Software del sistema de biblioteca de sistema de cartuchos automático StorageTek

Guía de seguridad

Versión 8.4

E68246-01

Septiembre de 2015

ORACLE

Software del sistema de biblioteca de sistema de cartuchos automático StorageTek
Guía de seguridad

E68246-01

Tabla de contenidos

Prólogo

En este documento, se describen las funciones de seguridad de StorageTek Automated Cartridge System Library Software (ACSLS) de Oracle y la solución de alta disponibilidad de ACSLS (ACSLS HA). Como ACSLS HA y el agente SNMP de ACSLS también se ejecutan en el servidor de ACSLS, al proteger este servidor también se protegen ACSLS, ACSLS HA y el agente SNMP de ACSLS.

Destinatarios

Esta guía está destinada a cualquier persona que se encargue de la utilización de funciones de seguridad y de la instalación y la configuración seguras de ACSLS.

Accesibilidad a la documentación

Para obtener información sobre el compromiso de Oracle con la accesibilidad, visite el sitio web del Programa de Accesibilidad de Oracle en `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

Acceso a My Oracle Support
Los clientes de Oracle que hayan contratado servicios de soporte electrónico pueden acceder a ellos mediante My Oracle Support. Para obtener información, visite `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` o, si tiene alguna discapacidad auditiva, visite `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs`.

1

Visión general

En esta sección, se brinda una descripción general de ACSLS y se explican los principios generales de la seguridad de la aplicación.

Nota:

En este documento, se hace referencia al producto Automated Cartridge System Library Software como ACSLS y a la solución de alta disponibilidad de ACSLS como ACSLS HA.

Visión general del producto

ACSLS es el software del servidor de bibliotecas de cintas de Oracle que controla una o más bibliotecas de cintas StorageTek para clientes de sistemas abiertos. Un sistema de cartuchos automático (ACS) es una biblioteca de cintas o un grupo de bibliotecas de cintas conectadas mediante puertos Passthru (PTP). ACSLS gestiona uno o más ACS mediante comandos de "ruta de control" que se envían a través de la red. El software incluye un componente de administración del sistema, interfaces para aplicaciones de sistemas cliente y aplicaciones de gestión de bibliotecas.

Principios generales de seguridad

Los siguientes principios son fundamentales para usar cualquier producto de manera segura.

Mantenga el software actualizado

Uno de los principios de una buena práctica de seguridad es mantener todas las versiones y todos los parches de software actualizados. En este documento, se supone que está ejecutando ACSLS 8.4 o una versión posterior, con el mantenimiento pertinente aplicado. Ejecutar la última versión de ACSLS garantiza que tendrá las últimas mejoras y correcciones.

Aplique todos los parches de seguridad importantes al sistema operativo y los servicios instalados con él. Aplique estos parches de manera selectiva, ya que la aplicación de todas las actualizaciones disponibles podría instalar nuevas funciones e incluso versiones nuevas del sistema operativo con las que ACSLS y ACSLS HA todavía no se han probado.

Restrinja el acceso de red a los servicios críticos

Mantenga ACSLS y las bibliotecas que gestiona protegidos con un firewall. Se recomienda usar una red privada para comunicaciones TCP/IP entre ACSLS y las bibliotecas de cintas.

Siga el principio de privilegios mínimos

El principio del menor privilegio indica que los usuarios deben recibir la menor cantidad de privilegios para realizar sus trabajos. Los privilegios de usuarios deben ser revisados con regularidad para determinar la relevancia con las responsabilidades actuales de los puestos.

En ACSLS, esto significa que los operadores que solo emiten comandos de rutina mediante cmd_proc deberían conectarse como usuarios acssa. Los administradores de sistemas que se conectan como usuario acsss también tienen acceso a una gama más amplia de utilidades y comandos de configuración. Para las operaciones normales, no es necesario utilizar el ID de usuario acsdb.

Supervise la actividad del sistema

La seguridad del sistema depende de tres pilares: buenos protocolos de seguridad, configuración del sistema correcta y supervisión del sistema. Las auditorías y la revisión de los registros de auditoría son útiles para cumplir con este requisito. Cada componente dentro de un sistema tiene algún grado de capacidad de supervisión. Siga los consejos de auditoría de este documento y supervise los registros de auditoría en forma periódica.

Manténgase actualizado sobre la información de seguridad más reciente

Oracle mejora continuamente su software y su documentación. Consulte este documento con cada versión para ver las revisiones.

2

Instalación segura

En esta sección, se detalla el proceso de planificación e implementación para una instalación y configuración seguras, y se describen las topologías de implementación recomendadas para ACSLS.

Comprensión del entorno

Para comprender mejor las necesidades de seguridad, deben hacerse las siguientes preguntas:

¿Qué recursos necesitan protección?

Los recursos clave que ACSLS gestiona son las bibliotecas de cintas, las unidades y los cartuchos. Deben ser protegidos de accidentes y del acceso malicioso. Por ejemplo, evitar que las personas se conecten por error en un servidor ACSLS diferente mediante el uso de distintas contraseñas para los ID de usuario de ACSLS en diferentes servidores.

¿De quién se protegen los recursos?

Debe proteger los recursos de almacenamiento de cinta del acceso interno y externo no autorizado.

¿Qué sucede si falla la protección de los recursos estratégicos?

ACSLS puede montar cartuchos en unidades de cintas. Si un usuario puede conectarse a la unidad de cinta a través de la ruta de datos, también puede leer datos de la cinta si no está encriptada.

Los usuarios que tienen acceso a ACSLS y a una biblioteca de cintas pueden introducir y expulsar cartuchos de una biblioteca de cintas.

