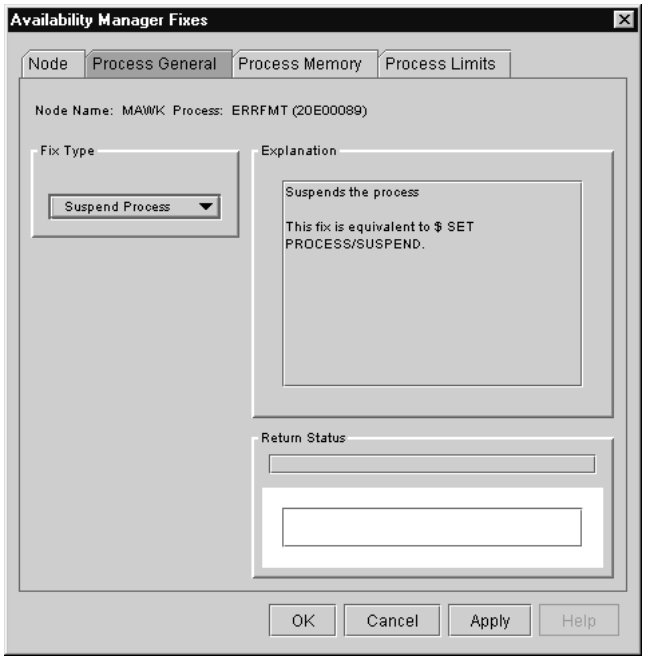
Suspending a process that is consuming excess CPU time can improve perceived CPU performance on the node by freeing the CPU for other processes to use. (Conversely, resuming a process that was using excess CPU time while running might reduce perceived CPU performance on the node.)

Caution

Do not suspend system processes, especially JOB_CONTROL, because this might make your system unusable. (See the *HP OpenVMS Programming Concepts Manual, Volume I* for more information.)

When you select the Suspend Process option, the Availability Manager displays the page shown in Figure 6–6.

Figure 6–6 Suspend Process Page



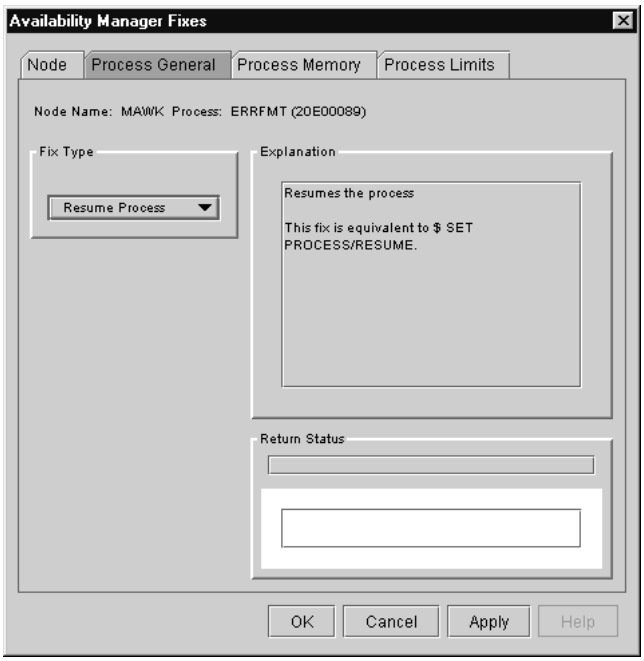
After reading the explanation, click **Apply** at the bottom of the page to apply the fix. A message displayed on the page indicates that the fix has been successful.

6.3.1.4 Resume Process

Resuming a process that was using excess CPU time while running might reduce perceived CPU performance on the node. (Conversely, suspending a process that is consuming excess CPU time can improve perceived CPU performance by freeing the CPU for other processes to use.)

When you select the Resume Process option, the Availability Manager displays the page shown in Figure 6–7.

Figure 6–7 Resume Process Page



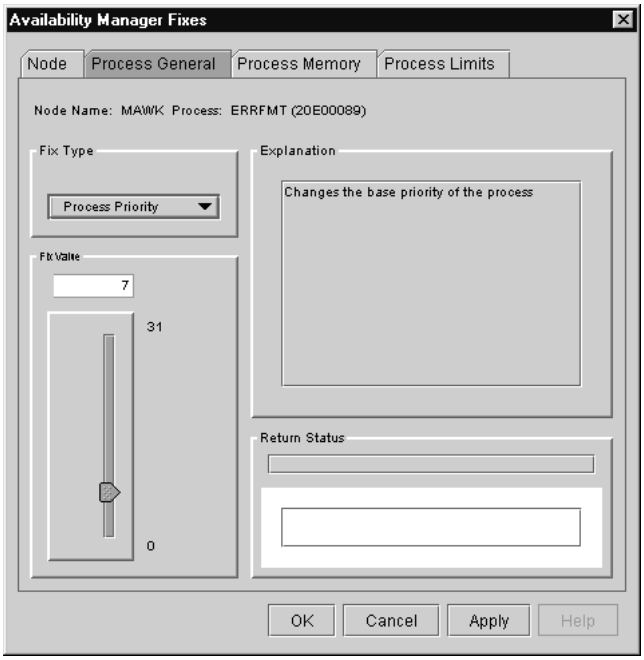
After reading the explanation, click **Apply** at the bottom of the page to apply the fix. A message displayed on the page indicates that the fix has been successful.

6.3.1.5 Process Priority

If the priority of a compute-bound process is too high, the process can consume all the CPU cycles on the node, affecting performance dramatically. On the other hand, if the priority of a process is too low, the process might not obtain enough CPU cycles to do its job, also affecting performance.

When you select the Process Priority option, the Availability Manager displays the page shown in Figure 6–8.

Figure 6–8 Process Priority Page



To change the base priority for a process, drag the slider on the scale to the number you want. The current priority number is displayed in a small box above the slider. You can also click the line above or below the slider to adjust the number by 1.

When you are satisfied with the new base priority, click **Apply** at the bottom of the page to apply the fix. A message displayed on the page indicates that the fix has been successful.

6.3.2 Process Memory Fixes

The following sections describe the Availability Manager fixes you can use to correct process memory problems:

- Purge Working Set
- Adjust Working Set

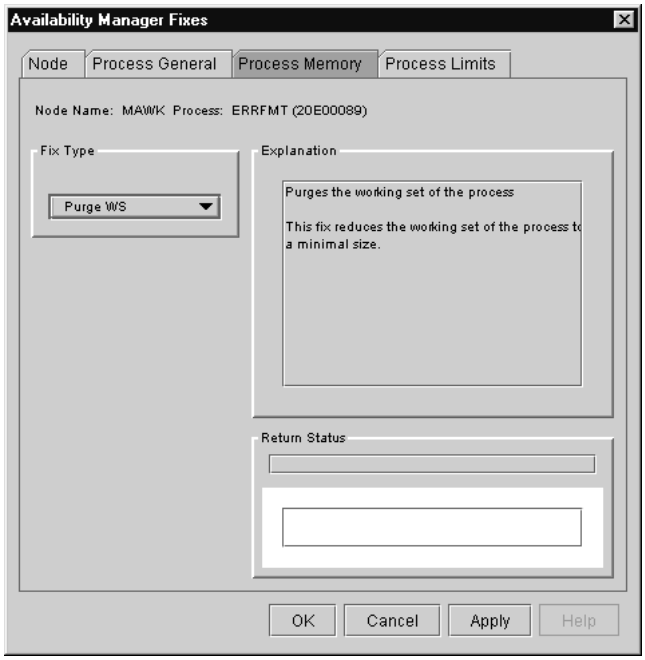
6.3.2.1 Purge Working Set

This fix purges the working set to a minimal size. You can use this fix to reclaim a process's pages that are not in active use. If the process is in a wait state, the working set remains at a minimal size, and the purged pages become available for other uses. If the process becomes active, pages the process needs are page-faulted back into memory, and the unneeded pages are available for other uses.

Be careful not to repeat this fix too often: a process that continually reclaims needed pages can cause excessive page faulting, which can affect system performance.

When you select the Purge Working Set option, the Availability Manager displays the page shown in Figure 6–9.

Figure 6–9 Purge Working Set Page



After reading the explanation on the page, click **Apply** at the bottom of the page to apply the fix. A message displayed on the page indicates that the fix has been successful.

6.3.2.2 Adjust Working Set

Adjusting the working set of a process might prove to be useful in situations similar to the following ones:

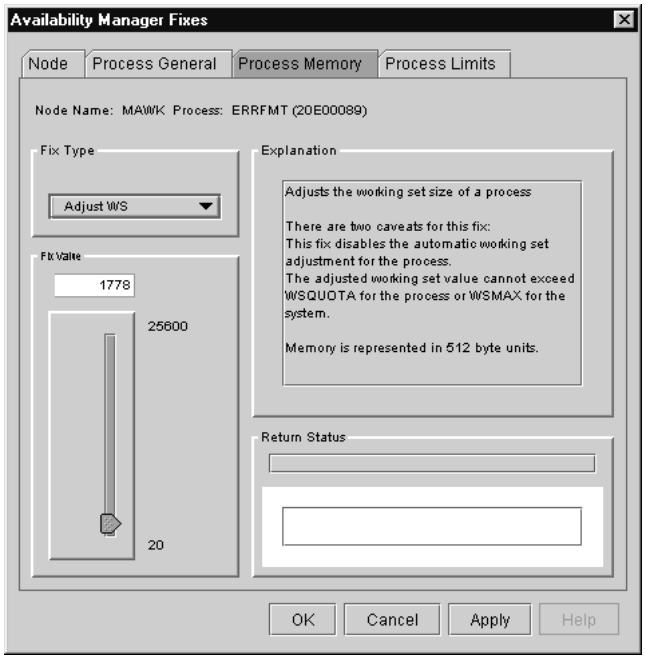
- If a process is page-faulting because of insufficient memory, you can reclaim unused memory from other processes by decreasing the working set of one or more of them.
- If a process is page-faulting too frequently because its working set is too small, you can increase its working set.

Caution

If the automatic working set adjustment is enabled for the system, a fix to adjust the working set size disables the automatic adjustment for the process. For more information, see OpenVMS online help for SET WORKING_SET/ADJUST, which includes /NOADJUST.

When you select the Adjust Working Set fix, the Availability Manager displays the page shown in Figure 6–10.

Figure 6–10 Adjust Working Set Page



To perform this fix, use the slider to adjust the working set to the limit you want. You can also click the line above or below the slider to adjust the number by 1.

When you are satisfied with the new working set limit, click **Apply** at the bottom of the page to apply the fix. A message displayed on the page indicates that the fix has been successful.

6.3.3 Process Limits Fixes

If a process is waiting for a resource, you can use a Process Limits fix to increase the resource limit so that the process can continue. The increased limit is in effect only for the life of the process, however; any new process is assigned the quota that was set in the UAF.

When you click the Process Limits tab, you can select any of the following options:

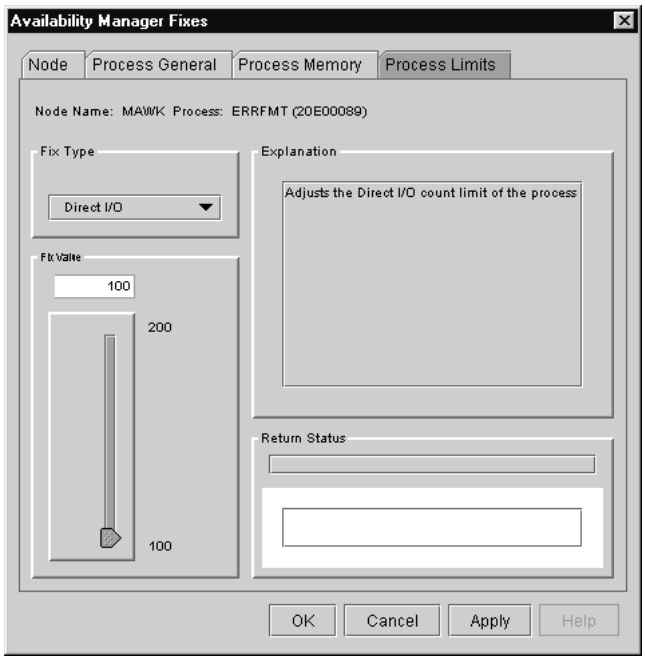
Direct I/O
Buffered I/O
AST
Open File
Lock
Timer
Subprocess
I/O Byte
Pagefile Quota

These fix options are described in the following sections.

6.3.3.1 Direct I/O Count Limit

You can use this fix to adjust the direct I/O count limit of a process. When you select the Direct I/O option, the Availability Manager displays the page shown in Figure 6–11.

Figure 6–11 Direct I/O Count Limit Page



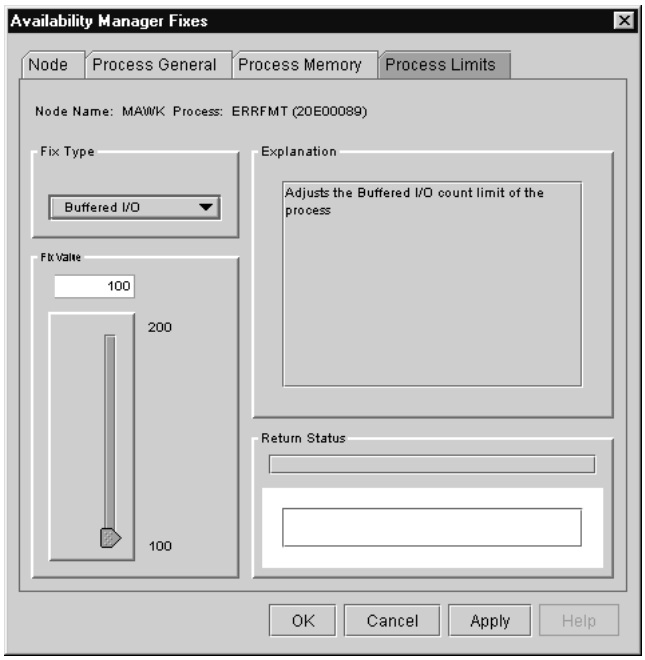
To perform this fix, use the slider to adjust the direct I/O count to the limit you want. You can also click the line above or below the slider to adjust the number by 1.

When you are satisfied with the new direct I/O count limit, click **Apply** at the bottom of the page to apply the fix. A message displayed on the page indicates that the fix has been successful.

6.3.3.2 Buffered I/O Count Limit

You can use this fix to adjust the buffered I/O count limit of a process. When you select the Buffered I/O option, the Availability Manager displays the page shown in Figure 6–12.

Figure 6–12 Buffered I/O Count Limit Page



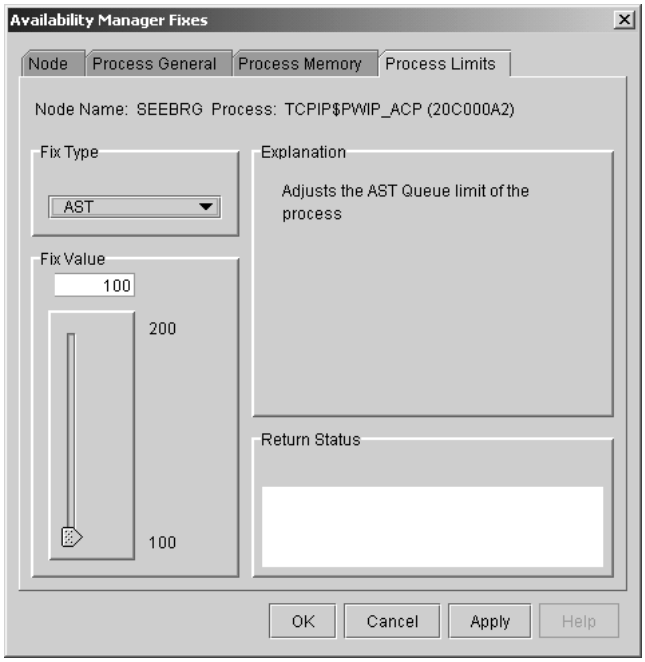
To perform this fix, use the slider to adjust the buffered I/O count to the limit you want. You can also click the line above or below the slider to adjust the number by 1.

When you are satisfied with the new buffered I/O count limit, click **Apply** at the bottom of the page to apply the fix. A message displayed on the page indicates that the fix has been successful.

6.3.3.3 AST Queue Limit

You can use this fix to adjust the AST queue limit of a process. When you select the AST option, the Availability Manager displays the page shown in Figure 6–13.

Figure 6–13 AST Queue Limit Page



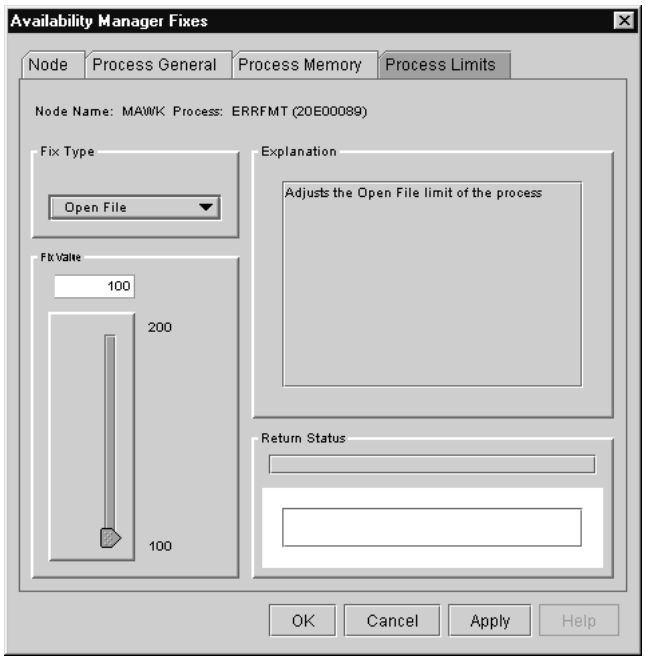
To perform this fix, use the slider to adjust the AST queue limit to the number you want. You can also click the line above or below the slider to adjust the number by 1.

When you are satisfied with the new AST queue limit, click **Apply** at the bottom of the page to apply the fix. A message displayed on the page indicates that the fix has been successful.

6.3.3.4 Open File Limit

You can use this fix to adjust the open file limit of a process. When you select the Open File option, the Availability Manager displays the page shown in Figure 6–14.

Figure 6–14 Open File Limit Page



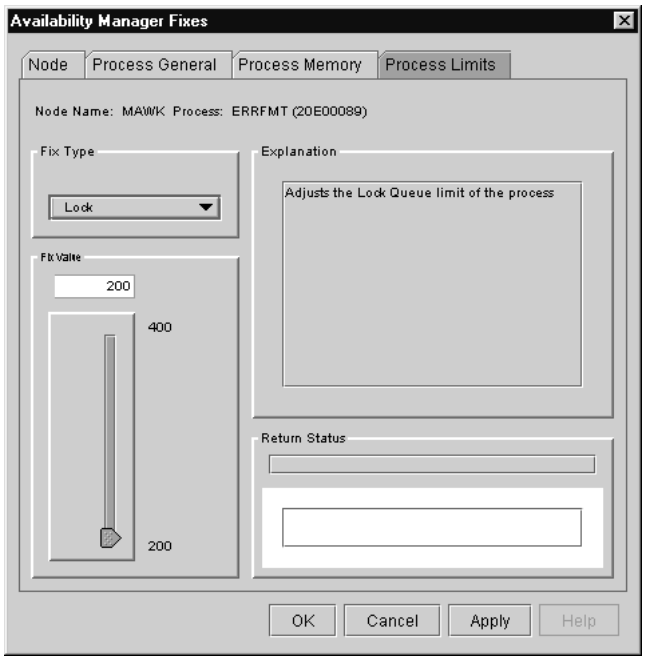
To perform this fix, use the slider to adjust the open file limit to the number you want. You can also click the line above or below the slider to adjust the number by 1.

