StorageTek Automated Cartridge System Library Software

安全指南

发行版 8.4

E68252-01

2015 年 9 月

ORACLE

StorageTek Automated Cartridge System Library Software
安全指南

E68252-01

版权所有 © 2015, Oracle 和/或其附属公司。保留所有权利。

本软件和相关文档是根据许可证协议提供的，该许可证协议中规定了关于使用和公开本软件和相关文档的各种限制，并受知识产权法的保护。除非在许可证协议中明确许可或适用法律明确授权，否则不得以任何形式、任何方式使用、拷贝、复制、翻译、广播、修改、授权、传播、分发、展示、执行、发布或显示本软件和相关文档的任何部分。除非法律要求实现互操作，否则严禁对本软件进行逆向工程设计、反汇编或反编译。

此文档所含信息可能随时被修改，恕不另行通知，我们不保证该信息没有错误。如果贵方发现任何问题，请书面通知我们。

如果将本软件或相关文档交付给美国政府，或者交付给以美国政府名义获得许可证的任何机构，则适用以下注意事项：

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

本软件或硬件是为了在各种信息管理应用领域内的一般使用而开发的。它不应被应用于任何存在危险或潜在危险的应用领域，也不是为此而开发的，其中包括可能会产生人身伤害的应用领域。如果在危险应用领域内使用本软件或硬件，贵方应负责采取所有适当的防范措施，包括备份、冗余和其它确保安全使用本软件或硬件的措施。对于因在危险应用领域内使用本软件或硬件所造成的一切损失或损害，Oracle Corporation 及其附属公司概不负责。

Oracle 和 Java 是 Oracle 和/或其附属公司的注册商标。其他名称可能是各自所有者的商标。

Intel 和 Intel Xeon 是 Intel Corporation 的商标或注册商标。所有 SPARC 商标均是 SPARC International, Inc 的商标或注册商标，并应按照许可证的规定使用。AMD、Opteron、AMD 徽标以及 AMD Opteron 徽标是 Advanced Micro Devices 的商标或注册商标。UNIX 是 The Open Group 的注册商标。

本软件或硬件以及文档可能提供了访问第三方内容、产品和服务的方式或有关这些内容、产品和服务的信息。除非您与 Oracle 签订的相应协议另行规定，否则对于第三方内容、产品和服务，Oracle Corporation 及其附属公司明确表示不承担任何种类的保证，亦不对其承担任何责任。除非您和 Oracle 签订的相应协议另行规定，否则对于因访问或使用第三方内容、产品或服务所造成的任何损失、成本或损害，Oracle Corporation 及其附属公司概不负责。

目录

前言

本文档介绍了 Oracle 的 StorageTek Automated Cartridge System Library Software (ACSLS) 和 ACSLS 高可用性解决方案 (ACSLS HA) 的安全功能。因为 ACSLS HA 和 ACSLS SNMP Agent 也在 ACSLS 服务器上运行，所以，保护 ACSLS 服务器将保护 ACSLS、ACSLS HA 和 ACSLS SNMP Agent。

目标读者

本指南的目标读者是要使用 ACSLS 的安全功能以及要安全可靠地安装和配置 ACSLS 的所有人。

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

第 1 章 概述

本部分概述了 ACSLS 并说明了应用程序的一般安全原则。

注意:

在本文档中，Automated Cartridge System Library Software 产品称为 ACSLS，ACSLS 高可用性解决方案称为 ACSLS HA。

产品概述

ACSLS 是 Oracle 的磁带库服务器软件，可以为开放式系统客户机控制一个或多个 StorageTek 磁带库。自动化磁带系统 (Automated Cartridge System, ACS) 是一个磁带库或一组通过直通端口 (pass-thru-port, PTP) 连接的磁带库。ACSLS 通过在网络间发送的 "control path" 命令来管理一个或多个 ACS。该软件包括系统管理组件、与客户机系统应用程序的接口和磁带库管理工具。

一般安全原则

以下原则是安全使用任何产品的基本原则。

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。本文档假定您运行的是 ACSLS 8.4 或更高发行版，并应用了所有相关维护。运行最新的 ACSLS 发行版可确保您拥有最新的增强和修复功能。

向 OS 以及随 OS 安装的服务应用所有重要的安全修补程序。请有选择地应用这些修补程序，因为应用所有可用更新可能会安装尚未针对 ACSLS 和 ACSLS HA 测试的新功能甚至是新的 OS 发行版。

限制对关键服务的网络访问

使 ACSLS 及其管理的磁带库位于防火墙后面。建议使用专用网络在 ACSLS 和磁带库之间进行 TCP/IP 通信。

遵循最小特权原则

最小特权原则是指应当向用户授予履行其职责所需的最小特权。应定期查看用户特权，以确保仅授予与当前工作职责相关的特权。

在 ACSLS 上，这意味着仅使用 cmd_proc 发出常规命令的操作员应该以 acssa 用户身份登录。以 acsss 用户身份登录的系统管理员还可以访问大量的实用程序和配置命令。对于常规操作，无需使用 acsdb 用户 ID。

监视系统活动

系统安全依靠以下三方面：良好的安全协议、合适的系统配置以及系统监视。审计和查看审计记录可满足系统安全性的第三个要求。系统中的每个组件都具有一定程度的监视能力。请遵循本文档中的审计建议，定期监视审计记录

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。请查看此文档的每个发行版，确定是否有修订内容。

2

第 2 章 安全安装

本部分概述了安全安装和配置的规划和实现过程，并介绍了 ACSLS 的建议部署拓扑。

了解您的环境

要更好地了解安全需求，必须回答以下问题：

需要保护哪些资源?

