

StorageTek Tape Analytics

Administration Guide

Release 2.0

E39010-01

April 2014

StorageTek Tape Analytics Administration Guide, Release 2.0

E39010-01

Copyright © 2012, 2014, Oracle and/or its affiliates. All rights reserved.

Primary Author: Kristofer Vickland

Contributing Authors: Nancy Stevens, Greg Barnes

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Contents

Preface	vii
Audience	vii
Documentation Accessibility	vii
Related Documents	vii
Conventions	viii
What's New	ix
1 RDA Logging	
1.1 Overview	1-1
1.2 Collecting RDA Information With the User Interface	1-2
1.2.1 Access the Service Logs Screen	1-2
1.2.2 Take an RDA Snapshot	1-2
1.2.3 Download a Log Snapshot	1-2
1.2.4 Display Log Run Information	1-3
1.2.5 Delete a Log Snapshot	1-3
1.3 Collecting RDA Information With the CLI	1-3
1.4 Forwarding the Log Snapshot to Oracle Support	1-4
2 Server Administration	
2.1 Managed Servers	2-1
2.2 Memory Usage Requirements	2-1
2.3 Global Administration Commands	2-2
2.4 Individual Service Administration Commands	2-3
3 Database Services Administration	
3.1 STA Services Daemon	3-1
3.2 STA Backup Service	3-2
3.2.1 Configuration	3-2
3.2.2 Full Backup Process	3-2
3.2.3 Display the Backup Service Preference Settings	3-3
3.2.4 Clear Preference Settings	3-3
3.2.5 Verify Files Have Been Sent to the Target Server	3-3
3.2.5.1 Check the Server Logs and Target Backup Server	3-4

3.2.6	Verify a Local Copy of the Backup Files Appears on the Server	3-4
3.2.7	Reset the STA Backup Service Password	3-4
3.3	STA Resource Monitor Service	3-4
3.3.1	Configuration	3-5
3.3.2	Query the Current Resource Monitor Preference Settings	3-5
3.3.3	Clear the Resource Monitor Preference Settings	3-6
3.3.4	Reset the STA Resource Monitor Password.....	3-6
3.4	Resource Monitor Reports	3-6
3.4.1	Resource Monitor Standard Report	3-6
3.4.2	Resource Depletion Alert Report.....	3-7
3.5	File Types and Locations	3-8
3.5.1	STA Services Daemon Startup/Shutdown Script.....	3-8
3.5.2	STA Administration Utilities	3-8
3.5.3	Executable Program Locations	3-9
3.5.4	Backup File Locations	3-9
3.5.4.1	STA Services Daemon and Backup Service Admin Logs	3-9
3.5.4.2	MYSQL Database Dump Files	3-10
3.5.4.3	MySQL Binary Logs	3-10
3.5.4.4	STA Services Daemon and WebLogic Configuration Files	3-10
3.5.5	Resource Monitor File Locations	3-11
3.5.5.1	STA Services Daemon and ResMonAdm Logs.....	3-11
3.5.5.2	STA Resource Monitor CSV File	3-11
3.6	Logging Configuration Files	3-13
3.7	STA Database Restoration	3-14
3.7.1	Copy Backup Files to the Server.....	3-14
3.7.2	Restore the Configuration Directory Files	3-15
3.7.3	Restore the Database	3-15
3.7.3.1	Reload the Database	3-15
3.7.3.2	Replay the Binlogs.....	3-15
3.7.3.2.1	Avoid Multiple Connections to the Server	3-16
3.7.3.3	Restart All Services.....	3-16
3.7.4	Point-in-Time Restorations.....	3-16
3.7.4.1	Restore from a Range of Log Numbers	3-16

4 Password Administration

4.1	Change an STA Database Account Password	4-1
4.2	Change the STA Backup Service and Resource Monitor Passwords	4-5

5 Managing SNMP Connections

5.1	SNMP Management Concepts	5-1
5.1.1	Overview	5-1
5.1.2	Testing Library SNMP Connections	5-1
5.1.3	Collecting Library Configuration Data.....	5-2
5.1.3.1	Building the STA Library Configuration Model.....	5-2
5.1.3.2	Keeping the Configuration Model Up-to-Date	5-3
5.1.4	Library Connection Status Information.....	5-4
5.2	SNMP Management Tasks	5-4

5.2.1	Confirm Network and SNMP Connectivity	5-5
5.2.2	SNMP Management Tasks — Library	5-6
5.2.2.1	Display All SNMP Trap Recipients	5-6
5.2.2.2	Delete or Modify the STA Trap Recipient.....	5-6
5.2.2.3	Add A New Trap Recipient	5-7
5.2.3	SNMP Management Tasks — STA User Interface.....	5-7
5.2.3.1	Change SNMP Client Attributes	5-7
5.2.3.2	Change Monitored Library Details	5-8
5.2.3.3	Export SNMP Connection Settings to a Text File	5-8
5.2.3.4	Remove a Library Connection	5-8
5.2.4	Tasks to Perform After a Library Firmware Upgrade.....	5-9
5.2.5	Tasks to Perform After a Redundant Electronics Switch.....	5-10
5.2.6	Tasks to Perform After Changing the Library or STA Server IP Address	5-10
5.2.7	Task to Perform After a Robot Change	5-10

A Preventing Denial of Service Attacks

A.1	Overview	A-1
A.2	Configure iptables Rules.....	A-2
A.3	iptables Sample Script	A-2

Index

Preface

This document describes administration of Oracle's StorageTek Tape Analytics (STA) product. Before reading this book, you should have already installed and configured STA as described in the *STA Installation and Configuration Guide*.

Audience

This document is intended for Linux administrators and STA administrators.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

Related Documents

- *STA Release Notes*¹
- *STA Requirements Guide*
- *STA Installation and Configuration Guide*
- *STA Quick Start Guide*
- *STA Screen Basics Guide*
- *STA User's Guide*
- *STA Data Reference Guide*
- *STA Security Guide*
- *STA Third Party Licenses and Notices*

¹ Included with the STA media pack download.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
monospace	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

What's New

This book has been updated with the following major changes since the STA 1.0.2 release, April 2013 revision.

Chapter 1, "RDA Logging"

- Updated UI screenshots
- Updated procedure to forward a log snapshot to Oracle Support

Chapter 2, "Server Administration"

- Added managed server descriptions
- Revised **STA** command usage

Chapter 3, "Database Services Administration"

- Revised overview of STA Services daemon
- Revised **STA** command usage
- Revised STA Backup service content
- Revised STA Resource Monitor service content
- Revised all content to reflect new file name time stamp format

Chapter 4, "Password Administration"

- Revised **STA** command usage
- Removed content to change user passwords in WebLogic (now handled within the STA UI and explained in the *STA Installation and Configuration Guide*)

Chapter 5, "Managing SNMP Connections"

- New chapter — content moved from *STA Data Reference Guide* and updated.

Appendix A, "Preventing Denial of Service Attacks"

- No major changes

RDA Logging

Using Remote Diagnostics Agent (RDA), STA collects information valuable for determining the source of an STA fault on your system. This chapter describes the RDA log snapshot process.

- ["Overview"](#) on page 1-1
- ["Collecting RDA Information With the User Interface"](#) on page 1-2
- ["Collecting RDA Information With the CLI"](#) on page 1-3
- ["Forwarding the Log Snapshot to Oracle Support"](#) on page 1-4

1.1 Overview

STA uses RDA to take a snapshot of all logs related to the STA application and database, including OS, installation, and configuration information. The logs are useful for performance analysis, debugging, security analysis, usage analysis, and other related purposes. STA stores a snapshot as a bundled file with an associated date/timestamp. You can create and store multiple RDA snapshots, and the log bundles are retained indefinitely until you delete them.

For troubleshooting purposes, you can download the log as a ZIP file and forward it to Oracle Service for analysis. RDA logs are valuable only for resolving STA GUI or WebLogic/MySQL issues.

Log Snapshot Process

1. Take an RDA snapshot — ["Take an RDA Snapshot"](#) on page 1-2
2. Download the snapshot ZIP file, selected by date/timestamp, to your computer — ["Download a Log Snapshot"](#) on page 1-2
3. Forward the ZIP file to Oracle Service — ["Forwarding the Log Snapshot to Oracle Support"](#) on page 1-4

Reasons for Taking a Log Snapshot

- An unexpected STA application event occurs and it appears to be a bug.
- Oracle Service requests that you take a snapshot.
- The STA user interface automatically displays a screen to take a snapshot.

Log bundles are retained indefinitely until you delete them and are only limited by the amount of disk space on your Linux system.

1.2 Collecting RDA Information With the User Interface

This is the easiest method for collecting RDA information. With this method, snapshots are stored in /Oracle/Middleware/rda/snapshots.

- ["Access the Service Logs Screen"](#) on page 1-2
- ["Take an RDA Snapshot"](#) on page 1-2
- ["Download a Log Snapshot"](#) on page 1-2
- ["Display Log Run Information"](#) on page 1-3
- ["Delete a Log Snapshot"](#) on page 1-3

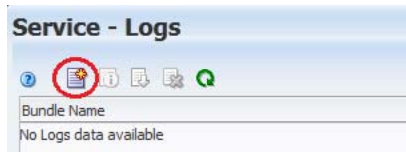
1.2.1 Access the Service Logs Screen

To access the Service Logs screen, select **Setup & Administration > Service > Logs**. The columns in the Service Logs table include:

- **Bundle Name** — The name you enter when you specify a new log snapshot. See ["Take an RDA Snapshot"](#) on page 1-2.
- **State** — The running state of the new log bundle (Running or Completed).
- **Date Created** — The date and time you started the RDA run.
- **File Size (KB)** — The size of the log file.

1.2.2 Take an RDA Snapshot

1. Click the **Create New Log Bundle** icon.



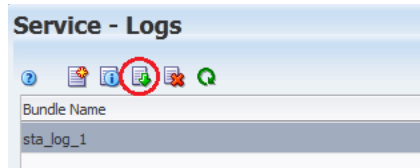
2. In the Log Bundle Name field, enter a snapshot name meeting these requirements:
 - Maximum of 210 characters
 - Can only contain alphanumeric characters and underscores (but cannot contain four or more consecutive underscores)
 - If spaces are entered, they will be replaced with underscores
 - Cannot begin with the following uppercase characters: COM, LPT, PRN, CON, AUX, or NUL.
3. Click **Save**.

A message appears telling you the job has been queued. It can take several minutes for the submitted job to appear in the table. You can click the **Refresh Table** icon to monitor the status of a background RDA run.



