# StorageTek Tape Analytics

Administration Guide

Version 2.1.0

**E58067-01**

January 2015

ORACLE

StorageTek Tape Analytics Administration Guide, Version 2.1.0

E58067-01



Primary Author: Nancy Stevens

Contributing Author:

# Contents

# 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 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 2.1.0.

## STA 2.1.0 January 2015

See the indicated manuals for details about new and enhanced features.

**Described in the *STA Requirements Guide***

- New library and drive recommended firmware levels to support STA 2.1.0.
- Support for TTI 5.50 protocol for Oracle's StorageTek T10000C and T10000D drives.
- Updated recommended library and drive requirements to support STA 2.1.0.
- Updated recommended STA server configuration.

**Described in the *STA Installation and Configuration Guide***

- New STA 2.1.0 installer and deinstaller, which provide the following new features:
  - Oracle install user and group—Linux user and group used exclusively for installing and upgrading Oracle products on the STA server.
  - User-defined Oracle storage home location—the STA application and associated Oracle software can be installed in any file system that contains sufficient space.
  - User-defined database and local backup locations.
  - Oracle central inventory location—directory for tracking information about Oracle products installed on the STA server.
  - STA installer and deinstaller silent mode—allows you to bypass the graphical user interface and supply the installation options in an XML properties file.
  - New detailed STA installer and deinstaller logs.
  - Context-sensitive help for all STA graphical installer and deinstaller screens.
- Additional Linux RPM package requirement—the xorg-x11-utils package must be installed to run the STA graphical installer.
- Default ports for the WebLogic administration console have been changed to 7019 (HTTP) and 7020 (HTTPS). If you have been using the previous default assignments, you may want to change them to the new ones.
- New password requirements for STA and MySQL usernames.

- New process to upgrade STA 1.0.x and STA 2.0.x databases to STA 2.1.0.

**Described in the *STA Quick Start Guide***

- No major changes

**Described in the *STA User's Guide***

- Minor updates to the following templates to provide additional information and improve usability:
  - STA-Complex-Configuration
  - STA-Complex-Utilization
  - STA-Lib-Configuration
  - STA-Drive-MV
  - STA-Media-All
  - STA-Media-MV-Calibration
  - Media Validation Overview screen, STA-Default template
- Documentation changes—the following chapters have been relocated from the *STA Administration Guide*. The *STA User's Guide* now describes all features and activities that can be performed from the STA user interface.
  - STA Usernames and Email
  - STA Service Logs
  - Managing SNMP Connections in STA

**Described in the *STA Screen Basics Guide***

- No major changes

**Described in the *STA Data Reference Guide***

- Attributes on some screens have been reorganized to improve usability.
- "Last Messages" attributes are available on the respective screens for CAPs, drives, elevators, libraries, PTPs, and robots.

**Described in the *STA Administration Guide***

- Documentation changes—the following chapters have been moved to the *STA User's Guide*:
  - Users and Email
  - Logging
  - SNMP Management

# 4

# Server Administration

The STA command is used to administer and verify the status of the various STA components. This chapter includes the following sections:



## STA Command Overview

The STA command variants are split into the following categories:

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

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

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

## Managed Servers

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

- staUi—STA user interface
- staEngine—Basic STA internal functions
- staAdapter—SNMP communication

You can manage the servers individually. See "Individual Service Administration Commands" on page 3.

# Memory Usage Requirements

Table 1–1 shows memory usage requirements for the STA domain server, STA managed servers, and MySQL.

***Table 1–1 Memory Usage Requirements***

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

# Global Administration Commands

You can use the following STA commands to start, stop, and check the status of the entire STA environment.

- STA start all starts the entire STA environment. For example:

  **# STA start all**

```
Starting mysql Service..
mysql service was successfully started
Starting staservd Service.
staservd service was successfully started
Starting weblogic Service......
weblogic service was successfully started
Starting staengine Service.........
staengine service was successfully started
Starting staadapter Service..........
staadapter service was successfully started
Starting staui Service..........
staui service was successfully started
#
```

- STA stop all stops the entire STA environment. For example:

  **# 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 weblogic service......
Successfully stopped the weblogic service
Stopping the staservd Service...
Successfully stopped staservd service
Stopping the mysql service.....
Successfully stopped mysql service
#
```

- STA status all displays the status of the entire STA environment. For example:

  **# STA status all**

```
mysql is running
staservd service is running
weblogic service is running
staengine service is running
```

