RMS RedMAXEMS
Administration and Maintenance Guide

May 4, 2010

Version: 2.2.1

Part Number: 70-00124-22-01

Disclaimer:

The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable; however, they are presented without express or implied warranty. Additionally, Redline makes no representations or warranties, either expressed or implied, regarding the contents of this document.

Redline Communications Inc. shall not be liable for any misuse regarding this product.

The information in this document is subject to change without notice.

Safety Notice:

The RMS product is designed to monitor and configure RedACCESS, RedCONNEX and RedMAX fixed wireless broadband equipment. Operators should read the User's Manual and Installation Guide for RedMAX wireless products described in this manual to understand and follow all operating and safety instructions before using the RMS. Keep all product information for future reference.

Confidential and Proprietary Information:

This document constitutes confidential and proprietary information of Redline Communications Inc.. The contents of this document may be accessed and/or used solely by a licensee of Redline Communications Inc. software product(s) and solely in connection with the licensee's authorized use of such product(s), or as otherwise expressly permitted by Redline Communications Inc. in writing. All other uses are prohibited. This document may not in any event be disclosed to any third party without the prior written authorization of Redline Communications Inc.

Trademark Information:

Redline Management Suite™, Redline®, RMS™, RedACCESS™, RedCONNEX™ and RedMAX™ are trademarks of Redline Communications Inc. All other brands and product names identified in this publication are trademarks or registered trademarks of their respective companies or organizations.

Table of Contents

CHAPTER 1 **About This Guide**

Overview 1-1
About This Document 1-1
Scope 1-1
Document Conventions 1-2
Supported Redline Equipment 1-3
. 1-3

CHAPTER 2 **System Administration**

Starting and Stopping Services 2-1
RMS 2-1
Stop RMS Services 2-2
Start RMS Services 2-3
Stand-Alone Provisioning Server 2-4
Solaris10 2-4
Windows Server 2003 2-4
Modify RMS and Provisioning Server Configuration 2-4
Modifying NE Upgrade Configuration 2-5
Configuring the Auto-Reset Behaviour 2-6
Modifying the Diagnostic Polling Interval 2-7
Java Memory Management 2-9
Collecting Garbage Collection Statistics from RMS 2-9
Collecting System Statistics Using the jstat Utility 2-12
Tuning Garbage Collection Behaviour 2-14
Generating Reports at the Command Line 2-18
Using HourlySCBandwidthReport.sh 2-20
Using HourlySUChanMeasurReport.sh 2-20

CHAPTER 3 **Managing RMS Using the GUI**

Monitoring Host Machine Resources 3-1
General Tab 3-2
Discovery Tab 3-3
VM Stats Tab 3-3
Memory Tab 3-4
Processors Tab 3-5
Storage Tab 3-5
Network Tab 3-5
TCA Config Tab 3-5
Creating a New Host Resource TCA 3-5
Configuring the HRStats Cleanup Task 3-6
Monitoring Network Element Connectivity 3-7
Viewing Network Element Connectivity 3-7
Customizing CINR Threshold Levels 3-10
Work Queues 3-11
Configuring Auxiliary Servers 3-12
Configuring an FTP Server 3-12
Add FTP Server 3-12
Delete FTP Server 3-12
Configuring TFTP Server 3-13
Add TFTP Server 3-13
Configure SMTP Server 3-13
Add SMTP Server 3-13
Update RMS License File 3-14
High Availability Configuration 3-15
Troubleshooting Tools 3-15
Host Reachable 3-16
Trace Route 3-16
Pass Through 3-18

CHAPTER 4 **Monitoring and Maintaining the RMS Host Machine**

Determining a Monitoring and Maintenance Plan 4-1
Monitoring and Maintaining the Hard Disk Drive 4-4
Checking Hard Disk Capacity 4-5
Removing Backup Files 4-6
Monitoring Disk I/O 4-7
Defragmenting the Disk Drive 4-11
Monitoring CPU Usage 4-12
Monitoring Core Saturation 4-15

Configuring and Using sar 4-16
Memory Management 4-17
Monitoring RMS Processes 4-17
Monitoring RMS Server Heap Settings 4-20
Modifying RMS Server Heap Settings 4-20
Monitoring Swap Space 4-22
UDP Buffer Overflow 4-23
Monitoring UDP Buffers 4-23
Modifying RMS SNMP Configuration Properties 4-24
Port Status 4-26
Verifying Port Status 4-27
Configuring Port Status 4-28

CHAPTER 5 **Routine Maintenance Tasks**

Working with System Tasks 5-1
Editing System Tasks 5-1
Configuring the Audit Task 5-3
Configuring the Cleanup Tasks 5-3
Configuring the Reporting Tasks 5-4
Viewing Task Details 5-5
Renaming a System Task 5-5
Duplicating a System Task 5-5
Working with Custom Tasks 5-5
Scheduling a Task 5-6
Configuring the Auto Discovery Task 5-8
Configuring the DbCleanup Task 5-8
Configuring the PM Export Task 5-9
Configuring NE Config Backup Task 5-10
Reviewing Task Log Files 5-12

CHAPTER 6 **Maintaining the RMS Database**

Overview 6-1
DbBackup Task 6-2
Running the DbBackup Task 6-2
Running DbBackup from the Command Line 6-3
Windows Server 2003 6-3
Solaris 10 6-4
Database Backup for High Availability via the Command Line 6-4
DbCleanup Task 6-5
Running DbCleanup 6-5

Database Usage Statistics for High Availability 6-6
DbRestore Task 6-7
Windows Server 2003 6-8
Solaris 10 6-9
Starting and Stopping the Database Service 6-10
Solaris 10 6-10
Windows Server 2003 6-11
Verifying Database Integrity 6-12
Windows Server 2003 6-12
Solaris 10 6-13
Optimizing the RMS Database Size 6-14
Verifying the Size of the Database 6-14
Windows Server 2003 6-15
Solaris10 6-15
Resizing the Database 6-15

CHAPTER 7 **Monitoring the Provisioning Server**

Generating Provisioning Reports 7-1
Running the PSCleanup Task 7-2
Reviewing Provisioning Server Log Files 7-2

CHAPTER 8 **High Availability Maintenance**

Failover of the RMS Server 8-1
Verifying Database Synchronization 8-1
Forcing Failover Through the RMS GUI 8-3
Completion of RMS Server Failover 8-4
High Availability Master Host Machine States 8-6
High Availability Maintenance Tasks 8-8
Performing a Database Dump from the Master to the Slave 8-8
Verifying Completion of a Database Backup (Dump) 8-10
Configuring the High Availability Cleanup Task 8-11
Synchronizing MyReports between Master and Slave 8-11
Removing the Virtual Interface from the Failover Machine 8-12
Modifying the Master for Extended Slave Downtime 8-13
Disabling Log Files 8-13
Enabling Log Files 8-14

APPENDIX A **SNMP Traps and Threshold Crossing Alerts A-1**

TCA Parameters for RedMAX Devices A-1
TCA Parameters for RedCONNEX Devices A-4

TCA Parameters for Point-to-Point (PTP) Devices A-5
TCA Parameters for Point-to-Multipoint (PMP) Devices A-7
TCA Parameters for Point-to-Multipoint (PMP) Connection States A-8
SNMP Traps for RedMAX Devices A-9
SNMP Traps for RedCONNEX/RedACCESS Devices A-12
SNMP Agent Alarms A-13

APPENDIX B **Synchronization Traps B-1**
RedMAX Synchronization Traps B-1
Viewing Network Event Logs B-2
Viewing Network Element Event Logs B-2
Interpreting RedMAX Synchronization Traps B-2

CHAPTER C **Installing a Hot-Swappable Hard Disk Drive C-1**
Backing Up the Installation C-2
Cleaning Up the High Availability Systems C-3
Shutting Down the Provisioning Service on the Slave Host Machine C-3
Shutting Down the RMS Services on the Slave Host Machine C-4
Installing and Formatting the New Hard Disk C-4
Adding RMS Files to the New Hard Disk Drive C-5
Start RMS Services on the Slave Host Machine C-6
Start the Provisioning Service on Slave Host Machine C-7
Verify High Availability Functionality C-7
Shutting Down the Provisioning Service on the Slave Host Machine C-8
Shutting Down the RMS Services on the Slave Host Machine C-8
Installing and Formatting the New Hard Disk C-9
Adding RMS Files to the New Hard Disk Drive C-10
Start RMS Services on Slave Host Machine C-11
Start Provisioning Services on Slave Host Machine C-11
Verify High Availability Functionality C-12

APPENDIX D **Configuring System Logging with Log4j.xml D-1**

INDEX

1

About This Guide

Overview

The Redline Management Suite (RMS) is a sophisticated element management solution that provides broadband network operators the ability to deploy, control, monitor and upgrade their Redline components network-wide using an intuitive user-friendly graphical interface. The Redline Management Suite acts as a gateway between your Redline equipment and your OSS/BSS, enabling full automation within your network.

RMS is a high performance, scalable Java-based application implemented using a MySQL database. Multiple operators at separate locations can use a secure, Web-based interface to access and manage broadband wireless access (BWA) network devices.

The RMS collects and stores statistical information about the managed wireless equipment. The inventory, statistical, and event information stored in the MySQL database is available to external management platforms to facilitate service provisioning, inventory, and maintenance functions through a CORBA-based northbound interface (NBI).

About This Document

Scope

This document provides detailed instructions for monitoring and maintaining the various components of your Redline Management Suite installation.

This document is intended for network administrators. It covers basic administration and maintenance procedures for RMS and its optional features.Basic maintenance of the RMS host machine is also covered.

Note Unless indicated otherwise the procedures throughout this guide require that you are either logged into an RMS client session and have the correct user account privileges to access network equipment, perform upgrades and other inventory-related functions; or are logged in at the command line with root or administrative user privileges.

Using RMS to manage and monitor your Redline network requires a comprehensive understanding of data networking. You should also have extensive experience with configuration and operation of Redline's broadband, fixed, wireless access products as part of a WiMAX network or backhaul infrastructure. Additional background knowledge should include computer operating systems and data networking theory.

Comprehensive operator and administrator training programs are available from Redline Communications. Please contact support@redlinecommunications.com for detailed information.

Document Conventions

The following document conventions are used throughout this guide.

Table 1-1 Document Conventions

Format	Description
Bold	Commands, titles, and keywords displayed in the RMS or the OS graphical user interface are displayed in bold.
<Italic> *User Guide:*	Arguments requiring an operator specified value are displayed in italics with angle brackets. Referenced Redline documents are also displayed in italics.
Ellipsis ...	An ellipsis before or after example text indicates there is more content either before or after the examples that are displayed. The entire contents of the file are not displayed.
[ ]	Elements in square brackets are optional.
{ x | y | z }	Required alternative command options are grouped in braces and separated by vertical bars.
[x | y | z]	Optional command options are grouped in square brackets and separated by vertical bars.
Navigation Steps >	Successive navigational steps are indicated with an arrow. You will need to progress through the navigational path using your mouse or keyboard shortcuts.
Ctrl+click	Hold down the Ctrl key and click on line items, to select multiple items in tables or drop-down menus.

The following naming conventions are used to denote customer-specific information.

Table 1-2 Document Conventions for Customer-Specific Information

Name	Description
<rms_host>	Name or IP address of the host machine, on which RMS is installed.
<rms_install_dir>	Directory that contains RMS.
<root password>	Password for the Solaris root account.

Supported Redline Equipment

The following Redline wireless equipment is supported:

Table 1-3 Supported RedMAX Equipment

Product	Supported Software Versions (IDs)		
RedMAX AN100U	2.0	2.1	2.2
RedMAX AN100UX	2.0	2.1	2.2
RedMAX SUO/SUI	2.0	2.1	2.2

Table 1-4 Other Supported Equipment

Product	Supported Software Versions (IDs)		
AN80i PTP	3.00	3.11	4.00
AN80i PMP	11.11	11.20	12.02
AN50e PTP	1.36		
AN50e PMP	3.03		
AN30e PTP	1.14		

Note The RMS license file (featureLicense.xml) must contain all of the equipment in your network, which RMS will manage.

Contact support@redlinecommunications.com for details on obtaining or updating your RMS license.

Redline communications

2

System Administration

This chapter provides instructions for RMS system administration. Common procedures such as starting and stopping the system as well as modifying the configuration are covered here.

Additional system administration tasks that can be performed through the RMS GUI client are provided in Chapter 3, “Managing RMS Using the GUI”.

Starting and Stopping Services

RMS

It may be necessary to stop the system in order to perform some types of administration and maintenance, including installing patches or updating the license. These changes should only take place in a maintenance window.

Configuration changes to the RMS via the GUI System Properties or modification of the configuration file, ServerConfiguration.xml requires that you stop and restart RMS in order for the changes to take effect. This also applies to changes to the Provisioning Server through the GUI System Properties or modification of the PS configuration file (ProvServerConfiguration.xml).

Most maintenance can be performed with the system running. The procedure below includes the Provisioning Server and MySQL database services. If the Provisioning Server is not installed, disregard references to provserverdX_Y_Z_nnn and EMS_provServerdX_Y_Z_nnn.

Note Provisioning Server option: the PS must be started after the RMS services are running.
High Availability option: Start the master and then the slave system. In a high availability configuration, to avoid possible database corruption, do not stop or start RMS if a database backup (dump) is in progress. Contact Redline customer support

immediately for support if the RMS or provisioning services are shut down during a database dump. See “Verifying Database Synchronization” on page 8-1. for information on determining whether a database dump is in progress.

Stop RMS Services

Solaris

Step 1 Log into the workstation that is hosting the RMS server, as the root user.

```
rlogin <rms_host> -l root
<root password>
```

Step 2 Verify the status of the RMS services. The grep command is used to filter the returned services and only display the services matching the pattern:

```
svcs -a | grep site
```

Step 3 You can also use the –x option to display an explanation of the current state of a service, where X_Y_Z_nnn is the RMS version. For example:

```
svcs -x redmaxemsdX_Y_Z_nnn
```

Step 4 To stop the services, disable them as follows:

```
svcadm disable -s
svc:/site/provserverdX_Y_Z_nnn:provserverdX_Y_Z_nnn
svcadm disable -s svc:/site/redmaxemsdX_Y_Z_nnn:redmaxemsdX_Y_Z_nnn
svcadm disable -s svc:/site/namingServicedX_Y_Z_nnn:
namingServicedX_Y_Z_nnn
svcadm disable -s svc:/site/notifsvcX_Y_Z_nnn:notifsvcX_Y_Z_nnn
svcadm disable -s svc:/site/mysqldX_Y_Z_nnn:mysqldX_Y_Z_nnn
```

Use the –s option to ensure the command does not return until the service instance is offline or svcadm determines it is not possible for the service to be disabled.

Step 5 Monitor the status of RMS services using one of the following commands, where X_Y is the RMS version:

```
svcs –av | grep site
svcs -av | grep X_Y
ps –ef | grep X_Y
```

Windows Server 2003

Step 1 As the administrative user, navigate to the Service dialog box on the RMS server.

Start > **Control Panel** > **Administrative Tools** > **Services**.

Step 2 Maximize the dialog box to see the full names of the listed services.

Step 3 Locate the RMS services, listed above and check their status. The status should be **Started** for all three (or four) services.

Step 4 If any of the following services are running, stop them in the following order:

- EMS_provServerdX_Y_Z_nnn
- EMS_RedMAXEMSX_Y_Z_nnn
- EMS_namingServicedX_Y_Z_nnn
- EMS_notifSvcX_Y_Z_nnn
- EMS_RMS_DBX_Y_Z_nnn

Step 5 Select the services that you want to stop and right-click to display the available options. Click on **Stop** to stop the selected service.

Start RMS Services

Solaris

Step 1 To start the services from any installed version, enable the services in the following order:

```
svcadm enable -s svc:/site/mysqldX_Y_Z_nnn:mysqldX_Y_Z_nnn
svcadm enable -s svc:/site/notifsvcX_Y_Z_nnn:notifsvcX_Y_Z_nnn
svcadm enable -s svc:/site/namingServicedX_Y_Z_nnn:
namingServicedX_Y_Z_nnn
svcadm enable -s svc:/site/redmaxemsdX_Y_Z_nnn:redmaxemsdX_Y_Z_nnn
svcadm enable -s
svc:/site/provserverdX_Y_Z_nnn:provserverdX_Y_Z_nnn
```

Use the –s option to ensure the command does not return until the service instance is offline or svcadm determines it is not possible for the service to be disabled.

Step 2 Monitor the status of RMS services using one of the following commands, where X_Y is the RMS version:

```
svcs –av | grep site
svcs -av | grep X_Y
ps –ef | grep X_Y
```

Windows 2003 Server

Step 1 As the administrative user, navigate to the **Service** dialog box on the RMS server.

Start > **Control Panel** > **Administrative Tools** > **Services**.

Step 2 Maximize the dialog box to see the full names of the listed services.

Step 3 Locate the RMS services, listed above and check their status. The status should be **Stopped** for all three (or four) services.

Step 4 Select the services that you want to start and right-click to display the available options. Click on **Start** to activate the selected service.Start the services in the following order:

- EMS_RMS_DBX_Y_Z_nnn
- EMS_notifSvcX_Y_Z_nnn
- EMS_namingServicedX_Y_Z_nnn
- EMS_RedMAXEMSX_Y_Z_nnn

- EMS_provServerdX_Y_Z_nnn

Stand-Alone Provisioning Server

The Provisioning Server downloads existing subscriber profiles and managed elements to its cache using the CORBA NBI to retrieve pre-provisioned subscribers from RMS. A CORBA notification service is used to synchronize subscriber profiles between the RMS Server and Provisioning Server.

Solaris10

Step 1 Log into the workstation hosting the RMS server, as the root user.

```
rlogin <rms_host> –l root
<root password>
```

Step 2 Confirm the path of the RMS services:

```
svcs –a | grep site
```

Step 3 To start the provisioning server service:

```
svcadm enable –s
svc:/site/EMS_provServerdX_Y_Z_nnn:EMS_provServerdX_Y_Z_nnn
```

Step 4 To stop the provisioning server service:

```
svcadm disable –s
svc:/site/EMS_provServerdX_Y_Z_nnn:EMS_provServerdX_Y_Z_nnn
```

Windows Server 2003

Step 1 As the administrative user, navigate to the **Service** dialog box on the RMS server.

Start > **Control Panel** > **Administrative Tools** > **Services**.

Step 2 Maximize the dialog box to see the full names of the listed services.

Step 3 If RMS is already running you only need to start the provisioning service. Select the service, EMS_provServerdX_Y_Z_nnn and right-click to display the available options.

Step 4 To start the provisioning server service, click on **Start** to start the selected service.

Step 5 To stop the provisioning server service, right-select **Stop** to stop the selected service.

Step 6 Monitor the services in the dialog box to verify that they have stopped.

Modify RMS and Provisioning Server Configuration

Most RMS and the Provisioning Server configuration parameters are managed through the **System Properties** page on the RMS GUI. In special cases it may be necessary to modify the XML configuration files.

Table 2-1 Modifying RMS and Provisioning Server Configuration

Configuration File	Reference
ServerConfiguration.xml	*Redline Management Suite Installation Guide*, Chapter 7.
ProvServerConfiguration.xml	*Redline Management Suite Installation Guide*, Chapter 7.
VirtualIfConfig.xml	*Redline Management Suite Installation Guide*, Chapter 6.

If these files are modified, the RMS services must be stopped and restarted for these changes to take effect.

Modifying NE Upgrade Configuration

The following tables list the configuration parameters that are used when RMS upgrades NE firmware. In general, the default settings will provide the best results. If necessary, you can update these settings in the ServerConfiguration.xml file.

Step 1 Run the ServiceConfigMgr utility as outlined in the *Redline Management Suite Installation Guide*.

Step 2 Edit the values, listed in Table 2-3, for your specific application.

Step 3 After saving your changes, stop and restart the RMS services in order to activate your changes. See “Most maintenance can be performed with the system running. The procedure below includes the Provisioning Server and MySQL database services. If the Provisioning Server is not installed, disregard references to provserverdX_Y_Z_nnn and EMS_provServerdX_Y_Z_nnn.” on page 2-1.

Table 2-2 Service Definition for UpgradeService in ServerConfiguration.xml

Name	UpgradeService
Service Qualifier Class	com.redline.nms.server.upgrade.UpgradeService
Service State	activate
Server Type	EMS

Table 2-3 Service Definition Properties for UpgradeService

Name	Type	Description	Value
switchAndSynch CompletionTimeout	IntegerType	Time interval to complete check, switch and synchronization. Default value is 30 minutes. Value in milliseconds (ms) = 30 min * 60 seconds/min * 1000 ms/s =1800000 ms.	1800000

Table 2-3 Service Definition Properties for UpgradeService (continued)

Name	Type	Description	Value
downloadExecution Timeout	IntegerType	Time interval to check download execution. Default value is 20 minutes. Value in milliseconds (ms) = 20 min * 60 seconds/min * 1000 ms/s =1200000 ms.	1200000
downloadCompletion Timeout	IntegerType	Time interval to check download completion Default value is 30 minutes (1800000 ms).	1800000
downloadStartedTimeout	IntegerType	Time interval since download started to be triggered for a large number of NEs Default value is 3 hours. Value in milliseconds (ms) = 3 hours * 60 min/hr * 60 seconds/min * 1000 ms/s =10800000 msec.	10800000
downloadTriggeredLast Time	IntegerType	Time interval since download was last triggered for a specific NE. Default value is 90 seconds. Value in milliseconds (ms) = 90 seconds/min * 1000 ms/s =90000 ms.	90000
stopTriggerDownload Time	IntegerType	Time interval, after which download ceases to be triggered for a specific NE, if upgrade has not successful Default value is 10 minutes. Value in milliseconds (ms) = 10 min * 60 seconds/min * 1000 ms/s =600000 ms.	600000
synchronizeDelay Time	IntegerType	Delay time before triggering synchronization, after NEs were rebooted, allowing the network to resume contact with the NE after it was rebooted. Default value is 5 minutes. Value in milliseconds (ms) = 5 min * 60 seconds/min * 1000 ms/s =300000 ms.	300000

Configuring the Auto-Reset Behaviour

When RMS has used available virtual memory, it needs to be reset. Ideally, you can monitor memory usage to ensure that RMS does not reach this threshold by clearing any unwanted processes that are using virtual memory or by adding more memory to the host machine. The exact value that causes the system to restart is configurable. The default value is 97%, which indicates that when there is less than 3% of the total available virtual memory, RMS will stop and restart all of its services in order to free up virtual memory.

Step 1 Run the ServiceConfigMgr utility as outlined in the *Redline Management Suite Installation Guide*.

Step 2 Edit the values, listed in Table 2-5, for your specific application.

Step 3 After saving your changes, stop and restart the RMS services in order for your changes to take effect. See “Most maintenance can be performed with the system running. The procedure below includes the Provisioning Server and MySQL database services. If the Provisioning Server is not installed, disregard references to provserverdX_Y_Z_nnn and EMS_provServerdX_Y_Z_nnn.” on page 2-1.

Table 2-4 Service Definition for SystemManager in ServerConfiguration.xml

Name	SystemManager
Service Qualifier Class	com.redline.nms.server.system.SystemManagerService
Service State	activate
Server Type	EMS

Table 2-5 Service Definition Properties for SystemManager

Name	Type	Description	Value
MemoryThreshold	IntegerType	Minimum amount of allowed free JVM memory as a percentage of the total allocated JVM memory. JVM will exit if this threshold is crossed. Range 1-20%.	3%
MemoryThresholdCheck Period	IntegerType	This value defines how often the JVM memory check is performed, in msec. Range 10000-60000 msec.	60000 msec

Modifying the Diagnostic Polling Interval

You must enable diagnostic polling on a sector controller for diagnostic performance reports. This value needs to be greater than or equal to the time required to connect to the specified devices and collect the required data.

Note If you have a large number of sector controllers (>1000) it is possible that too many diagnostic sessions will cause the RMS sever to respond very slowly and eventually become inaccessible.

Diagnostics is expensive in terms of memory usage. If you notice degradation in performance when diagnostics polling in enabled, you may want to consider reducing the amount of diagnostic data being collected. You will need to select fewer sector controllers to be polled at any one time. You can also increase the polling interval. i.e. 120 seconds instead of 60 seconds.

Step 1 Login into the GUI client on the RMS host machine.

Step 2 Navigate to **Config** > **System** > **System Properties**. The **System Properties** table is displayed.

Step 3 Select **PMPollingManager**. The properties associated with the selected service are now displayed below the table. If the selected service is running on more than one host machine, then all instances are displayed. This will be the case in a high availability system.

Note Changing system properties in a high availability system may require a maintenance window.

Step 4 Right-click any one of the properties and select **Edit**, to modify its value. The rows located below the table will now be write-accessible.

Table 2-6 Diagnostic Polling Interval Configuration Parameters

Service	Parameter	Description
PMPollingManager	pollFastTimeoutSecs	Fast polling timeout for interface and channel measurement statistics for sector controllers, in seconds.
	pollTimeoutMins	Slow polling timeout for interface and channel measurement statistics for sector controllers, in minutes.

Step 5 Enter the new value for pollFastTimeoutSecs, in the **Property Value** box and click **Submit** to save your changes.

If you are updating a high availability system, you will need to make these changes on the master only. These changes will be copied to the slave machine during the regular database replication process.

Note DO NOT change any property values unless you have verified the change with your system administrator and your network administrator. Changing property values may adversely affect your RMS system.

Step 6 Stop and restart all of the RMS services, including the Provisioning Server, as outlined in the “Most maintenance can be performed with the system running. The procedure below includes the Provisioning Server and MySQL database services. If the Provisioning Server is not installed, disregard references to provserverdX_Y_Z_nnn and EMS_provServerdX_Y_Z_nnn.” on page 2-1.

Step 7 Login to the RMS GUI and verify the modified functionality.

Java Memory Management

Java memory management utilizes the concept of a garbage collector, which is the entity responsible for traversing the heap and freeing space that is being consumed by unreferenced objects.

If your system is configured for high availability, then during failover, an extended garbage collection duration may result in unacceptable delays. Additionally, failover could actually be triggered by these extended garbage collection times.

In both HA and non-HA systems you may notice that the Web Client freezes momentarily and this may be due to extended garbage collection duration. You will likely only encounter this issue in a medium or large network.

Note Unless you have specific issues, you do not need to change the garbage collection parameters.

To reduce the impact of system delays due to garbage collection, use the following approach to collect statistics and characterize your system and then tune the garbage collection behavior of your system.

Note The following procedures are for experienced system administrators. If you are not familiar with Java garbage collection, please contact support@redlinecommunications.com for more information.

If you need to contact support@redlinecommunications.com, please have a copy of the log file, generated below and the jstat output available.

Refer to the Sun Java documentation for detailed information on tuning garbage collection.

Collecting Garbage Collection Statistics from RMS

Use the following procedure to log garbage collection activity to a file in the log directory This will allow you to collect and analyze system metrics for the garbage collection process.

Windows Server 2003

Step 1 As the administrative user, open a console window on the RMS server.

Start > **Programs** > **Accessories** > **Command Prompt**

Step 2 In the console window enter this command:

```
cd c:\
cd <rms_install_dir>\
```

Step 3 Stop redmaxemsdX_Y_Z_nnn service:

```
sc stop redmaxemsdX_Y_Z_nnn
```

Step 4 Delete the redmaxemsdX_Y_Z_nnn service:

```
sc delete redmaxemsdX_Y_Z_nnn
```

Step 5 Navigate to the following directory and make a backup copy of RMSServer.lax:

```
cd <rms_install_dir>\
copy RMSServer.lax RMSServer.backup
```

Step 6 Open RMSServer.lax in Windows Notepad, or any other text editor and add the following information:

```
-XX:+PrintGC -XX:+PrintGCDetails -XX:+PrintGCTimeStamps
-Xloggc:"<rms_install_dir>\logs\gc.log"
```

Where: %ROOT% is replaced with your actual RMS installation directory.

Example 2-1 Contents of RMSServer.lax for GC Statistics Collection

```
lax.command.line.args=C:\\RMS\\RedMAXEMSX_Y_Z_nnn\\bin\\RMSService -install
EMS_RedMAXEMSX_Y_Z_nnn C:\\RMS\\RedMAXEMSX_Y_Z_nnn\\jre\\bin\\server\\jvm.dll
-Xbootclasspath/p:C:\\RMS\\RedMAXEMSX_Y_Z_nnn\\lib\\OB.jar -server -Xmx1G -Xms1G
-XX:PermSize=128M -XX:MaxPermSize=128M -Xss192k -XX:NewSize=256M
-XX:MaxNewSize=256M -XX:+UseTLAB -XX:+AggressiveOpts
-XX:+PrintGC -XX:+PrintGCDetails -XX:+PrintGCTimeStamps
-Xloggc:"C:\RMS\RedMAXEMSX_Y_Z_nnn\logs\gc.log"
 -Djava.security.manager -Djava.security.policy=policy
-Djava.security.auth.login.config=C:\\RMS\\RedMAXEMSX_Y_Z_nnn\\conf\\login.conf
-Dcatalina.home=C:\\RMS\\RedMAXEMSX_Y_Z_nnn
-Djava.library.path=C:\\RMS\\RedMAXEMSX_Y_Z_nnn\\lib\\
```

Step 7 Save your changes and then execute RMSServer.exe to re-create the RMS service:

```
cd <rms_install_dir>\
RMSServer.exe
```

Step 8 Re-start redmaxemsdX_Y_Z_nnn service:

```
sc start redmaxemsdX_Y_Z_nnn
```

Step 9 Use the run command to launch regedit to verify your changes:

Start > **Run** > **regedit**

Step 10 Select HKEY_LOCAL_MACHINE and enter CTRL F and enter the key name, redmaxemsdX_Y_Z_nnn.

Step 11 Once you have located the service entry, select ‘Parameters’. You should see all services parameters including your updates.

Solaris 10

Step 1 In a high availability system, you need to determine which RMS server was the master, that is failing over.

Step 2 Log into this machine as the root user.

```
rlogin <rms_host> –l root
<root password>
```

Step 3 Stop the RMS services as outlined in “Starting and Stopping Services” on page 2-1.

Step 4 Navigate to the following directory:

```
cd <rms_install_dir>/bin
```

Step 5 Locate the file named redmaxServer.sh and create a backup copy of this file.

```
cp redmaxServer.sh redmaxServer.bak
```

Step 6 Open the file in your standard text editor and uncomment the line containing the string GC_LOG_OPS.

```
vi redmaxServer.sh
/GC_LOG_OPS
```

Step 7 Save your changes and close the file.

```
Esc (key)
:wq
```

Step 8 Restart the RMS services as outlined in “Starting and Stopping Services” on page 2-1.

Garbage collection activity will now be logged to a file called gc.log, located in the log directory.

Step 9 Navigate to the log directory and open the file.

```
cd <rms_install_dir>/logs
more gc.log
```

The contents of the file will be similar to the example shown below:

Example 2-2 Contents of Garbage Collection Log File

```
11.794: [GC 11.794: [ParNew: 78720K->4061K(88512K), 0.0181015 secs]
78720K->4061K(252352K), 0.0182057 secs] [Times: user=0.03 sys=0.00, real=0.02 secs]
13.352: [GC [1 CMS-initial-mark: 0K(163840K)] 40272K(252352K), 0.0230387 secs]
[Times: user=0.01 sys=0.00, real=0.03 secs]
13.375: [CMS-concurrent-mark-start]
13.438: [CMS-concurrent-mark: 0.061/0.062 secs] [Times: user=0.06 sys=0.02,
real=0.05 secs]
13.438: [CMS-concurrent-preclean-start]
13.455: [CMS-concurrent-preclean: 0.013/0.018 secs] [Times: user=0.03 sys=0.01,
real=0.03 secs]
13.455: [CMS-concurrent-abortable-preclean-start]
15.917: [GC 15.917: [ParNew: 82781K->9636K(88512K), 0.0246959 secs]
82781K->9636K(252352K), 0.0248289 secs] [Times: user=0.03 sys=0.03, real=0.03 secs]
18.421: [CMS-concurrent-abortable-preclean: 0.226/4.966 secs] [Times: user=3.17
sys=0.47, real=4.95 secs]
18.422: [GC[YG occupancy: 50243 K (88512 K)]18.422: [Rescan (parallel) , 0.0273563
secs]18.449: [weak refs processing, 0.0002866 secs] [1 CMS-remark: 0K(163840K)]
50243K(252352K), 0.0277789 secs] [Times: user=0.03 sys=0.02, real=0.03 secs]
18.450: [CMS-concurrent-sweep-start]
18.450: [CMS-concurrent-sweep: 0.000/0.000 secs] [Times: user=0.00 sys=0.00,
real=0.00 secs]
18.450: [CMS-concurrent-reset-start]
```

Collecting System Statistics Using the jstat Utility

If you are familiar with Java and have access to a full JDK, you can use the jstat utility to generate garbage collection statistical reports:

The full JDK must be installed and your environment must be configured correctly.

Note JRE 1.6.0_16 is installed with RMS. If you have another version of the JDK on your system, you must ensure that it does not interfere with RMS.

Step 1 From your JDK, use the following command to dump garbage collection statistics to the command line at 5-second intervals:

```
jstat -gcutil <vmId/pid> 5s
```

Where: -gcutil Provides a summary of garbage collection statistics

<vmId> This the virtual machine identifier. This is a string indicating the target JVM. The general syntax is [protocol:][//]lvmid[@hostname[:port]/servername]

<pid> This is the Java process ID. You need to specify the vmID or the pid.

5s This is the sampling interval in seconds.

