StorageTek Enterprise Library Software

安全指南

E63472-01

2015 年 3 月

ORACLE

StorageTek Enterprise Library Software
安全指南

E63472-01

內容

前言

本文件說明 Oracle 的 StorageTek Enterprise Library Software (ELS) 安全功能。

對象

本指南的對象為使用 StorageTek Enterprise Library Software (ELS) 安全功能與安全安裝及配置的所有人員。

文件輔助功能

如需 Oracle 對於輔助功能之承諾的相關資訊，請造訪 Oracle Accessibility Program 網站，網址為 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc。

取用 Oracle Support
已購買支援的 Oracle 客戶可以透過 My Oracle Support 使用電子支援。如需相關資訊，請造訪 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info；或如果您在聽力上需要特殊服務，請造訪 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs。

1

簡介

本節提供 ELS 軟體套件的簡介，並說明應用程式安全的一般原則。

1.1. 產品簡介

ELS 提供下列平台之 Oracle StorageTek 大型主機磁帶環境的磁帶自動化支援：

- IBM z/OS 平台。ELS 支援 TCP/IP 用戶端/伺服器磁帶自動化架構，允許 z/OS LPAR 上執行的 SMC 用戶端軟體與不同 z/OS LPAR 上執行的 HSC/VTCS 伺服器軟體通訊。
- IBM z/VM 平台。z/VM 系統的 ELS VM 用戶端軟體可與 z/OS LPAR 上執行的 HSC/VTCS 伺服器軟體通訊，使 z/VM 的虛擬和實體磁帶機處理自動化。
- Fujitsu MSP/EX 平台。在處理磁帶的每部主機上都必須執行 SMC。ELS 伺服器元件 (HSC/VTCS) 可在與 SMC 相同的 MSP/EX 主機上執行，或在不同的遠端主機上執行。當 SMC 與 HSC/VTCS 位於不同的 MSP/EX 主機時，將使用 TCP/IP 從用戶端主機傳送要求至伺服器主機。若要從遠端 SMC 用戶端接收 HTTP 要求，必須啟動執行於伺服器主機上之 SMC 的 HTTP 元件。

ELS 用戶端/伺服器通訊可用來為虛擬與實體磁帶磁碟區發出控制路徑要求，主要是掛載與卸載要求。這些控制路徑要求中所包含的資訊為 TapePlex 配置與原則資訊、虛擬/實體磁帶傳輸單元位址以及虛擬/實體磁帶磁碟區序號。最重要的是，ELS 用戶端/伺服器通訊絕不會包含任何客戶資料，客戶資料一律經由 IBM FICON/ESCON 資料路徑介面來傳送，此資料路徑介面連接主機 LPAR 至 Oracle StorageTek 磁帶傳輸或 VSM 虛擬磁帶裝置。

本「安全指南」中的資訊適用於所有 ELS 版本。如本指南的第 3 部分所述，若有安全上的需要，可以保護 ELS 用戶端/伺服器控制路徑通訊。此外，本文件會討論各種 ELS 安裝與後續安裝活動的安全層面。

1.2. 一般安全原則

下列原則為安全使用任何產品的基礎。

1.2.1. 將軟體保持在最新狀態

良好的安全措施之一，便是讓所有軟體版本與修補程式保持在最新的狀態。My Oracle Support (MOS) 提供最新 ELS 累積維護組合，以及個別 PTF 與 HOLDDATA。累積維護組合會每月更新，以包含最新 ELS 每月遞迴測試週期的所有 PTF。累積組合中

的所有 PTF 都會一起測試，如同完整的套件。訂閱 ELS 產品的「MOS 熱門主題警示」文件，即可收到 HIPER PTF 電子郵件通知。建議客戶維持目前的維護層次，讓 HOLDDATA 保持最新，並訂閱「熱門主題警示」以取得 HIPER 通知。

1.2.2. 限制網路存取

為了效能與安全的考量，ELS 控制路徑通訊應經由防火牆後的獨立網路。使用防火牆可確保只有透過已知的網路才能存取 ELS 系統，並且能依照需求來監督和限制這些網路。針對 ELS 用戶端/伺服器通訊使用專用網路，可避免與其他應用程式競爭網路，並改善磁帶系統效能。

1.2.3. 將安全資訊保持在最新狀態

Oracle 會持續改善其軟體和文件。請定期檢查此「安全指南」與所有其他 ELS 產品文件的修訂版本。本文件參照的所有 ELS 文件皆可自 Oracle Technical Network (OTN) 的 Tape Storage Products 段落中取得。

2

安全安裝

IBM z/OS System Authorization Facility (SAF) 提供 ELS 大部分安全方面的必要保護。SAF 通常是以 IBM RACF 套裝軟體或同等軟體實作。本節概要說明使用以 RACF 為基礎的 SAF 環境，來安裝與設定安全的 ELS 安裝。

2.1. 安裝 ELS

Oracle 文件 *StorageTek Enterprise Library Software: Installing ELS* 說明如何使用 RACF 保護，安裝與設定您的 ELS 版本。請參閱此文件以瞭解下列安全相關安裝主題的詳細資訊：

- 安裝基本軟體與最新累計維護組合
- ELS 載入磁帶櫃 APF 授權
- HSC user exit 磁帶櫃 APF 授權
- SMC JES3 載入磁帶櫃 APF 授權

