StorageTek Enterprise Library Software

Security Guide

E61233-01

March 2015

ORACLE

StorageTek Enterprise Library Software Security Guide

E61233-01

Contents

Preface

This document describes the security features of Oracle's StorageTek Enterprise Library Software (ELS).

Audience

This guide is intended for anyone involved with using security features and secure installation and configuration of StorageTek Enterprise Library Software (ELS).

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 ELS software suite and explains the general principles of application security.

Product Overview

ELS provides tape automation support for Oracle StorageTek mainframe tape environments for the following platforms:

- IBM z/OS platform. ELS supports a TCP/IP client/server tape automation architecture allowing the SMC client software running on one z/OS LPAR to communicate with the HSC/VTCS server software running on a different z/OS LPAR.
- IBM z/VM platform. The ELS VM Client software for z/VM systems communicates with the HSC/VTCS server software running on a z/OS LPAR to automate virtual and physical tape processing for z/VM.
- The Fujitsu MSP/EX platform. SMC must execute on every host where tape processing occurs. The ELS server component (HSC/VTCS) may execute on the same MSP/EX host as the SMC, or may execute on a separate, remote host. When SMC and HSC/VTCS reside on different MSP/EX hosts, TCP/IP is used to send requests from the client host to the server host. To receive HTTP requests from a remote SMC client, the HTTP component must be activated on the SMC executing on the server host.

ELS client/server communication is used to issue control path requests, primarily mount/dismount requests, for virtual and physical tape volumes. Information contained in these control path requests consists of TapePlex configuration and policy information, virtual/physical tape transport unit addresses and virtual/physical tape volume serial numbers. Most important, ELS client/server communication never contains any customer data, which always travels over IBM FICON/ESCON data path interfaces connecting host LPARs to Oracle StorageTek tape transports or VSM virtual tape devices.

The information in this Security Guide applies to all ELS releases. As discussed in Part 3 of this guide, it is possible to secure ELS client/server control path communications when such protection is desirable or is required. Additionally, this document discusses security aspects of various ELS installation and post-installation activities.

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. The latest ELS cumulative maintenance bundle, along with individual PTFs and HOLDDATA, are all available on My Oracle Support (MOS). Cumulative maintenance bundles are updated monthly to include all PTFs from the latest ELS monthly regression test cycle. All the PTFs in a cumulative bundle have been tested together as a complete package. HIPER PTF Email notification is available by subscribing to MOS Hot Topics Alert documents for the ELS products. Customers are encouraged to stay on current maintenance levels, keep HOLDDATA up-to-date and subscribe to Hot Topics Alerts for HIPER notifications.

Restrict Network Access

For performance and security, route ELS control path communications over an isolated network behind a firewall. Using a firewall provides assurance that access to ELS systems is limited to a known network, which can be monitored and restricted if necessary. Using a dedicated network for ELS client/server communications eliminates network contention with other applications and improves tape system performance.

Keep Up To Date on Latest Security Information

Oracle continually improves its software and documentation. Check for revisions to this Security Guide and all other ELS product documentation on a regular basis. All of the ELS documentation referenced in this document is available on the Oracle Technical Network in the Tape Storage Products section.

2

Secure Installation

The IBM z/OS System Authorization Facility (SAF) provides essential protection for most security aspects of ELS. SAF is typically implemented with the IBM RACF package or equivalent. This section outlines using a RACF-based SAF environment to install and configure a secure ELS installation.

Installing ELS

The Oracle document *StorageTek Enterprise Library Software: Installing ELS* describes how to install and configure your version of ELS using RACF protection. Refer to this document for more information on following security-related installation topics:

- Installing the base software and the latest cumulative maintenance bundle
- ELS load library APF authorization
- HSC user exit library APF authorization
- SMC JES3 load library APF authorization

ELS Post-Installation Configuration

These Oracle documents describe post-installation configuration tasks for your version of ELS:

- *StorageTek Enterprise Library Software: Configuring HSC and VTCS*
- *StorageTek Enterprise Library Software: Configuring and Managing SMC*
- *StorageTek Enterprise Library Software: ELS Programming Reference*

Refer to these documents for more information on the following security-related post-installation topics:

- Defining RACF protection for CDS data set security
- Defining command authority and programmatic interface authority using HSC user exit SLSUX15
- Defining volume access authority for mounting and ejecting volumes using HSC user exit SLSUX14
- Defining MVC pool and scratch subpool volser authority
- Defining an SMC OMVS RACF segment for communication with a remote HSC subsystem
- Defining an SMC OMVS RACF segment for communication with a VLE appliance

3

Security Features

This chapter describes the specific security mechanisms offered by ELS.

