StorageTek Automated Cartridge System Library Software

Sicherheitshandbuch

Release 8.4

E68245-01

September 2015

ORACLE

StorageTek Automated Cartridge System Library Software
Sicherheitshandbuch

E68245-01

Inhalt

Vorwort

In diesem Dokument werden die Sicherheitsfunktionen der Oracle StorageTek Automated Cartridge System Library Software (ACSLS) und der ACSLS High Availability-Lösung (ACSLS HA) beschrieben. Da ACSLS HA und der ACSLS-SNMP-Agent ebenfalls auf dem ACSLS-Server ausgeführt werden, werden durch den Schutz des ACSLS-Servers ACSLS, ACSLS HA und der ACSLS-SNMP-Agent geschützt.

Zielgruppe

Dieses Handbuch richtet sich an Personen, die an der Verwendung von Sicherheitsfunktionen und der sicheren Installation und Konfiguration von ACSLS beteiligt sind.

Barrierefreie Dokumentation

Informationen über Eingabehilfen für die Dokumentation finden Sie auf der Oracle Accessibility Program-Webseite unter `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

Zugang zum Oracle-Support
Oracle-Kunden mit einem gültigen Oracle-Supportvertrag haben Zugriff auf elektronischem Support über My Oracle Support. Weitere Informationen erhalten Sie unter `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` oder unter `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs`, falls Sie eine Hörbehinderung haben.

1

Kapitel 1. Überblick

Dieser Abschnitt enthält einen Überblick über ACSLS und erläutert die allgemeinen Grundsätze für die Anwendungssicherheit.

Hinweis:

In diesem Dokument wird das Automated Cartridge System Library Software-Produkt als ACSLS bezeichnet und die ACSLS High Availability-Lösung als ACSLS HA.

Produktüberblick

ACSLS ist die Bandbibliotheksserversoftware von Oracle, mit der StorageTek-Bandbibliotheken für offene Systemclients gesteuert werden. Ein Automated Cartridge System (ACS) ist eine Bandbibliothek oder eine Gruppe von Bandbibliotheken, die über Passthru-Ports (PTPs) miteinander verbunden sind. ACSLS verwaltet ACSs über "control path"-Befehle, die über ein Netzwerk gesendet werden. Die Software umfasst eine Systemadministrationskomponente, Schnittstellen zu Clientsystemanwendungen und Funktionen zur Bibliotheksverwaltung.

Allgemeine Sicherheitsgrundsätze

Die folgenden Grundsätze sind für die sichere Verwendung jedes Produkts von wesentlicher Bedeutung.

Software muss immer auf dem neuesten Stand sein

Einer der Grundsätze für einen sicheren Betrieb besteht darin, alle Softwareversionen und Patches auf dem neuesten Stand zu halten. In diesem Dokument wird davon ausgegangen, dass Sie ACSLS 8.4 oder ein höheres Release verwenden, in dem die relevanten Wartungspatches eingespielt wurden. Durch Ausführung des neuesten ACSLS-Release wird sichergestellt, dass alle Verbesserungen und Fehlerkorrekturen implementiert sind.

Spielen Sie alle wichtigen Sicherheitspatches in das BS und in Services, die im BS installiert sind, ein. Spielen Sie diese Patches selektiv ein. Wenn Sie nämlich alle verfügbaren Updates anwenden, können dadurch neue Funktionen und sogar neue BS-Releases installiert werden, mit denen ACSLS und ACSLS HA nicht getestet wurden.

Netzwerkzugriff auf kritische Services begrenzen

Sowohl ACSLS als auch die verwalteten Bibliotheken müssen sich hinter einer Firewall befinden. Die Verwendung eines privaten Netzwerks für TCP-/IP-Kommunikationen zwischen ACSLS und den Bandbibliotheken wird empfohlen.

Prinzip der geringsten Rechte

Das Prinzip der geringsten Rechte bedeutet, dass Benutzern so wenig Berechtigungen wie möglich zur Ausführung ihrer Aufgaben erteilt werden. Benutzerrechte müssen in regelmäßigen Abständen geprüft werden, um ihre Relevanz in Bezug auf berufliche Verantwortungsbereiche zu bestimmen.

Bei ACSLS bedeutet dies, dass Operatoren, die nur Routinebefehle mit cmd_proc absetzen, sich als acssa-Benutzer anmelden müssen. Systemadministratoren, die sich als acsss-Benutzer anmelden, haben auch Zugriff auf ein breiteres Spektrum an Dienstprogrammen und Konfigurationsbefehlen. Für normale Vorgänge ist die Verwendung der acsdb-Benutzer-ID nicht erforderlich.

Systemaktivität überwachen

Systemsicherheit steht auf drei Beinen: gute Sicherheitsprotokolle, richtige Systemkonfiguration und Systemüberwachung. Diese dritte Anforderung wird durch Auditing und Prüfung von Auditdatensätzen erfüllt. Jede Komponente innerhalb eines Systems verfügt zu einem gewissen Grad über Überwachungsmöglichkeiten. Audithinweise in diesem Dokument befolgen und Auditdatensätze regelmäßig überwachen

Sicherheitsinformationen immer auf dem neuesten Stand halten

Oracle nimmt fortwährend Verbesserungen an Software und Dokumentation vor. Prüfen Sie dieses Dokument mit jeder neuen Version auf Änderungen.

2

Kapitel 2. Sichere Installation

In diesem Abschnitt werden die Schritte bei der Planung und Implementierung für eine sichere Installation und Konfiguration aufgeführt, und die empfohlenen Deployment-Topologien für ACSLS werden beschrieben.

Umgebung analysieren

Damit Sie die Sicherheitsanforderungen besser verstehen, müssen die folgenden Fragen gestellt werden:

Welche Ressourcen müssen geschützt werden?

Die Schlüsselressourcen, die von ACSLS verwaltet werden, sind Bandbibliotheken, Laufwerke und Kassetten. Sie müssen vor unbeabsichtigtem und böswilligem Zugriff geschützt werden. Beispiel: Es muss verhindert werden, dass Personen sich versehentlich bei einem anderen ACSLS-Server anmelden, indem unterschiedliche Passwörter für die ACSLS-Benutzer-IDs auf unterschiedlichen Servern verwendet werden.

Vor wem müssen die Ressourcen geschützt werden?

Sie möchten die Bandspeicherungsressourcen vor unautorisiertem internen und externen Zugriff schützen.

Was geschieht, wenn der Schutz bei strategischen Ressourcen versagt?

ACSLS kann Kassetten in Bandlaufwerken mounten. Wenn ein Benutzer über den Datenpfad eine Verbindung zum Bandlaufwerk herstellen kann, kann er Daten auf dem Band lesen, die nicht verschlüsselt sind.

Benutzer, die sowohl auf ACSLS als auch auf eine Bandbibliothek Zugriff haben, können Kassetten in Bandbibliotheken einlegen und daraus entnehmen.

