StorageTek Automated Cartridge System Library Software

安全指南

版本 8.4

E68253-01

2015 年 9 月

ORACLE

StorageTek Automated Cartridge System Library Software
安全指南

E68253-01

內容

前言

本文件描述 Oracle's StorageTek Automated Cartridge System Library Software (ACSLS) 及 ACSLS High Availability 解決方案 (ACSLS HA) 的安全功能。ACSLS HA 和 ACSLS SNMP 代理程式也同樣在 ACSLS 伺服器上執行，因此保護 ACSLS 伺服器便可保護 ACSLS、ACSLS HA 及 ACSLS SNMP 代理程式。

對象

本指南適用於使用 ACSLS 安全功能、安全安裝及配置的相關人員。

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 ACSLS 的簡介並說明一般應用程式安全原則。

注意:

在本文件中，Automated Cartridge System Library Software 產品簡稱為 ACSLS，ACSLS High Availability 解決方案則簡稱為 ACSLS HA。

產品簡介

ACSLS 是 Oracle 的磁帶櫃伺服器軟體，可控制一或多部開放系統用戶端所使用的 StorageTek 磁帶櫃。Automated Cartridge System (ACS) 是透過 pass-thru-ports (PTPs) 連線的磁帶櫃或磁帶櫃群組。ACSLS 透過在網路間傳送的「控制路徑」指令，控制管理一或多個 ACS 。本軟體包括系統管理員件、用戶端系統應用程式的介面，以及磁帶櫃管理設備。

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。本文件假設您正在執行 ACSLS 8.4 或更新版本，並應用所有相關維護。執行最新的 ACSLS 版本可確保您具備最新的增強功能與修正。

將所有重要安全修正程式套用至作業系統和隨作業系統安裝的服務。請慎重套用這些修正程式，因為套用所有可用的更新可能會安裝新功能，甚至是尚未測試過 ACSLS 和 ACSLS HA 的新作業系統版本。

限制對重要服務的網路存取

將 ACSLS 及其管理的磁帶櫃保持在防火牆之後。建議使用專用網路來進行 ACSLS 和磁帶櫃之間的 TCP/IP 通訊。

遵循最低權限的原則

最低權限的原則是指使用者應被授予最少的權限來執行他們的工作。應定期複查使用者權限以判斷與現有工作責任的關聯。

在 ACSLS 上，這表示僅使用 cmd_proc 發出例行指令的操作者應以 acssa 使用者身分登入。以 acsss 使用者身分登入的系統管理員，同時具備眾多公用程式和配置指令的存取權。一般作業不需要使用 acsdb 使用者 ID。

監督系統活動

系統安全仰賴於三個條件：良好的安全協定、正確的系統配置以及系統監督。稽核並複查稽核記錄可解決第三項需求。系統內的每個元件都具備某種程度的監督功能。依循本文件中的稽核建議並定期監督稽核記錄

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配置的規劃及實作程序，並描述建議的 ACSLS 建置拓樸。

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？

ACSLS 管理的主要資源有磁帶櫃、磁帶機以及磁帶匣。必須保護它們不受到無意或惡意的存取。例如，防止有人使用不同伺服器上不同密碼的 ACSLS 使用者 ID，意外登入其他 ACSLS 伺服器。

必須保護資源避免哪些人存取？

您要保護磁帶儲存裝置資源不受未經授權的內部及外部存取。

萬一策略性資源的保護失敗會如何？

ACSLS 可以在磁帶機上掛載磁帶匣。如果使用者可以透過資料路徑連線至磁帶機，而磁帶上的資料未經加密，則使用者可加以讀取。

具備 ACSLS 和磁帶櫃存取權的使用者能夠從磁帶櫃送入與退出磁帶匣。

建議的保護 ACSLS 程序

保護 ACSLS 及必要的基礎架構元件時，請遵循本程序以確保 ACSLS 在經過變更之後仍可繼續運作：

- 安裝 ACSLS。
- 驗證 ACSLS 是否正確運作。其中包括配置與稽核磁帶櫃、掛載與卸載磁帶、送入與退出磁帶，以及備份與復原資料庫。
- 實作增進安全的變更。
- 驗證 ACSLS 仍可正確運作。

