StorageTek Automated Cartridge System Library Software

보안 설명서

릴리스 8.4

E68250-01

2015년 9월

ORACLE

StorageTek Automated Cartridge System Library Software
보안 설명서

E68250-01

차례

머리말

이 문서에서는 Oracle StorageTek ACSLS(Automated Cartridge System Library Software) 및 ACSLS HA(ACSLS High Availability) 솔루션의 보안 기능에 대해 설명합니다. ACSLS HA 및 ACSLS SNMP 에이전트는 ACSLS 서버에서 실행되며 ACSLS 서버를 보호하면 ACSLS, ACSLS HA 및 ACSLS SNMP 에이전트가 보호됩니다.

대상

이 설명서는 ACSLS의 보안 설치/구성 및 보안 기능 사용과 관련된 모든 사람을 대상으로 합니다.

설명서 접근성

오라클의 접근성 개선 노력에 대한 자세한 내용은 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc에서 Oracle Accessibility Program 웹 사이트를 방문하십시오.

오라클 고객지원센터 액세스
지원 서비스를 구매한 오라클 고객은 My Oracle Support를 통해 온라인 지원에 액세스할 수 있습니다. 자세한 내용은 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info를 참조하거나, 청각 장애가 있는 경우 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs를 방문하십시오.

1

개요

이 절에서는 ACSLS의 개요를 살펴보고 응용 프로그램 보안의 일반적인 원칙에 대해 설명합니다.

주:

이 설명서 전체에서 Automated Cartridge System Library Software 제품을 ACSLS라고 하며, ACSLS High Availability 솔루션을 ACSLS HA라고 합니다.

제품 개요

ACSLS는 오픈 시스템 클라이언트를 위해 하나 이상의 StorageTek 테이프 라이브러리를 제어하는 Oracle 테이프 라이브러리 서버 소프트웨어입니다. ACS(Automated Cartridge System)는 PTP(pass-thru-ports)를 통해 연결된 테이프 라이브러리 또는 테이프 라이브러리 그룹입니다. ACSLS는 네트워크에서 전송된 "control path" 명령을 통해 하나 이상의 ACS를 관리합니다. 이 소프트웨어에는 시스템 관리 구성 요소, 클라이언트 시스템 응용 프로그램 인터페이스, 라이브러리 관리 설비가 포함됩니다.

일반 보안 원칙

다음 원칙은 제품을 안전하게 사용하는 데 반드시 필요한 사항입니다.

소프트웨어를 최신 상태로 유지

올바른 보안 실행 원칙 중 하나는 모든 소프트웨어 버전 및 패치를 최신 상태로 유지하는 것입니다. 이 문서는 ACSLS 8.4 이상 릴리스를 실행 중이며 모든 관련 유지 관리가 적용된 상태라고 가정합니다. 최신 ACSLS 릴리스를 실행하면 최신의 향상된 기능과 수정 사항이 보장됩니다.

OS 및 OS와 함께 설치된 서비스에 중요한 보안 패치를 모두 적용합니다. 사용 가능한 모든 업데이트를 적용하면 새로운 기능과 함께 ACSLS 및 ACSLS HA가 테스트되지 않은 새 OS 릴리스도 설치될 수 있으므로 해당 패치는 선별적으로 적용하십시오.

중요한 서비스로 네트워크 액세스 제한

ACSLS와 관리되는 라이브러리를 방화벽 뒤에 둡니다. ACSLS와 테이프 라이브러리 간의 TCP/IP 통신에 사설 네트워크를 사용할 것을 권장합니다.

최소 권한 원칙 준수

최소 권한 원칙이란 사용자에게 작업을 수행할 수 있는 최소한의 권한을 부여해야 한다는 것입니다. 사용자 권한을 정기적으로 검토하여 현재 작업 책임에 따라 권한이 적절한지 확인해야 합니다.

ACSLS에서는 cmd_proc를 사용하여 루틴 명령을 실행한 운영자만 acssa 사용자로 로그인해야 한다는 것을 의미합니다. acsss 사용자로 로그인한 시스템 관리자는 더 폭넓은 유틸리티 및 구성 명령에 액세스할 수 있습니다. acsdb 사용자 ID는 일반적 작업에 사용할 필요가 없습니다.

시스템 작동 모니터

시스템 보안은 적합한 보안 프로토콜, 적절한 시스템 구성 및 시스템 모니터링을 기반으로 합니다. 감사 및 감사 레코드 검토는 세번째 요구 사항과 관련됩니다. 시스템 내의 각 구성 요소에는 어느 정도의 모니터링 기능이 있습니다. 이 문서에 있는 감사 권고 사항을 따르고 감사 레코드를 정기적으로 모니터합니다

최신 보안 정보 유지

Oracle은 지속적으로 소프트웨어 및 설명서를 개선하고 있습니다. 개정이 릴리스될 때마다 문서를 확인하십시오.

2

보안 설치

이 절에서는 보안 설치 및 구성에 대한 계획 및 구현 프로세스의 개요를 살펴보고, 권장되는 ACSLS 배치 토폴로지에 대해 설명합니다.

사용자 환경 이해

보안 요구 사항을 더 잘 이해하려면 다음과 같은 질문을 해야 합니다.

어떤 리소스를 보호해야 합니까?

ACSLS가 관리하는 주요 리소스는 테이프 라이브러리, 드라이브, 카트리지입니다. 부주의한 액세스나 악의적인 액세스로부터 보호해야 합니다. 예를 들어, 다양한 서버에서 ACSLS 사용자 ID에 다른 암호를 사용하여 다른 ACSLS 서버에 실수로 로그인하는 것을 막을 수 있습니다.

누구로부터 리소스를 보호합니까?

허용되지 않은 내/외부 액세스로부터 테이프 스토리지 리소스를 보호해야 합니다.

전략적 리소스에 대한 보호를 실패할 경우 어떤 일이 발생합니까?

ACSLS는 테이프 드라이브에 카트리지를 마운트할 수 있습니다. 사용자가 데이터 경로를 통해 테이프 드라이브에 연결할 수 있는 경우, 암호화되지 않은 데이터를 테이프에서 읽을 수 있습니다.

ACSLS와 테이프 라이브러리에 액세스할 수 있는 사용자는 테이프 라이브러리에서 카트리지를 넣고 꺼낼 수 있습니다.

권장되는 ACSLS 보안 절차

ACSLS와 필요한 기반구조 구성 요소를 보안할 때, 변경 후에도 ACSLS가 계속 작동하도록 하려면 이 절차를 따르십시오.