ACSLS 管理的关键资源包括磁带库、磁带机和磁带。这些资源需要受到保护，以防受到意外和恶意访问。例如，防止人员在不同的服务器上使用 ACSLS 用户 ID 的其他密码误登录到其他 ACSLS 服务器。

要避免资源被哪些用户访问?

您要避免未经授权的内部和外部用户访问磁带存储资源。

如果对战略性资源的保护失败，将会产生什么后果?

ACSLS 可以在磁带机上挂载磁带。如果用户可以通过数据路径连接到磁带机，则可以读取未加密的磁带数据。

能够同时访问 ACSLS 和磁带库的用户可以装入和弹出磁带库的磁带。

保护 ACSLS 的建议过程

保护 ACSLS 和必需的基础结构组件时，请遵循以下过程以确保 ACSLS 在进行更改后可以继续工作：

- 安装 ACSLS。
- 检验 ACSLS 是否可正常工作。包括配置和审计磁带库、挂载和卸载磁带、装入和弹出磁带以及备份和恢复数据库。
- 实施更改以提高安全性。
- 检验 ACSLS 是否仍可正常工作。

保护 ACSLS Internet 通信

本部分介绍了部署 ACSLS 以保护 Internet 访问的建议。

保护企业防火墙后面的 ACSLS 和磁带库

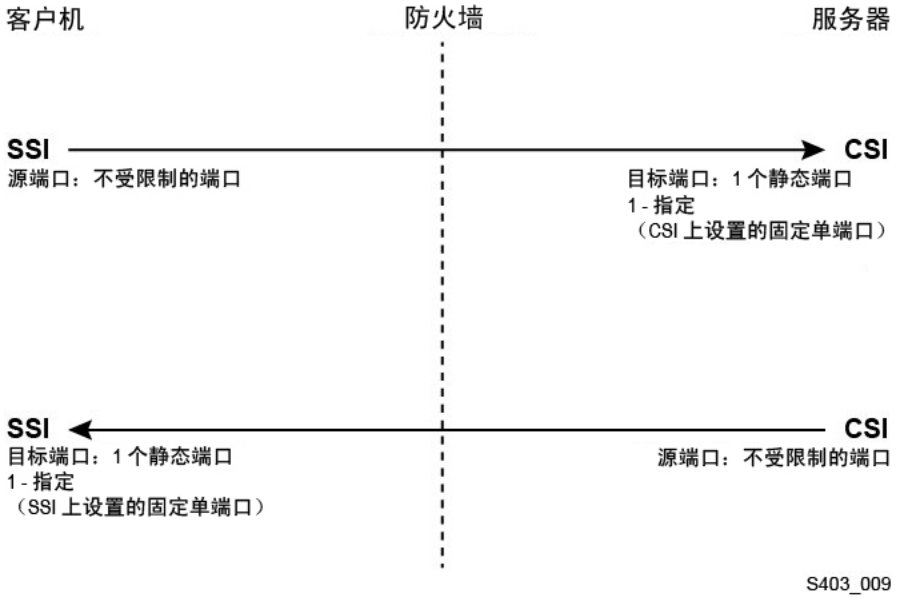
ACSLS 及其支持的磁带库应部署在企业防火墙后面。如果远程工作人员需要登录到 ACSLS 服务器，他们可以通过 VPN 进行访问。

注意:

如果具有基于 IPv4 的边缘防火墙，该防火墙应配置为删除所有出站 IPv4 协议 41 数据包和 UDP 端口 3544 数据包，以防止 Internet 主机使用任何 IPv6-over-IPv4 隧道通信访问内部主机。

ACSLS 防火墙安全选项

如果通过防火墙将使用 ACSLS 来挂载磁带和管理磁带库的客户机应用程序与 ACSLS 隔开，我们建议启用防火墙安全选项。即使未通过防火墙将客户机应用程序与 ACSLS 隔开，实施防火墙安全选项也可提供附加的 ACSLS 安全性（通过限制用于在 ACSLS 及其客户机应用程序之间通信的端口），如下所示。因此，CSI_FIREWALL_SECURE 静态变量在 ACSLS 8.1 和更高发行版中默认为 TRUE。



有关详细信息，请参见《ACSLS 管理员指南》中的“防火墙安全选项”附录。

用于 ACSLS 通信的以太网端口

- ACSLS 服务器上可使用以下端口。确保将任何防火墙配置为允许与这些端口进行通信。这包括由 Solaris 上的 ipfilter 或 Linux 上的 iptables 实施的防火墙。
  - 22 双向端口－用于 ssh 访问。
  - 111 端口映射器，除非已禁用端口映射器。
  - 115 端口，用于 SFTP（安全文件传输协议）。
  - 161 默认端口，用于 ACSLS SNMP 代理－get/set/walk。
  - 162 默认端口，用于 ACSLS SNMP 代理－陷阱。