Example 2-3 Contents of Garbage Collection Log File

```
S0      S1      E       O      P       YGC  YGCT    FGC  FGCT    GCT
 12.44  0.00   27.20    9.49   96.70   78   0.176   5    0.495   0.672
 12.44  0.00   62.16    9.49   96.70   78   0.176   5    0.495   0.672
 12.44  0.00   83.97    9.49   96.70   78   0.176   5    0.495   0.672
  0.00  7.74    0.00    9.51   96.70   79   0.177   5    0.495   0.673
  0.00  7.74   23.37    9.51   96.70   79   0.177   5    0.495   0.673
  0.00  7.74   43.82    9.51   96.70   79   0.177   5    0.495   0.673
  0.00  7.74   58.11    9.51   96.71   79   0.177   5    0.495   0.673
...
```

Where: S0 Survivor space 0 utilization as a percentage of the space's current capacity.

S1 Survivor space 1 utilization as a percentage of the space's current capacity.

E Eden space utilization as a percentage of the space's current capacity.

O Old space utilization as a percentage of the space's current capacity.

P Permanent space utilization as a percentage of the space's current capacity.

YGC Number of young generation GC events.

YGCT Young generation garbage collection time.

FGC Number of full GC events.

FGCT Full garbage collection time.

GCT Total garbage collection time.

The output of this example shows that a young generation collection occurred between the 3rd and 4th sample. The collection took 0.001 seconds and promoted objects from the eden space (E) to the old space (O), resulting in an increase of old space utilization from 9.49% to 9.51%. Before the collection, the survivor space was 12.44% utilized, but after this collection it is only 7.74% utilized.

You will need to monitor the FGCT and the GCT as well as the as well as percent area utilization to determine if you need to tune garbage collection for your system.

Tuning Garbage Collection Behaviour

The RMS garbage collection behavior can be tuned based on analysis of collected system metrics. It can take several days of execution with new settings to determine if there is a positive effect on the overall garbage collection intervals. After each tuning, you must collect system statistics as outlined above.

Garbage collection statistics can be monitored using the following menu item: **config->system-> host resources -> vmstats**. Refer to “Monitoring and Maintaining the RMS Host Machine”Chapter 4

Windows Server 2003

The following procedure modifies the RMS configuration files and re-creates the service, redmaxemsdX_Y_Z_nnn:

Step 1 As the administrative user, open a console window on the RMS server.

Start > **Programs** > **Accessories** > **Command Prompt**

Step 2 In the console window enter this command:

```
cd c:\
cd <rms_install_dir>\
```

Step 3 Stop redmaxemsdX_Y_Z_nnn service:

```
sc stop redmaxemsdX_Y_Z_nnn
```

Step 4 Delete the redmaxemsdX_Y_Z_nnn service:

```
sc delete redmaxemsdX_Y_Z_nnn
```

Step 5 Navigate to the following directory and make a backup copy of RMSServer.lax:

```
cd <rms_install_dir>\
copy RMSServer.lax RMSServer.backup
```

Step 6 Open RMSServer.lax in Windows Notepad, or any other text editor and modify the VM parameters. The actual values will be specific to your system. See Table 2-7 on page 2-16 for details of the configuration parameters.

Example 2-4 Contents of RMSServer.lax for Configuring Garbage Collection

```
lax.command.line.args=C:\\RMS\\redmaxemsdX_Y_Z_nnn\\bin\\RMSService
-install redmaxemsdX_Y_Z_nnn
C:\\RMS\\redmaxemsdX_Y_Z_nnn\\jre\\bin\\server\\jvm.dll
-Xbootclasspath/p:C:\\RMS\\redmaxemsdX_Y_Z_nnn\\lib\\OB.jar -server
-Xmx256M -Xms256M -XX:PermSize=128M -XX:MaxPermSize=128M -Xss192k
-XX:+UseParNewGC -XX:+UseConcMarkSweepGC -XX:+CMSIncrementalMode
-XX:+CMSParallelRemarkEnabled -XX:ParallelGCThreads=1
-XX:MaxGCPauseMillis=10000 -XX:NewSize=96M -XX:MaxNewSize=96M
-XX:CMSInitiatingOccupancyFraction=50
-XX:+UseCMSInitiatingOccupancyOnly -XX:-CMSIncrementalPacing
-XX:CMSIncrementalDutyCycle=20 -XX:CMSIncrementalSafetyFactor=20
-XX:+DisableExplicitGC -XX:+UseTLAB -XX:+AggressiveOpts
-Djava.security.manager -Djava.security.policy=policy
-Djava.security.auth.login.config=C:\\RMS\\redmaxemsdX_Y_Z_nnn\\con
f\\login.conf -Dcatalina.home=C:\\RMS\\redmaxemsdX_Y_Z_nnn
-Djava.library.path=C:\\RMS\\redmaxemsdX_Y_Z_nnn\\lib\\ ...
```

Step 7 Save your changes and then execute RMSServer.exe to re-create the RMS service:

```
cd <rms_install_dir>\
RMSServer.exe
```

Step 8 Re-start redmaxemsdX_Y_Z_nnn service:

```
sc start redmaxemsdX_Y_Z_nnn
```

Step 9 Use the run command to launch regedit to verify your changes:

Start > **Run** > **regedit**

Step 10 Select HKEY_LOCAL_MACHINE and enter CTRL F and enter the key name, redmaxemsdX_Y_Z_nnn.

Step 11 Once you have located the service entry, select ‘Parameters’. You should see all services parameters including your updates.

Step 12 You will need to re-evaluate the results by collecting new system statistics using the procedures outlined in “Collecting Garbage Collection Statistics from RMS” on page 2-9.

It may require several iterations to obtain the desired results. How you adjust the values each time will depend on what is observed in the gc log and jstat results.

Solaris 10

The garbage collection behavior is configured in the redmaxServer.sh with the following variables that are used to control how often incremental garbage collection is performed.

Table 2-7 Garbage Collection Tuning Variables

Parameter	Description/Example
MaxTenuringThreshold=5	This variable sets the 95% NewSize available to every NewGC cycle, and reduces the pause time by not evaluating tenured objects. Set this variable to 0 if you want to promote all live objects to old generation.
NewSize=128M MaxNewSize=128M	The parameters NewSize and MaxNewSize bound the young generation size from below and above. Setting these to the same value fixes the young generation, in the same way as setting -Xms and -Xmx to the same value fixes the total heap size. This is useful for tuning the young generation at a finer granularity than the integral multiples allowed by NewRatio. NewSize specifies a small young to tenured ratio as a heap size is much larger. You can also set -XX:SurvivorRatio=to a large value such as 128M. In order to minimize the duration of a full garbage collection, you can reduce the new generation size, resulting in more frequent garbage collection cycles but with each collection taking less time to complete. The following parameters marked with a variable depend on size of deployment: -server -Xmx@HEAP_SIZE@ -Xms@HEAP_SIZE@ -XX:PermSize=@PERM_SIZE@ -XX:MaxPermSize=@PERM_SIZE@ -Xss256k \ -XX:+UseParNewGC -XX:+UseConcMarkSweepGC -XX:+UseTLAB -XX:+CMSIncrementalMode \ -XX:ParallelGCThreads=20 -XX:+AggressiveOpts -XX:NewSize=@MIN_MAX_YGEN_HSIZE@ -XX:MaxNewSize=@MIN_MAX_YGEN_HSIZE@ \ -XX:+CMSIncrementalPacing -XX:CMSIncrementalDutyCycleMin=0 -XX:CMSIncrementalDutyCycle=10 -XX:MaxTenuringThreshold=0 \ -XX:SurvivorRatio=256 -XX:CMSInitiatingOccupancyFraction=50 \
CMSIncrementalPacing=enabled	Enables automatic pacing. The incremental mode duty cycle is automatically adjusted based on statistics collected while the JVM is running.

Table 2-7 Garbage Collection Tuning Variables (continued)

Parameter	Description/Example
CMSInitiatingOccupancy Fraction=50	Based on recent history, the concurrent collector maintains estimates of the time remaining before the tenured generation will be exhausted and of the time needed for a concurrent collection cycle. Based on these dynamic estimates, a concurrent collection cycle will be started with the aim of completing the collection cycle before the tenured generation is exhausted. These estimates are padded for safety, since the concurrent mode failure can be very costly. A concurrent collection will also start if the occupancy of the tenured generation exceeds an initiating occupancy, a percentage of the tenured generation. The default value of this initiating occupancy threshold is approximately 92%, but the value can be manually updated using this parameter. [1] The value of this parameter must be set to an integral percentage (0-100) of the tenured generation size.
CMSIncrementalDuty Cycle =50	The percentage (0-100) of time between minor collections that the concurrent collector is allowed to run. If CMSIncrementalPacing is enabled, then this is the initial value.
CMSIncrementalSafety Factor=10	The percentage (0-100) used to add conservatism when computing the duty cycle.

1. http://java.sun.com/javase/technologies/hotspot/gc/gc_tuning_6.html

Where: Boolean options are turned on with -XX:+<option> and turned off with -XX:-<option>.

Numeric options are set with -XX:<option>=<number>. Numbers can include 'm' or 'M' for megabytes, 'k' or 'K' for kilobytes, and 'g' or 'G' for gigabytes (for example, 32k is the same as 32768).

String options are set with -XX:<option>=<string>, are usually used to specify a file, a path, or a list of commands

These values can be updated in redmaxServer.sh in your Solaris environment.

Step 1 Log into this machine as the root user.

```
rlogin <rms_host> –l root
<root password>
```

Step 2 Stop the RMS services as outlined in “Starting and Stopping Services” on page 2-1.

Step 3 Navigate to the following directory:

```
cd <rms_install_dir>/bin
```

Step 4 Locate the file named redmaxServer.sh and create a backup copy of this file.

```
cp redmaxServer.sh redmaxServer.bak
```

Step 5 Open redmaxServer.sh in your standard text editor and modify the VM parameters.

Example 2-5 Contents of redmaxServer.sh for Configuring Garbage Collection

```
...
$ $JAVA -D64 -enableassertions -Xbootclasspath/p:"$ROOT/lib/OB.jar"
${GC_LOG_OPS} ${DEBUG_OPS} ${JPROFILER_OPS} \
> -server -Xmx256M -Xms256M -XX:PermSize=128M -XX:MaxPermSize=128M
-Xss256k \
> -XX:+UseParNewGC -XX:+UseConcMarkSweepGC -XX:+UseTLAB
-XX:+CMSIncrementalMode \
> -XX:MaxGCPauseMillis=10000 -XX:ParallelGCThreads=8
-XX:+AggressiveOpts -XX:NewSize=96M -XX:MaxNewSize=96M \
> -XX:+CMSIncrementalPacing -XX:CMSIncrementalDutyCycleMin=0
-XX:CMSIncrementalDutyCycle=10 -XX:MaxTenuringThreshold=0 \
> -XX:SurvivorRatio=256 -XX:CMSInitiatingOccupancyFraction=50
-XX:+DisableExplicitGC \
> ${JCONSOLE_OPS} \
> -Djava.security.auth.login.config=$ROOT/conf/login.conf \
> -Djava.library.path=$libpath \
> -Dorg.omg.CORBA.ORBClass=com.ooc.CORBA.ORB \
> -Dorg.omg.CORBA.ORBSingletonClass=com.ooc.CORBA.ORBSingleton \
...
```

Step 6 Save your changes and then re-start the redmaxemsdX_Y_Z_nnn service, as outlined in “Starting and Stopping Services” on page 2-1.

Step 7 If you change these values, you will need to re-evaluate the results by collecting new system statistics using the procedures outlined in “Collecting Garbage Collection Statistics from RMS” on page 2-9.

It may require several iterations to obtain the desired results. How you adjust the values each time will depend on what is observed in the gc log and jstat results.

Generating Reports at the Command Line

Three scripts have been provided that allow you to generate reports at the command line to report on system connection statistics:

- HourlySUChanMeasurReport.sh
- HourlySUBandwidthReport.sh
- HourlySCBandwidthReport.sh

These scripts collect data from the database for post processing. These scripts are currently only available in the Solaris environment.

When you no longer require these reports, you will need to manually remove them from your file system. These reports are not saved in the database and are not included in MyReports, nor are they removed by any of the database cleanup utilities.

If you are running on an HA system, these reports will only be accessible on the host machine on which they were generated. They are not replicated as part of any failover process.

Solaris 10

Step 1 Log into the RMS host machine as the root user.

```
rlogin <rms_host> –l root
<root password>
```

Step 2 Navigate to the following directory:

```
cd /<rms_install_dir>/bin
```

Step 3 Run the scripts as follows:

```
HourlySUChanMeasurReport.sh -m 00:09:02:01:6C:11 2009-04-10
```

Where:

-q	Indicates that you do not want to generate the report; only show the corresponding SQL query for the collection of required data.
-p	Indicates the number of significant digits to show after the decimal point in the report. The default value is 1.
-M <scMac>	Indicates that you only want to generate a report for one sector controller as indicated by the specified MAC Address in the format: xx:xx:xx:xx:xx:xx
-m <suMac>	Indicates that you only want to generate a report for one subscriber unit as indicated by the specified MAC Address in the format: xx:xx:xx:xx:xx:xx. This option is not available for HourlySCBandwidthReport.sh
-N <scName>	Indicates that you only want to generate a report for one sector controller as indicated by the specified name.
-n <suName>	Indicates that you only want to generate a report for one subscriber unit as indicated by the specified name. This option is not available for HourlySCBandwidthReport.sh

-y	Indicates that you want to report on yesterday's activity.
<date>	You must specify a date in the format YYYY-MM-DD.

Note Arguments for all of the above scripts are case-sensitive.

Step 4 The output reports will be saved in the following directory:

`/<rms_install_dir>/data`

Step 5 You can import these reports into any text editor or spreadsheet application for review. Refer to the *Redline Management Suite User Guide* for detailed information on working with RMS report data in Microsoft Excel.

Using HourlySCBandwidthReport.sh

You can view the data for a specific sector controller by specifying the device MAC address or device name. You can also view the SQL query used to generate the report using the -q option.

```
HourlySCBandwidthReport.sh -p2 -N "Sector_18" 2009-04-12
```

This report will generate an hourly bandwidth report for the sector controller named Sector_18 for April 12, 2009. The data will contain 2 decimal places and will be output to a file named HourlySCBandwidthReport-2009-04-12.csv.

Using HourlySUChanMeasurReport.sh

The following report will generate the query required to create an hourly channel measurement report. The data contain 2 decimal places and the query will be written to the file named query.txt.

```
HourlySUChanMeasurReport.sh -q -p2 > query.txt
```

3

Managing RMS Using the GUI

RMS provides a number of tools to configure and monitor your system directly through the client GUI to facilitate system management.

You can monitor the host resources and configure threshold crossing alerts (TCAs) for specific system resource.

You can also configure and monitor network link health through the client GUI.

RMS application re-configuration, previously managed through various XML files is now also managed through the GUI. System stop and restart is still required and this must be performed at the command line as outlined in “Starting and Stopping Services” on page 2-1.

Monitoring Host Machine Resources

You can now view various resources on selected host machines through the RMS GUI. RMS communicates directly with the OS via SNMP and JMX and reports on system resources.

Note You need to configure an SNMP agent on each RMS host machine, to support the Host-Resources MIB. Refer to the *Redline Management Suite Installation Guide* for detailed instructions.

JMX requires no additional configuration, other than specifying the port during installation. This port is used by the JMX agent that is embedded in JVMs that are configured and started automatically by RMS.

To view these pages:

Step 1 Navigate to **Config** > **System** > **Host Resources**. The **Host Resources** page is displayed.

Step 2 If RMS is installed over multiple machines (i.e. in a high availability configuration) you must first select the host machine from the **Host** drop down list. RMS will then update the statistics accordingly and display the results for the selected host machine.

Other host machines, such as those hosting a Provisioning Server or a high availability master or slave, must be configured during installation in order to be seen from drop down menu.

Step 3 Click on the various tabs for detailed information on specific resources.

General Tab

General Information about the host machine platform is provided on the **General** tab.

Table 3-1 System Information

Parameter	Description
Discovered IP	This is the IP address of the selected host machine. This may be the IP associated with a network interface card on the host machine. This is not the virtual IP address, if one is configured for either a Provisioning Serveror a high availability machine. RMS needs the actual IP address of the selected host machine in order to communicate with the SNMP agent, regardless of the HA state.
Discovered MAC	This is the MAC address of the selected host machine.
System Name	This is the name of the selected host machine, if a name has been configured.
System Date	This is the current date and time on the selected host machine.
System Description	This is a description of the OS, including the current patch level, if applicable.
SNMP Agent Vendor	This is the specific vendor name of the SNMP agent. Since this is third-party software that is not provided by Redline, and behavior may differ between vendors, this information is logged for troubleshooting purposes.
System Processes	This is the number of processes that are currently running on the selected host machine.
Memory Size	This is the amount of installed RAM, as reported by the host machine.

Four charts displaying resource usage are shown in the summary section on the lower part of the page.

Table 3-2 Resource Usage Charts

Chart	Description
Memory	This chart shows the percentage of RAM used over the past 24-hour period. Click on the **Memory** tab to see the detailed view.
Processors	This chart shows the percentage of available processor capacity used over the past 24-hour period. Click on the **Processors** tab to see the detailed view.

Table 3-2 Resource Usage Charts

Chart	Description
Storage	This chart shows the percentage of hard disk space that was used over the past 24-hour period. Each colour represents a different storage device. A legend (mapping line-colour to device) is provided on the corresponding detailed view. Click on the **Storage** tab to see the detailed view.
Network	This chart shows the percentage bandwidth utilization on an interface. A legend, mapping line-colour to device, is provided on the corresponding detailed view. Click on the **Network** tab to see the detailed view.

Discovery Tab

This tab provides information on the networks and sub-networks that have been discovered by RMS. Ensure all of the required sub-networks are displayed here. If a network or sub-network does not appear in this list then you will need to update the routing on the selected host machine so that all of the required sub-networks are accessible.

This information is related to network hardware rather than network elements. Discovered network elements are listed on the RMS home page and on the **Networks** page. See “Monitoring Network Element Connectivity” on page 3-7 for more details.

VM Stats Tab

The installation wizard sets the working memory allocation (heap) to a default size based on your network size. You will need to increase this value as additional network elements are added to your system. The actual value is dependent on your operating system and installed hardware.

Note The heap value is associated with the host machine operating system and should be increased only by the system administrator. Contact support@redlinecommunications.com for detailed instructions before you attempt to modify this setting.

The three graphs, on this tab show memory usage over the past 24-hours. The following data is logged at 1-minute intervals and presented in the charts:

- RMS Heap usage is shown in the first chart.
  - Free Heap Size (MB) - This is the amount of free Heap space (green) over the specified time.
  - Used Heap Size (MB) - This is the amount of used Heap space (blue) over the specified time. The maximum threshold is also shown (red).
  - A red line indicates the maximum Heap usage. If the used Heap exceeds this value you may encounter performance issues.

- Memory used by applications other than the RMS, is shown on the second chart.
  - Free Memory (MB) - This is the amount of free memory (yellow), not allocated to the RMS Heap at the specified time.
  - Used Memory (MB) - This is the amount of used memory (orange), but not used by the RMS Heap over the specified time.
  - A red line indicates the maximum Heap usage. If the used Heap exceeds this value you may encounter performance issues.
- Garbage collection statistics are shown on the last chart. Specifically, the time spent performing specific garbage collection is displayed.
  - Garbage Collection (mSec) - Time spent in garbage collection over the specified time. The ParNew collector (purple) and ConcurrentMarkSweep (grey) are shown in the last charts.

Note If your Provisioning Server is on the same host machine, you will see two sets of three charts: the first set are for RMS; the second set are for Provisioning Server identified by <server name>:<port>.

You can compare the Used Heap and Maximum Heap values to determine if adequate free space is available.

In general, RMS and the Provisioning Server heap should be less than 80% utilized.

Note The heap size cannot exceed 1.5 GB in Windows 2003 Standard OS. The exact value of 1.5 GB depends on contiguous memory available from the OS and may vary depending on available contiguous memory. Windows 2003 Extended version and Solaris do not have this limitation.

You can only modify the heap size directly through the operating system. See “Modifying RMS Server Heap Settings” on page 4-20 for detailed instructions.

Memory Tab

The chart on the **Memory** tab shows physical and virtual memory usage over the past 24-hour period.

The percentage of total physical memory used and the percentage of total virtual memory are plotted over the same time period. The table below the chart shows the data set, which is logged at 1-minute intervals.

If you are performing network maintenance tasks during off-peak hours, you can monitor memory usage to ensure you have adequate resources.

Processors Tab

The chart on the **Processors** tab shows how your system's CPU(s) has been used over the past 24-hour period.

The percentage of total processor capacity used over the past 24-hour period is plotted for each processor. The table below the chart shows the data set, which is logged at 1-minute intervals.

You can monitor memory usage to ensure you have adequate resources. As your network expands it may be necessary to add resources. Refer to the *Redline Management Suite Installation Guide* for resource guidelines for each network size.

See “Monitoring CPU Usage” on page 4-12 for other ways to monitor CPU usage.

Storage Tab

The chart on the **Storage** tab shows how your system's hard disk space has been used over the past 24-hour period.

The percentage of hard disk capacity used over the past 24-hour period is plotted for each device.The table below the chart shows the data set, which is logged at 1-minute intervals.

You can monitor usage to ensure you have adequate resources. As your network expands it may be necessary to add resources. Refer to the *Redline Management Suite Installation Guide* for resource guidelines for each network size.

See “Monitoring and Maintaining the Hard Disk Drive” on page 4-4 for other ways to manage and monitor hard disk usage.

Network Tab

The chart on the **Networks** tab shows how your system's network interfaces have been used over the past 24-hour period. Percentage usage of the selected interface versus time, is plotted on the displayed chart.

TCA Config Tab

You can set and view threshold crossing alerts (TCA) to monitor system resources. If the monitored parameter falls below the specified threshold an alarm will be generated.

Creating a New Host Resource TCA

You can set and view threshold crossing alerts (TCA) to monitor hard disk space and memory on a selected RMS host machine. If the monitored parameter falls below the specified threshold an alarm will be generated allowing to perform the required maintenance or add the required resources, before you system is seriously impacted.

You should set the thresholds accordingly so that you allow your network administrator enough time to address the problem. In some case this may be days or weeks, if additional hardware is required or DbBackup/Cleanup of a large database is required.

Step 1 From the **Config** menu select **System > Host Resources > TCA Config** tab.

Step 2 To create a storage threshold alarm, enter the following information for the selected host machine. If the combined storage capacity falls below the specified value, then an alarm will be generated

Table 3-3 Storage Threshold Alarm Settings

Setting	Description
Threshold Percent	Specify the percentage of the total storage capacity that should generate an alarm. In general this should be 10-15% of your total storage capacity, if you have more than 10GB of total, accessible storage. You can use the same guideline for the memory TCA. You may need to adjust the value, based on your network size.
Frequency (min.)	Specify the polling frequency, in minutes. You can specify a polling interval between 5-60 minutes.
Alarm Severity	Specify the severity of the alarm that should be generated when the storage capacity falls below the threshold percent.

The alarm severity will depend on your threshold percent. If the threshold is very low and will result in data being lost, then the alarm severity should be set to critical. If you have set the threshold so that the system can run for a few days, while you obtain replacement storage, then the alarm severity could be set to minor.

Step 3 To create a memory threshold alarm, enter the required information for the selected host machine. The parameters are same as those listed above for the storage threshold.

Step 4 Click **Submit** for the TCA be created and stored in the database.

Step 5 You can now create another TCA with a higher threshold to provide a warning.

Step 6 Once you have created and submitted all of the TCAs click **Close** to return to the **Network Elements** page.

Note Storage TCAs apply to all disks, and Memory TCAs apply to all memory types.

Configuring the HRStats Cleanup Task

You will need to create a DbCleanup task that is configured to backup and remove the host resources monitoring data from your database. This task should to be run on a regular basis to keep the database from becoming unmanageable.

Step 1 Navigate to **Config** > **Admin** > **Tasks**. The **Tasks** page is displayed.

Step 2 Click the **Add** button to create a new task.

Step 3 In the **Create Task** page enter a name and select DbCleanup as the Task Type. Enter the required scheduling information.

Step 4 Click **Next**. On the **Database Cleanup** page enter the directory to which the backup file should be stored

Step 5 Select **HRStats** to archive and remove host resources statistical data.

Step 6 Enter the **Window Interval**. The **Window Interval** is the period prior to the cleanup operation for which database records will be kept.

For example, setting the Window Interval to 3 months will result in the removal of all diagnostic data except for the last 3 months prior to the cleanup operation. The 3-month period does not include the current month. If you are performing the cleanup on July 14, and specify 3 months as the interval, then April, May, June and the first 14 days of July will be retained.

Step 7 Click **Save** to create the task and save it in the database.

Step 8 Your task will now appear in the **Task** page. You can right-click on it and select **View** to verify your configuration.

Monitoring Network Element Connectivity

You can view the status of your network elements from the **Networks** page. On this page RMS reports the number of devices that have been discovered. Devices are reported by device type. RMS also calculates the connectivity state for each device and reports on the number of devices with good, adequate or poor connectivity.

Viewing Network Element Connectivity

Navigate to the **Networks** page, by clicking the **Networks** button on the **Quick Menu** bar.

The following information is provided:

Table 3-4 Summary Count of Discovered Network Elements

Parameter	Description.
Total Discovered Network Elements	
Sector Controller Count	This is the number of sector controllers that have been discovered in the network.
Subscriber Unit	This is the number of subscriber units that have been discovered in the network
Discovered Network Elements by Connection Status	
Equipment Type	The names of all discovered equipment types are listed here.
Discovered	This number of devices, of the specified type that have been discovered.

Table 3-4 Summary Count of Discovered Network Elements

Parameter	Description.
Connected	This number of devices, of the specified type that are currently connected.
Disconnected	This number of devices, of the specified type that are currently disconnected. Disconnected devices are reported in red.

The second table on the **Networks** page, displays information on the connection status of the subscriber units. The ratio of carrier to interference-plus-noise ratio (CINR) is used to determine the status of the link between the subscriber unit and the sector controller.

The number of indoor and outdoor subscriber units, at each connectivity level, is listed. the data is a summary of the past 24-hours.

Table 3-5 Link Health Summary

Link Health	Description
Count Normal	This is the number of devices that have good connectivity. Good connectivity is determined based on all of the following criteria being met: • The current minimum CINR value for uplink traffic is greater than or equal to the set value for UL_NORMAL_CINR. • The current minimum RSSI value for uplink traffic is greater than or equal to the set value for UL_NORMAL_RSSI. • The current minimum CINR value for downlink traffic is greater than or equal to the set value for DL_NORMAL_CINR. • The current minimum RSSI value for downlink traffic is greater than or equal to the set value for DL_NORMAL_RSSI.
Percent Normal	This is the percentage of the total number of devices that have good connectivity, as defined above.
Count Uplink Poor	This is the number of devices that have poor uplink connectivity and normal downlink connectivity. Poor uplink connectivity is determined based on one of the following criteria being met: • The current minimum CINR value for uplink traffic is less than the set value for UL_NORMAL_CINR. • OR the current minimum RSSI value for uplink traffic is less than the set value for UL_NORMAL_RSSI. These device have good downlink connectivity based on all of the following criteria being met: • The current minimum CINR value for downlink traffic is greater than or equal to the set value for DL_NORMAL_CINR. • The current minimum RSSI value for downlink traffic is greater than or equal to the set value for DL_NORMAL_RSSI.
Percent Uplink Poor	This is the percentage of the total number of devices that have poor uplink connectivity, as defined above.

Table 3-5 Link Health Summary (continued)

Link Health	Description
Count Downlink Poor	This is the number of devices that have poor downlink connectivity and normal uplink connectivity. Poor downlink connectivity is determined based on one of the following criteria being met: • The current minimum CINR value for downlink traffic is less than the set value for DL_NORMAL_CINR. • OR the current minimum RSSI value for downlink traffic is less than the set value for DL_NORMAL_RSSI. These device have good uplink connectivity based on all of the following criteria being met: • The current minimum CINR value for uplink traffic is greater than or equal to the set value for UL_NORMAL_CINR. • The current minimum RSSI value for uplink traffic is greater than or equal to the set value for UL_NORMAL_RSSI.
Percent Downlink Poor	This is the percentage of the total number of devices that have poor downlink connectivity, as defined above.
Count Uplink and Downlink Poor	This is the number of devices that have poor connectivity. Poor connectivity is determined based on the following uplink criteria: • The current maximum uplink CINR value is less than the set value for UL_NORMAL_CINR. • OR: The current maximum uplink RSSI value is less than the set value for UL_NORMAL_RSSI. Additionally, one of the following downlink criteria are being met: • The current maximum downlink CINR value is less than the set value for DL_NORMAL_CINR. • OR: The current maximum downlink RSSI value is less than the set value for DL_NORMAL_RSSI.
Percent Uplink and Downlink Poor	This is the percentage of the total number of devices that have poor connectivity, as defined above.

Note The variables used here, are described in Table 3-6 below. The actual formulas are displayed on the Legend tab, of the RedMAX Links Health report.

The charts at the bottom of the **Networks** page show the number of indoor and outdoor subscriber units that have been connected, at each connectivity level, over the past 24-hour period.

Each chart may have up to three lines plotting the number of devices with good (green), adequate (blue) and poor (red) subscriber link connectivity over time.

Customizing CINR Threshold Levels

You can customize the values that determine the good, adequate and poor link connectivity, to suit your network. These values can be accessed through the **System Properties** page as follows:

Step 1 Navigate to **Config** > **System** > **System Properties**. The **System Properties** page is displayed.

Step 2 Select the **NetworkResourceService**. The properties of the selected service are displayed below the table. There are 19 properties listed for the **NetworkResourceService**. Only four of these properties are applicable to configuring CINR threshold levels.

Step 3 These four configuration variables are listed in Table 3-6 below. Right-click the property to be modified, and select **Edit**.

Step 4 Enter the new value in the box at the very bottom of the page and click **Submit**.

Step 5 Review the new value on the **Confirm System Properties** page and then click **Confirm** to save the changes to the database.

Step 6 You must stop all of the RMS services and restart them in order for your changes to take effect. See “Starting and Stopping Services” on page 2-1. You do not need to stop the MySQL service, RMS_DB2_2_0_23.

Table 3-6 Link Health Configuration Parameters

Parameter	Description
DL_NORMAL_CINR	This is the lower CINR threshold value for traffic for subscribers with normal downlink connectivity. Values that fall below this value are defined as poor.
DL_NORMAL_RSSI	This is the lower RSSI threshold value for traffic for subscribers with normal downlink connectivity. Values that fall below this value are defined as poor.
UL_NORMAL_CINR	This is the lower CINR threshold value for traffic for subscribers with normal uplink connectivity. Values that fall below this value are defined as poor.
UL_NORMAL_RSSI	This is the lower RSSI threshold value for traffic for subscribers with normal uplink connectivity. Values that fall below this value are defined as poor.

If you change the limits of what constitutes good, adequate and poor service, then once you restart the RMS services, all of your stored data will be re-organized and displayed using the new limits.

If the link health is consistently poor, you may need to check the physical connection of the subscriber unit; for sources of interference, etc. Refer to the *RedMAX AN100U/AN100UX Administration and Maintenance Guide* for troubleshooting information.

Work Queues

You can view information about how the RMS host machine is processing network information. Monitoring the work queues will provide an indication as to whether your system has adequate resources to efficiently manage your network devices. If tasks are queued for long periods you may need to review your host machine configuration.

These values can be accessed through the **Queues** page as follows:

Step 1 Navigate to **Config** > **System** > **Queues**. The **Queues** page is displayed.

Step 2 Use the navigation buttons at the bottom of the page to view the various work queues and thread pools.

Table 3-7 Work Queue Parameters

Parameter	Description
Name	This is the name of all of the processes that run as part of normal RMS operation.
Description	This is a description of the process.
Active # of Threads	This is the number of threads that are currently active and are being processed in the queue.
Number of Threads	This is the total number of threads, currently associated with queue (active and inactive), for this process that will be running at any given time.
Maximum Allocated Number of Threads	This is the maximum number of threads allocated to the queue since the last system reset.
Maximum Configured Number of Threads	This is the maximum number of threads that are allowed to be created and associated with the queue.
Current Queued Tasks	This is the number of threads, of this process, that are currently queued. Excessive numbers of queued process threads is an indication of inadequate system resources or system configuration issues.
Total Queued Tasks	This is the number of items in the queue that need to be processed by the number of threads.This is the total number of tasks that have been queued since system startup.
Total Completed Tasks	This is the total number of tasks that have been completed since system startup?

You can sort the table by **Current Queued Tasks**, to see the tasks waiting for system resources.

You can configure the maximum number of threads for any of the listed processes; however, you should routinely, review the current queued tasks and ensure that they do not grow unbounded or reach their maximum size, if set.

Configuring Auxiliary Servers

In addition to the RMS host machines, you will need to configure and maintain other servers to support RMS.

- FTP/TFTP servers are required to store network element configuration for backup and upgrade;
- SMTP (Simple Mail Transfer Protocol) servers are required to manage email notification for reports and alarm conditions.

Configuration of other supporting servers, such as an NTP, DHCP or Provisioning Server are covered in the *Redline Management Suite Installation Guide*.

Configuring an FTP Server

Add FTP Server

The FTP server, to which you are connecting, must be configured correctly and running on the specified host. You must also ensure the host machine has enough available disk space to store the required network element binary files.

Step 1 Navigate to **Config** > **Admin** > **FTP Servers**. The **FTP Servers** page is displayed.

Step 2 FTP servers that have already been configured are listed in the table. You can modify any of these servers by right-clicking on it and selecting **Modify**.

Step 3 If you need to add a new FTP server, click **Add** and enter the following information for each server.

