StorageTek Tape Analytics

Administration Guide

Version 2.2.0

E68625-01

February 2016

ORACLE

StorageTek Tape Analytics Administration Guide, Version 2.2.0

E68625-01

Primary Author: Nancy Stevens

Contents

3 Monitoring STA Server Resources

Preface

This document describes how to administer Oracle's StorageTek Tape Analytics (STA) and the dedicated server it runs on.

Audience

This document is intended for Linux 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 that have purchased support 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

The STA documentation set consists of the following documents.

For users of the STA application

- *STA Quick Start Guide*—Use this guide to introduce yourself to the STA application and some features of the user interface.
- *STA User's Guide*—Use this guide for instructions on using all STA application features, including the Dashboard, templates, filters, alerts, Executive Reports, logical groups, and STA media validation. This guide also provides instructions for administering and managing STA usernames, email addresses, service logs, and SNMP connections with the monitored libraries.
- *STA Screen Basics Guide*—Use this guide for full details about the STA user interface. It describes the screen navigation and layout, and the use of graphs and tables.
- *STA Data Reference Guide*—Use this guide to look up definitions for all STA tape library system screens and data attributes.

For installers and administrators of the STA server and application

- *STA Release Notes*—Read this document before installing and using STA. It contains important release information, including known issues. This document is included in the STA media pack download.
- *STA Requirements Guide*—Use this guide to learn about minimum and recommended requirements for using STA. This guide includes the following requirements: library, drive, server, user interface, STA media validation, and IBM RACF access control.
- *STA Installation and Configuration Guide*—Use this guide to plan for installation of STA, install the Linux operating system, install the STA application, and then configure STA to begin monitoring the libraries. This guide also provides instructions for upgrading to a new version of STA.
- *STA Administration Guide*—Use this guide for information about STA server administration tasks, such as STA services configuration, database backup and restore, and password administration for database accounts.
- *STA Security Guide*—Read this document for important STA security information, including requirements, recommendations, and general security principles.
- *STA Licensing Information User Manual*—Read this document for information about use of third-party technology distributed with the STA product.

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.
italic	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 section summarizes new and enhanced features for StorageTek Tape Analytics 2.2.0.

STA 2.2.0 February 2016

Oracle recommends upgrading to STA 2.2.0 or higher to take advantage of the new features described below.

- Maintenance fixes
- Performance improvements
- Updated recommended library and drive requirements to support STA 2.2.0 and higher. See the *STA Requirements Guide* for details.
- New response file build utility for the silent installer and deinstaller. The utility prompts you for the necessary information and saves the response file and an encryption key file to the directory of your choice. It writes passwords to the file in encrypted form. See the *STA Installation and Configuration Guide* for details.

1

Managing STA Services

This chapter includes the following sections:

About the STA Administration Environment

WebLogic is the application server that hosts the STA application. The STA administration environment consists of a single WebLogic domain, a MySQL database server, and the STA services daemon. The name assigned to the WebLogic domain is TBI, and this name must not be changed.

All resources for the STA environment are automatically started when the STA application is started. See "STA Application Startup and Shutdown Sequences" on page 1-2 for details.

Table 1–1 shows memory usage requirements for the environment.

Table 1–1 Memory Usage Requirements

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

Domain Servers

Following are the TBI domain servers and the processes they control.

- Administration server (staweblogic)—Control entity for the TBI domain; provides all security mechanisms.
- Managed servers:
  - staadapter—SNMP communication with the libraries; stores data received from the libraries.
  - staengine—Transforms data from the staadapter for the STA database.
  - staui—STA user interface

The administration server (staweblogic) must be running before the managed servers can be started. When the managed servers start up, they contact the administration server for their configuration information. Once they are up and running, if the administration server becomes unavailable, the managed servers continue to run uninterrupted.

STA Services Daemon

The STA Services daemon, staservd, is a continuously running Linux service that manages and runs the STA Backup and Resource Monitor (Resmon) services. The daemon must be running for these services to be available. The services run as separate execution threads within the STA services daemon.

The STA Services daemon is automatically started when the STA application is started and runs continuously in the background. The daemon is terminated when the STA application is shut down. See "STA Application Startup and Shutdown Sequences" on page 1-2.

You can also start, stop, and display the status of the STA services daemon independently of the STA application. See "STA Services Tasks" on page 1-3 for instructions.

Note: The Backup and Resmon services are disabled by default when STA is installed and you must configure the services to enable them. See "Administering the STA Database" on page 2-1 and "Monitoring STA Server Resources" on page 3-1 for details.

STA Application Startup and Shutdown Sequences

The STA processes are started and stopped in the following sequences when the STA application is started and shut down.

Startup sequence

When the STA application is started, the STA processes are started in the following sequence.

1. MySQL database server (mysql)
2. WebLogic administration server (staweblogic)
3. staEngine (staengine)
4. staAdapter (staadapter)
5. staUi (staui)
6. STA services daemon (staservd)

Shutdown sequence

When the STA application is shut down, the STA processes are stopped in the following sequence.

1. staUi (staui)
2. staAdapter (staadapter)
3. staEngine (staengine)
4. WebLogic administration server (staweblogic)
5. STA services daemon (staservd)

6. MySQL database (mysql)

Using the WebLogic Administration Console

The WebLogic administration console allows you to log in directly to the WebLogic server and display or modify the TBI domain. Because you perform almost all STA configuration and administration activities through the STA installer, STA application, or STA utilities, you do not normally need to use the WebLogic administration console.

Oracle recommends that you use the WebLogic administration console only for the following activities, depending on your site requirements.

- Configure security certificates for HTTPS/SSL ports; see the *STA Installation and Configuration Guide* for details.
- Configure external authentication providers (SSPs) to authenticate STA users; see the *STA Installation and Configuration Guide* for details.
- Create and maintain STA usernames for STA 1.0.x only; see the *STA Installation and Configuration Guide* for STA 1.0.x for details. Starting with STA 2.0.x usernames are created and maintained through the STA application; see the *STA User's Guide* for details.

All configuration information for the TBI domain is maintained in the following file:

/*Oracle_storage_home*/Middleware/user_projects/domains/TBI/config/config.xml

where *Oracle_storage_home* is the Oracle storage home location specified during STA installation.

STA Services Tasks

Note: The following tasks use the STA command. See "Using the STA Command" on page 1-8 for usage details.

Ensure the Correct root User Path

Use this procedure to ensure that the path for the system root user includes the directory for the STA command and the staresmonadm and staservadm utilities.

1. Open a terminal session on the STA server, and log in as the system root user.

2. Display the PATH variable and verify that it includes the following directory:

   /*Oracle_storage_home*/StorageTek_Tape_Analytics/common/bin

   where *Oracle_storage_home* is the Oracle storage home location specified during STA installation.

   For example:

   ```
   # echo $PATH
   /usr/lib64/qt-3.3/bin:/usr/local/sbin:/usr/local/bin:/root/bin:/sbin:/bin:/usr/
   sbin:/usr/bin:/Oracle/StorageTek_Tape_Analytics/common/bin
   ```

3. If the directory is missing, use a text editor to open the user profile and add it. For example:

   ```
   # vi /root/.bash_profile
   PATH=$PATH:/sbin:/bin:/usr/sbin:/usr/bin
   ```

   Save and exit the file.

4. Log out and log back in as the system root user.

5. Confirm that the PATH variable has been updated correctly.

   ```
   # echo $PATH
   /usr/lib64/qt-3.3/bin:/usr/local/sbin:/usr/local/bin:/root/bin:/sbin:/bin:/usr/
   sbin:/usr/bin:/Oracle/StorageTek_Tape_Analytics/common/bin
   ```

Display the Status of the STA Application

Use this procedure to display the current status of the STA application. The application is started automatically when you install STA, and therefore should normally be running.

1. Open a terminal session on the STA server, and log in as the system root user.

2. Display the application status. It may take a few minutes for the command to complete.

   ```
   # STA status all
   mysql is running
   staservd service is running
   staweblogic 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
   staui service is running
    .... and the deployed application for staui is in an ACTIVE state
   #
   ```

   If the application is not running, try restarting it. See "Start the STA Application" on page 1-5 for instructions.

Stop the STA Application

Use this procedure to gracefully shut down the STA application. You need to use this procedure when performing certain database tasks, such as moving or restoring the STA database. See "Administering the STA Database" on page 2-1 for details.

1. Open a terminal session on the STA server, and log in as the system root user.

2. Stop STA. It may take several minutes for the command to complete.

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

3. Verify the application has stopped.

```
# STA status all
mysql is shutdown
staservd service is shutdown
staweblogic service is shutdown
staengine service is shutdown.
staadapter service is shutdown.
staui service is shutdown.
#
```

Start the STA Application

Use this procedure to start the STA application, including all associated services. The application is automatically started when you install STA, so under normal circumstances, you only need to use this procedure to restart STA after performing certain database tasks, such as moving or restoring the STA database. See "Administering the STA Database" on page 2-1 for details.

1. Open a terminal session on the STA server, and log in as the system root user.
2. Start STA. It may take several minutes for the command to complete.

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

3. Verify the application has started successfully.

```
# STA status all
mysql is running
staservd service is running
staweblogic 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
staui service is running
 .... and the deployed application for staui is in an ACTIVE state
#
```

Display the Status of a Domain Server

Use this procedure to display the status of the administration server or a managed server.

1. Open a terminal session on the STA server, and log in as the system root user.
2. Display the status of the domain server using one of the following options:
   - staweblogic
   - staadapter
   - staengine
   - staui

   The following example shows the staengine server is running normally.

```
# STA status staengine
staengine service is running
 .... and the deployed application for staengine is in an ACTIVE state
#
```

   The following example shows the staui server is not running.

```
# STA status staui
staui service is shutdown
#
```

   If the domain server is not running, try restarting the STA applications. See "Stop the STA Application" on page 1-4 and "Start the STA Application" on page 1-5 for instructions.

> **Caution:** Although it is possible to stop and start individual STA domain servers, you should do so only under the direction of Oracle Service.

Display the Status of the STA Services Daemon

Use this procedure to verify that the STA services daemon is running. It must be running for the STA Backup and Resmon utilities to be available.

1. Open a terminal session on the STA server, and log in as the system root user.
2. Display the status of the daemon.

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

   If the daemon is not running, try restarting it. See "Stop the STA Services Daemon" on page 1-7 and "Start the STA Services Daemon" on page 1-7 for instructions.

Stop the STA Services Daemon

Use this procedure to stop the STA services daemon. Stopping the daemon does not interrupt the STA application, but the STA Backup and Resmon utilities will be unavailable until the daemon is restarted.

1. Open a terminal session on the STA server, and log in as the system root user.
2. Stop the STA services daemon.

```
# STA stop staservd
Stopping the staservd Service...
Successfully stopped staservd service
```

3. Verify the daemon has stopped.

```
# STA status staservd
staservd service is shutdown
#
```

Start the STA Services Daemon

Use this procedure start the STA services daemon. The daemon is started as part of the STA application startup sequence, so you only need to use this procedure if the daemon has been stopped.

1. Open a terminal session on the STA server, and log in as the system root user.
2. Start the STA services daemon.

```
# STA start staservd
Starting staservd Service.
staservd service was successfully started
#
```

3. Verify the daemon is running.

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

Start the MySQL Server

Use this procedure start the MySQL database server. The server is started when the STA application is started, so you only need to use this procedure if you are performing database management activities in which you must shut down the STA application and then restart just the MySQL server. See "Administering the STA Database" on page 2-1 for details.

1. Open a terminal session on the STA server, and log in as the system root user.
2. Start the MySQL service.

```
# STA start mysql
Starting mysql Service.
mysql service was successfully started
#
```

3. Verify the server is running.

```
# STA status mysql
mysql is running
#
```

Stop the MySQL Server

Use this procedure stop the MySQL database server. You should use this procedure only if you have been performing database management activities in which the MySQL server is running but the rest of the STA application is not. See "Administering the STA Database" on page 2-1 for details.

Caution: Do not stop the MySQL server if the rest of the STA application is running.

