# Oracle® Solaris 11 보안 지침

부품 번호: E53930-02
2014년 8월

ORACLE

# 목차

# 표

# 이 설명서 사용

- **개요** - Oracle Solaris 보안 기능에 대한 개요를 제공하고 이러한 기능을 사용하여 설치된 시스템 및 해당 응용 프로그램을 강화 및 보호하는 방법에 대한 개요
- **대상** - Oracle Solaris 11 시스템의 보안을 개발, 배치 또는 평가하는 시스템 관리자, 보안 관리자, 응용 프로그램 개발자 및 감사자
- **필요한 지식** - 사이트 보안 요구 사항

## 제품 설명서 라이브러리

이 제품에 대한 최신 정보 및 알려진 문제는 설명서 라이브러리(http://www.oracle.com/pls/topic/lookup?ctx=E56343)에서 확인할 수 있습니다.

## Oracle 지원 액세스

Oracle 고객은 My Oracle Support를 통해 온라인 지원에 액세스할 수 있습니다. 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.

## 피드백

http://www.oracle.com/goto/docfeedback에서 이 설명서에 대한 피드백을 보낼 수 있습니다.

♦ ♦ ♦ 1 장

# 1 Oracle Solaris 보안 정보

Oracle Solaris는 입증된 보안 기능을 제공하는 강력한 엔터프라이즈 운영 체제입니다. 사용자의 파일 액세스, 시스템 데이터베이스 보호, 시스템 리소스 사용 방법을 제어하는 정교한 네트워크 차원의 보안 시스템인 Oracle Solaris 11은 모든 계층에서 보안 요구를 처리합니다. 기존의 운영 체제가 고유의 보안 취약점을 내재한 반면, Oracle Solaris 11의 융통성을 사용으로 설정하면 엔터프라이즈 서버에서 데스크탑 클라이언트에 이르는 다양한 보안 목표를 만족시킬 수 있습니다. Oracle Solaris는 Oracle의 다양한 SPARC 및 x86 기반 시스템 및 타사 공급업체의 다른 하드웨어 플랫폼에서 완전히 테스트되었으며 지원됩니다.



## Oracle Solaris 11.2의 새로운 보안 기능

이 절에서는 기존 고객을 위해 이 릴리스의 새로운 중요 보안 기능에 대한 정보를 강조합니다.

- 새 `compliance` 명령으로 보안 표준에 대한 시스템의 준수 여부를 평가할 수 있습니다. 이렇게 설정하면 PCI-DSS를 포함한 업계 표준 보안 벤치마크에 대한 시스템의 준수 여부를 평가 및 보고할 수 있습니다. 자세한 내용은 “Oracle Solaris 11.2 보안 적합성 안내서 ” 및 `compliance`(1M) 매뉴얼 페이지를 참조하십시오.
- Oracle Solaris의 암호화 프레임워크 기능은 Oracle Solaris 11.1 SRU 5.5 및 Oracle Solaris 11.1 SRU 3 릴리스에서 userland 및 커널 기능에 대해 FIPS 140-2, 레벨 1에서 검증되었습니다.

  - Oracle FIPS 140 검증 제품 목록은 Oracle FIPS 140 Software Validations (http://www.oracle.com/technetwork/topics/security/fips140-software-validations-1703049.html)를 참조하십시오.
  - 시스템에서 FIPS 140 모드를 사용으로 설정하는 방법은 "Using a FIPS 140 Enabled System in Oracle Solaris 11.2 "을 참조하십시오.
- Oracle Solaris 11.1은 Canadian Common Criteria Scheme에 따라 인증되었습니다. "Oracle Solaris 11 Common Criteria EAL4+ Certification" [26]을 참조하십시오.
- 감사 서비스에서는 Oracle 감사 보관소를 사용하여 감사 레코드를 저장, 검토 및 분석합니다. "Oracle Solaris 11.2의 감사 관리 "의 "감사 레코드의 저장 및 분석을 위한 Oracle Audit Vault and Database Firewall 사용"을 참조하십시오.
- 확인된 부트는 Oracle SPARC T5 시리즈 서버 및 Oracle SPARC T7 시리즈 서버에 대한 위협으로부터 부트 프로세스를 보호합니다. 자세한 내용은 "Oracle Solaris 11.2에서 시스템 및 연결된 장치의 보안 "의 "확인된 부트 사용"을 참조하십시오.
- 인증서와 키를 사용하여 설치 서버, 지정한 클라이언트 시스템, 지정한 설치 서비스의 모든 클라이언트 및 기타 모든 AI 클라이언트에 대한 AI(자동 설치)를 보호할 수 있습니다. AI 보호는 사용자의 시스템에 대한 Oracle Solaris 패키지의 전송을 보호하는 것입니다. "Oracle Solaris 11.2 시스템 설치 "의 "자동 설치의 보안 수준 향상"을 참조하십시오.
- 새 그룹 설치 패키지 `pkg:/group/system/solaris-minimal-server`를 사용할 수 있습니다. 그룹 패키지 내용에 대한 설명 및 비교는 "Oracle Solaris 11.2 Package Group Lists "을 참조하십시오.
- AI를 사용하여 Kerberos 클라이언트를 설치하면 클라이언트가 처음 부트 시 Kerberios 화된 시스템이 됩니다. "Oracle Solaris 11.2 시스템 설치 "의 "AI를 사용한 Kerberos 클라이언트 구성 방법"을 참조하십시오.
- 이 릴리스에서는 물리적 글로벌 영역(변경할 수 없는 글로벌 영역) 및 가상 글로벌 영역(Oracle Solaris Kernel 영역)을 읽기 전용으로 설정할 수 있습니다. 변경할 수 없는 글로벌 영역은 Kernel 영역에 비해 약간 더 강력하지만 두 영역 모두 시스템의 하드웨어 또는 구성을 영구적으로 변경할 수는 없습니다. 읽기 전용 영역은 쓰기 가능 영역에 비해 부트 속도와 보안성이 더 뛰어납니다.

  유지 관리를 위해 변경할 수 없는 글로벌 영역은 TCB(Trusted Computing Base)라는 특별한 프로세스 세트를 정의합니다. TCB는 신뢰할 수 있는 경로라는 보호된 로그인을 통해 구성할 수 있습니다. 자세한 내용은 "Oracle Solaris 영역 만들기 및 사용 "의 12 장, "변경할 수 없는 영역 구성 및 관리"를 참조하십시오. 영역 구성 리소스에 대한 자세한 내용은 "Oracle Solaris 영역 소개 "를 참조하십시오. `mwac`(5) 및 `tpd`(5) 매뉴얼 페이지를 참조하십시오.

  Oracle Solaris 커널 영역은 호환 시스템 배치 시 유용합니다. 예를 들어 호환 시스템을 구성하고 통합 아카이브를 만든 다음 이미지를 커널 영역으로 배치할 수 있습니다. 자세한 내용은 `solaris-kz`(5) 매뉴얼 페이지, "Oracle Solaris 커널 영역 만들기 및 사용 ", "Oracle Solaris 11.2 가상화 환경 소개 "의 "Oracle Solaris 영역 개요" 및 "Oracle Solaris 11.2의 시스템 복구 및 복제용 Unified Archive 사용 "을 참조하십시오.
- 사용자 및 프로세스 권한의 새로운 기능은 다음과 같습니다.
  - PAM 서비스에 대한 시간 기반/위치 기반의 액세스 제어
  - ARMOR(Authorization Roles Managed on RBAC) 사전 정의 역할

- 권한 작업을 실행하기 전 사용자에게 암호를 요구하는 권한 프로파일
- `root`가 아니어도 권한으로 진단 명령 `ipstat`, `tcpstat`, `snoop`, `intrstat`를 실행하기 위한 네트워크 관찰성 및 시스템 관찰성 권한 프로파일

자세한 내용은 "Oracle Solaris 11.2의 사용자 및 프로세스 보안 "의 "Oracle Solaris 11.2 권한의 새로운 기능"을 참조하십시오.

- IKEv2(IKE 버전 2)에서는 IPsec로 보호된 네트워크 패킷의 자동 키 관리를 위해 최신 IKE 프로토콜을 제공합니다. 자세한 내용은 "Oracle Solaris 11.2의 네트워크 보안 "의 "Oracle Solaris 11.2에서 네트워크 보안의 새로운 기능"을 참조하십시오.
- Oracle HMP(Hardware Management Pack)에서는 펌웨어 구성 및 업데이트를 위한 명령줄 도구를 제공합니다. 네트워크 스위치 및 네트워크 인터페이스 카드 등 다른 Oracle 하드웨어 제품과 안전하게 HMP를 사용하는 방법에 대한 자세한 내용은 "Oracle Solaris용 Oracle Hardware Management Pack 보안 설명서 "를 참조하십시오.

# Oracle Solaris 11 설치 후 보안

Oracle Solaris는 SBD(Secure By Default) 방식으로 설치됩니다. 이 보안 방법은 다른 보안 기능 중에서도 침입으로부터 시스템을 보호하고 로그인 시도를 모니터하는 기능을 제공합니다.

## 시스템 액세스가 제한되고 모니터됨

**초기 사용자 및 `root` 역할 계정** - 초기 사용자 계정은 콘솔에서 로그인할 수 있습니다. 이 계정에는 `root` 역할이 지정됩니다. 설치 시 초기 사용자와 `root` 계정의 암호는 동일합니다.

- 로그인 후에는 초기 사용자가 `root` 역할을 가정하여 추가로 시스템을 구성할 수 있습니다. 역할을 가정한 후에는 사용자에게 `root` 암호를 변경하라는 메시지가 표시됩니다. `root` 역할을 포함하여 아무도 직접 로그인할 수 없습니다.
- 초기 사용자에게는 `/etc/security/policy.conf` 파일에서 기본값이 지정됩니다. 기본값에는 기본 Solaris 사용자 권한 프로파일 및 콘솔 사용자 권한 프로파일이 포함됩니다. 이러한 권한 프로파일을 통해 사용자는 CD 또는 DVD에서 데이터를 읽고 쓰고, 권한 없이 시스템에서 명령을 실행하고, 콘솔에 있는 경우 시스템을 중지하고 다시 시작할 수 있습니다.
- 초기 사용자 계정에는 또한 시스템 관리자 권한 프로파일이 지정됩니다. 따라서 `root` 역할을 가정하지 않아도 초기 사용자에게는 소프트웨어 설치 및 이름 지정 서비스 관리 권한과 같은 일부 관리 권한이 있습니다.

**암호 요구 사항** - 사용자 암호는 길이가 최소 6자 이상이어야 하고 최소한 2자 이상의 영문자와 1자 이상의 영문자가 아닌 문자가 포함되어 있어야 합니다. 암호는 `SHA256` 알고리즘을 사용하여 해싱됩니다. 암호를 변경할 때는 `root` 역할을 포함하여 모든 사용자가 이러한 암호 요구 사항을 준수해야 합니다.

**제한된 네트워크 액세스** - 설치 후 시스템은 네트워크를 통한 침입으로부터 보호됩니다. 초기 사용자의 원격 로그인은 `ssh` 프로토콜을 사용하는 인증되고 암호화된 연결을 통해서 허용됩니다. 이 프로토콜은 수신 패킷을 수락하는 유일한 네트워크 프로토콜입니다. `ssh` 키는 `AES128` 알고리즘으로 래핑됩니다. 사용자는 암호화 및 인증을 사용하여 가로채기, 수정 또는 스푸핑 위험 없이 원격 시스템에 연결할 수 있습니다.

**기록된 로그인 시도** - 감사 서비스는 모든 `login/logout` 이벤트(로그인, 로그아웃, 사용자 전환, `ssh` 세션 시작 및 중지, 화면 잠금) 및 모든 부적합한(실패한) 로그인에 대해 사용으로 설정됩니다. `root` 역할은 로그인할 수 없으므로 `root`로 가정 중인 사용자의 이름이 감사 추적에 기록됩니다. 초기 사용자는 시스템 관리자 권한 프로파일을 통해 부여된 권한에 따라 감사 로그를 검토할 수 있습니다.

## 커널, 파일 및 데스크탑 보호가 배치됨

초기 사용자가 로그인한 다음에는 커널, 파일 시스템, 시스템 파일 및 데스크탑 응용 프로그램이 파일 권한, 권한 및 사용자 권한을 통해 보호됩니다. 사용자 권한은 RBAC(*role-based access control*)라고도 합니다.

**커널 보호** - 여러 데몬 및 관리 명령에는 해당 작업을 수행하는 데 필요한 수준의 권한만 지정됩니다. 여러 데몬은 다른 작업을 수행하는 데 악용될 수 없도록 `root`(`UID=0`) 권한이 없는 특별한 관리 계정으로 실행됩니다. 이러한 특별한 관리 계정은 로그인을 수행할 수 없습니다. 장치는 권한에 따라 보호됩니다.