Procedimiento recomendado para asegurar ACSLS

Al asegurar ACSLS y los componentes de infraestructura necesarios, siga este procedimiento a fin de garantizar la continuidad del funcionamiento de ACSLS una vez realizados los cambios:

- Instale ACSLS.
- Verifique que ACSLS esté funcionando correctamente. Esto incluye la configuración y la auditoría de bibliotecas, el montaje y el desmontaje de las cintas, la introducción y expulsión de las cintas y la realización de copias de seguridad y restauración de la base de datos.
- Implemente el cambio para aumentar la seguridad.
- Verifique que ACSLS siga funcionando correctamente.

Protección de la comunicación de Internet con ACSLS

En esta sección, se describen las recomendaciones para la implementación de ACSLS para garantizar el acceso a Internet.

Protección de ACSLS y las bibliotecas de cintas detrás del firewall corporativo

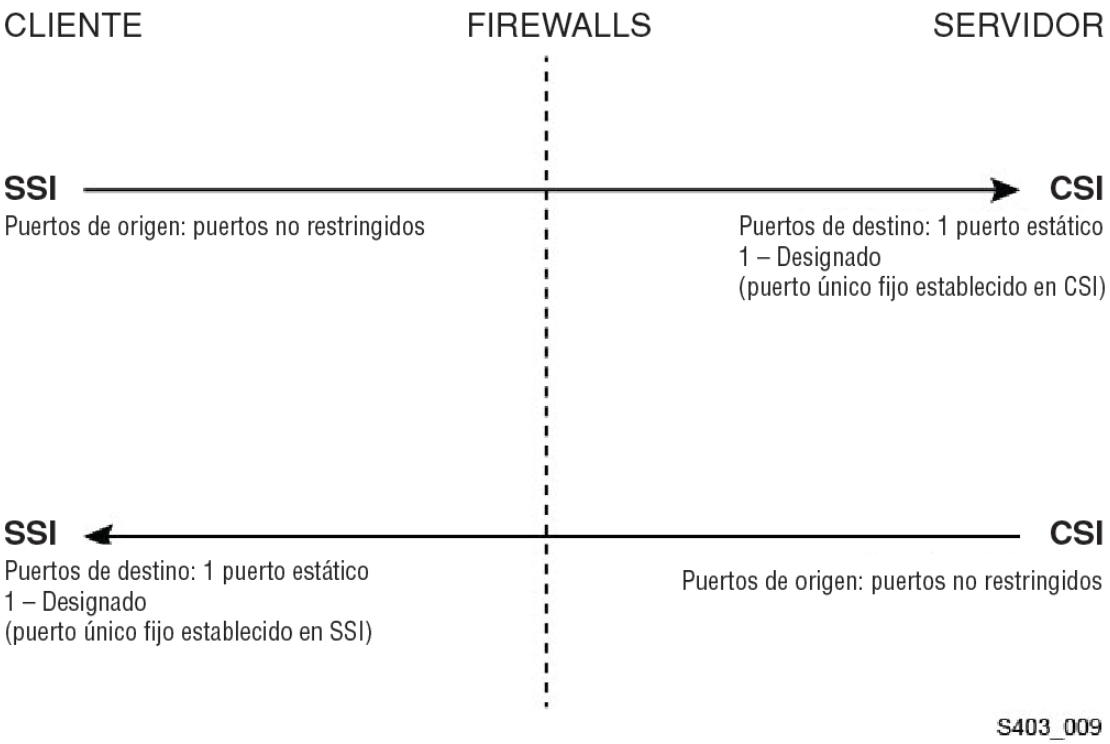
ACSLS y las bibliotecas de cintas que admite deberían implementarse detrás del firewall corporativo. Si las personas que trabajan en forma remota necesitan conectarse al servidor ACSLS, pueden hacerlo mediante una VPN.

Nota:

Si tiene un firewall de borde basado en IPv4, debería estar configurado para eliminar los 41 paquetes de IPv4 de salida y los 3544 paquetes de puerto UDP a fin de evitar que los host de Internet utilicen el tráfico de túnel IPv6 sobre IPv4 para llegar a los hosts internos.

Opción de seguridad de firewall de ACSLS

Si las aplicaciones cliente, que utilizan ACSLS para montar cintas y gestionar bibliotecas de cintas, están separadas de ACSLS por un firewall, recomendamos activar la opción de seguridad de firewall. Incluso si las aplicaciones cliente no están separadas de ACSLS por un firewall, la implementación de esta opción proporciona mayor seguridad a ACSLS al restringir los puertos utilizados para la comunicación entre ACSLS y sus aplicaciones cliente, como se muestra a continuación. Por estos motivos, la variable estática CSI_FIREWALL _SECURE tiene como valor por defecto TRUE (Verdadero) en ACSLS 8.1 y versiones posteriores.



Para obtener detalles, consulte el apéndice "Opción de seguridad de firewall" en la *Guía del administrador de ACSLS*.

Puertos Ethernet utilizados para la comunicación de ACSLS

- Los siguientes puertos se utilizan en el servidor ACSLS. Asegúrese de que los firewalls estén configurados para permitir el tráfico entre estos puertos. Esto incluye los firewalls implementados por ipfilter en Solaris o iptables en Linux.
  - 22 en ambas direcciones, utilizado para el acceso de ssh.
  - Asignador de puertos 111, a menos que el asignador de puertos esté desactivado.
  - 115 utilizado para SFTP (Secure File Transfer Protocol).
  - Puerto por defecto 161 para el agente SNMP de ACSLS - obtener/configurar/recorrer.
  - Puerto por defecto 162 para el agente SNMP de ACSLS - capturas.

    Nota:

    Los puertos utilizados por el agente SNMP de ACSLS se pueden configurar mediante el comando: *`AcslsAgtdSnmpConf [ -p port ] [-t trap port] [-d]`*. La opción *`-d`* muestra la configuración actual. Después de cambiar la configuración del puerto, debe reiniciar el agente con el comando *`agentRegister`*.

  - Puerto por defecto 5432 para comunicación interna de ACSLS con la base de datos de PostgreSQL (variable de entorno PGPORT para el ID de usuario de acsss).