Empfohlene Prozedur zur Sicherung von ACSLS

Bei der Sicherung von ACSLS und der erforderlichen Infrastrukturkomponenten gehen Sie wie hier beschrieben vor, um sicherzustellen, dass ACSLS auch nach den Änderungen weiter funktioniert:

- Installieren Sie ACSLS.
- Prüfen Sie, ob ACSLS ordnungsgemäß funktioniert. Konfigurieren und prüfen Sie dabei Bibliotheken, mounten und dismounten Sie Bänder, legen Sie Bänder ein, und entnehmen Sie diese. Erstellen Sie außerdem ein Backup der Datenbank, und stellen Sie diese wieder her.
- Implementieren Sie die Änderung, um die Sicherheit zu erhöhen.
- Prüfen Sie, ob ACSLS weiterhin ordnungsgemäß funktioniert.

Sichern der ACSLS-Internetkommunikation

In diesem Abschnitt wird beschrieben, wie Sie ACSLS für einen sicheren Internetzugang bereitstellen.

Sichern von ACSLS und Bandbibliotheken hinter der Unternehmensfirewall

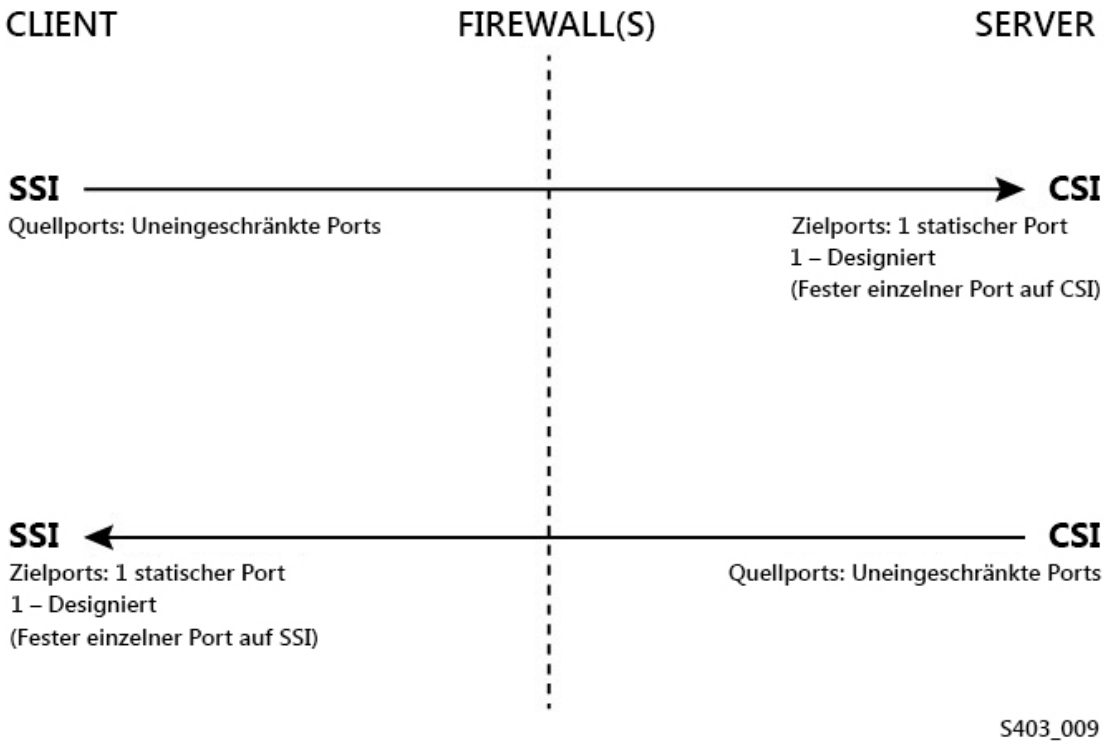
ACSLS und die davon unterstützten Bandbibliotheken müssen hinter der Unternehmensfirewall bereitgestellt werden. Wenn sich Personen, die entfernt arbeiten, beim ACSLS-Server anmelden müssen, können sie über ein VPN auf den Server zugreifen.

Hinweis:

Wenn Sie eine IPv4-basierte Edge-Firewall verwenden, muss diese so konfiguriert werden, dass alle ausgehenden IPv4-Protokoll-41-Pakete und UDP-Port-3544-Pakete gelöscht werden, um zu verhindern, dass Internethosts mit IPv6-over-IPv4-Tunnelmechanismen auf interne Hosts zugreifen können.

ACSLS Firewall Security-Option

Wenn Clientanwendungen, die ACSLS für das Mounten von Bändern und Verwalten von Bandbibliotheken verwenden, durch eine Firewall von ACSLS getrennt sind, wird empfohlen, die Firewall Security-Option zu aktivieren. Selbst wenn die Clientanwendungen nicht durch eine Firewall von ACSLS getrennt sind, bietet die Implementierung der Firewall Security-Option zusätzliche ACSLS-Sicherheit, indem die Ports begrenzt werden, die für die Kommunikation zwischen ACSLS und den Clientanwendungen verwendet werden (wie unten gezeigt). Deshalb ist die statische Variable CSI_FIREWALL_SECURE in ACSLS 8.1 und späteren Releases standardmäßig auf TRUE gesetzt.



Einzelheiten finden Sie im Anhang "Firewall Security-Option" im *ACSLS-Administratorhandbuch*.

Für die ACSLS-Kommunikation verwendete Ethernetports

- Die folgenden Ports werden auf dem ACSLS-Server verwendet. Stellen Sie sicher, dass die Firewalls so konfiguriert sind, dass Datenverkehr an diese Ports zulässig ist. Dies umfasst Firewalls, die mit ipfilter auf Solaris oder iptables auf Linux implementiert wurden.
  - 22 beide Richtungen – für SSH-Zugriff verwendet.
  - 111 Portmapper, es sei denn, Portmapper wurde deaktiviert.
  - 115 für SFTP (Secure File Transfer Protocol) verwendet.
  - 161 Standardport für ACSLS-SNMP-Agent - get/set/walk.
  - 162 Standardport für ACSLS-SNMP-Agent - Traps.

    Hinweis:

    Die vom ACSLS-SNMP-Agent verwendeten Ports können mit folgendem Befehl konfiguriert werden: *`AcslsAgtdSnmpConf [ -p port ] [-t trap port] [-d]`*. Die Option *`-d`* zeigt die aktuelle Einstellung an. Nach Änderung der Porteinstellung müssen Sie den Agent mit dem Befehl *`agentRegister`* neu starten.

  - 5432 Standardport für die interne Kommunikation von ACSLS mit der PostgreSQL-Datenbank (die PGPORT-Umgebungsvariable für die acsss-Benutzer-ID).

    Wenn Port 5432 belegt ist, wird die nächsthöhere verfügbare Portnummer verwendet.

Hinweis:

Port 5432 muss nur für localhost (127.0.0.1) zugänglich sein.

- 7001 und 7002 - werden von WebLogic und der ACSLS-GUI verwendet.
- 30031 oder der Listening-Port von ACSLS CSI, wird von CSI_INET_PORT festgelegt.
- 50003 Port wird zur internen Kommunikation zwischen der ACSLS-GUI und Java-Komponenten zur Legacy-ACSLS-Verarbeitung verwendet. Dieser Port ist nicht konfigurierbar.

