Oracle® ACSLS

Security Guide

Version 8.1

E26672-02

April 2012

ORACLE®

Oracle ACSLS Security Guide 8.1

E26672-02

Primary Author: Chris Morrison

Contributors: George Noble, Martin Ryder, Terry Schmitt, and Mike Williams

Contents

Part 1: Overview

This section gives an overview of ACSLS and explains the general principles of application security.

Product Overview

Automated Cartridge System Library Software (ACSLS) is Oracle's tape library server software that controls one or more StorageTek tape libraries for open systems clients. An Automated Cartridge System (ACS) is a tape library or a group of tape libraries connected through pass-thru-ports (PTPs). ACSLS manages one or more ACSs through "control path" commands sent across a network. The software includes a system administration component, interfaces to client system applications, and library management facilities.

General Security Principles

The following principles are fundamental to using any application securely.

Keep Software Up To Date

One of the principles of good security practice is to keep all software versions and patches up to date. Throughout this document, we assume ACSLS release 8.1 or later, with all relevant maintenance applied, as ACSLS 8.1 includes many security-related enhancements.

Restrict Network Access to Critical Services

Keep both the ACSLS and the libraries that it manages behind a firewall.

Using a private network for TCP/IP communications between ACSLS and tape libraries is recommended.

Follow the Principle of Least Privilege

The principle of least privilege states that users should be given the least amount of privilege to perform their jobs. User privileges should be reviewed periodically to determine relevance to current job responsibilities.

On ACSLS, this means that operators who only issue routine commands using cmd_proc should login as the acssa user. System administrators who login as the acsss user also have access to a wider range of utilities and configuration commands. Use of the acsdb user ID is not needed for normal operations.

Monitor System Activity

System security stands on three legs: good security protocols, proper system configuration, and system monitoring. Auditing and reviewing audit records address this third

requirement. Each component within a system has some degree of monitoring capability. Follow audit advice in this document and regularly monitor audit records.

Keep Up To Date on Latest Security Information

Oracle continually improves its software and documentation. Check this document for revisions as least yearly.

Part 2: Secure Installation and Configuration

Installation Overview

This section outlines the planning process for a secure installation and describes recommended deployment topologies for ACSLS.

Understand Your Environment

To better understand your security needs, ask yourself the following questions:

Which resources am I protecting?

> The key resources that ACSLS manages are tape libraries, drives, and cartridges. They need to be protected from inadvertent as well as malicious access. For example, prevent people from mistakenly logging into a different ACSLS server by using different passwords for the ACSLS user IDs on different servers.

From whom am I protecting the resources?

> You want to protect the tape storage resources from both unauthorized internal and external access.

What will happen if the protections on strategic resources fail?

> ACSLS can mount cartridges on tape drives. If a user can connect to the tape drive through the data path, they can read data on the tape if it is not encrypted.
>
> Users who have access to both ACSLS and a tape library can enter and eject cartridges from a tape library.