- ACSLS를 설치합니다.
- ACSLS가 올바르게 작동하는지 확인합니다. 라이브러리 구성 및 감사, 테이프 마운트 및 마운트 해제, 테이프 넣기/꺼내기, 데이터베이스 백업 및 복원이 포함됩니다.

- 보안을 강화하도록 변경 사항을 구현합니다.
- ACSLS가 여전히 올바르게 작동하는지 확인합니다.

ACSLS 인터넷 통신 보안

이 절에서는 인터넷 액세스 보안을 위해 ACSLS를 배치하기 위한 권장 사항을 설명합니다.

ACSLS 및 테이프 라이브러리를 회사 방화벽 뒤에 두기

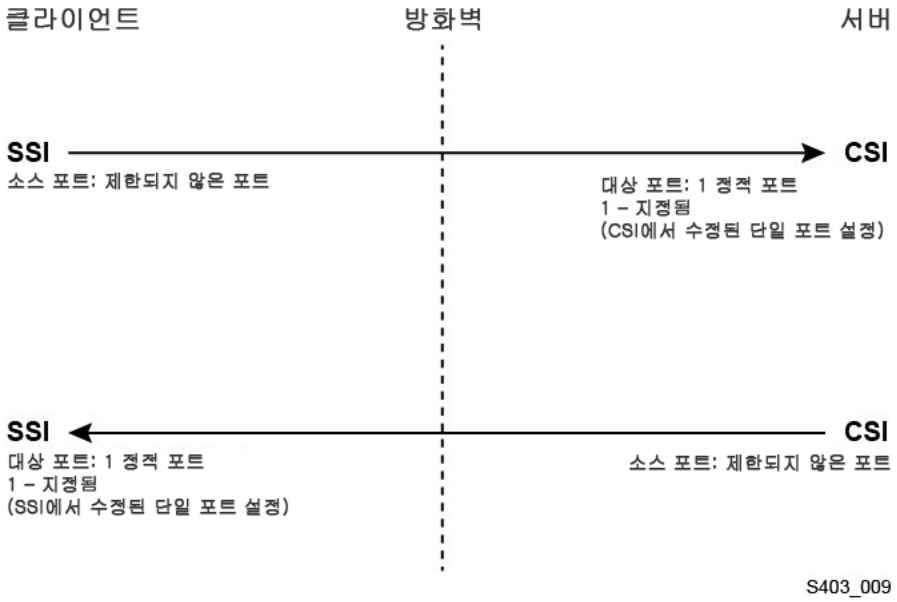
ACSLS와 지원되는 테이프 라이브러리를 회사 방화벽 뒤에 배치해야 합니다. 원격 작업자가 ACSLS 서버에 로그인해야 하는 경우 VPN을 통해 액세스할 수 있습니다.

주:

IPv4 기반의 경계면 방화벽을 사용하는 경우, IPv6-over-IPv4 터널링 트래픽이 내부 호스트에 도달할 수 없도록 모든 아웃바운드 IPv4 프로토콜 41 패킷과 UDP 포트 3544 패킷을 드롭하도록 구성되어야 합니다.

ACSLS 방화벽 보안 옵션

클라이언트 응용 프로그램(ACSLS를 사용하여 테이프를 마운트하고 테이프 라이브러리를 관리함)과 ACSLS가 방화벽으로 분리된 경우, 방화벽 보안 옵션을 사용으로 설정할 것을 권장합니다. 클라이언트 응용 프로그램과 ACSLS가 방화벽으로 분리되지 않았더라도, 방화벽 보안 옵션을 구현하면 아래 표시된 대로 ACSLS와 클라이언트 응용 프로그램 간의 통신에 사용되는 포트를 제한하여 ACSLS 보안을 강화할 수 있습니다. 이러한 이유로 ACSLS 8.1 이상 릴리스에서 CSI_FIREWALL_SECURE 정적 변수가 TRUE로 기본 설정됩니다.



자세한 내용은 *ACSLS Administrator's Guide*의 부록 "Firewall Security Option"을 참조하십시오.

ACSLS 통신에 사용되는 이더넷 포트

- 다음 포트는 ACSLS 서버에서 사용됩니다. 이러한 포트에 트래픽을 허용하도록 방화벽이 구성되었는지 확인합니다. Solaris에서 ipfilter 또는 Linux에서 iptables로 구현된 방화벽이 포함됩니다.
  - 22 - ssh 액세스에 사용되는 양방향 포트
  - 111 portmapper - portmapper가 사용 안함으로 설정되지 않은 경우에 한함
  - 115 - SFTP(Secure File Transfer Protocol)에 사용됨
  - 161 - ACSLS SNMP 에이전트 get/set/walk용 기본 포트
  - 162 - ACSLS SNMP 에이전트 trap용 기본 포트

    주:

    ACSLS SNMP 에이전트에서 사용되는 포트는 *AcslsAgtdSnmpConf [-p port] [-t trap port] [-d]* 명령으로 구성할 수 있습니다. *-d* 옵션은 현재 설정을 표시합니다. 포트 설정을 변경한 후에는 *agentRegister* 명령으로 에이전트를 다시 시작해야 합니다.
  - 5432 - ACSLS에서 PostgreSQL 데이터베이스로 향하는 내부 통신용 기본 포트 (acsss 사용자 ID의 경우 PGPORT 환경 변수)

    5432 포트가 사용 중이면 그 다음 사용 가능한 상위 포트 번호가 사용됩니다.

    주:

    5432 포트는 localhost(127.0.0.1)에서만 액세스할 수 있어야 합니다.
  - 7001 및 7002 - WebLogic 및 ACSLS GUI에서 사용됨
  - 30031 또는 ACSLS CSI의 CSI_INET_PORT로 설정된 수신 포트
  - 50003 - ACSLS GUI 및 Java 구성 요소에서 레거시 ACSLS 프로세싱으로 향하는 내부 통신용 포트. 이것은 구성할 수 없습니다.

- ACSAPI를 통해 ACSLS와 통신하는 클라이언트 응용 프로그램의 경우 다음 포트를 열어야 합니다.
  - 클라이언트 응용 프로그램은 ACSLS CSI의 수신 포트와 통신할 수 있어야 합니다. 기본값은 30031이며 CSI_INET_PORT 정적 변수로 설정됩니다.

    다음 명령을 Unix 셸에서 사용하여 ACSAPI 클라이언트에서 요청을 수신하기 위해 ACSLS에서 사용 중인 포트를 알아낼 수 있습니다.