- Damit Clientanwendungen über die ACSAPI mit ACSLS kommunizieren können, müssen die folgenden Ports geöffnet sein:
  - Die Clientanwendung muss mit dem Listening-Port von ACSLS CSI kommunizieren können. Der Standardport ist 30031. Er wird von der statischen Variable CSI_INET _PORT festgelegt.

    Mit dem folgenden Befehl aus der Unix-Shell können Sie ermitteln, welche Ports von ACSLS verwendet werden, um auf Anforderungen von ACSAPI-Clients zu horchen:

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

    Die Port-IDs werden im letzten Feld der Anzeige aufgeführt.
  - Der ACSAPI-Client (Beispiel: ein NetBackup- oder SAM-QFS-Server) legt seinen festen eingehenden Port mit der Umgebungsvariable SSI_INET_PORT fest. Geben Sie einen Port im Bereich von 1024 - 65535 an, ausgenommen die Ports 50001 und 50004. Der ACSLS-Server muss mit diesem Port kommunizieren können.

    Hinweis:

    Auf einem ACSAPI-Clientserver werden die Ports 50001 und 50004 für die AF_INET-Domain-IPC-Kommunikation mit dem Mini-Event Logger und von Clientanwendungen zu SSI verwendet.

  Im Anhang "Firewall Security-Option" im *ACSLS-Administratorhandbuch* finden Sie weitere Details zur Kommunikation zwischen Clientanwendungen und ACSLS.

- Wenn die XAPI-Komponente installiert ist. verwendet der XAPI-Server einen festen Listening-Port, um eingehende TCP-Anforderungen von ELS-Clients zu empfangen. Der XAPI-Listening-Port wird von der statischen Variablen XAPI_PORT definiert. XAPI _PORT ist standardmäßig 50020. Er muss zwischen 1024 und 65535 liegen und darf nicht mit anderen von ACSLS oder anderen Anwendungen verwendeten Ports in Konflikt stehen.

  Weitere Einzelheiten zum XAPI_PORT finden Sie im Anhang zur XAPI-Clientbenutzeroberfläche im *ACSLS-Administratorhandbuch*. Dieser Anhang enthält auch Details dazu, wie Sie die statische Variable XAPI_PORT anzeigen und festlegen.

- Ports, die in einer SL8500- oder SL3000-Bibliothek geöffnet sein müssen:

ACSLS kommuniziert mit diesen Ports über die 2A- und 2B-Ethernetverbindungen einer SL8500- oder SL3000-Bibliothek. Wenn die Kommunikation von ACSLS zu diesen Ports blockiert ist, kann ACSLS die Bibliothek nicht verwalten.

- 50001 – Wird für die gesamte normale Kommunikation zwischen ACSLS und der Bibliothek verwendet
- 50002 – Wird von ACSLS HA verwendet, um zu bestimmen, ob der alternative HA-Knoten mit der Bibliothek kommunizieren kann, bevor ein Failover zum alternativen Knoten erfolgt

Konfigurieren von Firewalls, die auf dem ACSLS-Server ausgeführt werden

Neben externen Firewalls kann der Firewallschutz auf dem ACSLS-Server über ipfilter bei Solaris oder iptables bei Linux implementiert werden. Hier wird beschrieben, wie diese Firewalls auf Ihrem ACSLS-Server verwaltet werden.

- Verwalten von ipfilter auf Solaris:

  Auf den Manpages finden Sie detaillierte Informationen zu ipf und ipfilter.

  - Die ipfilter-Firewall wird von "root" mit folgendem Befehl aktiviert (deaktiviert):

    ```
    svcadm enable ipfilter (svcadm disable ipfilter)
    ```
  - So ermitteln Sie die aktuellen Status von ipfilter:

    ```
    svcs ipfilter
    ```
  - Firewallrichtlinien werden in der Datei: /etc/ipf/ipf.conf definiert.

    Um die freie Kommunikation zwischen Komponenten auf dem lokalen Host zuzulassen (beispielsweise zwischen ACSLS und WebLogic oder zwischen der GUI und der ACSLS-Datenbank), nehmen Sie eine Anweisung wie die Folgende auf:

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

    oder

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

    Sie müssen Richtlinien definieren, die den Zugriff auf alle Ports ermöglichen, die für ACSLS benötigt werden. Beispiel: Um eine Richtlinie aufzunehmen, mit der entfernte webbasierte Browser auf die ACSLS-GUI zugreifen können, müssen Sie die Ports 7001 und 7002 öffnen.

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

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

Nachdem Sie ermittelt haben, welche Ports von ACSLS verwendet werden, um auf Anforderungen von ACSAPI-Clients zu horchen, fügen Sie "pass in quick"-Anweisungen für jeden dieser Ports hinzu.

Möglicherweise müssen Sie eine "pass in quick"-Anweisung für den RPC-Portmapper-Port 111 hinzufügen.

Die letzte Anweisung in der vorgeschlagenen Regelgruppe, "block in from any", gibt an, dass kein Datenverkehr den Host erreichen soll, wenn dies nicht in vorherigen Anweisungen ausdrücklich zugelassen wird.

- Verwalten von iptables auf Linux:
  - Die iptables-Firewall wird von "root" mit folgendem Befehl aktiviert (deaktiviert):

    ```
    service iptables start (service iptables stop)
    ```
  - So wird der Status von iptables geprüft:

    ```
    service iptables status
    ```
  - Die Richtliniendatei für iptables ist /etc/sysconfig/iptables:

    Sie müssen Richtlinien definieren, die den Zugriff auf alle Ports ermöglichen, die für ACSLS benötigt werden. Beispiel: Zur Aufnahme einer Richtlinie, die Remote-HTTP/HTTPS-Zugriff auf die ACSLS GUI zulässt, müssen Sie die Datei so aktualisieren, dass sie Ausnahmen für Ports 7001 und 7002 einbezieht. Dazu verwenden Sie Anweisungen wie die Folgenden:

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

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

    Nachdem Sie ermittelt haben, mit welchen Ports ACSLS auf Anforderungen von ACSAPI-Clients horcht, müssen Sie Ausnahmen für jeden dieser Ports zur iptables-Richtliniendatei hinzufügen. Möglicherweise müssen Sie eine Ausnahmeanweisung für den RPC-Portmapper-Port 111 hinzufügen.

Installieren und Konfigurieren von Solaris

In diesem Abschnitt wird beschrieben, wie Sie Solaris sicher installieren und konfigurieren.

Empfehlungen umfassen:

- Spielen Sie alle wichtigen Sicherheitspatches in das BS und in Services, die im BS installiert sind, ein. Spielen Sie diese Patches selektiv ein. Wenn Sie nämlich alle verfügbaren Updates anwenden, können dadurch neue Funktionen und sogar neue BS-Releases installiert werden, mit denen ACSLS und ACSLS HA nicht getestet wurden.
- Deaktivieren Sie telnet und rlogin. Verwenden Sie stattdessen ssh. Deaktivieren Sie außerdem ftp, und verwenden Sie stattdessen sftp.

Deaktivieren Sie die telnet-, rlogin- und ftp-Services, indem Sie die folgenden Befehle als "root" ausgeben.

