StorageTek T10000D

安全指南

E50324-04

2016 年 8 月

ORACLE

StorageTek T10000D
安全指南

E50324-04

目录

表格清单

前言

本文档介绍了 Oracle StorageTek T10000D 的安全功能。

目标读者

本指南的目标读者是要使用 StorageTek T10000D 的安全功能以及要安全可靠地安装和配置 StorageTek T10000D 的所有人。

文档可访问性

有关 Oracle 对可访问性的承诺，请访问 Oracle Accessibility Program 网站 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc。

获得 Oracle 支持
购买了支持服务的 Oracle 客户可通过 My Oracle Support 获得电子支持。有关信息，请访问 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info；如果您听力受损，请访问 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs。

1

第 1 章 概述

本节概述了 StorageTek T10000D 磁带机并说明了磁带机的一般性安全原则。

产品概述

T10000D Enterprise 磁带机可通过光纤通道协议连接到开放式系统 SCSI，通过 FICON 协议连接到大型机。T10000D 磁带机可向主机传输数据和从中读取数据，并将数据存储在可移除的磁介质中。T10000D 磁带机主要用于为需要高占空比和高可靠性的企业客户提供高可靠性、大容量备份、归档和数据处理功能。该产品可提供可选的数据加密功能。客户可以选择启用加密功能。该磁带机产品在容量和本机磁带速度方面进行了增强。此外，还增加了数据管理功能。

T10000D 的容量和性能

T10000D 磁带机的容量最多为 8.5 TB，本机磁带速度为每秒 252 MB。

安全性

T10000D 磁带机设计为在受控硬件环境中使用，产品文档中也是这样要求的。磁带机应始终位于受控数据中心中，通常位于磁带库中。在某些情况下，客户会使用机架装配版本，但并不常见。此外，受控数据中心应位于由客户自己的安全策略保护的防火墙内。这可保证最佳的功能使用和安全防护，避免来自 Internet 一般访客和运行磁带机的内部实体的侵害。

一般性安全原则

以下原则是安全使用任何产品的基本原则。

使软件保持最新

良好的安全做法包括许多原则，其中一条就是使所有软件版本和修补程序保持最新。在整个文档中，假设使用以下软件级别：

T10000D 4.XX.1XX

限制网络访问

将磁带机置于数据中心防火墙后面。防火墙可确保对这些系统的访问限定在已知的网络路由范围内，如有必要，可对其进行监视和限制。此外，防火墙路由器可代替多

个独立的防火墙。建议您标识允许连接到磁带机的主机并阻止所有其他主机（如果可能）。

密切关注最新安全信息

Oracle 会持续不断地改进其软件和文档。请查看此文档中的每个发行版，确定是否有修订内容。

2

第 2 章 安全安装

本节概述了安全安装和配置的规划和实现过程，介绍了系统的几种建议部署拓扑并说明了如何确保磁带库安全。

了解您的环境

要更好地了解安全需求，必须回答以下问题：

需要保护哪些资源?

可以保护生产环境中的许多资源。确定必须提供的安全级别时，请考虑需要保护的资源。

要避免资源被哪些用户访问?

必须避免磁带机被 Internet 上的任何人访问。但是，是否应避免磁带机被企业内联网中的员工访问?

如果对战略性资源的保护失败，将会产生什么后果?

在某些情况下，安全架构中出现的故障很容易被检测到，并且这种故障仅仅被视为操作不便。其他情况下，故障可能对使用磁带机的公司或个人客户造成巨大损害。了解每个资源的安全后果有助于对其进行正确的保护。

确保磁带机安全

默认情况下，磁带机使用下表中列出的端口。应将防火墙配置为允许使用这些端口进行通信并阻止那些未使用的端口。磁带机支持 IPv6 和 IPv4。

表 2.1. 所用网络端口

端口	T10000D
22 tcp－SSH VOP	X
22 tcp－SFTP	X
161 udp－SNMPV1 磁带机代理请求－入站有状态	X
162 udp－SNMPV1 磁带机陷阱和通知－对于陷阱，出站无状态；对于通知，出站有状态	X

端口	T10000D
23 tcp－TELNET	
21 tcp－FTP	
9842 tcp－EPT	
3331 OKM－质询和根 CA 服务	X
3332 OKM－注册。Cyber strength（加密强度）为 AES256	X
3334 OKM－加密密钥交换。Cyber strength（加密强度）为 AES256	X
3335 OKM－群集搜索。Cyber strength（加密强度）为 AES256	X

对于 T10000D，将对我们的客户禁用端口 21 和 23。如果客户需要访问不安全的 TELNET 和/或不安全的 FTP，则可以使用 VOP 配置选项。

安装 Virtual Operator Panel (VOP) 应用程序

VOP 应仅安装在与磁带机相同的受保护网络基础结构内的系统中。应在安装了 VOP 的系统上强制执行客户访问控制，以确保对磁带机的访问受到限制。请参见表 2.1 “所用网络端口” 了解 VOP 使用的端口。

有关通过 Web 启动 VOP 安装的说明，请参阅以下 VOP 用户指南。

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

安装后配置

本节讲述了安装后必须进行的安全配置更改。

为用户指定 (admin) 密码

客户的管理员帐户密码应由客户在站点中进行更改且归客户所有。密码安全性必须满足 Oracle 标准。在磁带机的整个生命期内可使用无数个密码。如果忘记管理员密码，可对其进行重置。第一个密码是随磁带机提供的默认密码。

加强密码管理

必须对管理员密码应用基本密码管理规则（例如密码长度和复杂度）。

密码管理规则要求至少满足以下规则之一。

- 长度必须为 8 到 16 个字符
- 小写字母 (a-z)
- 大写字母 (A-Z)
- 十进制数字 (0-9)
- 特殊字符 (.?;:"{}[]()!@#$%&, ...)

3

第 3 章 安全功能

本节概述了本产品提供的具体安全机制。

T10000D 磁带机通过安全通道与 Oracle 密钥管理系统进行通信。T10000D 将通过 SSH 和 SFTP 与 Virtual Operator Panel 通信，将对客户禁用 TELNET 和 FTP。这些不应是保护磁带机的唯一安全防线。理想情况下，磁带机应位于物理上安全的数据中心中，且该数据中心还应具有仅允许利用其功能的服务器进行访问的安全网络。基于磁带库运行的这些服务器和应用程序也应得到安全保护。此外，客户可以选择将磁带机的安全级别提升到其他级别。其中一个选项是对其数据进行加密。

附录 A

附录 A. 安全部署核对表

以下安全核对表包括有助于确保磁带机安全的准则：

1. 加强密码管理。
2. 加强访问控制。
3. 限制网络访问。
   a. 应实现防火墙。
   b. 必须不危害防火墙。
   c. 应监视系统访问。
   d. 应检查网络 IP 地址。
4. 如果 Oracle 磁带机中存在漏洞，请联系 Oracle 服务部门、Oracle 磁带库工程部门或客户代表。

附录 B

附录 B. 参考

您可以从以下网址访问 VOP 用户指南：

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