

RSF (Remote Services Facilities)

User's Guide

AIX



REFERENCE
86 A2 95AQ 03

ESCALA

RSF (Remote Services Facilities)

User's Guide

AIX

Software

October 1999

BULL CEDOC
357 AVENUE PATTON
B.P.20845
49008 ANGERS CEDEX 01
FRANCE

REFERENCE
86 A2 95AQ 03

The following copyright notice protects this book under Copyright laws which prohibit such actions as, but not limited to, copying, distributing, modifying, and making derivative works.

Copyright © Bull SAS 1992, 1999

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.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries

The information in this document is subject to change without notice. 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 RSF (Remote Services Facilities) and performing associated administration tasks.

RSF is a software package dedicated to system error monitoring and remote maintenance operations. It provides a link between your system and the Bull Customer Service Center.

Who Should Use This Book

This book is intended for the system administrator responsible for managing a system that is monitored through the RSF product.

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, “Introduction to RSF,”** explains what RSF is and summarizes its features and operating principles.
- **Chapter 2, “Getting Started with RSF,”** provides basic information and instructions for getting started (installation concerns, accessing RSF functions through SMIT, and RSF functions usage).
- **Chapter 3, “RSF Management,”** explains how to start or stop RSF and how to view its current status.
- **Chapter 4, “Remote Session and Security Management,”** explains how to manage remote sessions and security features (authorizations, callback feature, remote session mirroring, recording and reviewing). As the administrator of the monitored system, management of remote sessions and security is the main point you will have to deal with.
- **Chapter 5, “Dial Out Management,”** explains how to enable or disable alarm messages transmission and how to view the dial out log file.

Ordering Publications

To order additional copies of this book, use Order Number 86 A2 95AQ.

Contents

Chapter 1. Introduction to RSF	1-1
What is RSF?	1-1
RSF: Remote Services Facilities	1-1
Installation Requirements	1-1
RSF's Main Functions	1-1
Benefits of RSF	1-2
Security Features	1-2
Operating Principles	1-2
Operation Outlines	1-2
Error Monitoring and Alarm Transmission	1-3
RSF Daemons	1-3
Error Monitoring	1-3
Alarm Transmission	1-3
Error Count and Alarm Threshold	1-3
Error Count Reset	1-3
Security and Management of Remote Service Sessions	1-3
The "remote" User Account	1-3
Remote Session and Security Management Overview	1-4
Transmission Link / Cluster Configuration	1-4
Chapter 2. Getting Started With RSF	2-1
Installation and Configuration Concerns	2-1
Accessing RSF Functions	2-2
Preliminary Remarks	2-2
Using SMIT	2-2
SMIT Fast Paths	2-2
SMIT Interface	2-2
You Must Be root	2-2
Accessing the RSF Main Menu	2-2
RSF Functions Usage	2-3
Chapter 3. RSF Management	3-1
Starting and Stopping RSF	3-1
Understanding Start/Stop RSF Usage	3-1
Automatic RSF Startup	3-1
Clearing the AIX Error Log File Before Restarting RSF	3-1
Procedure for Starting or Stopping RSF	3-1
Viewing RSF Status	3-2
Procedure for Viewing RSF Status	3-2
Understanding the Status Information	3-3
RSF Status	3-3
Action on Alarm	3-3
Dial Out Status	3-3
Remote Status	3-3

Chapter 4. Remote Session and Security Management	4-1
Security Features and Remote Session Management	4-1
Choosing a Security Scheme	4-1
Remote Connection Control	4-1
“remote” User Access Control	4-2
Remote Session Control	4-2
Accessing Remote Session and Security Management Functions	4-3
Managing Remote Connection Security	4-3
Understanding the “Remote Authorisation” and “Callback” Security Features ..	4-3
Scenarios for Connection Control	4-4
Scenario 1: Direct Connections Authorized	4-4
Scenario 2: Automatic Callback	4-4
Scenario 3: Manual Callback	4-5
Scenario 4: Any Connection Forbidden	4-5
Note on RSF “Cluster Configurations”	4-5
Setting Remote Access Authorization	4-5
Setting Up the Callback Mode	4-6
Managing Phone Numbers	4-6
Managing the Account for the “remote” User	4-7
Changing the Password for the “remote” User	4-7
Prior Knowledge	4-7
Procedure	4-8
Allowing or Disallowing Root Access for the “remote” User	4-8
Allowing or Disallowing PPP Protocol	4-8
Using the Manual Callback Feature: Call Remote Service Center	4-9
Remote Session Mirroring: Supervising a Remote Session	4-10
Initiating the Remote Session Mirroring Feature	4-10
What Happens When Initiating the Remote Session Mirroring Feature	4-10
Possible Actions During Remote Session Mirroring	4-10
Managing Remote Session Recording	4-11
Recording Remote Sessions	4-11
Reviewing Recorded Sessions	4-11
Removing a Recorded Session	4-12
Chapter 5. Dial Out Management	5-1
Dial Out Management With RSF (Remote Services Facilities)	5-1
Accessing Dial Out Management Functions	5-1
Functions Usage	5-1
Enabling and Disabling Alarm Messages Transmission	5-2
Procedure	5-2
Viewing the Current Dial Out Status	5-2
Listing Information Related to Alarm Messages Transmission	5-3
Procedure	5-3
Understanding the Dial Out Log	5-3

Chapter 1. Introduction to RSF

This chapter, which provides an overview of RSF, includes the following sections:

- What is RSF?
- Operating Principles

What is RSF?

RSF: Remote Services Facilities

RSF, which stands for *Remote Services Facilities*, is a software package dedicated to system error monitoring and remote maintenance operations. It provides a link between your system and the Bull Customer Service Center.

RSF is designed as an integrated SMIT (System Management Interface Tool) application.

A Note on “Extended RSF”

Extended RSF is a separate, optional, software package that allows monitoring of any ASCII log file. When specific messages occur in the monitored files, *Extended RSF* execute specific, user-configurable, actions.

For additional information, refer to the *Extended RSF User's Guide*, Order Number 86 A7 14GX.

Installation Requirements

RSF is available on ESCALA systems running the AIX operating system. It is delivered to customers who have an appropriate maintenance contract.

RSF should have been installed and configured by your Bull service representative. RSF installation requirements follow:

- A phone line, usually provided by the customer, is required.
- The modem is installed under the control of your service representative. On most models, this is an external modem connected to the S2 TTY line of the system. However, on some Escala models (including the EPC400, T and E series), an internal modem (working through the S4 TTY line) may be used instead of an external modem.
- Once RSF is installed, you should consider that the TTY line as well as the modem are dedicated to remote maintenance. You must not modify their configuration.
- RSF needs 6 MBytes of disk space and uses at the most 1 MByte of RAM.

RSF's Main Functions

RSF handles two main functions: (1) error monitoring and alarm transmission, and (2) management of remote service sessions.

Error Monitoring and Alarm Transmission

RSF scans periodically the AIX error log file for the occurrence of new errors, so that it can detect actual and pending failures.

When RSF identifies relevant errors, it notifies them to the Bull Customer Service Center, by sending alarm messages using a phone line and a modem.

Management of Remote Service Sessions

When the service center receives an alarm message from RSF, a technical expert of the service center may initiate a remote service session for problem diagnosis and possible correction.

For security concerns, RSF provides you with remote session and security management functions (see below).

Benefits of RSF

RSF brings better diagnostic and faster repair for actual failures, as well as notification for pending failures. Generally speaking, RSF enhances the availability of the monitored system. Note the following benefits:

- Notifications of actual and pending failures are done automatically, without an explicit customer intervention. These notifications allow the service center to carry out not only corrective actions, but also preventive ones.
- Significant data concerning failures is automatically collected and included within the alarm messages that are sent to the service center. In this way, data available to the Service Center is always accurate.
- With RSF the service center can handle remote sessions in character mode, but also in graphic mode through a PPP (Point-to-Point Protocol) connection; this feature allows the service center to run graphic applications, such as WebSM.

Security Features

RSF provides security features to protect the monitored system from unauthorized access, and to give you control over the actions of remote service personnel.