**파일 시스템** - 기본적으로 모든 파일 시스템은 ZFS 파일 시스템입니다. 사용자의 `umask`는 `022`입니다. 따라서 사용자가 새 파일 또는 디렉토리를 만들면 해당 사용자만 이를 수정할 수 있습니다. 사용자 그룹의 구성원은 디렉토리에 대해 읽기 및 검색, 파일 읽기가 허용됩니다. 사용자 그룹 외부에서 로그인한 경우 디렉토리를 나열하고 파일을 읽을 수 있습니다. 기본 디렉토리 권한은 `drwxr-xr-x`(`755`)입니다. 파일 권한은 `-rw-r--r--`(`644`)입니다.

**시스템 파일** - 시스템 구성 파일은 파일 권한을 통해 보호됩니다. `root` 권한 또는 특정 시스템 파일에 대한 편집 권한이 지정된 사용자만 시스템 파일을 수정할 수 있습니다.

**데스크탑 애플릿** - 데스크탑 애플릿은 권한 관리를 통해 보호됩니다. 그러므로 인쇄 관리자의 원격 프린터 추가와 같은 관리 작업은 인쇄 관리 권한이 있는 사용자 및 역할로 제한됩니다.

## Oracle Hardware Management Package

Oracle Hardware Management Package는 Oracle 서버 구성, 관리 및 모니터링을 위한 유틸리티 세트를 제공합니다. 이 Oracle 하드웨어용 값 추가 도구 세트는 항상 사용할 수 있습니다. 특정 하드웨어 관련 정보를 자동으로 ILOM으로 전달하여 시스템 하드웨어의 보기를 완료할 수 있습니다. 유틸리티 및 보안에 대한 자세한 내용은 Systems Management and Diagnostics Documentation"> (http://www.oracle.com/goto/ohmp/docs)를 참조하십시오.

# Oracle Solaris 구성 가능한 보안

Oracle Solaris 기본 보안이 제공하는 확고한 기반 외에, Oracle Solaris 시스템의 보안 체계를 구성하여 다양한 보안 요구 사항을 만족할 수 있습니다.

다음 섹션에서는 Oracle Solaris의 보안 기능에 대해 간단히 소개합니다. 설명에는 자세한 추가 설명 및 이 설명서의 절차, 이러한 기능을 보여 주는 다른 Oracle Solaris 시스템 관리 설명서에 대한 참조가 포함됩니다.

# 데이터 보호

Oracle Solaris는 설치, 사용 및 아카이브를 통한 부트로부터 데이터를 보호합니다.

## 파일 권한 및 액세스 제어 항목

파일 시스템에서 객체를 보호하기 위한 첫번째 방어선은 모든 파일 시스템 객체에 지정되는 기본 UNIX 권한입니다. UNIX 권한은 객체 소유자, 객체에 지정되는 그룹 및 모든 항목에 대한 고유한 액세스 권한 지정을 지원합니다. 또한 기본 파일 시스템인 ZFS는 각 파일 시스템 객체 또는 그룹에 대한 액세스를 더욱 세부적으로 제어하는 ACL(액세스 제어 목록)을 지원합니다.

자세한 내용은 다음을 참조하십시오.

- 파일 권한에 대한 개요는 "Oracle Solaris 11.2의 파일 보안 및 파일 무결성 확인 "의 "UNIX 사용 권한으로 파일 보호"을 참조하십시오.
- ZFS 파일 보호의 개요 및 예는 "Oracle Solaris 11.2의 ZFS 파일 시스템 관리 "의 7 장, "ACL 및 속성을 사용하여 Oracle Solaris ZFS 파일 보호" 및 매뉴얼 페이지를 참조하십시오.
- ZFS 파일에서의 ACL 설정에 대한 지침은 `chmod`(1) 매뉴얼 페이지를 참조하십시오.

## 암호화 서비스

Oracle Solaris의 암호화 프레임워크 기능 및 Oracle Solaris의 KMF(키 관리 프레임워크) 기능은 암호화 서비스 및 키 관리에 대한 중앙 저장소를 제공합니다. 하드웨어, 소프트웨어 및 일반 사용자는 최적화된 알고리즘을 효과적으로 사용할 수 있습니다. KMF에서는 다양한 PKI(공개 키 기반구조)용 저장소 방식, 관리 유틸리티 및 프로그래밍 인터페이스에 대한 통합 인터페이스를 제공합니다.

암호화 프레임워크는 암호화 요구 사항을 처리하기 위한 알고리즘 및 PKCS #11 라이브러리의 공통 저장소를 제공합니다. PKCS #11 라이브러리는 RSA Security Inc.의 PKCS #11 암

호화 토큰 인터페이스(Cryptoki) 표준에 따라 구현됩니다. 파일 암호화 및 해독 등의 암호화 서비스는 일반 사용자에게 사용이 허용됩니다.

KMF는 중앙에서 관리되는 공개 키 객체(예:X.509 인증서 및 공개/개인 키 쌍)에 대한 도구 및 프로그래밍 인터페이스를 제공합니다. 이러한 객체의 저장 형식은 다양할 수 있습니다. 또한 KMF는 응용 프로그램의 X.509 인증서 사용을 정의하는 정책 관리용 도구를 제공합니다. KMF는 타사 플러그인을 지원합니다.

자세한 내용은 다음을 참조하십시오.

- 선택한 매뉴얼 페이지에는 `cryptoadm`(1M), `encrypt`(1), `mac`(1), `pktool`(1) 및 `kmfcfg`(1)가 포함됩니다.
- 암호화 서비스의 개요는 "Oracle Solaris 11.2의 암호화 및 인증서 관리 "의 1 장, "암호화 프레임워크" 및 "Oracle Solaris 11.2의 암호화 및 인증서 관리 "의 4 장, "키 관리 프레임워크"을 참조하십시오.
- 암호화 프레임워크 사용의 예는 "Oracle Solaris 11.2의 암호화 및 인증서 관리 "의 3 장, "암호화 프레임워크" 및 매뉴얼 페이지를 참조하십시오.
- 암호화 프레임워크 FIPS 140 공급자를 사용으로 설정하려면 "Oracle Solaris 11.2의 암호화 및 인증서 관리 "의 "FIPS 140이 사용으로 설정된 부트 환경을 만드는 방법"을 참조하십시오.

## Oracle Solaris ZFS 파일 시스템

ZFS는 Oracle Solaris 11의 기본 파일 시스템입니다. ZFS 파일 시스템은 기본적으로 Oracle Solaris 파일 시스템의 관리 방식을 변경합니다. ZFS는 강력하고, 확장 가능하며, 관리하기도 쉽습니다. ZFS에서는 파일 시스템 만들기가 간단하므로 할당량 및 예약된 공간을 쉽게 설정할 수 있습니다. UNIX 권한 및 ACL은 파일을 보호하며 만들 때 전체 데이터 세트를 암호화할 수 있습니다. Oracle Solaris 권한 관리는 ZFS 데이터 세트의 위임된 관리를 지원합니다. 즉, 제한된 권한 세트가 지정된 사용자가 ZFS 데이터 세트를 관리할 수 있습니다.

자세한 내용은 다음을 참조하십시오.

- "Oracle Solaris 11.2의 사용자 및 프로세스 보안 "의 "사용자 권한 관리"
- "Oracle Solaris 11.2의 ZFS 파일 시스템 관리 "의 1 장, "Oracle Solaris ZFS 파일 시스템(소개)"
- "Oracle Solaris 11.2의 ZFS 파일 시스템 관리 "의 "Oracle Solaris ZFS와 전통적인 파일 시스템의 차이"
- "Oracle Solaris 11.2의 ZFS 파일 시스템 관리 "의 5 장, "Oracle Solaris ZFS 파일 시스템 관리"
- "Oracle Solaris 11.2의 보안 셸 액세스 관리 "의 "보안 셸을 사용하여 ZFS를 원격으로 관리하는 방법"
- 선택한 매뉴얼 페이지에는 `zfs`(1M) 및 `zfs`(7FS)가 포함됩니다.

## Java Cryptography Extension

JCE(Java Cryptography Extension)는 Java 응용 프로그램 개발자를 위한 기능입니다. 자세한 내용은 Java SE Security (http://www.oracle.com/technetwork/java/javase/tech/index-jsp-136007.html)를 참조하십시오.

# 응용 프로그램 보호 및 격리

응용 프로그램은 맬웨어 및 악의적인 사용자의 진입점이 될 수 있습니다. 영역 내의 권한 사용 및 응용 프로그램 제약을 통해 Oracle Solaris에서 이러한 위협을 완화할 수 있습니다. 응용 프로그램에 필요한 권한만으로 응용 프로그램을 실행할 수 있으므로 악의가 있는 사용자에게는 시스템의 나머지 부분을 액세스할 수 있는 root 권한이 없습니다. 영역을 사용하여 공격 범위를 제한할 수 있습니다. 응용 프로그램의 비글로벌 영역이 공격을 받을 경우 영역의 호스트 시스템이 아니라 해당 영역의 프로세스에만 영향을 줍니다.

ASLR(주소 공간 레이아웃 임의 지정) 및 SMF(서비스 관리 기능)는 응용 프로그램을 보호하기 위한 추가 기능입니다. ASLR은 침입자의 실행 파일 하이재킹을 어렵게 하며 SMF 기능은 관리자에게 응용 프로그램을 시작, 중지 및 사용할 수 있는 권한을 부여합니다.

## Oracle Solaris의 권한

권한은 커널에 강제 적용되는 프로세스에 대한 세밀하게 조정된 고유한 권한입니다. Oracle Solaris는 `file_read`와 같은 기본 권한에서부터 `proc_clock_highres`와 같은 보다 전문적인 권한까지 80개 이상의 권한을 정의합니다. 프로세스, 사용자 또는 역할에 권한을 부여할 수 있습니다. 여러 Oracle Solaris 명령 및 데몬은 해당 작업을 수행하는 데 필요한 권한만으로 실행됩니다. 권한 인식 프로그램은 침입자가 프로그램 자체에서 사용하는 것보다 많은 권한을 부여하지 못하도록 방지합니다.

권한 사용은 프로세스 권한 관리라고도 부릅니다. 권한을 사용으로 설정하면 조직은 해당 시스템에서 실행되는 서비스 및 프로세스에 부여되는 권한을 지정(제한)할 수 있습니다.

자세한 내용은 다음을 참조하십시오.

- “Oracle Solaris 11.2의 사용자 및 프로세스 보안 ”의 “프로세스 권한 관리”
- “Developer’s Guide to Oracle Solaris 11 Security ”의 2 장, “Developing Privileged Applications”
- 선택한 매뉴얼 페이지에는 `ppriv`(1) 및 `privileges`(5)가 포함됩니다.

## Oracle Solaris 영역

Oracle Solaris Zones 소프트웨어 분할 기술을 사용하면 하드웨어 리소스를 동시에 공유하면서 서버당 하나의 응용 프로그램 배치 모델을 유지 관리할 수 있습니다.

영역은 여러 응용 프로그램이 동일한 물리적 하드웨어에서 서로 격리된 상태로 실행할 수 있게 해주는 가상화된 작동 환경입니다. 이러한 격리성은 한 영역 내에서 실행되는 프로세스가 다른 영역에서 실행되는 프로세스를 모니터링하거나 영향을 주거나, 서로 데이터를 보거나, 기본 하드웨어를 조작하지 않도록 방지합니다. 영역은 또한 물리적 장치 경로 및 네트워크 인터페이스 이름과 같이 응용 프로그램이 배치된 시스템의 물리적 속성으로부터 응용 프로그램을 구분하는 추상화 계층을 제공합니다.

Oracle Solaris 11.2에서는 변경할 수 없는 root 파일 시스템을 구성할 수 있습니다.

자세한 내용은 다음을 참조하십시오.

- "Oracle Solaris 영역 만들기 및 사용 "의 "읽기 전용 영역 구성"
- "Oracle Solaris 영역 소개 "
- 선택한 매뉴얼 페이지에는 `brands`(5), `zoneadm`(1M) 및 `zonecfg`(1M)이 포함됩니다.

## 주소 공간 레이아웃 임의 지정

ASLR(주소 공간 레이아웃 임의 지정)은 특정 프로그램에 사용되는 주소를 임의로 지정합니다. ASLR은 특정 메모리 범위의 정확한 위치에 대한 식별을 기반으로 하는 특정 유형의 공격을 방지하고 프로그램 중지 시도를 감지할 수 있습니다. 자세한 내용은 "Oracle Solaris 11.2에서 시스템 및 연결된 장치의 보안 "의 "주소 공간 레이아웃 모든 지정" 및 ASLR의 사용 설정 여부 확인 방법 [31]을 참조하십시오.

## 서비스 관리 기능

서비스는 지속적으로 실행되는 응용 프로그램입니다. 서비스는 실행 중인 응용 프로그램, 장치의 소프트웨어 상태 또는 일련의 다른 서비스를 나타낼 수 있습니다. Oracle Solaris의 SMF(서비스 관리 기능) 기능은 서비스 추가, 제거, 구성 및 관리를 위해 사용됩니다. SMF는 권한 관리를 사용하여 시스템에서 서비스 관리 기능에 대한 액세스를 제어합니다. 특히 SMF는 권한 부여를 사용하여 서비스를 관리할 수 있는 사용자 및 사용자가 수행할 수 있는 작업을 결정합니다.

