# StorageTek SL150 Modular Tape Library

安全指南

**E41028-03**

**2015 年 6 月**

ORACLE

**StorageTek SL150 Modular Tape Library**
安全指南

**E41028-03**

# 內容

**序言** ..... 7

對象 ..... 7
文件輔助功能 ..... 7

**1. 簡介** ..... 9

產品簡介 ..... 9
安全 ..... 9
一般安全原則 ..... 9
將軟體保持在最新狀態 ..... 9
限制網路存取 ..... 9
將安全資訊保持在最新狀態 ..... 10

**2. 安全安裝** ..... 11

瞭解您的環境 ..... 11
需要保護哪些資源？ ..... 11
必須防止哪些人存取資源？ ..... 11
萬一策略性資源的保護失敗會如何？ ..... 11
保護磁帶櫃 ..... 11
安裝配置 ..... 12
指定使用者 (admin) 密碼 ..... 12
強制密碼管理 ..... 12
瀏覽器 UI 認證 ..... 13

**3. 安全功能** ..... 15

**4. 重新建置** ..... 17

**A. 安全建置檢查清單** ..... 19

**B. 參考資料** ..... 21

# 附表目錄

2.1. SL150 網路連接埠 ..... 11

# 前言

本文件說明 Oracle StorageTek SL150 Modular Tape Library 的安全功能。

## 對象

本指南適用於安全安裝及配置 Oracle StorageTek SL150 Modular Tape Library 及使用其安全功能的所有相關人員。

## 文件輔助功能

如需 Oracle 對於輔助功能的承諾的相關資訊，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

本節簡介 Oracle’s StorageTek SL150 Modular Tape Library 並說明磁帶櫃安全一般原則。

## 產品簡介

StorageTek SL150 Modular Tape Library 是由 Oracle Corporation 推出的 3U 至 21U 19" 機架式模組化自動磁帶櫃。提供的儲存容量從 30 至 300 個 LTO 磁帶匣、1 至 20 部 LTO 光纖通道磁帶機或 SAS 磁帶機，以及透過其中一個安裝的磁帶機提供橋式驅動的光纖或 SAS 埠控制路徑。

## 安全

所有磁帶櫃產品的設計與說明皆是針對在受控制的伺服器環境 (沒有一般網路或使用者存取) 中使用。如此可提供最佳的功能與保護，使一般網際網路與內部個體無法操作磁帶機。

## 一般安全原則

下列原則為安全使用任何產品的基礎。

### 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。自 2015 年 4 月起，已發行的 SL150 韌體版本如下：

June 2012 v1.00 (RTA 0.1.0.0.0)
September 2012 v1.03 (RTA 0.1.0.3.0)
October 2012 v1.50 (RTA 0.1.5.0.0)
January 2013 v1.82 (RTA 0.1.8.2.0)
August 2013 v2.0 (RTA 0.2.0.0.0)
October 2013 v2.01(RTA 0.2.0.1.0)
April 2014 v2.25 (RTA 0.2.2.5.0)
June 2015 v2.50 (RTA 0.2.5.0.0)

### 限制網路存取

磁帶櫃應置於資料中心防火牆之後。防火牆可確保只有透過已知的網路路徑才能存取這些系統，並依照需求監督與限制這些網路路徑。另外，也可以使用防火牆路由器

取代多部獨立的防火牆。建議儘可能指定允許連接磁帶櫃的主機，並封鎖所有其他主機。

## 將安全資訊保持在最新狀態

Oracle 會持續改善其軟體和文件。請查看本文件的每個版本，瞭解修訂項目。

# 2

# 安全安裝

本節概述安全安裝的規劃程序、描述數種建議的系統建置拓樸，以及說明如何保護磁帶櫃。

## 瞭解您的環境

為了更進一步瞭解安全需求，請考量下列問題：

### 需要保護哪些資源？

在實際執行環境中有許多資源可受到保護。決定您必須提供的安全等級時，請考慮需要保護的資源。

### 必須防止哪些人存取資源？

磁帶櫃必須受到保護，避免網際網路上的任何人及未經授權的內部網路使用者存取。

### 萬一策略性資源的保護失敗會如何？

在某些情況下，系統可以輕易偵測到安全方案中的失誤，因此只會造成輕微困擾。在其他情況下，失誤可能造成使用磁帶櫃的公司或個人客戶重大損失。瞭解每種資源的安全相關問題，有助於適當地保護資源。

## 保護磁帶櫃

磁帶櫃預設會使用表格 2.1, 「SL150 網路連接埠」中列示的連接埠。防火牆應設定為允許使用這些連接埠，同時封鎖任何未使用的連接埠。

**附表 2.1. SL150 網路連接埠**

| 連接埠 | 類型 | 描述 |
|---|---|---|
| 22 | TCP | SSH CLI 存取 – 內送狀態性<br>僅供開發測試與除錯之用，不可用於現場 |
| 25 | TCP | SMTP (不使用認證) |
| 67 | DHCP | 用戶端 - 外送 |
| 68 | DHCP | 用戶端 - 內送 |

| 連接埠 | 類型 | 描述 |
|---|---|---|
| 80 | HTTP | 遠端使用者介面的 WebLogic 連接埠 |
| 123 | NTP | 網路時間協定 (NTP) (啟用此功能時) |
| 161 | UDP | SNMP 磁帶櫃代理程式要求 - 內送狀態性 |
| 162 | UDP | SNMP 磁帶櫃攔截與告知通知 - 外送非狀態性攔截、外送狀態性告知 |
| 465 | TCP | SMTP (使用 SSL 或 TLS 認證) |
| 443 | HTTPS | 遠端使用者介面的 HTTPS WebLogic 連接埠 |
| 546 | DHCPv6 | IPv6 DHCP 用戶端 - 外送 |
| 547 | DHCPv6 | IPv6 DHCP 用戶端 - 內送 |
| 33200-33500 | TRACEROUTE | 軟體開發使用 |