Table 3-8 Adding FTP Servers

Parameters	Description
FTP User	Specify the user ID to log into the FTP server.
FTP Password	Specify the password for this FTP user. This information and the user name will be used to login to the FTP server.
Retype FTP Password	Retype the FTP Password for confirmation.
FTP Address	This is the network IP address of the FTP server. Network routing must be available to this IP address in order to use this server.
Max Number of NEs	Specify the maximum number of NEs that can connect, concurrently to this FTP server.

Step 4 Click **Add** to add your FTP server to the list. Repeat this step to add any other FTP servers.

Delete FTP Server

You can delete servers from the list as required:

Step 1 Navigate to **Config** > **Admin** > **FTP Servers**. The **FTP Servers** page is displayed.

Step 2 Select the server to be deleted, from the list. Right-click and selecting **Delete**.

Step 3 Click **Confirm** to verify the delete operation

Configuring TFTP Server

Add TFTP Server

The TFTP server, to which you are connecting, must also be configured correctly and be running on the specified host. You must also ensure the host machine has enough available disk space to store the required network element configuration files.

Step 1 Navigate to **Config** > **Admin** > **TFTP Servers**. The **TFTP Servers** page is displayed.

Step 2 TFTP servers that have already been configured are listed in the table. You can modify any of these server by right-clicking on it and selecting **Modify**.

Step 3 If you need to add a new TFTP server, click **Add** and enter the following information for each server.

Table 3-9 Adding a TFTP Servers

Parameters	Description
Server Address	The IP address of the TFTP server being added/modified.
Server Port	Specify the TFTP server port number; to which RMS should connect. This is usually port 69.
Server Folder	Specify the full path to the base directory of the TFTP server.
Server Description	A brief description of the TFTP server (optional). If more than one server is to be configured, you should specify a clear description for each server.

Step 4 Click **Add** to add your TFTP server to the list. Repeat this step to add any other TFTP servers.

Configure SMTP Server

Add SMTP Server

You add an SMTP server to RMS so that you can send reports or alarm notification, via email

Step 1 Navigate to **Config** > **Admin** > **Messaging Servers**. The **Messaging Servers** page is displayed.

Step 2 Messaging servers that have already been configured are listed in the table. You can modify any of these servers by right-clicking on it and selecting **Modify**.

Step 3 If you want to add a new messaging servers, click **Add** and enter the following information for each server.

Table 3-10 Adding a SMTP Servers

Parameters	Description
Server Name	Specify the name of the messaging server. This is required to log onto the server. When setting the server name, do not use any special characters. (i.e. / \ *, : ; = +? | < > & % ' ")
Server Type	Specify the type of message server to be created. Currently, only SMTP is supported.
Server Port	Specify the messaging server port number; to which RMS should connect. This is usually port 25.
Server Description	A brief description of the SMTP server (optional). If more than one server is to be configured, you should specify a clear description for each server.
Default	Enable this check box if you want this messaging server to be the default, to which all messages from RMS, will be sent.

Step 4 Click **Add** to add your TFTP server to the list. Repeat this step to add any other messaging servers.

Update RMS License File

Replacing/reloading featureLicenses.xml requires that the RMS (and Provisioning Server if installed) services be stopped and restarted. This procedure should be performed in a maintenance window.

Step 1 Copy the new license file (featureLicenses.xml) to the following directory. If the RMS and Provisioning Server are installed on the same host, the license file must be copied to both of the following directories.

- RMS host: <*rms_install_dir*>/conf.
- Provisioning Server host: <*rms_install_dir*>/provServer/conf.

Step 2 In the RMS GUI, navigate to **Help** > **Licenses**. Click the **Reload** button on the **Licenses** page. The Confirmation page will be displayed. Click the **Reload** button to load the new license information and automatically stop and restart the RMS services. The current session is terminated and you must login to the RMS after the system has restarted.

If the Provisioning Server is installed, this service must be manually stopped and restarted. Refer to “Stand-Alone Provisioning Server” on page 2-4.

High Availability Configuration

This procedure assumes the preferred master is the currently the master.

Step 1 Copy the new license file (featureLicenses.xml) to the following directory on the master and slave systems. If the RMS and Provisioning Server are installed on the same host, the license file must be copied to both of the following directories.

- RMS host: <*rms_install_dir*>/conf.
- Provisioning Server host: <*rms_install_dir*>/provServer/conf.

Wait until the master and slave are fully synchronized, then initiate a failover from the preferred master to the slave and wait for the slave to become ‘master’.

Step 2 On the preferred master (operating as slave), navigate to **Help** > **Licenses** and click **Reload** on the **Licenses** page. When the Confirmation page is displayed, click **Reload** to automatically stop and restart the RMS services. The current session is terminated and you must login to the RMS after the system has restarted.

If the Provisioning Server is installed, this service must be manually stopped and restarted on the master Provisioning Server host. Refer to “Stand-Alone Provisioning Server” on page 2-4.

Step 3 When the preferred master has restarted, login and verify the new license features are active. Also check the Provisioning Server if installed.

Wait for the systems to synchronize, and then initiate a failover back to the preferred master and wait for preferred master to become ‘master’.

Step 4 On the slave (operating as slave), navigate to **Help** > **Licenses** and click **Reload** on the **Licenses** page. When the Confirmation page is displayed, click **Reload** to automatically stop and restart the RMS services. The current session is terminated and you must login to the RMS after the system has restarted.

If the Provisioning Server is installed, this service must be manually stopped and restarted on the slave Provisioning Server host. Refer to “Stand-Alone Provisioning Server” on page 2-4.

Step 5 When the preferred master has restarted, login and verify the new license features are active. Also check the Provisioning Server if installed.

Troubleshooting Tools

RMS provides some tools that allow you troubleshoot connectivity issues from the GUI client. RMS provides the following network connectivity tools:

- Host Reachable - Allows you to send packets with retry and timeout parameters to a desired destination address for testing whether a particular host is reachable.
- Trace Route - Allows you to see the route that packets take to reach a desired host/destination. You can specify parameters controlling timeout and maximum number of hops to follow.

- Pass-through - Launches a new Web browser window and attempts to connect to a sector controller's 'native' Web interface via HTTP.

Host Reachable

This tool allows you to test whether or not another network device can be reached, through the existing network routing, from RMS.

Step 1 Navigate to **Tools** > **Host Reachable**.

Step 2 On the **Host Reachable** page, enter the following information:

Table 3-11 Host Reachable Configuration Parameters

Parameters	Description
IP Address	Specify the IP address of the destination network element or host machine.
Retries	Specify the number of retries before stopping the connection attempt.
Timeout	Specify the elapsed time, in seconds, to wait before RMS will stop the connection attempt.

Step 3 Click **Submit** to ping the destination network element or host machine. The results are displayed at the bottom of the page:

Table 3-12 Host Reachable Results

Parameters	Description
Checking Reachability For	This is the IP address which was tested for connectivity.
Statistics For	This is the IP address on which the results are based.
Packets Sent	This is the number of packets sent, to verify connectivity.
Packets Received	This is the number of packets received at the destination address, to verify connectivity.
Packets Lost	This is the number of packets lost. Lost packets indicate a lack of connectivity.
Approximate Response Time	This is the application amount of elapsed time to either verify connectivity or fail the attempt.

Trace Route

This tool allows you to determine the route taken by packets across an IP network to reach another network device from RMS.

Trace route is implemented by increasing the "time-to-live" value of each successive batch of packets sent. The first three packets that are sent have a time-to-live (TTL) value of one (indicating that they are not forwarded by the next router and make only a single hop). The next three packets have a TTL value of 2, and so on. When a packet passes through a host, the host decrements the TTL value by one, and forwards the packet to the next host.

When a packet with a TTL of one reaches a host, the host discards the packet and sends a notification packet back to the sender. The trace route utility uses these returning packets to produce a list of hosts that the packets have traversed en route to the destination.

Note IP does not guarantee that all the packets take the same route each time.

Step 1 Navigate to **Tools** > **Trace Route**.

Step 2 On the **Trace Route** page, enter the following information:

Table 3-13 Trace Route Configuration Parameters

Parameters	Description
IP Address	Specify the IP address of the destination network element or host machine.
Maximum Hops	Specify the maximum number of hops that the trace should follow before it stops.
Timeout	Specify the elapsed time, in seconds, to wait before RMS will stop the trace attempt.
Resolve Domain Names	If this option is checked, the Trace Route attempts to resolve the domain names of each IP address encountered along the route.

Step 3 Click **Trace** to trace the route to the destination network element or host machine. The results are displayed at the bottom of the page:

Table 3-14 Trace Route Results

Parameters	Description
Hop #	This is the list of segments that comprise the complete route between RMS and the destination network element or host machine,
ms(one)	The three timestamp values returned for each host along the path are the delay (latency) values in milliseconds (ms) for each packet in the batch. If a packet does not return within the expected timeout window, an asterisk is displayed.
ms(two)	
ms(three)	
IP Address	This is the IP address of the device containing the endpoint of the segment.
Domain Name	This is the domain name containing the endpoint of the segment, if it can be determined.
Report	Any relevant trace status messages are displayed here.

Pass Through

This operation allows you to connect directly to the network element's web-interface, passing through RMS. In order to use this feature, you must have connectivity between the target network element and the host machine that is running the RMS browser.

Note The AN30e and the AN50e do not support the Mozilla FireFox™ web browser. If you need to access either of these devices directly using the pass through feature, you must be logged into RMS using Internet Explorer®.

Step 1 Click the **NE** button on the **Quick Menu** bar, then select a sector controller, right-click and selecting **Details**.

Step 2 Select the network element of interest. Right-click and select **Passthrough > HTTP**.

Step 3 A new browser window opens, in which you will be prompted to enter the user name and password to access the device. Once you have gained access to the device's client interface, you can control it directly, independently of RMS.

Refer to the documentation provided with the specific network element to navigate the interface and verify operation.

4

Monitoring and Maintaining the RMS Host Machine

The Redline Management Suite provides a robust client/server architecture that allows you to manage and maintain your Redline equipment. In order for your RMS system to operate in an efficient and trouble-free manner, you need to monitor and maintain both the applications and the host machines on which they are running as well as any other servers that are part of your network.

In order to do this you will need to develop a routine maintenance plan. This plan will depend on many things including:

- The size and architecture of your network e.g. the number of sector controllers and registered subscriber units.
- The RMS options that you have installed e.g. high availability, Provisioning Server, performance management options.
- The number and type of transactions performed daily.
- Your server's operating system and hardware configuration.

As part of this plan you will monitor key functions of your system and then decide which maintenance tasks need to be performed and how frequently.

Determining a Monitoring and Maintenance Plan

Note Maintenance of RMS requires a comprehensive understanding of data networking computer operating systems and database operation and maintenance. You should also have extensive experience with configuration and operation of Redline's broadband, portable and mobile, wireless access products as part of a WiMAX network.

Once your system is running, you will next need to analyze your system and determine a maintenance plan.

You will need to monitor the system parameters and make your decision about how frequently you need to perform maintenance tasks based on your observations.

The following table provides general guidelines for RMS system monitoring and maintenance. You will need to modify this schedule based on your particular system parameters.

Table 4-1 RMS System Monitoring and Maintenance Plan

Parameter/Task	Description
Monthly Monitoring and Maintenance	
Starting and Stopping the Database Service	Data integrity can be compromised if any tables become corrupt. MySQL provides a utility for checking tables and repairing them should any problems be found. This task should be performed by the system administrator or the database administrator.
Running DbBackup	In order to preserve disk space and optimize database performance you should clean up your database regularly. RMS provides an automated task (DbCleanup) that removes out-dated database records from your database. These records are archived to the file system. RMS also provided a backup task that allows you to maintain regular backups of your database. This task should be run daily. See below for more details. These tasks should be performed by the system administrator or the database administrator.
Configuring the Audit Task	The network audit task allows you to remove unused service flows. This task can also be used to replace the subscriber unit name, entered on the device, with the name that is entered in RMS. This task should be performed by the RMS administrator. Refer to “Configuring the Audit Task” on page 5-3 for detailed instructions on configuring and using this task.
Weekly Monitoring and Maintenance	
Monitoring CPU Usage	You need to monitor CPU utilization. If your CPU is consistently running at full capacity or is under-utilized, you may need to review your workflow. It may also be necessary to reconfigure internal settings such as buffer size. This task should be performed by the system administrator.
Memory Management	This is the total available system memory. You will need to monitor memory utilization to avoid system memory from being used up, etc. This task should be performed by the system administrator.
Monitoring Disk I/O	This specifies the number of read/write operations per second and the number of transfers per second, for each device. This will provide a gauge of overall system activity. This task should be performed by the system administrator.

Table 4-1 RMS System Monitoring and Maintenance Plan (continued)

Parameter/Task	Description
Number of Concurrent Users	The number of concurrent users will impact performance. The actual performance impact will be determined by what the users are doing while they are logged into the system. You can disconnect inactive sessions and limit user access. These tasks should be performed by the RMS administrator. Refer to the *Redline Management Suite User Guide* for detailed information on monitoring user accounts.
Forcing Failover of the RMS Server High Availability Maintenance Tasks	If your system is configured for high availability, you need to verify high availability functionality by forcing a system failover regularly, to ensure both the master and slave systems are available and operating correctly. There are a number of parameters to be monitored if you have the high availability option installed. You also need to clean up outdated high availability data from database. RMS also provides a task to backup your generated reports on the slave system. This task should be performed by the system administrator with the aid of the RMS administrator.
Monitoring the Provisioning Server	There are a number of parameters to be monitored if you have the Provisioning Server installed, such as Provisioning Server DHCP request success, failure rates and response times, provisioning/un-provisioning rates and response times. This task should be performed by the RMS administrator. Refer to the *Redline Management Suite Installation Guide* for detailed information on configuring the Provisioning Server. Refer to the *Redline Management Suite User Guide* for detailed information on generating reports.
Performance Management	The performance management option, if installed, will collect large volumes of data that need to be reviewed and managed weekly. Monitoring and cleanup may need to be done more frequently if the volume of collected data affects RMS Server performance. Additionally the collection of the data itself may impact system performance if the polling interval is very short. The PMCleanup task should be performed by the RMS administrator. Refer to the *Redline Management Suite User Guide* for detailed information on configuring and using RMS performance management tools.
UDP Buffer Overflow	Your operating system needs to be configured correctly or you may experience a loss of data or reduced performance. Data ports may overflow when a sudden increase in network traffic occurs. This task should be performed by the system administrator.

Table 4-1 RMS System Monitoring and Maintenance Plan (continued)

Parameter/Task	Description
Port Status	The RMS Server and the Provisioning Server utilize many communication ports at various levels of the operating system. You should verify port usage regularly to ensure the ports have been configured correctly and that network traffic is flowing as expected. This task should be performed by the system administrator.
Daily Monitoring and Maintenance	
Running DbBackup	It is important to backup your database regularly so that you can recover your data. RMS provides a task that can be configured to perform regularly scheduled database backups. This task should be performed by the RMS administrator. Note Execution time of DbBackup and DbCleanup depend on the size of the database. The larger the database, the longer the execution times.
Checking Hard Disk Capacity	This is the total volume of hard disk space over all disks mounted on each server. You will need to maintain a margin of available disk space so you will need to know what percentage of the total volume is already in use, on each server. This task should be performed by the system administrator.

It may be necessary to stop the system in order to perform some types of administration and maintenance, like installing patches or updating the license. Any re-configuration of RMS, via the GUI **System Properties** or modification of the configuration file, ServerConfiguration.xml requires that you stop and restart RMS in order for the changes to take effect. These changes should only take place in a maintenance window.

The maintenance procedures listed in Table 4-1 on page 4-2, do not require that RMS or the Provisioning Server be shut down. In fact, some tasks, such as monitoring CPU performance, memory usage and disk I/O usage can only be performed when the system is running.

You will need to start and stop your system in a specific order depending on which options you have installed.See “Starting and Stopping Services” for detailed instructions.

Monitoring and Maintaining the Hard Disk Drive

You need to closely monitor the capacity of your servers’ hard disk as this will impact RMS performance. You need to monitor the percentage usage and perform a cleanup when the disk reaches approximately 90% of its current partition size. The exact percentage of the total capacity, at which clean up should occur is determined by how long it takes to perform the required clean up task and how much data will be collected in that time.

You should log and chart hard disk resources. This will allow you to add resources before you observe a significant drop in performance. Once the available space falls below 10% or 5 GB on the current partition, whichever is larger, you will need to clean up the hard, disk, increase the size of the RMS partition or add additional hard disk drives.

You can also monitor hard disk (storage) resources directly through RMS as outlined in “Monitoring Host Machine Resources” on page 3-1.

Required hard disks sizes are provided in the *Redline Management Suite Installation Guide*.

You will need to monitor and maintain hard disk resources on the host machines in your system. Refer to the system resource guidelines provided in the *Redline Management Suite Installation Guide* to determine if your system meets the required standards for the amount of hard disk space required for your network.

Once you have established that the hard disk needs to be cleaned up, you will now need to determine what type of information can be archived, moved or deleted.

Once you have cleaned up the database and the file system, you can defragment the disk to improve performance and possibly provide additional free space.

The following table shows how quickly hard disk space is used for various networks:

Table 4-2 Average Hard Disk Usage

Operating System	Solaris 10 or Windows	Solaris 10		
Network Size	Entry	Small	Medium	Large
Element Count	5050	10,100	25,250	75,750
Sector Controllers	50	100	250	750
Subscriber Units	5000	10,000	25,000	75,000
Database Increase[1]	300 MB/day	600 MB/day	1.5 GB/day	4.1 GB/day

1. These values are based on the following configuration: standard polling interval of 15-minutes; diagnostic polling disabled; four service flows per subscriber.

Checking Hard Disk Capacity

Checking hard disk capacity may be a daily task and depending on usage may be required more frequently unless you are able to add resources to suit your needs.

You may want to log daily values for a few weeks and chart these results in order to determine system requirements and cleanup frequency for your system maintenance plan.

Windows Server 2003

Step 1 Open Windows Explorer and select the disk drive to be checked.

Step 2 Right-click on the disk and select **Properties**. The disk information is shown on the **General** tab.

Solaris 10

Step 1 Log into the workstation that is hosting the RMS server, as the root user.

```
rlogin <rms_host> –l root
<root password>
```

Step 2 Run the disk free command to determine the available disk space:

```
df -k
```

You can use other options to determine only free disk space (-b) or available space on unmounted devices (-F).

Removing Backup Files

In general log files and all RMS data are stored in the database. When you perform a DbBackup or a DbCleanup, the resulting archive files are stored on the file system. Files created by DbBackup are located in the backup directory within the RMS installation and have the following naming convention:

<*rms_install_dir*>/backup/backup_filename_<*date*><*time*>.sql

The DbCleanup utility will create its own directory within the RMS installation and have the following naming convention:

<*rms_install_dir*>/backup/archives/<*date*>/

For every cleaned table you will see <*tableName*> file saved in this directory. Possible table names are:

- ActiveAlarm
- AlarmHistory
- BsSsPacketCounters
- Systemstats.
- Events
- ChannelMeasurementCounters
- Logrecord
- IfxPacketCounters

The exact number of files that will be stored here depends on the details of your cleanup operation.

Unless there are specific errors or events that need to be retained, you can remove DbBackup or a DbCleanup archive files from the current partition, retaining one or two of the most recent backups, according to your network archive policy.

Windows Server 2003

Step 1 Open Windows Explorer and navigate to the location where the log files are stored.

`<rms_install_dir>\logs\task_logs`

Step 2 You can compress and move the files for later review (recommended), using your standard compression utility.

Step 3 Move the compressed file to another location to be archived.

There are several additional things you can do to free up disk space:

- Empty the Recycle Bin.
- Run the Disk Defragmentation tool. This may take some time so it is best to run this utility in a maintenance window or when system activity is low.
- Run the Disk Cleanup Wizard.
- If you have more than one partition or disk drive, select one that has sufficient disk space for temporary file storage area.

Solaris 10

Step 1 Log into the RMS host machine as the root user. Since RMS was installed as the root user, only the root user will have read/write/execute privileges for all files created by the RMS installation wizard.

```
rlogin <rms_host> –l root
<root password>
```

Step 2 Navigate to the log directory:

```
cd /<rms_install_dir>/logs/task_logs
```

Step 3 You can compress and move the files for later review (recommended).

```
tar -cvf /home/RMS_admin/logfiles_<date>.tar *.log
compress /home/RMS_admin/logfiles_<date>.tar
```

Step 4 Repeat for the other log file directories

Monitoring Disk I/O

There are many factors that impact disk performance, such as I/O, bus access, bus transfer time, seek time, rotation time, etc. Depending on your operating system, you can monitor these various aspects your hard drive performance using either third-party utilities or those provided with your operating system.

Refer to the documentation provided with your OS for detailed disk maintenance procedures.

Windows Server 2003

You can also run the perfmon utility from the command line. The perfmon utility provides a graphical view of the CPU, disk and memory usage.

A basic disk is a physical disk that contains primary partitions, extended partitions, or logical drives. Partitions and logical drives on basic disks are known as basic volumes. You can only create basic volumes on basic disks.

Step 1 As the administrative user, open a console window on the RMS host machine.

Start > **Programs** > **Accessories** > **Command Prompt**

Step 2 In the console window enter the following command:

```
perfmon
```

Step 3 The system performance monitoring console is displayed. A graph of resource usage is displayed on the right side of the console. Refer to the table located below the graph for a description of what is being monitored.

Step 4 Click on the **New Counter Set** icon, at the top of the screen, to clear the current set of counters.

Step 5 Right-click on the table and select **Add Counters** to customize perfmon to monitor disk I/O.

Step 6 In the **Add Counters** dialog box, select **PhysicalDisk** as the **Performance Object**.

Step 7 If you are using one or more partitions on a physical hard disk, then select **LogicalDisk** and select the partitions to monitor, using the **Select instances from list** radio button.

Step 8 Enable the **Select Counter from List** radio button and select the following counters to determine if the hard disk is adequate for your system:

Table 4-3 Monitoring Hard Disk Resources with perfmon

Counter	Description
%Disk Read Time	Provides disk read latency statistics.
%Disk Read Time	Provides disk write latency statistics.
Disk Reads/sec	This is the rate of read operations on the selected disk.
Disk Transfers/sec	This is the rate of read and write operations on the disk. This is a useful for total volume input/output per second (IOPS).
Disk Writes/sec	This is the rate of write operations on the selected disk.
Disk Bytes/sec	This is the rate at which bytes are transferred to or from the disk during write or read operations. This is a measure of total throughput.
Disk Read Bytes/sec	This is the rate at which bytes are transferred from the disk during read operations.
Disk Write Bytes/sec	This is the rate at which bytes are transferred to the disk during write operations.

Table 4-3 Monitoring Hard Disk Resources with perfmon (continued)

Counter	Description
Avg. Disk Bytes/Read	This is the average number of bytes transferred from the disk during read operations.
Avg. Disk Bytes/Write	This is the average number of bytes transferred to the disk during write operations.
Current Disk Queue Length	This is the number of requests outstanding on the disk at the time the performance data is collected. It also includes requests in service at the time of data collection. This is an instantaneous snapshot, not an average over the time interval. Multi-spindle disk devices can have multiple requests that are active at one time, while other concurrent requests are awaiting service. This counter might reflect a transitory high or low queue length, but if there is a sustained load on the disk drive, it is likely that this will be consistently high. Requests experience delays proportional to the length of this queue minus the number of spindles on the disk array. For good performance, this difference should average less than two.

Solaris 10

The Solaris iostat command provides statistics on the disk I/O subsystem. The iostat command has many options. The following options provide basic information on locating disk I/O bottlenecks.

Step 1 Log into the RMS host machine as the root user:

```
rlogin <rms_host> –l root
<root password>
```

Step 2 Use the iostat command during busy times to look at the I/O characteristics of your devices.

```
iostat -xd 10 5
```

Where -x This option provides the extended statistics listing.

-d, -c, -t or -tdc These options allow you to specify the device for which information is required. d-disk, c-CPU or t-terminal.

Where -x This option provides the extended statistics listing.

10 This is the interval period, in seconds between samples. In the example above, statistics will be collected at 10-second intervals.

5 This is the count of the number of times the data is output. In the example above, statistics will be collected 5 times. The output is shown below.

Example 4-1 iostat Output

```
                  extended device statistics
device   r/s    w/s   kr/s   kw/s wait actv  svc_t  %w  %b
sd0      0.0    4.7   0.0   37.3  0.0  0.1   14.1   0   3
sd1      0.0    0.0   0.0    0.0  0.0  0.0    0.0   0   0
sd3      0.0    0.0   0.0    0.0  0.0  0.0    0.0   0   0
nfs1     0.0    0.0   0.0    0.0  0.0  0.0    0.0   0   0
```

The following statistical information is provided for the selected device:

Table 4-4 iostat Output Statistics Description

Statistic	Description
device	The name of the disk.
r/s	The number of reads per second.
w/s	The number of writes per second.
kr/s	The number of kilobytes read per second.
kw/s	The number of kilobytes written per second.
wait	The average number of transactions waiting for service (the queue length).
actv	The average number of transactions actively being serviced (removed from the queue but not yet completed).

Table 4-4 iostat Output Statistics Description (continued)

Statistic	Description
%w	The percentage of time that there are transactions waiting for service (the queue is non-empty). A high disk saturation, as measured via %w, always causes some level of performance impact, since I/Os are forced to queue up. Even if the disk is not saturated now, it is useful to look at the throughput numbers and compare them to the expected maximum values to make sure that there is adequate room for unusually high activity. You can measure the maximum value directly using dd or mkfile and looking at the reported throughput. If iostat is consistently reporting %w > 5, the disk subsystem is too busy. In this case, you can set sd_max_throttle to reduce the size of the wait queue. The sd_max_throttle parameter determines how many jobs can be queued on a single device, and is set to 256 by default. Reducing sd_max_throttle is a temporary resolution only.
%b	The percent of time the disk is busy (transactions in progress). If a disk is more than 60% busy over sustained periods of time, this can indicate overuse of that resource. This statistic provides a reasonable measure for utilization of regular disk resources. The same statistic can be viewed via iostat -D in Solaris 10.

If a disk shows consistently high numbers for reads/writes along with the percentage busy (%b) of the disk is greater than 5%, and the average service time (svc_t) is greater than 30-milliseconds, then one of the following actions needs to be taken.

1. Spread the file system onto two or more disks using the disk striping feature of the volume manager/disk suite utilities.
2. Increase the system parameter values for inode cache, ufs_ninode, which is the number of inodes to be held in memory. Inodes are cached globally (for UFS), not on a per-file system basis.
3. Move the file system to another faster disk /controller or replace existing disk/controller to a faster one.

Defragmenting the Disk Drive

Fragmentation occurs over time as you save, change, or delete files. The changes that you save to a file are often stored at a location on the hard disk that is different from the original file. Additional changes are saved to even more locations. Over time, both the file and the hard disk itself become fragmented, and your computer slows down as it searches many different locations to open a file.

Disk defragmentation is the process of consolidating fragmented files on the hard disk.

Windows Server 2003

The Windows disk defragmentation utility may be running on a schedule, but you can also defragment your hard disk manually.

Step 1 Open Windows Explorer and navigate to **Start** > **Settings** > **Performance & Maintenance** > **Disk Defragmenter**.

Step 2 If you are prompted for an administrator password or confirmation, enter the password or provide the confirmation.

Step 3 Click **Defragment Now**

The disk defragmenter may take from several minutes to a few hours to finish, depending on the size and degree of fragmentation of your hard disk. You can still use your computer during the defragmentation process.

Note If defragmentation is being performed on a schedule, consider scheduling the task to run during periods of minimal system activity.

Solaris 10

The file system check utility (fsck) audits and interactively repairs inconsistent file system conditions. If the file system is inconsistent, the default action for each correction is to wait for the user to respond yes or no. If the user does not have write permission, the file system check utility defaults to “no action”. Some corrective actions may result in loss of data. The amount and severity of data loss can be determined from the diagnostic output.

Step 1 Log into the RMS host machine as the root user:

```
rlogin <rms_host> –l root
<root password>
```

Step 2 Perform a file system check (fsck) on the selected partition. With no options you will be prompted at each inconsistency.

```
fsck –y /dev/rdsk/c0t3d0s1
```

Where –y Answers yes to each query and proceeds with the check.

/dev/rdsk/c0t3d0s1 Specifies the device to check.

Monitoring CPU Usage

Excessive CPU usage (usage rates consistently near 100%) may cause your system to become unresponsive either intermittently or continuously. Monitoring CPU utilization is also important for performance and capacity planning.

Refer to the system resource guidelines provided in the *Redline Management Suite Installation Guide* to determine if your system meets the required standards for the type of processor(s) required for your network.

You can monitor CPU usage and troubleshoot processes that are using excessive cycles using the utilities provided with your operating system.You can also review the CPU usage through the RMS GUI. See “Monitoring Host Machine Resources” on page 3-1.

A CPU bottleneck can sometimes look like a processor or hard disk limitation. If your system does not have enough physical memory, the processor spends substantial time paging. Before adding or upgrading your processors or hard disks, you should monitor the server memory usage. For more information about monitoring memory, see “Memory Management” on page 4-17.

Windows Server 2003

To monitor CPU usage on your Windows platform, use the following procedure:

Note The Windows System Idle Process is supposed to have a high CPU usage rate at idle. This process accounts for unused system time. If your system is responsive and the System Idle Process CPU usage is high, then you do not have a CPU usage issue.

Step 1 Press **Ctrl**+**Alt**+**Del** to display the Task Manager.

Step 2 Select the **Task Manager** button.

Step 3 Click on the **Performance** tab, to monitor CPU usage. The total number of running processes is shown here. You can click on the **Processes** tab, to see a listing of the processes and usage statistics by process.

Note Do not end processes unless you are sure of their functionality.

You can also run the perfmon utility from the command line. The perfmon utility provides a graphical view of the CPU, disk and memory usage.

Step 4 As the administrative user, open a console window on the RMS server.

Start > **Programs** > **Accessories** > **Command Prompt**

Step 5 In the console window enter the following command:

```
perfmon
```

Step 6 The system performance monitoring console is displayed. A graph of resource usage is displayed on the right side of the console. Refer to the table below the graph for a description of what is being monitored.

Step 7 Click on the **New Counter Set** icon, at the top of the screen, to clear the current set of counters.

Step 8 Right-click on the table and select **Add Counters** to customize perfmon to monitor your system.

Step 9 In the **Add Counters** dialog box, select Processor as the **Performance Object**.

Step 10 Enable the **Select Counter from List** radio button and select the following counters to determine if the processor is adequate for your system:

Table 4-5 Monitoring CPU Resources with perfmon

Counter	Description
System\ Processor Queue Length	This is the number of threads waiting for processor time. If this value exceeds 2 for a sustained period of time, that processor may be the system bottleneck.
Processor\ % Processor Time (Total instance)	This is the sum of processor time for each processor.
Processor\ % Processor Time	This is the percentage of the use for each processor (#0, #1, etc). On a multi-processor server, this counter can show unequal distribution of processor loads.
Processor\ % Privileged Time	This is the percentage of processor time spent in privileged mode. In the Windows Server 2003 operating system, only privileged mode code has direct access to hardware and to all memory in the system. Application threads can be only be switched to privileged mode to run operating system services.
Processor\ % User Time	This is the percentage of processor time spent in user mode. User mode is the processor mode in which application services run.
Process\ % Processor Time	This is the percentage of processor time attributed to each processor, either for a particular process or for the total for all processes.

Solaris 10

To monitor CPU usage on your Solaris 10 platform, use the following procedure:

Step 1 Log into the workstation that is hosting RMS, as the root user:

```
rlogin <rms_host> –l <RMS_admin>
<password>
```

Step 2 Use the following command to obtain kernel statistics on CPU usage.

```
mpstat 10 5
```

Where: 10 This is the period, in seconds between samples. In the example above, statistics will be collected at 10-second intervals.

5 This is the number of times the data is collected. In the example above, statistics will be collected 5 times. The output is shown below.

Example 4-2 mpstat Output

CPU	minf	mjf	xcal	intr	ithr	csw	icsw	migr	smtx	srw	syscl	usr	sys	wt	idl
0	1	0	0	345	224	589	220	0	0	0	799	29	1	0	70
0	1	0	0	302	200	752	371	0	0	0	1191	99	1	0	0
0	0	0	0	341	221	767	375	0	0	0	1301	100	0	0	0
0	0	0	0	411	256	776	378	0	0	0	1313	99	1	0	0
0	0	0	0	241	738	363	378	0	0	0	1313	99	1	0	0

If the combined user time and system time are at 100 and the idle time is at 0 (column headings usr, sys, idl) this indicates that the CPU is completely consumed.

Step 3 After gathering the data from mpstat, which indicates that the system CPU resources are consumed, you will use prstat to identify which processes are consuming the CPU resources:

```
prstat -s cpu -n 10
```

Where: -s cpu Indicates to prstat to sort the output by CPU usage.

-n 10 indicates to prstat to restrict the output to the top 10 processes.

Monitoring Core Saturation

Solaris 10

Another aspect of CPU usage is core saturation (measured using corestat). Typically, you will monitor both core saturation and virtual CPU saturation simultaneously in order to determine whether an application is likely to saturate the core by using fewer application threads. In such cases, increasing workload (e.g. by increasing the number of threads) may not yield improved performance. On the other hand, most often you will see applications having high Cycles Per Instructions (CPI) and thereby not being able to saturate the core fully before achieving 100% CPU utilization.

Step 1 Run the following commands to monitor core saturation. By specifying the interval, you can use this utility to observe system activity interactively.

```
corestat –i 300
```

Where: -i 300 This is the period, in seconds between samples. In the example above, statistics will be collected at 300-second interval.

Note The corestat options may differ depending on which Sun server your are using. Refer to the man pages for specific usage details.

Configuring and Using sar

Solaris 10

System activity data can be accessed automatically, on a routine basis, using cron and two shell scripts, sa1 and sa2. There scripts are used to sample, save, and process system activity data.