SMF를 통해 조직에서는 서비스에 대한 액세스를 제어하고 이러한 서비스의 시작, 중지 및 새로 고침 방법을 제어할 수 있습니다.

자세한 내용은 다음을 참조하십시오.

- "Oracle Solaris 11.2의 시스템 서비스 관리 "
- "Oracle Solaris 11.2의 사용자 및 프로세스 보안 "의 "Apache 웹 서버에 특정 권한을 지정하는 방법"
- 선택한 매뉴얼 페이지에는 `svcadm`(1M), `svcs`(1), `smf`(5)가 포함됩니다.

# 사용자 보호 및 추가 권한 지정

"시스템 액세스가 제한되고 모니터됨" [13]에 설명된 초기 사용자의 경우와 같이 사용자에게는 `/etc/security/policy.conf` 파일에서 기본적인 권한, 권한 프로파일 및 인증 세트가 지정됩니다. 이러한 권한은 구성 가능합니다. 기본 권한을 거부하고 사용자에 대한 권한을 강화할 수 있습니다.

Oracle Solaris에서는 암호에 대한 유연성 있고 복잡한 요구 사항, 여러 사이트 요구 사항에 따라 구성 가능한 인증 및 사용자 권한 관리를 통해 사용자를 보호합니다. 이러한 기능은 권한 프로파일, 권한 부여 및 권한을 사용하여 신뢰할 수 있는 사용자에 대한 관리 권한을 제한 및 배포합니다. 또한 역할이라는 특수 공유 계정을 사용하여 사용자가 해당 역할을 맡을 때 해당 관리 권한만 지정합니다. ARMOR(Authorization Rules Managed On RBAC) 패키지는 미리 정의된 역할을 제공합니다.

## 암호 및 암호 제약 조건

강력한 사용자 암호는 무차별 대입을 포함한 여러 공격을 방어하는 데 도움이 됩니다.

Oracle Solaris에서는 사이트 요구에 따라 사용자 암호를 구성할 때 사용할 수 있는 여러 가지 기능을 제공합니다. 암호 길이, 내용, 변경 빈도, 수정 요구 사항을 지정하고 암호 기록을 유지할 수 있습니다. 사용하지 않아야 하는 암호에 대해서도 사전이 제공됩니다. 일부 사용 가능한 암호 해시 알고리즘도 제공됩니다. 기본값은 SHA256입니다.

자세한 내용은 다음을 참조하십시오.

- "Oracle Solaris 11.2에서 시스템 및 연결된 장치의 보안 "의 "로그인 제어 유지 관리"
- "Oracle Solaris 11.2에서 시스템 및 연결된 장치의 보안 "의 "로그인 및 암호 보안"
- 선택한 매뉴얼 페이지에는 `passwd`(1) 및 `crypt.conf`(4)가 포함됩니다.

## 플러그 가능한 인증 모듈

관리자는 PAM(Pluggable Authentication Module) 프레임워크를 사용하여 인증이 필요한 서비스를 수정하지 않고 계정, 자격 증명, 세션 및 암호에 대한 사용자 인증 요구 사항을 조정하고 구성할 수 있습니다.

PAM 프레임워크를 통해 조직은 계정, 세션 및 암호 관리 기능뿐만 아니라 사용자 인증 환경을 사용자 정의할 수 있습니다. `login` and `ssh`와 같은 시스템 입력 서비스는 PAM 프레임워크를 사용하여 새로 설치한 시스템의 모든 진입점을 보호합니다. PAM을 사용하면 새로 발견된 취약점으로부터 시스템을 보호하기 위해 PAM 프레임워크를 사용하는 시스템 서비스를 변경하지 않고 필드에서 인증 모듈을 교체하거나 수정할 수 있습니다.

Oracle Solaris는 대부분의 사이트 정책을 만족시키기 위해 다양한 PAM 모듈 및 구성 세트를 전달합니다. 자세한 내용은 다음을 참조하십시오.

- "Oracle Solaris 11.2의 Kerberos 및 기타 인증 서비스 관리 "의 1 장, "플러그 가능한 인증 모듈 사용"
- "Developer's Guide to Oracle Solaris 11 Security "의 "Writing Applications That Use PAM Services"
- `pam.conf`(4) 매뉴얼 페이지

## 사용자 권한 관리

Oracle Solaris의 사용자 권한은 최소 권한의 보안 정책을 통해 관리됩니다. 조직에서는 조직의 요구 사항 및 고유한 필요에 따라 사용자 또는 역할에 대해 선택적으로 관리 권한을 부여할 수 있습니다. 또한 필요할 때 사용자의 권한을 거부할 수도 있습니다. 권한은 사용자 또는 SMF 메서드에 대한 권한 부여 및 프로세스에 대한 권한으로 구현됩니다. 권한 프로파일을 사용하면 권한 및 권한 부여를 하나의 관련 권한 번들로 간편하게 수집할 수 있습니다.

자세한 내용은 다음을 참조하십시오.

- "Oracle Solaris 11.2의 사용자 및 프로세스 보안 "
- 선택한 매뉴얼 페이지에는 `auths`(1), `privileges`(5). `profiles`(1), `rbac`(5), `roleadd`(1M), `roles`(1), `user_attr`(4)가 포함됩니다.

# 네트워크 통신 보안

방화벽, 네트워크 응용 프로그램의 TCP 래퍼 및 암호화되고 인증된 원격 연결 등의 기능을 통해 네트워크 통신을 보호할 수 있습니다.

## 패킷 필터링

패킷 필터링은 네트워크 기반 공격에 대한 기본 보호를 제공합니다. Oracle Solaris에는 IP 필터 기능과 TCP 래퍼가 포함됩니다.

### 방화벽

Oracle Solaris의 IP 필터는 네트워크 기반 공격을 방어하기 위한 방화벽을 만듭니다.

특히 IP 필터는 stateful 패킷 필터링 기능을 제공하며, IP 주소 또는 네트워크, 포트, 프로토콜, 네트워크 인터페이스 및 트래픽 방향에 따라 패킷을 필터링할 수 있습니다. 또한 stateless 패킷 필터링 및 주소 풀 만들기 및 관리를 위한 기능이 포함됩니다. 또한 IP 필터는 NAT(네트워크 주소 변환) 및 PAT(포트 주소 변환)를 수행하는 기능도 포함합니다.

자세한 내용은 다음을 참조하십시오.

- IP 필터에 대한 개요는 "Oracle Solaris 11.2의 네트워크 보안 "의 4 장, "Oracle Solaris의 IP 필터 정보"를 참조하십시오.
- IP 필터 사용의 예는 "Oracle Solaris 11.2의 네트워크 보안 "의 5 장, "IP 필터 구성" 및 매뉴얼 페이지를 참조하십시오.
- IP 필터 정책 언어의 구문에 대한 자세한 내용 및 예는 `ipnat`(4) 매뉴얼 페이지를 참조하십시오.
- 선택한 매뉴얼 페이지에는 `ipfilter`(5), `ipf`(1M), `ipnat`(1M), `svc.ipfd`(1M) 및 `ipf`(4)가 포함됩니다.

### TCP 래퍼

TCP 래퍼는 인터넷 서비스에 대한 액세스 제어를 제공합니다. 다양한 인터넷(`inetd`) 서비스를 사용으로 설정한 경우 `tcpd` 데몬이 ACL에 대해 특정 네트워크 서비스를 요구하는 호스트의 주소를 확인합니다. 요청은 이에 따라 허용 또는 거부됩니다. 또한 TCP 래퍼는 유용한 모니터링 기능인 `syslog`의 네트워크 서비스에 대한 호스트 요청을 기록합니다.

Oracle Solaris의 `sendmail` 및 `ssh`(Secure Shell) 기능은 TCP 래퍼를 사용하도록 구성됩니다. `proftpd` 및 `rpcbind` 등 실행 파일에 대해 일대일 매핑되는 네트워크 서비스는 TCP 래퍼의 후보입니다.

TCP 래퍼는 조직이 보안 정책을 전역뿐만 아니라 서비스별 기반으로도 지정할 수 있도록 하는 다양한 기능의 구성 정책 언어를 지원합니다. 서비스에 대한 추가 액세스는 호스트 이름, IPv4 또는 IPv6 주소, netgroup 이름, 네트워크 및 심지어 DNS 이름에 따라서도 허용하거나 제한할 수 있습니다.

TCP 래퍼에 대한 자세한 내용은 다음을 참조하십시오.

- TCP 래퍼 사용 방법 [44]
- TCP 래퍼의 액세스 제어 언어의 구문에 대한 자세한 내용 및 예를 보려면 `hosts_access`(4) 매뉴얼 페이지를 참조하십시오.
- 선택한 매뉴얼 페이지에는 `tcpd`(1M) 및 `inetd`(1M)가 포함됩니다.

## 원격 액세스

원격 액세스 공격은 시스템 및 네트워크에 손상을 줄 수 있습니다. Oracle Solaris에서는 네트워크 전송에 대해 강력한 방어 기능을 제공합니다. 방어 기능에는 데이터 전송에 대한 암호화 및 인증 확인, 로그인 인증, 불필요한 원격 서비스 사용 안함으로 설정 등이 포함됩니다.

### IPsec 및 IKE

IPsec(IP 보안)는 IP 패킷을 인증 및/또는 암호화하여 네트워크 전송을 보호합니다. IPsec는 응용 프로그램 계층 아래에서 올바르게 구현되기 때문에 인터넷 응용 프로그램은 해당 코드를 수정할 필요 없이 IPsec를 활용할 수 있습니다.

IPsec 및 해당 자동 키 교환 프로토콜인 IKE는 암호화 프레임워크의 알고리즘을 사용합니다. 또한 암호화 프레임워크에서는 중앙 키 저장소를 제공합니다. IKE가 metaslot을 사용하도록 구성된 경우 조직에서는 키를 디스크, 연결된 하드웨어 키 저장소 또는 *softtoken*라는 소프트웨어 키 저장소에 저장할 수 있습니다.

IPsec 및 IKE는 구성이 필요하므로 설치는 되지만 기본적으로 사용으로 설정되지 않습니다. 올바르게 관리할 경우 IPsec는 네트워크 보안 작업에 효과적으로 활용할 수 있습니다.

자세한 내용은 다음을 참조하십시오.

- "Oracle Solaris 11.2의 네트워크 보안 "의 6 장, "IP Security Architecture 정보"
- "Oracle Solaris 11.2의 네트워크 보안 "의 7 장, "IPsec 구성"
- "Oracle Solaris 11.2의 네트워크 보안 "의 "IPsec 및 FIPS 140"
- "Oracle Solaris 11.2의 네트워크 보안 "의 8 장, "IKE(Internet Key Exchange)"
- "Oracle Solaris 11.2의 네트워크 보안 "의 9 장, "IKEv2 구성"
- 선택한 매뉴얼 페이지에는 `ipsecconf`(1M) 및 `in.iked`(1M)가 포함됩니다.

## Secure Shell

기본적으로 Oracle Solaris의 Secure Shell 기능은 새로 설치된 시스템에서 유일하게 활성화되는 원격 액세스 방식입니다. 기타 다른 네트워크 서비스는 사용 안함으로 설정되거나 수신 전용 모드입니다.

Secure Shell에서는 시스템 간의 암호화된 통신 채널을 만듭니다. 또한 Secure Shell은 X Window 시스템 트래픽을 전달하거나 인증되고 암호화된 네트워크 링크를 통해 로컬 시스템과 원격 시스템 간의 개별 포트 번호에 연결할 수 있는 요청 시 VPN(가상 사설망)으로 사용될 수도 있습니다.

따라서 Secure Shell는 잠재적인 침입자가 가로챈 통신 내용을 읽지 못하도록 방지하고 시스템을 스푸핑하지 못하도록 방지합니다.

자세한 내용은 다음을 참조하십시오.

- "Oracle Solaris 11.2의 보안 셸 액세스 관리 "의 1 장, "보안 셸 사용(작업)"
- "Oracle Solaris 11.2의 보안 셸 액세스 관리 "의 "보안 셸 및 FIPS 140"
- 선택한 매뉴얼 페이지에는 `ssh`(1), `sshd`(1M), `sshd_config`(4) 및 `ssh_config`(4)가 포함됩니다.

## Kerberos 서비스

Oracle Solaris의 Kerberos 기능을 사용하면 시스템에서 다른 운영 체제와 Kerberos 서비스를 실행하는 이기종 네트워크에서도 Single Sign-On 및 보안 트랜잭션을 사용할 수 있습니다.

Kerberos는 MIT(Massachusetts Institute of Technology)에서 개발된 Kerberos V5 네트워크 인증 프로토콜을 기반으로 합니다. Kerberos 서비스는 무결성 및 프라이버시를 비롯하

여 강력한 사용자 인증을 제공합니다. Kerberos 서비스를 사용하면 다른 시스템에 한번만 로그인하여, 명령을 실행하고, 데이터를 교환하고, 파일을 안전하게 전송할 수 있습니다. 또한 서비스를 통해 관리자가 서비스 및 시스템에 대한 액세스를 제한할 수 있습니다.