注意:

ACSLS SNMP 代理使用的端口可由以下命令进行配置：*AcslsAgtdSnmpConf [-p port] [-t trap port] [-d]*。*-d* 选项用于显示当前设置。更改端口设置后，必须使用命令 *agentRegister* 重新启动代理。

- 5432 默认端口，用于从 ACSLS 到 PostgreSQL 数据库的内部通信（acsss 用户 ID 对应的 PGPORT 环境变量）。

  如果已获取端口 5432，则将使用下一个可用的较高端口号。

  注意:

  端口 5432 仅需本地主机 (127.0.0.1) 访问。

- 7001 和 7002－由 WebLogic 和 ACSLS GUI 使用。
- 30031 或 ACSLS CSI 的侦听端口，由 CSI_INET_PORT 设置。
- 50003 端口用于从 ACSLS GUI 和 Java 组件到旧版 ACSLS 处理的内部通信。此端口不可配置。

- 要让客户机应用程序通过 ACSAPI 与 ACSLS 进行通信，必须开启以下端口：
  - 客户机应用程序必须能够与 ACSLS CSI 的侦听端口进行通信。该端口默认为 30031，由 CSI_INET_PORT 静态变量进行设置。

    您可以从 Unix shell 中使用以下命令来搜索哪些端口正由 ACSLS 用来侦听来自 ACSAPI 客户机的请求：

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

    显示的最后一个字段中将列出端口 ID。
  - ACSAPI 客户机（例如，NetBackup 或 SAM-QFS 服务器）可使用 SSI_INET _PORT 环境变量设置其固定传入端口。指定 1024-65535 范围内的端口（端口 50001 和 50004 除外）。ACSLS 服务器必须能够与此端口通信。

    注意:

    在 ACSAPI 客户机服务器上，端口 50001 和 50004 用于 AF_INET 域 IPC 与小型事件记录程序的通信，以及从客户机应用程序到 SSI 的通信。

  有关客户机应用程序与 ACSLS 之间通信的更多详细信息，请参见《ACSLS 管理员指南》中的“防火墙安全选项”附录。

- 如果安装了 XAPI 组件，则 XAPI 服务器将使用固定的侦听端口接收来自 ELS 客户机的传入 TCP 请求。XAPI 侦听端口是由 XAPI_PORT 静态变量定义的。XAPI _PORT 默认为 50020。它必须介于 1024 和 65535 之间，并且不能与 ACSLS 或其他应用程序使用的任何其他端口冲突。

  有关 XAPI_PORT 的更多详细信息，请参见《ACSLS 管理员指南》中的“XAPI 客户机接口”附录。该附录还提供了有关如何显示和设置 XAPI_PORT 静态变量的详细信息。

- SL8500 或 SL3000 磁带库上必须开启的端口：

  ACSLS 在 SL8500 或 SL3000 磁带库的 2A 和 2B 以太网连接上与这些端口进行通信。如果从 ACSLS 到这些端口的通信被阻止，则 ACSLS 将无法管理磁带库。
  - 50001－用于 ACSLS 和磁带库之间的所有正常通信
  - 50002－供 ACSLS HA 用来确定备用 HA 节点是否能够在故障转移到备用节点前与磁带库进行通信

配置在 ACSLS 服务器上运行的防火墙

除了外部防火墙，还可以通过 Solaris 上的 ipfilter 或 Linux 上的 iptables 在 ACSLS 服务器上实施防火墙保护。下面介绍如何管理这些在 ACSLS 服务器上运行的防火墙。

- 管理 Solaris 上的 ipfilter：

  有关详细信息，请参阅 ipf 和 ipfilter 的手册页。
  - ipfilter 防火墙由 "root" 使用以下命令启用（禁用）：

    ```
    svcadm enable ipfilter (svcadm disable ipfilter)
    ```
  - 了解 ipfilter 的当前状态：

    ```
    svcs ipfilter
    ```
  - 以下文件中定义了防火墙策略：/etc/ipf/ipf.conf

    要允许在本地主机上的组件之间（例如，ACSLS 和 WebLogic 之间或 GUI 和 ACSLS 数据库之间）自由通信，请包含如下语句：

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

    或

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

    需要定义策略以允许访问 ACSLS 所需的所有端口。例如，要包含允许基于 Web 的远程浏览器访问 ACSLS GUI 的策略，需要开启端口 7001 和 7002。

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

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

    在搜索 ACSLS 使用哪些端口来侦听来自 ACSAPI 客户机的请求之后，为这些端口中的每个端口添加 "pass in quick" 语句。

    可能需要为 RPC 端口映射器端口 111 包含 "pass in quick" 语句。

    建议规则集中的最后一条语句 "block in from any" 指出，除非先前的语句中特别允许，否则不应当有通往主机的通信。
- 管理 Linux 上的 iptables：

- iptables 防火墙由 "root" 使用以下命令启用（禁用）：

  ```
  service iptables start (service iptables stop)
  ```

