Bull Escala and Escala EPC

Extended RSF
(Extended Remote Services Facilities)
Reference Manual

AIX

ORDER REFERENCE
86 A2 14GX 01

Bull Escala and Escala EPC

Extended RSF
(Extended Remote Services Facilities)
Reference Manual

AIX

Software

June 1998

BULL ELECTRONICS EUROPE S.A.
Service CEDOC
331 Avenue PATTON – BP 428
49004 ANGERS CEDEX 01
FRANCE

ORDER REFERENCE
86 A2 14GX 01

Printed in France

Suggestions and criticisms concerning the form, content, and presentation of this book are invited. A form is provided at the end of this book for this purpose.

To order additional copies of this book or other Bull Technical Publications, you are invited to use the Ordering Form also provided at the end of this book.

Trademarks and Acknowledgements

We acknowledge the right of proprietors of trademarks mentioned in this book.

AIX is a registered trademark of International Business Machines Corporation, and is being used under licence.

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

The information in this document is subject to change without notice. Groupe Bull will not be liable for errors contained herein, or for incidental or consequential damages in connection with the use of this material.

About This Book

This book provides information for understanding, installing, and using *Extended RSF* (Extended Remote Services Facilities).

Who Should Use This Book

This book is intended for the field personnel and/or system administrators responsible for implementing *Extended RSF*.

We shall assume here that you are familiar with SMIT, the AIX System Management Interface Tool. For information concerning SMIT, refer to your AIX documentation.

Overview of Contents

This book contains the following chapters:

- **Chapter 1, "Getting Started With Extended RSF,"** explains what *Extended RSF* is, and summarizes the essential concepts and procedures you should know to use it. It is a recommended reading if you are looking for a tutorial.
- **Chapter 2, "Configuring Actions,"** provides reference information on how to configure actions.
- **Chapter 3, "Configuring Monitored Sources and Associated Messages,"** includes reference information on how to configure monitored sources and associated messages.
- **Chapter 4, "Management Tasks,"** discusses management tasks related to *Extended RSF*, such as: supervising the monitoring process; resetting message counts; listing information about actions, monitored sources and associated messages; changing actions; etc.
- **Appendix A, "Installing Extended RSF,"** explains how to install *Extended RSF*.
- **Appendix B, "Configuring ISM for use with Extended RSF,"** explains how to set up the ISM (Integrated System Management) product to handle SNMP (Simple Network Management Protocol) traps emitted through *Extended RSF*. ISM is a Bull product designed to monitor and manage distributed systems and networks, in a user-friendly way, through a configurable graphical interface.

Related Publications

Extended RSF Documentation

To get additional copies of the *Extended RSF User's Guide*, this present document, use Order Number 86 A2 14GX.

RSF Documentation

Extended RSF is based on and requires the RSF software package. Two books are dedicated to RSF:

- The *RSF User's Guide* is intended for the customer. It does not contain installation and setup instructions. To obtain it, use Order Number 86 A2 95AQ. This guide is also available online, through InfoExplorer.
- The *RSF Field Guide* is intended for the service personnel. It does include installation and setup instructions. To obtain it, use Order Number 86 A7 96AQ.

Contents

Chapter 1. Getting Started With Extended RSF

Read this chapter if you are looking for a tutorial. For reference material, refer to the subsequent chapters.

This chapter includes the following sections:

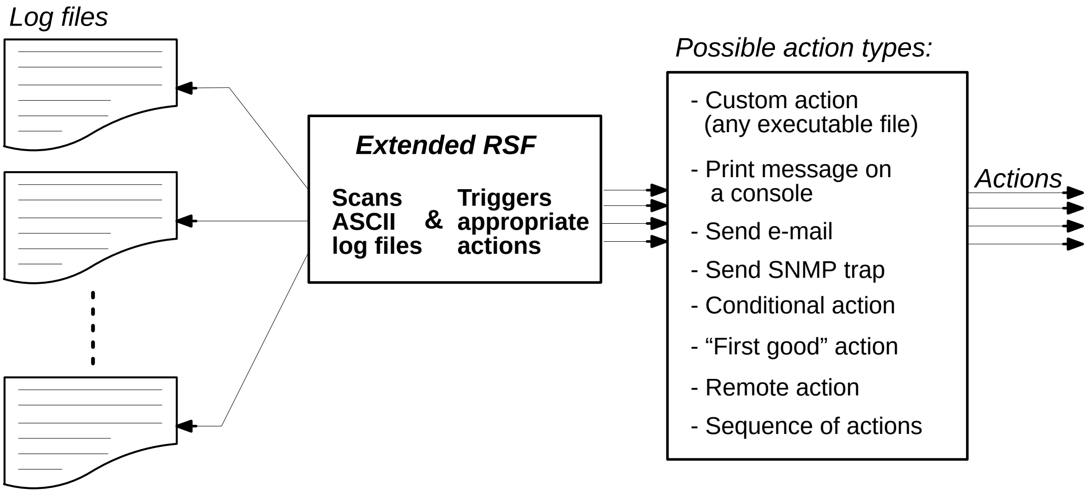
- What is Extended RSF?
- Concepts and Terminology
- General Procedures for using Extended RSF

What is Extended RSF?

Functionality

Extended RSF, which stands for *Extended Remote Services Facilities*, is an application dedicated to log file monitoring:

- it scans ASCII log files for the occurrence of specific messages;
- as specific messages occur in the monitored files, it checks for an over-threshold condition: if an over-threshold condition is detected, it executes specific, user-configurable, actions.



Benefits

Extended RSF can simplify the task of system administrators, who often have to deal with dispersed and/or voluminous log files used by various applications. Notably, with *Extended RSF*, it is easier to:

- detect and be aware of significant entries added to the various log files,
- perform automated administrative tasks as well as corrective actions, based on specific events logged by the various applications.

Requirements

Extended RSF is available on DPX/20 systems running the AIX operating system. It is an optional software package based on RSF (Remote Services Facilities), which is a prerequisite. *Extended RSF* functions are accessible through SMIT, the AIX System Management Interface Tool.

Installation requirements are detailed in appendix A, “Installing Extended RSF”.

Basic Concepts and Terminology

This section introduces concepts and terms you must understand to use *Extended RSF*.

Monitored Sources and Associated Messages

According to the *Extended RSF*’s terminology:

- A “monitored source” is an ASCII log file that *Extended RSF* monitors for the occurrence of messages.
- The “associated messages” of a monitored source are the messages that are to be detected in this monitored source. *Extended RSF* uses regular expressions as search criteria.

Over-threshold Messages

Once *Extended RSF* has been set up to monitor a source, it periodically scans the log file for the occurrence of associated messages.

Extended RSF provides a flexible action manager to trigger actions when a message goes over-threshold. The conditions governing when a message has gone over-threshold are based upon the following criteria:

- identification of specific messages which should provoke actions,
- number of occurrences of the message within a specified time frame.

Message Count

Each time *Extended RSF* detects a relevant message, it updates the count for this message.

IMPORTANT!

Once a given message has gone over-threshold, it will not go over-threshold again until you explicitely reset the count for this message. This avoids continually repeated actions for the same event.

If it is necessary to have an action performed at every occurrence of a message, then the message count should be reset by the action itself in order to “re-arm” the message. For details, refer to “Resetting Message Counts”, on page 4-3.

Actions

When a message in a monitored source goes over-threshold, *Extended RSF* triggers the associated action. Actions typically perform a notification function or some form of automated maintenance activity.

You can associate an action with messages on a per-message basis (as an attribute of the message). You can also associate an action with a source. In the latter case, the action is the default action for any messages in the source which do not have a specific action associated with them.

Possible Action Types

You can define any custom action you need (“Custom action” type), or you can take advantage of predefined and ready-to-use action types (the other action types).

The possible action types are summarized in the table below.

Action Type	Usage and Comments
Custom action	To configure any executable file as an action. You can integrate any notification function or corrective action, through any customized binary program or shell script.
Print message on a console	To display detected messages on a terminal, such as the system console.
Send e-mail	To send a message to an electronic mail address.
Send SNMP trap	To send specific SNMP traps. Any system management software based on SNMP can take advantage of this feature. As an example, appendix B explains how to set up the ISM Bull product to monitor SNMP traps emitted by *Extended RS*F.
Conditional action	To execute an ”if-then-else” sequence of already defined actions.
“First good” action	To execute actions sequentially until one of the actions completes successfully.
Remote action	To execute an action that is already defined on another host running *Extended RSF*.
Sequence of actions	To execute a sequence of already defined actions.

Event Scanner

The software module that is responsible for scanning the log files is referred as the “event scanner”.

Note: The event scanner module is provided by the basic RSF software package. RSF uses the event scanner to scan the AIX error log, while *Extended RSF* uses it to scan any ASCII log file.

General Procedures for Using Extended RSF

This section, which can be seen as a tutorial, describes the general procedures for using *Extended RSF* to monitor log files.

For detailed explanations on the different features and menu options of *Extended RSF*, refer to the subsequent chapters, and to the on-line help provided within the SMIT menus.

Prerequisites

Before enabling log file monitoring through *Extended RSF*, make sure that:

- the *Extended RSF* software package is installed
- RSF is running (i.e. the RSF daemons has been started)

For additional information, refer to appendix A, “Installing Extended RSF”.

How To Access the Extended RSF Main Menu

Using SMIT

You will access all *Extended RSF* functions through SMIT, the AIX *System Management Interface Tool*. If needed, refer to your AIX documentation for information on using SMIT.

Note: The SMIT facility can run in two interfaces: either ASCII (nongraphical) or AIXwindows (graphical). Using one or the other makes no difference.

You Must Be root

You must be logged in as root each time you access *Extended RSF* functions.

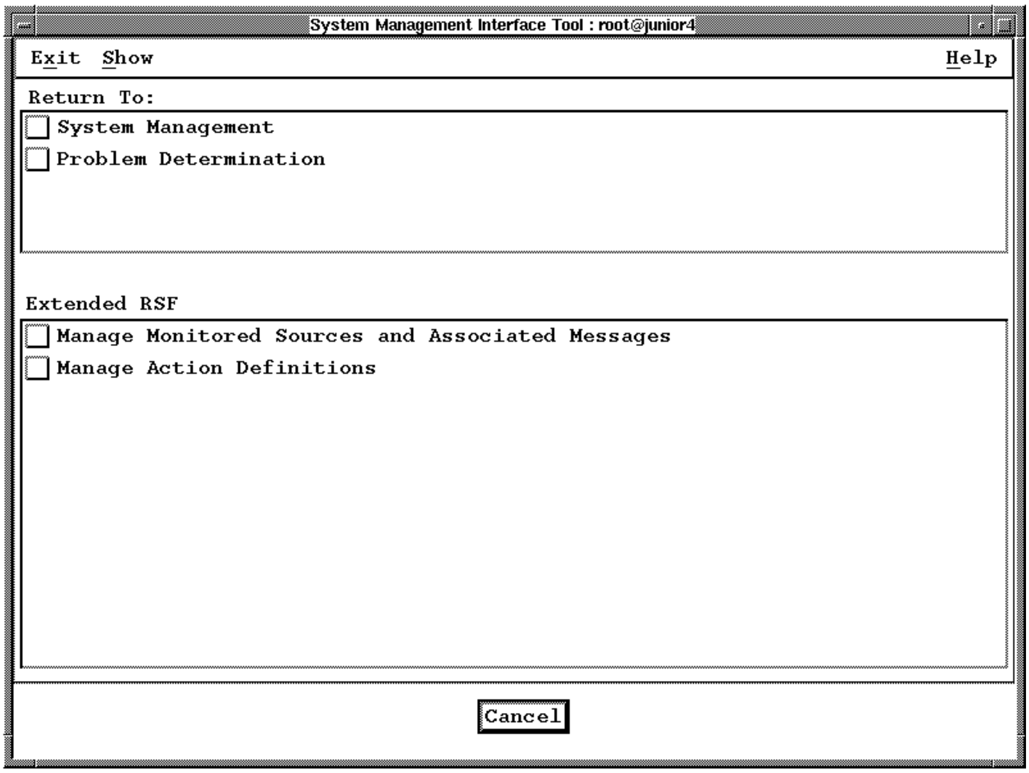
Accessing the Extended RSF Main Menu

To access the main menu of *Extended RSF*:

1. Log in as **root** and invoke SMIT by typing **smit**.
2. From the SMIT top level menu, choose **Problem Determination**, then **Extended RSF (Remote Services Facilities)**. The *Extended RSF* main menu is displayed (see illustration below).

SMIT Fast Path

You can also access directely the *Extended RSF* menu, bypassing the upper-level menus, by using the **smit ext_rsf** fast path.


System Management Interface Tool : root@junior4
Exit
Show
Help
Return To:
System Management
Problem Determination
Extended RSF
Manage Monitored Sources and Associated Messages
Manage Action Definitions
Cancel

Extended RSF Main Menu

Configuring Extended RSF to Monitor Log Files

When configuring *Extended RSF* to monitor log files, your work consists in three tasks:

Task 1:	Configure actions
Task 2:	Configure monitored sources
Task 3:	Configure messages associated with the sources

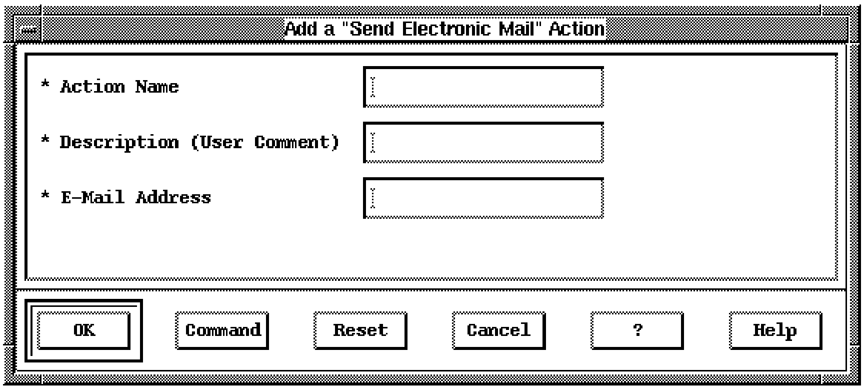
You may want to experiment with the guidelines below, as you read them.

Task 1: Configure Actions

This task consists in defining one or several actions and giving them a name. Guidelines are provided below. For details, refer to the on-line help provided within the SMIT menus, or to chapter “Configuring Actions”, starting on page 2-1.

1. Go to the **Manage Action Definitions** menu, then choose **Add Action**.
2. Choose an action type from the displayed list.

   For your first tests and trials, choose a simple action type, such as **Send Electronic Mail**, **Print Messages on a Console**, or **Custom Action**.
3. A new screen appears, containing several fields. As an example, the figure below shows the **Add a “Send Electronic Mail” Action** menu.



Add a "Send Electronic Mail" Action

* Action Name

* Description (User Comment)

* E-Mail Address

   The fields differ according to the action type you have chosen, however these two fields are common to all action types:

   Action Name: Specify a name for the action you are defining (up to 11 characters). In the other menus, you will use this name to designate this action.

   Description (User Comment): Enter the descriptive text you want. It may be useful when managing actions, specially if you plan to use numerous different actions.

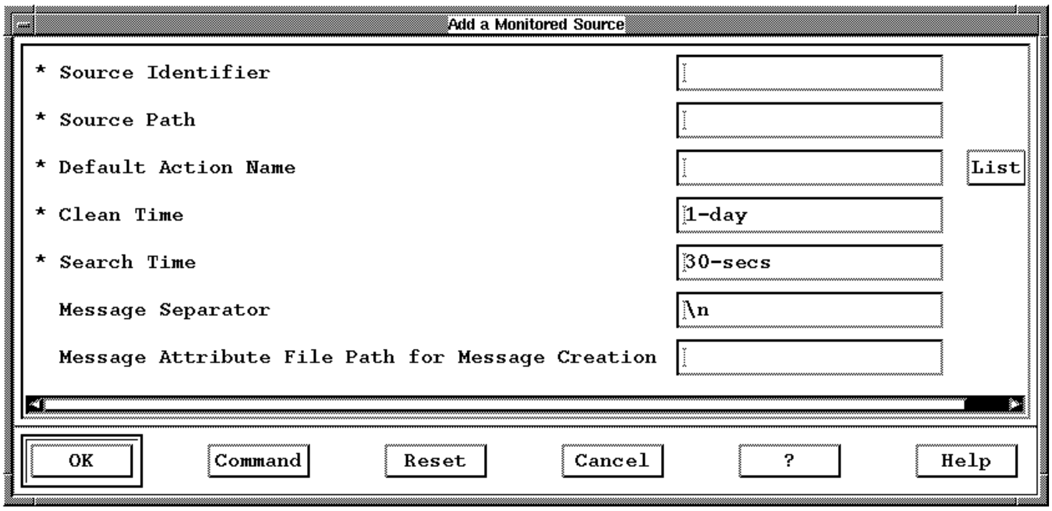
   Fill in the other fields as well, according to the effects you want the action to achieve.
4. Validate the screen to define the action, i.e. to make the action known by Extended RSF.
5. Optionally, repeat the steps above to define other actions (this is not needed for first tests and trials). Note that:
   – Once you have defined at least one action, you can try the features of Extended RSF, as explained below.
   – In subsequent tasks, you can associate the same action to different monitored sources.

Task 2: Configure Monitored Sources

Once you have defined actions, you can instruct *Extended RSF* to trigger them when a message goes over-threshold in a monitored source.