When you are satisfied with the new open file limit, click **Apply** at the bottom of the page to apply the fix. A message displayed on the page indicates that the fix has been successful.

6.3.3.5 Lock Queue Limit

You can use this fix to adjust the lock queue limit of a process. When you select the Lock option, the Availability Manager displays the page shown in Figure 6–15.

Figure 6–15 Lock Queue Limit Page



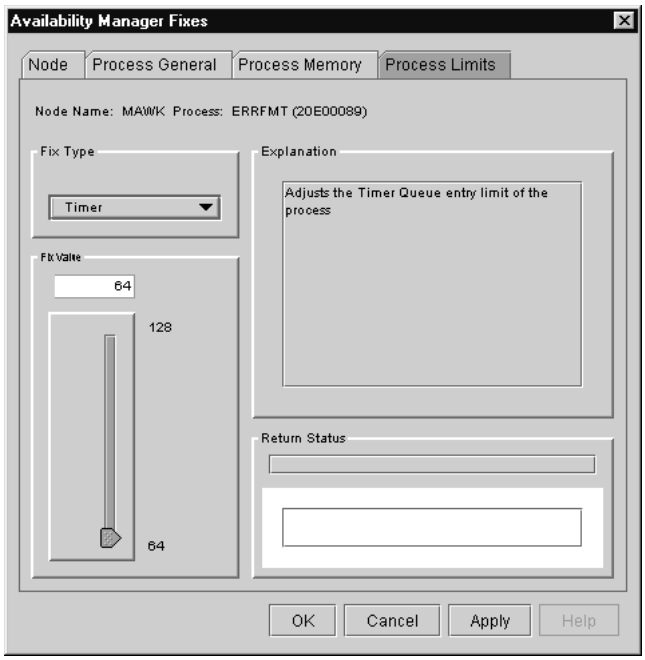
To perform this fix, use the slider to adjust the lock queue limit to the number you want. You can also click the line above or below the slider to adjust the number by 1.

When you are satisfied with the new lock queue limit, click **Apply** at the bottom of the page to apply the fix. A message displayed on the page indicates that the fix has been successful.

6.3.3.6 Timer Queue Entry Limit

You can use this fix to adjust the timer queue entry limit of a process. When you select the Timer option, the Availability Manager displays the page shown in Figure 6–16.

Figure 6–16 Timer Queue Entry Limit Page



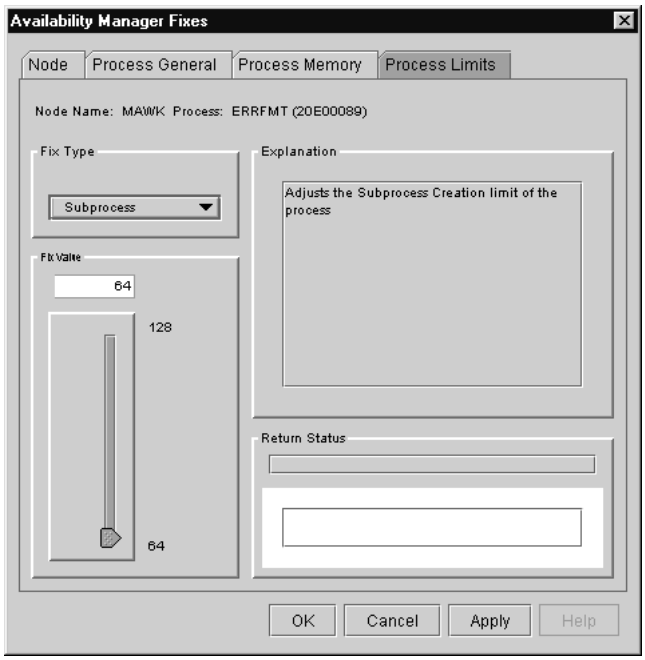
To perform this fix, use the slider to adjust the timer queue entry limit to the number you want. You can also click the line above or below the slider to adjust the number by 1.

When you are satisfied with the new timer queue entry limit, click **Apply** at the bottom of the page to apply the fix. A message displayed on the page indicates that the fix has been successful.

6.3.3.7 Subprocess Creation Limit

You can use this fix to adjust the creation limit of the subprocess of a process. When you select the Subprocess option, the Availability Manager displays the page shown in Figure 6–17.

Figure 6–17 Subprocess Creation Limit Page



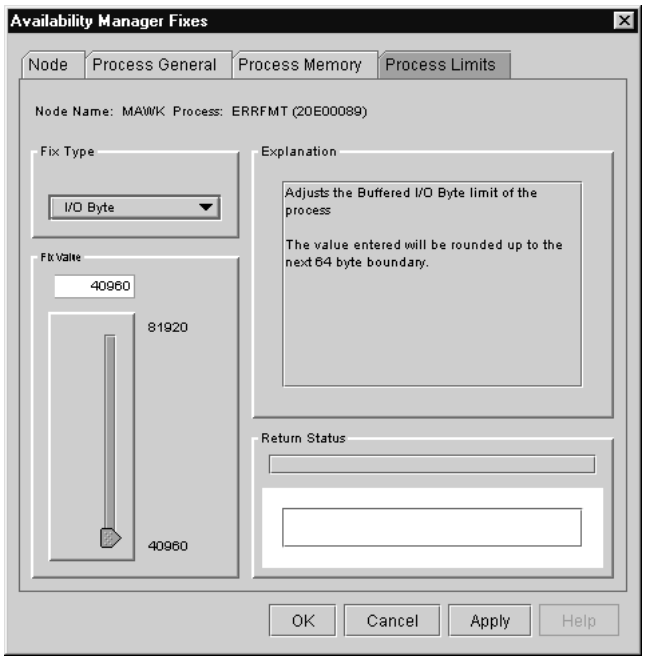
To perform this fix, use the slider to adjust the subprocess creation limit of a process to the number you want. You can also click the line above or below the slider to adjust the number by 1.

When you are satisfied with the new subprocess creation limit, click **Apply** at the bottom of the page to apply the fix. A message displayed on the page indicates that the fix has been successful.

6.3.3.8 I/O Byte

You can use this fix to adjust the I/O byte limit of a process. When you select the I/O Byte option, the Availability Manager displays the page shown in Figure 6–18.

Figure 6–18 I/O Byte Page



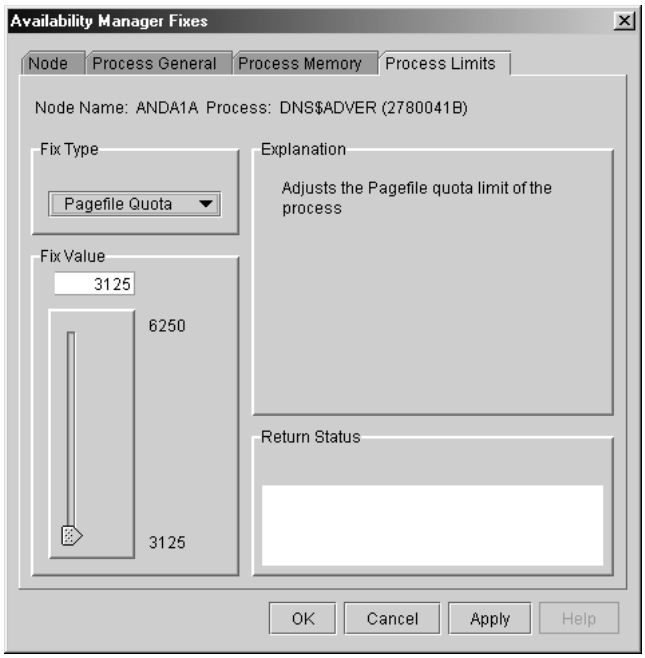
To perform this fix, use the slider to adjust the I/O byte limit to the number you want. You can also click the line above or below the slider to adjust the number by 1.

When you are satisfied with the new I/O byte limit, click **Apply** at the bottom of the page to apply the fix. A message displayed on the page indicates that the fix has been successful.

6.3.3.9 Pagefile Quota

You can use this fix to adjust the pagefile quota limit of a process. This quota is share among all the processes in a job. When you select the Pagefile Quota option, the Availability Manager displays the page shown in Figure 6–19.

Figure 6–19 Pagefile Quota Page



To perform this fix, use the slider to adjust the pagefile quota limit to the number you want. You can also click above or below the slider to adjust the fix value by 1.

When you are satisfied with the new pagefile quota limit, click **Apply** at the bottom of the page to apply the fix. A message displayed on the page indicates that the fix has been successful.

6.4 Performing Cluster Interconnect Fixes

Cluster interconnect fixes have been added to the Availability Manager beginning in Version 2.0. The following are categories of cluster interconnect fixes:

- Port adjust priority fix
- Circuit adjust priority fix
- LAN virtual circuit (VC) summary fixes
- LAN channel (path) fixes
- LAN device fixes

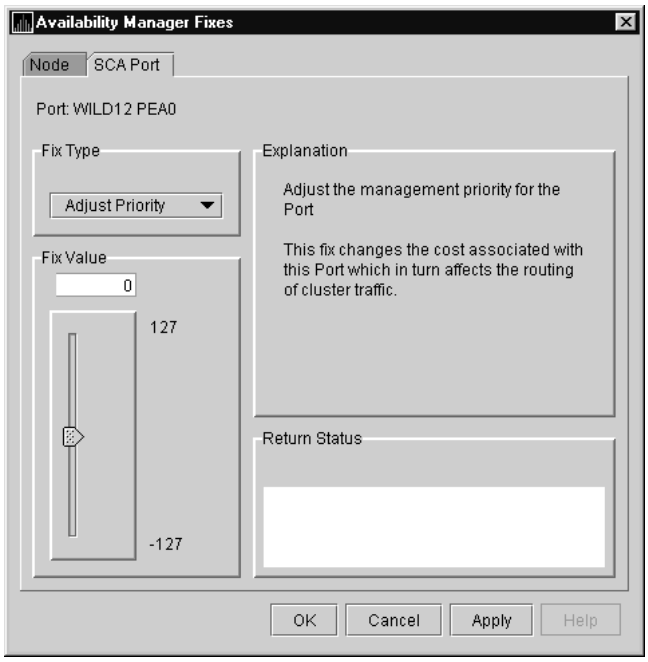
The following sections describe these types of fixes and tell how to access them and how to perform them. The descriptions also indicate whether or not the fix is currently available.

6.4.1 Port Adjust Priority Fix

To access the Port Adjust Priority fix, right-click a data item in the local port data display line (see Figure 4–3). The Availability Manager displays a popup menu with the Port Fix option.

This page (Figure 6–20) allows you to change the cost associated with this port, which, in turn, affects the routing of cluster traffic.

Figure 6–20 Port Adjust Priority Page

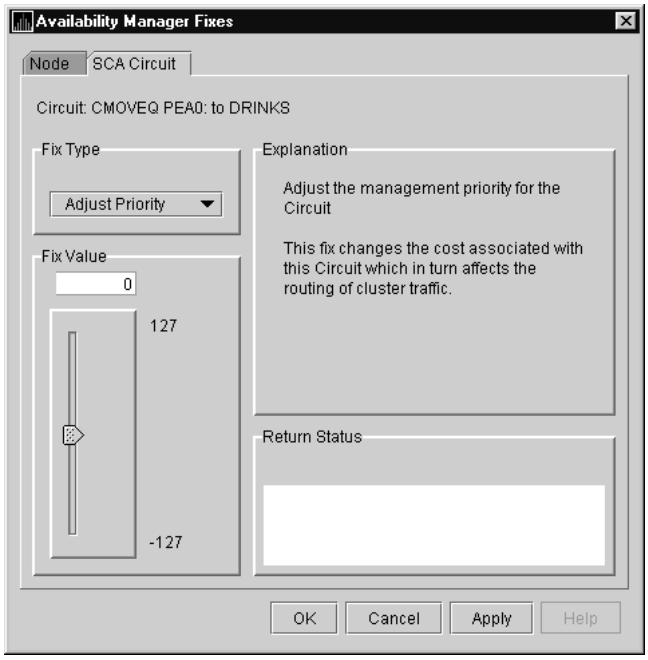


6.4.2 Circuit Adjust Priority Fix

To access the Circuit Adjust Priority fix, right-click a data item in the local port data display line (see Figure 4–4). The Availability Manager displays a popup menu with the Circuit Fix option.

This page (Figure 6–21) allows you to change the cost associated with this circuit, which, in turn, affects the routing of cluster traffic.

Figure 6–21 Circuit Adjust Priority Page



6.4.3 LAN Virtual Circuit Summary Fixes

To access LAN virtual circuit summary fixes, right-click a data item in the LAN Virtual Circuit Summary category (see Figure 4–6). The Availability Manager displays a popup menu with the following options:

- Channel Summary
- VC LAN Details...
- VC LAN Fix...

When you select VC LAN Fix..., the Availability Manager displays the first of several fix pages, the Maximum Transmit Window Size. By clicking Maximum Transmit Window Size, you can display a list of all the LAN VC summary fixes:

- Maximum Transmit Window Size
- Maximum Receive Window Size
- Checksumming
- Compression

These fixes are described in the following sections.

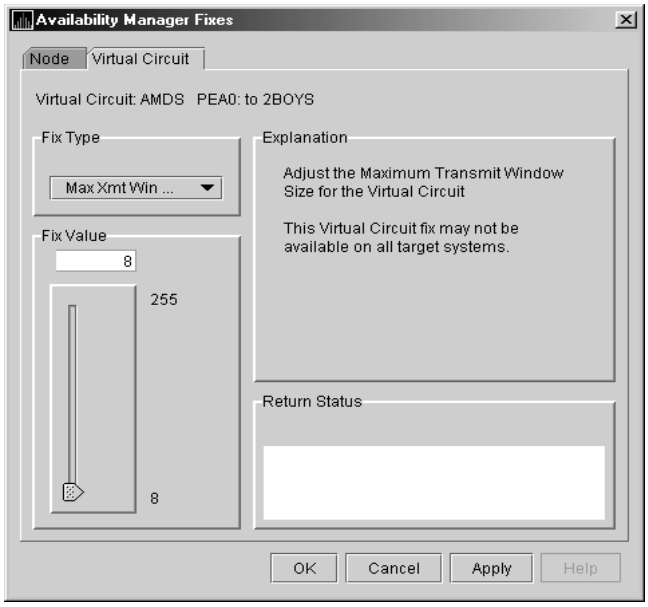
6.4.3.1 LAN VC Maximum Transmit Window Size Fix

This page (Figure 6–22) allows you to adjust the maximum transmit window size for the virtual circuit.

Note

As of OpenVMS Version 7.3-1, this fix is not recognized by PEDRIVER. However, the fix might become available in a future OpenVMS or remedial release.

Figure 6–22 LAN VC Maximum Transmit Window Size Page



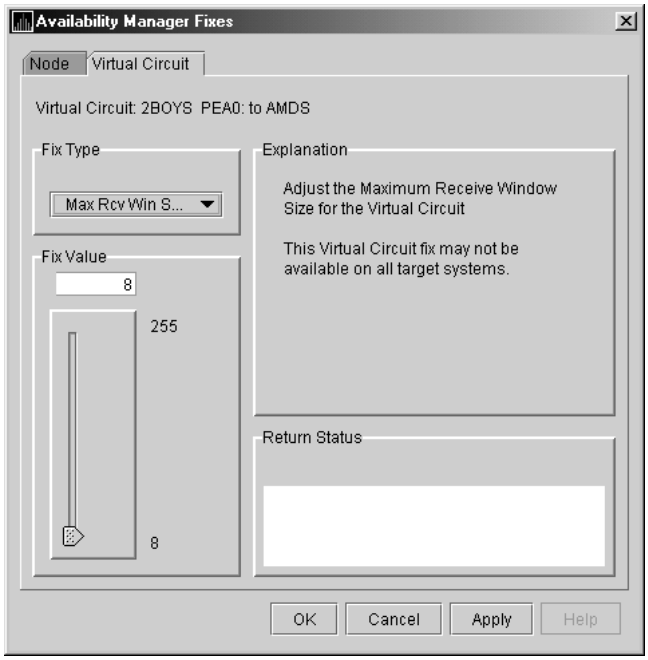
6.4.3.2 LAN VC Maximum Receive Window Size Fix

This page, (Figure 6–23) allows you to adjust the maximum receive window size for the virtual circuit.

Note

As of OpenVMS Version 7.3-1, this fix is not recognized by PEDRIVER. However, the fix might become available in a future OpenVMS or remedial release.

Figure 6–23 LAN VC Maximum Receive Window Size Page



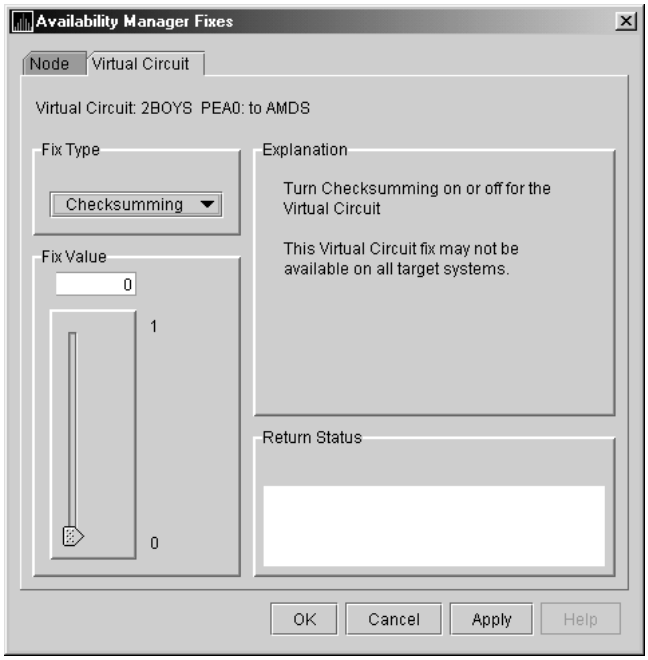
6.4.3.3 LAN VC Checksumming Fix

This page (Figure 6–24) allows you to turn checksumming on or off for the virtual circuit.

Note

As of OpenVMS Version 7.3-1, this fix is not recognized by PEDRIVER. However, the fix might become available in a future OpenVMS or remedial release.

Figure 6–24 LAN VC Checksumming Page



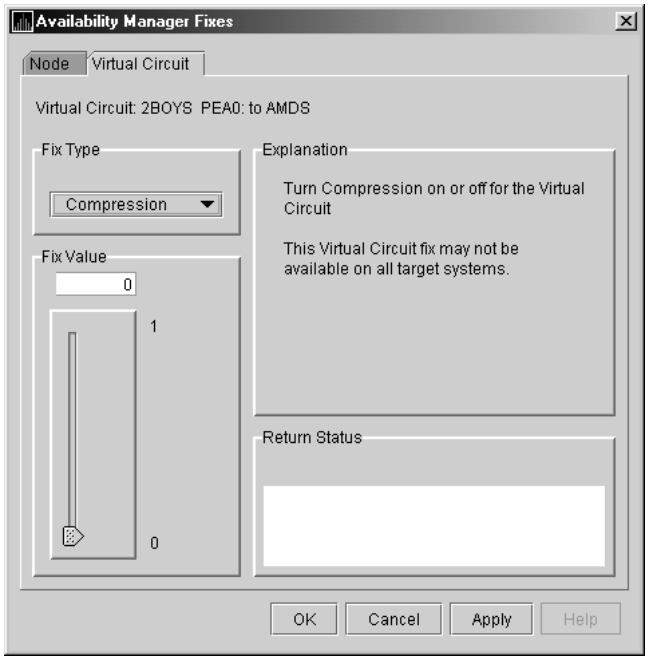
6.4.3.4 LAN VC Compression Fix

This page (Figure 6–24) allows you to turn compression on or off for the virtual circuit.