- 检查 iptables 的状态：

  ```
  service iptables status
  ```

- iptables 对应的策略文件是 /etc/sysconfig/iptables：

  需要定义策略以允许访问 ACSLS 所需的所有端口。例如，要包含允许通过 http/https 远程访问 ACSLS GUI 的策略，应该使用类似以下的语句更新该文件，以包含端口 7001 和 7002 的例外情况：

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

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

  在搜索 ACSLS 使用哪些端口来侦听来自 ACSAPI 客户机的请求之后，需要将这些端口中的每个端口的例外情况添加到 iptables 策略文件。可能需要为 RPC 端口映射器端口 111 包含例外情况语句。

安装和配置 Solaris

本部分介绍如何安全地安装和配置 Solaris。

建议包括：

- 向 OS 以及随 OS 安装的服务应用所有重要的安全修补程序。请有选择地应用这些修补程序，因为应用所有可用更新可能会安装尚未针对 ACSLS 和 ACSLS HA 测试的新功能甚至是新的 OS 发行版。
- 禁用 telnet 和 rlogin。改用 ssh。还要禁用 ftp，改用 sftp。

  通过以 root 身份发出以下命令来禁用 telnet、rlogin 和 ftp 服务。

  查看所有服务：

  ```
  svcs
  ```

  禁用 telnet、rlogin 和 ftp：

  ```
  svcadm disable telnet
  ```

  ```
  svcadm disable rlogin
  ```

  ```
  svcadm disable ftp
  ```

- 请勿禁用 ssh。您想要用户使用 ssh 而不是 telnet 或 rlogin 远程登录到 ACSLS。同样，请勿禁用 sftp。
- ACSLS 需要 rpc-bind。请勿禁用它。

如果使用 "Secure by Default" 选项安装了 Solaris，则需要更改 rpc-bind 的网络配置属性以允许 ACSAPI 客户机将请求发送到 ACSLS。

有关详细信息，请参阅 ACSLS 安装手册的 "Installing ACSLS on Solaris" 一章中的 "Installing Solaris" 一节。

- 需要开启 ACSLS 服务器上的一些以太网端口，才能与 ACSLS 进行通信。客户机应用程序使用特定的以太网端口与 ACSLS 进行通信，而 ACSLS 与磁带库上的特定端口进行通信。有关需要用于供 ACSLS 通信的端口，请参见用于 ACSLS 通信的以太网端口。在 ACSLS 服务器上，请确保将 ipfilter 配置为允许与 ACSLS 所用的端口进行通信。

确定 Solaris 审计策略。《Oracle Solaris 管理：安全服务》中的“在 Oracle Solaris 中审计”部分可帮助您规划要审计的事件、审计日志应保存的位置以及如何查看日志。

安装和配置 Linux

安全地安装和配置 Linux 的建议：

- 向 OS 以及随 OS 安装的服务应用所有重要的安全修补程序。请有选择地应用这些修补程序，因为应用所有可用更新可能会安装尚未针对 ACSLS 和 ACSLS HA 测试的新功能甚至是新的 OS 发行版。
- 确保未安装 telnet 和 rlogin 或禁用 telnet 和 rlogin。改用 ssh。

  同样，请确保未安装 ftp 或禁用 ftp，并改用 sftp。

  要查看所有服务，请以 root 身份登录并运行以下命令：

  ```
  service --status-all
  ```
- 要永久删除服务，请使用：

  ```
  svccfg delete -f service-name
  ```
- 请勿禁用 ssh。您想要用户使用 ssh 而不是 telnet 或 rlogin 远程登录到 ACSLS。同样，请勿禁用 sftp。
- 必须启用网络服务（特别是 rpcbind），以便允许 ACSLS 客户机通信。

  在 Linux 上启动 rpc 时，请使用 –i 标志。
- 需要开启 ACSLS 服务器上的一些以太网端口，才能与 ACSLS 进行通信。客户机应用程序使用特定的以太网端口与 ACSLS 进行通信，而 ACSLS 与磁带库上的特定端口进行通信。有关需要用于供 ACSLS 通信的端口，请参见用于 ACSLS 通信的以太网端口。在 ACSLS 服务器上，请确保将 iptables 配置为允许与 ACSLS 所用的端口进行通信。

审计 Linux 安全性

确定 Linux 审计策略。《Oracle Linux: Security Guide for Release 6》中的 "Configuring and Using Auditing" 部分可帮助您规划要审计的事件、审计日志应保存的位置以及如何查看日志。

用于审计 Linux 安全性的有用日志和命令包括：

- 以 root 身份查看 var/log/secure 以了解登录尝试和其他访问消息的历史记录。
- 命令 "last | more" 提供登录的用户的历史记录。
- /var/log/audit/audit.log.[0-9] 保存了 SE Linux 拒绝的访问尝试的日志。必须成为 root 用户才能查看这些内容。

SELinux 安全性

ACSLS 8.4 设计为在可选的安全性增强型 Linux 环境中运行。SELinux 提供对文件、目录和其他系统资源的访问控制，超越了 Unix 环境中作为标准的传统保护。除了 owner-group-public 权限访问，SELinux 还包括基于用户角色、域和上下文的访问控制。对所有系统资源实施访问控制的代理是 Linux 内核。

