

StorageTek Tape Analytics

Administration Guide

Version 2.3.1

F30273-01

June 2020

Copyright © 2012, 2020, Oracle and/or its affiliates.

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

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

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

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or "commercial computer software documentation" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

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

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

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

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

Preface	vii
Documentation Accessibility	vii
Related Documentation	vii
1 About the Administration Environment	
STA Application Startup and Shutdown Sequences	1-1
Server Memory Requirements for STA Administration Environment	1-2
When to Use the WebLogic Administration Console	1-2
STA Services Administration Logs	1-2
Configure the Correct Oracle User Path	1-3
2 STA Command	
STA Command Directory	2-1
STA Application - Stop, Restart, or Show Status	2-1
Display the Status of the STA Application	2-1
Stop the STA Application	2-2
Restart the STA Application	2-2
Services Daemon - Stop, Restart, or Show Status	2-2
Display the Status of the STA Services Daemon	2-3
Stop and Restart the STA Services Daemon	2-3
Domain Server - Show Status	2-3
MySQL Server - Stop or Restart	2-4
Stop the MySQL Server	2-5
Restart the MySQL Server	2-5
3 Backup Service	
Database Backup Best Practices	3-1
About the STA Backup Service	3-2
Full Database Dump Files	3-2
Configuration Directories	3-3
Incremental Backup Files (Binary Logs)	3-4
Configure the Backup Service Using staservadm	3-4
Display Current STA Backup Settings	3-5
Enable the STA Backup Service	3-6
Disable the STA Backup Service	3-6

Define the Time of Day for Full Backups	3-7
Define the Incremental Backup Interval	3-7
Prepare an External Backup Server	3-7
View Backup Information	3-8
View Log Entries for a Backup	3-9
List All Files for a Full Database Dump	3-9
List Incremental Backup Files (Binary Logs)	3-10
Verify a Local Backup	3-10
View Binary Log Contents	3-11
Restore the STA Database from a Backup	3-11
Prepare a Replacement STA Server (optional)	3-12
Copy Backup Files to the Server	3-12
Restore the Database Configuration Directory Files	3-12
Reload the Database	3-13
Perform a Full Restore From All Incremental Backups	3-14
Perform a Partial Restore From a Range of Incremental Backups	3-15
How to Determine Which Incremental Backups to Restore	3-16
Transfer the STA Database to Another Server	3-16
Prepare the Target Server	3-16
Dump the STA Database	3-16
Transfer the Dump File to the Target Server	3-18
Process and Load the STA Database on the Target Server	3-18
Post-transfer Configuration	3-19

4 Resource Monitor (Resmon)

About the STA Resource Monitor Service	4-1
Resmon Resource Report	4-2
Resource Report CSV File	4-3
Resource Depletion Alert Report	4-4
Configure the Resource Monitor Using staresmonadm	4-5
Display Current Resmon Settings	4-6
Enable the Resmon Service	4-7
Disable the Resmon Service	4-7
Define Resmon Email Settings	4-8
Troubleshoot Resmon Email Issues	4-8
Define Resource Report Settings	4-9

5 Password Change Utility

Username and Password Requirements	5-1
Change a Password with the Utility	5-1
What Occurs If a Password Update Fails When Changing All Passwords	5-3
Updates Made by the Password Change Utility	5-3
Password Change Utility Logs	5-4

6 Port Change Utility

Unconfigurable Ports	6-1
-----------------------------------	-----

Configurable Ports	6-1
Ports for Communications with SDP (optional)	6-2
Change Ports Using the Utility	6-3
Port Change Utility Logs.....	6-4

A Troubleshooting

ISSUE: Cannot Access the STA GUI	A-1
ISSUE: Exchanges Not Showing Up in STA.....	A-2
ISSUE: SNMP Library Connection Test Fails.....	A-4
ISSUE: Cannot Connect to SDP.....	A-4
ISSUE: Weblogic Server Processes Not Starting.....	A-4
ISSUE: Authentication Prompts During STA start Command	A-5
ISSUE: Backup Service or Resource Monitor Fails.....	A-5

B Prevent Denial-of-Service Attacks

Preface

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

Visit the Oracle Help Center for other STA documentation: <https://docs.oracle.com/en/storage/storage-software/storagetek-tape-analytics/>

STA documentation includes:

- *Installation and Configuration Guide*
- *Administration Guide*
- *User's Guide*
- *Security Guide*
- *Licensing Information User Manual*

About the Administration Environment

The STA administration environment consists of a single WebLogic domain, a MySQL database server, and the STA services daemon. WebLogic is the application server that hosts the STA application.

You can control aspects of the administration environment using STA administration tools such as the STA command, Backup Service, Resource Monitor, Password Utility, and Port Utility.

- [STA Application Startup and Shutdown Sequences](#)
- [Server Memory Requirements for STA Administration Environment](#)
- [When to Use the WebLogic Administration Console](#)
- [STA Services Administration Logs](#)
- [Configure the Correct Oracle User Path](#)

STA Application Startup and Shutdown Sequences

The sequence of startup and shutdown for the STA application always follows the same order. Understanding the sequence can help troubleshoot issues.

Startup Sequence

All resources for the STA environment automatically start when the STA application starts.

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

Shutdown Sequence

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

6. MySQL database (mysql)

Server Memory Requirements for STA Administration Environment

The STA administration environment has minimum server memory requirements.

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

When to Use the WebLogic Administration Console

In a limited number of circumstances, you can use the WebLogic Administration console to log in directly to the WebLogic server and display or modify the TBI domain.

You should use the WebLogic Administration console only in the following limited circumstances, which may apply to your site depending on your site requirements. See the *STA Installation and Configuration Guide* for details.

- Configure security certificates for HTTPS/SSL ports.
- Configure external authentication providers (SSPs) to authenticate STA users.

The name assigned to the WebLogic domain is TBI. Do not change this name.

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 home location specified during STA installation.

Caution: Do not use the WebLogic Administration console to change any passwords for the STA application, database, or WebLogic Administration console as it will require you to reinstall STA. Instead use the password utility. See [Change a Password with the Utility](#).

STA Services Administration Logs

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

The services administration logs are located in: /var/log/tbi/db/backups

The types of logs are:

- staservd.log—STA services daemon log. Records when the STA Backup and Resource Monitor services perform their activities.
- 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 log type, there may be up to 10 different log files in the directory. Each has 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, STA rotates the logs. Log "0" becomes log "1", log "1" becomes log "2", and so on. Any existing log "9" is overwritten by log "8" and effectively deleted. Then, STA starts a new log "0".

The following is a sample directory listing showing the files.

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

Configure the Correct Oracle User Path

To use the administration utilities, the path for the Oracle user must include the directory that contains STA command, staresmonadm, staservadm, changeSTAPassword.sh, and changeSTAports.sh.

The Oracle user is a Linux user that installs Oracle products on the STA server and runs the STA application and utilities. See the *STA Installation and Configuration Guide* for details about the Oracle user and group.

1. Open a terminal session on the STA server, and log in as the Oracle 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/bin:/bin:/usr/bin:/usr/local/sbin:/usr/sbin:/sbin:/home/oracle/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 /home/oracle/.bash_profile
PATH=$PATH:/sbin:/bin:/usr/sbin:/usr/bin
```

Save and exit the file.

4. Log out and log back in as the Oracle user.
5. Confirm that the PATH variable has been updated correctly.

