StorageTek Enterprise Library Software

安全指南

E63471-01

2015 年 3 月

ORACLE

StorageTek Enterprise Library Software
安全指南

E63471-01

目录

前言

本文档介绍了 Oracle StorageTek Enterprise Library Software (ELS) 的安全功能。

目标读者

本指南的目标读者是涉及使用 StorageTek Enterprise Library Software (ELS) 的安全功能以及对其进行安全安装和配置的任何人。

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

本部分概述了 ELS 软件套件并说明了应用程序的一般性安全原则。

1.1. 产品概述

ELS 可为以下平台的 Oracle StorageTek 大型机磁带环境提供磁带自动化支持：

- IBM z/OS 平台。ELS 支持 TCP/IP 客户机/服务器磁带自动化体系结构，该体系结构允许在一个 z/OS LPAR 上运行的 SMC 客户机软件与在其他 z/OS LPAR 上运行的 HSC/VTCS 服务器软件通信。
- IBM z/VM 平台。适用于 z/VM 系统的 ELS VM 客户机软件与 z/OS LPAR 上运行的 HSC/VTCS 服务器软件进行通信以实现 z/VM 的虚拟和物理磁带处理自动化。
- Fujitsu MSP/EX 平台。SMC 必须在进行磁带处理的每台主机上执行。ELS 服务器组件 (HSC/VTCS) 可以在与 SMC 相同的 MSP/EX 主机上执行，也可以在单独的远程主机上执行。当 SMC 和 HSC/VTCS 位于不同的 MSP/EX 主机上时，使用 TCP/IP 发送从客户机主机到服务器主机的请求。要接收来自远程 SMC 客户机的 HTTP 请求，必须在服务器主机上执行的 SMC 上激活 HTTP 组件。

ELS 客户机/服务器通信用于为虚拟和物理磁带卷发出控制路径请求，主要是挂载/卸载请求。这些控制路径请求包含的信息由 TapePlex 配置和策略信息、虚拟/物理磁带传输单元地址和虚拟/物理磁带卷序列号组成。大多数重要的 ELS 客户机/服务器通信从不包含任何客户数据，客户数据始终通过将主机 LPAR 连接到 Oracle StorageTek 磁带传输设备或 VSM 虚拟磁带设备的 IBM FICON/ESCON 数据路径接口进行传输。

本安全指南中的信息适用于所有 ELS 发行版。如本指南第 3 部分所讨论，需要或必须采用此类保护时，可以确保 ELS 客户机/服务器控制路径通信的安全。此外，本文档还讨论了各种 ELS 安装和安装后活动的安全方面。

1.2. 常规安全原则

以下原则是安全使用任何产品的基本原则。

1.2.1. 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。最新的 ELS 累积维护包以及各个 PTF 和 HOLDDATA 均可在 My Oracle Support (MOS) 中获得。累积维护包每月进行更新以从最新的 ELS 每月回归测试周期中包括所有 PTF。累积包中的所有 PTF 均已作为完整软件包一起进行了测试。通过为 ELS

产品订阅 MOS 热门主题警报文档，可以获得 HIPER PTF 电子邮件通知。鼓励客户保持处于最新的维护级别、使 HOLDDATA 保持最新并订阅热门主题警报以获取 HIPER 通知。

1.2.2. 限制网络访问

出于性能和安全性考虑，通过防火墙后的隔离网络来路由 ELS 控制路径通信。使用防火墙可确保对 ELS 系统的访问限定在已知网络范围内，如有必要，可对其进行监视和限制。使用专用网络进行 ELS 客户机/服务器通信消除了与其他应用程序的网络争用并改善了磁带系统性能。

1.2.3. 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。请定期检查此安全指南和所有其他 ELS 产品文档的修订版。本文档中引用的所有 ELS 文档均可在 Oracle Technical Network（Oracle 技术网）的 "Tape Storage Products"（磁带存储产品）部分中找到。

2

安全安装

IBM z/OS 系统授权工具 (System Authorization Facility, SAF) 可为 ELS 的大多数安全方面提供基本保护。SAF 通常通过 IBM RACF 软件包或等效软件包来实现。本部分概述了如何使用基于 RACF 的 SAF 环境来安装和配置安全的 ELS 安装。

2.1. 安装 ELS

Oracle 文档《*StorageTek Enterprise Library Software*：安装 *ELS*》介绍了如何使用 RACF 保护机制安装和配置您所用版本的 ELS。有关以下与安全有关的安装主题的更多信息，请参阅此文档：

- 安装基本软件和最新的累积维护包
- ELS 装入磁带库 APF 授权
- HSC 用户退出磁带库 APF 授权
- SMC JES3 装入磁带库 APF 授权

2.2. ELS 安装后配置

以下 Oracle 文档介绍了您所用版本的 ELS 的安装后配置任务：

- 《*StorageTek Enterprise Library Software: Configuring HSC and VTCS*》
- 《*StorageTek Enterprise Library Software*：配置和管理 *SMC*》
- 《*StorageTek Enterprise Library Software: ELS Programming Reference*》