磁帶櫃的有效連接埠號碼選擇是使用保留的連接埠，或是依照上面表格清單的建議。合法的連接埠號碼是從數字 1 開始，0 並非合法的連接埠號碼。

基於機密、完整性與認證功能，在設定 SNMP 時強烈建議使用 SNMPv3 取代 SNMPv2c。

設定 SMTP 時，強烈建議使用 TLS 認證來取代 SSL 或無認證選項。

# 安裝配置

本節說明安裝期間必須變更的安全配置。

## 指定使用者 (admin) 密碼

首次開啟電源時，本機操作面板上會自動執行設定精靈，以取得基本配置資訊。這包含管理員帳號使用者名稱與密碼、網路設定，以及其他基本設定。

完成設定精靈之後，磁帶櫃才能開始運作。

安裝人員必須在設定精靈的第一個步驟中，輸入產品出廠時提供的登入帳號。使用者接著必須輸入新密碼，才能完成安裝精靈。

完成初始安裝精靈並完全啟動磁帶櫃之後，可以透過適用於所有磁帶櫃設定的瀏覽器使用者介面 (BUI) 對進行磁帶櫃配置的其他修改。

## 強制密碼管理

必須對所有密碼套用基本密碼管理規則 (例如密碼長度、歷史記錄及複雜程度)。SL150 密碼必須是 8 到 128 個字元，且必須至少包含一個數字或特殊字元。預設密碼必須在安裝期間變更，且不可重複使用。

**注意:**

顯示的字元數目會經過遮罩，並不代表輸入字元的確實數目。

# 瀏覽器 UI 認證

限制存取遠端使用者介面所使用的瀏覽器設定值維持在 TLS 1.0 或更高版本，以減輕韌體等級低於版本 2.50 的 CVE-2014-3566 漏洞所造成的風險。在版本 2.50 的磁帶櫃韌體中，將不會自動降為使用 SSLv3。

# 3

# 安全功能

本節概述產品提供的特定安全機制。

磁帶櫃提供內部防火牆以自我保護。這不應該是保護磁帶櫃的唯一安全防線。建議將磁帶櫃置於受到實體保護的資料中心，且資料中心應位於安全網路，僅允許從使用其功能的伺服器來存取。這些伺服器與在上面執行的應用程式均應受到保護。

使用者帳號應限制為 *operator* 角色層次，而不要將 *admin* 角色層次授權給所有使用者。應熟悉 *service* 使用者角色的正確使用。視需要建立、啟用或停用 *service* 使用者角色帳號。service 角色具有較 *operator* 更大的權限，幾乎具有和 *admin* 角色相同的授權。

若因調查用途而需要磁帶櫃活動歷史記錄，可以複查和匯出「活動日誌 (Activity Log)」以供進一步的分析。使用者介面上的「活動日誌 (Activity Log)」會顯示使用者登入、主機或 UI 起始的動作以供追蹤。

# 4

# 重新建置

本節描述如何將磁帶櫃還原為出廠預設狀態，以清除任何客戶資料。

若客戶想要使磁帶櫃退役，可使用提供的程序，移除所有客戶配置資訊與所有日誌檔，並將磁帶櫃還原為出廠預設狀態。若要呼叫此程序，請將磁帶櫃置於 "locate" 模式，接著同時按住前後的 locate 按鈕 10 秒鐘以上，然後放開這兩個按鈕。

按住 Locate 按鈕的時間足夠時會以 LED 燈號的變更指示，LED 燈號的閃爍會從慢變快。

# 附錄 A

# 安全建置檢查清單

下列安全檢查清單包含協助保護磁帶櫃的指示：

1. 對所有使用者帳號強制進行密碼管理。
2. 強制存取控制，無論是實體的接觸還是透過介面 (如 SCSI、UI、SNMP... 等等) 存取。
3. 限制網路存取。
   a. 應實作防火牆。
   b. 防火牆絕對不可被入侵。
   c. 系統存取應受到監督。
   d. 網路 IP 位址應受檢查。
   e. 服務中的部分工具可能需要正確密碼或存取控制受到監督 (例如 SDP-2 以允許自動下載日誌資訊或其他存取)
4. 若在 Oracle Tape Library 中發現漏洞，請聯絡 Oracle Services、Oracle Tape Library Engineering 或客戶代表。
5. SMTP 應改用 TLS，而不要使用保護性較低的協定，例如 SSL 或沒有認證。
6. SNMP 應改設為 V3 等級，而不要使用 V2C 或功能較低的等級。

# 附錄 B

# 參考資料

*SL150 User Guide* 位於：

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

您可以在編號 E35103-07 的線上文件集中找到 SL150 的所有相關文件。