RSF (Remote Services Facilities) for HMC V7 and later

User's Guide

ESCALA

AIX

REFERENCE
86 A2 64EV 00

BLANK

ESCALA

RSF (Remote Services Facilities) for HMC V7 and later

User's Guide

AIX

Software

June 2007

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

REFERENCE
86 A2 64EV 00

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

About This Book

This book, *RSF for HMC User's Guide*, 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.

RSF for HMC allows RSF to run on the Hardware Maintenance Console (HMC) using a Web-based User Interface.

Who Should Use This Book

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

This book applies to RSF V3.12 and later with HMC V7 and later.

About HMC Version 7

Web-based user interface:

Starting from Version 7 Hardware Management Console, the HMC User Interface (UI) has changed to a standard HTML (Web browser) implementation. WebSM is no longer used. When the HMC has been enabled to accept remote connections, any supported Web browser can be pointed at the HMC and used as the remote console.

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 Web-based User Interface 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.

Related Publications

- *RSF User's Guide* (86 A2 95AQ) is dedicated to the basic SMIT-based RSF product.
- *Hypertext Library for AIX and Related Products* CD-ROM for all information about your AIX system.
- For RSF prior to V3.12 please refer to RSF for HMC User's Guide 86 A2 98EF.

Table of Contents

Table of Figures

Chapter 1. Introduction to RSF

This chapter is an overview of RSF. It includes the following sections:

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.

While the basic RSF product is designed as an integrated SMIT (System Management Interface Tool) application, RSF for HMC - the subject of the present manual - is designed as a Web-based User Interface 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,* Ref. 86 A7 14GX.

Installation Requirements

RSF is available on HMC systems running the Linux 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 tty S1 line of the system.
- 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 V3.12 is required for HMC V7 and later.

Main Functions

RSF handles two main functions:

- error monitoring and alarm transmission,
- and management of remote service sessions.

Error Monitoring and Alarm Transmission

RSF scans periodically the 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.

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.

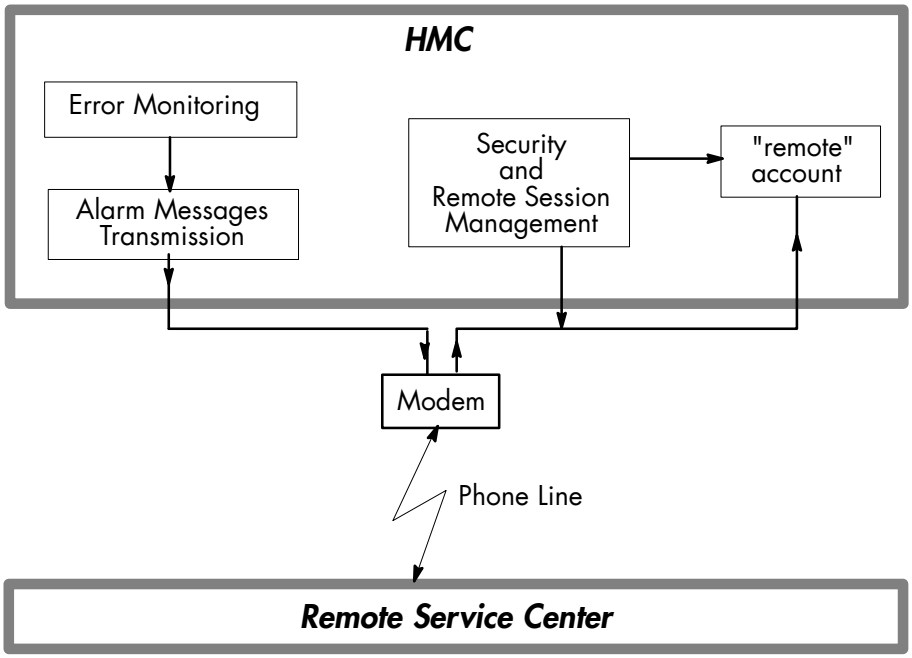
RSF respects your security policy. You may choose to let the service center intervene alone, or to fully control the course of remote service sessions.

For further information, refer to *Security and Management of Remote Service Sessions*, on page 1-4.

Operating Principles

Operation Outlines

The following figure outines RSF operating principles.



RSF Operation Outlines

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

Software errors (system) are logged in the **/var/log/messages** file.

Hardware errors are logged in files:

- **/var/rsf/hmc_errdata/error*** for **syst_os** errors coming from sfp (service focal Point).
- **/var/ct/IW/log/mc/IBM.ServiceRM/CSPdat** and **/var/ct/IW/log/mc/IBM.ServiceRM/CSPdat.bak** for **syst_cec** errors.

RSF scans periodically the error log files 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 (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, see 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

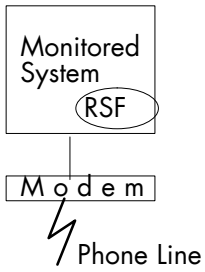
- You are notified with both a message on the console and e-mail when someone is logging in (or logging out) via the "remote" account.
- Through the session mirroring feature, you have control over what is happening during the remote session. You can view all operations performed and also participate 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.

Simple configuration



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).

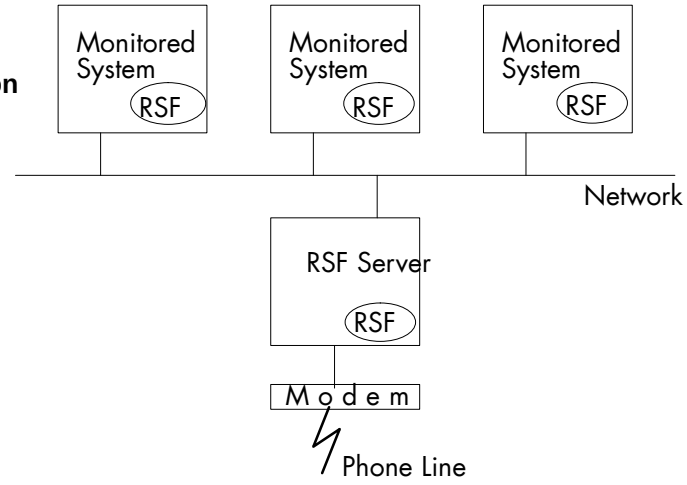
In this case, one of the systems acts as an RSF server:

- 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.

