5

Monitoring Your Network Systems

ENlighten/DSM provides you with powerful tools for monitoring and gathering information about host and network problems, displaying that information in effective and meaningful ways, and helping you to fix the problem. Events testing is the mechanism that allows you to gather specific kinds of information. The Status Map feature displays the status of all of the systems managed on the network and shows which hosts or pools are having problems indicated by event testing.

ENlighten/DSM's Events feature collects and saves status, configuration, performance, and capacity information, and makes it available for monitoring by the Status Map and commercial SNMP managers.

This chapter provides information about:

- Monitoring systems with Events

- Viewing system status

- Monitoring logins, processes, and CPU usage

- Auditing security checks

Monitoring UNIX Systems with Events

This section contains information about using ENlighten/DSM's Events feature to monitor your UNIX systems. It includes information about how to add, modify, and delete tests. For a detailed overview of Events capabilities and features, standards compliance, and the basics of building a testtab file, refer to Chapter 10, "Events," in the *ENlighten/DSM Reference Manual.*

How Events Works

The Events feature helps predict problems, reports the event, and takes corrective action defined by the user.

You can use the data collected by Events to assist in tasks, such as:

- system tuning
- load balancing
- resource planning and justification
- upgrade requirement analysis

Events collects this data by monitoring the following:

- memory subsystems
- individual files
- directory queues
- filesystems
- printer queues
- critical processes
- network statistics
- hardware inventory
- software inventory
- user-provided data

An appropriate message can be sent to network managers, system managers, or both when an alarm condition occurs. Events can send alarms using one or more of the following methods:

- SNMP (Simple Network Management Protocol) trap messages

- e-mail

- Programmable Events Processor (PEP) messages

Events can also pass the alarm to a process you've defined for possible corrective action. You can specify the same process for all tests or a separate process for each test.

Adding an Events Test

To create a new Events test,

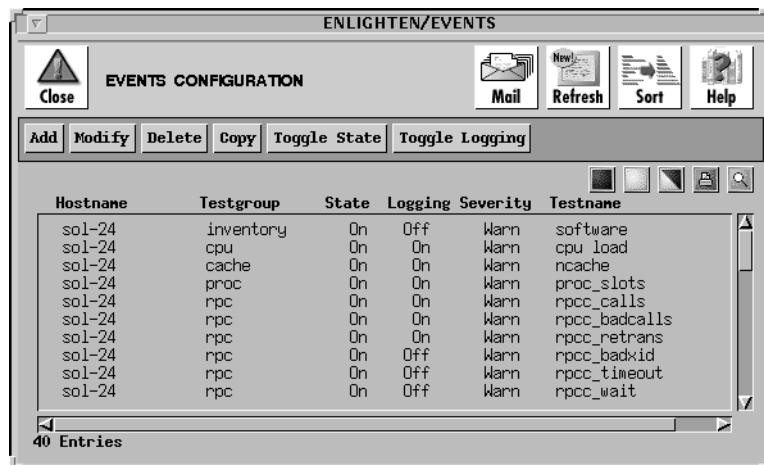1) Choose Configure from the Events menu. The Events Configuration window appears.

Figure 5-1 Events Configuration window

This window displays the hostname, the test group, whether the test is turned on or off, whether logging for the test is turned on or off, the severity level, and the test name for each test ENlighten/DSM finds on your default host.

2) Click the Add button to select the test type for this new Events test. A Select New Event Type window appears allowing you to select which type of test you want to create.
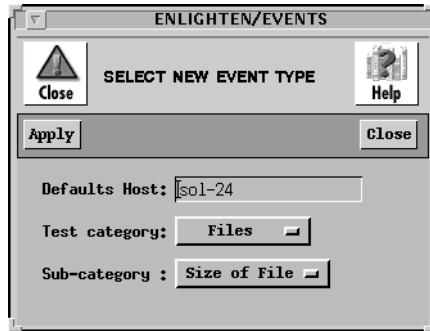

Figure 5-2 Select New Event Type window

3) Enter the hostname that will contain the default settings for the tests you will be creating.