자세한 내용은 다음을 참조하십시오.

- "Oracle Solaris 11.2의 Kerberos 및 기타 인증 서비스 관리 "
- "Oracle Solaris 11.2의 Kerberos 및 기타 인증 서비스 관리 "의 "FIPS 140 알고리즘 및 Kerberos 암호화 유형"
- 선택한 매뉴얼 페이지에는 `kadmin`(1M), `kdcmgr`(1M), `kerberos`(5), `kinit`(1) 및 `krb5.conf`(4)가 포함됩니다.

# 시스템 보안 유지

Oracle Solaris에서는 시스템 보안을 유지하기 위해 다음 기능을 제공합니다.

- 확인된 부트 - 부트 프로세스를 보호합니다. 확인된 부트는 기본적으로 사용 안함으로 설정됩니다.
- 패키지 확인 - 설치된 패키지가 원본 저장소의 패키지와 동일한지 확인합니다.
- 감사 서비스 - 시스템 액세스 및 사용을 감사합니다. 감사 기능은 기본적으로 사용으로 설정됩니다.
- 파일 무결성 확인 - BART 매니페스트는 시스템의 모든 파일을 나열할 수 있으며 매니페스트 비교를 사용하여 파일 무결성을 확인합니다.
- 로그 파일 - SMF는 모든 서비스에 대한 로그 파일을 제공합니다. `syslog` 유틸리티는 시스템 서비스의 이름 지정 및 구성 로그를 위한 중앙 파일을 제공하며 선택적으로 관리자에게 중요한 이벤트를 통지할 수 있습니다. 감사 등의 기타 기능도 자체 로그를 만듭니다.
- 준수 보고서 - Oracle Solaris에서는 시스템을 평가하는 여러 가지 보안 벤치마크를 제공합니다. 평가 결과로, 시스템의 보안 체계를 평가하는 보고서가 만들어집니다.

## 확인된 부트

확인된 부트는 시스템의 부트 프로세스를 보호하는 Oracle Solaris 기능입니다. 이 기능은 허용되지 않은 커널 모듈 및 트로이 목마 응용 프로그램 설치 등의 위협으로부터 시스템을 보호합니다. 기본적으로 확인된 부트는 사용 안함으로 설정됩니다.

자세한 내용은 "Oracle Solaris 11.2에서 시스템 및 연결된 장치의 보안 "의 2 장, "Oracle Solaris 시스템 무결성 보호"를 참조하십시오.

## 패키지 무결성 확인

패키지를 설치 또는 업데이트한 후에는 `pkg verify` 명령을 실행하여 시스템의 패키지가 원본 저장소의 패키지와 동일한지 확인할 수 있습니다.

자세한 내용은 pkg(1) 매뉴얼 페이지 및 패키지 확인 방법 [30]을 참조하십시오.

## 감사 서비스

Oracle Solaris에서는 시스템 액세스 및 사용에 대한 데이터를 수집하는 감사 서비스를 제공합니다. 감사 데이터는 보안 관련 시스템 이벤트의 신뢰할 수 있는 시간 기록 로그를 제공합니다. 그런 다음 이 데이터를 사용하여 시스템에서 발생한 작업에 대한 책임을 지정할 수 있습니다.

감사는 보안 평가, 검증, 준수 및 인증 주체에 대한 기본 요구 사항입니다. 감사는 잠재적인 침입자에 대한 억제력을 제공할 수도 있습니다.

자세한 내용은 다음을 참조하십시오.

- 감사 관련 매뉴얼 페이지의 목록은 "Oracle Solaris 11.2의 감사 관리 "의 7 장, "감사 참조"를 참조하십시오.
- 자세한 내용은 로그인/로그아웃 이외의 중요 이벤트를 감사하는 방법 [41] 및 매뉴얼 페이지를 참조하십시오.
- 감사에 대한 개요는 "Oracle Solaris 11.2의 감사 관리 "의 1 장, "Oracle Solaris의 감사 정보"를 참조하십시오.
- 감사 작업에 대해서는 "Oracle Solaris 11.2의 감사 관리 "의 3 장, "감사 서비스 관리"를 참조하십시오.

## 파일 무결성 확인

Oracle Solaris의 BART를 사용하면 시간 경과에 따른 시스템에 대한 파일 레벨 검사를 수행하여 시스템을 포괄적으로 검증할 수 있습니다. 설치 후 `pkg verify` 명령은 소스와 대상 패키지의 내용이 동일한지 확인합니다. 패키지 확인 후 BART 매니페스트는 쉽고 안정적으로 시스템의 파일에 대한 정보를 수집할 수 있습니다.

BART는 한 시스템 또는 시스템 네트워크에서 무결성 관리를 위한 유용한 도구입니다. 시스템의 파일을 시스템의 원본 파일 및 다른 시스템의 파일과 비교할 수 있습니다. 보고서에는 시스템이 패치되지 않거나, 침입자가 승인되지 않은 파일을 설치했거나, 침입자가 `root` 소유의 파일 등 중요한 파일에 대한 내용 또는 사용 권한을 변경한 사항이 기록될 수 있습니다.

자세한 내용은 다음을 참조하십시오.

- 지침은 "BART를 사용하여 파일 무결성 확인" [52], "BART를 사용하여 파일 무결성 확인" [52] 및 매뉴얼 페이지를 참조하십시오.
- BART에 대한 개요는 "Oracle Solaris 11.2의 파일 보안 및 파일 무결성 확인 "의 2 장, "BART를 사용하여 파일 무결성 확인"을 참조하십시오.
- BART 사용의 예는 "Oracle Solaris 11.2의 파일 보안 및 파일 무결성 확인 "의 "BART 사용 정보" 및 매뉴얼 페이지를 참조하십시오.
- 선택한 매뉴얼 페이지에는 `bart`(1M), `bart_rules`(4) 및 `bart_manifest`(4)가 포함됩니다.

## 로그 파일

Oracle Solaris의 SMF(서비스 관리 기능) 기능은 서비스당 해당 서비스의 상태를 기록합니다. 감사 및 Secure Shell 등의 여러 서비스는 해당 로그를 기록합니다. `syslog` 또는 `rsyslog` 데몬은 관리자에게 여러 서비스의 중요한 조건에 대해 알리거나 경고할 수 있는 중앙화된 로그를 기록합니다. 예를 들어 요약된 감사 레코드를 `syslog`에 기록하도록 감사를 구성할 수 있습니다. `syslogd`(1M) 및 `syslog.conf`(4) 매뉴얼 페이지를 참조하십시오.

## 보안 표준 준수

`compliance assess` 명령은 시스템의 보안 체계에 대한 스냅샷을 제공합니다. 평가 보고서에는 업계 보안 벤치마크를 만족하기 위해 시스템에서 변경해야 할 사항이 제안됩니다. 자세한 내용은 "Oracle Solaris 11.2 보안 적합성 안내서 " 및 `compliance`(1M) 매뉴얼 페이지를 참조하십시오.

# 레이블이 있는 보안

Oracle Solaris의 Trusted Extensions 기능에서는 레이블이 있는 보안이 제공됩니다.

## Oracle Solaris의 Trusted Extensions 기능

Oracle Solaris의 Trusted Extensions 기능은 데이터 보안 정책을 데이터 소유권과 구분하도록 하는 보안 레이블 지정 기술에서 선택적으로 사용으로 설정된 계층입니다. Trusted Extensions는 소유권을 기반으로 하는 기존의 DAC(임의의 액세스 제어) 및 레이블 기반의 MAC(필수 액세스 제어) 정책을 모두 지원합니다. Trusted Extensions 계층이 사용으로 설정되지 않은 한 모든 레이블이 서로 동일하여 커널이 MAC 정책을 적용하도록 구성되지 않습니다. 레이블 기반 MAC 정책이 사용으로 설정된 경우 액세스를 요청하는 프로세스(주체) 및 데이터를 포함하는 객체와 연관된 레이블의 비교에 따라 모든 데이터 플로우가 제한됩니다.

Trusted Extensions 구현은 호환성을 극대화하고 오버헤드를 최소화하는 반면 높은 보장성을 제공한다는 점에서 고유한 특성을 갖습니다. Trusted Extensions는 "Oracle Solaris 11 Common Criteria EAL4+ Certification" [26]의 일부입니다.

Trusted Extensions는 Common Criteria LSP(Labeled Security Package)의 요구 사항을 만족합니다. "Oracle Solaris 11 Common Criteria EAL4+ Certification" [26]을 참조하십시오.

자세한 내용은 다음을 참조하십시오.

- Trusted Extensions 구성 및 유지 관리에 대한 자세한 내용은 "Trusted Extensions 구성 및 관리 "를 참조하십시오.

- 선택한 매뉴얼 페이지에는 `trusted_extensions`(5), `labeladm`(1M) 및 `labeld`(1M)가 포함됩니다.

## 레이블이 있는 파일 시스템

기본적으로 파일 시스템에는 동일한 레이블의 영역 내에서 단일 레이블이 지정됩니다. 다중 레벨 ZFS 데이터 세트를 만들고, 이 데이터 세트를 Trusted Extensions 시스템에 마운트하고, 적절한 권한으로 해당 데이터 세트의 파일을 업그레이드 및 다운그레이드할 수 있습니다. 자세한 내용은 "Trusted Extensions 구성 및 관리 "의 "파일의 레이블 다시 지정을 위한 다중 레벨 데이터 세트"를 참조하십시오.

## 레이블이 있는 네트워크 통신

Trusted Extensions에서는 네트워크 통신에 레이블을 지정합니다. 시작 네트워크 끝점 및 수신 네트워크 끝점과 연관된 레이블 비교를 기반으로 데이터 흐름이 제한됩니다. 통신 레이블의 정보를 전달하려면 게이트웨이 및 중간 호프에도 레이블을 지정해야 합니다. NFS 및 다중 레벨 ZFS 데이터 세트는 네트워크에 대한 추가 기능을 제공합니다.

자세한 내용은 다음을 참조하십시오.

- "Trusted Extensions 구성 및 관리 "의 "ProductShort;에서 네트워크 인터페이스 구성"
- "Trusted Extensions 구성 및 관리 "의 15 장, "신뢰할 수 있는 네트워킹"
- "Trusted Extensions 구성 및 관리 "의 16 장, "Trusted Extensions에서 네트워크 관리"

## Trusted Extensions 다중 레벨 데스크탑

다른 다중 레벨 운영 체제와 달리 Trusted Extensions에는 다중 레벨 데스크탑이 포함됩니다. 사용자가 본인에게 허용된 레이블만 볼 수 있도록 구성할 수 있습니다. 별도의 암호가 필요하도록 각 레이블을 구성할 수 있습니다.

자세한 내용은 "Trusted Extensions 사용자 설명서 "를 참조하십시오. 사용자를 구성하려면 "Trusted Extensions 구성 및 관리 "의 11 장, "Trusted Extensions에서 사용자, 권한 및 역할 관리"를 참조하십시오.

# Oracle Solaris 11 Common Criteria EAL4+ Certification

Oracle Solaris 11은 Canadian Common Criteria Scheme의 EAL4(Evaluation Assurance Level 4)에 따라 인증되었으며 결함 수정으로 등급이 향상되었습니다(EAL4+). EAL4는 CCRA(Common Criteria Recognition Arrangement)에 따라 26개 국가에서 상호 인정되는 가장 높은 평가 레벨입니다.

이 인증은 OSPP(운영 체제 보호 프로파일)에 대해 수행되며 다음과 같은 네 가지 확장 패키지를 포함합니다.

- 고급 관리
- 확장 식별 및 인증
- 레이블이 있는 보안
- 가상화

인증에 대한 자세한 내용은 다음을 참조하십시오.

- Oracle Security Evaluations Matrix (http://www.oracle.com/technetwork/topics/security/security-evaluations-099357.html)
- The Common Criteria Recognition Arrangement (http://www.commoncriteriaportal.org/ccra/)
- Operating System Protection Profile (http://www.commoncriteriaportal.org/files/ppfiles/pp0067b_pdf.pdf)

## 사이트 보안 정책 및 실행

보안 시스템 또는 시스템 네트워크를 위해서는 해당 정책을 지원하는 보안 실행과 함께 사이트에 보안 정책이 배치되어 있어야 합니다. 프로그램을 개발 중이거나 타사 프로그램을 설치하는 경우 해당 프로그램을 보안에 맞게 개발 및 설치해야 합니다.

자세한 내용은 다음을 참조하십시오.

- Importance of Software Security Assurance (http://www.oracle.com/us/support/assurance/overview/index.html)
- “Developer’s Guide to Oracle Solaris 11 Security ”의 부록 A, “Secure Coding Guidelines for Developers”
- “Trusted Extensions 구성 및 관리 ”의 부록 A, “사이트 보안 정책”
- “Trusted Extensions 구성 및 관리 ”의 “보안 요구 사항 적용”
- Keeping Your Code Secure (http://blogs.oracle.com/maryanndavidson/entry/those_who_can_t_do)

♦ ♦ ♦ 2 장

# 2 Oracle Solaris 보안 구성

이 장에서는 시스템에서 보안을 구성하기 위해 수행해야 하는 작업에 대해 설명합니다. 이 장에서는 패키지 설치, 시스템 자체 구성, 다양한 부속 시스템 구성 및 IPsec와 같은 필요할 수 있는 추가 응용 프로그램에 대해 설명합니다.