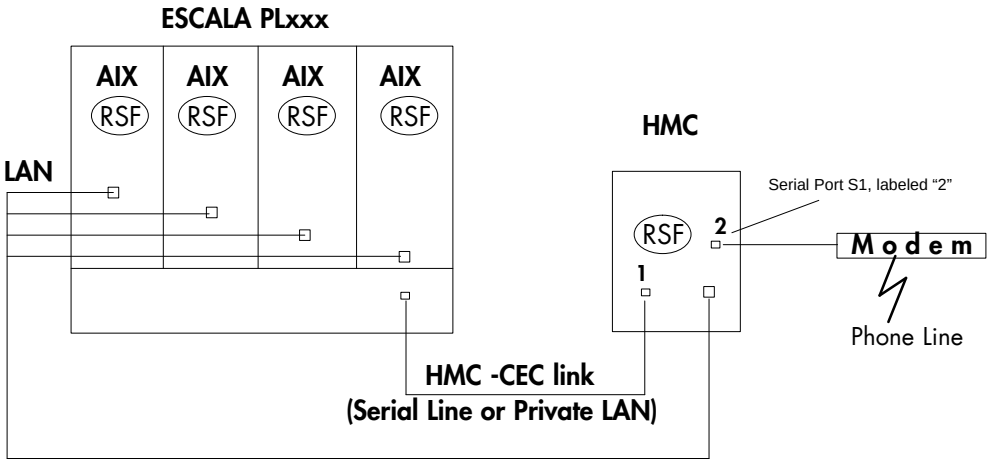
Cluster configuration



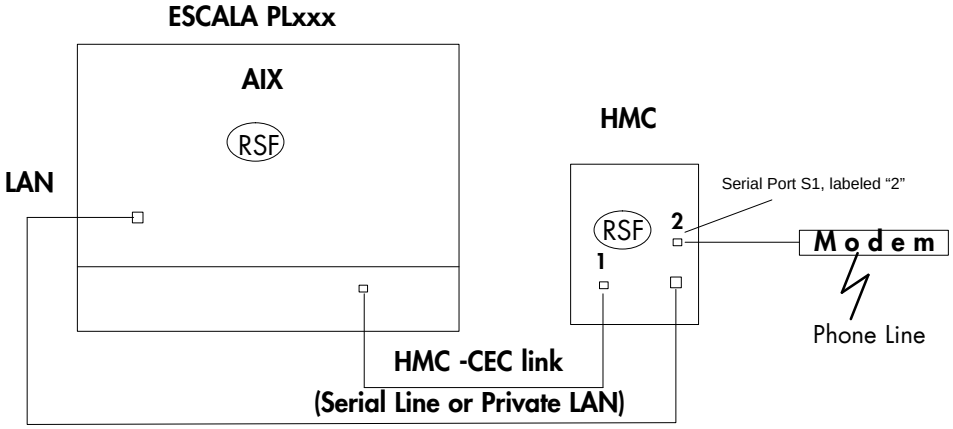
Configuration in SMP or Partinioning Mode

The figures below illustrate the configurations where the HMC is connected to ESCALA PLxxx systems that support partinioning.

Configuration in partition mode



Configuration in SMP mode



☞ **Note:**
On rack-mounted HMC only one serial line is available. Contact your Bull support representative for the installation of the modem.

Chapter 2. Getting Started With RSF

This chapter includes the following sections:

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.

/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, enter:

```
rpm –qa rsf.rsflite
```

Accessing RSF Functions

Preliminary Remarks

You will access all RSF functions through the Web-based User Interface of the HMC, which is automatically started during boot operation.

You must be logged in as **hscroot** each time you access RSF functions from the Web-based User Interface.

Accessing RSF Main Window

To access RSF main window:

1. Log in as **hscroot** on the console.
2. From the first Web-based User Interface window click on the Remote Service Facilitites icon, as in the following figure:

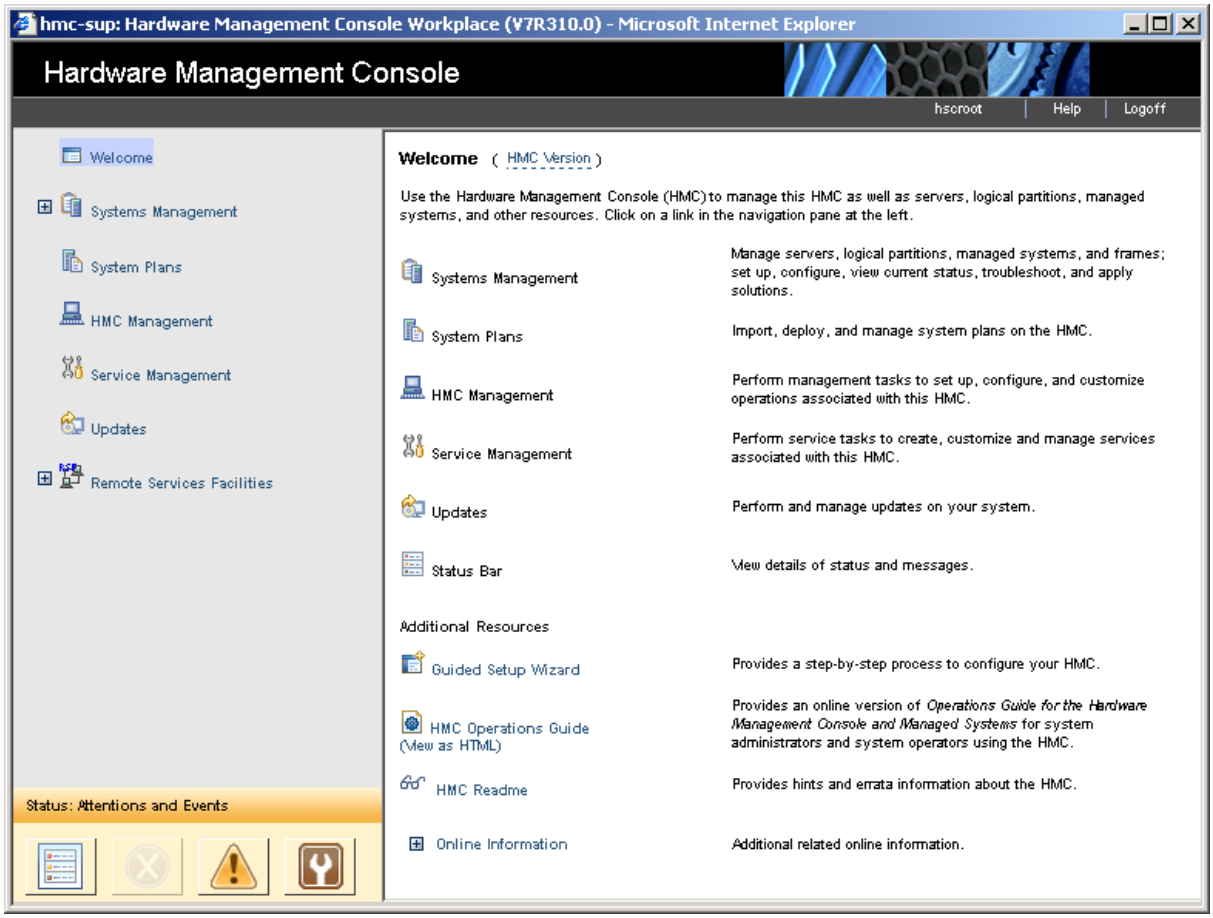


Figure 1. Web-based User Interface first window

3. The RSF main frame is displayed, as follows:

Figure 2. RSF for HMC main frame

RSF Functions Usage

The RSF application offers the following options:

Overview and Tasks

- 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 .
- 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.