4) From the Test Category field, choose the test type for your test. The options are:

- Files (the default)

- Processes

- Directories

5) From the Sub-category field, specify a subcategory of the test types. If you selected the Files option in the Test Category field, you can further specify what kind of files test you want:

- Size of File (the default)

- Last Modified

- Last Accessed

- File Clamping

If you selected the Processes option in the Test Category field, you can further specify what kind of process test you want:

- Instance of Process (the default)

- Size of Process

- Time Used by Process

There are no further subcategory options if you selected the Directories option in the Test Category field.

6) Click the Apply button to display the Add Events Test window for the test type you selected. Then enter the parameters for your new Events test.

Figure 5-3 Add Events Test window

Entering Test Parameters

You use the Add Events Test window to define the parameters for a new Events test. For more information on the formats of these fields or if you want to run Events from a command-line mode, refer to Chapter 10, "Events," in the *ENlighten/DSM Reference Manual*.

This section describes how to use each field and button in the Add Events Test window.

Hostnames field

Type the hostnames you want configured for this test. Leave a blank space between hostnames for multiple entries. You can also click the arrow button to the right to pop up a pick list of all hosts within the current pool and make your selection(s) from there.

Testname field

Type the name for your test. This must be the full pathname of the file or directory you want to monitor, or the process name to monitor.

Units of Measure field

This view-only field shows what the standard units of measure are for this test.

Sub-command field

This view-only field shows the Events-defined subcommand, if any, this test will use during its execution.

Internal Test field

This view-only field shows whether this test is an Events built-in test (Yes setting) or a user-defined test (No setting).

Test Group field

This view-only field shows the test group type for this test.

State field

Use this toggle to turn the test On (the default) or Off.

Severity field

Use this toggle to choose the level of severity to assign this test from the following message types:

- OK

- Informational (the default)

- Warning

- Error

- Severe

Use PEP field

Use this toggle to specify whether this test should use PEP to report its results and/or filter any action to be taken. The default setting is Yes.

Logging field

Use this toggle to specify whether logging should be enabled for this test. The default is Yes.

Delta field

If you enabled Logging, you can use this field to establish a "changed by" (delta) value. ENlighten/DSM will record the most recent value measured by the test if that value differs by at least this delta amount from the previously logged value.

See Chapter 10, "Events," in the *ENlighten/DSM Reference Manual* for more details.

Mailer field

You can use this field to specify which mail program should be used to deliver any alarms to the User. The default is /bin/mail. If you use another mail program, it must use the same syntax as the standard UNIX mail program.

User field

You can use this field to specify the user(s) who should receive any alarm information. The default is value is root. Leave a blank space between each user name for multiple entries. If you set this value to nobody, no mail will be sent.

Command field

You can use this field to specify any executable this test should run when it sets an alarm. This can be a script or a compiled executable.

Age field

This field can specify a threshold for when a file is considered to have "aged" in a directory. This value is only available if this test will monitor a directory queue.

You can use this field to select (in minutes) what the "aged" threshold is. Only files more than 'age' minutes old are counted as 'old'.

Test Freq field

Use this field to specify how often in minutes to run this test. The default is every five minutes.

Alarm Freq field

Use this field to specify how long to wait in minutes before sending another new alarm about this test. The default is every hour.

High Thresh field

This field allows you to specify an absolute high-level alarm set point for the data you're measuring in this test. This can be an integer or floating-point value.

Low Thresh field

This field allows you to specify an absolute low-level alarm set point for the data you're measuring in this test. This can be an integer or floating-point value.

Pos Rate field

This field allows you to specify a positive percentage change alarm set point for the data you're measuring in this test. This threshold compares the current test value with the last measured value (check for percentage of change since last tested). This must be a floating-point value.

