System Reliability Manager for Sun™ Management Center 3.0 Software User's Guide

Sun Microsystems, Inc.
901 San Antonio Road
Palo Alto, CA 94303
U.S.A. 650-960-1300

Part No. 816-0859-10
May 2001, Revision A

Contents

Preface

The *System Reliability Manager for Sun Management Center 3.0 Software User's Guide* provides instructions on how to use the modules that are part of the System Reliability Manager. These add-on packages relate to system administration and management.

Audience

This document is intended for users familiar with the Sun Management Center product; hence, many terms and concepts specific to the Sun Management Center are not explained here. For more information about the Sun Management Center, refer to the *Sun Management Center User's Guide*.

Contents in this Manual

This document describes the System Reliability Manager (SysRM). The SysRM contains five modules. These modules run on the Solaris™ 2.5.1, Solaris 2.6, Solaris 7, Solaris 8 operating environments; on all the platforms on which the Sun Management Center agent can run; and are supported by Sun Management Center 3.0.

This document describes the five modules that are part of the System Reliability Manager:

- OS Crash Dump Analyzer
- File Watcher
- Patch Management

- Script Repository and Script Launcher

OS Crash Dump Analyzer enables you to detect operating system crash dumps and analyze the data contained in them. File Watcher enables you to monitor a list of files for record additions, deletions, and modifications. Patch Management produces alarms on suggested patches. Script Repository and Script Launcher enable you to run scripts on agents.

Sun Management Center users can install the add-on modules, load the modules, and manage the alarm events generated by those modules. For information on Sun Management Center, refer to the *Sun Management Center 3.0 User's Guide* and related material.

Access to Latest Information on the Sun Management Center

For the latest information on the Sun Management Center 3.0 software and the System Reliability Manager (SysRM) Add-on product, refer to the following site:

```
http://www.sun.com/sunmanagementcenter/
```

Using UNIX Commands

This document does not contain information on basic UNIX® commands and procedures, such as shutting down the system, booting the system, and configuring devices. See one or more of the following for this information:

- *Solaris Handbook for Sun Peripherals*
- AnswerBook™ online documentation for the Solaris operating environment
- Other software documentation that you received with your system

Shell Prompts

Shell	Prompt
C shell	*machine_name*%
C shell superuser	*machine_name*#
Bourne shell and Korn shell	$
Bourne shell and Korn shell superuser	#

Typographic Conventions

TABLE P-1 Typographic Conventions

Typeface	Meaning	Examples
`AaBbCc123`	The names of commands, files, and directories; on-screen computer output	Edit your `.login` file. Use `ls -a` to list all files. `% You have mail.`
`AaBbCc123`	What you type, when contrasted with on-screen computer output	`% su` `Password:`
`<abc>` or `<`*`abc`*`>`	These are both acceptable formats that define variables. They are only pertinent to this document and do not denote Sun's standard usage.	`<abc>` `<`*`abc`*`>`
AaBbCc123	Book titles, new words or terms, words to be emphasized	Read Chapter 6 in the *User's Guide.* These are called *class* options. You *must* be superuser to do this.
	Command-line variable; replace with a real name or value	To delete a file, type `rm` *filename.*

Sun Documentation on the Web

The docs.sun.com[sm] web site enables you to access Sun technical documentation on the web. You can browse the docs.sun.com archive or search for a specific book title or subject at:

```
http://docs.sun.com
```

Related Documentation

For a list of related documents, see the *Sun Management Center 3.0 Software Release Notes* on the Sun Management Center website:

```
http://www.sun.com/sunmanagementcenter
```

Sun Welcomes Your Comments

We are interested in improving our documentation and welcome your comments and suggestions. You can email your comments to us at:

```
docfeedback@sun.com
```

Please include the part number of your document in the subject line of your email.

CHAPTER 1

System Reliability Manager Packaging and Installation

This chapter covers the following topics:

The System Reliability Manager Add-on

The System Reliability Manager (SysRM) is installed as an add-on to the Sun Management Center 3.0 software.

The SysRM consists of three packages:

- `SUNWesasm` for agent layer
- `SUNWesssm` for server layer
- `SUNWeshsm` for console or server layer (online help files)

Installing the System Reliability Manager Add-on

When you run the `es-inst` install script, the System Reliability Manager installs the packages, making sure that for each package the corresponding Sun Management Center layer (agent, server, or console) is installed. The script installs the right add-on package on the right layer.

Note – For the agent layer, the module configuration files and libraries are stored in standard Sun Management Center locations. The following directory stores data files: `/var/opt/SUNWsymon/SysMgmtPack/<modulename>`.

▼ To Install the SysRM

1. **Become superuser:**

```
% su
```

2. **Go to the `$BASEDIR` directory where Sun Management Center was installed, for example:**

```
# cd $BASEDIR
```

   where `$BASEDIR` is `/opt/SUNWsymon/sbin`.

3. **Run the following command:**

```
# ./es-inst
```

4. **Provide the source directory of the System Reliability Manager files when prompted:**

```
Please enter the source directory: /<SysRM_directory>/image
```

5. **To install the System Reliability Manager (SysRM), answer "Yes" when prompted.**

   The `es-inst` script will help you to install the System Reliability Manager for the Sun Management Center 3.0 software.

```
This script will help you to install the Sun Management Center
software.
Please enter the source directory: /<SysRM_directory>/image

Target directory: /opt

Sun Management Center 3.0 Addons Product Selection:

Do you want to install the product: System Reliability Manager
Product? [y|n|q]: y
```

6. **SysRM is a licensed product. Enter or install the license for the product as applicable.**

   a. **If you have the Production Environment (PE) of the Sun Management Center software installed on your system, enter the license when prompted.**

   For example, in the Production Environment, you will see the following after you enter "y" in answer to the question on installing SysRM:

```
Do you want to install the product: System Reliability Manager
Product? [y|n|q]: y
Installing the product: System Reliability Manager Product
Please enter System Reliability Manager Product license or press
return: <Enter the License Here>
```

b. If you have the Developer Environment (DE) of the Sun Management Center software installed on your system, install the license manually.

For example, in the Developer Environment, you will not be asked to provide the license during installation. You will only see the following:

```
Do you want to install the product: System Reliability Manager
Product? [y|n|q]: y
```

To install the license for SysRM when you have the Sun Management Center Developer Environment:

i. Go to the following directory:

```
# cd $BASEDIR
```

ii. Use the following script to enter the license:

```
es-lic
```

Setting Up the System Reliability Manager Add-on

Run setup for the System Reliability Manager on the server and agent layers.

▼ To Set Up the System Reliability Manager Add-on

At the end of the installation, `es-inst` prompts you to see whether you want to run setup.

To set up the System Reliability Manager Add-on, do the following:

1. **Answer ‘y’ or ‘n’ depending upon whether you want to run setup.**
   - If you want run setup for all the components found on the system, answer, ‘`y`’ for “Yes.” Running the Sun Management Center setup script invokes the setup script for add-ons automatically.
   - If you want to run setup only for the newly-installed add-on, after installation, answer ‘n’ for “No.”

2. **Become superuser:**

```
% su
```

3. **Go to the following directory:**

```
# cd $BASEDIR
```

`$BASEDIR` is the directory where Sun Management Center is installed. For example:

```
# cd /opt/SUNWsymon/sbin
```

4. **Run the following command to set-up the add-ons:**

```
# ./es-setup -p SystemManagement
```

where `SystemManagement` is the directory where the add-on is installed.

The following is an example of the output from setup on a machine where both the server and the agent layers are installed:

```
Setup for System Reliability Manager - Server Layer
Creating new group: esscrusers

Setup for System Reliability Manager - Agent Layer
System Reliability Manager Setup complete
#
```

- On the server layer, Sun Management Center creates a new group, `esscrusers`. This group is later used by the Script Launcher module.
- On the agent layer, setup cleans up the following directory and regenerates the files needed by the modules:

```
/var/opt/SUNWsymon/SysMgmtPack
```

Removing an Add-on

The Sun Management Center 3.0 software does not allow you to separately uninstall any add-on product currently.

▼ To Remove an Add-on

1. **Remove an add-on, run** `pkgrm` **on** `SUNWesasm`**,** `SUNWesssm`**, and** `SUNWeshsm`**.**

   The `pkgrm` script will remove most of the module-related files from the following directory:

   ```
   /var/opt/SUNWsymon/SysMgmtPack
   ```

   Note – The `pkgrm` script will not remove the `filewatch/scripts` directory or the `script-launcher/scripts` directory in order to save user-defined scripts.

2. **Delete the following** `.dat` **and the** `patch.xref` **files:**

   ```
   /var/opt/SUNWsymon/cfg/filewch.dat
   /var/opt/SUNWsymon/cfg/filewch+filewch.dat

   /var/opt/SUNWsymon/cfg/crashdump.dat
   /var/opt/SUNWsymon/cfg/crashdump+crashdump.dat

   /var/opt/SUNWsymon/cfg/patchmgt.dat
   /var/opt/SUNWsymon/cfg/patchmgt+patchmgt.dat

   /var/opt/SUNWsymon/cfg/script-launcher+<instance_name>.dat
   /var/opt/SUNWsymon/cfg/script-launcher+script_launcher.dat

   /var/opt/SUNWsymon/cfg/patch.xref
   ```

CHAPTER 2

OS Crash Dump Analyzer

This chapter covers the following topics:

The OS Crash Dump Analyzer Module

The OS Crash Dump Analyzer checks the dump configuration of a system and detects OS crash dumps.

This module also does the following:

- It displays the current configuration of the system crash dump data and helps detect OS crash dumps saved in the `savecore` directory.
- Then, it helps you to analyze the crash dumps by printing out the initial system crash dump analysis.
- Finally, it enables you to specify one or more email addresses to which the resulting output can be sent.