Recommended Deployment Topologies

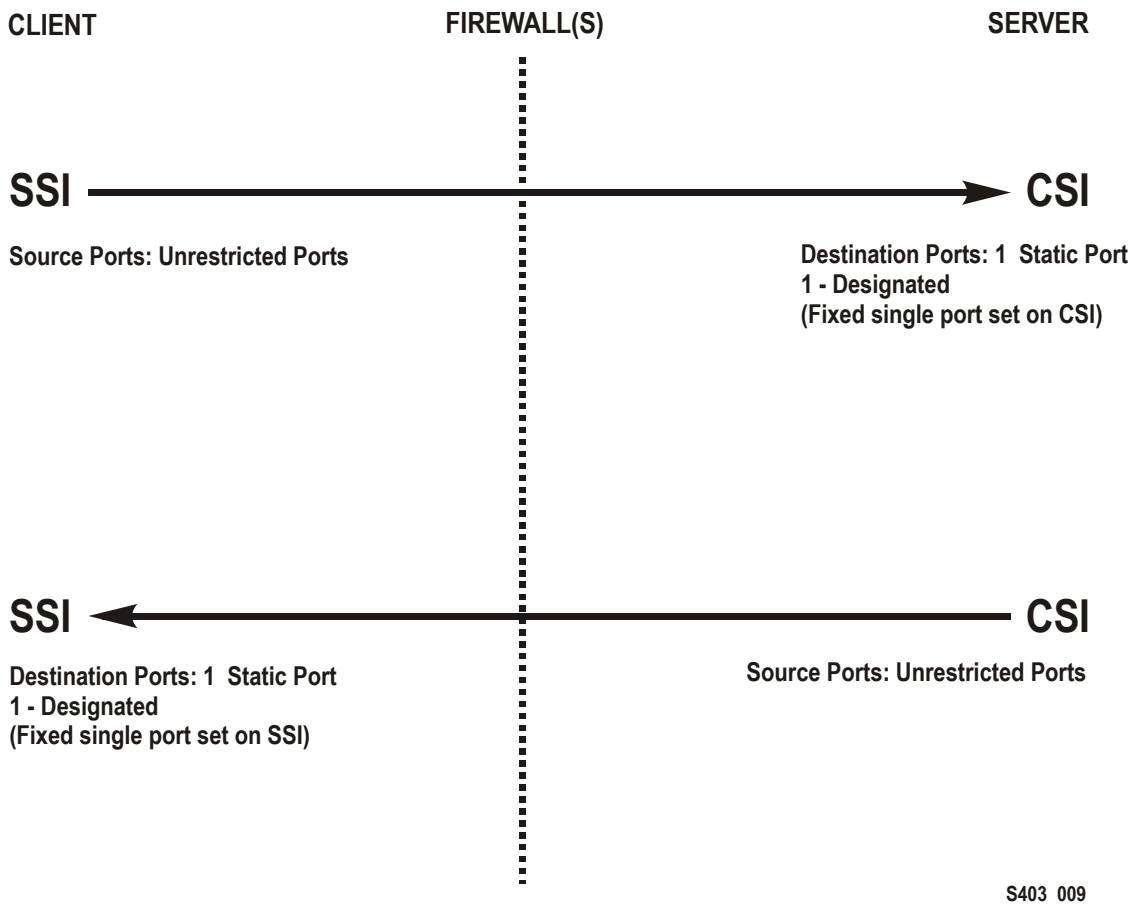
This section describes recommended architectures for deploying ACSLS to secure Internet access.

Secure ACSLS and Tape Libraries Behind the Corporate Firewall

ACSLS and the tape libraries it supports should be deployed behind the corporate firewall. If people working remotely need to login to the ACSLS server, they can access it through a VPN.

Recommended Deployment Topologies: Firewall Security Option

If client applications, which use ACSLS to mount tapes and manage tape libraries, are separated from ACSLS by a firewall, we recommend enabling the Firewall Security Option. Even if the client applications are not separated from ACSLS by a firewall, implementing the Firewall Security Option provides additional security by restricting the ports used for communication between ACSLS and its client applications, as shown below. For these reasons, the CSI_FIREWALL_SECURE static variable now defaults to TRUE with ACSLS 8.1.



For details, see the “Firewall Security Option” appendix in the ***ACSLS 8.1 Administrator’s Guide***.

Recommended Procedure for Securing ACSLS and Infrastructure Components

When securing ACSLS and required infrastructure components, follow this procedure to ensure that ACSLS will continue to function after the changes are made:

- Install ACSLS.
- Verify that ACSLS is functioning correctly. Include configuring and auditing libraries, mounting and dismounting tapes, entering and ejecting tapes, and backing-up and restoring the database.
- Implement the change to increase security.
- Verify that ACSLS still functions correctly.

Installing and Configuring Solaris

This section describes how to install and configure Solaris securely.

Suggestions include:

- Disable telnet and rlogin. Use ssh instead. Also disable ftp and use sftp instead.
  Disable the telnet, rlogin, and ftp services by issuing the following commands as root
  See all the services by:
  svcs
  Disable telnet, rlogin, and ftp by:
  svcadm disable telnet
  svcadm disable rlogin
  svcadm disable ftp

- Don't disable ssh. You want users to remotely login to the ACSLS using ssh, not telnet or rlogin. Also do not disable sftp.

