StorageTek SL150 Modular Tape Library

Security Guide

E35113-09

December 2018

ORACLE

StorageTek SL150 Modular Tape Library Security Guide

E35113-09

Contents

Preface

This document describes the security features of Oracle's StorageTek SL150 Modular Tape Library.

Audience

This guide is intended for anyone involved with secure installation and configuration of Oracle's StorageTek SL150 Modular Tape Library and using its security features.

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

Go to the Tape Storage section of the Oracle Help Center (http://docs.oracle.com/en/storage/#tape) for additional SL150 documentation.

1

Security Overview

This section gives an overview of Oracle's StorageTek SL150 Modular Tape Library and explains the general principles of tape library security.

Product Overview

StorageTek SL150 Modular Tape Library is a 19" rack mounted modular automated tape library by Oracle Corporation. It offers storage capacity for LTO tape cartridges, supports LTO Fibre Channel drives or SAS tape drives, and a bridged drive Fibre or SAS port control path through one of the installed tape drives. The SL150 v3.50 release has VPAT #6237 and #7171.

Security

All tape library products are designed and documented for use within a controlled server environment with no general network or user access. This provides the best functionality and protection from compromise, both from the internet in general and from the internal entity operating the library.

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 SL150 Firmware versions released since June 2012 are as follows:

June 2012 v1.00 (RTA 0.1.0.0.0)
September 2012 v1.03 (RTA 0.1.0.3.0)
October 2012 v1.50 (RTA 0.1.5.0.0)
January 2013 v1.82 (RTA 0.1.8.2.0)

August 2013 v2.0 (RTA 0.2.0.0.0)
October 2013 v2.01(RTA 0.2.0.1.0)
April 2014 v2.25 (RTA 0.2.2.5.0)
June 2015 v2.50 (RTA 0.2.5.0.0)
March 2016 v2.60 (RA 0.2.6.0.0)
June 2017 v3.00 (RA 0.3.0.0.0)
November 2018 v3.20 (RA 0.3.2.0.0)
July 2018 v3.50 (RA 0.3.5.0.0)

Restrict Network Access

Keep the library 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.

Keep Up To Date on Latest Security Information

Oracle continually improves its software and documentation. Check this document every release for revisions.

2

Secure Installation

This section outlines the planning process for a secure installation, describes several recommended deployment topologies for the systems, and explains how to secure the library.

Understand Your Environment

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

Which resources need to be protected?

Many resources in the production environment can be protected. Consider the resources needing protection when deciding the level of security that you must provide.

From whom are the resources being protected?

The library must be protected from everyone on the Internet and unauthorized intranet users.

What will happen if the protections on strategic resources fail?

In some cases, a fault in a security scheme is easily detected and considered nothing more than an inconvenience. In other cases, a fault might cause great damage to companies or individual clients that use the library. Understanding the security ramifications of each resource will help protect it properly.

Securing the Library

The following table lists the library ports used by default. The firewall should be configured to allow traffic to use these ports and that any unused ports are blocked.

Table 2–1 SL150 Network Ports

Port	Type	Description
22	TCP	SSH CLI access –inbound stateful For development test and debug only, not available in the field
25	TCP	SMTP without authentication
67	DHCP	client - outbound
68	DHCP	client - inbound
80	HTTP	WebLogic port for remote user interface
123	NTP	Network Time Protocol (if enabled)
161	UDP	SNMP library agent requests - inbound stateful
162	UDP	SNMP library traps and inform notifications - outbound stateless for traps, outbound stateful for inform
465	TCP	SMTP with SSL or TLS authentication
443	HTTPS	WebLogic port for remote user interface for HTTPS
546	DHCPv6	IPv6 DHCP client - outbound
547	DHCPv6	IPv6 DHCP client - inbound
33200-33500	TRACEROUTE	Software development use

Valid port number selection for library use are either reserved or recommended per the above table list. Legitimate port numbers commence at the numeric number 1, as zero is not a legitimate port number.