```
$ echo $PATH  
/usr/lib64/qt-3.3/bin:/usr/local/bin:/bin:/usr/bin:/usr/local/sbin:/usr/sbin:/s  
bin:/home/oracle/bin:/Oracle/StorageTek_Tape_Analytics/common/bin
```

STA Command

The **STA** command can start, stop, and show the status of the entire STA application or an individual service within the STA administration environment. Use **STA help** to display complete command syntax and usage information.

Caution: Do not stop and start individual STA managed servers (such as `staadapter`, `staiui`, or `staengine`), unless directed to by Oracle.

- [STA Command Directory](#)
- [STA Application - Stop, Restart, or Show Status](#)
- [Services Daemon - Stop, Restart, or Show Status](#)
- [Domain Server - Show Status](#)
- [MySQL Server - Stop or Restart](#)

STA Command Directory

The STA command is located in:

```
/<Oracle_storage_home>/StorageTek_Tape_Analytics/common/bin
```

where `<Oracle_storage_home>` is the Oracle storage home location specified during installation.

Before using the STA command, make sure the Oracle user path is correctly configured. See [Configure the Correct Oracle User Path](#).

STA Application - Stop, Restart, or Show Status

Use the STA command to start, stop, or show the status of the STA application.

- [Display the Status of the STA Application](#)
- [Stop the STA Application](#)
- [Restart the STA Application](#)

Display the Status of the STA Application

Display the current status of the STA application to see if it is running.

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

2. Display the application status:

```
$ STA status all
```

It may take a few minutes. Once complete, you should see:

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

3. If the application is not running, try restarting it. See [Restart the STA Application](#).

Stop the STA Application

Always shut down the STA application gracefully whenever possible. You must stop the STA application when moving or restoring the STA database.

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

2. Stop STA:

```
$ STA stop all
```

It may take several minutes. Once complete, you should see:

```
Successfully stopped mysql service
```

3. Verify the application has stopped:

```
$ STA status all
```

You should see:

```
stau1 service is shutdown.
```

Restart the STA Application

STA automatically starts after you install it, so under normal circumstances, only restart STA after performing certain database tasks, such as moving or restoring the STA database.

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

2. Start STA:

```
$ STA start all
```

It may take several minutes. Once complete, you should see:

```
staservd service was successfully started
```

3. Verify the application has started successfully:

```
$ STA status all
```

You should see:

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

Services Daemon - Stop, Restart, or Show Status

Use the STA command to start, stop, or show the status of the services daemon. The services daemon, `staservd`, is a continuously running Linux service that manages and runs the Backup and Resmon services.

The daemon must be running for the Backup or Resmon services to be available. The services run as separate execution threads within the STA services daemon. The Backup and Resmon services are disabled by default after STA installation. See [Backup Service](#) and [Resource Monitor \(Resmon\)](#) for details.

- [Display the Status of the STA Services Daemon](#)
- [Stop and Restart the STA Services Daemon](#)

Display the Status of the STA Services Daemon

Display the status of the services daemon to verify it is running. The daemon must be running for the Backup and Resmon utilities to be available.

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

```
$ STA status staservd
```

You should see:

```
staservd service is running
```

3. If the daemon is not running, try stopping and then restarting it. See [Stop and Restart the STA Services Daemon](#).

Stop and Restart the STA Services Daemon

You may need to stop and restart the daemon to apply configuration changes made to the Resmon or Backup services. Stopping the daemon does not interrupt STA, but the Backup and Resmon services will be unavailable until the daemon is restarted.

By default, new service settings take effect when the service wakes from its sleep interval. However, stopping and restarting the daemon will apply the settings immediately.

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

```
$ STA stop staservd
```

3. Verify the daemon has stopped:

```
$ STA status staservd
```

You should see:

```
staservd service is shutdown
```

4. Start the STA services daemon:

```
$ STA start staservd
```

5. Verify the daemon is running:

```
$ STA status staservd
```

You should see:

```
staservd service is running
```

Domain Server - Show Status

Use the STA command 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 Oracle user.
2. Display the status of the domain server:

```
$ STA status [server]
```

Where the **[server]** is one of the following options:

- staweblogic
- staadapter
- staengine
- stai

For example:

```
$ STA status staengine
```

If the server is running normally, you would see:

```
[server] service is running  
.... and the deployed application for [server] is in an ACTIVE state
```

If the server is not running, you would see:

```
[server] service is shutdown
```

3. If the domain server is not running, try restarting the STA applications. See [Stop the STA Application](#) and [Restart the STA Application](#).

Caution: Do not start or stop individual STA domain servers, unless directed to by Oracle Service.

About the TBI Domain Servers

The 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.
 - stai—STA user interface

The administration server (staweblogic) must be running before the managed servers can be started. When the managed servers start, 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.

MySQL Server - Stop or Restart

Use the STA command to stop or restart the MySQL server. You may need to do this during database management activities.

- [Stop the MySQL Server](#)
- [Restart the MySQL Server](#)

Stop the MySQL Server

Stop the MySQL database server when performing database management activities in which the MySQL server is running, but the rest of the STA application is not.

1. **IMPORTANT:** Do not stop the MySQL server if the rest of the STA application is running.
2. Open a terminal session on the STA server, and log in as the Oracle user.
3. Stop the MySQL server:

```
$ STA stop mysql
```

4. Verify the server is not running:

```
$ STA status mysql
```

You should see:

```
mysql is shutdown
```

Restart the MySQL Server

Restart the MySQL database server when performing database management activities in which you must shut down the STA application and then restart just the MySQL server.

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

```
$ STA start mysql
```

3. Verify the server is running:

```
$ STA status mysql
```

You should see:

```
mysql is running
```

Backup Service

Regular backups of the STA database can protect your site from potential data loss. STA provides a Backup Service, but if you have a preferred backup application at your site, you can use that instead.

The STA Backup Service is disabled by default. Use the `staservadm` utility to configure it. Once configured, the service performs regular backups of the STA database and saves it on either the STA server or an external server.

- [Database Backup Best Practices](#)
- [About the STA Backup Service](#)
- [Configure the Backup Service Using `staservadm`](#)
- [Prepare an External Backup Server](#)
- [View Backup Information](#)
- [Restore the STA Database from a Backup](#)
- [Transfer the STA Database to Another Server](#)

Database Backup Best Practices

Follow best practices when implementing a backup strategy to maximize the effectiveness of your backups.

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. 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. 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.

Automate your space management policies

If you back up the database to an external server, you can use a backup service of your choice to manage the files according to your site policies. Absent a backup service, you can set up a Linux cron job to delete old backups.

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. A suggested practice is to archive files more than one or two weeks old and delete archives more than one or two months old.

Manage the database and backup space

It is the customer's responsibility to manage space on the STA server and the backup server. To help keep the active database at a reasonable size, STA automatically rolls off detailed exchange and SNMP trap data that is more than 60 days old.

Use the STA Resource Monitor to monitor space on the STA server

Oracle recommends that usage for any partition should never exceed 80 percent. You can use STA Resource Monitor to define high-water marks for disk usage, and the Resource Monitor will alert you if these are exceeded.

About the STA Backup Service

The Backup Service (`staservadm`) can automate database backups. Once enabled, the service runs in the background and performs a routine set of processes.

Once a day, at the time you have specified, the service:

- Uses the `mysqldump` command to create a high-speed dump of the current STA database.
- Transfers all existing backup files to the location you have specified. This includes the following files:
 - Database dump file just created
 - Compressed STA services and WebLogic configuration directories
 - All incremental backups (binary log files) created within the last 24 hours

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

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

Periodically, at the time interval you have specified, the service closes the current binary log file and opens a new one. This step is repeated at the sleep interval specified until the next full backup.

Full Database Dump Files

A full backup, or database dump, is a complete record of the STA database schema and data contents at a point in time. The Backup Service creates a dump once a day at the time you have defined with the `staservadm` utility.

Dump File Names

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, `20200114_180525.stafullback.sql` would be a database dump file created on January 14, 2020 at 18:05:25.

Dump File 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 installation (see the *STA Installation and Configuration Guide* for details). The Backup Service automatically creates the `local` subdirectory if it does not exist already.

The 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 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.

The 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. 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.

See Also:

- [Define the Time of Day for Full Backups](#)
- [List All Files for a Full Database Dump](#)

Configuration Directories

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

Configuration File Names

The file names 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, `20200114_180525.conf.zip` and `20200114_180525.fmwconfig.zip` would be compressed WebLogic and STA services configuration directories, respectively, created on January 14, 2020 at 18:05:25.

Configuration File 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, records changes to the database that have occurred since the last backup. The incremental backups are significantly smaller than a full database backup. The logs are saved in binary format.

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.

Binary Log File Names

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.

Binary Log 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.

The 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. You can keep as many days worth of incremental backups on the backup server as your site's policies require.

See Also:

- [Define the Incremental Backup Interval](#)
- [List Incremental Backup Files \(Binary Logs\)](#)
- [View Binary Log Contents](#)

Configure the Backup Service Using staservadm

Use the `staservadm` utility to configure the STA Backup Service.

Prerequisites

- The Services Daemon must be running to use the Backup Service.
See [Services Daemon - Stop, Restart, or Show Status](#).
- The Oracle user path must be correctly configured.

See [Configure the Correct Oracle User Path](#).

Parameters

The `staservadm` utility uses the parameters listed in the table below. You can submit as many parameters as you want in each `staservadm` command line. The utility only updates the parameters you specify. The unspecified parameters remain at their current value.

Some settings (denoted by * in the table) require you to stop and restart the Services Daemon if you want the setting to take effect immediately. Otherwise these changes take effect as soon as the Backup Service wakes from its current sleep interval.

Name	Parameter	Description	Sample Value
Help	-h, --help	Displays command usage information.	NA
Clear Settings	-C, --clear	Clears all settings and disables the backup service.	NA
Query Settings	-Q, --query	Displays the current Backup service settings.	NA
File Transfer	-S, --scp -F, --ftp	The file transfer method: SCP or FTP. SCP is recommended.	SCP (default)
Full Backup Time*	-T, --time	The time of day full backups are performed. 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.	23:30 00:00 (default)
Sleep Interval*	-i, --int	The number of seconds between incremental backups. Valid entries: integers 1 to 86399.	1800 (=30 minutes) 300 (default)
Backup Hostname	-s, --server	The hostname or IP address of the server which the STA Backup service copies the backup files to. You can specify an IPv4 or IPv6 address, or a fully qualified DNS host name.	stabackup
Backup Username	-u, --usr	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. If you specify a username, you must also specify a password.	root
Backup Password	-p, --pwd	The password for the backup username. If you enter just -p on the command line, the utility will prompt for the password, which is hidden when you type it.	NA
Backup Directory	-d, --dir	Directory on the backup server where the backup files will be copied. This directory must already exist on the server.	/dbbackup
Database Username	-U, --dbusr	The MySQL database administrator account created during STA installation.	stadba blank (default)
Database Password	-P, --dbpwd	Password for the database root username.	blank (default)

Display Current STA Backup Settings

Display the current settings to determine if the Backup service is configured.

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