- ACSLS requires RPC and bind. Do not disable them.

- The following ports are used on the ACSLS server. Ensure that iptables is configured to allow traffic to these ports:

  - 22 both directions – used for ssh access

  - 111 portmapper, unless portmapper has been disabled

  - 115 used for SFTP (Secure File Transfer Protocol)

  - 161 default port for ACSLS SNMP agent - get/set/walk

  - 162 default port for ACSLS SNMP agent - traps

    Note: The ports used by the ACSLS SNMP agent are configurable by the command: AcslsAgtdSnmpConf [-p <port>] [-t <trap port>] [-d]. The '-d' option displays the current setting. After changing the port setting, you must restart the agent with the command, 'agentRegister'.

  - 7001 and 7002 - used by WebLogic and the ACSLS GUI

  - 30031 or the ACSLS CSI's listening port, set by CSI_INET_PORT

- ACSLS communicates with these ports on an SL8500 or SL3000 library's 2A and 2B Ethernet ports.

  - 50001 – Used for all normal communication between ACSLS and the library.

- 50002 – Used for by ACSLS HA to determine whether the alternate HA node can communicate with the library before failing over to the alternate node.

Determine your Solaris auditing policy. The “Oracle Solaris Auditing” section in ***Oracle System Administration: Security Services*** can help you plan for what events to audit, where your audit logs should be saved, and how you want to review them.

Installing and Configuring ACSLS

This section explains how to securely install ACSLS.

Perform a Standard ACSLS Installation

Performing a standard ACSLS installation ensures that you will have all necessary components.

If you are migrating to ACSLS 8.1 from a previous ACSLS release, review your settings for dynamic and static variables to see if you want to use more secure options, especially regarding the Firewall Secure Option.

Use Strong Passwords for the ACSLS User IDs

ACSLS requires the ACSLS user IDs: acsss, acssa, and acsdb. Choose strong passwords for these IDs, and change the passwords on a regular basis.

Restrict Access to ACSLS Files

ACSLS generally restricts access to the ACSLS files to only acsls group, which includes the acsss, acssa, acsdb, and root user IDs. Some database and diagnostic files are only accessible by a single acsls user ID. ACSLS runs with a umask setting of 027.

ACSLS files should not be made world readable or writable. However, restricting access beyond the installation defaults may cause ACSLS functions to fail.

Review Settings for ACSLS Static and Dynamic Variables

The ACSLS static and dynamic variables control the behavior of many ACSLS functions. Set these variables using the **acsss_config** utility. Secure settings for many of these variables are discussed in this document. When the options for a variable are presented by acsss_config, replying with a question mark (?) will cause a detailed explanation of the variable to be displayed. This information is also available in the "Setting Variables that Control ACSLS Behavior" chapter of the ***ACSLS 8.1 Administrator's Guide***.

Configuring WebLogic

ACSLS 8.1 uses WebLogic for its web server. WebLogic is installed with ACSLS.

Refer to Securing ***Oracle WebLogic Server 11g Release 1 (10.3.3) Securing Oracle WebLogic Server 11g Release 1 (10.3.3)*** for the options for securing a WebLogic server, and the audit trail possibilities with WebLogic.

Use the ACSLS userAdmin.sh utility to create and maintain ACSLS GUI users

The userAdmin.sh menu-driven utility is used to administer ACSLS GUI user passwords. You can add users, remove users, list users, and change user passwords. WebLogic must be running to use this utility. If it is not up, this utility starts WebLogic and confirms that it is online before displaying the menu.
The userAdmin.sh utility must be run by root, and requires acsls_admin authentication. The acsls_admin user account is configured during ACSLS 8.1 installation.

Using the ACSLS GUI

Install the Latest JRE Version on GUI Client Systems

Make sure the latest version of the Java Runtime Environment (JRE) is installed on the systems that will use the ACSLS GUI to access ACSLS.