To do so, you first configure a monitored source, i.e. you instruct *Extended RSF* which log file it must monitor, with which scanning parameters. Guidelines are provided below. For details, refer to the on-line help provided within the SMIT menus, or to chapter "Configuring Monitored Sources and Associated Messages", starting on page 3-1.

1. Go to the **Manage Monitored Sources and Associated Messages** menu, then choose **Add a Monitored Source**. A new screen appears, containing several fields (see below).



Add a Monitored Source

```
* Source Identifier
* Source Path
* Default Action Name
* Clean Time                                        1-day
* Search Time                                       30-secs
  Message Separator                                 \n
  Message Attribute File Path for Message Creation
```

2. Fill in the different fields, referring to the hints below:

   Source Identifier: Specify a logical name for the source you want to monitor.

   Source Path: Specify the full path name of the source (the log file) to be monitored. For your first tests and trials:
   - you may want to specify a dummy test log file, such as **/tmp/test.log**, to which you will manually append messages in order to see how *Extended RSF* reacts;
   - do not include metacharacters (`*`, ?, `[`, `]`) when specifying the path, since they have special meanings.

   Default Action Name: A default action is associated with any monitored source. You may want to display the list of available actions (use the F4 key or click on the "List" button), which includes the actions you already have defined. Choose an action from the list.

   Clean Time: For your first tests and trials, leave the default value, **1–day**, as it is.

   Search Time: For your first tests and trials, specify a short delay, such as **5–secs**. The **5–secs** value instructs *Extended RSF* to scan the source for new messages every 5 seconds. As a consequence, the delay for *Extended RSF* to execute actions when a message goes over-threshold will not be greater than 5 seconds. For test purposes, a short delay allows you to quickly verify that *Extended RSF* executes the expected actions (i.e. you do not need to wait a long time before you can see the expected action effects).

   Message Separator: For your first tests and trials, you probably want to leave the default value, **\n**, as it is. The **\n** value denotes the newline character. Extended RSF considers that distinct messages in the monitred source are separated by newlines.

   Message Attribute File Path: For your first tests and trials, leave this field empty. It relates to a special feature which consists in configuring monitored sources and messages by using special configuration files.

3. Validate the screen to configure the monitored source, i.e. to make Extended RSF aware that the specified source is to be monitored. However, after this step, *Extended RSF* still does not not carry out any monitoring activity, since you have not yet specified which messages it must look for in the monitored source.

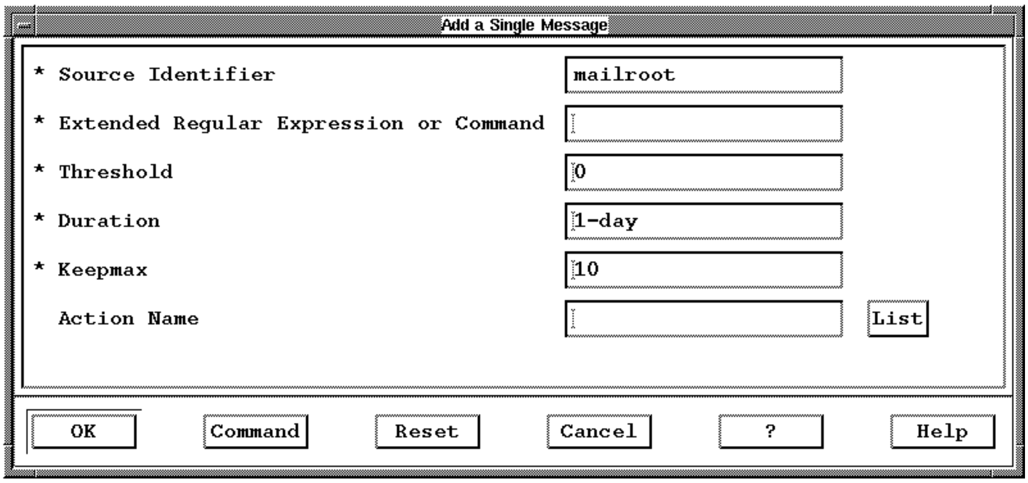
Task 3: Configure Messages Associated with the Sources

Once you have configured a source, you must configure one or several associated messages in order to instruct *Extended RSF* which message(s) it must look for in the source.

Configuring a message mainly consists in specifying a search pattern that matches a message to be monitored. Guidelines are provided below. For details, refer to the on-line help provided within the SMIT menus, or to section “Adding to a Source New Messages to be Monitored”, on page 3-6.

Note: The procedure below explains how to configure messages one by one, by using for each message the **Add a Single Message** menu. However, you should know that you can also configure a group of messages all at once, by creating an initialization file and applying this file through the **Add a Group of Associated Messages** menu. The latter method is discussed in “Adding a Group of Messages”, on page 3-13.

1. Go to the **Manage Monitored Sources and Associated Messages** menu, then successively choose **Add Associated Messages for a Monitored Source** and **Add a Single Message**.
2. A list appears, that include the sources you already have defined. Select the desired source. A new screen appears, containing several fields (see below).



```
* Source Identifier                          mailroot
* Extended Regular Expression or Command
* Threshold                                  0
* Duration                                   1-day
* Keepmax                                    10
  Action Name                                               List
```

3. Fill in the different fields, referring to the hints below.

Source Identifier: This is not an editable field. This value, which indicates the source you have just selected, is shown as a reminder.

Extended Regular Expression or Command: Enter the extended regular expression to be used by *Extended RSF* to track in the source the message you are configuring. *Extended RSF* accepts the same regular expressions as those valid with the **egrep** command (for details, refer to page 3-8). See the examples below:

`warning`
→ Matches any message in the source that contains the `warning` string.

`^warning`
→ Matches any message that contain the `warning` string, but only if this string occurs at the beginning of the message.

`[Ff]atal`
→ Matches any message that contains either the `fatal` or the `Fatal` string.

`warning|fatal`
→ Matches any message that contains either the `warning` or the `fatal` string.

`error10[0-5abc]`
→ Matches any message that contains the `error10` string followed by any digit from `0` to `5`, or by the letter a, b or c. For example, this matches `error102`, and `error10c`, but not `error106`.

`\\([[:lower:][:upper:]]+\\)|\\([0–9]+\\)`
→ Matches any message that contains letters in parentheses or digits in parentheses, but not parenthesized letter-digit combinations. For example, it matches `(xYz)` and `(783902)`, but not `(alpha19c)`. Note that, within a regular expression, parentheses are special characters. In our example, their special meaning is canceled through the use of two `\` (backslash) characters.

Notes:

– For your first tests and trials, specify a simple expression, such as `warning|fatal` or `warning`. Later, you may want to manually append various messages to the source to see how *Extended RSF* reacts.

– Note that it is possible to specify a command instead of an extended regular expression. In this case, the command is used as a filter to detect the messages you want (for details, refer to page 3-10). You may want to forget this feature for your first tests and trials, and reserve it for future experimentation.

Threshold: More than this number of messages must occur for an over-threshold condition to occur (and thus, for the corresponding action to be triggered). Actually, the **Threshold** field is related to the **Duration** field: see below.

For your first tests and trials, you may want to leave the `0` default value, so that the over-threshold condition is reached as soon as one message occurrence is detected in the source.

Duration: For the over-theshold condition to be reached, the number of occurrences of the message (i.e. the number specified in the **Threshold** field) must occur within the time frame you specify here.

The **Duration** value must be specified using a special but simple syntax. For example, valid values for the **Duration** field are 2-mins, `180-mins`, `3-hours`, `1-day`, `1-days`, and `7-days`.

*An Example Showing How **Duration** relates to **Threshold**:*

If you specify 3 as the **Threshold** and `1-hour` as the **Duration**, the over-threshold condition is reached only if 4 message occurrences are detected within a 1-hour period. If 3 occurrences are detected within a 1-hour time frame, and a little later a fourth occurrence is detected, the over-threshold condition is not reached (and thus, *Extended RSF* does not trigger any action).

Keepmax: This integer value specifies the number of occurrences that are stored by *Extended RSF*: only the most recent occurrences are kept in the history. Specify here a value greater than the **Threshold** value.

Action Name: In the previous task (“Task 2: Configure Monitored Sources”) you have specified the default action associated with the source (through the **Default Action Name** field of the **Add a Monitored Source** screen). Here, you can:

– Either leave empty the **Action Name** field, so that the action corresponding to the message you are configuring will be the default action you have associated with the source.

– Or, if the default action does not match your requirements for the message you are configuring, fill in the **Action Name** with a specific action (use the F4 key or click on the “List” button to display the list of available actions). In this case, when

Extended RSF detects an over-threshold condition for this message, it triggers this specific action instead of the default action.

4. Validate the screen to configure the message:

   – SMIT displays the “OK” message;

   – *Extended RSF* immediately begins to track the message in the monitored source and to look for the occurrence of an over-threshold condition (provided that RSF is running, which is normally the case).

   If you are carrying out first test and trials, you may want to manually append different messages to the monitored source and see how *Extended RSF* reacts: it must trigger actions, in accordance with the specifications you have entered.

5. If you want, you can configure other messages to be scanned for in the same source. To do so, repeat the steps above, using the **Add a Single Message** screen.

Where You Go From Here

In the course of this chapter, you have learned the essential concepts and procedures involved in using *Extended RSF*. The best way to learn more on *Extended RSF* is to use it.

- Do not hesitate to experiment with the different features of *Extended RSF.* Most of the menu options are self-explanatory.
- When you require reference information for configuring log file monitoring, consult as needed:
  - the on-line help provided with the SMIT menus,
  - chapter 2, “Configuring Actions”,
  - chapter 3, “Configuring Monitored Sources and Associated Messages”.
- Also refer to chapter 4, “Management Tasks”, to know which administrative tasks are involved in using *Extended RSF*. These tasks notably include: supervising the monitoring process (**resetting message counts** being an important topic); listing information about actions, monitored sources and associated messages; changing actions.

Chapter 2. Configuring Actions

This chapter includes reference information about *Extended RSF* menu options used to configure actions.

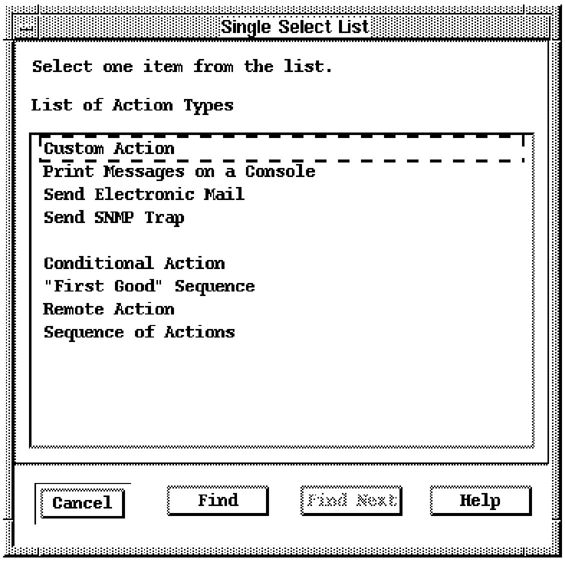
- Overview
- Adding a “Custom Action” Action
- Adding a “Print Messages on a Console” Action
- Adding a “Send Electronic Mail” Action
- Adding a “Send SNMP Trap” Action
- Adding a “Conditional Action” Action
- Adding a “First Good Sequence” Action
- Adding a “Remote Action” Action
- Adding a “Sequence of Actions” Action

Overview

When configuring *Extended RSF* to monitor log files, you have to specify which action is to be triggered when an over-threshold condition occurs. Thus, you have first to configure (i.e. to define) the actions that you plan to use.

Action configuration is achieved through the **Add Action** menu option. Use it as follows:

1. Bring up the *Extended RSF* main menu (as explained on page 1-4).
2. Successively choose **Manage Action Definitions**, then **Add Action**. A list appears, that displays the possible action types you can define.



Select one item from the list.

List of Action Types

3. Choose the desired action type. A new menu appears, containing different fields specific to the action type you have chosen.

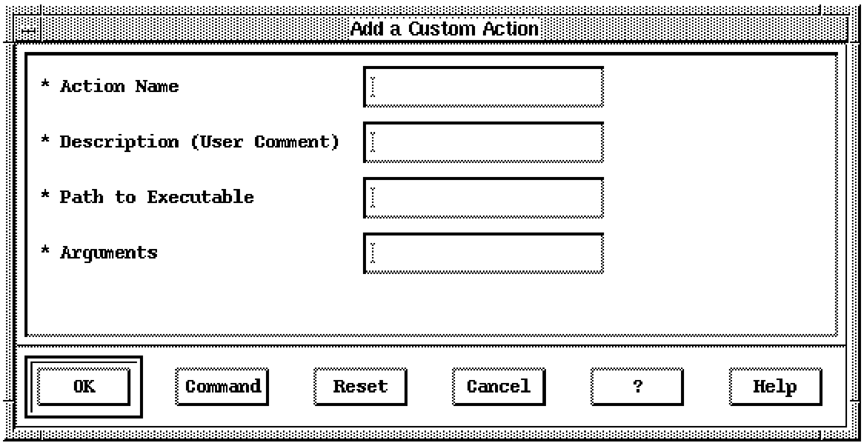
The sections below provide reference information about the menus corresponding to the different action types. In addition, note that:

- “Actions”, on page 1-2, provides a summary of possible action types.
- “Task 1: Configure Actions”, on page 1-5, gives general guidelines on configuring actions.

Adding a “Custom Action” Action

The **Custom Action** action type allows you to configure any executable file as an action. Through this feature, you can integrate any notification functionality or corrective action, through any customized binary program or shell script.

The figure below shows the **Add a Custom Action** menu.



Action Name

In the **Action Name** field, specify a name for the action you are defining. Up to 11 characters are allowed. Each action you define must have a unique name, which is used in various menus to designate the action.

Description (User Comment)

In the **Description (User Comment)** field, enter the descriptive text you want. Such an informative text may be useful when managing actions, specially if you plan to use numerous different actions.

Path to Executable

In the **Path to Executable** field, enter the full path name of the executable file responsible for executing the action you are defining. The executable file can be either a binary file or a shell script file. The arguments it can handle are discusses below.

Arguments

In the **Arguments** field, enter the arguments that need to be passed to the executable file. The arguments, which must be separated by a blank, can be:

- either constant strings, which are passed literally to the executable,
- or special keywords (beginning with the `%` character), which are substituted before being passed to the executable, as explained below.

Constant Strings

Any constant string is passed literally as an argument, without being interpreted by a shell. That means in particular that you cannot implement input/output redirection by specifying characters such as “>” and “<” in the **Arguments** field.

For example, if you specify the following value in the **Arguments** field:

```
>> /foobar/file
```

Then, “>>” is treated as an ordinary constant string, without any special meaning, which is passed to the executable as its first argument (just as the string “`/foobar/file`” is passed as its second argument).

If you want to pass a constant string that include blanks, enclose the string with double-quotes.

For example, if you specify the following value in the **Arguments** field:

```
oof ”foo bar” rab
```

Then, three arguments are passed to the executable (the “`foo bar`” string is treated as a single string, and thus, as a single argument).

Special Keywords

When an over-threshold condition occurs, *Extended RSF* replaces the special keywords with specific values. These values denote specific information related to that particular instance of the over-threshold condition. Thus, you can tailor the executable file to act in different ways, based upon the specific values that are passed as arguments.

The available keywords are summarized in the table below. Note that:

- **%source**, **%tag**, **%text**, and **%time** are the most commonly used,
- **%message_host** and **%action_host** can be useful in the context of actions defined as **Remote Actions**,
- the other keywords are rather rarely used.

Keyword	Substituted Value
%source	The identifier of the source that went over threshold. This identifier is the text string you specify in the **Source Identifier** field when configuring a source through the **Add a Monitored Source** menu.
%tag	The name of the action being executed. This name is the text string you specify in the **Action Name** field when configuring the action (see above).
%text	The full path name of the temporary file (created by *Extended RSF*) that contains the text of the message whose occurrence triggered the action. Using the **%text** keyword makes it possible for the executable to handle the message text for further processing. Note that the temporary file is automatically removed after the action is executed.
%time	The date and time the message occurred. The substituted value is a single string, thus it is viewed as a single argument by the executable. Below is an example of string returned by the **%time** keyword: `Tue Nov 14 12:57:02 1995`
%message_host	The name of the host on which the message occurred.
%action_host	The name of the host on which the action is being performed. If the action is not a “remote action”, then **%action_host** and the **%message_host** yields the same host name. Otherwise, **%action_host** is the machine that is performing the action on behalf of the **%message_host** (that is, the over-threshold condition is on the **%message_host**).

%action_id	A unique numeric identifier of the action being executed. Indeed, each time *Extended RSF* triggers an action, it adds an entry to the **/var/rsf/actionlog** log file of RSF, including a unique identifier for this action. This identifier is an RSF internal number (e.g. 00000054). The **Display Dial Out Log File** function of RSF allows you to examine the **/var/rsf/actionlog** RSF log file. This provides you with a way of reviewing information related to actions carried out by RSF and by *Extended RSF*.
%id	The numeric identifier associated with the message that went over threshold. Indeed, when you configure a message to be monitored in a source, *Extended RSF* associates it with a numeric identifier, which is unique among the different messages associated with the source. 0000001 is the ID of the first message you associate with a source, 0000002 is the ID of the second one you associate with the same source, and so on. **Notes:** – For information related to message identifiers, refer to “Order Significance in Message Specifications”, on page 3-6. – You can know the identifier of any configured message by using the **Change/Show Associated Message of a Monitored Source** menu.
%origine_site	The name of a special file (usually **/var/rsf/custom.cfg**) stored on the **%message_host** host. This file used by RSF to hold site-related configuration parameters. The **%origine_site** keyword is mainly intended for service personnel.
%local_site	The name of a special file (usually **/var/rsf/custom.cfg**) stored on the **%action_host** host. This file is used by RSF to hold site-related configuration parameters. The **%local_site** keyword is mainly intended for service personnel.