```
$ staservadm -Q
```

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

```

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

Enable the Backup Service to perform automatic backups of the STA database according to the defined settings. The Backup Service is disabled by default.

1. Open a terminal session on the STA server, and log in as the Oracle user.
2. To enable the service, all parameters must be defined. For parameters with default values, you can retain the defaults or define new values. See [Configure the Backup Service Using staservadm](#) for a list of parameters.

Define the required parameters in one or more commands. For example:

```
$ staservadm -s stabackup -d /dbbackup -u root -p -U stadba -P
```

3. The utility runs the first full backup at the full backup time and incremental backups periodically after that. You do not need to stop and restart the STA services daemon.
4. If the utility fails with:

```
Error: java.util.prefs.BackingStoreException: Couldn't get file lock.
```

See [ISSUE: Backup Service or Resource Monitor Fails](#).

Disable the STA Backup Service

Disable the STA Backup service by clearing all settings.

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

```
$ ./staservadm -C
```

```

Current STA Backup Service Settings:
Configured           [no]
File Transfer        -S [SCP]
Full Backup          -T [00:00]
Sleep Interval       -i [300 sec]
Backup Hostname      -s []
Backup Username      -u []
Backup Password      -p []
Backup Directory     -d []
Database Username    -U []
Database Password    -P []
    
```

3. The service is disabled immediately. You do not need to stop and restart the STA services daemon.
4. If the utility fails with:

Error: java.util.prefs.BackingStoreException: Couldn't get file lock.

See [ISSUE: Backup Service or Resource Monitor Fails](#).

Define the Time of Day for Full Backups

The Backup service performs a full backup at the time defined in the settings. The time is based on the system time on the STA server.

1. Open a terminal session on the STA server, and log in as the Oracle user.
2. Use the `-T` command to define the time to perform backups. For example:

```
$ staservadm -T 23:30
```

3. If you want the new settings to take effect immediately, you must stop and restart the STA services daemon. See [Services Daemon - Stop, Restart, or Show Status](#).

Note: If a full backup has already occurred earlier in the day, the service won't create a full backup today at the new time. See below.

Why didn't the backup run today after I changed the time settings?

The Backup service only runs a single full backup per day. Therefore, if a full backup occurred earlier in the day, the service won't run a second backup after you change the time.

For example, the previous settings were 1:00 (1 a.m.) and you change the settings to 23:00 (11 p.m.). If you changed the settings after the 1 a.m. backup has occurred, the service will not perform a full backup at 11 p.m. because a backup has already occurred today. The service will start performing backups at 11 p.m. the following day.

Define the Incremental Backup Interval

The sleep interval defines the amount of time in seconds between incremental backups. Define a time that meets your site's backup requirements.

1. Open a terminal session on the STA server, and log in as the Oracle user.
2. Use the `-i` command to define the interval time in seconds. Valid values are 1 to 86399. The default is 300.

For example, to take an incremental backup every 30 minutes:

```
$ staservadm -i 1800
```

3. If you want the new settings to take effect immediately, you must stop and restart the STA services daemon. See [Services Daemon - Stop, Restart, or Show Status](#).

See Also:

- [Incremental Backup Files \(Binary Logs\)](#)
- [List Incremental Backup Files \(Binary Logs\)](#)

Prepare an External Backup Server

Oracle recommends backing up the database to an external backup server to protect against data loss.

The required space on the backup server is 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.

1. Obtain the names and credentials of the Oracle user and group used on the STA server.

Because the Backup Service is run as the Oracle user, and this user owns all STA backups, you must create this same user and group on the external backup server. See the *STA Installation and Configuration Guide* for details about the Oracle user and group.

2. On the external server, open a terminal session. Log in as the system root user.
3. Create the Oracle group. For example:

```
# groupadd oinstall
```

4. Create the Oracle user and assign the same password as on the STA server. For example:

```
# useradd -g oinstall -d /home/oracle oracle
# passwd oracle
```

where:

- `-g oinstall` assigns the user to the Oracle group.
- `-d /home/oracle` creates the user's home directory.

5. Create the directory where the STA backups will be written. For example:

```
# mkdir -p /remote_backups/STAbackups
```

where:

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

6. Assign ownership of the backup directory to the Oracle user and group. For example:

```
# chown -R oracle:oinstall /remote_backups/STAbackups
```

where:

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

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

```
# ls -l /remote_backups
total 4
drwxr-xr-x 2 oracle oinstall 256000 Jan  2 13:20 STAbackups
```

View Backup Information

Use a terminal session on the STA server to view information about the backups.

- [View Log Entries for a Backup](#)
- [List All Files for a Full Database Dump](#)

- [List Incremental Backup Files \(Binary Logs\)](#)
- [View Binary Log Contents](#)
- [Verify a Local Backup](#)

View Log Entries for a Backup

View STA server log entries for a backup.

1. Open a terminal session on the STA server, and log in as the Oracle 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.

You may need to search more than one log file to find the applicable entries. 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).

- Display all backups recorded in the `staservd.log.1` log file.

```
$ grep 'StaBackup' staservd.log.1 | grep 'Database dump completed'
```

- Refine the search to display entries just for the backup in question. This example shows entries for the backup done on January 23, 2020.

```
$ grep 'StaBackup' staservd.log.1 | grep 20200123
```

- Refine the search to display the name of the host where the files for the backup in question were sent.

```
$ grep 'StaBackup' staservd.log.1 | grep 20200123 | grep 'sending file'
```

List All Files for a Full Database Dump

Verify that files for a full backup have been successfully saved to the right location and check the size of the files.

1. Open a terminal session on the applicable server, and log in as the Oracle user.
2. Change to the backup directory.

The backup directory may be on the local STA server or an external server. Oracle recommends backing up the database to an external backup server. The backup location is defined by the `staservadm` utility. See [Display Current STA Backup Settings](#) for instructions on displaying the location.

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, 2020.
 - 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 name ending in `conf.zip`.

```
$ ls -l *20200123*
```

```
-rw-r--r-- 1 oracle oinstall 11081 Jan 23 17:02 20200123_170250.conf.zip.gz
-rw-r--r-- 1 oracle oinstall 195524 Jan 23 17:02 20200123_
170250.fmwconfig.zip.gz
-rw-r--r-- 1 oracle oinstall 37968 Jan 24 17:03 20200123_
170250.stadb-bin.000028.gz
-rw-r--r-- 1 oracle oinstall 461721 Jan 23 17:02 20200123_
170250.stafullbackup.sql.gz
```

List Incremental Backup Files (Binary Logs)

View 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 Oracle 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.
 - 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 oracle oinstall 4096 Jan 24 02:52 backups
-rw-rw---- 1 oracle oinstall 161351 Jan 24 17:03 stadb-bin.000028
-rw-rw---- 1 oracle oinstall 146592 Jan 25 14:55 stadb-bin.000029
-rw-rw---- 1 oracle oinstall 66 Jan 24 17:03 stadb-bin.index
-rw----- 1 oracle oinstall 6561 Jan 24 17:03 stadb-slow.log
```

Verify a Local Backup

Verify the local backup was completed on a particular date.

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

```
$ ls -l /var/log/tbi/db/backups
```

3. To determine which backups have been performed recently:

```
$ grep 'StaBackup' staservd.log.0 | grep 'Database dump completed'
```

4. Verify that the latest backup was saved correctly:
 - a. Change to the local backup subdirectory for your site. For example:

```
$ cd /dbbackup/local
```

- b. List the directory. It should contain the most recent backup files, including a full database dump and configuration files, created by the Backup Service.