Configuration and Maintenance Contract

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

☞ **Notes:**

1. The HMC Serial Number is automatically configured in RSF V3.12 and later.
2. Maintenance Contract Flags must be configured locally on the customer HMC.

Chapter 3. RSF Management

This chapter includes the following sections:

Starting and Stopping RSF

Understanding Start and Stop 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** (see 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 thereforward.

☞ **Notes:**

- The RSF daemons are **rsfd**, **calld**, **bmapd** and **acterd** .
- 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.

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.

To start or stop the RSF daemons:

1. Log in as **hscroot** on the console, and click on the RSF icon to display the RSF main window.

2. Click on **Overview and Tasks**: a new window is displayed that indicates if RSF is currently running or down:

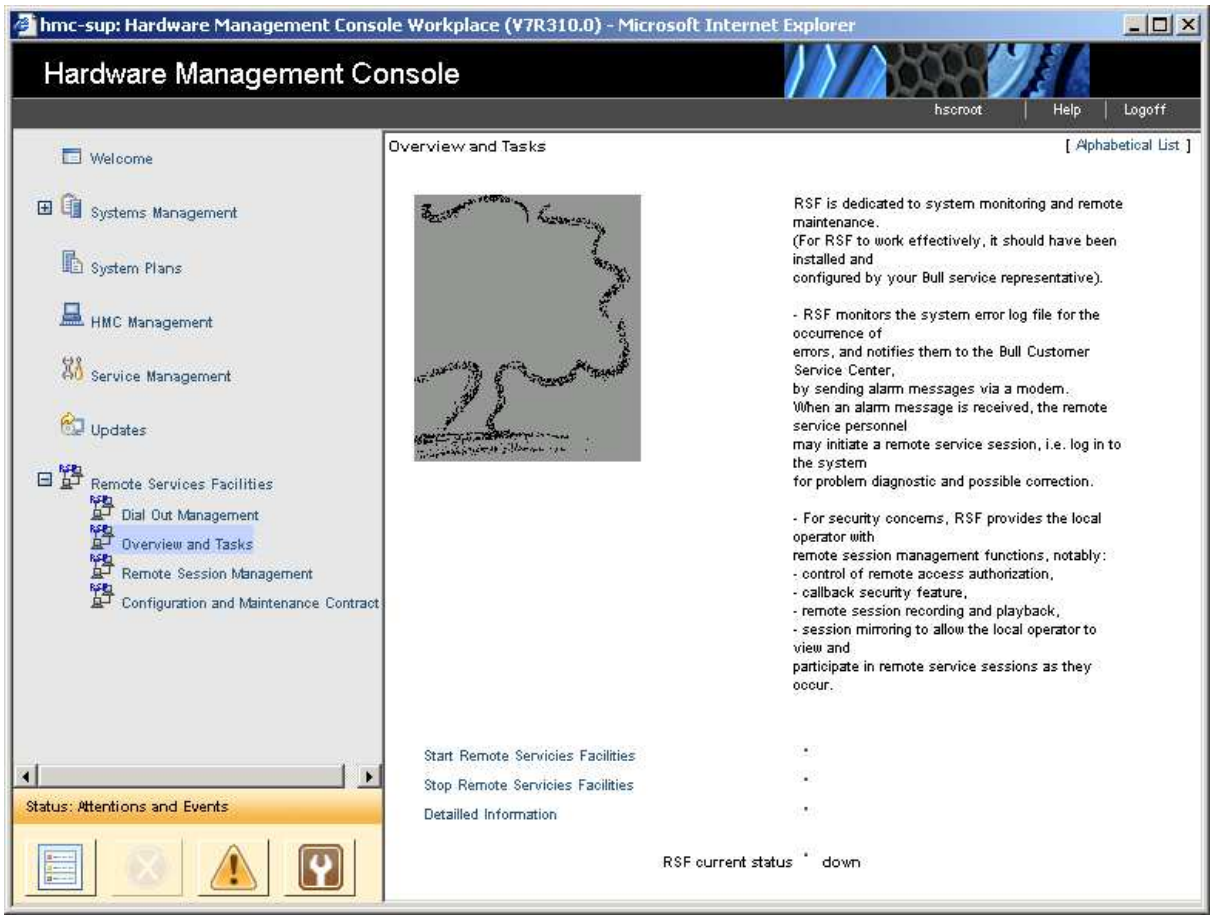


Figure 3. Overview and Tasks window

3. Click on the appropriate link to stop or to start RSF. As an example, the following figure illustrates the result of a Start RSF action:

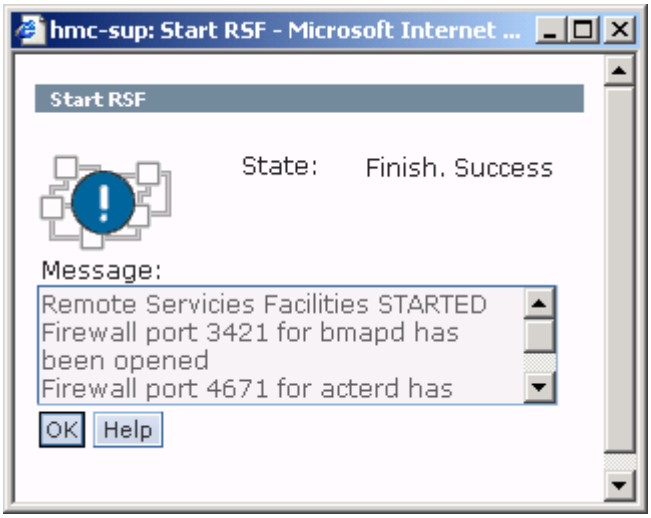


Figure 4. Start RSF result

Clic OK to close the window and verify that the RSF current status has changed to "start".