The OS Crash Dump module generates:

- An alert alarm when it detects at least one crash dump is detected.
- A caution alarm if `savecore` is disabled, since this is not a recommended configuration.
- A caution alarm for each UNIX or `vmcore` file the module cannot find.

You can configure the alarm thresholds through the Attributes window. For more information on the Attributes window, refer to the *Sun Management Center 3.0 Software User's Guide*.

The `dumpadm` command on which the data acquisition for the module is based is available only on Solaris 7 and 8 operating environments. Therefore, if at setup time the `dumpadm` tool cannot be found, the module prompts for the location of the `savecore` directory. The usual location is `/var/crash/<`*system_name*`>`. This information is then saved in a configuration file:

```
/var/opt/SUNWsymon/SysMgtPack/crashdump/dumpadm.cfg
```

The content of this file is then used (instead of the `dumpadm` command) to get the data. If both the `dumpadm` command and this configuration file are not accessible, the module becomes unavailable and generates an error alarm.

▼ To Access the OS Crash Dump Analyzer

1. **Load the OS Dump Analyzer module.**

   To learn how to load a module, refer to the *Sun Management Center 3.0 Software User's Guide*. The Sun Management Center loads this module under the `Operating System` category. You can also specify your contact email address at this time.

2. **Double-click the Operating System option in the Navigator window.**

3. **Double-click the OS Crash Dump Analyzer option.**

   The Viewer displays the OS Dump Analyzer icon in the Viewer window.

4. **Double click the OS Crash Dumps icon in the Viewer window.**

   Sun Management Center displays the Details window and presents the following OS Crash Analyzer tables:

   - Dump Configuration Property Table
   - List of UNIX/`vmcore` Files Table

   On the right side of each table title, the OS Crash Dump Analyzer displays the associated alarm counts.

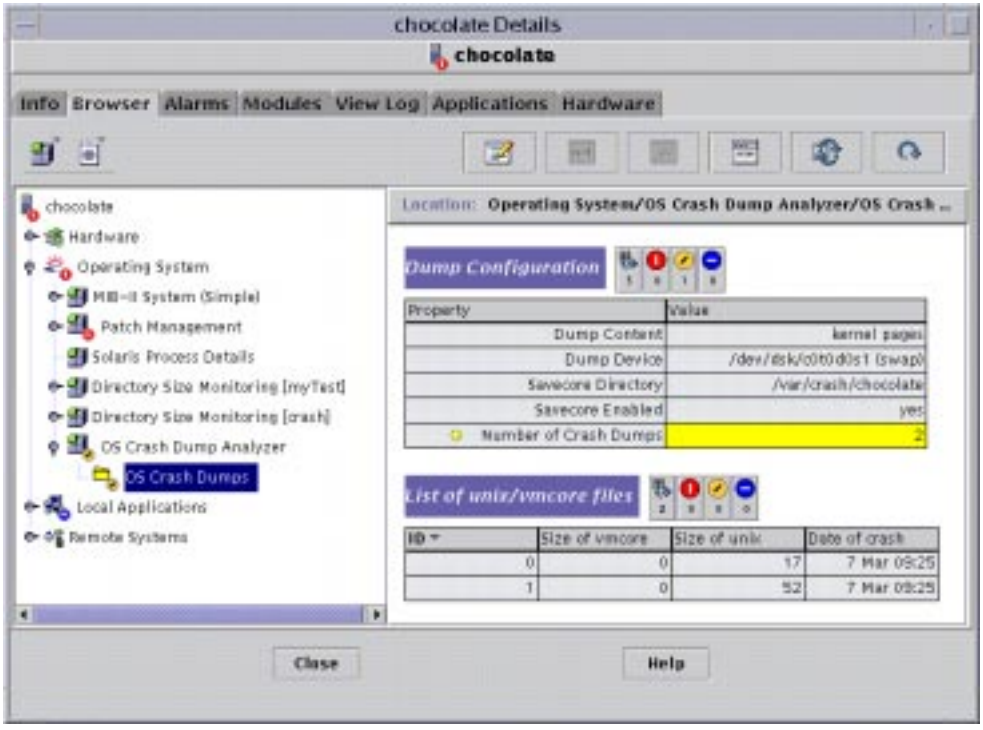

FIGURE 2-1 OS Crash Dump Analyzer Tables

The Dump Configuration Property Table does not show the same information on Solaris 2.5.1 and Solaris 2.6. On these operating systems, only the `savecore` directory and number of crash dumps contain values. In FIGURE 2-1, you see the following:

- Dump Configuration Property Table
- Dump Configuration Property Table Alarms
- List of UNIX/`vmcore` Files Table
- List of UNIX/`vmcore` Files Table Alarms

Dump Configuration Property Table

The Dump Configuration Property Table displays the following values.

TABLE 2-1 Dump Configuration Property Table

Field Name	Description
Dump Content	Includes possible values for any one of the following: • "Kernel pages" for kernel memory pages only • "All pages" for all memory pages
Dump Device	Possible values include: • "Dump-device," which is a specific dump device specified as an absolute pathname, such as `/dev/dsk/cNtNdNsN` • "Swap," where if the special token *swap* is specified as the dump device, `dumpadm` examines the active swap entries and selects the most appropriate entry to configure as the dump device.
Savecore Directory	Path to the `savecore` directory.
Savecore Enabled	"Yes" when enabled; "No" when disabled.
Number of Crash Dumps	Number of crash dumps detected in the `savecore` directory.

Dump Configuration Property Table Alarms

- The Dump Configuration Property Table Alarms module generates a warning alarm if it detects at least one crash dump.
- The module generates an information alarm if `savecore` is disabled.

Note – The alarm threshold is configurable through the Attribute Editor window.

List of UNIX/vmcore Files Table

The List of unix/vmcore Files Table gives more information about each crash dump.

TABLE 2-2 List of unix/vmcore Files Table

Field	Description
ID	File identification
Size of vmcore	Size of vmcore file
Size of unix core	Size of UNIX core file
Timestamp	Timestamp

List of UNIX/vmcore Files Table Alarms

- The module will generate a caution alarm for each unix.x or vmcore.x file that it cannot find.

Available Commands

This module offers commands at the following levels:

- From the Navigator
- At the Managed Object Level
- At the List of UNIX/vmcore Files Table Level

From the Navigator

▼ To Access OS Dump Analyzer Commands

- **Proceed with one of the following:**
  - Right-click any object in the Navigator or Viewer window at the Managed Object level.
  - Right-click any field, row, or column to access commands at the lower levels.

To access the OS Dump Configuration and the crash dumps, refer to “To Access the OS Crash Dump Analyzer” on page 8.

At the Managed Object Level

▼ To Display the Savecore Filesystem Size

- **Right-click OS Crash Dumps at the Navigator window and select** `Savecore Filesystem Size`**.**

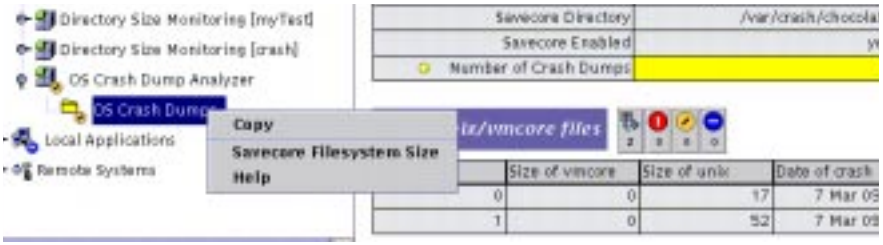

FIGURE 2-2 `savecore` Filesystem Size Command

Sun Management Center displays the Probe Viewer window with the results of the above command:

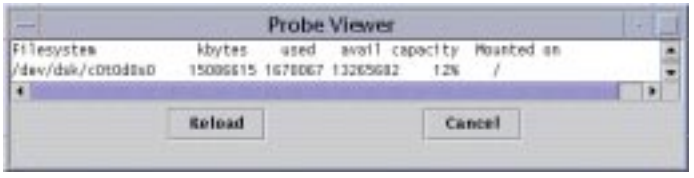

FIGURE 2-3 `savecore` Filesystem Size Command Output

At the List of UNIX/`vmcore` Files Table Level

▼ To Analyze the Crash Dump

1. **Select a crash dump in the list.**

2. **Right-click anywhere on the row.**

   SysRM displays a pull-down menu of choices.

