StorageTek T10000D

Security Guide

E27518-04

August 2016

ORACLE

StorageTek T10000D Security Guide

E27518-04

Copyright © 2014, 2016, Oracle and/or its affiliates. All rights reserved.

Primary Author: Dave Hostetter

Contributing Author:

Contributor:

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 is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware 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 that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about 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 unless otherwise set forth in an applicable agreement between you and Oracle. 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, except as set forth in an applicable agreement between you and Oracle.

Contents

Preface v

Audience v
Documentation Accessibility v

1 Overview

Product Overview 1-1
Capacity and Performance of T10000D 1-1
Security 1-1
General Security Principles 1-1
Keep Software Up To Date 1-1
Restrict Network Access 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
Securing the Tape Drive 2-1
Installing Virtual Operator Panel (VOP) application 2-2
Post Installation Configuration 2-2
Assign the user (admin) password. 2-2
Enforce password management 2-2

3 Security Features

A Secure Deployment Checklist

B References

Preface

This document describes the security features of Oracle's StorageTek T10000D.

Audience

This guide is intended for anyone involved with using security features and secure installation and configuration of StorageTek T10000D.

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 StorageTek T10000D tape drive and explains the general principles of tape drive security.

Product Overview

The T10000D Enterprise tape drive attaches to open systems SCSI over Fibre Channel protocol, and mainframe over FICON protocol. The T10000D tape drive transfers data to and from a host and stores it on a removable magnetic media. The T10000D tape drive is intended primarily to provide high reliability, high capacity back up, archive, and data processing capabilities for enterprise customers that demand high duty cycle and reliability. The product provides optional data encryption. The customer has the option to enable the encryption feature. The tape drive product was enhanced for capacity and native tape speed. In addition, data management features were also added along the way.

Capacity and Performance of T10000D

The T10000D tape drive has up to 8.5TB capacity and 252 MB per second native tape speed.

Security

The T10000D tape drive is designed and documented for use within a controlled hardware environment. Tape drives are always located inside a controlled data center and they are typically located inside of a tape library. In some cases, the customer will use a rack mount version but that is rare. The controlled data center is also inside a fire wall that is protected by the customer's own security policies. This will give the best functionality and protection from compromise, both from the internet in general and from the internal entity operating the tape drive.

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. Throughout this document, the following software level is assumed:

T10000D 4.XX.1XX

Restrict Network Access

Keep the tape drive 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 tape drive 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 and implementation process for a secure installation and configuration, describes several recommended deployment topologies for the systems, and explains how to secure a tape library.

Understand Your Environment

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

Which resources need to be protected?

Many resources in the production environment can be protected. Consider the resources needing protection when deciding the level of security that you must provide.

From whom are the resources being protected?

The tape drive must be protected from everyone on the Internet. But should the tape drive be protected from the employees on the intranet in your enterprise?

What will happen if the protections on strategic resources fail?

In some cases, a fault in a security scheme is easily detected and considered nothing more than an inconvenience. In other cases, a fault might cause great damage to companies or individual clients that use the tape drive. Understanding the security ramifications of each resource will help protect it properly.

Securing the Tape Drive

By default, the tape drive uses ports listed in the following table. The firewall should be configured to allow traffic to use these ports and that any unused ports are blocked. The tape drives support IPv6 and IPv4.

Table 2–1 Network ports used

Port	T10000D
22 tcp - SSH VOP	X
22 tcp - SFTP	X
161 udp - SNMPV1 Tape Drive agent requests - inbound stateful	X
162 udp - SNMPV1 Tape Drive traps and inform notifications - outbound stateless for traps, outbound stateful for inform	X

Table 2–1 (Cont.) Network ports used

Port	T10000D
23 tcp - TELNET	
21 tcp - FTP	
9842 tcp - EPT	
3331 OKM - challenge and root CA service	X
3332 OKM – Enrollment. Cyber strength is AES256	X
3334 OKM – Encryption key exchange. Cyber strength is AES256	X
3335 OKM – Cluster discovery. Cyber strength is AES256	X

Ports 21 and 23 will be disabled for our customers for T10000D. If a customer requires access to a non-secure TELNET, or a non-secure FTP, or both, then a VOP configuration option is available.

Installing Virtual Operator Panel (VOP) application

VOP should only be installed on systems that are within the same protected network infrastructure as the tape drive. Customer access controls should be enforced on the systems where VOP is installed to assure restricted access to the tape drive. See Table 2–1 for ports used by VOP.

Refer to the following VOP user guide for web launch VOP install instructions.

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

Post Installation Configuration

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

Assign the user (admin) password.

The customer admin account password should be changed by the customer at the site and is owned by the customer. The password security meets Oracle standards. An infinite number of passwords is available for use over the life of the tape drive. If the admin password is forgotten, it can be reset. The first password is the default password sent with the tape drive.

Enforce password management

Basic password management rules, such as password length, and complexity must be applied to the administrator password.

The password management rules require at least one of each of the following rules.

- Must be between 8 and 16 characters long
- Lower case (a-z)
- Upper case (A-Z)
- Decimal digit (0-9)

- Special characters (.?;:"{}[]()!@#$%&, ...)

3

Security Features

This section outlines the specific security mechanisms offered by the product.

The T10000D tape drive communicates on a secure channel to the Oracle Key Management System. The T10000D will communicate SSH and SFTP to the Virtual Operator Panel and TELNET and FTP will be disabled for our customers. These should not be the only line of security to protect the Tape Drive. Ideally, the Tape Drives should be in a physically secured data center that also has a secured network that only allows access from the servers utilizing its functionality. These servers and applications running on them should also be secured. In addition, the customer has the option to elevate the security of the tape drive to yet another level. One of the options is to encrypt their data.

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 if you come across vulnerabilities in Oracle tape drives.

B

References

You can access the VOP User Guide from:

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