保護 ACSLS 網際網路通訊

本節描述建置 ACSLS 以保護網際網路存取的建議。

將 ACSLS 和磁帶櫃保護在企業防火牆之後

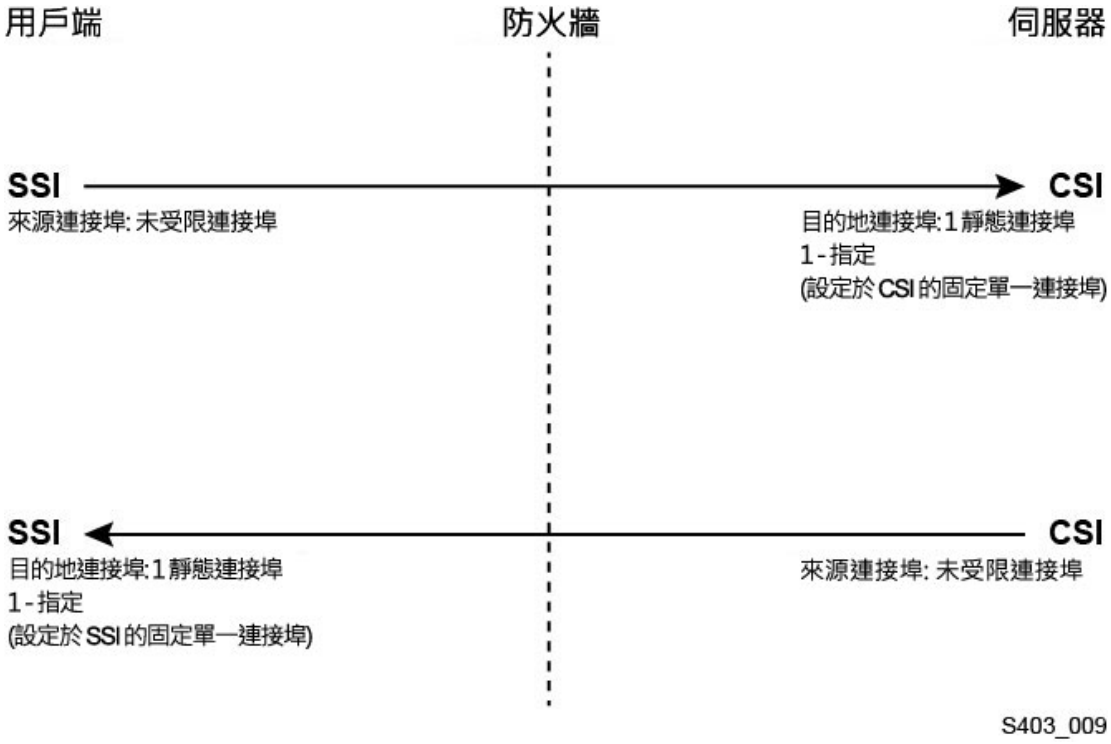
ACSLS 及其支援的磁帶櫃應建置在企業防火牆之後。如果遠端工作的人員需要登入 ACSLS 伺服器，可以透過 VPN 來存取。

注意:

如果您有以 IPv4 為基礎的邊緣防火牆 (Edge Firewall)，應將它配置為刪除所有外送 IPv4 協定 41 的封包和 UDP 連接埠 3544 的封包，以防止網際網路主機使用任何 IPv6-over-IPv4 通道流量來連線內部主機。

ACSLS 防火牆安全選項

如果使用 ACSLS 來掛載磁帶及管理磁帶櫃的用戶端應用程式，和 ACSLS 之間被防火牆隔開，建議您啟用「防火牆安全選項」。即使用戶端應用程式和 ACSLS 不是被防火牆隔開，實作「防火牆安全選項」仍可限制 ACSLS 與其用戶端應用程式之間的通訊所使用的連接埠，提供額外的 ACSLS 安全，如下所示。基於這些原因，在 ACSLS 8.1 和更新版本中，CSI_FIREWALL_SECURE 靜態變數預設為 TRUE。



如需詳細資訊，請參閱 *ACSLS Administrator's Guide* 中的附錄 "Firewall Security Option"。

用於 ACSLS 通訊的乙太網路連接埠

- ACSLS 伺服器使用下列連接埠。請確定已配置所有防火牆，允許這些連接埠的流量。包括由 Solaris 的 ipfilter 或 Linux 的 iptables 所實作的防火牆。
  - 22 雙向 – 用於 ssh 存取。

- 111 portmapper，除非 portmapper 已經停用。
- 115 用於 SFTP (安全檔案傳輸協定)。
- ACSLS SNMP 代理程式的設預設連接埠 161 - get/set/walk。
- ACSLS SNMP 代理程式的預設連接埠 162 - traps。

注意:

ACSLS SNMP 代理程式所使用的連接埠可使用下列指令配置：*AcslsAgtdSnmpConf [-p port] [-t trap port] [-d]*。 *-d* 選項會顯示目前的設定。 變更連接埠設定後，您必須使用下列指令重新啟動代理程式：*agentRegister*。

- 從 ACSLS 到 PostgreSQL 資料庫之內部通訊的預設連接埠 5432 (acsss 使用者 ID 的 PGPORT 環境變數)。

  如果連接埠 5432 已被使用，則會使用下一個可用、號碼較大的連接埠。

注意:

連接埠 5432 必須只能從 localhost (127.0.0.1) 存取。

- 7001 和 7002 - 用於 WebLogic 和 ACSLS GUI。
- 30031 或 ACSLS CSI 的監聽連接埠，由 CSI_INET_PORT 設定。
- 連接埠 50003，用於從 ACSLS GUI 和 Java 元件至傳統 ACSLS 處理的內部通訊。這個項目不可配置。

- 對於透過 ACSAPI 與 ACSLS 通訊的用戶端應用程式，必須開啟下列連接埠：
  - 用戶端應用程式必須能夠與 ACSLS CSI 的監聽器連接埠通訊。此連接埠預設為 30031，是由 CSI_INET_PORT 靜態變數所設定。

    您可以從 Unix shell 使用下列指令，找出 ACSLS 使用哪個連接埠來監聽來自 ACSAPI 用戶端的要求：

    ```
    rpcinfo -p | egrep "300031 | 536871166"
    ```

    連接埠 ID 會列在畫面的最後一欄。
  - ACSAPI 用戶端 (例如，NetBackup 或 SAM-QFS 伺服器) 會使用 SSI_INET _PORT 環境變數設定固定的內送連接埠。請指定範圍 1024-65535 的連接埠，並排除連接埠 50001 和 50004。ACSLS 伺服器必須能夠與此連接埠通訊。