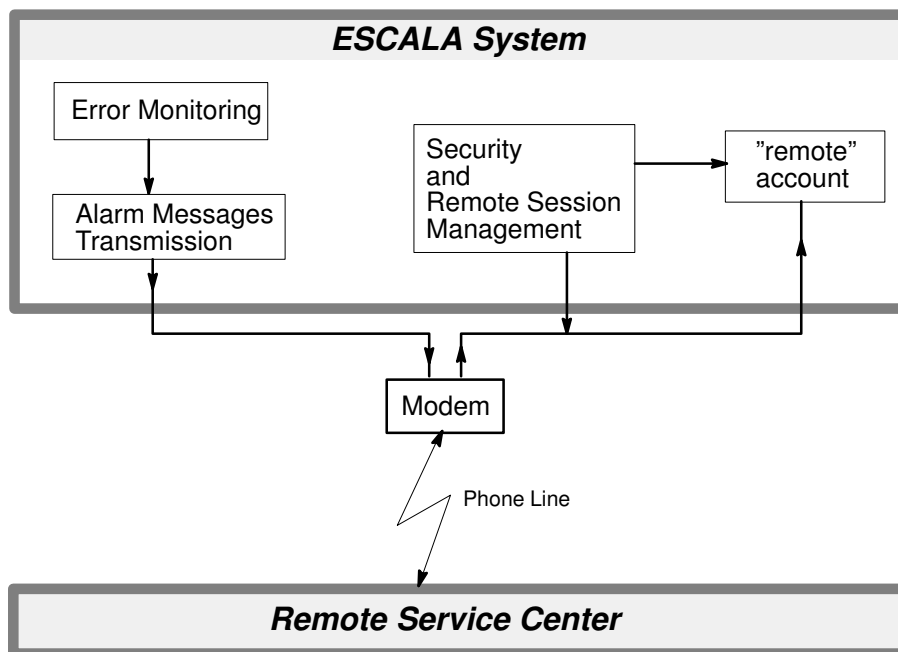
RSF respects your security policy. You may choose to let the service center intervene alone, or to fully control the course of remote service sessions.

For further information, refer to *Security and Management of Remote Service Sessions*, on page 1-3.

Operating Principles

Operation Outlines

The following figure outlines RSF operating principles.



Error Monitoring and Alarm Transmission

RSF Daemons

Error monitoring and alarm transmission functions are handled through a set of daemons that run on the monitored system. We will refer to them as the “RSF daemons”.

Error Monitoring

RSF scans periodically the AIX error log file (usually `/usr/adm/ras/errlog`) for the occurrence of new errors.

- Among the logged errors, RSF takes into account only those that relate to the basic system (including the operating system and the hardware). RSF ignores errors possibly logged by specific applications.
- In accordance with its current configuration, RSF will only take into account errors that fall in one of these three categories: “HARD”, “SOFT”, and “HARD & SOFT”. RSF will discard all errors that do not pertain to the category RSF has been set up for.

Note: The configuration of RSF has been set up by your service representative.

Alarm Transmission

Once RSF has detected a relevant error, it has to decide what action to perform.

Error Count and Alarm Threshold

First, RSF updates the error count for this error; then:

- If the error count reaches a preset threshold value, RSF sends an alarm message to the service center.
- Otherwise (i.e. if the error count does not reach the threshold value, or already exceeds it), RSF performs no further action.

The preset threshold value depends on the error type. For permanent actual errors, the threshold is 0, while for temporary–recovered errors, this is usually two for a 1–day period. (Actually, this last threshold value may vary, depending on the current RSF configuration that has been set up at your site.) In other words, the more severe errors are notified the first time they occur, while the less severe ones are notified when they occur for the third time within a 1–day period.

Once an alarm message has been transmitted, there will be no more alarms transmitted for the same error code until someone resets the error count for this error code. This avoids continually repeated alarms for the same error.

Error Count Reset

Typically, the error count is reset by the remote service personnel, after having resolved the problem. This re–enables the transmission of errors that had previously reached an over–threshold condition (and thus, that were not transmitted anymore).

Security and Management of Remote Service Sessions

The “remote” User Account

When the service center has received an alarm message from RSF, the remote service personnel may initiate a remote service session for problem diagnosis and possible correction.

Practically, “remote service session” means that the remote service personnel logs in to your system as the “remote” user. The “remote” account is created on your system at RSF installation time, specifically for this purpose.

Remote Session and Security Management Overview

For security concerns, RSF provides you with remote session and security management functions. These functions are summarized below. For details, refer to Chapter *Remote Session and Security Management*, starting on page 4-1.

Access Control Features

- You can control the way remote connections are established. You can choose to authorize remote connections through incoming calls. Or, for enhanced security, you may prefer to enable the callback security feature.

When the callback feature is enabled, incoming calls are intercepted, and the caller cannot log in to the system. In that case, it is up to the monitored system to call the remote service center back, through the modem and using a trusted phone number, so that the remote service personnel can in turn log in to the system. Manual and automatic callback modes are available.

- You can grant or deny access authorization to the “remote” user, i.e. to the remote service personnel.
- The “remote” account is password protected. In addition, you may grant or deny root access to the “remote” user.

Remote Session Control Features

- You are notified with both a message on the console and e-mail when someone is logging in (or logging out) via the “remote” account.
- Through the session mirroring feature, you have control over what is happening during the remote session. You can view all operations performed and also participate in the session itself (you can even abruptly end the session in progress.)
- You can record remote sessions for later review.

Transmission Link / Cluster Configuration

Transmission Link

RSF uses only one transmission link, that serves both for sending alarm messages to the service center and for handling remote sessions initiated from the service center. Communications take place through a modem connected to a phone line.

Cluster Configuration

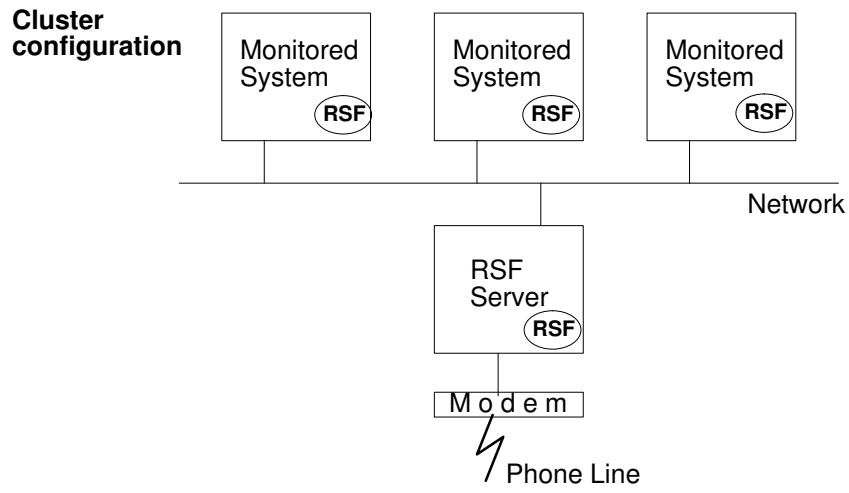
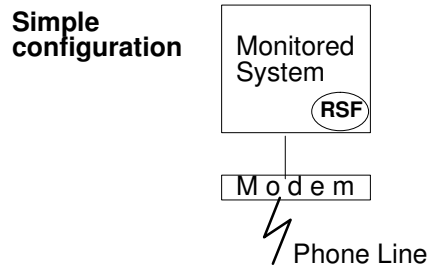
If your site includes several networked systems to be monitored by RSF, your service representative may have chosen to implement a “cluster configuration” (see illustration).

In this case, one of the systems acts as an RSF server:

- It handles alarms that come from RSF client systems and sends them to the service center.
- Conversely, it handles communications that come from the service center: the remote service personnel first logs in to the RSF server, then connects to the appropriate host through **rlogin**.

Only one modem is used, connected to the RSF server.

Note: In a cluster configuration, the system that acts as the RSF server is also monitored by RSF.



Chapter 2. Getting Started With RSF

This chapter includes the following sections:

- Installation and Configuration Concerns
- Accessing RSF Functions
- RSF Functions Usage

Installation and Configuration Concerns

Your service representative is responsible for installing, configuring and checking RSF. Consequently, you do not have to deal with these preliminary operations.

However, as the system administrator, you may want to know what files and processes are affected. Note the following information:

/etc/inittab and RSF daemons

The installation phase updates the **/etc/inittab** file so that RSF daemons are automatically started whenever the system starts up. The RSF daemons, namely **rsfd**, **calld**, **bmapd** and **acterd**, handle error monitoring and alarm transmission.

Note: Another daemon, **asid**, which may be implemented, relates to the SNMP package of the *Extended RSF* software. This daemon is not required for RSF operation.

/etc/services The installation phase adds two specific entries to the **/etc/services** file. These entries relate to the **bmapd** RSF daemon.

“remote” account

The installation phase creates an account for the “remote” user. It will be used by the remote service personnel to log in remotely to your system, in case an intervention is needed.

Data and executable files

RSF uses various data and executable files that are installed in several directories. To know what files are installed on your system, type at the AIX prompt:

```
lslpp -f 'rsf*'
```

IP Configuration

If the service representative needs to run graphical applications, such as WebSM, on his remote station, he will configure the RSF server as a PPP server.