Step 1 Log into the workstation that is hosting RMS, as the root user:

```
rlogin <rms_host> –l <RMS_admin>
<password>
```

Step 2 Enter the following command to edit your crontab file:

```
export EDITOR=vi
crontab -e
```

Step 3 You need to add the following lines, to begin collecting system activity data:

Example 4-3 Configuring crontab Options

```
# Collect measurements at 15-minute intervals.
0,15,30,45 * * * *   /usr/lib/sa/sa1

# Create daily reports and purge old files at 11:00PM.
* 23 * * *   /usr/lib/sa/sa2 -A"
```

Where: sa1 The shell script sa1 is used to collect and store data in the binary file /var/adm/sa/sa<*dd*>, where <*dd*> is the current day.

sa2 The shell script sa2, a variant of sar, writes a daily report in the file /var/adm/sa/sar<*dd*>. Where <*dd*> is the date.

-A Report all data including buffer activity, system calls, activity for each block device, paging activities, kernel memory allocation (KMA) activities, message activities, average queue length, unused memory pages and disk blocks, CPU utilization, status of process, i-node, file tables, system swapping and switching activity and TTY device activity

The above entries in /var/spool/cron/crontabs/sys will report activity at 15-minute intervals, and create daily reports and purge old files at 11:00PM.

Step 4 Save and exit the crontab, using the editor commands:

```
:wq
```

Step 5 You will then use the sar command to view the contents of the binary files.

```
sar -s 8:00 -e 18:00 -A
```

The sar comand extracts data from the previously created filename, specified by the -f option or, by default, from the standard system activity daily data file /var/adm/sa/sar<*dd*> for the current day <*dd*>.

Memory Management

Memory management allocates portions of memory to applications at their request, and then frees it up for reuse when it is no longer needed. The management of virtual memory is critical to performance.

If your system is slow or behaving unexpectedly, it is possible that unwanted processes are still consuming system memory or that you do not have enough memory for your current applications.

When the applications require memory resources that exceed the physical memory available on the machine, the system moves units of memory called pages to your hard disk to make memory available for an active section of the application. This is known as paging. If your system starts paging, there will be a significant drop in performance.

In UNIX-based operating systems, there are differences between paging and swapping. Paging moves individual pages to swap space on the disk; swapping is a bigger operation that moves the entire address space of a process to the hard disk swap space in one operation.

You should monitor memory usage and increase or decrease settings as required. You may want to log and chart memory use in order to see trends and allow you to add resource before you observe a significant drop in performance. You can monitor memory usage and troubleshoot processes that are using excessive resources using the utilities provided with your operating system.You can also review the memory usage through the RMS GUI. See “Monitoring Host Machine Resources” on page 3-1.

Refer to the system resource guidelines provided in the *Redline Management Suite Installation Guide* to determine if your system meets the required standards for the amount memory required for your network.

Monitoring RMS Processes

If you have observed decreased performance, you will need to determine which processes, if any are consuming memory. You will also need to determine if these processes are running normally (in which case you may need to expand your system

resources) or if they are running abnormally, in which case you will need to troubleshoot the problem. When your system is running normally, you should view the system processes to determine the normal memory usage. You may want to record this information as an operational baseline with which to compare your system in the future.

Windows Server 2003

To monitor memory usage on your Windows platform, use the following procedure:

Step 1 Press **Ctrl** +**Alt** +**Del** to display the Task Manager.

Step 2 Select the **Task Manager** button.

Step 3 Click on the **Processes** tab, to see the processes currently running. You can click on the **Mem Usage** header to sort the list by memory usage.

Solaris 10

To monitor memory usage on your Solaris 10 platform, use the following procedure:

Step 1 Log into the RMS host machine as the root user:

`rlogin <rms_host> –l <RMS_admin> <password>`

Step 2 Use the sar command to see the paging statistics for your system.

The sar command must be configured to gather the required statistics using cron. Refer to the OS documentation to configure these monitors.

```
sar -g 5 5
```

Where: -g Shows paging activity.

-d Shows disk utilization during is the period, in seconds between samples.

5 This is the period, in seconds between samples. In the example above, statistics will be collected at 5-second intervals.

5 This is the number of times the data is collected. In the example above, statistics will be collected 5 times. The output is shown below.

No options shows CPU usage. The output is shown below.

Example 4-4 Solaris sar Output

```
13:20:37   pgout/s     ppgout/s   pgfree/s    pgscan/s    %ufs_ipf
13:20:42   39.92       538.72     670.26      1147.31     0.00
```

Example 4-4 Solaris sar Output

```
13:20:47   36.60       483.80     515.40     353.80     0.00
13:20:52   40.20       508.20     632.00     1125.20    0.00
13:20:57   35.80       462.60     580.40     1141.60    0.00
13:21:02   0.00        0.00       0.00       0.00       0.00
Average    30.51       398.72     479.69     753.74     0.00
```

Step 3 Once you have determined that decreased system performance is a result of paging activity, the next step is to determine which processes have introduced the increase. Also, any time scanning occurs (as indicated by the column pgscan/s in the above example) there is a memory shortage on the system. It is not easy to identify the reasons for paging, but identifying the processes that are consuming the most virtual memory is a good start. To view the process consuming the most virtual memory, use prstat:

```
prstat -s cpu -n 10
```

Where: -s cpu Tells prstat to sort the output by CPU usage.

-n 10 Tells prstat to restrict the output to the top ten processes.

Step 4 The command vmstat reports process virtual memory statistics for processes including, virtual memory usage, disk, trap, and CPU activity.

```
vmstats 5 4
```

Where: 5 This is the period, in seconds between samples. In the example above, statistics will be collected at 5-second intervals.

4 This is the number of times the data is collected. In the example above, statistics will be collected 4 times. The output is shown below.

Example 4-5 Solaris vmstats Output

```
procs   memory       page                    disk          faults          cpu
r  b  w  swap   free  re  mf  pi  p  fr  de  sr  s0  s1  s2  s3  in   sy   cs   us  sy  id
0  0  0  11456  4120  1   41  19  1  3   0   2   0   4   0   0   48   112  130  4   14  82
0  0  1  10132  4280  0   4   44  0  0   0   0   0   23  0   0   211  230  144  3   35  62
0  0  1  10132  4616  0   0   20  0  0   0   0   0   19  0   0   150  172  146  3   33  64
0  0  1  10132  5292  0   0   9   0  0   0   0   0   21  0   0   165  105  130  1   21  78
```

Memory information is displayed as follows:

Table 4-6 Solaris vmstats Output for Memory Management

Parameter	Description
Memory (in Kbytes)	Total memory in Kbytes
swap	The amount of swap space currently available.
free	The size of the free space in the current swap allocation.
Page (in units per second)	
re	The number of page reclaims per second.
mf	The number of minor faults per second.
pi	The number of kilobytes paged in per second.
po	The number of kilobytes paged out per second.
fr	The number of kilobytes freed per second.
de	The anticipated short-term memory shortfall (kbytes) per second.
sr	The number of pages scanned by clock algorithm per second.

Monitoring RMS Server Heap Settings

The installation wizard sets the working memory allocation (heap) to a default size based on your network size. You may need to increase this value as additional network elements are added to your system and the your network size increases. The actual value is dependent on your operating system and your installed hardware.

The heap value is associated with the server operating system and should be increased only by the system administrator. Contact support@redlinecommunications.com for detailed instructions before you attempt to modify this setting.

You can monitor the working memory allocation through the RMS client as outlined in “VM Stats Tab” on page 3-3.

You can also configure the system to automatically stop and restart all of the RMS services when virtual memory is down to 97% of total available virtual memory. See “Starting and Stopping Services” on page 2-1.

Modifying RMS Server Heap Settings

You can only modify the heap size directly through the operating system, or or can edit lax file and delete and re-add the associated service.

Windows Server 2003

Step 1 Stop the RMS services as outlined in “Starting and Stopping Services” on page 2-1.

Step 2 Use the run command to launch the registry editing utility, regedit.

Start > Run > regedit

Step 3 Select **Export Registry File** to create a backup of the registry.

Step 4 Select **Find** to locate the following key:

`RedMAXEMSX_Y_Z_nnnn (HKEY_LOCAL_MACHINE)`

Where: X - Major Rel., Y - Minor Rel., Z - Maintenance Rel., nnnn - Build Number

Step 5 Expand the sub-tree for this key and select **Parameters**.

Step 6 Locate and select the parameter with the value –Xmx (usually JVM Option Number 3). This is the maximum value for the Heap.

Step 7 You can also set the value –Xms (usually JVM Option Number 2). This is the start value for the Heap.

Step 8 Right-click and choose **Modify** from the pop-up menu.

Step 9 Change the parameter setting to the recommended value and click OK.

Step 10 Restart the RMS services as outlined in “Starting and Stopping Services” on page 2-1.

Note RMS will not start if the Windows OS cannot allocate a contiguous block of memory of the size you have just specified.

Solaris 10

To modify the heap size on your Solaris platform, use the following procedure.

Step 1 Stop RMS as outlined in “Starting and Stopping Services” on page 2-1.

Step 2 On the RMS host machine, navigate to the RMS binary directory:

`cd <rms_install_dir>/bin`

Step 3 Locate the file named redmaxServer.sh and create a backup copy of this file.

`cp redmaxServer.sh redmaxServer.bak`

Step 4 Use your standard text editor to open the redmaxServer.sh file and locate the current setting (i.e., Xmx1024m). This is the maximum value for the Heap.

`vi redmaxServer.sh`

Step 5 Change this to the recommended value and save the modified redmaxServer.sh file.

`:wq`

Step 6 Restart RMS as outlined in “Starting and Stopping Services” on page 2-1.

Monitoring Swap Space

The Solaris 10 operating system will use space allocated on the hard disk as virtual memory when the system does not have enough physical memory to handle its current processes. Since many applications rely on swap space, you should know how to plan for, monitor, and add more swap space as required. In general, for both RMS and the Provisioning Server you should set the swap space to a minimum of 30% of the total amount of RAM up to maximum of twice the total amount of RAM.

Solaris 10

Step 1 Log into the RMS host machine as the root user:

```
rlogin <rms_host> –l root
<password>
```

Step 2 Use the swap command to monitor swap resources.

```
swap -s
```

The used value plus the available value equals the total swap space on the system, which includes a portion of physical memory and swap devices (or files).

You can use the total amount of available and used swap space as a way to monitor swap space usage over time. If your system's performance is good, use swap -s to see how much swap space is available.

When the performance degrades, check the amount of available swap space to see if it has decreased. You will now need to identify what changes to the system might have caused increased swap space usage.

When using this command, keep in mind that the amount of physical memory available for swap usage changes dynamically as the kernel and user processes lock down and release physical memory.

Step 3 To increase the size of the swap file, create the new swap file.

```
mkfile 100m /files/swapfile
```

Where: -100 Indicates the file size.

m Indicates this file size is in Mbytes.

/files/swapfile is the path where the file should be created and file name.

Step 4 Activate the swap file:

```
swap -a /files/swapfile
```

You must use the absolute path name to specify the swap file. The swap file is added and is available until the file system is unmounted, the system is rebooted, or the swap file is removed.

Note You cannot unmount a file system while some process or program is swapping to the swap file.

Step 5 Add an entry for the swap file to the /etc/vfstab file that specifies the full path name of the file, and designates swap as the file system type, as follows:

```
vi /etc/vfstab
```

Step 6 Copy an existing line, add it to the bottom of the file and update it as follows:

```
/files/swapfile   -       -       swap     -     no     -
```

Step 7 Verify that the swap file is added:

```
swap -a
```

Step 8 Log into the workstation that is hosting RMS, as the root user:

```
rlogin <rms_host> –l root
<password>
```

Step 9 Use the swap command to monitor swap resources:

```
swap -s
```

UDP Buffer Overflow

A buffer overflow may be caused by frequent polling for discovery or performance data collection. In this case there are more requests being sent to the UDP port than the port can handle. Requests may be dropped or the system may stop.

RMS running on Solaris 10 and Windows Server 2003 operating systems may need to be tuned in order to run performance reports. If the OS is not configured correctly, you may experience a loss of performance management data (channel parameters or data throughput due to a UDP buffer overflow.

The overflow is the result of too many UDP packets arriving to quickly for listeners on sockets to process. When this happens, you can increase the UDP buffer size or priority of the services reading the specified socket.

Monitoring UDP Buffers

Windows Server 2003

To check for a possible UDP buffer overflow, check the following.

Step 1 As the administrative user, open a console window on the RMS server.

Start > **Programs** > **Accessories** > **Command Prompt**

Step 2 In the console window enter the following command:

```
netstat -s
```

Step 3 Look for Receive Errors in the UDP Statistics for IPv4 section. For example:

```
UDP Statistics for IPv4
  Receive Errors          = 131213
```

Step 4 Repeat this command over a 5-minute interval to look for incremental changes in the counter. If the counter increases in the magnitude of thousands per minute, the operating system needs to be tuned. Contact support@redlinecommunications.com for details of the system parameters that need to be addressed.

Solaris 10

Run the following command to determine the status of the UDP buffer:

Step 1 Log into the RMS host machine as the root user:

```
rlogin <rms_host> –l root
<password>
```

Step 2 Enter this command:

```
kstat | grep udpInOverflows
```

Step 3 Repeat this command over a 5-minute interval to look for incremental changes in the counter. If the counter increases in the magnitude of thousands per minute, the operating system needs to be tuned. Contact support@redlinecommunications.com for details of the system parameters that need to be addressed.

Modifying RMS SNMP Configuration Properties

There are two RMS configuration properties that can be modified to address UDP buffer overflows.

Step 1 Run the ServiceConfigMgr utility as outlined in the *Redline Management Suite Installation Guide*.

Step 2 Edit the values, listed in Table 4-7, for your specific application.

Step 3 After saving your changes, stop and restart the RMS services in order for your changes to take effect. See “Starting and Stopping Services” on page 2-1.

Table 4-7 Service Definition for MyReportsService from ServerConfiguration.xml

Name	ProxyAgent
Service Qualifier Class	com.redline.nms.net.snmp.proxy.agent.ProxyAgentService
Service State	activate
Server Type	EMS

Table 4-8 Service Definition Properties for ProxyAgent

Name	Type	Description	Value
ReceiveBufferSize	IntegerType	This is the receive buffer size for use by the SNMP transport socket, in bytes. This value sets the size for each individual socket. Values must be based on the size of each deployment. You must have the OS level permissions to set this value. You can use the ndd command on Solaris to set the maximum value.	2097152
NumberOfSnmp Sockets	IntegerType	Specify the number of SNMP sockets to create, over which, to round-robin SNMP traffic. Values must be based on the size of each deployment.	2

Solaris 10

The parameter udp_max_buf controls how large your system send and receive buffers can be for a UDP socket. The default value is 2,097,152 bytes.

Note If this parameter is set to a very large value, your UDP socket applications can consume too much memory.

Step 1 Log into the RMS host machine as the root user:

```
rlogin <rms_host> –l root
<password>
```

Step 2 Enter the ndd command to set and then verify the value:

```
ndd /dev/udp -set udp_max_buf 2097152

ndd /dev/udp udp_max_buf
```

Note To make settings persistent, add to an rc script (/etc/init.d). See man -s4 init.d

Port Status

RMS and the Provisioning Server utilize many communication ports at various levels of the operating system. You should verify port usage regularly to ensure the ports have been configured correctly.

Confirm the RMS and MySQL services are running, and make sure the following ports are in listen mode.

Table 4-9 RMS System Port Allocation

Port #	Description
Ports Used by the RMS Services	
161 UDP	Sector controller SNMP communication port.
162 UDP	SNMP trap listening port on the RMS host machine. There are other OS-assigned ports, also used to send/receive SNMP PDUs. The exact number of ports is determined by the RMS configuration variable, NumberOfSnmpSockets. See Table 4-8 for more information.
1099	RMI port.
2222	CORBA notification port.
3306	MySQL database port.
8686	JMX port.
41111	Naming Service CORBA port.
10000	NBI CORBA port.
Operator specific	Provisioning Server port for connection to RMS.
Operator specific (80 or 8080)	Web and SOAP connection ports.
Ports Used by the Provisioning Service	
67/68 UDP	DHCP request/relay port, configured on the Provisioning Server (67) and the DHCP server (68).
1162 UDP	SNMP trap listening port on the Provisioning Server host machine. If the Provisioning Server is installed on the RMS host machine, you will need to configure a different SNMP trap listening port.
11000	Provisioning Server CORBA port.
Port Used by the TFTP Servers	
69	TCP/UDP port.
Port Used by the NTP Server	
123	TCP/UDP port (jitter buffer).
Port Used by the FTP server	
21	TCP/UDP port.

Verifying Port Status

You can use the following procedure to verify port status.

Windows Server 2003

Step 1 As the administrative user, navigate to the command line interface on the RMS server.

Start > **Programs** > **Accessories** > **Command Prompt**

Step 2 Generate a list of TCP and UDP ports on this device, that are both active and inactive:

```
netstat -ab
```

The netstat command provides the following statistics:

Table 4-10 Network Statistics on Port Usage

Statistic	Description
Proto	The name of the protocol (TCP or UDP).
Local Address	The IP address of the local computer and the port number being used. The name of the local computer that corresponds to the IP address and the name of the port is shown unless the -n parameter is specified. If the port is not yet established, the port number is shown as an asterisk (*).
Foreign Address	The IP address and port number of the remote computer to which the socket is connected. The names that corresponds to the IP address and the port are shown unless the -n parameter is specified. If the port is not yet established, the port number is shown as an asterisk (*).
State	Indicates the state of TCP connections.

Step 3 Close the command line interface by clicking on the Window's close icon, or typing exit.

Solaris 10

Step 1 Log into the RMS host machine as the root user:

```
rlogin <rms_host> –l root
<root password>
```

Step 2 Generate a list of UDP ports on this device, that are both active and inactive:

```
netstat –an
```

The output will be similar to that described in the table above, provided for Windows.

Configuring Port Status

Verify the ports are idle and then restart the services on the required ports. You may need to review the following files to ensure the port numbers have been configured correctly:

- ServerConfiguration.xml
- ProvServerConfiguration.xml

Note The RMS services should be stopped before making any changes to the port configurations.

Refer to “Starting and Stopping Services” on page 2-1 for details on starting and stopping RMS, the Provisioning Server and the database services.

Redline communications

5

Routine Maintenance Tasks

A number of pre-configured monitoring, maintenance and cleanup tasks are provided with RMS. You should schedule the maintenance utilities to run at regular intervals to maintain your database and keep your system running optimally.

You can also create custom tasks to monitor, maintain and report on your network performance.

Working with System Tasks

The following standard system tasks facilitate cleanup and monitoring of your RMS system and your host machine(s). You cannot delete the system tasks.

- Audit
- Diagnostics Cleanup

The following tasks are included if you have the corresponding option installed:

- HA Cleanup (only available in a high availability system)
- HA MyReport Synchronization (only available in a high availability system)
- PM Cleanup (only available in systems with Performance Management)
- PM Export (only available in systems with Performance Management)
- Provisioning Server (PS) Statistics Cleanup (only available in a system with a Provisioning Server)

Editing System Tasks

The following procedure provides general instructions for editing the standard system tasks. You may want to retain an original version of the system task for future reference. You can do this by first duplicating the system task, renaming it and then modifying the duplicate.

Step 1 Navigate to **Config > Admin > Tasks**. The **Tasks** page is displayed.

Step 2 Select the task that you want to schedule.Right-click and select **Edit**.

Step 3 In the **Edit Task** page enter the scheduling information:

Table 5-1 Task Scheduling Parameters

Parameter	Description
Recurrence	Specify how you want to run this task. Select **Scheduled** for automatic, scheduled execution. When this option is selected, RMS displays additional options for you to set the required schedule and frequency. You can also select **On-demand** for manual, on-demand execution.
Schedule Options	Select how often you want this task to run (Minutely, Hourly, Daily, Weekly, or Monthly). Depending on your selection, the displayed options will be updated. For example if you select daily, you will then need to select the day of week, on which to run the task. If you select monthly, you will be prompted to enter the day of the month.  Note Enter absolute times and dates instead of relative values. For example, if you want the task to run every 12 hours, enter daily and then enter 11:00AM and 11:00PM.
Scope	Select one of the three scope options. • Select **No End Date** so that the task will execute indefinitely. • Select **End After** if you want the task to end after a specified number of occurrences. You will then need to enter the number of occurrences after which the schedule will end. • Select **End on Date** if you want the task to stop running at a specified date and time. You will then need to enter the date and time after which the schedule will end.

Step 4 Click **Next** to configure the selected utility. Depending on the task that you have selected, additional configuration is required. Complete the configuration as outlined in the following sections:

- “Configuring the Audit Task” on page 5-3
- “Configuring the DbCleanup Task” on page 5-8
- “Configuring the Reporting Tasks” on page 5-4
- “Running the DbBackup Task” on page 6-2
- “Configuring the High Availability Cleanup Task” on page 8-11
- “Synchronizing MyReports between Master and Slave” on page 8-11

Step 5 Click **Save** to save any changes to the task and return to the **Tasks** page.

Step 6 If you need to run the task immediately, you can right-click the task and select **Run**.

Configuring the Audit Task

Once the subscriber unit has been provisioned you can change the name of the device to synchronize it with the name that is entered in RMS. You can also remove unused service classes or retain the services classes and list unused classes in the audit trail.

Step 1 Navigate to **Config > Admin > Tasks**.

Step 2 Select the **Audit Task,** right-click and select **Edit** to modify the task.

Step 3 In the **Edit Task** page, enter the required scheduling information. Click **Next**.

Step 4 Enter the type of audit you want to perform.

Table 5-2 Network Audit Task

Parameter	Description
Sync Subscriber System Name	Select the required operation to be performed when the name stored in RMS and the name entered on the subscriber unit do not match. • False (default) - discrepancies are logged to the audit trail; • True - discrepancies are repaired by replacing the name entered at the subscriber unit name with the RMS, provisioned subscriber name, and the results are logged to the audit trail.
Clean Unused Service Classes	Select the required operation to be performed when unused service flows are found on a subscriber unit. • False (default) - instances of unused service classes are logged to the audit trail; • True - unused service classes are removed, and the results are logged to the audit trail.

Step 5 Click **Save** to save any changes to the task and return to the **Tasks** page.

Step 6 If you need to run the task immediately, you can right-click the task and select **Run**.

Configuring the Cleanup Tasks

The PM Cleanup, PS Cleanup and Diagnostics Cleanup tasks should be scheduled to run weekly to remove excess data.

Note When scheduling these tasks remember that both PMCleanup, PS Cleanup and DiagnosticsCleanup delete records from the database permanently. You may want to run the DbBackup utility before running any of the cleanup utilities.

Step 1 Navigate to **Config** > **Admin** > **Tasks**.

Step 2 On the **Tasks** page, select the Diagnostics Cleanup, PMCleanup or PSCleanup task from the list, right-click and select **Edit**.

Step 3 Enter the required scheduling options. Select daily or weekly and then enter the exact details of when the task should run. If you have a regular maintenance window, try and run this task in that window.

Note Enter absolute times and dates instead of relative values. For example, if you want the task to run every 12 hours, enter daily and then enter 11:00AM and 11:00PM.

Step 4 Click **Next** and enter the **Window Interval**. The **Window Interval** is the period prior to the cleanup operation for which database records will be kept.

For example, setting the Window Interval to 3 months will result in the removal of all diagnostic data except for the last 3 months prior to the cleanup operation. The 3-month period does not include the current month. If you are performing the cleanup on July 14, and specify 3 months as the interval, then April, May, June and the first 14 days of July will be retained.

Step 5 Click **Save** to save any change to the task and return to the **Tasks** page.

Step 6 If you need to run either task immediately, you can right-click the task and select **Run**.

Configuring the Reporting Tasks

You can configure a task to automatically generate various types of reports.You can run these tasks and then run the cleanup tasks, to maintain optimum database performance.

Step 1 Navigate to **Config > Admin > Tasks**.

Step 2 On the **Tasks** page, select the Event Report, Performance Report or System Report task from the table, right-click and select **Edit**.

Step 3 Enter the required scheduling options. Select daily or weekly and then enter the exact details of when the task should run. If you have a regular maintenance window, try and run this task in that window.

Note Enter absolute times and dates instead of relative values. For example, if you want the task to run every 12 hours, enter daily and then enter 11:00AM and 11:00PM.

Step 4 Specify whether or not you want this report sent to you. If this feature is enabled, you then need to provide the location, where you want the report sent.

Note An SMTP server must be configured and enabled on the system for this option. See “Configure SMTP Server” on page 3-13 for details.

Step 5 Specify the details of the event, performance or system report. Refer to the *Redline Management Suite User Guide* for details.

Step 6 Click **Save** to save any changes to the task and return to the **Tasks** page.

Step 7 If you need to run the task immediately, you can right-click the task and select **Run**. The generated report will be stored in the database and can be reviewed from the **My Reports** page. Refer to the *Redline Management Suite User Guide* for details.

Viewing Task Details

You can review the configuration details of any of the system tasks.

Step 1 Navigate to **Config > Admin > Tasks**.

Step 2 On the **Tasks** page, select the task from the table, right-click and select **View**.

The configuration details are displayed below the table, on the current page. You cannot edit any parameters from this page.

Renaming a System Task

You can rename a system task to better suit your application. You can also rename a task if you make a duplicate. The duplicate task must have another name:

Step 1 Navigate to **Config > Admin > Tasks**.

Step 2 On the **Tasks** page, select the task from the table, right-click and select **Rename**.

Step 3 Enter the new name on the **Rename Task** page.

Step 4 Click **Save** to save any change to the task and return to the **Tasks** page.

Duplicating a System Task

You can duplicate a system task to make a backup version of the task. You cannot delete the system tasks; however if you have made duplicates of a tasks, the duplicate can be deleted. You can also rename your duplicate task:

Step 1 Navigate to **Config > Admin > Tasks**.

Step 2 On the **Tasks** page, select the task from the table, right-click and select **Duplicate**.

Step 3 The duplicated task is displayed on the **Tasks** page. You should rename the duplicate as outlined above.

Working with Custom Tasks

In addition to the system tasks, that are provided with RMS, you can create you own tasks to monitor and maintain your system. You can configure tasks using the following operations:

- Auto Discovery
- NE Config Backup
- DB Backup
- DB Cleanup
- PM Data Export
- Inventory Report
- Performance Report
- Events Report
- System Report

The following procedures provide general instructions for creating and scheduling custom tasks.

Scheduling a Task

The task list provides a set of templates for scheduling activities on the RMS. For each task type, you can create multiple instances, each having individual schedules and unique operating parameters.

Step 1 Navigate to **Config > Admin > Tasks**.

Step 2 Click the **Add** button to schedule a new task.

Step 3 In the **Create Task** page enter the following information:

Table 5-3 Task Scheduling Parameters

Parameter	Description
Task Name	Enter a name for your this task.
Task Type	Contains a list of functions that can be executed: Auto Discovery, NE Config Backup, DbBackup, DbCleanup, Inventory Report, Performance Report, Events Report, System Report and Audit. When editing system tasks, you cannot select other task types.
Recurrence	Specify the schedule type for this task. Tasks set for **On-demand** will be executed only when initiated by operator action. Tasks set for **Scheduled** execution can be set to execute at a specific time and repeat if desired.

Table 5-3 Task Scheduling Parameters (continued)

Parameter	Description
Schedule Options	Select how often you want this task to run (Minutely, Hourly, Daily, Weekly, or Monthly). Depending on your selection, the displayed options will be updated. For example if you select daily, you will then need to select the day of week, on which to run the task. If you select monthly, you will be prompted to enter the day of the month. Note Enter absolute times and dates instead of relative values. For example, if you want the task to run every 12 hours, enter daily and then enter 11:00AM and 11:00PM For a DbCleanup task, the following directory <*DDMMSS*> will be created in the <*rms_install_dir*>/backup
Scope	Select one of the three scope options. • Select **No End Date** so that the task will execute indefinitely. • Select **End After** if you want the task to end after a specified number of occurrences. You will then need to enter the number of occurrences after which the schedule will end. • Select **End on Date** if you want the task to stop running at a specified date and time. You will then need to enter the date and time after which the schedule will end.

Step 4 Click **Next** to configure the selected utility. Depending on the task that you have selected, additional configuration is required. Complete the configuration as outlined in the following sections:

- “Configuring the Auto Discovery Task” on page 5-8
- “Configuring the DbCleanup Task” on page 5-8
- “Configuring the PM Export Task” on page 5-9
- “Configuring NE Config Backup Task” on page 5-10

Step 5 Click **Save** to save any change to the task and return to the **Tasks** page.

Step 6 If you need to run the task immediately, you can right-click the task and select **Run**.

Step 7 Click **Save** to create the task.

Step 8 Your task will now appear in the **Task** page. You can right-click the task and select **Details** to verify your configuration.

Configuring the Auto Discovery Task

Auto Discovery provides periodic, scheduled discovery of your network using the existing discovery parameters. If new sector controllers are identified, then full inventory information is captured for installed software and the table of registered subscriber units, on each sector controller, is checked to discover new subscribers.

The Auto Discovery task can be configured with specific parameters for either scheduled or on-demand execution.

Step 1 Navigate to **Config** > **Admin** > **Tasks**. The **Tasks** page is displayed.

Step 2 Click the **Add** button to create a new task.

Step 3 In the **Create Task** page select **Auto Discovery** as the Task Type and enter a name for the task.

Step 4 Select your Recurrence preference: **Scheduled** or **On Demand**. If you select **Scheduled**, then enter the required scheduling information and click **Next**.

Step 5 On the **Select Networks** page select the networks to be included in the discovery process. If you select the root network, then all sub-networks and sector controllers will be discovered or re-discovered.

Step 6 Click **Save** to create the task and save it in the database.

Step 7 Your task will now appear in the **Task** page. You can right-click the task and select **View** to verify your configuration.

Configuring the DbCleanup Task

DbCleanup can be configured to backup and remove various types of statistical data from your database. This task should be run on a regular basis to keep the database from becoming very large and potentially affecting performance.

Step 1 Navigate to **Config** > **Admin** > **Tasks**. The **Tasks** page is displayed.

Step 2 Click the **Add** button to create a new task.

Step 3 In the **Create Task** page select DbCleanup as the Task Type and enter a name for the task.

Step 4 Select your Recurrence preference: **Scheduled** or **On Demand**. If you select **Scheduled**, then enter the required scheduling information and click **Next**.

Step 5 On the **Database Cleanup** page select the type of data to be archived and the associated options (e.g., compress backup data).

Table 5-4 DbCleanup Configuration Parameters

Parameter	Description
Directory Name	Enter a name for the directory that will be created to contain the archived data. This directory will be created under your <*rms_install_dir*>/backup directory, with a timestamp appended to the name you specify here. Data will be archived to the specified location and then removed from the database.
Type	Select the type of data to remove from the RMS database. • **pms** - Removes the specified interval of Performance Management data. • **logs** - Removes the specified interval of log files. • **events** - Removes the specified interval of event data. • **PSStats** - Removes the specified interval of Provisioning Server statistical data. • **HRStats** - Removes the specified interval of host resources statistical data. • **All** - Removes the specified interval of all the above types of data.
Window Interval	Specify the period, prior to the cleanup operation for which database records will be retained for use in reports. You specify the period in days, weeks or months.

Step 6 Click **Save** to create the task and save it in the database.

Step 7 Your task will now appear in the **Task** page. You can right-click the task and select **View** to verify your configuration.

Configuring the PM Export Task

PM Export can be configured to export performance management data to .CSV file. Once the data has been exported you can then use the PM cleanup task to cleanup the database Using PM export with PM clean up allows to maintain system performance by routinely removing performance management data from the database while retaining a copy of the data for generating your own reports.

Step 1 Navigate to **Config** > **Admin** > **Tasks**. The **Tasks** page is displayed.

Step 2 Click the **Add** button to create a new task.

Step 3 In the **Create Task** page enter a name and select **PM Data Export** as the Task Type. Enter a name for your task.

Step 4 Select your Recurrence preference: **Scheduled** or **On Demand**. If you have select **Scheduled**, then enter the required scheduling information and then click **Next**.

Step 5 Click **Next**. The **Add FTP Servers** page is displayed. FTP servers that have already been configured for export are listed in the **FTP Servers** box. If you need to add a new FTP server, enter the following information for each new server.

Table 5-5 Add FTP Servers

Parameters	Description
FTP User	Specify the user ID to log into the FTP server.
FTP Password	Specify the password for this FTP user. This information and the user name will be used to login to the FTP server.
Retype FTP Password	Retype the FTP Password for confirmation.
FTP Address	This is the network IP address of the FTP server. Network routing must be available to this IP address in order to use this server.

Step 6 Click **Add** to add your FTP server to the list. Repeat this step to add all of your FTP servers. Select and FTP server from the list. Click **Next** to continue.

Step 7 The **PM Data Export** page is displayed. Specify the destination and the scope of the data export.

Table 5-6 Define Scope of PM Export

Parameters	Description
Select an FTP Server	Select an FTP server from the drop down list. The server that you selected on the last page is displayed here.
FTP Directory	Specify a directory on the FTP server, in which to store the exported data. All of the stored performance data will be exported, so you must ensure that you have enough space on the hard disk of the selected FTP server.
Network IP Address	Specify the IP address of the network for which you want to export performance management data
Network mask Length	Specify the mask length of the network IP address for which you want to export performance management data
Use SFTP	Enable this check box if you want to use secure FTP to transfer the data. The FTP server must be configured correctly.

Step 8 Click **Save** to create the task and save it in the database.

Step 9 Your task will now appear in the **Task** page. You can right-click the task and select **View** to verify your configuration.