Note

As of OpenVMS Version 7.3-1, this fix is not recognized by PEDRIVER. However, the fix might become available in a future OpenVMS or remedial release.

Figure 6–25 LAN VC Compression Page



6.4.4 LAN Channel Fixes

To access LAN path fixes, right-click an item in the LAN Channel Summary category (see Figure 4–7). The Availability Manager displays a popup menu with the following options:

- Channel Details...
- LAN Device Details...
- Fixes...

Click the Fixes... menu item to display this list of available fixes:

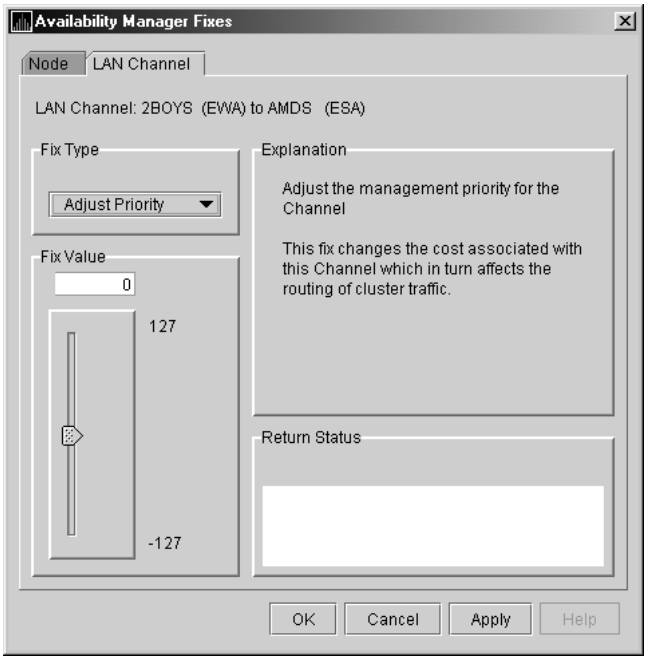
- Adjust Priority
- Hops
- Maximum Packet Size

These fixes are described in the following sections.

6.4.4.1 LAN Path Adjust Priority Fix

This page (Figure 6–26) allows you to change the cost associated with this channel. This, in turn, affects the routing of cluster traffic.

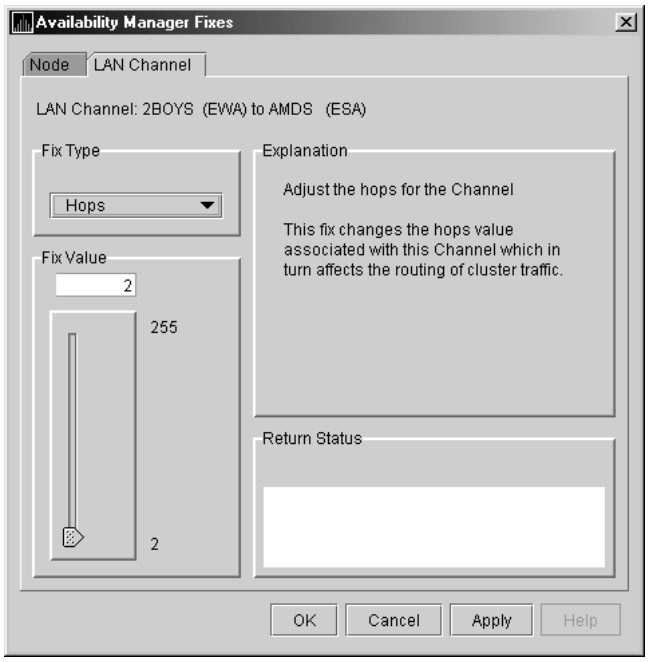
Figure 6–26 LAN Path Adjust Priority Page



6.4.4.2 LAN Path Hops Fix

This page (Figure 6–27) allows you to change the hops for the channel. This fix changes the hops value associated with this channel. This, in turn, affects the routing of cluster traffic.

Figure 6–27 LAN Path Hops Page



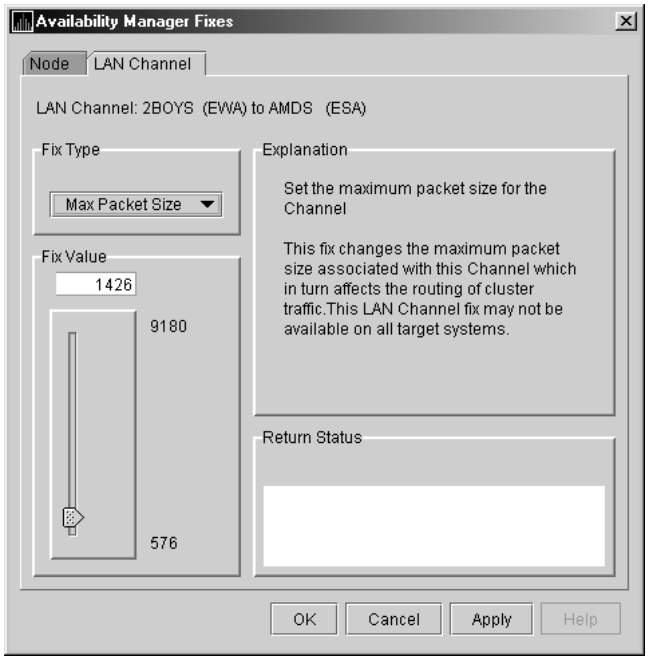
6.4.4.3 LAN Path Maximum Packet Size Fix

This page (Figure 6–28) allows you to set the maximum packet size associated with this channel. This, in turn, affects the routing of cluster traffic.

Note

As of OpenVMS Version 7.3-1, this fix is not recognized by PEDRIVER. However, the fix might become available in a future OpenVMS or remedial release.

Figure 6–28 LAN Path Maximum Packet Size Page



6.4.5 LAN Device Fixes

To access LAN device fixes, right-click an item in the LAN Path (Channel) Summary category (see Figure 4–7). The Availability Manager displays a popup menu with the following options:

- Channel Details...
- LAN Device Details...
- Fixes...

Select the LAN Device Details menu item to display the LAN Device Details window. From the Devicer Details window, select Fix... from the Fix menu. The Availability Manager displays the first of several pages, each of which contains a fix option:

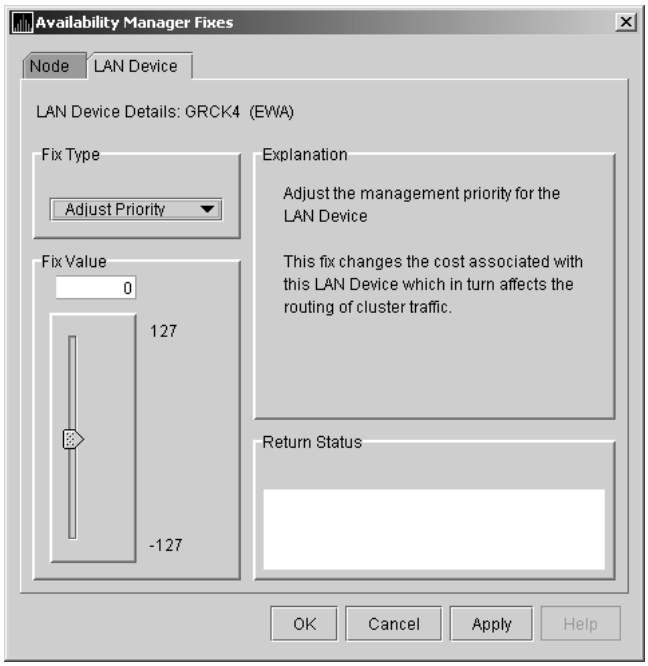
Adjust Priority
Set Max Buffer Size
Start Device
Stop Device

These fixes are described in the following sections.

6.4.5.1 LAN Device Adjust Priority Fix

This page (Figure 6–29) allows you to adjust the management priority for the device. This fix changes the cost associated with this device. This, in turn, affects the routing of cluster traffic.

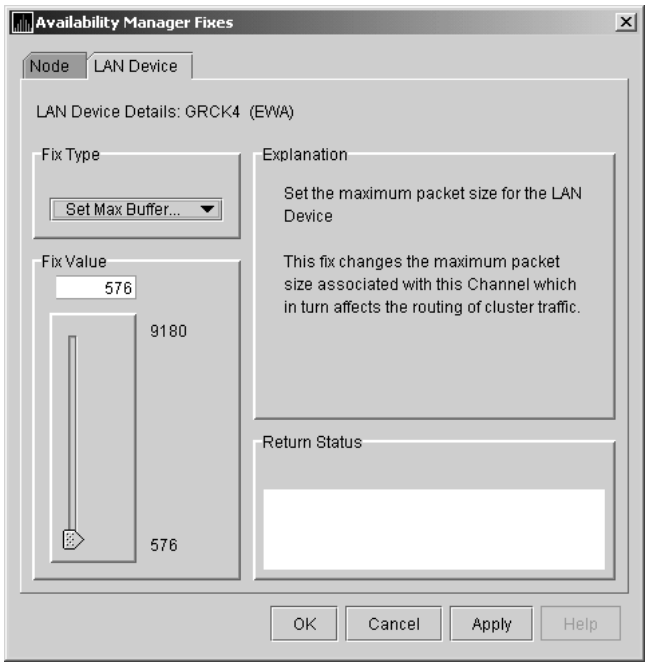
Figure 6–29 LAN Device Adjust Priority Page



6.4.5.2 LAN Device Set Maximum Buffer Fix

This page (Figure 6–30) allows you to set the maximum packet size for the device. This fix changes the maximum packet size associate with this channel. This, in turn, affects the routing of cluster traffic.

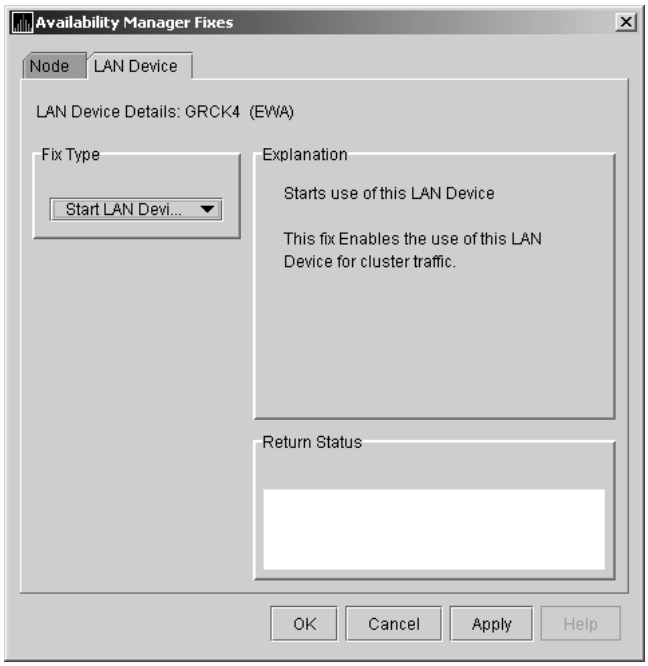
Figure 6–30 LAN Device Set Maximum Buffer Size Page



6.4.5.3 LAN Device Start Fix

This page (Figure 6–31) starts the use of this device. This fix enables the use of this device for cluster traffic.

Figure 6–31 LAN Device Start Page



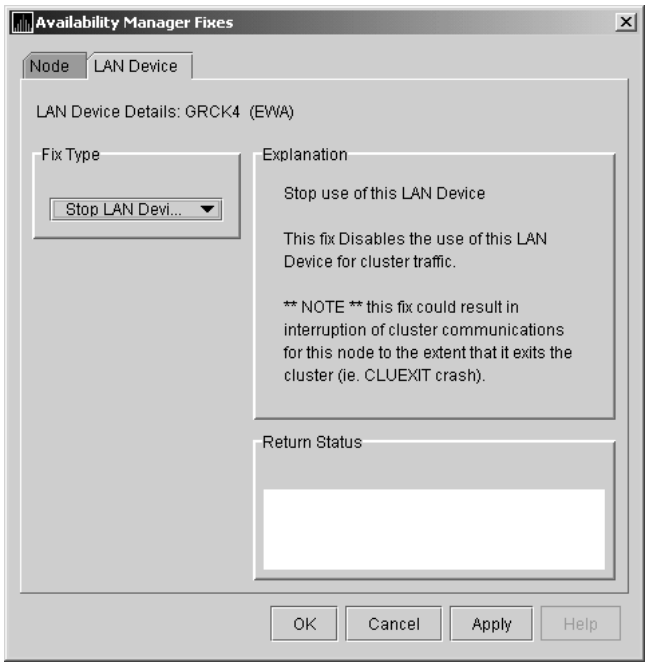
6.4.5.4 LAN Device Stop Fix

This page (Figure 6–32) stops the use of this device . This fix disables the use of this device for cluster traffic.

Caution

This fix could result in interruption of cluster communications for this node. The node may exit the cluster (CLUEXIT crash).

Figure 6–32 LAN Device Stop Page



7

Customizing the Availability Manager

This chapter explains how to customize the following Availability Manager features:

Feature	Description
Nodes or node groups	You can select one or more groups or individual nodes to monitor.
Data collection	For OpenVMS nodes, you can choose the types of data you want to collect as well as set several types of collection intervals. (On Windows nodes, specific types of data are collected by default.)
Data filters	For OpenVMS nodes, you can specify a number of parameters and values that limit the amount of data that is collected.
Event filters	You can specify the severity of events that are displayed as well as several other filter settings for events.
Security	On Data Analyzer and Data Collector nodes, you can change passwords. On OpenVMS Data Collector nodes, you can edit a file that contains security triplets.
Watch process	You can specify up to eight processes for the Availability Manager to monitor and report on if they disappear and also if they subsequently reappear.

In addition, you can change the group membership of nodes as explained in Section 7.3.

Table 7–1 shows the levels of customization the Availability Manager provides. At each level, you can customize specific features. The table shows which features can be customized at which levels.

Table 7–1 Customization Levels

Customizable Features	A.M. Default	Application	Operating System	Group	Node
Nodes or node groups	X	X			
Data collection	X		X	X	X
Data filters	X		X	X	X
Event filters	X		X	X	X
Security	X		X	X	X
Watch process	X		X	X	X

7.1 Specifying Levels of Customization

You can customize each feature at one or more of the following levels, as shown in Table 7–1:

1. A.M. Default
2. Application
3. Operating System
4. Group
5. Node

The Availability Manager (A.M.) Default level consists of values that are preset within the Availability Manager. Any customization overrides A.M. Default values. For example, customizing values for filters at the Group level overrides values for filters at the Operating System level. Similarly, customizing values for filters at the Node level overrides values for filters at the Group level. The Application level is unique because it is the only level at which you can select or change the nodes or groups of nodes you want to display.

To return to the values set at the preceding level, you can click the **Use default values** button at the top of the customization page.

Examples of Setting Levels of Customization

If you monitor several groups but the password for the nodes in one of those groups is different from the password of nodes in other groups, right-click the group you want to change, choose **Customize** from the popup menu, click the **Security** tab, and change the password. This new password is then used for each node that is a member of that group.

As a second example, to change the password of one node in a group to a different password than the other nodes in the group, right-click that node, choose **Customize**, click the **Security** tab, and change the password to one that differs from the other nodes in the group. For that node, the new password overrides the group password.

The Availability Manager keeps track of the next higher level of a particular setting. This means that you can reset a value to that of the next higher level. In the second password example, if you want to set the password for the single node back to the password that the rest of the group uses, simply click the **Use default value** button. The password value for the node now comes from the group-level password setting. At this point, if you change the group password, all the nodes in the group have the new password.

Understanding the Terms "Use Default Value" and "System Default"

The **Use default value** button and the "system default" setting are not necessarily the same value. A system default is a value stored in the Availability Manager and is a value that is used until a user overrides it. Clicking the **Use default value** button sets a value to conform to the value set at the next higher level of customization.

If you want to override the system default for all OpenVMS nodes, click the **Customize** button on the main menu bar, and choose **Customize OpenVMS**. Whatever changes you make subsequently are set for all OpenVMS nodes except those nodes on which a particular parameter has been set at the group or node level.

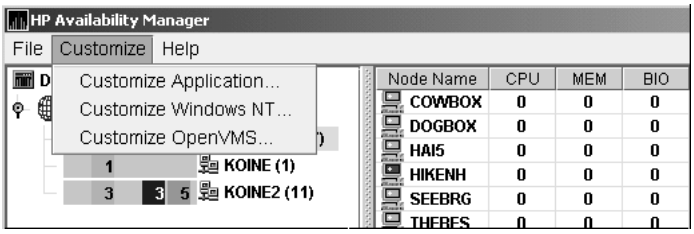
A two-line status box at the bottom of the Customization page tells you the level at which the selected parameter will be configured and what level the value will come from if you press the **Use default value** button. In this way, you can tell what level of customization you are overriding when you make changes.

In the main Application window (see Figure 1–1), you can select the levels of customization that are shown in Table 7–1. The following sections explain these levels.

7.1.1 Application and Operating System Customization Levels

In the Application window menu bar, click the **Customize** menu. The Availability Manager displays the popup menu shown in Figure 7–1.

Figure 7–1 Application and Operating System Customization Menu

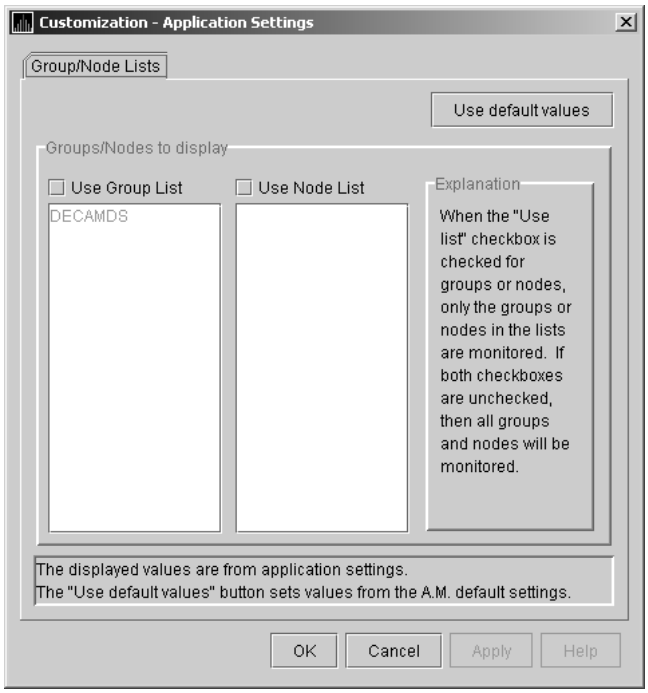


Notice that you have a choice of two levels of customization: application and operating system levels. The operation system level has two choices: Windows NT and OpenVMS. The following sections describe these choices.

7.1.1.1 Application Customization

When you choose **Customize Application**, the Availability Manager displays the page shown in Figure 7–2, where you can select groups of nodes or individual nodes to be displayed. Section 7.2 explains how to do this.

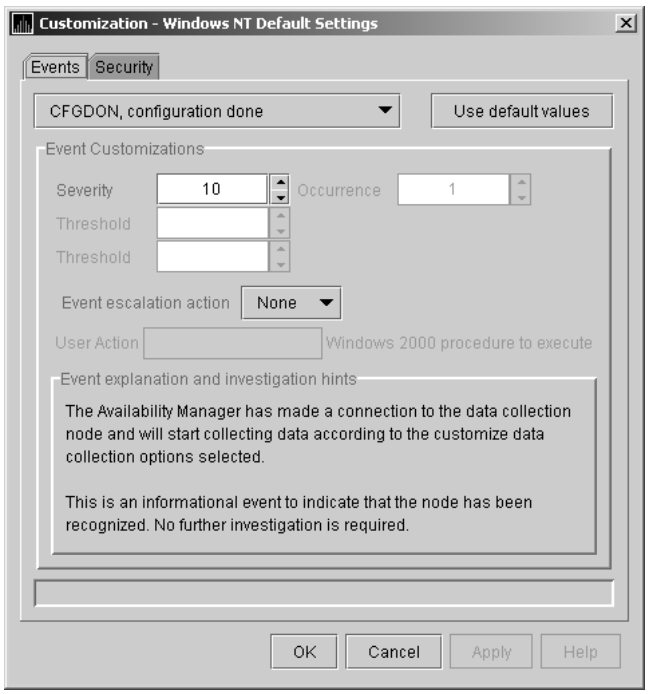
Figure 7–2 Application Customization Page



7.1.1.2 Windows Operating System of Customization

When you choose **Customize Windows NT**, the Availability Manager displays the page shown in Figure 7–3.