By default RSF gives the IP address **101.99.99.1** to the server and **101.99.99.2** to the remote station. These addresses are dedicated to test, and thus will not disturb the other IP addresses.

In a cluster configuration the service representative may add IP routes to reach the graphic applications running on monitored systems.

Accessing RSF Functions

Preliminary Remarks

Using SMIT

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

SMIT Fast Paths

All RSF functions may be accessed either from the top level SMIT menu, or directly from the command line, bypassing the upper-level menus. In the last case, you must specify to SMIT the corresponding fast path (appropriate fast paths are indicated throughout this book). For example, to go directly to the **Remote Session Management** menu of RSF, type at the AIX prompt:

```
smit servenv
```

SMIT Interface

The SMIT facility can run in two interfaces: either ASCII (nongraphical) or AIXwindows (graphical). Using one or the other makes no difference. Note that by convention, all illustrations in this book correspond to the AIXwindows SMIT interface.

You Must Be root

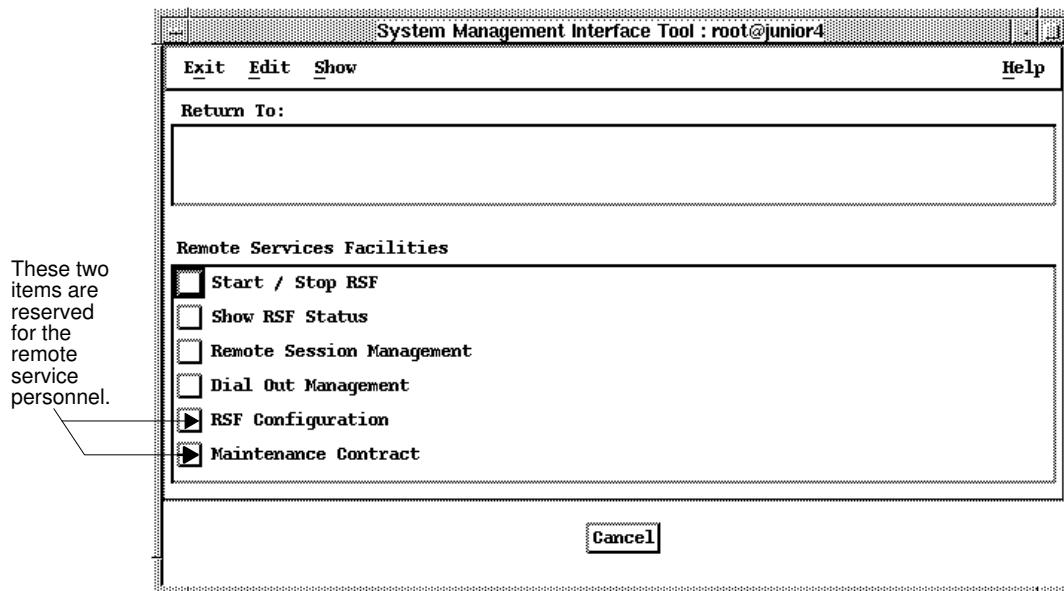
You must be logged in as root each time you access RSF functions from the SMIT main menu or using SMIT fast paths.

Accessing the RSF Main Menu

Fast Path: `smit rsf`

To access the RSF main menu:

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



RSF Functions Usage

Note: As indicated below, some RSF features are intended for the remote service personnel and thus are not described in this book.

The RSF main menu includes the following options:

Start / Stop RSF

To start or stop the RSF daemons. In practice, it is never or rarely needed.
For details, see Chapter *RSF Management*, starting on page 3-1 .

Show RSF Status

To view the status of RSF daemons and other RSF–related information.
For details, see Chapter *RSF Management* , starting on page 3-1.

Remote Session Management

To manage security and remote service sessions. As the administrator of the monitored system, **these will be the main points you will have to deal with.**
For details, see Chapter *Remote Session and Security Management*, starting on page 4-1.

Dial Out Management

To enable or disable modem alarm messages transmission, and to view logged information related to alarm message transmission.
For details, see Chapter *Dial Out Management*, starting on page 5-1.

RSF Configuration and Maintenance Contract

These two options are intended for the remote service personnel and **are not documented.** You should not use them.

Chapter 3. RSF Management

This chapter includes the following sections:

- Starting and Stopping RSF
- Viewing RSF Status

Starting and Stopping RSF

Understanding Start/Stop RSF Usage

Usually, starting RSF will be done only once by your service representative, at installation time. In practice, it is likely that you will never have to stop and restart RSF.

Note: If you are experimenting special software or hardware on your system, you should disable the **Dial Out Authorisation** (cf. page 5-2) in order to prevent errors generated by this experimentation to be transmitted to the service center. This method is better than the one which consists in stopping RSF.

Automatic RSF Startup

At installation time, RSF is configured so that RSF daemons start automatically at boot time. If you stop RSF for some reason, it will not start again at boot time until explicitly started. Starting RSF also configures RSF to automatically restart at boot time thereafter.

Notes:

- The RSF daemons are **rsfd**, **calld**, **bmapd** and **acterd** (another daemon, **asid**, which may be implemented, relates to the SNMP package of the *Extended RSF* software; this daemon is not required for RSF operation).
- Starting or stopping RSF modifies the entries for the RSF daemons in **/etc/inittab** (their action part are accordingly set to **wait** or **off**) in order to enable or disable automatic daemons startup at boot time.

Clearing the AIX Error Log File Before Restarting RSF

When you restart RSF, it scans the AIX error log file for errors that occurred after RSF was stopped but not older than 7 days. If you think that the error log includes errors that are not relevant (due, for example, to some system experimentation you have carried out), it is advisable to clear the error log in order to prevent RSF from transmitting non-relevant alarms.

To clear the error log, execute the following command (from the shell, being root):

```
errclear 0
```

Procedure for Starting or Stopping RSF

Note: Before starting or stopping the RSF daemons, you may want to view their status: refer to section *Viewing RSF Status* below.

Fast Path: **smit rsf_run**

To start or stop the RSF daemons:

1. Log in as **root**, and go to the RSF main menu by typing **smit rsf**.
2. Choose **Start / Stop RSF**: a new screen appears. The displayed message indicates if RSF is currently running or down, and accordingly prompts you either to stop or to start RSF.
3. Choose **Do** to perform the task or **Cancel** to abandon.

Viewing RSF Status

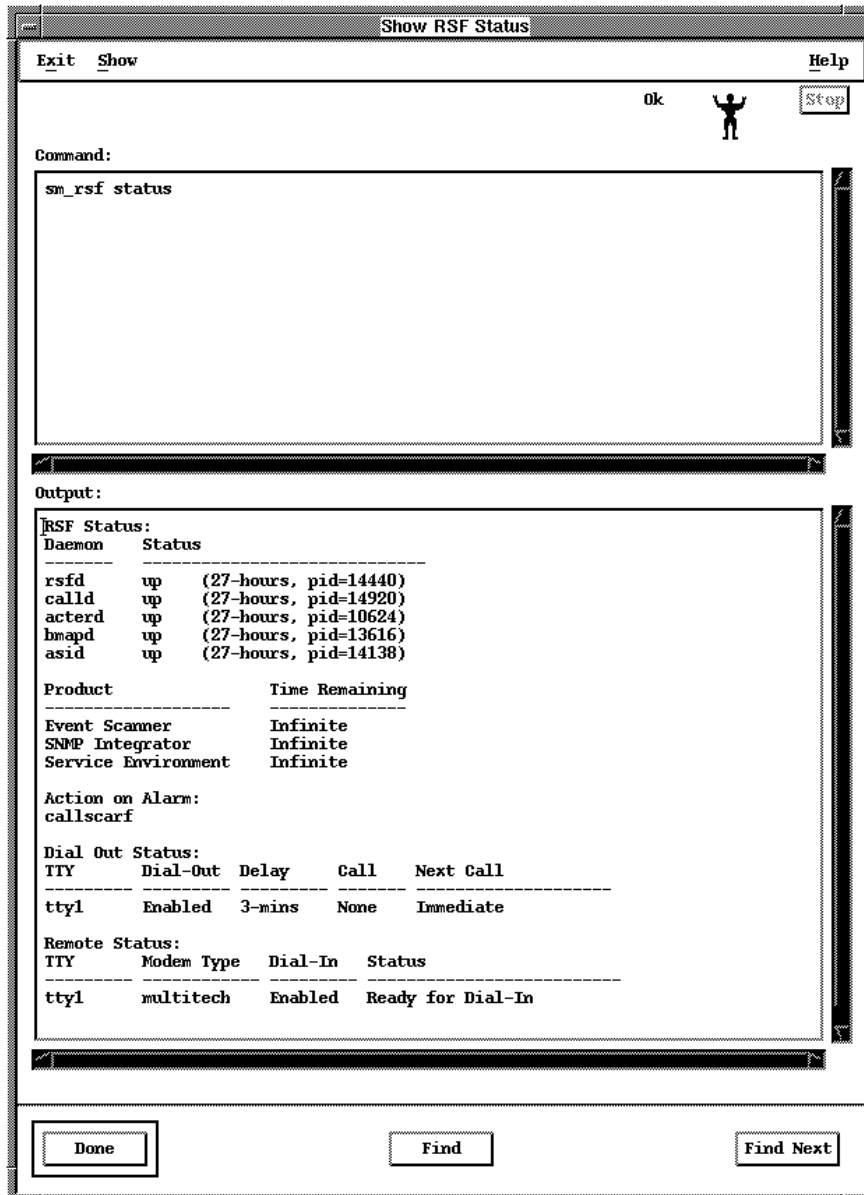
Once RSF is installed and started, it works without any human intervention. However, you may want to know the status of the different RSF components.