1. Open a terminal session on the STA server, and log in as the system root user.
2. Stop the MySQL server.

```
# STA stop mysql
Stopping the mysql service.....
Successfully stopped mysql service
#
```

3. Verify the server is not running.

```
# STA status mysql
mysql is shutdown
#
```

STA Command Reference

The STA command is located in the following directory:

/*Oracle_storage_home*/StorageTek_Tape_Analytics/common/bin

where *Oracle_storage_home* is the Oracle storage home location specified during STA installation.

See "Ensure the Correct root User Path" on page 1-3 for instructions on adding the directory to the system root user path.

Using the STA Command

The STA command is used to start, stop, and show the status of the entire STA application or an individual service. Use the command STA help to display complete command syntax and usage information.

Caution: Although it is possible to stop and start individual STA managed servers, you should do so only under the direction of Oracle Service.

STA Services Administration Logs

The STA services administration logs track all activity of the STA services daemon (staservd) the STA Backup utility (staservadm) and the STA Resource Monitor utility (staresmonadm). The logs can useful for troubleshooting issues with the STA services daemon or the services themselves.

The services administration logs are located in the following directory:

/var/log/tbi/db/backups

Following is a sample directory listing showing the files.

```
# ls -l /var/log/tbi/db/backups
total 9664
-rw-r--r-- 1 root root    1304 Dec  7 15:19 staresmonadm.log.0
-rw-r--r-- 1 root root    6353 Jan  8 16:17 staservadm.log.0
-rw-r--r-- 1 root root  808936 Feb  3 12:54 staservd.log.0
-rw-r--r-- 1 root root       0 Nov  4 12:31 staservd.log.0.lck
-rw-r--r-- 1 root root 1000085 Jan 28 01:34 staservd.log.1
-rw-r--r-- 1 root root 1000148 Jan 20 02:53 staservd.log.2
-rw-r--r-- 1 root root 1000114 Jan 12 03:57 staservd.log.3
-rw-r--r-- 1 root root 1000082 Jan  4 05:31 staservd.log.4
-rw-r--r-- 1 root root 1000006 Dec 27 06:24 staservd.log.5
-rw-r--r-- 1 root root 1000058 Dec 19 08:23 staservd.log.6
-rw-r--r-- 1 root root 1000098 Dec 11 09:47 staservd.log.7
-rw-r--r-- 1 root root 1000138 Dec  3 10:07 staservd.log.8
-rw-r--r-- 1 root root 1000082 Nov 25 10:52 staservd.log.9
```

The types of logs are as follows:

- staservd.log—STA services daemon log. Records when the STA Backup and Resource Monitor services perform their activities. See "STA Backup Service Process" on page 2-2 and "ResMon Service Process" on page 3-1 for details.
- staservadm.log—STA Backup utility log. Provides an audit trail of all usage of the staservadm utility.
- staresmonadm.log—STA Resource Monitor utility log. Provides an audit trail of all usage of the staresmonadm utility.

For each type of log, there may be up to 10 different log files in the directory, each with a sequential number, 0 to 9, indicating their order. Log "0" is always the active log, and logs "1" through "9" are historical. Log files have a 1.0 MB size limit, and when log "0" reaches the limit, the logs are rotated—log "0" becomes log "1", log "1" becomes log "2", and so on—and a new log "0" is started. Any existing log "9" is overwritten by log "8" and effectively deleted, or *rolled off*.

2

Administering the STA Database

This section includes the following topics:

Defining a Backup Strategy for the STA Database

It is essential that you perform regular automatic backups of the STA database to protect your site from potential data loss due to issues such as software crashes, hardware failures, or human error.

Database Best Practices

Oracle recommends that you implement a backup strategy that includes the following best practices.

Use redundant drives

Using mirrored or RAID drives for the database on the STA server helps to protect against a single drive failure.

Make regular backups

Back up the database regularly, and schedule full backups when database and server activity is low. The STA Backup service provides an easy way to do this; see "About the STA Backup Service" on page 2-2 for details. Frequent backups enable you to recover the database to a state close to current.

Back up to an external server

External backups protect your data from an operating system or hardware failure on the STA server. Additionally, once backup files are on an external server, you can manage the files using your site's preferred methods and tools. See "Prepare an External Backup Server" on page 2-6 for instructions.

The required space on the backup server is variable—the size should be a multiple of the size used for the STA database local backup, depending on the number of copies to be retained. Backup server storage should be mirrored or striped.

Archive older backups
Archived backups provide added protection in case your most recent backup is corrupted. Depending on your site policies, you can archive backups to tape or another server, and then delete archives older than a certain age.

Manage the database and backup space
It is the customer's responsibility to manage space on the STA server and the backup server. You should periodically check the amount of space consumed by the STA database backups and take appropriate action when space is running low.

Configure the STA Resource Monitor on the STA server
To assist with management of the STA server, you can define high-water marks for disk usage, and the Resource Monitor will alert you if these are exceeded. See "Monitoring STA Server Resources" on page 3-1 for details.

About the STA Backup Service

The STA Backup service allows you schedule regular backups of the STA database and save them to a designated location on either the STA server or an external server. It automatically performs a daily full backup of the STA database and key STA configuration directories and saves incremental backups at the intervals you specify. These are *hot backups*, meaning they are done while the MySQL server and the STA application are running.

The STA Backup service is disabled by default when STA is installed, and you must configure the service to enable it. You configure the STA Backup service with the staservadm utility. See "staservadm Utility Reference" on page 2-22 for command usage details. The STA Backup service is managed by the STA services daemon; see "STA Services Daemon" on page 1-2 for details.

Use of the STA Backup service is optional; if you have a preferred backup application at your site, you can use that instead.

STA Backup Service Process

Once enabled, the STA Backup service runs in the background and performs the following process. See "STA Backup Service Files" on page 2-24 for details about the contents and locations of all files that are created.

1. Once a day, at the time you have specified, the service performs the following actions.
   a. Uses the mysqldump command to create a high-speed dump of the current STA database (see "Define the Time of Day for Full Backups" on page 2-5 for instructions).
   b. Transfers all existing backup files to the backup location you have specified (see "Define Backup Host Information" on page 2-7 for details). This includes the following files:
      – Database dump file just created
      – Compressed STA services and WebLogic configuration directories
      – All incremental backups (binary log files) created in the past 24 hours

These files are purged from the local STA server, but if you are doing remote backups, the STA Backup service *never* deletes files from the external server. For remote backups, the files are compressed before being transferred to the external server.

c. Opens a new binary log file to save database changes that occur from this point forward.

2. Periodically, at the time interval you have specified, the service closes the current binary log file and opens a new one (see "Define the Interval Between Incremental Backups" on page 2-6 for details). This step is repeated at the intervals you have specified until the next full backup.

Tasks for Configuring the STA Backup Service

Note: These tasks use the staservadm utility, which requires the STA Services Daemon; see "Display the Status of the STA Services Daemon" on page 1-6 to verify that the daemon is running.

See "Using the staservadm Utility" on page 2-23 for usage details.

Display Current STA Backup Settings

Use this procedure to display the current settings for the STA Backup service.

1. Open a terminal session on the STA server, and log in as the system root user.
2. Display the current STA Backup service settings.

   Example 2–1 and Example 2–2 are sample outputs.

Example 2–1 STA Backup not configured

In this example the STA Backup service is disabled and therefore not performing any backups. The values displayed are the parameter defaults.

```
# staservadm -Q
Contacting daemon...connected.
Querying Preferences.
 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 []
 ====================================
```

Example 2–2 STA Backup configured

In this example, the STA Backup service is enabled and configured.

```
# staservadm -Q
Contacting daemon...connected.
Querying Preferences.
 Current STA Backup Service Settings:
   Configured            [yes]
   File Transfer      -S [SCP]
   Full Backup        -T [23:00]
   Sleep Interval     -i [350 sec]
   Backup Hostname    -s [stabackup]
   Backup Username    -u [root]
   Backup Password    -p [*******]
   Backup Directory   -d [/dbbackup]
   Database Username  -U [stadba]
   Database Password  -P [*********]
 ====================================
```

Enable the STA Backup Service

When STA is installed, the STA Backup service is disabled by default. Use this procedure to enable the service. Once enabled, the STA Backup service performs automatic full and incremental backups of the STA database according to the defined settings.

To enable the service, all parameters must be defined. For parameters with default values, you can retain the defaults or define new values.

1. Open a terminal session on the STA server, and log in as the system root user.
2. Define the required parameters in one or more commands.

```
# staservadm -s stabackup -d /dbbackup -u root -p -U stadba -P
Enter server password:
Enter database password:
Contacting daemon...connected.
Setting Backup Hostname..... stabackup
Setting Backup Username..... root
Setting Backup Password..... *******
Setting Backup Directory..... /dbbackup
Setting Database Username.... stadba
Setting Database Password.... *******
Done.
 Current STA Backup Service Settings:
   Configured            [yes]
   File Transfer      -S [SCP]
   Full Backup        -T [00:00]
   Sleep Interval     -i [300 sec]
   Backup Hostname    -s [stabackup]
   Backup Username    -u [root]
   Backup Password    -p [*******]
   Backup Directory   -d [/dbbackup]
   Database Username  -U [stadba]
```

```
  Database Password  -P [*******]
 ====================================
```

The utility will perform the first full backup at the time indicated and incremental backups periodically after that; you to not need to stop and restart the STA services daemon.

Disable the STA Backup Service

Use this procedure to clear all STA Backup service preference settings and disable the service. When disabled, the service does not perform backups.

1. Open a terminal session on the STA server, and log in as the system root user.
2. Clear all preference settings.

```
# ./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 []
 ====================================
```

The service is disabled immediately; you do not need to stop and restart the STA services daemon.

Define the Time of Day for Full Backups

Use this procedure to define the time of day when full backups are performed.

1. Open a terminal session on the STA server, and log in as the system root user.
2. Define the time of day to perform the backups; this is according to the system time on the STA server. In this example, the time is set to 23:30.

```
# staservadm -T 23:30
Contacting daemon...connected.
Setting Full Backup Time..... 23:30
Done.
 Current STA Backup Service Settings:
   Configured            [yes]
   File Transfer      -S [SCP]
   Full Backup        -T [23:30]
   Sleep Interval     -i [1800 sec]
   Backup Hostname    -s [stabackup]
   Backup Username    -u [root]
   Backup Password    -p [*******]
   Backup Directory   -d [/dbbackup]
   Database Username  -U [root]
   Database Password  -P [******]
 ====================================
```

3. If you want the new time to take effect immediately, you must stop and restart the STA services daemon. See "Stop the STA Services Daemon" on page 1-7 and "Start the STA Services Daemon" on page 1-7 for instructions.

Define the Interval Between Incremental Backups

Use this procedure to define the number of seconds between incremental backups.

1. Open a terminal session on the STA server, and log in as the system root user.
2. Define the interval between backups, in seconds.

   In this example, the interval is set to 1800 seconds, or 30 minutes.

```
# staservadm -i 1800
Setting Sleep Interval........ 1800
Done.
```

3. If you want the new interval to take effect immediately, you must stop and restart the STA services daemon. See "Stop the STA Services Daemon" on page 1-7 and "Start the STA Services Daemon" on page 1-7 for instructions.

Prepare an External Backup Server

Oracle recommends backing up the database to an external backup server. Use this procedure to configure the external server so it can be used by the STA Backup service.

> **Note:** This procedure is performed entirely on the external backup server.

1. Open a terminal session on the external server, and log in as the system root user.
2. Create a new group for the STA Backup user. For example:

```
# groupadd -g 54321 backupgroup
```

   Where:

   - -g 54321 assigns the specified numerical group ID to the group.
   - backupgroup is the backup group name.

3. Confirm the group exists.

```
# cat /etc/group | grep backupgroup
backupgroup:x:54321:
```

4. Create the STA Backup user. For example:

```
# useradd stabackup -c "STA DB backup user" -m -d /home/stabackup -g
backupgroup -s /bin/bash -u 98765
```

   Where:

   - stabackup is the username.
   - -c specifies a comment, which is enclosed in quotes.
   - -m creates the user's home directory.
   - -d specifies the absolute path of the user's home directory.