Linux 系统上的 root 用户可以通过 *`setenforce`* 命令将实施状态设置为开启或关闭。

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

使用 *`Enforcing`* 或 1 可将 SELinux 置于实施模式。使用 *`Permissive`* 或 0 可将 SELinux 置于许可模式

要查看当前的系统实施状态，请使用命令 *`getenforce`*。

安装 ACSLS 时，内核中会装入三个 SELinux 策略模块：allowPostgr、acsdb 和 acsdb1。SELinux 实施方案有效时，这些模块提供 ACSLS 访问自身数据库和其他系统资源所需的定义和实施方案例外情况。安装这些模块后，您应当能够运行常规 ACSLS 操作，包括数据库操作（例如 bdb.acsss、rdb.acsss、db_export.sh 和 db_import.sh），无需禁用 SELinux 实施方案。

有关更多信息，请参阅《StorageTek ACSLS 8.4 管理员指南》的“故障排除”附录中有关 SELinux 的部分。

安装和配置 ACSLS

本部分说明如何安全地安装 ACSLS。

执行标准 ACSLS 安装

执行标准 ACSLS 安装可确保您具备所有必需的组件。

如果要从以前的 ACSLS 发行版迁移到较后的 ACSLS 发行版，请查看动态变量和静态变量的设置，了解是否要使用更多的安全选项，特别是有关防火墙安全选项。

对 ACSLS 用户 ID 使用强密码

ACSLS 需要 ACSLS 用户 ID：acsss、acssa 和 acsdb。对于这些 ID，请选择强密码，并定期更改密码。

限定对 ACSLS 文件的访问

ACSLS 通常将对 ACSLS 文件的访问仅限定于 acsls 组，其中包括 acsss、acssa、acsdb 和 root 用户 ID。某些数据库和诊断文件仅可由单个 acsls 用户 ID 访问。ACSLS 运行时采用的 umask 设置为 027。

ACSLS 文件不应设置为全局可读或全局可写。但是，限制默认安装设置以外的访问可能会造成 ACSLS 运行失败。

对于三个 ACSLS 文件，将 "root" 设置为有效用户 ID

安装脚本建议客户必须在 /export/home/ACSSS 文件系统的三个可执行文件中设置 "root" 的有效用户 ID (setuid)：

- *acsss*（该二进制文件必须以 "root" 特权运行，因为它用于启动和停止 ACSLS 应用程序所需的系统服务。）
- *db_command*（该二进制文件可启动和停止用于控制和维护 ACSLS 数据库的 PostgreSQL 数据库引擎。）
- *get_diags*（该二进制文件由客户调用以收集全面的系统诊断信息，服务支持调用的上下文中可能需要这些信息。）

使用 pkgadd 安装 ACSLS 期间，系统会提示客户：*Do you want to install these as setuid/setgid files?*（您是否要安装这些文件使之成为 setuid/setgid 文件？）针对提示回答 *y*，将允许 acsls 组中的用户运行这三个命令，即使实用程序执行某些要求 root 特权的系统操作也是如此。

查看 ACSLS 静态和动态变量的设置

ACSLS 静态和动态变量控制许多 ACSLS 功能的行为。使用 *acsss_config* 实用程序设置这些变量。本文档讨论了这些变量中许多变量的安全设置。*acsss_config* 显示某一变量的选项时，以问号 (?) 形式作答将会显示该变量的详细解释。《ACSLS 管理员指南》的“设置控制 ACSLS 行为的变量”一章中也提供了此信息。

配置 WebLogic

ACSLS 8.1 和更高发行版使用 WebLogic 作为其 Web 服务器。WebLogic 随 ACSLS 一起安装。

有关保护 WebLogic 服务器以及 WebLogic 审计迹可能性的选项，请参阅《Oracle Fusion Middleware Understanding Security for Oracle WebLogic Server 11g Release 1 (10.3.6)》。

使用 ACSLS userAdmin.sh 实用程序创建和维护 ACSLS GUI 用户

userAdmin.sh 菜单驱动的实用程序用于管理 ACSLS GUI 用户密码。您可以添加用户、删除用户、列出用户以及更改用户密码。必须运行 WebLogic 才能使用该实用程序。如果 WebLogic 尚未运行，该实用程序会启动 WebLogic 并确认联机后才显示菜单。

userAdmin.sh 实用程序必须由 root 运行，并需要 acsls_admin 验证。ACSLS 安装期间将配置 acsls_admin 用户帐户。

使用 ACSLS GUI

要使用 ACSLS GUI，您需要安装最新的 JRE 版本，并通过浏览器访问 ACSLS GUI。

在 GUI 客户机系统上安装最新的 JRE 版本

确保在系统上安装了 Java Runtime Environment (JRE) 的最新版本，系统将使用 ACSLS GUI 访问 ACSLS。

访问 ACSLS GUI

打开浏览器，按照以下格式输入包含服务器主机名或 IP 地址的 URL：

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

最好使用主机的全限定主机名或 IP 地址。如果 WebLogic 不能完全解析 URL，则一些页面（包括 ACSLS 帮助页面）可能不会正确显示。

如果同时使用 http 和端口 7001，则 WebLogic 将自动将您重新路由到端口 7002 上的 https。

由于 WebLogic 使用安全 https 协议，因此您的浏览器可能会向您发出警告，指出站点安全证书尚未注册，因而不可信。如果您确信该 URL 是本地 ACSLS 计算机，则可以放心地继续执行操作。此时，您应当看到登录屏幕。