So zeigen Sie alle Services an:

```
svcs
```

So deaktivieren Sie telnet, rlogin und ftp:

```
svcadm disable telnet
```

```
svcadm disable rlogin
```

```
svcadm disable ftp
```

- Deaktivieren Sie ssh nicht. Benutzer sollen sich entfernt bei ACSLS mit ssh und nicht mit telnet oder rlogin anmelden. Deaktivieren Sie auch nicht sftp.
- ACSLS erfordert rpc-bind. Deaktivieren Sie es nicht.

  Wenn Solaris mit der Option "Secure by Default" installiert wird, müssen Sie eine Netzwerkkonfigurationseigenschaft für rpc-bind ändern, damit ACSAPI-Clients Anforderungen an ACSLS senden können.

  Weitere Einzelheiten finden Sie im *ACSLS-Installationshandbuch*, Kapitel "Installieren von ACSLS unter Solaris", Abschnitt "Installieren von Solaris".
- Einige Ethernetports auf dem ACSLS-Server müssen zur Kommunikation mit ACSLS geöffnet sein. Clientanwendungen verwenden spezifische Ethernetports zur Kommunikation mit ACSLS, und ACSLS kommuniziert mit spezifischen Ports in Bandbibliotheken. In Für die ACSLS-Kommunikation verwendete Ethernetports werden die Ports aufgeführt, die für die ACSLS-Kommunikation verfügbar sein müssen. Stellen Sie auf dem ACSLS-Server sicher, dass ipfilter so konfiguriert ist, dass Datenverkehr zu den von ACSLS verwendeten Ports zugelassen ist.

Bestimmen Sie die Solaris-Auditingrichtlinie. Anhand des Abschnitts "Auditing in Oracle Solaris" in "Oracle System Administration: Security Services" können Sie die Ereignisse planen, die auditiert werden sollen. Außerdem können Sie angeben, wo die Auditlogs gespeichert werden sollen und wie sie geprüft werden sollen.

Installieren und Konfigurieren von Linux

Empfehlungen zur sicheren Installation und Konfiguration von Linux:

- Spielen Sie alle wichtigen Sicherheitspatches in das BS und in Services, die im BS installiert sind, ein. Spielen Sie diese Patches selektiv ein. Wenn Sie nämlich alle verfügbaren Updates anwenden, können dadurch neue Funktionen und sogar neue BS-Releases installiert werden, mit denen ACSLS und ACSLS HA nicht getestet wurden.
- Stellen Sie sicher, dass telnet und rlogin nicht installiert sind oder deaktiviert sind. Verwenden Sie stattdessen ssh.

Stellen Sie außerdem sicher, dass ftp nicht installiert ist oder deaktiviert ist, und verwenden Sie stattdessen sftp.

Um alle Services anzuzeigen, melden Sie sich als root an, und führen Sie folgenden Befehl aus:

```
service –-status-all
```

- Um Services endgültig zu löschen, verwenden Sie:

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

- Deaktivieren Sie ssh nicht. Benutzer sollen sich entfernt bei ACSLS mit ssh und nicht mit telnet oder rlogin anmelden. Deaktivieren Sie auch nicht sftp.
- Netzwerkservices, insbesondere rpcbind, müssen aktiviert sein, um die ACSLS-Clientkommunikation zu ermöglichen.

  Wenn rpc auf Linux gestartet werden soll, starten Sie es mit dem Kennzeichen –i.
- Einige Ethernetports auf dem ACSLS-Server müssen zur Kommunikation mit ACSLS geöffnet sein. Clientanwendungen verwenden spezifische Ethernetports zur Kommunikation mit ACSLS, und ACSLS kommuniziert mit spezifischen Ports in Bandbibliotheken. In Für die ACSLS-Kommunikation verwendete Ethernetports werden die Ports aufgeführt, die für die ACSLS-Kommunikation verfügbar sein müssen. Stellen Sie auf dem ACSLS-Server sicher, dass iptables so konfiguriert ist, dass Datenverkehr zu den von ACSLS verwendeten Ports zugelassen ist.

Auditing von Linux-Sicherheit

Bestimmen Sie die Linux-Auditingrichtlinien. Im Abschnitt "Configuring and Using Auditing" in *Oracle Linux: Security Guide for Release 6* können Sie die Ereignisse planen, die auditiert werden sollen. Außerdem können Sie angeben, wo die Auditlogs gespeichert werden sollen und wie sie geprüft werden sollen.

Einige nützliche Logs und Befehle zum Auditing der Linux-Sicherheit umfassen:

- Zeigen Sie var/log/secure als root an, um die Historie der Anmeldeversuche und andere Zugriffsmeldungen anzuzeigen.
- Mit dem Befehl "last | more" erhalten Sie eine Historie der angemeldeten Benutzer.
- Das /var/log/audit/audit.log.[0-9] enthält ein Log der Zugriffsversuche, die von SELinux abgelehnt wurden. Sie könne diese nur als Root-Benutzer anzeigen.

SELinux-Sicherheit

ACSLS 8.4 ist zur Ausführung in optionalen Security Enhanced Linux-Umgebungen ausgelegt. SELinux ermöglicht eine Zugriffskontrolle für Dateien, Verzeichnisse und andere Systemressourcen, die über den üblichen Standardschutz in Unix-Umgebungen hinausgeht. Zusätzlich zur "owner-group-public"-Zugriffsberechtigung umfasst SELinux

eine Zugriffskontrolle basierend auf Benutzerrolle, Domain und Kontext. Der Agent, der die Zugriffskontrolle über alle Systemressourcen durchsetzt, ist der Linux-Kernel.

Der Root-Benutzer in einem Linux-System kann das Enforcement mit dem Befehl *setenforce* aktivieren oder deaktivieren.

setenforce [Enforcing | Permissive | 1 | 0]

Verwenden Sie *Enforcing* oder 1, um SELinux in den Enforcing-Modus zu versetzen. Verwenden Sie *Permissive* oder 0, um SELinux in den Permissive-Modus zu versetzen

Um den aktuellen System-Enforcement-Status anzuzeigen, verwenden Sie den Befehl *getenforce*.

Drei SELinux-Richtlinienmodule werden in den Kernel geladen, wenn Sie ACSLS installieren: allowPostgr, acsdb und acsdb1. Diese Module stellen die Definitionen und Enforcement-Ausnahmen bereit, die ACSLS benötigt, um auf seine eigene Datenbank und andere Systemressourcen zuzugreifen, während das SELinux Enforcement aktiv ist. Wenn diese Module installiert sind, sollten Sie in der Lage sein, normale ACSLS-Vorgänge auszuführen, einschließlich Datenbankvorgänge wie bdb.acsss, rdb.acsss, db_export.sh und db_import.sh, ohne dass das SELinux-Enforcement deaktiviert werden muss.

Weitere Informationen finden Sie im Abschnitt zu SELinux im Anhang "Fehlerbehebung" im *StorageTek ACSLS 8.4 Administratorhandbuch*.

Installieren und Konfigurieren von ACSLS

In diesem Abschnitt wird beschrieben, wie ACSLS sicher installiert wird.