- -g assigns the user to the backupusers group.
- -s assigns the specified login shell to the user.
- -u assigns the specified numerical user ID to the user.

5. Confirm the user exists.

```
#  cat /etc/passwd | grep stabackup
stabackup:x:98765:54321:STA DB backup user:/home/stabackup:/bin/bash
```

6. Assign a password to the user.

```
# passwd stabackup
Changing password for user stabackup.
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
```

7. Create the directory where the STA backups will be copied. For example:

```
# mkdir -p /remote_backups/STAbackups
# ls -l /remote_backups
total 4
drwxr-xr-x 2 root root 4096 Jan  2 13:20 STAbackups
```

Where:

- -p indicates to create the parent directory if it does not exist already.
- /remote_backups/STAbackups is the absolute path to the new directory.

8. Assign exclusive ownership and access rights for the directory to the STA Backups user and group. For example:

```
# chown -R stabackup:backupgroup /remote_backups/STAbackups
# chmod -R 700 /remote_backups/STAbackups
```

Where:

- -R indicates to recursively assign the specified attributes to the directory and its files.

9. List the directory to confirm that all information has been entered correctly. For example:

```
# ls -l /remote_backups
drwx------ 2 stabackup backupgroup 4096 Jan 2 14:20 STAbackups
```

Define Backup Host Information

Use this procedure to specify the following information about the backup host:

- File transfer method (SCP or FTP)
- Backup host name or IP address
- Target directory on the backup host
- Backup username and password; if you specify the username, you must also specify the password.

Note: Oracle recommends backing up the database to an external backup server. See "Prepare an External Backup Server" on page 2-6 to configure the backup server for use with the STA Backup service.

1. Open a terminal session on the STA server, and log in as the system root user.
2. Specify the backup host information. To specify the password, you can use either of the following methods:
   - Enter -p and the password in clear text on the command line.
   - Enter -p with no password on the command line. When you submit the command, the utility prompts for the password, which is hidden when you type it.

   In this example, the utility prompts for the password.

```
# staservadm -s stabackup -d /dbbackup -u root -p
Enter server password:
Contacting daemon...connected.
Setting Backup Hostname...... stabackup
Setting Backup Username...... root
Setting Backup Password...... *******
Setting Backup Directory..... /dbbackup
Done.
 Current STA Backup Service Settings:
   Configured            [yes]
   File Transfer      -S [SCP]
   Full Backup        -T [00:00]
   Sleep Interval     -i [300 sec]
   Backup Hostname    -s [stabackup]
   Backup Username    -u [root]
   Backup Password    -p [*******]
   Backup Directory   -d [/dbbackup]
   Database Username  -U [stadba]
   Database Password  -P [*******]
 ====================================
```

3. If you want the new settings to take effect immediately, you must stop and restart the STA services daemon. See "Stop the STA Services Daemon" on page 1-7 and "Start the STA Services Daemon" on page 1-7 for instructions.

Specify the Database Username and Password

Use this procedure to specify the MySQL account that the STA Backup service uses to connect to the MySQL server and perform the backups. This must be the MySQL database administrator account created during STA installation.

1. Open a terminal session on the STA server, and log in as the system root user.
2. Specify the MySQL database administrator username and the user password. You can use either of the following methods to specify the password:
   - Enter -P and the password in clear text on the command line.
   - Enter -P with no password on the command line. When you submit the command, the utility prompts for the password, which is hidden when you type it.

   In this example, the utility prompts for the password.

```
# staservadm -U stadba -P
Enter database password:
Contacting daemon...connected.
Setting Database Username.... stadba
Setting Database Password.... *******
Done.
```

3. If you want the new settings to take effect immediately, you must stop and restart the STA services daemon. See "Stop the STA Services Daemon" on page 1-7 and "Start the STA Services Daemon" on page 1-7 for instructions.

Tasks for Managing Backups Created by the STA Backup Service

View Log Entries for a Backup

Use this procedure to find STA server log entries for a backup.

1. Open a terminal session on the STA server, and log in as the system root user.
2. Change to the STA services log directory.

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

3. Use any of the following searches to find log entries for the backup.

   Note: Depending on the amount of log activity and when the backup was performed, entries for the backup in question may be in the current log file (staservd.log.0) or an earlier one (staservd.log.1, staservd.log.2, and so on). You may need to search more than one log file to find the applicable entries.

   - Display all backups recorded in the log file. In this example, backups for January 21 through 23 are included in the staservd.log.1 log file.

     ```
     # grep 'StaBackup' staservd.log.1 | grep 'Database dump completed'
     INFO: {StaBackup} done. Database dump completed, file located at
     /dbbackup/local/20160121_111203.stafullbackup.sql
     INFO: {StaBackup} done. Database dump completed, file located at
     /dbbackup/local/20160122_170231.stafullbackup.sql
     INFO: {StaBackup} done. Database dump completed, file located at
     /dbbackup/local/20160123_170250.stafullbackup.sql
     ```

   - Refine the search to display entries just for the backup in question. This example shows entries for the backup done on January 23, 2016.

     ```
     # grep 'StaBackup' staservd.log.1 | grep 20160123
     INFO: {StaBackup} sending file /dbbackup/local/20160123_170250.conf.zip to
     stabackup.mycompany.com
     INFO: {StaBackup} sending file /dbbackup/local/20160123_
     170250.fmwconfig.zip to stabackup.mycompany.com
     ```

```
INFO: {StaBackup} done. Database dump completed, file located at
/dbbackup/local/20160123_170250.stafullbackup.sql
INFO: {StaBackup} sending file /dbbackup/local/20160123_
170250.stafullbackup.sql to stabackup.mycompany.com
```

- Refine the search to display the name of the host where the files for the backup in question were sent. In this example, the files were sent to stabackup.mycompany.com. This may be the local server or an external server.

```
# grep 'StaBackup' staservd.log.1 | grep 20160123 | grep 'sending file'
INFO: {StaBackup} sending file /dbbackup/local/20160123_170250.conf.zip to
stabackup.mycompany.com
INFO: {StaBackup} sending file /dbbackup/local/20160123_
170250.fmwconfig.zip to stabackup.mycompany.com
INFO: {StaBackup} sending file /dbbackup/local/20160123_
170250.stafullbackup.sql to stabackup.mycompany.com
```

List All Files for a Full Database Dump

Use the following steps to verify that files for a full backup have been successfully saved to the right location and to check the size of the files.

1. Open a terminal session on the applicable server, and log in as the system root user.

   Note: The backup directory may be on the local STA server or an external server. The location is defined by the staservadm utility; see "Display Current STA Backup Settings" on page 2-3 for instructions on displaying the location.

   Oracle recommends backing up the database to an external backup server.

2. Change to the backup directory. The following example shows an external backup server.

```
# cd /remote_backups/stabackups
```

3. List the files for the backup in question. This example includes the following files for the full backup done on January 23, 2016.
   - A full dump of the STA database, identified by the file name ending in stafullbackup.sql.
   - MySQL server configuration files, identified by the file name ending in fmwconfig.zip.
   - STA services configuration files, identified by the file name ending in conf.zip.

```
# ls -l *20160123*
-rw-r--r-- 1 stabck stabckgr  11081 Jan 23 17:02 20160123_170250.conf.zip.gz
-rw-r--r-- 1 stabck stabckgr 195524 Jan 23 17:02 20160123_170250.fmwconfig.zip.gz
-rw-r--r-- 1 stabck stabckgr  37968 Jan 24 17:03 20160123_170250.stadb-bin.000028.gz
-rw-r--r-- 1 stabck stabckgr 461721 Jan 23 17:02 20160123_170250.stafullbackup.sql.gz
```

List Incremental Backup Files (Binary Logs)

Use the following steps to list the incremental backups (binary log files) created since the last full backup. Incremental backups are always located on the local STA server.

Note: Frequent incremental backups can generate a significant number of binary log files that may consume considerable hard drive space. You may want to purge old binary logs periodically.

1. Open a terminal session on the STA server, and log in as the system root user.
2. Change to the incremental backup directory.

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

3. List the directory. This example shows the following incremental backup files:
   - Incremental backups (binary log files), which have the file names stadb-bin.000028 and stadb-bin.000029. These files are created at the intervals defined with the staservadm utility (see "Define the Interval Between Incremental Backups" on page 2-6 for instructions).
   - Index file for the binary log files, which has the name stadb-bin.index.
   - "Slow queries" log, which has the name stadb-slow.log. This log lists MySQL queries that take a long time to execute and is a tool used by Oracle Service and development.

```
# ls -l
total 876
drwxr--r-- 2 mysql mysql   4096 Jan 24 02:52 backups
-rw-rw---- 1 mysql mysql 161351 Jan 24 17:03 stadb-bin.000028
-rw-rw---- 1 mysql mysql 146592 Jan 25 14:55 stadb-bin.000029
-rw-rw---- 1 mysql mysql     66 Jan 24 17:03 stadb-bin.index
-rw------- 1 mysql mysql   6561 Jan 24 17:03 stadb-slow.log
```

View Binary Log Contents

When doing a database restore, you may not want to apply an entire incremental backup file if you suspect it contains corrupted database operations. In this case, you can view the contents of the binary log to identify the valid events you want to apply.

To view binary log events, you must use the MySQL mysqlbinlog utility. The utility converts the binary file contents to text form. This procedure provides some sample methods for using the utility. See the mysqlbinlog utility reference for complete details.

Example 2–3 View Binary Log Contents Directly

```
# mysqlbinlog stadb-bin.000016 | more
/*!50530 SET @@SESSION.PSEUDO_SLAVE_MODE=1*/;
/*!40019 SET @@session.max_insert_delayed_threads=0*/;
/*!50003 SET @OLD_COMPLETION_TYPE=@@COMPLETION_TYPE,COMPLETION_TYPE=0*/;
DELIMITER /*!*/;
# at 4
#160125 17:03:36 server id 1  end_log_pos 120 CRC32 0x2a76ef3b  Start: binlog v 4,
server v 5.6.18-enterprise-commercial
-advanced-log created 160125 17:03:36
BINLOG '
2LemVg8BAAAAdAAAAHgAAAAAAAQANS42LjE4LWVudGVycHJpc2UtY29tbWVyY2lhbC1hZHZhbmNl
ZC1sb2cAAAAAAAAAAAAAAAAAAEzgNAAgAEgAEBAQEEgAAXAAEGggAAAAICAgCAAAACgoKGRkAATvv
dio=
'/*!*/;
# at 120
--More--
```

Example 2–4 Save Binary Log Contents to a Text File for Viewing

```
# mysqlbinlog stadb-bin.000030 > ./tmpfile
# tail tmpfile
SET @@session.character_set_client=33,@@session.collation_
connection=33,@@session.collation_server=8/*!*/;
FLUSH TABLES
/*!*/;
# at 172335
#160126 17:04:01 server id 1  end_log_pos 172382 CRC32 0x5ab0deca       Rotate to
stadb-bin.000031  pos: 4
DELIMITER ;
# End of log file
ROLLBACK /* added by mysqlbinlog */;
/*!50003 SET COMPLETION_TYPE=@OLD_COMPLETION_TYPE*/;
/*!50530 SET @@SESSION.PSEUDO_SLAVE_MODE=0*/;
#
```

Verify a Local Backup

1. Open a terminal session on the STA server, and log in as the system root user.
2. List the STA services log directory. For example:

```
# ls -l /var/log/tbi/db/backups
total 3268
-rw-r--r-- 1 root root   87255 Jan  7 14:53 staresmonadm.log.0
-rw-r--r-- 1 root root   46017 Jan 22 12:42 staservadm.log.0
-rw-r--r-- 1 root root  173908 Jan 25 12:32 staservd.log.0
-rw-r--r-- 1 root root       0 Jan 21 16:47 staservd.log.0.lck
-rw-r--r-- 1 root root 1000085 Jan 24 02:52 staservd.log.1
-rw-r--r-- 1 root root 1000226 Jan 16 02:45 staservd.log.2
-rw-r--r-- 1 root root 1000104 Jan  8 02:05 staservd.log.3
```

3. To determine which services log includes entries for the date you want to confirm, use the following search:

4. Use the following steps to list the most recent full backup.
   a. Change to the local backup subdirectory for your site. For example:

      ```
      # cd /dbbackup/local
      ```

   b. List the directory.

