StorageTek Virtual Library Extension

Security Guide

E27726-03

October 2013

ORACLE

StorageTek Virtual Library Extension Security Guide

E27726-03

Primary Author:

Contributing Author:

Contributor:

Contents

Preface v

Audience v
Documentation Accessibility v

1 Overview

Product Overview 1-1
General Security Principles 1-1
Keep Software Up To Date 1-1
Restrict Network Access to Critical Services 1-1
Follow the Principle of Least Privilege 1-1
Monitor System Activity 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
Recommended Deployment Topologies 2-1
Secure ACSLS and Tape Libraries Behind the Corporate Firewall 2-1
Recommended Deployment Topologies: Firewall Security Option 2-2
Ethernet Ports Used for ACSLS Communication 2-2
Recommended Procedure for Securing ACSLS and Infrastructure Components 2-3
Installing and Configuring Solaris 2-4
Installing and Configuring ACSLS 2-4
Perform a Standard ACSLS Installation 2-4
Use Strong Passwords for the ACSLS User IDs 2-5
Restrict Access to ACSLS Files 2-5
Set 'root' as the Effective User ID for Three ACSLS Files 2-5
Review Settings for ACSLS Static and Dynamic Variables 2-5
Configuring WebLogic 2-5
Use the ACSLS userAdmin.sh utility to create and maintain ACSLS GUI users 2-5
Using the ACSLS GUI 2-6
Install the Latest JRE Version on GUI Client Systems 2-6
Accessing the ACSLS GUI 2-6

Installing ACSLS HA 2-6

3 Security Features

The Security Model 3-1
Configuring and Using Authentication 3-1
ACSLS User Authentication by the Solaris OS 3-1
ACSLS GUI User Authentication by WebLogic 3-1
Audit Considerations 3-2
Keeping Audited Information Manageable 3-2
Evaluate the purpose for auditing 3-2
Audit knowledgeably 3-2
Configuring and Using the ACSLS Audit Logs 3-2
ACSLS Log Directory 3-2
ACSLS Log/sslm Directory 3-3
Viewing ACSLS Audit Trails from the GUI's Log Viewer 3-4
View System Events from the GUI 3-4
Configuring and Using the Solaris Audit Logs 3-4
Configuring and Using the WebLogic Audit Logs 3-5

4 Security Considerations for Developers

Enable the Firewall Security on the Client Application's Server 4-1

A Secure Deployment Checklist

B References

Preface

This document describes the security features of Oracle's StorageTek Virtual Library Extension (VLE).

Audience

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

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.

1

Overview

This section gives an overview of VLE and explains the general principles of application security.

Note: This Guide applies to all versions of VLE.

Product Overview

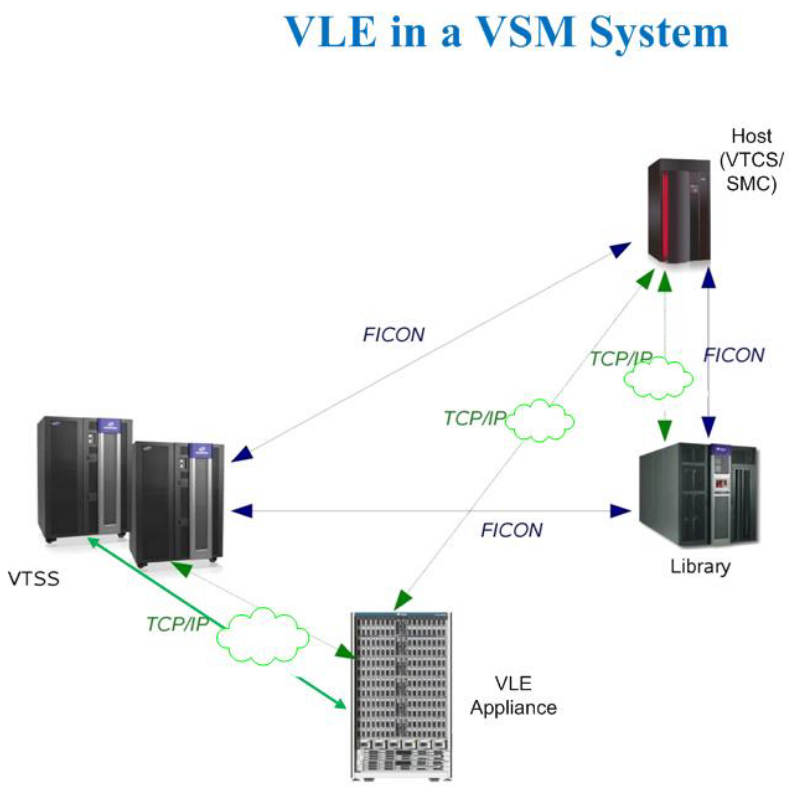
Oracle's Virtual Library Extension (VLE) is packaged as an engineered system built on existing Oracle server and storage platforms. The servers, disk storage and standard rack mount enclosure are delivered as a packaged system.