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

    화면의 마지막 필드에 포트 ID가 나열됩니다.
  - ACSAPI 클라이언트(예: NetBackup 또는 SAM-QFS 서버)는 SSI_INET_PORT 환경 변수를 사용하여 고정된 수신 포트를 설정합니다. 1024-65535 범위에서 50001 및 50004를 제외한 포트를 지정합니다. ACSLS 서버는 이 포트와 통신할 수 있어야 합니다.

주:

ACSAPI 클라이언트 서버에서 50001 및 50004 포트는 미니 이벤트 로거에 대한 AF_INET 도메인 IPC 통신이나 클라이언트 응용 프로그램에서 SSI로 향하는 통신에 사용됩니다.

클라이언트 응용 프로그램과 ACSLS 간의 통신에 대한 자세한 내용은 *ACSLS Administrator's Guide*의 부록 Firewall Security Option을 참조하십시오.

- XAPI 구성 요소가 설치된 경우 XAPI 서버에서는 고정된 수신 포트를 사용하여 ELS 클라이언트에서 수신 TCP 요청을 받습니다. XAPI 수신 포트는 XAPI_PORT 정적 변수를 통해 정의됩니다. XAPI_PORT의 기본값은 50020입니다. 1024에서 65535 사이여야 하며 ACSLS 또는 기타 응용 프로그램에서 사용되는 다른 포트와 충돌할 수 없습니다.

  XAPI_PORT에 대한 자세한 내용은 *ACSLS Adiminstrator's Guide*의 부록 XAPI Client Interface를 참조하십시오. 이 부록에서는 XAPI_PORT 정적 변수 표시 및 설정 방법에 대한 자세한 내용도 제공합니다.

- SL8500 또는 SL3000 라이브러리에서 다음 포트를 열어야 합니다.

  ACSLS는 SL8500 또는 SL3000 라이브러리의 2A 및 2B 이더넷 연결 시 이러한 포트와 통신합니다. ACSLS에서 이러한 포트에 대한 통신이 차단될 경우 ACSLS가 라이브러리를 관리할 수 없습니다.
  - 50001 – ACSLS와 라이브러리 간의 모든 일반적 통신에 사용됨
  - 50002 – ACSLS HA에서 대체 HA 노드로 페일오버하기 전에 라이브러리와 통신할 수 있는지 여부를 결정하는 데 사용됨

ACSLS 서버에서 실행되는 방화벽 구성

외부 방화벽 외에도 Solaris에서 ipfilter 또는 Linux에서 iptables를 통해 ACSLS 서버에 방화벽 보호를 구현할 수 있습니다. 여기서는 ACSLS 서버에서 실행되는 방화벽을 관리하는 방법을 설명합니다.

- Solaris에서 ipfilter 관리:

  자세한 내용은 ipf 및 ipfilter 매뉴얼 페이지를 참조하십시오.
  - 다음 명령을 'root'로 사용하여 ipfilter 방화벽을 사용(사용 안함)으로 설정합니다.

    ```
    svcadm enable ipfilter (svcadm disable ipfilter)
    ```
  - ipfilter의 현재 상태를 확인하려면 다음을 사용합니다.

    ```
    svcs ipfilter
    ```
  - 방화벽 정책은 /etc/ipf/ipf.conf 파일에 정의됩니다.

    로컬 호스트에서 구성 요소 간에 자유로운 통신을 허용하려면(예: ACSLS와 WebLogic 사이 또는 GUI와 ACSLS 데이터베이스 사이) 다음 명령문을 포함합니다.

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

또는

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

ACSLS에 필요한 모든 포트에 액세스를 허용하도록 정책을 정의해야 합니다. 예를 들어, 원격 웹 기반 브라우저에서 ACSLS GUI에 액세스를 허용하는 정책을 포함하려면 7001 및 7002 포트를 열어야 합니다.

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

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

ACSAPI 클라이언트에서 요청을 수신하기 위해 ACSLS에서 사용 중인 포트를 알아낸 후에 이러한 포트에 'pass in quick' 문을 추가합니다.

RPC portmapper 포트 111에 대해 'pass in quick' 문을 포함해야 할 수도 있습니다.

제안된 규칙 세트의 마지막 명령문인 "block in from any"는 이전 명령문에서 특별히 허용되지 않는 한 트래픽이 호스트에 도달할 수 없음을 나타냅니다.

- Linux에서 iptables 관리:
  - 다음 명령을 'root'로 사용하여 iptables 방화벽을 사용(사용 안함)으로 설정합니다.

    ```
    service iptables start (service iptables stop)
    ```
  - iptables의 상태를 확인하려면 다음을 사용합니다.

    ```
    service iptables status
    ```
  - iptables의 정책 파일은 /etc/sysconfig/iptables입니다.

    ACSLS에 필요한 모든 포트에 액세스를 허용하도록 정책을 정의해야 합니다. 예를 들어, ACSLS GUI에 원격 http/https 액세스를 허용하는 정책을 포함하려면 다음 명령문을 사용하여 7001 및 7002 포트에 대한 예외가 포함되도록 파일을 업데이트해야 합니다.

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

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

    ACSAPI 클라이언트에서 요청을 수신하기 위해 ACSLS에서 사용 중인 포트를 알아낸 후에 이러한 포트에 대한 예외를 iptables 정책 파일에 추가해야 합니다. RPC portmapper 포트 111에 대해 예외 명령문을 포함해야 할 수도 있습니다.

Solaris 설치 및 구성

이 절에서는 Solaris를 안전하게 설치하고 구성하는 방법을 설명합니다.

제안 사항은 다음과 같습니다.

- OS 및 OS와 함께 설치된 서비스에 중요한 보안 패치를 모두 적용합니다. 사용 가능한 모든 업데이트를 적용하면 새로운 기능과 함께 ACSLS 및 ACSLS HA가 테스트되지 않은 새 OS 릴리스도 설치될 수 있으므로 해당 패치는 선별적으로 적용하십시오.
- telnet 및 rlogin을 사용 안함으로 설정합니다. 대신 ssh를 사용하십시오. 또한 ftp를 사용 안함으로 설정하고 대신 sftp를 사용하십시오.

  다음 명령을 root로 실행하여 telnet, rlogin, ftp 서비스를 사용 안함으로 설정합니다.

