

**StorageTek Automated Cartridge System Library
Software**

Security Guide

Release 8.3

E49313-02

June 2014

StorageTek Automated Cartridge System Library Software Security Guide, Release 8.3

E49313-02

Copyright © 2013, 2014, Oracle and/or its affiliates. All rights reserved.

Primary Author: Chris Morrison

Contributing Author: George Noble, Martin Ryder, Veda Prescott, Terry Schmitt, and Mike Williams

Contributor:

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

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.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Contents

Preface	v
Audience.....	v
Documentation Accessibility	v
1 Overview	
Product Overview	1-1
General Security Principles	1-1
Keep Software Up To Date	1-1
Restrict Network Access to Critical Services.....	1-1
Follow the Principle of Least Privilege	1-2
Monitor System Activity	1-2
Keep Up To Date on Latest Security Information	1-2
2 Secure Installation	
Understand Your Environment	2-1
Which resources need to be protected?	2-1
From whom are the resources being protected?.....	2-1
What will happen if the protections on strategic resources fail?	2-1
Recommended Procedure for Securing ACSLS	2-1
Securing ACSLS Internet Communication	2-2
Secure ACSLS and Tape Libraries Behind the Corporate Firewall	2-2
ACSLS Firewall Security Option.....	2-2
Ethernet Ports Used for ACSLS Communication.....	2-2
Configuring Firewalls running on the ACSLS Server	2-4
Installing and Configuring Solaris	2-5
Installing and Configuring Linux	2-6
Auditing Linux Security.....	2-6
SELinux Security	2-6
Installing and Configuring ACSLS	2-7
Perform a Standard ACSLS Installation	2-7
Use Strong Passwords for the ACSLS User IDs	2-7
Restrict Access to ACSLS Files	2-7
Set 'root' as the Effective User ID for Three ACSLS Files	2-7
Review Settings for ACSLS Static and Dynamic Variables.....	2-8
Configuring WebLogic	2-8

Use the ACSLS userAdmin.sh utility to create and maintain ACSLS GUI users.....	2-8
Using the ACSLS GUI.....	2-8
Install the Latest JRE Version on GUI Client Systems	2-8
Accessing the ACSLS GUI	2-8
Installing ACSLS HA	2-9

3 Security Features

The Security Model.....	3-1
Configuring and Using Authentication.....	3-1
ACSLS User Authentication by the Solaris or Linux Operating Systems.....	3-1
ACSLS GUI User Authentication by WebLogic	3-1
Audit Considerations	3-2
Keeping Audited Information Manageable	3-2
Evaluate the purpose for auditing.....	3-2
Audit knowledgeably.....	3-2
Configuring and Using the ACSLS Audit Logs	3-2
ACSLS Log Directory	3-2
ACSLS Log/sslm Directory	3-3
Viewing ACSLS Audit Trails from the GUI's Log Viewer	3-4
View System Events from the GUI.....	3-4
Configuring and Using the Solaris Audit Logs.....	3-4
Configuring and Using the Linux Audit Logs.....	3-5
Configuring and Using the WebLogic Audit Logs.....	3-5

4 Security Considerations for Developers

Enable the Firewall Security on the Client Application's Server.....	4-1
--	-----

A Secure Deployment Checklist

B References

Preface

This document describes the security features of Oracle's StorageTek Automated Cartridge System Library Software (ACSL) and the ACSL High Availability solution (ACSL HA).

Because ACSL HA and the ACSL SNMP Agent also run on the ACSL server, protecting the ACSL server protects ACSL, ACSL HA, and the ACSL SNMP Agent.

Audience

This guide is intended for anyone involved with using security features and secure installation and configuration of ACSL.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

Overview

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

Note: Throughout this document, the Automated Cartridge System Library Software product is referred to as ACSLS, and the ACSLS High Availability solution is referred to as ACSLS HA.