Standard-ACSLS-Installation durchführen

Bei einer Standard-ACSLS-Installation wird gewährleistet, dass Sie über alle erforderlichen Komponenten verfügen.

Wenn Sie von einem früheren ACSLS-Release zu einem späteren ACSLS-Release migrieren, prüfen Sie die Einstellungen für dynamische und statische Variablen. Dabei können Sie feststellen, ob Sie sicherere Optionen verwenden möchten, insbesondere was die Firewall Secure-Option betrifft.

Sichere Passwörter für die ACSLS-Benutzer-IDs verwenden

ACSLS erfordert die ACSLS-Benutzer-IDs: acsss, acssa und acsdb. Wählen Sie sichere Passwörter für diese IDs, und ändern Sie die Passwörter regelmäßig.

Zugriff auf ACSLS-Dateien begrenzen

ACSLS begrenzt den Zugriff auf die ACSLS-Dateien im Allgemeinen nur auf die acsls-Gruppe, die die acsss-, acssa-, acsdb- und root-Benutzer-IDs umfasst. Auf einige Datenbank- und Diagnosedateien kann nur mit einer einzelnen acsls-Benutzer-ID zugegriffen werden. ACSLS wird mit einer umask-Einstellung von 027 ausgeführt.

ACSLS-Dateien dürfen nicht global lesbar oder beschreibbar gemacht werden. Die Einschränkung des Zugriffs über die Installationsstandardwerte hinaus kann jedoch dazu führen, dass ACSLS-Funktionen nicht erfolgreich ausgeführt werden.

"root" als effektive Benutzer-ID für drei ACSLS-Dateien festlegen

Im Installationsskript werden Kunden darauf hingewiesen, dass die effektive Benutzer-ID "root" in drei ausführbaren Dateien im /export/home/ACSSS-Dateisystem festgelegt werden muss (setuid):

- *`acsss`* (Diese Binärdatei muss mit "root"-Berechtigungen ausgeführt werden, da sie für das Starten und Stoppen von Systemservices verwendet wird, die von der ACSLS-Anwendung benötigt werden.)
- *`db_command`* (Diese Binärdatei startet und stoppt die PostgreSQL-Datenbank-Engine, die die ACSLS-Datenbank steuert und verwaltet.)
- *`get_diags`* (Diese Binärdatei wird von einem Kunden aufgerufen, um umfassende Systemdiagnoseinformationen zu erfassen, die möglicherweise bei einem Servicesupportanruf benötigt werden.)

Während der Installation von ACSLS mit pkgadd wird der folgende Prompt für Kunden angezeigt: *`Do you want to install these as setuid/setgid files?`* Wenn Sie den Prompt mit *`y`* beantworten, lassen Sie zu, dass diese drei Befehle von Benutzern in der acsls-Gruppe ausgeführt werden, selbst wenn die Dienstprogramme bestimmte Systemvorgänge ausführen, die Root-Berechtigungen erfordern.

Einstellungen für statische und dynamische ACSLS-Variablen prüfen

Die statischen und dynamischen ACSLS-Variablen steuern das Verhalten von vielen ACSLS-Funktionen. Legen Sie diese Variablen mit dem Dienstprogramm *`acsss_config`* fest. In diesem Dokument werden sichere Einstellungen für viele dieser Variablen beschrieben. Wenn die Optionen für eine Variable von *`acsss_config`* angezeigt werden und Sie mit einem Fragezeichen (?) antworten, wird eine detaillierte Erläuterung der Variable angezeigt. Diese Informationen sind auch im Kapitel "Variablen festlegen, die das ACSLS-Behavior kontrollieren" im *ACSLS-Administratorhandbuch* verfügbar.

Konfigurieren von WebLogic

ACSLS 8.1 Releases und höher verwenden WebLogic als Webserver. WebLogic wird mit ACSLS installiert.

In *Oracle Fusion Middleware; Sicherheit für Oracle WebLogic Server 11g Release 1 (10.3.6)* werden die Optionen zur Sicherung eines WebLogic-Servers und die Audittrailmöglichkeiten bei WebLogic beschrieben.

Erstellen und Verwalten von ACSLS-GUI-Benutzern mit dem ACSLS-Dienstprogramm userAdmin.sh

Das menügesteuerte Dienstprogramm *`userAdmin.sh`* wird zur Verwaltung von ACSLS-GUI-Benutzerpasswörtern verwendet. Sie können Benutzer hinzufügen, Benutzer entfernen, Benutzer auflisten und Benutzerpasswörter ändern. WebLogic muss gestartet sein, damit dieses Dienstprogramm verwendet werden kann. Wenn WebLogic nicht hochgefahren ist, startet dieses Dienstprogramm es und prüft, ob es online ist, bevor das Menü angezeigt wird.

Das Dienstprogramm *`userAdmin.sh`* muss von root ausgeführt werden und erfordert die acsls_admin-Authentifizierung. Das acsls_admin-Benutzerkonto wird während der ACSLS-Installation konfiguriert.

Verwenden der ACSLS-GUI

Zur Verwendung der ACSLS-GUI müssen Sie die neueste JRE-Version installieren und über einen Browser auf die ACSLS-GUI zugreifen.

Neueste JRE-Version auf GUI-Clientsystemen installieren

Stellen Sie sicher, dass die neueste Version von Java Runtime Environment (JRE) auf den Systemen installiert ist, die die ACSLS-GUI für den Zugriff auf ACSLS verwenden.

Zugreifen auf die ACSLS-GUI

Öffnen Sie einen Browser, und geben Sie eine URL mit dem Serverhostnamen oder der IP-Adresse im folgenden Format ein:

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

Am besten geben Sie einen vollqualifizierten Hostnamen oder die IP-Adresse des Hostrechners ein. Einige Seiten, einschließlich der ACSLS-Hilfeseiten, werden möglicherweise nicht korrekt angezeigt, wenn die URL nicht vollständig von WebLogic aufgelöst werden kann.

Wenn Sie HTTP mit Port 7001 verwenden, nimmt WebLogic automatisch eine Umleitung zu HTTPS auf Port 7002 vor.

Weil WebLogic das sichere HTTPS-Protokoll verwendet, wird im Browser möglicherweise eine Warnung angezeigt, dass das Sitesicherheitszertifikat nicht registriert wurde und die Site somit nicht vertrauenswürdig ist. Wenn Sie sicher sind, dass die URL dem lokalen ACSLS-Rechner entspricht, können Sie gefahrlos fortfahren. Daraufhin sollte der Anmeldebildschirm angezeigt werden.