## Oracle Solaris OS 설치

Oracle Solaris OS는 is 패키지 저장소에서 그룹이라는 패키지 세트를 선택하여 설치됩니다. 각 그룹은 다목적 서버, 최소 설치 시스템 및 데스크탑 시스템 등 용도별 패키지를 제공합니다. 패키지에 서명하여 해당 보안 전송을 확인할 수 있습니다.

Oracle Solaris OS를 설치할 때는 다음과 같이 적합한 그룹 패키지를 설치하는 매체를 선택합니다.

- **Oracle Solaris 대규모 서버** - AI(자동 설치 프로그램) 설치의 기본 매니페스트 및 텍스트 설치 프로그램은 모두 Oracle Solaris 대규모 서버 환경을 제공하는 `group/system/solaris-large-server` 그룹을 설치합니다.
- **Oracle Solaris 소규모 서버** - AI(자동 설치 프로그램) 설치 및 텍스트 설치 프로그램은 선택적으로 `group/system/solaris-small-server` 그룹을 설치합니다. 이 그룹은 패키지를 추가할 수 있는 유용한 명령줄 환경을 제공합니다.
- **Oracle Solaris 최소 서버** - AI(자동 설치 프로그램) 설치 및 텍스트 설치 프로그램은 선택적으로 `group/system/solaris-minimal-server` 그룹을 설치합니다. 이 그룹은 원하는 패키지만 추가할 수 있는 최소 명령줄 환경을 제공합니다.
- **Oracle Solaris 데스크탑** - 라이브 매체는 Oracle Solaris 11 데스크탑 환경을 제공하는 `group/system/solaris-desktop` 그룹을 설치합니다.

중앙 집중식 용도의 데스크탑 시스템을 만들려면 데스크탑 서버에 `group/feature/multi-user-desktop` 그룹을 추가합니다. 자세한 내용은 "Optimizing the Oracle Solaris 11 Desktop for a Multiuser Environment " 문서를 참조하십시오.

AI(자동 설치 프로그램)를 통한 자동 설치는 "Oracle Solaris 11.2 시스템 설치 "의 제III부, "설치 서버를 사용하여 설치"를 참조하십시오.

매체 선택에 대한 도움을 받으려면 다음 설치 및 패키지 내용 설명서를 참조하십시오.

- "Oracle Solaris 11.2 시스템 설치 "
- "사용자 정의 Oracle Solaris 11.2 설치 이미지 만들기 "
- "Oracle Solaris 11.2의 소프트웨어 추가 및 업데이트 "
- "Oracle Solaris 11.2 Package Group Lists "

# 초기 시스템 보안

다음 작업은 순서대로 수행하는 것이 가장 좋습니다. 현재 Oracle Solaris가 설치되어 있고 `root` 역할을 소비할 수 있는 초기 사용자만 시스템에 액세스할 수 있습니다.

**표 2-1** 시스템 작업 맵 보안

| 작업 | 설명 | 수행 방법 |
|---|---|---|
| 1. 시스템에서 패키지를 확인합니다. | 설치 소스의 패키지가 설치된 패키지와 동일한지 확인합니다. | 패키지 확인 방법 [30] |
| 2. 실행 파일이 보호되었는지 확인합니다. | ASLR이 사용으로 설정되었는지 확인합니다. | ASLR의 사용 설정 여부 확인 방법 [31] |
| 3. 시스템에서 하드웨어 설정을 보호합니다. | 하드웨어 설정을 변경하려면 암호를 입력하도록 요구하여 하드웨어를 보호합니다. x86에서는 GRUB 메뉴에 대한 액세스가 제어됩니다. SPARC에서는 `eeprom` 명령이 하드웨어를 보호합니다. | "Oracle Solaris 11.2에서 시스템 및 연결된 장치의 보안 "의 "시스템 하드웨어에 대한 액세스 제어" |
| 3. 필요하지 않은 서비스를 사용 안함으로 설정합니다. | 시스템의 필수 기능에 포함되지 않는 프로세스가 실행되지 않도록 방지합니다. | 불필요한 서비스를 사용 안함으로 설정하는 방법 [32] |
| 5. 워크스테이션 소유자가 시스템 전원을 끄지 않도록 방지합니다. | 콘솔 사용자가 시스템을 종료하거나 일시 중지하지 않도록 방지합니다. | 사용자의 전원 관리 기능을 제거하는 방법 [32] |
| 6. 사이트의 보안 정책이 반영된 로그인 경고 메시지를 만듭니다. | 인증 전/후 사용자에게 시스템이 모니터되고 있음을 알립니다. | 배너 파일에 보안 메시지를 배치하는 방법 [33]<br><br>데스크탑 로그인 화면에 보안 메시지를 배치하는 방법 [34] |

## ▼ 패키지 확인 방법

설치 후 바로 패키지를 확인하여 설치를 검증합니다.

**시작하기 전에** root 역할을 가져야 합니다. 자세한 내용은 "Oracle Solaris 11.2의 사용자 및 프로세스 보안"의 "지정된 관리 권한 사용"을 참조하십시오.

1. **설치 로그를 검토합니다.**

2. **pkg verify 명령을 실행합니다.**
   레코드를 보존하려면 명령 출력을 파일로 전송합니다.

   ```
   # pkg verify > /var/pkgverifylog
   ```

3. **로그에서 오류를 검토합니다.**

4. **오류가 있으면 매체에서 재설치하거나 오류를 수정합니다.**

**참조** 자세한 내용은 pkg(1) 및 pkg(5) 매뉴얼 페이지를 참조하십시오. 매뉴얼 페이지에는 pkg verify 명령 사용 예가 포함되어 있습니다.

## ▼ ASLR의 사용 설정 여부 확인 방법

기본적으로, 태그가 지정된 실행 명령이 연결되지 않은 주소 공간에 기록되어 침입자가 실행 가능 스택에 명령을 주입할 가능성을 줄입니다.

**시작하기 전에** root 역할을 가져야 합니다. 자세한 내용은 "Oracle Solaris 11.2의 사용자 및 프로세스 보안"의 "지정된 관리 권한 사용"을 참조하십시오.

1. **ASLR이 사용으로 설정되어 있는지 확인합니다.**

   ```
   # sxadm info
   EXTENSION       STATUS                  CONFIGURATION
   aslr            enabled (all)           enabled (all)
   ```

   all 값은 기본값보다 강력하므로 응용 프로그램에서 메모리의 연속 스택에 의존하는 오류가 발생할 수 있습니다. 예를 들어 데이터베이스에서 메모리의 연속 스택에 의존할 수 있습니다.

2. **ASLR이 사용 안함으로 설정된 경우 기본값을 사용으로 설정하고 유효한지 확인합니다.**

   ```
   # sxadm delcust aslr
   # sxadm info
   EXTENSION       STATUS                  CONFIGURATION
   aslr            enabled (tagged-files)  system default (default)
   ```

**참조** 디버깅을 위해 특정 이진에서 sxadm 명령을 호출하여 ASLR을 해제할 수 있습니다. 예제는 sxadm(1M) 매뉴얼 페이지를 참조하십시오.

## ▼ 불필요한 서비스를 사용 안함으로 설정하는 방법

이 절차를 사용하여 시스템에서 필요하지 않은 서비스를 사용 안함으로 설정합니다.

**시작하기 전에** `root` 역할을 가져야 합니다. 자세한 내용은 "Oracle Solaris 11.2의 사용자 및 프로세스 보안"의 "지정된 관리 권한 사용"을 참조하십시오.

1. **온라인 네트워크 서비스를 나열합니다.**

```
# svcs | grep network
online         Sep_07   svc:/network/loopback:default
online         Sep_07   svc:/network/http:apache22
online         Sep_07   svc:/network/nfs/server:default
...
online         Sep_07   svc:/network/ssh:default
```

2. **이 시스템에 필요하지 않은 서비스를 사용 안함으로 설정합니다.**

   예를 들어, 시스템이 NFS 서버 또는 웹 서버가 아니고 서비스가 온라인인 경우 서비스를 사용 안함으로 설정합니다.

```
# svcadm disable svc:/network/nfs/server:default
# svcadm disable svc:/network/http:apache22
```

**참조** 자세한 내용은 "Oracle Solaris 11.2의 시스템 서비스 관리"의 1 장, "서비스 관리 기능 소개" 및 `svcs`(1) 매뉴얼 페이지를 참조하십시오.

## ▼ 사용자의 전원 관리 기능을 제거하는 방법

이 절차에 따라 시스템 콘솔의 사용자가 시스템을 일시 중지하거나 전원을 끄지 않도록 방지합니다. 콘솔 사용자가 시스템 하드웨어의 전원을 끌 수 있는 경우 이 시스템 솔루션은 효과가 없습니다.

**시작하기 전에** `root` 역할을 가져야 합니다. 자세한 내용은 "Oracle Solaris 11.2의 사용자 및 프로세스 보안"의 "지정된 관리 권한 사용"을 참조하십시오.

1. **콘솔 사용자 권한 프로파일의 내용을 검토합니다.**

```
% profiles -p "Console User" info
 name=Console User
 desc=Manage System as the Console User
 auths=solaris.system.shutdown,solaris.device.cdrw,
             solaris.smf.manage.vbiosd,solaris.smf.value.vbiosd
 profiles=Suspend To RAM,Suspend To Disk,Brightness,CPU Power Management,
                Network Autoconf User
 help=RtConsUser.html
```

2. **사용자가 보존하게 하려는 콘솔 사용자 프로파일의 모든 권한이 포함된 권한 프로파일을 만듭니다.**
   자세한 내용은 “Oracle Solaris 11.2의 사용자 및 프로세스 보안 ”의 “권한 프로파일을 만드는 방법”을 참조하십시오.

3. **`/etc/security/policy.conf` 파일의 콘솔 사용자 권한 프로파일을 주석 처리합니다.**

```
#CONSOLE_USER=Console User
```

4. **2단계에서 만든 권한 프로파일을 지정합니다.**

   - 여러 사용자가 권한 프로파일을 공유하는 경우 권한 프로파일에서 이 값을 설정하는 것은 확장 가능한 솔루션이 될 수 있습니다.

     ```
     # usermod -P shared-profile username
     ```

   - 또한 `policy.conf` 파일에서 시스템당 프로파일을 지정할 수도 있습니다.

     ```
     # pfedit /etc/security/policy.conf...
     #PROFS_GRANTED=Basic Solaris User
     PROFS_GRANTED=shared-profile,Basic Solaris User
     ```

참조 자세한 내용은 “Oracle Solaris 11.2의 사용자 및 프로세스 보안 ”의 “policy.conf 파일” 및 `policy.conf`(4) and `usermod`(1M) 매뉴얼 페이지를 참조하십시오.

## ▼ 배너 파일에 보안 메시지를 배치하는 방법

이 절차를 수행하여 두 개의 배너 파일에서 사이트의 보안 정책이 반영된 보안 메시지를 만듭니다. 인증 전에는 `/etc/issue` 파일이 표시되고 인증 후에는 `/etc/motd` 파일이 표시됩니다.

**참고** - 이 절차의 샘플 메시지는 미국 정부 요구 사항을 충족하지 않으며 사용자의 보안 정책을 충족하지도 않습니다. 보안 메시지 내용에 대해서는 회사의 법률 전문가와 상의하십시오.

시작하기 전에 Administrator Message Edit 권한 프로파일에 지정된 관리자여야 합니다. 자세한 내용은 “Oracle Solaris 11.2의 사용자 및 프로세스 보안 ”의 “지정된 관리 권한 사용”을 참조하십시오.

1. **`/etc/issue` 파일을 만들고 보안 메시지를 추가합니다.**

```
# pfedit /etc/issue
ALERT   ALERT   ALERT   ALERT   ALERT

This machine is available to authorized users only.

If you are an authorized user, continue.

Your actions are monitored, and can be recorded.
```

login 명령은 ssh, telnet 및 FTP 서비스에서와 같이 인증 전에 /etc/issue 내용을 표시합니다. 데스크탑 로그인 시 /etc/issue 내용을 표시하려면 데스크탑 로그인 화면에 보안 메시지를 배치하는 방법 [34]을 참조하십시오.

자세한 내용은 issue(4) 및 pfedit(1M) 매뉴얼 페이지를 참조하십시오.

2. **/etc/motd 파일에 보안 메시지를 추가합니다.**

```
# pfedit /etc/motd
This system serves authorized users only. Activity is monitored and reported.
```

Oracle Solaris에서 사용자의 초기 셸에는 /etc/motd 파일의 내용이 표시됩니다.

## ▼ 데스크탑 로그인 화면에 보안 메시지를 배치하는 방법

인증 전 및/또는 후에 사용자가 검토할 보안 메시지를 만들 수 있는 여러 가지 방법 중에서 선택합니다. 인증 전에는 /etc/issue 파일이 표시되고 인증 후에는 /etc/motd 파일이 표시됩니다.