  모든 서비스를 보려면 다음을 사용합니다.

  ```
  svcs
  ```

  telnet, rlogin, ftp를 사용 안함으로 설정하려면 다음을 사용합니다.

  ```
  svcadm disable telnet
  ```

  ```
  svcadm disable rlogin
  ```

  ```
  svcadm disable ftp
  ```
- ssh를 사용 안함으로 설정하지 마십시오. 사용자는 telnet/rlogin이 아닌 ssh를 사용하여 ACSLS에 원격으로 로그인하게 됩니다. 또한 sftp를 사용 안함으로 설정하지 마십시오.
- ACSLS에는 rpc-bind가 필요합니다. 사용 안함으로 설정하지 마십시오.

  Solaris가 Secure by Default 옵션으로 설치된 경우 ACSAPI 클라이언트가 ACSLS에 요청을 전송할 수 있도록 rpc-bind에 대한 네트워크 구성 등록 정보를 변경해야 합니다.

  자세한 내용은 *ACSLS Installation manual*의 "Installing ACSLS on Solaris" 장, "Installing Solaris" 절을 참조하십시오.
- ACSLS와 통신을 위해 ACSLS 서버의 일부 이더넷 포트를 열어야 합니다. 클라이언트 응용 프로그램은 ACSLS와 통신을 위해 특정 이더넷 포트를 사용하며, ACSLS는 테이프 라이브러리의 특정 포트와 통신합니다. ACSLS 통신에 사용할 수 있는 포트는 ACSLS 통신에 사용되는 이더넷 포트를 참조하십시오. ACSLS 서버에서 ACSLS에 사용되는 포트에 트래픽을 허용하도록 ipfilter가 구성되었는지 확인합니다.

Solaris 감사 정책을 결정합니다. "Oracle Solaris Administration: Security Services"의 "Auditing in Oracle Solaris" 절을 참조하여 감사할 이벤트 종류, 감사 로그를 저장할 위치, 이들의 검토 방법을 계획할 수 있습니다.

Linux 설치 및 구성

Linux를 안전하게 설치하고 구성하기 위한 제안 사항은 다음과 같습니다.

- OS 및 OS와 함께 설치된 서비스에 중요한 보안 패치를 모두 적용합니다. 사용 가능한 모든 업데이트를 적용하면 새로운 기능과 함께 ACSLS 및 ACSLS HA가 테스트되지 않은 새 OS 릴리스도 설치될 수 있으므로 해당 패치는 선별적으로 적용하십시오.
- telnet 및 rlogin이 설치되지 않았거나 사용 안함으로 설정되었는지 확인합니다. 대신 ssh를 사용하십시오.

또한 ftp가 설치되지 않았거나 사용 안함으로 설정되었는지 확인하고 대신 sftp를 사용하십시오.

모든 서비스를 보려면 root로 로그인하고 다음을 수행합니다.

```
service –-status-all
```

- 서비스를 영구적으로 삭제하려면 다음을 사용합니다.

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

- ssh를 사용 안함으로 설정하지 마십시오. 사용자는 telnet/rlogin이 아닌 ssh를 사용하여 ACSLS에 원격으로 로그인하게 됩니다. 또한 sftp를 사용 안함으로 설정하지 마십시오.
- ACSLS 클라이언트 통신을 허용하려면 네트워크 서비스, 특히 rpcbind를 사용으로 설정해야 합니다.

  Linux에서 rpc를 실행할 때 –i 플래그와 함께 실행합니다.
- ACSLS와 통신을 위해 ACSLS 서버의 일부 이더넷 포트를 열어야 합니다. 클라이언트 응용 프로그램은 ACSLS와 통신을 위해 특정 이더넷 포트를 사용하며, ACSLS는 테이프 라이브러리의 특정 포트와 통신합니다. ACSLS 통신에 사용할 수 있는 포트는 ACSLS 통신에 사용되는 이더넷 포트를 참조하십시오. ACSLS 서버에서 ACSLS에 사용되는 포트에 트래픽을 허용하도록 iptables가 구성되었는지 확인합니다.

Linux 보안 감사

Linux 감사 정책을 결정합니다. *Oracle Linux: Security Guide for Release 6*의 "Configuring and Using Auditing" 절을 참조하여 감사할 이벤트 종류, 감사 로그를 저장할 위치, 이들의 검토 방법을 계획할 수 있습니다.

Linux 보안 감사에 유용한 몇 가지 로그 및 명령은 다음과 같습니다.

- var/log/secure를 root로 실행하여 로그인 시도 내역 및 기타 액세스 메시지를 봅니다.
- 'last | more' 명령은 로그인한 사용자 내역을 제공합니다.
- /var/log/audit/audit.log.[0-9]는 SE Linux에서 거부된 액세스 시도 로그를 보관합니다. 이들을 보려면 root 사용자여야 합니다.

SELinux 보안

ACSLS 8.4은 선택적 Security Enhanced Linux 환경에서 실행하도록 설계되었습니다. SELinux는 Unix 환경에서 전통적인 보호 표준을 넘어서 파일, 디렉토리 및 기타 시스템 리소스에 대한 액세스 제어를 제공합니다. owner-group-public 권한 액세스 외에도 SELinux는 사용자 역할, 도메인, 컨텍스트에 따라 액세스 제어를 제공합니다. 모든 시스템 리소스에 대한 액세스 제어를 시행하는 에이전트는 Linux 커널입니다.

Linux 시스템의 root 사용자는 `setenforce` 명령으로 시행을 설정하거나 해제할 수 있습니다.

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

Enforcing 또는 1은 SELinux를 강제 모드에 넣습니다. *Permissive* 또는 0은 SELinux를 허가 모드에 넣습니다.

현재 시스템 시행 상태를 보려면 *getenforce* 명령을 사용합니다.

ACSLS를 설치할 때 세 가지 SELinux 정책 모듈 allowPostgr, acsdb, acsdb1이 커널에 로드됩니다. 이러한 모듈은 SELinux 시행이 활성인 동안 ACSLS가 고유의 데이터베이스 및 기타 시스템 리소스에 액세스하는 데 필요한 정의 및 시행 예외사항을 제공합니다. 이러한 모듈이 설치된 상태에서 SELinux 시행을 사용 안함으로 설정할 필요 없이 bdb.acsss, rdb.acsss, db_export.sh, db_import.sh와 같은 데이터베이스 작업을 포함한 일반적인 ACSLS 작업을 실행할 수 있어야 합니다.

자세한 내용은 *StorageTek ACSLS 8.4 Administrator's Guide*의 부록 "Troubleshooting"의 SELinux 절을 참조하십시오.