```
 .... and the deployed application for staengine is in an ACTIVE state
staadapter service is running
 .... and the deployed application for staadapter is in an ACTIVE state
staui service is running
 .... and the deployed application for staui is in an ACTIVE state
```

## Individual Service Administration Commands

You can use the following STA commands to start and stop individual STA components or to check the status of those components.

> **Caution:** The individual STA service commands are provided for reference only. Use these commands only if directed by Oracle Support.

- STA start | stop | status mysql

  Starts or stops MySQL, or displays its status.

- STA start | stop | status staservd

  Starts or stops the STA Services Daemon, or displays its status.

- STA start | stop | status weblogic

  Starts or stops the WebLogic AdminServer, or displays its status.

- STA start | stop | status staadapter

  Starts or stops the staAdapter managed server, or displays its status.

- STA start | stop | status staengine

  Starts or stops the staEngine managed server, or displays its status.

- STA start | stop | status staui

  Starts or stops the staUi managed server, or displays its status.

# 5

# Database Services Administration

This chapter details the administration of various STA services. To configure these services for the first time, see the *STA Installation and Configuration Guide*.

This chapter includes the following sections:



## STA Services Daemon

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

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

- To start the STA Services daemon:

  **# STA start staservd**

  Starting staservd Service...

  staservd service was successfully started

- To stop the STA Services daemon:

  **# STA stop staservd**

  Stopping the staservd Service...

  Successfully stopped staservd service

- To check the status of the STA Services daemon:

  **# STA status staservd**

  staservd service is running

For more information about the STA command, see Chapter 1, "Server Administration."

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

# STA Backup Service

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

Before proceeding, verify the STA Services Daemon is running. See "STA Services Daemon" on page 5-1.



## Configuration

The STA Backup Service is configured using its administration utility, staservadm, located in /*Oracle_storage_home*/StorageTek_Tape_Analytics/common/bin. To configure the STA Backup service, see the *STA Installation and Configuration Guide*.

## Full Backup Process

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

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

## Display the Backup Service Preference Settings

1. Display the status of the current preference settings.

   **# ./staservadm –Q**

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

2. If the Configured field is [no], the Backup Service is running in an idle mode and is not performing any backups. You must supply the proper configuration settings; see the *STA Installation and Configuration Guide* for details.

## Clear Preference Settings

1. Clear the current 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 []
```

2. The backup service is no longer configured and returns to the idle state. You can now provide new settings; see the *STA Installation and Configuration Guide* for details.

## Verify Backup Files Have Been Sent to the Target Server

To verify that files have been sent successfully to the target server:

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

1. Log on to the STA server as the system root user.
2. Change to the STA database backup log directory.

   **# cd /***sta_logs***/db/backups**

3. Search the staservd.log.0 file for the following string: "INFO: done. Database dump completed." This file registers the activities of the Backup Services configuration utility.

   **# grep "INFO: done. Database dump completed" staservd.log.0**

```
INFO: done. Database dump completed, file located at
/dbbackup/local/20130721_133755.stafullbackup.sql
INFO: done. Database dump completed, file located at
/dbbackup/local/20130722_133755.stafullbackup.sql
INFO: done. Database dump completed, file located at
/dbbackup/local/20130723_133755.stafullbackup.sql
INFO: done. Database dump completed, file located at
/dbbackup/local/20130724_133755.stafullbackup.sql
```

4. Log on to the target backup server.
5. List the files in the database backups directory.

   In this example, the directory /backups/tbivb01 was previously set up to receive the backup files from the STA server "tbivb01".

   **# ls –1 /backups/tbivb01**

```
0.stadb-bin.000023.gz
0.stadb-bin.000024.gz
0.stadb-bin.000026.gz
0.stadb-bin.000027.gz
20130723_133755.stadb-bin.000023.gz
20130723_133755.conf.zip.gz
20130723_133755.fmwconfig.zip.gz
20130723_133755.stadb-bin.000025.gz
20130723_133755.stadb-bin.000026.gz
20130723_133755.stafullbackup.sql.gz
```

### Verify a Local Copy of the Backup Files is on the STA Server

Verify that a copy of the most recent backup files has been saved locally on the STA server by listing the files in the /*sta_db_backup*/local directory. For example:

**# ls –l /dbbackup/local**

```
20130721_133755.conf.zip
20130721_133755.fmwconfig.zip
20130721_133755.stafullbackup.zip
```

The listed files have the name format *YYYYMMDD_HHMMSS.filename*.zip.

### Reset the STA Backup Service Password

See Chapter 3, "Password Administration".