Neg Rate field

This field allows you to specify a negative percentage change alarm set point for the data you're measuring in this test. This threshold compares the current test value with the last measured value (check for percentage of change since last tested). This must be a floating-point value.

Pos Jump field

You can use this field to specify a positive incremental change alarm set point for the data you're measuring in this test. This threshold compares the current test value with the last measured value (check for change of X points since last tested). This can be an integer or floating-point value.

Neg Jump field

You can use this field to specify a negative incremental change alarm set point for the data you're measuring in this test. This threshold compares the current test value with the last measured value (check for change of X points since last tested). This can be an integer or floating-point value.

API File field

If you're creating an API test, use this field to specify the full pathname of the file that will hold the values you are monitoring.

☞ See Chapter 10, "Events," in the *ENlighten/DSM Reference Manual* for examples and more information on creating API tests.

API Data Field

If you're creating an API test, specify which field or column holds the data value to monitor. Use a digit prefaced by an 'f' for a field number or a 'c' for a column number. The default assumes this value is a field number. If you're using a column designator, each character in any input file line/row is handled as one column.

API Label Field

If you're creating an API test, you can use this field to specify which field in your file contains a descriptive word or label.

Logfile Clamping Regular Expressions field

You can use regular expressions to define "types" of messages based on pattern matching. When one or more of these message types are found in a file, an alarm is sent to the agents you specify in your test. Each time this test runs, it evaluates only those file entries that were added since the last occurrence of the test.

For more information on regular expressions, see your *on-line O/S manual, section regx(3)* (typically this is located in `/usr/man/man3`).

Apply button

Click the Apply button to add the test configuration to the testtab files for all specified hosts and update the Events process that is monitoring the data.

☞ ENlighten/DSM is updated immediately and the testtab file is updated two minutes later.

Set Defaults button

Click Set Defaults button to set default values in the text fields based on the test type category you previously specified in the Select New Event Type window.

Modifying an Existing Test

Click the Modify button in the Events Configuration window
(Figure 5-1) to modify an existing test configuration. A window
similar to the Add Events Test window will appear, except you cannot
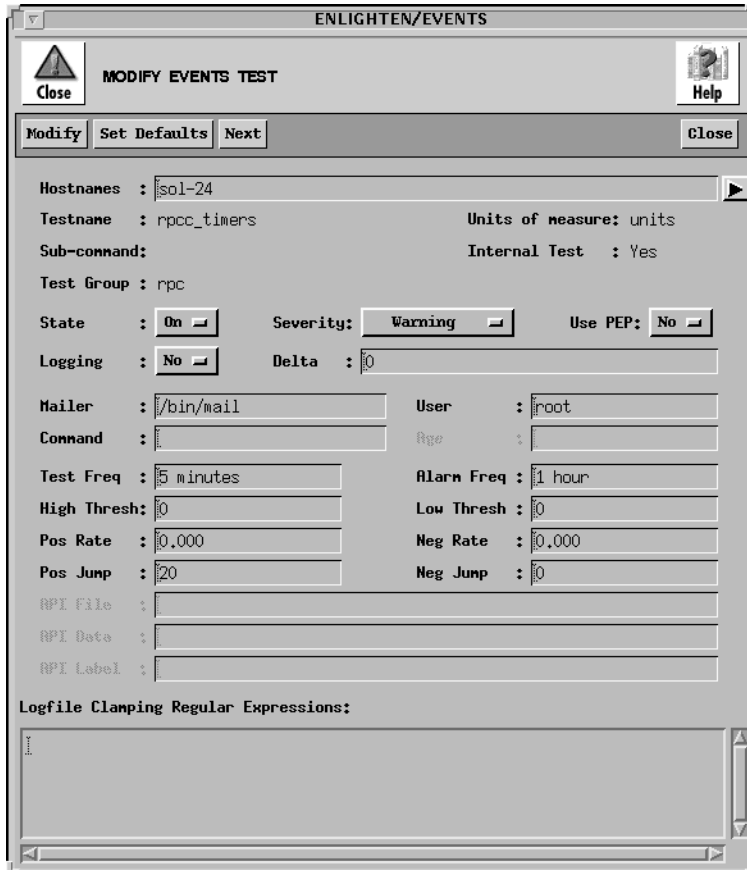modify the Testname field.