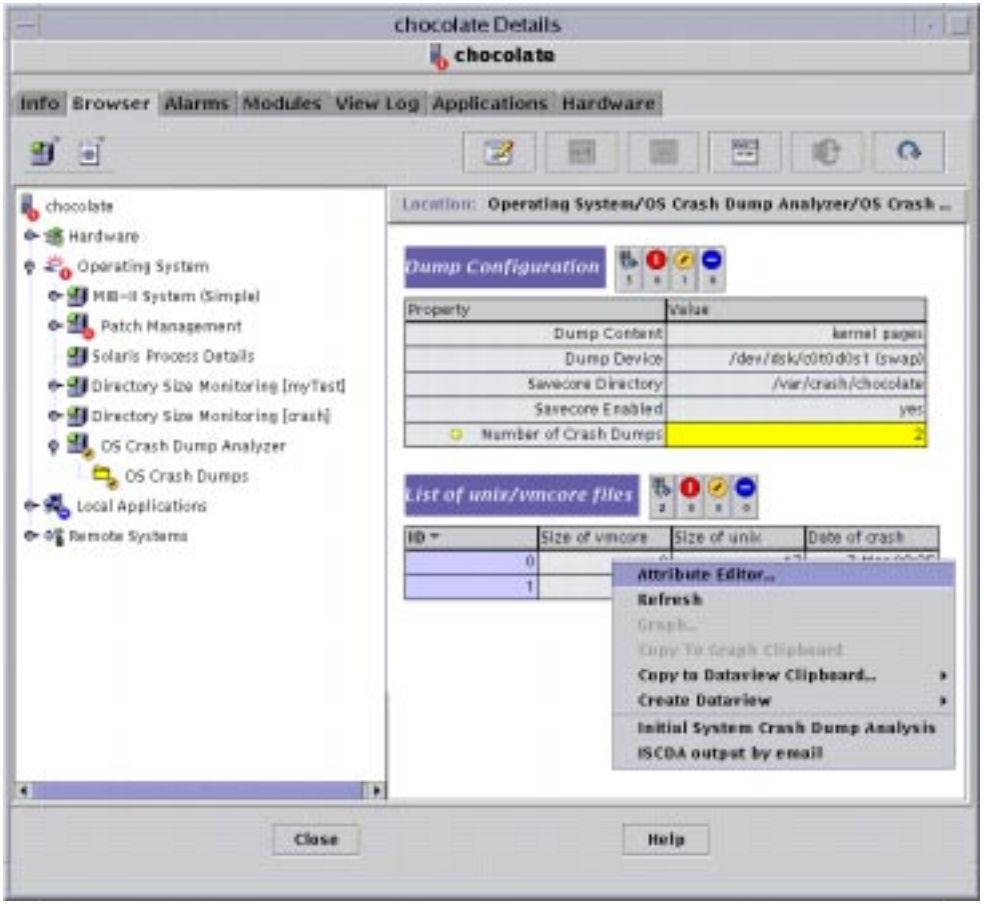

FIGURE 2-4 Row Level Probe Commands

3. **Select Initial System Crash Dump Analysis.**

   This option displays the results in the Probe Viewer window. The information includes stack trace, process information, message buffers, and other such detail.

   If files are corrupted, for example, the Probe Viewer displays an incomplete report providing only status information.

▼ To Send Notification Mail

1. **Select a crash dump in the list.**

   Sun Management Center displays menu choices (FIGURE 2-4).

2. **Right-click and select** `ISCDA output by e-mail.`

   This option sends an email with the output to the specified contact person. If a contact email address is available, the Probe Viewer displays the results with the current status of the email notification.

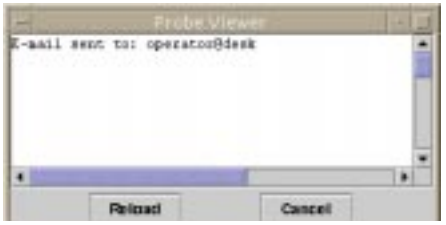

FIGURE 2-5 Email Sent Successfully

If an address is not available, it displays the status and aborts the function.

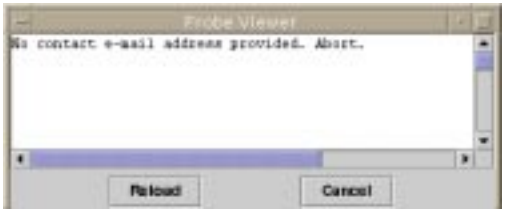

FIGURE 2-6 Results When Email Address Not Provided

▼ To Specify an Email Address

The module assumes that you provided an email address when you loaded the module. To specify an email address, do the following.

1. **Select** `OS Crash Dump Analyzer` **in the Navigator window.**
2. **Right-click and select the** `Edit Module` **from the menu.**
3. **Fill in the contact email address.**
4. **Click OK.**

CHAPTER 3

File Watcher

This chapter covers the following topics:

The File Watcher module monitors a list of files for additions, deletions, and modifications. If changes are detected, it builds events and displays them in a table. It provides default capabilities for some of the popular files, such as `passwd`, `vfstab`, and so on.

You can add, remove, or edit entries in this default list. To add a new file, you must define the record format of the file being monitored. In the case of a record addition event, a record deletion event, or a record modification event, you have to also specify the file-specific severities of the alarms to be generated.

Note – The purpose of the File Watcher module is to monitor files that are not modified frequently, and therefore, it is useful to get notified when a change occurs. Therefore, module should only be used to monitor system files that are not expected to change frequently, for example, the `passwd` file.

The File Watcher Module

▼ To Access the File Watcher or the File Watch Module

1. **Load the File Watch module.**

   For instructions on how to load a module, refer to the *Sun Management Center 3.0 User's Guide*.

2. **Double-click** `Local Applications` **in the Navigator window.**

3. **Double-click on** `File Watch` **in the Navigator window.**

4. **Double-click on the** `File Watcher` **option.**

   The Viewer displays the File Watch icon in the Viewer window.

5. **Double click on the** `File Watch` **icon in the Viewer window.**

   Sun Management Center displays the following File Watch tables:

   - Watched File Table
   - File Change Table

   On the right side of each table title, File Watch lists the associated alarm counts.

   The Watched File Table is used to monitor the existence of files. The Change Table is used to monitor the changes in existing files.

   File changes can only be noticed once the file has been detected as *existing*. This means that if a file does not exist or is non-existing, the module detects that it is existing with a size bigger than 0. For example, when a file has two records already, the module will not be able to notice those two records. However, the module will notice all future modifications.

FIGURE 3-1 displays the File Watcher tables.

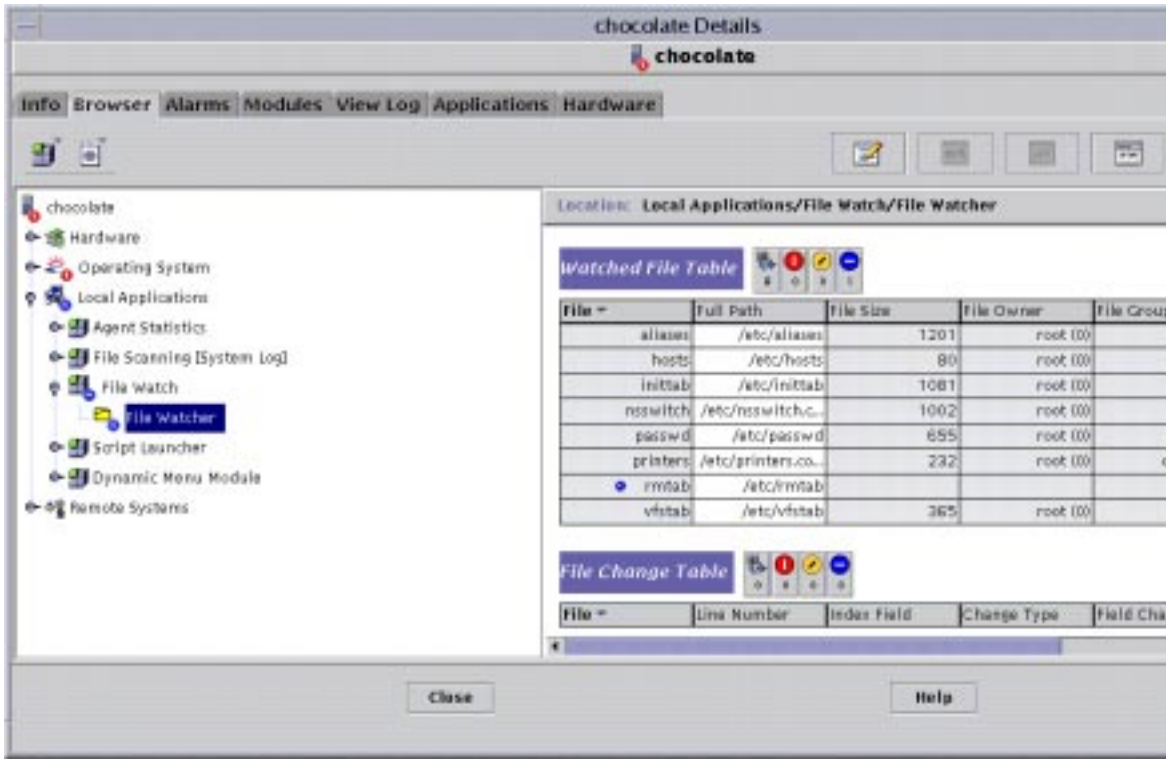

FIGURE 3-1 File Watch Module

This table is initialized with seven system files through `filewch.dat`:

- `/etc/hosts`
- `/etc/aliases`
- `/etc/nsswitch.conf`
- `/etc/inittab`
- `/etc/vfstab`
- `/etc/passwd`
- `/etc/printers`
- `/etc/mnttab`
- `/etc/rmtab`

Watched File Table

The Watched File Table lists all the files being monitored by the module. It displays some of the more commonly used attributes at the top level and other hidden attributes in a lower level. For more information on hidden attributes, refer to “To Access Hidden Attributes” on page 18.

Displayed Attributes

The Watched File Table displays information about each file and provides the data on the following.

TABLE 3-1 Watched File Table

Field	Description
Name	Name of the file
Full Path	Path to file and the real name
File Size	Size of the file in bytes.
File Owner	The owner of the file
File Group	The group the file belongs to
File Permissions	Permissions on the file
Timestamp	Time when the file was last updated
Validation Script	It is the path to the validation script to be used to validate the file (for a row) when its timestamp changes. Save the script in `/var/opt/SUNWsymon/SysMgmtPack/filewch/scripts` and enter the path as one that is relative to this directory. The value for script may or may not be provided.
Exit Code	Displays the exit code of the last execution of the validation script.

▼ To Access Hidden Attributes

1. **Select a row.**
2. **Right-click and select Edit Row.**

   Sun Management Center displays the Row Editor with all the attributes displayed in the Watched File Table, and those that are hidden.

Hidden Attributes

The following attributes are hidden and can be accessed by right clicking on any row and selecting Edit Row. You will see the Row Editor.

TABLE 3-2 Row Editor

Field	Description
Delimiter	Delimiter between columns.
Comment char	Type of the char that delimits a comment line.
Number of fields	Number of fields in each file entry.
Num key field	Number of fields composing the key. The key is assumed to be at the beginning of the record. A key is an identifier for the record. For example, in the `passwd` file, the key for each record is the first field: `user name`. It is unique for each record.
Field names	Names of the different columns in the file entries.
Hide values flag	One of the following values: • FALSE = Display the value that changed • TRUE = Do not display
Addition Severity	Possible values: Info, Warning, Error, None.
Deletion Severity	Possible values: Info, Warning, Error, None.
Change Severity	Possible values: Info, Warning, Error, None.
Record Format	Format of the record. Refer to “Validation Script” on page 19 for more information.