Example

To create a custom action that is similar to the “Send Electronic Mail” action proposed in the Extended RSF menus, you could specify:

Path to Executable: `/home/john/mailaction`

Arguments: `Overthreshold root %text`

The `/home/john/mailaction` being the following shell script:

```
#!/bin/ksh
# script called by Extended RSF with 3 arguments:
# $1 : the string to be used as the mail’s subject
# $2 : the string to be used as the mail’s recipient
# $3 : the value yielded by the %text special keyword, i.e. the
#      name of the temporary file that contains the text of the
#      message
#
/usr/bin/mail –s $1 $2 < $3
#
#end of script
```

When this sample custom action is performed, *Extended RSF* replaces the `%text` keyword with the name of the temporary file containing the message that went over-threshold. Then, the `/home/john/mailaction` script is executed to send the message text (read from $3, i.e. from the temporary file) to $2 (here, `root`) with the specified subject (–s $1, $1 having here the “`Overthreshold`” value).

Note: You could not implement input redirection by directly specifying the “<” character in the **Arguments** field: for a related discussion, see section “Constant Strings”, on page 2-2.

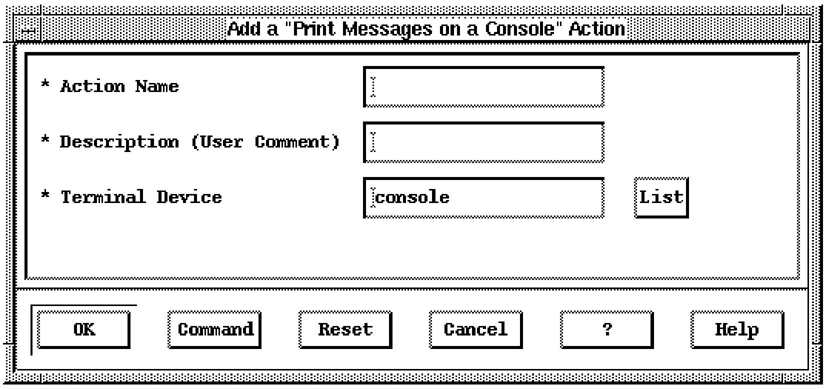
Resetting a Message Count from Within a Custom Action

It may be useful to reset a message count from within a custom action. For details, refer to page 4-4.

Adding a “Print Messages on a Console” Action

The **Print Messages on a Console** action type allows you to direct over-threshold messages to the console or to any other terminal device.

The figure below shows the **Add a “Print Messages on a Console” Action** menu.



Add a "Print Messages on a Console" Action

* Action Name

* Description (User Comment)

* Terminal Device: console

Action Name

In the **Action Name** field, specify a name for the action you are defining. Up to 11 characters are allowed. Each action you define must have a unique name, which is used in various menus to designate the action.

Description (User Comment)

In the **Description (User Comment)** field, enter the descriptive text you want. Such an informative text may be useful when managing actions, specially if you plan to use numerous different actions.

Terminal Device

In the **Terminal Device** field, enter the name of the device to which the messages are to be directed. You may use the F4 key or click on the “List” button to display the list of terminal devices available on the system.

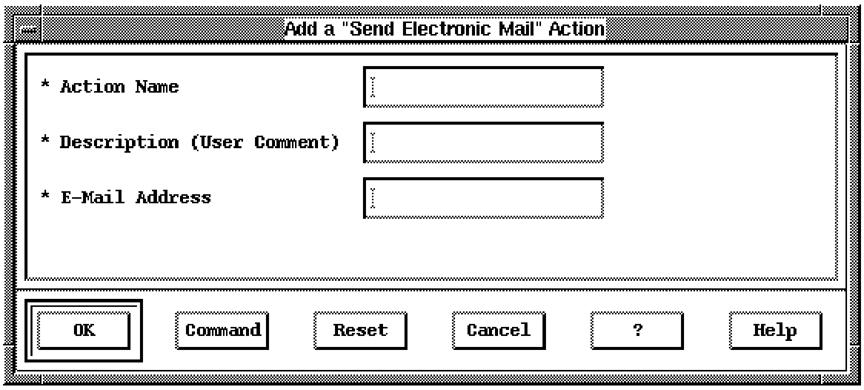
- The default value, `console`, corresponds to the system console (`/dev/console`).
- Other typical values are for example `tty0` and `tty1`, which correspond to `/dev/tty0` and `/dev/tty1` (and which may be available or not, depending on the terminal devices available on your system).
- You can also specify a pseudo-terminal, for example `pts/0` or `pts/3`, which correspond to `/dev/pts/0` and `/dev/pts/3`. Note that pseudo-terminals are not displayed when you list the available terminal devices using F4 or the “List” button.

Adding a “Send Electronic Mail” Action

The **Send Electronic Mail** action type allows you to transmit to an electronic mail address a mail message for notification of over-threshold conditions. Note the following:

- Any sent electronic mail message contains all the information related to the over-threshold condition occurrence.
- You may want to know that *Extended RSF* implements this action by using the **/usr/bin/mailact** shell script, which comes with the RSF software package. However, you must not modify this shell script. If you want to implement notification by mail with customized mail message contents, write an ad-hoc script and use the **Add a Custom Action** feature to bind it to an action.

The figure below shows the **Add a “Send Electronic Mail” Action** menu.



Add a "Send Electronic Mail" Action

* Action Name

* Description (User Comment)

* E-Mail Address

Action Name

In the **Action Name** field, specify a name for the action you are defining. Up to 11 characters are allowed. Each action you define must have a unique name, which is used in various menus to designate the action.

Description (User Comment)

In the **Description (User Comment)** field, enter the descriptive text you want. Such an informative text may be useful when managing actions, specially if you plan to use numerous different actions.

E-Mail Address

In the **E-Mail Address** field, enter the electronic mail address to which mail is to be sent.

You can specify a single address or multiple addresses separated with blanks as in the example below:

```
jack@foobar root@foobar bill@raboof.com
```

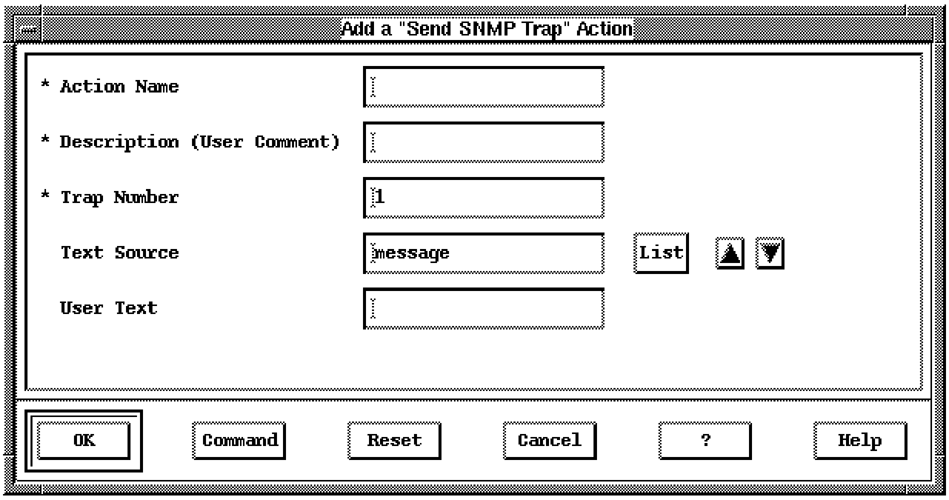
Adding a “Send SNMP Trap” Action

The **Send SNMP Trap** action type allows you to send specific SNMP traps for notification of over-threshold conditions.

While simple in concept, this is a very powerfull feature because this extends the benefit of SNMP-based system management down to the application level. Indeed, any application which writes a log file can have its error conditions forwarded to a system management software.

Any system management software based on SNMP can take advantage of this feature. As an example, appendix B explains how to set up the ISM Bull product to monitor SNMP traps emitted by *Extended RS*F.

The figure below shows the **Add a “Send SNMP Trap” Action** menu.



Add a "Send SNMP Trap" Action

* Action Name	
* Description (User Comment)	
* Trap Number	1
Text Source	message
User Text	

Action Name

In the **Action Name** field, specify a name for the action you are defining. Up to 11 characters are allowed. Each action you define must have a unique name, which is used in various menus to designate the action.

Description (User Comment)

In the **Description (User Comment)** field, enter the descriptive text you want.

Such an informative text may be useful when managing actions, specially if you plan to use numerous different actions.

Trap Number

In the **Trap Number** field, enter an integer ranging from 1 to 255.

SNMP traps emitted through *Extended RSF* are “enterprise-specific” traps (also known as “#6 generic traps”) with a specific trap number equal to the number specified in the **Trap Number** field. In addition, note the following:

- For the SNMP traps feature to be effective, the involved SNMP daemons must be appropriately configured and enabled. Refer to appendix B for details.
- You may want to know that, according to the RSF Management Information Base (MIB), the RSF agent object responsible for SNMP handling is identified through the following enterprise object identifier (OID):

```
1.3.6.1.4.1.107.121.1
```

Text Source

In the **Text Source** field, specify either `user`, `description` or `message`, depending on the text you want to be included within the SNMP trap.

`user` The SNMP trap will include the text you specify in the **User Text** field.

`description` The SNMP trap will include *the first text line* of the message that went over-threshold in the monitored source.

`message` The SNMP trap will include *the full text* of the message that went over-threshold in the monitored source.

Note: You may use the F4 key or click on the “List” button to display the three available values and to pick up the one you desire.

User Text

This field makes sense only if you have set the **Text Source** field to the `user` value. In that case, enter in the **User Text** field the text you want to be included within the SNMP trap.

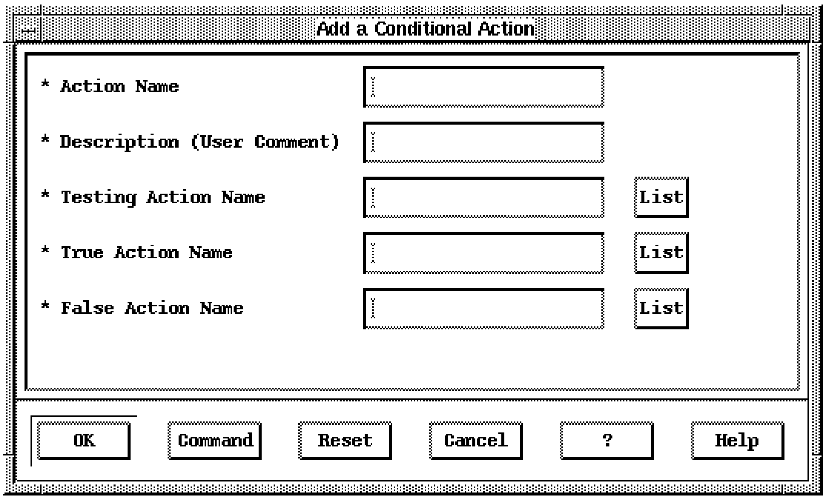
Adding a “Conditional Action” Action

The **Conditional Action** action type is an if-then-else sequence of already-defined actions.

When configuring a conditional action, three actions are involved: a testing action, a true action and a false action. When the conditional action is triggered:

- the “testing action” is always executed
- if the “testing action” returns success (zero exit value), then the “true action” is executed,
- otherwise (non-zero exit value), the “false action” is executed.

The figure below shows the **Add a Conditional Action** menu.



Action Name

In the **Action Name** field, specify a name for the action you are defining. Up to 11 characters are allowed. Each action you define must have a unique name, which is used in various menus to designate the action.

Description (User Comment)

In the **Description (User Comment)** field, enter the descriptive text you want. Such an informative text may be useful when managing actions, specially if you plan to use numerous different actions.

Testing Action Name

In the **Testing Action Name** field, enter the name of an already-defined action that you want to use as the “testing action”. You may use the F4 key or click on the “List” button to display the list of already-defined actions.

Note: Beware of loops: when defining a conditional action, do not use that same action name as the testing, true, or false action to execute.

True Action Name

In the **True Action Name** field, enter the name of an already-defined action that you want to use as the “true action” (i.e. the action to execute if the “testing action” has terminated with the zero exit value). You may use the F4 key or click on the “List” button to display the list of already-defined actions.

Note: Beware of loops: when defining a conditional action, do not use that same action name as the testing, true, or false action to execute.

False Action Name

In the **True Action Name** field, enter the name of an already-defined action that you want to use as the “false action” (i.e. the action to execute if the “testing action” has terminated with a non-zero exit value). You may use the F4 key or click on the “List” button to display the list of already-defined actions.

Note: Beware of loops: when defining a conditional action, do not use that same action name as the testing, true, or false action to execute.

Example of a Conditional Action

Assume that you already have configured the three actions below:

- A custom action named `fix_it`, developed to attempt to correct a situation when a certain over-threshold condition is detected.
- A “Send Electronic Mail” action named `mail_jack` to send electronic mail to Jack.
- A custom action `beep_jack`, developed to trigger a callout to Jack’s beeper.

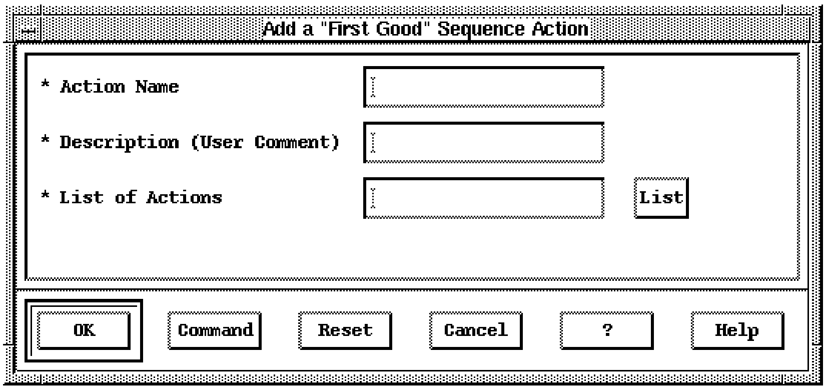
Then, you can configure a conditional action so that:

- `fix_it` is the “testing action”.
- `mail_jack` is the “true action”: if `fix_it` returns success, `mail_jack` is executed to let Jack know that the problem has been automatically corrected.
- beep_jack is the “false action”: if `fix_it` returns failure, `beep_jack` is executed to immediately notify Jack that something is wrong.

Adding a “First Good Sequence” Action

The **“First Good” Sequence** action type provides the means to execute sequentially already-defined actions until one of the actions completes successfully.

The figure below shows the **Add a “First Good” Sequence Action** menu.


Add a "First Good" Sequence Action
* Action Name
* Description (User Comment)
* List of Actions
List
OK
Command
Reset
Cancel
?
Help

Action Name

In the **Action Name** field, specify a name for the action you are defining. Up to 11 characters are allowed. Each action you define must have a unique name, which is used in various menus to designate the action.

Description (User Comment)

In the **Description (User Comment)** field, enter the descriptive text you want. Such an informative text may be useful when managing actions, specially if you plan to use numerous different actions.

List of Actions

In the **List of Actions** field, enter the list of actions to be executed sequentially until one of them completes successfully.

- Action names must be separated with a blank.
- Specify the actions according to the desired execution order: the first action specified will be the first executed in the sequence.
- You may use the F4 key or click on the “List” button to display the list of already-defined actions. Once the list is displayed, select the actions you want to include in the **List of Actions** field.

Note: Beware of loops: when defining a “first good sequence” action, do not use that same action name in the list of actions to execute.

Adding a “Remote Action” Action

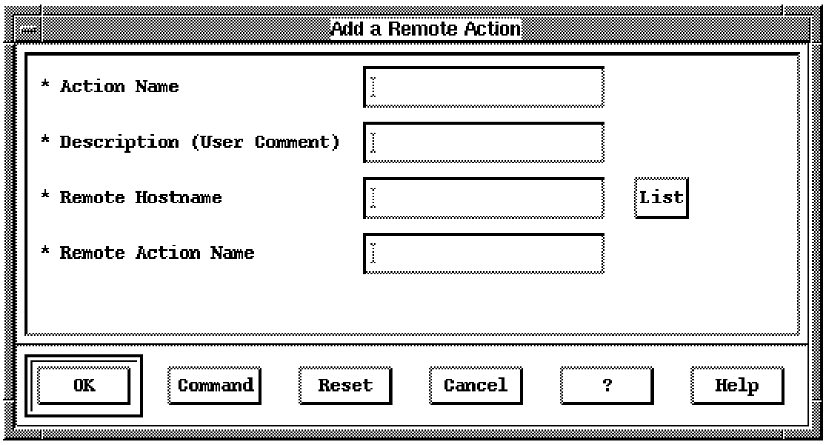
The **Remote Action** action type allows you to execute an *Extended RSF* action remotely on another host where *Extended RSF* is implemented.

For example, assume your network includes a host named `modemhost` which is equipped with a modem. A possible scenario would be:

- On the `modemhost` host, you configure a custom action named `beep_jack`, developed to trigger a callout to Jack’s beeper.
- On other host(s), you configure a remote action named `beep_jack`, that refers to the `beep_jack` action on the host with the modem.

Note: If the remote host is not accessible from the local host (perhaps due to network problems or other failures), the remote action will fail. Thus, you may want to place remote actions into conditional actions or “first good sequence” actions to provide alternative actions.