```
$ ls -l
```

View Binary Log Contents

When restoring the database, you may not want to apply an entire incremental backup file if you suspect it contains corrupted database operations. View the contents of the binary log to identify valid events.

To view binary log events, you must use the MySQL `mysqlbinlog` utility. The utility converts the binary file contents to text form. See the `mysqlbinlog` utility reference for complete details.

The following shows an example of the binary log content:

```
$ 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 '
2LemVg8BAAAAAdAAAAHgAAAAAAQANS42LjE4LWVudGVycHJpc2UtY29tbWVyY2lhbC1hZHhbmNl
ZC1sb2cAAAAAAAAAAAAAAAAAEzgNAAgAEgAEBAQEgAAXAAEGggAAAAICAgCAAAACgoKGRkAATvv
dio=
'/*!*/;
# at 120
--More--
```

Restore the STA Database from a Backup

To resolve certain STA application issues, you may need to restore the database to the last incremental backup.

To restore the database, you will 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 these tasks in order:

1. [Prepare a Replacement STA Server \(optional\)](#)
2. [Copy Backup Files to the Server](#)
3. [Restore the Database Configuration Directory Files](#)
4. [Reload the Database](#)
5. Depending on which incremental backups need to be restored, use the following:
 - [Perform a Full Restore From All Incremental Backups](#)

- [Perform a Partial Restore From a Range of Incremental Backups](#)

For additional information about restoring a MySQL database, see the MySQL documentation at: <http://docs.oracle.com/en/database/>

Prepare a Replacement STA Server (optional)

You may need to install and configure a replacement STA server if the STA server experienced a catastrophic failure.

See the *STA Installation and Configuration Guide* to perform the following:

1. Install Linux on the replacement server. The replacement server must run the same version of Linux and STA as the original STA server.
2. Install STA on the replacement server.
3. Add the replacement server as an SNMP trap recipient on all libraries monitored by STA.

Copy Backup Files to the Server

Copy the 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 Oracle 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 *20200123* staserver.mycompany.com:/tmp/.
```

where:

- `*20200123*` 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 Oracle user.
 - b. Change to the target directory and verify the compressed files were successfully copied.

```
$ cd /tmp
$ ls -l *20200123*
```

- c. Decompressed files.

```
$ unzip *20200123*.gz
$ ls -l *20200123*
```

Restore the Database Configuration Directory Files

To ensure a clean restore, remove any existing directories after first saving a copy, and then completely replace the directories.

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

1. On the STA server, open a terminal session. Log in as the Oracle user.

2. Stop all STA processes:

```
$ STA stop all
```

3. Restart the MySQL server:

```
$ STA start mysql
```

4. As a safeguard, save the existing STA services and database server configuration directories to zip files. For example:

```
$ cd /Oracle/StorageTek_Tape_Analytics/common
```

```
$ zip -vr conf.orig.zip conf
```

```
$ cd /Oracle/Middleware/user_projects/domains/TBI/config
```

```
$ zip -vr fmwconfig.orig.zip fmwconfig
```

5. Delete the existing configuration directories.

```
$ rm -rf /Oracle/StorageTek_Tape_Analytics/common/conf
```

```
$ rm -rf /Oracle/Middleware/user_projects/domains/TBI/config/fmwconfig
```

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

```
$ cd /tmp
```

```
$ unzip -X -d / 20160123_170250.conf.zip
```

```
...
```

```
$
```

```
$ unzip -X -d / 20160123_170250.fmwconfig.zip
```

```
$
```

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.
7. 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

Reload the STA database from the last full database dump.

1. On the STA server, open a terminal session. Log in as the Oracle 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:
- [Perform a Full Restore From All Incremental Backups](#).
  - [Perform a Partial Restore From a Range of Incremental Backups](#). Use this 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

Restore all incremental backups (binary logs) since the last full backup. Make sure you restor the incremental backups in the proper order.

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

---

---

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

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!!
```

---

---

2. Run the binary logs in chronological order, from oldest to newest. If you have more than one binary log to execute, you must 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:
```

## Perform a Partial Restore From a Range of Incremental Backups

Partially restore the STA database from a range of incremental backups. This restores the database from the last full dump and then applies just the incremental backups that fall within the start and end points specified.

1. On the STA server, open a terminal session. Log in as the Oracle user.

2. Stop all STA processes:

```
$ STA stop all
```

3. Restart the MySQL server:

```
$ STA start mysql
```

4. 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.000007` is the binary log file you want to extract from.
- `./recover.sql` is the file you want to write the entries to.

5. 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.

6. Restart STA and all associated processes. See [Restart the STA Application](#).

### How to Determine Which Incremental Backups to Restore

Incremental backups (binary logs) are labeled with unique sequential numbers. Therefore, if you identify a corrupt entry you can restore all logs before the erroneous entry.

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.

You would want to 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".

## Transfer the STA Database to Another Server

You may want to transfer the STA database to another server to test a new feature or replace the existing server with a new one.

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

1. [Prepare the Target Server](#)
2. [Dump the STA Database](#)
3. [Transfer the Dump File to the Target Server](#)
4. [Process and Load the STA Database on the Target Server](#)
5. [Post-transfer Configuration](#)

### Prepare the Target Server

Prepare the target server before importing the STA database. The target server must run the same version of Linux and STA as the current server.

Refer to the *STA Installation and Configuration Guide* to perform the following:

1. Install Linux on the target server.
2. Install STA on the target server.
3. 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.
  - 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.

### Dump the STA Database

Perform a full dump of the STA database 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 Oracle 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:

```
$ STA stop all
```

4. Restart the MySQL server:

```
$ 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:** Do not use the --verbose command option, 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 oracle oinstall 3875509 Jan 15 14:05 160115_SavedSTADatabase.sql
```

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

```
$ zip 160115_SavedSTADatabase.sql
$ ls -l 160115*.gz
```

```
-rw-r--r-- 1 oracle oinstall 365282 Jan 15 14:34 160115_
SavedSTADatabase.sql.gz
```

## Transfer the Dump File to the Target Server

Transfer and decompress the STA database dump file on the target server.

1. On the target server, verify there is sufficient space for the *decompressed* database dump file (which may be 10 to 15 times the size as the compressed database).
  - a. Open a terminal session on the target server and log in as the Oracle 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 while dumping the database.

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 Oracle 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 Oracle user.
  - b. Decompress the dump file. For example:

```
$ cd /tmp
$ unzip 160115_SavedSTADatabase.sql.gz
$ ls -l 160115*.sql
-rw-r--r-- 1 oracle oinstall 3875509 Jan 15 15:05 160115_
SavedSTADatabase.sql
```

## Process and Load the STA Database on the Target Server

Load the decompressed dump file into the database on the target server.

1. On the target server, open a terminal session. Log in as the Oracle user.
2. Stop all STA processes:

```
$ STA stop all
```

- Restart the MySQL server:

```
$ STA start mysql
```

- 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.

---

## Post-transfer Configuration

After transferring the database, you must configure STA on the target server.

- Add the target STA server as a trap recipient on the libraries you want STA to monitor. See the library configuration tasks in the *STA Installation and Configuration Guide* for instructions.
- Use the following tasks to configure library connections to each library. See the SNMP connection management tasks in the *STA Installation and Configuration Guide* for complete instructions. These tasks are all performed on the target server.
  - Enter the configuration settings for the STA SNMP client.
  - Reconfigure the SNMP connection to each library you want STA to monitor.
  - Establish SNMP communication between STA and the libraries by testing the connection to each library.
  - Get the latest SNMP library configuration data from each library.
- Configure STA users and application data, as applicable. These tasks are all performed on the target server. Refer to the *STA User's Guide* for instructions.
  - Create STA usernames and passwords.
  - If the STA email server requires authentication, you must enter the email account username and password.
  - Assign ownership to custom templates, as applicable.