Figure 5-4 Modify Events Test window

See the previous section, "Entering Test Parameters" on page 5-7 for information about each field.

There are also differences of two buttons in the Modify Events Test window:

- You use the Modify button (rather than the Add button) to save your changes.

- You use the Next button to modify additional test configurations if you've selected more than one to modify from the Events Configuration list.

Deleting an Events Test

Highlight the Events test you want to delete from the Events Configuration window. Click the Delete button. ENlighten/DSM prompts you to confirm your action.

☞ You can only delete tests *you* have added. You can turn off built-in tests, but you cannot delete them from the Configure Events list.

Copying an Events Test

To copy the contents of an events test and create a second test, highlight the events tests that you want to copy and then click the Copy button. The Add Events Test window will appear showing the highlighted job's settings in each field. You can edit this window as needed and then click the Apply button to complete the copy.

See "Entering Test Parameters" on page 5-7 for information about each field.

☞ You can only copy tests you have added.

Viewing System Status

The Status Map allows you to view hosts and pools in your network and their current state. Using information provided by Events, it graphically displays the state of systems being managed on your network using color-coded icons. Depending on the priority level, you can ignore the status, or query events, and then fix the problem.

This section describes how to interpret and navigate the Status Map, query events using the Status Map window, and how to clear the Status Map of events.

Interpreting the Status Map

To view the Status Map, choose Open Map from the Status Map menu.

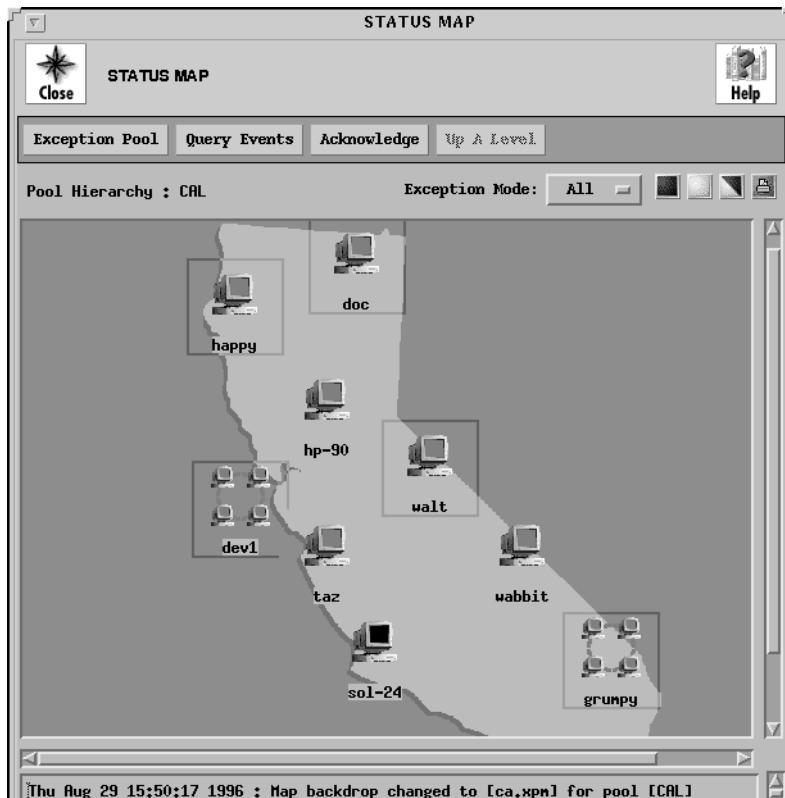A map similar to the one in appears.