## STA Resource Monitor Service

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

You may set usage high watermarks (HWM) for each resource. A high watermark is a threshold at which an alert will be raised. When the threshold is reached or exceeded,

an alert is recorded in the standard daily resource report and optionally emailed to one or more designated recipients.

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



## Configuration

The STA Resource Monitor service is configured using its administration utility, staresmonadm, located in */Oracle_storage_home/*StorageTek_Tape_Analytics/common/bin. To configure the STA Resource Monitor service, see the *STA Installation and Configuration Guide*.

## Query the Current Resource Monitor Preference Settings

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

**# ./staresmonadm –Q**

If the Configured field says "no," then the Resource Monitor Service is running in an "idle" mode neither monitoring resources nor sending reports. You will need to configure the server; see the *STA Installation and Configuration Guide* for details.

Example output of a configured STA Resource Monitor Service:

**# ./staresmonadm –Q**

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

### Clear the Resource Monitor Preference Settings

Enter the following command to clear the current preference settings:

**# ./staresmonadm –C**

The Resource Monitor service is no longer configured and returns to the idle state. You can now provide new settings; see the *STA Installation and Configuration Guide* for details. For example:

**# ./staresmonadm –C**

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

### Reset the STA Resource Monitor Password

See Chapter 3, "Password Administration."

## Resource Monitor Reports

Resource Monitor reports are configured using the STA Resource Monitor service administration utility, staresmonadm. To configure the STA Resource Monitor service, see the *STA Installation and Configuration Guide*.

The Resource Monitor can produce two different reports:

- "Resource Monitor Standard Report" on page 5-6
- "Resource Depletion Alert Report" on page 5-7

### Resource Monitor Standard Report

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

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

- Database tablespace and volume

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

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

***Example 2–1 Example Standard Report (truncated)***

```
STA RESOURCE MONITOR STANDARD REPORT
System: tbivb03
Scanned: 2013-10-24 11:30:14
Database Tablespace
  HWM            : 60.00%
  Used           : <0.1%
  MB Used        : 13
  MB Free        : 75763
  MB Total       : 75776
  Location       : /dbdata/mysql
Database Volume
  HWM            : 60.00%
  Used           : 6.80%
  MB Used        : 6855
  MB Free        : 93939
  MB Total       : 100794
  Directory      : /dbdata/mysql
...
```

## Resource Depletion Alert Report

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

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

***Example 2–2 Example Resource Depletion Alert Report***

```
STA RESOURCE DEPLETION REPORT
System: server01
Scanned: 2013-10-24 11:34:47
************************************************************
*                     A L E R T S                          *
************************************************************
================================================
ALERT - Low System Physical Memory
================================================
  Physical memory usage has exceeded threshold value!
  HWM            [1.00%]
  Used           [48.24%] (!)
  MB Used        [7757]
  MB Free        [8324]
  MB Total       [16080]
```

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

# File Types and Locations

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



## STA Services Daemon Startup and Shutdown Script

The STA Services daemon startup and shutdown script, staservd, and system run-level symbolic links are located in the following directories. This script and its associated symbolic links are created by the STA installer.

/etc/init.d/staservd—Main startup and shutdown script

/etc/rc0.d/K04staservd—Symbolic link for system shutdown

/etc/rc1.d/K04staservd—Symbolic link for system shutdown

/etc/rc2.d/S96staservd—Symbolic link for system startup

/etc/rc3.d/S96staservd—Symbolic link for system startup

/etc/rc4.d/S96staservd—Symbolic link for system startup

/etc/rc5.d/S96staservd—Symbolic link for system startup

/etc/rc6.d/K04staservd—Symbolic link for system shutdown

## STA Administration Utilities

The STA Backup Service administration utility, staservadm, is a Perl script that calls a Java client application named ServerAdm that is contained in the oracle.tbi.serveradm.jar file. For more information, see "STA Backup Service" on page 5-2.

The STA Resources Monitor administration utility, staresmonadm, is a Perl script that calls a Java client application named StaResMonAdm that is contained in the oracle.tbi.resmonadm.jar file. StaResMonAdm is an RMI client that communicates with the STA Services daemon to set and reset runtime preferences. For more information, see "STA Resource Monitor Service" on page 5-4.

## Executable Program Locations

Table 2–1 lists the executable programs and their locations.