ACSLS 설치 및 구성

이 절에서는 ACSLS를 안전하게 설치하는 방법을 설명합니다.

표준 ACSLS 설치 수행

표준 ACSLS 설치를 수행하면 모든 필요한 구성 요소를 갖추게 됩니다.

이전 ACSLS 릴리스에서 이후 ACSLS 릴리스로 마이그레이션하는 경우 더 많은 보안 옵션, 특히 방화벽 보안 옵션을 사용하려면 동적/정적 변수에 대한 설정을 검토합니다.

ACSLS 사용자 ID에 대한 강력한 암호 사용

ACSLS에는 ACSLS 사용자 ID로 acsss, acssa, acsdb가 필요합니다. 이러한 ID에 대한 강력한 암호를 선택하고 정기적으로 암호를 변경합니다.

ACSLS 파일에 대한 액세스 제한

ACSLS는 일반적으로 ACSLS 파일에 대한 액세스를 acsss, acssa, acsdb, root 사용자 ID가 포함된 acsls 그룹으로만 제한합니다. 일부 데이터베이스 및 진단 파일은 단일 acsls 사용자 ID만 액세스할 수 있습니다. ACSLS는 umask 설정 027로 실행됩니다.

ACSLS 파일은 누구나 읽거나 쓰기 가능하도록 만들면 안됩니다. 그러나 설치 기본값 이상으로 액세스를 제한하면 ACSLS 작동이 실패할 수 있습니다.

세 개의 ACSLS 파일에 대한 유효한 사용자 ID로 'root' 설정

설치 스크립트에서는 /export/home/ACSSS 파일 시스템에 있는 세 개의 실행 파일에서 유효한 사용자 ID로 'root'를 설정할 것(setuid)을 고객에게 권고합니다.

- *acsss* (이 바이너리는 ACSLS 응용 프로그램에서 필요한 시스템 서비스를 시작/중지하는 데 사용되므로 'root' 권한으로 실행되어야 합니다.)

- *db_command* (이 바이너리는 ACSLS 데이터베이스를 제어하고 유지 관리하는 PostgreSQL 데이터베이스 엔진을 시작/중지합니다.)
- *get_diags* (이 바이너리는 고객이 서비스 지원 통화 시 필요한 종합적인 시스템 진단 정보를 수집하기 위해 호출됩니다.)

pkgadd로 ACSLS를 설치하는 동안 고객에게 *Do you want to install these as setuid/setgid files?*라는 프롬프트가 나타납니다. 프롬프트에 *y*로 답하면 유틸리티에서 root 권한이 필요한 특정 시스템 작업을 수행하더라도 이러한 세 가지 명령을 acsls 그룹의 사용자가 실행할 수 있게 됩니다.

ACSLS 정적/동적 변수에 대한 설정 검토

ACSLS 정적/동적 변수는 많은 ACSLS 함수의 동작을 제어합니다. *acsss_config* 유틸리티를 사용하여 이러한 변수를 설정합니다. 이러한 변수에 대한 보안 설정은 이 문서에서 설명합니다. 변수의 옵션이 *acsss_config*로 제시된 경우 물음표(?)로 답하면 변수에 대한 상세한 설명이 표시됩니다. 이 정보는 *ACSLS Administrator's Guide*의 "Setting Variables that Control ACSLS Behavior" 장에서도 제공됩니다.

WebLogic 구성

ACSLS 8.1 이상 릴리스는 웹 서버로 WebLogic을 사용합니다. WebLogic은 ACSLS와 함께 설치됩니다.

WebLogic Server 보안 옵션과 WebLogic 감사 추적 가능성은 *Oracle Fusion Middleware; Understanding Security for Oracle WebLogic Server 11g Release 1 (10.3.6)*을 참조하십시오.

ACSLS userAdmin.sh 유틸리티를 사용하여 ACSLS GUI 사용자 만들기/유지 관리

userAdmin.sh 메뉴 방식 유틸리티는 ACSLS GUI 사용자 암호를 관리하는 데 사용됩니다. 사용자 추가, 사용자 제거, 사용자 나열, 사용자 암호 변경을 수행할 수 있습니다. 이 유틸리티를 사용하려면 WebLogic이 실행 중이어야 합니다. 작동 중이 아닌 경우 이 유틸리티가 WebLogic을 시작하고 메뉴를 표시하기 전에 온라인인지 확인합니다.

userAdmin.sh 유틸리티는 root로 실행되어야 하고 acsls_admin 인증이 필요합니다. acsls_admin 사용자 계정은 ACSLS 설치 중 구성됩니다.

ACSLS GUI 사용

ACSLS GUI를 사용하려면 최신 JRE 버전을 설치하고 브라우저를 통해 ACSLS GUI에 액세스해야 합니다.

GUI 클라이언트 시스템에 최신 JRE 버전 설치

ACSLS GUI를 사용하여 ACSLS에 액세스할 시스템에 최신 버전의 JRE(Java Runtime Environment)가 설치되었는지 확인합니다.

ACSLS GUI 액세스

브라우저를 열고 다음 형식으로 서버 호스트 이름 또는 IP 주소가 포함된 URL을 입력합니다.

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

호스트 시스템의 전체 호스트 이름 또는 IP 주소를 사용하는 것이 가장 좋습니다. WebLogic에서 URL을 완전히 분석할 수 없는 경우 ACSLS 도움말 페이지를 포함한 일부 페이지가 제대로 표시되지 않을 수 있습니다.

http와 7001 포트를 사용하는 경우 WebLogic이 자동으로 https와 7002 포트에 다시 경로를 지정합니다.

WebLogic이 보안 https 프로토콜을 사용하기 때문에 브라우저에 사이트 보안 인증서가 등록되지 않았으므로 신뢰할 수 없다는 경고가 나타날 수 있습니다. URL이 로컬 ACSLS 시스템이라고 확신하면 계속 진행해도 안전합니다. 이 시점에 로그인 화면이 표시됩니다.

ACSLS GUI 사용

WebLogic의 AcslsDomain에 액세스하려면 보안 프로토콜(https)을 사용하십시오. 이 프로토콜은 개인 키 및 디지털 인증서를 사용하여 브라우저와 서버 간에 암호화된 통신을 사용합니다. 다음 방법으로 디지털 인증서를 얻을 수 있습니다.

