StorageTek T10000D

安全指南

E50325-04

2016 年 8 月

ORACLE

StorageTek T10000D
安全指南

E50325-04

內容

附表目錄

前言

本文件說明 Oracle StorageTek T10000D 的安全功能。

對象

本指南適用於使用 StorageTek T10000D 安全功能、安全安裝及組態的相關人員。

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

第 1 章 簡介

本節提供 StorageTek T10000D 磁帶機的簡介，並說明磁帶機安全一般原則。

產品簡介

企業級磁帶機 T10000D 可透過光纖通道協定連接開放式系統 SCSI，以及透過 FICON 協定連接大型主機。T10000D 磁帶機可與主機相互傳輸資料，並將資料儲存在可移除的磁性媒體上。T10000D 磁帶機針對企業客戶高工作週期與可靠性的需求，提供高度可靠、高容量備份、歸檔及資料處理能力。本產品提供選擇性的資料加密。客戶可選擇啟用加密功能。磁帶機產品加強了容量與原生磁帶速度。此外，也加入了資料管理功能。

T10000D 的容量與效能

T10000D 磁帶機具備最高可達 8.5TB 的容量，及每秒 252 MB 的原生磁帶速度。

安全

T10000D 磁帶機的設計與文件均註明其適用於受控制的硬體環境。磁帶機應位於受控制的資料中心內，且通常位於磁帶櫃內部。在某些情況下，客戶會使用機架式版本，但很少見。受控制的資料中心也應位於防火牆內，受到客戶本身安全原則的保護。如此可提供最佳的功能與保護，使得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。本文件的預設軟體等級為：

T10000D 4.XX.1XX

限制網路存取

磁帶機應維持在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，防火牆路由器可取代多部獨立的防火牆。建議儘可能指定允許連接磁帶機的主機，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

第 2 章 安全安裝

本節概述安全安裝與組態的規劃及實作程序、描述數種建議的系統部署拓樸，以及說明如何保護磁帶櫃。

瞭解環境

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？

在生產環境中可保護許多資源。決定您必須提供的安全等級時，請考慮需要保護的資源。

必須保護資源避免哪些人存取？

磁帶機必須受到保護，避免網際網路上任何人的存取。但是，企業內部網路中的員工是否可存取磁帶機？

萬一策略性資源的保護失敗會如何？

在某些情況下，可以輕易偵測到安全方案中的失誤，只會造成輕微困擾。在其他情況下，失誤可能造成使用磁帶機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。

保護磁帶機

磁帶機預設會使用下表列示的連接埠。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。磁帶機支援 IPv6 與 IPv4。

表格 2.1. 使用的網路連接埠

連接埠	T10000D
22 tcp - SSH VOP	X
22 tcp - SFTP	X
161 udp - SNMPV1 磁帶機代理程式要求 - 內送狀態性	X
162 udp - SNMPV1 磁帶機攔截與告知通知 - 外送非狀態性攔截、外送狀態性告知	X

連接埠	T10000D
23 tcp - TELNET	
21 tcp - FTP	
9842 tcp - EPT	
3331 OKM - 查問與根 CA 服務	X
3332 OKM – 註冊。加密強度為 AES256	X
3334 OKM – 加密金鑰交換。加密強度為 AES256	X
3335 OKM – 叢集尋找。加密強度為 AES256	X

對於 T10000D 的客戶，將會停用連接埠 21 與 23。如果客戶需要存取不安全的 TELNET 或 不安全的 FTP (或二者)，可使用 VOP 組態選項。

安裝 Virtual Operator Panel (VOP)

安裝 VOP 的系統應和磁帶機一樣，位於受保護的網路基礎架構內。安裝 VOP 的系統應強制實施客戶存取控制，以確保限制對磁帶機的存取。請參閱表格 2.1, 「使用的網路連接埠」，瞭解 VOP 所使用的連接埠。

請參閱下列 VOP 使用者指南，取得從 Web 啟動的 VOP 安裝指示。

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

安裝後組態

本節說明安裝後必須變更的安全組態。

指定使用者 (admin) 密碼

客戶管理帳號密碼應由客戶在現場變更，並由客戶持有。密碼安全性要符合 Oracle 標準。磁帶機的生命週期中可使用不限數目的密碼。若忘記管理員密碼，可加以重設。第一個密碼為磁帶機出廠所附的預設密碼。

強制密碼管理

必須對管理員密碼套用基本密碼管理規則 (例如密碼長度與複雜程度)。

密碼管理規則至少需要下列規則其中之一。

- 長度必須介於 8 與 16 個字元之間
- 小寫 (a-z)
- 大寫 (A-Z)
- 數字 (0-9)
- 特殊字元 (.?;:"{}[]()!@#$%&, ...)

3

第 3 章 安全功能

本節概述產品提供的特定安全機制。

T10000D 磁帶機可使用安全通道與 Oracle Key Management System 通訊。T10000D 將會透過 SSH 和 SFTP 與 Virtual Operator Panel 通訊，同時會為客戶停用 TELNET 與 FTP。這些不應是保護磁帶機的唯一安全防線。磁帶機應置於受到實體保護的資料中心，資料中心應具有安全網路，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。此外，客戶可選擇提高磁帶機的加密等級。其中一個選擇是將他們的資料加密。

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機的指示：

1. 強制密碼管理。
2. 強制存取控制。
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。
4. 若在 Oracle 磁帶機中發現漏洞，請聯絡 Oracle Services、Oracle Tape Library Engineering 或客戶代表。

附錄 B

附錄 B. 參考資料

您可以從下列網址存取 VOP User Guide：

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