1.2.3 Download a Log Snapshot

1. Select the log bundle to download.
2. Click the **Download Selected Log Bundle** icon.



3. Save the file.

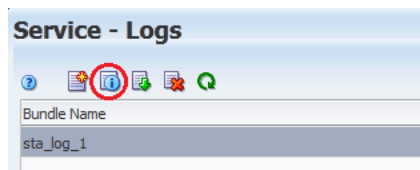
Note: If you see this error message in the log file, you may ignore it:

```
WARNING:
java.lang.ClassNotFoundException:
oracle.tbi.view.faces.ExceptionHandler
```

1.2.4 Display Log Run Information

This procedure displays a dialog box showing what was captured in the log.

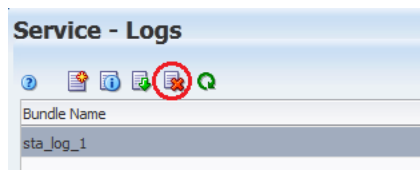
1. Select a log under the Bundle Name column.
2. Click the **Log Bundle Run Info** icon.



1.2.5 Delete a Log Snapshot

To permanently erase the selected RDA log snapshot from STA:

1. Select a log under the Bundle Name column.
2. Click the **Delete Selected Log Bundle** icon.



1.3 Collecting RDA Information With the CLI

You can collect RDA information manually if you are not able to access the STA UI. With this method, snapshots are stored in `/Oracle/Middleware/rda/output/`.

1. Log on to the STA server.
2. Access the rda directory.


```
# cd /Oracle/Middleware/rda
```
3. To ensure the setup.cfg file is found, enter the following command:

```
# ./rda.sh [-v] -f
```

The `-v` option allows you to view the progress of the data collection. The `-f` option forces a current data collection. The `-h` option provides `rda.sh` help.

4. When `rda.sh` is executed manually, it always generates the same RDA log bundle into the same named file. Rename the current RDA ZIP file.

```
# mv /Oracle/Middleware/rda/output/RDA.STA__HOSTNAME.zip  
/Oracle/Middleware/rda/output/RDA.STA__HOSTNAME_XXXX.zip
```

where `XXXX` is the new RDA ZIP file name.

5. To access the files just created on the server, go to:

```
file:///Oracle/Middleware/rda/output/STA__start.htm
```

6. To access the files from the client host, download the newly-created RDA log ZIP file, unzip the bundle, and access the log files through the URL above, modified as appropriate.

7. Display the man page for the specific `rda.sh` module, if desired.

```
# rda.sh -M [module]
```

where *module* is the module name (for example, `STA`). If you do not specify a module, general RDA information is displayed.

1.4 Forwarding the Log Snapshot to Oracle Support

1. Access the My Oracle Support website:
<https://support.oracle.com/CSP/ui/flash.html>
2. Click **Sign In** and provide your user name and password.
3. Go to the Service Requests tab and select **Create SR**. Use the wizard tips to the right to complete each required field.
4. Complete the What is the Problem? section with a summary and description of the issue.
5. Complete the Where is the Problem? section and choose the Support tab (software, hardware, cloud, etc.) for the issue type being reported.
6. Choose a problem type from the list.
7. Select the applicable support identifier (SI) and click **Next**.
8. Review any preferred knowledge article(s).
9. To continue with SR creation, upload files and provide additional information as needed.
10. Select severity, confirm contact information, and click **Submit**.

Server Administration

The **STA** command is used to administer and check the status of the various STA components. The STA command variants are split into two categories:

- Commands that bring the entire STA environment up or down, or check the status of the entire STA environment
- Commands that bring individual STA services up or down, or check the status of individual STA services.

Caution: The individual STA service commands are provided for reference only. Do not execute these commands unless directed by Oracle Support.

You can use the command **STA help** at any time to obtain a list of valid STA command arguments.

- ["Managed Servers"](#) on page 2-1.
- ["Memory Usage Requirements"](#) on page 2-1.
- ["Global Administration Commands"](#) on page 2-2.
- ["Individual Service Administration Commands"](#) on page 2-3.

2.1 Managed Servers

The various STA processes are split into the following three managed servers:

- `staUi` — the STA user interface
- `staEngine` — basic STA internal functions
- `staAdapter` — SNMP communication

The managed servers can be administered on an individual basis. See ["Individual Service Administration Commands"](#) on page 3.

2.2 Memory Usage Requirements

[Table 2-1](#) shows memory usage requirements for the STA domain server, STA managed servers, and MySQL.

Table 2-1 Memory Usage Requirements

Item	Memory Requirement
STA domain server	2 GB heap size
STA managed servers	2 GB heap size
MySQL	2 GB memory

2.3 Global Administration Commands

The following STA commands can be used to start and stop the entire STA environment, as well as check the status of the entire STA environment.

- **STA start all**

Starts the entire STA environment.

```
# STA start all
Starting mysql Service..
mysql service was successfully started
Starting staservd Service.
staservd service was successfully started
Starting weblogic Service.....
weblogic service was successfully started
Starting staengine Service.....
staengine service was successfully started
Starting staadapter Service.....
staadapter service was successfully started
Starting stau Service.....
stau service was successfully started
```

- **STA stop all**

Stops the entire STA environment.

```
# STA stop all
Stopping the stau service.....
Successfully stopped the stau service
Stopping the staadapter service.....
Successfully stopped the staadapter service
Stopping the staengine service.....
Successfully stopped the staengine service
Stopping the weblogic service.....
Successfully stopped the weblogic service
Stopping the staservd Service...
Successfully stopped staservd service
Stopping the mysql service.....
Successfully stopped mysql service
```

- **STA status all**

Displays the status of the entire STA environment.

```
# STA status all
mysql service is running
staservd service is running
weblogic service is running
staengine service is running
.... and the deployed application for staengine is in an ACTIVE state
staadapter service is running
.... and the deployed application for staadapter is in an ACTIVE state
stau service is running
```


.... and the deployed application for stau1 is in an ACTIVE state

2.4 Individual Service Administration Commands

The following STA commands can be used to start and stop individual STA components, or to check the status of those components.

Caution: The individual STA service commands are provided for reference only. Do not execute these commands unless directed by Oracle Support.

- **STA start | stop | status mysql**
Starts or stops MySQL, or displays its status.
- **STA start | stop | status staservd**
Starts or stops the STA Services Daemon, or displays its status.
- **STA start | stop | status weblogic**
Starts or stops the WebLogic AdminServer, or displays its status.
- **STA start | stop | status staadapter**
Starts or stops the staAdapter managed server, or displays its status.
- **STA start | stop | status staengine**
Starts or stops the staEngine managed server, or displays its status.
- **STA start | stop | status stau1**
Starts or stops the staUi managed server, or displays its status.

Database Services Administration

This chapter details the administration of various STA services. To initially configure these services, see the “Configuring STA Services” chapter within the *STA Installation and Configuration Guide*.

- ["STA Services Daemon"](#) on page 3-1
- ["STA Backup Service"](#) on page 3-2
- ["STA Resource Monitor Service"](#) on page 3-4
- ["Resource Monitor Reports"](#) on page 3-6
- ["File Types and Locations"](#) on page 3-8
- ["Logging Configuration Files"](#) on page 3-13
- ["STA Database Restoration"](#) on page 3-14

3.1 STA Services Daemon

The STA Services daemon, **staservd**, is a continuously-running Linux service that manages and runs the STA Backup and STA Resource Monitor services. Both the STA Backup and the STA Resource Monitor services run as separate execution threads within the STA Services daemon.

The STA Services daemon starts when the STA server is booted up (with the **STA start all** command), and terminates when the server is shut down. You can also start, stop, and check the status of the STA Services daemon with the following commands:

- To start the STA Services daemon:

```
# STA start staservd
Starting staservd Service...
staservd service was successfully started
```
- To stop the STA Services daemon:

```
# STA stop staservd
Stopping the staservd Service...
Successfully stopped staservd service
```
- To check the status of the STA Services daemon:

```
# STA status staservd
staservd service is running
```

For more information about the **STA** command, see [Chapter 2, "Server Administration."](#)

Note: After installation of STA, the STA Services daemon starts the STA Backup and STA Resource Monitor services, but they are not activated until configured. To configure these services, see the "Configuring STA Services" chapter in the *STA Installation and Configuration Guide*.

3.2 STA Backup Service

The STA Backup Service is one of several services running within the STA Services Daemon. It performs an automatic full backup of the STA database and key configuration directories, writing these files to a specified location on the STA server or in compressed form to a remote server. Oracle recommends that you configure a remote backup server.

Before proceeding, check to ensure the STA Services Daemon is running. See "[STA Services Daemon](#)" on page 3-1.

- "[Configuration](#)" on page 3-2
- "[Full Backup Process](#)" on page 3-2
- "[Display the Backup Service Preference Settings](#)" on page 3-3
- "[Clear Preference Settings](#)" on page 3-3
- "[Verify Files Have Been Sent to the Target Server](#)" on page 3-3
- "[Verify a Local Copy of the Backup Files Appears on the Server](#)" on page 3-4
- "[Reset the STA Backup Service Password](#)" on page 3-4

3.2.1 Configuration

The STA Backup Service is configured using its administration utility, `staservadm`, located in `/Oracle/StorageTek_Tape_Analytics/common/bin`. To configure the STA Backup service, see the "Configuring STA Services" chapter within the *STA Installation and Configuration Guide*.

3.2.2 Full Backup Process

Once configured, the STA Backup service performs the following process once every 24 hours:

1. Initiates a high-speed dump (also referred to as a "hot backup") of the following file types:
 - MySQL database dump file
 - MySQL binary log files
 - STA Services daemon and STA WebLogic configuration files
 - STA Services daemon and STA Backup service administration logs
2. Transfers the dump file to the designated backup host
3. Deletes the previous day's full dump files from the STA server
4. Writes a copy of the current day's dump files to the `/dbbackup/local` directory on the STA server.

3.2.3 Display the Backup Service Preference Settings

Enter the following command to display the status of the current preference settings:

```
# ./staservadm -Q
```

If the "Configured" field says "no," then the Backup Service is running in an "idle" mode and is not performing any backups. You will need to supply the proper configuration settings, as per the *STA Installation and Configuration Guide*.