ACSLS 데모 인증서

ACSLS는 '데모'라는 인증서를 제공합니다. 고객이 추가 구성 단계를 수행하지 않고도 ACSLS GUI를 사용할 수 있도록 최소 레벨의 암호화 보안이 제공됩니다. ACSLS 라이브러리와의 고객 상호 작용이 보안 인트라넷 내에서만 이루어지는 경우 일반적으로 이 데모 인증서 방법이면 충분합니다. 하지만 이 방법은 특정 브라우저, 특히 Internet Explorer 및 FireFox 버전 39 이상에서 지원되지 않는 512비트 암호화 키를 사용합니다.

자체 서명된 디지털 인증서 구성

ACSLS Installation Guide에서 2048비트 길이의 자체 서명된 디지털 인증서를 구성하려는 ACSLS 관리자를 대상으로 단계별 방법을 제공합니다. 'Configuring an SSL Encryption Key' 절에서 이 방법은 모든 브라우저에서 지원되는 인증서를 제공합니다. 자체 서명된 인증서를 사용하여 https 사이트에 액세스하는 사용자는 웹 리소스가 신뢰할 수 있는 사이트임을 확신할 수 없는 경우 사이트에서 작업을 계속하지 않는 것이 좋습니다. ACSLS 사용자 및 라이브러리 컨트롤 서버 컨텍스트에서 일반적으로 이 신뢰 레벨은 잘 알려져 있으며, 대부분의 경우 사이트에서 타사 서명 확인을 통해 무결성을 증명할 필요가 없습니다.

타사 서명 기관에서 서명한 디지털 인증서

타사 서명 기관(예: Verisign 또는 Entrust.net)에 의한 인증서 인증을 제공해야 할지 여부는 각 고객 사이트에서 결정하는 것입니다. 서명된 디지털 인증서 등의 생성 절차는 Oracle 온라인 문서 Configuring Identity and Trust on에서 설명됩니다.

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

ACSLS HA 설치

ACSLS 고가용성 솔루션을 사용하는 경우 ACSLS-HA Cluster: Installation, Configuration, and Operations의 지침을 따르십시오.

3

보안 기능

이 절에서는 ACSLS에서 제공하는 구체적인 보안 메커니즘을 설명합니다.

보안 모델

ACSLS 보안 요구 사항은 첫째 우발적 손실 및 손상으로부터 데이터를 보호하고, 둘째 허용되지 않은 고의적인 데이터 액세스나 개조 시도로부터 데이터를 보호할 필요성에서 기인합니다. 부수적 고려 사항은 데이터 액세스나 사용 시 과도한 지연으로부터 보호하거나, 서비스 거부라고 생각될 정도의 간섭으로부터 보호하는 것입니다.

이러한 보호를 제공하는 중요 보안 기능은 다음과 같습니다.

- 인증 – 권한이 부여된 개인만 시스템 및 데이터에 액세스할 수 있도록 합니다.
- 권한 부여 – 시스템 권한 및 데이터에 대한 액세스 제어를 제공합니다. 이것은 개인이 적절한 액세스 권한을 얻도록 하는 인증에 기초합니다.
- 감사 – 관리자가 인증 메커니즘 침해 시도와 액세스 제어 침해 시도나 성공을 감지할 수 있습니다.

인증 구성 및 사용

기본적으로 Linux 또는 Solaris에서 ACSLS 사용자는 PAM(플러그 가능한 인증 모듈)을 통해 인증됩니다. Solaris 매뉴얼 페이지 또는 *Linux-PAM System Administrators Guide*를 참조하십시오.

ACSLS GUI 사용자는 WebLogic의 포함된 LDAP 서버를 통해 인증됩니다. Managing the Embedded LDAP Server 문서를 참조하십시오.

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

Solaris 또는 Linux 운영체제에서 ACSLS 사용자 인증

ACSLS 사용자 acsss 및 acssa는 Solaris 또는 Linux에 로그인하여 운영체제에 의해 인증되어야 cmd_proc를 사용할 수 있으며, acsss 사용자의 경우 ACSLS 유틸리티 및 구성 명령을 실행할 수 있습니다. acsdb 사용자 ID는 데이터베이스 관련 작업에도 사용됩니다. ACSLS 설치 프로세스의 일부로 고객은 처음 로그인할 때 이러한 ID에 대한 암호를 설정해야 합니다. 자세한 내용은 *ACSLS Installation Guide*를 참조하십시오.

WebLogic에서 ACSLS GUI 사용자 인증

ACSLS GUI 사용자는 WebLogic에 로그인하여 인증되어야 합니다. ACSLS 설치 중 acsls_admin이 만들어지고 고객이 암호를 설정해야 합니다. 고객은 *`userAdmin.sh`* 유틸리티

를 사용하여 원하는 대로 다른 GUI 사용자를 추가할 수 있습니다. 자세한 내용은 *ACSLS Installation Guide* 및 *ACSLS Administrator's Guide*의 "Utilities" 장, `userAdmin.sh` 절을 참조하십시오.

감사 고려 사항

ACSLS에 적용되는 일반적인 감사 고려 사항이 여기에 설명됩니다.

감사 정보를 관리 가능하도록 유지

감사는 비교적 비용이 저렴하지만 가능한 한 감사되는 이벤트 수를 제한합니다. 이렇게 하면 감사되는 명령문 실행과 감사 추적 크기에 미치는 성능 영향이 최소화되므로 더 쉽게 분석, 이해, 관리할 수 있습니다.

감사 전략을 세울 때 다음과 같은 일반적 지침을 사용하십시오.

감사 목적 평가

감사 이유를 명확히 이해한 후에 적절한 감사 전략을 세우면 불필요한 감사를 피할 수 있습니다.

지능적으로 감사

목표한 정보를 얻는 데 필요한 최소한의 명령문, 사용자, 객체를 감사합니다.

ACSLS 감사 로그 구성 및 사용

ACSLS에는 ACSLS 작동을 기록하고 점검할 수 있는 여러 가지 로그 정보가 있습니다.

- 대부분 vi 및 기타 편집기를 사용하여 볼 수 있습니다. 시스템 이벤트는 ACSLS GUI에서만 볼 수 있습니다.
- 이러한 로그의 대부분은 고객이 정의한 크기에 도달할 때 자동으로 아카이브할 수 있으며, 고객이 지정한 로그 개수가 보존됩니다. ACSLS 파일 시스템이 가득 차지 않도록 보존할 로그 개수에 대한 제한을 구성할 수 있습니다. 이러한 로그 파일을 더 많이 보존하거나 다른 시스템에 보존하려면 자체 절차를 개발하여 충분한 공간이 있는 위치에 아카이브해야 합니다.
- 아카이브된 로그의 크기, 보존할 개수와 이러한 파일의 기타 특성은 ACSLS 동적/정적 변수로 정의할 수 있습니다.