Figure 5-5 Example of a Status Map

The state of each host or pool icon is displayed according to the icon color. The color of each host icon reflects the current highest priority event for any host that has not been cleared. The color of each pool icon reflects the current highest priority uncleared event for *any host* within that pool:

- Green - OK

- White - Informational

- Yellow - Warning

- Blue - Error

- Red - Severe

A blinking host or pool icon indicates the following:

- If a host icon is blinking, an unacknowledged event has occurred for that host. If a pool icon is blinking, an unacknowledged event has occurred for at least one host contained in the pool.

- An unacknowledged event is any event message that you have not yet acknowledged using the Status Map.

☞ If you haven't recently viewed the Status Map and an icon is blinking green, look at the preceding activity for that host or pool. An alarm might have occurred and cleared itself between viewings. For example, if an unauthorized user logged on to your system and then exited, and an Events test had already checked for this type of alert, a green alert would appear. All ENlighten/DSM system admininstration functions act upon any hosts selected in the Status Map.

To change the background of the Status Map, place the arrow cursor over the map and click the right mouse button. A list of backgrounds appears from which to choose a background.

Navigating the Status Map

To navigate the Status Map,

- If you select a pool icon, all hosts within the pool are selected and can be managed as a single unit.

- If you want to perform administration functions on a subset of hosts in a pool, select those hosts by single-clicking on the host icons.

- You can also use the standard mouse "select rectangle" or "sweep" method to define a temporary group.

Querying Events

To search for and view alarms and messages logged by events,

1) Click the Query Events button in the Status Map window. The Status Map Query Events window appears.
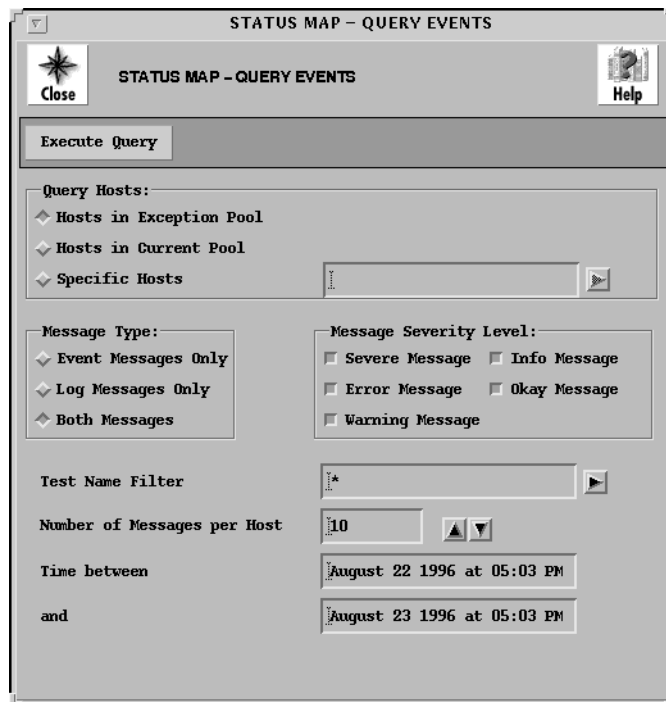
Figure 5-6 Status Map Query Events window

2) Choose the hosts that you want to query from the Query Hosts field. The options are:

- Hosts In Exception Pool (the default)

- Hosts In Current Pool

- Specific Host(s)

If you choose the Specific Host(s) option, use the text field to the right of that option to specify which host(s) to check for messages. Leave a blank space between hostnames for multiple entries.

3) Choose the type of messages you want to search for from the Message Type field. The options are:

- Event Messages Only. Events alarm messages generated by a test violating a predefined threshold.

- Log Messages Only. The Events informational messages generated when a test runs without generating an event and that (successful) result is logged.

- Both Messages (the default).

4) Choose the severity level you want to use in the search from the Message Severity Level field. The options are:

- Severe Message

- Info Message

- Error Message

- Okay Message

- Warning Message

Select one or more severity levels to use in the search. The default setting is all levels of message severity will be queried during the search.