The figure below shows the **Add a Remote Action** menu.



Action Name

In the **Action Name** field, specify a name for the action you are defining. Up to 11 characters are allowed. Each action you define must have a unique name, which is used in various menus to designate the action.

Description (User Comment)

In the **Description (User Comment)** field, enter the descriptive text you want. Such an informative text may be useful when managing actions, specially if you plan to use numerous different actions.

Remote Hostname

In the **Remote Hostname** field, enter the name of the host on which the remote action is located.

Remote Action Name

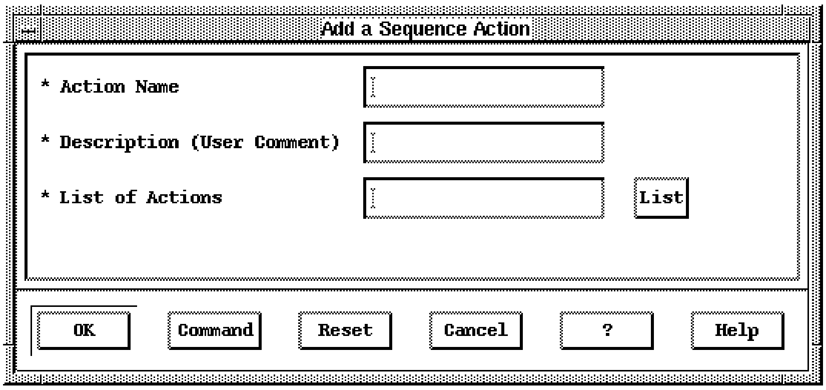
In the **Remote Action Name**, enter the name of the action to execute on the remote host.

Note: Beware of loops: when defining a “remote action” action, do not specify an action that would trigger the action you are defining.

Adding a “Sequence of Actions” Action

The **Sequence of Actions** action type provides the means to execute a sequence of other already-defined actions.

The figure below shows the **Add a Sequence Action** menu.



Action Name

In the **Action Name** field, specify a name for the action you are defining. Up to 11 characters are allowed. Each action you define must have a unique name, which is used in various menus to designate the action.

Description (User Comment)

In the **Description (User Comment)** field, enter the descriptive text you want. Such an informative text may be useful when managing actions, specially if you plan to use numerous different actions.

List of Actions

In the **List of Actions** field, enter the list of actions to be executed sequentially.

- Action names must be separated with a blank.
- Specify the actions according to the desired execution order: the first action specified will be the first executed in the sequence.
- You may use the F4 key or click on the “List” button to display the list of already-defined actions. Once the list is displayed, select the actions you want to include in the **List of Actions** field.

Note: Beware of loops: when defining a “sequence of actions” action, do not use that same action name in the list of actions to execute.

Chapter 3. Configuring Monitored Sources and Associated Messages

This chapter includes reference information about *Extended RSF* menu options used to configure monitored sources and associated messages.

- Overview
- Adding a New Source to be Monitored
- Knowledge Required for Adding New Messages to a Source
- Adding a Single Message
- Adding a Group of Messages

Overview

When To Configure Monitored Sources and Associated Messages

Once you have defined actions, you can instruct *Extended RSF* to trigger them when a message goes over-threshold in a monitored source. To do so, you have first to configure a monitored source, i.e. to instruct *Extended RSF* which log file it must monitor, with which scanning parameters.

Once you have configured a source, you must configure one or several associated messages in order to instruct *Extended RSF* which message(s) it must look for in the source.

Involved Menus

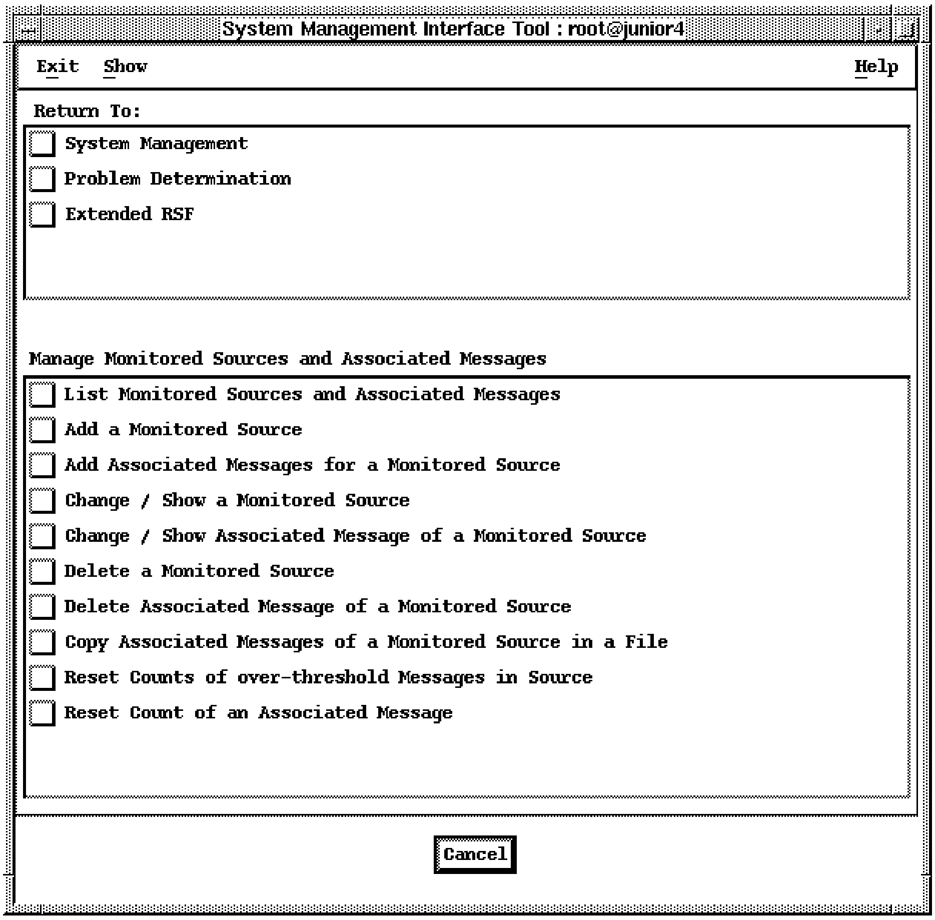
Sources and messages configuration is achieved through the **Manage Monitored Sources and Associated Messages** menu. To access this menu:

1. Bring up the *Extended RSF* main menu (as explained on page 1-4).
2. Choose **Manage Monitored Sources and Associated Messages**. The corresponding menu is displayed (see the illustration below).

Among the various options included in the menu, the following two allow you to configure monitored sources and associated messages:

- **Add a Monitored Source**
- **Add Associated Messages for a Monitored Source**

These menu options are described in the subsequent sections.


System Management Interface Tool : root@junior4

Exit Show Help

Return To:

- □ System Management
- □ Problem Determination
- □ Extended RSF

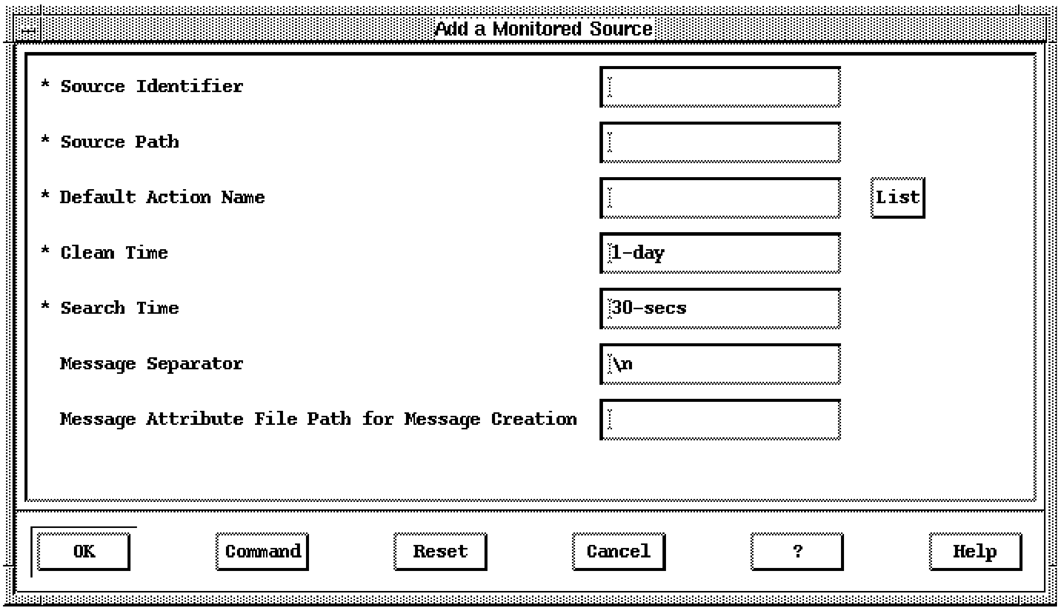
Manage Monitored Sources and Associated Messages

- □ List Monitored Sources and Associated Messages
- □ Add a Monitored Source
- □ Add Associated Messages for a Monitored Source
- □ Change / Show a Monitored Source
- □ Change / Show Associated Message of a Monitored Source
- □ Delete a Monitored Source
- □ Delete Associated Message of a Monitored Source
- □ Copy Associated Messages of a Monitored Source in a File
- □ Reset Counts of over-threshold Messages in Source
- □ Reset Count of an Associated Message

Adding a New Source to be Monitored

Accessing the “Add a Monitored Source” Menu

To add a new source for Extended RSF to monitor, go to the **Manage Monitored Sources and Associated Messages** menu, and choose **Add a Monitored Source**. The corresponding menu is displayed, as shown below:


Add a Monitored Source

* Source Identifier	
* Source Path	
* Default Action Name	
* Clean Time	1-day
* Search Time	30-secs
Message Separator	\n
Message Attribute File Path for Message Creation	

Entering the Field Values

Once the **Add a Monitored Source** is displayed, enter field values as explained below.

Source Identifier

In the **Source Identifier** field, specify a name for the source you are configuring (i.e. for the source you want to monitor). Up to 15 characters are allowed. Each monitored source must have a unique name, which is used in various menus to designate the source.

Source Path

In the **Source Path** field, specify the full path name of the source (the log file) to be monitored. For example:

```
/var/adm/foobar/foobar.log
```

File Name Substitution

Instead of specifying a path name litteraly, as in the example above, you can use pattern-matching characters. Indeed, if the value you specify as the **Source Path** contains any of the characters `*` (asterisk), ? (question mark), or [ ] (braces), then the value is a candidate for file name substitution.

These characters, which apply only to basenames (see the note below), indicate substitutions, according to those same rules that are used by the shell for file name substitution.

*	Matches any string.
?	Matches any single character.
`[...]`	Matches any one of the enclosed characters. A pair of characters separated by a – (hyphen) matches any character lexically within the inclusive range of that pair, according to the binary ordering of character values. If the first character following the opening [(left bracket) is an ! (exclamation point), then any character not enclosed is matched. A – (hyphen) can be included in the character set by putting it as the first or last character.

(For details, refer to your shell documentation.)

Note: You can use these characters only to substitute the basename part of the file path, not to substitute a subdirectory name within the path. For example, `/var/adm/foobar/*.log` is a valid specification because the `*` relates to the file basename; on the other hand, `/var/adm/*bar/*.log` is not valid, because `*bar` relates to a directory name (not to the basename).

If the value specified in the **Source Path** field matches several file names, then *Extended RSF* elects the most recently created file as the file to be monitored.

Example

Assume that you want to monitor log files written by an application named “foobar”. Suppose that this application creates each day a new log file to log information. For example, it creates and uses the `/var/adm/foobar/log.1201` file to log events that occur on the 1st december; then it creates and uses the `/var/adm/foobar/log.1202` file to log events that occur on the 2nd december; and so on.

If you want to monitor the log file of such an application, you cannot rely on a fixed file name, since the name of the log file changes every day. Thus, when specifying the **Source Path** field to configure the source, you must enter a non-litteral value as the following:

```
/var/adm/foobar/log.*
```

With this setting, you instruct *Extended RSF* to always monitor the most recently created file among all the files that match the `/var/adm/foobar/log.*` expression. Thus, when the “foobar” application creates a new log file, *Extended RSF* monitors this new log file instead of the old one.

Default Action Name

In the **Default Action Name** field, specify the default action associated with the source. This is the default action for any messages in the source which do not have a specific action associated with them.

You may use the F4 key or click on the “List” button to display the list of available actions, which includes the actions you already have defined

Note: You can associate an action with messages on a per-message basis, as an attribute of the message. In this case, the specific action associated with a given message of the source overrides the default action associated with the source. For details, refer to “Action Name” 3-12.

Clean Time

In the **Clean Time** field, enter the time interval at which *Extended RSF* cleans out its history database (which contains old messages) to conserve disk space.

Note: Within *Extended RSF*, time intervals are specified using a special notation. The following specifications are examples of valid time intervals: `60–secs`, `10–mins`, `12–hours`, `3–days` and `1–week`.

A recommended **Clean Time** is `1–day` (the default value). Do not use a **Clean Time** of less than `1–hour`, because *Extended RSF* performance could suffer.

Search Time

In the **Search Time** field, enter the time interval at which *Extended RSF* scans the source for new messages.

Note: Within *Extended RSF*, time intervals are specified using a special notation. The following specifications are explanatory examples of valid time intervals: `60–secs`, `10–mins`, `12–hours` and `3–days`.

A recommended **Search Time** is `5–mins`. The setting of this parameter can be very important as there is a tradeoff between:

- the system resources used by *Extended RSF* each time that the log file is scanned, and
- the possible delay for *Extended RSF* to execute actions after an over-threshold condition occurs.

For example, if you set the **Search Time** to `6–hours`, *Extended RSF* will scan the source for new messages every 6 hours. Thus, it is possible that 6 hours could pass after a message goes over-threshold before the appropriate action is executed.

Message Separator

In the **Message Separator** field, enter the string to be used by *Extended RSF* to identify message boundaries.

The `\n` and `\t` strings have a special meaning: they denote respectively the newline and the tabulation characters.

The most commonly used setting for the **Message Separator** field is `\n`. With this setting, *Extended RSF* considers that distinct messages in the monitored source are separated by a newline character.

However, other settings may be useful to monitor log files where there are logged messages that span multiple lines. For example, suppose that an application logs multi-line messages, and that each message begins with the "ERROR" string. Here is an excerpt from this fictitious log file:

```
ERROR
Wed Dec 13 17:42:08 MET 1995
no such user: john
access denied
ERROR
Wed Dec 13 17:43:38 MET 1995
host unreachable: foobar
ERROR
Wed Dec 13 17:44:02 MET 1995
...
```

In this example, we see that each message spans several lines. Moreover, the messages may include any number of lines. With such a log file, you probably would want to specify the `ERROR` string as the **Message Separator**.

Message Attribute File Path for Message Creation

The optional **Message Attribute File Path for Message Creation** field relates to a special feature which consists of applying an initialization file in order to configure all at once a group of messages for this source.

If you do not plan to use this feature, leave this field blank. Otherwise, specify the full path name of the initialization file to be applied. The syntax of such an initialization file is described in "Understanding Initialization Files", on page 3-13.

Using Source "Snapshots"

When configuring *Extended RSF* on numerous hosts, you may want to take source "snapshots" in order to apply these "snapshots" to other hosts. For further information, refer to "Creating a Source Snapshot", on page 3-15.

Knowledge Required for Adding New Messages to a Source

General Considerations

Note: For an overview of related concepts (including the important notion of message count), also refer to “Basic Concepts and Terminology”, on page 1-2.

Once you have configured a source, you must add (i.e. configure) one or several associated messages in order to instruct *Extended RSF* which message(s) it must look for in the source.

Configuring a message consists of specifying the criteria that, when matched, yield an over-threshold condition, and thus the triggering of an action. The conditions governing when a message goes over-threshold are based upon the following criteria:

- identification, through a regular expression, of specific messages which should provoke actions,
- number of occurrences of the message within a specified time frame.

Order Significance in Message Specifications (IMPORTANT)

Within *Extended RSF*, messages are associated with a source in an ordered fashion.

Each time you add a message to a source, *Extended RSF* associates it with an order number. The first message you add is assigned the number 00000001, the second is assigned the number 00000002, and so on.