Product Overview

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 product 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. This document assumes that you are running ACSLS 8.3 or a later release, with all relevant maintenance applied. Running the latest ACSLS release assures that you have the latest enhancements and fixes.

Apply all significant security patches to the OS and to services installed with the OS. Please apply these patches selectively, because applying all available updates may install new features and even new OS releases that ACSLS and ACSLS HA have not been tested with.

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 every release for revisions.

Secure Installation

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

Understand Your Environment

To better understand security needs, the following questions must be asked:

Which resources need to be protected?

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 are the resources being protected?

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 Procedure for Securing ACSLS

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.

Securing ACSLS Internet Communication

This section describes recommendations for deploying ACSLS to secure Internet access.

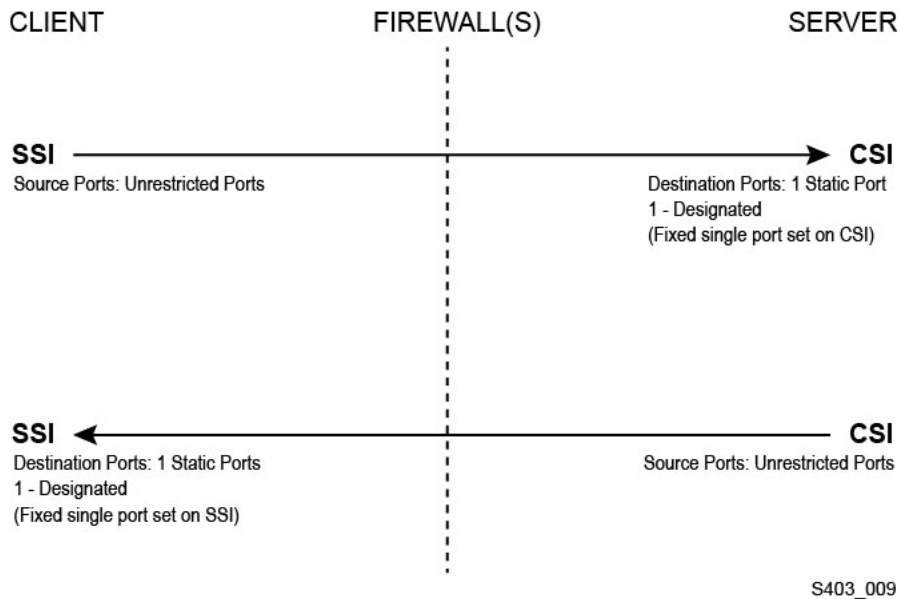
Secure ACSLS and Tape Libraries Behind the Corporate Firewall

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.

Note: If you have an IPv4-based edge firewall, it should be configured to drop all outbound IPv4 protocol 41 packets and UDP port 3544 packets to prevent Internet hosts from using any IPv6-over-IPv4 tunnelled traffic to reach internal hosts.

ACSLS 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 ACSLS 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 defaults to TRUE in ACSLS 8.1 and later releases.



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

Ethernet Ports Used for ACSLS Communication

- The following ports are used on the ACSLS server. Ensure that any firewalls are configured to allow traffic to these ports. This included firewalls implemented by ipfilter on Solaris or iptables on Linux.
 - 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`.

- 5432 default port for internal communication from ACSLS to the PostgreSQL database (the `PGPORT` environment variable for the `acsss` user ID).
If port 5432 is taken, the next available higher port number is used.

Note: Port 5432 only needs to be accessible from localhost (127.0.0.1).

- 7001 and 7002 - used by WebLogic and the ACSLS GUI.
- 30031 or the ACSLS CSI's listening port, set by `CSI_INET_PORT`.
- 50003 port used for internal communication from the ACSLS GUI and Java components to legacy ACSLS processing. This is not configurable.
- For client applications to communicate with ACSLS through the ACSAPI, the following ports must be open:
 - The client application must be able to communicate with the ACSLS CSI's listening port. This defaults to 30031, and is set by the `CSI_INET_PORT` static variable.