Accessing the ACSLS GUI

Open a browser and enter a URL with the server hostname or IP address in the following format:

> https://myAcslsHostName.myDomainName:7002/SlimGUI/faces/Slim.jsp -or-
> https://127.99.99.99:7002/SlimGUI/faces/Slim.jsp

It is best to use the fully-qualified host name or the IP address of the host machine. Some pages, including the ACSLS help pages, may not display properly if the URL cannot be fully resolved by WebLogic.

If you use http with port 7001, WebLogic will automatically re-route you to https on port 7002.

Since WebLogic is using the secure https protocol, your browser may warn you that the site security certificate has not been registered, and therefore is untrusted. If you are confident that the URL is your local ACSLS machine, you are safe to proceed. At this point, you should see the login screen.

Installing ACSLS HA

If you are using the ACSLS High Availability solution follow the instructions in the ***ACSLS-HA 8.1 Cluster: Installation, Configuration, and Operations***.

Part 3: Security Features

The Security Model

ACSLS security requirements arise from the need to protect data: first, from accidental loss and corruption; and second from deliberate unauthorized attempts to access or alter that data. Secondary concerns include protecting against undue delays in accessing or using data, or even against interference to the point of denial of service.

The critical security features that provide these protections are:

- Authentication – ensures that only authorized individuals get access to the system and data.
- Authorization – provides access control to system privileges and data. This builds on authentication to ensure that individuals only get appropriate access.
- Audit – allows administrators to detect attempted breaches of the authentication mechanism and attempted or successful breaches of access control.

Configuring and Using Authentication

ACSLS User Authentication by the Solaris OS

The ACSLS users: acsss and acssa must log into Solaris and be authenticated by the Solaris operating system before they can use cmd_proc or, for the acsss user, execute ACSLS utilities and configuration commands. The acsdb user ID is also used for database-related operations. As part of the ACSLS installation process, customers must set the passwords for these IDs the first time they log into them. See the ***ACSLS 8.1 Installation Guide*** for details.

ACSLS GUI User Authentication by WebLogic

ACSLS GUI users must log into and be authenticated by WebLogic. The acsls_admin is created during ACSLS installation, and customers must set its password. Customers can add other GUI users as desired using the userAdmin.sh utility. For details see the ***ACSLS 8.1 Installation Guide*** and the ***ACSLS 8.1 Administrator's Guide***, "Utilities" chapter, section on userAdmin.sh.

Audit Considerations

Keeping Audited Information Manageable

Although auditing is relatively inexpensive, limit the number of audited events as much as possible. Doing so minimizes the performance impact on the execution of audited statements and the size of the audit trail, making it easier to analyze, understand, and manage.

Use the following general guidelines when devising an auditing strategy:

Evaluate the purpose for auditing

After you have a clear understanding of the reasons for auditing, you can devise an appropriate auditing strategy and avoid unnecessary auditing.

Audit knowledgeably

Audit the minimum number of statements, users, or objects required to get the targeted information.

Configuring and Using the ACSLS Audit Logs

ACSLS has several logs of information that let you record and inspect ACSLS activity.

- You can view most of them using vi and other editors. System Events can only be viewed by using the ACSLS GUI.
- Most of these logs can be automatically archived when they reach a customer defined size, and a customer specified number of logs will be retained. To avoid filling the ACSLS filesystem there is a configurable limit to the number of logs that will be retained. If you want to retain more of these log files or retain them on another system, you need to develop your own procedure to archive them in a location that has sufficient space.
- The size, number of archived logs to retain, and other characteristics of these files are defined by ACSLS dynamic and static variables.

ACSLS log directory

The ACSLS log directory is controlled by the LOG_PATH static variable. The default is the $ACS_HOME/log directory. This directory includes these logs:

- **acsss_event.log** – This records messages for significant ACSLS system events, library events, and errors.