Securing ELS with AT-TLS – z/OS Only

The IBM z/OS Application Transparent Transport Layer Security (AT-TLS) facility uses SSL data encryption to secure z/OS TCP/IP applications. For more information on AT-TLS, refer to the *IBM publication z/OS Communications Server: IP Configuration Guide*, and see information on the AT-TLS Policy Agent information in the *IBM publication z/OS Communications Server: IP Configuration Reference*.

Securing ELS client/server communications between SMC and HSC/VTCS is described in the Oracle white paper *Using AT-TLS with HSC/SMC Client/Server z/OS Solution: Implementation Example*. This white paper is published on the Oracle Technical Network in the Tape Storage Products section. Refer to this publication for detailed configuration information.

To secure ELS with AT-TLS, Oracle recommends using any of these SSL cryptographic algorithms:

- SHA-2 family (SHA-256, SHA-384, SHA-512)
- AES >= 128-bit
- RSA >= 2048-bit
- Diffie-Hellman (DH) >= 2048-bit
- ECC >= 256-bit

Any other SSL cryptographic algorithms provide weaker protection and should not be used with ELS.

Note: The StorageTek Virtual Library Extension (VLE) appliance for VSM does not currently support AT-TLS communications. Do not secure ELS VLE communications with AT-TLS.

Using the ELS XAPI Security Feature

ELS 7.3 introduces a new XAPI security feature for client-server communication, enabled as a default in the SMC HTTP server. The XAPI security feature provides additional user authentication facilities as part of the XAPI protocol that are internal to and wholly contained within ELS. To use the XAPI security feature you must define security credentials (userids and passwords) for ELS clients and servers. ELS 7.3

TapePlex operations use these security credentials to secure XAPI transactions (mount, dismount, volume lookup, scratch, and so on). XAPI security credential usage is completely transparent and requires no additional user or operator intervention. Refer to *Configuring and Managing SMC 7.3* for more information about configuring the XAPI security feature.

The preferred method for securing XAPI transactions for TapePlexes that host ELS client applications only (SMC and VM Client) is to use the AT/TLS facilities as described in the "Securing ELS with AT-TLS – z/OS Only" on page 3-1. AT/TLS is a transport layer facility that is external and transparent to ELS.

Use the ELS 7.3 XAPI security feature to secure TapePlexes that host non-ELS clients (open systems clients) or a mixture of ELS clients (SMC and VM Client) and non-ELS clients. AT-TLS can be used in these environments in addition to the ELS 7.3 XAPI security feature but it will not secure XAPI transactions for non-ELS clients.

4

Security Considerations for Developers

The Oracle document *StorageTek Enterprise Library Software: ELS Programming Reference* describes ELS APIs available to application developers. Programmatic interface to ELS uses the Unified User Interface (UUI), which uses the HSC command security exit SLSUX15 to manage access to its functions based on RACF authorization (or equivalent). See "ELS Post-Installation Configuration" on page 2-1, for more information on securing SLSUX15 with RACF.

A

Secure Deployment Checklist

1. Use RACF protection (or equivalent) as discussed in this Security Guide.
2. Restrict network access. ELS and the tape libraries it manages should be behind the corporate firewall.
3. Secure ELS network traffic with the IBM AT-TLS facility or the ELS XAPI security feature if required.
4. Apply all ELS PTFs and HOLDDATA.
5. Contact Oracle software support at http://www.myoraclesupport.com/ if you encounter vulnerability in Oracle ELS software.

B

References

The ELS documentation is saved in libraries organized by ELS release. Access this from Tape Storage Documentation page.

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