That means that the order in which you configure messages is significant. Indeed, when *Extended RSF* monitors a source, it proceeds as follows:

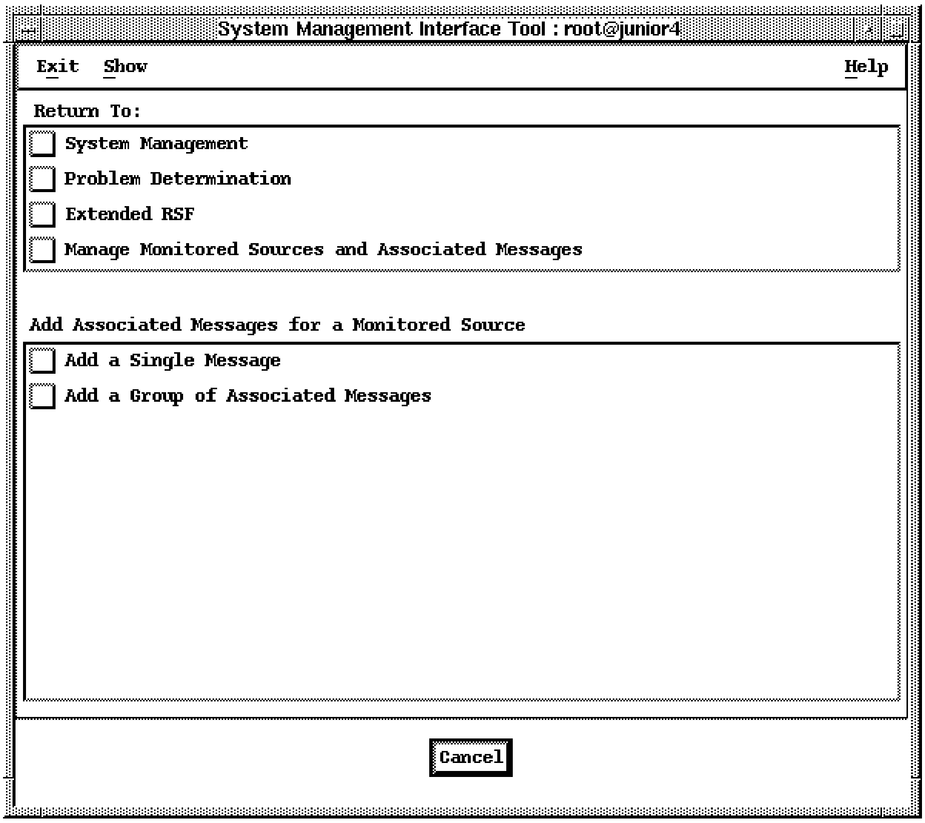
- It first uses the regular expression that characterizes *the first* associated message to perform a pattern match against the source.
  - If a match is found, *Extended RSF* performs no further pattern match: the subsequent associated messages are simply ignored, i.e. they are not compared against the source.
  - If no match is found, *Extended RSF* uses the regular expression that characterizes *the second* associated message to perform a pattern match against the source.
- And so on: *Extended RSF* continues to walk through the successive associated messages, and stops as soon as a match occurs.

A practical consequence is that you must configure messages in an appropriate order. You must configure first the message whose search pattern is the most specific, and configure the other messages always going from the most specific to the most general. Examples later in this chapter illustrate this important consideration.

Note: To know the respective precedence order of the different messages associated with a source, go to the **Manage Monitored Sources and Associated Messages**, and choose **Change / Show Associated Message of a Monitored Source**. In the list of defined sources that appears, select the desired source. Then, a new screen appears, that shows the messages associated with the source, along with their respective order numbers (00000001, 00000002...).

Two Methods for Adding New Messages to be Monitored

To add to a source new messages to be monitored, go to the **Manage Monitored Sources and Associated Messages** menu, and choose **Add Associated Messages for a Monitored Source**. A new menu appears, as shown below:


System Management Interface Tool : root@junior4
Exit
Show
Help
Return To:
□ System Management
□ Problem Determination
□ Extended RSF
□ Manage Monitored Sources and Associated Messages
Add Associated Messages for a Monitored Source
□ Add a Single Message
□ Add a Group of Associated Messages
Cancel

This menu includes two options. Indeed, *Extended RSF* provides two methods for adding to a source new messages to be monitored:

- You can add messages one by one, by using for each message the **Add a Single Message** menu. This method is discussed in “Adding a Single Message”, on page 3-7.
- You can also add a group of messages all at once, by creating an initialization file and applying this file through the **Add a Group of Associated Messages** menu. This method is discussed in “Adding a Group of Messages”, on page 3-13.

Adding a Single Message

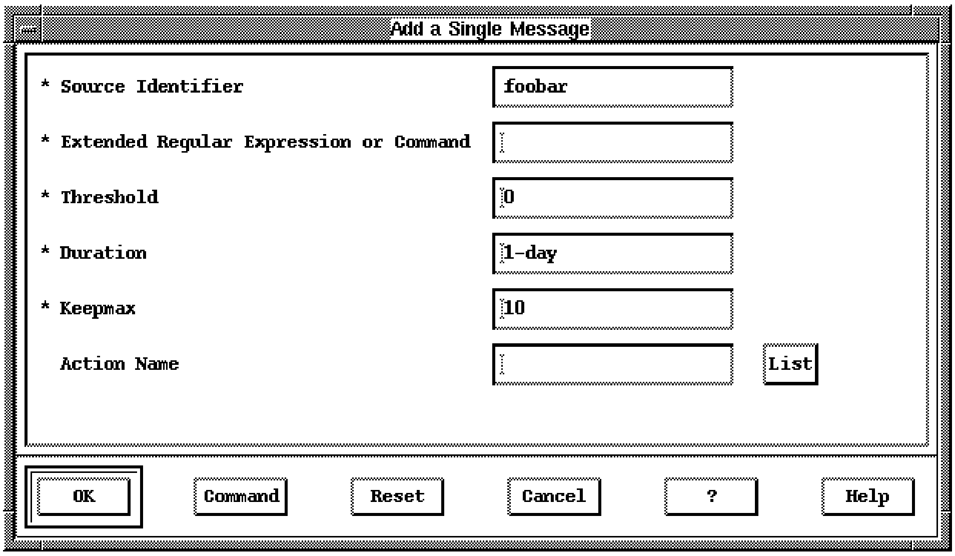
General Procedure

To add to a source a message to be monitored:

1. Go to the **Manage Monitored Sources and Associated Messages** menu, then successively choose **Add Associated Messages for a Monitored Source** and **Add a Single Message**. A list appears, that displays the sources that are currently defined.
2. Select the source to which you want to add an associated message. The Add a Single Message menu appears, containing different fields.
3. Enter the field values, as explained below.
4. As soon as you validate the entered values, *Extended RSF* begins to track the message you just have configured and to look for the occurrence of an over-threshold condition. In other words, no further operation is required for *Extended RSF* to take into account the new associated message.

5. If needed, repeat the previous steps to configure other messages you want to monitor in the source. Do not forget that the order in which you configure the different messages associated with the source is significant (see the previous section).

The figure below shows the **Add a Single Message** menu.



* Source Identifier: foobar

* Extended Regular Expression or Command:

* Threshold: 0

* Duration: 1-day

* Keepmax: 10

Action Name:

Source Identifier

Source Identifier, which is not an editable field, indicates the unique name you have specified when you configured the source (see “Source Identifier” on page 3-3). This name is shown here as a reminder to indicate the source you have just selected, i.e. the source with which the message you are defining is to be associated.

Extended Regular Expression or Command

In the **Extended Regular Expression or Command** field, you can enter either an extended regular expression or a command.

- If the first character of the field is not a slash (/), then the entered value is interpreted as an extended regular expression. Extended regular expressions are discussed below.
- Otherwise, i.e. if the entered value begins with a slash, then it is interpreted as a command. Specify the full path name of the executable file you want to use to detect relevant messages in the source. Command usage is discussed in “Filter Commands”, on page 3-10.

Whatever you enter, the purpose of either the extended regular expression or the command is the same: it will serve as a filter to track in the source the message you are configuring. A command, however, is also able to change the contents of a message before it is passed for further processing.

Extended Regular Expressions

If you specify an extended regular expression, *Extended RSF* uses it to perform a pattern match against the source.

The extended regular expressions valid within *Extended RSF* are similar to those used by the **awk** and **egrep** command (*Extended RSF* processes the extended regular expressions through the **regcomp** subroutine).

- Extended regular expressions are made up of ordinary and special characters. The indications below are not exhaustive and are provided as guidelines only.
- For a complete description of extended regular expressions (sometimes referred as “ERE”), refer to the **awk** command (and to the **regcomp** subroutine) in your AIX documentation.

Ordinary characters

In an extended regular expression, any ordinary character matches itself. For example, an `x` in a regular expression matches the `x` character.

Special characters

Special characters have a special meaning in an extended regular expression. The main special characters are summarized below. Refer to the **awk** command (and to the **regcomp** subroutine) in your AIX documentation for full details.

`/` Within *Extended RSF*, this character is special in the sense that, if it appears as the first character in the **Extended Regular Expression or Command** field, then the whole value is not considered as a regular expression but as a command. When not first, the slash is treated as an ordinary character. If needed, you can use the `[/]` expression (instead of `/)` to avoid to specify the slash as the first character of the expression.

`\` A `\` (backslash) preceding a special character cancels the special meaning of this character, which is therefore treated litterally. In fact two successive backslashes must be specified to cancel the special meaning of the following chracter. For example, `\\*` matches the asterisk symbol (which otherwise would have a special meaning).
Note that in the `\n` and `\t` expressions, which denote the newline and the tabulation characters, only one slash must be specified.

`.` The `.` (dot) matches any single character except the newline character. For example, the `foo.bar` expression matches any string made of the `foo` string followed by any character, followed by the `bar` string.

`+` An expression followed by a `+` (plus sign) matches one or more occurrences of the expression. For example, the `abcx+` expression matches the strings `abcx`, `abcxx` and `abcxxxxx`., but not the string `abc`.

`*` An expression followed by a `*` (asterisk) matches zero or more occurrences of the expression. For example, the `abcx*` expression matches the string `abc`, as well as the strings `abcx`, `abcxx` and `abcxxxxx`. Note that the `.*` expression matches any string (including the empty string).

`?` An expression followed by a `?` (question mark) matches zero or one occurrence of the expression. For example, the `abcx?d` expression matches the strings `abcd` and `abcxd`, but not the string `abcxxd`.

`|` Two expressions separated by a `|` (vertical bar) match a string that is matched by either. In other words, a `|` is like a logical “or”. For example, the `abc|xyz` expression matches the strings `abc` as well as the string `xyz`.

`()` Parenthesis provide the means to group strings together in regular expressions. For example, the `a(xx)?b` expression matches the strings `ab` and `axxb`.

`{}` Braces expressions such as `{m}`, `{m,}` and `{m,n}` (where `m` and `n` are integers) are also referred as interval expressions. The following exemplifies braces expressions: the `x{2}` expression matches a string that contains exactly two consecutive occurrences of the `x` character; `x{4,}` matches a strings that contains at least four consecutive occurrences of the `x` character; `x{2,4}` matches a string that contains between two and four, inclusive, consecutive occurrences of the `x` character (thus, two, three, or four occurrences).

`[]` A bracket expression of the form `[`*`specif`*`]` matches any character that pertains to the character set specified through the indicated *`specif`*.

For example `[abc]` matches `a`, `b` and `c`; `[a–zA–Z]` matches any lower- or uppercase letter; `[a–zA–Z]+` matches any string made of one or more letters.

Instead of range expressions, you can use a character class expression within brackets to match characters. The system interprets this type of expression according to the current character class definition. For example: `[[:upper:]]` matches any uppercase letter; `[[:digit:]]` matches any digit; `[[:alnum:]]` matches any character being either an upper or lowercase character or a digit;`[abc[:digit:]]` matches any character being a digit or being either an `a`, `b` or `c` letter.
The supported character classes are: `[:upper:]`, `[:lower:]`, `[:alpha:]`, `[:digit:]`, `[:alnum:]`, `[:xdigit:]`, `[:punct:]`, `[:space:]`, and `[:print:]`.

A `^` (caret) at the beginning of a bracket expression indicates that the expression does not match any characters within the brackets. For example, `[^abc]` matches any character excepted the `a`, `b`, and `c` characters, and `[^[:spaces:]]` matches any character which does not pertain to the `[:spaces:]` character class.

`^`

A `^` (caret) signifies the beginning of a line. For example, the `^foobar` expression matches the string `foobar` if it is at the beginning of the line.

`$`

A `$` (dollar sign) signifies the end of a line. For example, the `foobar$` expression matches the string `foobar` if it is at the end of the line, while the `^foobar$` matches a line consisting only of the `foobar` string.

Filter Commands

In the **Extended Regular Expression or Command** field of the **Add a Single Message** menu, you can enter either an extended regular expression (see above) or a command. When the first character of the field is a slash (`/`), the entered value is interpreted as a command.

If you specify a command, *Extended RSF* uses it to filter messages in the monitored source. Each time a new message occurs in the source, *Extended RSF* runs the filter command. The message text is passed to the command as its last argument. Then:

- If the command exits with a non-zero exit status, then *Extended RSF* assumes that the message is not relevant and thus, it does not increment the count for this message.
- If the command exits with a zero (`0`) exit status, then:
  - *Extended RSF* assumes that the message is relevant, and thus, it increments the count for this message;
  - in addition, *Extended RSF* replaces the message text with the standard output of the command. In other words, the standard output of the command becomes the message occurrence.

Example

The following example illustrates this feature.

Assume that you configure a new message, specifying /home/adm/filt_foobar in the **Extended Regular Expression or Command** field of the **Add a Single Message** menu. The /home/adm/filt_foobar command could be a shell script like the following:

```
#!/bin/ksh
# filt_foobar script to filter log messages

MSG="$1"  # store the message's text in the MSG variable

# For our application, messages other than the 'StartBuild'
# string are considered as non relevant. So, exit with a
# non-zero status for these non relevant messages:

if [ "$MSG" != 'StartBuild' ] ; then exit 1; fi

# The following applies only to 'StartBuild' messages. When such
# a message occurs, we want to call the cleanup_build_dir
# command which attempts to clean up a directory used by our
# fictitious application. If cleanup_build_dir succeeds, we
# do not need to be aware of the 'StartBuild' message; but if it
# fails, we want to be alerted since the build process of
# our application could fail.

if cleanup_build_dir
   then    # that is OK: throw the message away
       # return a non-zero exit value
         exit 1

   else    # cleanup_build_dir failed, we want to be alerted
       # write a message on standard output
         echo 'StartBuild: cleanup_build_dir failed'
       # and return a zero exit value
         exit 0
fi
```

Threshold

In the **Threshold** field of the **Add a Single Message** menu, enter an integer value. More than this number of messages must occur for an over-threshold condition to occur (and thus, for the corresponding action to be triggered).

- Actually, the occurrence of an over-threshold condition depends also on the **Duration** value (see below).
- Each time a message occurs in the source, the count for this message is incremented. An exception is the case where both **Threshold** and **Keepmax** are set to the 0 value. This special case is discussed on page 3-12.

Duration

For the over-theshold condition to be reached, the number of occurrences of the message (i.e. the number specified in the **Threshold** field) must occur within the time frame you specify in the **Duration** field.

The **Duration** value must be specified using a special but simple syntax. For example, valid values for the **Duration** field are `2-mins`, `180-mins`, `3-hours`, `1-day`, `1-days`, and `7-days`.

Examples:

- If you specify 3 as the **Threshold** and `1-hour` as the **Duration**, the over-threshold condition is reached only if more than 3 message occurrences are detected within a 1-hour period. If only 3 occurrences are detected within a 1-hour time frame, and a little later a fourth occurrence is detected, the over-threshold condition is not reached (and thus, *Extended RSF* does not trigger any action).
- If you specify `0` as the **Threshold**, the over-threshold condition is reached as soon as one message occurrence is detected in the source. Note that when the **Threshold** is `0`, the **Duration** value does not matter.

Keepmax

In the **Threshold** field of the **Add a Single Message** menu, enter an integer value. This value specifies the number of occurrences that are stored by *Extended RSF*. Only the most recent occurrences are kept in the history. These kept messages can be displayed at any time using the **List Message Text for Overthreshold Messages** option of the **List Monitored Sources and Associated Messages** menu.

When specifying the **Keepmax** value, have in mind the following:

- You must specify a **Keepmax** value greater than the **Threshold** value (regardless, if you try to specify a smaller value, an error message is displayed when you validate the SMIT screen, prompting you to enter a greater value).
- However, it is valid to specify the 0 value for both **Threshold** and **Keepmax**. This special case is discussed below.

Special Case where Threshold = Keepmax = 0

Setting both the **Threshold** and the **Keepmax** values to `0` has a special meaning.

In this case, even when a matching message is detected, the message count is not incremented, so it is never necessary to reset the count for this message to “re-arm” it. The over-threshold condition will occur (and thus the corresponding action will be triggered) for each occurrence of a matching message.

In addition, note that in this special case, since the value of **Keepmax** is 0, no message occurence is kept in the history.

Note: For an introduction to the important notion of message count, refer to “Message Count”, on page 1-2.

Action Name

Any source has associated with it a default action. When configuring a message, you can override this default action by filling in the **Action Name** field.

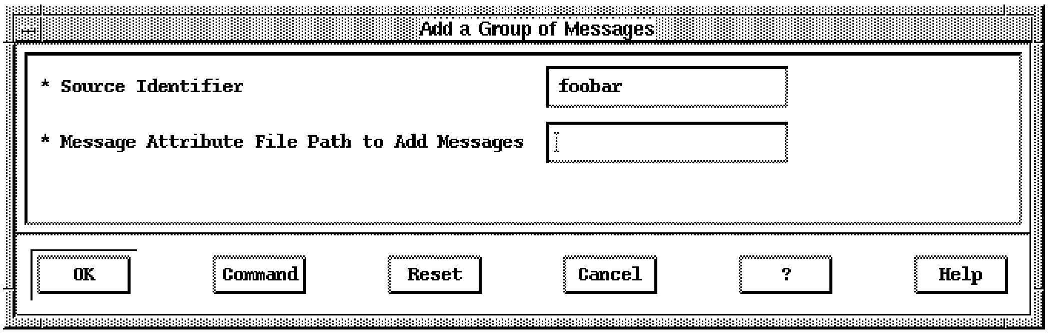
- either leave the **Action Name** field empty, so that the action corresponding to the message you are configuring is the default action associated with the source,
- or, if the default action associated with the source does not match your requirements for the message you are configuring, fill in the **Action Name** with a specific action (use the F4 key or click on the “List” button to display the list of available actions). In this case, when *Extended RSF* detects an over-threshold condition for this message, it triggers this specific action instead of the default action associated with the source.