Configuring NE Config Backup Task

NE Config Backup can be scheduled to run at regular scheduled intervals using a task. You can configure the task with specific parameters for either scheduled or on-demand execution.

To setup an NE Config Backup task, use the following procedure:

Step 1 Navigate to **Config** > **Admin** > **Tasks**. The **Tasks** page is displayed.

Step 2 Click the **Add** button to create a new task.

Step 3 In the **Create Task** page enter a name and select **NE Config Backup** as the Task Type. Enter a name for your task.

Step 4 Select your Recurrence preference: **Scheduled** or **On Demand**. If you have select **Scheduled**, then enter the required scheduling information and then click **Next**.

Step 5 The **Add FTP Servers** page is displayed. FTP servers that have already been configured for backup are listed in the **FTP Servers** box, on the right side of page. If you need to add a new FTP server, enter the following information for each new server.

Table 5-7 Add FTP Servers

Parameters	Description
FTP User	Specify the user ID to log into the FTP server.
FTP Password	Specify the password for this FTP user. This information and the user name will be used to login to the FTP server.
Retype FTP Password	Retype the FTP Password for confirmation.
FTP Address	This is the network IP address of the FTP server. Network routing must be available to this IP address in order to use this server.
Max Number of NEs	Specify the maximum number of NEs that can connect, concurrently to this FTP server.

Step 6 Click **Add** to add your FTP server to the list. Repeat this step to add all of your FTP servers.

Step 7 Click **Next** to define the scope of the backup. A list of selected sector controllers, their active and reserved images as well as a list of the subscriber CPE network elements involved, is displayed on the **Set Selection** page. Review the list of NEs in the **Backup** table. To deselect a network element, clear the corresponding check box in the **Selection Set** column. Refer to the *Redline Management Suite User Guide* for more detailed information on configuring backup of network element configuration.

Step 8 The FTP server you selected previously is displayed here. If the selected FTP server is running, click the **Browse** button and specify the FTP directory in which to store the backup software image.

If your FTP server is not running, type the name of the software image file in the **Image Name** field. You can use any of the following variables in the file name:

- <T> is the time
- <P> is the IP Address of the network element
- <M> is the MAC Address of the network element
- <N> is the network element name

For example: mybackup<P><M>_<T>.cfg. Actual values for the IP address, MAC address and a timestamp will be substituted when the file is saved to the FTP server.

Note When setting the image name, ensure that it is consistent with the syntax requirements of the FTP server's operating system. Typically, this means you should not use spaces, or any special characters. (i.e. / \ *, : ; = +? | < > & % ' ")

Step 9 Click **Apply** to select the checked network elements for the backup operation.

Step 10 Click **Next** to proceed. The **Confirm Backup Schedule** page is displayed. Review your selection and click **Confirm**.

Step 11 Click **Save** to create the task and save it in the database.

Step 12 Your task will now appear on the **Task** page. You can right-click the task and select **Details** to verify your configuration.

Note During the NE Config backup, NE configuration is saved to the specified FTP servers only. NE configuration is not saved to the RMS database.

Reviewing Task Log Files

You can review the log files that are generated during your execution of all scheduled tasks and those that were run immediately. You should review these log files periodically to ensure your tasks are running as expected.

Step 1 Navigate to **Fault** > **Logs**.

Step 2 In the pane located on the left side of the page, select **Logs** > **Task Log**.

Note Separate log files are available for the NE Backup task. This log provide information on all NE backup operations, not just those performed by the NE Config Backup task

Step 3 All available task log files are displayed in the **Task Log** page. You can filter the list to display only the information related to a specific task, user or date/time.

Step 4 In the pane located on the left side of the page, select **Filter**. The filter page provides options for filtering the displayed logs according to time period and type of task. Enter your filtering criteria to obtain the desired listing and click **Submit**.

Step 5 Click **Reset** to see the complete list.

Redline communications

6

Maintaining the RMS Database

Overview

The RMS database must also be monitored and maintained in order for RMS to run efficiently. If the database gets too large, you may notice performance degradation and the time required to perform routine maintenance will increase significantly, further impacting performance.

Using the automated database maintenance tasks is the most effective way to maintain the RMS database.

Three utilities are provided to streamline database maintenance and integrity. Maintaining the operational integrity of the database is imperative to system operation.

Table 6-1 Database Maintenance Utilities

Utility	Description
DbBackup	This task creates a copy of the current RMS database. The backup file is saved in the directory <*rms_install_dir*>\backup. This task can be scheduled as outlined in “Working with System Tasks” on page 5-1.
DbCleanup	This task creates a new directory under the <*rms_install_dir*>/backup directory for each scheduled DbCleanup task. All the performance management data, log, and event data are archived and stored in this directory and then removed from the database. This task can be scheduled as outlined in “Configuring the DbCleanup Task” on page 5-8.

Table 6-1 Database Maintenance Utilities (continued)

Utility	Description
DbRestore	This command line utility restores the database from the specified backup file that was created. You first need to drop or rename the existing database. In order to restore the RMS database, you need to shut down the RMS Server and then run this utility from the command line. You will need to rename your existing database if you want to keep it for further investigation. If you know the database is corrupted you will need to drop it before you perform the restore. You can use this utility to create a mirror of your installation for testing purposes.
mysqlcheck	This command line utility checks, repairs, optimizes and analyzes your database tables. This utility must be run when the database service is running. You must backup your database before running this utility. **Important**: All RMS other services must be shutdown before running this utility.

Redline recommends scheduling the DbBackup task on a regular basis to ensure you have recent version of your data. Additionally you should run the DbBackup task through to completion, before running the DbCleanup task. This will allow you to recover data removed by the DbCleanup task, if required.

You need to allow sufficient time, (potentially a number of hours, depending on your system) for the DbBackup task to complete before starting DbCleanup. The two tasks cannot overlap.

Redline also recommends that you move both the DbBackup and DbCleanup files from the RMS Server to another machine and/or storage media as soon as possible to free-up space on the local hard disk.

DbBackup Task

Running the DbBackup Task

You should schedule DbBackup to run at regular intervals.

Step 1 Navigate to **Config** > **Admin >Tasks**.

Step 2 Select DbBackup from the list. DbBackup is one of the standard tasks. If a task has not been configured, then you can create a new task or configure the standard task as outlined in “Working with System Tasks” on page 5-1.

Step 3 Right-click on the task and select **View** to review the task’s settings.

Step 4 Review the scheduling options and update them as required. Select daily or weekly and then enter the exact details of when the task should run. If you have a regular maintenance window, then try and run this task in that window.

The default value of scope is **No End Date** so this task will continue to run indefinitely.

Step 5 Click **Next** and enter a name for the backup file and the number of subsequent backup files to maintain (0 means no limit). MySQL will append the date and time to the specified filename and store the file in the following location:

<*rms_install_dir*>\backup

Step 6 Click **Save** to save the settings to the RMS database and return to the **Tasks** page.

Step 7 If you need to run this task immediately, you can right-click on it and select **Run**.

Your database is dumped to a file, with the specified file name. Depending on the size of the database this could take a few minutes or a few hours. Ensure that you move the DbBackup files from the RMS server to another machine and/or storage media as soon as possible, to maintain adequate space on the local hard disk.

Running DbBackup from the Command Line

When you are performing an upgrade, you must backup the current RMS database and move all of the database backup files to a remote location before beginning the RMS upgrade.

The following procedure does not impact the DbBackup scheduled task.

Use the following procedures to backup the existing RMS database at any time without interrupting operation of the RMS application:

Windows Server 2003

Step 1 As the administrative user, navigate to the command line interface on the RMS host machine:

Start > **Programs** > **Accessories** > **Command Prompt**

Step 2 At the command line, navigate to the following directory and locate the dbBackup.bat utility:

`cd <rms_install_dir>\bin`

Step 3 Run dbBackup.bat:

`dbBackup.bat <filename>`

DbBackup appends the .sql extension to the filename you specify and the backup file is saved in the backup directory <*rms_install_dir*>\backup.

Note Depending on the size of the database, this could take several hours.

Step 4 Copy or move this file to a location, separate from the RMS installation directory:

```
cp <filename> d:\network_archives\<date>
```

Step 5 To close the command line interface click on the window's close icon, or type exit.

Solaris 10

Step 1 Log into the RMS host machine as the root user:

```
rlogin <rms_host> –l root
<root password>
```

Step 2 Navigate to the following directory and locate the dbBackup.sh utility:

```
cd <rms_install_dir>/bin
```

Step 3 Run dbBackup.sh:

```
dbBackup.sh <filename>
```

Step 4 The backup file is saved in the backup directory <*rms_install_dir*>\backup using the filename specified on the command line.

Note Depending on the size of the database, this may take some time.

Step 5 Copy or move this file to a location, separate from the RMS installation directory:

```
cp <filename> /disk4/network_archives/<date>
```

Database Backup for High Availability via the Command Line

The following procedure is required only for RMS systems using the CLI utility dbBackup.sh. The RMS task DbBackup is not affected.

Note You must modify the command line utility dbBackup.sh when the HA function has been manually enabled on an RMS server that was initially installed without HA.

If the utility is not updated, the dbBackup.sh utility will not provide a useful database backup. If the high availability feature was configured during initial installation, then your dbBackup.sh will be configured correctly and you do not need to modify it here.

Step 1 Log into the workstation that is hosting the RMS server, as the root user:

```
rlogin <rms_host> –l root
<root password>
```

Step 2 Navigate to the following directory and locate the dbBackup.sh utility:

```
cd <rms_install_dir>/bin
```

Step 3 Make a copy of the file:

```
cp dbBackup.sh dbBackup.bak
```

Step 4 Open the dbBackup.sh file for editing:

```
vi dbBackup.sh
```

Step 5 Locate the --databases parameter and append <*database name*>Ha immediately after the database name. For example, if you are using the default database name 'RedMAXnms' the modified portion of the command line should be modified as follows:

```
...
--databases redmaxnms redmaxnmsHa
...
```

Step 6 Save the changes and close the dbBackup.sh file.

```
:wq
```

DbCleanup Task

Running DbCleanup

You should schedule DbCleanup to run at regular intervals after the completion of DbBackup.

Step 1 Navigate to **Config** > **Admin >Tasks**.

Step 2 Select the appropriate task from the list. If a task has not been created, then create one as outlined in “Working with Custom Tasks” on page 5-5.

Step 3 Right-click on the task and select **View** to review the task’s settings.

Step 4 Review the scheduling options and update them as required. Select daily or weekly and then enter the exact details of when the task should run. If you have a regular maintenance window, then try and run this task in that window.

Note The default value of scope is **No End Date** so this task will continue to run as long as performance data is being collected.

Step 5 Click **Next** and select the **Window Interval**. The **Window Interval** is the period prior to the cleanup operation for which database records will be kept.

For example, setting the Window Interval to 3 months will result in the removal of all diagnostic data except for the last 3 months prior to the cleanup operation. The 3-month period does not include the current month. If you are performing the cleanup on July 14, and specify 3 months as the interval, then April, May, June and the first 14 days of July will be retained.

Step 6 Click **Save** to save the settings to the RMS database.

Step 7 If you need to run this task immediately, you can right-click on it and select **Run**.

Ensure that you move both the DbBackup files from the RMS Server to another machine and/or storage media as soon as possible, to maintain adequate space on the local hard disk.

Database Usage Statistics for High Availability

Database disk space usage statistics are provided on the **HA** page to help you better manage your HA host machines. You should review these statistics frequently to maintain optimum performance.

Step 1 Navigate to **Config > System > HA**. On the **High Availability** page check the last columns in the table.

Step 2 This is the composite amount of free disk space available to MySQL. This column contains the disk space availability for the various different database directories on your Solaris file system. The information for each directory is displayed as: Disk Space Name | Free Disk Space in Mb | Percent Available.

Table 6-2 High Availability Disk Space Usage Statistics

Parameter	Description
Disk Space Name | Free Space in Mb | Percent Available	This is the composite amount of free disk space available to MySQL. This column contains the disk space availability for the various different database directories on your Solaris file system. The information for each directory is displayed as: Disk Space Name | Free Disk Space in Mb | Percent Available.
Disk Space Name	The first field, Disk Space Name has four values for the current Solaris HA deployment:
	• /<RMS_install_dir>/mysql - This is the file system where RMS is installed • /<RMS_install_dir>/mysql/data - This is the file system where the RMS database is installed. In most cases this will be the same as above. • /tmp - This is the file system for temporary files that is used during HA MysSQL synchronization. • /var/tmp - This is the file system for temporary MySQL tables, for sorting, etc.

Table 6-2 High Availability Disk Space Usage Statistics (continued)

Parameter	Description
Free Disk Space	This is the amount of free disk (in Mb) space available to MySQL, on the specified partition.
Percent Available	This is the percentage of disk space available to MySQL, on the specified partition. When this percentage reaches 1% (i.e. 99% is used) the system will failover.

Step 3 When free disk space is low, you need to run the DbCleanup as outlined below.

DbRestore Task

You will only need to restore the database as a last resort if it has been corrupted or if you have lost a significant amount of data.

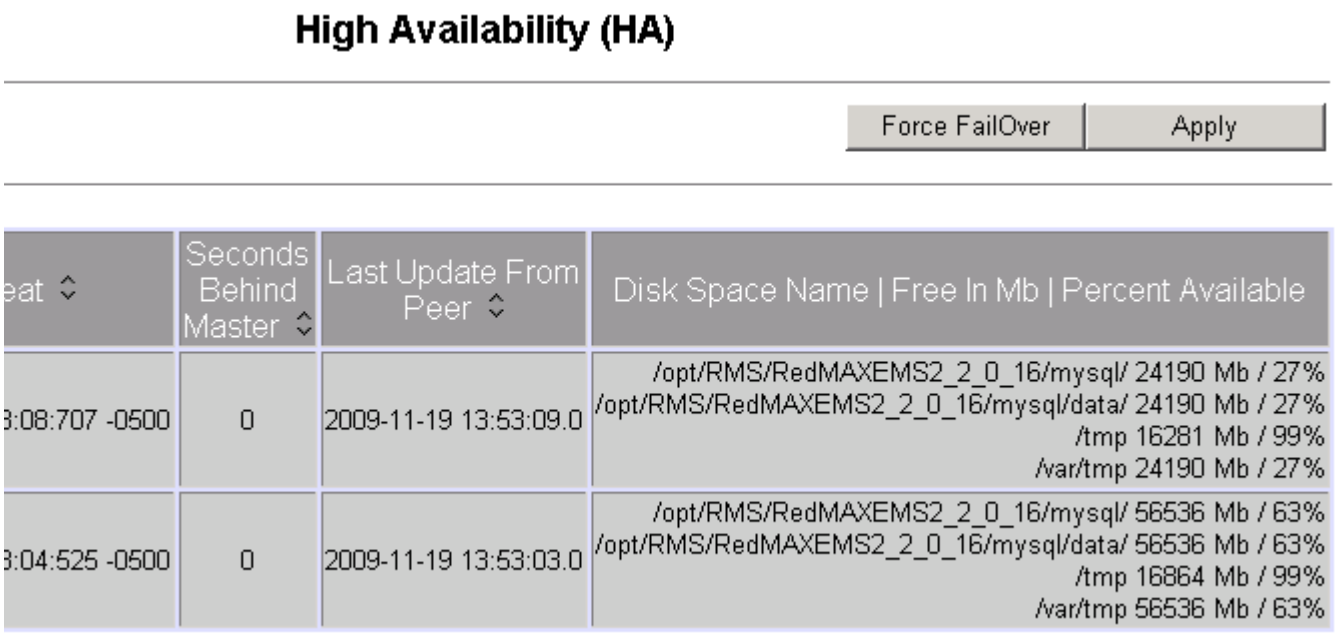
It may be necessary to drop the original database before restoring the backup. This will depend on many things and you should consult with your database administrator before proceeding.

Before restoring the database, you should verify that the database server has enough system resources (memory and disk space) and that it is stable and running.

If you are restoring a database from another system for testing or evaluation purposes, you must have a valid RMS administrator user account and password in order to access the RMS GUI client after the restore is completed.

Note DbRestore will overwrite the current RMS database, so you should run DbBackup, unless you already have a current backup.

Figure 6-1 High Availability Disk Space Usage Statistics



Windows Server 2003

To restore your database on a Windows Server 2003 platform, use the following procedure.

Step 1 Stop the RMS Server as outlined in “Starting and Stopping Services” on page 2-1. The database service must be running.

Step 2 As the administrative user, navigate to the command line interface on the RMS server.

Start > **Programs** > **Accessories** > **Command Prompt**

Step 3 Navigate to the following directory and locate the most recent database backup file. Verify that this is the data to be restored.

```
cd <rms_install_dir>\backup
dir
```

Step 4 Navigate to the following directory and locate the DbRestore utility.

```
cd <rms_install_dir>\bin
```

Step 5 Run DbRestore specifying the path and filename of the file to be restored.

```
dbRestore.bat
<rms_install_dir>\backup\db-backup_2009_04_29_01_00_00.sql
```

Note Depending on the size of the database, this could take several hours.

Step 6 When the command line prompt returns the database restore is complete. Close the command line interface by typing exit.

Step 7 Start the RMS Server as outlined in “Starting and Stopping Services” on page 2-1.

Solaris 10

To restore your database on a Solaris platform, use the following procedure.

Step 1 Log into the RMS host machine as the root user:

```
rlogin <rms_host> –l root
<root password>
```

Step 2 Stop the RMS Server as outlined in “Starting and Stopping Services” on page 2-1.

Step 3 Navigate to the following directory and locate the most recent database backup file. The dbRestore utility automatically picks up the most recent database-backup file from the backup directory. Verify that this is the data to be restored:

```
cd <rms_install_dir>/backup
ls -ltr
```

Step 4 Navigate to the following directory and locate the dbRestore utility:

```
cd <rms_install_dir>/bin
```

Step 5 Run DbRestore specifying the path and filename of the file to be restored.

```
.\dbRestore.bat
<rms_install_dir>/backup/database-backup_2010_05_03_01_00_00.sql
```

Note Depending on the size of the database, this process may take hours to complete.

Step 6 Start the RMS Server as outlined in “Starting and Stopping Services” on page 2-1.

Starting and Stopping the Database Service

The MySQL server can be started and shut down manually from the command line.

Solaris 10

Step 1 Log into the RMS host machine as the root user:

```
rlogin <rms_host> –l root
<root password>
```

Step 2 Confirm the path of the MySQL service:

```
svcs –a | grep mysql
```

Step 3 Enable the MySQL service:

```
svcadm enable –s svc:/site/mysqldX_Y_Z_nnn:mysqldX_Y_Z_nnn
```

Step 4 To stop the services, disable the MySQL service:

```
svcadm disable –s svc:/site/mysqldX_Y_Z_nnn:mysqldX_Y_Z_nnn
```

Step 5 If mysqld does not start, check the error log to see any messages that may indicate the cause of the problem.

The error log is located in the following directory:

<*rms_install_dir*>/mysql/data

Look in the data directory for files with names of the form <*host_name*>.err and <*host_name*>.log, where <*host_name*> is the name of your server host machine. Review the last few lines of these files.

```
tail -20 <host_name>.log
```

Step 6 You can start mysqld with the standalone and debug options. In this case, mysqld writes a log file in /tmp/mysqld.trace that should contain some troubleshooting information:

```
mysqld –-standalone --debug
```

Use the verbose and help options to display all the mysqld command set:

```
mysqld --verbose --help
```

Step 7 Verify the status of MySQL service using one of the following commands:

```
svcs –av | grep mysql
ps –ef | grep mysql
```

You can verify various database functionality from the command line using the following MySQL queries:

Windows Server 2003

In Windows, the recommended way to run MySQL is to install it as a Windows' service. As a Windows' service, MySQL starts and stops automatically when Windows starts and stops. A MySQL server installed as a service can also be managed from the command line using .NET commands, or with the graphical Services utility.

To start the MySQL server from the command line, use the following procedure:

Step 1 As the administrative user, open a console window on the RMS server.

Start > **Programs** > **Accessories** > **Command Prompt**

Step 2 In the console window enter this command:

```
cd c:\
cd \<rms_install_dir>\bin\
mysqld
```

The path to mysqld may vary depending on the installation location of MySQL on your system.

Step 3 You can stop the MySQL server by executing the command:

```
cd c:\
cd \<rms_install_dir>\bin\
mysqladmin" -u root –p <password> shutdown
```

Step 4 Monitor the services listed in the **Services** dialog box to verify that the service has stopped (e.g., service name EMS_RMS_DBX_Y_Z_nnn).

This command invokes the MySQL administrative utility mysqladmin to connect to the server and shut it down. The command connects as the MySQL root user, which is the default administrative account in the MySQL grant system. Users in the MySQL grant system are independent from any login users under Windows. Refer to the MySQL documentation for information on database user account management.

Step 5 If mysqld does not start, check the error log to see any messages that may indicate the cause of the problem.

The error log is located in the following directory:

`C:\RMS\RedMAXEMS\MySQL\data\<hostname>.err`

The log files have the extensions .err. and .log. You can view the file with any text editor.

Step 6 You can start mysqld with the standalone and debug options. In this case, mysqld writes a log file C:\mysqld.trace that should contain system troubleshooting information:

```
mysqld –-standalone --debug
```

Use the verbose and help options to display the mysqld command set.

```
mysqld --verbose --help
```

Verifying Database Integrity

You can perform a database integrity check if you suspect that your database is corrupted because it was not shut down properly or there has been a hardware/driver failure.

Note IMPORTANT: All RMS services (except mysql) must be stopped before running the MySQL utility.

The mysqlcheck utility checks, repairs, optimizes, and analyzes your tables. This utility must be run when the database service is running. You should backup your database before running this utility.

You must have a version of mysqld that has been compiled with debugging support in order to generate trace files. You can check this by executing mysqld -V. If the version number ends with -debug, your version has been compiled with support for trace files.

Depending on the size of your database, this check may take hours to run. You should run this utility during periods on minimal activity to reduce the time required to complete the operation and to minimize the impact on database performance.

Windows Server 2003

To verify database integrity on your Windows platform, use the following procedure:

Note On Windows Server 2003, starting with MySQL 4.1, the debugging server is named mysqld-debug.

Step 1 Log into the server as the admin user. Navigate to the command line interface on the mysql client.

Start > **Programs** > **Accessories** > **Command Prompt**

Step 2 Navigate to the following directory:

cd <*rms_install_dir*>\mysql

Step 3 In order to generate a trace files, invoke mysqld as follows:

```
mysqld --debug
```

The trace file can become very big! If you want to generate a smaller trace file, you can use debugging options similar to:

```
mysqld --debug=d,info,error,query,general,where:O,/C:\mysqld.trace
```

This only prints information with the most useful tags to the trace file.

Refer to the documentation provided with MySQL to configure and use the log and tracing features.

Step 4 Run the mysqlcheck utility. As each table is verified, the table name and status are output to the screen. This may take hours for a large database. e.g. 10 GB.

```
mysqlcheck –u root –p –P 3306 reamaxnms
<password>
```

Where: -u specifies the database administrator user name

-p prompts the user to enter the password. Do not use –p<password>. It is an insecure method for entering your password.

-P specifies the database port number

reamaxnms is the name of the database.

Step 5 Close the command line interface by clicking on the window's close icon, or type exit.

Step 6 If the integrity check fails, please contact support@redlinecommunications.com with your trace. The trace file should be located in:

```
C:\mysqld.trace
```

The exact location of the trace file will depend on how mysqld has been configured.

Solaris 10

To verify database integrity on your UNIX platform, use the following procedure:

Step 1 Log into the RMS host machine as the root user:

```
rlogin <db_host> –l root
<root password>
```

Step 2 Navigate to the following directory:

```
cd <rms_install_dir>/bin/mysql
```

Step 3 In order to generate a trace file, invoke mysqld as follows:

```
mysqld --debug
```

The trace file can become very big! If you want to generate a smaller trace file, you can use debugging options similar to:

```
mysqld --debug=d,info,error,query,general,where:O,/tmp/mysqld.trace
```

This only prints information with the most useful tags to the trace file.

Refer to the documentation provided with MySQL to configure and use the log and tracing features.

Step 4 Run the mysqlcheck utility. As with other database utilities, this check may take some time depending on the size of your database.

```
mysqlcheck –uroot –p –P3306 reamaxnms
```

Where: -u specifies the database administrator user name.

-p prompts the user to enter the password. Do not use –p<password>. It is an insecure method for entering your password.

-P specifies the database port number.

redmaxnms is the name of the database.

Step 5 Optionally you can save the output to a file for further review and investigation:

```
mytsqlcheck –uroot –proot –P3306 reamaxnms >> sqlcheck.txt
```

Step 6 If the integrity check fails, please contact support@redlinecommunications.comt with your trace. The trace file should be located in:

```
/tmp/mysqld.trace
```

The exact location of the trace file will depend on how mysqld has been configured.

Optimizing the RMS Database Size

The RMS database will grow with the addition of network element management and performance management/log/alarm data over time. Network element management-related data needs to be retained in the database but the other types of data can be removed from the database using the DbCleanup utility.

One way to keep the database size manageable is to perform DbCleanup regularly. The space that used to hold the deleted data from DbCleanup task will be made available to new data. However, not all seemingly empty space will be used due to the fragmentation of the previously deleted data. You will observe, over time that the database size will continue to increase, even with scheduled DbCleanup tasks. The rate, at which the RMS database grows, will depend on the size of your network and the frequency of the scheduled DbCleanup task.

The following procedures allows you to optimize the database layout on disk with tables laid out in contiguous memory removing the fragmentation that occurs over time.

Verifying the Size of the Database

Use the following procedure to determine the size of your current RMS database.

Windows Server 2003

Step 1 As the administrative user, open Windows Explorer.

Step 2 Navigate to the following directory.

<*rms_install_dir*>\mysql

Step 3 Locate the directory named **data**. Right-click on this file and select **Properties**.

Step 4 On the **General** tab you can see the file size. This tells you the size of your RMS database.

Solaris10

Step 1 Log into the workstation that is hosting the RMS server, as the root user:

```
rlogin <rms_host> –l root
<root password>
```

Step 2 Navigate to the following directory:

```
<rms_install_dir>/mysql/
```

Step 3 Execute the following command on the data directory:

```
du -s -k installdir/mysql/data
```

Resizing the Database

It may be necessary to resize your database when it exceeds its existing partition, even after being cleaned and optimized. This may be the case if your network has expanded beyond the original size estimates, on which system resource allocations were based.

When the file, ibdata1, fills the available disk partition size, the MySQL services will be stopped. You will need to add a hard drive and then configure a second database file (ibdata2) on the new partition.

The InnoDB storage engine is fully integrated with the MySQL Server and stores its tables and indexes in a tablespace, which may consist of several files (or raw disk partitions). InnoDB tables can be very large even on operating systems where file size is limited to 2GB.

You can increase the size of your tablespace by adding another data file. To do this, you have to shut down the MySQL server, change the tablespace configuration to add a new data file to the end of innodb_data_file_path, and re-start the server.

Note If your existing data file is defined with the keyword autoextend, the procedure for reconfiguring the tablespace must take into account the size of the existing data.

Step 1 Stop RMS and MySQL as outlined in “Starting and Stopping Services” on page 2-1.

Step 2 Obtain the size of the existing data file, round it down to nearest 1MB:

```
cd innodb_data_home_dir
ls -la
```

Step 3 Ensure the path is empty:

```
innodb_data_file_path =
```

Step 4 Specify the rounded file size explicitly in innodb_data_file_path when you are adding the second data file.

```
innodb_data_file_path =
/ibdata/ibdata1:988M;/disk2/ibdata2:50M:autoextend
```

Note Only the last data file in the innodb_data_file_path can be specified as auto-extending.

Step 5 Restart RMS and MySQL as outlined in “Starting and Stopping Services” on page 2-1.

When you add a new file to the tablespace configuration, you must ensure the file does not already exist, as InnoDB will create and initialize the specified file when you restart the server.

You cannot remove a data file from the tablespace so ibdata1 will remain on your system and can be referenced at any time.

Redline communications

7

Monitoring the Provisioning Server

Like any other RMS component, you will also need to monitor and maintain your Provisioning Server. If the Provisioning Server is installed on a separate host machine, you will need to monitor and maintain the host machine as outlined in the previous chapters.

Additionally, you will need to use the procedures in Chapter 4, “Monitoring and Maintaining the RMS Host Machine” to ensure the Provisioning Server is running optimally. For example you will need to monitor hard disk space and memory usage on this host machine, in addition to the RMS host machine.

Generating Provisioning Reports

You can review the performance of the Provisioning Server with system reports: The following report types are available:

- Provisioning Server DHCP Statistics - This report shows the various DHCP statistical information for the Provisioning Server.
- Provisioning Server Statistics - This report shows provisioning statistics, including the number of subscriber units that have been successfully provisioned.
- Provisioning Server Profile Statistics - This report summarizes the subscriber profile information on the Provisioning Server.

Generating system reports is identical to generating other types of performance reports:

Step 1 In the RMS GUI, navigate to **Reports > System**.

Step 2 In the **Report Type** page select one type of system report.

Step 3 Click **Next** to proceed. The **Date Range** page is displayed. The current report criteria are displayed below the page title. This list is updated as you make selections.

Step 4 Click **Next**. On the **Options** page, specify the desired format and layout options.

Step 5 Click **Create** to generate the report. The report is displayed in a new browser window.

Step 6 You can print this report or save it to your local hard disk, using the **Print** or **Save** buttons on the toolbar of the PDF viewer.

Running the PSCleanup Task

In order to prevent the database from becoming filled with out-dated statistical data, you need to run the various cleanup tasks regularly.

The PSCleanup task should be scheduled to run weekly to remove excess statistical data. You may also want to schedule a weekly task to generate the required Provisioning Server reports and then run PSCleanup.

When scheduling this task remember that PSCleanup deletes records from the database permanently.

You should run the DbBackup task before running the PSCleanup task.

Step 1 Navigate to **Config** > **Admin** > **Tasks**.

Step 2 On the **Tasks** page, select the **PSCleanup** task from the list, right-click and select **Edit**.

Step 3 Enter the scheduling options settings. Select daily or weekly and then enter the exact details of when the task should run. If you have a regular maintenance window, then try and run this task in that window.

Note The default value of scope is **No End Date** so this task will continue indefinitely.

Step 4 Click **Next** and select the **Window Interval**. The **Window Interval** is the period prior to the cleanup operation for which database records will be kept.

For example, setting the window interval to 3 months will result in the removal of all Provisioning Server data except for the last 3 months prior to the cleanup operation. The 3-month period does not include the current month. If you are performing the cleanup on July 14, and specify 3 months as the interval, then April, May, June and the first 14 days of July will be retained.

Step 5 Click **Save** to save any changes to the task and return to the **Tasks** page.

Step 6 If you need to the task immediately, right-click on it and select **Run**.

Reviewing Provisioning Server Log Files

You can monitor the following parameters on the Provisioning Server:

- Provisioning Server DHCP request success;
- Failure rates and response times;
- Provisioning/un-provisioning rates and response times.

All of these parameters are logged in Provisioning Server log files. You can review these files for performance metrics and troubleshooting information.

RMS GUI

Step 1 Navigate to **Fault** > **Logs**.

Step 2 In the pane located on the left side of the page, select **Logs** > **Provisioning Log**.

Step 3 All available log files, associated with the Provisioning Server are displayed in the **Provisioning Log** page. You can filter the list to display only the information related to a specific session, user or date/time, etc.

Step 4 In the pane located on the left side of the page, select **Filter**. The filter page provides options for filtering the displayed log files according to time period and user. Enter your filtering criteria to obtain the desired listing and click **Submit**.

Step 5 Click **Reset** to see the complete list.

Windows Server 2003

To review the contents of the Provisioning Server log files on your Windows Server 2003 platform, use the following procedure:

Step 1 Log into the server as the admin user and navigate to the following directory:

`<rms_install_dir>\logs`

Step 2 Using your standard text editor, open the file provserver.log.

Step 3 Review the contents of the log files. You can search for specific information or review the contents of the file. You may want to start of the bottom of the file, to review the most recent information first.

This file is constantly being updated so you should not make any changes to the information or save the file. You can make a copy of the file if you need to generate any reports from the contents of the file.

Solaris 10

To review the contents of the Provisioning Server log files on your UNIX platform, use the following procedure:

Step 1 Log into the RMS host machine as the root user:

```
rlogin <db_host> –l root
<root password>
```

Step 2 Navigate to the following directory:

```
cd <rms_install_dir>/log/
```

Step 3 Use the foolowing command to view the most recent 25 entries in the log file:

```
tail -25 provserver.log
```

Where: -f Specifies the file will be followed as it grows. Each new entry to the file will be displayed. Use Ctrl+C to end the tail command.

-25 Specifies that you want to see 25 lines from the end of the file.

Step 4 Optionally, you can review the entire file:

```
more provserver.log
```

You can search for specific strings:

```
more provserver.log
/ DHCP
```

You can also use the grep command to search for specific strings:

```
grep DHCP provserver.log
```

8

High Availability Maintenance

When configured for high availability, your system requires regular maintenance in order to ensure both the master and slave are operating efficiently. This ensures that any failover process performed for maintenance or under a failure condition will proceed quickly with minimal network interruption.

You must ensure that routine maintenance, described in previous chapters for a single host machine, is performed on both HA host machines.

The procedures provided in this chapter must be performed in addition to the maintenance of each host machine.

Failover of the RMS Server

If your system is configured for high availability, you need to verify high availability functionality by forcing a system failover regularly, to ensure both the master and slave systems are available and operating correctly.

Failover is configured to occur automatically when any one of the four RMS services fail. Failover occurs if the SNMP heartbeat message is not exchanged between the master and slave within the allowed interval. This will happen if, for example, the hard disk is full, the connection pool is full or the master host machine has failed, for any reason.