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

To view the status of RSF:

1. Log in as **hscroot** on the console, and click on the RSF icon to display the RSF main window.
2. Click on **Overview and Tasks**. The following window is displayed:

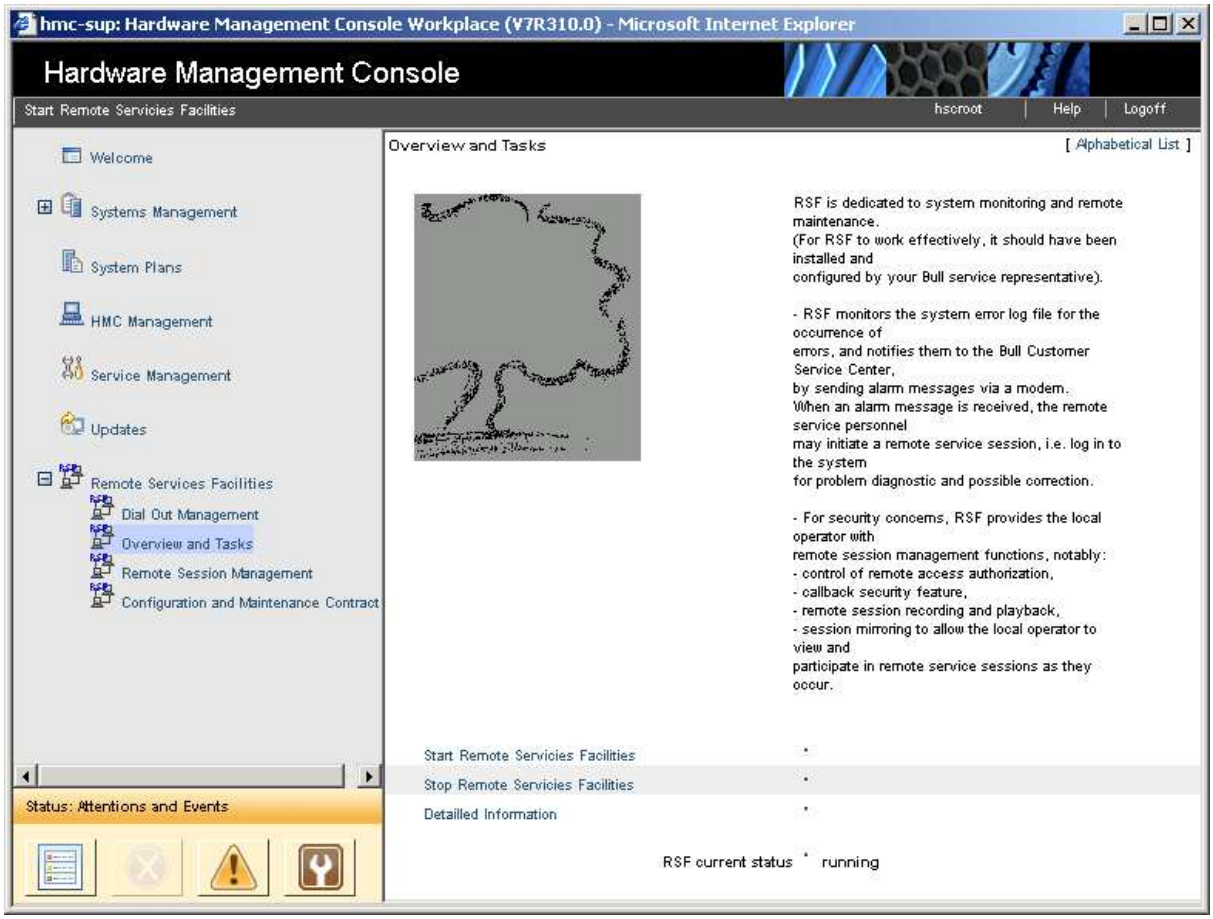


Figure 5. Overview and Tasks window

3. Click on **Detailed Information**. A window similar to the following is displayed:

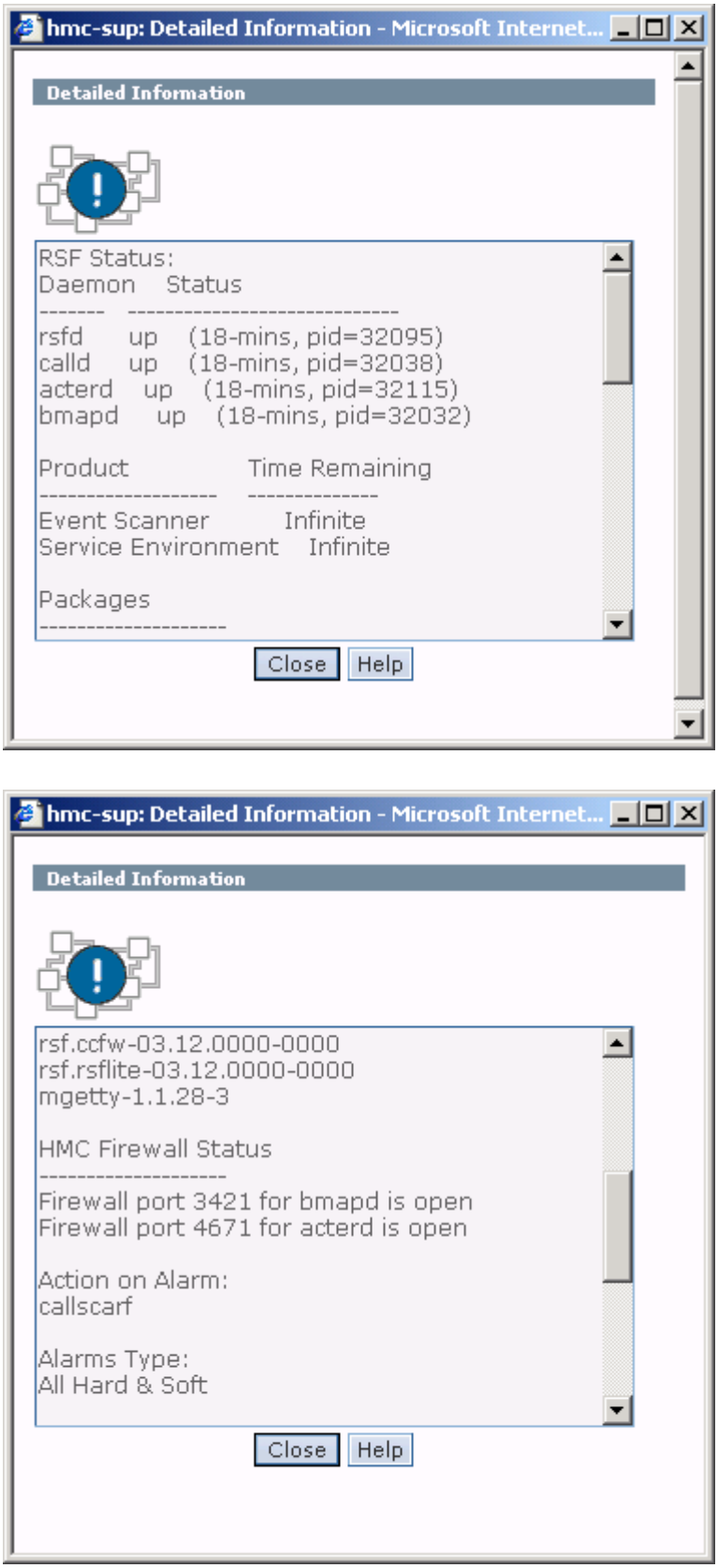


Figure 6. RSF Status window (part1 / part2)

Understanding the Status Information

The displayed information is organized into five sections, described below:

- **RSF Status**,
- **Action on Alarm**,
- **Alarms Type**,
- **Dial Out Status**,
- **Remote Status**.