Validation Script

During a refresh, if the module detects that the timestamp of a file has changed, the validation script associated with the file, if provided, will be executed. The exit code of the last execution will be displayed in Exit Code. When a new value is given to the script field, the module checks if the path given is a valid file. If it is not, the Exit Code field will display `NO_SUCH_SCRIPT`. (The field could also display “`killed`” in the event that the validation script running was killed. In this case, specify regular expressions on which to generate alarms for Exit Code.)

You can place your own scripts in `/var/opt/SUNWsymon/SysMgmtPack/filewch/scripts` or use the `fileparse` binary installed with the module.

- If `fileparse` is specified, the module will ignore the parameters provided and will build the arguments from the delimiter, comment, and record format values known for the file.

- If you specify a value such as
  “`fileparse -c 55 -d 556 -f “STRING*” -n /tmp/banana`”
  for example, all the parameters will be replaced by the ones built into the module, to make sure no unsupported comment or delimiter gets specified.
- If you specify “`mytest.sh -a myarg`”, the script executed will be the `mytest.sh` script, with `-a myarg` as argument.

Fileparse

The default list of files has a value set for Validation Script and Record Format. For example, for `/etc/hosts`:

- Validation Script is set to `fileparse`
- Record Format is set to `IPADDRESS STRING STRING`

`fileparse` is a C binary located in:

```
/var/opt/SUNWsymon/SysMgmtPack/filewch/scripts/
```

It accepts four arguments: delimiter, comment, record format, filename. Its usage is:

```
./fileparse -d index -c index -f record_format -n input_filename
```

The binary parses an input file against the file format specified as parameters, and reports an error if the file contents do not conform to the input file format. Blank lines and comment lines are skipped. The default comment is “NULL”, which means there is no comment. The binary returns the following values:

```
0: Success;

1: cannot open file.

2: record_format is not correct.

3: input_file’s format is not correct.

-1: program error, such as not enough memory.

-2: argument error.
```

Fileparse Arguments

`fileparse` accepts four parameters. The module will provide the correct values as arguments when `fileparse` is invoked.

```
%fileparse -d index -c index -f record_format -n input_filename
```

where

`-d index`	Specifies the delimiter index;
`-c index`	Specifies the comment index;
`-f record_format`	Specifies grammar expression, where grammar expression support 4 kinds of operation on datatypes.

The datatypes supported are:

```
datatype = {STRING, INT, IPADDRESS, ZERO_STRING, CONST}
```

where

`STRING`	The string can not be empty.
`ZERO_STRING`	The string can be empty or not empty.
`CONST`	The field value must match.

A constant string can be declared by enclosing it in double quotes. For example:

```
“+” | “-” | STRING STRING
```

Syntax of record format:

The operators available are:

```
operator = | , [], *
```

where

|	Means “or”. For example: - line-format = “+” | “-” | STRING STRING
[]	Means optional. For example: - line-format = STRING [STRING|IPADDRESS]
*	Means zero or multiple repetition of one datatype. For example: - line-format= IPADDRESS STRING STRING*

For example, the record format to validate `/etc/passwd` is:

```
STRING STRING INT INT ZERO_STRING STRING ZERO_STRING | “+” | “-”
```

The precedence of the operators is:

```
[] , | , *
```

Watched File Table Alarms

- You can use the Attribute Editor to set a regular expression alarm threshold on Exit Code. There is no default alarm threshold.
- If the file to be monitored does not exist, File Watcher generates an info alarm. However, it still adds the file to the Watched File Table but does not display any other information about this file.
- If the file to be monitored (such as a directory) exists but cannot be opened, File Watcher adds it to the Watched File Table, however, it displays no other information on this file. It also generates an information (`info`) alarm in this case.

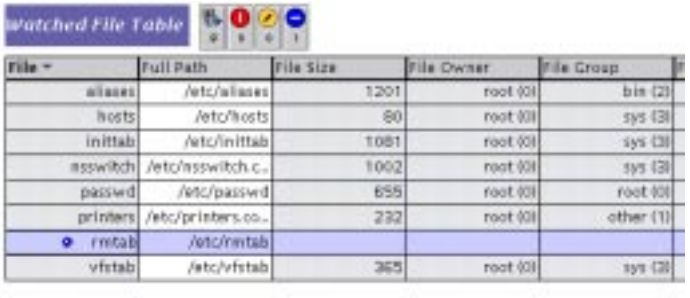

FIGURE 3-2 Handling of Erroneous File Names

File Change Table

The File Change Table monitors files and displays their record additions, deletions, or modifications.

Displayed Attributes

The File Change Table displays information about each file and provides the data on the following.

TABLE 3-3 File Change Table

Field	Description
File Name	Name of the file.
Line Number	The number of the line.
Index Key	Value found in the key field for the changed record.
Change Type	Whether one of the following occurred: addition, deletion, or change.
Field Changed	One of the following: • In case of an addition or a deletion, the cell displays “All.” • In case of a change, the cell displays the column name, as specified when the “Watched File” entry was created.

TABLE 3-3 File Change Table *(Continued)*

Field	Description
Old Value	One of the following: • Since this pertains to an old value, in case of a new addition, the cell displays “NA.” • If the hidden value flag for this file is set to TRUE, the cell displays “hidden.” • The actual old value.
New Value	One of the following: • Since this pertains to a new value, in case of a deletion, the cell displays “NA.” • If the hidden value flag for this file is set to TRUE, the cell displays “hidden.” • The actual new value.
Time Changed	The time when the changes occurred.

File Change Table Alarms

- When File Watcher detects a new event, it displays the event and generates the corresponding alarm that was specified when the file was added to the Watched File Table. File Watcher colors the File Name cell the color appropriate to the event value (`info`, `warning`, `error`, or `none`) you specified when you added the file to the Watch File Table.
- When the probe function, “Dump all events to log,” is invoked, the rule leaves the open state.

Available Commands

Commands are available at the following levels:

- At the Watched File Table Level
- At the File Change Table Level

At the Watched File Table Level

▼ To Add a New File to the List of Files to Be Monitored

1. **Right-click over the header or any selected row in the table to access the pull-down menu commands.**

FIGURE 3-3 Watched File Table Commands

2. **Select Add Row.**
3. **Add a row to add a file.**
4. **Enter the following values to describe the format of the file to be monitored.**

TABLE 3-4 Watched File Table Entries

Field	Value to Enter
Name	Enter a meaningful name.
File Name	Enter the complete path to the file.
Delimiter	Enter the type of the delimiter.
File Comment Char	Enter the type of the character that delimits the comment line. The only possible values are: `tab`, `colon`, `semicolon`, `comma`, `hash`, and `pipe`. You can select the value from the pull-down menu in the Row Add or Row Edit windows.

TABLE 3-4 Watched File Table Entries *(Continued)*

Field	Value to Enter
Number of Fields	Enter the number of fields in each file entry.
Num Key Field	Enter the number of fields composing the key. The key is assumed to be at the beginning of the record.
Field names	Enter the meaningful names of the different columns in the file.
Hide values flag	Possible values are: • FALSE = Display the value • TRUE = Do not display the value. (This is used to prevent users with insufficient privileges from viewing information they should not have access to.)
Addition Severity	Info, Warning, Error, None.
Deletion Severity	Info, Warning, Error, None.
Change Severity	Info, Warning, Error, None.
Validation Script	It is the path to the validation script to be used to validate the file (for the row) when its timestamp changes.
Record Format	Format of the record (if `fileparse` is specified as the only required validation script).
Exit Code	The code to exit.

▼ To Modify or Edit a Row

1. **Select the row where the file name is present.**
2. **Right-click and select Edit Row.**
3. **Modify the path name and the definition of the record format of the file.**
4. **Click OK.**

▼ To Delete a Row

1. **Select the row where the file name is present.**
2. **Right-click and select Delete Row.**
3. **Remove a file from the list of files to be monitored.**

Note – If you remove a file from the list of files to be watched, the events that have already been detected for that file will not be automatically removed from the events log and will continue to be displayed in the File Changes Table. To clear the File Change Table, issue the Dump events to log command.

At the File Change Table Level

▼ To Dump Events to a Log

1. **Right click anywhere in the row.**

FIGURE 3-4 File Change Table Properties

2. **Select Dump events to log.**
3. **Delete the corresponding events by moving** `events.log` **to** `events_<`*timestamp*`>.log` **in the log directory.**

   The Probe Viewer then provides the location of the log file to which `events.log` was moved.

FIGURE 3-5 Output of the Probe Command

CHAPTER 4

Patch Management

This chapter covers the following topics:

The Patch Management Module

The Patch Management module generates alarms on uninstalled patches. The alarm level depends on the type of patch. It requires an external file to exist on the host being monitored. This external file is called `patch.xref` or the cross reference patch matrix. Based on the content of a `patch.xref` file, the Patch Management module detects the number of patches that are available but not installed and generates alarms against those counts. The module also lists the suggested patches in a table. The table can be filtered on the suggested patch category.

This module performs the following functions:

- Checks installed patches and detects uninstalled patches.
- Displays the list of missing patches in a table and enables you to run a command to get the list of packages and patches installed on the system.
- Displays important categories buried within the `patch.xref` file. It displays this information in the Patch Matrix table. (Refer to “Patch Matrix” on page 32 for more information.) It also displays the number of uninstall patches of the following type:
  - recommended security
  - security
  - recommended
  - regular
- Generates alarms when the number of uninstall patches reaches a certain threshold. These thresholds are configured through the Attribute Editor window.