Verifying Database Synchronization

You must also ensure the slave database in synchronized with the master before forcing a failover. This can be done from the RMS GUI client:

Step 1 Navigate to **Config > System > HA**.

Step 2 On the **High Availability (HA)** page, review the following values for the slave host machine

Table 8-1 Status of HA Slave Host Machine

Parameter	Description
Seconds Behind Master	The number of seconds that the slave currently lags the master. Since MySQL uses asynchronous replication, the slave machine can get behind the master from time to time. The slave will usually synchronize itself, over time. • A value of 0 indicates that the slave is currently synchronized with the master. • A value greater than 0 indicated the slave is not synchronized. You need to wait until it becomes zero before forcing a failover. This may take some time; even several hours in order to fully synchronize the slave, depending on the size of the database and how far behind the slave has become. • A negative value means MySQL synchronization has stopped and there are currently no updates from master (peer).
Last Update From Peer	This is current status of the "heart beat" thread. The purpose of this heart beat is to check the status of the peer host machine. By default the slave checks with the master every 5 seconds and the master checks on the slave, also every 5 seconds. • If the value of **Seconds Behind Master** is >= 0, then the this field should be approximately 5 seconds + the number of **Seconds Behind Master**. This is the normal operating scenario. If the mySQL service is running on both master and slave then this value should be 0. This will also be the case if the RMS service is not running. As far as MySQL is concerned, database synchronization is still proceeding. If the My SQL service goes down, then **Seconds Behind Master** would change from a value of 0 to -1. • If **Seconds Behind Maste**r is >= 0 and this field is not being updated, then even though synchronization is running, the slave database updates are lagging behind the master, significantly. This could be due to long running queries that are temorarily blocking the database. • If **Seconds Behind Master** is -1 then this field is not updated because synchronization has stopped. The slave MySQL may have stopped and synchronization is no longer possible.

If the slave is more than 5 minutes (360 seconds) behind the master, you will need to investigate the cause of the delay. As the delay increases, it is less likely that the slave will be able to synchronize with the master.

At a certain point, it will be more efficient to stop the synchronization and force a data dump from the master to the slave in order to restore the slave and then restart synchronization. See “Forcing Failover Through the RMS GUI” on page 8-3. This decision will depend on the size of your database.

If the parameter, **Last Update From Peer**, is not being updated every 5 seconds then you need to verify that synchronization is running.

Step 1 Verify the slave status by running the following MySQL command on the slave host machine:

```
show slave status \G"
```

Table 8-2 show slave status Output

Parameter	Description
Slave_IO_State	This tells you what the slave thread is doing: i.e. trying to connect to the master, waiting for events from the master, reconnecting to the master, etc.
Slave_IO_Running	This tells you whether the slave I/O thread is started and has connected successfully to the master.
Slave_SQL_Running	This tells you whether or not the slave SQL thread has started.
Replicate_Do_DB	This is the name the databases that was specified with the --replicate-do-db command. Normally, this will be redmaxnms.
Seconds_Behind_Master	When the slave SQL thread is actively running (processing updates), this parameter shows the number of seconds that have elapsed since the timestamp of the most recent event, executed on the master. When the SQL thread has caught up to the slave I/O thread and is waiting for more events from the I/O thread, this field is zero.

If the values of “Slave_IO_Running” and “Slave_SQL_Running” are both “Yes”, Then synchronization is running. If they are not running, you will need to determine why they are stopped before restarting synchronization

Forcing Failover Through the RMS GUI

This can be done from the RMS GUI client:

Step 1 Navigate to **Config > System > HA**.

Step 2 Click on the **Force FailOver** button to transfer RMS services to the Slave (backup) machine.

The failover operation takes up to one minute on a Solaris server. During this time the following operations are occurring:

- The Virtual IP is created on the RMS slave server according to the information provided in the VirtualIfConfig.xml. All devices, referencing the Virtual IP address are not impacted as the Virtual IP is being created.
- The SNMP trap listening port is set as port 162 on the new host machine. The IP address of the new host machine is configured as the trap listener on all network elements.
- If the Provisioning Server is installed and configured for high availability, the master Provisioning Server also goes down and the slave Provisioning Server begins operation with the slave RMS server. If a virtual interface has been configured for Provisioning Server, it will created on the slave host machine, according to the information provided in the VirtualIfConfig.xml.
- Database replication continues, without impact.

- The RMS slave server continues to monitor the master server for a heartbeat.
- Any active GUI client sessions will terminate and users will need to reconnect to the slave server after it has restarted.

Note You will need to wait for at least one minute after failover is initiated before attempting to login to the RMS server. Attempting to login during this period will display the error message, “!! Resources with key Remote not found!!”

The master is now out of service and all RMS transactions are being processed by the slave system. While the system is in this configuration, no information is being saved on the master system; however, the master database remains synchronized with the slave database. The previous slave host machine is now the high availability master. When the previous master host machine becomes active, it will function as the slave.

Completion of RMS Server Failover

Following a failover the master and slave databases will synchronize themselves automatically. While the database synchronization is being performed, the **High Availability** status page displays the status of the master as ”gotoslave”.

Step 1 Navigate to **Config** > **System** > **System Properties**.

Step 2 Select the **HA Service**. The properties of the selected service are displayed below the table. Verify the following information for the HA Service:

Table 8-3 High Availability in ServerConfiguration.xml

Parameter	Description
Virtual IP Address	This is the virtual IP address configured between the RMS master and slave servers
Peer Network Element IP Address	This is the IP address of the other HA machine. If you are configuring the master, then enter the IP address of the slave host machine. If you are configuring the slave, then enter the IP address of the master host machine. If you are entering more than one IP Address, separate each entry with a semi-colon. i.e. 192.168.121.20; 192.168.121.21
Peer Database Name	This is the unique name of the database, hosted on the other HA machine. If you are configuring the master, then enter the database name on the slave host machine.
Peer Database Port	This is the database port, on the other HA machine. If you are configuring the master, then enter the corresponding port on the slave host machine.

Table 8-3 High Availability in ServerConfiguration.xml (continued)

Peer CORBA Port	This is the CORBA port, on the other HA machine. If you are configuring the master, then enter the corresponding CORBA port on the slave host machine.
Peer Virtual IP Mask	This is the Virtual IP Mask, on the other HA machine. If you are configuring the master, then enter the corresponding mask on the slave host machine
Physical Interface Name	This is the name of the physical interface, on the other HA machine.

During your initial installation, you should have recorded the correct values for each of these parameters in your installation worksheet. Ensure that this information is correct against any information that may have changed as a result of a failover.

Step 3 Ensure the NBI interface is not set to 0.0.0.0. This information will also be in the **System Properties** page. Select the **OrbConfigService** for the Provisioning Server. See "Modifying RMS Configuration Parameters through the GUI", in the *Redline Management Suite Installation Guide*.

Step 4 Navigate to **Config > System > HA**. On the **High Availability** page ensure that only the master RMS server is assigned as the "Preferred Master".

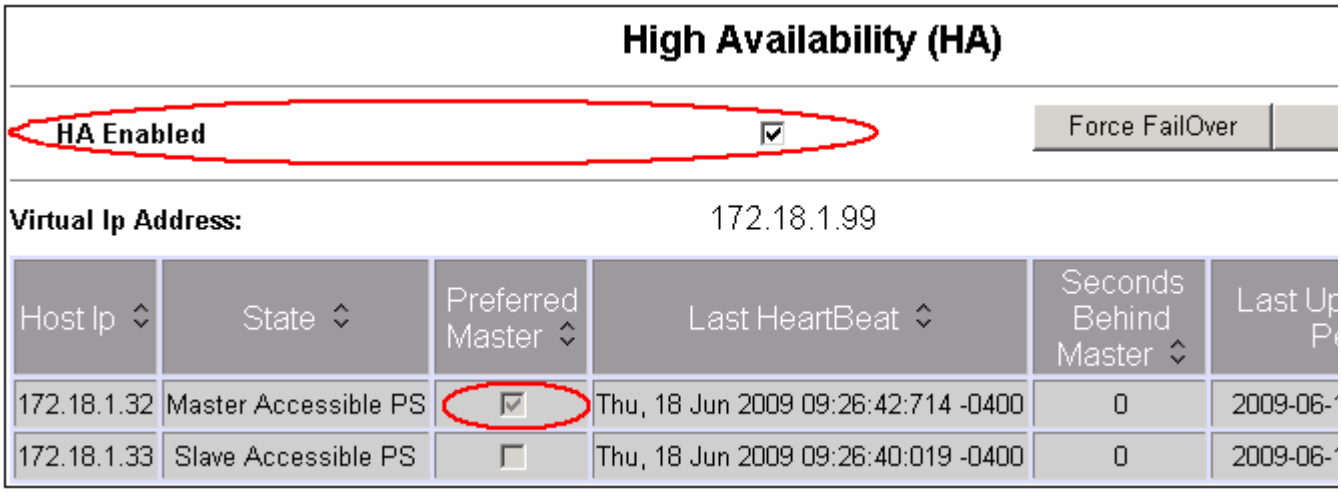
Step 5 Also on the **High Availability** page, ensure the status of both the master and slave are:

- Master Accessible PS
- Slave Accessible PS

Step 6 Ensure that the **High Availability** option is enabled. The **HA Enabled** check box should be selected. See Figure 8-1.

Step 7 Ensure that the host machine, intended as the master server is the "Preferred Master". The check box should be selected.

Figure 8-1 High Availability Page



High Availability Master Host Machine States

Due to the dynamic nature of a high availability system, the master and slave may pass through a number of different states during both normal operation and failover. The current state of both the master and slave as viewed from the master host machine are listed in the following table.

Table 8-4 High Availability Master Host Machine Status Messages

Status	Description
Master Host Machine	
Master	The master RMS is available. As long as the slave host machine is also accessible, your high availability system is fully functional. A Provisioning Server is not installed in this system.
Master Accessible PS	The master RMS and Provisioning Server are available. As long as the slave host machine and the Provisioning Server are also accessible, your high availability system is fully functional.
Disabled Master	The **HA Enabled** check box is not checked. There is no automatic failover; however, MySQL remains synchronized with the slave via database replication.
Master Inaccessible PS	The master RMS is available; however the Provisioning Server is not available.
Unreachable	The master RMS server and the Provisioning Server, if one is installed, are not reachable. The database may be shut down or the machine(s) may be powered down or non-existent.

Table 8-4 High Availability Master Host Machine Status Messages (continued)

Status	Description
Pending Go to Failover	This is a transitional state as the master is failing over to the slave. The master is waiting for confirmation from the peer, that all services have started. You will see this message if you have initiated the failover.
Go to Failover	This is a transitional state as the master is in the process of failing over and becoming the slave. A full database synchronization may be in progress. You will see this message if you have initiated the failover.
Pending Go to Slave	This is a transitional state as the master is failing over to the slave. The master is waiting for confirmation from the peer, that all services have started. You will see this message if this was an automatic failover, initiated by RMS.
Go to Slave	This is a transitional state as the master is in the process of becoming the slave. A full database synchronization may be in progress. You will see this message if this was an automatic failover, initiated by RMS.
failoverAccessible ProvisioningServer	The master has failed over and the slave is now acting as the master. The Provisioning Server is accessible. As long as one RMS host machine is down, the system is functioning but is not in high availability mode.
failoverInaccessible ProvisioningServer	The master has failed over and the slave is now acting as the master; however the Provisioning Server is inaccessible.
Init	You may see this state when the system is turned on for the first time. Both master and slave will be starting and initializing high availability operation.
Vote	This is another status message that may be seen during the initial startup. Two RMS servers have been detected and as they startup and configure themselves, one server will be defined as the master and the other as the slave and high availability will be established.
Slave Host Machine	
Slave	The slave RMS is available. As long as the master host machine is also accessible, your high availability system is fully functional A Provisioning Server is not installed in this system.
Slave Accessible PS	The slave RMS and the Provisioning Server are available. As long as the master host machine is also accessible, your high availability system is fully functional.
Slave Inaccessible PS	The slave RMS is available; however the slave Provisioning Server is not available.

Table 8-4 High Availability Master Host Machine Status Messages (continued)

Status	Description
Unreachable	The slave RMS and Provisioning Server are not reachable. It may be powered down or non-existent. The database may be shut down or the machine(s) may be powered down or non-existent.
Disabled Slave	The **HA Enabled** check box is not checked. There is no automatic failover. MySQL remains synchronized with the master via database replication.

High Availability Maintenance Tasks

Performing a Database Dump from the Master to the Slave

If the slave has fallen far behind the master or if synchronization has failed then you need to restore the slave. You can do this by performing a database dump.

mysqldump -u root -p<password> --opt exampledb > exampledb.sql (Replace <password> with the real password for the MySQL user root! Important: There is no space between -p and <password>!)

You should perform a complete database backup before doing performing this procedure. You should also cleanup the database to reduce the amount to time required for database reloading and synchronization.

Step 1 Log into the workstation that is hosting the slave RMS server, as the root user:

```
rlogin <rms_host> –l root
<root password>
```

Step 2 Stop the RMS and Provisioning services:

```
svcadm disable -s svc:/site/ProvServerd2_2_0_23:ProvServerd2_2_0_23
svcadm disable -s svc:/site/RedMAXEMS2_2_0_23:RedMAXEMS2_2_0_23
svcadm disable -s svc:/site/namingServiced2_2_0_23:
namingServiced2_2_0_23
svcadm disable -s svc:/site/notifSvc2_2_0_23:notifSvc2_2_0_23
svcadm disable -s svc:/site/RMS_DB2_2_0_23:RMS_DB2_2_0_23
```

Step 3 Navigate to the following directory on the slave RMS server:

```
cd <rms_install_dir>/mysql/data
```

Step 4 Delete the following files under mysql/data:

- ib_logfile0
- ib_logfile1
- ib_logfile2
- ibdata1
- ibdata2 (if configured)
- master.info
- relay-log.info
- <*rms_host*>-bin.*
- <*rms_host*>-relay*
- <*rms_host*>.err

Step 5 Delete the following directories:

- redmaxnms
- redmaxnmsha

You must remove both of these directories.

Note Do not delete the mysql directory.

Step 6 Start the database service:

```
svcadm enable –s svc:/site/RMS_DB2_2_0_23:RMS_DB2_2_0_23
```

The deleted files will be re-created.

Step 7 Start the following RMS services on the slave host machine:

```
svcadm enable –s
svc:/site/namingServiced2_2_0_23:namingServiced2_2_0_23
svcadm enable –s svc:/site/notifSvc2_2_0_23:notifSvc2_2_0_23
svcadm enable –s svc:/site/RedMAXEMS2_2_0_23:RedMAXEMS2_2_0_23
```

Step 8 A database dump from the master to the slave should start automatically. Wait for the full database synchronization to complete.

Note If your database is large, the database dump and synchronization could take many hours.

You can run the following command to check the status of the database dump progress:

```
ps –ef | grep dump
```

Repeat this step until the process no longer appears. See “Verifying Database Synchronization” on page 8-1.

Step 9 When the dump is completed, check the HA status on the RMS GUI:

Navigate to **Config > System > HA**. On the **High Availability** page, the status of the slave should be “Slave Inaccessible PS”.

Step 10 Verify that the slave database is now synchronized with the master by running the following MySQL command at the command line on the slave host machine:

```
show slave status \G"
```

Step 11 Review the results and ensure the following values are the same as listed above in Table 8-2.

Verifying Completion of a Database Backup (Dump)

Before you initiate a failover ensure that the database is not in the process of a database backup (data dump). The data dump may be planned or may be the result of a database error, but you cannot failover the system while the dump is in progress.

Before running any database utilities or forcing failover, you also want to disable any scheduled DbBackup tasks that will result in a data dump.

Solaris 10

To verify that a data dump is **not** in progress, use the following command:

Step 1 Log into the RMS host machine as the root user:

```
rlogin <rms_host> –l root
<root password>
```

Step 2 Generate a list of running processes, filtering for the word “dump”:

```
ps –ef |grep dump
```

If any processes, related to the RMS database are returned, you need to wait until the data dump is completed before forcing failover. Depending on the size of your database, this could take several hours. You may want to configure a cron job to monitor the dump and send a message when it is completed.

RMS GUI

You can use the following procedure, only to verify that a planned data dump is not already in progress.

Note If a data dump is the result of unforeseen circumstances, then it will not show up here.

Step 1 Navigate to **Config > Admin > Tasks**.

Step 2 On the **Tasks** page, check the status of the dbBackup task status. If the status is **Progress=running** then you need to wait until the task is complete before forcing failover.

Configuring the High Availability Cleanup Task

The high availability feature can be configured to log event data in a binary log. If there is a lot of network activity and HA polling is enabled, then your system may be overwhelmed by the size and volume of binary log files.

You will need to check the bin.log file size on the RMS Server and cleanup this area using the HA Cleanup task. You will need to set the frequency of the HA Cleanup task accordingly, in order to maintain the required amount of free disk space on the RMS server.

The following procedure provides general instructions for creating and scheduling tasks.

Step 1 Perform a database backup as outlined in “Running DbCleanup” on page 6-5. You must ensure that the backup is completed before you start this procedure. See “Verifying Database Synchronization” on page 8-1 foe details.

Step 2 Navigate to **Config** > **Admin** >**Tasks**.

Step 3 Select the HaCleanup task and right-click. Select **Edit** from the displayed menu.

Step 4 In the **Create Task** page, that is displayed, enter the required scheduling information. Specify how often you want this task to occur (Hourly, Daily, Weekly, or Monthly). Depending on your selection, the displayed options will be updated.

Step 5 Click on the **Save** button to modify the task and save it to the database.

Step 6 If you need to run this task immediately, you can right-click on it and select **Run**.

Synchronizing MyReports between Master and Slave

You need to schedule a task to synchronize the MyReports feature between the Master and Slave RMS host machines. This task can be run on demand, but should be scheduled to run at regular intervals after you have created new reports.

You need to complete the following setup prior to using the task HaMyReportSync:

- RMS should be installed using the same path, on both the master and slave machines.
- SFTP and SSH should be configured and available on each host.
- Additionally, you need to add a new UNIX user account (e.g., reportsync) on both the master and slave RMS machines. This user account will be used by SFTP to connect to the Master and Slave RMS host machines. Contact your system administrator for more details.

Use the following steps to setup HaMyReportSync:

Step 1 Log into the RMS client GUI as the administrative user.

Step 2 Navigate to **Config > Admin > Tasks**.

Step 3 Select HaMyReportSync then right-click and choose **Edit** to modify the task.

Step 4 Enter the desired schedule and click **Next** to continue.

Step 5 Enter the User Name (e.g., reportsync) and password for the report account created for this purpose.

Step 6 Click **Save** to save the changes to the database and update the task.

When the HaMyReportSync runs, all MyReport information will be synchronized between the master and slave RMS machines.

Removing the Virtual Interface from the Failover Machine

Normally when a failover occurs, the virtual interface that existed on the previous master will be removed automatically. If any issues occurred during failover, you may need to remove the virtual interface manually.

Step 1 Log into the workstation that is hosting the RMS server that failed while it was the master, as the *root user*.

```
rlogin <rms_host> –l root
<root password>
```

Step 2 Stop the RMS services as outlined in “Starting and Stopping Services” on page 2-1.

Step 3 Generate a list of all active network interfaces:

```
ifconfig –a
```

Sample output, similar to the following example, should be displayed:

Example 8-1 Interface Configuration

```
lo0: flags=2001000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4, VIRTUAL>
mtu 8232 index 1 inet 127.0.0.1 netmask ff000000

bge0: flags=1100843<UP,BROADCAST,RUNNING,MULTICAST,ROUTER,IPv4> mtu
1500 index 2 inet 192.168.45.214 netmask ffffff00 broadcast
192.168.45.255 ether 0:14:4f:9f:4f:52

bge1:1: flags=1100843<UP,BROADCAST,RUNNING,MULTICAST,ROUTER, IPv4>
mtu 1500 index 3 inet 192.168.12.2 netmask ffffff00 broadcast
192.168.12.255

bge2: flags=1100843<UP,BROADCAST,RUNNING,MULTICAST,ROUTER, IPv4>
mtu 1500 index 3 inet 192.168.12.250 netmask ffffff00 broadcast
192.168.12.255 ether 0:14:4f:9f:4f:54
```

Step 4 Remove the redundant virtual interface:

```
ifconfig bge1 removeif 192.168.12.2 netmask 255.255.255.0
```

In this example, we removed a virtual network interface with IP address: 192.168.12.2 and net-mask: 255.255.255.0 from the physical network interface bge1.

Step 5 Ensure that the virtual network interface has been removed.

```
ifconfig –a
```

Sample output, similar to the following example, should be displayed:

Example 8-2 Modified Interface Configuration

```
lo0:  flags=2001000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4, VIRTUAL>
mtu 8232 index 1 inet 127.0.0.1 netmask ff000000

bge0: flags=1100843<UP,BROADCAST,RUNNING,MULTICAST,ROUTER, IPv4>
mtu 1500 index 2 inet 192.168.45.214 netmask ffffff00 broadcast
192.168.45.255  ether 0:14:4f:9f:4f:52

bge2: flags=1100843<UP,BROADCAST,RUNNING,MULTICAST,ROUTER, IPv4>
mtu 1500 index 3 inet 192.168.12.250 netmask ffffff00 broadcast
192.168.12.255 ether 0:14:4f:9f:4f:54
```

In this example only bge0 and bge2 are currently active; interface lo0 is a loopback interface. Interface bge1 is no longer configured.

Step 6 Start RMS as outlined in “Starting and Stopping Services” on page 2-1.

Modifying the Master for Extended Slave Downtime

If your slave host machine will be down for more than 24 hours you must configure MySQL on the master host machine to stop generating the bin log and bin relay logs files. This is done to prevent these files from growing unncecessarily and consuming disk space.

Disabling Log Files

Step 1 Perform a database backup as outlined in “Running the DbBackup Task” on page 6-2.

Step 2 Perform a database cleanup as outlined in “Running DbCleanup” on page 6-5 and then backup the database again.

Step 3 Log into the machine that is hosting the RMS master, as the MySQL user:

```
rlogin <rms_host> –l mysql
<mysql password>
```

Step 4 Navigate to the following directory:

```
cd <rms_install_dir>/mysql/data/
```

Step 5 Locate the file named my.cnf and create a backup copy of this file.

```
cp my.cnf my.bak
```

Step 6 Use your standard text editor to open the file and comment out the settings show in Example 8-3 on page 8-14:

```
vi my.cnf
```

Example 8-3 MySQLConfiguration File

```
#log-bin=mysql-bin
#relay-log=mysql-relay-bin
#binlog_format=mixed
#sync_binlog=1
#server-id=1
#replicate-ignore-table=redmaxnmsHa.HighAvailability
#replicate-do-db=redmaxnms
#replicate-ignore-table=redmaxnms.SystemReleaseInfo
#replicate-wild-ignore-table=redmaxnms.temp%
#slave-skip-errors=1141,1147,1269,1022,1062
```

Step 7 Save the modified file.

```
: wq
```

Step 8 Remove the following files from the master host machine:

```
rm -f <rms_install_dir>/mysql/data/*bin*
rm -f <rms_install_dir>/mysql/data/*.info
```

Step 9 Stop and restart RMS and MySQL as outlined in “Starting and Stopping Services” on page 2-1.

Step 10 Review the MySQL error log and ensure there are no errors on restarting, related to relay logs.

Enabling Log Files

Once the slave host machine is available you will need to re-enable the generation of the bin log and bin relay logs files.

Step 1 Perform a database backup as outlined in the *Redline Management Suite Administration and Maintenance Guide*.

Step 2 Perform a database cleanup as outlined in “Running DbCleanup” on page 6-5 and then backup the database again.

Step 3 Log into the machine that is hosting the RMS master, as the MySQL user:

```
rlogin <rms_host> –l mysql
<mysql password>
```

Step 4 Navigate to the following directory:

```
cd <rms_install_dir>/mysql/data/
```

Step 5 If you have not made any changes to the my.cnf file you can rollback the previous version of the file:

```
cp my.bak my.cnf
```

Step 6 Stop and restart RMS and MySQL as outlined in “Starting and Stopping Services” on page 2-1.

Step 7 Stop the slave database and reload the master as outlined in “Forcing Failover Through the RMS GUI” on page 8-3.

Redline communications

A

SNMP Traps and Threshold Crossing Alerts

This appendix provides a complete list of available threshold crossing alerts (TCAs) and SNMP traps that can be used to define your RMS fault management system.

Refer to the Fault Management chapter in the *Redline Management Suite User Guide* for details on using and monitoring TCAs and SNMP trap messages.

TCA Parameters for RedMAX Devices

There are three network interfaces on RedMAX devices, which are identified by name, and defined in the interface MIB.

Table A-1 RedMAX Device interfaces

Interface	Name Value	Description
RF (Wireless)	Signal	The signal interface.
Data	Data	The data interface is mapped directly to the AN100U Ethernet port labeled “Data”
Management	Mgt	The Management interface is mapped directly to the AN100U Ethernet port labeled “Mgt”.

For each interface (data, management and signal), the following threshold crossing alerts are available:

Table A-2 TCA Parameters for RedMAX Devices

Interface Parameters	OID	Description
ifHCInBroadcastPkts.Data	1.3.6.1.2.1.31.1.1.1.3	The total number of valid Ethernet frames received at the interface, with a broadcast destination address.
ifHCInBroadcastPkts.Signal		
ifHCInBroadcastPkts.Mgt		

Table A-2 TCA Parameters for RedMAX Devices (continued)

Interface Parameters	OID	Description
ifHCInMulticastPkts.Data	1.3.6.1.2.1.31.1.1.1.8	The total number of valid Ethernet frames received at the interface, with a multicast destination address.
ifHCInMulticastPkts.Signal		
ifHCInMulticastPkts.Mgt		
ifHCInOctets.Data	1.3.6.1.2.1.31.1.1.1.6	The total number of good octets received at the interface.
ifHCInOctets.Signal		
ifHCInOctets.Mgt		
ifHCInUcastPkts.Data	1.3.6.1.2.1.31.1.1.1.7	The total number of valid Ethernet frames received at the interface, with a unicast destination address.
ifHCInUcastPkts.Signal		
ifHCInUcastPkts.Mgt		
ifHCOutBroadcastPkts.Data	1.3.6.1.2.1.31.1.1.1.13	The total number of frames transmitted from the interface, with a broadcast destination address.
ifHCOutBroadcastPkts.Signal		
ifHCOutBroadcastPkts.Mgt		
ifHCOutMulticastPkts.Data	1.3.6.1.2.1.31.1.1.1.12	The total number of valid Ethernet frames received at the interface, with a multicast destination address.
ifHCOutMulticastPkts.Signal		
ifHCOutMulticastPkts.Mgt		
ifHCOutOctets.Data	1.3.6.1.2.1.31.1.1.1.10	The total number of good octets transmitted from the interface.
ifHCOutOctets.Signal		
ifHCOutOctets.Mgt		
ifHCOutUcastPkts.Data	1.3.6.1.2.1.31.1.1.1.11	The total number of frames transmitted from the interface, with a unicast Destination address.
ifHCOutUcastPkts.Signal		
ifHCOutUcastPkts.Mgt		
ifInBroadcastPkts.Data	1.3.6.1.2.1.31.1.1.1.3	The total number of valid Ethernet frames received at the interface, with a broadcast destination address.
ifInBroadcastPkts.Signal		
ifInBroadcastPkts.Mgt		
ifInDiscards.Data	1.3.6.1.2.1.2.2.1.13	The total number of valid Ethernet frames that are discarded due to lack of buffer space. This includes both frames discarded at ingress and at egress due to priority and congestion at the output queues.
ifInDiscards.Signal		
ifInDiscards.Mgt		
ifInErrors.Data	1.3.6.1.2.1.2.2.1.14	The total number of packets received at the interface, with an invalid Frame Check Sequence (FSC).
ifInErrors.Signal		
ifInErrors.Mgt		
ifInMulticastPkts.Data	1.3.6.1.2.1.31.1.1.1.2	The total number of frames received at the interface, with a multicast destination address.
ifInMulticastPkts.Signal		
ifInMulticastPkts.Mgt		

Table A-2 TCA Parameters for RedMAX Devices (continued)

Interface Parameters	OID	Description
ifOutBroadcastPkts.Data	1.3.6.1.2.1.31.1.1.1.13	The total number of frames transmitted from the interface, with a broadcast destination address.
ifOutBroadcastPkts.Signal		
ifOutBroadcastPkts.Mgt		
ifOutDiscards.Data	1.3.6.1.2.1.2.2.1.19	The total number of valid Ethernet frames that are discarded due to lack of buffer space. This counter is always 0 because all such discards are already counted by ifnDiscards.
ifOutDiscards.Signal		
ifOutDiscards.Mgt		
ifOutErrors.Data	1.3.6.1.2.1.2.2.1.20	The total number of packets transmitted from the interface, with an invalid FCS.
ifOutErrors.Signal		
ifOutErrors.Mgt		
ifOutMulticastPkts.Data	1.3.6.1.2.1.31.1.1.1.4	The total number of frames transmitted from the interface, with a multicast destination address.
ifOutMulticastPkts.Signal		
ifOutMulticastPkts.Mgt		

For each active service flow, the following TCAs are available:

Table A-3 Service Flow TCA Parameters for RedMAX Devices

Interface Parameters	OID	Description
wmanIfBsSsMacSdu Count	1.3.6.1.2.1.10.184.1.1.1.5.1.1	The SDU is the data unit exchanged between two adjacent protocol layers. This object counts the number of MAC SDUs or MAC messages that have been transmitted or received over the air interface
wmanIfBsSsOctetCount	1.3.6.1.2.1.10.184.1.1.1.5.1.2	This object counts the number of octets of MAC SDUs or MAC messages that have been transmitted or received over the air interface.
redlineWmanIfBsSect ActiveSFSumMax SustainedRate	1.3.6.1.4.1.10728.2.10.1.11.1.1	This object measures the maximum sustained rate for an active service flow.
redlineWmanIfBsSect ProvisSFSumMax SustainedRate	1.3.6.1.4.1.10728.2.10.1.11.1.2	This object measures the maximum sustained rate for a provisioned service flow for the sector.

Table A-3 Service Flow TCA Parameters for RedMAX Devices (continued)

Interface Parameters	OID	Description
redlineWmanIfBsSect ActiveSFSumMin SustainedRate	1.3.6.1.4.1.10728.2.10.1.11.1.3	This object measures the minimum sustained rate for an active service flow for the sector.
redlineWmanIfBsSect ProvisSFSumMin SustainedRate	1.3.6.1.4.1.10728.2.10.1.11.1.	This object measures the minimum sustained rate for a provisioned service flow for the sector.
redlineWmanIfBsSector BandwidthUsage	1.3.6.1.4.1.10728.2.10.1.11.1.5	This object measures the bandwidth usage for the sector.

TCA Parameters for RedCONNEX Devices

For each interface (Wireless and Ethernet), the following threshold crossing alerts are available:

Table A-4 TCA Parameters for RedCONNEX Devices

Interface Parameters	OID	Description
ifHCInBroadcastPkts	1.3.6.1.2.1.31.1.1.1.3	The total number of valid Ethernet frames received at the interface, with a broadcast destination address.
ifHCInMulticastPkts	1.3.6.1.2.1.31.1.1.1.8	The total number of valid Ethernet frames received at the interface, with a multicast destination address.
ifHCInOctets	1.3.6.1.2.1.31.1.1.1.6	The total number of good octets received at the interface.
ifHCInUcastPkts	1.3.6.1.2.1.31.1.1.1.7	The total number of valid Ethernet frames received at the interface, with a unicast destination address.
ifHCOutBroadcastPkts	1.3.6.1.2.1.31.1.1.1.13	The total number of frames, with a broadcast destination address, transmitted from the interface.
ifHCOutMulticastPkts	1.3.6.1.2.1.31.1.1.1.12	The total number of valid Ethernet frames received at the interface, with a multicast destination address.
ifHCOutOctets	1.3.6.1.2.1.31.1.1.1.10	The total number of good octets transmitted from the interface.
ifHCOutUcastPkts	1.3.6.1.2.1.31.1.1.1.11	The total number of frames transmitted from the interface, with a unicast destination address.

Table A-4 TCA Parameters for RedCONNEX Devices (continued)

Interface Parameters	OID	Description
ifInBroadcastPkts	1.3.6.1.2.1.31.1.1.1.3	The total number of valid Ethernet frames received at the interface, with a broadcast destination address.
ifInDiscards	1.3.6.1.2.1.2.2.1.13	The total number of valid Ethernet frames that are discarded due to lack of buffer space. This includes both frames discarded at ingress and at egress due to priority and congestion at the output queues.
ifInErrors	1.3.6.1.2.1.2.2.1.14	The total number of packets received at the interface, with an invalid Frame Check Sequence (FSC).
ifInMulticastPkts	1.3.6.1.2.1.31.1.1.1.2	The total number of frames received at the interface, with a multicast destination address.
ifOutBroadcastPkts	1.3.6.1.2.1.31.1.1.1.13	The total number of frames transmitted from the interface, with a broadcast destination address.
ifOutDiscards	1.3.6.1.2.1.2.2.1.19	The total number of valid Ethernet frames that are discarded due to lack of buffer space. This counter is always 0 because all such discards are already counted by ifnDiscards.
ifOutErrors	1.3.6.1.2.1.2.2.1.20	The total number of packets, with an invalid FCS, transmitted from the interface.
ifOutMulticastPkts	1.3.6.1.2.1.31.1.1.1.4	The total number of frames transmitted from the interface, with a multicast destination address.