注意:

在 ACSAPI 用戶端伺服器上，連接埠 50001 和 50004 是用於 AF_INET 網域 IPC 到「迷你事件記錄器」的通訊，以及從用戶端應用程式到 SSI 的通訊。

請參閱 *ACSLS Administrator's Guide* 的附錄 Firewall Security Option，瞭解用戶端應用程式和 ACSLS 之間通訊的進一步詳細資訊。

- 若已安裝 XAPI 元件，XAPI 伺服器會使用固定的監聽連接埠來接收來自 ELS 用戶端的內送 TCP 要求。XAPI 監聽連接埠是由 XAPI_PORT 靜態變數定義。XAPI

_PORT 預設為 50020。它必須介於 1024 到 65535 之間，且不能和 ACSLS 或其他應用程式使用的任何其他連接埠相衝突。

請參閱 *ACSLS Adiminstrator's Guide* 中的 XAPI Client Interface 附錄，瞭解關於 XAPI_PORT 的詳細資訊。此附錄還提供關於如何顯示與設定 XAPI_PORT 靜態變數的詳細資訊。

- 必須在 SL8500 或 SL3000 磁帶櫃開啟的連接埠：

  ACSLS 與 SL8500 或 SL3000 磁帶櫃之 2A 和 2B 乙太網路連線上的這些連接埠通訊。如果 ACSLS 對這些連接埠的通訊被封鎖，ACSLS 就無法管理磁帶櫃。
  - 50001 – 用於 ACSLS 和磁帶櫃之間的所有一般通訊
  - 50002 – ACSLS HA 用來在替代節點失敗之前，判斷替代 HA 節點是否能與磁帶櫃通訊。

配置 ACSLS 伺服器上執行的防火牆

除了外部防火牆之外，還可以透過 Solaris 的 ipfilter 或 Linux 的 iptables 在您的 ACSLS 伺服器上實作防火牆保護。此處描述如何管理 ACSLS 伺服器上執行的這些防火牆。

- 管理 Solaris 上的 ipfilter：

  請參閱 ipf 和 ipfilter 線上手冊以瞭解詳細資訊。
  - 'root' 可使用下列指令啟用 (停用) ipfilter 防火牆：

    ```
    svcadm enable ipfilter (svcadm disable ipfilter)
    ```
  - 瞭解 ipfilter 目前的狀態：

    ```
    svcs ipfilter
    ```
  - 防火牆原則定義於右列檔案中：/etc/ipf/ipf.conf

    若要允許本機主機上的元件之間 (例如 ACSLS 和 WebLogic 之間，或 GUI 和 ACSLS 資料庫之間) 的自由通訊，請包括像下列這樣的一行敘述句：

    ```
    pass in quick from 127.0.0.1 to 127.0.0.1
    ```

    或

    ```
    pass in quick from 127.0.0.1 to all
    ```

    您必須定義允許存取 ACSLS 所需之所有連接埠的原則。例如，若要包括允許遠端 Web 式瀏覽器存取 ACSLS GIU 的原則，您必須開啟連接埠 7001 和 7002。

    ```
    pass in quick from any to any port = 7001
    ```

    ```
    pass in quick from any to any port = 7002
    ```

找出 ACSLS 使用哪些連接埠來監聽 ACSAPI 用戶端的要求之後，請針對這些連接埠一一新增 'pass in quick' 敘述句。

可能必須針對 RPC portmapper 連接埠 111 新增一行 'pass in quick' 敘述句。

規則集中的最後一個敘述句 "block in from any"，說明除非前面的敘述句允許，否則不允許任何流量連線該主機。

- 管理 Linux 上的 iptables：
  - 'root' 可使用下列指令啟用 (停用) iptables 防火牆：

    ```
    service iptables start (service iptables stop)
    ```
  - 檢查 iptables 的狀態：

    ```
    service iptables status
    ```
  - iptables 的原則檔是 /etc/sysconfig/iptables:

    您必須定義允許存取 ACSLS 所需之所有連接埠的原則。例如，若要包括允許遠端 http/https 存取 ACSLS GUI 的原則，您應該使用像下面這樣的敘述句更新該檔案，以包括連接埠 7001 和 7002：

    ```
    -A input -p tcp --dport 7001 -j ACCEPT
    ```

    ```
    -A input -p tcp --dport 7002 -j ACCEPT
    ```

    找出 ACSLS 使用哪些連接埠來監聽 ACSAPI 用戶端的要求之後，您必須將這些例外一一加入 iptables 原則檔案中。可能必須針對 RPC portmapper 連接埠 111 包括一行例外敘述句。

安裝與配置 Solaris

本節描述如何安全地安裝與配置 Solaris。

建議包括：

- 將所有重要安全修正程式套用至作業系統和隨作業系統安裝的服務。請慎重套用這些修正程式，因為套用所有可用的更新可能會安裝新功能，甚至是尚未測試過 ACSLS 和 ACSLS HA 的新作業系統版本。
- 停用 telnet 和 rlogin。請改用 ssh。同時停用 ftp，並改用 sftp。

  以 root 身分發出下列指令，停用 telnet、rlogin 及 ftp 服務。

  查看所有服務：

  ```
  svcs
  ```

  停用 telnet、rlogin 及 ftp：

```
svcadm disable telnet

svcadm disable rlogin

svcadm disable ftp
```