Si el puerto 5432 está tomado, se utiliza el siguiente número de puerto más alto disponible.

Nota:

El puerto 5432 solo debe ser accesible desde el host local (127.0.0.1).

- 7001 y 7002 - utilizado por WebLogic y la GUI de ACSLS.
- 30031 o el puerto de recepción de CSI de ACSLS, configurado mediante CSI _INET_PORT.
- Puerto 50003 utilizado para la comunicación interna desde la GUI de ACSLS y los componentes Java para el procesamiento de ACSLS heredado. Esto no se puede configurar.

- Para que las aplicaciones cliente se comuniquen con ACSLS a través de ACSAPI, los siguientes puertos deben estar abiertos:
  - La aplicación cliente debe poder comunicarse con el puerto de recepción de CSI de ACSLS. Esto tiene como valor por defecto 30031 y se configura mediante la variable estática CSI_INET_PORT.

    Puede descubrir qué puertos utiliza ACSLS para recibir solicitudes de clientes ACSAPI con el siguiente comando del shell de Unix:

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

    Los ID de puerto se mostrarán en el último campo de la pantalla.
  - El cliente ACSAPI (por ejemplo, un servidor NetBackup o SAM-QFS) define su puerto de entrada fijo con la variable de entorno SSI_INET_PORT. Especifique un puerto en el rango de 1024 a 65535, excepto los puertos 50001 y 50004. El servidor ACSLS debe poder comunicarse con este puerto.

    Nota:

    En un servidor cliente ACSAPI, los puertos 50001 and 50004 son utilizados para la comunicación IPC del dominio AF_INET con el mini log de eventos y desde las aplicaciones cliente a SSI.

  Consulte el apéndice Opción de seguridad de firewall en la *Guía del administrador de ACSLS* para obtener más información acerca de la comunicación entre las aplicaciones cliente y ACSLS.

- Si está instalado el componente XAPI, el servidor de XAPI usa un puerto de recepción fijo para recibir las solicitudes de TCP entrantes provenientes de los clientes de ELS. El puerto de recepción de XAPI se define mediante la variable estática XAPI_PORT. El valor por defecto del puerto XAPI_PORT es 50020. Debe ser un puerto entre 1024 y 65535, y no puede estar en conflicto con ningún otro puerto utilizado por ACSLS ni ninguna otra aplicación.

Consulte el apéndice Interfaz de cliente XAPI en la *Guía del administrador de ACSLS* para obtener más detalles acerca de XAPI_PORT. En este apéndice, también se proporcionan detalles para mostrar y configurar la variable estática XAPI_PORT.

- Puertos que deben estar abiertos en una biblioteca SL8500 o SL3000:

  ACSLS se comunica con estos puertos en las conexiones Ethernet 2A y 2B de una biblioteca SL8500 o SL3000. Si la comunicación desde ACSLS hacia estos puertos está bloqueada, ACSLS no puede gestionar la biblioteca.
  - 50001: se utiliza para la comunicación normal entre ACSLS y la biblioteca
  - 50002: es utilizado por ACSLS HA para determinar si el nodo HA alternativo se puede comunicar con la biblioteca antes de conmutar por error a un nodo alternativo

Configuración de firewalls que se ejecutan en el servidor ACSLS

Además de los firewalls externos, la protección de firewall se puede implementar en su servidor ACSLS a través de ipfilter en Solaris o iptables en Linux. Esto describe cómo gestionar estos firewalls que se ejecutan en su servidor ACSLS.

- Gestión de ipfilter en Solaris:

  Consulte las páginas del comando man para ipf e ipfilter para obtener información detallada.
  - El firewall ipfilter se activa (desactiva) mediante 'root' con el comando:

    ```
    svcadm enable ipfilter (svcadm disable ipfilter)
    ```
  - Para conocer el estado actual de ipfilter:

    ```
    svcs ipfilter
    ```
  - Las políticas de firewall se definen en el archivo: /etc/ipf/ipf.conf

    Para permitir la comunicación libre entre componentes del host local (por ejemplo, entre ACSLS y WebLogic o entre la GUI y la base de datos de ACSLS), incluya una instrucción como:

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

    o

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

    Debe definir políticas que permitan el acceso a todos los puertos necesarios para ACSLS. Por ejemplo, para incluir una política que permita a los exploradores basados en Web acceder a la GUI de ACSLS, debe abrir los puertos 7001 y 7002.

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

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

Después de detectar qué puertos son usados por ACSLS para recibir solicitudes de clientes ACSAPI, agregue las instrucciones 'pass in quick' para cada uno de estos puertos.

Es posible que sea necesario incluir una instrucción 'pass in quick' para el puerto asignador de puertos RPC, 111.

La última instrucción de su conjunto de reglas propuesto, "block in from any", indica que no debe haber tráfico que llegue al host, a menos que se permite específicamente en instrucciones anteriores.

- Gestión de iptables en Linux:
  - El firewall iptables se activa (desactiva) mediante 'root' con el comando:

    ```
    service iptables start (service iptables stop)
    ```
  - Para comprobar el estado de iptables:

    ```
    service iptables status
    ```
  - El archivo de la política para iptables es /etc/sysconfig/iptables:

    Debe definir políticas que permitan el acceso a todos los puertos necesarios para ACSLS. Por ejemplo, para incluir una política que permita el acceso remoto http/https a la GUI de ACSLS, debe actualizar ese archivo para incluir excepciones para los puertos 7001 y 7002 con instrucciones como:

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

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

    Después de detectar qué puertos son utilizados por ACSLS para recibir solicitudes de clientes ACSAPI, deberá agregar excepciones para cada uno de estos en el archivo de la política iptables. Es posible que sea necesario incluir una instrucción de excepción para el puerto asignador de puertos RPC, 111.

Instalación y configuración de Solaris

En esta sección, se describe cómo instalar y configurar Solaris de manera segura.