*Table 2–1 Executable Program Locations*

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

Where:

*$STAHOME* =/*Oracle_storage_home*/StorageTek_Tape_Analytics

## Backup File Locations

The STA database backup includes the following types of files:

- STA Services Daemon and Backup Service Administration Logs
- MySQL Database Dump Files
- MySQL Binary Logs
- STA Services Daemon and WebLogic Configuration Files

### STA Services Daemon and Backup Service Administration Logs

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

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

/*STA_logs*/db/backups

The default location for *STA_logs* is /var/log/tbi.

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

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

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

Where:

*$STAHOME* =/*Oracle_storage_home*/StorageTek_Tape_Analytics

### MySQL Database Dump Files

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

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

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

### MySQL Binary Logs

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

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

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

The backup binary log naming format is *YYYYMMDD_HHMMSS*.stadb–bin.*log_sequence_number*.

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

/*STA_logs*/db

Local copies of the backup binlog files are located at:

/*sta_db_backup*/local

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

**Caution:** Never manually delete the binlog files.

### STA Services Daemon and WebLogic Configuration Files

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

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

The source and target locations of these backups are shown in Table 2–2:

*Table 2–2 Backup Source/Target Locations*

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

Where:

*$STAHOME* = /*Oracle_storage_home*/StorageTek_Tape_Analytics

*$WLHOME* = /*Oracle_storage_home*/Middleware/user_projects/domains/TBI

*$BACKUPS* =/*dbdata*/mysql/backups

*$RHOST* = Backup server IP address or name

*$RDIR* = Directory on backup server

## Resource Monitor File Locations

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

- STA Services Daemon and ResMonAdm Logs
- STA Resource Monitor CSV File

### STA Services Daemon and ResMonAdm Logs

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

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

/*STA_logs*/db/backups

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

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

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

Where:

*$STAHOME* =/*Oracle_storage_home*/StorageTek_Tape_Analytics

### STA Resource Monitor CSV File

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

/*STA_logs*/db/staresmon.csv

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

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

Each record in staresmon.csv represents a scan of the system. The format of the 21 column record is shown in Table 2–3.

***Table 2–3 Resource Monitor CSV File Format***

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

# Logging Configuration Files

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

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

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

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

Where *$STA_HOME* is the STA home location specified during STA installation; see the *STA Installation and Configuration Guide* for details.

The logging file contents and format are controlled by the Java Log Manage properties in these files. Table 2–4 summarizes these properties. For additional details, see the Oracle Java SE documentation at the following site:

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

***Table 2–4 Java Logging Properties***

| Property | Description | STA Setting |
|---|---|---|
| java.util.logging.FileHandler.append | Specifies whether the File Handler should append to existing files. Defaults to false. | true |
| java.util.logging.FileHandler.count | Specifies the number of output files to cycle through. Defaults to 1. | 10 |
| java.util.logging.FileHandler.formatter | Specifies the Formatter class name. Defaults to java.util.logging.XMLFormatter. | Java.util.logging.SimpleFormatter for human readability. The java.util.logging.XMLFormatter is commented out and available |
| java.util.logging.FileHandler.level | Specifies the default level for the Handler. Defaults to Level. ALL. | CONFIG |
| java.util.logging.FileHandler.limit | Specifies the approximate maximum number of bytes to write to any one file. An entry of zero indicates no limit. Defaults to no limit. | 500000 (.5 MB) |
| java.util.logging.FileHandler.pattern | Specifies the output file name pattern. Defaults to "%h/java%u.log". | /*STA_logs*/db/backups/staservd.log.%g<br>/*STA_logs*/db/backups/staservadm.log.%g<br>Where *STA_logs* is the logs location established during Linux installation; see the *STA Installation and Configuration Guide* for details. |

Log levels are controlled by the STA logging properties in these files. Table 2–5 summarizes the properties.

***Table 2–5 STA Services Logging Properties***

| Property | Description | STA Setting |
|---|---|---|
| oracle.tbi.server.level | Specifies the log level for the server. | CONFIG |
| oracle.tbi.serveradm.level | Specifies the log level for the server administration functions. | CONFIG |
| oracle.tbi.resmonadm.level | Specifies the log level for the resource monitor administration functions. | CONFIG |

# STA Database Restoration

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

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

**# cd /data/stabackups**

**# ls –1**

```
20130721_133755.conf.zip.gz
20130721_133755.fmwconfig.zip.gz
20130721_133755.stadb-bin.000024.gz
20130721_133755.stafullbackup.sql.gz
20130722_133755.conf.zip.gz
20130722_133755.fmwconfig.zip.gz
20130722_133755.stadb-bin.000024.gz
20130722_133755.stafullbackup.sql.gz
20130723_133755.conf.zip.gz
20130723_133755.fmwconfig.zip.gz
20130723_133755.stadb-bin.000021.gz
20130723_133755.stadb-bin.000022.gz
20130723_133755.stadb-bin.000023.gz
20130723_133755.stadb-bin.000024.gz
20130723_133755.stafullbackup.sql.gz
```

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

The following administration tasks are discussed here:

- "Copy Backup Files to the Server" on page 5-14
- "Restore the Configuration Directory Files" on page 5-15
- "Restore the Database" on page 5-15
- "Point-in-time Restorations" on page 5-16

## Copy Backup Files to the Server

Use this procedure to copy backup files to the STA server.