使用 ACSLS GUI

访问 WebLogic 中的 AcslsDomain 时使用安全协议 https。该协议使用私钥和数字证书在浏览器与服务器之间提供加密的通信。下面是用于获取数字证书的选项：

ACSLS 演示证书

ACSLS 附带了一个所谓的“演示”证书。这提供了最低级别的加密安全性，使客户不需要执行进一步的配置步骤即可开始使用 ACSLS GUI。如果客户与 ACSLS 磁带库之间

的交互完全在安全的内联网内进行，则此演示认证方法通常就足够了。不过，此方法采用一个 512 位加密密钥，某些浏览器上不支持此密钥，特别是 Internet Explorer 和 FireFox 版本 39 及更高版本。

配置自签名数字证书

《ACSLS 安装指南》为 ACSLS 管理员提供了配置长度为 2048 位的自签名数字证书的分步方法。在名为“配置 SSL 加密密钥”的部分中，此方法提供了一个在所有浏览器上都受支持的证书。访问使用自签名证书的 https 站点的用户会被劝告不要继续访问该站点，除非他们自己知道该 Web 资源是一个可信站点。在 ACSLS 用户和磁带库控制服务器的上下文中，此信任级别通常很好理解，在大多数情况下，站点不需要使用第三方签名验证来证明其完整性。

由第三方签名机构签名的数字证书

每个客户站点自行决定它们是否需要由第三方签名机构（例如 Verisign 或 Entrust .net）提供证书验证。Oracle 联机文档《Configuring Identity and Trust》中介绍了用于生成此类签名数字证书的过程，该文档位于：

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

安装 ACSLS HA

如果您要使用 ACSLS 高可用性解决方案，请按照《ACSLS-HA Cluster: Installation, Configuration, and Operations》中的说明执行操作。

3

第 3 章 安全功能

本部分介绍了 ACSLS 提供的具体安全机制。

安全模型

ACSLS 安全要求来源于保护数据的需要：第一，防止数据意外丢失和损坏，第二，防止未经授权蓄意访问或修改数据。第二项关注内容包括防止访问或使用数据时的过度延迟，甚至是避免来自拒绝服务的干扰。

提供这些保护的关键安全功能包括：

- 验证－确保只有经过授权才能访问系统和数据。
- 授权－提供对系统特权和数据的访问控制。授权基于验证，可确保个人仅能获取相应的访问权限。
- 审计－允许管理员检测尝试进行的验证机制违规行为以及尝试进行的或成功进行的访问控制违规行为。

配置和使用验证

默认情况下，在 Linux 或 Solaris 上，ACSLS 用户由 PAM（Pluggable Authentication Module，可插拔验证模块）进行验证。请参阅 Solaris 手册页或《Linux-PAM System Administrators Guide》。

ACSLS GUI 的用户由 WebLogic 中的嵌入式 LDAP 服务器进行验证。请参阅文档《Managing the Embedded LDAP Server》：

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

由 Solaris 或 Linux 操作系统执行的 ACSLS 用户验证

ACSLS 用户：acsss 和 acssa 必须登录到 Solaris 或 Linux 并通过操作系统验证才能使用 cmd_proc 或执行 ACSLS 实用程序和配置命令（对于 acsss 用户）。acsdb 用户 ID 还用于与数据库相关的操作。作为 ACSLS 安装过程的一部分，客户在第一次登录时必须设置这些 ID 的密码。有关详细信息，请参见《ACSLS 安装指南》。

由 WebLogic 执行的 ACSLS GUI 用户验证

ACSLS GUI 用户必须登录 WebLogic 并通过 WebLogic 验证。ACSLS 安装期间将创建 acsls_admin，客户必须设置其密码。客户可以使用 *userAdmin.sh* 实用程序根据

需要添加其他 GUI 用户。有关详细信息，请参见《ACSLS 安装指南》和《ACSLS 管理员指南》中“实用程序”一章有关 *userAdmin.sh* 的部分。

审计注意事项

下面介绍了适用于 ACSLS 的一般审计注意事项。

使审计信息保持具有可管理性

虽然审计的成本相对廉价，但是请尽可能限制审计事件的数量。这样做可以最大限度地减少对审计语句执行性能的影响，并最大限度地减小审计迹的大小，从而可以更轻松地进行分析、理解和管理。