Adding a Group of Messages

Instead of configuring one by one the messages to be monitored in a source, you can configure a group of messages at once, by creating an initialization file and applying this initialization file through the **Add a Group of Associated Messages** menu.

General Procedure

1. Create an initialization file that corresponds to your requirements, as explained in “Initialization Files”, on page 3-13.
2. Go to the **Manage Monitored Sources and Associated Messages** menu, then successively choose **Add Associated Messages for a Monitored Source** and **Add a Group of Associated Messages**. A list appears, that displays the sources that are currently defined.
3. Select the source to which you want to add the associated messages defined in the initialization file. The **Add a Group of Messages** menu appears, as shown below.



Add a Group of Messages

* Source Identifier: foobar

* Message Attribute File Path to Add Messages:

4. Enter the field values, as explained below:

   Source Identifier, which is not an editable field, indicates the unique name you have specified when you have configured the source (see “Source Identifier” on page 3-3). This name is shown here as a reminder to indicate the source you have just selected, i.e. the source with which the messages are to be associated.

   In the **Message Attribute File Path to Add Messages** field, specify the full path name of the initialization file to apply.
5. Validate the screen to apply the message definitions specified in the initialization file.

   As soon as the initialization file is applied, *Extended RSF* begins to track the corresponding messages and to look for the occurrence of over-threshold conditions. In other words, no further operation is required for *Extended RSF* to take into account the new associated messages.

Understanding Initialization Files

An initialization file describes the characteristics of the messages that are to be associated with the source. Once you have created an initialization file, you can apply it by specifying its name in the **Message Attribute File Path to Add Messages** field explained above, or in the **Message Attribute File Path for Message Creation** field discussed on page 3-5.

Syntax

An initialization file must follow the syntax conventions described below.

- Comment lines can be inserted in the file by putting a # character at the beginning of the line.
- Each non-comment line describes the characteristics of one message to be monitored. Each line is made up of 5 fields separated by blanks (spaces or tabs). The 5th field is optional. The general format is:

  ```
  ERE   threshold    duration    keepmax    <action>
  ```

- The five fields are explained below.

  `ERE`: The extended regular expression to be used by *Extended RSF* to track the message in the source. This expression must be enclosed within quotes. This field has the same role as the **Extended Regular Expression** field of the **Add a Single Message** menu (see details on page 3-8).

  `duration`: An expression specifying the time frame within wich the number of occurrences of the message (i.e. the `threshold`) must occur for the over-threshold condition to be reached. It corresponds to the **Duration** field of the **Add a Single Message** menu (see details on page 3-12).

  `threshold`: An integer specifying the message threshold value. It corresponds to the **Threshold** field of the **Add a Single Message** menu (see details on page 3-11).

  `keepmax`: An integer greater than `threshold` (may be equal to `threshold` only if both `keepmax` and threshold are set to `0`). This field has the same role as the **Keepmax** field of the **Add a Single Message** menu (see details on page 3-12).

  `action` (optional): The name of the specific action to be associated with this message. This field has the same role as the **Action Name** field of the **Add a Single Message** menu (see details on page 3-12).

Order Significance

Within *Extended RSF*, messages are associated with a source in an ordered fashion. That means that the order in which messages are configured is significant. This important consideration is discussed in “Order Significance in Message Specifications”, on page 3-6.

A practical consequence, for the initialization files, is that you must enter message specifications from the most specific to the more general.

Example 1

```
# Sample initilalization file to configure messages to
# be monitored in the ”foobar” source.
#
# ERE                  threshold  duration keepmax  <action>
#
’FATAL’                0          1–day    0        urgent_act
’ERROR.*still trying’  5          5–mins   15       beep_admin
’ERROR.*(4099|3722)’   0          1–day    8        notify_joe
’ERROR|WARNING’        5          1–day    15
#
# end of initialization file
```

The sample file above allows you to configure and associate four messages with a source. Here are some additional comments:

- The first specification (`’FATAL’`...) instructs *Extended RSF* to search for any message that contains the FATAL string. Both the *threshold* and the *keepmax* values are set to `0`. This setting has a special meaning: even when a matching message is detected, the message count is not incremented, so it is never necessary to reset the count for this message to “re-arm” it. The over-threshold condition will occur (and thus the `urgent_act` action will be triggered) for each occurrence of a matching message.

- The second specification (`’ERROR.*still trying’...`) instructs *Extended RSF* to search for any message that contains the `ERROR` string, followed by any number (possibly zero) of any character (except newline), followed by the `still trying` string. The over-threshold condition is reached (and thus the `beep_admin` is executed) if more than 5 matching messages occur within a 5-minute time frame.
- The third specification is similar to the previous one.
- The last specification includes only 4 fields. Since the fifth field is not specified, no specific action is associated with this message. Thus, the default action associated with the source will be used.

Example 2

Consider the following initialization file, which is similar to the previous sample, except that the message specifications are entered in a different order:

```
’FATAL’               0          1–day    0        urgent_act
’ERROR|WARNING’       5          1–day    15
’ERROR.*still trying’ 5          5–mins   15       beep_admin
’ERROR.*(4099|3722)’  0          1–day    8        notify_joe
```

Here, *Extended RSF* will never trigger actions corresponding to the two last specifications. This is because the second specification is more general than the last two, since it matches any message that contains the `ERROR` string. Thus, when *Extended RSF* detects a message matching the second specification, it triggers the corresponding action and stops here. Since a matching message has been detected, it does not walk through the remaining message specifications.

Creating a Source “Snapshot”

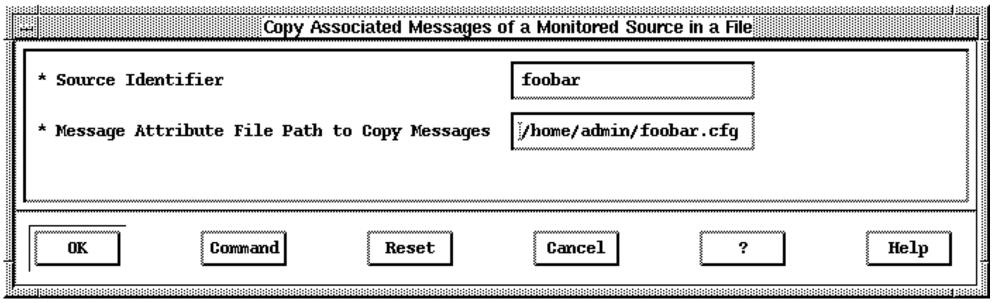
Note that you can create an initialization file corresponding to the current setup of a given monitored source. The created initialization file can be seen as a “snapshot” of the source setup.

This feature can have various purposes.

- For example, you may want to create an initialization file from a source you have manually set up on a host, copy the file to other hosts, then apply the initialization file to set up *Extended RSF* on these hosts.
- Another case where this feature can be useful is when you want to change the order precedence of the messages associated with a source. See “Snapshot Usage Example: Changing Message Precedence Order” below.

To create such a “snapshot”:

1. Select the **Copy Associated Messages of a Monitored Source in a File** option of the **Manage Monitored Sources and Associated Messages** menu.
2. In the list that appears, select the desired source. The following menu is displayed:



Copy Associated Messages of a Monitored Source in a File

* Source Identifier: foobar

* Message Attribute File Path to Copy Messages: /home/admin/foobar.cfg

3. In the **Message Attribute File Path to Copy Messages** field, enter the full pathname of the initialization file you want to create.

4. Validate the screen to create the initialization file.

Snapshot Usage Example: Changing Message Precedence Order

As explained on page 3-6, messages are associated with a source in an ordered fashion. Once you have associated messages with a source, if you want subsequently change the order of the messages, two methods are possible:

- **Method 1**: Using the SMIT menus, delete the messages associated with the source, then reconfigure them in the desired order. If there are numerous messages, this method may be tedious.
- **Method 2**: Create a snapshot of the source, then edit the obtained snapshot and change the message order as desired, then apply the modified snapshot to the source. This method is more appropriate than the previous one if many messages are associated with the source. Indeed, with this second method, you have not to reconfigure the messages one by one with the SMIT menus.

The steps below summarize the second method, based on snapshots:

1. Create a snapshot of the source whose associated messages are to be reordered. Use the **Manage Monitored Sources and Associated Messages** menu as explained above.
2. Edit the snapshot you have just created (using **vi** or another text editor). Make the desired changes to the file (you may change the order of the messages as well as message parameters), and save the file.
3. From the Extended RSF main menu, select **Manage Monitored Sources and Associated Messages**, then **Change/Show a Monitored Source**.
4. From the list that appears, select the source you want to change. The **Change/Show a Monitored Source** menu is displayed.
5. In the **Message Attribute File Path to replace Messages** field, specify the full pathname of the snapshot you have edited and saved. When you validate the screen, the source is reconfigured according to the message specifications (message order and parameters) found in the snapshot file.

Chapter 4. Management Tasks

This chapter discusses management tasks related to *Extended RSF*.

- Supervising the Monitoring Process
- Managing Action Definitions
- Managing Source and Message Definitions

Supervising the Monitoring Process

This section describes the different management tasks you may want to perform in order to supervise the monitoring process carried out by *Extended RSF*. The following tasks are described:

- Understanding the Monitoring Process
- Enabling the Monitoring Process
- Listing Information about Over-threshold Messages
- Listing Information about Executed Actions
- Resetting the Action History
- Resetting Message Counts
- Stopping Monitoring a Source or a Specific Associated Message

Understanding the Monitoring Process

To understand the monitoring process carried out by *Extended RSF*, please refer to chapter “Getting Started with Extended RSF”, starting on page 1-1. More specifically, refer to “Basic Concepts and Terminology”, on page 1-2, and pay particular attention to the following concepts:

- Over-threshold Messages
- Message Count

Enabling the Monitoring Process

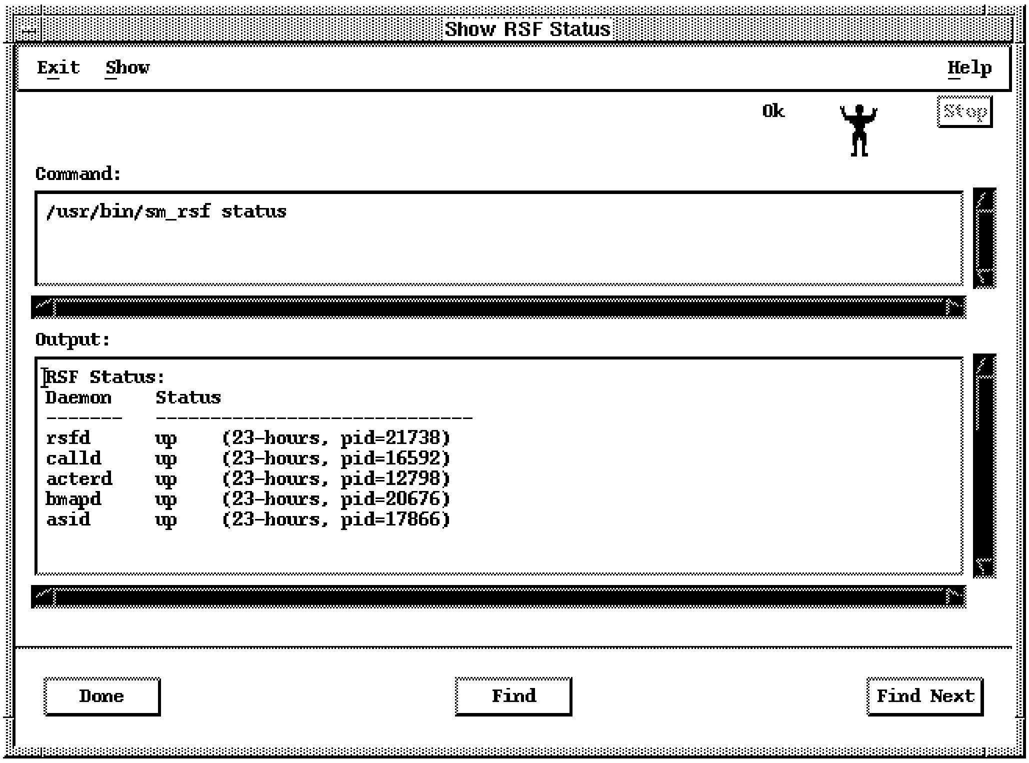
As soon as you configure a source to be monitored, the monitoring process takes place (no further operation is required).

This supposes, however, that RSF is running (*Extended RSF* relies on mechanisms provided by RSF daemons). This should be the case if you have installed RSF and *Extended RSF* as explained in appendix “Installing Extended RSF”.

If in doubt, you may want to check that RSF is effectively running:

1. Go to the RSF main menu: from the SMIT top level menu, choose **Problem Determination**, then **RSF (Remote Services Facilities)**.

2. Choose the **Show RSF Status** option. At the top of the screen that appears, you see an area whose title is **RSF Status**, which indicates the status of the RSF daemons (see the illustration below):



```
/usr/bin/sm_rsf status
```

```
RSF Status:
Daemon    Status
-------   ----------------------------
rsfd      up    (23-hours, pid=21738)
calld     up    (23-hours, pid=16592)
acterd    up    (23-hours, pid=12798)
bmapd     up    (23-hours, pid=20676)
asid      up    (23-hours, pid=17866)
```

3. Check that the four RSF daemons **rsfd**, **calld**, **acterd** and **bmapd** are **up**.
4. If you use actions of the type **Send SNMP Trap**, the **asid** daemon is also required, so you must check that it is **up**.
5. If any of the required daemons is **down**, restart RSF using the **Start / Stop RSF** option. For further information, refer to “Carrying Out Setup Tasks” in the appendix “Installing Extended RSF”.

Listing Information about Over-threshold Messages

Note: The notion of over-threshold messages is discussed on page 1-2.

At any time, you can list the messages that went over-threshold. Several options are provided that differ in the type of information included in the list they display (see below).

Listing Message Text for Over-threshold Messages

To list the message text for over-threshold messages associated with a given source:

1. Select the **List Message Text for Overthreshold Messages** option of the **List Monitored Sources and Associated Messages**.
2. From the list that appears, select the desired source. For each over-threshold message (if any), this displays the message identifier and the text of the messages that have been kept in the history.

Note: If the **Keepmax** value associated with a message is `0`, the message does not appear in the list (since no message occurrence is kept in the history). For details on **Keepmax**, refer to page 3-12.

Listing Attributes and Count for Over-threshold Messages

To list the attributes and count for over-threshold messages associated with a given source:

1. Select the **List Attributes for Overthreshold Messages** option of the **List Monitored Sources and Associated Messages**.
2. From the list that appears, select the desired source. For each over-threshold message (if any), the following information is displayed: the extended regular expression used for message matching; the count (i.e. how many times the message occurred in the monitored source); the threshold; the duration; the keepmax; the associated action. This information (except the message count) corresponds to the field values entered when configuring the message (see “Adding a Single Message”, on page 3-7).

Listing Information about Executed Actions

When a message goes over-threshold, *Extended RSF* triggers the action associated with the message. At any time, you can list the actions that *Extended RSF* has executed due to the occurrence of over-threshold conditions. This provides you with a way of reviewing what has been done by *Extended RSF*.

To list a history of the triggered actions:

1. Go to the RSF main menu: from the SMIT top level menu, choose **Problem Determination**, then **RSF (Remote Services Facilities**).
2. Select **Dial Out Management**, then **Display Dial Out Log File** option. This displays the history of triggered actions.

   Note that the history includes actions triggered by *Extended RSF* as well as actions triggered by RSF. However, you can easily identify the latter, since their name is always **callscarf**, **callrcs2** or **cluster** (these are callouts issued for remote maintenance purposes).

Note: The action history is recorded in the **/var/rsf/actionlog** file. See below for related information.

Resetting Message Counts (to Acknowledge Actions)

Background Notions

Each time *Extended RSF* detects a relevant message in a monitored source, it updates the count for this message.

Once a given message has gone over-threshold, it will not go over-threshold again (no further action will be triggered) until you explicitely reset the count for this message. This avoids continually repeated actions for the same event.

Note: Conceptually speaking, resetting a message count means acknowledging the occurrence of the corresponding action.

Manually Resetting Message Counts (using SMIT)

To reset the count of a message in a monitored source using SMIT:

1. Go to the **Manage Monitored Sources and Associated Messages** menu.
2. Select either **Reset Counts of over-threshold Messages in Source** or **Reset Count of an Associated Message**.

   The first option allows you to reset the count of all messages that went over-threshold in a given source. The second allows you to reset the count of any specific message, whether or not it went over-threshold.
3. From the list that appears, select the desired source, then:
   - If you have selected **Reset Counts of over-threshold Messages in Source**, the count of over-threshold messages is reset as soon as you have selected the desired source and you have confirmed the operation.

– If you have selected **Reset Count of an Associated Message**, a new list appears, showing the messages associated with the source. From this list, select one or more messages. When you validate your selection (you are prompted for a confirmation), the count of the selected messages is reset.

Resetting a Message Count from within a Custom Action

If it is necessary to have an action performed at every occurrence of a message, then the message count should be reset by the action itself in order to "re-arm" the message. This can be achieved by invoking the **chmsrc** command from within the triggered custom action.

Note: A "custom action" can be any executable file. In particular, it may be a shell script. Custom actions are discussed in "Adding a 'Custom Action' Action", on page 2-2.

chmsrc Command Syntax:

/usr/bin/chmsrc –r –n <*source*>

where <*source*> is the source identifier (this is the string that identifies the source: see "Source Identifier" on page 3-3)

This command resets the count of **all** over-threshold messages in the specified source.