Verwenden der ACSLS-GUI

Sie greifen mit dem sicheren HTTPS-Protokoll auf die AcslsDomain in WebLogic zu. Dieses Protokoll nutzt verschlüsselte Kommunikation zwischen Browser und Server anhand von

Private Keys und digitalen Zertifikaten. Sie haben folgende Optionen, ein digitales Zertifikat zu erhalten:

ACSLS-Demozertifikat

ACSLS wird mit einem so genannten "Demozertifikat" bereitgestellt. Dieses Zertifikat bietet eine minimale Ebene an Verschlüsselungssicherheit, sodass Kunden mit der Verwendung der ACSLS-GUI beginnen können, ohne weitere Konfigurationsschritte ausführen zu müssen. Wenn die Kundeninteraktion mit der ACSLS-Bibliothek vollständig innerhalb eines gesicherten Intranets stattfindet, ist dieses Demozertifikat normalerweise ausreichend. Bei dieser Methode wird aber ein 512-Bit-Verschlüsselungsschlüssel eingesetzt, der bei bestimmten Browsern nicht unterstützt wird, vor allem Internet Explorer und FireFox Version 39 und höher.

Konfigurieren eines selbstsignierten digitalen Zertifikats

Im ACSLS-Installationshandbuch wird die Methode, mit der ACSLS-Administratoren ein selbstsigniertes digitales Zertifikat mit einer Länge von 2048 Bit konfigurieren, ausführlich beschrieben. Mit der Methode im Abschnitt "Konfigurieren eines SSL-Verschlüsselungsschlüssels" erhalten Sie ein Zertifikat, das auf allen Browsern unterstützt wird. Benutzer, die mit einem selbstsignierten Zertifikat auf eine HTTPS-Site zugreifen, sollten die Site nur dann verwenden, wenn sie genau wissen, dass die Webressource eine vertrauenswürdige Site ist. Im Kontext von ACSLS-Benutzern und dem Bibliothekskontrollserver ist diese Vertrauensebene normalerweise klar umrissen, und in den meisten Fällen ist es nicht erforderlich, dass die Site ihre Integrität anhand einer Drittanbieter-Signaturüberprüfung nachweist.

Von einer Drittanbieter-Signaturstelle signierte digitale Zertifikate

Jede Kundensite kann bestimmen, ob die Zertifikatsauthentifizierung durch eine Drittanbieter-Signaturstelle, wie Verisign oder Entrust.net, bereitgestellt werden muss. Das Verfahren zum Generieren eines derartigen signierten digitalen Zertifikats wird im Oracle-Onlinedokument "Configuring Identity and Trust" unter:

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

Installieren von ACSLS HA

Wenn Sie die ACSLS High Availability-Lösung verwenden, befolgen Sie die Anweisungen in ACSLS-HA-Cluster: Installation, Konfiguration und Vorgänge.

3

Kapitel 3. Sicherheitsfunktionen

In diesem Abschnitt werden die spezifischen Sicherheitsverfahren bei ACSLS beschrieben.

Sicherheitsmodell

Die ACSLS-Sicherheitsanforderungen ergeben sich aus der Notwendigkeit, Daten zu schützen: erstens vor versehentlichem Verlust oder Beschädigung und zweitens vor absichtlichen nicht autorisierten Versuchen, auf diese Daten zuzugreifen oder sie zu ändern. Danach kommt der Schutz vor ungebührlichen Verzögerungen beim Zugriff auf Daten oder der Verwendung von Daten oder sogar vor Störungen bis zu Denial of Service.

Folgende kritische Sicherheitsfunktionen bieten diesen Schutz:

- Authentifizierung: Stellt sicher, dass nur autorisierte Personen auf das System und die Daten zugreifen können.
- Autorisierung: Ermöglicht Zugriffskontrolle für Systemberechtigungen und Daten. Dies baut auf der Authentifizierung auf, um sicherzustellen, dass Einzelpersonen nur den erforderlichen Zugriff erhalten.
- Audit: Beim Audit können Administratoren versuchte Verletzungen des Authentifizierungsverfahrens und versuchte oder erfolgreiche Verletzungen der Zugriffskontrolle erkennen.

Konfigurieren und Verwenden der Authentifizierung

Standardmäßig werden ACSLS-Benutzer bei Linux oder Solaris über PAM (Pluggable Authentication Modules) authentifiziert. Weitere Informationen finden Sie auf den Solaris-Manpages oder im *Linux-PAM System Administrators Guide*.

Benutzer der ACSLS-GUI werden über den eingebetteten LDAP-Server in WebLogic authentifiziert. Weitere Informationen finden Sie im Dokument "Managing the Embedded LDAP Server":

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

ACSLS-Benutzerauthentifizierung durch die Solaris- oder Linux-Betriebssysteme

Die ACSLS-Benutzer acsss und acssa müssen sich bei Solaris oder Linux anmelden. Sie werden vom Betriebssystem authentifiziert, bevor sie cmd_proc verwenden oder (beim

acsss-Benutzer) ACSLS-Dienstprogramme und Konfigurationsbefehle ausführen können. Außerdem wird die acsdb-Benutzer-ID bei datenbankbezogenen Vorgängen verwendet. Im Rahmen der ACSLS-Installation müssen Kunden die Passwörter für diese IDs festlegen, wenn sie sich das erste Mal bei ihnen anmelden. Weitere Einzelheiten finden Sie im *ACSLS-Installationshandbuch*.

ACSLS-GUI-Benutzerauthentifizierung durch WebLogic

ACSLS-GUI-Benutzer müssen sich bei WebLogic anmelden und von WebLogic authentifiziert werden. Der acsls_admin wird während der ACSLS-Installation erstellt, und Kunden müssen sein Passwort festlegen. Kunden können nach Bedarf andere GUI-Benutzer mit dem Dienstprogramm `userAdmin.sh` hinzufügen. Weitere Einzelheiten finden Sie im *ACSLS-Installationshandbuch* und im Kapitel "Utilitys", Abschnitt `userAdmin.sh`, im *ACSLS-Administratorhandbuch*.

Überlegungen zum Auditing

Hier werden allgemeine Überlegungen zum Auditing bei ACSLS beschrieben.

Auditierte Informationen müssen verwaltbar bleiben

Auch wenn das Auditing relativ unaufwendig ist, begrenzen Sie die Anzahl von auditierten Ereignissen so weit wie möglich. Auf diese Weise werden die Performanceauswirkungen bei der Ausführung von auditierten Anweisungen und die Größe des Audittrails minimiert, sodass dieser einfacher zu analysieren, zu verstehen und zu verwalten ist.

Beachten Sie die folgenden allgemeinen Richtlinien bei der Festlegung einer Auditstrategie:

Zweck des Auditings festlegen

Wenn Sie die Gründe für das Auditing genau verstanden haben, können Sie eine entsprechende Auditingstrategie festlegen und ein unnötiges Auditing vermeiden.

Auditing mit Bedacht

Auditieren Sie die Mindestanzahl von erforderlichen Anweisungen, Benutzern oder Objekten, um die gewünschten Informationen zu erhalten.

Konfigurieren und Verwenden der ACSLS-Auditlogs

ACSLS verfügt über verschiedene Logs mit Informationen, mit denen Sie die ACSLS-Aktivität aufzeichnen und prüfen können.

- Die meisten Logs können mit vi und anderen Editoren angezeigt werden. Systemereignisse können nur mit der ACSLS-GUI angezeigt werden.