RSF Status

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

Daemon / Status

Indicates the status of the four RSF daemons (**up** or **down**). If the status is **up**, it also indicates the time since the daemon is up and the daemon process ID (**pid**). If RSF is running, the four RSF daemons (**rsfd**, **calld**, **acterd** and **bmapd**) should be **up**.

Product / Time Remaining

Indicates the time that remains before your RSF license expires. The displayed information depends on your maintenance contract. A license is associated with the two standard RSF products **Event Scanner** and **Service Environment**.

Packages Name and version ot the installed rpms on the HMC

```
rsf.ccfw-03.12.0000-0000
rsf.rsflite-03.12.0000-0000
mgetty-1.1.28-3)
```

HMC Firewall Status

Firewall port3421 for **bmapd**, port4671 for **acterd** is open when theses processes are running and closed when they are down.

Action on Alarm

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

Alarms Type

This section displays the type of alarm currently configured.

Dial-Out Status

This section gives information about the transmission of alarm messages to the service center (**dial-out**). The displayed information depends on **Action on Alarm** type:

- If **Action on Alarm** is **cluster**, the **Dial-Out Status** section indicates only if the dial-out is **Enabled** or **Disabled**.
- If **Action on Alarm** is **callscarf** and **callrcs2**, the following information is displayed:

  TTY tty port to which the modem is attached (usually `ttyS1`).

  Dial-Out either **Enabled** or **Disabled**. **Enabled** means that outgoing calls are allowed, thus RSF is able to transmit alarm messages to the remote service center. Refer to *Dial Out Management*, starting on page 5-1.

  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 "none".

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 the connections initiated by the service center personnel (**dial-in**). The displayed information depends on **Action on Alarm** parameter:

- If the current **Action on Alarm** is **cluster**, the **Remote Status** section indicates only if the dial-in is **Enabled** or **Disabled**.
- If the current **Action on Alarm** is **callscarf** and **callrcs2**, the following information is displayed:

TTY tty port to which the modem is attached (usually `ttyS1`).

Modem Type type of the modem (for example, `multitech.fr`).

Dial-In either `Enabled` or `Disabled`. Enabled means that incoming calls are allowed, thus the remote service personnel is able to initiate a remote service session. Refer to *Setting Remote Access Authorization*, on page 4-6, for related information.

Status The current status of the modem. Among possible status there 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 used 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 is 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

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. 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 4-4.

"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 4-8*.

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.

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

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

1. Log in as **hscroot** on the console, and click on the RSF icon to display the RSF main window.
2. Click on **Remote Session Management**: a new window is displayed :

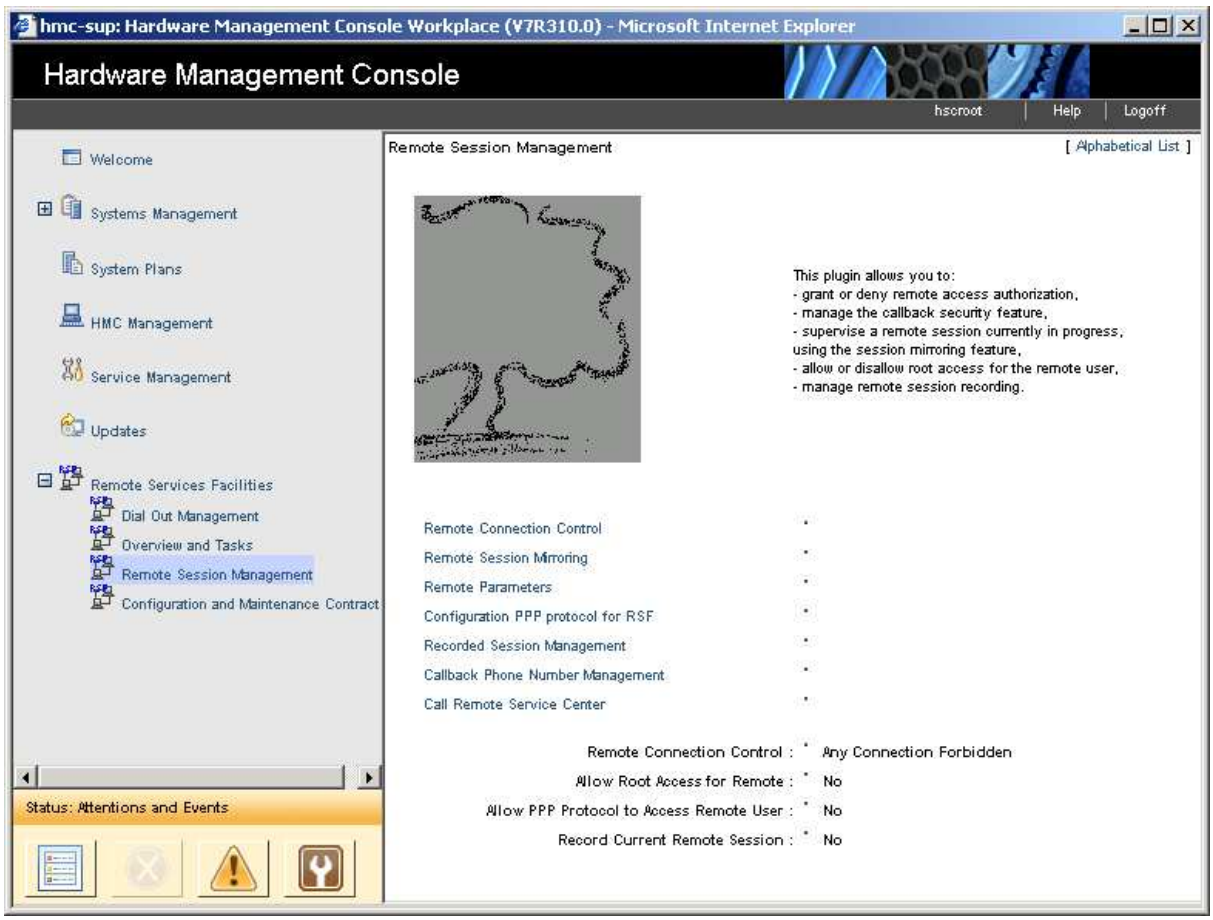


Figure 7. Remote Session Management window

Managing Remote Connection Security

This section explains how to implement your security policy for handling remote connections. This topic relates to the **Remote Connection Control** task.

Understanding Remote Connection Control

The way incoming calls are handled depends on the **Remote Connection Control** configuration that you choose:

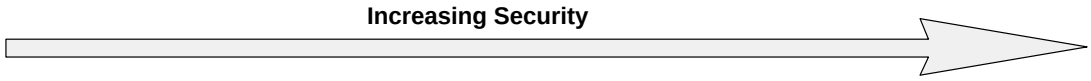
- you can grant or deny remote access authorization,
- you can specify the desired callback mode.

These two 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 table below.

Security Levels for Connection Control

- First, determine which of the four security levels discussed below matches your security policy.
- Then set the **Remote Connection Control** accordingly, as explained in *Setting Remote Connection Control*, on page 4-6.