Example output of a configured STA Backup Service:

```
# ./staservadm -Q
Contacting daemon...connected.
Querying Preferences.
Current STA Backup Service Settings:
Configured          [yes]
File Transfer       -S [SCP]
Full Backup         -T [11:00]
Sleep Interval      -i [350 sec]
Backup Hostname     -s [stabaksvr]
Backup Username     -u [stabck]
Backup Password     -p [*****]
Backup Directory    -d [/home/stabck/STAbackups]
Database Username   -U [stadba]
Database Password   -P [*****]
```

3.2.4 Clear Preference Settings

Enter the following command to clear the current preference settings:

```
# ./staservadm -C
```

The backup service is no longer configured and will return to the "idle" state. You can now provide new settings as per the *StorageTek Tape Analytics Installation and Configuration Guide*. For example:

```
# ./staservadm -C
Contacting daemon...connected.
Clearing Preferences.
Done.
Current STA Backup Service Settings:
Configured          [no]
File Transfer       -S [SCP]
Full Backup         -T [00:00]
Sleep Interval      -i [300 sec]
Backup Hostname     -s []
Backup Username     -u []
Backup Password     -p []
Backup Directory    -d []
Database Username   -U []
Database Password   -P []
```

3.2.5 Verify Files Have Been Sent to the Target Server

To verify that files have been sent successfully:

- Check the logs on the STA server.
- Log on to the target backup server and list the contents of the backup directory.

3.2.5.1 Check the Server Logs and Target Backup Server

The `staservd.log.0` file registers the activities of the Backup Services configuration utility.

1. Change the working directory to the STA backup log directory.

```
# cd /var/log/tbi/db/backups
```

2. Search the `staservd.log.0` file for the string “INFO: done. Database dump completed.”

```
# grep "INFO: done. Database dump completed" staservd.log.0
INFO: done. Database dump completed, file located at
/dbbackup/local/20130721_133755.stafullbackup.sql
INFO: done. Database dump completed, file located at
/dbbackup/local/20130722_133755.stafullbackup.sql
INFO: done. Database dump completed, file located at
/dbbackup/local/20130723_133755.stafullbackup.sql
INFO: done. Database dump completed, file located at
/dbbackup/local/20130724_133755.stafullbackup.sql
```

3. Log on to the target backup server.
4. List the files. In this example, the directory `/backups/tbivb01` has previously been set up to receive the backup files from the STA server “`tbivb01`”.

```
# ls -l /backups/tbivb01
0.stadb-bin.000023.gz
0.stadb-bin.000024.gz
0.stadb-bin.000026.gz
0.stadb-bin.000027.gz
20130723_133755.stadb-bin.000023.gz
20130723_133755.conf.zip.gz
20130723_133755.fmwconfig.zip.gz
20130723_133755.stadb-bin.000025.gz
20130723_133755.stadb-bin.000026.gz
20130723_133755.stafullbackup.sql.gz
```

3.2.6 Verify a Local Copy of the Backup Files Appears on the Server

Verify that a copy of the most recent backup files has been saved locally on the STA server by listing the files in the `/dbbackup/local` directory:

```
# ls -l /dbbackup/local
20130721_133755.conf.zip
20130721_133755.fmwconfig.zip
20130721_133755.stafullbackup.zip
```

The listed files will have the format `YYYYMMDD_HHMMSS.filename.zip`.

3.2.7 Reset the STA Backup Service Password

See [Chapter 4, "Password Administration"](#).

3.3 STA Resource Monitor Service

The STA Resource Monitor service monitors and reports on STA server resources, including database tablespace and disk volume space, logging volume disk space, and physical memory usage.

You may set usage high watermarks (HWM) for each resource. A high watermark is a threshold at which an alert will be raised. When the threshold is reached or exceeded, an alert is recorded in the standard daily resource report and optionally emailed to one or more designated recipients.

For example, if you set the database tablespace HWM to 60%, when the STA Resource Monitor detects that the STA application has used 60% or more of the maximum allowable database tablespace, it turns on the tablespace alert and sends an email to the designated recipients. Additionally, if nag mode is turned on, the Resource Monitor continues to send an alert email each time it scans the system.

- ["Configuration"](#) on page 3-5
- ["Query the Current Resource Monitor Preference Settings"](#) on page 3-5
- ["Clear the Resource Monitor Preference Settings"](#) on page 3-6
- ["Reset the STA Resource Monitor Password"](#) on page 3-6

3.3.1 Configuration

The STA Resource Monitor service is configured using its administration utility, `staresmonadm`, located in `/Oracle/StorageTek_Tape_Analytics/common/bin`. To configure the STA Resource Monitor service, see the "Configuring STA Services" chapter within the *STA Installation and Configuration Guide*.

3.3.2 Query the Current Resource Monitor Preference Settings

Enter the following command to query the current state of the preference settings:

```
# ./staresmonadm -Q
```

If the Configured field says "no," then the Resource Monitor Service is running in an "idle" mode neither monitoring resources nor sending reports. You will need to configure the server as per the *StorageTek Tape Analytics Installation and Configuration Guide*.

Example output of a configured STA Resource Monitor Service:

```
# ./staresmonadm -Q
Contacting daemon...connected.
Querying Preferences.
Current STA Resource Monitor Service Settings:
  Configured                               [yes]
  Send Reports                             -T [13:00]
  Sleep Interval                           -i [600 sec]
  Alert Nagging                             -n [on]
  DB Username                              -U [sta_dba]
  DB Password                              -P [*****]
  DB Tablespace hwm                         -t [65%]
  DB Backup hwm (/dbbackup)                 -b [65%]
  DB Data hwm (/dbdata)                     -d [65%]
  Log Volume hwm (/var/log/tbi)             -l [65%]
  Root Volume hwm (/)                       -z [70%]
  Tmp Volume hwm (/tmp)                     -x [80%]
  System Memory hwm                         -m [75%]
  Email 'From:'                             -f [StaResMon@localhost]
  Email 'To:'                               -r [john.doe@company.com]
  Email 'Subject:'                           -s [STA Resource Monitor Report]
  Output File                               -o [/var/log/tbi/db/staresmon.csv]
```

3.3.3 Clear the Resource Monitor Preference Settings

Enter the following command to clear the current preference settings:

```
# ./staresmonadm -C
```

The Resource Monitor service is no longer configured and will return to the “idle” state. You can now provide new settings as per the *StorageTek Tape Analytics Installation and Configuration Guide*. For example:

```
# ./staresmonadm -C
Contacting daemon...connected.
Clearing Preferences.
Done.
Current STA Resource Monitor Service Settings:
Configured                               [no]
Send Reports                             -T [00:00]
Sleep Interval                           -i [300 sec]
Alert Nagging                            -n [off]
DB Username                              -U []
DB Password                              -P []
DB Tablespace hwm                        -t [-1%]
DB Backup hwm (/dbbackup)                -b [-1%]
DB Data hwm (/dbdata)                   -d [-1%]
Log Volume hwm (/var/log/tbi)            -l [-1%]
Root Volume hwm (/)                      -z [-1%]
Tmp Volume hwm (/tmp)                    -x [-1%]
System Memory hwm                        -m [-1%]
Email 'From:'                            -f [StaResMon@localhost]
Email 'To:'                              -r []
Email 'Subject:'                         -s [STA Resource Monitor Report]
Output File                              -o [/var/log/tbi/db/staresmon.csv]
```

3.3.4 Reset the STA Resource Monitor Password

See [Chapter 4, "Password Administration."](#)

3.4 Resource Monitor Reports

Resource Monitor reports are configured using the STA Resource Monitor service administration utility, `staresmonadm`. To configure the STA Resource Monitor service, see the “Configuring STA Services” chapter within the *STA Installation and Configuration Guide*.

The Resource Monitor can produce two different reports:

- ["Resource Monitor Standard Report"](#) on page 3-6
- ["Resource Depletion Alert Report"](#) on page 3-7

3.4.1 Resource Monitor Standard Report

A Resource Monitor Standard Report is sent once a day at approximately the time specified by the `staresmonadm -T` option. If you do not set a time, the report is sent at the first scan after midnight. The report is sent to the email recipients you specified when you configured this service.

The report provides data for the following server resources. If any of these resources exceeds a high watermark threshold, an alert appears in the report.

- Database tablespace and volume

- Logging, backup, and root volume
- Temporary directory
- System memory usage

Note: Reported values rely on mount points. If multiple monitored items share the same mount point, the reported values for these items will be identical.

Example Standard Report (truncated)

```
STA RESOURCE MONITOR STANDARD REPORT
System: tbivb03
Scanned: 2013-10-24 11:30:14
```

```
Database Tablespace
HWM           : 60.00%
Used          : <0.1%
MB Used       : 13
MB Free       : 75763
MB Total      : 75776
Location      : /dbdata/mysql
```

```
Database Volume
HWM           : 60.00%
Used          : 6.80%
MB Used       : 6855
MB Free       : 93939
MB Total      : 100794
Directory     : /dbdata/mysql
```

```
...
```

3.4.2 Resource Depletion Alert Report

A Resource Depletion Alert Report is sent after every scan if the `staesmonadm` alert nag mode (-n) option is set to "on". If nag mode is off, alerts are shown only in the Standard Report.

The interval between each scan is determined by the Sleep Interval (-i) attribute, and the report is sent to the email recipients you specified when you configured this service. Recommendations are provided within the report to help resolve the noted issue(s).

Example Resource Depletion Alert Report

```
STA RESOURCE DEPLETION REPORT
System: server01
Scanned: 2013-10-24 11:34:47
*****
*                               A L E R T S                               *
*****
=====
ALERT - Low System Physical Memory
=====
Physical memory usage has exceeded threshold value!
HWM           [1.00%]
Used          [48.24%] (!)
MB Used       [7757]
MB Free       [8324]
```

```
MB Total          [16080]
Hostname          [server01]
Recommendations:
1) Shutdown unneeded processes.
2) Under Linux, try releasing unused caches using commands:
    # free -m
    # sync
    # /sbin/sysctl -q vm.drop_caches=3
    # free -m
3) Install additional memory.
```

3.5 File Types and Locations

The STA Services are comprised of executable scripts, java jar files containing server and client applications, configuration files, dump file, logging files, and a cumulative data file. This section describes their purposes and locations.

- ["STA Services Daemon Startup/Shutdown Script"](#) on page 3-8
- ["STA Administration Utilities"](#) on page 3-8
- ["Executable Program Locations"](#) on page 3-9
- ["Backup File Locations"](#) on page 3-9
- ["Resource Monitor File Locations"](#) on page 3-11

3.5.1 STA Services Daemon Startup/Shutdown Script

The STA Services daemon startup/shutdown script, `staservd`, and system run level symbolic links are located at:

```
/etc/init.d/staservd - Main startup/shutdown script
/etc/rc0.d/K04staservd - Symbolic link for system shutdown
/etc/rc1.d/K04staservd - Symbolic link for system shutdown
/etc/rc2.d/S96staservd - Symbolic link for system startup
/etc/rc3.d/S96staservd - Symbolic link for system startup
/etc/rc4.d/S96staservd - Symbolic link for system startup
/etc/rc5.d/S96staservd - Symbolic link for system startup
/etc/rc6.d/K04staservd - Symbolic link for system shutdown
```

The `staservd` init script and its associated symbolic links are created by the STA installer.