Procedure for Viewing RSF Status

Fast Path: `smit rsfstat`

To view the status of RSF:

1. Log in as **root**, and go to the RSF main menu by typing `smit rsf`.
2. Choose **Show RSF Status** to display information about RSF status (see illustration).



Understanding the Status Information

The displayed status information is organized into four sections: **RSF Status**, **Action on Alarm**, **Dial Out Status** and **Remote Status**. These four sections are described below.

RSF Status

This section includes two areas: **Daemon / Status** and **Product / Time Remaining**.

Daemon / Status

This area indicates the status of the four RSF daemons, which may be either **up** or **down**. If the status is **up**, then how long the daemon has been up and the process ID of the daemon are also displayed.

If RSF is running, the four RSF daemons (**rsfd**, **calld**, **acterd** and **bmapd**) should be **up**.

Note: The **asid** daemon, which can also appear in the list, relates to the SNMP package of the *Extended RSF* software. This daemon is not required for RSF operation.

Product / Time Remaining

This section indicates the remaining time before your RSF license expires; it depends on your maintenance contract.

- RSF is made up of two products, namely *Event Scanner* and *Service Environment*, hence the two distinct lines displayed corresponding to these two products.
- In addition, the *SNMP Integrator* product is also mentioned when the SNMP package of the *Extended RSF* software is installed. This product is not required for RSF operation.

Action on Alarm

This section indicates which is the action type which is currently in effect: **cluster**, **callscarf** or **callrcs2**. This information is intended for the remote service personnel.

Dial Out Status

This section gives information about dial-out, i.e. alarm messages transmission to the service center.

Note: If the current **Action on Alarm** is **cluster**, the **Dial Out Status** section indicates only if dial-out is Enabled or Disabled. The information below applies only to **callscarf** and **callrcs2** action types.

TTY	The tty port to which the modem is attached (usually <i>tty1</i>).
Dial-Out	Either <i>Enabled</i> or <i>Disabled</i> . <i>Enabled</i> means that outgoing calls are allowed, thus RSF is able to transmit alarm messages to the remote service center. Refer to Chapter 5, <i>Dial Out Management</i> , for related information.
Delay	Time delay before beginning to process the next outgoing call to the remote service center.
Call	If an outgoing call is being processed, shows which call it is; otherwise, displays the none indication.
Next Call	Shows when the next callout is due to be processed (taking into account the call Delay).

Remote Status

This section gives information about dial-in, i.e. connections initiated by the service center personnel.

Note: If the current **Action on Alarm** is **cluster**, the **Remote Status** section indicates only if dial-in is Enabled or Disabled. The information below applies only to **callscarf** and **callrcs2** action types.

TTY	The tty port to which the modem is attached (usually <i>tty1</i>).
------------	---

Modem Type	The type of the modem (for example, <i>multitech</i> , <i>cardinal</i> and <i>scout</i>).
Dial-In	Either <i>Enabled</i> or <i>Disabled</i> . <i>Enabled</i> means that incoming calls are allowed, thus the remote service personnel is able to initiate a remote service session. Refer to <i>Setting Remote Access Authorization</i> , on page 4-5, for related information.
Status	The current status of the modem. Among possible status are: Ready for Dial-In: Normal status if dial-in is enabled. Disabled: Normal status if dial-in is disabled. Disabled for Callout: RSF is using the modem for alarm message transmission. In Use (Local): Modem is in use by some local application (such as cu or ate) that is not RSF-related. Someone is Connected: Someone is currently connected through the modem (not necessarily as the “remote” user). Cannot Detect Modem: The modem has been turned off, or there is a problem with the cables used to attach the modem to the system.

Chapter 4. Remote Session and Security Management

This chapter includes the following sections:

- Security Features and Remote Session Management
- Accessing Remote Session and Security Management Functions
- Managing Remote Connection Security (Callback and Remote Authorization)
- Managing the Account for the “remote” User
- Using the Manual Callback Feature (“Call Remote Service Center”)
- Remote Session Mirroring: Supervising a Remote Session
- Managing Remote Session Recording

Security Features and Remote Session Management

Choosing a Security Scheme

As the administrator of the monitored system, remote session and security management is the main point you will have to deal with. However, using these features is optional. So, regarding remote session management, there are two main policies:

- If your security-related constraints are not too strong, you may decide to let the remote service personnel intervene without authorization or supervision. In this case, you will have little to worry about, and you can almost forget that RSF is running on your system.
- On the other hand, if you have security-related requirements regarding the course of the remote sessions, you can take advantage of RSF’s remote session and security management functions. These functions, summarized below, fall into three categories:
 - Remote Connection Control
 - “remote” User Access Control
 - Remote Session Control

Remote Connection Control

To protect the system from unauthorized dial-in access, you can control the way remote connections are established:

- You can enable or disable **remote access authorization**, i.e. you can authorize or reject incoming calls.
- For enhanced security and flexibility, you may enable the **callback security feature**. The callback feature enhances security by providing control over the location of a connection’s remote side.

When the callback feature is enabled, incoming calls are intercepted, and the caller cannot log in to the system. In that case, it is up to the monitored system to call the remote service center back, through the modem and using a trusted phone number, so that the remote service personnel can in turn log in to the system. Manual and automatic callback modes are available.

For further information, refer to *Managing Remote Connection Security*, on page 4-3.

“remote” User Access Control

Further protection is achieved through the following features:

- The “remote” account is password protected.
- You may grant or deny root access to the “remote” user.

For details, refer to *Managing the Account for the “remote” User*, on page 4-7.

Remote Session Control

RSF provides features that let you control the progress of remote sessions (before, during, and after they occur).

Remote Login/Logout Notification

You are notified with both a message on the console and e-mail when someone is logging in or logging out via the “remote” account.

Remote Session Mirroring

Through the session mirroring feature, you have control over what is happening during the remote session. You can view all operations performed and also participate in the session itself. You can even abruptly end the session in progress.

Note: You can mirror only the remote sessions that are handled in character mode. The remote sessions through a PPP connection to graphical applications – typically WebSM – cannot be mirrored.

For details, refer to *Remote Session Mirroring: Supervising a Remote Session*, on page 4-10.

Remote Session Recording and Playback

You can record remote sessions for later review.

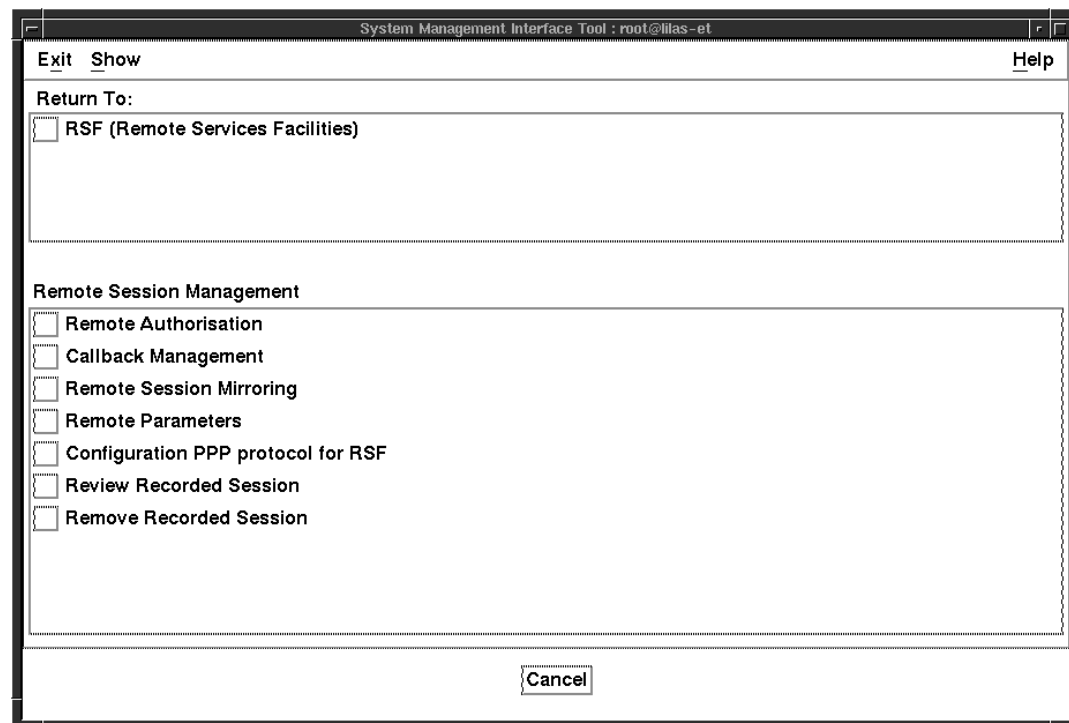
For details, refer to *Managing Remote Session Recording*, on page 4-11.