Figure 7–3 Windows Operating System Customization Page

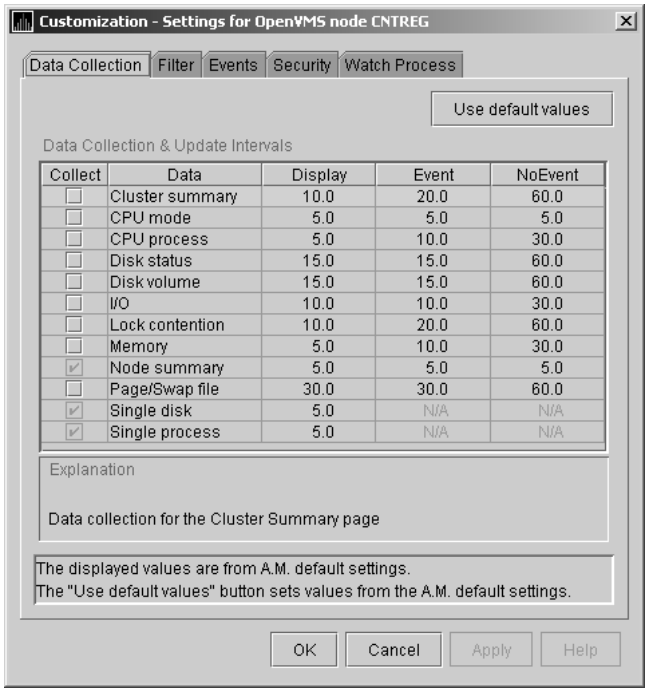


The default page displayed is the Events Customization page. Instructions for using this page are in Section 7.6.1. The other tab displayed is the Security Customization page, which is explained in Section 7.7.1.2.

7.1.1.3 OpenVMS Operating System Customization

When you choose **Customize OpenVMS**, the Availability Manager displays the page shown in Figure 7–4, which contains tabs for the last five types of customizations listed in Table 7–1.

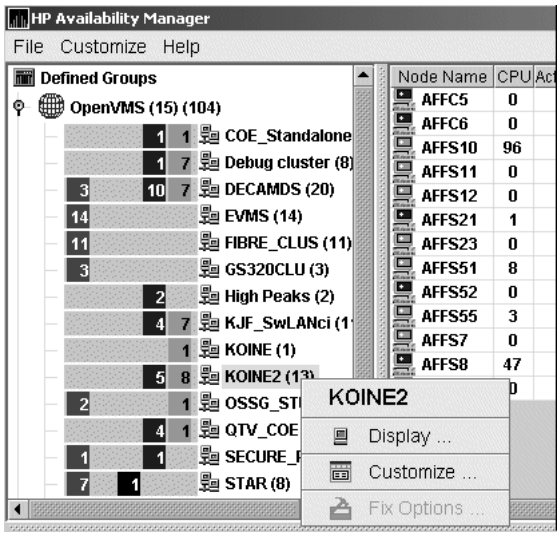
Figure 7–4 OpenVMS Operating System Customization Page



7.1.2 Group Customization Level

To perform customizations at the group level, right-click a group name in the Application window. The Availability Manager displays a small menu similar to the one shown in Figure 7–5.

Figure 7–5 Group Customization Menu



When you choose **Customize**, the Availability Manager displays the page shown in Figure 7–4.

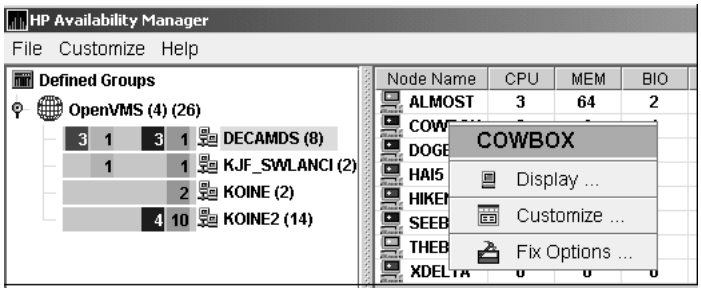
7.1.3 Node Customization Level

To customize a specific node, right-click a node name in the Node pane of the Application window (see Figure 1–1). The Availability Manager displays the popup menu shown in Figure 7–6.

Note

You can customize nodes in any state, not just those displayed in red or green (colors that indicate that the security check has been successful for these nodes).

Figure 7–6 Node Customization Menu



When you choose **Customize**, the Availability Manager displays a customization page similar to the one shown in Figure 7–4.

Number of Nodes Affected by Customization

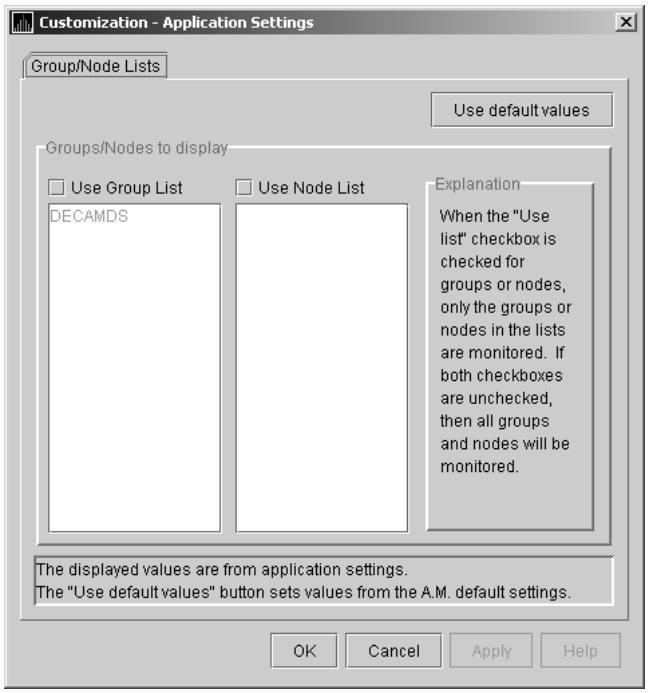
Depending on which customization menu you use and your choice of menu items, your customizations can affect one or more nodes, as indicated in the following table.

Nodes Affected	Action
All nodes	Choose **Customize Application...** on the menu shown in Figure 7–1.
All Windows nodes	Choose **Customize Windows NT...** on the menu shown in Figure 7–1.
All OpenVMS nodes	Choose **Customize OpenVMS...** on the menu shown in Figure 7–1.
A group of nodes	Choose **Customize...** on the popup menu shown in Figure 7–5. The customization options you choose affect only the group of nodes that you select.
One node	Choose **Customize...** on the popup menu shown in Figure 7–6. The customization options you choose affect only the node that you select.

7.2 Specifying Groups or Individual Nodes to Monitor

When you choose **Customize Application** on the Application window Customize menu (Figure 7–1), the Availability Manager displays a **Group/Node Lists** tab (Figure 7–7).

Figure 7–7 Group/Node Customization Page



You have the following choices:

- Check **Use Group List**.

First check the box preceding Use Group List. Then, using the correct case, enter the names of the groups of nodes you want to monitor.

- Check **Use Node List**.

  First check the box preceding Use Node List. Then enter the names of individual nodes you want to monitor. (The names are case-sensitive, so be sure to enter the correct case.)

- Check both boxes.

  If you check both boxes, you can enter the names of groups of nodes and also individual nodes you want to monitor. (If you enter the name of an individual node, the Availability Manager displays the name of the group that node is in, but only one node in that group.)

- Check neither box.

  Do not enter any groups or nodes; all groups and all nodes will be monitored.

If you decide to return to the default (Use Group List: DECAMDS) or to enter names again, click **Use default values**.

After you enter a list of nodes or groups of nodes, click one of the following buttons at the bottom of the page:

Option	Description
OK	Accepts the choice of names you have entered and exits the page.
Cancel	Cancels the choice of names and does not exit the page.
Apply	Accepts the choice of names you have entered but does not exit the page.

To put the list into effect, exit the Availability Manager and restart it.

7.3 Changing the Group Membership of a Node

Each Availability Manager Data Collector node is assigned to the DECAMDS group by default. The following sections explain how to change the group membership of nodes.

Note

You need to place nodes belonging to the same cluster in the same group. If such nodes are placed in different groups, some of the data collected might be misleading.

7.3.1 Changing the Group of an OpenVMS Node

You need to edit a logical on each Data Collector node to change the group for that node. To do this, follow these steps:

1. Assign a unique name of up to 15 alphanumeric characters to the AMDS$GROUP_NAME logical name in the AMDS$AM_SYSTEM:AMDS$AM_LOGICALS.COM file. For example:

```
$ AMDS$DEF AMDS$GROUP_NAME FINANCE ! Group FINANCE; OpenVMS Cluster alias
```

2. Apply the logical name by restarting the Data Collector:

```
$ @SYS$STARTUP:AMDS$AM_STARTUP RESTART
```

Note

The configuration files for DECamds and the Availability Manager are separate; only one set is used, depending on which startup command procedure you use to start the driver.

For further explanations of the configuration files set up for both DECamds and the Availability Manager, refer to the *HP Availability Manager Installation Instructions for OpenVMS Alpha Systems*

7.3.2 Changing the Group of a Windows Node

You need to edit the Registry to change the group of a Windows node. To edit the Registry, follow these steps:

1. Click the Windows **Start** button. On the menu displayed, first click **Programs**, then **Accessories**, and then **Command Prompt**.
2. Type REGEDIT after the angle prompt (>).

   The system displays a screen for the Registry Editor, with a list of entries under My Computer.
3. On the list displayed, expand th **HKEY_LOCAL_MACHINE** entry.
4. Double-click **SYSTEM**.
5. Click **CurrentControlSet**.
6. Click **Services**.
7. Click **damdrvr**.
8. Click **Parameters**.
9. Double-click **Group Name**. Then type a new group name of 15 alphanumeric characters or fewer, and click **OK** to make the change.
10. On the Control Panel, click **Services**, and then click **Stop** for “PerfServ.”
11. Again on the Control Panel, click **Devices**, and then click **Stop** for “damdrvr.”
12. First restart **damdrvr** under “Devices,” and then restart **PerfServ** under “Services.”

    This step completes the change of groups for this node.

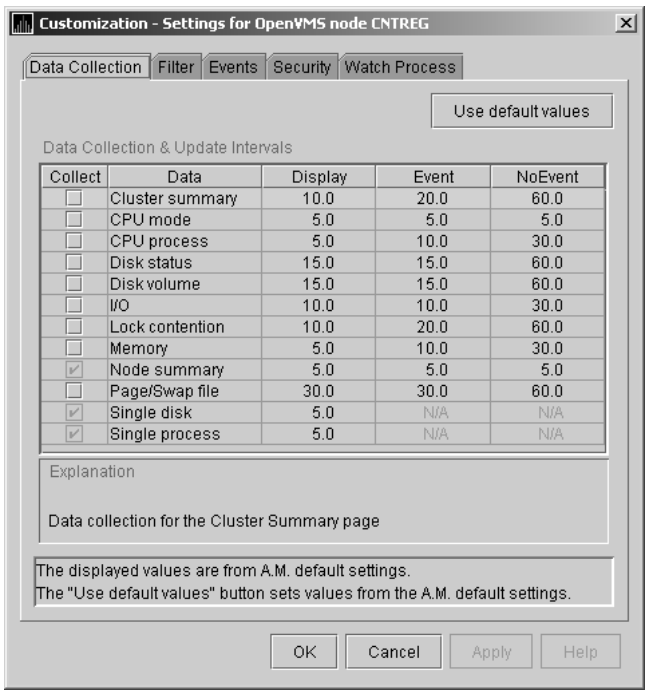
7.4 Customizing OpenVMS Data Collection

Note

Before you start this section, be sure to read the explanation of data collection, events, thresholds, and occurrences in Chapter 1.

When you choose the **Customize OpenVMS** menu option in the Application window (see Figure 7–1), by default the Availability Manager displays the OpenVMS Data Collection Customization page, shown in Figure 7–8, where you can select types of data you want to collect for all of the OpenVMS nodes you are currently monitoring. You can also change the default Availability Manager intervals at which data is collected or updated.

Figure 7–8 OpenVMS Data Collection Customization Page



You can also customize data collection at the group and node levels (see Section 7.1). Keep in mind that the customizations that you make at the various levels override the ones set at the previous level (see Table 7–1).

Table 7–2 identifies the page where each type of data collected appears and indicates whether or not that type of data collection is a default.

Table 7–2 Data Collection Choices

Data Collected	Default	Page Where Data Is Displayed
Cluster summary data	No	Cluster Summary page
CPU mode data	No	CPU Modes Summary page
CPU summary data	No	CPU Process States page
Disk status data	No	Disk Status Summary page
Disk volume data	No	Disk Volume Summary page
I/O data	No	I/O Summary page
Lock contention data	No	Lock Contention page
Memory data	No	Memory Summary page

(continued on next page)

Table 7–2 (Cont.) Data Collection Choices

Data Collected	Default	Page Where Data Is Displayed
Node summary data	Yes	Node pane, Node Summary page, and the top pane of the CPU, Memory, and I/O pages
Page/Swap file data	No	I/O Page Faults page
Single disk data	Yes[1]	Single Disk Summary page
Single process data	Yes[2]	Data collection for the Process Information page

[1]Data is collected by default when you open a Single Disk Summary page.

[2]Data is collected by default when you open a Single Process page.

You can choose additional types of data to collect by selecting the Collect check box on the Data Collection Customization page of the **Customize OpenVMS...** menu (Figure 7–4). A check mark indicates that data will be collected at the intervals described in Table 7–3.

Table 7–3 Data Collection Intervals

Interval (in seconds)	Description
Display	How often the data is collected when its corresponding display is active.
Event	How often the data is collected when its corresponding display is not active and when events are active.
NoEvent	How often the data is collected when its corresponding display is not active and when events are not active.

You can enter a different collection interval by selecting a row of data and clicking a value. Then delete the old value and enter a new one.

If you change your mind and decide to return to the default collection interval, select one or more rows of data items: then click **Use default values**. The system displays the default values for all the collection intervals.

When you finish customizing your data collection, click one of the following buttons at the bottom of the page:

Option	Description
OK	To confirm any changes you have made and exit the page.
Cancel	To cancel any changes you have made and exit the page.
Apply	To confirm and apply any changes you have made and not exit the page.

7.5 Customizing OpenVMS Data Filters

When you choose the **Customize OpenVMS...** menu option and click the **Filter** tab, the Availability Manager displays a page that allows you to display specific kinds of data by selecting check boxes. The types of data filters available are as follows:

- CPU Filters

- Disk Status
- Disk Volume
- I/O
- Lock Contention
- Memory Filters
- Page/Swap File

Filters can vary depending on the type of data collected. For example, filters might be process states or a variety of rates and counts. The following sections describe data filters that are available for various types of data collection.

You can also customize filters at the group and node levels (see Section 7.1). Keep in mind that the customizations that you make at the various levels override the ones set at the previous level (see Table 7–1). The note on each filter page reminds you that: "Changes to these settings will override the ... settings."

If you change your mind and decide to return to filter values set at a previous level, click **Use default values**.

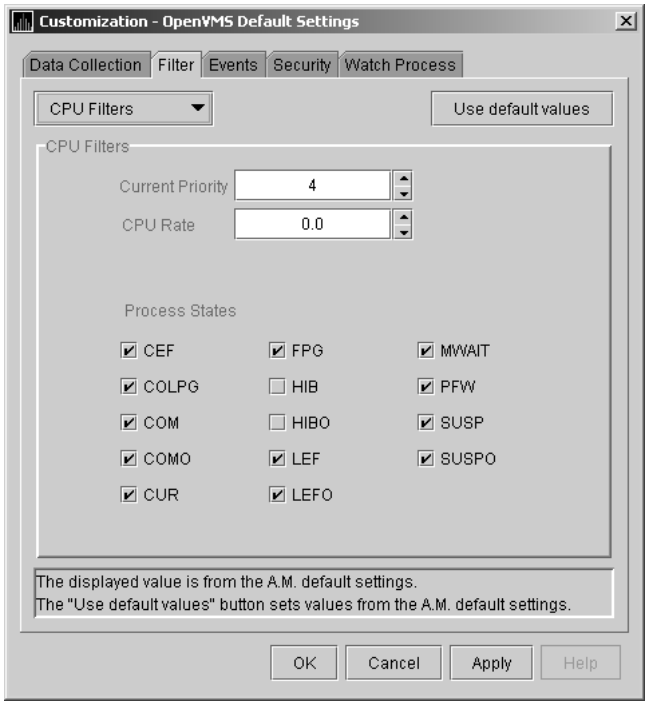
When you finish modifying a filters page, click one of the following buttons at the bottom of the page:

Option	Description
OK	To confirm any changes you have made and exit the page.
Cancel	To cancel any changes you have made and exit the page.
Apply	To confirm and apply any changes you have made and continue to display the page.

7.5.1 OpenVMS CPU Filters

When you click **CPU Filters** on the Filter page, the Availability Manager displays the OpenVMS CPU Filters page (Figure 7–9).

Figure 7–9 OpenVMS CPU Filters Page



This page allows you to change and select values that are displayed on the OpenVMS CPU Process States page (Figure 3–8).

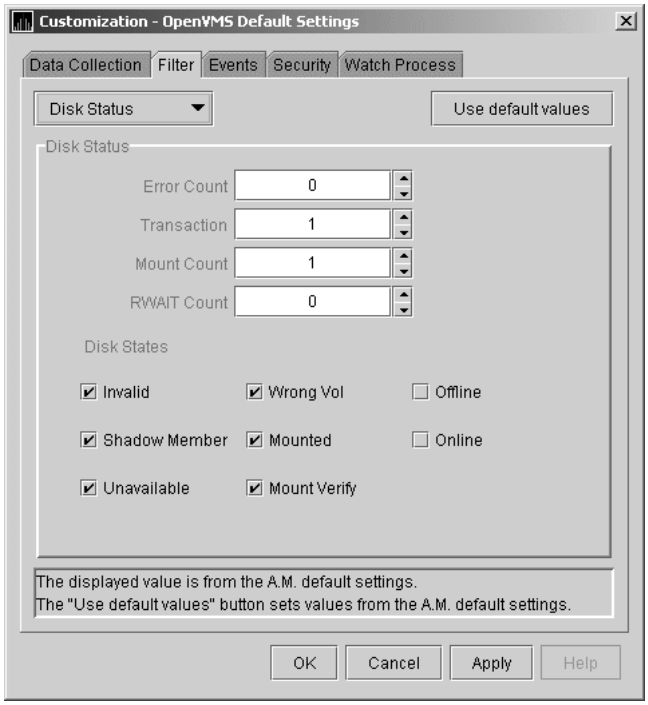
You can change the current priority and rate of a process. By default, a process is displayed only if it has a Current Priority of 4 or more. Click the up or down arrow to increase or decrease the priority value by one. The default CPU rate is 0.0, which means that processes with any CPU rate used will be displayed. To limit the number of processes displayed, you can click the up or down arrow to increase or decrease the CPU rate by .5 each time you click.

The OpenVMS CPU Filters page also allows you to select the states of the processes that you want to display on the CPU Process States page. Select the check box for each state you want to display. (Process states are described in Appendix B.)

