Oracle® Virtual Library Extension

Security Guide

All Versions

E27726-02

October 2012

Oracle Virtual Library Extension Security Guide – All Versions

E27726-02

Primary Author: VLE Development

Contents

Part 1: Overview

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

Product Overview

Oracle's Virtual Library Extension (VLE) appliance 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, or appliance.

The VLE appliance 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 appliance is designed to preclude the need for customer administration of the system.

> **Warning - Only qualified Oracle personnel are permitted to maintain the system and administer any configuration changes.**

The VLE appliance is just one component of a VSM solution.

Major subsystems include:

- VTSS hardware and software

  The 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.

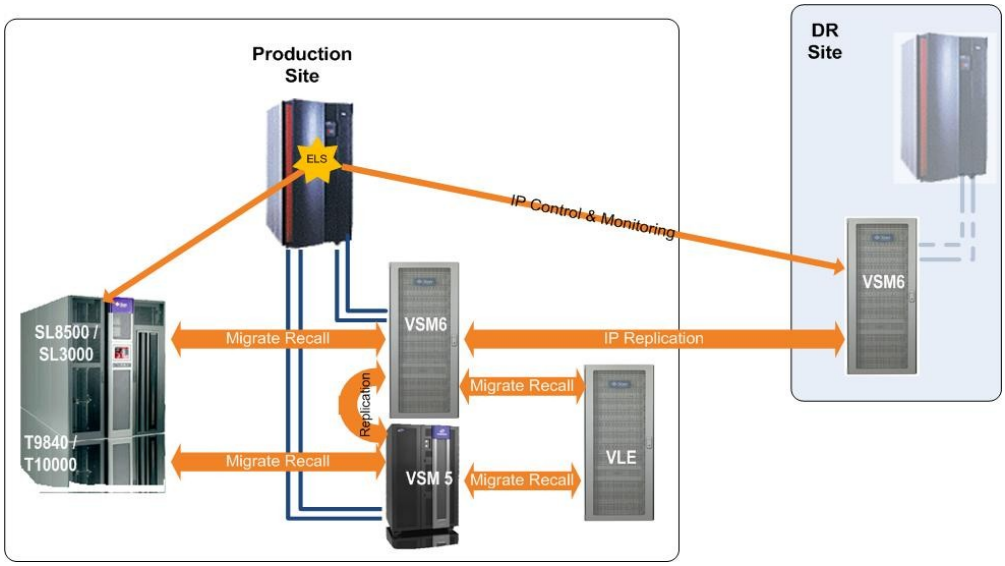
- Enterprise Library Software (ELS) and Virtual Tape Control Software (VTCS)

  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.



Elements of the Virtual Storage Manager Solution

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

Appliances 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

Non-VTSS user accounts are not 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 note yearly for revisions.

Part 2: Secure Installation and Configuration

All software is pre-installed in the VLE appliance. 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.

Part 3: Security Features

There are no configurable security features offered in the VLE appliance.

Part 4: Security Considerations for Developers

Not applicable. Applications installed and configured on the appliance are internally developed and tested by Oracle development.

Part 5: Appendices

Appendix A: Secure Deployment Checklist

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

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

References