Accessing Remote Session and Security Management Functions

Fast Path: `smit servenv`

To access remote session and security management functions, go to the **Remote Session Management** menu:

1. Log in as **root**, and go to the RSF main menu by typing `smit rsf`.
2. Choose **Remote Session Management**. The corresponding menu is displayed (see illustration).



Remote Session Management

Managing Remote Connection Security

This section explains how to implement your security policy for handling remote connections. This topic relates to the **Remote Authorisation** and **Callback Management** RSF menus.

Understanding the “Remote Authorisation” and “Callback” Security Features

The way incoming calls are handled depends on the **Remote Authorisation** and the **Callback Mode** RSF parameters.

- The **Remote Authorisation** specifies whether incoming calls are authorized or rejected.
- The **Callback Mode** specifies the desired callback mode, which may be **disabled**, **manual** or **automatic**. The callback feature (either manual or automatic) enhances security by providing control over the location of connection’s remote side. When it is enabled, the caller cannot log in to the system. In that case, it is up to the monitored system to call the remote service center back, through the modem and using a trusted phone number, so that the remote service personnel can in turn log in to the system.

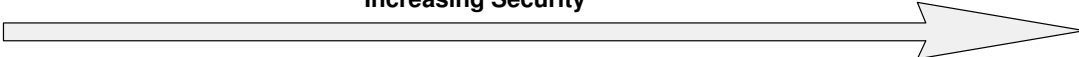
These two related parameters offer the means to protect the system from unauthorized

dial-in access. You must ensure they are set in accordance with your security policy. The possible settings, together with their corresponding behavior, are summarized in the 4 scenarios below.

Scenarios for Connection Control

- First, determine which of the four scenarios discussed below matches your security policy.
- Then set the **Remote Authorisation** and **Callback Mode** RSF parameters accordingly, as explained in *Setting Remote Access Authorization*, on page 4-5, and in *Setting Up the Callback Mode*, on page 4-6.

The following table summarizes the four possible scenarios, which are discussed below.

Increasing Security 

	Scenario 1: direct connections authorized	Scenario 2: automatic callback	Scenario 3: manual callback	Scenario 4: any connection forbidden
Remote Authorisation parameter:	enabled	enabled	disabled	disabled
Callback Mode parameter:	disabled	automatic	manual	disabled

Scenario 1: Direct Connections Authorized

Remote Authorisation: **enabled**
Callback Mode: **disabled**

Note: This configuration is mandatory to set up a PPP connection between the customer site and the service center.

Since **Remote Authorisation** is **enabled**, incoming calls and remote login are authorized. And since **Callback Mode** is **disabled**, connections initiated by the remote side are authorized (whether or not they actually come from the service center).

The remote caller, once connected, sees the AIX login banner and thus, has the opportunity to log in to the system. Anyone knowing a valid user name and its corresponding password can log in (the remote service personnel use the “remote” account to log in to the system).

Scenario 2: Automatic Callback

Remote Authorisation: **enabled**
Callback Mode: **automatic**

Note: Setting the **Callback Mode** to **automatic** automatically sets the **Remote Authorisation** to the **enabled** value.

Note: This configuration does not allow to set up a PPP connection between the customer site and the service center.

Here, the **Remote Authorisation** is **enabled**, but since the **Callback Mode** is set to **automatic**, incoming calls are intercepted. Indeed, the remote caller has not the opportunity to log in to the system, but is prompted to enter a phone number to call back. Then:

- If the entered number matches one of the predefined (trusted) phone numbers, RSF hangs up the communication and automatically calls this number back to establish a connection with the remote service center. The personnel at the remote service center then see the AIX login banner and can log in to the system (using the “remote” account).
- If the entered number does not match any predefined phone number, RSF simply hangs up the communication.

Scenario 3: Manual Callback

Remote Authorisation: disabled
Callback Mode: manual

Note: Setting the **Callback Mode** to **manual** automatically sets the **Remote Authorisation** to the **disabled** value.

Note: This configuration does not allow to set up a PPP connection between the customer site and the service center.

Since **Remote Authorisation** is **disabled**, any incoming call is rejected. And since **Callback Mode** is **manual**, calling the remote service center requires manual intervention.

When the remote service personnel want to connect to the system, they must phone to an operator at your site and request a manual callback to the remote service center using the **Call Remote Service Center** menu (discussed on page 4-9). When this is done, the personnel at the remote service center see the AIX login banner and can log in to the system (using the “remote” account).

Scenario 4: Any Connection Forbidden

Remote Authorisation: disabled
Callback Mode: disabled

As in scenario 3, **Remote Authorisation** is **disabled**, and thus, any incoming call is rejected. But here, because the **Callback Mode** is set to **disabled**, the **Call Remote Service Center** manual function is inoperative, and you cannot dial a phone number to connect to the remote service center. Thus, remote connections cannot take place, whether initiated locally or remotely.

This scenario is rarely implemented. If, however, it is chosen, then when the remote service personnel want to connect to the system, they must phone to an operator at your site and request him to temporarily change the **Remote Authorisation** and/or the **Callback Mode** settings so that a connection can be initiated.

Note on RSF “Cluster Configurations”

In an RSF “cluster configuration”, several systems are monitored by RSF, but only one of them, referred as the “RSF server”, is equipped with a modem (see page 1-4). All communications occur through the modem of the RSF server.

Important:

Keep in mind that functions of the **Callback Management** menu (**Callback Mode** setting, **Call Remote Service Center** function, management of phone numbers used for the callback feature) must be performed from the RSF server (i.e. from the system that is equipped with a modem).

If you perform these operations from another system (from an RSF client not equipped with a modem), the settings will have no effect.

Setting Remote Access Authorization

The **Remote Authorisation** specifies whether incoming calls and remote logins are authorized or rejected (for a discussion, refer to *Understanding the “Remote Authorisation” and “Callback” Security Features* above).

Fast Path: smit rauth

To change the **Remote Authorisation** setting:

1. Note that as long as the **Callback Mode** is set to **manual** or **automatic**, you cannot change the **Remote Authorisation**. In other words, you can change the **Remote Authorisation** only if the **Callback Mode** is currently **disabled**.
2. From the **Remote Session Management** RSF menu, choose **Remote Session Management**, then **Remote Authorisation**: a new screen appears. The displayed

message indicates if remote authorization is currently enabled or disabled, and accordingly prompts you either to disable or to enable it.

3. Choose **Do** to perform the task or **Cancel** to abandon.

Note: You may want to know that the RSF **Remote Authorisation** menu actually modifies the “Remote Authorization” flag, which is also used by SSF (*System Service Facility*). SSF concerns only the ESCALA M, D, R and EPC800 systems. It is a collection of firmware programs which run on the BUMP (*Bring-Up MicroProcessor*) and allow an operator to perform system maintenance functions.

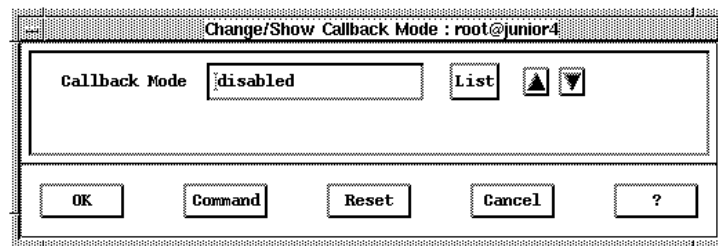
Setting Up the Callback Mode

The **Callback Mode** specifies the desired callback mode, which may be **disabled**, **manual** or **automatic** (for a discussion, refer to *Understanding the “Remote Authorisation” and “Callback” Security Features* above).