- 請勿停用 ssh。要求使用者使用 ssh 從遠端登入 ACSLS，而不要使用 telnet 或 rlogin。同時請勿停用 sftp。
- ACSLS 需要 rpc-bind。請勿予以停用。

  如果 Solaris 是使用 Secure by Default 選項安裝的，您必須更改 rpc-bind 的網路配置特性，允許 ACSAPI 用戶端傳送要求給 ACSLS。

  請參閱 *ACSLS Installation manual* 中 "Installing ACSLS on Solaris" 一章的 "Installing Solaris" 小節，瞭解詳細資訊。
- ACSLS 伺服器上的部分乙太網路連接埠必須開啟，才能與 ACSLS 通訊。用戶端應用程式使用特定的乙太網路連接埠與 ACSLS 通訊，而 ACSLS 與磁帶櫃上特定的連接埠通訊。請參閱用於 ACSLS 通訊的乙太網路連接埠，瞭解必須可供 ACSLS 通訊使用的連接埠。在 ACSLS 伺服器上，確定 ipfilter 已配置為允許 ACSLS 所使用之連接埠的流量。

判斷您的 Solaris 稽核原則。"Oracle System Administration: Security Services" 中的 ”Auditing in Oracle Solaris” 小節，可協助您規劃要稽核的事件、應儲存稽核日誌的位置以及如何複查稽核日誌。

安裝與配置 Linux

安全地安裝與配置 Linux 的建議：

- 將所有重要安全修正程式套用至作業系統和隨作業系統安裝的服務。請慎重套用這些修正程式，因為套用所有可用的更新可能會安裝新功能，甚至是尚未測試過 ACSLS 和 ACSLS HA 的新作業系統版本。
- 確定未安裝或已經停用 telnet 和 rlogin。請改用 ssh。

  並確定未安裝或已經停用 ftp，並改用 sftp。

  若要查看所有服務，請以 root 身分登入並使用下列指令：

  ```
  service --status-all
  ```
- 若要永久刪除服務，請使用：

  ```
  svccfg delete -f service-name
  ```
- 請勿停用 ssh。要求使用者使用 ssh 從遠端登入 ACSLS，而不要使用 telnet 或 rlogin。同時請勿停用 sftp。
- 必須啟用網路服務 (特別是 rpcbind) 以允許 ACSLS 用戶端通訊。

  在 Linux 上啟動 rpc 時，請使用 –i 旗標啟動。

- ACSLS 伺服器上的部分乙太網路連接埠必須開啟，才能與 ACSLS 通訊。用戶端應用程式使用特定的乙太網路連接埠與 ACSLS 通訊，而 ACSLS 與磁帶櫃上特定的連接埠通訊。請參閱用於 ACSLS 通訊的乙太網路連接埠，瞭解必須可供 ACSLS 通訊使用的連接埠。在 ACSLS 伺服器上，確定 iptables 已配置為允許 ACSLS 所使用之連接埠的流量。

稽核 Linux 安全

判斷您的 Linux 稽核原則。*Oracle Linux: Security Guide for Release 6* 中的 ”Configuring and Using Auditing” 小節，可協助您規劃要稽核的事件、應儲存稽核日誌的位置以及如何複查稽核日誌。

部分有用的日誌及稽核 Linux 安全的指令包括：

- 以 root 身分檢視 var/log/secure，查看登入嘗試的歷史記錄及其他存取訊息。
- 'last | more' 指令可提供使用者登入的歷史記錄。
- /var/log/audit/audit.log.[0-9] 保存 SE Linux 所拒絕之存取嘗試的日誌。您必須是 root 使用者才能檢視這些日誌。

SELinux 安全

設計 ACSLS 8.4 的目的是為了讓您能夠在選用的 Security Enhanced Linux 環境中執行。SELinux 除了標準 Unix 環境下可用的傳統保護之外，還提供對檔案、目錄及其他系統資源的存取控制。除了 owner-group-public 權限存取，SELinux 還包括根據使用者角色、網域及環境定義的存取控制。在所有系統資源上強制實施存取控制的代理程式是 Linux 核心。

Linux 系統上的 root 使用者可以使用 *`setenforce`* 指令，設定強制開啟或關閉。

```
setenforce [Enforcing | Permissive | 1 | 0 ]
```

使用 *`Enforcing`* 或 1 會讓 SELinux 處於強制模式。使用 *`Permissive`* 或 0 會讓 SELinux 處於寬容模式

若要檢視目前的系統強制狀態，請使用 *`getenforce`* 指令。

當您安裝 ACSLS 時，會有 3 個 SELinux 原則模組被載入核心中：allowPostgr、acsdb 及 acsdb1。這些模組可在 SELinux 強制作用時，提供 ACSLS 存取自己的資料庫和其他系統資源所需的定義和強制例外。隨著這些模組的安裝，您應該能夠執行包括資料庫作業 (像是 bdb.acsss、rdb.acsss、db_export.sh 及 db_import.sh) 的一般 ACSLS 作業，而不需停用 SELinux 強制。

如需詳細資訊，請參閱 *StorageTek ACSLS 8.4 Administrator’s Guide* 中附錄 ”Troubleshooting” 的 SELinux 小節。