- d. Assign ownership to private Executive Report policies, as applicable.
  - e. Assign ownership to logical groups by recreating the groups, as applicable.
4. Configure the Backup Service on the target server.  
See [Configure the Backup Service Using staservadm](#).
  5. Configure the Resource Monitor on the target server.  
See [Configure the Resource Monitor Using staresmonadm](#).

---

---

## Resource Monitor (Resmon)

The STA Resource Monitor (Resmon) service monitors usage levels of key resources on the STA server. It produces a daily usage report and an optional resource depletion report that alerts you when resources have exceeded user-defined high-water marks.

The Resmon service is disabled by default. Use the `staresmonadm` utility to configure it.

- [About the STA Resource Monitor Service](#)
- [Configure the Resource Monitor Using `staresmonadm`](#)

### About the STA Resource Monitor Service

Once enabled, the Resmon service runs in the background and monitors usage levels of resources on the STA server.

Resmon does the following:

- 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 and optionally emails the report.
- Optionally sends a Resource Depletion Alert Report whenever it detects that a monitored resource has exceeded a user-defined high-water mark (HWM).

#### 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

The Resmon service will perform the following:

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.
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.
3. Every day at 08:41 (Send Reports time), Resmon sends a copy of the Resource Report to the designated email recipient.

## Resmon Resource Report

The Resmon resource report is a daily report that provides data for all monitored resources and alerts for any resources that have exceeded their defined high-water marks.

The Resmon service sends the Resource Report to all Resmon email recipients once a day, at approximately the "Send Reports" time. Reported values rely on mount points. If multiple monitored resources share a mount point, their reported values will be identical.

### **Example 4-1 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

```

## Resource Report CSV File

The Resource Report file is a comma-delimited (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. 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.

The Resource Report data file, by default has the following location and file name.

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

Import the file into spreadsheet or database management applications to create reports and graphs of the values.

**Table 4–1 Resource Report Record Format**

| Col | Header          | Description                                                                                | Format                 |
|-----|-----------------|--------------------------------------------------------------------------------------------|------------------------|
| 1   | TIMESTAMP       | Date and time of the scan                                                                  | YYYY-MM-DD<br>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%                 |
| 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                    |

**Table 4–1 (Cont.) Resource Report Record Format**

| Col | Header       | Description                                                                           | Format |
|-----|--------------|---------------------------------------------------------------------------------------|--------|
| 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% |

## Resource Depletion Alert Report

If you enable alert nagging, Resmon sends a Resource Depletion Alert Report whenever it detects that any monitored resources have exceeded their defined high-water marks. If you disable alert nagging, alerts appear only in the daily Resource Report.

### Example 4–2 Example Resource Depletion Report email

```
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.
```

## Configure the Resource Monitor Using staresmonadm

Use the `staresmonadm` utility to configure the resource monitor (Resmon).

### Prerequisites

- The Services Daemon must be running to use `staresmonadm`.  
See [Services Daemon - Stop, Restart, or Show Status](#).
- The Oracle user path must be correctly configured.  
See [Configure the Correct Oracle User Path](#).

### Parameters

The `staresmonadm` utility uses the parameters listed in the table below. To enable, you must specify all required parameters. You can submit as many parameters as you want in each `staresmonadm` command line. The utility only updates the parameters you specify. The unspecified parameters remain at their current value.

Some settings (denoted by \* in the table) require you to stop and restart the Services Daemon if you want the setting to take effect immediately. Otherwise these changes take effect as soon as the backup service wakes from its current sleep interval. See [Services Daemon - Stop, Restart, or Show Status](#).

A value of "-1" indicates the parameter is not configured.

**Table 4–2 staresmonadm Parameters**

| Name                          | Parameter         | Description                                                                                                                                                                                                                                                                                                                                       | Default Value |
|-------------------------------|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| Query                         | -Q, --query       | Display the current Resmon settings.                                                                                                                                                                                                                                                                                                              | None          |
| Clear                         | -C, --clear       | Clear all Resmon settings and disable the service.                                                                                                                                                                                                                                                                                                | None          |
| Verbose                       | -v,<br>--verbose  | Enables verbose mode, which displays detailed progress information for the command.                                                                                                                                                                                                                                                               | None          |
| Help                          | -h, --help        | Displays complete syntax information for the command.                                                                                                                                                                                                                                                                                             | None          |
| Daily report time (required)  | -T, --time        | Time of day Resmon sends the Resource Report. Format is hh:mm, using 24-hour time.<br><br>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.                                                                                       | 00:00         |
| Scan Interval* (required)     | -i,<br>--interval | Time in seconds Resmon waits between scans. Valid entries: integers greater than 0.                                                                                                                                                                                                                                                               | 300           |
| Alert nagging*                | -n, --nag         | 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.<br><br>When enabled, Resmon sends alert reports whenever it performs a periodic scan and detects a resource has exceeded its high-water mark (as opposed to just sending during the daily report). | off           |
| Database username* (required) | -U, --dbusr       | Database username that the Resmon service uses to perform queries against the <code>information_schema</code> tables and the MySQL server internal system global variables.<br><br>This must be a user with full access to the STA database, either the STA database root user or the STA database administrator.                                 | blank         |
| Database password* (required) | -P, --dbpwd       | Password assigned to the database username.                                                                                                                                                                                                                                                                                                       | blank         |

**Table 4–2 (Cont.) staresmonadm Parameters**

| Name                                 | Parameter           | Description                                                                                                                                                                                                                                                                                          | Default Value                 |
|--------------------------------------|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|
| Database tablespace HWM* (required)  | -t,<br>--tblsphwm   | High-water mark for the database tablespace, entered as a percentage of the total allocated. Valid entries: integers 0–100<br><br>Oracle recommends that usage never exceeds 80 percent.                                                                                                             | -1                            |
| Local backup HWM* (required)         | -b,<br>--backvolhwm | 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<br><br>Oracle recommends that usage never exceeds 80 percent.                                                                      | -1                            |
| Database disk volume HWM* (required) | -d,<br>--dbvolhwm   | 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<br><br>Oracle recommends that usage never exceeds 80 percent.                                                                               | -1                            |
| Logging disk volume HWM* (required)  | -l,<br>--logvolhwm  | 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<br><br>Oracle recommends that usage never exceeds 80 percent.                                                                              | -1                            |
| Root volume HWM* (required)          | -z,<br>--rootvolhwm | High-water mark for the root volume (/), entered as a percentage of the total allocated. Valid entries: integers 0–100<br><br>Oracle recommends that usage never exceeds 80 percent.                                                                                                                 | -1                            |
| Tmp volume HWM* (required)           | -x,<br>--tmpvolhwm  | High-water mark for the temporary directory volume (default is /tmp), entered as a percentage of the total allocated. Valid entries: integers 0–100<br><br>Oracle recommends that usage never exceeds 80 percent.                                                                                    | -1                            |
| Physical memory (RAM) HWM*           | -m,<br>--memhwm     | High-water mark for the total system memory (except virtual memory), entered as a percentage of the total allocated. Valid entries: integers 0–100<br><br>Oracle recommends that usage never exceeds 80 percent.                                                                                     | -1                            |
| Email from*                          | -f, --from          | Name or email address that appears in the "From" field of emails sent by the Resmon service.                                                                                                                                                                                                         | StaResMon@localhost           |
| Email recipients* (required)         | -r,<br>--recips     | Email addresses to which Resmon sends the daily Resource Report and periodic Resource Depletion Alert Report. Entered as a colon-delimited list (such as .                                                                                                                                           | blank                         |
| Email subject*                       | -s,<br>--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.<br><br>A time stamp in yyyy-mm-dd hh:mm:ss form is appended to your entry when the email is sent. | STA Resource Monitor Report   |
| Output data file                     | -o,<br>--outfile    | Absolute path of the Resource Report data file. The file name must end in .csv. The database user must have privileges to the directory.                                                                                                                                                             | /var/log/tbi/db/staresmon.csv |

## Display Current Resmon Settings

Display the current settings for the Resmon service to determine if it is enabled.

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

```
$ staresmonadm -Q
```

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 [stadb]
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

Enable the Resmon service by defining required parameters. The Resmon service is disabled by default. Once enabled, the service scans the monitored resources on the STA server according to the defined settings.

1. On the STA server, open a terminal session. Log in as the Oracle user.
2. To enable the service, define the required parameters in one or more commands.

For a list of all parameters, see the table in [Configure the Resource Monitor Using staresmonadm](#).

You must define at least the following settings:

- All high-water marks, except system memory
- Email 'To:'
- Daily report send time
- Sleep Interval
- DB Username and Password—this is the database administrator user created during STA installation.

For example:

```
$ 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 stadb -P
```

3. Resmon will run its first scan at the time you have specified; you do not have to stop and restart the STA services daemon.
4. If the utility fails with:

```
Error: java.util.prefs.BackingStoreException: Couldn't get file lock.
```

See [ISSUE: Backup Service or Resource Monitor Fails](#).

## Disable the Resmon Service

Disable the Resmon service by clearing all settings. 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 Oracle user.
2. Clear all Resmon settings.  