Fast Path: `smit callbackmode`

To change the **Callback Mode**:

1. **Make sure you are logged in to the RSF server** (i.e. to the system which is equipped with a modem). The *Note on RSF Cluster Configurations*, on page 4-5, explains why this is needed.
2. From the **Remote Session Management** RSF menu, select **Callback Management**, then **Change/Show Callback Mode**: a new screen appears that prompts you to enter the desired **Callback Mode**.



Change/Show Callback Mode

3. In accordance with your requirements (see *Scenarios for Connection Control* starting on page 4-4), select **disabled**, **manual**, or **automatic**, then validate the screen to apply the setting. Note that:
 - Setting the **Callback Mode** to **automatic** automatically sets the **Remote Authorisation** to the **enabled** value.
 - Similarly, setting the **Callback Mode** to **manual** automatically sets the **Remote Authorisation** to the **disabled** value.
4. If you have chosen either **manual** or **automatic**, make sure that at least one phone number, used for calling the remote service center back, is defined. Refer to *Managing Phone Numbers* below.

Managing Phone Numbers

RSF maintains a list of phone numbers that are used to call the remote service center when the (manual or automatic) callback feature is enabled.

- When the callback mode is automatic, incoming calls are intercepted, and the remote caller is prompted to enter a phone number to call back. The entered number is checked against the phone number list, which is supposed to include trusted phone numbers.
- When the callback mode is manual, you must manually call the remote service center using the **Call Remote Service Center** menu (discussed on page 4-9). From this menu,

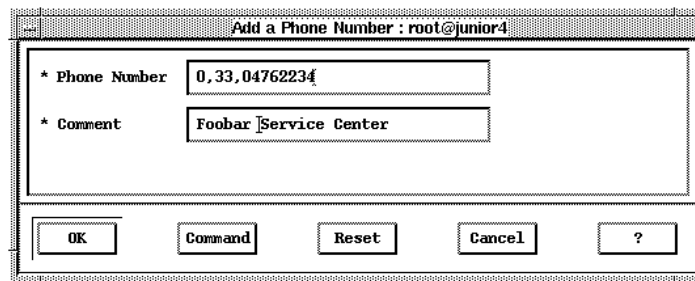
you can display the list of phone numbers, and thus, easily pick up the appropriate number to dial.

The phone number list is usually set up at RSF configuration time by your service representative. It typically includes a single phone number, suitable to connect to your Remote Service Center.

To access functions for managing phone numbers:

1. **Make sure you are logged in to the RSF server** (i.e. to the system which is equipped with a modem). The *Note on RSF Cluster Configurations*, on page 4-5, explains why this is needed.
2. From the **Remote Session Management** menu, select **Callback Management**.
3. Use the menu options for adding, changing/showing and removing phone numbers used by the callback feature.

As an example, the figure below shows the **Add a Phone Number** menu:



Add a Phone Number

The **Add a Phone Number** menu includes two fields, **Phone Number** and **Comment**. In the **Comment** field, enter a short descriptive text (serves as a reminder).

Specifying a Phone Number

When filling the **Phone Number** field, have in mind the following:

- The number may be optionally interspersed with special characters that the modem understands. As a typical example, note that many modems interpret the “,” (comma) as meaning “wait a short delay before issuing the next digit”. For example, you could specify a string such as “33,04762234” so that the modem, after it has issued “33”, waits a short delay before proceeding with the other digits.
- If applicable (depending on the telephone system in use at your site), do not forget to prefix the service center’s phone number with any digit which may be required to issue an outgoing call from your site.

Managing the Account for the “remote” User

Changing the Password for the “remote” User

The initial configuration set up by your service representative works as it is, so you do not have to worry about password setting for the “remote” user. However, if you have strong requirements concerning security, you may want to change the password for the “remote” user.

Prior Knowledge

The password for the “remote” user is actually configured in two places:

- There is the real, functional password which is configured using the AIX **passwd** command.

- There is the so-called *published* password which is a string known by RSF. This string has been specified at RSF configuration time by your service representative, through the **RSF Configuration** menu (**Password for “remote”** field). When RSF transmits an alarm message to the service centers, it includes this *published* password in the message, so that the remote service personnel knows it.

Consequently, if you change the real password, the remote service experts have no means to know it, and will not be able to connect to your system. Thus, you will have to tell them by phone the next time they will try to log in to your system.

Procedure

To change the password for the “remote” user:

1. Use the AIX **passwd** command to change the password for the “remote” user:

```
passwd remote
```

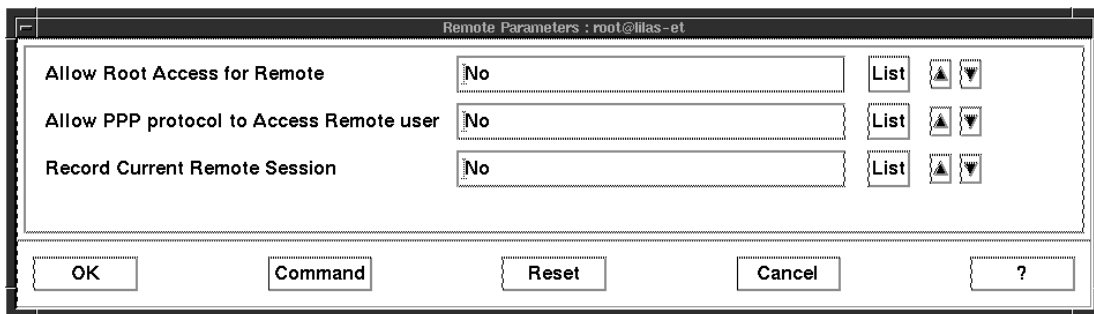
2. Being root, edit the **/etc/security/passwd**. Go to the “remote” user stanza and check that the flag **ADMCHG** has been removed. If not, remove it. (This ensures that the “remote” user is not required to change the password the next time he logs in.)

Allowing or Disallowing Root Access for the “remote” User

Fast Path: **smit cbkcfg**

To allow or disallow root access for the “remote” user:

1. From the **Remote Session Management** menu, select **Remote Parameters**: a new menu appears (see illustration below).
2. Change the **Allow Root Access for Remote** field to either **Yes** or **No** (**Yes** indicates that “remote” is allowed to have root privileges).
3. Choose **Do** to confirm or **Cancel** to abandon.



Remote Parameters

Allowing or Disallowing PPP Protocol

Fast Path: **smit cbkcfg**

You may, for security reasons, decide to allow or disallow access through a PPP connection for the “remote” user. By default this parameter is set to **No**, indicating that “remote” is not allowed to connect through a PPP link.

To allow or disallow PPP protocol to access remote user:

1. From the **Remote Session Management** menu, select **Remote Parameters**: a new menu appears (see illustration above).
2. Change the **Allow PPP Protocol to Access Remote User** field to either **Yes** or **No**.
3. Choose **Do** to confirm or **Cancel** to abandon.

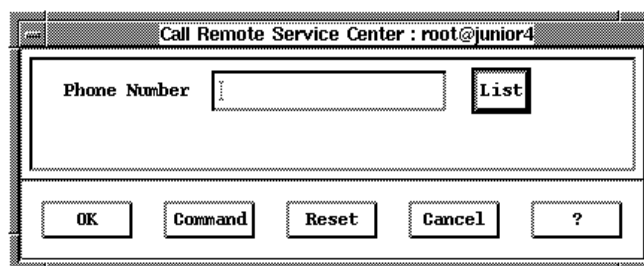
Using the Manual Callback Feature: Call Remote Service Center

When the **Callback Mode** is **manual**, calling the remote service center requires manual intervention (for a discussion, refer to *Scenario 3: Manual Callback*, on page 4-5).

In the event a remote service session is needed, the remote service personnel may ask by phone you establish a connection with the remote service center. In that case, proceed as follows:

Fast Path: `smit callremote`

1. **Make sure you are logged in to the RSF server** (i.e. to the system which is equipped with a modem). The *Note on RSF Cluster Configurations*, on page 4-5, explains why this is needed.
2. Note that the **Call Remote Service Center** function works only when the **Callback Mode** is **manual**. To show or change the **Callback Mode**, refer to *Setting Up the Callback Mode*, on page 4-6.
3. From the **Remote Session Management** menu, select **Callback Management**, then **Call Remote Service Center**: a new screen appears that prompts you to enter the appropriate **Phone Number**.



Call Remote Service Center

4. Press F4 (or use the “List” button) to retrieve the list of phone numbers that have been defined through the **Add a Phone Number** menu. From this list, select the desired phone number. Please note the following:
 - Alternatively, you may also enter any other phone number, if appropriate.
 - The phone number may be optionally interspersed with special characters that the modem understands. For a discussion, refer to *Specifying a Phone Number*, on page 4-7.
5. Validate the screen to dial the specified number, and wait for the command completion. After a delay of ten seconds to one minute, a message should indicate that the connection is established. Then, at the remote service center, the personnel sees the AIX login banner and can log in to the system (using the “remote” account) to carry out a remote service session.
6. When the remote service personnel logs in to the system as the “remote” user, you are notified with both a message on the console and an e-mail message. Then, you may decide to supervise the remote session through the remote session mirroring feature, as explained in *Remote Session Mirroring* below.