2.2. ELS 安裝後配置

這些 Oracle 文件說明您 ELS 版本的安裝後配置工作：

- *StorageTek Enterprise Library Software: Configuring HSC and VTCS*
- *StorageTek Enterprise Library Software: Configuring and Managing SMC*
- *StorageTek Enterprise Library Software: ELS Programming Reference*

請參閱這些文件以瞭解下列安全相關後續安裝主題的詳細資訊：

- 定義 CDS 資料集安全的 RACF 保護
- 使用 HSC user exit SLSUX15 定義指令權限與程式設計介面權限
- 使用 HSC user exit SLSUX14 定義掛載與退出磁碟區的磁碟區存取權限
- 定義 MVC 集區與暫用子集區 Volser 權限
- 定義遠端 HSC 子系統通訊的 SMC OMVS RACF 區段
- 定義 VLE 設備通訊的 SMC OMVS RACF 區段

3

安全功能

本章描述 ELS 提供的特定安全機制。

3.1. 使用 AT-TLS 保護 ELS – 僅限 z/OS

IBM z/OS Application Transparent Transport Layer Security (AT-TLS) 設備使用 SSL 資料加密來保護 z/OS TCP/IP 應用程式。如需 AT-TLS 的詳細資訊，請參閱 *IBM publication z/OS Communications Server: IP Configuration Guide*，以及 *IBM publication z/OS Communications Server: IP Configuration Reference* 中的 AT-TLS 原則代理程式資訊。

保護 SMC 與 HSC/VTCS 之間 ELS 用戶端/伺服器通訊的說明，請參閱 Oracle 白皮書 *Using AT-TLS with HSC/SMC Client/Server z/OS Solution: Implementation Example*。此白皮書發佈於 Oracle Technical Network (OTN) 的 Tape Storage Products 段落。請參閱此文件以瞭解詳細配置資訊。

若要使用 AT-TLS 保護 ELS，Oracle 建議使用下列任何一種 SSL 加密演算法：

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

其他 SSL 加密演算法提供的保護較差，不應用於 ELS。

注意:

VSM 的 StorageTek Virtual Library Extension (VLE) 設備目前不支援 AT-TLS 通訊。請勿使用 AT-TLS 保護 ELS VLE 通訊。

3.2. 使用 ELS XAPI 安全功能

ELS 7.3 針對用戶端與伺服器間的通訊導入新的 XAPI 安全功能，SMC HTTP 伺服器中預設會啟用此功能。XAPI 安全功能提供額外的使用者認證設備作為 XAPI 協定的一部分，此協定位於 ELS 內部且完整包含在其中。若要使用 XAPI 安全功能，您必須定義 ELS 用戶端和伺服器的安全證明資料 (使用者 ID 和密碼)。ELS 7.3 TapePlex 作業會使用這些安全證明資料來保護 XAPI 交易 (掛載、卸載、磁碟區查詢、暫用... 等等)。XAPI 安全證明資料是以完全通透的方式來使用，無須額外的使用者或操作者介

入。請參閱 *Configuring and Managing SMC 7.3* ，瞭解有關配置 XAPI 安全功能的詳細資訊。

保護僅代管 ELS 用戶端應用程式 (SMC 和 VM 用戶端) 之 TapePlexes 的 XAPI 交易的慣用方法，便是使用 AT/TLS 設備，如節 3.1, 「使用 AT-TLS 保護 ELS – 僅限 z/OS」中所述。AT/TLS 是一種傳輸層設備，位於 ELS 外部，並可讓 ELS 通透地使用。

使用 ELS 7.3 XAPI 安全功能來保護代管非 ELS 用戶端 (開放式系統用戶端) 的 TapePlexes，或是混合安裝 ELS 用戶端 (SMC 和 VM 用戶端) 和非 ELS 用戶端的 TapePlexes。除了 ELS 7.3 XAPI 安全功能之外，還可以在這些環境中使用 AT-TLS，但 AT-TLS 不會保護非 ELS 用戶端的 XAPI 交易。

4

開發人員的安全考量

Oracle 文件 *StorageTek Enterprise Library Software: ELS Programming Reference* 說明應用程式開發人員可用的 ELS API。ELS 程式設計介面使用「統一使用者介面 (UUI)」，UUI 根據 RACF 授權 (或同等的功能)，使用 HSC 指令安全結束 SLSUX15 來管理其函數的存取權。如需使用 RACF 保護 SLSUX15 的詳細資訊，請參閱節 2.2, 「ELS 安裝後配置」。

附錄 A

安全建置檢查清單

1. 使用 RACF 保護 (或同等的功能)，如本「安全指南」所述。
2. 限制網路存取。ELS 及其管理的磁帶櫃應位於企業防火牆之後。
3. 使用 IBM AT-TLS 設備或 ELS XAPI 安全功能來保護 ELS 網路流量 (若有需要)。
4. 套用所有的 ELS PTF 與 HOLDDATA。
5. 若在 Oracle ELS 軟體中發現漏洞，請洽詢 Oracle 軟體支援，網址為：http://www.myoraclesupport.com/。

附錄 B

參考資料

ELS 文件儲存在依 ELS 版本組織的文件庫中。請從「磁帶儲存裝置文件」頁面存取此文件。

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