```
$ staresmonadm -C
```
3. The service is disabled immediately; you do not have to stop and restart the STA services daemon.
4. If the utility fails with:  

```
Error: java.util.prefs.BackingStoreException: Couldn't get file lock.
```

  
See [ISSUE: Backup Service or Resource Monitor Fails](#).

## Define Resmon Email Settings

Define email addresses to receive the daily Resource Report and periodic Resource Depletion Report. 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. On the STA server, open a terminal session. Log in as the Oracle 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.

```
$ staresmonadm -r charlie@mycompany.com:lucy@mycompany.com -f
STAResmon@staserver.mycompany.com -s "STA Resource Monitor Report for
staserver"
```

3. If you want the new settings to take effect immediately, you must stop and restart the STA services daemon. See [Services Daemon - Stop, Restart, or Show Status](#).
4. If the utility fails with:  

```
Error: java.util.prefs.BackingStoreException: Couldn't get file lock.
```

  
See [ISSUE: Backup Service or Resource Monitor Fails](#).

## Troubleshoot Resmon Email Issues

If you are not receiving emails from Resmon, use the logs to verify that the service is sending emails, check your email server and filter settings, and verify the Resmon settings are correct.

### Check the staservd.log

If Resmon has sent out an email, it will be recorded in the log.

1. Open the `staservd.log` located in the `/var/log/tbi/db/backups` directory.
2. Look for the following messages:

```
INFO: {StaResMon} Alert report email complete.
```

```
INFO: {StaResMon} Standard report email complete.
```

3. If you see either of the above messages, the Resmon service is sending emails. This means the issue may be with your email server or email filtering.

If you don't see the above messages in the log, Resmon has not sent an email. Verify the Resmon settings are correct.

### Check your email settings

The email service on your server may not be configured correctly or some email security features may be filtering out the Resmon emails. Make sure the "From" line has a legitimate host name. Use the `staresmonadm -f` command to modify.

### Check the Resmon settings

If you did not see either of the logging message above and you are sure that Resmon should have sent an email based on the report time settings and alert settings, then verify the Resmon settings are correct. Use the `staresmonadm -Q` command to view the current settings. Make sure the DB username and password are set correctly for the STA DB mysql application.

## Define Resource Report Settings

Change the time of day when Resmon sends the Resource Report, the report file name, and location of the report file. If you specify a new file name, and the file does not already exist, the Resmon service creates it with the next scan.

1. On the STA server, open a terminal session. Log in as the Oracle 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 file name extension must be `.csv`.

For example:

```
$ staresmonadm -T 23:59 -o /var/log/tbi/db/ResmonReport.csv
```

3. If you want the new settings to take effect immediately, you must stop and restart the STA services daemon. See [Services Daemon - Stop, Restart, or Show Status](#).





---

---

## Password Change Utility

Starting with STA version 2.3.0, you must use the Password Change Utility to alter the passwords for the Weblogic administrator, STA administrator, and database accounts.

- [Username and Password Requirements](#)
- [Change a Password with the Utility](#)

**See Also:**

- *STA User's Guide* — To create and manage regular usernames for logging in to the STA GUI application.
- *STA Installation and Configuration Guide* — To see a description of the users created during the STA installation

### Username and Password Requirements

The STA administration and database accounts must meet minimum requirements.

**Usernames**

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

**Passwords**

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

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

### Change a Password with the Utility

Use the Password Change Utility to alter the password of administration and database accounts.

---

---

**Caution:** Starting with STA 2.3.0, you must use the utility to change passwords for the STA application, database, and WebLogic console. Do *not* use the WebLogic Administration console as it will result in password mismatches, and you will need to reinstall STA.

---

---

### Prerequisites

- STA version 2.3.0 or above
- You must be logged in as the system root user.
- The STA application must be running. See [Display the Status of the STA Application](#) to verify.
- You must know the Weblogic administrator username and password.
- You must know the username and current password of the accounts you are updating.
- If you are changing a database account password, you must also know the current STA database root account password.
- The Oracle user path must be correctly configured. See [Configure the Correct Oracle User Path](#).

### Procedure

1. Verify all prerequisites listed above.
2. The utility will stop and restart all STA processes to implement the new passwords. Therefore, you should back up the STA database before using the utility.
3. On the STA server, open a terminal session. Log in as the Oracle user.
4. Verify that the STA application is running:

```
$ STA status all
```

It may take a few minutes. Once complete, you should see:

```
stai service is running
```

```
... and the deployed application for stai is in an ACTIVE state
```

If the application is not running, restart it. See [Restart the STA Application](#).

5. Start the Password Change Utility.

```
$ changeSTAPasswords.sh
```

6. At the prompts, enter the WebLogic administrator username and password.

```
Enter WebLogic Administrator username : weblogic
```

```
Enter current WebLogic Administrator password :
```

7. The utility main menu appears.

```
Select password to change
```

- 1) All STA Account passwords
- 2) WebLogic Administrator password
- 3) STA Administrator password
- 4) STA Database Root User password
- 5) STA Database Application User password
- 6) STA Database Reports User password
- 7) STA Database Administrator password
- 8) Exit

8. Select an option and follow the prompts to change the password of the user.

If changing All STA Account passwords, review [What Occurs If a Password Update Fails When Changing All Passwords](#).

---



---

**Caution:** Always record and track password changes in a secure location. There is no way to recover a forgotten password.

---



---

9. The utility updates the passwords in the WebLogic server and the MySQL database.

```
Connecting to MySQL and updating STA Database Administrator password
.STA Backup Service does not exist.
.Updating DBA password for STA backup service.
STA Resource Monitor Service does not exist.
```

```
Password change successful. ...
```

10. The utility restarts the STA application and all associated services. This may take several minutes. When the process is done, press Enter to return to the utility Main Menu.

```
Restarting all STA services. This operation may take up to 20 minutes.
.....Press [ENTER] to return to Main Menu
```

11. **IMPORTANT:** If you changed the STA Database Administrator password, you must update the Resource Monitor and Backup Services with the new password. Then, stop and restart the Services Daemon.

## What Occurs If a Password Update Fails When Changing All Passwords

If a password update fails, the utility does not modify the affected account and exits the change operation. However, all earlier password changes remain and do not revert back.

The change All STA Account Passwords operation breaks the password change into six transactions, one for each account: Weblogic user, STA administrator, database root, STA application user, STA report user, and STA database administrator. In total, you will enter about 20 passwords, including the current passwords for each account and the new passwords which you will enter twice to ensure they are not mis-typed. You should carefully enter all passwords. The update operation will fail if you incorrectly enter an existing password, and the utility does not always allow you to correct a mistake. When the failure occurs, the utility does not modify the affected account and exits the password change operation. However, it does update any earlier password changes that you made before the failure.

If a failure occurs while updating all password, you should verify which passwords were changed and track the password changes in a secure location. There is no way to recover a forgotten password.

## Updates Made by the Password Change Utility

When you have finished specifying new passwords, the utility makes specific updates to the applications.

The utility:

- Synchronizes the new passwords between the WebLogic server, MySQL database, and STA application, as applicable.
- Stops and restarts all STA processes. Some library transactions will be lost during this process.

- If you changed the STA database administrator password, the utility does not automatically update the Backup Service and Resource Monitor Service with the new password. You must update the services with the new password and then restart the Services Daemon.

## Password Change Utility Logs

The STA Password Change Utility logs track all updates made by the utility. The logs can be useful for troubleshooting issues with the STA utility or the accounts themselves.

The logs are located in the following directory:

```
/var/log/tbi/changeutility
```

Following is a sample directory listing showing the files.