The `patch.xref` File

The `patch.xref` file is bundled with the module. It is a formatted version of the `patchdiag.xref` file that is available from SunSolve[SM], a group within Sun that provides its contract customers with up-to-date patches.

▼ To Access the Patch Management Module

1. **Load the module.**
2. **Double-click on the Operating System folder.**
3. **Double-click on Patch Management module.**
4. **Double-click on Suggested Patches.**

   The Patch Management module displays the following tables:

   - Patch Matrix
   - Patch List Filtering Options
   - Patch List

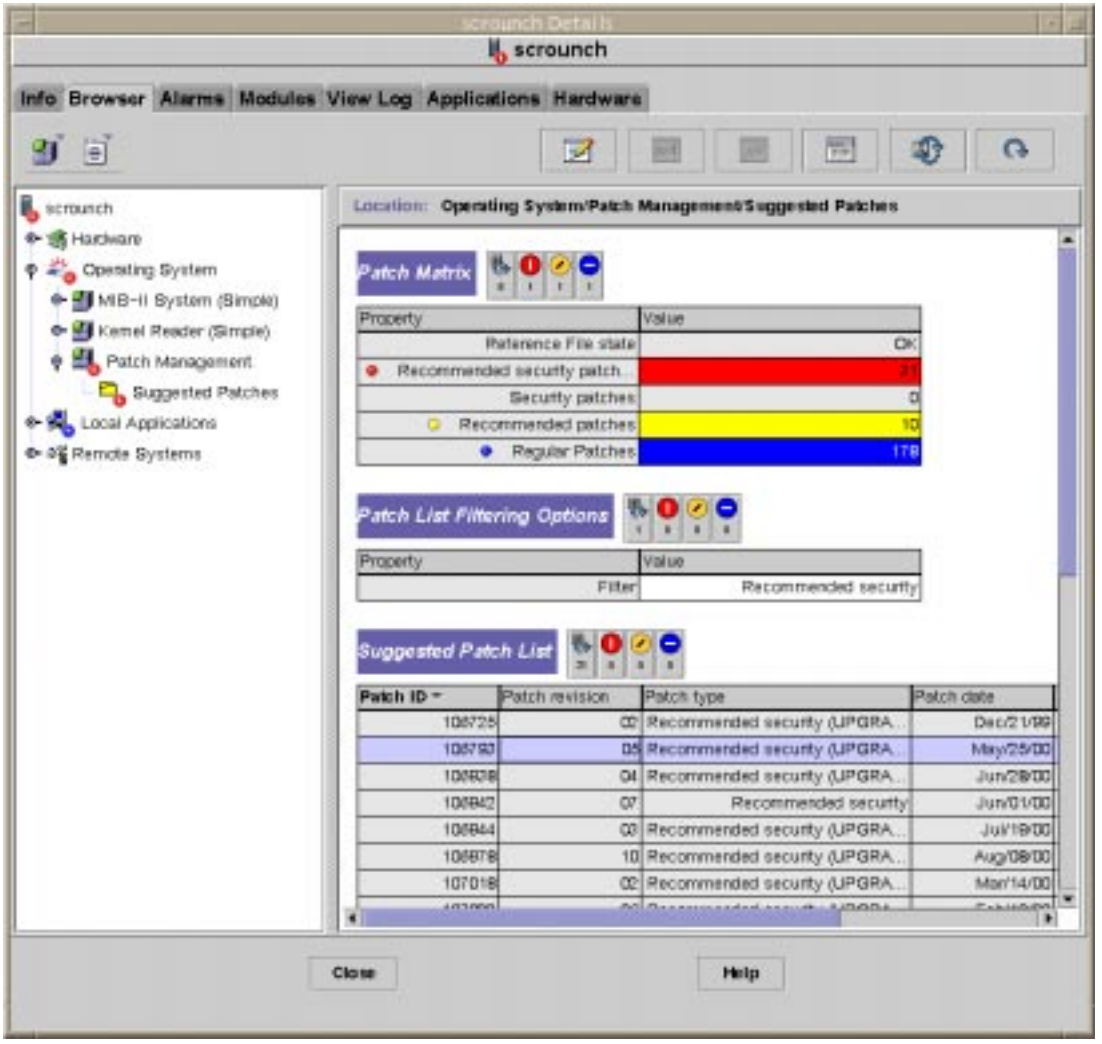

FIGURE 4-1 Patch Management Module

Patch Matrix

At the top of the window, a property table displays the number of patches from each type that are missing from the monitored system. The first field lists the properties and the second column displays their color-coded values to represent each state:

TABLE 4-1 Patch Matrix State

Patch Matrix State	Description
Patch matrix state	One of the following: • OK • UNUSABLE: This patch matrix state means that the `patch.xref` file in `/var/opt/SUNWsymon/cfg` is either missing or corrupted. For more information, refer to “Alarms” on page 33.
Recommended security patches	The number of patches of this type.
Security patches	The number of patches of this type.
Recommended patches	The number of patches of this type.
Regular Patches	The number of patches of this type.

Patch List Filtering Options

The Patch List Filtering Options table presents a filter combo box where you can select the type of missing patches to be displayed in the table. It is initialized to “Recommended Security.”

You can select one of the following values:

- Recommended Security
- Security
- Recommended
- Regular
- All

FIGURE 4-2 Patch List Filtering Options

Suggested Patch List

This table lists the missing patches and the following information about them.

TABLE 4-2 Missing Patch Information

Patch ID	The identification number of the patch.
Patch revision	The revision number of the patch.
Patch type	One of the following: • Recommended Security • Security • Recommended • Regular If "(UPGRADE)" appears next to the patch type, it means that an older revision of the patch is already installed on your system. We however recommend that you install and access a newer version.
Patch date	The date the patch was created.
Packages affected	The packages that are impacted.
Patch description	The description of the patch.

Alarms

The Patch Management module generates the following alarms:

- If the `patch.xref` cannot be opened or read or if it seems corrupted, for example, when an entry does not contain the expected number of fields, SysRM generates a warning alarm. Basically, if the patch matrix state is unusable, the module generates a warning alarm. To correct the problem, make sure that the `patch.xref` file is identical to the one installed in Sun Management Center.

Correct the problem by making the necessary changes or by running the add-on setup and overwriting the `patch.xref` file already present in `/var/opt/SUNWsymon/cfg` (you will be prompted for confirmation).

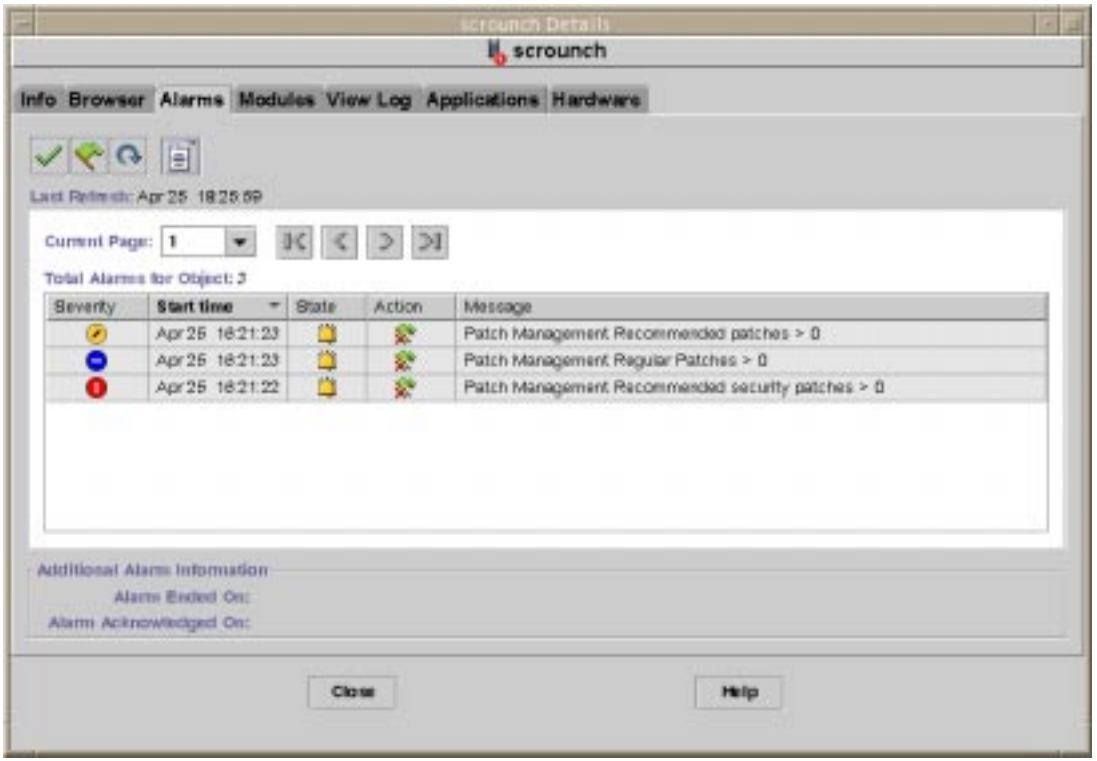

FIGURE 4-3 Alarm to Reflect Problem

- The module generates an alarm when the number of un-installed patches in each category reaches a certain threshold.

Recommended Security	`error-gt = 0`
Security patches	`error-gt = 0`
Recommended patches	`warning-gt = 0`
Regular patches	`info-gt = 0`

Note – You can configure these thresholds through the Attribute Editor window.

Available Commands

A new window is launched to display the output of the different commands.

At the Managed Object Level

▼ To View Installed Patches and Packages

1. **Double-click Patch Management in the Navigator window.**
2. **Right-click on Suggested Patches to view the pull-down menu commands.**

   a. Select Show Installed Patches to view a patch list.

