

StorageTek

Security Guide for SL500, SL3000, and SL8500

E23535-02

October 2013

StorageTek Security Guide for SL500, SL3000, and SL8500

E23535-02

Copyright © 2011, 2013, Oracle and/or its affiliates. All rights reserved.

Primary Author: Robert Creager

Contributing Author:

Contributor:

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, 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 on 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. 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.

Contents

Preface	v
Audience.....	v
Documentation Accessibility	v
1 Overview	
Product Overview.....	1-1
Security.....	1-2
General Security Principles.....	1-2
Keep Software Up To Date	1-2
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
Securing the Library	2-1
Installing Streamline Library Console (SLC) application and the Web Application Archive (WAR) file	2-2
Post Installation Configuration.....	2-2
Assign the user (admin) password.....	2-2
Enforce password management.....	2-2
3 Security Features	
A Secure Deployment Checklist	
B References	

Preface

This document describes the security features of Oracle's StorageTek SL500, SL3000, and SL8500 libraries.

Audience

This guide is intended for anyone involved with using security features and secure installation and configuration of StorageTek SL500, SL3000, and SL8500.

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 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.

Overview

This section gives an overview of the SL500, SL3000, SL8500 libraries and explains the general principles of tape library security.

Product Overview

SL500

SL500 is a 40U 19" rack mounted modular automated tape library by Oracle Corporation. It offers storage capacity of 30 to 500 LTO or SDLT tape cartridges, from 1 to 18 LTO or SDLT SCSI LVD, Fibre, or SAS tape drives, with either a separate SCSI LVD or Fibre Library control path, or a bridged drive Fibre or SAS port control path. A bridged path indicates that the control path is through an HP5 drive port.

SL3000

SL3000 is a tape library, which provides the following features:

- Attachment to both open systems and mainframe environments using HLI over Ethernet, and SCSI over FC
- Economic scalability for both tape drives (1 to 56) and cartridges (200 to 4500) to allow entry level pricing and field upgradeable expansion as the customer data storage needs grow
- Live replacement of redundant components, including power supplies, robotics and electronics
- True mixed media support - any cartridge / any slot

SL8500

SL8500 is an automated tape library, which provides the following features:

- Attachment to both open systems and mainframe environments using HLI over Ethernet with either the ACSLS open systems host or the HSC mainframe host
- Economic scalability for both tape drives (1 to 64) and cartridges (500 to 10,000) to allow entry level pricing and field upgradeable expansion as the customer data storage needs grow
- Live replacement of redundant components, including power supplies, robotics and electronics
- True mixed media support - any cartridge / any slot

Security

All tape library products are designed and documented for use within a controlled server environment with no general network access. This will give 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. Throughout this document, we assume software levels of:

- SL500 1485
- SL3000 4.02
- SL8500 8.31

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 and implementation process for a secure installation and configuration, describes several recommended deployment topologies for the systems, and explains how to secure a tape 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. But should the library be protected from the employees on the intranet in your enterprise?

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 tape drive. Understanding the security ramifications of each resource will help protect it properly.

Securing the Library

By default, the library uses ports listed in the following table. The firewall should be configured to allow traffic to use these ports and that any unused ports are blocked. The SL8500 and SL3000 libraries support IPv4.

Table 2-1 Network ports used

Port	SL500	SL3000	SL8500
22 tcp - SSH CLI and SLC access - inbound stateful	X	X	X
115 tcp - SFTP code download from SLC inbound stateful	X	X	X
161 udp - SNMP library agent requests - inbound stateful	X	X	X

Table 2–1 (Cont.) Network ports used

Port	SL500	SL3000	SL8500
162 udp - SNMP library traps and inform notifications - outbound stateless for traps, outbound stateful for inform	X	X	X
68udp - dhcp client - inbound and outbound	X		
50001-50016 tcp - HLI host access - inbound stateful		X	X
33200-33500 udp - traceroute (CLI debugging of route tables) - outbound stateful		X	X

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

Installing Streamline Library Console (SLC) application and the Web Application Archive (WAR) file

SLC should only be installed on systems that are within the same protected network infrastructure as the library. Customer access controls should be enforced on the systems where SLC is installed to assure restricted access to the library. See [Table 2–1](#) for ports used by SLC

Refer to the following library user guides for web launch SLC install instructions.

- SL500 User Guide
- SL3000 User Guide
- SL8500 User Guide

Post Installation Configuration

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

Assign the user (admin) password.

The customer admin account password is managed by a One Time Password (OTP) infrastructure. There are 280 passwords available for use over the life of the library if the admin password is forgotten and has to be reset. The first OTP is on a label affixed to the frame. Your service representative will use this OTP when installing your library. You can then enter a password of your choice.

Enforce password management

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

3

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. Ideally, the library should be in a physically secured data center that also has a secured network that only allows access from the servers utilizing its functionality. These servers and applications running on them should also be secured.

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 to report suspected vulnerabilities in Oracle tape libraries.

B

References

- SL500 User Guide
- SL3000 User Guide
- SL8500 User Guide