设计审计策略时，请遵循以下一般准则：

评估审计目的

在清楚了解审计原因之后，可以设计相应的审计策略并避免不必要的审计。

目标明确地进行审计

审计获取目标信息所必需的最少量的语句、用户或对象。

配置和使用 ACSLS 审计日志

ACSLS 具有多个信息日志，允许您记录和检查 ACSLS 活动。

- 您可以使用 vi 和其他编辑器查看大多数日志。系统事件只能通过使用 ACSLS GUI 进行查看。
- 这些日志中的大多数日志在达到客户定义的大小后可以自动归档，客户指定数量的日志将被保留。为避免填满 ACSLS 文件系统，将限制保留的日志数量，可对该限制进行配置。如果要保留更多的日志文件或将其保留在其他系统上，则需要开发自己的程序，将其归档到某个有足够空间的位置。
- 要保留的归档日志的大小、数量和这些文件的其他特性可由 ACSLS 动态和静态变量进行定义。

ACSLS 日志目录

ACSLS 日志目录由 LOG_PATH 静态变量进行控制。默认目录为 $ACS_HOME/log。该目录包含以下日志：

acsss_event.log
该日志记录了重要的 ACSLS 系统事件、磁带库事件和错误的消息。

当 acsss_event.log 达到 LOG_SIZE 动态变量定义的阈值大小后，系统会将其复制到 event0.log 并清除。在复制过程中，保留的事件日志会被复制到编号更

高的保留日志中，编号最高的保留日志将被覆盖。例如：event8.log 被复制到 event9.log，event7.log 被复制到 event8.log，…，event0.log 被复制到 event1 .log，acsss_event.log 被复制到 event0.log，然后 acsss_event.log 被清除。这一操作由以下变量控制：

- *EVENT_FILE_NUMBER* 指定要保留的事件日志数量。
- *LOG_SIZE* 指定阈值大小，事件日志一旦达到此阈值就会被复制到保留事件日志并被截断。

使用 *greplog* 实用程序过滤 acsss_event 日志以包括或排除包含特定关键字的消息。有关更多详细信息，请参见《ACSLS 管理员指南》的“实用程序”一章中的 greplog。

配置日志
当 ACSLS 更新存储在 ACSLS 数据库中的磁带库配置时，有两个日志记录了详细信息。*acsss_config* 和 *Dynamic Config*（*config* 实用程序）的配置更改会记录在以下位置。

acsss_config.log
记录 ACSLS 支持的磁带库的所有配置或重新配置详细信息。最后的配置更改附加在先前的配置记录后面。

acsss_config_event.log
记录在配置和重新配置期间发生的事件。

rpTrail.log
记录 ACSAPI 客户机或 cmd_proc 对 ACSLS 的所有请求的响应，以及记录对 GUI 或与逻辑磁带库连接的 SCSI 客户机接口的所有请求（数据库查询除外）的响应。记录的信息包括请求者、请求和请求时间戳。

rpTrail.log 由以下变量进行管理：

- *LM_RP_TRAIL* 启用 ACSLS 事件的此审计迹。默认值为 TRUE。
- *RP_TRAIL_LOG_SIZE* 指定压缩和归档 rpTrail.log 的阈值大小。
- *RP_TRAIL_FILE_NUM* 指定要保留的归档 rpTrail 日志的数量。
- *RP_TRAIL_DIAG* 指定 rpTrail 消息是否应该包含其他诊断信息。默认值为 FALSE。

磁带库卷统计信息
记录所有影响磁带库中的卷（磁带）的事件，包括审计或磁带恢复何时挂载、卸载、移动、装入、弹出或发现卷。如果启用磁带库卷统计信息，则 acsss_stats .log 中将记录此信息。

磁带库卷统计信息由以下变量进行管理：

- *LIB_VOL_STATS* 启用此磁带库卷统计信息。默认值为 OFF。
- *VOL_STATS_FILE_NUM* 指定要保留的归档 acsss_stats.log 文件的数量。
- *VOL_STATS_FILE_SIZE* 指定归档 acsss_stats.log 的阈值大小。

ACSLS 日志/sslm 目录

在 ACSLS 日志目录中，有关 ACSLS GUI 和与逻辑磁带库连接的 SCSI 客户机接口的信息记录在 sslm 目录中。该目录包含指向 WebLogic 审计日志的链接。sslm 目录包含以下日志：

slim_event.g#.log[.pp#]
该日志记录 ACSLS GUI 和 SCSI 客户机接口的事件。其中包括逻辑磁带库配置更改和 SCSI 客户机事件的消息。

- .g# 是该日志的生成号。
- .pp# 是该日志的并行进程号。如果同时记录多个进程，则将向其他进程的日志分配一个并行进程号。

smce_trace.log
该日志使用 SCSI 介质转换器接口仿真跟踪从 SCSI 客户机到 ACSLS 逻辑磁带库的活动。

guiAccess.log
这是指向 WebLogic 的 access.log 的链接。请参见配置和使用 WebLogic 审计日志。

AcslsDomain.log
这是指向 WebLogic 的 AcslsDomain.log 的链接。请参见配置和使用 WebLogic 审计日志。

AdminServer.log
这是指向 WebLogic 的 AdminServer.log 的链接。请参见配置和使用 WebLogic 审计日志。

从 GUI 日志查看器中查看 ACSLS 审计迹

从 GUI 导航树的 "Configuration and Administration" 部分访问日志查看器。日志查看器将显示 acsss_event.log 和 smce_trace.log 中的组合信息。