You can discover which ports are in use by ACSLS to listen for requests from ACSAPI clients with the following command from your Unix shell:

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

The port IDs will be listed in the last field of the display.

- The ACSAPI client (for example, a NetBackup or SAM-QFS server) sets its fixed incoming port using the `SSI_INET_PORT` environmental variable. Specify a port in the range of 1024-65535, excluding ports 50001 and 50004. The ACSLS server must be able to communicate with this port.

Note: On an ACSAPI client server, ports 50001 and 50004 are used for `AF_INET` domain IPC communication to the mini-Event Logger and from client applications to the SSI.

See the Firewall Security Option appendix in the *ACSLs Administrator's Guide* for more details about communication between client applications and ACSLS.

- Ports that must be open on an SL8500 or SL3000 library:

ACSLs communicates with these ports on an SL8500 or SL3000 library's 2A and 2B Ethernet connections. If communication from ACSLS to these ports is blocked, ACSLS cannot manage the library.

- 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

Configuring Firewalls running on the ACSLS Server

Besides external firewalls, firewall protection can be implemented on your ACSLS server through ipfilter on Solaris or iptables on Linux. This describes how to manage these firewalls running on your ACSLS server.

- Managing ipfilter on Solaris:

Consult the man pages for ipf and ipfilter for detailed information.

- The ipfilter firewall is enabled (disabled) by 'root' using the command:

```
svcadm enable ipfilter (svcadm disable ipfilter)
```

- To learn the current status of ipfilter:

```
svcs ipfilter
```

- Firewall policies are defined in the file: /etc/ipf/ipf.conf

To allow free communication between components on the local host (e.g. between ACSLS and WebLogic or between the GUI and the ACSLS database), include a statement such as:

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

or

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

You need to define policies that allow access to all of the ports that are needed for ACSLS. For example, to include a policy allowing remote Web-based browsers to access the ACSLS GIU, you need to open up ports 7001 and 7002.

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

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

After you discover which ports are used by ACSLS to listen for requests from ACSAPI clients, add 'pass in quick' statements for each of these ports.

It may be necessary to include a 'pass in quick' statement for the RPC portmapper port, 111.

The last statement in your proposed rule set, "block in from any", states that no traffic should reach the host unless specifically allowed in previous statements.

- Managing iptables on Linux:

- The iptables firewall is enabled (disabled) by 'root' using the command:

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

- To check the status of iptables:

```
service iptables status
```

- The policy file for iptables is /etc/sysconfig/iptables:

You need to define policies that allow access to all of the ports that are needed for ACSLS. For example, to include a policy that allows remote http/https access to the ACSLS GUI, you should update that file to include exceptions for ports 7001 and 7002 using statements like:

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

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

After you discover which ports are used by ACSLS to listen for requests from ACSAPI clients, you will need to add exceptions for each of these to the iptables policy file. It may be necessary to include an exception statement for the RPC portmapper port, 111.

Installing and Configuring Solaris

This section describes how to install and configure Solaris securely.

Suggestions include:

- Apply all significant security patches to the OS and to services installed with the OS. Please apply these patches selectively, because applying all available updates may install new features and even new OS releases that ACSLS and ACSLS HA have not been tested with.

- 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.