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



	Security level 1	Security level 2	Security level 3	Security level 4
	Direct Connections Authorized	**Automatic Callback**	**Manual Callback**	**Any Connection Forbidden**
Remote Authorisation	enabled	enabled	disabled	disabled
Callback Mode	disabled	automatic	manual	disabled

Security Level 1: Direct Connections Authorized

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

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 Linux 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).

Security Level 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.

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 Linux 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.

Security Level 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.

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** window (discussed on page 4-9). When this is done, the personnel at the remote service center see the Linux login banner and can log in to the system (using the "remote" account).

Security Level 4: Any Connection Forbidden

Remote Authorisation: **disabled**

Callback Mode: **disabled**

As in Security level 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 Security level 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 1-5). All communications occur through the modem of the RSF server.

Important:

Keep in mind that functions of the **Callback Management** window (**Callback Mode** setting, **Call Remote Service Center** function, management of phone numbers used for the callback feature) must been 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 Connection Control

The **Remote Connection Control** specifies whether incoming calls and remote logins are authorized or rejected.

To change the **Remote Connection Control** setting:

1. Access the **Remote Session Management** window.
2. Choose **Remote Connection Control**. The following window is displayed:

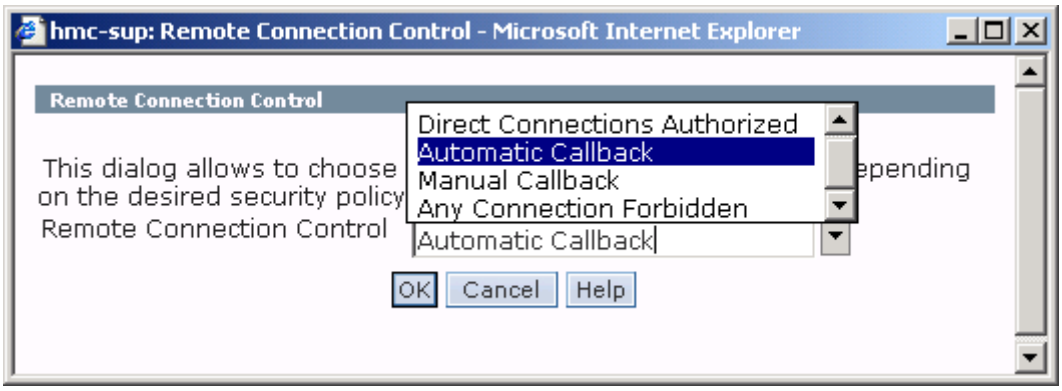


Figure 8. Remote Connection Control window

3. Select between the four options (Direct Connections Authorized, Automatic Callback, Manual Callback, Any Connection Forbidden) the security level you need.
4. Choose **OK** to perform the task or **Cancel** to abandon.

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** task (discussed on page 4-9). From this window, 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. Access the **Remote Session Management** window.

3. Choose **Callback Phone Number Management**. The following window appears:

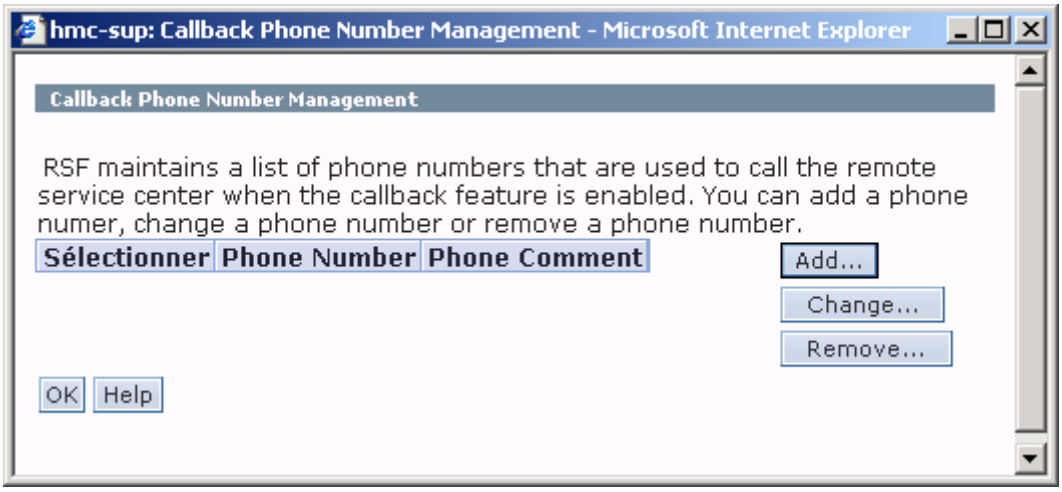


Figure 9. Callback Phone Number Management window

4. Use the buttons for adding, changing/showing and removing phone numbers used by the callback feature.

   Choosing the **Add** button displays the **New Phone Number** window as follows:

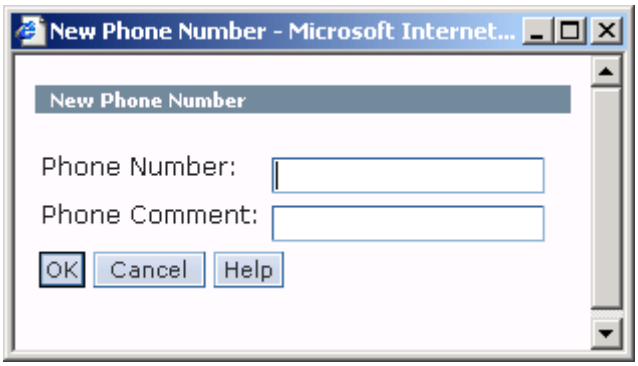


Figure 10. New Phone Number window

This window includes two fields, **Phone Number** and **Phone Comment**. In the **Phone 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

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** window (**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. Log in as **hscroot** on a shell console.
2. Log in as root using the following command:

```
su -
```

3. Enter the following Linux command:

```
passwd remote
```

4. Enter a new password.

Allowing or Disallowing Root Access for the "remote" User

To allow or disallow root access for the "remote" user:

