StorageTek SL150 模块化磁带库

安全指南

E40925-03

2015 年 6 月

ORACLE

StorageTek SL150 模块化磁带库
安全指南

E40925-03

目录

表格清单

前言

本文档介绍了 Oracle StorageTek SL150 模块化磁带库的安全功能。

目标读者

本指南的目标读者是要安全可靠地安装和配置 Oracle StorageTek SL150 模块化磁带机以及要使用其安全功能的所有人。

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

概述

本节概述了 Oracle StorageTek SL150 模块化磁带库并说明了磁带库的一般性安全原则。

产品概述

StorageTek SL150 模块化磁带库是 Oracle Corporation 推出的一种 3U 至 21U、19 英寸机架装配式的模块化自动磁带库。该产品提供 30 到 300 个 LTO 盒式磁带的存储容量，1 到 20 个 LTO 光纤通道磁带机或 SAS 磁带机以及一个通过一个已安装磁带机的桥接磁带机光纤或 SAS 端口控制路径。

安全性

所有磁带库产品都设计为在不允许常规网络或用户访问的受控服务器环境中使用，产品文档中也是这样要求的。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库的内部实体的侵害。

常规安全原则

以下原则是安全使用任何产品的基本原则。

保持软件为最新版本

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。自 2015 年 4 月以来发布的 SL150 固件版本如下：

2012 年 6 月 v1.00 (RTA 0.1.0.0.0)
2012 年 9 月 v1.03 (RTA 0.1.0.3.0)
2012 年 10 月 v1.50 (RTA 0.1.5.0.0)
2013 年 1 月 v1.82 (RTA 0.1.8.2.0)
2013 年 8 月 v2.0 (RTA 0.2.0.0.0)
2013 年 10 月 v2.01(RTA 0.2.0.1.0)
2014 年 4 月 v2.25 (RTA 0.2.2.5.0)
2015 年 6 月 v2.50 (RTA 0.2.5.0.0)

限制网络访问

将磁带库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库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

安全安装

本节概述了安全安装的规划过程，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 Internet 上的任何人和未经授权的内联网用户访问磁带库。

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库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。

确保磁带库安全

默认情况下，磁带库使用表 2.1 “SL150 网络端口”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。

表 2.1. SL150 网络端口

端口	类型	说明
22	TCP	SSH CLI 访问－入站有状态 仅用于开发测试和调试，未在字段中提供
25	TCP	无验证的 SMTP
67	DHCP	客户机－出站
68	DHCP	客户机－入站

端口	类型	说明
80	HTTP	用于远程用户界面的 WebLogic 端口
123	NTP	网络时间协议（如果启用）
161	UDP	SNMP 库代理请求－入站有状态
162	UDP	SNMP 库陷阱和通知－对于陷阱，出站无状态；对于通知，出站有状态
465	TCP	具有 SSL 或 TLS 验证的 SMTP
443	HTTPS	用于远程用户界面的 WebLogic HTTPS 端口
546	DHCPv6	IPv6 DHCP 客户机－出站
547	DHCPv6	IPv6 DHCP 客户机－入站
33200-33500	TRACEROUTE	软件开发使用

按上面的表列表保留或建议供磁带库使用的有效端口号选择。合法端口号从数字 1 开始，因为零不是合法端口号。

配置 SNMP 时，强烈建议使用 SNMPv3（而不使用 SNMPv2c），以利用其保密性、完整性和验证功能。

配置 SMTP 时，强烈建议使用 TLS 验证（而不使用 SSL 或无验证选项）。

安装配置

本节讲述了安装期间必须进行的安全配置更改。

指定用户 (admin) 密码

首次打开电源时，设置向导将自动在本地操作面板上运行，以获取基本配置信息。这包括管理员帐户用户名和密码、网络设置以及其他基本设置。

只有在完成设置向导步骤后，磁带库才会工作。

随产品提供了一个登录帐户，安装人员必须在设置向导例程的第一步中输入该帐户。之后，用户必须输入新密码，设置向导才能完成。

完成了初始设置向导并且磁带库已充分通电后，可以通过针对所有磁带库设置的浏览器用户界面 (browser user interface, BUI) 执行对磁带库配置的其他修改。

加强密码管理

必须对所有密码应用基本密码管理规则（例如密码长度、密码历史记录和复杂度）。SL150 密码必须介于 8 到 128 个字符之间，且必须至少包含一个数字或特殊字符。安装期间必须更改默认密码且不能重用该密码。

注:

所显示经过掩码的字符数不指示准确的已输入字符数。

浏览器 UI 验证

将用于访问远程用户界面的浏览器设置限制为保持 TLS 1.0 或更高版本，以为低于版本 2.50 的固件级别防范 CVE-2014-3566 风险。磁带库固件将不向下自动协商到版本 2.50 中的 SSLv3。

3

安全功能

本节概述了本产品提供的具体安全机制。

磁带库具有保护自身的内部防火墙。这不应是保护磁带库的唯一安全防线。建议将磁带库置于物理上安全的数据中心，且该数据中心位于仅允许利用其功能的服务器进行访问的安全网络中。基于磁带机运行的这些服务器和应用程序也应得到安全保护。

用户帐户应限制为 *operator* 角色级别，而不是向所有用户授权 *Admin* 角色级别。应练习正确使用 *service* 用户角色。根据需要创建、启用或禁用 *service* 用户角色帐户。Service 角色的权限大于 *operator*，与 *admin* 角色几乎具有相同授权。

如果需要磁带库活动的历史记录以用于调查目的，可以检查和导出 "Activity Log"（活动日志）进行进一步的分析。用户界面上的 "Activity Log"（活动日志）可以显示用户登录名、主机或 UI 启动的操作以实现可跟踪性。

4

重新部署

本节介绍了如何将磁带库恢复到出厂默认状态以清除所有客户数据。

如果客户需要停用某个磁带库，可以使用产品提供的一个过程来删除所有客户配置信息和所有日志文件并将磁带库恢复到出厂默认状态。将磁带库置于 "locate" 模式，然后同时按住前后定位按钮 10 秒以上再松开这两个按钮，即可进入此过程。

LED 指示灯闪烁频率从慢变快指示按下定位按钮的时间已足够。

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库安全的准则：

1. 加强所有用户帐户的密码管理。
2. 强制实施访问控制，无论物理上邻近还是通过 SCSI、UI、SNMP 等接口连接都是如此。
3. 限制网络访问。
   a. 应实现防火墙。
   b. 防火墙必须未损坏。
   c. 应监视系统访问。
   d. 应检查网络 IP 地址。
   e. 服务可能具有需要提供正确密码或监视访问控制的工具（例如 SDP-2，以允许自动下载日志信息或其他访问）
4. 如果 Oracle 磁带库中存在漏洞，请联系 Oracle 服务部门、Oracle 磁带库工程部门或客户代表。
5. SMTP 应该使用 TLS，而不是 SSL 等较少的协议或没有协议。
6. SNMP 应设置为 V3 级别，而不是 V2C 或较少功能。

附录 B

参考

《*SL150 User Guide*》位于：

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

与 SL150 有关的所有文档位于文件号码为 E35103-07 的联机文档集中。