安裝與配置 ACSLS

本節說明如何安全地安裝 ACSLS。

執行標準 ACSLS 安裝

執行標準 ACSLS 安裝，確保您具備所有需要的元件。

如果您是從舊版 ACSLS 移轉至新版的 ACSLS，請複查動態和靜態變數的設定，檢查您是否要使用更多的安全選項，特別是防火牆安全相關選項。

為 ACSLS 使用者 ID 使用更安全的密碼

ACSLS 需要右列 ACSLS 使用者 ID：acsss、acssa 及 acsdb。請為這些 ID 選擇更安全的密碼，並定期變更密碼。

限制 ACSLS 檔案的存取權

ACSLS 一般會將 ACSLS 檔案的存取權限制為只有 acsls 群組，此群組包括 acsss、acssa、acsdb 及 root 使用者 ID。部分資料庫和診斷檔案只能由單一 acsls 使用者 ID 存取。ACSLS 使用 umask 設定值 027 執行。

不應將 ACSLS 檔案開放給所有人讀取或寫入。但是，存取權的限制如果比安裝預設值還要嚴格，可能會導致 ACSLS 運作失敗。

將 'root' 設為三個 ACSLS 檔案的有效使用者 ID

安裝命令檔會建議客戶必須將 'root' 設為 /export/home/ACSSS 檔案系統中三個可執行檔的有效使用者 ID (setuid) ：

- *`acsss`* (此二進位檔案必須以 'root' 權限執行，因為它是用來啟動與停止 ACSLS 應用程式所需的系統服務。)
- *`db_command`* (此二進位檔案可啟動與停止控制與維護 ACSLS 資料庫的 PostgreSQL 資料庫引擎。)
- *`get_diags`* (此二進位檔案由客戶所呼叫，其作用在於收集綜合系統診斷資訊，與客服人員溝通時可能需要這些內容。)

使用 pkgadd 安裝 ACSLS 期間，會提示客戶 *`Do you want to install these as setuid/setgid files?`* 回答 *`y`*，表示您允許 acsls 群組中的使用者執行這三個指令，即使這些公用程式執行需要 root 權限的特定系統作業亦然。

複查 ACSLS 靜態和動態變數的設定

ACSLS 靜態和動態變數控制許多 ACSLS 功能的行為方式。請使用 *`acsss_config`* 公用程式來設定這些變數。本文件中討論許多這些變數的安全設定。當 *`acsss_config`* 顯示某變數的選項時，使用問號 (?) 回覆將會顯示該變數的詳細說明。此資訊同時可在 *ACSLS Administrator's Guide* 的 "Setting Variables that Control ACSLS Behavior" 章節中取得。

配置 WebLogic

ACSLS 8.1 及更新版本使用 WebLogic 作為 Web 伺服器。WebLogic 會隨 ACSLS 一同安裝。

請參閱 *Oracle Fusion Middleware; Understanding Security for Oracle WebLogic Server 11g Release 1 (10.3.6)*，瞭解保護 WebLogic 伺服器的選項，以及可能隨 WebLogic 產生的稽核歷程檔。

使用 ACSLS userAdmin.sh 公用程式來建立與維護 ACSLS GUI 使用者

`userAdmin.sh` 功能表導向公用程式可用來管理 ACSLS GUI 使用者密碼。您可以新增使用者、移除使用者、列出使用者，以及變更使用者密碼。必須執行 WebLogic 才能使用此公用程式。如果未啟動，此公用程式會啟動 WebLogic 並確認它已上線，才會顯示功能表。

`userAdmin.sh` 公用程式必須由 root 執行，且需要 acsls_admin 認證。acsls_admin 使用者帳戶是在安裝 ACSLS 期間配置的。

使用 ACSLS GUI

若要使用 ACSLS GUI，您必須安裝最新的 JRE 版本，並透過瀏覽器存取 ACSLS GUI。

在 GUI 用戶端系統上安裝最新的 JRE 版本

確定最新版本的 Java Runtime Environment (JRE) 已安裝在系統上，ACSLS GUI 將會使用它來存取 ACSLS。

存取 ACSLS GUI

開啟瀏覽器，並使用下列格式的伺服器主機名稱或 IP 位址輸入 URL：

`https://myAcslsHostName.myDomainName:7002/SlimGUI/faces/Slim.jsp` 或 *`https://127.99.99.99:7002/SlimGUI/faces/Slim.jsp`*

最好是使用主機機器的完整主機名稱或 IP 位址。如果 WebLogic 無法完整解析該 URL，某些頁面 (包括 ACSLS 說明頁面) 可能無法正確顯示。

如果您使用 http (連接埠 7001)，WebLogic 將會自動重新路由到連接埠 7002 上的 https。

由於 WebLogic 是使用安全 https 協定，您的瀏覽器可能會警告網站安全憑證尚未註冊，因此不受信任。如果您確信該 URL 是您本機的 ACSLS 機器，就可以安全地繼續。此時，您應該會看到登入畫面。

使用 ACSLS GUI

WebLogic 中的 AcslsDomain 可以使用 HTTPS 安全協定存取。此協定會使用私密金鑰和數位憑證，在瀏覽器與伺服器之間進行加密通訊。您可以使用下列方式來取得數位憑證：