The VLE includes pre-installed pre-configured software for VLE functionality so that limited site-level configuration is required to integrate the product into the customer's managed tape environment. The VLE is designed to preclude the need for customer administration of the system.

Note: Only qualified Oracle personnel are permitted to maintain the system and administer any configuration changes.

As shown in Figure 1–1, VLE is just one component of Oracle's StorageTek Virtual Storage Manager (VSM) system.

Figure 1–1 VLE in a VSM System



Major subsystems include:

VTSS hardware and software
The Oracle VTSS supports emulated tape connectivity over FICON interfaces to IBM MVS, VM and zLinux hosts and also FICON attachment to Real Tape Drives (RTDs) and TCP/IP attachment to other VTSSs and VLEs. FICON is an IBM-driven standard for channel protocol between CPU (zOS) and devices.

Enterprise Library Software (ELS), which includes Virtual Tape Control Software (VTCS)
ELS is the consolidated suite of StorageTek mainframe software that enables and manages the VTSS. The ELS base software consists of Host Software Component (HSC), Storage Management Component (SMC), HTTP Server and Virtual Tape Control Software (VTCS).

VTCS is the ELS component that controls virtual tape creation, deletion, replication, migration and recall of virtual tape images on the VTSS subsystem, and also captures reporting information from the VTSS subsystem.

Virtual Library Extension (VLE) hardware and software
The VLE subsystem functions as a migrate and recall target for VTSS Virtual Tape Volumes (VTVs). The VLE is IP-attached to the VTSS.

Critical Security Principles

The following principles are fundamental to maintaining system security.

Keep Software Up To Date

Patches and system updates will be installed by qualified Oracle personnel.

Restrict Network Access to Critical Services

VLE should be installed in secure physical locations with access limited to authorized customer employees/agents and Oracle service personnel. The system should be networked behind a firewall. Only Oracle service personnel are permitted to administer the system.

Authentication

Ensure that only authorized personnel can access system. Passwords should be changed when deployed at the customer site.

Follow the Principle of Least Privilege

No additional user accounts are permitted. Only pre-existing accounts are used for system maintenance and administration.

Monitor System Activity

System security stands on three legs: good security protocols, proper system configuration and system monitoring. Auditing and reviewing audit records address this third requirement.

Keep Up To Date on Latest Security Information

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

2

Secure Installation

All software is pre-installed in the VLE. The only step to secure the system is to change the VLE administrator account password. The system will force a password reset at the initial power-up.

Data is compressed and sent in a proprietary format including predominance of intercommunication with legacy systems that are currently installed in customer environments. IP communication should be on a private, dedicated network that provides encryption built into the IP infrastructure.

A

Secure Deployment Checklist

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

- Reset the VLE administrator account at initial power-up of the VLE.