7.5.2 OpenVMS Disk Status Filters

When you click **Disk Status** on the Filter page, the Availability Manager displays the OpenVMS Disk Status Filters page (Figure 7–10).

Figure 7–10 OpenVMS Disk Status Filters Page



The OpenVMS Disk Status Summary page (Figure 3–14) displays the values you set on this filters page.

This filters page lets you change the following default values:

Data	Description
Error Count	The number of errors generated by the disk (a quick indicator of device problems).
Transaction	The number of in-progress file system operations for the disk.
Mount Count	The number of nodes that have the specified disk mounted.
RWAIT Count	An indicator that a system I/O operation is stalled, usually during normal connection failure recovery or volume processing of host-based shadowing.

This filters page also lets you check the states of the disks you want to display, as described in the following table:

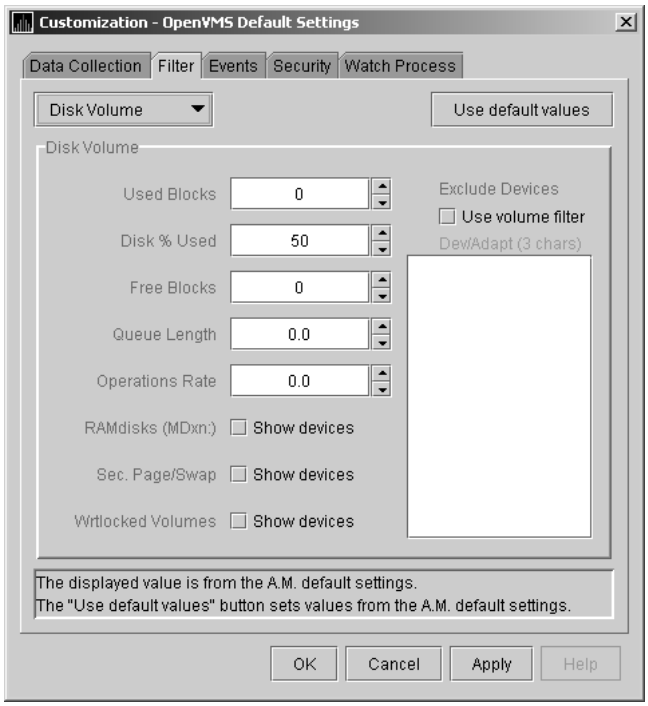
Disk State	Description
Invalid	Disk is in an invalid state (Mount Verify Timeout is likely).
Shadow Member	Disk is a member of a shadow set.
Unavailable	Disk is set to unavailable.
Wrong Vol	Disk was mounted with the wrong volume name.
Mounted	Disk is logically mounted by a MOUNT command or a service call.
Mount Verify	Disk is waiting for a mount verification.
Offline	Disk is no longer physically mounted in device drive.

Disk State	Description
Online	Disk is physically mounted in device drive.

7.5.3 OpenVMS Disk Volume Filters

When you click **Disk Volume** on the Filter page, the Availability Manager displays the OpenVMS Disk Volume Filters page (Figure 7–11).

Figure 7–11 OpenVMS Disk Volume Filters Page



The OpenVMS Disk Volume Filters page allows you to change the values for the following data:

Data	Description
Used Blocks	The number of volume blocks in use.
Disk % Used	The percentage of the number of volume blocks in use in relation to the total volume blocks available.
Free Blocks	The number of blocks of volume space available for new data.
Queue Length	Current length of I/O queue for a volume.
Operations Rate	The rate at which the operations count to the volume has changed since the last sampling. The rate measures the amount of activity on a volume. The optimal load is device specific.

You can also change options for the following to be on (checked) or off (unchecked):

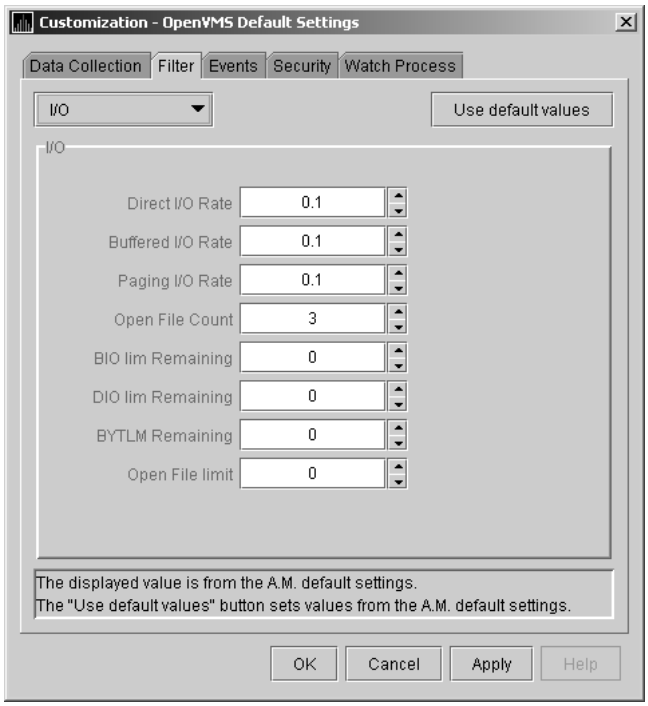
- RAMdisks (MDxn:): Show devices
- Wrtlocked Volumes: Show devices
- Sec. Page/Swap: Show devices

- Filtered Volumes: Use filter

7.5.4 OpenVMS I/O Filters

When you click **I/O** on the Filter page, the Availability Manager displays the OpenVMS I/O Filters page (Figure 7–12).

Figure 7–12 OpenVMS I/O Filters Page



The OpenVMS I/O Summary page (Figure 3–12) displays the values you set on this filters page.

This filters page allows you to change values for the following data:

Data	Description
Direct I/O Rate	The rate of direct I/O transfers. Direct I/O is the average percentage of time that the process waits for data to be read from or written to a disk or tape. The possible state is DIO. Direct I/O is usually disk or tape I/O.
Buffered I/O Rate	The rate of buffered I/O transfers. Buffered I/O is the average percentage of time that the process waits for data to be read from or written to a slower device such as a terminal, line printer, mailbox. The possible state is BIO. Buffered I/O is usually terminal, printer I/O, or network traffic.
Paging I/O Rate	The rate of read attempts necessary to satisfy page faults (also known as Page Read I/O or the Hard Fault Rate).
Open File Count	The number of open files.
BIO lim Remaining	The number of remaining buffered I/O operations available before the process reaches its quota. BIOLM quota is the maximum number of buffered I/O operations a process can have outstanding at one time.

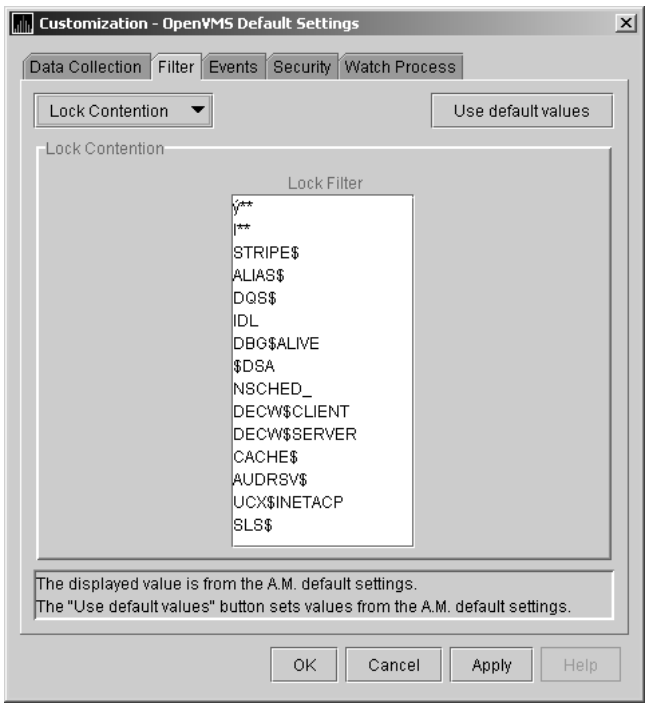
Data	Description
DIO lim Remaining	The number of remaining direct I/O limit operations available before the process reaches its quota. DIOLM quota is the maximum number of direct I/O operations a process can have outstanding at one time.
BYTLM Remaining	The number of buffered I/O bytes available before the process reaches its quota. BYTLM is the maximum number of bytes of nonpaged system dynamic memory that a process can claim at one time.
Open File limit	The number of additional files the process can open before reaching its quota. FILLM quota is the maximum number of files that can be opened simultaneously by the process, including active network logical links.

7.5.5 OpenVMS Lock Contention Filters

The OpenVMS Lock Contention Filters page allows you to remove (filter out) resource names from the Lock Contention page (Figure 3–19).

When you click **Lock Contention** on the Filter page, the Availability Manager displays the OpenVMS Lock Contention Filters page (Figure 7–13).

Figure 7–13 OpenVMS Lock Contention Filters Page

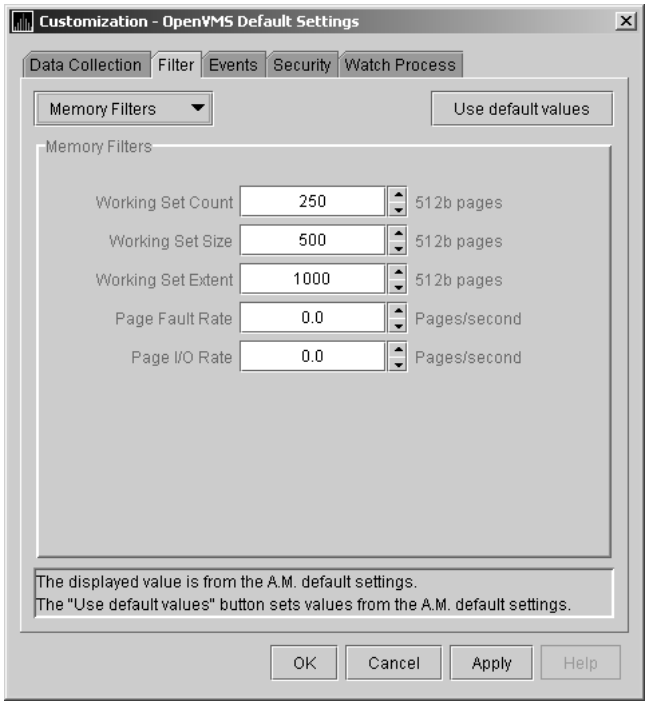


Each entry on the Lock Contention Filters page is a resource name or part of a resource name that you want to filter out. For example, the STRIPE$ entry filters out any value that starts with the characters STRIPE$. To redisplay original entries, click **Use default values**.

7.5.6 OpenVMS Memory Filters

When you click **Memory Filters** on the Filter page, the Availability Manager displays the OpenVMS Memory Filters page (Figure 7–14).

Figure 7–14 OpenVMS Memory Filters Page



The OpenVMS Memory page (Figure 3–10) displays the values on this filters page.

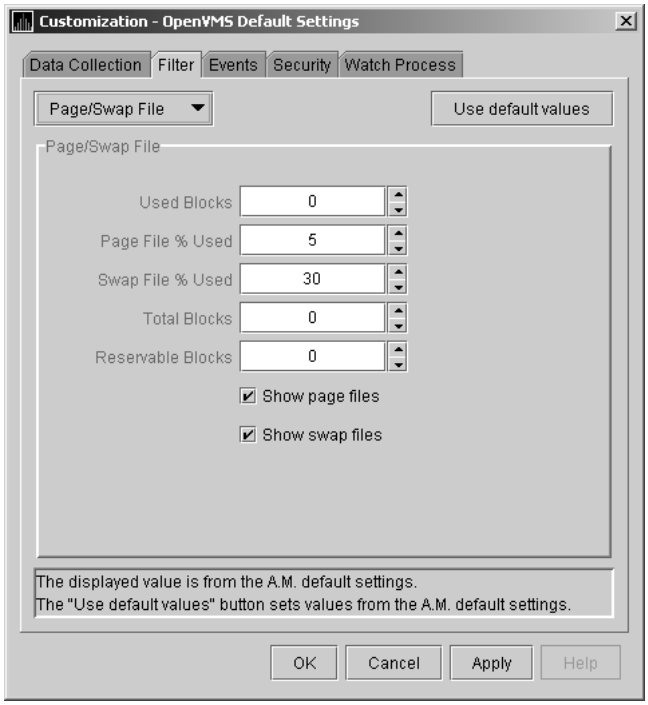
The OpenVMS Memory Filters page allows you to change values for the following data:

Data	Description
Working Set Count	The number of physical pages or pagelets of memory that the process is using.
Working Set Size	The number of pages or pagelets of memory the process is allowed to use. The operating system periodically adjusts this value based on an analysis of page faults relative to CPU time used. An increase in this value in large units indicates a process is receiving a lot of page faults and its memory allocation is increasing.
Working Set Extent	The number of pages or pagelets of memory in the process's WSEXTENT quota as defined in the user authorization file (UAF). The number of pages or pagelets will not exceed the value of the system parameter WSMAX.
Page Fault Rate	The number of page faults per second for the process.
Page I/O Rate	The rate of read attempts necessary to satisfy page faults (also known as page read I/O or the hard fault rate).

7.5.7 OpenVMS Page/Swap File Filters

When you click **Page/Swap File** on the Filter page, the Availability Manager displays the OpenVMS Page/Swap File Filters page (Figure 7–15).

Figure 7–15 OpenVMS Page/Swap File Filters Page



The OpenVMS I/O Summary page (Figure 3–12) displays the values that you set on this filters page.

This filters page allows you to change values for the following data:

Data	Description
Used Blocks	The number of used blocks within the file.
Page File % Used	The percentage of the blocks from the page file that have been used.
Swap File % Used	The percentage of the blocks from the swap file that have been used.
Total Blocks	The total number of blocks in paging and swapping files.
Reservable Blocks	Number of reservable blocks in each paging and swapping file currently installed. Reservable blocks can be logically claimed by a process for a future physical allocation. A negative value indicates that the file might be overcommitted. Note that a negative value is not an immediate concern but indicates that the file might become overcommitted if physical memory becomes scarce. Note: Reservable blocks are not used in more recent versions of OpenVMS.

You can also select (turn on) or clear (turn off) the following options:

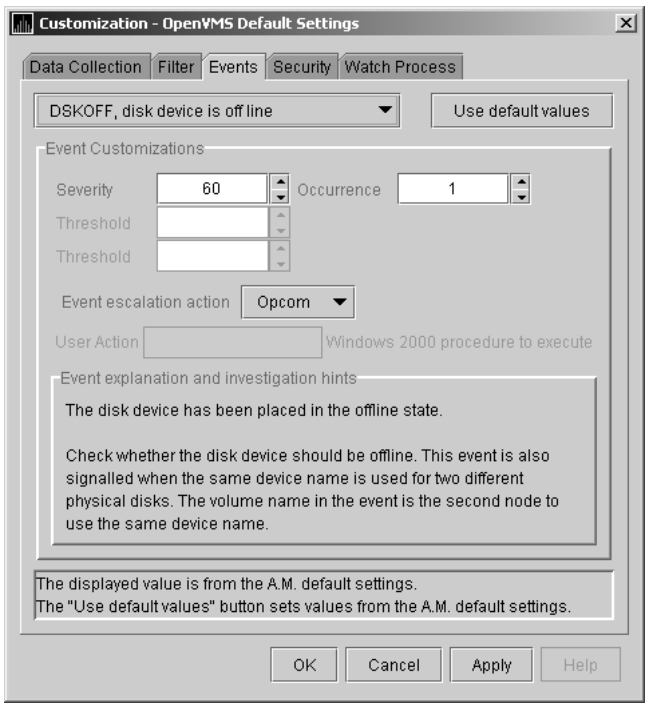
- Show page files
- Show swap files

7.6 Customizing Events and User Notification of Events

You can customize a number of characteristics of the events that are displayed in the Event pane of the Application window (Figure 1–1). You can also use customization options to notify users when specific events occur.

When you choose the **Customize OpenVMS...** or **Customize Windows NT...** option from the Application window's **Customize** menu, the Availability Manager displays a tabbed page similar to the one shown in Figure 7–16.

Figure 7–16 Events Customization Page



On OpenVMS systems, you can also customize events at the group and node levels. Keep in mind that, for a group, the events that you customize at the group level override the events customized at the previous level (see Table 7–1).

7.6.1 Customizing Events

You can change the values for any data that is available (not dimmed) on this page.

The following table describes the data you can change:

Data	Description
Severity	Controls the severity level at which events are displayed in the Event pane. By default, all events are displayed. Increasing this value reduces the number of event messages in the Event pane and can improve perceived response time.

Data	Description
Occurrence	Each Availability Manager event is assigned an **occurrence** value, that is, the number of consecutive data samples that must exceed the event threshold before the event is signaled. By default, events have low occurrence values. However, you might find that a certain event indicates a problem only when it occurs repeatedly over an extended period. You can change the occurrence value assigned to that event so that the Availability Manager signals it only when necessary. For example, suppose page fault spikes are common in your environment, and the Availability Manager frequently signals intermittent *HITTLP, total page fault rate is high* events. You could change the event's occurrence value to 3, so that the total page fault rate must exceed the threshold for three consecutive collection intervals before being signaled to the event log. To avoid displaying insignificant events, you can customize an event so that the Availability Manager signals it only when it occurs continuously.
Threshold	Most events are checked against only one threshold; however, some events have dual thresholds, where the event is triggered if either one is true. For example, for the *LOVLSP, node disk volume free space is low* event, the Availability Manager checks both of the following thresholds: • Number of blocks remaining • Percentage of total blocks remaining
Event escalation action	You can enter one of the following values: • None: Take no action if this event occurs. • Opcom: **Not yet implemented.** • User: If the event occurs, the Availability Manager refers to the "User Action" field to determine what action to take.
User Action	When the "Event escalation action" field is set to User, User Action is no longer dimmed. You can enter the name of a procedure to be executed if the event displayed at the top of the page occurs. To use this field, see the instructions in Section 7.6.2.

The "Event explanation and investigation hints" section of the Event Customization page, which is not customizable, includes a description of the event displayed and a suggestion for how to correct any problems that the event signals.

7.6.2 Entering a User Action

Note

OpenVMS and Windows execute the User Action procedure somewhat differently, as explained in the following paragraphs.

The following notes pertain to writing and executing User Action commands or command procedures. These notes apply to User Actions on both OpenVMS and Windows systems.

- The procedure that you specify as the User Action will be executed in the following manner:
  - It will be issued to the operating system that is running the Availability Manager Data Analyzer.
  - It will be issued as a process separate from the one running the Availability Manager to avoid affecting its operation.
  - It will be run under the same account as the one running the Availability Manager Data Analyzer.
- User Actions are intended to execute procedures that do not require interactive displays or user input.
- You can enter User Actions for events on either a systemwide basis or a per-node basis:
  - On a systemwide basis, the User Action is issued for an event that occurs on any node.
  - On a per-node basis, the User Action is issued for an event that occurs only on a specific node.
- If event logging is enabled, the Availability Manager writes events to the event log file (called AnalyzerEvents.log by default on OpenVMS systems and AvailManEvents.log by default on Windows systems). A status line matching the original line indicates whether the User Action was successfully issued. For example:

  ```
  AMGR/KOINE -- 13-Apr-2001 15:33:02.531 --<0,CFGDON>KOINE configuration done
  AMGR/KOINE -- 13-Apr-2001 15:33:02.531 --<0,CFGDON>KOINE configuration done
  (User Action issued for this event on the client O/S)
  ```

  Other events might appear between the first logging and the status line. The log file does *not* indicate whether the User Action executed successfully. You must obtain the execution status from the operating system, for example, the OpenVMS batch procedure log.
- The User Action functionality might be enhanced in a future release of the Availability Manager, but backward compatibility is not guaranteed for the format of User Action procedure strings or for the method of executing the procedures on a particular operating system.