TCA Parameters for Point-to-Point (PTP) Devices

Table A-5 TCA Parameters for Point-to-Point (PTP) Devices

TCA/	OID	Description
an80iIfCurrUncoded BurstRate	1.3.6.1.4.1.10728.2.10.2.1.2.1	This object indicates the link's current uncoded burst rate. With adaptive modulation enabled, this rate may change over time.
an80iIfPtpLinkStatus	1.3.6.1.4.1.10728.2.10.2.1.2.2	This object indicates whether or not the link has been established.
an80iIfRxPackets	1.3.6.1.4.1.10728.2.10.2.1.2.3	This object indicates the number of received wireless packets with a correct CRC.

Table A-5 TCA Parameters for Point-to-Point (PTP) Devices (continued)

TCA/	OID	Description
an80iIfRxPacketsReTx	1.3.6.1.4.1.10728.2.10.2.1.2.4	This object indicates the number of received re-transmitted wireless packets with a correct CRC.
an80iIfRxPacketsDisc	1.3.6.1.4.1.10728.2.10.2.1.2.5	This object indicates the number of received wireless packets that were not received correctly by the other equipment.
an80iIfTxPackets	1.3.6.1.4.1.10728.2.10.2.1.2.6	This object indicates the number of transmitted packets that were received correctly by the other equipment.
an80iIfTxPacketsReTx	1.3.6.1.4.1.10728.2.10.2.1.2.7	This object indicates the number of retransmitted wireless packets received correctly by the other equipment.
an80iIfTxPacketsDisc	1.3.6.1.4.1.10728.2.10.2.1.2.8	This object indicates the number of re-transmitted wireless packets that were not received correctly by the other equipment.
an80iIfRssiMin	1.3.6.1.4.1.10728.2.10.2.1.2.9	This object indicates the minimum received signal strength for the measuring interval.
an80iIfRssiMean	1.3.6.1.4.1.10728.2.10.2.1.2.10	This object indicates the average received signal strength for the measuring interval.
an80iIfRssiMax	1.3.6.1.4.1.10728.2.10.2.1.2.11	This object indicates the maximum received signal strength for the measuring interval.
an80iIfAvrSinAdr	1.3.6.1.4.1.10728.2.10.2.1.2.12	This object indicates the signal-to-interference, noise and distortion ratio.

TCA Parameters for Point-to-Multipoint (PMP) Devices

Table A-6 TCA Parameters Point-to-Multipoint (PMP) Devices

TCA	OID	Description
an80iIfPmpLinkStatus	1.3.6.1.4.1.10728.2.10.2.2.3.1.1	This object indicates whether or not the link has been established.
an80iIfPmpLinkStatus Code	1.3.6.1.4.1.10728.2.10.2.2.3.1.2	Indicates the link status code, in which each bit represents a specific condition, error, status.
an80iIfRegPmpLink Conns	1.3.6.1.4.1.10728.2.10.2.2.3.1.3	This object indicates the registered connections for this link.
an80iIfPmpLinkUp Time	1.3.6.1.4.1.10728.2.10.2.2.3.1.4	The time (in hundredths of a second) that has elapsed since the link was established (up).
an80iIfPmpLinkLost Count	1.3.6.1.4.1.10728.2.10.2.2.3.1.5	The number of times the link has been lost since the system started.
an80iIfPmpLinkCurrDLUncB urstRate	1.3.6.1.4.1.10728.2.10.2.2.3.1.6	This object indicates the link's downlink actual uncoded burst rate.
an80iIfPmpLinkDLRssi	1.3.6.1.4.1.10728.2.10.2.2.3.1.7	This object indicates the link's download RSSI (Received Signal Strength Indicator).
an80iIfPmpLinkDL SinAdr	1.3.6.1.4.1.10728.2.10.2.2.3.1.8	This object indicates the link's download SINADR (Signal Interference and Noise Distortion Ratio).
an80iIfPmpLinkDLLost Frm	1.3.6.1.4.1.10728.2.10.2.2.3.1.9	This object indicates the link's download lost frames.
an80iIfPmpLinkDLBlksTot	1.3.6.1.4.1.10728.2.10.2.2.3.1.10	This object indicates the link's download blocks transmitted.
an80iIfPmpLinkDLBlksRetr	1.3.6.1.4.1.10728.2.10.2.2.3.1.11	This object indicates the link's download block re-transmitted.
an80iIfPmpLinkDLBlksDisc	1.3.6.1.4.1.10728.2.10.2.2.3.1.12	This object indicates the link's download blocks lost.
an80iIfPmpLinkCurrULUncB urstRate	1.3.6.1.4.1.10728.2.10.2.2.3.1.13	This object indicates the link's actual upload uncoded burst rate.

Table A-6 TCA Parameters Point-to-Multipoint (PMP) Devices (continued)

TCA	OID	Description
an80iIfPmpLinkULRssi	1.3.6.1.4.1.10728.2.10.2.2.3.1.14	This object indicates the link's upload RSSI (Received Signal Strength Indicator).
an80iIfPmpLinkUL SinAdr	1.3.6.1.4.1.10728.2.10.2.2.3.1.15	This object indicates the link's upload SINADR (Signal Interference and Noise Distortion Ratio).
an80iIfPmpLinkULLost Frm	1.3.6.1.4.1.10728.2.10.2.2.3.1.16	This object indicates the link's upload lost frames.
an80iIfPmpLinkULBlksTot	1.3.6.1.4.1.10728.2.10.2.2.3.1.17	This object indicates the link's upload blocks transmitted.
an80iIfPmpLinkULBlksRetr	1.3.6.1.4.1.10728.2.10.2.2.3.1.18	This object indicates the link's upload block re-transmitted.
an80iIfPmpLinkULBlksDisc	1.3.6.1.4.1.10728.2.10.2.2.3.1.19	This object indicates the link's lost upload blocks.
an80iIfPmpLinkStats Status	1.3.6.1.4.1.10728.2.10.2.2.3.1.20	This object is used to create a new row or to modify or delete an existing row in this table.

TCA Parameters for Point-to-Multipoint (PMP) Connection States

Table A-7 TCA Parameters Point-to-Multipoint (PMP) Devices

TCA	OID	Description
an80iIfPmpConnDL PacketsTx	1.3.6.1.4.1.10728.2.10.2.2.6.1.8	This object specifies the transferred packets for the download connection.
an80iIfPmpConnDL PacketsRx	1.3.6.1.4.1.10728.2.10.2.2.7.1.2	This object specifies the received packets for the download connection.
an80iIfPmpConnDL PacketsDisc	1.3.6.1.4.1.10728.2.10.2.2.7.1.3	This object specifies the discarded packets for the download connection.
an80iIfPmpConnUL PacketsTx	1.3.6.1.4.1.10728.2.10.2.2.7.1.	This object specifies the transferred packets for the upload connection.
an80iIfPmpConnUL PacketsRx	1.3.6.1.4.1.10728.2.10.2.2.7.1.5	This object specifies the received packets for the upload connection.
an80iIfPmpConnUL PacketsDisc	1.3.6.1.4.1.10728.2.10.2.2.7.1.6	This object specifies the discarded packets for the upload connection.

SNMP Traps for RedMAX Devices

The network elements manged by RMS, support a number of SNMP traps. Detailed instructions and examples of trap-related management functions are provided in the *AN100U V2.1-SNMP Agent and MIB Description*

The AN100U SNMP traps are referenced in the following MIB files:

- IF-MIB (RFC 2863) - This MIB describes objects used for managing network interfaces.RedMAX devices use a subset of the objects listed in this MIB.
- SNMPV2-MIB (RFC 3418) - This MIB defines managed objects, which describe the behavior of the SNMP entity. RedMAX devices use a subset of the objects listed in this MIB.
- REDLINE-SYSTEM-MIB - This MIB contains the Redline extensions to the SNMPv2 MIB System Group. RedMAX devices use a subset of the objects listed in this MIB.
- REDLINE-BS-MIB - This MIB contains object definitions applicable only to the Redline Base Station. RedMAX devices use a subset of the objects listed in this MIB.
- WMAN-IF-MIB (IEEE 802.16) - This MIB describes managed objects used to support the management of MAC (Medium Access Control) and physical layer features as defined by IEEE 802.16/2004.

Note LinkUp and LinkDown traps sent from AN50e systems do not have a specified source index. Consequently, RMS is unable to determine, to which interface these traps apply.

Table A-8 SNMP Traps for AN100U/AN100UX Devices

Trap	OID	Defined in	Description
coldstart	1.3.6.1.6.3.1.1.5.1	SNMPV2-MIB	This event signifies that the AN80i unit is reinitializing itself and that its configuration may have been altered.
warmStart	1.3.6.1.6.3.1.1.5.2	SNMPV2-MIB	This event signifies that the AN80i unit is reinitializing itself such that its configuration is unaltered.
linkdown	1.3.6.1.6.3.1.1.5.3	IF-MIB	This event signifies that the ifOperStatus object for one of the communication links is about to enter the down state from some other state (but not from the notPresent state).

Table A-8 SNMP Traps for AN100U/AN100UX Devices (continued)

Trap	OID	Defined in	Description
linkup	1.3.6.1.6.3.1.1.5.4	IF-MIB	This event signifies that the ifOperStatus object for one of the communication links left the down state and transitioned into the up state.
authenticationFailure	1.3.6.1.6.3.1.1.5.5	SNMPV2-MIB	This event signifies the receipt of a protocol message that is not properly authenticated.
redlineWmanIfBsSs ModulThresholdTrap	1.3.6.1.4.1.10728.2.10.1.15.0.1	REDLINE-WMAN-IF-MIB	This event reports modulation threshold notification/clear.
redlineBsPower SupplyStatusTrap	1.3.6.1.4.1.10728.2.1.2.11.0.1	REDLINE-BS-MIB	This event reports changes in the status of the base station power supply (on/off).
redlineSWUpgrade StatusTrap	1.3.6.1.4.1.10728.2.1.1.4.3.1	REDLINE-SYSTEM-MIB	This event reports software upgrade progress and status changes.
redlineBsSynchroniz ationTrap	1.3.6.1.4.1.10728.2.1.2.11.0.3	REDLINE-BS-MIB	This event reports whether or not the sector controller is synchronzed with a Master or Master with GPS and if so, whether or not it is receiving a clocking signal.
redlineBsTemp ThresholdTrap	1.3.6.1.4.1.10728.2.1.2.11.0.2	REDLINE-BS-MIB	This event signifies the internal temperature has exceeded the specified safe operating range.
wmanIfBsSsStatus NotificationTrap	1.3.6.1.2.1.10.184.1.1.4.2.0.1	WMAN-IF-MIB	This event reports on the sector controller or subscriber unit that has changed status.
redlineWmanIfBsCir Trap	1.3.6.1.4.1.10728.2.10.1.15.0.3	REDLINE-WMAN-IF-MIB	This event reports whether or not the Committed Information Rate (CIR) exceeds capacity.
redlineBsGpsTrap	1.3.6.1.4.1.10728.2.1.2.11.0.4	REDLINE-BS-MIB	This event reports whether or not the sector controller is receiving a GPS signal and whether or not the GPS is in holdover mode.
redlineWmanIfBsMax ActiveSfTrap	1.3.6.1.4.1.10728.2.10.1.15.0.2	REDLINE-WMAN-IF-MIB	This event reports when the number of maximum, active service flows has been reached.
redlineBsOduL01 Trap	1.3.6.1.4.1.10728.2.1.2.11.0.5	REDLINE-BS-MIB	This event reports when an ODU module encounters an L01 error."
redlineBsOduL02 Trap	1.3.6.1.4.1.10728.2.1.2.11.0.6	REDLINE-BS-MIB	This event reports when an ODU module encounters an L02 error."
redlineBsOduL03 Trap	1.3.6.1.4.1.10728.2.1.2.11.0.7	REDLINE-BS-MIB	This event reports when an ODU module encounters an L03 error."

Table A-8 SNMP Traps for AN100U/AN100UX Devices (continued)

Trap	OID	Defined in	Description
redlineBsOdu ReferenceFrequency Trap	1.3.6.1.4.1.10728.2.1.2.11.0.8	REDLINE-BS-MIB	This event reports when an ODU module encounters a reference frequency (RRF) error."
redlineBsOduIFCable DisconnectedTrap	1.3.6.1.4.1.10728.2.1.2.11.0.9	REDLINE-BS-MIB	This event reports an ODU IF cable disconnected error."
redlineNoiseThreshol dTrap	.1.3.6.1.4.1.10728.2.1.2.11.0.10	REDLINE-BS-MIB	This event occurs when the measured noise exceeds or drops below the level set by the RF configuration parameter 'Noise Threshold'. Set/clear trap messages are limited to a maximum rate of one each eight seconds (as required).

Table A-9 SNMP Traps for AN50e Devices

An50DFSEvent	1.3.6.1.2.1.10.184.1.8.0.11	An event to report the radar frequency detection.
An50TftpFailTrap	1.3.6.1.4.1.10728.1.8.0.1	An event that reports the failure of an AN50e software upgrade operation. The intended network element experienced a failure during upgrade.
An50TftpSuccess Trap	1.3.6.1.4.1.10728.1.8.0.2	An event that reports the success of an AN50e software upgrade operation.
An50PswdChange FailTrap	3.6.1.4.1.10728.1.8.0.3	An event to report the failure of an AN50e password change.
An50FirmwareConfig FailTrap	1.3.6.1.4.1.10728.1.8.0.4	This event reports the failure of the AN50e firmware configuration.
An50Eeprom CorruptedTrap	1.3.6.1.4.1.10728.1.8.0.5	This event reports the corruption of the AN50e EEPROM.
An50PowerSupply FailureTrap	1.3.6.1.4.1.10728.1.8.0.6	This event reports the AN50e power supply failure.
An50SaveConfigTrap	1.3.6.1.4.1.10728.1.8.0.7	This event reports saving of the AN50e configuration.
An50ModifiedIdTrap	1.3.6.1.4.1.10728.1.8.0.8	This event reports the modification in the configuration of an AN50e ID.

Table A-9 SNMP Traps for AN50e Devices (continued)

An50pmpRegistration Missed	1.3.6.1.4.1.10728.1.8.0.9	This event reports the failure of an AN50e registration attempt of a subscriber unit that is not defined in the link table.
An50pmpRegistration Successful	1.3.6.1.4.1.10728.1.8.0.10	This event reports the success of an AN50e registration attempt of a subscriber unit that is not defined in the link table.

Table A-10 SNMP Traps for Other RedMAX Devices

WmanIfBsSsDynamic ServiceFailTrap	1.3.6.1.2.1.10.184.1.1.4.2.0.2	This event reports the failure of a dynamic service operation that may have happened during the dynamic services process and was detected on the sector controller side. This trap is not currently supported.
WmanIfBsSsRssi StatusChangeTrap	1.3.6.1.2.1.10.184.1.1.4.2.0.3	This event reports that the uplink RSSI is below the low-RSSI threshold, or above high-RSSI threshold after restore. This trap is not currently supported.
WmanIfBsSsPkmFail Trap	1.3.6.1.2.1.10.184.1.1.4.2.0.4	This event reports the failure of a PKM operation. This trap is not currently supported.
WmanIfBsSsRegister Trap	1.3.6.1.2.1.10.184.1.1.4.2.0.5	This event reports the subscriber unit has changed status. This trap is not currently supported.

SNMP Traps for RedCONNEX/RedACCESS Devices

Table A-11 SNMP Traps for RedCONNEX/RedACCESS Devices

Trap Name/	OID	Description
an80iPswdChangeFailTrap	1.3.6.1.4.1.10728.2.1.3.0.1	This event reports the failure of a password change on the network element.
an80iFirmwareConfig FailedTrap	1.3.6.1.4.1.10728.2.1.3.0.2	This event reports the failure of a firmware re-configuration on the network element

Table A-11 SNMP Traps for RedCONNEX/RedACCESS Devices (continued)

Trap Name/	OID	Description
an80iEeprom CorruptedTrap	1.3.6.1.4.1.10728.2.1.3.0.3	This event reports the corruption of the EEPROM on the network element
an80iHardwareFail Trap	1.3.6.1.4.1.10728.2.1.3.0.4	This event reports device hardware failure on the network element
an80iSaveConfigTrap	1.3.6.1.4.1.10728.2.1.3.0.5	This event reports saving the network elements's running configuration to an FTP server.
an80iDFSEventTrap	1.3.6.1.4.1.10728.2.1.3.0.6	This event reports the radar frequency detection on the network element
an80iIdChangedTrap	1.3.6.1.4.1.10728.2.1.3.0.7	This event reports the modification in the configuration of an ID on the network element
an80iSWUpgradeFailed	1.3.6.1.4.1.10728.2.1.3.0.8	This event reports the failure of a software upgrade operation on the network element
an80iIdSWUpgrade Success	1.3.6.1.4.1.10728.2.1.3.0.9	This event reports the success of a software upgrade operation on the network element
an80iIfRegistration FailedTrap	1.3.6.1.4.1.10728.2.10.2.0.1	This event reports the failure of a registration attempt of a subscriber unit that is not defined in the sector controller's link table.
AN80iIfRegistrationOKTrap	1.3.6.1.4.1.10728.2.10.2.0.2	This event reports the successful subscriber unit registration.
PowerSupplyFailure Trap	1.3.6.1.4.1.10728.1.8.0.6	This event reports a power supply failure on the network element. This event is only supported for AN50e devices.

SNMP Agent Alarms

The SNMP agent, can be configured to report on the health of the host system. You can configure a TCA alarm to be generated when a threshold has been exceeded.

On the **Alarms Severity Assignment** page, select **NE type** as MicrosoftSNMP_2003, NET-SNMP-SUN or NetSNMP.

Table A-12 SNMP Agent Alarms

Alarm	OID	Description
System Alarm	System Alarm	Indicates that a system fault has occurred
TCAAlarm	TCAAlarm	Indicates that a threshold for a host resource has been crossed

Redline communications

B

Synchronization Traps

RedMAX Synchronization Traps

The following event log messages and correspond traps are specific to sector controller synchronization. There are four traps that provide RMS with the status of sector controller synchronization. Two of these traps can be used for both local and GPS synchronization while the other two are specific to GPS synchronization.Network Element:Event Log Listing

Table B-1 AN100U/UX Local Synchronization Traps

Trap Name and Setting	Description
RedMAXSynchronizationTrap synchLost	The sector controller has detected a signal on the **Sync Out** port, but it is out of phase and synchronization is not currently possible. This will result in an event log and status page message showing "No synchro". A trap is sent to specified trap receivers such as RMS. When the AN100U/UX internal clock is locked and tracking again, this trap is cleared.
RedMAXSynchronizationTrap synchSignalLost	When a slave AN100U/UX does not detect the clock input signal from the Master, a trap is sent to RMS. This trap can also be sent if the Master with GPS can no longer detect the signal from the GPS. When the signal is detected again, the trap state is cleared.

Table B-1 AN100U/UX Local Synchronization Traps

Trap Name and Setting	Description
RedlineBsGpsTrapTrigger gpsHoldover	The holdover trap is able to interpret the 30-second signal suppression used by the GPS clock, to indicate the transition to holdover mode. When the AN100U has encountered the following, a trap is sent: • The message “Synchronization with GPS is Not Detected” is logged. • Thirty seconds later the message “GPS Synchronization Ok” is logged. This sequence indicates that the GPS has gone into holdover mode. The Master with GPS and all of the slave sector controllers are now being synchronized with the GPS unit’s internal oscillator. Currently the trap is not cleared. The RedMAX GPS clock does not signal a holdover_off event, and thus provides no indication to the sector controllers that a satellite signal has been re-acquired.
RedlineBsGpsTrapTrigger gpsSignalLost	When the AN100U does not detect the GPS clock input signal for longer than 30 seconds, a trap is sent. When the signal is detected again, the trap state is cleared.

Viewing Network Event Logs

You can review the event log messages, that correspond to SNMP traps being sent to RMS, on the **Network Events Log** page.

Step 1 Navigating to **Fault** > **Logs** > **Network Event Logs**.

Step 2 On the left side of the page click on the **Logs** tab and select **Network Events Logs**.

Viewing Network Element Event Logs

You can view a network element’s event messages using the pass through feature to log onto the device directly and review all of the event log messages. See “Pass Through” on page 3-18.

Interpreting RedMAX Synchronization Traps

The following table shows you the chain of events that result in synchronization traps being sent to RMS and the resulting alarms and messages in RMS, if you have configured these traps. All troubleshooting information is specific to the RedMAX network elements and the GPS clock. Other than acknowledging the alarms, you cannot correct synchronization issues from within RMS.

Table B-2 AN100U/UX Synchronization Event Log Messages

Message Reported By	Event Log Message (Logged starting from bottom to top)	Recommended Troubleshooting	RMS Log Message	RMS Alarm Details
Master with GPS	Master with GPS Function Activated GPS Synchronization Ok	Backup Master is not active. Normal Operation. No action required.	No Synchronization Alarm	
Backup Master	Synchronization with Master Ok Master Detected	Backup Master is ready, but not active. Normal Operation. No action required.	No Synchronization Alarm	
Slave	Synchronization Ok Master Detected	Slave synchronized to Master is active. Normal Operation. No action required.	No Synchronization Alarm	
Backup Master	Synchronization with GPS Ok GPS Detected Backup Function Activated Master is not Detected	Master has become disconnected, during normal operation. Normal Operation. No action required.	No Synchronization Alarm	
Backup Master	Backup Function Activated Synchronization with GPS Ok GPS Detected	Backup Master is now active. Master is Offline after reboot. Normal Operation. No action required.	No Synchronization Alarm	
Backup Master	17:33:06 GPS Synchronization Ok 17:33:02 GPS Detected 17:32:31 GPS is not Detected 17:01:33 Master with GPS Function Activated	GPS is in holdover mode GPS antenna may have become disconnected, during normal operation. After 30 Minutes of satellite signal loss, the GPS halts (squelches) its signal for 30 seconds to indicate its holdover status to the Master with GPS sector controller. Check the GPS connection to its external antenna. Refer to the RedMAX *GPS Clock User Manual.*	GPS-synchSignalLost	RedMAXSynchronizationTrap Trigger: synchSignalLost Device: masterWithGps

Table B-2 AN100U/UX Synchronization Event Log Messages (continued)

Message Reported By	Event Log Message (Logged starting from bottom to top)	Recommended Troubleshooting	RMS Log Message	RMS Alarm Details
Slave	Synchronization Signal not Detected	Master and Backup Master have become disconnected, during normal operation. Check the Master with GPS and the Backup Master and ensure they are online and that the GPS is connected to the **Sync Out** port.	No Alarms on RMS	
Backup Master (after rebooting)	Master or GPS must be connected. Waiting...	No connection between the GPS and the Master with GPS. The Master with GPS is offline. Check the Master with GPS and ensure it is online and that the GPS is connected to the **Sync In** port of the Master with GPS. Ensure that the Master with GPS is also connected to the **Sync In** port of the Backup Master.	GPS-synchLost	RedMAXSynchronizationTrap Trigger: synchLost Device: backupMaster
Slave	Synchronization Signal not Detected. Waiting...	Master and Backup Master are offline, after rebooting. Check the Master with GPS and the Backup Master and ensure they are online and that the GPS is connected to the **Sync Out** port.	GPS-synchLost	RedMAXSynchronizationTrap Trigger: synchLost Device:slave
Master	Other Master Detected. Waiting...	More than one sector controller has been configured as the Master with GPS. Change the configuration of one sector controller so that you have only one device configured as the Master with GPS.	No Alarms on RMS	

Table B-2 AN100U/UX Synchronization Event Log Messages (continued)

Message Reported By	Event Log Message (Logged starting from bottom to top)	Recommended Troubleshooting	RMS Log Message	RMS Alarm Details
Backup Master	Other Backup Detected. Waiting...	More than one sector controller has been configured as the Backup Master. Change the configuration of one sector controller so that you have only one device configured as the Backup Master.	No Alarms on RMS	
Master	Synchronization Signal not Detected. Waiting...	No Connection between the Master with GPS and the GPS Clock. Check the Master with GPS and ensure it is online and that the GPS is connected to the **Sync In** port. Check that the Master and Backup Master are synchronized.	No Alarms on RMS	
Master	GPS is not Detected	No Connection between the GPS and the Master with GPS. No event log message is displayed by the Backup Master or the Slave devices. Check the Master with GPS and ensure it is online and that the GPS is connected to the **Sync In** port.	GPS-synchLost GPS-synchSignalLost	RedMAXSynchronizationTrap Trigger: synchLost Device: masterWithGps or RedMAXSynchronizationTrap Trigger: synchSignalLost Device: masterWithGps

Table B-2 AN100U/UX Synchronization Event Log Messages (continued)

Message Reported By	Event Log Message (Logged starting from bottom to top)	Recommended Troubleshooting	RMS Log Message	RMS Alarm Details
Backup Master	State changes from Synchronization OK to GPS Synchronization Ok. All of the following messages are displayed: • Synchronization with GPS Ok • GPS Detected • Backup Function Activated • Master is not Detected • Synchronization with Master is Lost • Synchronization OK	50-ohm termination has been disconnected. Check the wiring of the GPS and the 50-ohm load termination. Verify that the load termination on the Backup Master is correctly connected and is secure. Verify that the synchronization cables on the Backup Master is correctly connected and is secure.	GPS-synchLost GPS-synchSignalLost	RedMAXSynchronizationTrap Trigger: synchLost Device: backupMaster or RedMAXSynchronizationTrap Trigger: synchSignalLost Device: backupMaster
Slave	State changes from Synchronization OK to Synchronization Lost. All of the following messages are displayed: • Synchronization Signal Detected • Synchronization Signal not Detected • Synchronization Lost • Synchronization OK	50-ohm termination has been disconnected. You should see the above-listed messages on the Backup Master.	GPS-synchLost GPS-synchSignalLost	RedMAXSynchronizationTrap Trigger is: synchLost Device: backupMaster or RedMAXSynchronizationTrap Trigger: synchSignalLost Device: backupMaster

Table B-2 AN100U/UX Synchronization Event Log Messages (continued)

Message Reported By	Event Log Message (Logged starting from bottom to top)	Recommended Troubleshooting	RMS Log Message	RMS Alarm Details
Slave	Synchronization Ok Backup Detected	Master is offline, after rebooting. Check the Master with GPS and ensure it is online and that the GPS is connected to the Master's **Sync In** port. Verify that the synchronization cables from the Master with GPS and/or the Backup Master are correctly connected to the Slaves' **Sync Out** port.	No Alarms on RMS	
Master	GPS is not Detected on the Master	No connection between the GPS and Master with GPS and the Backup Master on **Sync In** or **Sync Out** port. Check the wiring connections between Master with GPS and Backup Master, check the connection to the GPS unit. No corresponding event log messages are displayed by the Slave devices.	GPS-synchLost GPS-synchSignalLost	RedMAXSynchronizationTrap Trigger: synchLost Device: masterWithGps
Backup Master	Backup Function Activated Master is not Detected	No connection between the GPS and Master with GPS and the Backup Master on **Sync In** or **Sync Out** port. You should see the above-listed messages on the Master. Check the wiring connections between Master with GPS and the Backup Master. Also check the connections to the GPS unit. No corresponding event log messages are displayed by the Slave devices.	No Alarms on RMS	RedMAXSynchronizationTrap Trigger: synchSignalLost Device: masterWithGps

Table B-2 AN100U/UX Synchronization Event Log Messages (continued)

Message Reported By	Event Log Message (Logged starting from bottom to top)	Recommended Troubleshooting	RMS Log Message	RMS Alarm Details
Master	GPS is not Detected	No connection between the GPS and the Master with GPS and between the Master with GPS and Backup Master on the **Sync In** port. Check the wiring connections between the Master with GPS amd the Backup Master. Check the connection to the GPS unit. No corresponding event log messages are displayed by the Slave devices.	GPS-synchLost GPS-synchSignalLost	RedMAXSynchronizationTrap Trigger: synchLost Device: masterWithGps or: RedMAXSynchronizationTrap Trigger: synchSignalLost Device: masterWithGps

Redline communications

C

Installing a Hot-Swappable Hard Disk Drive

When your hard disk drive reaches 90% of its capacity you will need to add a new disk, Some operating systems will allow you to add the disk drive while the server is still running, however you will need to stop both the RMS and provisioning services.

Detailed instructions for adding a new HDD to a Sun workstation are provided here. These instructions will allow you to take down your current system, add the hardware and re-start RMS with a Provisioning Server, both configured for high availability operation.

You must proceed through the following steps in order to maintain the integrity of your system while the hardware is being replaced:

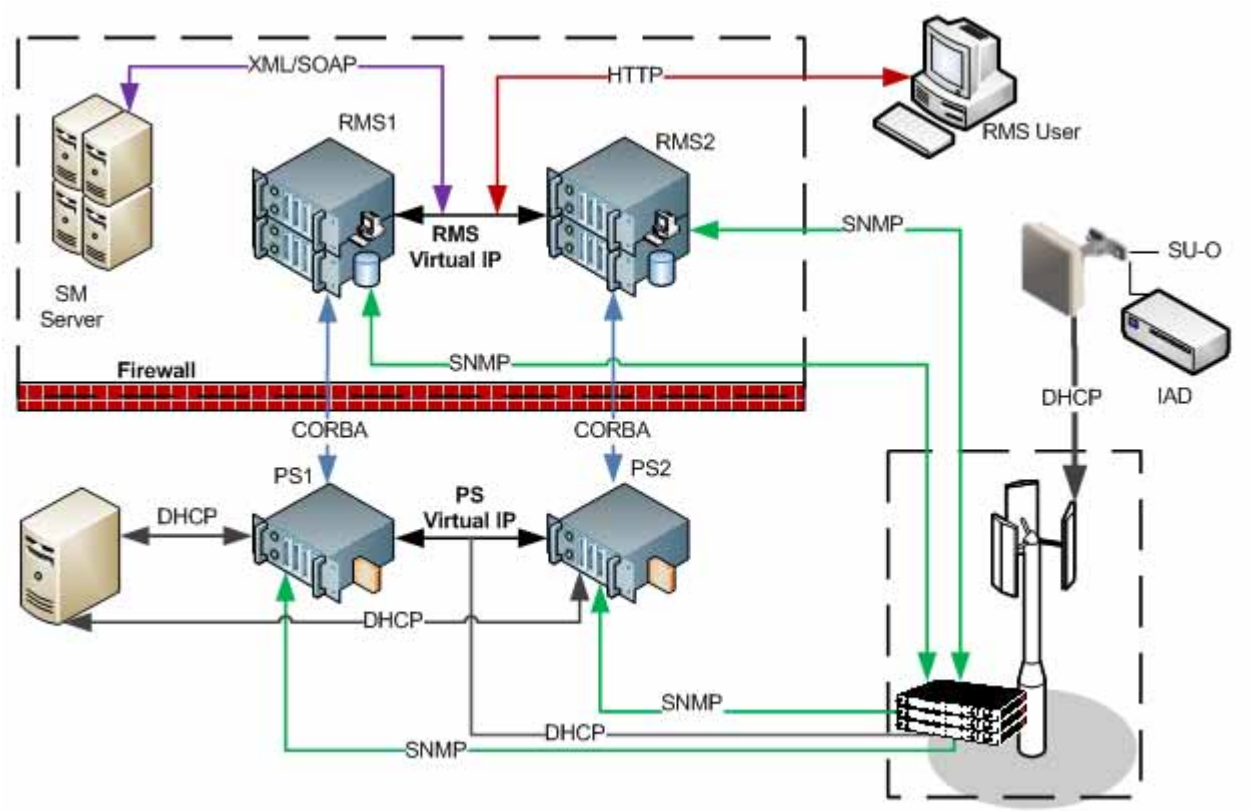
1. Backup the installation.
2. Backup the database.
3. Clean up all of the servers involved in the high availability configuration
4. Move the RMS file system from the RMS1 server (master) to a temporary storage location.
5. Shut down the provisioning services on ps2 (slave) host machine.
6. Shut down the RMS services on RMS2 (slave) host machine; the master system remains functional.
7. Add the new hard disk on RMS2 (slave) host machine.
8. Return the RMS file system to RMS2 (slave) host machine and place it on the new hard disk.
9. Restart the RMS services on RMS2 (slave) host machine.
10. Restart the provisioning services on ps2 (slave) host machine.
11. Force failover of RMS1 (master) onto the newly upgraded RMS2 (slave) system. The previous slave is now the master: RMS2 (master) and ps2 (master)
12. Shut down the provisioning services on ps1 (now slave) host machine.
13. Shut down the RMS services on RMS1 (now slave) host machine; The new master systems remain functional.

14. Add the new hard disk on RMS1 (now slave) host machine
15. Restart the RMS services on RMS1 (now slave) host machine.
16. Restart the provisioning services on ps1 (now slave) host machine.
17. This procedure also allows you to utilize the new drive as an expansion of the existing disk drive and expand the server's overall disk drive capacity.

The system in this example consists of a master and slave RMS Server as well as a master and slave Provisioning Server.

Instructions are only provided for Solaris 10 as the high availability option is only supported in this operating system. See Figure 11.

Figure C-1 Example of High Availability Configuration



Backing Up the Installation

Step 1 Backup the RMS installation from the RMS master.You can use any device with enough space to backup the directory.

On RMS1 (master), mount /<*rms_install_dir*>/RedMAXEMSX_Y_Z_nnn/backup of RMS1 onto the Provisioning Server PS2 (slave). Run the following command:

```
mount <RMS1>/opt/remotebackup
<PS2>/opt/<rms_install_dir>/RedMAXEMSX_Y_Z_nnn/backup
```

Step 2 Verify the directory is mounted on the temporary storage location:

```
df -k
```

Step 3 Backup the RMS database using the DbBackup task from the RMS GUI client. If you have created a backup task, then run it as follows:

Config > **Admin** > **Tasks**

Select the backup task from the list on the **Tasks** page, right-click and select **Run** from the popup box.

Step 4 If you need to create a new task, refer to “DbBackup Task” on page 6-2. Configure the new task recurrence as **On Demand,** so that it can be run immediately.