자세한 내용을 보려면 데스크탑에서 System(시스템) -> Help(도움말) 메뉴를 눌러 GNOME 도움말 브라우저를 표시합니다. yelp 명령을 사용해도 됩니다. 데스크탑 로그인 스크립트는 gdm(1M) 매뉴얼 페이지의 GDM Login Scripts and Session Files 절을 참조하십시오.

**참고** - 이 절차의 샘플 메시지는 미국 정부 요구 사항을 충족하지 않으며 사용자의 보안 정책을 충족하지도 않습니다. 보안 메시지 내용에 대해서는 회사의 법률 전문가와 상의하십시오.

**시작하기 전에** 파일을 만들려면 root 역할을 가져야 합니다. 기존 파일을 수정하려면 solaris.admin.edit/*path-to-existing-file* 권한이 지정된 관리자여야 합니다.

1. **다음 옵션 중 하나를 사용하여 인증 전 데스크탑 로그인 화면에 보안 메시지를 배치합니다.**

   인증 전 대화 상자를 만드는 옵션은 1단계 배너 파일에 보안 메시지를 배치하는 방법 [33]에서 /etc/issue 파일의 보안 메시지를 사용합니다.

   - **옵션 1: 대화 상자에 보안 메시지가 표시되도록 GDM 초기화 스크립트를 수정합니다.**

     /etc/gdm 디렉토리에는 인증 전후에 보안 메시지를 표시하는 세 가지 초기화 스크립트가 포함되어 있습니다.

     ```
     # pfedit /etc/gdm/Init/Default
     /usr/bin/zenity --text-info --width=800 --height=300 \
     --title="Security Message"  --filename=/etc/issue
     ```

     비root 사용자로서 시스템 파일을 편집하는 데 대한 자세한 내용은 pfedit(1M) 매뉴얼 페이지를 참조하십시오.

■ **옵션 2: 입력 필드 위에 보안 메시지가 표시되도록 로그인 창을 수정합니다.**

메시지에 맞게 로그인 창이 확대됩니다. 이 방법에서는 `/etc/issue` 파일을 사용하지 않습니다. GUI에 텍스트를 입력해야 합니다.

---

**참고** - 로그인 창(`gdm-greeter-login-window.ui`)은 `pkg fix` 및 `pkg update` 명령에 의해 겹쳐 쓰여집니다. 변경 사항을 보존하려면 구성 파일 디렉토리에 파일을 복사하고 시스템 업그레이드 후 새 파일에 변경 사항을 병합하십시오. 자세한 내용은 pkg(5) 매뉴얼 페이지를 참조하십시오.

---

a. **로그인 창 사용자 인터페이스로 디렉토리를 변경합니다.**

```
# cd /usr/share/gdm
```

b. **(옵션) 원래 로그인 창 UI의 복사본을 저장합니다.**

```
# cp gdm-greeter-login-window.ui /etc/gdm/gdm-greeter-login-window.ui.orig
```

c. **GNOME 툴킷 인터페이스 디자인 프로그램을 사용하여 로그인 창에 레이블을 추가합니다.**

`glade-3` 프로그램이 GTK+ 인터페이스 디자인 프로그램을 엽니다. 사용자 입력 필드 위에 표시되는 레이블에 보안 메시지를 입력합니다.

```
# /usr/bin/glade-3 /usr/share/gdm/gdm-greeter-login-window.ui
```

인터페이스 디자인 프로그램에 대한 지침을 검토하려면 GNOME 도움말 브라우저에서 Development(개발)를 누릅니다. 그러면 Manual Pages(설명서 페이지)의 Applications(응용 프로그램) 아래에 `glade-3`(1) 매뉴얼 페이지가 나열됩니다.

d. **(옵션) 수정된 로그인 창 UI의 복사본을 저장합니다.**

```
# cp gdm-greeter-login-window.ui /etc/gdm/gdm-greeter-login-window.ui.site
```

2. **다음 옵션 중 하나를 사용하여 인증 후 데스크탑 로그인 화면에 보안 메시지를 배치합니다.**

인증 후 대화 상자를 만드는 옵션은 2단계 배너 파일에 보안 메시지를 배치하는 방법 [33]에서 `/etc/motd` 파일의 보안 메시지를 사용합니다.

■ **옵션 1: 인증 후 데스크탑에 보안 메시지를 배치합니다.**

```
# pfedit /etc/gdm/PreSession/Default
/usr/bin/zenity --text-info --width=800 --height=300 \
--title="Security Message"  --filename=/etc/motd
```

---

**참고** - 사용자 작업 공간에 여러 창이 표시된 경우 대화 상자가 가려질 수 있습니다.

---

- **옵션 2: 인증 후 추가 창에 보안 메시지를 표시하는 데스크탑 파일을 만듭니다.**

```
# pfedit /usr/share/gdm/autostart/LoginWindow/banner.desktop
[Desktop Entry]
Type=Application
Name=Banner Dialog
Exec=/usr/bin/zenity --text-info --width=800 --height=300 \
--title="Security Message" \
--filename=/etc/motd
OnlyShowIn=GNOME;
X-GNOME-Autostart-Phase=Application
```

로그인 창에서 인증 후 작업 공간에 연결하려면 보안 메시지 창을 닫아야 합니다. `zenity` 명령 옵션은 `zenity`(1) 매뉴얼 페이지를 참조하십시오.

**예 2-1** 데스크탑 로그인 시 간단한 경고 메시지 만들기

이 예에서 관리자는 데스크탑 파일에 `zenity` 명령에 대한 인수로 간단한 메시지를 입력합니다. 또한 관리자는 `--warning` 옵션을 사용하여 메시지와 함께 경고 아이콘을 표시하도록 할 수 있습니다.

```
# pfedit /usr/share/gdm/autostart/LoginWindow/bannershort.desktop
[Desktop Entry]
Type=Application
Name=Banner Dialog
Exec=/usr/bin/zenity --warning --width=800  --height=150 --title="Security Message" \
--text="This system serves authorized users only. Activity is monitored and reported."
OnlyShowIn=GNOME;
X-GNOME-Autostart-Phase=Application
```

# 사용자 보안

이제 `root` 역할을 사용할 수 있는 초기 사용자만 시스템에 액세스할 수 있습니다. 다음 작업은 일반 사용자가 로그인하기 전에 순서대로 수행하는 것이 가장 좋습니다.

**표 2-2** 사용자 작업 맵 보안

| 작업 | 설명 | 수행 방법 |
|---|---|---|
| 강력한 암호를 사용하고 암호를 정기적으로 변경해야 합니다. | 각 시스템에서 기본 암호 제약 조건을 강화합니다. | 보다 강력한 암호 제약 조건을 설정하는 방법 [37] |
| 일반 사용자에 대해 제한적인 파일 권한을 구성합니다. | 일반 사용자의 파일 권한에 대해 `022`보다 제한적인 값을 설정합니다. | 일반 사용자에 대해 더 제한적인 `umask` 값을 설정하는 방법 [40]. |
| 일반 사용자에 대한 계정 잠금을 설정합니다. | 관리에 사용되지 않는 시스템에서 시스템 차원의 계정 잠금을 설정하고 잠금을 활성화하는 로그인 수를 줄입니다. | 일반 사용자에 대한 계정 잠금을 설정하는 방법 [38] |
| 모든 사용자에 대해 `cusa` 감사 클래스를 미리 선택합니다. | 시스템의 잠재적 위협에 대해 보다 효과적인 모니터링 및 레코딩 기능을 제공합니다. | 로그인/로그아웃 이외의 중요 이벤트를 감사하는 방법 [41] |

| 작업 | 설명 | 수행 방법 |
|---|---|---|
| 역할을 만듭니다. | 한 명의 사용자가 시스템을 손상시킬 수 없도록 여러 신뢰할 수 있는 사용자에게 고유한 관리 작업을 분배합니다.<br><br>미리 정의된 ARMOR 역할을 사용하거나, 직접 역할을 만들거나, 자신의 역할로 ARMOR를 확장할 수 있습니다. | "Oracle Solaris 11.2의 사용자 계정 및 사용자 환경 관리 "의 "CLI를 사용하여 사용자 계정 관리"<br><br>"Oracle Solaris 11.2의 사용자 및 프로세스 보안 "의 "사용자에게 권한 지정" |
| 표시 가능한 GNOME 데스크탑 응용 프로그램 수를 줄입니다. | 사용자가 보안에 영향을 줄 수 있는 데스크탑 응용 프로그램을 사용하지 못하도록 방지합니다. | "Oracle Solaris 11.2 데스크탑 관리자 설명서 "의 11 장, "Oracle Solaris Desktop 시스템의 기능 사용 안함"을 참조하십시오. |
| 사용자의 권한을 제한합니다. | 사용자에게 필요하지 않은 기본 권한을 제거합니다. | 사용자의 불필요한 기본 권한을 제거하는 방법 [41] |

# ▼ 보다 강력한 암호 제약 조건을 설정하는 방법

기본값이 사용자의 사이트 보안 요구 사항을 충족하지 못할 경우 이 절차를 수행합니다. 단계는 `/etc/default/passwd` 파일의 변수 항목 순서에 따릅니다.

**시작하기 전에** `solaris.admin.edit/etc/default/passwd` 권한 부여가 지정된 관리자여야 합니다. 자세한 내용은 "Oracle Solaris 11.2의 사용자 및 프로세스 보안 "의 "지정된 관리 권한 사용"을 참조하십시오.

- **`/etc/default/passwd` 파일에서 다음을 변경하려면 `pfedit` 명령을 사용하십시오.**

  a. **사용자가 3주~4개월마다 암호를 변경하도록 요구합니다.**

  ```
  ## /etc/default/passwd
  ##
  #MAXWEEKS=
  #MINWEEKS=
  MAXWEEKS=13
  MINWEEKS=3
  ```

  b. **최소 8자 이상의 암호를 요구합니다.**

  ```
  #PASSLENGTH=6
  PASSLENGTH=8
  ```

  c. **암호 기록을 유지합니다.**

  ```
  #HISTORY=0
  HISTORY=10
  ```

  d. **이전 암호와 최소한의 차이를 요구합니다.**

  ```
  #MINDIFF=3
  ```

```
MINDIFF=4
```

e. **최소한 1자 이상의 대문자를 요구합니다.**

```
#MINUPPER=0
MINUPPER=1
```

f. **최소한 1자 이상의 숫자를 요구합니다.**

```
#MINDIGIT=0
MINDIGIT=1
```

참조
- 암호 만들기를 제약하는 변수 목록은 passwd(1) 매뉴얼 페이지를 참조하십시오.
- 설치 후 적용되는 암호 제약 조건은 "시스템 액세스가 제한되고 모니터됨" [13]을 참조하십시오.

## ▼ 일반 사용자에 대한 계정 잠금을 설정하는 방법

로그인 시도가 특정 횟수만큼 실패한 후 일반 사용자 계정을 잠그려면 이 절차를 수행합니다.

**참고** - 역할은 공유 계정입니다. 잠긴 사용자가 역할을 잠글 수 있으므로 역할을 맡을 수 있는 사용자에 대해 계정 잠금을 설정하지 마십시오.

시작하기 전에 관리 작업을 수행하기 위해 사용하는 시스템에서 이 시스템 차원의 보호를 설정하지 마십시오. 대신 관리자가 계속 사용할 수 있도록 관리 시스템의 비정상적인 사용을 모니터링합니다.

root 역할을 가져야 합니다. 자세한 내용은 "Oracle Solaris 11.2의 사용자 및 프로세스 보안"의 "지정된 관리 권한 사용"을 참조하십시오.

1. **LOCK_AFTER_RETRIES 보안 속성을 YES로 설정합니다.**
   속성 값 범위를 선택합니다.

   - **시스템 차원 설정**
     이 보호는 시스템 사용을 시도하는 모든 사용자에게 적용됩니다.

     ```
     # pfedit /etc/security/policy.conf
     ...
     #LOCK_AFTER_RETRIES=NO
     LOCK_AFTER_RETRIES=YES
     ...
     ```

   - **사용자별 설정**
     이 보호는 이 명령을 실행한 사용자에게만 적용됩니다. 사용자가 여러 명인 경우 확장 가능한 솔루션이 아닙니다.

```
# usermod -K lock_after_retries=yes username
```

■ **권한 프로파일을 만들고 지정합니다.**

이 보호는 이 권한 프로파일을 지정한 모든 사용자 또는 시스템에 적용됩니다.

a. **권한 프로파일을 만듭니다.**

```
# profiles -p shared-profile -S ldap
shared-profile: set lock_after_retries=yes
...
```

권한 프로파일 만들기에 대한 자세한 내용은 "Oracle Solaris 11.2의 사용자 및 프로세스 보안 "의 "권한 프로파일 및 권한 부여 만들기"를 참조하십시오.

b. **사용자 또는 시스템 차원에 권한 프로파일을 지정합니다.**

여러 사용자가 권한 프로파일을 공유하는 경우 권한 프로파일에서 이 값을 설정하는 것은 확장 가능한 솔루션이 될 수 있습니다.

```
# usermod -P shared-profile username
```

또한 `policy.conf` 파일에서 시스템당 프로파일을 지정할 수도 있습니다.

```
# pfedit /etc/security/policy.conf
...
#PROFS_GRANTED=Basic Solaris User
PROFS_GRANTED=shared-profile,Basic Solaris User
```

2. **RETRIES 보안 속성을 3으로 설정합니다.**

속성 값 범위를 선택합니다.