To see all the services:

```
svcs
```

To disable telnet, rlogin, and ftp:

```
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-bind. Do not disable it.

If Solaris is installed with the Secure by Default option, you need to alter a network configuration property for rpc-bind to permit ACSAPI clients to send requests to ACSLS.

See the *ACSLs Installation manual*, "Installing ACSLS on Solaris" chapter, "Installing Solaris" section for details.

- Some Ethernet ports on the ACSLS server need to be open for communication with ACSLS. Client applications use specific Ethernet ports for communication with ACSLS, and ACSLS communicates with specific ports on tape libraries. See [Ethernet Ports Used for ACSLS Communication](#) for the ports that need to be available for ACSLS communication. On the ACSLS server ensure that ipfilter is configured to allow traffic to the ports used by ACSLS.

Determine your Solaris auditing policy. The "Auditing in Oracle Solaris" 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 Linux

Suggestions to install and configure Linux securely:

- Apply all significant security patches to the OS and to services installed with the OS. Please apply these patches selectively, because applying all available updates may install new features and even new OS releases that ACSLS and ACSLS HA have not been tested with.

- Make sure that telnet and rlogin are not installed or disabled. Use ssh instead.

Also make sure that ftp is not installed or disabled, and use sftp instead.

To see all services, login as root and:

```
service --status-all
```

- To delete services permanently, use:

```
svccfg delete -f service-name
```

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

- Network services, specifically rpcbind, must be enabled to allow ACSLS client communication.

When launching rpc on Linux, launch it with the `-i` flag.

- Some Ethernet ports on the ACSLS server need to be open for communication with ACSLS. Client applications use specific Ethernet ports for communication with ACSLS, and ACSLS communicates with specific ports on tape libraries. See [Ethernet Ports Used for ACSLS Communication](#) for the ports that need to be available for ACSLS communication. On the ACSLS server ensure that iptables is configured to allow traffic to the ports used by ACSLS.

Auditing Linux Security

Determine your Linux auditing policies. The “Configuring and Using Auditing” section in *Oracle Linux: Security Guide for Release 6* can help you plan for what events to audit, where your audit logs should be saved, and how you want to review them.

Some useful logs and commands for auditing Linux security include:

- View `var/log/secure` as root to see the history of login attempts and other access messages.
- The parameter `'last' | more` gives you a history of users logged in.
- The `/var/log/audit/audit.log.[0-9]` keeps a log of access attempts that were denied by SE Linux. You must be user root to view these.

SELinux Security

ACSL 8.3 is designed to run in optional Security Enhanced Linux environments. SELinux provides access control to files, directories, and other system resources that go beyond the traditional protection found standard in Unix environments. In addition to owner-group-public permission access, SELinux includes access control based on user role, domain, and context. The agent that enforces access control over all system resources is the Linux kernel.

The root user on a Linux system can set enforcement on or off with the `setenforce` command.

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

Use `Enforcing` or `1` to put SELinux in enforcing mode. Use `Permissive` or `0` to put SELinux in permissive mode

To view the current system enforcement status, use the command `getenforce`.

Three SELinux policy modules are loaded into the kernel when you install ACSLS: `allowPostgr`, `acsdb`, and `acsdb1`. These modules provide the definitions and enforcement exceptions that are necessary for ACSLS to access its own database and other system resources while SELinux enforcement is active. With these modules installed, you should be able to run normal ACSLS operations, including database operations such as `bdb.acsss`, `rdb.acsss`, `db_export.sh` and `db_import.sh` without the need to disable SELinux enforcement.

For more information, refer to the section on SELinux in the “Troubleshooting” Appendix in the *StorageTek ACSLS 8.3 Administrator’s Guide*.

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 a latter ACSLS release 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.

Set ‘root’ as the Effective User ID for Three ACSLS Files

The installation script advises customers that the effective user id of ‘root’ must be set (`setuid`) in three executable files in the `/export/home/ACSSS` file system:

- `acsss` (This binary must be run with ‘root’ privileges because it is used to start and stop system services required by the ACSLS application.)
- `db_command` (This binary starts and stops the PostgreSQL database engine that controls and maintains the ACSLS database.)
- `get_diags` (This binary is invoked by a customer to collect comprehensive system diagnostic information that may be needed in the context of a service support call.)

During the installation of ACSLS with `pkgadd`, customers are prompted Do you want to install these as `setuid/setgid` files? By answering `y` to the prompt, you allow these three commands to be run by users in the `acsls` group, even though the utilities perform certain system operations that require root privileges.

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 Administrator’s Guide*.

Configuring WebLogic

ACSLs 8.1 and later releases use WebLogic for its web server. WebLogic is installed with ACSLS.

Refer to *Oracle Fusion Middleware Securing Oracle WebLogic Server 11g Release 1 (10.3.5)* 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 installation.

Using the ACSLS GUI

To use ACSLS GUI, you need to install the latest JRE Version and access the ACSLS GUI through a browser.

Install the Latest JRE Version on GUI Client Systems

Make sure the latest version of the Java Runtime Environment (JRE) 1.6 is installed on the systems that will use the ACSLS GUI to access ACSLS.

Note: ACSLS 8.3 requires JRE 1.6 or 1.7.

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 Cluster: Installation, Configuration, and Operations.

Security Features

This section describes the specific security mechanisms offered by ACSLS.

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 users are authenticated by the Solaris or Linux OSs while ACSLS GUI users are authenticated by WebLogic.

ACSLs User Authentication by the Solaris or Linux Operating Systems

The ACSLS users: `acsss` and `acssa` must log into Solaris or Linux and be authenticated by the 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 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 Installation Guide* and the *ACSLs Administrator's Guide*, "Utilities" chapter, section on `userAdmin.sh`.

Audit Considerations

General audit considerations that apply to ACSLS are described here.

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 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 (for example `last acsss`). For more information see the man pages for: `wtmpx`, `last`, and `getutent`.
- The `.*_history` (that is `[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 Linux Audit Logs

Refer to the Configuring and Using Auditing and Configuring and Using System Logging sections in *Oracle Linux: Security Guide for Release 6* for details about collecting and analyzing audit and system logs.

Configuring and Using the WebLogic Audit Logs

Refer to *Oracle Fusion Middleware Securing Oracle WebLogic Server 11g Release 1 (10.3.5)* 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##### (for example 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/sslsm/guiAccess.log.

- AcslsDomain.log
 - This reports WebLogic and ACSLS GUI operations.

Note: There is a link to the access log in: \$ACS_HOME/logs/sslsm/AcslsDomain.log.

- AdminServer.log
 - This reports WebLogic and ACSLS GUI operations.

Note: There is a link to the access log in: \$ACS_HOME/logs/sslsm/AdminServer.log.

Security Considerations for Developers

This section provides information useful to developers developing or supporting applications that use ACSLS to manage Oracle's 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."

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 or Linux operating system.
4. Apply all security patches and workarounds.
5. Contact Oracle Services, Oracle Tape Library Engineering, or account representative if you come across vulnerability in StorageTek ACSLS.



References

ACSLS Documentation

The ACSLS documentation is saved in libraries organized by ACSLS release. Access this from Tape Storage Documentation page.

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

(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 documentation includes:

- *ACSLS Installation Guide*
- *ACSLS Administrator's Guide*
- *ACSLS Product Information*

This includes software and hardware requirements, an overview of ACSLS, plus the tape libraries, tape drives, and media supported.

- ACSLS Messages (and status codes)
- *ACSLS Release Notes*
- *ACSLS-HA Cluster: Installation, Configuration, and Operations*
- *ACSLS Interface Reference Manual*

Oracle Solaris

The Oracle Solaris 10 1/13 [U11] Information Library includes the *Oracle Solaris 10 Security Guidelines*. Refer to it for details.

The Oracle Solaris 11.1 Information Library includes the *Oracle Solaris 11 Security Guidelines*. Refer to it for details.

Oracle Linux

The Oracle Linux 6 Information Library includes the *Oracle Linux: Security Guide for Release 6*. Refer to it for details.

Oracle WebLogic

The Oracle WebLogic Server Documentation Library for WebLogic 10.3.5 (which is used by ACSLS 8.2) has a section on Security.

Oracle Fusion Middleware Securing Oracle WebLogic Server 11G Release 1 (10.3.5) explains the details of securing a WebLogic server.