Remote Session Mirroring: Supervising a Remote Session

When a remote service expert logs in to your system (as the “remote” user), you are notified with both a message on the console and an e–mail message. Then, you may decide to supervise the session through the remote session mirroring feature.

Note: You can mirror only the remote sessions that are handled in character mode. The remote sessions through a PPP connection to graphical applications – typically WebSM – cannot be mirrored.

Note: The console where the remote session notifications are displayed was defined by your service representative at RSF configuration. It is usually the S1 console device.

Remote session mirroring allows you to not only view what the “remote” user is doing, but also to actually participate in the session itself. In other words, input from your terminal will appear in the session screen as well as the “remote” user’s session screen. This is like a two way mirror: both sides see what the other is doing.

Initiating the Remote Session Mirroring Feature

Two methods are available to initiate the remote session mirroring feature: the **Remote Session Mirroring** option of the RSF SMIT menu, and the **joinses** command. The two methods, which are equivalent, are explained below.

Using the “Remote Session Mirroring” Menu Option

1. Log in as **root**, and go to the RSF main menu by typing **smit rsf**.
2. Choose **Remote Session Management**, then **Remote Session Mirroring**: a new screen appears, that allows you to participate in the remote session.

Note that you can also use the **smit joinses** fast path.

Using the **joinses** Command

1. Log in as **root**, and enter **joinses**.
2. You can now participate in the remote session.

What Happens When Initiating the Remote Session Mirroring Feature

- If there is no remote session currently in progress, an appropriate message is displayed, and you are asked to specify whether or not you want to wait for a remote connection:
 - If you answer **y**, the message “Waiting remote connection...” is displayed until the “remote” user logs in to the system. Note that, at this point, if you no longer want to wait for a remote connection, you can exit the session mirroring feature by entering the shell interrupt character, which is usually Ctrl-C or Del.
 - If you answer **n**, the session mirroring feature closes.
- If the **Remote Authorisation** flag (which is discussed in “Setting Remote Access Authorization”, on page 4-5) is currently disabled, a message prompts you to enable it. Note that the “remote” user is unable to log in to the system as long as the **Remote Authorisation** flag stays disabled.

Possible Actions During Remote Session Mirroring

Once the “remote” user is logged in to the system, you view what he is doing. You can participate in the session by typing commands from the keyboard as you would normally. In addition, the following special key sequences are available:

Ctrl–X Q Allows you to quit the session, without disconnecting the “remote” user. Use this key sequence if you no longer want to supervise the session, while letting the “remote” user continue the service session.

Ctrl-X K Allows you to abruptly disconnect the “remote” user. The **Ctrl-X K** also disables the **Remote Authorisation** flag (which is discussed in “Setting Remote Access Authorization”, on page 4-5). The **Ctrl-X K** sequence is rarely used, since the remote service experts know their work and are not “spying” on your system. However this feature may be of interest for those sites where sensitive information is processed and security-related constraints are strong.

When the “remote” user terminates the remote service session by logging out, the session mirroring feature closes, and the **Remote Authorisation** flag automatically reverts to its initial state (enabled or disabled).

Managing Remote Session Recording

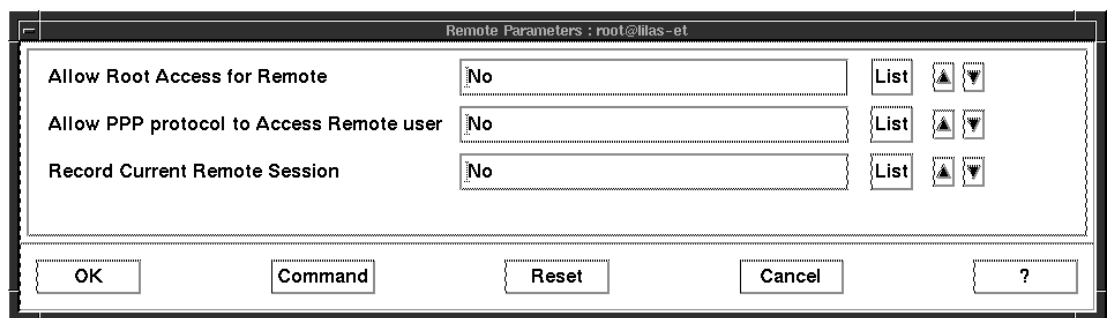
Recording Remote Sessions

You may want RSF to record remote sessions, so that you can review them subsequently. When recording is enabled, RSF saves all remote sessions to disk (in the `/var/rsf/sessions` directory).

Fast Path: `smit cbkcfg`

To enable or disable remote sessions recording:

1. Log in as **root**, and go to the RSF main menu by typing `smit rsf`.
2. Choose **Remote Session Management**, then **Remote Parameters**: a new menu appears (see illustration below).



Remote Parameters

3. Change the **Record Current Remote Session** field to either **Yes** or **No** (**Yes** indicates that recording is enabled).
4. Choose **Do** to confirm or **Cancel** to abandon.

The sections below explain how to review and remove recorded sessions.

Reviewing Recorded Sessions

Fast Path: `smit showlses`

To review a recorded remote session:

1. Access the **Remote Session Management** menu.
2. Choose **Review Recorded Session**: a list of recorded sessions is displayed.
3. Select in the list the session you want to review.
4. When reviewing a recorded session:
 - To pause and un-pause the session playback, use the **P** key.
 - To speed up the playback, use the **!** key.

- To return to normal speed, use the spacebar.
- To quit reviewing the session, press the **Q** key.

Removing a Recorded Session

Once you have reviewed recorded sessions and you do not need them anymore, it is advisable to remove them in order to save disk space. Of course, this administrative task is necessary only if you make use of the session recording feature.

Fast Path: `smit rmlses`

To remove a recorded remote session:

1. Access the **Remote Session Management** menu.
2. Choose **Remove Recorded Session**: a list of recorded sessions is displayed.
3. Select in the list the session you want to remove.
4. Choose **OK** to confirm or **Cancel** to abandon.

Chapter 5. Dial Out Management

Dial Out Management With RSF (Remote Services Facilities)

This chapter includes the following sections:

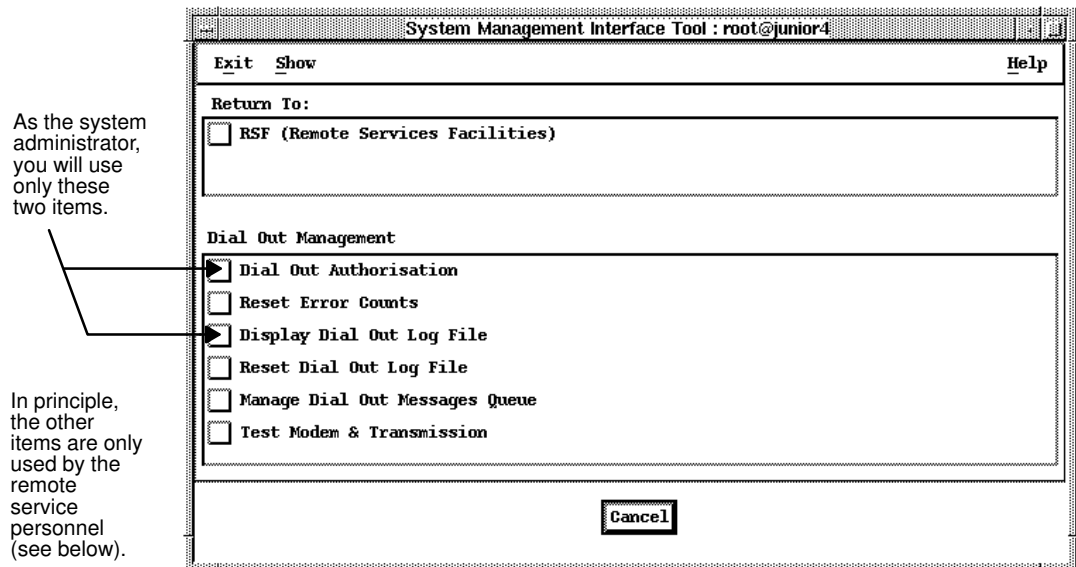
- Accessing Dial Out Management Functions
- Enabling and Disabling Alarm Messages Transmission
- Listing Information Related to Alarm Messages Transmission

Accessing Dial Out Management Functions

Fast Path: `smit callout`

To access the **Dial Out Management** menu:

1. Log in as **root**, and go to the RSF main menu by typing `smit rsf`.
2. Choose **Dial Out Management**. The corresponding menu is displayed (see illustration).