      ```
      # ls -l
      total 23573716
      -rw-r--r-- 1 root root       11807 Jan  8 00:03 20160108_240323.conf.zip
      -rw-r--r-- 1 root root      266625 Jan  8 00:03 20160108_
      240323.fmwconfig.zip
      -rw-r--r-- 1 root root 23294354241 Jan  8 02:40 20160108_
      240323.stafullbackup.sql
      ```

Tasks for Restoring the STA Database From Backup

- "Restore the Database Configuration Directory Files" on page 2-14
- "Reload the Database" on page 2-16
- "Perform a Partial Restore From a Range of Log Numbers" on page 2-17

For additional information about restoring a MySQL database, see the MySQL documentation at the following site:

http://docs.oracle.com/en/database/

Database Restoration Process

This process restores the database to the point when the last incremental backup was completed. You load the most recent full database dump and then apply the incremental backups created since the dump. Depending on the size of your database and the number of incremental backups, this may be a lengthy process.

To restore the STA database, perform the tasks in the order listed.

1. "Prepare a Replacement STA Server (optional)" on page 2-13
2. "Copy Backup Files to the Server" on page 2-13
3. "Restore the Database Configuration Directory Files" on page 2-14
4. "Reload the Database" on page 2-16
5. Either of the following procedures, depending on which incremental backups need to be restored:
   - "Perform a Full Restore From All Incremental Backups" on page 2-16
   - "Perform a Partial Restore From a Range of Log Numbers" on page 2-17

Prepare a Replacement STA Server (optional)

Use this procedure if the STA server experienced a catastrophic failure and you need to install and configure a replacement STA server.

> **Note:** The replacement server must run the same version of Linux and STA as the original STA server.

1. Install Linux on the replacement server. See the *STA Installation and Configuration Guide* for instructions.
2. Install STA on the replacement server. See the *STA Installation and Configuration Guide* for instructions.
3. Add the replacement server as an SNMP trap recipient on all libraries monitored by STA. See the *STA Installation and Configuration Guide* for instructions.

Copy Backup Files to the Server

Use this procedure to copy the complete set of files for the most recent backup from the backup server to the STA server. This includes the most recent full database dump file and all incremental backups created since then.

1. On the backup server, copy the backup files to the STA server.
   a. Open a terminal session on the backup server, and log in as the system root user. If you are only doing local backups, this is the STA server.

b. Copy the complete set of one day's backup files to the STA server. Oracle recommends copying the files to the /tmp directory. For example:

```
# scp *20160123* staserver.mycompany.com:/tmp/.
root@staserver.mycompany.com's password:
20160123_170250.conf.zip.gz                 100%   11KB  10.8KB/s   00:00
20160123_170250.fmwconfig.zip.gz            100%  191KB 190.9KB/s   00:00
20160123_170250.stadb-bin.000028.gz         100%   37KB  37.1KB/s   00:00
20160123_170250.stafullbackup.sql.gz        100%  451KB 450.9KB/s   00:00
```

where:

– *20160123* indicates to copy all files with this date stamp.

– staserver.mycompany.com is the name of the STA server.

– /tmp is the target directory.

2. On the STA server, verify and decompress the files.

a. Open a terminal session on the STA server, and log in as the system root user.

b. Change to the target directory and verify the compressed files were successfully copied.

```
# cd /tmp
# ls -l *20160123*
-rw-r--r-- 1 root root  11081 Jan 27 15:18 20160123_170250.conf.zip.gz
-rw-r--r-- 1 root root 195524 Jan 27 15:18 20160123_170250.fmwconfig.zip.gz
-rw-r--r-- 1 root root  37968 Jan 27 15:18 20160123_
170250.stadb-bin.000028.gz
-rw-r--r-- 1 root root 461721 Jan 27 15:18 20160123_
170250.stafullbackup.sql.gz
```

c. Unzip the compressed files.

```
# gunzip *20160123*.gz
# ls -l *20160123*
-rw-r--r-- 1 root root   11939 Jan 27 15:18 20160123_170250.conf.zip
-rw-r--r-- 1 root root  259328 Jan 27 15:18 20160123_170250.fmwconfig.zip
-rw-r--r-- 1 root root  161351 Jan 27 15:18 20160123_
170250.stadb-bin.000028
-rw-r--r-- 1 root root 3653692 Jan 27 15:18 20160123_
170250.stafullbackup.sql
```

Restore the Database Configuration Directory Files

Use this procedure to restore the STA service and server configuration directory files. To ensure a clean restore, remove any existing directories after first backing them up, and then completely replace the directories from the backups.

The backup zip files were created with the full directory paths to allow you to restore or overwrite existing files.

Note: This procedure is performed entirely on the STA server.

1. Open a terminal session on the STA server, and log in as the system root user.

2. Stop all STA processes. See "Stop the STA Application" on page 1-4 for details.

```
# STA stop all
```

3. Restart the MySQL server. See "Start the MySQL Server" on page 1-7 for details.

```
# STA start mysql
```

4. As a safeguard, save the existing STA services configuration directory to a zip file. For example:

```
# cd /Oracle/StorageTek_Tape_Analytics/common
# zip -vr conf.orig.zip conf
  adding: conf/ (in=0) (out=0) (stored 0%)
  adding: conf/staservadm.log.props     (in=934) (out=355) (deflated 62%)
...
total bytes=102262, compressed=10598 -> 90% savings
#
```

5. As a safeguard, save the existing database server configuration directory to a zip file. For example:

```
# cd /Oracle/Middleware/user_projects/domains/TBI/config
# zip -vr fmwconfig.orig.zip fmwconfig
  adding: fmwconfig/ (stored 0%)
  adding: fmwconfig/mbeans/ (stored 0%)
  adding: fmwconfig/mbeans/jps_mbeans.xml (deflated 72%)
...
total bytes=1846687, compressed=222531 -> 88% savings
#
```

6. Delete the existing configuration directories.

```
# rm -rf /Oracle/StorageTek_Tape_Analytics/common/conf
# rm -rf /Oracle/Middleware/user_projects/domains/TBI/config/fmwconfig
```

7. Unzip the backup STA services and database server configuration directories. For example:

```
# cd /tmp
# unzip -X -d / 20160123_170250.conf.zip
Archive:  20160123_170250.conf.zip
warning:  stripped absolute path spec from /Oracle/StorageTek_Tape_
Analytics/common/conf/staservadm.log.props
  inflating: /Oracle/StorageTek_Tape_Analytics/common/conf/staservadm.log.props
warning:  stripped absolute path spec from /Oracle/StorageTek_Tape_
Analytics/common/conf/staresmonadm.log.props
  inflating: /Oracle/StorageTek_Tape_
Analytics/common/conf/staresmonadm.log.props
...
#
#  unzip -X -d / 20160123_170250.fmwconfig.zip
Archive:  20160123_170250.fmwconfig.zip
warning:  stripped absolute path spec from /Oracle/Middleware/user_
projects/domains/TBI/config/fmwconfig/mbeans/jps_mbeans.xml
  inflating: /Oracle/Middleware/user_
projects/domains/TBI/config/fmwconfig/mbeans/jps_mbeans.xml
warning:  stripped absolute path spec from /Oracle/Middleware/user_
projects/domains/TBI/config/fmwconfig/mbeans/igf_mbeans.xml
  inflating: /Oracle/Middleware/user_
projects/domains/TBI/config/fmwconfig/mbeans/igf_mbeans.xml
...
#
```

where:

- -X indicates to restore user and group ownership.

- -d / indicates to restore the files to the root directory (/). Since the backup zip files were created using the full directory paths for each file, this restores the files to their original locations.

8. Verify the configuration directories have been restored. For example:

```
# ls -l /Oracle/StorageTek_Tape_Analytics/common
# ls -l /Oracle/Middleware/user_projects/domains/TBI/config
```

Reload the Database

Use this procedure to reload the STA database from the full database dump.

1. Open a terminal session on the STA server, and log in as the MySQL root user.
2. Ensure there is no residual STA database left on the server. The STA database has the name stadb. For example:

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

where:

- -u root indicates to execute the command as the MySQL root user
- -p indicates to prompt for the user password.
- -e indicates to execute the following MySQL statement and then quit the mysql command. The statement must be enclosed in quotes.
  - 'drop database stadb'—Removes the database named stadb, which is the STA database.

3. Load the latest full database backup. For example:

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

where:

- -u root specifies the MySQL root username.
- -p indicates to prompt for the user password.
- -e indicates to execute the following MySQL statement and then quit the mysql command. The statement must be enclosed in quotes.
  - 'source 20130723_133755.stafullbackup.sql;'— Executes the specified database dump file; the dump file creates the schema and installs all the data.

4. Continue to either of the following procedures, depending on whether you want to restore all incremental backups or only selected ones.
   - To restore all incremental backups created after the last full dump, see "Perform a Full Restore From All Incremental Backups" on page 2-16.
   - To restore only a range of incremental backups, see "Perform a Partial Restore From a Range of Log Numbers" on page 2-17. Use this procedure if you suspect a database operation may have corrupted the database and you only want to restore operations up to, but not including, that one.

Perform a Full Restore From All Incremental Backups

Use this procedure to restore all incremental backups (binary logs) since the last full backup, in the proper order. This procedure uses the MySQL mysqlbinlog utility.

1. Open a terminal session on the STA server, and log in as the MySQL root user.
2. Run the binary logs in chronological order, from oldest to newest.

   If you have more than one binary log to execute, you should process them all using a single connection to the MySQL server. Use one of the following methods:

   - The safest method is to use a single connection to the server and a single MySQL process to execute the contents of all 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
     Password:
     ```

   - Another safe method is to concatenate all applicable binary logs to a single file and then process that file. For example:

     ```
     # 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'
     Password:
     ```

     Caution: Do *not* use multiple connections to the MySQL 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."

     Following is an example of how *not* to process the binary logs, as this method may create multiple connections to the server.

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

Perform a Partial Restore From a Range of Log Numbers

Use this procedure to do a partial restore of the STA database, also known as a *point-in-time* restore, from a range of log numbers. Using this method, you restore the database from the last full dump and then apply just the binary log operations that fall within the start and end points you specify.

Log positions are labeled in the binary log as log_pos followed by a unique number.

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. Therefore, you want to restore the database only up to the last good entry (#6817916), excluding the erroneous operation and all that follow.

In this procedure, you restore the database from the full dump done the day before, and then replay the most recent binary log from its initial log entry number "176" through entry number "6817916".

1. Open a terminal session on the STA server, and log in as the system root user.
2. Stop all STA processes. See "Stop the STA Application" on page 1-4 for details.

```
# STA stop all
```

3. Restart the MySQL server. See "Start the MySQL Server" on page 1-7 for details.

```
# STA start mysql
```

4. Open a terminal session on the STA server, and log in as the MySQL root user.
5. Extract the valid operations from the binary logs. For example:

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

   where:

   - --start-position is the first log entry you want to extract.
   - --stop-position is the last log entry you want to extract. In this example, entries 176 to 6817916 are extracted.
   - /var/log/tbi/db/stadb-bin.00007 is the binary log file you want to extract from.
   - ./recover.sql is the file you want to write the entries to.

6. Apply the selected operations to the database. For example:

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

   where:

   - -u root specifies the STA database root username.
   - -p indicates to prompt for the user password.
   - -e indicates to execute the following MySQL statement and then quit the mysql command. The statement must be enclosed in quotes.
     - 'source ./recover.sql'—Applies the entries in the specified file to the database.

7. Open a terminal session on the STA server, and log in as the system root user.
8. Restart STA and all associated processes; see "Start the STA Application" on page 1-5 for instructions.