■ **시스템 차원 설정**

```
# pfedit /etc/default/login
...
#RETRIES=5
RETRIES=3
...
```

■ **사용자별 설정**

```
# usermod -K lock_after_retries=3 username
```

■ **권한 프로파일을 만들고 지정합니다.**

1.3단계의 단계에 따라 `lock_after_retries=3`을 포함하는 권한 프로파일을 만듭니다.

참조 ■ 사용자 및 역할 보안 속성에 대한 자세한 내용은 "Oracle Solaris 11.2의 사용자 및 프로세스 보안 "의 8 장, "Oracle Solaris 권한에 대한 참조"를 참조하십시오.

- 선택한 매뉴얼 페이지에는 policy.conf(4), profiles(1), user_attr(4), usermod(1M)가 포함됩니다.

## ▼ 일반 사용자에 대해 더 제한적인 umask 값을 설정하는 방법

umask 유틸리티는 사용자가 만든 파일의 파일 권한 비트를 설정합니다. 기본값인 umask 값 022가 충분히 제한적이지 않으면 이 절차에 따라 보다 제한적인 마스크를 설정합니다.

**시작하기 전에** 골격 파일에 대한 편집 권한이 부여된 관리자여야 합니다. root 역할에서 이러한 권한을 부여합니다. 자세한 내용은 "Oracle Solaris 11.2의 사용자 및 프로세스 보안 "의 "지정된 관리 권한 사용"을 참조하십시오.

1. **다음은 Oracle Solaris에서 사용자 셸 기본값을 제공하는 샘플 파일입니다.**

```
# ls -1a /etc/skel
.bashrc
.profile
local.cshrc
local.login
local.profile
```

2. **/etc/skel 파일에서 사용자에게 지정할 umask 값을 설정합니다.**

   다음 값 중 하나를 선택합니다.

   - umask 026 - 중간 수준의 파일 보호를 제공합니다.
     (751) - 그룹은 r, 기타는 x
   - umask 027 - 엄격한 파일 보호를 제공합니다.
     (750) - 그룹은 r, 기타는 액세스할 수 없음
   - umask 077 - 완전한 파일 보호를 제공합니다.
     (700) - 그룹 및 기타에 대한 액세스 권한이 제공되지 않습니다.

**참조** 자세한 내용은 다음을 참조하십시오.

- "Oracle Solaris 11.2의 사용자 계정 및 사용자 환경 관리 "의 "CLI를 사용하여 사용자 계정 관리"
- "Oracle Solaris 11.2의 파일 보안 및 파일 무결성 확인 "의 "기본 umask 값"
- 선택한 매뉴얼 페이지에는 useradd(1M) 및 umask(1)가 포함됩니다.

## ▼ 로그인/로그아웃 이외의 중요 이벤트를 감사하는 방법

이 절차에 따라 관리 명령, 시스템 액세스 및 사이트 보안 정책에 의해 지정된 기타 중요 이벤트를 감사합니다.

**참고** - 이 절차의 예로는 사용자의 보안 정책을 만족시키는 데 충분하지 않을 수 있습니다.

**시작하기 전에** `root` 역할을 가져야 합니다. 자세한 내용은 "Oracle Solaris 11.2의 사용자 및 프로세스 보안"의 "지정된 관리 권한 사용"을 참조하십시오.

1. **관리 권한 프로파일 및 역할이 지정된 사용자별로 권한 있는 명령의 사용을 모두 감사합니다.**
   `cusa` 감사 클래스를 사전 선택 마스크에 추가합니다.

   ```
   # usermod -K audit_flags=cusa:no username
   ```

   ```
   # rolemod -K audit_flags=cusa:no rolename
   ```

   `cusa` 메타 클래스에 포함된 감사 클래스가 `/etc/security/audit_class` 파일에 나열되는지 감사합니다.

2. **인수를 감사된 명령에 기록합니다.**

   ```
   # auditconfig -setpolicy +argv
   ```

3. **(옵션) 감사된 명령이 실행되는 환경을 기록합니다.**

   ```
   # auditconfig -setpolicy +arge
   ```

**참고** - 이 정책 옵션은 문제 해결 시 유용할 수 있습니다.

**참조**

- 감사 정책에 대한 자세한 내용은 "Oracle Solaris 11.2의 감사 관리 "의 "감사 정책"을 참조하십시오.
- 감사 플래그 설정의 예는 "Oracle Solaris 11.2의 감사 관리 "의 "감사 서비스 구성" 및 "Oracle Solaris 11.2의 감사 관리 "의 "감사 서비스 문제 해결"을 참조하십시오.
- `auditconfig`(1M) 매뉴얼 페이지

## ▼ 사용자의 불필요한 기본 권한을 제거하는 방법

특정 환경에서는 일반 사용자 또는 guest 사용자의 기본 세트에서 일부 기본 권한을 제거할 수 있습니다. 예를 들어 Sun Ray 사용자가 소유하지 않은 프로세스의 상태를 확인할 수 없도록 방지할 수 있습니다.

**시작하기 전에** `root` 역할을 가져야 합니다. 자세한 내용은 "Oracle Solaris 11.2의 사용자 및 프로세스 보안"의 "지정된 관리 권한 사용"을 참조하십시오.

1. **기본 권한 세트의 전체 정의를 나열합니다.**
   다음 세 가지 기본 권한을 제거할 수 있습니다.

```
% ppriv -lv basic
file_link_any
 Allows a process to create hardlinks to files owned by a uid
 different from the process' effective uid.
...
proc_info
 Allows a process to examine the status of processes other
 than those it can send signals to.  Processes which cannot
 be examined cannot be seen in /proc and appear not to exist.
proc_session
 Allows a process to send signals or trace processes outside its
 session.
...
```

2. **권한 제거 범위를 선택합니다.**

   - **시스템 차원 설정**
     시스템 사용을 시도하는 모든 사용자에게는 이러한 권한이 거부됩니다. 이 권한 제거 방법은 공개적으로 사용 가능한 컴퓨터에 적합할 수 있습니다.

```
# pfedit /etc/security/policy.conf
...
#PRIV_DEFAULT=basic
PRIV_DEFAULT=basic,!file_link_any,!proc_info,!proc_session
```

   - **개별 사용자의 권한을 제거합니다.**
     - **사용자가 소유하지 않는 파일에 사용자가 연결하지 못하도록 방지합니다.**

```
# usermod -K 'defaultpriv=basic,!file_link_any' user
```

     - **사용자가 소유하지 않는 프로세스를 사용자가 조사하지 못하도록 방지합니다.**

```
# usermod -K 'defaultpriv=basic,!proc_info' user
```

     - **ssh 세션을 시작하는 것과 같이 사용자가 현재 세션에서 두번째 세션을 시작하지 못하도록 방지합니다.**

```
# usermod -K 'defaultpriv=basic,!proc_session' user
```

     - **사용자의 기본 세트에서 세 가지 모든 권한을 제거합니다.**

```
# usermod -K 'defaultpriv=basic,!file_link_any,!proc_info,!proc_session' user
```

   - **권한 프로파일을 만들고 지정합니다.**
     이 보호는 이 권한 프로파일을 지정한 모든 사용자 또는 시스템에 적용됩니다.

a. **권한 프로파일을 만듭니다.**

```
# profiles -p shared-profile -S ldap
shared-profile: set defaultpriv=basic,!file_link_any,!proc_info,!proc_session
...
```

권한 프로파일 만들기에 대한 자세한 내용은 "Oracle Solaris 11.2의 사용자 및 프로세스 보안 "의 "권한 프로파일 및 권한 부여 만들기"를 참조하십시오.

b. **사용자 또는 시스템 차원에 권한 프로파일을 지정합니다.**

Sun Ray 또는 원격 사용자 등 여러 사용자가 권한 프로파일을 공유하는 경우 권한 프로파일에서 이 값을 설정하는 것은 확장 가능한 솔루션이 될 수 있습니다.

```
# usermod -P shared-profile username
```

또한 `policy.conf` 파일에서 시스템당 프로파일을 지정할 수도 있습니다.

```
# pfedit /etc/security/policy.conf
...
#PROFS_GRANTED=Basic Solaris User
PROFS_GRANTED=shared-profile,Basic Solaris User
```

참조 자세한 내용은 "Oracle Solaris 11.2의 사용자 및 프로세스 보안 "의 1 장, "권한을 사용하여 사용자 및 프로세스 제어 정보" 및 `privileges`(5) 매뉴얼 페이지를 참조하십시오.

# 네트워크 보호

이 때, 역할을 가정할 수 있는 사용자를 만들고 역할을 만들었을 수 있습니다.

다음 네트워크 작업에서 사이트 요구 사항에 따라 추가 보안을 제공하는 작업을 수행합니다. 이러한 네트워크 작업은 IP, ARP 및 TCP 프로토콜을 강화합니다.

**표 2-3** 네트워크 구성 작업 맵

| 작업 | 설명 | 수행 방법 |
|---|---|---|
| 네트워크 경로 지정 데몬을 사용 안함으로 설정합니다. | 잠재적인 네트워크 스니퍼에 의한 시스템 액세스를 제한합니다. | "Oracle Solaris 11.2의 네트워크 보안 "의 "네트워크 경로 지정 데몬을 사용 안함으로 설정하는 방법" |
| 네트워크 토폴로지 정보에 대한 배포를 방지합니다. | 패킷 브로드캐스트를 방지합니다. | "Oracle Solaris 11.2의 네트워크 보안 "의 "브로드캐스트 패킷 전달을 사용 안함으로 설정하는 방법" |
| | 브로드캐스트 에코 요청 및 멀티캐스트 에코 요청에 대한 응답을 방지합니다. | "Oracle Solaris 11.2의 네트워크 보안 "의 "에코 요청에 대한 응답을 사용 안함으로 설정하는 방법" |

| 작업 | 설명 | 수행 방법 |
| --- | --- | --- |
| 다른 도메인에 대한 게이트웨이인 시스템(예: 방화벽 또는 VPN 노드)의 경우 엄격한 소스 및 대상 다중 홈 지정을 설정합니다. | 헤더의 게이트웨이 주소를 포함하지 않는 패킷이 게이트웨이 외부로 이동하지 않도록 방지합니다. | "Oracle Solaris 11.2의 네트워크 보안 "의 "엄격한 다중 홈 지정을 설정하는 방법" |
| 완전하지 않은 시스템 연결 개수를 제한하여 DoS(서비스 거부) 공격을 방지합니다. | TCP 리스너에 대해 완전하지 않은 TCP 연결의 허용 가능한 개수를 제한합니다. | "Oracle Solaris 11.2의 네트워크 보안 "의 "완전하지 않은 TCP 연결의 최대 개수를 설정하는 방법" |
| 허용된 수신 연결 개수를 제한하여 DoS 공격을 방지합니다. | TCP 리스너에 대한 보류 중인 TCP 연결의 기본 최대 개수를 지정합니다. | "Oracle Solaris 11.2의 네트워크 보안 "의 "보류 중인 TCP 연결의 최대 개수를 설정하는 방법" |
| 네트워크 매개변수를 해당 보안 기본값으로 반환합니다. | 관리 작업으로 줄어든 보안을 늘립니다. | "Oracle Solaris 11.2의 네트워크 보안 "의 "네트워크 매개변수를 보안 값으로 재설정하는 방법" |
| 네트워크 서비스에 TCP 래퍼를 추가하여 응용 프로그램을 적합한 사용자로 제한합니다. | 네트워크 서비스에 대해 액세스가 허용되는 시스템을 지정합니다(예: FTP). | TCP 래퍼 사용 방법 |
| 방화벽을 구성합니다. | IP 필터 기능을 사용하여 방화벽을 제공합니다. | "Oracle Solaris 11.2의 네트워크 보안 "의 4 장, "Oracle Solaris의 IP 필터 정보"<br><br>"Oracle Solaris 11.2의 네트워크 보안 "의 5 장, "IP 필터 구성" |
| 암호화되고 인증된 네트워크 연결을 구성합니다. | IPsec 및 IKE를 사용하여 IPsec 및 IKE를 사용하여 공동으로 구성된 노드와 네트워크 사이의 네트워크 전송을 보호합니다. | "Oracle Solaris 11.2의 네트워크 보안 "의 7 장, "IPsec 구성"<br><br>"Oracle Solaris 11.2의 네트워크 보안 "의 9 장, "IKEv2 구성" |

# ▼ TCP 래퍼 사용 방법

다음 단계에서는 TCP 래퍼 사용 방법 또는 Oracle Solaris에서 사용하는 방법 3가지를 보여줍니다.