ACSLS 로그 디렉토리

ACSLS 로그 디렉토리는 LOG_PATH 정적 변수로 제어할 수 있습니다. 기본값은 $ACS_HOME/log 디렉토리입니다. 이 디렉토리는 다음 로그를 포함합니다.

acsss_event.log
중요한 ACSLS 시스템 이벤트, 라이브러리 이벤트 및 오류에 관한 메시지를 기록합니다.

acsss_event.log는 LOG_SIZE 동적 변수로 정의된 임계값 크기에 도달할 때 event0.log로 복사된 후 지워집니다. 복사 프로세스 동안 보존된 이벤트 로그는 더 높은 숫자의 보존된 로그로 복사되고 가장 높은 숫자의 보존된 로그가 포개집니다. 예를 들어, event8.log가 event9.log로 복사되고, event7.log가 event8.log로 복사되고, …, event0.log가 event1.log로 복사되고, acsss_event.log가 event0.log로 복사되고, acsss_event.log가 지워집니다. 다음 변수로 제어할 수 있습니다.

- *EVENT_FILE_NUMBER*는 보존할 이벤트 로그의 개수를 지정합니다.
- *LOG_SIZE*는 이벤트 로그가 보존된 이벤트 로그로 복사되고 잘리는 지점의 임계값 크기를 지정합니다.

`greplog` 유틸리티를 사용하여 특정 키워드가 포함된 메시지를 포함하거나 제외하도록 acsss_event 로그를 필터링할 수 있습니다. 자세한 내용은 *ACSLS Administrator's Guide*의 "Utilities" 장, greplog 절을 참조하십시오.

구성 로그

ACSLS가 ACSLS 데이터베이스에 저장된 라이브러리 구성을 업데이트할 때 세부정보를 기록하는 두 개의 로그가 있습니다. `acsss_config` 및 `Dynamic Config`(`config` 유틸리티)의 구성 변경 사항이 여기에 기록됩니다.

acsss_config.log
ACSLS가 지원하는 라이브러리의 모든 구성이나 재구성 세부정보를 기록합니다. 마지막 구성 변경은 이전 구성 레코드에 첨부됩니다.

acsss_config_event.log
구성이나 재구성 프로세스 동안 이벤트를 기록합니다.

rpTrail.log

ACSAPI 클라이언트나 cmd_proc에서 ACSLS로 향하는 모든 요청에 대한 응답을 기록하고, GUI 또는 SCSI 클라이언트 인터페이스에서 데이터베이스 질의를 제외한 논리적 라이브러리로 향하는 모든 요청을 기록합니다. 기록된 정보에는 요청자, 요청 내용, 요청 시간 기록이 포함됩니다.

다음 변수로 rpTrail.log가 관리됩니다.

- *LM_RP_TRAIL*은 ACSLS 이벤트 감사 추적을 사용으로 설정합니다. 기본값은 TRUE입니다.
- *RP_TRAIL_LOG_SIZE*는 rpTrail.log가 압축되고 아카이브되는 지점의 임계값 크기를 지정합니다.
- *RP_TRAIL_FILE_NUM*은 아카이브된 rpTrail 로그의 보존할 개수를 지정합니다.
- *RP_TRAIL_DIAG*는 rpTrail 메시지에 추가 진단 정보를 포함해야 하는지 여부를 지정합니다. 기본값은 FALSE입니다.

라이브러리 볼륨 통계

테이프 라이브러리에서 볼륨(카트리지)을 마운트/마운트 해제하고 이동하고 넣고 꺼내거나 감사나 카트리지 복구로 볼륨을 찾을 때 볼륨에 영향을 주는 모든 이벤트를 기록합니다. 라이브러리 볼륨 통계가 사용으로 설정된 경우 이 정보는 acsss_stats.log에 기록됩니다.

다음 변수로 라이브러리 볼륨 통계가 관리됩니다.

- *LIB_VOL_STATS*는 이 라이브러리 볼륨 통계를 사용으로 설정합니다. 기본값은 OFF입니다.
- *VOL_STATS_FILE_NUM*은 아카이브된 acsss_stats.log 파일의 보존할 개수를 지정합니다.
- *VOL_STATS_FILE_SIZE*는 acsss_stats.log가 아카이브되는 지점의 임계값 크기를 지정합니다.

ACSLS 로그/sslm 디렉토리

ACSLS 로그 디렉토리 내에서, ACSLS GUI 및 SCSI 클라이언트 인터페이스의 논리적 라이브러리에 관한 정보는 sslm 디렉토리에 기록됩니다. 이 디렉토리는 WebLogic 감사 로그에 대한 링크를 포함합니다. sslm 디렉토리는 다음 로그를 포함합니다.

slim_event.g#.log[.pp#]
ACSLS GUI 및 SCSI 클라이언트 인터페이스의 이벤트를 기록합니다. 논리적 라이브러리 구성 변경 메시지와 SCSI 클라이언트 이벤트가 포함됩니다.

- .g#은 이 로그의 세대 번호입니다.
- .pp#은 이 로그의 병렬 프로세스 번호입니다. 여러 프로세스가 동시에 기록되는 경우 추가 프로세스 로그에 병렬 프로세스 번호가 지정됩니다.

smce_trace.log
SCSI 매체 교환기 인터페이스 에뮬레이션을 사용하여 SCSI 클라이언트에서 ACSLS 논리적 라이브러리로 향하는 작동을 추적합니다.

guiAccess.log
WebLogic의 access.log에 대한 링크입니다. WebLogic 감사 로그 구성 및 사용을 참조하십시오.

AcslsDomain.log
WebLogic의 AcslsDomain.log에 대한 링크입니다. WebLogic 감사 로그 구성 및 사용을 참조하십시오.

AdminServer.log
WebLogic의 AdminServer.log에 대한 링크입니다. WebLogic 감사 로그 구성 및 사용을 참조하십시오.

GUI 로그 뷰어에서 ACSLS 감사 추적 보기

GUI 탐색 트리의 Configuration and Administration 섹션에서 Log Viewer에 액세스합니다. 로그 뷰어는 ???TITLE???와 ???TITLE???에서 결합한 정보를 표시합니다.

