StorageTek Tape Analytics

Security Guide

Release 2.2

E69782-01

February 2016

ORACLE

StorageTek Tape Analytics Security Guide, Release 2.2

E69782-01

Copyright © 2012, 2016, Oracle and/or its affiliates. All rights reserved.

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

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

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

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

This software or hardware and documentation may provide access to or information 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 v

Audience v
Documentation Accessibility v

1 Overview

Product Overview 1-1
Security 1-1
Physical 1-1
Network 1-1
User Access 1-1
General Security Principles 1-1
Keep Software Up To Date 1-1
Restrict Network Access 1-2
Keep Up To Date on Latest Security Information 1-2

2 Secure Installation

Understand Your Environment 2-1
Which resources need to be protected? 2-1
From whom are the resources being protected? 2-1
What will happen if the protections on strategic resources fail? 2-1
Installing StorageTek Tape Analytics (STA) 2-1
Post Installation Configuration 2-1
Assign the user (admin) password. 2-2
Enforce password management 2-2

3 Security Features

A Secure Deployment Checklist

B References

Related Documents B-1
For users of the STA application B-1
For installers and administrators of the STA server and application B-1

Preface

This document describes the security features of Oracle's StorageTek Tape Analytics (STA) version 2.2 and higher.

Audience

This guide is intended for anyone involved with using security features and secure installation and configuration of STA version 2.2 and higher.

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.

1

Overview

This section gives an overview of StorageTek Tape Analytics (STA) version 2.2 and higher, and explains the general principles of its security.

Product Overview

StorageTek Tape Analytics is an Oracle software product that provides customers with tape business intelligence to efficiently and proactively monitor and manage their data center's tape operations.

STA supports both Enterprise MVS and Open Systems tape customers. The STA solution provides value for low-to-high-end tape market customers.

Security

There are three aspects to STA security: physical, network, and user 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 SNMP access to libraries for which data will be accessed.

User Access

The STA Application access is controlled by username and password authentication. Usernames and passwords are setup during initial installation by the customer. Passwords must meet Oracle standard requirements.

General Security Principles

The following principles are fundamental to using any product securely.

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 the software level of:

STA version 2.2 and higher

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 *STA Requirements Guide*.

To enable the best security available, Oracle recommends keeping OS up to date with the latest security patches. However, 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. You will need to determine the acceptable OS security patch level for your environment.

Restrict Network Access

It is recommended the STA host server is kept behind a data center firewall. The firewall provides assurance that access to these systems is restricted 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 (Internet) network.

Keep Up To Date on Latest Security Information

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

2

Secure Installation

This section outlines the planning process for a secure installation and describes several recommended deployment topologies for the systems. The *STA Installation and Configuration Guide* and *STA Administration Guide* cover installation, configuration, and administration in detail.

Understand Your Environment

To better understand security needs, the following questions must be asked:

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.

What will happen if the protections 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)

STA should only be installed on systems that are within the same protected (firewalled) network infrastructure as the monitored devices, that is, libraries. Customer access controls should be enforced on the systems where STA is installed to assure restricted access to the application.

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

Post Installation Configuration

There are no post-installation configuration security changes. The configuration is set by the customer during installation.

Assign the user (admin) password.

The customer administration account password is set by the customer during the installation.

Enforce password management

Customer Corporate password management rules such as password length, history, and complexity must be applied to the administrator password.

3

Security Features

This section outlines the specific security mechanisms offered by the product.

The STA application provides user with encrypted password roles to protect itself. This is not the only line of security to protect the application. The application should be in a physically secured data center, which also has a secured network that allows access only to authorized users.

A

Secure Deployment Checklist

The following security checklist includes guidelines that help secure the library:

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. Contact your Oracle Services, Oracle Tape Library Engineering, or account representative if you come across vulnerabilities in Oracle tape drives.

B

References

Tape storage product documentation can be found at the following website:

http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#opensyssoft

Related Documents

The STA documentation set consists of the following documents.

For users of the STA application

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

For installers and administrators of the STA server and application

- *STA Release Notes*—Read this document before installing and using STA. It contains important release information, including known issues. This document is included in the STA media pack download.
- *STA Requirements Guide*—Use this guide to learn about minimum and recommended requirements for using STA. This guide includes the following requirements: library, drive, server, user interface, STA media validation, and IBM RACF access control.
- *STA Installation and Configuration Guide*—Use this guide to plan for installation of STA, install the Linux operating system, install the STA application, and then configure STA to begin monitoring the libraries. This guide also provides instructions for upgrading to a new version of STA.

- *STA Administration Guide*—Use this guide for information about STA server administration tasks, such as STA services configuration, database backup and restore, and password administration for database accounts.
- *STA Security Guide*—Read this document for important STA security information, including requirements, recommendations, and general security principles.
- *STA Licensing Information User Manual*—Read this document for information about use of third-party technology distributed with the STA product.