- Die meisten dieser Logs können automatisch archiviert werden, wenn sie eine bestimmte vom Kunden definierte Größe erreichen. Eine vom Kunden festgelegte Anzahl von Logs wird beibehalten. Damit das ACSLS-Dateisystem nicht zu sehr gefüllt wird, gibt es einen konfigurierbaren Grenzwert für die Anzahl von beibehaltenen Logs. Wenn Sie mehr Logdateien beibehalten oder diese auf einem anderen System beibehalten möchten, müssen Sie Ihre eigene Prozedur entwickeln, um sie an einem Ort mit ausreichend Speicherplatz zu archivieren.
- Größe, Anzahl von beizubehaltenden archivierten Logs und andere Eigenschaften dieser Dateien werden von dynamischen und statischen ACSLS-Variablen definiert.

ACSLS-Logverzeichnis

Das ACSLS-Logverzeichnis wird von der statischen Variable LOG_PATH gesteuert. Das Standardverzeichnis ist $ACS_HOME/log. Dieses Verzeichnis enthält folgende Logs:

acsss_event.log
In diesem Log werden Meldungen für wichtige ACSLS-Systemereignisse, Bibliotheksereignisse und Fehler aufgezeichnet.

Wenn die Größe von acsss_event.log einen von der dynamischen Variable LOG_SIZE definierten Schwellenwert erreicht, wird es in das event0.log kopiert und gelöscht. Beim Kopieren werden die beibehaltenen Ereignislogs in beibehaltene Logs mit einer höheren Nummer kopiert, und das beibehaltene Log mit der höchsten Nummer wird überschrieben. Beispiel: event8.log wird über event9.log kopiert, event7.log wird über event8.log kopiert, …, event0.log wird über event1.log kopiert, acsss_event.log wird über event0.log kopiert, und acsss_event.log wird gelöscht. Dies wird von folgenden Variablen gesteuert:

- *EVENT_FILE_NUMBER* gibt die Anzahl von beizubehaltenden Ereignislogs an.
- *LOG_SIZE* gibt die Schwellenwertgröße an, bei der das Ereignislog in ein beibehaltenes Ereignislog kopiert und abgeschnitten wird.

Mit dem Dienstprogramm *`greplog`* können Sie das acsss_event-Log so filtern, dass Meldungen mit bestimmten Schlüsselwörtern einbezogen oder ausgeschlossen werden. Weitere Einzelheiten finden Sie unter "greplog" im Kapitel "Utilitys" im *ACSLS-Administratorhandbuch*.

Konfigurationslogs
Es gibt zwei Logs, in denen Details aufgezeichnet werden, wenn ACSLS die Bibliothekskonfiguration aktualisiert, die in der ACSLS-Datenbank gespeichert ist. Konfigurationsänderungen von *`acsss_config`* und *`Dynamic Config`* (dem Dienstprogramm *`config`*) werden hier aufgezeichnet.

acsss_config.log
Zeichnet die Details aller Konfigurationen oder erneuten Konfigurationen der Bibliotheken auf, die von ACSLS unterstützt werden. Die letzte Konfigurationsänderung wird an die Aufzeichnung der vorherigen Konfigurationen angehängt.

acsss_config_event.log
Zeichnet Ereignisse während der Konfiguration oder erneuten Konfiguration auf.

rpTrail.log
Zeichnet die Antwort auf alle Anforderungen an ACSLS von ACSAPI-Clients oder cmd_proc und alle Anforderungen an die GUI oder die SCSI-Clientschnittstelle für logische Bibliotheken auf, mit Ausnahme von Datenbankabfragen. Die protokollierten Informationen umfassen den Anforderer, die Anforderung und den Zeitstempel der Anforderung.

rpTrail.log wird von den folgenden Variablen verwaltet:

- *LM_RP_TRAIL* aktiviert diesen Audittrail von ACSLS-Ereignissen. Der Standardwert ist TRUE.
- *RP_TRAIL_LOG_SIZE* gibt die Schwellenwertgröße an, bei der rpTrail.log komprimiert und archiviert wird.
- *RP_TRAIL_FILE_NUM* gibt die Anzahl von archivierten rpTrail-Logs an, die beibehalten werden sollen.
- *RP_TRAIL_DIAG* gibt an, ob die rpTrail-Meldungen zusätzliche Diagnoseinformationen enthalten sollen. Der Standardwert ist FALSE.

Library Volume Statistics
Zeichnet alle Ereignisse auf, die sich auf Datenträger (Kassetten) in einer Bandbibliothek auswirken. Dies umfasst die Angabe, wann ein Datenträger gemountet, dismountet, verschoben, eingelegt, entnommen oder beim Audit oder der Wiederherstellung von Kassetten gefunden wurde. Wenn "Library Volume Statistics" aktiviert ist, werden diese Informationen im acsss_stats.log aufgezeichnet.

Library Volume Statistics werden von folgenden Variablen verwaltet:

- *LIB_VOL_STATS* aktiviert diese Library Volume Statistics. Der Standardwert ist OFF.
- *VOL_STATS_FILE_NUM* gibt die Anzahl von archivierten acsss_stats.log-Dateien an, die beibehalten werden sollen.
- *VOL_STATS_FILE_SIZE* gibt die Schwellenwertgröße an, bei der acsss_stats.log archiviert wird.

ACSLS-Log-/sslm-Verzeichnis

Innerhalb des ACSLS-Logverzeichnisses werden Informationen zur ACSLS-GUI und zur SCSI-Clientschnittstelle zu logischen Bibliotheken im sslm-Verzeichnis aufgezeichnet. Dieses Verzeichnis umfasst Links zu WebLogic-Auditlogs. Das sslm-Verzeichnis enthält die folgenden Logs:

slim_event.g#.log[.pp#]
In diesem Log werden Ereignisse aus der ACSLS-GUI und der SCSI-Clientschnittstelle aufgezeichnet. Es enthält Meldungen über Änderungen der logischen Bibliothekskonfiguration und SCSI-Clientereignisse.

- .g# ist die Generierungsnummer dieses Logs.
- .pp# ist die parallele Prozessnummer dieses Logs. Wenn mehrere Prozesse gleichzeitig protokolliert werden, wird den Logs aus den zusätzlichen Prozessen eine parallele Prozessnummer zugewiesen.

smce_trace.log
Dieses Log verfolgt Aktivitäten von SCSI-Clients zu logischen ACSLS-Bibliotheken mit der SCSI Media Changer Interface-Emulation.

guiAccess.log
Dies ist ein Link zu access.log von WebLogic. Siehe Konfigurieren und Verwenden der WebLogic-Auditlogs.

AcslsDomain.log
Dies ist ein Link zu AcslsDomain.log von WebLogic. Siehe Konfigurieren und Verwenden der WebLogic-Auditlogs.

AdminServer.log
Dies ist ein Link zu AdminServer.log von WebLogic. Siehe Konfigurieren und Verwenden der WebLogic-Auditlogs.

Anzeigen von ACSLS-Audittrails aus dem GUI-Log-Viewer

Rufen Sie den Log-Viewer aus dem Abschnitt "Configuration and Administration" des GUI-Navigationsbaums auf. Der Log-Viewer zeigt aus acsss_event.log und smce_trace.log kombinierte Informationen an.