Entre las sugerencias se incluye:

- Aplique todos los parches de seguridad importantes al sistema operativo y los servicios instalados con él. Aplique estos parches de manera selectiva, ya que la aplicación de todas las actualizaciones disponibles podría instalar nuevas funciones e incluso versiones nuevas del sistema operativo con las que ACSLS y ACSLS HA todavía no se han probado.

- Desactive telnet y rlogin. En su lugar, utilice ssh. También desactive ftp y utilice sftp en su lugar.

  Desactive los servicios telnet, rlogin y ftp emitiendo los siguientes comandos como root.

  Para ver todos los servicios:

  ```
  svcs
  ```

  Para desactivar telnet, rlogin y ftp:

  ```
  svcadm disable telnet
  ```

  ```
  svcadm disable rlogin
  ```

  ```
  svcadm disable ftp
  ```
- No desactive ssh. Usted desea que los usuarios se conecten de manera remota con ACSLS mediante ssh, no telnet o rlogin. Tampoco desactive sftp.
- ACSLS necesita el enlace de rpc. No lo desactive.

  Si Solaris está instalado con la opción Secure by Default (Proteger por defecto), debe alterar una propiedad de la configuración de red para el enlace de rpc permita que los clientes ACSAPI puedan enviar solicitudes a ACSLS.

  Consulte el *Manual de instalación de ACSLS*, capítulo "Instalación e ACSLS" en Solaris, sección "Instalación de Solaris" para obtener más información.
- Algunos puertos Ethernet del servidor ACSLS necesitan abrirse para la comunicación con ACSLS. Las aplicaciones cliente utilizan puertos Ethernet específicos para la comunicación con ACSLS, y ACSLS se comunica con puertos específicos en las bibliotecas de cintas. Consulte Puertos Ethernet utilizados para la comunicación de ACSLS para conocer los puertos que deben estar disponibles para la comunicación de ACSLS. En el servidor ACSLS, asegúrese de que ipfilter esté configurado para permitir el tráfico hacia los puertos utilizados por ACSLS.

Determine su política de auditoría de Solaris. La sección "Auditoría en Oracle Solaris" en "Administración del sistema Oracle: Servicios de seguridad" puede ayudarlo a planear qué eventos desea auditar, dónde guardar los logs de auditoría y cómo desea revisarlos.

Instalación y configuración de Linux

Sugerencias para instalar y configurar Linux de forma segura:

- Aplique todos los parches de seguridad importantes al sistema operativo y los servicios instalados con él. Aplique estos parches de manera selectiva, ya que la aplicación de todas las actualizaciones disponibles podría instalar nuevas funciones e incluso versiones nuevas del sistema operativo con las que ACSLS y ACSLS HA todavía no se han probado.
- Asegúrese de que telnet y rlogin no estén instalados o desactivados. En su lugar, utilice ssh.

También asegúrese de que ftp no esté instalado o desactivado, y use sftp en su lugar.

Para ver todos los servicios, conéctese como root y use:

```
service –-status-all
```

- Para suprimir servicios de forma permanente, use:

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

- No desactive ssh. Usted desea que los usuarios se conecten de manera remota con ACSLS mediante ssh, no telnet o rlogin. Tampoco desactive sftp.
- Los servicios de red, específicamente rpcbind, deben estar activados para permitir la comunicación del cliente ACSLS.

  Al iniciar rpc o Linux, hágalo con el indicador –i.
- Algunos puertos Ethernet del servidor ACSLS necesitan abrirse para la comunicación con ACSLS. Las aplicaciones cliente utilizan puertos Ethernet específicos para la comunicación con ACSLS, y ACSLS se comunica con puertos específicos en las bibliotecas de cintas. Consulte Puertos Ethernet utilizados para la comunicación de ACSLS para conocer los puertos que deben estar disponibles para la comunicación de ACSLS. En el servidor ACSLS, asegúrese de que iptables esté configurado para permitir el tráfico hacia los puertos utilizados por ACSLS.

Auditoría de la seguridad de Linux

Determine sus políticas de auditoría de Linux. La sección "Configuración y utilización de auditoría", de *Oracle Linux: Guía de seguridad para la versión 6* puede ayudarlo a planear qué eventos desea auditar, dónde guardar los logs de auditoría y cómo desea revisarlos.

Aquí se muestran algunos logs y comandos útiles para la auditoría de la seguridad de Linux:

- Ver var/log/secure como root para revisar el historial de intentos de inicio de sesión y otros mensajes de acceso.
- El comando 'last | more' devuelve un historial de los usuarios conectados.
- /var/log/audit/audit.log.[0-9] guarda un log de los intentos de acceso denegados por SE Linux. Para ver esto, debe ser usuario root.

Seguridad de SELinux

ACSLS 8.4 está diseñado para ejecutarse en entornos Security Enhanced Linux opcionales. SELinux proporciona control de acceso a archivos, directorios y otros recursos del sistema que traspasan la protección tradicional encontrada en entornos Unix. Además del acceso con permiso propietario-grupo-público, SELinux incluye control de acceso basado en el rol de usuario, el dominio y el contexto. El agente que ejerce el control de acceso sobre todos los recursos del sistema es el núcleo Linux.

El usuario root de un sistema Linux puede activar o desactivar la aplicación con el comando *setenforce*.

setenforce [Enforcing | Permissive | 1 | 0]

Utilice *Enforcing* o 1 para activar el modo de aplicación en SELinux. Utilice *Permissive* o 0 para activar el modo permisivo en SELinux

Para ver el sistema de aplicación actual del sistema, utilice el comando *getenforce*.

Cuando instala ACSLS, se cargan tres módulos de política SELinux en el núcleo: allowPostgr, acsdb y acsdb1. Estos módulos proporcionan definiciones y excepciones de aplicación que son necesarias para que ACSLS tenga acceso a su propia base de datos y a otros recursos del sistema, mientras la aplicación de SELinux está activa. Con estos módulos instalados, debe poder ejecutar las operaciones normales de ACSLS, incluidas las operaciones de la base de datos, como bdb.acsss, rdb.acsss, db_export.sh y db_import.sh sin la necesidad de desactivar la aplicación de SELinux.