When configuring SNMP, using SNMPv3 is strongly recommended over SNMPv2c for its confidentiality, integrity, and authentication capabilities.

From within the library User Interface, disable SNMP when not using this feature to further increase security robustness. By default, SNMP is disabled.

When configuring SMTP, using TLS authentication is strongly recommended over both SSL or the no-authentication option.

Installation Configuration

This section documents security configuration changes that must be made during installation.

- Assign the user (admin) password
- Enforce password management

Assign the user (admin) password

At first power-on, a setup wizard automatically runs on the local operator panel to obtain basic configuration information. This includes administrator account username and password, network settings, and other basic settings.

The library is prevented from becoming operational until the setup wizard has been completed.

A login account is provided with the product shipment which the installer must enter as the first step in the setup wizard routine. The user must then enter a new password before the setup wizard will complete.

Once the Initial setup wizard has been completed and the library is fully powered on, additional modifications to the library configuration can be performed through the browser user interface (BUI) for all library settings.

Enforce password management

Basic password management rules, such as password length, history, and complexity must be applied to all passwords. SL150 passwords must be between 8 to 128 characters and contain at least one numeric or special character. The default password must be changed during installation and may not be reused.

Note: The number of characters shown masked are not indicative of the exact number of entered characters.

Browser UI Authentication

Limit the browser settings used to access the remote user interface to remain at TLS 1.0 or higher to mitigate CVE-2014-3566 for firmware levels below version 2.50. The library firmware will not auto-negotiate down to SSLv3 in version 2.50.

With the v2.60 release, the Java and Weblogic components were updated to versions JDK1.6_105 and WLS 10.3.6 PSU 12 to reduce the security vulnerabilities.

With the v3.50 release, the Java and Weblogic components were updated to versions JDK 1.6_181 and WLS 10.3.6 PSU 12 to reduce security vulnerabilities. Weblogic now internally uses TLS 1.2.

Security Features

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

The library provides an internal firewall to protect itself. This should not be the only line of security to protect the library. It is recommended the library is in a physically secured data center on a secured network only allowing access from servers utilizing its functionality. These servers and applications running on them should also be secured.

User accounts should be limited to *operator* role level instead of granting all users the *Admin* role level. Proper use of the *service* user role should be practiced. Create, enable, or disable the *service* user role accounts as needed. Service roles have greater privilege than *operator* to the point of nearly the same authorization as the *admin* role.

If a history of library activity is needed for investigative purposes, the "Activity Log" may be reviewed and exported for further analysis. The Activity Log on the user interface can show user logins, Host or UI initiated actions for traceability.

Redeployment

This section describes how the library is returned to a factory default state to clear any customer data.

In the event the customer needs to decommission a library, a procedure is provided which removes all customer configuration information and all log files, and returns the library to a factory default state. This procedure is invoked by placing the library in a "locate" mode, then simultaneously holding the front and rear locate buttons for more than 10 seconds and then letting go of both the buttons.

Sufficient time in depressing the Locate button is signalled by the change in LED light blinking rate from slow to rapid.

Secure Deployment Checklist

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

1. Enforce password management for all user accounts.
2. Enforce access controls, both physical proximity and through interfaces such as SCSI, UI, SNMP and so on.
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.
   e. Services may have tools that need proper password or access controls monitored (for example, SDP-2 to allow automatic downloading of log information or other access)
4. Contact your Oracle Services, Oracle Tape Library Engineering, or account representative if you come across vulnerability in Oracle Tape Libraries.
5. SMTP should use TLS instead of lesser protocols like SSL or none.
6. SNMP, when enabled, should be set up with V3 level instead of V2C or lesser capabilities.
7. With version 3.50 firmware the library managed encryption (LME) port 2 may be configured to allow a private network to the OKM cluster. Refer to the user documentation for more information on the LME feature.