StorageTek Linear Tape File System, Library Edition

Security Guide

Release 1

E38511-02

July 2016

ORACLE

StorageTek Linear Tape File System, Library Edition Security Guide, Release 1

E38511-02

Contents

Preface

This document describes the security features of Oracle's StorageTek Linear Tape File System, Library Edition (LTFS-LE).

Audience

This guide is intended for anyone involved with using security features and secure installation and configuration of LTFS-LE.

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 LTFS-LE and explains the general principles of its security.

Product Overview

Today, tape storage faces the threat of being relegated entirely into the backup and archive market, even as customers beg for a more cost efficient storage platform that could be used for nearline storage because of perceived usability and performance issues. The pioneering groundwork from StorageTek and Sun engineers to eradicate this attack line from disk vendors finally manifested itself in 2010 with the debut of the Linear Tape File System (LTFS) for single tape drives. First released as an open-source specification by IBM and the LTO consortium, LTFS allows a single drive to be treated like a thumb drive or memory stick. This new presentation abstracted the pains of tape storage and made it more usable. In addition, it opened new possibilities for increasing the value of tape as industries that require their storage to be portable now have a cost-effective storage platform.

Oracle adopted the specification with its T10000C tape drive. However, LTFS for a single drive has limited value for both the customer and Oracle. Extending LTFS to an entire library allows customers to essentially have thousands of thumb drives. They can then manage petabytes of data in their library through just a basic desktop explorer interface. Not only does this make tape easier to use, it also gives users peace of mind because all their content is written in an open format. Customers will no longer be chained to their backup application or other proprietary format. In addition, the portability benefits are greatly enhanced. Finally, LTFS – Library Edition (LTFS-LE) enables future Oracle applications and middleware to use tape as a storage format by providing a single, simple access point.

Security

There are three aspects to LTFS-LE security: physical, network, and user access.

Physical

It is required that LTFS-LE is installed on a standalone server within an organization's data center. Physical access to the server would be dictated by customer company policy.

Network

It is required that LTFS-LE 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 LTFS-LE Application access is controlled by username and password authentication. These are set up 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:

LTFS-LE Release 1.0 or higher

Note: It is expected that libraries, library software, and drives also meet minimum firmware version levels that are connected to the LTFS-LE application. These firmware levels are specified in the LTFS-LE release notes.

Restrict Network Access

Keep the LTFS-LE host server 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 and describes several recommended deployment topologies for the systems. The following will not detail the installation, configuration, and administration of the LTFS-LE application. The installation, configuration, and administration will be covered in the LTFS-LE Installation and Administration Guide 1.0.

Understand Your Environment

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

Which resources need to be protected?

For LTFS-LE, the host server and the associated network must be protected from unauthorized access

From whom are the resources being protected?

LTFS-LE must be protected from everyone on the Internet, external users, and unauthorized internal users.

What will happen if the protections on strategic resources fail?

It is possible that someone could maliciously cause data loss to tape storage with unauthorized access to LTFS-LE.

Installing Linear Tape File System – Library Edition (LTFS-LE)

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

Refer to the following LTFS-LE user guides for installation instructions.

Oracle LTFS-LE Planning and Installation

Post Installation Configuration

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

A

Secure Deployment Checklist

The following security checklist includes guidelines that help secure the tape drive:

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 LTFS-LE or Oracle Tape Libraries.

B

References

Oracle LTFS-LE Planning and Installation