3.5.2 STA Administration Utilities

The STA Backup Service administration utility, `staservadm`, is a Perl script that calls a Java client application named `ServerAdm` that is contained in the `oracle.tbi.serveradm.jar` file. For more information, see ["STA Backup Service"](#) on page 3-2.

The STA Resources Monitor administration utility, `staresmonadm`, is a Perl script that calls a Java client application named `StaResMonAdm` that is contained in the `oracle.tbi.resmonadm.jar` file. `StaResMonAdm` is an RMI client that communicates with the STA Services daemon to set and reset run-time preferences. For more information, see ["STA Resource Monitor Service"](#) on page 3-4.

3.5.3 Executable Program Locations

Table 3–1 lists the executable programs and their locations.

Table 3–1 Executable Program Locations

Program	Location
STA Services program jar file	\$STAHOME/common/lib/oracle.tbi.server.jar
STA Backup Services Administration Utility Java application jar file	\$STAHOME/common/lib/oracle.tbi.serveradm.jar
STA Backup Service Administration Utility user script file, staservadm	\$STAHOME/common/bin/staservadm
STA ResMon Administration Utility Java application jar file	\$STAHOME/common/lib/oracle.tbi.resmonadm.jar
STA ResMon Administration Utility Java user script file, staresmonadm	\$STAHOME/common/bin/staresmonadm

Where:

\$STAHOME = /Oracle/StorageTek_Tape_Analytics

3.5.4 Backup File Locations

These are the kinds of files involved in the backup operation:

- [STA Services Daemon and Backup Service Admin Logs](#)
- [MYSQL Database Dump Files](#)
- [MySQL Binary Logs](#)
- [STA Services Daemon and WebLogic Configuration Files](#)

3.5.4.1 STA Services Daemon and Backup Service Admin Logs

These log the activities of the STA Services Daemon Server, STAServer, and its Backup services configuration utility, ServerAdm. Admin logs are collections of up to 10 log files, each up to 1.0 MB in size. The log file names are of the format "*.log.N," where "N" is the number of the log (staservd.log.0, staservadm.log.0, staservd.log.1, and so forth).

The logs are circularly rotated such that log file #1 will be reused when staservd.log.9 has been filled up. The active log file is always #0 (staservd.log.0). When log #0 fills up, it is renamed to log #1 and a new log #0 is started. By default the STAServer and ServerAdm logs are located at:

/var/log/tbi/db/backups

The location of and internal log format type (either simple ASCII text or XML markup) is controlled by the logging properties file staservd.log.props and staservadm.log.props located at:

\$STAHOME/common/conf/staservd.log.props

\$STAHOME/common/conf/staservadm.log.props

Where:

\$STAHOME = /Oracle/StorageTek_Tape_Analytics

3.5.4.2 MySQL Database Dump Files

The MySQL database dump file is a snapshot-in-time of the database schema and data contents. STA Backup service performs these actions:

1. Initiates a high-speed dump (sometimes called a "hot backup") once every 24 hours of the file types discussed in this section
2. Transfers the latest dump file to the designated backup host
3. Deletes the previous day's full dump files from the local backup directory
4. Writes a copy of the current days' dump file to the local backup directory.

The STA Backup Service by default will place its local dump files and incremental binlog files into the /dbbackup/local directory with format `YYYYMMDD_HHMMSS.filename.sql`.

3.5.4.3 MySQL Binary Logs

The term *incremental dumps* refers to the MySQL binary logs (binlogs) that record all transactions that result in a change to a database. The STA Backup Service treats binlogs as incremental backups following the main database dump.

STA incremental dumps are comprised of all the binary logs that are produced since the last full dump. By replaying the binlogs, you can restore a database to its state up the last transaction recorded in the log. A restore consists of loading the latest dump file, and then replaying, in order, all the MySQL binlogs that were generated following the latest database dump.

Backing up the binlogs consists of making a list of all the binlogs created since the most recent full dump and then transmitting each of those logs (except the current one because it is still open) to the backup server.

The backup binary log naming format is `YYYYMMDD_HHMMSS.stadb-bin.log_sequence_number`.

The MySQL binary log location is defined in the MySQL settings file /etc/my.cnf. That is currently set to:

```
/var/log/tbi/db/
```

Local copies of the backup binlog files are located at:

```
/dbbackup/local
```

All but the most recent binlog successfully transferred to the backup server are purged using the MySQL command `PURGE BINARY LOGS BEFORE NOW()`. The current binlog and the current day's full backup file thus remain on the server.

Caution: Never manually delete the binlog files.

3.5.4.4 STA Services Daemon and WebLogic Configuration Files

In addition to files necessary to recover the STA application database, the STA Backup Service also backs up STA's WebLogic configuration files as well as its own STA Services daemon configuration files. The backup is a recursive backup of all the files and directories in their respective configuration directories.

Configuration file backups are performed once every 24 hours when the full STA database dump is performed. The backup file names format is `YYYYMMDD_HHMMSS.filename.zip.gz`.

The source and target locations of these backups are shown in [Table 3–2](#):

Table 3–2 Backup Source/Target Locations

Source Location	Local Copy	Remote Copy
\$STAHOME/common/conf/*	\$BACKUPS/YYYYMMDD_HHMMSS.conf.zip	\$RHOST:\$RDIR/YYYYMMDD_HHMMSS.conf.zip.gz
\$WLHOME/config/fmconfig/*	\$BACKUPS/YYYYMMDD_HHMMSS.fmconfig.zip	\$RHOST:\$RDIR/YYYYMMDD_HHMMSS.fmconfig.zip.gz

Where:

\$STAHOME = /Oracle/StorageTek_Tape_Analytics

\$WLHOME = /Oracle/Middleware/user_projects/domains/TBI

\$BACKUPS = /dbdata/mysql/backups

\$RHOST = Backup server IP address or name

\$RDIR = Directory on backup server

3.5.5 Resource Monitor File Locations

There are two kinds of files involved in the monitoring operations:

- [STA Services Daemon and ResMonAdm Logs](#)
- [STA Resource Monitor CSV File](#)

3.5.5.1 STA Services Daemon and ResMonAdm Logs

These log the activities of the STA Services daemon and the Resource Monitor Administration utility, *staresmonadm*. These logs are collections of up to 10 log files, each up to 1.0 MB in size. The log file names are of the format **.log.N*, where "N" is the number of the log (*staservd.log.0*, *staresmonadm.log.0*, *staservd.log.1*, and so forth).

The logs are circularly rotated such that log file #1 will be reused when *staservd.log.9* has been filled up. The active log file is always #0 (*staservd.log.0*). When log #0 fills up, it is renamed to log #1 and a new log #0 is started. By default, the STA Services, STA ResMon, and STA ResMonAdm logs are all located at:

```
/var/log/tbi/db/backups
```

The location and log format (either simple ASCII text or XML markup) are controlled by the logging properties file, *staservd.log.props*, and *staresmonadm.log.props* located at:

```
$STAHOME/common/conf/staservd.log.props
```

```
$STAHOME/common/conf/staresmonadm.log.props
```

Where:

\$STAHOME = /Oracle/StorageTek_Tape_Analytics

3.5.5.2 STA Resource Monitor CSV File

Each time ResMon scans the system, it writes the gathered values out to a comma-separated-value (CSV) file located, by default, at:

```
/var/log/tbi/db/staresmon.csv
```

Programs such as Excel and MySQL can load this data file and perform various analytic and graphing functions with time-based values (for example, analysis of resource depletion trends).

Note: The ResMon CSV file is neither purged, rolled, nor backed up by the STA Backup Service.

Each record in staresmon.csv represents a scan of the system. The format of the 21 column record is shown in [Table 3-3](#).

Table 3-3 Resource Monitor CSV File Format

Col	Header	Description	Format
1	TIMESTAMP	Date and time of the scan	"YYYY-MM-DD HH:MM:SS"
2	TS_MB_MAX	Maximum tablespace	123
3	TS_MB_USED	Total database space used	123
4	TS_MB_AVAIL	Database space remaining	123
5	TS_PCT_USED	Database tablespace used as a percentage of the max	12.34%
6	TS_PCT_HWM	Database tablespace high water mark as a percentage of the max	12.34%
7	DBVOL_MB_MAX	Maximum available space on the volume containing the database	123
8	DBVOL_MB_USED	Total database disk volume space used	123
9	DBVOL_MB_AVAIL	Database volume disk space remaining	123
10	DBVOL_PCT_USED	Database volume disk space used as a percentage of the max	12.34%
11	DBVOL_PCT_HWM	Database volume high water mark as a percentage of the max	12.34%
12	LOGVOL_MB_MAX	Maximum available space on the volume containing the logs	123
13	LOGVOL_MB_USED	Total logging disk volume space used	123
14	LOGVOL_MB_AVAIL	Logging volume disk space remaining	123
15	LOGVOL_PCT_USED	Logging volume disk space used as a percentage of the max	12.34%
16	LOGVOL_PCT_HWM	Logging volume high water mark as a percentage of the max	12.34%
17	MEM_MB_MAX	Maximum installed physical RAM	123
18	MEM_MB_USED	Total physical memory used	123
19	MEM_MB_AVAIL	Physical memory space remaining	123
20	MEM_PCT_USED	Physical memory space used as a percentage of the max	12.34%
21	MEM_PCT_HWM	Physical memory high water mark as a percentage of the max	12.34%

3.6 Logging Configuration Files

Logging for the STA Services daemon, the Backup Service, Backup Service Administration Utility, and STA Resource Monitor Utility is controlled by logging configuration files located at:

`$STAHOME/common/conf/staservd.log.props`

`$STAHOME/common/conf/staservadm.log.props`

`$STAHOME/common/conf/staresmonadm.log.props`

Where:

`$STAHOME = /Oracle/StorageTek_Tape_Analytics`

The logging file contents and format are initialized and controlled by the Java Log Manager configuration properties. These properties are read from the logging properties files noted above. The following information can be found at:

<http://download.oracle.com/javase/1.4.2/docs/api/java/util/logging/FileHandler.html>.