Para obtener más información, consulte la sección sobre SELinux en el apéndice "Resolución de problemas" en la *Guía del administrador de StorageTek ACSLS 8.4*.

Instalación y configuración de ACSLS

En esta sección, se explica cómo instalar ACSLS de manera segura.

Instalación estándar de ACSLS

Realizar una instalación estándar de ACSLS garantiza que tendrá los componentes necesarios.

Si está migrando a una versión posterior de ACSLS de una versión anterior, revise su configuración de las variables estáticas y dinámicas para ver si desea usar más opciones de seguridad, en especial, con respecto a la opción de seguridad de firewall.

Uso de contraseñas seguras para los ID de usuario de ACSLS

ACSLS requiere los ID de usuario de ACSLS: acsss, acssa y acsdb. Elija contraseñas seguras para estos ID y cámbielas en forma regular.

Restricción del acceso a archivos de ACSLS

ACSLS generalmente restringe el acceso a archivos de ACSLS solo al grupo acsls, que incluye los ID de usuario acsss, acssa, acsdb y root. Algunos archivos de base de datos y diagnóstico solo pueden verse mediante un ID de usuario acsls. ACSLS se ejecuta con una configuración umask de 027.

Los archivos de ACSLS no deben permitir la lectura o escritura de todo el mundo. Sin embargo, restringir el acceso más allá de los valores por defecto de la instalación podría hacer que algunas funciones de ACSLS fallen.

Definición de 'root' como el ID de usuario efectivo para tres archivos de ACSLS

La secuencia de comandos de instalación recomienda a los clientes que se defina el ID de usuario de 'root' en tres archivos ejecutables del sistema de archivos /export/home/ACSSS:

- *acsss* (Este binario debe ejecutarse con privilegios 'root' ya que es usado para iniciar y detener los servicios del sistema requeridos por la aplicación ACSLS).
- *db_command* (Este binario inicia y detiene el motor de base de datos de PostgreSQL que controla y mantiene la base de datos ACSLS).
- *get_diags* (Este binario es invocado por un cliente para recopilar información de diagnóstico del sistema completa que podría ser necesaria en el contexto de una llamada al servicio de asistencia técnica).

Durante la instalación de ACSLS con pkgadd, los clientes reciben la pregunta *Do you want to install these as setuid/setgid files?* (¿Desea instalar estos como archivos setuid/setgid?) Al responder *y* (Sí), permite que estos tres comandos sean ejecutados por usuarios en el grupo acsls, aunque las utilidades realicen determinadas operaciones del sistema que requieren privilegios root.

Revisión de la configuración para variables estáticas y dinámicas de ACSLS

Las variables estáticas y dinámicas de ACSLS controlan el comportamiento de muchas funciones de ACSLS. Configure estas variables con la utilidad *acsss_config*. En este documento, se detalla la configuración segura para muchas de estas variables. Cuando las opciones para una variable son presentadas por *acsss_config*; si responde con un signo de interrogación (?), hará que aparezca una explicación detallada de la variable. Esta información también está disponible en el capítulo "Configuración de variables que controlan el comportamiento de ACSLS" de la *Guía del administrador de ACSLS*.

Configuración de WebLogic

ACSLS 8.1 y versiones posteriores usan WebLogic para este servidor web. WebLogic se instala con ACSLS.

Consulte *Oracle Fusion Middleware: Conceptos de seguridad para Oracle WebLogic Server 11g versión 1 (10.3.6)* para conocer las opciones para proteger un servidor WebLogic y las posibilidades de la pista de auditoría con WebLogic.

Uso de la utilidad userAdmin.sh de ACSLS para crear y realizar mantenimiento a los usuarios de la GUI de ACSLS

La utilidad controlada por menú *userAdmin.sh* se utiliza para administrar contraseñas de usuarios de la GUI de ACSLS. Puede agregar usuarios, eliminarlos, mostrarlos en una lista y

cambiar sus contraseñas. WebLogic debe estar ejecutándose para usar esta utilidad. De no ser así, esta utilidad inicia WebLogic y confirma que está en línea antes de mostrar el menú.

La utilidad *`userAdmin.sh`* debe ser ejecutada por root y requiere autenticación acsls_admin. La cuenta de usuario acsls_admin se configura durante la instalación de ACSLS.

Uso de la GUI de ACSLS

Para usar la GUI de ACSLS, debe instalar la última versión de JRE y acceder a la GUI de ACSLS mediante un explorador.

Instalación de la última versión de JRE en sistemas cliente GUI

Asegúrese de tener instalada la última versión de Java Runtime Environment (JRE) en los sistemas que utilizarán la GUI de ACSLS para acceder a ACSLS.

Acceso a la GUI de ACSLS

Abra un explorador e introduzca una URL con el nombre de host del servidor o dirección IP con el siguiente formato:

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

Es mejor utilizar el nombre de host completo o la dirección IP del equipo host. Algunas páginas, incluidas las páginas de ayuda de ACSLS, podrían no verse correctamente si la URL no puede ser resuelta por completo por WebLogic.

Si utiliza http con el puerto 7001, WebLogic automáticamente enrutará sus https al puerto 7002.

Debido a que WebLogic utiliza el protocolo https seguro, su explorador podría advertirle de que el certificado de seguridad no fue registrado y, por lo tanto, no es confiable. Si está seguro de que la URL es su equipo ACSLS, es seguro continuar. En este punto, debería ver la pantalla de inicio de sesión.