1. Access the **Remote Session Management** window.
2. Choose **Remote Parameters.** The following window appears.

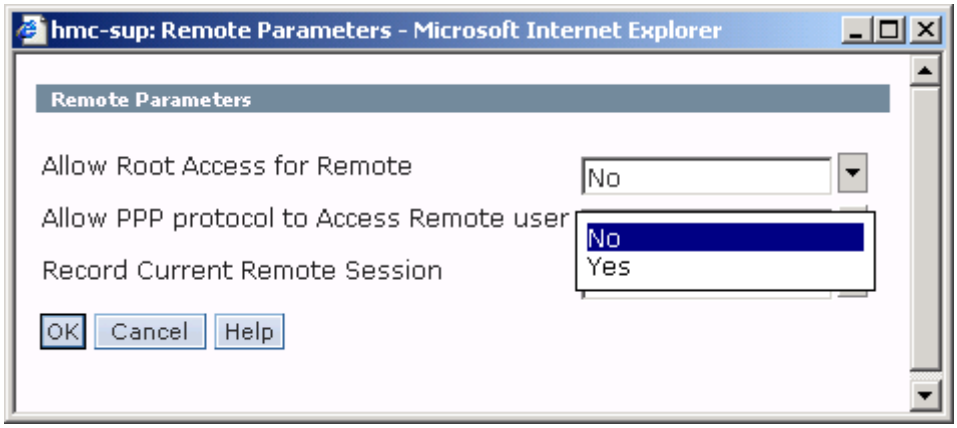


Figure 11. Remote Parameters window

3. Change the **Allow Root Access for Remote** field to either **Yes** or **No** (**Yes** indicates that "remote" is allowed to have root privileges).
4. Choose **OK** 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 *Security level 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, do as follows:

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**.
3. Access the **Remote Session Management** window.
4. Choose **Call Remote Service Center**. The following window appears that prompts you to enter the appropriate **Phone Number**.

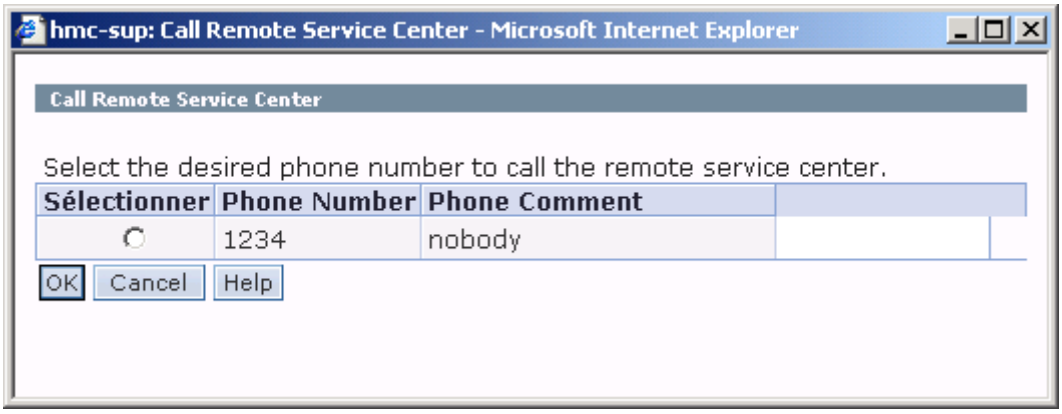


Figure 12. Call Remote Service Center window

5. The phone numbers that have been defined through the **Add a Phone Number** window are listed. 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.
6. Validate with "OK" 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 Linux login banner and can log in to the system (using the "remote" account) to carry out a remote service session.
7. 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:**
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.

Procedure

Proceed as follows to initiate a Remote Session Mirroring

1. Access the **Remote Session Management** window.
2. Choose **Remote Session Mirroring**. A new window appears that allows you to participate in the remote session.

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 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. 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).

To enable or disable remote sessions recording:

1. Access the **Remote Session Management** window.
2. Choose **Remote Parameters**: a new window appears.
3. Change the **Record Current Remote Session** field to either **Yes** or **No** (**Yes** indicates that recording is enabled).
4. Choose **OK** to confirm or **Cancel** to abandon.

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

Reviewing Recorded Sessions

To review a recorded remote session:

1. Access the **Remote Session Management** window.
2. Choose **Recorded Session Mangement**: 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.

To remove a recorded remote session:

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

Chapter 5. Dial Out Management

This chapter includes the following sections:

Accessing Dial Out Management Functions

To access the Dial Out Management window:

1. Log in as **hscroot** on the console and click on the RSF icon to display the RSF main window.
2. Click on **Dial Out Management**.The following window is displayed:

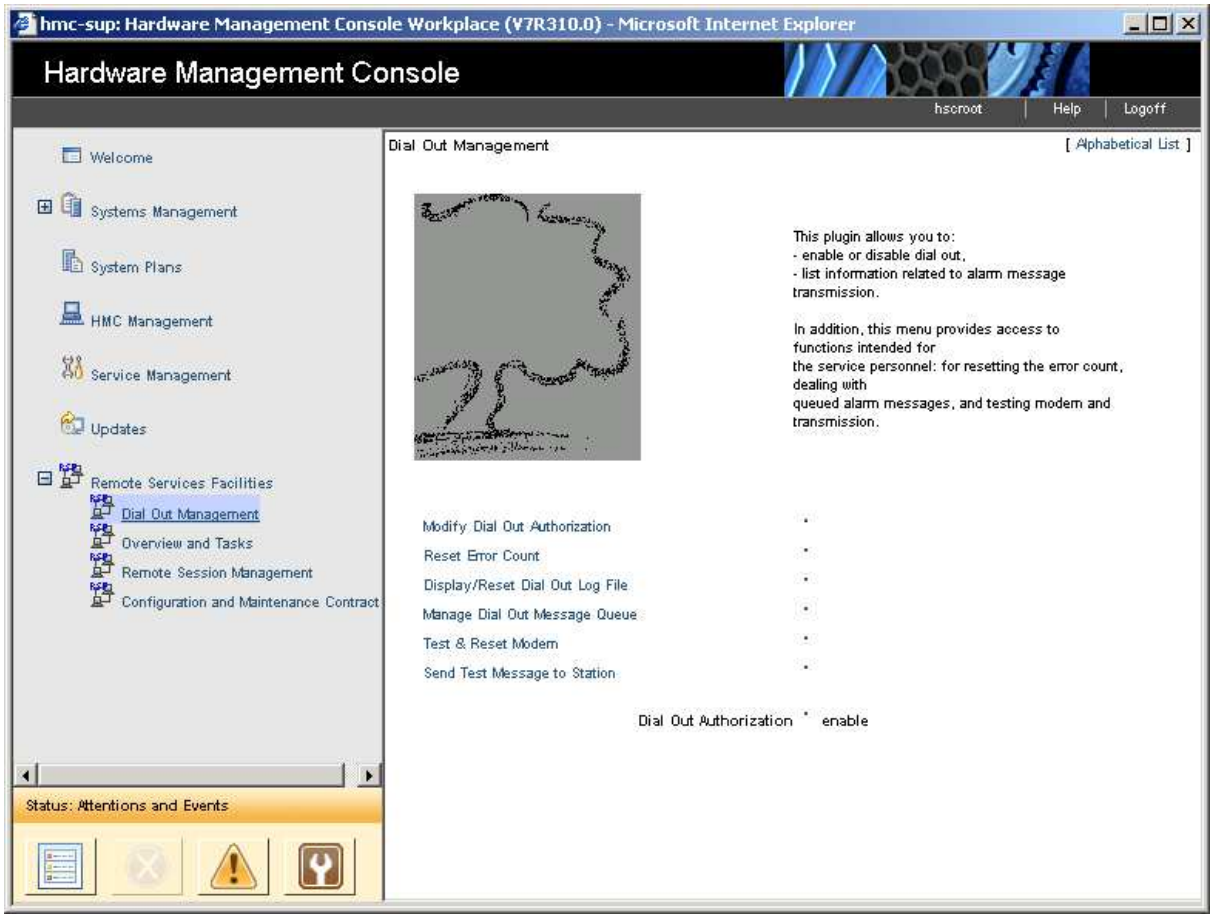


Figure 13. Dial Out Management window

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

- **Modify Dial Out Authorisation**
- **Display/Reset 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 Count**, **Test & Reset Modem**, and **Send Test Message to Station** 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.