ACSLS 示範憑證

ACSLS 隨附一個名稱為 'demo' 的憑證。可提供最低層次的加密安全，讓客戶無需任何進一步的配置步驟便可開始使用 ACSLS GUI。若客戶與 ACSLS 磁帶櫃的互動完全在安全的內部網路中，此示範憑證方法通常便已足夠。不過，某些瀏覽器並不支援此方法所使用的 512 位元加密金鑰，尤其是 Internet Explorer 及 FireFox 版本 39 和更新版本。

配置自行簽署的數位憑證

ACSLS Installation Guide 為 ACSLS 管理員提供了配置自行簽署、長度為 2048 位元之數位憑證的方法。在標題為 'Configuring an SSL Encryption Key' 的小節中，此方法提供一個所有瀏覽器均支援的憑證。使用者在存取使用自行簽署憑證的 HTTPS 網站時，會被建議不要繼續存取該網站，除非使用者具備個人知識，瞭解此 Web 資源是信任的網站。如果是 ACSLS 使用者和磁帶櫃控制伺服器，通常可以完全瞭解此信任等級，而且在大多數情況下，並不需要網站使用第三方簽章驗證來證明其完整性。

由第三方簽署授權機構簽署的數位憑證

保留讓每個客戶網站決定是否需要由第三方簽署授權機構 (例如 Verisign 或 Entrust .net) 提供憑證認證。Oracle 線上文件 Configuring Identity and Trust 中描述了產生這類簽署數位憑證的程序，網址為：

http://docs.oracle.com/cd/E13222_01/wls/docs92/secmanage/identity_trust.html

安裝 ACSLS HA

如果您是使用 ACSLS High Availability 解決方案，請遵循 ACSLS-HA Cluster: Installation, Configuration, and Operations 中的指示。

3

第 3 章 安全功能

本節描述 ACSLS 提供的特定安全機制。

安全模型

為了因應保護資料的需要，ACSLS 安全需求應運而生，其主要目的在於：第一，避免意外失去和損毀資料。第二，保護資料不受未經授權的存取或更改。其他關注的焦點包括避免存取或使用資料時不必要的延遲，或避免遭受拒絕服務的干擾。

提供這些保護的重要安全功能包括：

- 認證 – 確保只有經過授權的個人才能夠存取系統和資料。
- 授權 – 提供對系統權限和資料的存取控制。此功能的基礎建立在認證上，可確保個人只能得到適當的存取權。
- 稽核 – 可讓管理員偵測到違反認證機制的嘗試，以及違反或成功的存取控制嘗試。

配置與使用認證

在 Linux 或 Solaris 上預設會使用 PAM (可插式認證模組) 來認證 ACSLS 使用者。請參閱 Solaris 線上手冊，或 *Linux-PAM System Administrators Guide*。

在 WebLogic 中，會使用內嵌的 LDAP 伺服器來認證 ACSLS GUI 使用者。請參閱文件 Managing the Embedded LDAP Server，網址為：

`http://docs.oracle.com/cd/E13222_01/wls/docs81/secmanage/ldap.html`

由 Solaris 或 Linux 作業系統認證的 ACSLS 使用者認證

ACSLS 使用者：acsss 和 acssa 必須先登入 Solaris 或 Linux 並經過作業系統認證，才能夠使用 cmd_proc，或是執行 ACSLS 公用程式與配置指令 (acsss 使用者)。acsdb 使用者 ID 同時用於資料庫相關作業。在 ACSLS 安裝程序期間，客戶必須為這些 ID 設定第一次登入時使用的密碼。請參閱 *ACSLS Installation Guide* 以瞭解詳細資訊。

由 WebLogic 認證的 ACSLS GUI 使用者

ACSLS GUI 使用者必須登入並經過 WebLogic 認證。acsls_admin 是在 ACSLS 安裝期間建立的，客戶必須設定它的密碼。客戶可以使用 *`userAdmin.sh`* 公用程式，

視需要建立其他 GUI 使用者。如需詳細資訊，請參閱 *ACSLS Installation Guide* 及 *ACSLS Administrator's Guide* 之 "Utilities" 章節中關於 `userAdmin.sh` 的小節。

稽核考量

這裡說明適用於 ACSLS 的一般稽核考量。

讓稽核資訊保持在可管理的狀態

雖然稽核的成本相對較為低廉，還是要儘可能限制稽核事件的數目。這樣做可將執行稽核敘述句對效能的影響以及稽核歷程檔的大小降至最低，使稽核歷程檔易於分析、瞭解與管理。

設計稽核策略時，請運用下列一般指導方針：

評估稽核的目的

清楚瞭解稽核的原因之後，您就能夠設計適當的稽核策略，避免不必要的稽核。

聰明地稽核

稽核時使用取得目標資訊所需之最少數目的敘述句、使用者或物件。

配置與使用 ACSLS 稽核日誌

ACSLS 具有數種資訊的日誌，可讓您記錄與檢查 ACSLS 活動。

- 您可以使用 vi 或其他編輯程式來檢視大部分的記錄。「系統事件」只能使用 ACSLS GUI 來檢視。
- 大多數的日誌都可以在達到客戶定義的大小、客戶指定的保留日誌數目時自動歸檔。為了避免塞滿 ACSLS 檔案系統，可以配置限制保留的日誌數目。如果您想要保留較多的日誌檔，或是將它們保留在其他系統上，您必須開發自己的程序來將它們歸檔在足夠空間的位置。
- 要保留之歸檔日誌的大小、數目以及這些檔案的其他特性，都是使用 ACSLS 動態和靜態變數來定義。