5) To limit the search to a few tests, type the entire test name or just the first few letters of the test name in the Test Name Filter field.

All tests whose name contains part or all of the specified string will be queried. Leave a blank space between test names for multiple entries. You can also click the arrow button to the right to pop up a pick list of all pre-defined standard Events tests and make your selection(s) from there. You can also use the standard UNIX wildcards '*', '[]', and '?' in this field (for example, /home/*).

6) Enter the number of messages for each host that you want to search in the Number of Messages per Host field. The most recent messages are displayed first. You can also use the counter buttons to the right to increment or decrement the number displayed.

7) Enter a start and ending time to limit the search to messages logged between the specified times in the time fields.

8) Click the Execute Query button to begin the search process. When the query is completed, the results are displayed (Figure 5-7).

Figure 5-7 Query results

The list box shows all the messages matching your search criteria. Each line in the list displays the hostname, test name, logged value, units, severity, status, and time stamp.

You can select one of the tests and click the Reconfigure Test button to bring up the Modify Events Test window for that test. For details on how to use the Modify Events Test window and modify the test, see .

Clearing an Event from the Status Map

You can clear an event when the condition that triggered the event no longer exists. Either Events or Sys Admin can determine an 'event condition' has been cleared and relay this to the Status Map. There are two ways to clear an event:

- The event clears itself (for example, an Events CPU load test returns an OK result).

- You correct the activity that caused the original event/problem to occur (for example, by correcting whatever is overloading the CPU load).

After all events for a host/pool are cleared, the color for that icon is set to green (current status = OK).

Auditing Security Checks

ENlighten/DSM security feature provides a host of tools that check various system and network functions and report the findings into a logfile. ENlighten/DSM checks vital files, filesystem devices, boot and shutdown scripts, crontab contents, password integrity, group files, home directories, and break-in attempts. You can choose the functions that you want to audit.

For information on each one of the security features, refer to Chapter 3, "Security," in the *ENlighten/DSM Reference Manual*.

Monitoring Logins, Processes, and CPUs

ENlighten/DSM allows you to easily monitor login activity, process statuses, and CPU usage with Activity Monitor commands in the User menu.

The rest of this section details how to use each of these options.

Monitoring Logins

To see at a glance which users are currently logged in (accessing) the system, choose Activity Monitor and then Who Is Logged In from the User menu. The Who Is Logged In window appears (Figure 5-8).
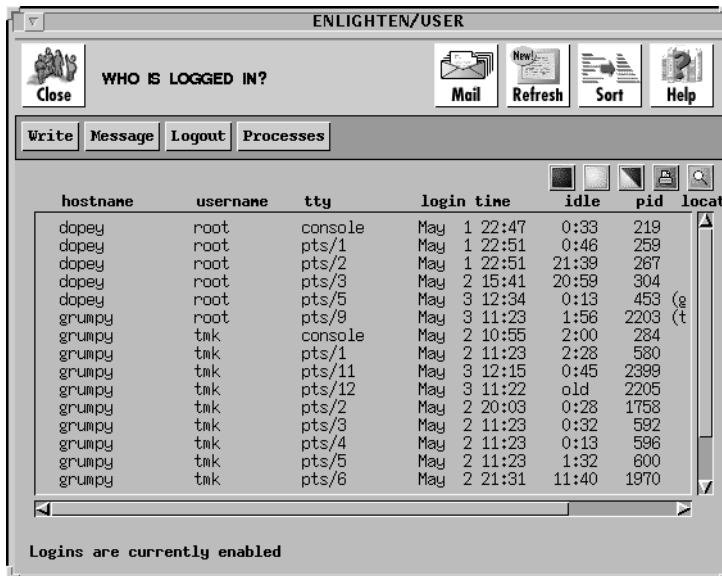

Figure 5-8 Who Is Logged In window

The window displays the hostname, user name, tty, login time, idle time, process ID, and the location of the tty (if available). To select one or more user accounts for further information, highlight the users you want and then select one of the following options.