Uso de la GUI de ACSLS

El acceso a AcslsDomain en WebLogic se realiza mediante el protocolo seguro https. Este protocolo usa comunicación cifrada entre el explorador y el servidor usando claves privadas y certificados digitales. A continuación se muestran las opciones para obtener un certificado digital:

Certificado de demostración de ACSLS

ACSLS incluye lo que se conoce cono certificado de "demostración". Este certificado proporciona un nivel mínimo de seguridad de cifrado que permite a los clientes comenzar

a usar la GUI de ACSLS sin ningún otro paso de configuración. En los casos en los que la interacción del cliente con la biblioteca de ACSLS se realice por completo dentro de una intranet protegida, este método de certificado de demostración normalmente es suficiente. Sin embargo, este método emplea una clave de cifrado de 512 bits que no es compatible con ciertos exploradores, entre los que se destacan Internet Explorer y FireFox versión 39 y superiores.

Configuración de un certificado digital autofirmado

En la Guía de instalación de ACSLS se proporciona un método detallado paso a paso para que los administradores de ACSLS configuren un certificado digital autofirmado de 2048 bits de longitud. En la sección titulada "Configuración de una clave de cifrado SSL", este método proporciona un certificado compatible con todos los exploradores. Se recomienda a los usuarios no acceder a sitios https con un certificado autofirmado a menos que tengan conocimiento personal de que el recurso web es un sitio de confianza. En el contexto de usuarios de ACSLS y el servidor de control de biblioteca, este nivel de confianza normalmente se comprende bien y, en la mayoría de los casos, no hay necesidad de que el sitio demuestre su integridad mediante la verificación de la firma por parte de un tercero.

Certificados digitales firmados por una autoridad de firma externa

Cada sitio de cliente debe determinar si necesitan proporcionar autenticación de certificado a través de una autoridad de firma externa, como Verisign o Entrust.net. El procedimiento para generar un certificado digital de este tipo se describe en el documento en línea de Oracle de configuración de identidad y confianza, que se encuentra en:

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

Instalación de ACSLS HA

Si utiliza la solución ACSLS High Availability, siga las instrucciones del cluster de ACSLS-HA: instalación, configuración y operaciones.

3

Funciones de seguridad

En esta sección, se describen los mecanismos de seguridad específicos que ofrece ACSLS.

El modelo de seguridad

Los requisitos de seguridad de ACSLS surgen a partir de la necesidad de proteger datos: primero, de la pérdida o el daño accidental y, segundo, de los intentos deliberados no autorizados por acceder a los datos o alterarlos. Entre las preocupaciones secundarias se incluyen la protección contra retrasos innecesarios en el acceso o uso de los datos, o incluso contra la interferencia al punto de la negación de servicio.

Las características de seguridad críticas que brindan estas protecciones son:

- Autenticación: garantiza que solo las personas autorizadas puedan acceder al sistema y a los datos.
- Autorización: brinda control de acceso a los privilegios y los datos del sistema. Esto se amplía con la autenticación, para garantizar que las personas obtengan el acceso adecuado.
- Auditoría: permite a los administradores detectar los intentos de violación del mecanismo de autenticación y los intentos de violación o las violaciones del control de acceso.

Configuración y uso de la autenticación

Por defecto, en Linux y Solaris, los usuarios de ACSLS se autentican mediante PAM (módulos de autenticación conectables). Consulte las páginas man de Solaris o la *Guía del Administrador del Sistema Linux-PAM*.

Los usuarios de la GUI de ACSLS se autentican mediante el servidor LDAP incrustado en WebLogic. Consulte el documento Administración del servidor LDAP incrustado:

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

Autenticación del usuario de ACSLS por los sistemas operativos Solaris o Linux

Los usuarios de ACSLS acsss y acssa deben iniciar sesión en Solaris o Linux y ser autenticados por el sistema operativo para poder usar cmd_proc o, para el usuario acsss, ejecutar utilidades y comandos de configuración de ACSLS. El ID de usuario acsdb también se utiliza para operaciones relacionadas con bases de datos. Como parte del proceso de

instalación de ACSLS, los clientes deben establecer contraseñas para estos ID la primera vez que se conectan. Consulte la *Guía de instalación de ACSLS* para obtener más información.

Autenticación del usuario de la GUI de ACSLS por WebLogic

Los usuarios de la GUI de ACSLS deben conectarse y ser autenticados por WebLogic. acsls_admin se crea durante la instalación de ACSLS y los clientes deben establecer la contraseña. Los clientes pueden agregar otros usuarios de GUI si lo desean con la utilidad `userAdmin.sh`. Para obtener información detallada, consulte la *Guía de instalación de ACSLS* y la *Guía del administrador de ACSLS*, capítulo "Utilidades", sección sobre `userAdmin.sh`.

Consideraciones de auditoría

Aquí se describen las consideraciones generales de auditoría que se aplican a ACSLS.

Conservación de la información auditada de manera que se pueda gestionar

Si bien la auditoría prácticamente no tiene costo, limite la cantidad de eventos auditados lo más posible. Esto minimiza el impacto en el rendimiento en la ejecución de indicaciones auditadas y el tamaño de la pista de auditoría, lo que facilita el análisis, la comprensión y la gestión.

Utilice las siguientes directrices generales para idear una estrategia de auditoría:

Evalúe el propósito de la auditoría

Una vez comprendidos con claridad los motivos de la auditoría, puede idear una estrategia de auditoría adecuada y evitar las auditorías no necesarias.

Audite con conocimiento

Audite el mínimo de las indicaciones, usuarios u objetos necesarios para obtener la información necesaria.

Configuración y uso de los logs de auditoría de ACSLS

ACSLS tiene varios logs de información que le permiten registrar e inspeccionar la actividad de ACSLS.

- Puede ver la mayoría de ellos con vi u otros editores. Los eventos del sistema solo se pueden ver con la GUI de ACSLS.
- La mayoría de los logs se pueden archivar automáticamente cuando alcanzan el tamaño definido por el cliente y se conservará un número de logs especificado por el cliente. Para evitar llenar el sistema de archivos ACSLS, existe un límite configurable para el número

de logs que se conservará. Si desea conservar más archivos log o conservarlos en otro sistema, debe desarrollar su propio procedimiento para archivarlos en una ubicación que tenga espacio suficiente.