7.6.2.1 Executing a Procedure on an OpenVMS System

The User Action procedure and arguments are passed as string values to the DCL command interpreter as follows:

SUBMIT/NOPRINTER/LOG *user_action_procedure arg_1 arg_2 arg_3 arg_4*

where:

- The first command is the DCL command SUBMIT with associated qualifiers.
- *user_action_procedure* is a valid OpenVMS file name.

  Enter the name of the procedure you want OpenVMS to execute using the following format:

  disk:[directory]filename.COM

  where:
  - *disk* is the name of the disk where the procedure resides.

- *directory* is the name of the directory where the procedure resides.
- *filename*.COM is the file name of the command procedure you want OpenVMS to execute. The file name must follow OpenVMS file-naming conventions.

The file you submit must contain one or more DCL command statements that form a valid OpenVMS command procedure.

- The arguments correspond to the following data:

Argument	Description
arg_1	Node name of the node that generated the event.
arg_2	Date and time that the event was generated.
arg_3	Name of the event.
arg_4	Description of the event.

The Availability Manager does not interpret the string contents. You can supply any content in the User Action procedure that DCL accepts in the OpenVMS environment for the user account running the Data Analyzer. However, if you include arguments in the User Action procedure, they might displace or overwrite arguments supplied by the Availability Manager.

A suitable batch queue must be available on the Data Analyzer computer to be the target of the SUBMIT command. See the *HP OpenVMS DCL Dictionary* for the SUBMIT, INITIALIZE/QUEUE, and START/QUEUE commands for use of batch queues and the queue manager.

The following is an example of a DCL command procedure:

```
$ if (p3.eqs."DSKOFF").and.(p1.eqs."PAYROL")
$ then
$   mail/subject="''p2' ''p3' ''p4'" urgent_instructions.txt
call_center,finance,adams
$ else
$   mail/subject="''p2' ''p3' ''p4'" instructions.txt call_center
$ endif
```

The p*n* numbers in the DCL procedure correspond in type, number, and position to the arguments in the preceding table.

You might use a procedure like this one to notify several groups if the payroll disk goes off line, or to notify the call center if any other event occurs.

7.6.2.2 Executing a Procedure on a Windows System

The user action procedure and arguments are passed as string values to the Windows command interpreter as follows:

"AT *time* CMD/C *user_action_procedure arg_1 arg_2 arg_3 arg_4*"

where:

- AT is the Windows command that schedules commands and programs at a specified time and date.
- The *time* substring is a short period of time— aproximately 2 minutes—in the future so that the AT utility processes the user action procedure today rather than tomorrow. This is necessary because the AT utility cannot execute a procedure “now” rather than at an explicitly stated time.

- *user_action_procedure* is a Windows command or valid file name. The file must contain one or more Windows command statements to form a valid command procedure. (See the example in this section.)

  Enter the name of the procedure you want Windows to execute using the following format:

  device:\(*directory**filename*.BAT

  where:

  – *device* is the disk on which the procedure is located.

  – *directory* is the folder in which the procedure is located.

  – *filename.*BAT is the name of the command file to be executed.

  Notes

  The file name must follow Windows file-naming conventions. However, due to the processing of spaces in the Java JRE, HP recommends that you do not use spaces in a path or file name.

  HP recommends that you use a batch file to process and call procedures and applications.

- The arguments are listed in the table in Section 7.6.2.1.

The Availability Manager does not interpret the string contents. You can supply any content in the string that the Windows command-line interpreter accepts for the user account running the Data Analyzer. However, if you include arguments in the User Action procedure, they might displace or overwrite arguments supplied by the Availability Manager.

You cannot specify positional command-line switches or arguments to the AT command, although you can include switches in the User Action procedure substring as qualifiers to the user-supplied command. This is a limitation of both the Windows command-line interpreter and the way the entire string is passed from the Availability Manager to Windows.

The Schedule service must be running on the Data Analyzer computer in order to use the AT command. However, the Schedule service does not run by default. To start the Schedule service, see the Windows documentation for instructions in the use of the CONTROL PANEL->SERVICES->SCHEDULE->[startup button].

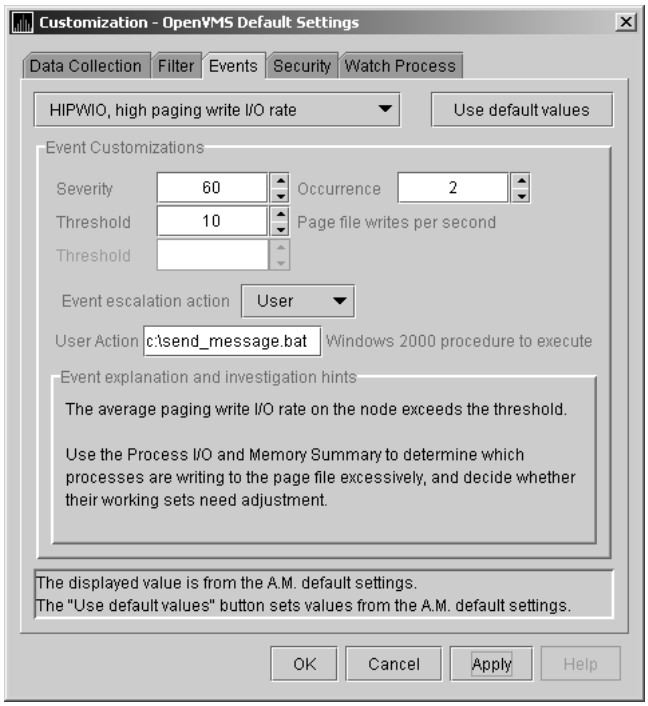
Windows Example

To set up a user action, follow these steps:

1. Select an event on the Events Customization page, for example, HIBIOR (see Figure 7–17).
2. Change the Event escalation action to User.
3. Enter the name of the program to run, for example:

   ```
   c:\send_message.bat
   ```

Figure 7–17 User Action Example

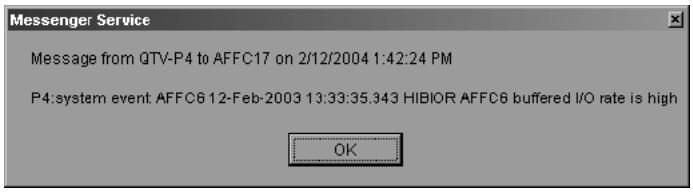


The command line parameters are automatically added when Availability Manager passes the command to the command processor.

The contents of "send_message.bat" are the following:

```
net send affc17 "P4:system event: %1 %2 %3 %4"
```

On the target node, AFFC17, a message similar to the following is displayed:



You can now apply the User Action to one node, all nodes, or a group of nodes, as explained in Section 7.6.2.

7.7 Customizing Security Features

The following sections explain how to change these security features:

- Data Analyzer passwords for OpenVMS and Windows Data Collector nodes
- OpenVMS Data Collector security triplets
- A Windows Data Collector password

Note

OpenVMS Data Collector nodes can have more than one password: each password is part of a security triplet. (Windows nodes allow you to have

only one password per node.)

7.7.1 Changing Data Analyzer Passwords

You can change the passwords that the Windows Data Analyzer uses for OpenVMS Data Collector nodes and for Windows Data Collector nodes. The following sections explain how to perform both actions.

7.7.1.1 Changing a Data Analyzer Password for an OpenVMS Data Collector Node

When you click **Customize OpenVMS...** on the **Customize** menu of the Application window, the Availability Manager displays a default customization page. On it is a tab marked **Security**, which, if you select it, displays the OpenVMS Security Customization page shown in Figure 7–18.

Figure 7–18 OpenVMS Security Customization Page

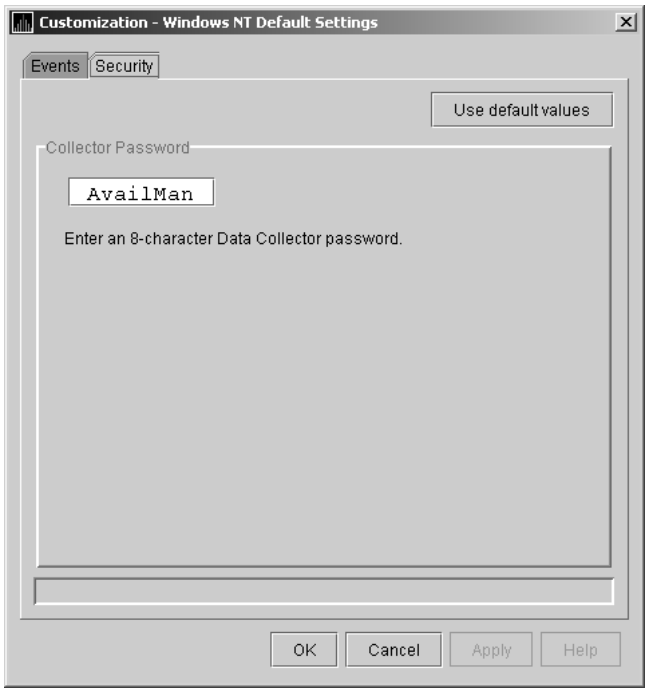
To change the default password for the Data Analyzer to use to access OpenVMS Data Collector nodes, enter a password of exactly 8 uppercase alphanumeric characters. The Availability Manager will use this password to access OpenVMS Data Collector nodes. This password must match the password that is part of the OpenVMS Data Collector security triplet (see Section 7.7.2).

When you are satisfied with your password, click **OK**. Exit the Availability Manager, and restart the application for the password to take effect.

7.7.1.2 Changing a Data Analyzer Password for a Windows Data Collector Node

When you click **Customize Windows NT...** on the **Customize** menu of the Application window, the Availability Manager displays a Windows Security Customization page (Figure 7–19).

Figure 7–19 Windows Security Customization Page



To change the default password for the Data Analyzer to use to access Windows Data Collector nodes, enter a password of exactly 8 alphanumeric characters. Note that this password is case sensitive; any time you type it, you must use the original capitalization.

This password must also match the password for the Windows Data Collector node that you want to access. (See Section 7.7.3 for instructions for changing that password.)

When you are satisfied with your password, click **OK**. Exit and restart the Availability Manager for the password to take effect. affc

7.7.2 Changing Security Triplets on OpenVMS Data Collector Nodes

To change security triplets on an OpenVMS Data Collector node, you must edit the AMDS$DRIVER_ACCESS.DAT file, which is installed on all Data Collector nodes. The following sections explain what a security triplet is, how the Availability Manager uses it, and how to change it.

7.7.2.1 Understanding OpenVMS Security Triplets

A security triplet determines which nodes can access system data from an OpenVMS Data Collector node. The AMDS$DRIVER_ACCESS.DAT file on OpenVMS Data Collector nodes lists security triplets.

On OpenVMS Data Collector nodes, the AMDS$AM_CONFIG logical translates to the location of the default security file, AMDS$DRIVER_ACCESS.DAT. This file is installed on all OpenVMS Data Collector nodes.

A security triplet is a three-part record whose fields are separated by backslashes (\ ). A triplet consists of the following fields:

- A network address (hardware address or wildcard character)
- An 8-character alphanumeric password

  The password is not case sensitive (so the passwords “testtest” and “TESTTEST” are considered to be the same).
- A read, write, or control (R, W, or C) access verification code

The exclamation point (!) is a comment delimiter; any characters to the right of the comment delimiter are ignored.

Example

All Data Collector nodes in group FINANCE have the following AMDS$DRIVER_ACCESS.DAT file:

```
*\FINGROUP\R   ! Let anyone with FINGROUP password read
               !
2.1\DEVGROUP\W ! Let only DECnet node 2.1 with
               ! DEVGROUP password perform fixes (writes)
```

7.7.2.2 How to Change a Security Triplet

Note

The configuration files for DECamds and the Availability Manager are separate; only one set is used, depending on which startup command procedure you use to start the driver.

See *Installing the Availability Manager on OpenVMS Alpha Systems and Running DECamds and the Availability Manager Concurrently* for a further explanation of the configuration file setup for both DECamds and the Availability Manager.

On each Data Collector node on which you want to change security, you must edit the AMDS$DRIVER_ACCESS.DAT file. The data in the AMDS$DRIVER_ACCESS.DAT file is set up as follows:

```
Network address\password\access
```

Use a backslash character (\ ) to separate the three fields.

To edit the AMDS$DRIVER_ACCESS.DAT file, follow these steps:

1. Edit the network address.

   The network address can be either of the following:

   - Hardware address

     The hardware address field is the physical hardware address in the LAN device chip. It is used if you have multiple LAN devices or are running the hp DECnet-Plus for OpenVMS networking software on the system (not the hp DECnet Phase IV for OpenVMS networking software).

     For devices provided by HP, the hardware address is in the form 08-00-2B-*xx-xx-xx*, where the 08-00-2B portion is HP’s valid range of LAN addresses as defined by the IEEE 802 standards, and the *xx-xx-xx* portion is chip specific.

To determine the value of the hardware address on a node, use the OpenVMS System Dump Analyzer (SDA) as follows:

```
$ ANALYZE/SYSTEM
SDA> SHOW LAN
```

These commands display a list of available devices. Choose the template device of the LAN device you will be using, and then enter the following command:

```
SDA> SHOW LAN/DEVICE=xxA0
```

- Wildcard address

  The wildcard character (*) allows any incoming triplet with a matching password field to access the Data Collector node. Use the wildcard character to allow read access and to run the console application from any node in your network.

  Because the Data Analyzer does not use this field, use the wildcard character in this field in the AMDS$CONSOLE_ACCESS.DAT file.

  Caution: Use of the wildcard character for write-access security triplets enables any person using that node to perform system-altering fixes.

2. Edit the password field.

   The password field **must be** an 8-byte alphanumeric field. The Availability Manager forces upper-case on the password, so "aaaaaaaa" and "AAAAAAAA" are essentially the same password to the Data Collector.

   The password field gives you a second level of protection when you want to use the wildcard address denotation to allow multiple modes of access to your monitored system.

3. Enter R, W, or C as an access code:

   - R means READONLY access to the Data Analyzer.
   - W means READ/WRITE access to the Data Analyzer. (WRITE implies READ.)
   - C means CONTROL access to the Data Analyzer. CONTROL allows you to manipulate objects from which data are derived. (CONTROL implies both WRITE and READ.)

The following security triplets are all valid; an explanation follows the exclamation point (!).

```
*\1decamds\r   ! Anyone with password "1decamds" can monitor
*\1decamds\w   ! Anyone with password "1decamds" can monitor or write
2.1\1decamds\r ! Only node 2.1 with password "1decamds" can monitor
2.1\1decamds\w ! Only node 2.1 with password "1decamds" can monitor and write
08-00-2b-03-23-cd\1decamds\w ! Allows a particular hardware address to write
08-00-2b-03-23-cd\1decamds\r ! Allows a particular hardware address to read node
```

OpenVMS Data Collector nodes accept more than one password. Therefore, you might have several security triplets in an AMDS$DRIVER_ACCESS.DAT file for one Data Collector node. For example:

```
*\1DECAMDS\R
*\KOINECLS\R
*\KOINEFIX\W
*\AVAILMAN\C
```

In this example, Data Analyzer nodes with the passwords 1DECAMDS and KOINECLS would be able to see the Data Collector data, but only the Data Analyzer node with the KOINEFIX password would be able to write or change information, including performing fixes, on the Data Collector node. The Data Analyzer node with the AVAILMAN password would be able to perform switched LAN fixes.

If you want, you can set up your AMDS$DRIVER_ACCESS.DAT file to allow anyone in the world to read from your system but allow only certain nodes to write or change process or device characteristics on your system.

Note

After editing the AMDS$DRIVER_ACCESS.DAT file, you must stop and then restart the Data Collector. This action loads the new data into the driver.

7.7.2.3 How the Availability Manager Ensures Security

The Availability Manager performs these steps when using security triplets to ensure security among Data Analyzer and Data Collector nodes:

1. A message is broadcast at regular intervals to all nodes within the LAN indicating the availability of a Data Collector node to communicate with a Data Analyzer node.
2. The node running the Data Analyzer receives the availability message and returns a security triplet that identifies it to the Data Collector, and requests system data from the Data Collector.
3. The Data Collector examines the security triplet to determine whether the Data Analyzer is listed in the AMDS$DRIVER_ACCESS.DAT file to permit access to the system.
   - If the AMDS$DRIVER_ACCESS.DAT file lists Data Analyzer access information, then the Data Provider and the Data Analyzer can exchange information.
   - If the Data Analyzer is not listed in the AMDS$DRIVER_ACCESS.DAT file or does not have appropriate access information, then access is denied and a message is logged to OPCOM. The Data Analyzer receives a message stating that access to that node is not permitted.

Table 7–4 describes how the Data Collector node interprets a security triplet match.

Table 7–4 Security Triplet Verification

Security Triplet	Interpretation
08-00-2B-12-34-56\ HOMETOWN\ W	The Data Analyzer has write access to the node only when the Data Analyzer is run from a node with this hardware address (multiadapter or DECnet-Plus system) and with the password HOMETOWN.

(continued on next page)

Table 7–4 (Cont.) Security Triplet Verification

Security Triplet	Interpretation
2.1\HOMETOWN\R	The Data Analyzer has read access to the node when run from a node with DECnet for OpenVMS Phase IV address 2.1 and the password HOMETOWN.
*\HOMETOWN\R	Any Data Analyzer with the password HOMETOWN has read access to the node.

7.7.3 Changing a Password on a Windows Data Collector

To change the Data Collector password in the Registry, follow these steps:

1. Click the Windows **Start** button. On the menu displayed, first click **Programs**, then **Accessories**, and then **Command Prompt**.
2. Type `regedit` after the angle prompt (>).

   The system displays a screen for the Registry Editor, with a list of entries under My Computer.
3. On the list displayed, expand the **HKEY_LOCAL_MACHINE** entry.
4. Double-click **SYSTEM**.
5. Click **CurrentControlSet**.
6. Click **Services**.
7. Click **damdrvr**.
8. Click **Parameters**.
9. Double-click **Read Password**. Then type a new 8-character alphanumeric password, and click **OK** to make the change.
10. To store the new password, click **Exit** under File on the main menu bar.
11. On the Control Panel, click **Services** and then **Stop** for "PerfServ."
12. Again on the Control Panel, click **Devices** and then **Stop** for "damdrvr."
13. First restart **damdrvr** under "Devices" and then restart **PerfServ** under "Services."

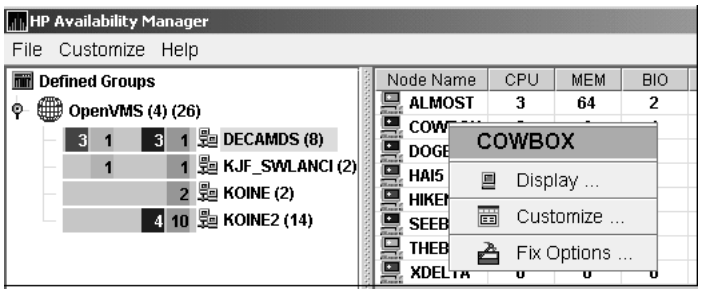
    This step completes the change of your Data Collector password.

7.8 Monitoring Processes on a Node

You can monitor up to eight processes on an individual node or a node that is part of a group that you select on the Group/Node Lists Customization page (see Section 7.2). After you enter the names of processes you want to monitor, the Availability Manager notifies you when these processes disappear and also when they reappear. (You cannot, however, use this feature to notify you about processes that should *not* be there.)