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

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

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

   Password:

2. Log in to the STA server as root.
3. Unzip the *.gz files. For example:

   **# cd /tmp**

   **# gunzip 20130723*.*.gz**

## Restore the Configuration Directory Files

Use this procedure to restore the configuration directory files.

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

   # **STA stop all**

   # **STA start mysql**

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

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

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

   # cd *$WLSHOME*

   # zip –vr fmwconfig.orig.zip fmwconfig

   # rm –rf fmwconfig

   # cd /tmp

   # unzip –X –d/ 20130723_133755.fmwconfig.zip

   # cd *$STAHOME*/common

   # zip –vr conf.orig.zip conf

   # rm –rf conf

   # cd /tmp

   # unzip –X –d/ 20130723_133755.conf.zip

Where:

*$WLSHOME* =/*Oracle_storage_home*/Middleware/user_projects/domains/TBI/config

*$STAHOME* =/*Oracle_storage_home*/StorageTek_Tape_Analytics

## Restore the Database

Perform the following commands as the MySQL root user.

### Reload the Database

To reload the database:

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

   # mysql –uroot –p –e 'drop database stadb;'

   Password:

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

   # mysql –uroot –p –e 'source 20130723_133755.stafullbackup.sql;'

   Password:

### Replay the Binlogs

To replay the binlogs:

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

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

   For example:

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

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

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

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

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

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

### Restart All Services

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

```
# STA start all
```

## Point-in-time Restorations

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

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

### Restore From a Range of Log Numbers

Use this procedure to restore the STA database from a range of log numbers.

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

   # **STA stop all**

   # **STA start mysql**

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

   # mysqlbinlog —start–position=176 —stop–position=6817916

   /var/log/tbi/db/stadb–bin.000007 > ./recover.sql

3. Apply them to the database. For example:

   # mysql –uroot –p –e 'source ./recover.sql'

   Password:

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

   # **STA start all**

For more information on point-in-time or incremental recovery operations refer to the MySQL documentation at the following site:

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

# 6

# Password Administration

This chapter describes changing various STA database and service passwords. To change an STA username password, see the *STA Installation and Configuration 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:



## 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 Database Root Account, Reports Account, or DBA Account password, go to Step 11.
   - If you are changing the STA Application Account password, go to the next step to first change the password in WebLogic.

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

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

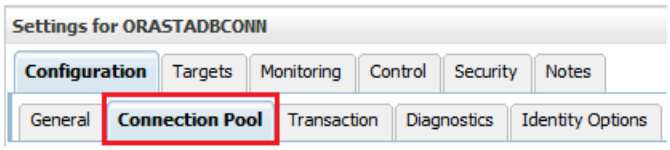
   **https://***yourHostName***:***PortNumber***/console**

3. Log in using the WebLogic Administration console username and password.

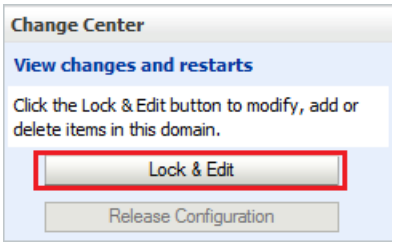
4. From the **Domain Structure** menu, select **Services**, then select **Data Sources**.