- El tamaño, el número de logs archivados que se conservan y otras características de estos archivos son definidas por las variables dinámicas y estáticas ACSLS.

Directorio de logs de ACSLS

El directorio de logs de ACSLS es controlado por la variable estática LOG_PATH. El directorio por defecto es $ACS_HOME/log. Este directorio incluye estos logs:

acsss_event.log
Registra los mensajes de los eventos del sistema ACSLS significativos, los eventos de la biblioteca y los errores.

Cuando el acsss_event.log alcanza el tamaño umbral definido por la variable dinámica LOG_SIZE, se copia en event0.log y se elimina. Durante el proceso de copiado, los logs de eventos se copian en logs conservados con un número mayor y se superpone al log guardado con el número más alto. Por ejemplo: event8.log se copia sobre event9.log, event7.log se copia sobre event8.log, …, event0.log se copia sobre event1.log, acsss _event.log se copia sobre event0.log y acsss_event.log se borra. Esto es controlado por las siguientes variables:

- *EVENT_FILE_NUMBER* especifica el número de logs de eventos que se deben conservar.
- *LOG_SIZE* especifica el tamaño umbral en el que se copia el log de eventos en un log conservado y se trunca.

Use la utilidad *`greplog`* para filtrar el acceso al log acsss_event para incluir o excluir mensajes que contengan palabras específicas. Consulte la sección sobre greplog en el capítulo "Utilidades", de la *Guía del administrador de ACSLS* para obtener más detalles.

Logs de configuración
Existen dos logs que guardan los detalles cuando ACSLS actualiza la configuración de la biblioteca almacenada en la base de datos de ACSLS. Los cambios en la configuración de *`acsss_config`* y *`Dynamic Config`* (la utilidad *`config`*) se registran aquí.

acsss_config.log
Registra los detalles de todas las configuraciones o reconfiguraciones de la(s) biblioteca(s) que admite ACSLS. El último cambio en la configuración se agrega al log de las configuraciones anteriores.

acsss_config_event.log
Registra los eventos producidos durante el proceso de configuración o reconfiguración.

rpTrail.log
Registra la respuesta a todas las solicitudes realizadas a ACSLS desde clientes ACSAPI o cmd_proc, y todas las solicitudes a la GUI o la interfaz cliente de SCSI para bibliotecas

lógicas, salvo las consultas de la base de datos. La información registrada incluye el solicitante, la solicitud y el log de hora de la solicitud.

rpTrail.log es gestionado por las siguientes variables:

- *LM_RP_TRAIL* activa esta pista de auditoría de eventos de ACSLS. El valor por defecto es TRUE (Verdadero).
- *RP_TRAIL_LOG_SIZE* especifica el tamaño umbral en el cual se comprime y se archiva el log rpTrail.log.
- *RP_TRAIL_FILE_NUM* especifica la cantidad de logs rpTrail que se deben conservar.
- *RP_TRAIL_DIAG* especifica si los mensajes de rpTrail deben incluir información de diagnóstico adicional. El valor por defecto es FALSO (Falso).

Estadísticas de volumen de la biblioteca
Registra todos los eventos que afectan los volúmenes (cartuchos) de una biblioteca de cintas, incluye cada vez que se monta, desmonta, mueve, introduce, expulsa o encuentra un volumen a través de la auditoría o la recuperación de cartuchos. Si las estadísticas de volumen de la biblioteca están activadas, esta información se registra en el acsss _stats.log.

Las estadísticas de volumen de la biblioteca son gestionadas por las siguientes variables:

- *LIB_VOL_STATS* activa las estadísticas de volumen de la biblioteca. El valor por defecto es OFF (Desactivado).
- *VOL_STATS_FILE_NUM* especifica el número de archivos acsss_stats.log que se deben conservar.
- *VOL_STATS_FILE_SIZE* especifica el tamaño umbral en el cual se archiva el log acsss _stats.log.

Directorio sslm/de logs de ACSLS

Dentro del directorio de logs de ACSLS, la información sobre la GUI de ACSLS y la interfaz de cliente SCSI para bibliotecas lógicas se registra en el directorio sslm. Este directorio incluye enlaces a logs de auditoría de WebLogic. El directorio sslm incluye estos logs:

slim_event.g#.log[.pp#]
Registra los eventos de la GUI de ACSLS y de la interfaz de cliente SCSI. Incluye mensajes de cambios en la configuración de la biblioteca lógica y eventos de cliente SCSI.

- .g# es el número de generación de este log.
- .pp# es el número de proceso paralelo de este log. Si hay varios procesos registrándose al mismo tiempo, los logs de los procesos adicionales recibirán un número de proceso paralelo.

smce_trace.log
Realiza un seguimiento de la actividad de clientes SCSI en bibliotecas lógicas de ACSLS mediante la emulación de la interfaz del cambiador de medios SCSI.

guiAccess.log
Este es un enlace al log access.log de WebLogic. Consulte Configuración y uso de los logs de auditoría de WebLogic.

AcslsDomain.log
Este es un enlace al log AcslsDomain.log de WebLogic. Consulte Configuración y uso de los logs de auditoría de WebLogic.

AdminServer.log
Este es un enlace al log AdminServer.log de WebLogic. Consulte Configuración y uso de los logs de auditoría de WebLogic.

Visualización de las pistas de auditoría de ACSLS desde el visor de logs de la GUI

Acceda al visor de logs desde la sección de configuración y administración del árbol de navegación de la GUI. El visor de logs muestra información combinada de ???TITLE??? y ???TITLE???.

Visualización de eventos del sistema desde la GUI

También puede ver eventos del sistema desde la sección de configuración y administración del árbol de navegación de la GUI. Cada operación discreta de la biblioteca se guarda en el log de eventos del sistema. Cada entrada de este log contiene una marca de tiempo de un evento, un tipo de evento y una descripción del evento.

