

Oracle® Virtual Library Extension

Security Guide

All Versions

E27726-02

October 2012

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 software or related documentation 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 RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software

License (2011). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software 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 which may create a risk of personal injury. If you use this software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications. Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

This software 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

Part 1: Overview.....	4
Product Overview.....	4
Critical Security Principles.....	6
Part 2: Secure Installation and Configuration.....	7
Part 3: Security Features.....	8
Part 4: Security Considerations for Developers.....	9
Part 5: Appendices.....	10
Appendix A: Secure Deployment Checklist.....	10
References.....	11

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.

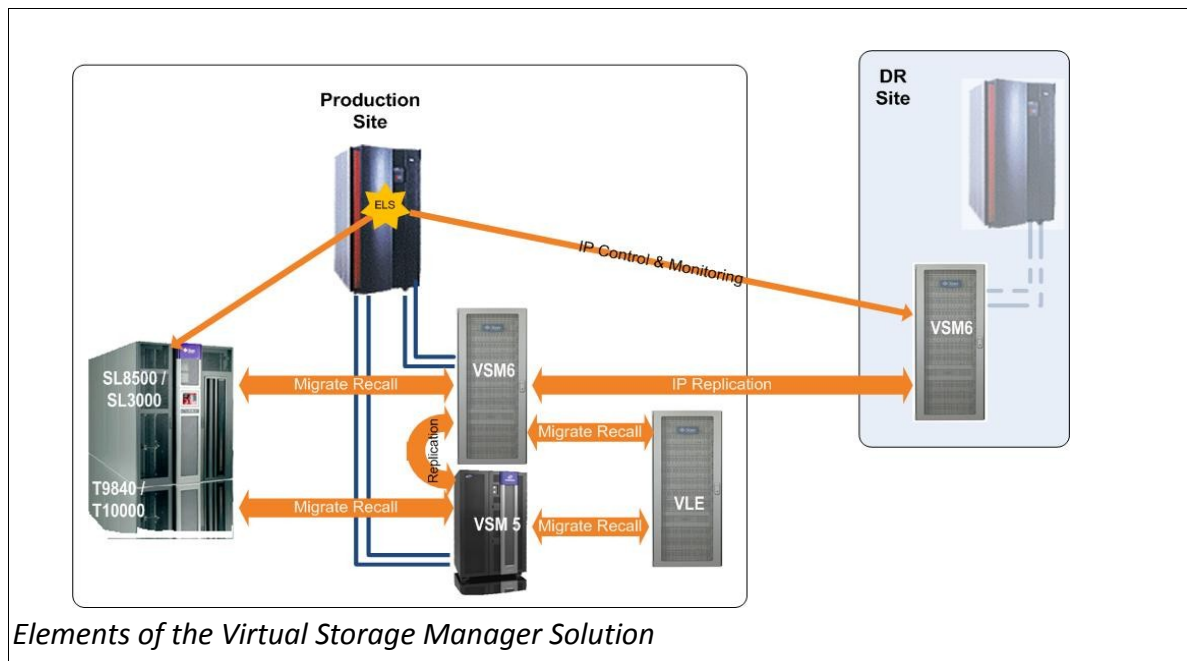
- Enterprise Library Software (ELS) and Virtual Tape Control Software (VTCS)

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.



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