Oracle® Virtual Operator Panel

Security Guide

E48643-02

March 2014

ORACLE®

Oracle Virtual Operator Panel Security Guide

E48643-02

Contents

Preface

This document describes the security features of Oracle's Virtual Operator Panel.

Audience

This guide is intended for anyone involved with using security features and secure installation and configuration of Oracle's Virtual Operator Panel.

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 the product and explains the general principles of application security.

Product Overview

Oracle's Virtual Operator Panel is a suite of Java applications that provide a graphical user interface for managing tape drives. Customers and service engineers use Virtual Operator Panel to view, set or modify configuration parameters, display or monitor status, and perform diagnostics, troubleshooting, and service tasks (for example, download firmware).

General Security Principles

The following principles are fundamental to using any application 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 Oracle Virtual Operator Panel version of 2.0 or later.

- Restrict Network Access

  Keep the Oracle Virtual Operator Panel application behind a firewall, in a secure, data center environment. Also, if possible, it is preferable to install the Oracle Virtual Operator Panel application on a server on a private LAN. The firewalls provide assurance that access to these systems is restricted to a known network route, which can be monitored and restricted, if necessary. The Oracle Virtual Operator Panel application is not designed to have public or internet access.

- Follow the Principle of Least Privilege

  The principle of least privilege states that users should be given the least amount of privilege to perform their jobs. User privileges should be reviewed periodically to determine relevance to current job responsibilities.

- 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.

2

Secure Installation and Configuration

This section provides Oracle Virtual Operator Panel application security as it relates to installation and configuration.

Installation Overview

This section outlines the planning process for a secure installation.

Understand Your Environment

Oracle Virtual Operator Panel is intended to be used in a secure environment. Be sure to install on computers, and in networks, that are in a secure environment, for both physical access and network access.

Installing Oracle Virtual Operator Panel

For more information about installing Oracle Virtual Operator Panel, refer to the *Oracle Virtual Operator Panel User's Guide*.

Post Installation Configuration

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

Change Default Passwords

Security is most easily broken when a default user account still has a default password even after installation

Enforce Password Management

Apply basic password management rules, such as password length, history, and complexity, to all user passwords.

3

Security Features

This section outlines security mechanisms offered by Oracle Virtual Operator Panel.

The Security Model

Because the intended environment for Oracle Virtual Operator Panel is a secure, data center environment, the security model is minimal, and depends on the computer and network being physically secure.

For legacy tape drives (for example, StorageTek 9840D, T10000C, IBM LTO5, HP LTO5, and earlier) the protocols used are telnet (port 23) and FTP (port 20, 21), which are unencrypted.

Beginning with this release (VOP 2.0), and future drives which support it, SSH and SFTP are the defaults.

A

Secure Deployment Checklist

Ensure that you do the following:

- Keep Oracle Virtual Operator Panel and the tape drives it manages behind the corporate firewall.
- Harden the Solaris or Linux operating system.
- Apply all security patches and workarounds.
- Contact your Oracle Services, Oracle Tape Library Engineering, or account representative if you come across vulnerabilities in Oracle tape drives.

B

Open Ports

The following lists the default ports that might be open on Oracle Virtual Operator Panel:

Port: 22

- Protocol: TCP
- Service: SSH
- Open by Default? Yes

C

References

You can access Oracle Virtual Operator Panel user documentation from the Oracle Technical Network (OTN) Tape Storage Products page:

http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html