Anzeigen von Systemereignissen aus der GUI

Sie können im Abschnitt "Configuration and Administration" des GUI-Navigationsbaums auch Systemereignisse anzeigen. Jeder einzelne Bibliotheksvorgang wird im Systemereignislog aufgezeichnet. Jeder Datensatz in diesem Log enthält einen Ereigniszeitstempel, einen Ereignistyp und eine Beschreibung des Ereignisses.

Konfigurieren und Verwenden der Solaris-Auditlogs

Bestimmen Sie die Solaris-Auditingrichtlinie. Im Abschnitt "Oracle Solaris Auditing" im *Oracle System Administration: Security Services*-Handbuch wird beschrieben, wie Sie die Ereignisse planen, die auditiert werden sollen, und wie Sie angeben, wo die Auditlogs gespeichert und wie sie geprüft werden sollen.

Wenn Sie keine benutzerdefinierten Solaris-Audittrails aktiviert haben, sind diese Audittrails zu Anmeldungen und Unix-Befehlen, die von den acsss-, acsdb- und acssa-Benutzern abgesetzt wurden, verfügbar:

- Benutzer, die derzeit bei Unix angemeldet sind, werden in der Unix utmpx-Datenbank und frühere Benutzerzugriffe in der wtmpx-Datenbank aufgezeichnet.

- Mit dem Befehl *last* können Sie alle Zugriffe auf eine Benutzer-ID anzeigen (Beispiel: *last acsss*). Weitere Informationen finden Sie in den Manpages für: wtmpx, *last* und getutxent.
- In den .*_history-(d.h. [dot]*_history-)Dateien im Home-Verzeichnis eines Benutzers werden die von diesem Benutzer abgesetzten Befehle aufgezeichnet.

  Für den acsss-Benutzer können dies folgende Dateien sein:
  - .bash_history
  - .psql_history
  - .sh_history

  Unter Solaris werden in /var/adm/sulog erfolgreiche und nicht erfolgreiche Versuche aufgezeichnet, *su* auszuführen und Superuser oder ein anderer Benutzer zu werden.

Konfigurieren und Verwenden der Linux-Auditlogs

In den Abschnitten "Configuring and Using Auditing" und "Configuring and Using System Logging" im *Oracle Linux: Security Guide for Release 6* wird beschrieben, wie Audit- und Systemlogs erfasst und analysiert werden.

Konfigurieren und Verwenden der WebLogic-Auditlogs

In *Oracle Fusion Middleware; Sicherheit für Oracle WebLogic Server 11g Release 1 (10.3.6)* werden die Optionen zur Sicherung eines WebLogic-Servers und die Audittrailmöglichkeiten bei WebLogic beschrieben.

WebLogic zeichnet die Zugriffe auf die ACSLS-GUI in folgendem Verzeichnis auf:

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

Dieses Verzeichnis umfasst die folgenden Dateien:

- access.log
  - Es enthält die archivierten Versionen namens access.log##### (Beispiel: access .log00001)
  - So erhalten Sie einen detaillierten Audittrail der GUI-Benutzeraktivität.
  - Anmeldungen finden Sie in "AcslsLoginForm".

    Hinweis:

    Es gibt einen Link zum Zugriffslog in: $ACS_HOME/logs/sslm/guiAccess.log.
- AcslsDomain.log
  - In diesem Log werden WebLogic- und ACSLS-GUI-Vorgänge aufgeführt.

    Hinweis:

    Es gibt einen Link zum Zugriffslog in: $ACS_HOME/logs/sslm/AcslsDomain.log.

- AdminServer.log
  - In diesem Log werden WebLogic- und ACSLS-GUI-Vorgänge aufgeführt.

Hinweis:

Es gibt einen Link zum Zugriffslog in: $ACS_HOME/logs/sslm/AdminServer.log.

4

Kapitel 4. Sicherheitsinformationen für Entwickler

Dieser Abschnitt enthält nützliche Informationen für Entwickler, die Anwendungen entwickeln oder unterstützen, die ACSLS zur Verwaltung der Oracle StorageTek-Bandbibliotheken verwenden.

Aktivieren der Firewallsicherheit auf dem Server der Clientanwendung

Begrenzen Sie die für die Kommunikation verwenden Ports, und deaktivieren Sie Portmapper auf dem Anwendungsserver des Clients, indem Sie die Firewallsicherheit aktivieren. Siehe *CSC-Developer - Toolkit-Benutzerhandbuch*, "Anhang B: Firewall-Secure-Vorgang".

Anhang A

Anhang A. Prüfliste für sicheres Deployment

1. Setzen Sie die Passwortverwaltung durch.
2. Schränken Sie den Netzwerkzugriff ein.
   a. ACSLS und die davon verwalteten Bandbibliotheken müssen sich hinter der Unternehmensfirewall befinden.
   b. Aktivieren Sie die ACSLS Firewall Secure-Option.
   c. Sie sollten auch die Firewallsicherheit für ACSLS-Clientanwendungen aktivieren.
3. Schützen Sie das Solaris- oder Linux-Betriebssystem.
4. Spielen Sie alle Sicherheitspatches und Workarounds ein.
5. Wenn Sie Sicherheitslücken in StorageTek ACSLS feststellen, wenden Sie sich an Oracle Services, Oracle Tape Library Engineering oder den zuständigen Oracle-Vertreter für Ihr Benutzerkonto.

Anhang B

Anhang B. Referenzen

ACSLS-Dokumentation
Die ACSLS-Dokumentation ist je nach ACSLS-Release in verschiedenen Bibliotheken gespeichert. Rufen Sie diese auf der Seite "Tape Storage Documentation" auf.

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

(Die einzelnen ACSLS-Dokumentationsbibliotheken enthalten die Versionsnummer in den URLs. Somit ist ein Link zu einer spezifischen Bibliothek veraltet, sobald die Bibliothek aktualisiert wird.) Die ACSLS-Dokumentation umfasst:

- *ACSLS-Installationshandbuch*
- *ACSLS-Administratorhandbuch*
- *ACSLS-Produktinformationen*

  Dies umfasst Hardware- und Softwareanforderungen, einen Überblick über ACSLS sowie Bandbibliotheken, Bandlaufwerke und unterstützte Medien.
- ACSLS-Meldungen (und Statuscodes)
- *ACSLS-Versionshinweise*
- *ACSLS-HA-Cluster: Installation, Konfiguration und Vorgänge*
- *ACSLS-Schnittstelle - Referenzhandbuch*

Oracle Solaris
Die Oracle Solaris 11.2 Information Library umfasst *Securing the Oracle Solaris 11 Operating System*. Dort finden Sie weitere Einzelheiten.

Oracle Linux
Die Oracle Linux 6 Information Library umfasst den *Oracle Linux 6 Security Guide*. Dort finden Sie weitere Einzelheiten.

Oracle WebLogic
Die Oracle WebLogic Server Documentation Library für WebLogic 10.3.6 (das von ACSLS 8.2 verwendet wird) enthält einen Abschnitt zur Sicherheit.

In *Oracle Fusion Middleware; Understanding Security for Oracle WebLogic Server 11g Release 1 (10.3.6)* werden die Details zur Sicherung eines WebLogic-Servers erläutert.