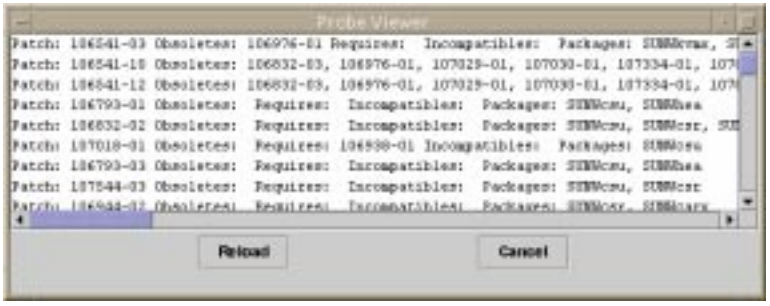

FIGURE 4-4 Show Installed Patches Results

b. Select Show Installed Packages to view a list of available packages.

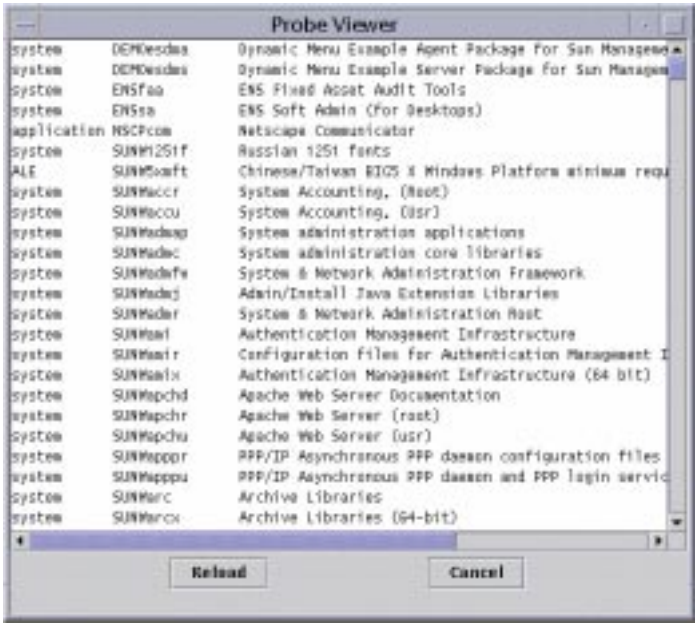

FIGURE 4-5 Show Installed Packages Results

At the Suggested Patch List Table Level

▼ To View the Suggested Patch List Table Commands

1. **Right-click on a row in the Patch List Table.**

   The module displays choices for viewing references to patches in the `patch.xref` file and installed patches.

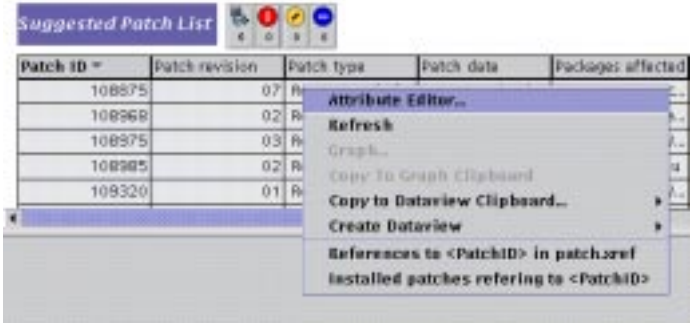

FIGURE 4-6 Available Commands at the Row Level of the Patch List Table

a. Select References to <PatchID> in patch.xref to view the following results:

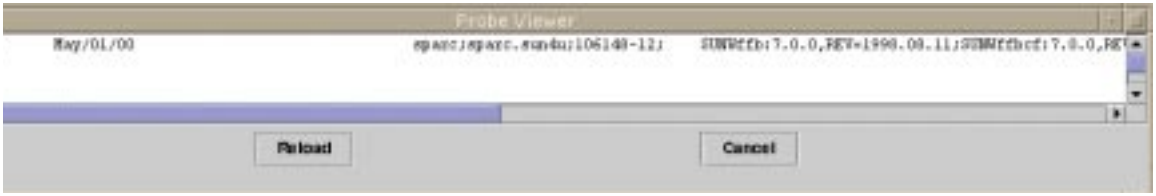

FIGURE 4-7 References to Selected Patch in `patch.xref`

b. Select Installed patches referring to <PatchID> to view the following results:

FIGURE 4-8 Example of Installed Patches making Reference to the Selected Patch

The following example illustrates the result when there is no installed patch making reference to the selected patch ID.

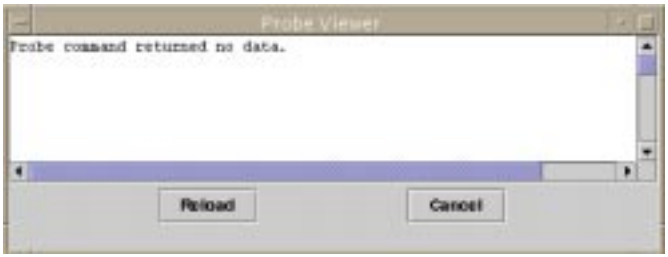

FIGURE 4-9 Example When There is No Installed Patch Making any Reference

At the Patch List Filtering Options Level

▼ To Filter the Category of Suggested Patches to Be Displayed

1. **Go to the pull-down menu in Patch List Filtering Options.**

   The result is listed in the Patch List table.

2. **Click OK to commit the value.**

Downloading a New Matrix

The patch matrix is updated when patches are released. Customers with support contracts receive notices of such updates through their regular channels. As a customer, you can download the matrix from the SunSolve web site.

▼ To Download a New Matrix

1. **Download the new matrix from the following FTP site:**

```
ftp://sunsolve.Sun.COM/pub/patches/patchdiag.xref
```

2. **Use the script,** `patchdiag-convert.sh`, **to the convert the matrix to the right format. If the Sun Management Center was installed in the default** `/opt` **directory on a system running the Solaris 7 operating environment, then the conversion shell script is in the following location:**

```
/opt/SUNWsymon/util/bin/sparc-sun-solaris2.7
```

3. **Copy the new file manually to the following location:**

```
/var/opt/SUNWsymon/cfg/patch.xref
```

When running setup, you can choose to have the above file overwritten by the one in the following location:

```
$BASEDIR/base/cfg
```

CHAPTER 5

Script Repository and Script Launcher

This chapter covers the following topics:

The Script Repository and Script Launcher modules enable you to execute scripts that perform arbitrary management tasks on remote devices. Executing scripts on remote devices reduces the processing load on a central management station and provides a mechanism for keeping polling local.

This section details the following topics:

- Script Information
- Launch Area
- Available Commands

The Script Repository Module

The Script Repository module enables you to view the scripts available on the agent to be run by the Script Launcher module. The Script Repository module also lists the languages supported by the Script Launcher module.

▼ To Access the Script Repository Module

1. **Load the module.**

   See the *Sun Management Center 3.0 User's Guide* for more information. The Script Repository module is available under Local Applications in the Navigator window.

2. **Double-click Local Applications in the Navigator window.**

3. **Double-click Script Repository.**

   The Script Repository displays the following folder or group in the Viewer:

   - Script Information

   a. **Double-click Script Information to view the Language Table and the Script Table.**

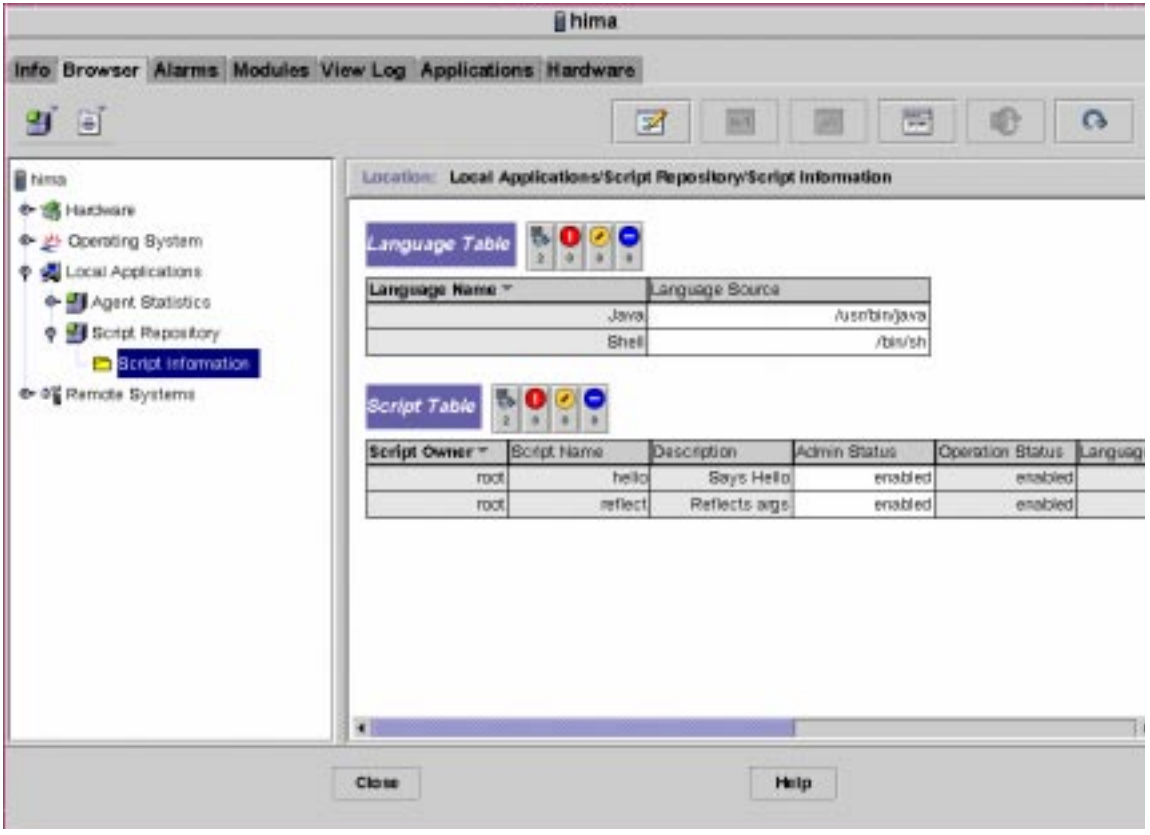

FIGURE 5-1 Script Repository Module

Script Information

This group includes two tables:

- The Language Table, which lists the supported languages (currently, Java and shell script).