ACSLS 日誌目錄

ACSLS 日誌目錄是由 LOG_PATH 靜態變數所控制。預設為 $ACS_HOME/log 目錄。此目錄包含下列日誌：

acsss_event.log
記錄了重大的 ACSLS 系統事件、磁帶櫃事件以及錯誤的訊息。

當 acsss_event.log 達到 LOG_SIZE 動態變數所定義的臨界大小時，就會複製到 event0.log 並清除。在複製處理作業期間，保留事件日誌會複製到較高編號的保留日誌中，而最高編號的保留日誌會被覆蓋。例如：event8.log 會複製到 event9.log 上，event7.log 會複製到 event8.log 上 ...，event0.log 會複製到 event1.log

上，acsss_event.log 會複製到 event0.log 上，而 acsss_event.log 則會被清除。這是由下列變數所控制：

- *EVENT_FILE_NUMBER* 指定保留的事件日誌數目。
- *LOG_SIZE* 指定事件日誌要複製到保留事件日誌並截斷的臨界大小。

使用 *greplog* 公用程式可篩選 acsss_event 日誌，以包括或排除包含特定關鍵字的訊息。請參閱 *ACSLS Administrator's Guide* 之 "Utilities" 章節中的 greplog，以瞭解詳細資訊。

配置日誌
當 ACSLS 更新 ACSLS 資料庫中儲存的磁帶櫃組態時，會有兩個記錄詳細資訊的日誌。*acsss_config* 和 *Dynamic Config* (*config* 公用程式) 的配置變更會記錄在此。

acsss_config.log
記錄 ACSLS 支援之磁帶櫃的所有配置或重新配置詳細資訊。最新的配置變更會附加至先前的配置記錄。

acsss_config_event.log
記錄配置或重新配置處理作業期間的事件。

rpTrail.log
記錄 ACSAPI 用戶端或 cmd_proc 對 ACSLS 之所有要求的回應，以及對 GUI 或邏輯磁帶櫃 SCSI 用戶端介面的所有要求 (資料庫查詢除外) 的回應。記錄的資訊包括要求者、要求以及要求的時戳。

rpTrail.log 受到下列變數的管理：

- *LM_RP_TRAIL* 啟用此 ACSLS 事件稽核歷程檔。預設為 TRUE。
- *RP_TRAIL_LOG_SIZE* 指定要將 rpTrail.log 壓縮並歸檔的臨界大小。
- *RP_TRAIL_FILE_NUM* 指定要保留之歸檔 rpTrail 日誌的數目。
- *RP_TRAIL_DIAG* 指定 rpTrail 訊息是否應包括其他診斷資訊。預設為 FALSE。

磁帶櫃磁碟區統計資料
記錄影響磁帶櫃中的磁碟區 (磁帶匣) 的所有事件，包括掛載、卸載、移動、送入、退出磁碟區的時間，或是被稽核或磁帶匣復原發現的時間。如果啟用「磁帶櫃磁碟區統計資料」，此資訊會記錄在 acsss_stats.log 中。

「磁帶櫃磁碟區統計資料」受到下列變數的管理：

- *LIB_VOL_STATS* 啟用「磁帶櫃磁碟區統計資料」。預設為 OFF。
- *VOL_STATS_FILE_NUM* 指定要保留之歸檔 acsss_stats.log files 的數目。
- *VOL_STATS_FILE_SIZE* 指定要歸檔 acsss_stats.log 的臨界大小。

ACSLS Log/sslm 目錄

在 ACSLS 日誌目錄中，關於 ACSLS GUI 和邏輯磁帶櫃 SCSI 用戶端介面的資訊會記錄在 sslm 目錄中。此目錄包含 WebLogic 稽核日誌的連結。sslm 目錄包含下列日誌：

slim_event.g#.log[.pp#]
記錄 ACSLS GUI 和 SCSI 用戶端介面的事件。包括邏輯磁帶櫃配置變更的訊息，以及 SCSI 用戶端事件。

- .g# 是此日誌的世代編號。
- .pp# 是此日誌的平行處理編號。如果同時記錄了多個處理作業，其他處理作業的日誌就會被指派平行處理編號。

smce_trace.log
追蹤使用 SCSI Media Changer Interface 模擬從 SCSI 用戶端至 ACSLS 邏輯磁帶櫃的活動。

guiAccess.log
這是 WebLogic 之 access.log 的連結。請參閱配置與使用 WebLogic 稽核日誌。

AcslsDomain.log
這是 WebLogic 之 AcslsDomain.log 的連結。請參閱配置與使用 WebLogic 稽核日誌。

AdminServer.log
這是 WebLogic 之 AdminServer.log 的連結。請參閱配置與使用 WebLogic 稽核日誌。

從 GUI 的日誌檢視器 (Log Viewer) 檢視 ACSLS 稽核歷程檔

從 GUI 導覽樹狀結構的「配置 (Configuration)」和「管理 (Administration)」區段存取日誌檢視器。日誌檢視器可顯示從 acsss_event.log 和 smce_trace.log 結合的資訊。

從 GUI 檢視系統事件 (System Events)

您也可以從 GUI 導覽樹狀結構的「配置」和「管理」區段檢視「系統事件」。每個離散的磁帶櫃作業都會記錄在「系統事件」日誌中。此日誌中的每筆記錄都包含事件時戳、事件類型以及事件的描述。