Step 5 Check the /opt/<*rms_install_dir*>/RedMAXEMSX_Y_Z_nnn/backup directory on RMS1 (master) to confirm that the DbBackup<*DDMMYY*>.sql file has been created. The same file should also appear in /opt/remotebackup directory on the PS2 (slave) host machine.

```
cd /opt/<rms_install_dir>/
ls
cd /ps2/opt/remotebackup
ls
```

Cleaning Up the High Availability Systems

You now need to clean up the HA system by running HACleanup. If you have created a backup task, then run it as follows:

Step 1 In the RMS GUI client, navigate to:

Config > **Admin** > **Tasks**

Step 2 Select the HACleanup task from the list on the **Tasks** page, right-click and select **Run** from the popup box.

Step 3 If you need to create a new task, refer to “Configuring the DbCleanup Task” on page 5-8.

Shutting Down the Provisioning Service on the Slave Host Machine

If the Provisioning Server is installed on a separate machine, shut down the provisioning service as follows. on the PS2 (slave) host

Step 1 Log in as root via SSH:

```
ssh root@<IP Address of PS2>
<password>
```

Step 2 Navigate to /<*rms_install_dir*>/RedMAXEMSX_Y_Z_nnn:

```
cd /<rms_install_dir>/*X_Y_Z_nnn
```

Step 3 Shut down ProvServerdX_Y_Z_nnn service on PS2 (slave) host.

```
svcadm disable –s
svc:/site/ProvServerdX_Y_Z_nnn:ProvServerdX_Y_Z_nnn
```

Shutting Down the RMS Services on the Slave Host Machine

On RMS2 (slave) machine shut down the RMS services.

Step 1 Log in as root via SSH:

```
ssh root@<IP Address of RMS2>
<password>
```

Step 2 Navigate to /<*rms_install_dir*>/RedMAXEMSX_Y_Z_nnn

```
cd /<rms_install_dir>/*X_Y_Z_nnn
```

Step 3 Shut down the RMS, Naming, Notification and MySQL services on RMS2 (slave) host machine. Stop the provisioning service first, if it is installed on the same machine.

```
svcadm disable -s
svc:/site/ProvServerdX_Y_Z_nnn:ProvServerdX_Y_Z_nnn
svcadm disable -s svc:/site/RedMAXEMSX_Y_Z_nnn:RedMAXEMSX_Y_Z_nnn
svcadm disable -s svc:/site/namingServicedX_Y_Z_nnn:
namingServicedX_Y_Z_nnn
svcadm disable -s svc:/site/notifSvcX_Y_Z_nnn:notifSvcX_Y_Z_nnn
svcadm disable -s svc:/site/RMS_DBX_Y_Z_nnn:RMS_DBX_Y_Z_nnn
```

Step 4 Verify the status of the RMS services:

```
ps –ef | grep X_Y
```

Installing and Formatting the New Hard Disk

Step 1 Install the new hard disk as outlined in your Sun Server Module Service Manual.

Note If the new hard disk drive is not hot swappable then you must power down your machine. Please refer to the instructions provided with the hard disk and to the applicable Service Manual.

Step 2 Obtain the file system name of the new hard disk <*new_hd*>. You will need this file system name to mount the device.

Use the Solaris 10 command cfgadm -al to list all disks in the device tree, including disks that have not yet been configured. The cfgadm command provides configuration administration operations on dynamically, reconfigurable hardware resources.

```
cfgadm -al
```

Step 3 The utility devfsadm maintains the /dev namespace. The default operation is to attempt to load every driver in the system and attach to all possible device instances. Next, devfsadm creates logical links to device nodes in /dev and /devices and loads the device policy.

The daemon version, devfsadmd of devfsadm is started during system startup and is responsible for handling both reconfiguration boot processing and updating /dev and /devices in response to dynamic reconfiguration event notifications from the kernel.

If the disk is not in the list, such as with a newly installed disk, and devfsadmd is not running you can use devfsadm to configure the new hard disk into the device tree. Refer to the man page for devfsadm for more details.

```
devfsadm -r /
```

Where: -r root_dir indicates that the /dev directory trees are located directly under root (/).

Step 4 Format the new disk drive. When you use the Solaris format utility, you need to provide various types of information depending how you will use the disk drive. Please refer to the documentation provided with your hard disk or to sun.com for specific details

Adding RMS Files to the New Hard Disk Drive

Step 1 Create a new file system and mount it to a temporary location on the new drive.

```
mkdir –p /mnt/tempdir
mount /dev/<new_hd> /mnt/tempdir
```

Step 2 Move all of your directories from /<*rms_install_dir*> to the temporary directory on the new drive:

```
mv /<rms_install_dir>/* /mnt/tempdir/
```

Step 3 Verify the RMS data is on the new drive:

```
ls –ltr
```

Step 4 Remove the old directory from the file system:

```
umount /<rms_install_dir>
```

Step 5 Mount the new drive to the correct location on the file system:

```
mount /dev/<new_hd> /<rms_install_dir>
```

Step 6 Make this change permanent, by updating the record in /etc/vfstab. You must ensure the selected mount point is added to the selected device at boot.

```
vi /etc/vfstab
```

Example C-1 Updating /etc/vfstab

```
#device             devices               mount      FS     fsck   mount at  mount
#to mount           to fsck               point      type   pass   boot      options
/dev/dsk/c0t3d0s7   /dev/rdsk/c0t3d0s7     /opt/RMS   ufs    2      yes       -
```

Step 7 Save your changes and close the file:

```
:wq
```

Step 8 Move RMS data from /mnt/tempdir to the newly mounted RMS directory:

```
mv /mnt/tempdir/* /<rms_install_dir>/
```

Step 9 Unmount the temporary directory:

```
umount /mnt/tempdir
```

Step 10 Verify the new disk has been configured correctly and that the available space has increased.

```
df -k
```

Start RMS Services on the Slave Host Machine

On the RMS2 (slave) host machine start the RMS services:

Step 1 Log in as root via SSH:

```
ssh root@<IP Address of RMS2>
<password>
```

Step 2 Verify the status of the system:

```
ps –ef | grep X_Y
```

Step 3 If no services are running start each RMS service in the following order: MySQL, notifications service, naming service and then RMS. Start the Provisioning Server last, if it is installed on the same machine.

```
svcadm enable -s svc:/site/RMS_DBX_Y_Z_nnn:RMS_DBX_Y_Z_nnn
svcadm enable -s svc:/site/notifSvcX_Y_Z_nnn:notifSvcX_Y_Z_nnn
svcadm enable -s svc:/site/namingServicedX_Y_Z_nnn:
namingServicedX_Y_Z_nnn
svcadm enable -s svc:/site/RedMAXEMSX_Y_Z_nnn:RedMAXEMSX_Y_Z_nnn
svcadm enable -s svc:/site/ProvServerdX_Y_Z_nnn:ProvServerdX_Y_Z_nnn
```

Step 4 Verify the status of the RMS services:

```
ps –ef | grep X_Y
```

Start the Provisioning Service on Slave Host Machine

If the Provisioning Server is installed on a separate machine, start it up as follows. In Figure C-1, this is the PS2 (slave) machine.

Step 1 Log in as root via SSH:

```
ssh root@<IP Address of PS2>
<password>
```

Step 2 Verify the status of the system:

```
ps –ef | grep prov
```

Step 3 If the provisioning service is not running, start it now:

```
svcadm enable –s svc:/site/ProvServerdX_Y_Z_nnn:ProvServerdX_Y_Z_nnn
```

Step 4 Verify these services have started:

```
ps –ef | grep prov
```

Verify High Availability Functionality

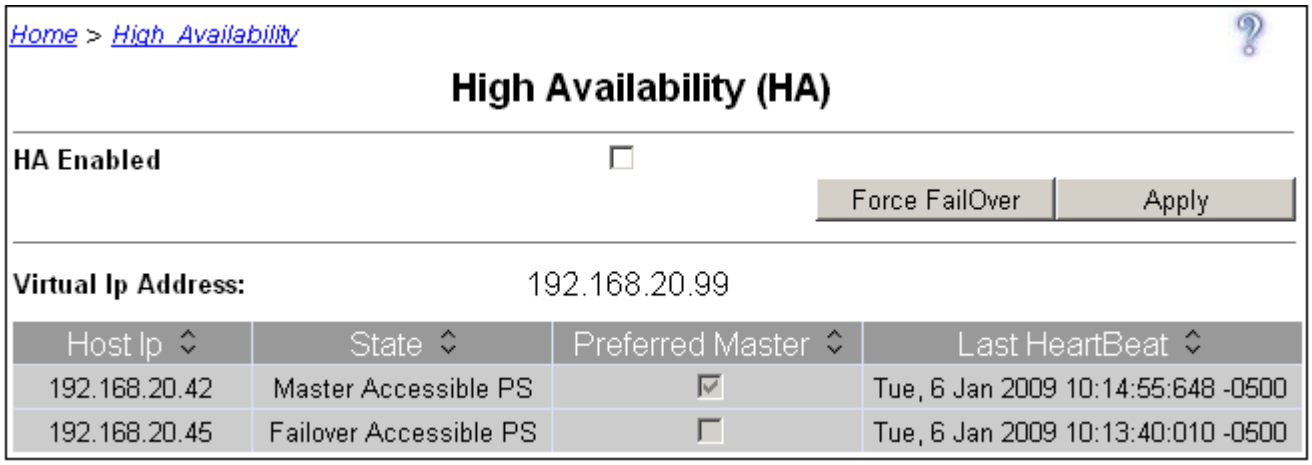
Once the slave systems have been re-started the system should return to high availability operation

Step 1 Verify high availability functionality on the RMS GUI client. Open a browser and log into RMS using http://<*Virtual IP*>:8080/RedMAXEMS/

Step 2 Navigate to **Config > System > HA**.

Step 3 Ensure both master and slave RMS services are accessible to the Provisioning Server(s).

Figure C-2 High Availability Page



Step 4 While still on the **High Availability** page, click the **Force Failover** button to force failover from the current master (RMS1) to the slave (RMS2).

RMS2 now becomes the master server, so that you can upgrade RMS1

Shutting Down the Provisioning Service on the Slave Host Machine

If the Provisioning Server is installed on a separate host machine, then stop the provisioning services. In Figure C-1, this is the PS1 (now slave) machine.

Step 1 Log in as root via SSH:

```
ssh root@<IP Address of PS1>
<password>
```

Step 2 Navigate to /*<rms_install_dir>*/RedMAXEMSX_Y_Z_nnn:

```
cd /<rms_install_dir>/*X_Y_Z_nnn
```

Step 3 Shut down ProvServerdX_Y_Z_nnn service on PS2 (slave) host.

```
svcadm disable –s
svc:/site/ProvServerdX_Y_Z_nnn:ProvServerdX_Y_Z_nnn
```

Shutting Down the RMS Services on the Slave Host Machine

On the RMS1 (now slave) machine shut down the RMS services. Stop the Provisioning Server first, if it is installed on the same machine.

Step 1 Log in as root via SSH:

```
ssh root@<IP Address of RMS1>
<password>
```

Step 2 Navigate to /<*rms_install_dir*>/RedMAXEMSX_Y_Z_nnn

```
cd /<rms_install_dir>/*X_Y_Z_nnn
```

Step 3 Shut down the RMS, Notification and MySQL services on the RMS1 (now slave) host machine. Shut down the Provisioning Server first, if it is installed on the same machine.

```
svcadm disable -s
svc:/site/ProvServerdX_Y_Z_nnn:ProvServerdX_Y_Z_nnn
svcadm disable -s svc:/site/RedMAXEMSX_Y_Z_nnn:RedMAXEMSX_Y_Z_nnn
svcadm disable -s svc:/site/namingServicedX_Y_Z_nnn:
namingServicedX_Y_Z_nnn
svcadm disable -s svc:/site/notifSvcX_Y_Z_nnn:notifSvcX_Y_Z_nnn
svcadm disable -s svc:/site/RMS_DBX_Y_Z_nnn:RMS_DBX_Y_Z_nnn
```

Step 4 Verify the status of the RMS services:

```
ps –ef | grep X_Y
```

Installing and Formatting the New Hard Disk

Step 1 Install the new hard disk as outlined in the Sun Server Module Service Manual.

Note If the new hard disk drive is not hot swappable then you must power down your machine. Please refer to the instructions provided with the hard disk and to the applicable Service Manual.

Step 2 Obtain the file system name of the new hard disk <*new_hd2*>. You will need this file system name to mount the device.

List all disks in the device tree, including disks that have not yet been configured.

```
cfgadm -al
```

If the disk is not in the list, such as with a newly installed disk, and devfsadmd not running you can use devfsadm to configure the new hard disk into the device tree. See the devfsadm man page for details.

```
devfsadm -r /
```

Step 3 Format the new disk drive. When you use the Solaris format utility, you need to provide various types of information depending on how you will use the disk drive. Please refer to the documentation provided with your hard disk or to sun.com for specific details

You can format your hard drive in different ways depending on your requirements. For example, you can use logical values to allow for growth of your data beyond the current disk boundaries, or you can use partitions to increase concurrency. This will be determined as part of your network management plan. Consult your system administrator for details.

Adding RMS Files to the New Hard Disk Drive

Step 1 Create a new file system and mount it to a temporary location on the new drive.

```
mkdir –p /mnt/tempdir
mount /dev/<new_hd> /mnt/tempdir
```

Step 2 Move all of your directories from //<*rms_install_dir*> to the temporary directory on the new drive:

```
mv /<rms_install_dir>/* /mnt/tempdir/
```

Step 3 Verify that the RMS data is on the new drive:

```
ls –ltr
```

Step 4 Remove the old directory from the file system:

```
umount /<rms_install_dir>
```

Step 5 Mount the new drive to the correct location on the file system:

```
mount /dev/<new_hd2> /<rms_install_dir>
```

Step 6 Make this change permanent, by updating the record in /etc/vfstab. You want to ensure the selected mount point is added to the selected device at boot. See on page C-6

```
vi /etc/vfstab
```

Step 7 Save your changes and close the file:

```
:wq
```

Step 8 Move RMS data from /mnt/tempdir to the newly mounted RMS directory:

```
mv /mnt/tempdir/* /<rms_install_dir>/
```

Step 9 Unmount the temporary directory:

```
umount /mnt/tempdir
```

Step 10 Verify the new disk has been configured correctly and that the available space has increased.

```
df -k
```

Start RMS Services on Slave Host Machine

On the RMS1 (now slave) host machine start the RMS services. Start the Provisioning Server last, if it is installed on the same machine.

Step 1 Log in as root via SSH:

```
ssh root@<IP Address of RMS1>
<password>
```

Step 2 Verify the status of the RMS services:

```
ps –ef | grep X_Y
```

Step 3 If no services are running start each RMS service in the following order: MySQL, Notification, Naming and then RMS. If the Provisioning Server is installed on the same machine start that service last.

```
svcadm enable -s svc:/site/RMS_DBX_Y_Z_nnn:RMS_DBX_Y_Z_nnn
svcadm enable -s svc:/site/notifSvcX_Y_Z_nnn:notifSvcX_Y_Z_nnn
svcadm enable -s svc:/site/namingServicedX_Y_Z_nnn:
namingServicedX_Y_Z_nnn
svcadm enable -s svc:/site/RedMAXEMSX_Y_Z_nnn:RedMAXEMSX_Y_Z_nnn
svcadm enable -s svc:/site/ProvServerdX_Y_Z_nnn:ProvServerdX_Y_Z_nnn
```

Step 4 Verify the status of the RMS services:

```
ps –ef | grep X_Y
```

Start Provisioning Services on Slave Host Machine

If the Provisioning Server is installed on a separate host machine, then start the provisioning services. In Figure C-1, this is the PS1 (now slave) machine.

Step 1 Log in as root via SSH:

```
ssh root@<IP Address of RMS2>
<password>
```

Step 2 Verify the status of the system:

```
ps –ef | grep prov
```

Step 3 If the provisioning service is not running, start it now:

```
svcadm enable –s svc:/site/ProvServerdX_Y_Z_nnn:ProvServerdX_Y_Z_nnn
```

Step 4 Verify these services have started:

```
ps –ef | grep prov
```

Verify High Availability Functionality

Once the RMS and Provisioning Server slave systems have been re-started the system should return to high availability operation.

Step 1 Verify high availability functionality on the RMS GUI client. Open a browser and log into RMS using http:// <*Virtual IP Address of* RMS>:8080/RedMAXEMS/

Step 2 Navigate to **Config** > **System > HA**.

Step 3 Ensure both master and slave RMS services are accessible to the Provisioning Servers.

Step 4 While still on the **High Availability** page, click on the **Force Failover** button to force failover from RMS2 back to RMS1.

Step 5 Ensure RMS1 is selected as the Preferred Master, by enabling the appropriate check box on the **High Availability** page. See Figure C-1.

Step 6 Monitor the system for stability for 5 to10 days. Monitor the host resources and ensure memory usage is stable. Monitor the system for unexpected failover.

Redline communications

D

Configuring System Logging with Log4j.xml

Apache log4j is a Java-based logging utility. Logging of various types of RMS information and system parameters is managed by the log4j utility. You can configure the way in which RMS and the Provisioning Server manage logged data and enable different types of logging by editing the log4j.xml files.

Configuring logging using a configuration file allows you to turn logging on or off without modifying RMS functionality. RMS can run with logging off until you encounter a problem, and then logging can be turned on by modifying the configuration file.

The following table defines the log levels and messages in Log4j, in decreasing order of severity. The first column lists the log level designation in Log4j and the second column provides a brief description of each log level.

Table D-1 Log4j Error Levels

Level	Description
FATAL	Severe errors that result in unexpected termination of RMS services. This level is not used by RMS.
ERROR	Other runtime errors or unexpected conditions.
WARN	Use of deprecated APIs, poor use of API, 'almost' errors, any other runtime situation that is undesirable or unexpected, but will not lead to system failure.
INFO	Interesting runtime events, such server startup or shutdown.
DEBUG	Detailed information on the data flowing through the system. Expect these to be written only to logs.
TRACE	More detailed logging information. Expect these to be written to logs only. This level is not used by RMS.

You can configure log4j through the log4j.xml file. Three main components are defined in this file: Loggers, Appenders and Layouts.

- Loggers are logical log file names known to the Java application. Each logger can be configured independently with respect to the logging level (ERROR, etc) it provides.

- Appenders provide the actual log output. There are numerous Appenders available, with descriptive names, such as FileAppender, ConsoleAppender, SocketAppender, SyslogAppender, NTEventLogAppender and SMTPAppender. Multiple Appenders can be attached to any Logger, so it is possible, for example, to log the same information to a file locally and to a socket listener on another computer.
- Layouts are used by the Appenders, to format the log entries, such as (as SimpleLayout or PatternLayout.

Separate log4j configuration files are provided for RMS and the Provisioning Server.

Note When editing the XML files you must be very careful with carriage returns. No end-of-line (EOL) characters are allowed in these configuration files. You must only replace selected values.

After the log4j.xml configuration file has been revised changes to logging configuration will take effect on the server within a few minutes.

Note Enabling logging or changing levels from error to warn/info/debug will impact system performance.

Windows Server 2003

Step 1 Using Windows Explorer, navigate to the following directory.

`<rms_install_dir>\conf`

Step 2 Locate the file named log4j.xml and create a backup copy of this file. This is the configuration file for RMS logging.

Right-click on the file name and select **Copy**. Right-click in the selected directory and select **Paste**. Rename the copy to log4j.bak

Step 3 Open the file in a text editor that recognizes XML file structures and make your required changes. Save and close the updated file.

Step 4 The log4j configuration file for the Provisioning Server is located in the following directory:

`<rms_install_dir>\provServer\conf`

Step 5 Create a backup copy of this file. This is the configuration file for Provisioning Server logging.

```
cp log4j.xml log4j.bak
```

Step 6 Update the file, making the same changes that you have made for the RMS Server.

Solaris 10

Step 1 Log into the RMS host machine as the root user:

```
rlogin <rms_host> –l root
<root password>
```

Step 2 Navigate to the following directory.

```
<rms_install_dir>/bin/
```

Step 3 Locate the file named log4j.xml and create a backup copy of this file. This is the configuration file for RMS logging.

```
cp log4j.xml log4j.bak
```

Step 4 Open the file in a text editor that recognizes XML file structures and make your required changes. Save and close the updated file.

Step 5 The log4j configuration file for the Provisioning Server is located in the following directory:

```
<rms_install_dir>/provServer/bin
```

Step 6 Create a backup copy of this file. This is the configuration file for Provisioning Server logging.

```
cp log4j.xml log4j.bak
```

Step 7 Update the file, making the same changes that you have made for the RMS Server.

Index

A

Adding
- New Hard Disk Drive C-1

Administration, System 2-1

Archiving RMS Data 4-6

Auto Discovery, Configuring Task 5-8

Auto-Reset, Configuring 2-6

B

Backup
- Database Command Line Utility 6-3
- Database Task 6-2
- NE Config, Log Files 5-12
- NE Config Image Name 5-11
- NE Config Scheduling Option 5-10

Buffer Overflow 4-8, 4-23

C

Charts, Host Resource Usage 3-2

CINR
- Threshold Values 3-10, 3-11

CINR Threshold Values 3-7

Configuring
- Auto Discovery 3-6, 5-8, 5-9
- Auto-Reset 2-6
- DbCleanup 5-8
- DbCleanup of HRStats 3-6
- HaMyReportSync Task 8-11
- NE Config Backup Task 5-10
- PMCleanup 5-3
- PM Data Export Task 5-9
- PSCleanup 5-3
- Reporting Tasks 5-4
- Solaris sar Command 4-16

Connectivity
- Normal/Poor 3-7

CORBA Port
- Provisioning Server 2-8

CPU Usage 4-2
- Core Saturation 4-15
- Monitoring 4-12
- Monitoring Using sar 4-16
- Monitoring Using Windows perfmon 4-8, 4-13

D

Database
- Backup 6-3
- Backup using CLI 6-4

CLI commands and Queries 6-10
Disk Usage Statistics 6-6
Dump and Failover 8-10
Maintenance, HACleanup 8-11
Maintenance Utilities 6-1
mysqlcheck Utility 6-12
Optimizing 6-14
Port Number 6-13, 6-14
Resizing 6-15
Starting and Stopping 6-10
Synchronization 8-2, 8-10
Trace 6-12, 6-13, 6-14
Verifying Integrity 6-12
Veriyfing Size 6-14
DbBackup
Command Line Utility 6-3
File Location 6-3
Running 6-2
DbCleanup
Configuring HRStats Task 3-6
Configuring Task 5-8
Running 6-5
Window Interval 5-4, 6-6
Defragmenting Hard Disk 4-11
Determining a System Maintenance Plan 4-1
Diagnostic
Configuring Data Cleanup 5-3
Generating Performance Reports 7-1
Running Cleanup 5-3, 7-2
Diagnostic Polling
Modifying Interval 2-7
Setting Interval 2-7
Discovery Tab, Host Resources 3-3
Duplicating System Task 5-5

E

Error Message 8-4
Resources with Key Remote not found 8-4
Event Log
Synchronization Messages B-2
Exporting, Performance Management Data . . 5-9

F

Failover
and Data Dump 8-1
and Garbage Collection 2-9
Forced 8-1
For Maintenance Purposes C-8
Recovery from 8-4
Filtering
Provisioning Log Entries 7-3
Task Log Entries 5-12
FTP Server
Adding/Modifying 3-12
Adding/Modifying for NE Backup Config . . 5-11
Adding/Modifying for PM Data Export 5-10

G

Garbage Collection 2-9
General Tab, Host Resources 3-2
Generating System Reports 7-1
GPS Synchronization
Holdover Mode B-3
Traps B-1
Troubleshooting B-2

H

HACleanup, Running C-3
HaMyReportSync, Creating Task 8-11
Hard Disk
  Adding New Hardware C-1
  Checking Capacity 4-5
  Clearing Space 4-6
  Defragmenting 4-11
  HACleanup Utility 8-11
  Monitoring I/O 4-7
  Monitoring Swap Space 4-22
  Monitoring Usage 4-4
  Optimizing Database 6-14
Heap Size
  Configuring Auto-Reset 2-6
  Setting for Memory Allocation 3-3, 4-20
High Availability
  and Garbage Collection 2-9
  Database Backup 6-4
  Database Dump 8-10
  Disk Cleanup Utility 8-11
  Example Configuration C-2
  Extended Slave Downtime 8-13
  Force Failover 8-1
  HaMyReportSync Task 8-11
  Maintenance 8-1
  Recovering from Failover 8-4
  Server Status 8-6
  Status Messages 8-6
  Using for Maintenance C-1
Host Reachable Utility 3-16
Host Resources
  Creating TCA 3-6
  Discovery Tab 3-3
  General Tab 3-2
  Maintenance Plan 4-1
  Memory Tab 3-4
  Monitoring 3-1
  Network Tab 3-5
  Processors Tab 3-5
  RMS 4-2
  Storage Tab 3-5
  Usage Charts 3-2
  VM Stats Tab 3-3
HourlySCBandwidthReport.sh 2-18
HourlySUBandwidthReport.sh 2-18
HourlySUChanMeasurReport.sh 2-18

I

InnoDB, Increase Tablespace 6-15

J

Java
  JDK 2-12
  JMX Configuration 3-1
  jstat Utility 2-12
  JVM Memory Threshold 2-6
  Tuning Garbage Collection 2-9

L

Link Health 3-10, 3-11
  Normal/Poor 3-7
  Subscriber Unit 3-7
Log Entries 5-12
  Filtering 5-12, 7-3
  Modifying Log4j D-2

Network Event Logs B-2
Provisioning Server 7-3
Upgrade 5-12, 7-2
Log Files
MySQL Bin and Bin Relay 8-13
Provisioning Server 7-2
Removing from RMS 4-6
Reviewing 7-2

M

Maintenance
Creating a Plan 4-1
Creating Tasks 5-6
Database Utilities 6-1
High Availability 8-1
Plan for Host Machines 4-1
SystemTasks 5-1
Managing
Reports 8-11
RMS Through the GUI 3-1
Memory
Heap Settings 3-3
Monitoring 4-18
Monitoring Swap Space 4-22
Setting Heap Size 4-20
Memory Tab, Host Resources 3-4
Messages
Synchronization B-2
Modifying
CINR Threshold Values 3-10, 3-11
Diagnostic Polling Interval 2-7
log4j.xml D-2
NE Upgrade Configuration 2-5
Provisioning Server Configuration Files ... 2-4
RMS Configuration Files 2-4
SNMP Parameters 4-24
System Tasks 5-1
Upgrade Configuration 2-5
Virtual Memory 4-20
Monitoring
CPU Usage 4-2, 4-12
Determining a Plan 4-1
Hard Disk I/O 4-7
Hard Disk Usage 4-4
Host Machine Resources 3-1
Memory Management 4-17
Network Element Connectivity 3-7
RMS Processes Memory Usage 4-18
Swap Space 4-22
MySQL
CLI Commands and Queries 6-10
Debug 6-14
Extended Slave Downtime 8-13
mysqlcheck Utility 6-12
Starting and Stopping Service .. 2-9, 2-14, 6-11
Trace File 6-14
Trace Utility 6-12, 6-13, 6-14
Veriyfing Database Size 6-14

N

Naming Subscriber Units 5-3
NE Config Backup
Configuring Task 5-10
Image Name 5-11
netstat usage 4-27
Network Element
Audit Task 5-3
Auto-Discovery Task 5-8

Configuration Backup 5-10
Discovered Sub-Networks 3-3
Enabling Diagnostic Polling 2-7
Event Log Listing B-2
Link Health 3-10, 3-11
Synchronization Traps B-1
NetworkTab, Host Resources 3-5

P

Pass Through Utility 3-18
Performance
Tuning Garbage Collection 2-9
Performance Reports
Enabling Diagnostic Polling 2-7
PMCleanup
Configuring 5-3
Running 5-3, 7-2
PM Data Export, Configuring Task 5-9
Polling Interval
Modifying Diagnostic 2-7
Setting Diagnostic 2-7
Port
Allocation 4-4, 4-26
Database 6-13, 6-14
Verifying Status 4-4, 4-27
Processors Tab, Host Resources 3-5
Properties
ProxyAgent 4-25
SystemManager Service 2-7
UpgradeService 2-5
Provisioning Server
Log Entries 7-2
Log Files 7-2
PSCleanup Task 7-2
Replacing/Updating License 3-14, 3-15
Viewing Log Entries 7-3
Provisioning Service
Starting Slave C-7, C-11
Stopping Slave C-3, C-8
PSCleanup
Configuring 5-3
Running 7-2
Window Interval 7-2

R

RedMAX
SNMP Traps A-10
Threshold Crossing Alerts A-1
redmaxServer.sh 2-11, 2-18
Renaming a Task 5-5
Reports
Automated Task 5-4
Generating from the Command Line 2-18
Provisioning Server 7-1
Resizing the Database 6-15
Resources with Key Remote not Found Message 8-4
RMS
Host Resources 4-2
Monitoring Processes) 4-18
Services 2-3
Supported Hardware 1-3
Supported Redline Equipment 1-3
Tuning Garbage Collection 2-9
Utility C-4, C-8
RMS Services
Starting Slave C-6
Stopping Slave C-4, C-8

RSSI
Threshold Values 3-7
Running
DbBackup 6-2
DbCleanup 6-5
DbRestore 6-7
Diagnostic Cleanup 5-3, 7-2
HACleanup 8-11, C-3
mysqlcheck 6-12
PMCleanup 5-3
PSCleanup 7-2
Reporting Utilities 2-18

S

Scheduling
Maintenance Tasks 5-1, 5-6
System Tasks 5-1
Service
Starting/Stopping MySQL 2-9, 2-14, 6-11
Starting Provisioning Slave C-7, C-11
Starting RMS Slave C-6
Stopping Provisioning Slave C-3, C-8
Stopping RMS Slave C-4, C-8
Verifying Status of RMS C-7, C-11
Service Definition
ProxyAgent 4-25
SystemManager 2-7
UpgradeService 2-5
Setting
Diagnostic Polling Interval 2-7
SMTP Server, Adding/Modifying 3-13
SNMP Parameters
Modifying 4-24
SNMP Traps
Network Element Synchronization B-1
RedACCESS Devices A-12
RedCONNEX Devices A-12
RedMAX Devices A-10
Solaris
crontab 4-16
sar Command 4-16
Special Characters 3-14, 5-12
Starting
Provisioning Slave Services C-7, C-11
RMS Slave Services C-6
Starting and Stopping
Database Service 6-10
MySQL 2-9, 2-14, 6-11
Status
High Availability Servers 8-6
Stopping
Provisioning Slave Service C-3, C-8
RMS Slave Services C-4, C-8
Storage Tab, Host Resources 3-5
Subscriber Units
HourlySUBandwidthReport.sh 2-18
Replacing Name 5-3
Supported
Redline Equipment 1-3
Supported Hardware 1-3
Swap Space, Monitoring 4-22
Synchronization
Messages B-2
System
Administration 2-1
Garbage Collection Statistics 2-9
Maintenance Plan 4-1
Monitoring CPU Usage 4-12
Monitoring Heap Settings 3-3

Monitoring Host Resources 3-1
Monitoring Memory Management 4-17
Monitoring Swap Space 4-22
Reports 7-1
Tasks 5-1

T

Task
Auto Discovery 3-6, 5-8, 5-9
Configuring Reporting 5-4
Creating Custom 5-6
DbCleanup 5-8
DbCleanup of HRStats 3-6
Diagnostics Cleanup 5-3
Duplicating 5-5
HACleanup 8-11, C-3
HaMyReportSync 8-11
NE Config Backup 5-10
Network Audit 5-3
PMCleanup 5-3
PMDataExport 5-9
PSCleanup 5-3
Renaming 5-5
Reviewing Log Entries 5-12, 7-3
Running DiagnosticCleanup 5-3, 7-2
Running PMCleanup 5-3, 7-2
Running PSCleanup 7-2
Scheduling 5-1, 5-6
Standard System 5-1
Viewing Details 5-5
Viewing Log Entries 5-12
TCA, Creating for Host Resources 3-6
TFTP Server
Adding/Modifying 3-13
Threshold Crossing Alerts
Creating for Host Resources 3-6
PMP Connection States A-8
PMP Devices A-7
PTP Devices A-5
RedCONNEX Devices A-4
RedMAX Devices A-1
Service Flows A-3
Trace Route Utility 3-16
Traps
Network Element Synchronization B-1
RedACCESS Devices A-12
RedCONNEX Devices A-12
RedMAX Devices A-10
Troubleshooting Tools
Host Reachable 3-16
Pass Through 3-18
Trace Route 3-16

U

UDP Buffer Overflow 4-8, 4-23
Upgrade
Log Entries 5-12
Modifying Configuration 2-5
Service Definition 2-5
User Account, For Restored Database 6-7
Utility
DbBackup.bat/ksh 6-3
HACleanup 8-11
HourlySCBandwidthReport.sh 2-18
HourlySUBandwidthReport.sh 2-18
HourlySUChanMeasurReport.sh 2-18
jstat 2-12
mysqlcheck 6-12

redmaxServer.sh 2-11, 2-18
RMS C-4, C-8
ServiceConfigMgr.bat 2-5, 2-6, 4-24

V

Variables
NE Config Backup Image Name 5-11
Verifying
Database Backup Completion 8-10
Database Size 6-14
High Availability Functionality C-12
Port Status 4-4, 4-27
RMS Service Status C-7, C-11
Viewing Task Details 5-5
Virtual Memory
Modifying 4-20
VM Stats
Host Resources Tab 3-3
Monitoring 4-20

W

Wizard
Windows' Disk Cleanup 4-7

X

XML Configuration File
log4j.xml D-2
ProvServerConfiguration.xml 2-5
ServerConfiguration.xml 2-5
VirtualIfConfig.xml 2-5