Tasks for Transferring the STA Database to Another Server

The se tasks assume the new (*target*) server will use the same version of STA as the current server. To upgrade the database to a new version of STA, see the upgrade instructions in the *STA Installation and Configuration Guide*.

Following are some reasons why you may want to transfer the STA database to another server.

- You may want to replace the current STA server with a new one, in which case you need to permanently relocate the database.
- You may want to test a feature you have not used before, such as STA media validation or alerts, in which case you want to temporarily set up another instance of STA with a fully populated database.

Database Transfer Process

To transfer the STA database, perform the tasks in the order listed.

1. "Prepare the Target Server" on page 19.
2. "Dump the STA Database" on page 19.
3. "Transfer the Dump File to the Target Server" on page 20.
4. "Process and Load the STA Database on the Target Server" on page 21.
5. "Perform Post-transfer Configuration Tasks" on page 22.

Prepare the Target Server

Use this procedure to prepare the target server for the STA database. The target server must run the same version of Linux and STA as the current STA server.

1. Install Linux on the target server. See the *STA Installation and Configuration Guide* for instructions.
2. Install STA on the target server. See the *STA Installation and Configuration Guide* for instructions.
3. Perform the following steps on all libraries monitored by STA.
   a. Add the target server as an SNMP trap recipient; this will cause the libraries to send SNMP data to the target server. See the *STA Installation and Configuration Guide* for instructions.
   b. If the target server is replacing the current STA server, remove the current STA server as an SNMP trap recipient; this will cause the libraries to stop sending SNMP data to the current server. See the *STA Installation and Configuration Guide* for instructions.

Dump the STA Database

Use this procedure to perform a full dump of the current STA database.

Note: This procedure is performed entirely on the current STA server.

---

1. Display the size of your current STA database.
   a. Open a browser window and log in to STA.
   b. Click **About** in the Status Bar.
   c. In the About dialog box, scroll down to where the Database Current Size is displayed, and record the value.
2. Verify that the location where you want to dump the database has sufficient space.
   a. Open a terminal session on the STA server and log in as the system root user.
   b. Display the space available in the database dump destination, and verify it is sufficient for the dump file. The following example checks the space in /tmp.

```
# df -h /tmp
Filesystem                      Size  Used Avail Use% Mounted on
/dev/mapper/sta_server-STA_DbVol  200G   53G  243G  27% /
```

3. Stop all STA processes. See "Stop the STA Application" on page 1-4 for details.

```
# STA stop all
```

4. Restart the MySQL server. See "Start the MySQL Server" on page 1-7 for details.

```
# STA start mysql
```

5. Dump the STA database into a single file. Enter the database root user password when prompted. For example:

```
# mysqldump -u root -p --opt --add-drop-database --comments --complete-insert
--dump-date --events --flush-logs --routines --single-transaction --triggers
--databases stadb > /tmp/160115_SavedSTADatabase.sql
Enter password:
#
```

where:

- -u root specifies the STA database root username.
- -p indicates to prompt for the user password.
- --flush-logs indicates to flush the MySQL server log files before starting the dump.
- --databases stadb specifies the name of the database to dump.
- /tmp/160115_SavedSTADatabase.sql specifies the name of the dump file to create. The name must end with .sql.
- For descriptions of the other options, see the *MySQL Reference Manual*.

> **Note:** The --verbose command option is not recommended, as it displays many messages in the terminal window and can significantly slow down the command process for large databases.

6. Verify the dump file has been created, and note the size. You will use the size information in the next procedure. For example:

```
# cd /tmp
# ls -l 160115*sql
-rw-r--r-- 1 root root 3875509 Jan 15 14:05 160115_SavedSTADatabase.sql
```

7. To reduce the dump file size by approximately 50 percent, compress the file. For example:

```
# gzip 160115_SavedSTADatabase.sql
# ls -l 160115*gz
-rw-r--r--   1 root root 365282 Jan 15 14:34 160115_SavedSTADatabase.sql.gz
```

Transfer the Dump File to the Target Server

Use this procedure to transfer the compressed STA database dump file to the target server and then decompress it there. The decompressed database may require 10 to 15 times as much space as the compressed database.

1. On the target server, verify there is sufficient space for the *decompressed* database dump file.
   a. Open a terminal session on the target server and log in as the system root user.
   b. Display the space available in the destination directory, and verify it is sufficient for the size of the *decompressed* dump file, which you displayed in the previous task; see "Dump the STA Database" on page 2-19. The following example displays the space in /tmp.

```
# df -h /tmp
Filesystem                          Size  Used Avail Use% Mounted on
/dev/mapper/newstaserver-lv_root  150G   32G  118G  21% /
```

2. On the STA server, transfer the compressed dump file to the target server.
   a. Open a terminal session on the STA server, and log in as the system root user.
   b. Transfer the file to the target server using a transfer utility such as SCP. For example:

```
# cd /tmp
# scp -p 160115_SavedSTADatabase.sql.gz newstaserver:/tmp
```

   where:
   - -p indicates to preserve timestamp values from the original files.
   - 160115_SavedSTADatabase.sql.gz is the name of the compressed database dump file.
   - newstaserver is the name of the target server.
   - /tmp is the target directory on the server.

3. On the target server, decompress the database dump file.
   a. Open a terminal session on the target server and log in as the system root user.
   b. Decompress the dump file. For example:

```
# cd /tmp
# gunzip 160115_SavedSTADatabase.sql.gz
# ls -l 160115*sql
-rw-r--r-- 1 root   root     3875509 Jan 15 15:05 160115_
SavedSTADatabase.sql
```

Process and Load the STA Database on the Target Server

Use this procedure to load the decompressed dump file into the database on the target server.

> **Note:** This procedure is performed entirely on the target server.

1. Open a terminal session on the target server, and log in as the system root user.
2. Stop all STA processes. See "Stop the STA Application" on page 1-4 for details.

```
# STA stop all
```

3. Restart the MySQL server. See "Start the MySQL Server" on page 1-7 for details.

```
# STA start mysql
```

4. Load the dump file into the STA database. Enter the database root user password when prompted. For example:

```
# mysql -u root -p -e "SET SESSION SQL_LOG_BIN=0; SOURCE /tmp/160115_
SavedSTADatabase.sql;"
Password:
#
```

where:

- -u root specifies the database root username.
- -p indicates to prompt for the user password.
- -e indicates to execute the following MySQL statements and then quit the mysql command. The statements must be enclosed in quotes.
  - SET SESSION SQL_LOG_BIN=0;—Temporarily disables binary logging during the load, speeding up the process.
  - SOURCE /tmp/160115_SavedSTADatabase.sql—Loads the dump file into the database.

There is no command output as the process runs. If the command is successful, you are returned to the command prompt once the process completes.

Note: The --verbose command option is not recommended, as it displays many messages in the terminal window and can significantly slow down the command process for large databases.

Perform Post-transfer Configuration Tasks

Perform the following tasks to configure STA on the target server.

Note: This procedure is performed entirely on the target server.

1. Perform the following tasks to configure library connections in STA so it can begin monitoring library activity. See the *STA User's Guide* for complete instructions.
   - Verify SNMP communication with the library
   - Configure SNMP client settings for STA
   - Configure the SNMP connection to the library
   - Test the library connection
   - Perform a manual data collection for the library
2. Create STA usernames and passwords as needed. See the *STA User's Guide* for instructions.
3. If the STA email server requires authentication, you must specify the email account username and password. See the *STA User's Guide* for instructions.
4. Configure STA services. See "Tasks for Configuring the STA Backup Service" on page 2-3 and "Resource Monitor Tasks" on page 3-2.

staservadm Utility Reference

The staservadm utility is located in the following directory:

/*Oracle_storage_home*/StorageTek_Tape_Analytics/common/bin

where *Oracle_storage_home* is the Oracle storage home location specified during STA installation.

See "Ensure the Correct root User Path" on page 1-3 for instructions on adding the directory to the system root user path.

Using the staservadm Utility

You can use the staservadm utility only if the STA services daemon is running. See "Display the Status of the STA Services Daemon" on page 1-6 to verify.

You can submit as many parameters as you want in each staservadm command line; only the parameters you specify are updated, and the unspecified ones remain at their current value.

Changes to the STA Backup service take effect as soon as one of the following actions occurs:

- The STA Backup service wakes from its current sleep interval and processes the new settings.
- You manually restart the STA services daemon. See "Stop the STA Services Daemon" on page 1-7 and "Start the STA Services Daemon" on page 1-7 for instructions.

staservadm Utility Parameters

Table 2–1 provides detailed information about the staservadm command parameters. A value of "NA" indicates there is no default value.

Table 2–1 staservadm Parameters

Parameter	Name	Description	Default Value
-Q, --query	Query	Display the current STA Backup service settings. See "Display Current STA Backup Settings" on page 2-3 for instructions.	NA
-C, --clear	Clear	Clear all STA Backup service settings and disable the service. See "Disable the STA Backup Service" on page 2-5 for instructions.	NA
-h, --help	Help	Display command usage information	NA
-T, --time	Full backup dump time	Time of day the STA Backup service performs a full database backup, or dump. Format is hh:mm, using 24-hour time. The dump is performed automatically every 24 hours at approximately this time. The actual time is within one incremental backup interval after this time. See "Define the Time of Day for Full Backups" on page 2-5 for instructions.	00:00
-i, --int	Interval between incremental backups	Frequency, in number of seconds, at which the STA Backup service scans the database for changes. If it detects changes, the STA Backup service performs an incremental backup. Valid entries: integers 1 to 86399. See "Define the Interval Between Incremental Backups" on page 2-6 for instructions.	300

Table 2–1 (Cont.) staservadm Parameters

Parameter	Name	Description	Default Value
-U, --dbusr	Database username	Database username the STA Backup service uses to perform the backups. This must be a user on the STA server that is authorized to perform the mysqldump command—for example, the STA database root user or the STA database administrator. See "Specify the Database Username and Password" on page 2-8 for instructions.	blank
-P, --dbpwd	Database password	Password assigned to the database username. See "Specify the Database Username and Password" on page 2-8 for instructions.	blank
-S, --scp | -F, --ftp	File transfer method	File transfer method used to copy the backup files from the STA server to the backup host. You can specify either SCP (recommended) or FTP. See "Define Backup Host Information" on page 2-7 for instructions.	SCP
-s, --server	Backup host name	Server host to which the STA Backup service copies the backup files. You can specify an IPv4 or IPv6 address, or a fully qualified DNS host name. Oracle recommends using an external server for backups. See "Define Backup Host Information" on page 2-7 for instructions.	NA
-d, --dir	Target directory	Target directory on the backup server to which the STA Backup service copies the backup files. This directory must already exist. See "Define Backup Host Information" on page 2-7 for instructions.	NA
-u, --usr	Backup username	System username that writes the database backup files to the target directory. This must be a user on the backup server that has write privileges to the target directory. See "Define Backup Host Information" on page 2-7 for instructions.	NA
-p, --pwd	Backup password	Password assigned to the backup username. See "Define Backup Host Information" on page 2-7 for instructions.	NA

STA Backup Service Files

This section provides detailed information about the backup files created by the STA Backup service.

Full Database Dump Files

A full backup, or *database dump*, is a complete snapshot of the STA database schema and data contents at a point in time. The dump is created once every 24 hours at the time you have defined with the staservadm utility (see "Define the Time of Day for Full

Backups" on page 2-5 for instructions).

Filenames

Each dump file is assigned the following name:

datestamp_timestamp.stafullbackup.sql

where:

- *datestamp* is the current date in yyyymmdd format.
- *timestamp* is the current time, in hhmmss format.

For example, 20160114_180525.stafullback.sql would be a database dump file created on January 14, 2016 at 18:05:25.

Locations

Files for the most recent full backup (full database dump) are located in the /*backup_directory*/local directory on the STA server, where /*backup_directory* is the database backup location specified during STA installation (see the *STA Installation and Configuration Guide* for details). The STA Backup service automatically creates the local subdirectory if it does not exist already.

The STA Backup service automatically removes the previous day's full backup files from this directory when it completes each day's full backup.