有关以下与安全有关的安装后主题的更多信息，请参阅以下文档：

- 《Defining RACF protection for CDS data set security》（《针对 CDS 数据集安全定义 RACF 保护》）
- 《Defining command authority and programmatic interface authority using HSC user exit SLSUX15》（《使用 HSC 用户退出 SLSUX15 定义命令授权和程序接口授权》）
- 《Defining volume access authority for mounting and ejecting volumes using HSC user exit SLSUX14》（《使用 HSC 用户退出 SLSUX14 定义卷访问授权以挂载和弹出卷》）
- 《Defining MVC pool and scratch subpool volser authority》（《定义 MVC 池和临时子池卷序列号授权》）

- 《Defining an SMC OMVS RACF segment for communication with a remote HSC subsystem》（《定义 SMC OMVS RACF 段以与远程 HSC 子系统通信》）
- 《Defining an SMC OMVS RACF segment for communication with a VLE appliance》（《定义 SMC OMVS RACF 段以与 VLE 设备通信》）

3

安全功能

本章介绍了 ELS 提供的具体安全机制。

3.1. 使用 AT-TLS 保护 ELS 的安全－仅限 z/OS

IBM z/OS 应用程序透明传输层安全 (Application Transparent Transport Layer Security, AT-TLS) 工具使用 SSL 数据加密保护 z/OS TCP/IP 应用程序的安全。有关 AT-TLS 的更多信息，请参阅 IBM 出版物《*z/OS Communications Server: IP Configuration Guide*》（《z/OS 通信服务器：IP 配置指南》，并参见 IBM 出版物《*z/OS Communications Server: IP Configuration Reference*》（《z/OS 通信服务器：IP 配置参考》）中有关 AT-TLS 策略代理的信息。

Oracle 白皮书《*Using AT-TLS with HSC/SMC Client/Server z/OS Solution: Implementation Example*》（《将 AT-TLS 用于 HSC/SMC 客户机/服务器 z/OS 解决方案：实施示例》）中介绍了在 SMC 和 HSC/VTCS 之间保护 ELS 客户机/服务器通信的安全。此白皮书发布在 Oracle Technical Network（Oracle 技术网）的 "Tape Storage Products"（磁带存储产品）部分中。有关详细的配置信息，请参阅此出版物。

要使用 AT-TLS 保护 ELS 的安全，Oracle 建议使用以下任何 SSL 加密算法：

- SHA-2 系列 (SHA-256, SHA-384, SHA-512)
- AES >= 128 位
- RSA >= 2048 位
- Diffie-Hellman (DH) >= 2048 位
- ECC >= 256 位

任何其他 SSL 加密算法提供较弱的保护，不应当用于 ELS。

注:

用于 VSM 的 StorageTek 虚拟磁带库扩展 (Virtual Library Extension, VLE) 设备当前不支持 AT-TLS 通信。不要使用 AT-TLS 保护 ELS VLE 通信的安全。

3.2. 使用 ELS XAPI 安全功能

ELS 7.3 引入了新的 XAPI 安全功能，用于进行客户机/服务器通信，在 SMC HTTP 服务器中作为默认选项启用。XAPI 安全功能提供附加的用户验证工具（作为 XAPI 协议的一部分），这些工具位于 ELS 内部且完全包含在其中。要使用 XAPI 安全功能，必

须为 ELS 客户机和服务器定义安全凭证（用户 ID 和密码）。ELS 7.3 TapePlex 操作使用这些安全凭证保护 XAPI 事务（挂载、卸载、卷查找、暂存等）的安全。XAPI 安全凭证的使用完全透明，不需要任何额外的用户或操作员介入。有关配置 XAPI 安全功能的更多信息，请参阅配置和管理 *SMC 7.3*。

为只托管 ELS 客户机应用程序（SMC 和 VM 客户机）的 TapePlex 的 XAPI 事务提供安全保护时，首选方法是使用 AT/TLS 工具，如第 3.1 节 “使用 AT-TLS 保护 ELS 的安全－仅限 z/OS” 中所述。AT/TLS 是一个传输层工具，位于 ELS 外部且对其透明。

使用 ELS 7.3 XAPI 安全功能保护托管以下客户机的 TapePlex 的安全：非 ELS 客户机（开放系统客户机）或者混合存在的 ELS 客户机（SMC 和 VM 客户机）与非 ELS 客户机。除了 ELS 7.3 XAPI 安全功能，还可以在这些环境中使用 AT-TLS，但是它将不能保护非 ELS 客户机的 XAPI 事务安全。

4

针对开发者的安全注意事项

Oracle 文档《*StorageTek Enterprise Library Software: ELS Programming Reference*》介绍了可供应用程序开发者使用的 ELS API。ELS 的程序接口使用统一用户接口 (Unified User Interface, UUI)，该接口使用 HSC 命令 security exit SLSUX15 基于 RACF 授权（或等效机制）来管理对其功能的访问。有关使用 RACF 保护 SLSUX15 的安全的更多信息，请参见第 2.2 节 “ELS 安装后配置”。

附录 A

安全部署核对表

1. 如本安全指南所讨论，使用 RACF 保护（或等效机制）。
2. 限制网络访问。ELS 及其管理的磁带库应位于企业防火墙后面。
3. 如果需要，使用 IBM AT-TLS 工具或 ELS XAPI 安全功能保护 ELS 网络通信的安全。
4. 应用所有 ELS PTF 和 HOLDDATA。
5. 如果在使用 Oracle ELS 软件时发现漏洞，请与 Oracle 软件支持部门联系，网址为 http://www.myoraclesupport.com/。

附录 B

参考

ELS 文档保存在按 ELS 发行版组织的库中。可以从磁带存储文档页面访问此文档。

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