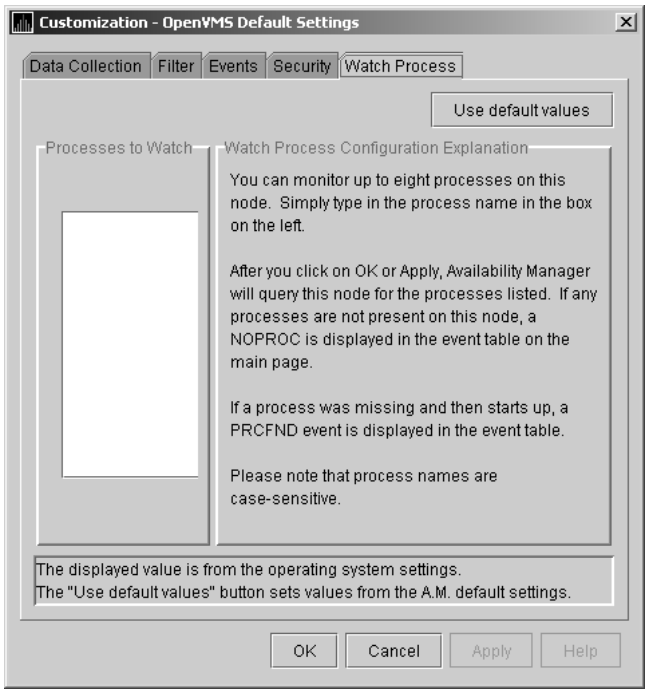
To use the Watch Process feature, right-click a node on the Node pane to display the Node pane Customization Menu shown in Figure 7–20.

Figure 7–20 Node Customization Menu



On this menu, choose **Customize** to display the options available for customizing individual nodes. One of these options is Watch Process, which you can select to display the Watch Process page shown in Figure 7–21.

Figure 7–21 Watch Process Page



An explanation of the watch process feature is displayed on the right side of the page. You can enter up to 8 processes on the left side of the page. After you enter process names, the Availability Manager monitors these processes on the node you have selected.

For a process that is not present on the node at the time you entered it on the Watch Process page, the Availability Manager displays the following event in the Event pane of the Application Window (see Figure 5–1):

```
NOPROC -- The process process-name has disappeared on
          the node node-name.
```

If a process that was signalled by a NOPROC event reappears on the node, the Availability Manager displays the following event in the Event pane of the Application Window:

```
PRCFND -- The process process-name has recently
          reappeared on the node node-name.
```

A

CPU Process States

The CPU process states shown in Table A–1 are displayed in the OpenVMS CPU Process States page (see Figure 3–8) and in the OpenVMS Process Information page (see Figure 3–23).

Table A–1 CPU Process States

Process State	Description
CEF	Common Event Flag, waiting for a common event flag
COLPG	Collided Page Wait, involuntary wait state; likely to indicate a memory shortage, waiting for hard page faults
COM	Computable; ready to execute
COMO	Computable Outswapped, COM, but swapped out
CUR	Current, currently executing in a CPU
FPG	Free Page Wait, involuntary wait state; most likely indicates a memory shortage
LEF	Local Event Flag, waiting for a Local Event Flag
LEFO	Local Event Flag Outswapped; LEF, but outswapped
HIB	Hibernate, voluntary wait state requested by the process; it is inactive
HIBO	Hibernate Outswapped, hibernating but swapped out

(continued on next page)

Table A–1 (Cont.) CPU Process States

Process State	Description
MWAIT	Miscellaneous Resource Wait, involuntary wait state, possibly caused by a shortage of a systemwide resource, such as no page or swap file capacity or no synchronizations for single-threaded code. Types of MWAIT states are shown in the following table:

MWAIT State	Definition
BWAIT	Process waiting for buffered I/O byte count quota.
JWAIT	Process in either BWAIT or TWAIT state.
TWAIT	Process waiting for timer queue entry quota.
EXH	Kernel thread in exit handler (not currently used).
IMODE	Kernel thread waiting to acquire inner-mode semaphore.
PSXFR	Process waiting during a POSIX fork operation.
RWAST	Process waiting for system or special kernel mode AST.
RWMBX	Process waiting because mailbox is full.
RWNBX	Process waiting for nonpaged dynamic memory.
RWPFF	Process waiting because page file is full.
RWPAG	Process waiting for paged dynamic memory.
RWMPE	Process waiting because modified page list is empty.
RWMPB	Process waiting because modified page writer is busy.
RWSCS	Process waiting for distributed lock manager.
RWCLU	Process waiting because OpenVMS Cluster is in transition.
RWCAP	Process waiting for CPU that has its capability set.
RWCSV	Kernel thread waiting for request completion by OpenVMS Cluster server process.

PFW	Page Fault Wait, involuntary wait state; possibly indicates a memory shortage, waiting for hard page faults.
RWAST	Resource Wait State, waiting for delivery of an asynchronous system trap (AST) that signals a resource availability; usually an I/O is outstanding or a process quota is exhausted.
RWBRK	Resource Wait for BROADCAST to finish
RWCAP	Resource Wait for CPU Capability
RWCLU	Resource Wait for Cluster Transition
RWCSV	Resource Wait for Cluster Server Process

(continued on next page)

Table A–1 (Cont.) CPU Process States

Process State	Description
RWIMG	Resource Wait for Image Activation Lock
RWLCK	Resource Wait for Lock ID data base
RWMBX	Resource Wait on MailBox, either waiting for data in mailbox (to read) or waiting to place data (write) into a full mailbox (some other process has not read from it; mailbox is full so this process cannot write).
RWMPB	Resource Wait for Modified Page writer Busy
RWMPE	Resource Wait for Modified Page list Empty
RWNPG	Resource Wait for Non Paged Pool
RWPAG	Resource Wait for Paged Pool
RWPFF	Resource Wait for Page File Full
RWQUO	Resource Wait for Pooled Quota
RWSCS	Resource Wait for System Communications Services
RWSWP	Resource Wait for Swap File space
SUSP	Suspended, wait state process placed into suspension; it can be resumed at the request of an external process
SUSPO	Suspended Outswapped, suspended but swapped out

B
Tables of Events

This appendix contains the following tables of events:

- OpenVMS Events Table B–1
- Windows Events Table B–2

Each table provides the following information:

- Alphabetical list of the events that the Availability Manager signals in the Event pane of the Application window (see Figure 1–1)
- Abbreviation and brief description of each event (also displayed in the Event pane)
- Explanation of the event and a suggestion for remedial action, if applicable

Table B–1 OpenVMS Events

Event	Description	Explanation	Recommended Action
CFGDON	Configuration done	The server application has made a connection to the node and will start collecting the data according to the Customize Data Collection options.	This informational event indicates that the node is recognized. No further investigation is required.
DPGERR	Error executing driver program	The Data Collector has detected a program error while executing the data collection program.	This event can occur if you have a bad driver program library, or there is a bug in the driver program. Make sure you have the program library that shipped with the kit; if it is correct, contact your customer support representative with the full text of the event.
DSKERR	High disk error count	The error count for the disk device exceeds the threshold.	Check error log entries for device errors. A disk device with a high error count could indicate a problem with the disk or with the connection between the disk and the system.
DSKINV	Disk is invalid	The valid bit in the disk device status field is not set. The disk device is not considered valid by the operating system.	Make sure that the disk device is valid and is known to the operating system.

(continued on next page)

Table B–1 (Cont.) OpenVMS Events

Event	Description	Explanation	Recommended Action
DSKMNV	Disk in mount verify state	The disk device is performing a mount verification.	The system is performing a mount verification for the disk device. This could be caused by: • A removable disk on a local or remote node was removed. • A disk on a local or remote node has gone offline due to errors. • The node that serves the disk is down. • The connection to a remote disk is down.
DSKOFF	Disk device is off line	The disk device has been placed in the off line state.	Check whether the disk device should be off line. This event is also signalled when the same device name is used for two different physical disks. The volume name in the event is the second node to use the same device name.
DSKQLN	High disk queue length	The average number of pending I/Os to the disk device exceeds the threshold.	More I/O requests are being queued to the disk device than the device can service. Reasons include a slow disk or too much work being done on the disk.
DSKRWT	High disk RWAIT count	The RWAIT count on the disk device exceeds the threshold.	RWAIT is an indicator that an I/O operation has stalled, usually during normal connection failure recovery or volume processing of host-based shadowing. A node has probably failed and shadowing is recovering data.
DSKUNA	Disk device is unavailable	The disk device has been placed in the Unavailable state.	The disk device state has been set to /NOAVAILABLE. See DCL help for the SET DEVICE/AVAILABLE command.
DSKWRV	Wrong volume mounted	The disk device has been mounted with the wrong volume label.	Set the correct volume name by entering the DCL command SET VOLUME/LABEL on the node.
ELIBCR	Bad CRC for exportable program library	The CRC calculation for the exportable program library does not match the CRC value in the library.	The exportable program library may be corrupt. Restore the exportable program library from its original source.
ELIBNP	No privilege to access exportable program library	Unable to access the exportable program library.	Check to make sure that the Availability Manager has the proper security access to the exportable program library file.
ELIBUR	Unable to read exportable program library	Unable to read the exportable program library for the combination of hardware architecture and OpenVMS version.	The exportable program library may be corrupt. Restore the exportable program library from its original source.

(continued on next page)

Table B–1 (Cont.) OpenVMS Events

Event	Description	Explanation	Recommended Action
FXCPKT	Received a corrupt fix response packet from node	The Availability Manager tried to perform a fix, but the fix acknowledgment from the node was corrupt.	This event could occur if there is network congestion or some problem with the node. Confirm the connection to the node, and reapply the fix if necessary.
FXCRSH	Crash node fix	The Availability Manager has successfully performed a Crash Node fix on the node.	This informational message indicates a successful fix. Expect to see a Path Lost event for the node.
FXDCPR	Decrement process priority fix	The Availability Manager has successfully performed a Decrement Process Priority fix on the process.	This informational message indicates a successful fix. Setting a process priority too low takes CPU time away from the process.
FXDCWS	Decrement process working set size fix	The Availability Manager has successfully decreased the working set size of the process on the node by performing an Adjust Working Set fix.	This informational message indicates a successful fix. This fix disables the automatic working set adjustment for the process.
FXDLPR	Delete process fix	The Availability Manager has successfully performed a Delete Process fix on the process.	This informational message indicates a successful fix. If the process is in RWAST state, this fix does not work. This fix also does not work on processes created with the no delete option.
FXEXIT	Exit image fix	The Availability Manager has successfully performed an Exit Image fix on the process.	This informational message indicates a successful fix. Forcing a system process to exit its current image can corrupt the kernel.
FXINPR	Increment process priority fix	The Availability Manager has successfully performed an Increment Process Priority fix on the process.	This informational message indicates a successful fix. Setting a process priority too high takes CPU time away from other processes. Set the priority above 15 only for “real-time” processing.
FXINQU	Increment process quota limits fix	The Availability Manager has successfully increased the quota limit of the process on the node by placing a new limit value in the limit field of the quota.	This informational message indicates a successful fix. This fix is only for the life of the process. If the problem continues, change the limit for the account in the UAF file.
FXINWS	Increment process working set size fix	The Availability Manager has successfully increased the working set size of the process on the node by performing an Adjust Working Set fix.	This informational message indicates a successful fix. This fix disables the automatic working set adjustment for the process. The adjusted working set value cannot exceed WSQUOTA for the process or WSMAX for the system.
FXNOPR	No-change process priority fix	The Availability Manager has successfully performed a Process Priority fix on the process that resulted in no change to the process priority.	This informational message indicates a successful fix. The Fix Value slider was set to the current priority of the process.

(continued on next page)

Table B–1 (Cont.) OpenVMS Events

Event	Description	Explanation	Recommended Action
FXNOQU	No-change process quota limits fix	The Availability Manager has successfully performed a quota limit fix for the process that resulted in no change to the quota limit.	This informational message indicates a successful fix. The Fix Value slider was set to the current quota of the process.
FXNOWS	No-change process working set size fix	The Availability Manager has successfully performed Adjust Working Set fix on the process.	This informational message indicates a successful fix. The Fix Value slider was set to the current working set size of the process.
FXPGWS	Purge working set fix	The Availability Manager has successfully performed a Purge Working Set fix on the process.	This informational message indicates a successful fix. The purged process might page fault to retrieve memory it needs for current processing.
FXPRIV	No privilege to attempt fix	The Availability Manager cannot perform a fix on the node due either to no CMKRNL privilege or to unmatched security triplets.	See Chapter 6 for details about setting up security.
FXQUOR	Adjust quorum fix	The Availability Manager has successfully performed an Adjust Quorum fix on the node.	This informational message indicates a successful fix. Use this fix when you find many processes in RWCAP state on a cluster node.
FXRESM	Resume process fix	The Availability Manager has successfully performed a Resume Process fix on the process.	This informational message indicates a successful fix. If the process goes back into suspend state, check the AUDIT_ SERVER process for problems.
FXSUSP	Suspend process fix	The Availability Manager has successfully performed a Suspend Process fix on the process.	This informational message indicates a successful fix. Do not suspend system processes.
FXTIMO	Fix timeout	The Availability Manager tried to perform a fix, but no acknowledgment for the fix was received from the node within the timeout period.	This event can occur if there is network congestion, if some problem is causing the node not to respond, or if the fix request failed to reach the node. Confirm the connection to the node, and reapply the fix if necessary.
FXUERR	Unknown error code for fix	The Availability Manager tried to perform a fix, but the fix failed for an unexpected reason.	Please contact your HP customer support representative with the text of this event. The event text is also recorded in the event log.
HIBIOR	High buffered I/O rate	The node's average buffered I/O rate exceeds the threshold.	A high buffered I/O rate can cause high system overhead. If this is affecting overall system performance, use the I/O Summary to determine the high buffered I/O processes, and adjust their priorities or suspend them as needed.
HICOMQ	Many processes waiting in COM or COMO	The average number of processes on the node in the COM or COMO queues exceeds the threshold.	Use the CPU Mode Summary to determine which processes are competing for CPU resources. Possible adjustments include changing process priorities and suspending processes.

(continued on next page)

Table B–1 (Cont.) OpenVMS Events

Event	Description	Explanation	Recommended Action
HIDIOR	High direct I/O rate	The average direct I/O rate on the node exceeds the threshold.	A high direct I/O rate can cause high system overhead. If this is affecting overall system performance, use the I/O Summary to determine the high direct I/O processes, and adjust their priorities or suspend them as needed.
HIHRDP	High hard page fault rate	The average hard page fault rate on the node exceeds the threshold.	A high hard page fault indicates that the free or modified page list is too small. Check Chapter 6 for possible actions.
HIMWTQ	Many processes waiting in MWAIT	The average number of processes on the node in the Miscellaneous Resource Wait (MWAIT) queues exceeds the threshold.	Use the CPU and Single Process pages to determine which resource is awaited. See Chapter 6 for more information about wait states.
HINTER	High interrupt mode time	The average percentage of time the node spends in interrupt mode exceeds the threshold.	Consistently high interrupt time prohibits processes from obtaining CPU time. Determine which device or devices are overusing this mode.
HIPRCT	High process count	The proportion of actual processes to maximum processes is too high. If the number of processes reaches the maximum (MAXPROCESSCNT), no more processes can be created and the system might hang as a result.	Decrease the number of actual processes. Increase SYSGEN parameter MAXPROCESSCNT.
HIPWIO	High paging write I/O rate	The average paging write I/O rate on the node exceeds the threshold.	Use the Process I/O and Memory Summary pages to determine which processes are writing to the page file excessively, and decide whether their working sets need adjustment.
HIPWTQ	Many processes waiting in COLPG, PFW, or FPG	The average number of processes on the node that are waiting for page file space exceeds the threshold.	Use the CPU Process States and Memory Summary to determine which processes are in the COLPG, PFW, or FPG state. COLPG and PFW processes might be constrained by too little physical memory, too restrictive working set quotas, or lack of available page file space. FPG processes indicate too little physical memory is available.
HISYSP	High system page fault rate	The node's average page fault rate for pageable system areas exceeds the threshold.	These are page faults from pageable sections in loadable executive images, page pool, and the global page table. The system parameter SYSMWCNT might be set too low. Use AUTOGEN to adjust this parameter.
HITTLP	High total page fault rate	The average total page fault rate on the node exceeds the threshold.	Use the Memory Summary to find the page faulting processes, and make sure that their working sets are set properly.
HMPSYN	High multiprocessor (MP) synchronization mode time	The average percentage of time the node handles multiprocessor (MP) synchronization exceeds the threshold.	High synchronization time prevents other devices and processes from obtaining CPU time. Determine which device is overusing this mode.

(continued on next page)

Table B–1 (Cont.) OpenVMS Events

Event	Description	Explanation	Recommended Action
KTHIMD	Kernel thread waiting for inner-mode semaphore	The average percentage of time that the kernel thread waits for the inner-mode semaphore exceeds the threshold.	Use SDA to determine which kernel thread of the process has the semaphore.
LCKBLK	Lock blocking	The process holds the highest priority lock in the resource's granted lock queue. This lock is blocking all other locks from gaining access to the resource.	Use the Single Process Windows to determine what the process is doing. If the process is in an RW*xxx* state, try exiting the image or deleting the process. If this fails, crashing the blocking node might be the only other fix option.
LCKCNT	Lock contention	The resource has a contention situation, with multiple locks competing for the same resource. The competing locks are the currently granted lock and those that are waiting in the conversion queue or in the waiting queue.	Use Lock Contention to investigate a potential lock contention situation. Locks for the same resource might have the NODLCKWT wait flag enabled and be on every member of the cluster. Usually this is not a lock contention situation, and these locks can be filtered out.
LCKWAT	Lock waiting	The process that has access to the resource is blocking the process that is waiting for it. Once the blocking process releases its access, the next highest lock request acquires the blocking lock.	If the blocking process holds the resource too long, check to see whether the process is working correctly; if not, one of the fixes might solve the problem.
LOASTQ	Process has used most of ASTLM quota	Either the remaining number of asynchronous system traps (ASTs) the process can request is below the threshold, or the percentage of ASTs used compared to the allowed quota is above the threshold.	If the amount used reaches the quota, the process enters RWAST state. If the process requires a higher quota, you can increase the ASTLM quota for the process in the UAF file. ASTLM is only a count; system resources are not compromised by increasing this count.
LOBIOQ	Process has used most of BIOLM quota	Either the remaining number of Buffered I/Os (BIO) the process can request is below the threshold, or the percentage of BIOs used is above the threshold.	If the amount used reaches the quota, the process enters RWAST state. If the process requires a higher quota, you can increasing the BIOLM quota for the process in the UAF file. BIOLM is only a count; system resources are not compromised by increasing this count.
LOBYTQ	Process has used most of BYTLM quota	Either the remaining number of bytes for the buffered I/O byte count (BYTCNT) that the process can request is below the threshold, or the percentage of bytes used is above the threshold.	If the amount used reaches the quota, the process enters RWAST state. If the process requires a higher quota, you can raise the BYTLM quota for the process in the UAF file. BYTLM is the number of bytes in nonpaged pool used for buffered I/O.
LODIOQ	Process has used most of DIOLM quota	Either the remaining number of Direct I/Os (DIOs) the process can request is below the threshold, or the percentage of DIOs used is above the threshold.	If the amount used reaches the quota, the process enters RWAST state. If the process requires a higher quota, you can increase the DIOLM quota for the process in the UAF file. DIOLM is only a count; system resources are not compromised by increasing this count.