Viewing the Dial Out Authorization Status

Access the **Dial Out Management** window. The **Dial Out Authorization** status is displayed.

Modifying the Dial Out Authorization

1. Access the **Dial Out Management** window.
2. Choose **Modify Dial Out Authorization** option. The **Dial Out Authorization** status is immediately modified.

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

1. Access the **Dial Out Management** window.

2. Choose **Display/Reset Dial Out Log File** option. A window that shows dial out information and similar to the following one is displayed:

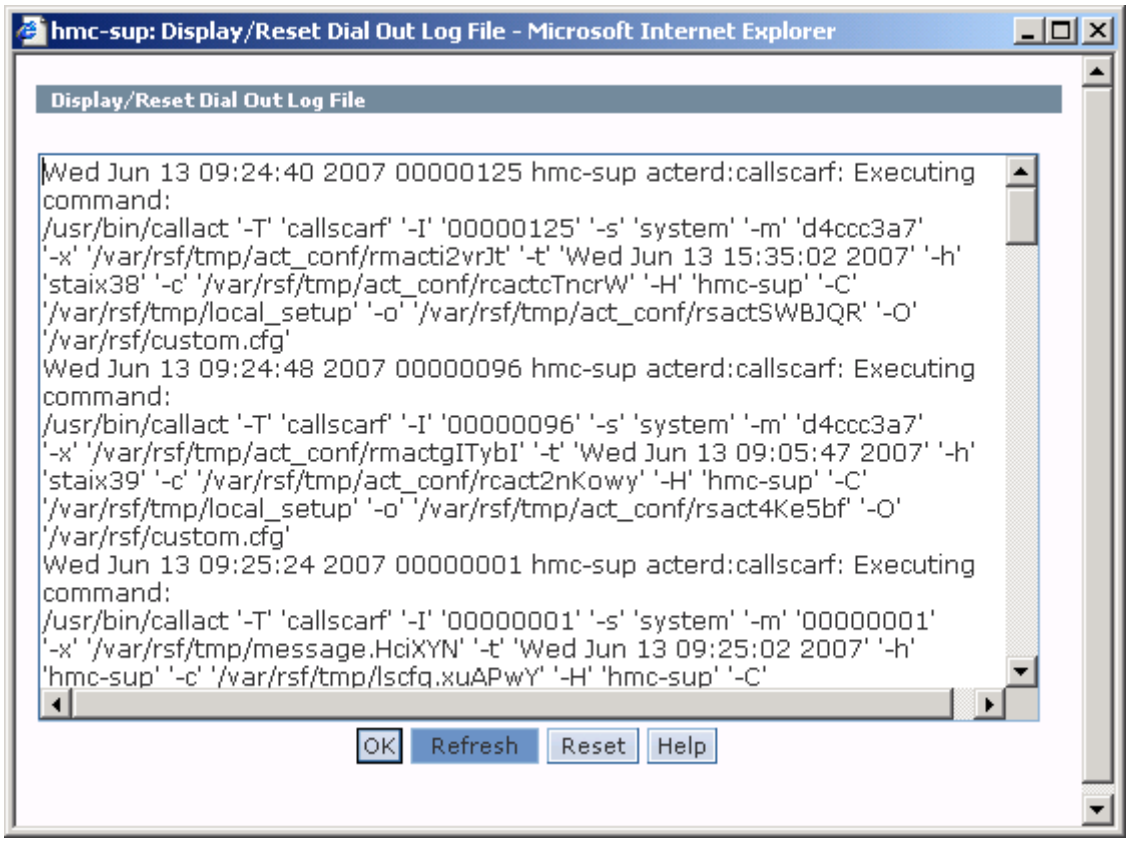


Figure 14. Display/Reset Dial Out Log File window

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 (for example 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*.

Technical publication remarks form

Title :	ESCALA RSF (Remote Services Facilities) for HMC V7 and later User's Guide

Reference:	86 A2 64EV 00	**Date:**	June 2007

ERRORS IN PUBLICATION

SUGGESTIONS FOR IMPROVEMENT TO PUBLICATION

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

NAME : _____ Date : _____

COMPANY : _____

ADDRESS : _____

_____

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

Bull - Documentation Dept.
1 Rue de Provence
BP 208
38432 ECHIROLLES CEDEX
FRANCE
info@frec.bull.fr

Technical publications ordering form

To order additional publications, please fill in a copy of this form and send it via mail to:

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

Phone: +33 (0) 2 41 73 72 66
FAX: +33 (0) 2 41 73 70 66
E-Mail: srv.Duplicopy@bull.net

Reference	Designation	Qty
_ _ _ _ _ _ _ _ _ [_ _]		
_ _ _ _ _ _ _ _ _ [_ _]		
_ _ _ _ _ _ _ _ _ [_ _]		
_ _ _ _ _ _ _ _ _ [_ _]		
_ _ _ _ _ _ _ _ _ [_ _]		
_ _ _ _ _ _ _ _ _ [_ _]		
_ _ _ _ _ _ _ _ _ [_ _]		
_ _ _ _ _ _ _ _ _ [_ _]		
_ _ _ _ _ _ _ _ _ [_ _]		
_ _ _ _ _ _ _ _ _ [_ _]		
_ _ _ _ _ _ _ _ _ [_ _]		
_ _ _ _ _ _ _ _ _ [_ _]		
[_ _] : The latest revision will be provided if no revision number is given.		

NAME: ______________________________ Date: ____________

COMPANY: ______________________________

ADDRESS: ______________________________

____

PHONE: ____________________ FAX: ____________________

E-MAIL: ______________________________

For Bull Subsidiaries:

Identification: ______________________________

For Bull Affiliated Customers:

Customer Code: ______________________________

For Bull Internal Customers:

Budgetary Section: ______________________________

For Others: Please ask your Bull representative.

BLANK

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

REFERENCE
86 A2 64EV 00

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

ESCALA

AIX

RSF (Remote Services Facilities) for HMC V7 and la User's Guide

86 A2 64EV 00

ESCALA

AIX

RSF (Remote Services Facilities) for HMC V7 and la User's Guide

86 A2 64EV 00

ESCALA

AIX

RSF (Remote Services Facilities) for HMC V7 and la User's Guide

86 A2 64EV 00