Table 3–4 Logging File Contents

Property	Description	StorageTek Tape Analytics Setting
<code>java.util.logging.FileHandler.append</code>	Specifies whether the FileHandler should append onto any existing files (defaults to false)	true
<code>java.util.logging.FileHandler.count</code>	Specifies how many output files to cycle through (defaults to 1).	10
<code>java.util.logging.FileHandler.formatter</code>	Specifies the name of a Formatter class to use (defaults to <code>java.util.logging.XMLFormatter</code>)	<code>Java.util.logging.SimpleFormatter</code> for human readability. The <code>java.util.loggin.XMLFormatter</code> is commented out and available
<code>java.util.logging.FileHandler.level</code>	Specifies the default level for the Handler (defaults to Level.ALL).	CONFIG
<code>java.util.logging.FileHandler.limit</code>	Specifies an approximate maximum amount to write (in bytes) to any one file. If this is zero, then there is no limit. (Defaults to no limit).	1000000 (1MB)
<code>java.util.logging.FileHandler.pattern</code>	Specifies a pattern for generating the output file name. See below for details. (Defaults to <code>"%h/java%u.log"</code>).	<code>/var/log/tbi/db/backups/staservd.log.%g</code> <code>/var/log/tbi/db/backups/staservadm.log.%g</code>

Table 3–5 STA Services Daemon Properties

Property	Description	StorageTek Tape Analytics Setting
oracle.tbi.server.level	Specifies the log level for the server, server	CONFIG
oracle.tbi.serveradm.level	admin functions, or	CONFIG
oracle.tbi.resmonadm.level	the resource monitor admin functions.	

3.7 STA Database Restoration

The STA Restore procedure consists of loading the most recent full dump and then replaying all the binary logs immediately following that dump.

There are distinct sets of backup files on the backup server directory. For example:

```
# cd /data/stabackups
# ls -l
20130721_133755.conf.zip.gz
20130721_133755.fmwconfig.zip.gz
20130721_133755.stadb-bin.000024.gz
20130721_133755.stafullbackup.sql.gz
20130722_133755.conf.zip.gz
20130722_133755.fmwconfig.zip.gz
20130722_133755.stadb-bin.000024.gz
20130722_133755.stafullbackup.sql.gz
20130723_133755.conf.zip.gz
20130723_133755.fmwconfig.zip.gz
20130723_133755.stadb-bin.000021.gz
20130723_133755.stadb-bin.000022.gz
20130723_133755.stadb-bin.000023.gz
20130723_133755.stadb-bin.000024.gz
20130723_133755.stafullbackup.sql.gz
```

The file name time stamp format is YYYYMMDD_HHMMSS. All the binary logs having the same date tag will be replayed into the database after the full dump is loaded.

The following administration tasks are discussed here:

- ["Copy Backup Files to the Server"](#) on page 3-14
- ["Restore the Configuration Directory Files"](#) on page 3-15
- ["Restore the Database"](#) on page 3-15
- ["Point-in-Time Restorations"](#) on page 3-16

3.7.1 Copy Backup Files to the Server

To copy backup files to the server:

1. Copy the whole set of one day's files back to the STA server.

Oracle recommends copying everything to the /tmp directory. For example, assuming that STA is installed on the server sta.server.com and you are currently logged onto the backup server.

```
# scp 20130723*.* sta.server.com:/tmp/
Password:
```

2. Log on as root to the STA server and ungzip the *.gz files. For example:


```
# cd /tmp
# gunzip 20130723*.*.gz
```

3.7.2 Restore the Configuration Directory Files

To restore the configuration directory files:

1. Stop all STA processes. Then, restart only the MySQL server.

```
# STA stop all
# STA start mysql
```

2. Unzip the STAServer and STA Services Daemon configuration directories.

The zip files have been created with the full directory paths to allow you to restore and/or overwrite existing files. The `zip` command allows you to re-crown the root of the restore path with the `-d` option. Additional options allow more control, such as selective replace.

For a clean restoration, you should completely replace the existing configuration directory; however, back up the original first. For example:

```
# cd $WLSHOME
# zip -vr fmwconfig.orig.zip fmwconfig
# rm -rf fmwconfig
# cd /tmp
# unzip -X -d/ 20130723_133755.fmwconfig.zip
# cd $STAHOME/common
# zip -vr conf.orig.zip conf
# rm -rf conf
# cd /tmp
# unzip -X -d/ 20130723_133755.conf.zip
```

Where:

`$WLSHOME = /Oracle/Middleware/user_projects/domains/TBI/config`

`$STAHOME = /Oracle/StorageTek_Tape_Analytics`

3.7.3 Restore the Database

Perform the following commands as the MySQL root user:

3.7.3.1 Reload the Database

To reload the database:

1. Clean out any residual `stadb` database if it exists. For example:

```
# mysql -uroot -p -e 'drop database stadb;'
Password:
```

2. Load the latest full dump. This creates the schema and installs all the data. For example:

```
# mysql -uroot -p -e 'source 20130723_133755.stafullbackup.sql;'
Password:
```

3.7.3.2 Replay the Binlogs

To replay the binlogs:

1. Run each of the incremental dumps (binlogs) from youngest to oldest.

If you have more than one binary log to execute on the MySQL server, the safest method is to process them all using a single connection to the server and a single mysql process to execute the contents of all of the binary logs.

For example:

```
# mysqlbinlog 20130723_133755.sta-binlog.000021 \  
> 20130723_133755.sta-binlog.000022 \  
> 20130723_133755.sta-binlog.000023 \  
> 20130723_133755.sta-binlog.000024 |mysql -u root -p
```

Another approach is to concatenate all the logs to a single file and then process the file:

```
# mysqlbinlog 20130723_133755.sta-binlog.000021 > /tmp/recoversta.sql  
# mysqlbinlog 20130723_133755.sta-binlog.000022 >> /tmp/recoversta.sql  
# mysqlbinlog 20130723_133755.sta-binlog.000023 >> /tmp/recoversta.sql  
# mysqlbinlog 20130723_133755.sta-binlog.000024 >> /tmp/recoversta.sql  
# mysql -u root -p -e 'source /tmp/recoversta.sql'
```

Note: If you do not supply a password on the command line, MySQL prompts you for it before proceeding.

3.7.3.2.1 Avoid Multiple Connections to the Server Processing binary logs as shown in the example below may create multiple connections to the server. Multiple connections cause problems if the first log file contains a CREATE TEMPORARY TABLE statement, and the second log contains a statement that uses that temporary table. When the first mysql process terminates, the server drops the temporary table. When the second mysql process attempts to use that table, the server reports “unknown table.”

```
# mysqlbinlog binlog.000001 |mysql -u root -p #<=== DANGER!!  
# mysqlbinlog binlog.000002 |mysql -u root -p #<=== DANGER!!
```

3.7.3.3 Restart All Services

As the Linux system root user, enter the following command:

```
# STA start all
```

3.7.4 Point-in-Time Restorations

Another restoration method is “point-in-time,” where binary logs can be replayed from a specific start point to a specific end point in time.

For example, after examining the contents of a binary log, you discover that an erroneous operation resulted in dropping several tables immediately following log entry #6817916. After restoring the database from the full dump occurring the day before, and before restarting all the STA services, you can replay the most recent binary log from its initial log entry number “176” through entry number “6817916” with the commands shown in this procedure.

3.7.4.1 Restore from a Range of Log Numbers

To restore from a range of log numbers:

1. Make sure all the STA processes are shut down and only the MySQL server is running:

```
# STA stop all  
# STA start mysql
```

2. As the MySQL root user, extract the valid operations. For example:

```
# mysqlbinlog --start-position=176 --stop-position=6817916  
/var/log/tbi/db/stadb-bin.000007 > ./recover.sql
```

3. Apply them to the database. For example:

```
# mysql -uroot -p -e 'source ./recover.sql'  
Password:
```

4. As the Linux system root user, restart the STA application and STA Services Daemon:

```
# STA start all
```

For more information on point-in-time or incremental recovery operations refer to the MySQL Manual:

<http://dev.mysql.com/doc/refman/5.5/en/point-in-time-recovery.html>

Password Administration

This chapter describes changing various STA database and service passwords. To change STA user passwords (for example, the STA GUI Login password), see "Configuring Users" within the *STA Installation and Configuration Guide*.

Caution: Do not change the WebLogic Admin Console Login password. If you change this password, you will need to reinstall STA.

- ["Change an STA Database Account Password"](#) on page 4-1
- ["Change the STA Backup Service and Resource Monitor Passwords"](#) on page 4-5

4.1 Change an STA Database Account Password

Follow this procedure to change the STA Database Root Account¹, Application Account, Reports Account, or DBA Account password.

1. Begin as follows:
 - If you are changing the STA Database Root Account, Reports Account, or DBA Account password, skip to Step 11.
 - If you are changing the STA Application Account password, go to the next step to first change the password in WebLogic.

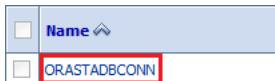
Caution: Changing the STA Application Account password requires synchronizing the password between WebLogic and the MySQL database and then stopping and re-starting all STA processes. Some library transactions will be lost. Oracle recommends that you back up the STA database before starting this procedure.

2. Go to the WebLogic console login screen using the HTTP (default is 7001) or HTTPS (default is 7002) port number you selected during STA installation.
`http(s)://yourHostName:PortNumber/console/`
3. Log in using the WebLogic Admin Console username and password.
4. Under Domain Structure > Services, select **Data Sources**.

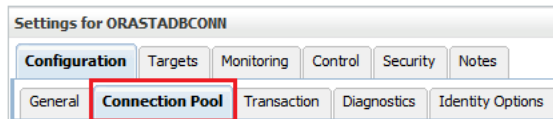
¹ Should only be changed by the MySQL database administrator.



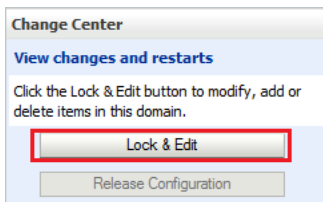
5. Select the **ORASTADBCONN** data source name (select the name, not the check box).



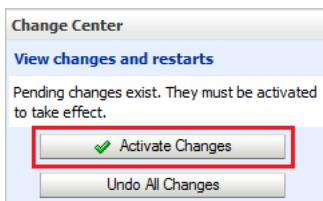
6. Click the **Connection Pool** tab.



7. Click the **Lock & Edit** button in the upper left-hand corner.



8. Enter and confirm the new password, and then click **Save**.
9. Click the **Activate Changes** button in the upper left-hand corner of the screen.



10. Log out of the WebLogic Administration Console.
11. Log in to the MySQL client as root user.

```
# mysql -uroot -p
Password: root-password
```

12. Enter the **use mysql** command.

```
mysql> use mysql;
```

13. Retrieve the list of STA database usernames.

```
mysql> select distinct(user) from user order by user;
```

14. Take note of the account username for which to change the password. You will use this username in the next step.
15. Issue the following commands to change the password. Use single quotes around the *new-password* and *username* variables.

```
mysql> update user set password=PASSWORD('new-password') where user='username';
mysql> commit;
mysql> flush privileges;
```

16. Exit out of the MySQL client.

```
mysql> quit;
```

17. Set the new login path. This step varies depending on which database user password you changed in the previous steps.