- The Script Table, which enables you to view available scripts on the agent.

Language Table

The first table in the Script Information group is the Language Table. It lists all the scripting languages supported on the agent. Each table entry has the following attributes:

- Language Name (for example, Java)
- Language Source (for example, `/usr/java`)

There are no commands available on this table. You cannot specify a new language or remove a language. The number of entries is fixed and is defined by the implementation of the module and the languages it supports.

You can modify only the Language Source field.

▼ To Change the Language Source

1. **Update the entry in the cell.**

   For example, if you want to change `/usr/java` to `/usr/java1.2`, enter it directly in the cell. The information that you enter here is made persistent.

Note – If you enter an invalid path name or file name, you will receive an alarm.

---

2. **Click OK to acknowledge, or Cancel to cancel, your edits in the confirmation box, as shown in** FIGURE 5-2**.**

FIGURE 5-2 An Alert Box Seeking Confirmation

▼ To Detect Alarms

- **SysRM generates an information (INFO) alarm if the language cannot be found at the specified location.**

Script Table

The Script Table lists all scripts known to the Script Launcher on the agent. Each entry in the table has the following attributes.

TABLE 5-1 Script Table Values

`Script Owner`	The user on the agent who owns this script.
`Script Name`	The script name.
`Description`	A description of the purpose of the script.
`Admin Status`	• Enabled indicates that the owner allows the script to be used by others. • Disabled indicates that the owner does not allow the script to be used by anyone else.
`Operation Status`	For example: • Enabled indicates that the script is available and can be started by a launch table entry. • Disabled indicates that the script cannot be used. • `NoSuchScript` indicates that the script does not exist at the specified location. • `WrongLanguage` indicates that the language is not known.
`Language`	The language in which the script is written. This value needs to be one of the languages listed in the ”Language Table.”
`Script Source`	File name of the script.
`Default Argument`	The default argument for this script.
`Script Users`	The users who are permitted to use this script.
`Groups`	The UNIX groups which are permitted to use this script.

Note – The only field you can modify is the Admin Status through the browser. The Admin Status is the area where you enter the desired status of your script. For example, the Admin Status can be “`enabled`” or “`disabled`.” While this choice reflects your desired status, only the Operation Status reflects the actual status once the module determines that all criteria have been met and are ready.

Script Table Alarms

- An info alarm will be issued if the script is not in a supported language.
- An info alarm will be issued if the script is not accessible.

The `ScriptInfo.dat` File

The `ScriptInfo.dat` contains information about the scripts that are available to be run. You can add a new script to the `ScriptInfo.dat` file so that the module recognizes it. All the scripts that belong to a user must be listed in this file.

▼ To Add a New Script

1. **Write a new script.**

   The format of the `ScriptInfo.dat` file follows the standard configuration file format.

   ```
   <slice>:<attribute>=<value>
   ```

2. **Save the new script in the `ScriptInfo.dat` file.**

   You can access the `ScriptInfo.dat` file in the following directory identified by your user name.

   For example:

   ```
   /var/opt/SUNWsymon/SysMgmtPack/script-launcher/scripts
   ```

3. **Place the information in the above directory.**

   If this file already contains information about a script, add your script below the current information.

   An example of the `ScriptInfo.dat` file, with two scripts, follows:

```
Script1:Owner = Scott
Script1:Name = MyHello
Script1:Desc = Says Hello
Script1:Language = Java1.2
Script1:Source = Hello.class
Script1:AdminStat = 1
Script1:OperStat = 1
Script1:Users = Noble
Script1:Groups = Staff
Script2:Owner = Denise
Script2:Name = MyFile
Script2:Desc = Says Hello
Script2:Language = Java1.2
Script2:Source = Hello.class
Script2:AdminStat = 1
Script2:OperStat = 1
Script2:Users = Noble
Script2:Groups = Staff
```

Security for Script Repository

The security for Script Repository is implemented as follows:

- Only the root user can place scripts in the following directory:

```
/var/opt/SUNWsymon/SysMgmtPack/script-launcher/scripts
```

- Each script specifies the users and groups who are allowed to execute the script. These are specified as entries within `Users` and `Groups` in the script configuration file. In addition these fields can be modified from the console through the Script Table. Only `esadm` users are allowed to modify these fields.
- `root` cannot be in the `Script Users` field of the Script Table.

The Script Launcher Module

The Script Launcher module enables you delegate management functions to agents. (Management functions are defined as management scripts written in a management scripting language.) The Script Launcher module is a multi-instance module. All instances of the Script Launcher module access the same Script Repository module for language and script information.

The Script Launcher module enables you to:

- Control who is allowed to read, write, and execute scripts from the Script Repository module.
- Specify arguments for management scripts.
- Initiate and terminate management scripts.
- Monitor and control running management scripts.
- View the results produced by running management scripts.
- Control who is allowed to read, write, and execute scripts.

▼ To Access the Script Launcher Module

1. **Load the module.**

   See the *Sun Management Center 3.0 User's Guide* for more information. The Script Repository module is available under Local Applications in the Navigator window.

2. **Double-click Local Applications in the Navigator window.**

3. **Double-click Script Launcher.**

   The Script Launcher displays the following two folders or groups in the Viewer:

   - Launch Table
   - Result Table

   a. Double-click Script Launcher to view the Launch Table and the Result Table.

Launch Area

This group includes two tables:

- The Launch Table enables you to create an entry, add a row, or define a script to be launched by creating an entry.
- The Result Table enables you to view the results of running a selected script.

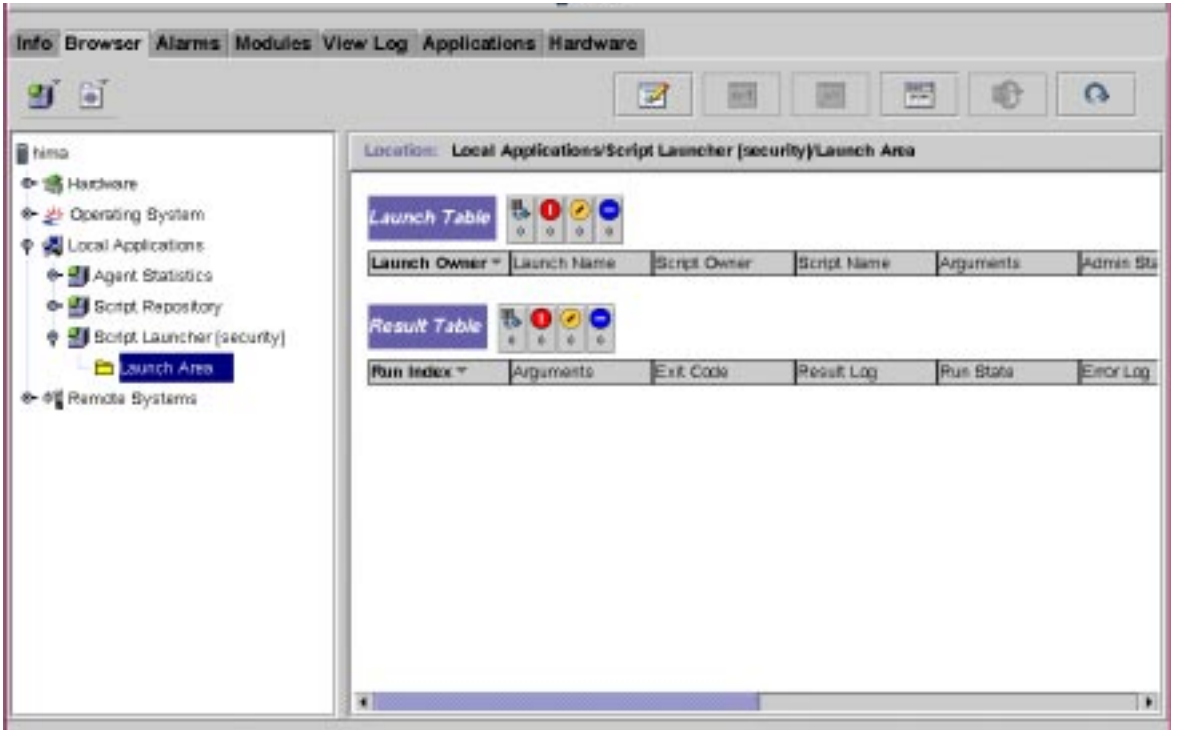

FIGURE 5-3 Script Launcher Module with the Launch Area Displayed

Launch Table

The Launch Table controls the execution of all scripts. The Launch Table describes scripts that are ready to be launched along with descriptions of their parameters. An entry in the Launch Table attaches an argument to a script.

An entry in the Launch Table also defines the owner, used to associate permissions to execute the script. Several instances of a script may be created through one single entry on this table, and several entries on this table may point to a same script on the Script Table. You can execute several identical scripts with different arguments and permissions.

Launch Table Attributes

The Launch Table has the following attributes.