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

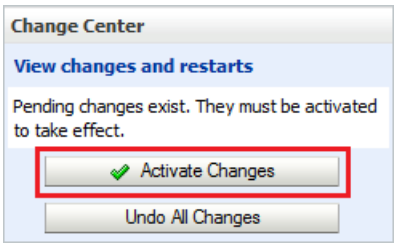

6. Click the **Connection Pool** tab.




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

    # **mysql -uroot -p**

    Password: *root_password*

12. Type the following command:

    mysql> **use mysql;**

13. Retrieve the list of STA database usernames.

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

14. Take note of the account username for which to change the password. You will use this username in the next step.

15. Issue the following commands to change the password. Use single quotes around the *new_password* and *username* variables.

    mysql> **update user set password=PASSWORD('***new_password***') where user='***username***';**

    mysql> **commit;**

    mysql> **flush privileges;**

16. Exit from the MySQL client.

    mysql> **quit;**

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

    - If you changed the STA Database Root Account password:

      **a.** Obtain a list of root user information.

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

      Enter password: *new_mysql_root_password*

      Example output:

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

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

      # **mysql_config_editor set --login-path=root_path --host=***host* **--user=root --password**

      Enter password: *new_mysql_root_password*

      WARNING : 'root_path' path already exists and will be overwritten.

      Continue? (Press y|Y for Yes, any other key for No) : **y**

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

      # **mysql --login-path=root_path --host=***host*

      Welcome to the MySQL monitor.  Commands end with ; or \g.

      Your MySQL connection id is 1234

Server version: 5.6.15-enterprise-commercial-advanced-log MySQL Enterprise Server - Advanced Edition (Commercial)

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

Oracle is a registered trademark of Oracle Corporation and/or its

affiliates. Other names may be trademarks of their respective

owners.

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

mysql> **quit**

Bye

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

  **a.** Obtain a list of database users.

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

  Enter password: *mysql_root_password*

  Example output:

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

  **b.** To set the new login path password, execute the following command for each listed user and associated 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
```

18. Proceed as follows:
    - If you changed the STA Database DBA Account password, see "Change the STA Backup Service and Resource Monitor Passwords" on page 6-5 to synchronize the password for these services.
    - If you changed the STA Database Application Account password, proceed to the next step.
    - If you changed the STA Database Root Account or Reports Account, you are finished.
19. As root on the STA server, stop and then start all STA processes by issuing the following commands:

    **# STA stop all**

    **# STA start all**

    For STA command usage details, see Chapter 1, "Server Administration."
20. Verify STA session connectivity:
    a. Go to the STA GUI login screen using the HTTP (default is 7021) or HTTPS (default is 7022) port number you selected during STA installation. STA must be uppercase. 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

If you changed the STA Database DBA Account password in "Change an STA Database Account Password" on page 6-1, you must update it in the STA Backup Service and Resource Monitor.

1. Change directories.

   **# cd /***Oracle_storage_home***/StorageTek_Tape_Analytics/common/bin**
2. Ensure the STA Backup Service and Resource Monitor is online.
   - Backup Service:

     **# ./staservadm -Q**

     Contacting daemon...connected.

     ...
   - Resource Monitor:

```
# ./staresmonadm -Q

Contacting daemon...connected.

...
```

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

   - Backup Service:

     ```
     # ./staservadm -U dba_user -P

     Enter database password: dba_password
     ```

   - Resource Monitor:

     ```
     # ./staresmonadm -U dba_user -P

     Enter database password: dba_password
     ```

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

# A

# Preventing Denial of Service Attacks

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

This appendix includes the following sections:



> **Note:** The procedures in this appendix are optional, and are provided for informational purposes only. Site security remains the responsibility of the customer.

## Overview

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

> **Note:** See the *STA Installation and Configuration Guide* for port information, including the default port values STA uses.

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

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

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

# Configure iptables Rules

To configure iptables rules:

1. Copy the source of the iptables Sample Script into a text editor.
2. Modify the following variables to suit your environment:
   - INTERFACE—Defines the ethernet interface to watch for attacks
   - PORT—Defines the port number to watch for attacks
   - PROTO—Defines the protocol (TCP or UDP)
   - HITS and TIME—Decide what are reasonable values for the number of requests (HITS) within a given time period in seconds (TIME) to block a server.
3. Save the script to your system and execute it.

   The new rules are added to iptables and take effect immediately.

# iptables Sample Script

The following is an iptables sample script.

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

```
 R=0
 while [$R -eq 0 ]; do
 /sbin/iptables -D $CHAIN 1 1>/dev/null 2>&1
 R=$?
 done
fi
# Logging rule
/sbin/iptables --append $CHAIN --jump LOG --log-level 4
# Interface rule
/sbin/iptables --insert $CHAIN --proto $PROTO --dport $PORT --in-interface $INTERFACE --match state
--state NEW --match recent --set
# Blocking rule
/sbin/iptables --insert $CHAIN --proto $PROTO --dport $PORT --in-interface $INTERFACE --match state
--state NEW --match recent --update --seconds $TIME --hitcount $HITS --jump DROP
```

# Index