- If you changed the STA Database Root Account password:

- a. Obtain a list of root user information.

```
# mysql -u root -p -e "select user, host, password from mysql.user
where user='root'"
Enter password: new-mysql-root-password
```

Example output:

```
+-----+-----+-----+
| user | host      | password |
+-----+-----+-----+
| root | localhost | *ABCDEF123456789ABCDEF123456789ABCDEF1234 |
| root | server1   | *ABCDEF123456789ABCDEF123456789ABCDEF1234 |
| root | 127.0.0.1 | *1234ABCDEF1234ABCDEF1234ABCDEF1234ABCDEF |
| root | ::1       | *1234ABCDEF1234ABCDEF1234ABCDEF1234ABCDEF |
| root | %         | *1234ABCDEF1234ABCDEF1234ABCDEF1234ABCDEF |
+-----+-----+-----+
```

- b. To set the new login path password, execute the following command for each listed host. For example, if your list of hosts resembled that of the example output above, you would execute this command five times, replacing *host* with *localhost*, *server1*, *127.0.0.1*, *::1*, and *%*.

```
# mysql_config_editor set --login-path=root_path --host=host
--user=root --password
Enter password: new-mysql-root-password
WARNING : 'root_path' path already exists and will be overwritten.
Continue? (Press y|Y for Yes, any other key for No) : y
```

- c. To test the new login path, execute the following command for each listed host.

```
# mysql --login-path=root_path --host=host
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 1234
Server version: 5.6.15-enterprise-commercial-advanced-log MySQL
Enterprise Server - Advanced Edition (Commercial)
```

Copyright (c) 2000, 2013, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

```
mysql> quit
Bye
```

- If you changed the STA Database Application Account, Reports Account, or DBA Account password:

- a. Obtain a list of database users.

```
# mysql -u root -p -e "select user, host, password from mysql.user
where user <> 'root'"
Enter password: mysql-root-password
```

Example output:

```
+-----+-----+-----+
| user   | host   | password                                     |
+-----+-----+-----+
| stadba | localhost | *ABCDEF123456789ABCDEF123456789ABCDEF1234 |
| stadba | %       | *ABCDEF123456789ABCDEF123456789ABCDEF1234 |
| staapp | localhost | *1234ABCDEF1234ABCDEF1234ABCDEF1234ABCDEF |
| staapp | %       | *1234ABCDEF1234ABCDEF1234ABCDEF1234ABCDEF |
| stausr | localhost | *1234ABCDEF1234ABCDEF1234ABCDEF1234ABCDEF |
| stausr | %       | *1234ABCDEF1234ABCDEF1234ABCDEF1234ABCDEF |
+-----+-----+-----+
```

- b. To set the new login path password, execute the following command for each listed user and associated host(s). For example, if your list of users resembled that of the example output above, you would execute this command six times, replacing *user* with each user name (stadba, staapp, or stausr), and *host* with each host name (localhost or %) for each user.

```
# mysql_config_editor set --login-path=user_path --host=host
--user=root --password
Enter password: new-user-password
WARNING : 'root_path' path already exists and will be overwritten.
Continue? (Press y|Y for Yes, any other key for No) : y
```

- c. To test the new login path, execute the following command for each listed user and associated host(s).

```
# mysql --login-path=user_path --host=host
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 1234
Server version: 5.6.15-enterprise-commercial-advanced-log MySQL
Enterprise Server - Advanced Edition (Commercial)
```

Copyright (c) 2000, 2013, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

```
mysql> quit
Bye
```


18. Proceed as follows:

- If you changed the STA Database DBA Account password, see ["Change the STA Backup Service and Resource Monitor Passwords"](#) on page 4-5 to synchronize the password for these services.
- If you changed the STA Database Application Account password, proceed to the next step.
- If you changed the STA Database Root Account or Reports Account, you are finished.

19. As root on the STA server, stop and then start all STA processes by issuing the following commands:

```
# STA stop all
# STA start all
```

For STA command usage details, see [Chapter 2, "Server Administration."](#)

20. Verify STA session connectivity:

- a. Go to the STA GUI login screen using the HTTP (default is 7021) or HTTPS (default is 7022) port number you selected during STA installation. "STA" must be uppercase.

```
http(s)://yourHostName:PortNumber/STA/
```

- b. Log in using the STA GUI Login username and password.
 - If you see a fully-populated Dashboard screen, you have successfully reset the STA Database Application Account password on both the WebLogic server and the MySQL database.
 - If you see an Application Error, then the password you defined in WebLogic does not match the STA Database Application Account password in the MySQL database. Ensure the passwords match.

4.2 Change the STA Backup Service and Resource Monitor Passwords

If you changed the STA Database DBA Account password in ["Change an STA Database Account Password"](#) on page 4-1, you must update it in the STA Backup Service and Resource Monitor.

1. Change directories.

```
# cd /Oracle/StorageTek_Tape_Analytics/common/bin
```

2. Ensure the STA Backup Service and Resource Monitor is online.

- Backup Service:

```
# ./staservadm -Q
Contacting daemon...connected.
...
```

- Resource Monitor:

```
# ./staresmonadm -Q
Contacting daemon...connected.
...
```

3. As the system root user, reset the STA Backup Service and Resource Monitor passwords by issuing the following commands, where *dba_user* is the STA Database DBA Account username and *dba_password* is the current STA Database DBA Account password:

- Backup Service:

```
# ./staservadm -U dba_user -P
Enter database password: dba_password
```

- Resource Monitor:

```
# ./staresmonadm -U dba_user -P
Enter database password: dba_password
```

Note: You may alternately enter the password on the command line after **-P**; however, doing so is less secure and is discouraged.

Managing SNMP Connections

This chapter provides concepts and procedures for managing Simple Network Management Protocol (SNMP) connections between STA and the libraries. For general SNMP information, see the *StorageTek SL150/SL500/SL3000/SL8500 SNMP Reference Guide*. To initially configure SNMP for STA, see the *STA Installation and Configuration Guide*.

- ["SNMP Management Concepts"](#) on page 5-1
- ["SNMP Management Tasks"](#) on page 5-4

5.1 SNMP Management Concepts

- ["Overview"](#) on page 5-1
- ["Testing Library SNMP Connections"](#) on page 5-1
- ["Collecting Library Configuration Data"](#) on page 5-2
- ["Library Connection Status Information"](#) on page 5-4

5.1.1 Overview

Libraries are monitored via the SNMP interface, with STA being a client agent and each library being a server agent.

Oracle recommends the SNMP v3 protocol. The authentication, encryption, and message integrity features in SNMP v3 provide a secure mechanism for sending library data. However, you can optionally choose SNMP v2c for one or more libraries (see "SNMP Configuration" in the *STA Installation and Configuration Guide*).

To set up SNMP connections, you must configure an SNMP user and an SNMP trap recipient on STA and each library. All libraries must use the same SNMP user and trap recipient.

Caution: Oracle's Service Delivery Platform (SDP) also uses SNMP. When defining SNMP user names for STA, do not make changes to the library SNMP configuration that conflict with SDP's requirements. Contact Oracle Support for assistance.

5.1.2 Testing Library SNMP Connections

A library connection test establishes or re-establishes the SNMP handshake between STA and the library. You can perform one connection test at a time.

Note: A connection test should be run only when required. Though it typically takes less than a second to test a library connection, no traps will be received from any libraries while the STA SNMP engine is restarted.

When to Perform a Connection Test

Oracle recommends that you perform a library connection test whenever you perform any of the activities in [Table 5-1](#), as each may cause the SNMP connection with a library to be dropped until the next scheduled data collection. You should also perform a connection test anytime you suspect loss of SNMP data from one or more libraries. Testing will minimize the time the connection is dropped and prevent the loss of large amounts of SNMP data.

To perform a connection test, see the "Test the SNMP Connection to the Library" section within the *STA Installation and Configuration Guide*.

Table 5-1 Activities Prompting a Connection Test

Activity	Description
Modification of STA SNMP client settings	These settings include the SNMP user name and the connection authorization and privacy passwords. After performing this activity, test the connections of all monitored libraries.
Modification of library SNMP settings	Whenever you modify these settings, the Library Engine ID field is blanked out to indicate that the SNMP connection with the library has been dropped. After performing this activity, test only the connection of the affected library.
Library reboot	Wait until the library is fully operational before initiating the connection test. If more than one library is rebooted, wait for all libraries to be fully operational, and then test only the connection for a single library.
Redundant Electronics switch	Wait until the switch has completed and the library is fully operational before initiating the connection test.

5.1.3 Collecting Library Configuration Data

Once an SNMP connection is established with a library, STA begins receiving SNMP traps and stores this data in the STA data store. However, this data will not be displayed in the user interface until the STA library configuration model has been built (see "STA Data Store" in the *STA Data Reference Guide* for a description of the types of data).

5.1.3.1 Building the STA Library Configuration Model

For STA to build the initial library configuration model, initiate a manual data collection once the library connection is established. During this data collection, STA retrieves configuration information, including:

- Locations of activated storage cells
- Partition information
- Drive types, identifiers, and locations
- Media types, volume serial numbers (volsers), and locations

Depending on the size and activity level of the library, the initial data collection may take several minutes to over an hour. During this process, you may see fluctuations in

various analytic and summary data. Once the data collection completes, the user interface displays a complete picture of the library configuration and ongoing exchange activity.

5.1.3.2 Keeping the Configuration Model Up-to-Date

After the initial data collection, the configuration model is updated through regular data collections. Only one data collection can be performed on a particular library at a time, and only five data collections can be running simultaneously.

Note: Data collections have little impact on library performance. However, a data collection during heavy library activity can take longer to complete. Scheduled and manual data collections should be performed during periods of low library activity.

Data collections are performed in the following ways:

- **Scheduled Data Collections** — Occur automatically every 24 hours at a defined time. This is a full collection of all library configuration data and should be scheduled during low levels of library activity. See ["Change Monitored Library Details"](#) on page 5-8.
- **Triggered Data Collections** — Initiated automatically whenever significant changes in the library state or configuration are detected (for example, the addition of a drive or media cartridge, or a change in partition configuration). This is a partial data collection that updates only the library configuration affected by the change.
- **Manual Data Collections** — This is a full collection of all library configuration data, initiated manually, as long as there is an active connection to the library. You must perform a manual data collection:
 - When a new library connection is configured.
 - After modifying SNMP settings in STA (see ["Change Monitored Library Details"](#) on page 5-8) and on the library (as described in "Library Configuration Process" in the *STA Installation and Configuration Guide*).
 - When a Redundant Electronics switch has occurred (see ["Tasks to Perform After a Redundant Electronics Switch"](#) on page 5-10).