Writing Messages to Users

Click the Write button to write a message directly to the selected users. A window appears with a field for composing a message of any length to each of the highlighted users. When you have completed your message, press the Return key and the message is sent. To close down the window, press the Control-C or the interrupt key. The recipient can respond to this message, allowing for a two-way conversation.

Message

The Message command is similar to the Mail command, except a predefined or custom form letter is sent directly to the user's screen instead of the user's mailbox. The recipient cannot reply to this message.

Logging Out

Click the Logout button to terminate all highlighted work sessions by killing the initial Shell process belonging to the marked users.

☞ Use this command with caution as it may also cause related user processes to be killed.

Displaying Processes

Click the Processes button to display a window of all processes currently running of the highlighted users. To further manipulate this information, see the next section, "Monitoring Process Status."

Monitoring Process Status

To view a list of all active processes, choose Activity Monitor and then Process Status from the User menu. The Processes window appears (Figure 5-9).
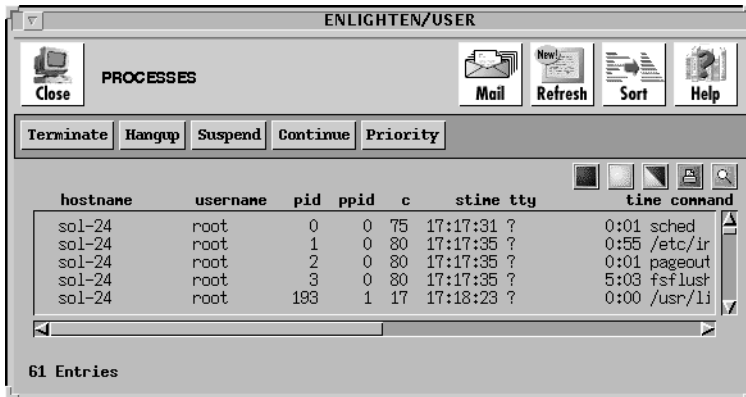

Figure 5-9 Processes window

You can highlight a process and use the command buttons in the window to perform the following actions on the selected processes.

Killing a Process

Click the Terminate button to immediately kill the highlighted process.

☞ This command will not kill related processes, so if there are child processes running, they will become orphans that you terminate separately or that are killed automatically. A pop-up window will prompt you for verification to terminate the process.

Hanging Up a Process

The Hangup command is similar to the Terminate command, except it provides enough time for the process to shut down properly. This means the process can close any files and terminate any child processes. A pop-up window will prompt you for verification to hang up the process.

Suspending and Continuing a Process

Click the Suspend button to stop a process from working but not terminate it. The process is put on hold and can be activated again later. Click Continue to re-activate a suspended process. A pop-up window will prompt you for verification to suspend or continue.

Changing Process Priorities

Click the Priority button to change the priority of a process. This priority determines when the CPU acts on a process. It may have a value from -20 to +20; the smaller the number, the higher the priority. You can enter the desired priority or use the arrow buttons to make your selection.

Monitoring CPU Usage

Choose Activity Monitor from the User menu and then CPU Monitor to view a breakdown of CPU usage by user. The Processes window shows all currently logged-in users, the current number of processes, and the total cumulative CPU usage for each active user (Figure 5-10).

Figure 5-10 Processes window

You can graph all or selected processes, or view individual processes.

Graphing Processes

To graph the processes, highlight the information you want to view and then click the Graph button. A window appears displaying the highlighted items in a graphical format. Press and hold down the middle mouse button to rotate the graph in the direction you move the mouse.

Viewing Processes

To view the processes, highlight the users you wish to view and then Click the Processes button. A window appears displaying all processes for the highlighted users. To further manipulate this information, see <u>"Monitoring Process Status" on page 5-23</u>.