TABLE 5-2 Launch Table Attributes

`Owner`	The manager who owns this entry.
`Name`	The name of the entry. This should be unique for each row in the launch table.
`Script Owner`	In combination with the script name, it identifies the script.
`Script Name`	In combination with the script owner, it identifies the script.
`Arguments`	Arguments to be supplied to the script.
`Admin Status`	The value of this object indicates the desired status of this launch table entry, which can be either “enabled” or “disabled.”
`Operation Status`	The value of this object indicates the actual status of this launch table entry, which can be either “enabled” or “disabled.”
`Max Running`	The maximum number of concurrently running scripts that may be invoked from this entry. The default value is 3. This field can be modified by directly writing into the field.
`Max Completed`	The default value is 3. The maximum number of finished scripts invoked from this entry in the “Launch Table” allowed to be retained in the “Result Table.”
`Life Time`	The default maximum amount of time a script launched from this entry may run. The default value is 86,400 seconds (1day).
`Expire Time`	The default maximum amount of time information about a script launched from this entry is kept in the “Result Table” after the script has completed execution.

Result Table

The Result Table lists all scripts that are currently running or have recently terminated.

This table contains information on the following types:

- When the script started and finished execution
- The reason the scripts finished executing
- The result of the script, the remaining time the script is allowed to run

Every row in the Result Table contains the arguments passed during script invocation, the results produced by the script, and the script exit code. The Result Table also provides information about the current run state, and start and end timestamps.

The Result Table has the following attributes.

TABLE 5-3 Result Table Attributes

`Run Index`	The locally arbitrary, but unique identifier associated with this running or finished script is obtained by prepending launchName with an increasing integer starting from 0.
`Argument`	The argument supplied to the script when it started.
`Start Time`	The date and time when the execution started.
`End Time`	The date and time when the execution terminated.
`Life Time`	How long the script can execute. If the script has not terminated when this time has expired, the script is killed automatically.
`Expire Time`	How long this row can exist in the “Result Table” after the script has terminated. This is the value of "Expire Time" field of Launch Table when the script was launched. A script entry will be removed from Result table when "Expire Time" seconds are past since the script comes to "Not Running" state.
`Exit Code`	The reason why a script finished execution. Possible values are: • None: Script is still in "initializing" or "Running" state. • Halted: Script has been aborted. • Successful: Script finished executing successfully • Failed: Script finished execution with an error.
`Result`	The path to the log file.
`Run State`	The script execution status. Possible values are: • Initializing: The script is initializing • Running: The script is running. • Not Running: Note that the script could be in this state because of successful completion, failing, or aborting. The exact reason why the script is “Not Running” is reflected in “Exit Code” field.
`Error`	The path to the log file.

Viewing Results

You can either view the results of running the scripts in the Show Result Table or you can view the entries in the Result Log.

▼ To View the Results from the Result Table

1. **Right-click on a running script entry in the Result Table.**
2. **Select View the Result Log to view the result log file corresponding to the selected running script in a new window.**

   The Probe Viewer displays the result of the log.

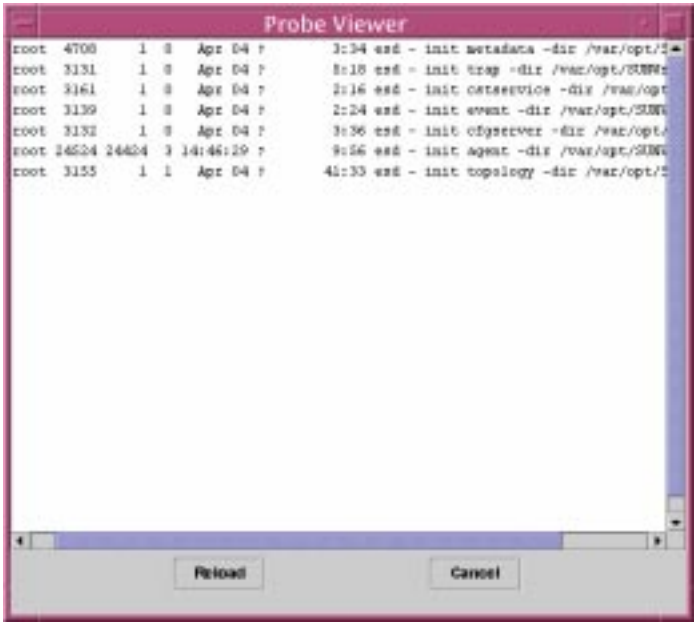

FIGURE 5-4 Sample Log Content

Result Table Alarms

An information (info) alarm is generated if a running script is aborted.

▼ To View the Result Table Log File From the Command Line

1. **Go to the following directory:**

```
/var/opt/SUNWsymon/SysMgmtPack/script-launcher/scripts/<UserName>/logs
```

The results of the scripts are saved in log files. The log files are saved in the above location. The log file name will carry the particular running instance so that the current log file can be identified when a user runs the same script several times.

2. **Open the file at the command line and view the results.**

Security for the Script Launcher

The security for Script Launcher is implemented as follows:

- `root` cannot be part of the `LaunchOwner` field of the Launch Table. In such cases, if you want the root of a machine to run scripts as a super-user, create a new user on the machine and use that user name to run the scripts.
- The `launchOwner` must be a part of new `esscrusers` group on the server. Only `esscrusers` can create rows or make changes in the Launch Table.
- The Launch Owner, or `launchOwner`, must be a valid user on the agent machine, which means the user must either be a local user or someone added through a service such as NIS on the agent. Scripts are run with the launch owner's permissions.

Available Commands

The following commands are available from the Script Launcher.

▼ To Add a New Entry to the Launch Table

1. **Right-click the Launch Table header.**

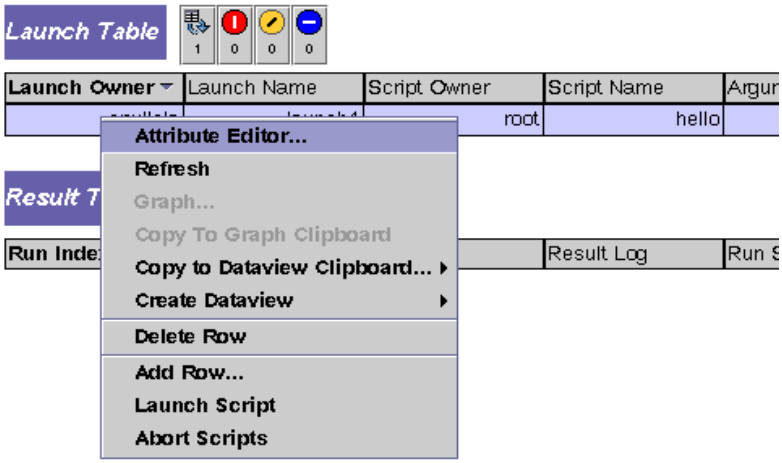

FIGURE 5-5 Commands available at the row level

2. **Select Add Row ...**

   Fill in all the required parameters.

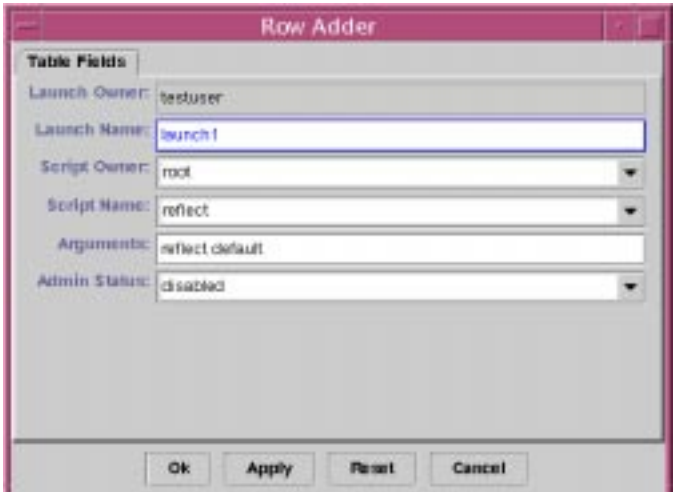

FIGURE 5-6 The Row Adder

The Script Owner and Script Name values point to the script that should be started from this launch button.

▼ To Delete an Entry in the Launch Table

- **Select Delete Row and proceed to delete the row.**

▼ To Launch An Instance of the Script

- **Select Launch Script.**

  An instance of the launch will be launched.

▼ To Abort Scripts

- **Select Abort Scripts to abort all the scripts launched from this row.**

From the Result Table

▼ To View the Result Log

1. **Right click on the row for which you want the results from the Result Table window.**

FIGURE 5-7 View result Log Command

2. **Select View Result Log.**

   SysRM displays the results in a corresponding window.

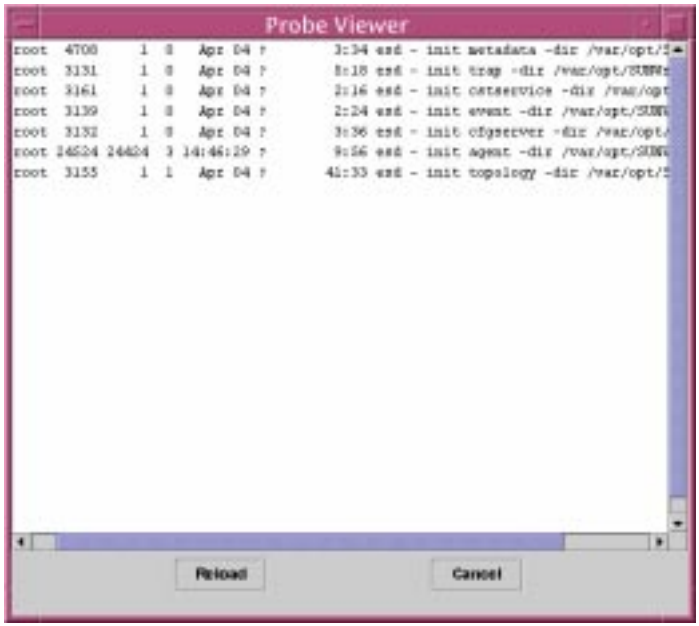

FIGURE 5-8 Sample Log Content

3. **View the result log file that contains results of the selected running script.**

▼ To Abort a Script

- **Select Abort Script.**

  The script instance corresponding to that row will be aborted.

Index

P

R

S

T

V

W