- If you are *not* doing remote backups, this is the only backup retained by the STA Backup service. You have only one day's full backup on the local STA server.
- If you are doing remote backups, compressed copies of all full backup files are also located in the remote backup directory defined with the staservadm utility (see Define Backup Host Information for instructions).

  The STA Backup service *never* deletes files from the external backup server, enabling you to maintain as many days worth of backups as your site's policies require. Also, it is your responsibility to manage the files and the space on the external server. You can use your site's preferred backup and archiving policies and tools to manage the files.

Configuration Directories

When the STA Backup service does a full database dump, it also creates compressed copies of the configuration directories for the STA services and WebLogic server, including the STA Resource Monitor and STA Backup service administration logs. These are recursive backups of all the files and directories in their respective configuration directories.

Filenames

The filenames are as follows:

STA services configuration directory—*datestamp_timestamp*.conf.zip
WebLogic configuration directory—*datestamp_timestamp*.fmwconfig.zip

where:

- *datestamp* is the current date in yyyymmdd format.
- *timestamp* is the current time, in hhmmss format.

For example, 20160114_180525.conf.zip and 20160114_180525.fmwconfig.zip would be compressed WebLogic and STA services configuration directories, respectively, created on January 14, 2016 at 18:05:25.

Locations

Compressed copies of the STA services and WebLogic configuration directories are located in the same directory as the full database dump files, and the STA Backup service manages these files in the same manner as the database dump files.

Incremental Backup Files (Binary Logs)

An incremental backup, or *binary log*, contains records of all transactions that change the database. As the name implies, binary logs are saved in binary format; see "View Binary Log Contents" on page 2-11 for information on viewing their contents.

To do a full database restore, you load the most recent full dump file and then apply, in sequential order, all the incremental backups that were generated after the dump. This process enables you to restore the database to its state up to the last transaction recorded in the binary logs.

Filenames

Each binary log is assigned the following file name:

stadb-bin.*nnnnnn*

where:

- *nnnnnn* is a unique number indicating the sequence in which the incremental backups were created.

For example, stadb-bin.000034, stadb-bin.000035, and stadb-bin.000036 could be three successive incremental backups created by the STA Backup service.

Locations

All incremental backups created since the last full backup are located in the /var/log/tbi/db directory on the STA server. The number of binary log files in the directory depends on the incremental backup interval you have specified (see Define the Interval Between Incremental Backups for instructions).

The STA Backup service removes all incremental backups from the /var/log/tbi/db directory when it completes a daily full backup. Therefore this directory only contains incremental backup files created since the last full backup. You should never delete binary log files from this directory yourself.

- If you are *not* doing remote backups, the incremental backups are deleted from this directory and not retained anywhere.
- If you are doing remote backups, the incremental backups are transferred to the remote backup directory every 24 hours, when the compressed full database dump files are moved (see STA Backup Service Process for details). You can keep as many days worth of incremental backups on the backup server as your site's policies require.

3

Monitoring STA Server Resources

About the STA Resource Monitor Service

The STA Resource Monitor (Resmon) service allows you to easily monitor usage levels of key resources on the STA server. It automatically produces a daily resource usage report and, optionally, a resource depletion report that periodically alerts you when resources have exceeded user-defined thresholds, or *high-water marks*.

The Resmon service is disabled by default when STA is installed, and you must configure the service to enable it. You configure the Resmon service with the staresmonadm utility. See "staresmonadm Utility Reference" on page 3-8 for command usage details. The Resmon service is managed by the STA services daemon; see "STA Services Daemon" on page 1-2 for details.

ResMon Service Process

Once enabled, the ResMon service runs in the background and performs the following activities:

- Periodically scans the following resources on the STA server.
  - Database tablespace
  - Database data
  - Database backup
  - Log volume (by default, /var/log/tbi)
  - Root volume (/)
  - Temp volume (by default, /tmp)
  - System memory
- Records current values for these resources in the Resource Report. Optionally, Resmon emails the report to designated email recipients once a day at a designated time. S1ee "Resmon Resource Report" on page 3-11 for details.
- Optionally sends a Resource Depletion Alert Report to designated email recipients whenever it detects that a monitored resource has exceeded a user-defined

high-water mark (HWM). See "Resource Depletion Alert Report" on page 3-14 for details.

Sample Resmon Scenario

The following scenario describes the Resmon service process.

Database tablespace usage on the STA server is currently 85 percent. The Resmon service is enabled with the following parameter values:

- Send Reports = 08:41
- Sleep Interval = 1800
- Alert Nagging = ON
- DB Tablespace high-water mark (HWM) = 80
- Email 'To:' = charlie@mycompany.com

1. Every 1800 seconds (30 minutes), Resmon scans the monitored resources on the STA server and adds a record of the current values to the end of the Resource Report file. See "Resource Report CSV File" on page 3-13 for details.
2. During the scan, Resmon detects that database tablespace has exceeded the defined high-water mark and performs the following actions:
   - Records an alert in the Resource Report file.
   - Because alert nagging is enabled, immediately sends a Resource Depletion Alert Report to the designated email recipient (Email 'To:'). Resmon continues to send the report every 1800 seconds until the tablespace usage is brought below the defined high-water mark. See "Resource Depletion Alert Report" on page 3-14 for a sample.
3. Every day at 08:41 (Send Reports time), Resmon sends a copy of the Resource Report to the designated email recipient. See "Resmon Resource Report" on page 3-11 for a sample.
4. At the end of every month, you move the Resource Report file to a separate location. You import the month's data into an Excel spreadsheet and use it to graph resource depletion trends on the STA server.

Resource Monitor Tasks

Note: The following tasks use the staresmonadm utility, which requires the STA Services daemon. See "Display the Status of the STA Services Daemon" on page 1-6 to verify that the daemon is running.

To use the utility, the See "Using the staresmonadm Utility" on page 3-8 for usage details.

Display Current Resmon Settings

Use this procedure to display the current settings for the Resmon service.

1. Open a terminal session on the STA server, and log in as the system root user.
2. Display the current Resmon settings.

   ```
   # staresmonadm -Q
   ```

   Example 3–1and Example 3–2 are sample outputs.

Example 3–1 Resmon not configured

In this example the Resmon service is disabled and therefore not performing scans. The values displayed are the parameter defaults. High-water mark settings of -1% indicate the parameters are disabled.

```
# staresmonadm -Q
Contacting daemon...connected.
Querying Preferences.
 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]
```

Example 3–2 Resmon configured

In this example, the Resmon service is enabled and configured.

```
# staresmonadm -Q
Contacting daemon...connected.
Querying Preferences.
 Current STA Resource Monitor Service Settings:
   Configured                        [yes]
   Send Reports                   -T [23:05]
   Sleep Interval                 -i [3600 sec]
   Alert Nagging                  -n [off]
   DB Username                    -U [stadba]
   DB Password                    -P [********]
   DB Tablespace hwm              -t [80%]
```

```
DB Backup hwm   (/dbbackup)    -b [70%]
DB Data hwm     (/dbdata)      -d [75%]
Log Volume hwm  (/var/log/tbi) -l [75%]
Root Volume hwm (/)            -z [75%]
Tmp Volume hwm  (/tmp)         -x [75%]
System Memory hwm              -m [80%]
Email 'From:'                  -f [STAResmon@staserver.mycompany.com]
Email 'To:'                    -r [charlie@mycompany.com:lucy@mycompany.com]
Email 'Subject:'               -s [STA Resource Monitor Report <staserver>]
Output File                    -o [/var/log/tbi/db/staresmon.csv]
```

Enable the Resmon Service

When STA is installed, the Resmon service is disabled by default. Use this procedure to enable the Resmon service. Once enabled, the service scans the monitored resources on the STA server according to the defined settings.

To enable the service, you must define at least the following settings:

- All high-water marks, except system memory
- Email 'To:'
- Send Time
- Sleep Interval
- DB Username and Password

You can optionally define other settings as well, but they are not required to enable the service.

1. Open a terminal session on the STA server, and log in as the system root user.
2. To enable the service, define the required parameters in one or more commands.

```
# staresmonadm -t 80 -b 70 -d 75 -l 75 -z 75 -x 75 -m 80
-r charlie@mycompany.com -T 23:05 -i 3600 -U stadba -P
Enter database password:
Contacting daemon...connected.
Setting DB Tablespace HWM..... 80
Setting DB Disk Volume HWM.... 75
Setting Logging Volume HWM.... 75
Setting Backup Volume HWM..... 70
Setting Root Volume HWM....... 75
Setting Temp Volume HWM....... 75
Setting System Memory HWM..... 80
Setting 'To:' addresses....... charlie.mycompany.com
Setting Send Time.............. 23:05
Setting Sleep Interval........ 3600
Setting DB Username........... stadba
Setting DB Password........... ********
Done.
 Current STA Resource Monitor Service Settings:
   Configured                      [yes]
   Send Reports                 -T [23:05]
   Sleep Interval               -i [3600 sec]
   Alert Nagging                -n [off]
   DB Username                  -U [stadba]
   DB Password                  -P [********]
   DB Tablespace hwm            -t [80%]
   DB Backup hwm   (/dbbackup)    -b [70%]
   DB Data hwm     (/dbdata)      -d [75%]
```

```
  Log Volume hwm  (/var/log/tbi) -l [75%]
  Root Volume hwm (/)            -z [75%]
  Tmp Volume hwm  (/tmp)         -x [75%]
  System Memory hwm              -m [80%]
  Email 'From:'                  -f [StaResMon@localhost]
  Email 'To:'                    -r [charlie@mycompany.com]
  Email 'Subject:'               -s [STA Resource Monitor Report]
  Output File                    -o [/var/log/tbi/db/staresmon.csv]
=====================================================
```

Resmon will run its first scan at the time you have specified; you do not have to stop and restart the STA services daemon.

Disable the Resmon Service

Use this procedure to clear all Resmon settings, which both disables the service and resets all parameter values to their defaults. When disabled, the service does not perform scans, send alerts, or produce reports.

1. Open a terminal session on the STA server, and log in as the system root user.
2. Clear all Resmon settings.

```
# 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]
```

The service is disabled immediately; you do not have to stop and restart the STA services daemon.

Define the Interval Between Scans

Use this procedure to define the number of seconds between Resmon scans.

1. Open a terminal session on the STA server, and log in as the system root user.
2. Define the interval between scans, in seconds. In this example, the interval is set to 1800 seconds, or 30 minutes.

```
# staresmonadm -i 1800
Setting Sleep Interval........ 1800
Done.
```

3. If you want the new interval to take effect immediately, you must stop and restart the STA services daemon. See "Stop the STA Services Daemon" on page 1-7 and "Start the STA Services Daemon" on page 1-7 for instructions.

Define High-water Marks for Monitored Resources

Use this procedure to set high-water marks for any of the monitored resources. You can set one or more high-water marks in a single command.

High-water marks are always entered as a percentage of the total allocated space.

Note: Oracle recommends that usage for any partition never exceed 80 percent.

1. Open a terminal session on the STA server, and log in as the system root user.
2. Specify the high-water marks you want to change. All unspecified high-water marks remain unchanged.

   In this example, the root and temp space high-water marks are set to 75 percent and 80 percent respectively.

```
# staresmonadm -z 75 -x 80
Contacting daemon...connected.
Setting Root Volume HWM....... 75
Setting Temp Volume HWM....... 80
Done.
```

3. If you want the new values to take effect immediately, you must stop and restart the STA services daemon. See "Stop the STA Services Daemon" on page 1-7 and "Start the STA Services Daemon" on page 1-7 for instructions.

Enable or Disable Alert Nagging

Use this procedure to enable or disable alert nagging.

1. Open a terminal session on the STA server, and log in as the system root user.
2. Change the alert nagging setting; all unspecified Resmon settings remain unchanged.