You should also perform a manual data collection whenever you perform any of the activities in [Table 5-2](#). Although STA initiates a triggered data collection for some of these activities, large-scale changes may take some time to complete.

Table 5-2 Activities Prompting A Recommended Manual Data Collection

Activity	Additional Information
Drive addition or swap	The lag time between the activity and notification to STA could result in data co-mingling. Before performing a manual data collection, wait 15 minutes after drive initialization.
Drive removal	Before performing a manual data collection, wait approximately one minute after removal.
Modification of active storage regions or partitions	Before performing a manual data collection, wait 15 minutes after the library controller database has been updated.

Table 5–2 (Cont.) Activities Prompting A Recommended Manual Data Collection

Activity	Additional Information
Large number of media cartridge enters or ejects	NA
Suspicion that library configuration data is out of sync on STA	See "Missing Media" and "Duplicate Volume Serial Numbers" in the <i>STA User's Guide</i> .
Suspicion that a data collection failed due to a reason external to the STA server	NA

To perform a manual data collection, see the "Get the Latest Configuration Data From the Library" section within the *STA Installation and Configuration Guide*.

5.1.4 Library Connection Status Information

The Setup & Administration > Configuration > SNMP Connections > Monitored Libraries table displays the status of the most recent library connection test or data collection — scheduled, triggered, or manual. [Table 5–3](#) describes the connection status fields.

Table 5–3 Library Connection Status Fields

Field	Description
Last Successful Connection	Date and time of the most recent successful connection test or data collection.
Last Connection Attempt	Date and time when the most recent connection test or data collection was attempted.
Last Connection Status	Status of the most recent connection test or data collection. In a data collection, the status is updated throughout the process according to the screen refresh rate defined for your STA username. Possible statuses are: <ul style="list-style-type: none"> ■ In progress – A data collection is underway. ■ Success – The connection test or data collection completed successfully. ■ Failed – The connection test or data collection failed. Possible reasons are listed in the Last Connection Failure Detail field. ■ Rejected – The data collection request was rejected, possibly because the library is busy or unavailable. ■ Duplicate – The data collection request was rejected because another one is already in progress.
Last Connection Failure Detail	If the connection test or data collection failed or was rejected, possible causes are listed in this field.

5.2 SNMP Management Tasks

The following sections describe SNMP-related tasks you can perform after initially configuring a library for STA monitoring. For example, you would need to update the SNMP connection settings in both the STA application and on affected libraries if you assign a new IP address to the STA server.

- ["Confirm Network and SNMP Connectivity"](#) on page 5-5
- ["SNMP Management Tasks — Library"](#) on page 5-6
- ["SNMP Management Tasks — STA User Interface"](#) on page 5-7

- "Tasks to Perform After a Library Firmware Upgrade" on page 5-9
- "Tasks to Perform After a Redundant Electronics Switch" on page 5-10
- "Tasks to Perform After Changing the Library or STA Server IP Address" on page 5-10
- "Task to Perform After a Robot Change" on page 5-10

5.2.1 Confirm Network and SNMP Connectivity

To confirm a good SNMP connection between the STA server and libraries, log in to the CLI on the STA server and perform these steps for each monitored library.

Note: If you have configured STA to support Redundant Electronics or Dual TCP/IP on an SL3000 or SL8500 library, perform each of these steps twice: once for the primary library IP address and once for the secondary IP address.

1. Test the v3 SNMP connection.

```
# snmpget -v3 -u SNMP_user -a SHA -A auth_pwd -x DES -X priv_pwd -l authPriv
library_IP_addr 1.3.6.1.4.1.1211.1.15.3.1.0
```

Where:

- *SNMP_user* is the SNMP v3 user.
- **SHA** indicates the authentication protocol.
- *auth_pwd* is the authorization password.
- **DES** indicates the privacy protocol.
- *priv_pwd* is the privacy password.
- **authPriv** indicates that privacy is performed on the command.
- *library_IP_addr* is the IP address of the public port on the library.

2. Test the v2c SNMP connection.

```
# snmpget -v2c -c public -l authPriv library_IP_addr
```

Where:

- *library_IP_addr* is the IP address of the public port on the library.

3. Confirm packet routing from the STA server to the library.

```
# traceroute -I library_IP_addr
```

Where:

- **-I** indicates to use Internet Control Message Protocol (ICMP) echo request packets instead of User Datagram Protocol (UDP) datagrams.
- *library_IP_addr* is the IP address of the public port on the library.

4. Monitor TCP/IP packets sent between the STA server and the library.

```
# tcpdump -v host library_IP_addr > /var/tmp/file_name &
```

Where:

- **-v** indicates verbose output.
- **host** indicates to collect packets to or from the indicated host only (in this case, the library).
- *library_IP_addr* is the IP address of the public port on the library.
- *file_name* is the name of the file to which to save the output.

5.2.2 SNMP Management Tasks — Library

You perform the following tasks on each monitored library. For SL500, SL3000, or SL8500 libraries, log in to the library's CLI. For SL150 libraries, log in to the library's browser user interface.

- ["Display All SNMP Trap Recipients"](#) on page 5-6
- ["Delete or Modify the STA Trap Recipient"](#) on page 5-6
- ["Add A New Trap Recipient"](#) on page 5-7

5.2.2.1 Display All SNMP Trap Recipients

- With the CLI (all libraries except SL150):

```
snmp listTrapRecipients
```

Note the index number of the STA trap recipient in the displayed output.

Example 5-1 Display all SNMP trap recipients with the CLI

```
ADMIN> snmp listTrapRecipients
requestId
requestId 1
Attributes Auth SHA
AuthPass *****
Engine Id 0x80001f88807ad87e39453f
Host 192.0.2.20
Index 1
Name STAuser
Port 162
Priv DES
Priv Pass *****
Trap Level 1,2,3,4,11,13,14,21,25,27,41,45,61,63,65,81,85,100
Version v3
Object Snmp snmp
Done
Failure Count 0
Success Count 1
COMPLETED
```

- With the SL150 browser interface:
Go to **SNMP > SNMP Trap Recipients** to see a list of trap recipients.

5.2.2.2 Delete or Modify the STA Trap Recipient

For all libraries except the SL150, you can use the CLI to first delete a trap recipient before re-adding it with new information. For the SL150, you can select and modify a trap recipient without deleting it.

- With the CLI (all libraries except SL150):


```
snmp deleteTrapRecipient id index
```

Where *index* is the index number of the trap recipient to be deleted.

Example 5-2 Delete a trap recipient

```
ADMIN> snmp deleteTrapRecipient id 1
requestId 1
requestId 2
Device 1,0,0,0
Success true
Done
Failure Count 0
Success Count 1
COMPLETED
```

- With the SL150 browser interface:
 1. Select a trap recipient from the list.
 2. Select **Edit Trap Recipient** or **Delete Trap Recipient**.
 3. If modifying a trap recipient, modify the settings, and then click **Save**.

5.2.2.3 Add A New Trap Recipient

To create a new trap recipient, see the following sections in the *STA Installation and Configuration Guide*:

- SNMP v3 — "Create an SNMP v3 Trap Recipient" in Chapter 5.
- SNMP v2c — "Create an SNMP v2c Trap Recipient" in Appendix B.

5.2.3 SNMP Management Tasks — STA User Interface

You perform the following tasks within the STA user interface.

- ["Change SNMP Client Attributes"](#) on page 5-7
- ["Change Monitored Library Details"](#) on page 5-8
- ["Export SNMP Connection Settings to a Text File"](#) on page 5-8
- ["Remove a Library Connection"](#) on page 5-8

5.2.3.1 Change SNMP Client Attributes

Use this procedure to modify existing SNMP connection settings for STA, including the SNMP user name and passwords. For the connection to be successful, the values specified in this procedure must match the ones on the library.

1. Go to **Setup & Administration > Configuration > SNMP Connections**.
2. In the Client Attributes table, select a row, and then click **Edit**.

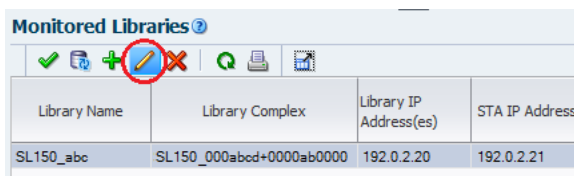
Configuration - SNMP Connections					
Client Attributes ?					
		Detach			
SNMP Username	Password Encryption	Privacy Encryption	Engine ID	User Community	Trap Com
STAsnmp	SHA	DES	0xab0def0000000000000000000000	public	public

3. In the Define SNMP Client Settings dialog box, enter any changes, and then click **Save**.
4. To avoid dropped connections and lost SNMP traps, you must test the connection to all monitored libraries. See "Test the SNMP Connection to the Library" in the *STA Installation and Configuration Guide*.

5.2.3.2 Change Monitored Library Details

Use this procedure to modify the SNMP connection settings for an existing library, including library IP addresses, library engine ID, and the STA server IP address. You can also change the library name, scheduled data collection time, and library time zone.

1. Go to **Setup & Administration > Configuration > SNMP Connections**.
2. In the Monitored Libraries table, select the library to modify, and then click **Edit**.



Library Name	Library Complex	Library IP Address(es)	STA IP Address
SL150_abc	SL150_000abcd+0000ab0000	192.0.2.20	192.0.2.21

3. In the Define Library Connection Details dialog box, enter any connection changes, and then click **Save**.

After you change library connection settings, the Library Engine ID field in the Monitored Libraries table will be blank, indicating the SNMP connection has been dropped.

Note: When changing the library IP address, STA verifies if the new IP address is associated with the serial number of the library you are modifying. You cannot specify the IP address of another library.

4. To re-establish the connection and avoid lost SNMP traps, you must test the connection to the affected library if you change any connection-related values, such as library IP address. See "Test the SNMP Connection to the Library" in the *STA Installation and Configuration Guide*.

5.2.3.3 Export SNMP Connection Settings to a Text File

Use this procedure to export all information appearing on the **Setup & Administration > Configuration > SNMP Connections** screen to a text file. This file is useful for troubleshooting connection issues or re-entering connection information. Passwords are not included in the file; they are masked with asterisks (*).

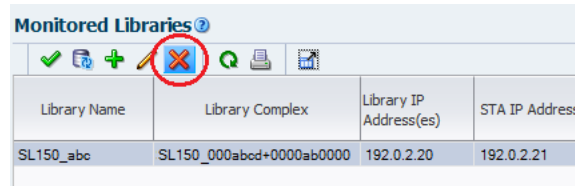
1. Go to **Setup & Administration > Configuration > SNMP Connections**.
2. At the bottom of the screen, click **Export**. The file will be saved with the name "SnmConfiguration."