Configuración y uso de los logs de auditoría de Solaris.

Determine su política de auditoría de Solaris. La sección de auditoría de Oracle Solaris del manual *Administración del sistema Oracle: Servicios de seguridad* puede ayudarlo a planear qué eventos desea auditar, dónde guardar los logs de auditoría y cómo desea revisarlos.

Si no activó las pistas de auditoría personalizadas de Solaris, están disponibles estas pistas de auditoría de inicios de sesión y comandos de Unix emitidos por acsss, acsdb y acssa:

- Los usuarios que actualmente están conectados a Unix se registran en utmpx de Unix y el acceso de usuario pasado se registra en la base de datos wtmpx.
- Utilice el *último* comando para ver todos los accesos de un ID de usuario (por ejemplo `last acsss`). Para obtener más información, consulte las páginas del comando man para: wtmpx, `last` y getutxent.
- Los archivos *_history (que es [dot]*_history) del directorio principal de un usuario registran los comandos emitidos por ese usuario.

  Para el usuario acsss, pueden incluir:
  - .bash_history
  - .psql_history

- .sh_history

En Solaris, /var/adm/sulog registra los intentos exitosos y fallidos para ejecutar *su* y convertirse en superusuario o en otro usuario.

Configuración y uso de los logs de auditoría de Linux

Consulte las secciones de configuración y uso de auditoría y de configuración y uso de los logs del sistema en *Oracle Linux: Guía de seguridad para la versión 6* para obtener información sobre cómo recopilar y analizar logs de auditoría y del sistema.

Configuración y uso de los logs de auditoría de WebLogic

Consulte *Oracle Fusion Middleware: Conceptos de seguridad para Oracle WebLogic Server 11g versión 1 (10.3.6)* para conocer las opciones para proteger un servidor WebLogic y las posibilidades de la pista de auditoría con WebLogic.

WebLogic registra el acceso a la GUI de ACSLS en el siguiente directorio:

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

Este directorio incluye los siguientes archivos:

- access.log
  - Hay versiones archivadas llamadas access.log##### (por ejemplo, access.log00001).
  - Esto proporciona una pista de auditoría detallada de la actividad de un usuario de la GUI.
  - Para ver los inicios de sesión, consulte "AcslsLoginForm".

    Nota:

    Existe un enlace para acceder al log en: $ACS_HOME/logs/sslm/guiAccess.log.
- AcslsDomain.log
  - Informa las operaciones de WebLogic y la GUI de ACSLS.

    Nota:

    Existe un enlace para acceder al log en: $ACS_HOME/logs/sslm/AcslsDomain.log.
- AdminServer.log
  - Informa las operaciones de WebLogic y la GUI de ACSLS.

    Nota:

    Existe un enlace para acceder al log en: $ACS_HOME/logs/sslm/AdminServer.log.

4

Consideraciones de seguridad para desarrolladores

En esta sección, se proporciona información útil para los desarrolladores que desarrollan o admiten aplicaciones que utilizan ACSLS para gestionar las bibliotecas de cintas de StorageTek de Oracle.

Activación de la seguridad de firewall en el servidor de la aplicación cliente

Restrinja los puertos utilizados para la comunicación y active la seguridad de firewall para desactivar el asignador de puertos en el servidor de la aplicación cliente. Consulte la *Guía del usuario del kit de herramientas para desarrollador de CSC*, en el apéndice B sobre el funcionamiento de la seguridad del firewall.

Apéndice A

Lista de comprobación de la implementación segura

1. Aplique la gestión de contraseñas.
2. Restrinja el acceso a la red.
   a. ACSLS y las bibliotecas de cintas que gestiona deberían estar detrás del firewall corporativo.
   b. Active la opción de seguridad de firewall de ACSLS.
   c. Considere activar la seguridad de firewall para aplicaciones cliente de ACSLS.
3. Proteja el sistema operativo Solaris o Linux.
4. Aplique todos los parches de seguridad y soluciones alternativas.
5. Póngase en contacto con Oracle Services, Oracle Tape Library Engineering o su representante de cuenta si encuentra vulnerabilidades en StorageTek ACSLS.

Apéndice B

Referencias

Documentación de ACSLS
La documentación de ACSLS se guarda en bibliotecas organizadas según la versión de ACSLS. Puede acceder a ellas desde la página de documentación de almacenamiento en cinta:

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

(Cada biblioteca de documentación de ACSLS incluye el número de versión en la URL. Por lo tanto, un enlace a una biblioteca específica se convierte en obsoleto cuando esa biblioteca es actualizada). La documentación de ACSLS incluye:

- *Guía de instalación de ACSLS*
- *Guía del administrador de ACSLS*
- *Información de producto de ACSLS*

  Incluye los requisitos de software y hardware, una descripción general de ACSLS y las bibliotecas de cintas, las unidades de cintas y los medios compatibles.
- Mensajes de ACSLS (y códigos de estado)
- *Notas de la versión de ACSLS*
- *Cluster de ACSLS-HA: instalación, configuración y operaciones*
- *Manual de referencia de la interfaz de ACSLS*

Oracle Solaris
La biblioteca de información de Oracle Solaris 11.2 incluye la *Protección del sistema operativo Oracle Solaris 11*. Consúltela para obtener más información.

Oracle Linux
La biblioteca de información de Oracle Linux 6 incluye la *Guía de seguridad de Oracle Linux 6*. Consúltela para obtener más información.

Oracle WebLogic
La biblioteca de documentación de Oracle WebLogic Server para WebLogic 10.3.6 (que es utilizado por ACSLS 8.2) tiene una sección sobre seguridad.

Oracle Fusion Middleware: Conceptos de seguridad para Oracle WebLogic Server 11g versión 1 (10.3.6) explica los detalles de la protección de un servidor WebLogic.