   This example enables alert nagging—you can specify yes, on, 1, or true.

```
# staresmonadm -n yes
Contacting daemon...connected.
Setting Alert Nag Mode........ YES
Done.
```

   This example disables alert nagging—you can specify no, off, 0, or false.

```
# staresmonadm -n no
Contacting daemon...connected.
Setting Alert Nag Mode........ NO
Done.
```

3. If you want the new setting to take effect immediately, you must stop and restart the STA services daemon. See "Stop the STA Services Daemon" on page 1-7 and "Start the STA Services Daemon" on page 1-7 for instructions.

Specify the Database Username and Password

Use this procedure to specify the database username that the Resmon service uses to perform queries against the STA database metadata. You must specify a user that has superuser access to the STA database, such as the STA database root user or the database administrator.

1. Open a terminal session on the STA server, and log in as the system root user.
2. Specify the STA database username Resmon must use, and the user password. You can use either of the following methods to specify the password:
   - Enter -P and the password in clear text on the command line.
   - Enter -P with no password on the command line. When you submit the command, the utility prompts for the password, which is hidden when you type it.

   In this example, the utility prompts for the password.

```
# staresmonadm -U stadba -P
Enter database password:
Contacting daemon...connected.
Setting DB Username.......... stadba
Setting DB Password.......... ********
Done.
```

3. If you want the new settings to take effect immediately, you must stop and restart the STA services daemon. See "Stop the STA Services Daemon" on page 1-7 and "Start the STA Services Daemon" on page 1-7 for instructions.

Define Resmon email Settings

Use this procedure to define email addresses to which Resmon sends the daily Resource Report and periodic Resource Depletion Report. You can also define an email sender and subject line to help recipients identify and organize emails from the Resmon service.

> **Note:** The email server and sender address used by the Resmon service may be different than those used by the STA application. See the *STA User's Guide* for details about STA application emails.

1. Open a terminal session on the STA server, and log in as the system root user.
2. Define email information.
   - To specify multiple recipients, separate the email addresses by a colon (:).
   - If the subject text includes spaces, enclose the text line in double-quotes (") or single-quotes (').

   This example defines two email recipients, the email sender, and a subject line for emails sent by the Resmon service.

```
# staresmonadm -r charlie@mycompany.com:lucy@mycompany.com -f
STAResmon@staserver.mycompany.com -s "STA Resource Monitor Report for
staserver"
Contacting daemon...connected.
Setting 'From:' address....... StaResmMon@mycompany.com
Setting 'To:' addresses....... charlie@mycompany.com:lucy@mycompany.com
Setting 'Subject:' line....... STA Resource Monitor Report for staserver
```

```
Done.
```

3. If you want the new settings to take effect immediately, you must stop and restart the STA services daemon. See "Stop the STA Services Daemon" on page 1-7 and "Start the STA Services Daemon" on page 1-7 for instructions.

Define Resource Report Settings

Use this procedure to change the time of day when Resmon sends the Resource Report, and the filename and location of the report file. If you specify a new filename, and the file does not already exist, the Resmon service creates it with the next scan.

1. Open a terminal session on the STA server, and log in as the system root user.
2. Define report information.
   - Use 24-hour notation to specify the time of day.
   - The file location must be an absolute, not relative, path. The database user must have read/write privileges to the directory.
   - The filename extension must be .csv.

   This example specifies a time of day and a new filename.

```
# staresmonadm -T 23:59 -o /var/log/tbi/db/ResmonReport.csv
Contacting daemon...connected.
Setting Send Time.............. 23:59
Setting Output Filename....... /var/log/tbi/db/ResmonReport.csv
Done.
```

3. If you want the new settings to take effect immediately, you must stop and restart the STA services daemon. See "Stop the STA Services Daemon" on page 1-7 and "Start the STA Services Daemon" on page 1-7 for instructions.

staresmonadm Utility Reference

The staresmonadm utility is located in the following directory:

/*Oracle_storage_home*/StorageTek_Tape_Analytics/common/bin

where *Oracle_storage_home* is the Oracle storage home location specified during STA installation.

See "Ensure the Correct root User Path" on page 1-3 for instructions on adding the directory to the system root user path.

Using the staresmonadm Utility

You can use the staresmonadm utility only if the STA services daemon is running. See "Display the Status of the STA Services Daemon" on page 1-6 to verify that the daemon is running.

You can submit as many parameters as you want in each staresmonadm command line; only the parameters you specify are updated, and the unspecified ones remain at their current value.

Resmon changes take effect as soon as one of the following actions occurs:

- The Resmon service wakes from its current sleep interval and processes the new settings.

- You manually restart the STA services daemon. See "Stop the STA Services Daemon" on page 1-7 and "Start the STA Services Daemon" on page 1-7 for instructions.

staresmonadm Utility Parameters

Table 3–1 provides detailed information about the staresmonadm command parameters. A value of "-1" indicates the parameter is not configured. A value of "NA" indicates there is no default value.

Table 3–1 staresmonadm Parameters

Parameter	Name	Description	Default Value
-Q, --query	Query	Display the current Resmon settings.	NA
-C, --clear	Clear	Clear all Resmon settings and disable the service.	NA
-v, --verbose	Verbose	Enables verbose mode, which displays detailed progress information for the command.	NA
-h, --help	Help	Displays complete syntax information for the command.	NA
-T, --time	Daily report time	Time of day Resmon sends the Resource Report. Format is hh:mm, using 24-hour time. The report is sent automatically every 24 hours at approximately this time. The actual time is immediately after the first server scan performed after this time. See "Define Resource Report Settings" on page 3-8 for instructions.	00:00
-i, --interval	Interval between scans	Number of seconds Resmon waits between scans. Valid entries: integers greater than 0. See "Define the Interval Between Scans" on page 3-5 for instructions.	300
-n, --nag	Alert nagging	Indicates whether Resmon sends alerts if it finds that any high-water marks have been reached. Valid entries: on|off, yes|no, true|false, 1|0. See "Enable or Disable Alert Nagging" on page 3-6 for instructions. When enabled, alert nagging causes Resmon to send alert reports to the designated email recipients whenever it performs a periodic scan and detects a resource has exceeded its high-water mark. See "Resource Depletion Alert Report" on page 3-14 for details. Alert nagging is disabled by default, in which case, Resmon does not send alert reports. Alerts are included in the Resource Report, which is sent only once a day, at the designated "Send reports" time. See "Resmon Resource Report" on page 3-11 for details.	off

Table 3–1 (Cont.) staresmonadm Parameters

Parameter	Name	Description	Default Value
-U, --dbusr	Database username	Database username that the Resmon service uses to perform queries against the information_schema tables and the MySQL server internal system global variables. This must be a user with superuser access to the STA database, such as the STA database root user or the STA database administrator. See "Specify the Database Username and Password" on page 3-7 for instructions.	blank
-P, --dbpwd	Database password	Password assigned to the database username. See "Specify the Database Username and Password" on page 3-7 for instructions.	blank
-t, --tblsphwm	Database tablespace HWM	High-water mark for the database tablespace, entered as a percentage of the total allocated. Valid entries: integers 0–100 See "Define High-water Marks for Monitored Resources" on page 3-6 for instructions.	-1
-b, --backvolhwm	Local backup HWM	High-water mark for the STA database local backups volume (for example, /dbbackup), entered as a percentage of the total allocated. Valid entries: integers 0 –100 See "Define High-water Marks for Monitored Resources" on page 3-6 for instructions.	-1
-d, --dbvolhwm	Database disk volume HWM	High-water mark for the STA database volume (for example, /dbdata/mysql), entered as a percentage of the total allocated. Valid entries: integers 0 –100 See "Define High-water Marks for Monitored Resources" on page 3-6 for instructions.	-1
-l, --logvolhwm	Logging disk volume HWM	High-water mark for the STA database logs volume (default is /var/log/tbi), entered as a percentage of the total allocated. Valid entries: integers 0 –100 See "Define High-water Marks for Monitored Resources" on page 3-6 for instructions.	-1
-z, --rootvolhwm	Root volume HWM	High-water mark for the root volume (/), entered as a percentage of the total allocated. Valid entries: integers 0 –100 See "Define High-water Marks for Monitored Resources" on page 3-6 for instructions.	-1
-x, --tmpvolhwm	Tmp volume HWM	High-water mark for the temporary directory volume (default is /tmp), entered as a percentage of the total allocated. Valid entries: integers 0 –100 See "Define High-water Marks for Monitored Resources" on page 3-6 for instructions.	-1
-m, --memhwm	Physical memory (RAM) HWM	High-water mark for the total system memory (except virtual memory), entered as a percentage of the total allocated. Valid entries: integers 0 –100 See "Define High-water Marks for Monitored Resources" on page 3-6 for instructions.	-1

Table 3–1 (Cont.) staresmonadm Parameters

Parameter	Name	Description	Default Value
-f, --from	Email from	Name or email address that appears in the "From" field of emails sent by the Resmon service. See "Define Resmon email Settings" on page 3-7 for instructions.	StaResMon@localhost
-r, --recips	Email recipients	email addresses to which Resmon sends the daily Resource Report and periodic Resource Depletion Alert Report. Entered as a colon-delimited list. See "Define Resmon email Settings" on page 3-7 for instructions.	blank
-s, --subject	Email subject	Text string that appears in the "Subject" field of the standard daily report email, up to 128 characters. Enclose the text string in single-quotes (') or double-quotes (") if it contains spaces. A time stamp in yyyy-mm-dd hh:mm:ss form is appended to your entry when the email is sent. See "Define Resmon email Settings" on page 3-7 for instructions.	STA Resource Monitor Report
-o, --outfile	Output data file	Absolute path of the Resource Report data file. The file name must end in .csv. See "Resource Report CSV File" on page 3-13 for details about the default filename and location. The database user must have privileges to the directory. See "Define Resource Report Settings" on page 3-8 for instructions.	/var/log/tbi/db/staresmon.csv

STA Resource Monitor Reports

The Resmon service produces the following reports:

- "Resmon Resource Report" on page 3-11
- "Resource Depletion Alert Report" on page 3-14

Resmon Resource Report

The Resource Report is sent to all Resmon email recipients once a day, at approximately the "Send Reports" time; the exact time is upon completion of the scan that occurs directly after the "Send Reports" time.

The report provides data for all monitored resources (see "About the STA Resource Monitor Service" on page 3-1 for details). It also includes alerts for any resources that have exceeded their defined high-water marks. Example 3–3 is a sample email containing the report.

Note: Reported values rely on mount points. If multiple monitored resources share a mount point, their reported values will be identical.

Example 3–3 Sample Resource Report With Alerts email

```
From: StaResMon@mystaserver.mycompany.com
Subject: STA Resource Monitor Report [2015-12-21 23:13:33]
To: charlie@mycompany.com
```

```
STA RESOURCE MONITOR STANDARD REPORT
System: mystaserver
Scanned: 2015-12-21 23:13:33

Database Tablespace
  HWM            : 80.00%
  Used           : 1.38%
  MB Used        : 1046
  MB Free        : 74730
  MB Total       : 75776
  Location       : /dbdata/mysql

Database Volume
  HWM            : 75.00%
  Used           : 80.33% (!)
  MB Used        : 80967
  MB Free        : 19827
  MB Total       : 100794
  Directory      : /dbdata

Logging Volume
  HWM            : 75.00%
  Used           : 79.55% (!)
  MB Used        : 20045
  MB Free        : 5154
  MB Total       : 25199
  Directory      : /var/log/tbi

...

************************************************************
*                     A L E R T S                          *
************************************************************
==================================================
ALERT - Low Database Volume Disk Space
==================================================
  Database disk volume has exceeded threshold value!
  HWM             [75.00%]
  Used            [80.33%] (!)
  MB Used         [80967]
  Recommendations:
  1) Purge old backup files.
  2) Relocate database directory to a larger volume.

==================================================
ALERT - Low Logging Volume Disk Space
==================================================
  Logging volume disk usage has exceeded threshold value!
  HWM             [75.00%]
  Used            [79.55%] (!)
  MB Used         [20045]
  Recommendations:
  1) Purge STA log files.
  2) Purge MySQL binary logs.
  3) Purge MySQL error logs.
  4) Relocate logging directory to a larger volume.
```

Resource Report CSV File

The daily Resource Report is generated from the Resource Report data file. By default, the file has the following location and filename, which you can optionally change. See "Define Resource Report Settings" on page 3-8.