配置與使用 Solaris 稽核日誌

判斷您的 Solaris 稽核原則。*Oracle System Administration: Security Services* 手冊中的 Oracle Solaris Auditing 小節可協助您規劃要稽核的事件、應儲存稽核日誌的位置以及複查稽核日誌的方式。

如果您尚未啟用自訂 Solaris 稽核歷程檔，則可使用 acsss、acsdb 及 acssa 使用者發出之登入指令和 Unix 指令的稽核歷程檔：

- 目前登入 Unix 的使用者會記錄在 Unix utmpx，而過去的使用者存取會記錄在 wtmpx 資料庫中。
- 使用 *`last`* 指令即可查看對某使用者 ID 的所有存取 (例如 *`last acsss`*)。如需詳細資訊，請參閱下列指令的線上手冊：wtmpx、*`last`* 及 getutxent。
- 使用者主目錄中的 .*_history (亦即 [點]*_history) 檔案記錄該使用者所發出的指令。

對於 acsss 使用者而言，可能包括：

- .bash_history
- .psql_history
- .sh_history

在 Solaris 上，/var/adm/sulog 會記錄執行 *su* 並成為超級使用者或其他使用者的成功或失敗嘗試。

配置與使用 Linux 稽核日誌

請參閱 *Oracle Linux: Security Guide for Release 6* 中的 Configuring and Using Auditing and Configuring and Using System Logging 小節，瞭解關於收集與分析稽核和系統日誌的詳細資訊。

配置與使用 WebLogic 稽核日誌

請參閱 *Oracle Fusion Middleware; Understanding Security for Oracle WebLogic Server 11g Release 1 (10.3.6)*，瞭解保護 WebLogic 伺服器的選項，以及可能隨 WebLogic 產生的稽核歷程檔。

WebLogic 在下列目錄中記錄對 ACSLS GUI 的存取：

/export/home/SSLM/AcslsDomain/servers/AdminServer/logs

此目錄包含下列檔案：

- access.log
  - 歸檔的版本命名為 access.log##### (例如 access.log00001)
  - 此檔案提供 GUI 使用者活動的詳細稽核歷程檔。
  - 若是用於登入，看起來會像是 ”AcslsLoginForm”。

    注意:

    右列檔案中會有一個存取日誌的連結：$ACS_HOME/logs/sslm/guiAccess.log。
- AcslsDomain.log
  - 此檔案報告 WebLogic 和 ACSLS GUI 作業。

    注意:

    右列檔案中會有一個存取日誌的連結：$ACS_HOME/logs/sslm/AcslsDomain.log。
- AdminServer.log
  - 此檔案報告 WebLogic 和 ACSLS GUI 作業。

    注意:

    右列檔案中會有一個存取日誌的連結：$ACS_HOME/logs/sslm/AdminServer.log。

4

第 4 章 開發人員的安全考量

本節提供的資訊對開發人員在開發或支援使用 ACSLS 管理 Oracle StorageTek 磁帶櫃的應用程式非常有用。

啟用用戶端應用程式伺服器上的防火牆安全

啟用防火牆安全，限制用於通訊的連接埠並停用用戶端應用程式伺服器上的 portmapper。請參閱 *CSC Developer's Toolkit User's Guide* 的 "Appendix B: Firewall-Secure Operation"。

附錄 A

附錄 A. 安全建置檢查清單

1. 強制密碼管理。
2. 限制網路存取。
   a. ACSLS 及其管理的磁帶櫃應位於企業防火牆之後。
   b. 啟用 ACSLS 防火牆安全選項。
   c. 請考慮啟用 ACSLS 用戶端應用程式的防火牆安全。
3. 強化 Solaris 或 Linux 作業系統。
4. 套用所有安全修正程式和解決方法。
5. 若在 StorageTek ACSLS 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

ACSLS 文件
ACSLS 文件儲存在依 ACSLS 版本整理的文件庫中。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#opensyssoft

(個別 ACSLS 文件庫在其 URL 中包含版本號碼。因此，特定文件庫的連結可能會在文件庫更新時變成無法使用)。ACSLS 文件包括：

- *ACSLS Installation Guide*
- *ACSLS Administrator's Guide*
- *ACSLS* 產品資訊

  其中包括軟體和硬體需求、ACSLS 簡介，再加上支援的磁帶櫃、磁帶機以及媒體。
- ACSLS 訊息 (及狀態代碼)
- *ACSLS Release Notes*
- *ACSLS-HA Cluster: Installation, Configuration, and Operations*
- *ACSLS Interface Reference Manual*

Oracle Solaris
Oracle Solaris 11.2 Information Library 中包含的 *Securing the Oracle Solaris 11 Operating System*。請參閱以瞭解詳細資訊。

Oracle Linux
Oracle Linux 6 Information Library 中包含的 *Oracle Linux 6 Security Guide*。請參閱以瞭解詳細資訊。

Oracle WebLogic
Oracle WebLogic Server Documentation Library 中 WebLogic 10.3.6 (ACSLS 8.2 使用此版本) 的 Security 小節。

Oracle Fusion Middleware; Understanding Security for Oracle WebLogic Server 11g Release 1 (10.3.6) 說明保護 WebLogic 伺服器的詳細資訊。