(continued on next page)

Table B–1 (Cont.) OpenVMS Events

Event	Description	Explanation	Recommended Action
LOENQU	Process has used most of ENQLM quota	Either the remaining number of lock enqueues (ENQ) the process can request is below the threshold, or the percentage of ENQs used is above the threshold.	If the limit reaches the quota, the process is not able to make further lock queue requests. If the process requires a higher quota, you can increase the ENQLM quota for the process in the UAF file.
LOFILQ	Process has used most of FILLM quota	Either the remaining number of files the process can open is below the threshold, or the percentage of files open is above the threshold.	If the amount used reaches the quota, the process must first close some files before being allowed to open new ones. If the process requires a higher quota, you can increase the FILLM quota for the process in the UAF file.
LOMEMY	Free memory is low	For the node, the percentage of free memory compared to total memory is below the threshold.	Use the automatic Purge Working Set fix, or use the Memory and CPU Summary to select processes that that are either not currently executing or not page faulting, and purge their working sets.
LOPGFQ	Process has used most of PGFLQUOTA quota	Either the remaining number of pages the process can allocate from the system page file is below the threshold, or the percentage of pages allocated is above the threshold.	If the process requires a higher quota, you can raise the PGFLQUOTA quota for the process in the UAF file. This value limits the number of pages in the system page file that the account's processes can use.
LOPGSP	Low page file space	Either the remaining number of pages in the system page file is below the threshold, or the percentage of page file space remaining is below the threshold.	Either extend the size of this page file or create a new page file to allow new processes to use the new page file.
LOPRCQ	Process has used most of PRCLM quota	Either the remaining number of subprocesses the current process is allowed to create is below the threshold, or the percentage of created subprocesses is above the threshold.	If the amount used reaches the quota, the process is not allowed to create more subprocesses. If the process requires a higher quota, you can increase the PRCLM quota for the process in the UAF file.
LOSTVC	Lost virtual circuit to node	The virtual circuit between the listed nodes has been lost.	Check to see whether the second node listed has failed or whether the connection between the nodes is broken. The VC name listed in parentheses is the communication link between the nodes.
LOSWSP	Low swap file space	Either the remaining number of pages in the system page file is below the threshold, or the percentage of page file space remaining is below the threshold.	Either increase the size of this page file, or create a new page file to allow new processes to use the new page file.
LOTQEQ	Process has used most of TQELM quota	Either the remaining number of Timer Queue Entries (TQEs) the process can request is below the threshold, or the percentage of TQEs used to the allowed quota is above the threshold.	If the amount used reaches the quota, the process enters RWAST state. If the process requires a higher quota, you can raise the TQELM quota for the process in the UAF file. TQELM is only a count; system resources are not compromised by raising it.

(continued on next page)

Table B–1 (Cont.) OpenVMS Events

Event	Description	Explanation	Recommended Action
LOVLSP	Low disk volume free space	Either the remaining number of blocks on the volume is below the threshold, or the percentage of free blocks remaining on the volume is below the threshold.	You must free up some disk volume space. If part of the purpose of the volume is to be filled, such as a page/swap device, then you can filter the volume from the display.
LOVOTE	Low cluster votes	The difference between the number of VOTES and the QUORUM in the cluster is below the threshold.	Check to see whether voting members have failed. To avoid the hang that results if VOTES goes below QUORUM, use the Adjust Quorum fix.
LOWEXT	Low process working set extent	The process page fault rate exceeds the threshold, and the percentage of working set size compared to working set extent exceeds the threshold.	This event indicates that the WSEXTENT value in the UAF file might be too low. The process needs more physical memory but cannot obtain it; therefore, the process page faults excessively.
LOWSQU	Low process working set quota	The process page fault rate exceeds the threshold, and the percentage of working set size exceeds the threshold.	This event indicates the process needs more memory but might not be able to obtain it because one of the following is true: • The WSQUOTA value in the UAF file is set too low for the size of memory allocation requests or • The system is memory constrained.
LRGHSH	Remote lock hash table too large to collect data on	The Availability Manager cannot investigate the node's resource hash table (RESHASHTBL). It is either too sparse or too dense to investigate efficiently.	This event indicates that the Availability Manager will take too many collection iterations to analyze lock contention situations efficiently. Make sure that the SYSGEN parameter RESHASHTBL is set properly for the node.
NOPGFL	No page file	The Availability Manager cannot find a page file on the node.	Use SYSGEN to create and connect a page file on the node.
NOPLIB	No program library	The program library for the combination of hardware architecture and OpenVMS version was not found.	Check to see that all the program library files exist in the program library directory.
NOPRIV	Not allowed to monitor node	The Availability Manager cannot monitor the node due to unmatched security triplets.	See Chapter 6 for details on setting up security.
NOPROC	Specific process not found	The Availability Manager cannot find the process name selected in the Process Name Search dialog box on the Node Summary page.	This event can occur because the listed process no longer exists, or the process name is listed incorrectly in the dialog box.
NOSWFL	No swap file	The Availability Manager cannot find a swap file on the node.	If you do not use swap files, you can ignore this event. Otherwise, use SYSGEN to create and connect a swap file for the node.

(continued on next page)

Table B–1 (Cont.) OpenVMS Events

Event	Description	Explanation	Recommended Action
PKTFER	Packet format error	The data packet sent to the remote node was not in the correct format for the remote node to process.	Please contact your HP customer support representative with the full text of the event, the version of the Availability Manager, the configuration of the node running the Availability Manager, and the configuration of the nodes being monitored.
PLIBNP	No privilege to access program library	Unable to access the program library.	Check to see that the Availability Manager has the proper security access to the program library file.
PLIBUR	Unable to read program library	Unable to read the program library for the combination of hardware architecture and OpenVMS version.	The program library is either corrupt or from a different version of the Availability Manager. Restore the program library from the last installation.
PRBIOR	High process buffered I/O rate	The average buffered I/O rate of the process exceeds the threshold.	If the buffered I/O rate is affecting overall system performance, lowering the process priority or suspending the process would allow other processes to obtain access to the CPU.
PRBIOW	Process waiting for buffered I/O	The average percentage of time the process is waiting for a buffered I/O to complete exceeds the threshold.	Use SDA on the node to ensure that the device to which the process is performing buffered I/Os is still available and is not being overused.
PRCCOM	Process waiting in COM or COMO	The average number of processes on the node in the COM or COMO queues exceeds the threshold.	Use the CPU Summary to determine which processes should be given more CPU time, and adjust process priorities and states accordingly.
PRCCUR	Process has a high CPU rate	The average percentage of time the process is currently executing in the CPU exceeds the threshold.	Make sure that the listed process is not looping or preventing other processes from gaining access to the CPU. Adjust process priority or state as needed.
PRCFND	Process has recently been found	The Availability Manager has discovered the process name selected on the Watch Process page (see Figure 7–21).	No action required.
PRCMUT	Process waiting for a mutex	The average percentage of time the process is waiting for a particular system mutex exceeds the threshold.	Use SDA to help determine which mutex the process is waiting for and to help determine the owner of the mutex.
PRCMWT	Process waiting in MWAIT	The average percentage of time the process is in a Miscellaneous Resource Wait (MWAIT) state exceeds the threshold.	Various resource wait states are part of the collective wait state called MWAIT. See Appendix A for a list of these states. The CPU Process page and the Single Process page display which state the process is in. Check the Single Process page to determine which resource the process is waiting for and whether the resource is still available for the process.

(continued on next page)

Table B–1 (Cont.) OpenVMS Events

Event	Description	Explanation	Recommended Action
PRCPSX	Process waiting in PSXFR	The average percentage of time the process waits during a POSIX fork operation exceeds the threshold.	
PRCPUL	Most of CPULIM process quota used	The remaining CPU time available for the process is below the threshold.	Make sure the CPU time allowed for the process is sufficient for its processing needs. If not, increase the CPU quota in the UAF file of the node.
PRCPWT	Process waiting in COLPG, PFW or FPG	The average percentage of time the process is waiting to access the system page file database exceeds the threshold.	Check to make sure the system page file is large enough for all the resource requests being made.
PRCQUO	Process waiting for a quota	The average percentage of time the process is waiting for a particular quota exceeds the threshold.	Use the Single Process pages to determine which quota is too low. Then adjust the quotas of the account in the UAF file.
PRCRWA	Process waiting in RWAST	The average percentage of time the process is waiting in the RWAST state exceeds the threshold. RWAST indicates the process is waiting for an asynchronous system trap to complete.	Use the Single Process pages to determine if RWAST is due to the process quota being set too low. If not, use SDA to determine if RWAST is due to a problem between the process and a physical device.
PRCRWC	Process waiting in RWCAP	The average percentage of time the process is waiting in the RWCAP state exceeds the threshold. RWCAP indicates that the process is waiting for CPU capability.	When many processes are in this state, the system might be hung because not enough nodes are running in the cluster to maintain the cluster quorum. Use the Adjust Quorum fix to correct the problem.
PRCRWM	Process waiting in RWMBX	The average percentage of time the process is waiting in the RWMBX state exceeds the threshold. RWMBX indicates the process is waiting for a full mailbox to be empty.	Use SDA to help determine which mailbox the process is waiting for.
PRCRWP	Process waiting in RWPAG, RWNPG, RWMPE, or RWMPB	The average percentage of time the process is waiting in the RWPAG, RWNPG, RWMPE, or RWMPB state exceeds the threshold. RWPAG and RWNPG are for paged or nonpaged pool; RWMPE and RWMPB are for the modified page list.	Processes in the RWPAG or RWNPG state can indicate you need to increase the size of paged or nonpaged pool, respectively. Processes in the RWMPB state indicate that the modified page writer cannot handle all the modified pages being generated. Refer to Chapter 6 for suggestions.
PRCRWS	Process waiting in RWSCS, RWCLU, or RWCSV	The average percentage of time the process is waiting in the RWSCS, RWCLU, or RWCSV state exceeds the threshold. RWCSV is for the cluster server; RWCLU is for the cluster transition; RWSCS is for cluster communications. The process is waiting for a cluster event to complete.	Use the Show Cluster utility to help investigate.

(continued on next page)

Table B–1 (Cont.) OpenVMS Events

Event	Description	Explanation	Recommended Action
PRCUNK	Process waiting for a system resource	The average percentage of time the process is waiting for an undetermined system resource exceeds the threshold.	The state in which the process is waiting is unknown to the Availability Manager.
PRDIOR	High process direct I/O rate	The average direct I/O rate of the process exceeds the threshold.	If the I/O rate is affecting overall system performance, lowering the process priority might allow other processes to obtain access to the CPU.
PRDIOW	Process waiting for direct I/O	The average percentage of time the process is waiting for a direct I/O to complete exceeds the threshold.	Use SDA on the node to ensure that the device to which the process is performing direct I/Os is still available and is not being overused.
PRLCKW	Process waiting for a lock	The average percentage of time the process is waiting in the control wait state exceeds the threshold.	The control wait state indicates that a process is waiting for a lock. Although no locks might appear in Lock Contention, the awaited lock might be filtered out of the display.
PRPGFL	High process page fault rate	The average page fault rate of the process exceeds the threshold.	The process is memory constrained; it needs an increased number of pages to perform well. Make sure that the working set quotas and extents are set correctly. To increase the working set quota temporarily, use the Adjust Working Set fix.
PRPIOR	High process paging I/O rate	The average page read I/O rate of the process exceeds the threshold.	The process needs an increased number of pages to perform well. Make sure that the working set quotas and extents are set correctly. To increase the working set quota temporarily, use the Adjust Working Set fix.
PTHLST	Path lost	The connection between the server and collection node has been lost.	Check to see whether the node failed or whether the LAN segment to the node is having problems. This event occurs when the server no longer receives data from the node on which data is being collected.
RESDNS	Resource hash table dense	The percentage of occupied entries in the hash table exceeds the threshold.	A densely populated table can result in a performance degradation. Use the system parameter RESHASHTBL to adjust the total number of entries.

(continued on next page)

Table B–1 (Cont.) OpenVMS Events

Event	Description	Explanation	Recommended Action
RESPRS	Resource hash table sparse	The percentage of occupied entries in the hash table is less than the threshold.	A sparsely populated table wastes memory resources. Use the system parameter RESHASHTBL to adjust the total number of entries.
UEXPLB	Using OpenVMS program export library	The program library for the combination of hardware architecture and OpenVMS version was not found.	Check to see that all the program library files exist in the program library directory.
UNSUPP	Unsupported node	The Availability Manager does not support this combination of hardware architecture and OpenVMS version.	Check the product SPD for supported system configurations.
VLSZCH	Volume size changed	Informational message to indicate that the volume has been resized.	No further investigation is required.
WINTRN	High window turn rate	This indicates that current open files are fragmented. Reading from fragmented files or extending a file size, or both, can cause a high window turn rate.	Defragment heavily used volumes using BACKUP or a disk fragmentation program. For processes that extend the size of a file, make sure that the file extent value is large. (See the $SET RMS/EXTEND_QUANTITY command documentation for more information.)

Table B–2 Windows Events

Event	Description	Explanation	Recommended Action
CFGDON	Configuration done	The server application has made a connection to the node and will start collecting the data according to the Customize Data Collection options.	An informational event to indicate that the node is recognized. No further investigation is required.
NODATA	Unable to collect performance data	The Availability Manager is unable to collect performance data from the node.	The performance data is collected by the PerfServ service on the remote node. Check to see that the service is up and running properly.
NOPRIV	Not allowed to monitor node	The Availability Manager cannot monitor the node due to a password mismatch between the Data Collector and the Data Analyzer.	See Chapter 6 for details on setting up security.
PTHLST	Path lost	The connection between the Data Analyzer and the Data Collector has been lost.	Check if the node crashed or if the LAN segment to the node is having problems. This event occurs when the server no longer receives data from the node on which data is being collected.
PVRMIS	Packet version mismatch	This version of the Availability Manager is unable to collect performance data from the node because of a data packet version mismatch.	The version of the Availability Manager Data Collector is more recent than the Data Analyzer. To process data from the node, upgrade the Data Analyzer to correspond to the Data Collector.

C

OpenVMS Events by Type of Data Collected

This appendix shows the events that can be signaled for each type of OpenVMS data collected. The events are categorized as follows:

- Threshold events (Table C–1)
- Nonthreshold events (Table C–2)

Appendix B describes these events in detail and provides recommended actions.

Note

Enabling the data collections described in these tables is described in Chapter 7. The only exceptions are the events listed under "Process name scan" in Table C–1, which are enabled on the Watch Process Customization page (see Figure 7–21).

Table C–1 OpenVMS Threshold Events

Type of Data Collected	Event	Description
Disk status	DSKERR	High disk error count
	DSKINV	Disk is invalid
	DSKMNV	Disk in mount verify state
	DSKOFF	Disk device is off line
	DSKRWT	High disk RWAIT count
	DSKUNA	Disk device is unavailable
	DSKWRV	Wrong volume mounted
	WINTRN	High window turn rate
Disk volume	DSKQLN	High disk queue length
	LOVLSP	Low disk volume free space
	VLSZCH	Volume size changed
Node summary	HIBIOR	High buffered I/O rate
	HICOMQ	Many processes waiting in COM or COMO
	HIDIOR	High direct I/O rate
	HIHRDP	High hard page fault rate

(continued on next page)

Table C–1 (Cont.) OpenVMS Threshold Events

Type of Data Collected	Event	Description
	HIMWTQ	Many processes waiting in MWAIT
	HINTER	High interrupt mode time
	HIPRCT	High process count
	HIPWIO	High paging write I/O rate
	HIPWTQ	Many processes waiting in COLPG, PFW, or FPG
	HISYSP	High system page fault rate
	HITTLP	High total page fault rate
	HMPSYN	High multiprocessor (MP) synchronization mode time
	LOMEMY	Free memory is low
Lock contention	LCKCNT	Lock contention
	LRGHSH	Remote lock hash table too large to collect data
	RESDNS	Resource hash table dense
	RESPRS	Resource hash table sparse
Single lock	LCKBLK	Lock blocking
	LCKWAT	Lock waiting
Single process	KTHIMD	Kernel thread waiting for inner-mode semaphore
	LOASTQ	Process has used most of ASTLM quota
	LOBIOQ	Process has used most of BIOLM quota
	LOBYTQ	Process has used most of BYTLM quota
	LODIOQ	Process has used most of DIOLM quota
	LOENQU	Process has used most of ENQLM quota
	LOFILQ	Process has used most of FILLM quota
	LOPGFQ	Process has used most of PGFLQUOTA quota
	LOPRCQ	Process has used most of PRCLM quota
	LOTQEQ	Process has used most of TQELM quota
	LOWEXT	Low process working set extent
	LOWSQU	Low process working set quota
	PRBIOR	High process buffered I/O rate
	PRBIOW	Process waiting for buffered I/O
	PRCCOM	Process waiting in COM or COMO
	PRCCUR	Process has a high CPU rate
	PRCMUT	Process waiting for a mutex
	PRCPSX	Process waiting in PSXFR wait state
	PRCPUL	Most of CPULIM process quota used

(continued on next page)

Table C–1 (Cont.) OpenVMS Threshold Events

Type of Data Collected	Event	Description
	PRCPWT	Process waiting in COLPG, PFW, or FPG
	PRCQUO	Process waiting for a quota
	PRCRWA	Process waiting in RWAST
	PRCRWC	Process waiting in RWCAP
	PRCRWM	Process waiting in RWMBX
	PRCRWP	Process waiting in RWPAG, RWNPG, RWMPE, or RWMPB
	PRCRWS	Process waiting in RWSCS, RWCLU, or RWCSV
	PRCUNK	Process waiting for a system resource
	PRDIOR	High process direct I/O rate
	PRDIOW	Process waiting for direct I/O
	PRLCKW	Process waiting for a lock
	PRPGFL	High process page fault rate
	PRPIOR	High process paging I/O rate
Process I/O	LOBIOQ	Process has used most of BIOLM quota
	LOBYTQ	Process has used most of BYTLM quota
	LODIOQ	Process has used most of DIOLM quota
	LOFILQ	Process has used most of FILLM quota
	PRBIOR	High process buffered I/O rate
	PRDIOR	High process direct I/O rate
	PRPIOR	High process paging I/O rate
Page/swap file	LOPGSP	Low page file space
	LOSWSP	Low swap file space
	NOPGFL	No page file
	NOSWFL	No swap file
Cluster summary	LOVOTE	Low cluster votes
Memory	LOWEXT	Low process working set extent
	LOWSQU	Low process working set quota
	PRPGFL	High process page fault rate
	PRPIOR	High process paging I/O rate
CPU process	PRCCOM	Process waiting in COM or COMO
	PRCCUR	Process has a high CPU rate

(continued on next page)

Table C–1 (Cont.) OpenVMS Threshold Events

Type of Data Collected	Event	Description
	PRCMWT	Process waiting in MWAIT (See Appendix A for a breakdown of MWAIT state.)
	PRCPWT	Process waiting in COLPG, PFW, or FPG
Process name scan	NOPROC	Specific process not found
	PRCFND	Process has been discovered recently

Table C–2 OpenVMS Nonthreshold Events

Type of Data Collected	Event	Description
Node-level event	CFGDON	Configuration done
	DPGERR	Error executing driver program
	NOPRIV	Not allowed to monitor node
	PKTFER	Packet format error
Program library error	ELIBCR	Bad CRC for exportable program library
	ELIBNP	No privilege to access exportable program library
	ELIBUR	Unable to read exportable program library
	NOPLIB	No program library
	PLIBNP	No privilege to access program library
	PLIBUR	Unable to read program library
	UEXPLB	Using exportable program library
	UNSUPP	Unsupported node
Events generated by fixes	FXCPKT	Received a corrupt fix response packet from node
	FXCRSH	Crash node fix
	FXDCPR	Decrement process priority fix
	FXDCWS	Decrement process working set size fix
	FXDLPR	Delete process fix
	FXEXIT	Exit image fix
	FXINPR	Increment process priority fix
	FXINQU	Increment process quota limits fix
	FXINWS	Increment process working set size fix
	FXPGWS	Purge working set fix
	FXPRIV	No privilege to attempt fix
	FXQUOR	Adjust quorum fix

(continued on next page)

Table C–2 (Cont.) OpenVMS Nonthreshold Events

Type of Data Collected	Event	Description
	FXRESM	Resume process fix
	FXSUSP	Suspend process fix
	FXTIMO	Fix timeout
	FXUERR	Unknown error code for fix

Index

D

E

F

G

H

I

J

L

M

Q

R

S

T

U

V

W