Dial Out Management

Functions Usage

As the system administrator, you will use, from the **Dial Out Management** menu, only the two following items:

- **Dial Out Authorisation**
- **Display Dial Out Log File**

In principle, the other items are only used by the remote service personnel:

- You will never use **Manage Dial Out Messages Queue**, thus it is not documented.
- Although **Reset Error Counts**, **Reset Dial Out Log File**, and **Test Modem & Transmission** are primarily intended for the remote service personnel, you may have to use these functions in rare circumstances (when requested by the remote service personnel). These functions are not documented.

Enabling and Disabling Alarm Messages Transmission

As the system administrator, you may decide for some reason to disable dial out, i.e. to prevent RSF from transmitting alarm messages.

However, you will usually want alarm messages to be transmitted by RSF to the remote service center: if so, you may ignore the instructions below.

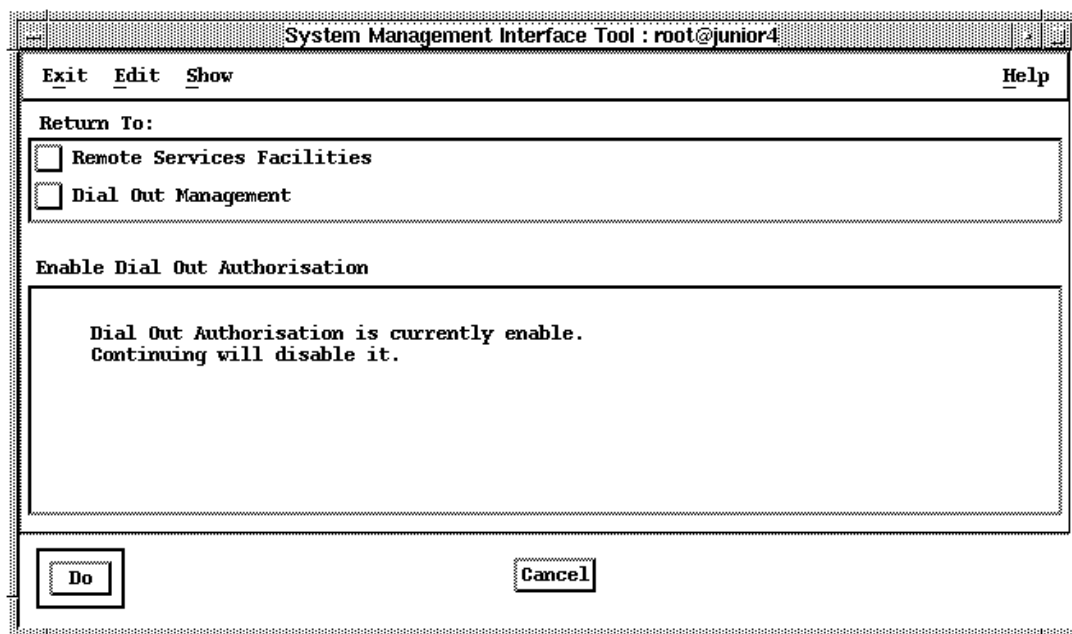
Procedure

Fast Path: `smit doauth`

To disable or enable alarm messages transmission:

1. Log in as **root**, and go to the RSF main menu by typing `smit rsf`.
2. Choose **Dial Out Management**, then **Dial Out Authorisation**: a new screen appears (see illustration). The displayed message indicates if dial out is currently enabled or disabled, and accordingly prompts you either to disable or to enable it.
3. Choose **Do** to perform the task or **Cancel** to abandon.

Note: You may want to know that the RSF **Dial Out Authorisation** menu actually modifies the “Dial-Out Authorization” flag, which is also used by SSF (*System Service Facility*). SSF concerns only ESCALA EPC800, R, M and D systems. It is a collection of firmware programs which run on the BUMP (*Bring-Up MicroProcessor*) and allow an operator to perform system maintenance functions.



Dial Out Authorisation

Viewing the Current Dial Out Status

You may view the current dial out status: refer to section *Viewing RSF Status*, on page 3-2.

Listing Information Related to Alarm Messages Transmission

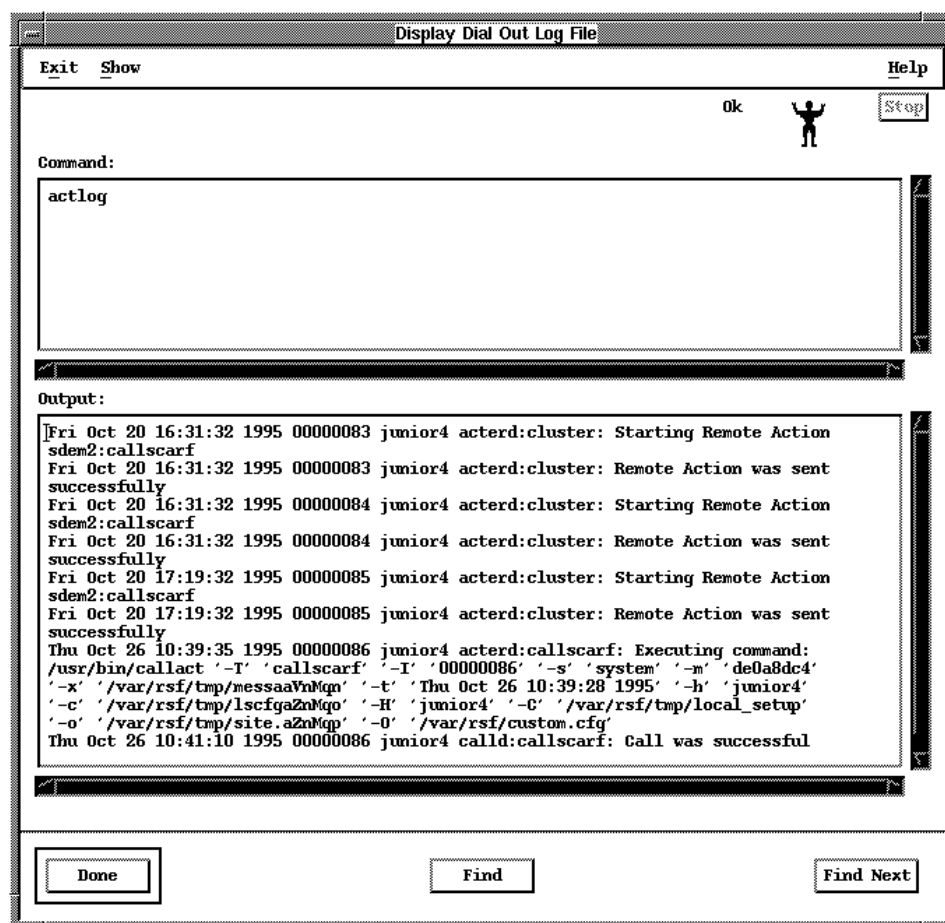
Each time RSF transmits an alarm message to the service center, the related information is logged. This provides you with a way of reviewing what has been done by RSF, although it is mainly intended for the remote service personnel.

Procedure

Fast Path: `smit show_actlog`

To display information about the alarm messages that have been transmitted to the service center:

1. Log in as **root** , and go to the RSF main menu by typing `smit rsf`.
2. Choose **Dial Out Management**, then **Display Dial Out Log File**: a new screen is displayed, that shows information (see illustration).
3. Choose **Do** to perform the task or **Cancel** to abandon.



Display Dial Out Log File

Understanding the Dial Out Log

The displayed information is primarily intended for the remote service personnel, so you may find it rather cryptic.

As a hint, note that each line includes: a date/time part; an RSF internal number for RSF action (e.g. 00000004); the name of the program writing into the log file (usually **acterd**); the action executed; a string indicating the result of the action. Also note that the listing may include information related to actions carried out by *Extended RSF*.

Vos remarques sur ce document / Technical publication remark form

Titre / Title : Bull ESCALA RSF (Remote Services Facilities) User's Guide

N° Référence / Reference N° : 86 A2 95AQ 03

Daté / Dated : October 1999

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 ANGERS
CEDOC
34 Rue du Nid de Pie – 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 ANGERS
CEDOC
ATTN / MME DUMOULIN
34 Rue du Nid de Pie – 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° Référence CEDOC	Qty Qté	CEDOC Reference # N° Référence CEDOC	Qty Qté	CEDOC Reference # N° 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.

BULL ELECTRONICS ANGERS
CEDOC
34 Rue du Nid de Pie – BP 428
49004 ANGERS CEDEX 01
FRANCE

ORDER REFERENCE
86 A2 95AQ 03

PLACE BAR CODE IN LOWER
LEFT CORNER



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