Example of Use:

You could create a custom action with the following parameters:

Path to Executable:	`/home/john/foobar_act`
Arguments:	`%text %source`

The `/home/john/foobar_act` being a shell script which invokes the **chmsrc** command, as in the example below:

```
#!/bin/ksh
# foobar_act script called by Extended RSF with 2 arguments:
# $1 : the value yielded by the %text keyword, i.e. the name of
#      the temporary file that contains the text of the message
# $2 : the source identifier (%source)
#
# Mail a notification message to root:
/usr/bin/mail –s ”The foobar_act action occurred” root < $1
#
# Reset the count of all overthreshold messages in the source:
/usr/bin/chmsrc –r –n $2
#
#end of script
```

Stopping Monitoring a Source or a Specific Associated Message

Stopping Source Monitoring

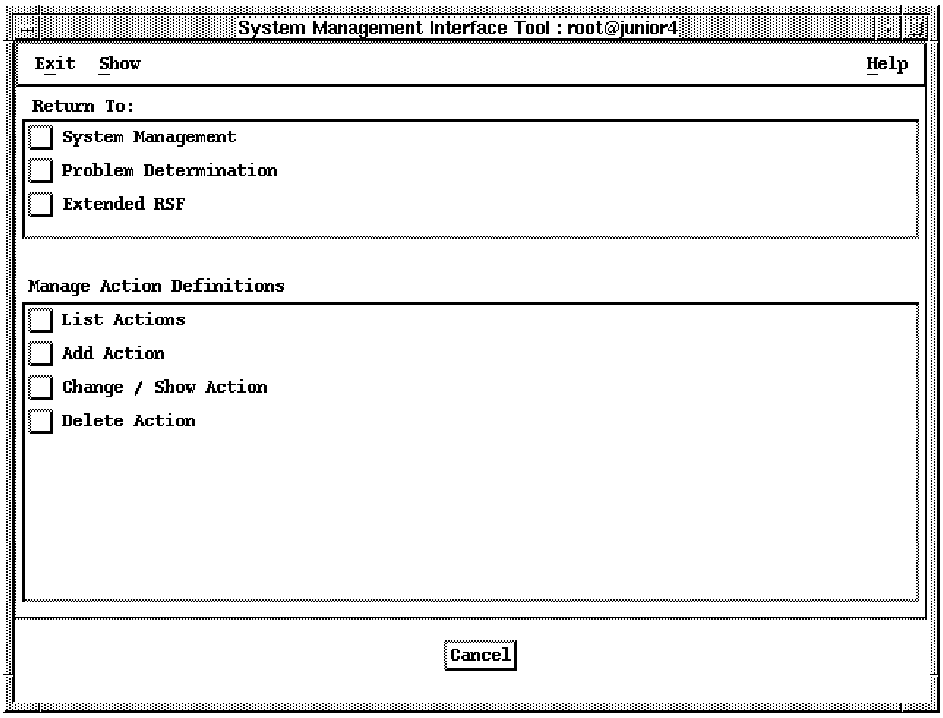
To tell *Extended RSF* to stop monitoring a source, remove the source from the list of monitored source. Refer to the **Delete a Monitored Source** option discussed on page 4-8.

Stopping the Monitoring of a Specific Message

To tell *Extended RSF* to stop monitoring a source, remove the message from the source. Refer to the **Delete Associated Message of a Monitored Source** option discussed on page 4-8.

Managing Action Definitions

The facilities related to action management are accessed through the **Manage Action Definitions** menu shown below.



The menu options are summarized below:

List Actions: This option displays a summary list of all the actions that are currently defined.

Add Action: This option allows you to define a new action. This is fully explained in chapter “Configuring Actions”, starting on page 2-1.

Change/Show Action:
This option shows or changes a defined action. It brings up a menu similar to the **Add Action** menu, except that this menu includes an additional field, **New Action Name**. Use this optional field only if you want to rename the action.

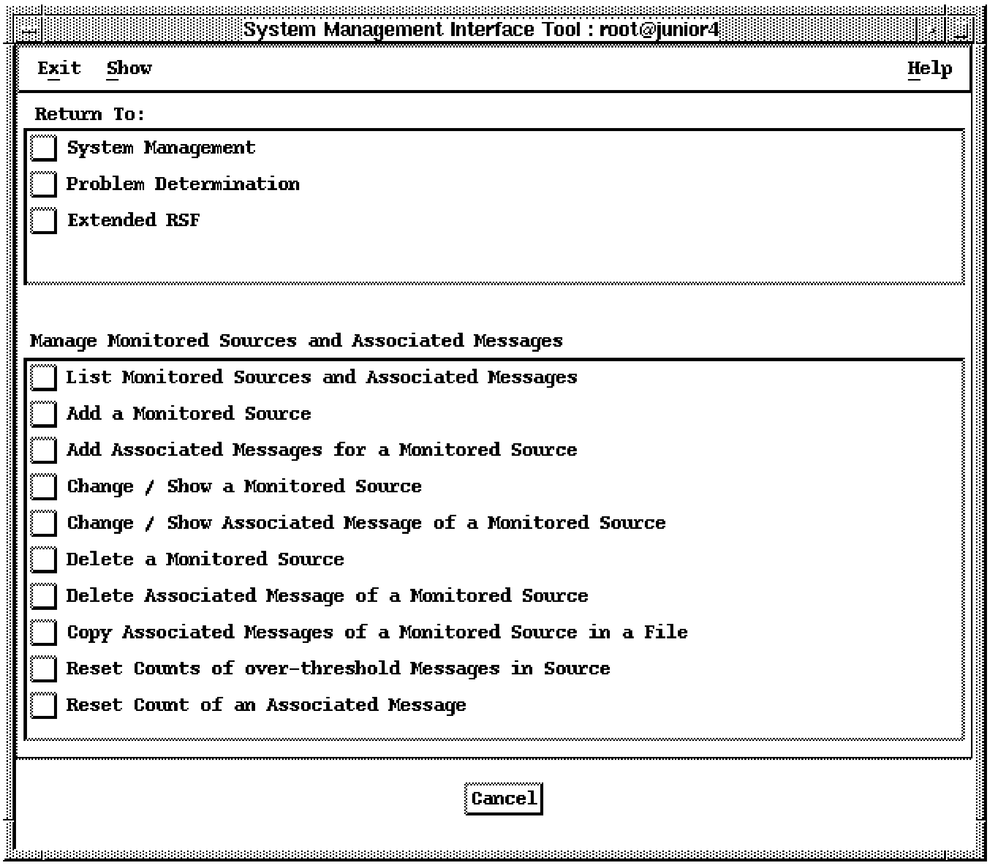
Delete Action: This option deletes a defined action you do not need anymore (a deleted action becomes undefined; be sure that no source makes use of the action you want to delete).

Managing Source and Message Definitions

The **Manage Monitored Sources and Associated Messages** menu, shown below, includes numerous options, which are related to two kind of tasks:

- Options related to the management of definitions. — They allow you to set up sources and associated messages, as well as to list or change the current definitions.
- Options related to the management of the monitoring process. — They allow you to know which over-threshold conditions occurred, and to reset the count for messages.

Note: This section discusses only the options related to the management of definitions. The options that relate to the management of the monitoring process are discussed in “Managing the Monitoring Process”, on page 4-1.



Return To:

□ System Management
□ Problem Determination
□ Extended RSF

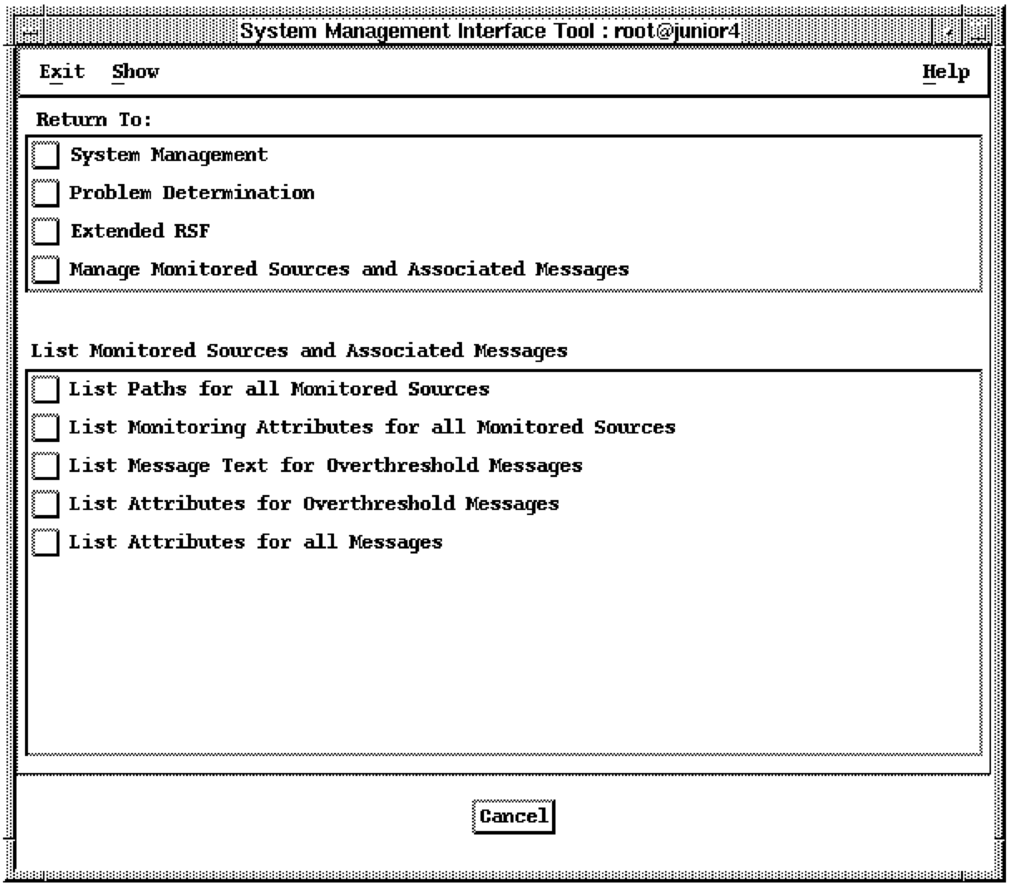
Manage Monitored Sources and Associated Messages

□ List Monitored Sources and Associated Messages
□ Add a Monitored Source
□ Add Associated Messages for a Monitored Source
□ Change / Show a Monitored Source
□ Change / Show Associated Message of a Monitored Source
□ Delete a Monitored Source
□ Delete Associated Message of a Monitored Source
□ Copy Associated Messages of a Monitored Source in a File
□ Reset Counts of over-threshold Messages in Source
□ Reset Count of an Associated Message

The options related to the management of source and message definitions are summarized below.

List Monitored Sources and Associated Messages

This option brings up the menu shown below:



Return To:

□ System Management
□ Problem Determination
□ Extended RSF
□ Manage Monitored Sources and Associated Messages

List Monitored Sources and Associated Messages

□ List Paths for all Monitored Sources
□ List Monitoring Attributes for all Monitored Sources
□ List Message Text for Overthreshold Messages
□ List Attributes for Overthreshold Messages
□ List Attributes for all Messages

- **List Paths for all Monitored Sources**:
This option shows the path of each monitored source currently defined. For each source, the list indicates the corresponding identifier and path (source identifier and path are discussed on page 3-3).

- **List Monitoring Attributes for all Monitored Sources**:
This option shows the attributes of each monitored source currently defined. These attributes (clean time, search time, etc) correspond to the field values described in “Entering the Field Values”, on page 3-3.
In addition, for each source, the list indicates whether or not an over-threshold condition occurred.(“Over” column of the listing).

- **List Message Text for Overthreshold Messages**
- **List Attributes for Overthreshold Message**
These two options allow you to obtain information concerning the messages that went over-threshold. For details, refer to “Listing Information about Over-threshold Messages”, on page 4-2.

- **List Attributes for all Messages**:
This option shows the attributes of the different messages associated with the monitored sources. These attributes (threshold, duration, etc) correspond to the field values described in “Adding a Single Message”, on page 3-7.
In addition, for each message, the list indicates its count, i.e. how many times the message occurred in the monitored source.

Add a Monitored Source

This option allows you to add a new source to be monitored. This is fully explained in "Adding a New Source to be Monitored", on page 3-2.

Add Associated Messages for a Monitored Source

This option allows you to add (i.e. configure) one or several associated messages in order to instruct *Extended RSF* which message(s) it must look for in the source. This task is fully explained in chapter "Configuring Monitored Sources and Associated Messages": for details, start with section "Prior Knowledge for Adding New Messages to a Source", on page 3-6.

Change/Show a Monitored Source

This option allows you to show or to change a defined source. It brings up a menu similar to the **Add a Monitored Source** menu (discussed on page 3-2), except that this menu includes an additional field, **New Source Identifier**. Use this optional field only if you want to give a new name to the source. For a usage example of the **Message Attribute File Path to replace Messages** optional field, refer to page 3-16.

Change/Show Associated Message of a Monitored Source

This option allows you to show or to change the defintion of a given message associated with a given source. When you choose this option, two pop-up menus are successively displayed that prompt you for the desired monitored source, then for the desired associated message.

Once you have selected the desired message, the **Change/Show Associated Message of a Monitored Source** menu is displayed. It is identical to the **Add a Single Message** menu (discussed on page 3-7), except that this menu includes an additional field, **Message Identifier**. This field, which is informative only (it is not editable), shows the numeric identifier associated with the message. For information related to message identifiers, refer to "Order Significance in Message Specifications", on page 3-6. For a discussion on how to change message precedence order, refer to page 3-16.

Delete a Monitored Source

This option allows you to undefine a given source, i.e.to remove the source definition from the *Extended RSF* setup (the monitored ASCII file itself is not deleted). As soon as you have deleted a source, *Extended RSF* stops monitoring it.

Delete Associated Message of a Monitored Source

This option allows you to remove a given message currently associated with a monitored source. As soon as you have deleted a message, *Extended RSF* stops looking for it in the source (however, *Extended RSF* continues monitoring the source, i.e. it looks for the remaining associated messages).

Copy Associated Messages of a Monitored Source in a File

This option allows you to create an initialization file corresponding to the current setup of a given monitored source. The created initialization file can be seen as a "snapshot" of the source setup. For details, refer to "Creating a Source Snapshot", on page 3-15.

Reset Counts of over-threshold Messages in Source
Reset Count of an Associated Message

These two options relate to the management of the monitoring process. Refer to "Resetting Message Counts", on page 4-3.

Appendix A. Installing Extended RSF

This appendix is meant to be used by the person responsible for installing RSF and *Extended RSF*.

Installing the Software

Checking that RSF is Preloaded

Preliminary Remarks

- *Extended RSF* is based on mechanisms provided by the RSF software. Thus, RSF is required for *Extended RSF* to work.
- RSF is normally preloaded on any DPX/20 ESCALA. For other DPX/20 systems, it may be preloaded or not. In any case, if you can get the software from media:
  - either the “Bull-Enhancement” CD-ROM.
  - or a specific, orderable, set of floppies (that include RSF and *Extended RSF*).

Software Packaging

RSF and *Extended RSF* are actually packaged as a unique LPP, namely **rsf**:

- RSF is made of two filesets, **rsf.rsflite** and **rsf.rsflite.data**. These filesets are required for *Extended RSF* operation.
- The *Extended RSF* software package is made of **rsf.extended** and optionaly **rsf.extended.snmp**. Note that these filesets are not required for basic RSF operation.

Checking Procedure

Check if RSF is preloaded by entering this command:

```
lslpp –L ’rsf*’
```

If this command does not list the appropriate RSF filesets (described above), then they are not preloaded, and thus, you must install them from a media. In any case, you have to install the *Extended RSF* filesets because they are not preloaded. Refer to the instructions below.

Installing the Software from a Media (CD-ROM or Floppies)

RSF and *Extended RSF* installation requires 6 MBytes of disk space.

Carrying Out the Installation

1. If you are using a CD–ROM, skip directly to step 2 below. If you are using floppies, first copy the product onto the hard disk, using the following SMIT command (as “root”):

   ```
   smit bffcreate
   ```

   Note: `bffcreate` is the smit fast path equivalent to the following succession of smit options: Software Installation and Maintenance → Copy Software to Hard Disk for Future Installation.

   As requested, specify the appropriate floppy drive, for example **/dev/fd0** (you may use F4 to display the list of available input devices). Once your choice is validated, a menu is displayed.

   Since the floppies contain only RSF, you may leave the “all” value in the field “Software package to copy”. All default values are suitable, so execute the copy by activating the

"Do" command. Successively load each floppy as you are prompted for it. Files are copied to the **/usr/sys/inst.images** directory. Now, proceed with step 2 below.

2. As root, enter the following command:

   ```
   smit install_selectable_all
   ```

   Note: `install_selectable_all` is the smit fast path equivalent to the following succession of smit options: Software Installation and Maintenance → Install and Update Software → Install/Update Selectable Software (Custom Install) → Install/Update From All Available Software.

   A SMIT menu is displayed, that prompts you to specify an input device or directory:

   – If you are installing RSF from a CD–ROM, specify the appropriate drive, for example **/dev/cd0** (you may use F4 to display the list of available input devices).

   – If you are installing RSF from floppies, specify the **/usr/sys/inst.images** directory (i.e. the directory into which you have copied files during step 1).

   Once you have validated your choice, a menu is displayed.

3. Fill in the **Software to install** field. Specify either **rsf** in order to install RSF as well as *Extended RSF*, or **rsf.extended** if RSF is already installed and you are installing *Extended RSF* only. (If you plan to use the SNMP capability of *Extended RSF*, you must also install the **rsf.extended.snmp** fileset.)