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

The Resource Report file is a comma-separated (CSV) file that provides a continuous record of every Resmon scan performed on the STA server since the file was created. Each time Resmon completes a scan, it adds a record containing the scanned values to the end of the file.

Because the Resource Report file is in CSV format, you can import it into spreadsheet and database management applications, such as Excel and MySQL, and create reports and graphs of the values. For example, you could use the Resource Report file data to report resource depletion trends for the STA server over time.

The Resource Report file continues to grow with each scan. Managing the file, including backing it up and managing the file size, is the customer's responsibility. It is not purged, rolled, nor backed up by the STA application nor the STA backup service.

Each row in the file represents one scan of the server and includes the columns listed in Table 3–2. Example 3–4 is a sample of the file header row and one complete scan record.

Table 3–2 Resource Report Record 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, in MB	123
3	TS_MB_USED	Total database tablespace used, in MB	123
4	TS_MB_AVAIL	Database tablespace remaining, in MB	123
5	TS_PCT_USED	Database tablespace used, as a percentage of the maximum	12.34%
6	TS_PCT_HWM	Database tablespace high-water mark, as a percentage of the maximum; this is user-defined.	12.34%
7	DBVOL_MB_MAX	Total allocated space on the volume containing the database, in MB	123
8	DBVOL_MB_USED	Total database disk volume space used, in MB	123
9	DBVOL_MB_AVAIL	Database volume disk space remaining, in MB	123
10	DBVOL_PCT_USED	Database volume disk space used, as a percentage of the maximum	12.34%
11	DBVOL_PCT_HWM	Database volume high-water mark, as a percentage of the maximum; this is user-defined.	12.34%
12	LOGVOL_MB_MAX	Total allocated space on the volume containing the logs, in MB	123
13	LOGVOL_MB_USED	Total logging disk volume space used, in MB	123
14	LOGVOL_MB_AVAIL	Logging volume disk space remaining, in MB	123
15	LOGVOL_PCT_USED	Logging volume disk space used, as a percentage of the maximum	12.34%

Table 3–2 (Cont.) Resource Report Record Format

Col	Header	Description	Format
16	LOGVOL_PCT_HWM	Logging volume high-water mark, as a percentage of the maximum; this is user-defined	12.34%
17	MEM_MB_MAX	Maximum installed physical RAM, in MB	123
18	MEM_MB_USED	Total physical memory used, in MB	123
19	MEM_MB_AVAIL	Physical memory space remaining, in MB	123
20	MEM_PCT_USED	Physical memory space used, as a percentage of the maximum	12.34%
21	MEM_PCT_HWM	Physical memory high-water mark as a percentage of the maximum; this is user-defined.	12.34%

Example 3–4 Sample CSV File Record

```
TIMESTAMP,TS_MB_MAX,TS_MB_USED,TS_MB_AVAIL,TS_PCT_USED,TS_PCT_HWM,DBVOL_MB_MAX,DBVOL_MB_USED,DBVOL_
MB_AVAIL,DBVOL_PCT_USED,DBVOL_PCT_HWM,LOGVOL_MB_MAX,LOGVOL_MB_USED,LOGVOL_MB_AVAIL,LOGVOL_PCT_
USED,LOGVOL_PCT_HWM,BCKVOL_MB_MAX,BCKVOL_MB_USED,BCKVOL_MB_AVAIL,BCKVOL_PCT_USED,BCKVOL_PCT_
HWM,RTVOL_MB_MAX,RTVOL_MB_USED,RTVOL_MB_AVAIL,RTVOL_PCT_USED,RTVOL_PCT_HWM,TMPVOL_MB_MAX,TMPVOL_MB_
USED,TMPVOL_MB_AVAIL,TMPVOL_PCT_USED,TMPVOL_PCT_HWM,MEM_MB_MAX,MEM_MB_USED,MEM_MB_AVAIL,MEM_PCT_
USED,MEM_PCT_HW
"2015-12-23 12:54:00",433152,18596,414556,4.29%,80.00%,570770,51653,519118,9.05%,75.00%,209317,1039
36,105382,49.65%,75.00%,779717,230478,549239,29.56%,70.00%,209317,103936,105382,49.65%,75.00%,20931
7,103936,105382,49.65%,75.00%,32167,27859,4309,86.61%,80.00%
```

Resource Depletion Alert Report

If alert nagging is enabled, the Resmon service sends a Resource Depletion Alert Report whenever it detects that any monitored resources have exceeded their defined high-water marks. The report includes recommendations for resolving the issues. Example 3–5 is a sample email containing the report.

If alert nagging is disabled, Resmon does not generate a Resource Depletion Alert Report, and alerts are shown only in the daily Resource Report.

See "Enable or Disable Alert Nagging" on page 3-6 for related instructions.

Example 3–5 Example Resource Depletion Report email

In this example, two high-water marks have been exceeded.

```
From: StaResMon@mystaserver.mycompany.com
Subject: ALERT::STA Resource Depletion [2015-12-22 09:13:36]
To: charlie@mycompany.com

STA RESOURCE DEPLETION REPORT
System: mystaserver
Scanned: 2015-12-22 09:13:36

*********************************************************
*                    A L E R T S                        *
*********************************************************
=================================================
ALERT - Low Database Volume Disk Space
=================================================
  Database disk volume has exceeded threshold value!
  HWM             [75.00%]
  Used            [80.33%] (!)
```

```
  MB Used         [80967]
  MB Free         [19827]
  MB Total        [100794]
  Directory       [/dbdata]
  Recommendations:
  1) Purge old backup files.
  2) Relocate database directory to a larger volume.

================================================
ALERT - Low Logging Volume Disk Space
================================================
  Logging volume disk usage has exceeded threshold value!
  HWM             [75.00%]
  Used            [79.55%] (!)
  MB Used         [20045]
  MB Free         [5154]
  MB Total        [25199]
  Location        [/var/log/tbi]
  Recommendations:
  1) Purge STA log files.
  2) Purge MySQL binary logs.
  3) Purge MySQL error logs.
  4) Relocate logging directory to a larger volume.
```

4

Administering Passwords

This chapter describes changing various STA database and service passwords. To change an STA username password, see the *STA User's Guide*.

> **Caution:** Do not change the WebLogic Administration console login password. If you change this password, you will need to reinstall STA.

This chapter includes the following sections:

Username and Password Requirements

Username requirements are as follows:

- Must be 1–16 characters in length
- All usernames must be unique

Password requirements are as follows:

- Must be 8–32 characters in length
- Must include at least one uppercase letter and one number
- Must not include spaces or tabs
- Must not include any of the following special characters:

```
% & ' ( ) < > ? { } * \ ' " ; , + = #
```

Change an STA Database Account Password

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

> **Note:** The STA Database Root Account password should be changed by the MySQL database administrator only.

1. Begin as follows:

- 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.

---

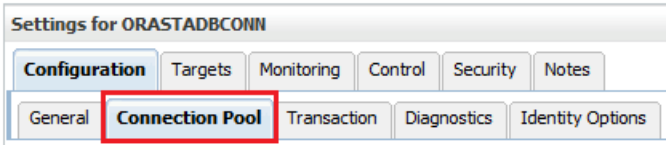
2. Go to the WebLogic console login screen using the HTTP (default is 7001) or HTTPS (default is 7002) port number you selected during STA installation. For example:

   https://*yourHostName***:***PortNumber***/console**

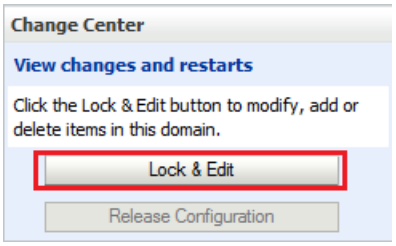
3. Log in using the WebLogic Administration console username and password.
4. From the **Domain Structure** menu, select **Services**, then select **Data Sources**.

5. In the Name column of the Data Source table, select **ORASTADBCONN** (select the name itself, not the check box).

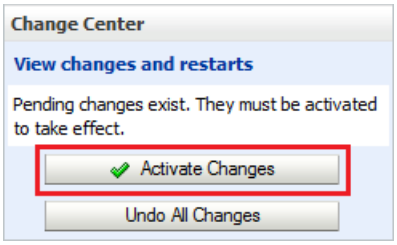
6. Click the **Connection Pool** tab.



7. In the Change Center section, click **Lock & Edit**.



8. Enter and confirm the new password, and then click **Save**.
9. In the Change Center section, click **Activate Changes**.



10. Log out of the WebLogic Administration Console.
11. As root on the STA server, restart the STA application. See "Stop the STA Application" on page 1-4 and "Start the STA Application" on page 1-5 for instructions.

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

12. 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. For example:

       https://*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.

Change an STA MySQL Account Password

Use this procedure to change the password for the STA Database Root Account, Reports Account, or DBA Account.

1. Log in to the MySQL client as the Linux root user.

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

2. Type the following command:

```
mysql> use mysql;
```

3. Retrieve the list of STA database usernames.

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

4. Take note of the account username for which to change the password. You will use this username in the next step.
5. 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;
```

6. Exit from the MySQL client.

```
mysql> quit;
#
```

7. 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. Enter the new root user password when prompted.

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

  ```
  # 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
  ```

8. Proceed as follows:

- If you changed the STA Database Root Account or Reports Account, you are finished.
- If you changed the STA Database DBA Account password, see "Change the STA Backup Service and Resource Monitor Passwords" on page 4-6 to synchronize the password for these services.

- If you changed the STA Database Application Account password, proceed to the next step.

9. As root on the STA server, restart the STA application. See "Stop the STA Application" on page 1-4 and "Start the STA Application" on page 1-5 for instructions.

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

10. 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. For example:

    https://*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.

Change the STA Backup Service and Resource Monitor Passwords

Use this procedure to update the STA Backup and Resource Monitor services with the new password for the STA database root user or database administrator. You must use this procedure whenever you use the procedure "Change an STA Database Account Password" on page 4-1.

1. Open a terminal session on the STA server, and log in as the system root user.
2. Verify that the STA services daemon is running. See "Display the Status of the STA Services Daemon" on page 1-6 for instructions.
3. Update the STA Backup service with the new password. See "Specify the Database Username and Password" on page 2-8 for instructions.
4. Update the STA Resource Monitor service with the new password. See "Specify the Database Username and Password" on page 3-7 for instructions.

A

Preventing Denial-of-Service Attacks

This appendix provides a sample procedure for preventing Denial-of-Service (DoS) attacks on STA. It provides instructions for using the sample script in Example A–1 to define input rules for the IPTables utility to block hosts based on any of the following criteria:

- Ethernet interface
- Ethernet protocol
- Port number
- Maximum number of requests within a specified time period

> **Note:** This procedure is optional and is provided as information only. Site security is the customer's responsibility.

Define Rules for Preventing DoS Attacks

> **Note:** Before using this procedure, configure and verify the library connections on STA. See the *STA User's Guide* for details.

Use this procedure to configure input rules for the IPTables utility to watch for and prevent attacks on STA.

For STA, Oracle recommends attaching rules to UDP port 162 (the port on which SNMP traps are received) and on the ports you have defined for the STA managed servers. See the *STA Installation and Configuration Guide* for details about the ports.

1. Log in to the STA server as the system root user.
2. Copy the contents of Example A–1 into a text editor.
3. Modify the following variables as appropriate for your environment.
   - INTERFACE—Ethernet interface to watch for attacks (Eth0, for example)
   - PROTO—Ethernet protocol to watch for attacks (TCP or UDP)
   - PORT—Port number to watch for attacks
   - HITS and TIME—Specify reasonable values for the number of requests (HITS) within a given time period, in seconds (TIME). Any host that exceeds the number of requests within the specified time period is blocked from further connections for the remainder of the period.

4. Save the script and execute it. The new rules are added to the IPTables utility and take effect immediately.
5. Verify that STA is still successfully monitoring your libraries. See the *STA User's Guide* for details.

Example A–1 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
```

Index