```
$ ls -l /var/log/tbi/changeutility
-rw-r--r-- 1 oracle oinstall 126 Feb 22 09:44 STChangeUtility-0.log
```

The log records when the STA Password Change Utility is used. For each 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*.

---

---

## Port Change Utility

Starting with STA 2.3.0, you can use the Port Change Utility to configure external and internal port numbers. For releases before 2.3.0, you must deinstall and reinstall STA to make any changes to port numbers.

- [Unconfigurable Ports](#)
- [Configurable Ports](#)
- [Ports for Communications with SDP \(optional\)](#)
- [Change Ports Using the Utility](#)

### Unconfigurable Ports

Some port values are fixed and cannot be changed during STA installation or after.

The firewall must allow communication between the STA server and the backup server (for SSH), and between the STA server and the monitored libraries (for SNMP and SNMPTRAP).

| Port | Protocol | Description                                                                                                                    |
|------|----------|--------------------------------------------------------------------------------------------------------------------------------|
| 22   | SSH      | Secure Shell. STA database backup; library log-in.                                                                             |
| 161  | SNMP     | Simple Network Management Protocol (SNMP). For transmittal of SNMP requests.                                                   |
| 162  | SNMPTRAP | For reception of SNMP notifications (traps). Traps are forwarded to configurable unprivileged internal port (default is 7027). |

### Configurable Ports

Configurable ports are initially defined during STA installation, but can be changed using the Port Change Utility. The utility automatically verifies that the new ports are not already in use on the network and updates all appropriate processes on the STA server to use the new ports.

---

---

**Note:** See your network administrator for assistance with port number assignments. Although it is permissible to have two different processes assigned to the same port number if they use different protocols, this practice is not recommended.

---

---

**External Ports**

These ports are the configurable equivalent of standard ports 80 and 8080 (HTTP) and 443 (HTTPS), and they must be unique from other HTTP and HTTPS ports on the network. The firewall must allow communication between the STA server and the client running the STA GUI.

| Default Port | Protocol | Description                                             |
|--------------|----------|---------------------------------------------------------|
| 7019         | HTTP     | Access to the WebLogic Administration console, unsecure |
| 7020         | HTTPS    | Access to the WebLogic Administration console, secure   |
| 7021         | HTTP     | staUi managed server. Access to the STA GUI, unsecure.  |
| 7022         | HTTPS    | staUi managed server. Access to the STA GUI, secure.    |

**Internal Ports**

| Default Port | Protocol | Description                                                                            |
|--------------|----------|----------------------------------------------------------------------------------------|
| 7023         | HTTP     | staEngine managed server. Basic STA internals, unsecure.                               |
| 7024         | HTTPS    | staEngine managed server. Basic STA internals, secure.                                 |
| 7025         | HTTP     | staAdapter managed server. SNMP communication, unsecure.                               |
| 7026         | HTTPS    | staAdapter managed server. SNMP communication, secure.                                 |
| 7027         | SNMPTRAP | Internal unprivileged port for SNMP traps forwarded from external privileged port 162. |

**Ports for Communications with SDP (optional)**

STA 2.3.0 and above supports optional automatic creation of service log bundles and forwarding of the bundles to StorageTek Service Delivery Platform (SDP). Communication with SDP requires specific port configuration.

See the following documents for details about these optional features:

- *STA User's Guide* for information on configuring and using these features in STA.
- *StorageTek Service Delivery Platform User's Guide* for information on configuring and using these features on the SDP host.

The table below summarizes the ports on the STA server that are used for communications with the SDP host.

**Table 6–1 Ports for Communications With StorageTek SDP**

| Port           | Protocol | Description/Purpose                                                                                                                                                                |
|----------------|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 7023 (default) | HTTP     | Inbound communications from the SDP host to STA. Messages from SDP come in on the unsecure port assigned to the staEngine managed server. See <a href="#">Configurable Ports</a> . |
| 7024 (default) | HTTPS    | Inbound communications from the SDP host to STA. Messages from SDP come in on the secure port assigned to the staEngine managed server. See <a href="#">Configurable Ports</a> .   |

**Table 6–1 (Cont.) Ports for Communications With StorageTek SDP**

| Port               | Protocol | Description/Purpose                                                                                                                                                                                                                                                                                                                                      |
|--------------------|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 15000<br>(default) | Java RMI | Outbound communications from STA to the SDP host. This port number is assigned when the SDP host is configured in STA. See the <i>STA User's Guide</i> for instructions.<br><br>The same port number must be configured on the SDP host to receive messages from STA. See the <i>StorageTek Service Delivery Platform User's Guide</i> for instructions. |

## Change Ports Using the Utility

Use the Port Change Utility to alter the configurable external and internal ports used by STA.

### Prerequisites

- STA version 2.3.0 or above
- You must be logged in as the Oracle user.
- The STA application and all STA services must be running.  
See [Display the Status of the STA Application](#) to verify.
- You must know the Weblogic administrator username and password.
- STA port numbers must be unique and dedicated to the specified STA process. To prevent port conflicts, you should verify that the port numbers you want to use are not already registered or in use by another process on the STA server.
- The Oracle user path must be correctly configured.  
See [Configure the Correct Oracle User Path](#).

### Procedures

1. Verify all prerequisites listed above.
2. The utility will stop and restart all STA processes to implement the new ports. Therefore, you should back up the STA database before using the utility.
3. On the STA server, open a terminal session. Log in as the Oracle user.
4. Verify that the STA application is running:

```
$ STA status all
```

It may take a few minutes. Once complete, you should see:

```
stai service is running
```

```
.... and the deployed application for stai is in an ACTIVE state
```

If the application is not running, restart it. See [Restart the STA Application](#).

5. Start the Port Change Utility.

```
$ changeSTAPorts.sh
```

6. At the prompts, enter the WebLogic administrator username and password.

```
Enter WebLogic Administrator username : weblogic
```

```
Enter current WebLogic Administrator password :
```

7. The utility main menu appears.

Select port numbers to change

- 1) WebLogic Administrator console port numbers
- 2) STA Engine port numbers
- 3) STA Adapter port numbers
- 4) STA UI port numbers
- 5) SNMP Trap Port Number
- 6) Exit

8. Select an option and follow the prompts to update the ports. See [Configurable Ports](#) for default values.
9. Once you confirm the change, the utility automatically restarts the WebLogic server and all STA managed servers, and then stops and restarts all STA processes. Some library transactions may not be recorded during this process.

## Port Change Utility Logs

The logs for the Port Change Utility track all updates made by the utility. You can use the logs to help troubleshoot issues with the utility or the ports.

The logs are located in the following directory:

```
/var/log/tbi/changeutility
```

The following is a sample directory listing showing the files.

```
$ ls -l /var/log/tbi/changeutility
-rw-r--r-- 1 oracle oinstall 126 Feb 22 09:44 STChangeUtility-0.log
```

There may be up to 10 different log files in the directory, each with a sequential number, 0 to 9. 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. Any existing log "9" is overwritten by log "8".



---

---

## Troubleshooting

Resolve issues with accessing the GUI, exchanges not showing up, SDP connection issues, or server processes not starting.

- [ISSUE: Cannot Access the STA GUI](#)
- [ISSUE: Exchanges Not Showing Up in STA](#)
- [ISSUE: SNMP Library Connection Test Fails](#)
- [ISSUE: Cannot Connect to SDP](#)
- [ISSUE: Weblogic Server Processes Not Starting](#)
- [ISSUE: Authentication Prompts During STA start Command](#)
- [ISSUE: Backup Service or Resource Monitor Fails](#)

### ISSUE: Cannot Access the STA GUI

If you cannot access the STA GUI, first verify STA is running. Then, verify the firewall settings and iptables.

#### Resolution

1. Verify STA is running by using the command:

```
STA status all
```

2. Verify you are using the correct URL:

```
http://<server name or IP address>:7021/STA
```

OR

```
https://<server name or IP address>:7022/STA
```

Ports 7021 and 7022 are the default installer port numbers. If you customized or changed the port numbers, use the corresponding custom port numbers instead.

3. If STA is running and you still cannot access the GUI, verify the following firewall settings:
  - Firewall is running
  - Check `hosts.allow` and `hosts.deny` files if using those OS services
  - REJECT rules are not interfering with the GUI ports (such as 162 and 7029)

To verify, open a terminal session and login as the root user. Issue the following:

- **For Linux 6 servers:**

```
service iptables status
iptables -L
```

- **For Linux 7 servers:**

```
systemctl status iptables
iptables -L
```

4. If needed, use the iptables command to remove or modify the firewall rules to allow access to the STA GUI. For example:

```
iptables -D INPUT 5
```

---

---

**WARNING: Removing or modifying firewall rules can create security risks and must be done by qualified security administrator.**

---

---

5. If the GUI was inaccessible after a server reboot occurred, verify the iptables:
  - a. Verify iptables rules were been saved correctly using the service iptables save command.

