StorageTek Tape Analytics

Security Guide

Release 2.3.1

F30299-01

June 2020

ORACLE

StorageTek Tape Analytics Security Guide, Release 2.3.1

F30299-01

Contents

Preface

This document describes the security features of Oracle's StorageTek Tape Analytics (STA) version 2.3.1.

For an overview of the product, refer to the *STA User's Guide*.

Audience

This guide is intended for anyone involved with the secure installation and configuration of STA version 2.3.1.

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*

1

Secure Installation and Configuration

Plan for a secure installation and follow recommended deployment guidelines when applicable.

General Aspects of Security

The main aspects to STA security are: physical, network, user access, and server access.

Physical

STA must be installed on a standalone server within an organization's data center. Physical access to the server would be dictated by the customer company policy.

Network

It is required that STA be added or configured to a customer internal firewall-protected network. This network needs SSH and SNMPv3 access to libraries for which data will be accessed.

To use the user interface, you need HTTPS access.

To enable optional log bundle forwarding to StorageTek Service Delivery Platform (SDP), a connection to the SDP host is also required within the customer internal firewall-protected network.

User Access

The STA application access is controlled by user name and password authentication. User names and passwords are set up during initial installation by the customer. Passwords must meet Oracle standard requirements.

Server Access

STA requires an OS level Oracle user for installation and runtime access.

You should limit the access to the server, especially super users (root), which could affect the STA application, functionality, and services.

General Security Principles

Follow fundamental principles to securely use the STA application.

Keep Software Up To Date

One of the principles of good security practice is to keep all software versions and patches up to date. This document is for STA version 2.3.1.

> **Note:** The libraries and drives must also meet minimum firmware version levels that are connected to the STA application. These firmware levels are specified in the "Requirements" section of the *Installation and Configuration Guide*.

To enable the best security available, Oracle recommends keeping the OS and all application components (like Weblogic, ADF, Java, and so on) up to date with the latest security patches. Oracle periodically provides security patches for components (like Weblogic, ADF, MySQL and Java) through the Oracle CPU (Critical Patch Update) advisories and other communications.

Because OS security patches are independent of the STA application, Oracle cannot guarantee that all patches will operate correctly with STA—especially patches released after an STA release. Determine the acceptable OS security patch level for your environment. Because of component patch and application interdependencies, Oracle cannot guarantee that all component patches will operate correctly with the STA application. Determine which component patches are needed for your environment and what affects it may have on the STA application.

Newer STA versions and STA specific patches may also be available. Check with Oracle service on the availability of a newer version of STA or an STA specific patch. Newer STA versions will contain more up to date security patches.

> **WARNING: Oracle strongly recommends using only trusted sites. Validate the source of all software downloads and patches to ensure that they do not contain any security vulnerabilities like malware, viruses, worms, and so on.**

Restrict Network Access

Oracle recommends that you keep the STA host server behind a data center firewall. The firewall restricts access to these systems to a known network route, which can be monitored and restricted, if necessary. As an alternative, a firewall router substitutes for multiple, independent firewalls. Identifying the hosts allowed to attach to the library and blocking all other hosts is recommended where possible. STA is not designed to be directly accessible from a public network.

Keep Up To Date on Latest Security Information

Oracle continually improves its software and documentation. For every STA release review the document for revisions. Specific security concerns may be addressed in release notes as well.

Understand Your Environment

Address key questions about your environment to better understand your security needs.

Which resources need to be protected?

For STA, the host server and the associated network must be protected from unauthorized access.

From whom are the resources being protected?

STA must be protected from everyone on the Internet, external users, and unauthorized internal users. You should ensure that you have intrusion protection and monitoring software.

What will happen if the protection on strategic resources fail?

As STA is a device monitoring and usage application, unauthorized access to STA will only affect STA. The monitored devices and associated data will not be affected.

Installing StorageTek Tape Analytics (STA)

Refer to the *Installation and Configuration Guide* for installation instructions.

Only install STA on a system that is within the same protected (firewalled) network infrastructure as the monitored libraries. You should enforce customer access controls on the systems where STA is installed to restrict access to the application.

The STA installer may modify permissions on some files and directories to allow the STA application running as Oracle user access to certain files. For example: /etc/.java.

Firewall Port Assignment

The firewall must allow communication on the ports used by the STA application. For a list of ports, see the following sections in the *Administration Guide*:

- "Configurable Ports"
- "Unconfigurable Ports"
- "Ports for Communications with SDP"

Firewall Configuration

Firewall configuration is dependant on the OS version. Review the configuration of the iptables and troubleshooting sections as needed.

- "Enable the Linux Firewall iptables" in the *Installation and Configuration Guide*
- "Troubleshooting" appendix in the *Administration Guide*

Post Installation Configuration

There are no post-installation configuration security changes. The installation process has you configure administration accounts, passwords, and ports. If necessary after installation, you can use the Password Change Utility to update passwords or the Port Change Utility to alter ports.

User (admin) Password Configuration

The installation process has you configure the administration account and password. You can use the Password Change Utility to update administration and database accounts after the installation. See the *Administration Guide* for more information.

Enforce Password Management

STA enforces minimum requirements on all passwords. You should always apply password management rules such as password length, history, and complexity to the all passwords. Oracle recommends periodically changing passwords to maximize security.

Port Assignment

The installation process has you configure port numbers. You can use the Port Change Utility to update the configurable ports after the installation. See the *Administration Guide* for more information.

Security Features

STA encrypts passwords and limits access to the application based on role and any external authenticator (such as your company's internal LDAP).

The STA application uses encrypted password roles to protect itself. The application should be in a physically secured data center, which also has a secured network that allows access only to authorized users.

Secure Deployment Checklist

Complete the deployment checklist to help secure your system.

1. Enforce password management.
2. Enforce access controls.
3. Restrict network access.
   a. A firewall should be implemented.
   b. The firewall must not be compromised.
   c. System access should be monitored.
   d. Network IP addresses should be checked.
4. Ensure intrusion monitoring software is installed.
5. Contact your Oracle Services, Oracle Tape Library Engineering, or account representative if you come across vulnerabilities in Oracle hardware and applications.