  When the acsss_event.log reaches a threshold size defined by the LOG_SIZE dynamic variable, it is copied to the event0.log and cleared. During the copy process, the retained event logs are copied into higher numbered retained logs and the highest numbered retained log is overlaid. For example: the event8.log is copied over the event9.log, the event7.log is copied over the event8.log, …, the event0.log is copied over the event1.log, the acsss_event.log is copied over the event0.log, and the acsss_event.log is cleared. This is controlled by the following variables:
  - EVENT_FILE_NUMBER specifies the number of event logs to retain.
  - LOG_SIZE specifies the threshold size at which the event log is copied to a retained event log and truncated.

  Use the greplog utility to filter the acsss_event log to include or to exclude messages containing specific keywords. See greplog in the “Utilities” Chapter in the ***ACSLS 8.1 Administrator’s Guide*** for more details.

- **Configuration logs**
  There are two logs that record details when ACSLS updates the library configuration stored in the ACSLS database. Configuration changes from both acsss_config and Dynamic Config (the config utility) are recorded here.
  - **acsss_config.log** – records the details of all configurations or re-configurations of the library(s) that ACSLS supports. The last configuration change is appended to the record of previous configurations.

- **acsss_config_event.log** – records events during the configuration or re-configuration process.

- **rpTrail.log** – Records the response to all requests to ACSLS from ACSAPI clients or cmd_proc, and all requests to the GUI or the SCSI Client interface to logical libraries except for database queries. The information logged includes the requestor, the request, and the request's time stamp.
  rpTrail.log is managed by the following variables:
  - LM_RP_TRAIL enables this audit trail of ACSLS events. The default is TRUE.
  - RP_TRAIL_LOG_SIZE specifies the threshold size at which the rpTrail.log is compressed and archived.
  - RP_TRAIL_FILE_NUM specifies the number of archived rpTrail logs to retain.
  - RP_TRAIL_DIAG specifies whether the rpTrail messages should include additional diagnostic information. The default is FALSE.

- **Library Volume Statistics** – Records all events affecting volumes (cartridges) in a tape library, including whenever a volume is mounted, dismounted, moved, entered, ejected, or found by audit or Cartridge Recovery. If Library Volume Statistics is enabled, this information is recorded in the acsss_stats.log.
  Library Volume Statistics is managed by the following variables:
  - LIB_VOL_STATS enables this Library Volume Statistics. The default is OFF.
  - VOL_STATS_FILE_NUM specifies the number of archived acsss_stats.log files to retain.
  - VOL_STATS_FILE_SIZE specifies the threshold size at which the acsss_stats.log is archived.

ACSLS log/sslm directory

Within the ACSLS log directory, information about the ACSLS GUI and the SCSI Client interface to logical libraries is logged in the sslm directory. This directory includes links to WebLogic audit logs. The sslm directory includes these logs:

- **slim_event.g#.log[.pp#]** – This records both events from the ACSLS GUI and the SCSI client interface. It includes messages of logical library configuration changes, and SCSI client events.
  - The **.g#** is the generation number of this log.
  - The **.pp#** is the parallel process number of this log. (If there are multiple processes logging at the same time, the logs from the additional processes will be assigned a parallel process number.

- **smce_trace.log** – This traces activity from SCSI clients to ACSLS logical libraries using SCSI Media Changer Interface emulation.

- **guiAccess.log** – This is a link to WebLogic's access.log. See Configuring and Using the WebLogic Audit Logs.

- **AcslsDomain.log** – This is a link to WebLogic's AcslsDomain.log. See Configuring and Using the WebLogic Audit Logs.
- **AdminServer.log** – This is a link to WebLogic's AdminServer.log. See Configuring and Using the WebLogic Audit Logs.

Viewing ACSLS Audit Trails from the GUI's Log Viewer

Access the Log Viewer from the Configuration and Administration section of the GUI Navigation Tree. The Log Viewer displays information combined from the acsss_event_log and the smce_trace_log.

View System Events from the GUI

You can also view System Events from the Configuration and Administration section of the GUI Navigation Tree. Every discrete library operation is recorded in the System Events log. Each record in this log contains an event time stamp, an event type, and a description of the event.