```
service iptables save
```

- b. **For Linux 6 servers:**

Verify the run levels for the iptables are correct. For example

```
chkconfig --list iptables
iptables 0:off 1:off 2:off 3:off 4:on 5:on
```

- c. **For Linux 7 servers:**

Verify the iptables server is enabled. For example

```
systemctl status iptables
systemctl start iptables
systemctl enable iptables
```

## ISSUE: Exchanges Not Showing Up in STA


If exchanges are not showing up within STA, the SNMP traps from the library may not be reaching STA. You should verify the SNMP configuration and verify the iptables.

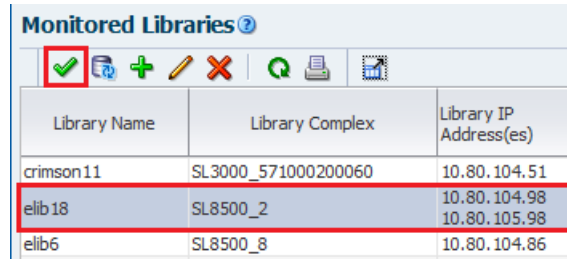
### Verify STA is Running

1. Open a terminal session on the STA server, and login in as the Oracle user.
2. Verify STA is running by using the command:

```
$ STA status all
```

### Test the SNMP Connection

1. Sign in to the STA GUI. In the left navigation, expand **Setup & Administration**, then click **SNMP Connections** (under the Configuration section).
2. Within the Monitored Libraries table, select the library in question and click **Test Connection** .



| Library Name | Library Complex     | Library IP Address(es)       |
|--------------|---------------------|------------------------------|
| crimson11    | SL3000_571000200060 | 10.80.104.51                 |
| elib18       | SL8500_2            | 10.80.104.98<br>10.80.105.98 |
| elib6        | SL8500_8            | 10.80.104.86                 |

If the MIB Walk or Trap Channel tests **FAIL**, see the following sections in the Installation and Configuration Guide "Configure SNMP" chapter:

- "Troubleshoot a Failed MIB Walk Channel Test"
- "Troubleshoot a Failed Trap Channel Test"
- If these do not correct the issue, proceed to [Verify Network Configuration](#).

If the tests **PASS**, proceed to [Verify iptables Configuration](#).

### Verify Network Configuration

1. If STA is running but the connection test fails, verify the following:
  - Firewall is running (also known as iptables)
  - hosts.allow and hosts.deny files (if using those services). You may need to add the library IP address to hosts.allow.
  - REJECT rules do not interfere with the GUI ports (for example 162 and 7029)
  - Port forwarding from 162 to 7029 (port 7029 may be different if you have customized it)
  - Network router configuration between the STA server and library. Some routers may drop UDP or SNMP packets.

To verify STA server settings, login as the root user and use the following commands:

- **For Linux 6 servers:**

```
service iptables status
more /etc/hosts.allow
```

- **For Linux 7 servers:**

```
systemctl status iptables
more /etc/hosts.allow
iptables -L
iptables -L -t nat
Chain PREROUTING (policy ACCEPT)
target prot opt source destination
REDIRECT udp -- anywhere anywhere udp dpt:snmptrap redir ports 7027
```

2. If needed, use the iptables command to add port forwarding or remove and modify the rules to all SNMP traps.

### Verify iptables Configuration

A server reboot can cause an issue with the iptable configuration. If the issue occurred following a reboot, verify the iptables are correct.

1. Use service iptables save command to verify the iptables rules are saved correctly.

```
service iptables save
```

## 2. For Linux 6 servers:

Verify the run levels for the iptables are correct. For example

```
chkconfig --list iptables
iptables 0:off 1:off 2:off 3:off 4:on 5:on
```

## 3. For Linux 7 or 8 servers:

Verify the iptables server is enabled. For example

```
systemctl status iptables
systemctl start iptables
systemctl enable iptables
```

## ISSUE: SNMP Library Connection Test Fails

The SNMP library connection test may fail for multiple reasons. Refer to [ISSUE: Exchanges Not Showing Up in STA](#) for details on how to troubleshoot this issue.

## ISSUE: Cannot Connect to SDP

STA may not be able to connect to SDP due to a hostname mismatch. Adding an entry to the `/etc/hosts` file on the STA server can resolve this issue.

### Symptom

SDP status within the STA GUI indicates "Unable to contact or connect to SDP host".

This can occur if the SDP server hostname defined on the public name servers does not match the hostname sent within the ASR packets. For example, the SDP server sends an ASR packet with its name as "sdp2host" but the name defined on the public name servers is "sdp2server.mycompany.com".

### Resolution

Define the SDP host in the `/etc/hosts` file on the STA server. Add an entry with the IP address of the SDP server and the hostname that the SDP server provides in the ASR packets. For example, "10.20.30.40 sdp2host".

## ISSUE: Weblogic Server Processes Not Starting

After a server reboot or non-graceful shutdown of STA, one of the Weblogic server processes like (staAdapter, staEngine, staUi, AdminServer) may not start. This can be caused by a Weblogic lock file (.lck) that was not properly removed during shutdown.

### Resolution

1. Open a terminal session on the STA server and login as the Oracle user.
2. Examine the Weblogic log files for the services that have not started. Look for errors or the presence of a .lck file.

The log files are located in:

```
TBI/servers/AdminServer/logs/weblogic.log
TBI/servers/staAdapter/logs/weblogic_staAdapter.log
TBI/servers/staUi/logs/weblogic_staUi.log
TBI/servers/staEngine/logs/weblogic_staEngine.log
```

3. Use the `rm -f` command to remove the lock file for the STA server process that has not started.
4. Restart STA using the command:

```
$ STA start all
```

## ISSUE: Authentication Prompts During STA start Command

When using Linux 7 or 8, you may see an authentication message after using the STA start command. The message should time out and the STA service should start. Or the server administrator can add polkit rules to remove the authentication requests.

### Symptom

While using the STA start command the following authentication messages appear:

```
Starting stawebllogic Service.==== AUTHENTICATING FOR
org.freedesktop.systemd1.manage-units ==
Authentication is required to manage system services or units.
Authenticating as: root
```

### Resolution

The OS polkit service running on the server generates this message. Depending on the server configuration this authentication prompt (password prompt) will time out and STA services will start normally.

If the authenticate does interfere with STA service starting, then contact your server administrator. The administrator can add polkit rules to remove the authentication requests in the following location:

```
/usr/share/polkit-1/rules.d/org.freedesktop.systemd1.manage-units.rules
```

---



---

**WARNING: Modifying polkit rules can create security risks and must be done by qualified security administrator.**

---



---

## ISSUE: Backup Service or Resource Monitor Fails

The Backup Service or Resource Monitor may fail if the Oracle user does not have write access to `/etc/.java` or `staservd` does not have write access to `/etc/.java/.systemPrefs`.

### Symptom

The service fails with the following:

```
Error: java.util.prefs.BackingStoreException: Couldn't get file lock.
```

### Resolution

1. Open a terminal session on the STA server and login as the root user.
2. Provide write access to the `/etc/.java` and `/etc/.java/.systemPrefs` directories. For example:

```
chmod 777 /etc/.java
chmod 777 /etc/.java/.systemPrefs
```

3. Switch to the Oracle user.
4. Stop the services daemon:

```
$ STA stop staservd
$ STA status staservd
```

You should see:  
staservd service is shutdown

5. Start the services daemon:  
\$ **STA start staservd**

---

---

## Prevent Denial-of-Service Attacks

Use a script to configure input rules for the iptables service to watch for and prevent Denial-of-Service (DoS) on STA.

---

---

**Note:** This procedure is optional and is provided as information only. Site security must be handled by a qualified security administrator.

---

---

The script defines input rules for the iptables service 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

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. Configure and verify the library connections on STA. See the *STA Installation and Configuration Guide* for details on testing the SNMP connection.
2. Log in to the STA server as the system root user.
3. Copy the contents of the following script example into a text editor.

```
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

```

4. 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.
5. Save the script and execute it. The new rules are added to the iptables service and take effect immediately.
6. Verify that STA is still successfully monitoring your libraries.