GUI에서 시스템 이벤트 보기

GUI 탐색 트리의 Configuration and Administration 섹션에서 System Events도 볼 수 있습니다. 모든 개별 라이브러리 작업이 시스템 이벤트 로그에 기록됩니다. 이 로그의 각 레코드에는 이벤트 시간 기록, 이벤트 유형, 이벤트 설명이 포함됩니다.

Solaris 감사 로그 구성 및 사용

Solaris 감사 정책을 결정합니다. *Oracle Solaris Administration: Security Services* 매뉴얼의 Oracle Solaris Auditing 절을 참조하여 감사할 이벤트 종류, 감사 로그를 저장할 위치, 이들의 검토 방법을 계획할 수 있습니다.

사용자 정의 Solaris 감사 추적이 사용으로 설정되지 않은 경우 다음과 같은 로그인 감사 추적과 acsss, acsdb, acssa 사용자가 실행한 Unix 명령을 사용할 수 있습니다.

- 현재 Unix에 사인온한 사용자는 Unix utmpx에 기록되고 과거 사용자 액세스는 wtmpx 데이터베이스에 기록됩니다.
- `last` 명령을 사용하여 사용자 ID에 대한 모든 액세스를 봅니다(예: `last acsss`). 자세한 내용은 wtmpx, `last`, getutxent 매뉴얼 페이지를 참조하십시오.
- 사용자 홈 디렉토리에 있는 .*_history([dot]*_history) 파일은 해당 사용자가 실행한 명령을 기록합니다.

  acsss 사용자의 경우 다음이 포함됩니다.
  - .bash_history
  - .psql_history
  - .sh_history

  Solaris에서 /var/adm/sulog는 *su*를 실행하여 수퍼 유저나 다른 사용자가 되려는 시도의 성공 및 실패를 기록합니다.

Linux 감사 로그 구성 및 사용

감사 및 시스템 로그 수집과 분석에 대한 자세한 내용은 *Oracle Linux: Security Guide for Release 6*의 Configuring and Using Auditing 및 Configuring and Using System Logging 절을 참조하십시오.

WebLogic 감사 로그 구성 및 사용

WebLogic Server 보안 옵션과 WebLogic 감사 추적 가능성은 *Oracle Fusion Middleware; Understanding Security for Oracle WebLogic Server 11g Release 1 (10.3.6)*을 참조하십시오.

WebLogic은 다음 디렉토리에 ACSLS GUI 액세스 정보를 기록합니다.

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

이 디렉토리는 다음 파일을 포함합니다.

- access.log
  - access.log#####(예: access.log00001)이라는 아카이브된 버전이 있습니다.
  - GUI 사용자 활동에 대한 상세한 감사 추적을 제공합니다.
  - 로그인 정보는 "AcslsLoginForm"을 확인하십시오.

주:

$ACS_HOME/logs/sslm/guiAccess.log에 액세스 로그에 대한 링크가 있습니다.

- AcslsDomain.log
  - WebLogic 및 ACSLS GUI 작업을 보고합니다.

주:

$ACS_HOME/logs/sslm/AcslsDomain.log에 액세스 로그에 대한 링크가 있습니다.

- AdminServer.log
  - WebLogic 및 ACSLS GUI 작업을 보고합니다.

주:

$ACS_HOME/logs/sslm/AdminServer.log에 액세스 로그에 대한 링크가 있습니다.

4

개발자용 보안 고려 사항

이 절에서는 Oracle StorageTek Tape Library를 관리하기 위해 ACSLS를 사용하는 응용 프로그램을 개발하거나 지원하는 개발자에게 유용한 정보를 제공합니다.

클라이언트 응용 프로그램의 서버에서 방화벽 보안 사용으로 설정

방화벽 보안을 사용으로 설정하여 통신에 사용되는 포트를 제한하고 클라이언트의 애플리케이션 서버에서 portmapper를 사용 안함으로 설정합니다. *CSC Developer's Toolkit User's Guide*의 "Appendix B: Firewall-Secure Operation"을 참조하십시오.

부록 A

보안 배치 점검 목록

1. 암호 관리를 적용합니다.
2. 네트워크 액세스를 제한합니다.
   a. ACSLS와 관리되는 테이프 라이브러리를 회사 방화벽 뒤에 두어야 합니다.
   b. ACSLS 방화벽 보안 옵션을 사용으로 설정합니다.
   c. ACSLS 클라이언트 응용 프로그램에 대해 방화벽 보안을 사용으로 설정하는 것이 좋습니다.
3. Solaris 또는 Linux 운영체제를 강화합니다.
4. 모든 보안 패치 및 임시해결책을 적용합니다.
5. StorageTek ACSLS에서 취약점이 발견되면 Oracle 서비스, Oracle 테이프 라이브러리 엔지니어링 또는 계정 담당자에게 문의합니다.

부록 B

참조

ACSLS 설명서
ACSLS 설명서는 ACSLS 릴리스로 구성된 라이브러리에 저장됩니다. Tape Storage Documentation 페이지에서 액세스할 수 있습니다.

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

(개별 ACSLS 설명서 라이브러리의 URL에는 버전 번호가 포함됩니다. 따라서 특정 라이브러리에 대한 링크는 라이브러리가 업데이트되자마자 쓸모없게 됩니다.) ACSLS 설명서는 다음과 같습니다.

- *ACSLS Installation Guide*
- *ACSLS Administrator's Guide*
- *ACSLS* 제품 정보

  소프트웨어 및 하드웨어 요구 사항, ACSLS 개요와 함께 지원되는 테이프 라이브러리, 테이프 드라이브 및 매체를 다룹니다.
- ACSLS Messages (및 상태 코드)
- *ACSLS Release Notes*
- *ACSLS-HA Cluster: Installation, Configuration, and Operations*
- *ACSLS Interface Reference Manual*

Oracle Solaris
Oracle Solaris 11.2 정보 라이브러리에 *Securing the Oracle Solaris 11 Operating System*이 있습니다. 자세한 내용은 본문을 참조하십시오.

Oracle Linux
Oracle Linux 6 정보 라이브러리에 *Oracle Linux 6 Security Guide*가 있습니다. 자세한 내용은 본문을 참조하십시오.

Oracle WebLogic
Oracle WebLogic Server 설명서 라이브러리에 WebLogic 10.3.6용(ACSLS 8.2에서 사용됨) Security 절이 있습니다.

*Oracle Fusion Middleware; Understanding Security for Oracle WebLogic Server 11g Release 1 (10.3.6)*에서는 WebLogic Server 보안에 대해 자세히 설명합니다.