从 GUI 中查看系统事件

还可以从 GUI 导航树的 "Configuration and Administration" 部分查看系统事件。系统事件日志中将记录每个独立的磁带库操作。该日志中的每条记录都包含事件时间戳、事件类型和事件描述。

配置和使用 Solaris 审计日志

确定 Solaris 审计策略。《Oracle Solaris 管理：安全服务》手册中的“在 Oracle Solaris 中审计”部分可帮助您规划要审计的事件、审计日志应保存的位置以及如何查看日志。

如果尚未启用定制 Solaris 审计迹，则这些登录的审计迹以及 acsss、acsdb 和 acssa 用户发出的 Unix 命令都可用：

- Unix utmpx 中将记录当前登录到 Unix 的用户，而 wtmpx 数据库中将记录用户过去的访问情况。
- 使用 *last* 命令查看对某一用户 ID 的所有访问（例如 *last acsss*）。有关更多信息，请参见 wtmpx、*last* 和 getutxent 的手册页。
- 用户主目录中的 .*_history（即 [点]*_history）文件记录了该用户发出的命令。

  对于 acsss 用户，这些文件可能包括：
  - .bash_history
  - .psql_history
  - .sh_history

  Solaris /var/adm/sulog 上记录了执行 *su* 并成为超级用户或其他用户的成功和失败尝试。

配置和使用 Linux 审计日志

有关收集和分析审计日志以及系统日志的详细信息，请参阅《Oracle Linux: Security Guide for Release 6》中的 "Configuring and Using Auditing" 和 "Configuring and Using System Logging" 部分。

配置和使用 WebLogic 审计日志

有关保护 WebLogic 服务器以及 WebLogic 审计迹可能性的选项，请参阅《Oracle Fusion Middleware Understanding Security for Oracle WebLogic Server 11g Release 1 (10.3.6)》。

WebLogic 在以下目录中记录对 ACSLS GUI 的访问情况：

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

该目录包含以下文件：

- access.log
  - 有一些名为 access.log##### 的归档版本（例如 access.log00001）
  - 该日志提供 GUI 用户活动的详细审计迹。
  - 有关登录，请查找 "AcslsLoginForm"。

    注意:

    存在指向 $ACS_HOME/logs/sslm/guiAccess.log 中的访问日志的链接。
- AcslsDomain.log
  - 该日志报告 WebLogic 和 ACSLS GUI 操作。

    注意:

    存在指向 $ACS_HOME/logs/sslm/AcslsDomain.log 中的访问日志的链接。

- AdminServer.log
  - 该日志报告 WebLogic 和 ACSLS GUI 操作。

注意:

存在指向 $ACS_HOME/logs/sslm/AdminServer.log 中的访问日志的链接。

4

第 4 章 针对开发者的安全注意事项

本部分提供的信息有助于开发者开发或支持使用 ACSLS 管理 Oracle StorageTek 磁带库的应用程序。

在客户机应用程序服务器上启用防火墙安全功能

通过启用防火墙安全功能来限制用于通信的端口，并禁用客户机应用程序服务器上的端口映射器。请参见《CSC Developer’s Toolkit User’s Guide》的 "Appendix B: Firewall-Secure Operation"。

附录 A

附录 A. 安全部署核对表

1. 强制实施密码管理。
2. 限制网络访问。
   a. ACSLS 及其管理的磁带库应位于企业防火墙后面。
   b. 启用 ACSLS 防火墙安全选项。
   c. 考虑对 ACSLS 客户机应用程序启用防火墙安全。
3. 强化 Solaris 或 Linux 操作系统。
4. 应用所有安全修补程序和解决方法。
5. 如果 StorageTek ACSLS 中存在漏洞，请联系 Oracle 服务部门、Oracle 磁带库工程部门或客户代表。

附录 B

附录 B. 参考

ACSLS 文档
ACSLS 文档保存在按 ACSLS 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#opensyssoft

（各个 ACSLS 文档库在其 URL 中包含版本号。因此，一旦库进行更新，指向特定库的链接就会过时。）ACSLS 文档包含以下内容：

- 《ACSLS 安装指南》
- 《ACSLS 管理员指南》
- 《ACSLS 产品信息》

  这包括软件和硬件要求、ACSLS 概述，以及支持的磁带库、磁带机和介质。
- 《ACSLS 消息》（和状态代码）
- 《ACSLS 发行说明》
- 《ACSLS-HA Cluster: Installation, Configuration, and Operations》
- 《ACSLS Interface Reference Manual》

Oracle Solaris
Oracle Solaris 11.2 信息库包含《确保 Oracle Solaris 11 操作系统安全》。有关详细信息，请参阅该文档。

Oracle Linux
Oracle Linux 6 信息库包含《Oracle Linux 6 Security Guide》。有关详细信息，请参阅该文档。

Oracle WebLogic
适用于 WebLogic 10.3.6（由 ACSLS 8.2 使用）的 Oracle WebLogic Server 文档库具有关于“安全”的部分。

《Oracle Fusion Middleware Understanding Security for Oracle WebLogic Server 11g Release 1 (10.3.6)》介绍了有关保护 WebLogic 服务器的详细信息。