5.2.3.4 Remove a Library Connection

Use this procedure to remove a library SNMP connection. All existing data for the library will be removed from the STA screens, but will be retained in the STA data store (see "Removed Libraries" in the *STA Data Reference Guide* for the impact of this procedure).

After performing this procedure, you can delete the STA SNMP trap recipient from the library. See ["Delete or Modify the STA Trap Recipient"](#) on page 5-6.

1. Go to **Setup & Administration > Configuration > SNMP Connections**.
2. In the Monitored Libraries table, select the library to remove, and then click **Delete**.



5.2.4 Tasks to Perform After a Library Firmware Upgrade

Note: This procedure does not apply to SL150 libraries.

Use this procedure to update the library and STA SNMP configurations after upgrading to one of the following library firmware versions or higher:

- SL500 – FRS 1468
- SL3000 – FRS 4.0
- SL8500 – FRS 8.0

Starting with these firmware versions, the library engine ID is generated with a new 32-bit value. If you do not perform this procedure, STA will be unable to receive SNMP traps from the library.

1. Log in to the STA user interface.
2. In the connection details for the upgraded library, clear the Library Engine ID field and click **Save**. See ["Change Monitored Library Details"](#) on page 5-8.
3. Re-establish the SNMP connection with the library. See ["Test the SNMP Connection to the Library"](#) in the *STA Installation and Configuration Guide*.
4. Record the new SNMP engine ID displayed on the SNMP connections table.
5. Log in to the CLI on the upgraded library.
6. Display all SNMP trap recipients. See ["Display All SNMP Trap Recipients"](#) on page 5-6.
7. Verify the SNMP Version level displayed for the STA server:
 - If it is "v2c", quit this procedure.
 - If it is "v3", continue to the next step.
8. Compare the displayed engine ID with the one you noted in Step 4:
 - If they match, quit this procedure.
 - If they do not match, continue to the next step.
9. Record the Index number of the STA trap recipient.
10. Delete the STA trap recipient. See ["Delete or Modify the STA Trap Recipient"](#) on page 5-6.

11. Re-add the STA v3 trap recipient using the new library engine ID. See ["Add A New Trap Recipient"](#) on page 5-7.

5.2.5 Tasks to Perform After a Redundant Electronics Switch

If a Redundant Electronics (RE) switch has occurred (SL3000 and SL8500 libraries only), do the following:

1. Wait 15 minutes after the newly-active card has fully initialized.
2. Perform a connection test to verify the library SNMP connection (see ["Test the SNMP Connection to the Library"](#) in the *STA Installation and Configuration Guide*).
3. Perform a data collection to retrieve the current library configuration data (see the ["Get the Latest Configuration Data From the Library"](#) section within the *STA Installation and Configuration Guide*).
4. If a controller card is replaced after the RE switch, update the library IP address in STA. See ["Change Monitored Library Details"](#) on page 5-8 for instructions.

STA configuration for RE is described in the "Library Configuration Concepts" chapter in the *STA Installation and Configuration Guide*.

5.2.6 Tasks to Perform After Changing the Library or STA Server IP Address

- If the IP address of a library changes, you will need to update the monitored library details in STA. See ["Change Monitored Library Details"](#) on page 5-8.
- If the IP address of the STA server changes, you will need to perform the following:
 1. Specify the STA server's new IP address as a trap recipient. See ["SNMP Management Tasks — Library"](#) on page 5-6.
 2. Update each monitored library's details in STA to reflect the STA server's new IP address. See ["Change Monitored Library Details"](#) on page 5-8.

5.2.7 Task to Perform After a Robot Change

If you make a robot change (add, remove, or swap), you should perform a manual data collection to retrieve current library configuration data (see the ["Get the Latest Configuration Data From the Library"](#) section within the *STA Installation and Configuration Guide*).

Preventing Denial of Service Attacks

This chapter describes a method to prevent Denial of Service (DoS) attacks on the STA server. Follow this procedure only after the initial library configuration is successful. After configuring IPTables, you should ensure that STA is still successfully monitoring your libraries.

Note: The following procedure is optional, and is provided for informational purposes only. Site security remains the responsibility of the customer.

- ["Overview"](#) on page A-1
- ["Configure iptables Rules"](#) on page A-2
- ["iptables Sample Script"](#) on page A-2

A.1 Overview

To protect the server from DoS attacks, configure the Linux **iptables** software to establish rules that filter ports and/or IP addresses. Based on the configuration of STA, Oracle recommends you attach rules to UDP 162 and the port values the STA managed servers are running on.

Note: See the "Port Configuration" section of the *STA Installation and Configuration Guide* for port information, including the default port values STA uses.

The [iptables Sample Script](#) can be used to define an input rule on the server to block hosts that attempt to connect, based on these criteria:

- A specific Ethernet interface
- A specific port
- A specific protocol
- The number of requests within a specified time period.

If the host connection count is exceeded within that time period, that host is blocked from further connections for the remainder of the time period.

A.2 Configure iptables Rules

To configure iptables rules:

1. Copy the source of the [iptables Sample Script](#) into a text editor.
2. Modify the following variables to suit your environment:
 - **INTERFACE**
Defines the ethernet interface to watch for attacks
 - **PORT**
Defines the port number to watch for attacks
 - **PROTO**
Defines the protocol (tcp or udp)
 - **HITS and TIME**
Decide what are reasonable values for the number of requests (HITS) within a given time period in seconds (TIME) to block a server.
3. Save the script to your system and execute it.
The new rules are added to iptables and take effect immediately.

A.3 iptables Sample Script

The following is an iptables sample script.

```
# The name of the iptable chain
CHAIN=INPUT
# The ethernet interface to watch for attacks
INTERFACE=eth0
# The port number to watch for attacks
PORT=80
# The protocol (tcp or udp)
PROTO=tcp
# A server that sends HITS number of requests within TIME seconds will be blocked
HITS=8
TIME=60
# Log filtered IPs to file
touch /var/log/iptables.log
grep iptables /etc/syslog.conf 1>/dev/null 2>&1
if [ $? -ne 0 ]; then
    echo kern.warning /var/log/iptables.log >>
    /etc/syslog.conf
    echo touch /var/log/iptables.log >> /etc/syslog.conf
    /etc/init.d/syslog restart
fi
# Undo any previous chaining for this combination of chain, proto, hits, and time
/sbin/iptables -L $CHAIN |grep $PROTO |grep $HITS |grep $TIME 1>/dev/null 2>&1
if [ $? -eq 0 ]; then
    R=0
    while [ $R -eq 0 ]; do
        /sbin/iptables -D $CHAIN 1 1>/dev/null 2>&1
        R=$?
    done
fi
# Logging rule
/sbin/iptables --append $CHAIN --jump LOG --log-level 4
```

```
# Interface rule
/sbin/iptables --insert $CHAIN --proto $PROTO --dport $PORT --in-interface
$INTERFACE --match state --state NEW --match recent --set
# Blocking rule
/sbin/iptables --insert $CHAIN --proto $PROTO --dport $PORT --in-interface
$INTERFACE --match state --state NEW --match recent --update --seconds $TIME
--hitcount $HITS --jump DROP
```


B

- backup service
 - administration utility, 3-8
 - binary logs, 3-10
 - clear preference settings, 3-3
 - configuration, 3-2
 - display preference settings, 3-3
 - dump files, 3-10
 - file locations, 3-9
 - logs, 3-9
 - overview, 3-2
 - process, 3-2
 - verify files have been sent to target server, 3-3
 - verify local backup files, 3-4

C

- changing library details, 5-8
- changing passwords, 4-1
- changing SNMP client attributes, 5-7
- checking STA processes, 2-2
- client attributes, 5-7
- configuration data
 - building, 5-2
 - collecting, 5-2
 - keeping up to date, 5-3
- connection status, 5-4

D

- database restoration, 3-14
- database services
 - administration overview, 3-1
 - executable program locations, 3-9
- denial of service attacks, preventing, A-1

E

- export connection settings, 5-8

F

- file types and locations, 3-8
- firmware upgrades, tasks after, 5-9

I

- IP address, tasks after changing, 5-10

L

- library connections, removing, 5-8
- library details, changing, 5-8
- log snapshot
 - access to logs screen, 1-2
 - deleting, 1-3
 - displaying run information, 1-3
 - downloading, 1-2
 - how to take, 1-2
 - process, 1-1
 - reasons for taking, 1-1
- logging, 1-1
 - collecting RDA information
 - with CLI, 1-3
 - with user interface, 1-2
 - forwarding log snapshot to Oracle Support, 1-4
 - overview, 1-1
- logs
 - backup, 3-9
 - configuration files, 3-13
 - MySQL binary, 3-10
 - ResMonAdm, 3-11
 - services daemon admin, 3-9, 3-11

P

- password
 - change backup service, 4-5
 - change database account, 4-1
 - change resource monitor, 4-5
 - changing, 4-1

R

- redundant electronics, tasks after a switch, 5-10
- removing library connections, 5-8
- reports
 - overview, 3-6
 - resource depletion alert report, 3-7
 - standard report, 3-6
- resource monitor service
 - administration utility, 3-8

- clear preference settings, 3-6
- configuration, 3-5
- CSV file, 3-11
- file locations, 3-11
- overview, 3-4
- query preference settings, 3-5
- reports overview, 3-6
- resource depletion alert report, 3-7
- standard report, 3-6
- restoration, database, 3-14
- robot, tasks after changing, 5-10

S

- service commands, 2-3
- services daemon
 - admin logs, 3-9
 - backup file locations, 3-9
 - configuration files, 3-10
 - logs, 3-11
 - overview, 3-1
 - startup and shutdown script, 3-8
- SNMP
 - configuration data, 5-2
 - confirm connectivity, 5-5
 - connection test, 5-2
 - management
 - add trap recipient, 5-7
 - change client attributes, 5-7
 - change library details, 5-8
 - delete or modify trap recipient, 5-6
 - display trap recipients, 5-6
 - export connection settings, 5-8
 - library, 5-6
 - remove library connection, 5-8
 - with user interface, 5-7
 - management concepts, 5-1
 - management tasks, 5-4
 - managing, 5-1
 - overview, 5-1
 - testing connections, 5-1
- STA command, 2-2
- STA server
 - administration, 2-1
 - administration commands, 2-2
 - managed servers, 2-1
 - memory usage requirements, 2-1
 - service commands, 2-3
- starting STA processes, 2-2
- status, connection, 5-4
- stopping STA processes, 2-2

T

- testing connections, 5-1
- testing connections, when to perform, 5-2
- trap recipients
 - adding, 5-7
 - deleting, 5-6
 - displaying, 5-6

- modifying, 5-6

U

- upgrading firmware, tasks after, 5-9

W

- WebLogic configuration files, 3-10