   All other field values are suitable, so run the installation process by activating the **Do** command. The installation process takes no more than two or three minutes.

4. Once the installation process is complete, you have to carry out initial setup tasks, as explained below.

Carrying Out Initial Setup Tasks

Once the software is installed, you have to proceed with the following tasks:

- Set up the RSF software as explained in the *RSF Field Guide*.
- If you plan to use the SNMP capability of *Extended RSF*, make sure that the snmpd daemon is running on the system (**snmpd** is discussed in the AIX documentation).
- Start RSF (i.e. the RSF daemons), by using the **Start / Stop RSF** option menu of RSF: for details, refer to page 4-2 or to the RSF documentation. Note that you can check the status of the RSF daemons by using the **Show RSF Status** option menu of RSF (discussed on page 4-2).

Once the RSF daemons are started, *Extended RSF* is able to monitor sources as desired. To know how to set up *Extended RSF* (actions, sources and messages), refer to the previous chapters.

Remarks on the SNMP Capability

If you plan not to use the SNMP capability of *Extended RSF*, we recommend that you discard the **rsf.extended.snmp** fileset.

Indeed, when this fileset is installed, RSF tries at startup to run the **asid** SMUX peer daemon. At this moment, if the **snmpd** daemon is not running on the system, **asid** is not able to run properly and displays the following message on the console:

```
asid: Warning: smux_init: systemError [join_tcp_server failed:...
```

This does not, however, prevent RSF and *Extended RSF* from operating normally.

Note: For details related to the SNMP capability and to the **asid** daemon, refer to the appendix "Configuring ISM for Use With Extended RSF", starting on page B-1.

Appendix B. Configuring ISM for Use With Extended RSF

This appendix explains how to set up the ISM product to handle SNMP traps emitted through *Extended RSF*. Although these explanations focus on the ISM software, they are intended to be useful even if you plan to use any other SNMP-based system/network management software.

- Concepts
- Setup Procedure Summary
- Installing and Enabling the asid SMUX Peer Daemon
- Setting Up the SNMP Environment
- Setting Up ISM
- Where You Go From Here
- Hints for Troubleshooting asid

Concepts

What is ISM?

ISM (Integrated System Management) is a Bull product designed to monitor and manage distributed systems and networks.

ISM offers a user-friendly and configurable graphical interface. In addition, ISM employs a sophisticated architecture in which all networked resources are defined as objects, making it easy to integrate different components into a single, consistent view.

Extended RSF and SNMP

“Send SNMP Trap” Actions

Within *Extended RSF*, you can define actions of the type **Send SNMP Trap**, so that when an over-threshold condition occurs, *Extended RSF* emits a trap.

Although this appendix focuses on the ISM software, any system/network management software based on SNMP can take advantage of this feature.

Note: For details about the **Send SNMP Trap** action, refer to “Adding a Send SNMP Trap Action”, on page 2-7.

asid, the SMUX Peer Daemon

The SNMP capability of *Extended RSF* is implemented through **asid**, a specific SMUX peer daemon that comes with *Extended RSF*. This SMUX peer daemon is responsible for communicating with **snmpd**, the standard SNMP agent that comes with AIX. For *Extended RSF* to be able to handle SNMP traps, both **asid** and **snmpd** must be implemented on the monitored system. This is explained later in this appendix.

Setup Procedure Summary

Implementing the SNMP capability of *Extended RSF* involves the following steps:

- Installing and Enabling the **asid** SMUX Peer Daemon
- Setting Up the SNMP Environment
- Setting Up ISM

These steps are explained in the sections that follow.

Installing and Enabling the asid SMUX Peer Daemon

Note: The role of the **asid** daemon is introduced in section “asid, the SMUX Peer Daemon”, on page B-1.

In order to implement the SNMP capability of *Extended RSF*, the **rsf.extended.snmp** fileset must be installed. This fileset provides notably the **asid** daemon.

When this fileset is installed, RSF at startup tries to run the **asid** daemon. For **asid** to work properly, the **snmpd** daemon (that comes in standard with AIX) must be enabled on the system.

- At any time, you can know if **asid** is running by using the **Show RSF Status** option of the RSF menu. The **asid** daemon is managed like other RSF daemons: it is started and stopped using the **Start / Stop RSF** option of the RSF menu.
- For details about fileset installation, refer to the appendix “Installing Extended RSF”, starting on page A-1. In addition, note that if the **rsf.extended.snmp** fileset is installed after the initial installation/setup of RSF, then you must start again the RSF daemons to ensure that the newly added **asid** daemon is started.
- For details about setting up **snmpd** and related files, see below.

Setting Up the SNMP Environment

This task must be carried out on any system you want to enable to send SNMP traps through *Extended RSF*. It consists essentially in configuring **snmpd**, the standard SNMP agent for AIX.

During the installation of the **rsf.extended.snmp** fileset, two configuration files, **/etc/snmpd.conf** and **/etc/snmpd.peers**, are updated with appropriate identification strings and passwords. Check and update these files as explained below.

Make Sure that snmpd is Enabled

The **snmpd** daemon is a subsytem controlled by the System Resource Controller (SRC). The **snmpd** daemon is a member of the **tcpip** system group.

The instructions of this appendix assume that the **snmpd** daemon is enabled on your system. This should be the case, since the **snmpd** daemon is enabled by default on a standard system.

If in doubt, enter the following command to display the status of **snmpd**:

```
lssrc –s snmpd
```

Check that the displayed status of **snmpd** is “active”. If not, enable **snmpd** by entering the following command:

```
startsrc –s snmpd
```

If needed, refer to your AIX documentation for further information on **snmpd** and SRC commands.

Edit /etc/snmpd.conf

Edit the **/etc/snmpd.conf** file and follow the steps below. If needed, refer to your AIX documentation for details on the **/etc/snmpd.conf** file.

1. Check that the line below has been added to the file (add it if necessary):

```
smux   1.3.6.1.4.1.107.121.1   rsf_password  # RSF
```

2. Near the end of the file, there should be a line which looks like the following (add it if necessary):

```
trap    public  127.0.0.1       1.2.3   fe      #loopback
```

3. Beneath this line, add trap definition lines as needed to specify which machines should receive traps generated by *Extended RSF*. You must add one line for each ISM manager station you plan to use for monitoring. In the example below, two trap lines were added corresponding to two ISM stations, **ism_foo** and **ism_bar**, whose IP addresses are 130.183.1.1 and 130.183.1.51. Both **ism_foo** and **ism_bar** stations will receive traps.

```
trap    public  130.183.1.1     1.2.4   fe      #ism_foo
trap    public  130.183.1.51    1.2.5   fe      #ism_bar
```

In the example above, the “`1.2.4`” and “`1.2.5`” specifications denote the *View* field. Although this field is not actually used by the AIX **snmpd** daemon, it must be unique among all trap definition lines. So, make sure that each trap definition line in the file has a unique *View* field. It suffices just to vary the last number e.g. `1.2.4`, `1.2.5`, `1.2.6` and so on.

Edit /etc/snmpd.peers

Edit the **/etc/snmpd.peers** file and check that the line below has been added to the file (add it if necessary):

```
″rsf″   1.3.6.1.4.1.107.121.1   ″rsf_password″
```

If needed, refer to your AIX documentation for details on the **/etc/snmpd.peers** file.

Refresh the snmpd Daemon

If you have made changes to the **/etc/snmpd.conf** or **/etc/snmpd.peers** files, you must refresh the **snmpd** daemon by running the following command:

```
refresh –s snmpd
```

Setting Up ISM

This task consists in setting up the ISM software so that it knows about traps sent by *Extended RSF*. Only guidelines are given below: if needed, refer to your ISM documentation for details on the involved ISM files and commands.

Shutting Down ISM

ISM is composed of a framework and various modules. All of ISM must be shut down before doing the configuration. So, shut down ISM (if needed, refer to your ISM documentation for instructions).

Updating ISM Configuration Files

You must then edit ISM configuration files: **trap.confdb** and possibly **snmppa.confdb**. As a hint, note that these files may be located in the directory **$ISMROOT/var/db/SNMP_AI**, or in

/usr/lib/ISM, or perhaps elsewhere; their actual location depends on the ISM version you are using.

Adding Trap Definitions to trap.confdb

Edit **trap.confdb** and go to the end of the file. For each SNMP trap susceptible of being sent by *Extended RSF*, add a trap definition, using the following format:

```
TRAPDEF        <RSFTrap>
SEVERITY       <severity>
PBTYPE         PROC 4
GENERIC        6
SPECIFIC       <trapnum>
ASSOBJECT      Internet:snmpSystem
ENTERPRISE     1.3.6.1.4.1.107.121.1
TRAPEND
```

Where:

- `<RSFTrap>` is a unique identifier for the trap. For example, if you add three trap definitions, you may want to specify the names `RSFTrap1`, `RSFTrap2` and `RSFTrap3` for their respective `TRAPDEF` identifier.
- `<severity>` is a severity code ranging from `0` to `5`. Choose an appropriate code, that reflects the severity of the event that originates the trap. ISM relies on this code notably to decide how to present the trap (icon color...). Below is a summary of the possible severity codes:

Severity Code	Meaning
0	Indeterminate
1	Critical
2	Major
3	Minor
4	Warning
5	Clear

- It is usual, but not mandatory, to assign the `PROC 4` value to `PBTYPE`. The `PROC 4` value correspond to the **sfwrEnvironmental** problem type.
- Always assign the `6` value to `GENERIC`. This values means that the trap is “enterprise-specific”.
- `<trapnum>` is a specific trap number between 1 and 255. This number must match the **Trap Number** field you specify when defining a **Send SNMP Trap** action within *Extended RSF* (this field is discussed on page 2-7). Each trap you add must have a unique trap number.
- Always assign the `Internet:snmpSystem` value to `ASSOBJECT`.
- Always assign the `1.3.6.1.4.1.107.121.1` value to `ENTERPRISE`. This is the appropriate enterprise object identifier (OID) that identifies the RSF agent object responsible for SNMP handling. It is defined in the RSF Management Information Base (MIB).

Updating the NTRAPDEF Line in trap.confdb

Once you have added the desired trap definitions, go to the start of the **trap.confdb** file and edit the `NTRAPDEF` line. This line tells ISM how many trap definitions there are in the file. Increment this number for each trap definition you have added. This terminates the configuration of **trap.confdb** (you can quit the file).

Editing snmppa.confdb

Edit **snmppa.confdb** if necessary, to contain an entry for the trap action system (see your ISM documentation).

Where You Go From Here

Once you have set up ISM to define the traps, you can restart it. From now on, ISM is able to handle the traps emitted through the SNMP capability of *Extended RSF*.

If you have not already configured *Extended RSF* to send SNMP traps, refer to “Adding a ’Send SNMP Trap’ Action” on page 2-7. Create **Send SNMP Trap** actions as desired, and configure sources and associated messages that make use of these actions.

Hints for Troubleshooting asid

Generally, errors which come from **asid** or problems using **asid** result from configuration problems. The following is a discussion of some specific problems and how to solve them.

General Requirement

Make sure that the **asid** daemon is running by using the **Show RSF Status** option of the RSF menu. The **asid** daemon must be present in the list, with the **Up** status. If it is **Down**, start it using the **Start / Stop RSF** option of the RSF menu. If it is not present in the list, that means that the **rsf.extended.snmp** fileset (which notably includes **asid** and the RSF MIB) has not been installed: install it.

“asid: YouLoseBig” Error Message

This message, which comes from the SMUX API library, can appear on the console if the SMUX entries from **/etc/snmpd.conf** and **/etc/snmpd.peers** are not properly set up.

Edit these files then refresh the snmpd daemon, as explained in section “Setting Up the SNMP Environment”, starting on page B-2.

“asid: Warning: smux_init systemError join_tcp_server failed” Error Message

This message may appear if the **snmpd** daemon is not running. The **asid** daemon requires **snmpd** to be running in order to register and manage the RSF MIB. (Note that you may ignore this warning message if you do not plan to use the SNMP capability. It does not prevent RSF and *Extended RSF* from operating normally).

Make sure that **snmpd** is enabled as explained on page B-2. Once **snmpd** is started, **asid** is able to establish its association with it. **asid** retries once every minute, so it may take about one minute before the RSF MIB becomes accessible.

“asid: cannot send SNMP traps to network management stations” Error Message

If this message appears, first check the items mentioned above (i.e. **/etc/snmpd.conf**, **/etc/snmpd.peers**, **snmpd** daemon). One easy way to test if things are configured correctly is to run the following command on the local host:

```
snmpinfo –o /var/rsf/rsf.defs –m get –c system rsfdUptime.0
```

The output should look like:

```
1.3.6.1.4.1.107.121.2.4.1.1.0 = 20651
```

If a message like `No response` or `No such name at position 1` appears, then the configuration is probably incorrect. Edit again the **/etc/snmpd.conf** file to check that the SNMP “community” called “system” is configured as shown below:

```
community     system   127.0.0.1  255.255.0.0  readWrite  1.17.2
```

Remember that any changes to **/etc/snmpd.conf** do not take effect until you refresh **snmpd** using the **refresh –s snmpd** command.

Index

Vos remarques sur ce document / Technical publication remark form

Titre / Title : Bull Escala and Escala EPC Extended RSF Reference Manual

Nº Reférence / Reference Nº : 86 A2 14GX 01

Daté / Dated : June 1998

ERREURS DETECTEES / ERRORS IN PUBLICATION

AMELIORATIONS SUGGEREES / SUGGESTIONS FOR IMPROVEMENT TO PUBLICATION

Vos remarques et suggestions seront examinées attentivement.
Si vous désirez une réponse écrite, veuillez indiquer ci-après votre adresse postale complète.

Your comments will be promptly investigated by qualified technical personnel and action will be taken as required.
If you require a written reply, please furnish your complete mailing address below.

NOM / NAME : ______________________________ Date : ________

SOCIETE / COMPANY : ______________________________

ADRESSE / ADDRESS : ______________________________

____

Remettez cet imprimé à un responsable BULL ou envoyez-le directement à :

Please give this technical publication remark form to your BULL representative or mail to:

BULL ELECTRONICS EUROPE S.A.
Service CEDOC
331 Avenue PATTON – BP 428
49004 ANGERS CEDEX 01
FRANCE

Technical Publications Ordering Form

Bon de Commande de Documents Techniques

To order additional publications, please fill up a copy of this form and send it via mail to:
Pour commander des documents techniques, remplissez une copie de ce formulaire et envoyez-la à :

BULL ELECTRONICS EUROPE S.A.
Service CEDOC
ATTN / MME DUMOULIN
331 Avenue PATTON – BP 428
49004 ANGERS CEDEX 01
FRANCE

Managers / Gestionnaires :
Mrs. / Mme : **C. DUMOULIN** +33 (0) 2 41 73 76 65
Mr. / M : **L. CHERUBIN** +33 (0) 2 41 73 63 96

FAX : +33 (0) 2 41 73 60 19
E–Mail / Courrier Electronique : srv.Cedoc@franp.bull.fr

Or visit our web site at: / Ou visitez notre site web à:
`http://www–frec.bull.com` (PUBLICATIONS, Technical Literature, Ordering Form)

CEDOC Reference # N^o Référence CEDOC	**Qty** Qté	**CEDOC Reference #** Nº Référence CEDOC	**Qty** Qté	**CEDOC Reference #** Nº Référence CEDOC	**Qty** Qté
__ __ ____ _ [__]		__ __ ____ _ [__]		__ __ ____ _ [__]	
__ __ ____ _ [__]		__ __ ____ _ [__]		__ __ ____ _ [__]	
__ __ ____ _ [__]		__ __ ____ _ [__]		__ __ ____ _ [__]	
__ __ ____ _ [__]		__ __ ____ _ [__]		__ __ ____ _ [__]	
__ __ ____ _ [__]		__ __ ____ _ [__]		__ __ ____ _ [__]	
__ __ ____ _ [__]		__ __ ____ _ [__]		__ __ ____ _ [__]	
__ __ ____ _ [__]		__ __ ____ _ [__]		__ __ ____ _ [__]	
[_ _] : **no revision number means latest revision** / pas de numéro de révision signifie révision la plus récente					

NOM / NAME : ____________________ Date : __________

SOCIETE / COMPANY : ____________________

ADRESSE / ADDRESS : ____________________

____

PHONE / TELEPHONE : ____________________ FAX : ____________________

E–MAIL : ____________________

For Bull Subsidiaries / Pour les Filiales Bull :
Identification: ____________________

For Bull Affiliated Customers / Pour les Clients Affiliés Bull :
Customer Code / Code Client : ____________________

For Bull Internal Customers / Pour les Clients Internes Bull :
Budgetary Section / Section Budgétaire : ____________________

For Others / Pour les Autres :
Please ask your Bull representative. / Merci de demander à votre contact Bull.

PLACE BAR CODE IN LOWER
LEFT CORNER

BULL ELECTRONICS EUROPE S.A.
Service CEDOC
331 Avenue PATTON – BP 428
49004 ANGERS CEDEX 01
FRANCE

ORDER REFERENCE
86 A2 14GX 01

Bull

Utiliser les marques de découpe pour obtenir les étiquettes.
Use the cut marks to get the labels.

Escala and
Escala EPC

AIX

Extended RSF
Reference Manual

86 A2 14GX 01

Escala and
Escala EPC

AIX

Extended RSF
Reference Manual

86 A2 14GX 01

Escala and
Escala EPC

AIX

Extended RSF
Reference Manual

86 A2 14GX 01