Configuring and Using the Solaris Audit Logs

Determine your Solaris auditing policy. The Oracle Solaris Auditing section in the ***Oracle System Administration: Security Services*** manual can help you plan for what events to audit, where your audit logs should be saved, and how you want to review them.

If you have not enabled custom Solaris audit trails, these audit trails of logins and Unix commands issued by the acsss, acsdb, and acssa users are available:

- Users who are currently signed on to Unix are recorded in the Unix utmpx and past user access is recorded in the wtmpx database.

- Use the "last" command to see all access to a user ID (e.g. "last acsss"). For more information see the man pages for: wtmpx, last, and getutxent.

- The .*_history (i.e. [dot]*_history) files in a user's home directory record the commands issued by that user.
  For the acsss user these may include:
  .bash_history
  .psql_history
  .sh_history

  On Solaris /var/adm/sulog records successful and unsuccessful attempts to execute su and become superuser or another user.

Configuring and Using the WebLogic Audit Logs

Refer to Securing ***Oracle WebLogic Server 11g Release 1 (10.3.3)*** for the options for securing a WebLogic server, and the audit trail possibilities with WebLogic.

WebLogic records access to the ACSLS GUI in the following directory:

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

This directory includes the following files:

access.log

- There are archived versions named access.log##### (e.g. access.log00001)
- This provides a detailed audit trail of a GUI user activity.
- For logins look for "AcslsLoginForm".
- Note: There is a link to the access log in: $ACS_HOME/logs/sslm/guiAccess.log

AcslsDomain.log

- This reports WebLogic and ACSLS GUI operations.
- Note: There is a link to the access log in: $ACS_HOME/logs/sslm/AcslsDomain.log

AdminServer.log

- This reports WebLogic and ACSLS GUI operations.
- Note: There is a link to the access log in: $ACS_HOME/logs/sslm/AdminServer.log

Part 4: Security Considerations for Developers

This section provides information useful to developers developing or supporting applications that use ACSLS to manage Oracle StorageTek Tape Libraries.

Enable the Firewall Security on the Client Application's Server

Restrict the ports used for communication and disable portmapper on the client's application server by enabling firewall security. See the ***CSC Developer's Toolkit User's Guide***, Appendix B: Firewall-Secure Operation.

Part 5: Appendices

Appendix A: Secure Deployment Checklist

1. Enforce password management.
2. Restrict network access.
    a) ACSLS and the tape libraries it manages should be behind the corporate firewall.
    b) Enable the ACSLS Firewall Secure Option.
    c) Consider enabling firewall security for ACSLS client applications.
3. Harden the Solaris operating system.
4. Apply all security patches and workarounds.
5. Contact Oracle Support if you come across vulnerability in Oracle ACSLS

References

ACSLS Documentation

The ACSLS documentation is saved in libraries organized by ACSLS release. Access this from Tape Storage Documentation page. (The individual ACSLS documentation libraries include the version number in their URLs. Hence, a link to a specific library becomes obsolete as soon as the library is updated.) The ACSLS 8.1 documentation includes:

- ***ACSLS 8.1 Installation Guide***
- ***ACSLS 8.1 Administrator's Guide***
- ***ACSLS 8.1 Product Information***
  This includes software and hardware requirements, an overview of ACSLS, plus the tape libraries, tape drives, and media supported.
- ***ACSLS 8.1 Messages*** (and status codes)
- ***ACSLS 8.1 Release Notes***
- ***ACSLS-HA 8.1 Cluster: Installation, Configuration, and Operations***
- ***ACSLS 8.1 Interface Reference Manual***

Oracle Solaris

The Oracle Solaris 10 8/11 [U9] Information Library includes a section on: Securing the Oracle Solaris 10 8/11 Operating System.

Reference ***Oracle Solaris 10 Security Guidelines*** for details.

Oracle WebLogic

The Oracle WebLogic Server Documentation Library for WebLogic 10.3.3 (which is used by ACSLS 8.1) has a section on Security.

Securing Oracle WebLogic Server 11G Release 1 (10.3.3) explains the details of securing a WebLogic server.