**시작하기 전에** TCP 래퍼를 사용하도록 프로그램을 수정하려면 `root` 역할로 전환해야 합니다.

1. **TCP 래퍼로 `sendmail` 응용 프로그램을 보호할 필요는 없습니다.**

   기본적으로 "Oracle Solaris 11.2에서의 sendmail 서비스 관리 "의 "sendmail 버전 8.12의 TCP 래퍼에 대한 지원"에 설명된 대로 TCP 래퍼로 보호됩니다.

2. **모든 `inetd` 서비스에 대해 TCP 래퍼를 사용으로 설정하려면 "Oracle Solaris 11.2의 TCP/IP 네트워크, IPMP 및 IP 터널 관리 "의 "TCP 래퍼를 사용하여 TCP 서비스에 대한 액세스를 제어하는 방법"을 참조하십시오.**

3. **FTP 네트워크 서비스는 TCP 래퍼로 보호합니다.**

   a. **`/usr/share/doc/proftpd/modules/mod_wrap.html` 모듈의 지침을 따릅니다.**

      모듈이 동적이므로 FTP에 TCP 래퍼를 사용하려면 로드해야 합니다.

b. **다음 지침에 따라 `proftpd.conf` 파일에 모듈을 로드하십시오.**

```
# pfedit /etc/proftpd.conf
<IfModule mod_dso.c>
    LoadModule mod_wrap.c
</IfModule>
```

c. **FTP 서비스를 다시 시작합니다.**

```
# svcadm restart svc:/network/ftp
```

# 파일 시스템 보호

ZFS 파일 시스템은 크기가 소형이고 암호화 및 압축할 수 있으며 예약된 공간 및 디스크 공간 쿼터를 사용하여 구성할 수 있습니다.

`tmpfs` 파일 시스템은 제한 없이 증가할 수 있습니다. DoS(서비스 거부) 공격을 방지하기 위해서는 `tmpfs` 파일 시스템의 크기를 제한하는 방법 [45]을 완료하십시오.

다음 작업에서는 `tmpfs`의 크기 제한을 구성하고 Oracle Solaris의 기본 파일 시스템인 ZFS에서 제공되는 보호 수단에 대해 개괄적으로 이해할 수 있습니다. 자세한 내용은 "Oracle Solaris 11.2의 ZFS 파일 시스템 관리 "의 "ZFS 쿼터 및 예약 설정" 및 `zfs`(1M) 매뉴얼 페이지를 참조하십시오.

**표 2-4** 파일 시스템 보호 작업 맵

| 작업 | 설명 | 수행 방법 |
|---|---|---|
| 디스크 공간을 관리 및 보존하여 DoS 공격을 방지합니다. | 사용자나 그룹 또는 프로젝트별로 파일 시스템의 디스크 공간 사용을 지정합니다. | "Oracle Solaris 11.2의 ZFS 파일 시스템 관리 "의 "ZFS 쿼터 및 예약 설정" |
| 데이터 세트 및 해당 종속 요소에 최소한의 디스크 공간을 보장합니다. | 파일 시스템, 사용자나 그룹 또는 프로젝트별로 디스크 공간을 보장합니다. | "Oracle Solaris 11.2의 ZFS 파일 시스템 관리 "의 "ZFS 파일 시스템에 대한 예약 설정" |
| 파일 시스템에서 데이터를 암호화합니다. | 데이터베이스를 만들 때 데이터 세트에 액세스하기 위한 문장암호 및 암호화를 사용하여 데이터 세트를 보호합니다. | "Oracle Solaris 11.2의 ZFS 파일 시스템 관리 "의 "ZFS 파일 시스템 암호화"<br><br>"Oracle Solaris 11.2의 ZFS 파일 시스템 관리 "의 "ZFS 파일 시스템 암호화의 예" |
| `tmpfs` 파일 시스템의 크기를 제한합니다. | 악의적인 사용자가 시스템 속도를 느리게 만들기 위해 `/tmp`에 큰 파일을 만들지 못하도록 방지합니다. | `tmpfs` 파일 시스템의 크기를 제한하는 방법 [45] |

## ▼ `tmpfs` 파일 시스템의 크기를 제한하는 방법

`tmpfs` 파일 시스템의 크기는 기본적으로 제한되지 않습니다. 따라서 `tmpfs`가 사용 가능한 시스템 메모리 및 스왑을 채울 수 있습니다. `/tmp` 디렉토리는 모든 응용 프로그램 및 사용자에

의해 사용되므로 응용 프로그램이 사용 가능한 모든 시스템 메모리를 차지할 수 있습니다. 마찬가지로 악의적인 의도를 갖고 있는 권한이 없는 사용자가 /tmp 디렉토리에 큰 파일을 만들어서 시스템 속도를 느리게 만들 수 있습니다. 성능 영향을 방지하기 위해서는 각 tmpfs 마운트의 크기를 제한할 수 있습니다.

최상의 시스템 성능을 얻기 위해 여러 값을 시도해볼 수 있습니다.

**시작하기 전에** vfstab 파일을 편집하려면 solaris.admin.edit/etc/vfstab 권한 부여가 지정된 관리자여야 합니다. 시스템을 재부트하려면 사용자에게 Maintenance and Repair 권한 프로파일이 지정되어 있어야 합니다. root 역할에는 이러한 권한이 모두 있습니다. 자세한 내용은 "Oracle Solaris 11.2의 사용자 및 프로세스 보안 "의 "지정된 관리 권한 사용"을 참조하십시오.

1. **시스템의 메모리 양을 확인합니다.**

   **참고** - 다음 예에 사용되는 SPARC T3 시리즈 시스템에는 더 신속한 I/O를 위한 SSD(Solid State Disk)와 8개의 279.40MB 디스크가 있습니다. 시스템 메모리는 약 500GB입니다.

   ```
   % prtconf | head
   System Configuration:  Oracle Corporation  sun4v
   Memory size: 523776 Megabytes
   System Peripherals (Software Nodes):

   ORCL,SPARC-T3-4
   scsi_vhci, instance #0
   disk, instance #4
   disk, instance #5
   disk, instance #6
   disk, instance #8
   ```

2. **tmpfs의 메모리 제한을 계산합니다.**

   시스템 메모리 크기에 따라 큰 시스템에서는 메모리 제한을 20% 정도로 계산하고 작은 시스템에서는 30% 정도로 계산할 수 있습니다.

   따라서 작은 시스템에서는 배수로 .30을 사용합니다.

   ```
   10240M x .30 ≈ 340M
   ```

   큰 시스템에서는 배수로 .20을 사용합니다.

   ```
   523776M x .20 ≈ 10475M
   ```

3. **/etc/vfstab 파일에서 swap 항목을 해당 크기 제한으로 수정합니다.**

   ```
   # pfedit /etc/vfstab
   #device     device       mount       FS      fsck    mount mount
   #to mount   to fsck      point       type    pass    at boot options
   #
   ...
   #swap       -            /tmp        tmpfs   -       yes     -
   ```

```
swap        -           /tmp        tmpfs   -       yes     size=10400m
/dev/zvol/dsk/rpool/swap   -      -  swap    -       no      -
```

4. **시스템을 재부트합니다.**

```
# reboot
```

5. **크기 제한이 적용되었는지 확인합니다.**

```
% mount -v
swap on /system/volatile type tmpfs
read/write/setuid/devices/rstchown/xattr/dev=89c0006 on Tues Feb 4 14:07:27 2014
swap on /tmp type tmpfs
read/write/setuid/devices/rstchown/xattr/size=10400m/dev=89c0006 on Tues ...
```

6. **메모리 사용량을 모니터하고 사이트 요구 사항에 맞게 조정합니다.**

   df 명령이 유용할 수 있습니다. swap 명령은 가장 유용한 통계를 제공합니다.

```
% df -h /tmp
Filesystem Size Used Available Capacity Mounted on
swap          7.  4G     44M    7.4G 1%       /tmp

% swap -s
total: 190248k bytes allocated + 30348k reserved = 220596k used,
7743780k available
```

   자세한 내용은 tmpfs(7FS), mount_tmpfs(1M), df(1M) 및 swap(1M) 매뉴얼 페이지를 참조하십시오.

# 파일 보호 및 수정

기본적으로 root 역할만 시스템 파일 권한을 수정할 수 있습니다. solaris.admin.edit/*path-to-system-file* 권한이 지정된 역할 및 사용자는 해당 *system-file*을 수정할 수 있습니다. root 역할만 모든 파일을 검색할 수 있습니다.

**표 2-5** 파일 보호 및 수정 작업 맵

| 작업 | 설명 | 수행 방법 |
|---|---|---|
| 일반 사용자에 대해 제한적인 파일 권한을 구성합니다. | 일반 사용자의 파일 권한에 대해 022보다 제한적인 값을 설정합니다. | 일반 사용자에 대해 더 제한적인 umask 값을 설정하는 방법 [40] |
| 일반 UNIX 파일 권한보다 세부적인 수준으로 파일을 보호하려면 ACL을 지정합니다. | 확장된 보안 속성은 파일을 보호하는 데 유용할 수 있습니다.<br><br>ACL 사용에 대한 주의 사항은 Hiding Within the Trees (http://www.usenix.org/publications/login/2004-02/pdfs/brunette.pdf)를 참조하십시오. | ZFS End-to-End Data Integrity (http://blogs.oracle.com/bonwick/entry/zfs_end_to_end_data) |

| 작업 | 설명 | 수행 방법 |
| --- | --- | --- |
| 시스템 파일 무결성을 유지 관리합니다. | 스크립트 또는 BART를 사용하여 허위 파일을 찾습니다. | “Oracle Solaris 11.2의 파일 보안 및 파일 무결성 확인 ”의 “특수 파일 사용 권한이 있는 파일을 찾는 방법” |

# 시스템 액세스 및 사용 보안

Oracle Solaris 보안 기능을 구성하여 시스템 및 네트워크의 응용 프로그램 및 서비스 등의 시스템 사용을 보호할 수 있습니다.

**표 2-6** 시스템 액세스 및 사용 보안 작업 맵

| 작업 | 설명 | 수행 방법 |
| --- | --- | --- |
| 프로그램이 실행 가능한 스택을 악용할 수 없도록 방지합니다. | 실행 가능한 스택을 악용하는 버퍼 오버플로우 악용을 방지하도록 시스템 변수를 설정합니다. | “Oracle Solaris 11.2의 파일 보안 및 파일 무결성 확인 ”의 “보안 손상으로부터 실행 파일 보호” |
| ASLR(주소 공간 레이아웃 임의 지정) 태그가 지정된 이진에서 ASLR을 사용할 수 있는지 확인합니다. | 태그가 지정된 이진에 대해 ASLR을 사용으로 설정합니다. | ASLR의 사용 설정 여부 확인 방법 [31] |
| 감사를 구성합니다. | 적용 범위 및 파일 무결성에 대한 구성을 사용자 정의합니다. | “감사 서비스 사용” [52] |
| 중요한 정보가 포함될 수 있는 코어 파일을 보호합니다. | 코어 파일 전용의 액세스가 제한된 디렉토리를 만듭니다. | “Oracle Solaris 11.2의 시스템 관리 문제 해결 ”의 “파일 경로 사용으로 설정”<br><br>“Oracle Solaris 11.2의 시스템 관리 문제 해결 ”의 “코어 파일 사양 관리” |
| SSL 커널 프록시로 웹 서버를 보호합니다. | SSL(Secure Sockets Layer) 프로토콜을 사용하여 웹 서버 통신을 암호화 및 가속화할 수 있습니다. | “Oracle Solaris 11.2의 네트워크 보안 ”의 3 장, “웹 서버 및 Secure Sockets Layer 프로토콜” |
| 응용 프로그램을 포함할 영역을 만듭니다. | 영역은 프로세스를 구분하는 컨테이너입니다. 응용 프로그램과 응용 프로그램의 일부를 격리할 수 있습니다. 예를 들어, 영역을 사용하여 웹 사이트의 데이터베이스를 사이트의 웹 서버와 구분할 수 있습니다. | “Oracle Solaris 영역 소개 ” |
| 영역에서 리소스를 관리합니다. | 영역은 영역 리소스 관리를 위한 다양한 도구를 제공합니다. | “Oracle Solaris 11.2의 리소스 관리 ” |

## SMF로 레거시 서비스 보호

Oracle Solaris의 SMF(서비스 관리 기능) 기능에 응용 프로그램을 추가하고, 서비스 시작, 새로 고침 및 중지 권한을 요구하여 신뢰할 수 있는 사용자 또는 역할로 응용 프로그램 구성을 제한할 수 있습니다.

자세한 내용 및 절차를 보려면 다음을 참조하십시오.

- “Oracle Solaris 11.2의 사용자 및 프로세스 보안 ”의 “확장 권한을 사용하여 리소스 잠금”

- Securing MySQL using SMF - the Ultimate Manifest (http://blogs.oracle.com/bobn/entry/securing_mysql_using_smf_the).
- 선택된 매뉴얼 페이지에는 `smf`(5), `smf_security`(5), `svcadm`(1M), `svcbundle`(1M) 및 `svccfg`(1M)이 포함됩니다.

## Kerberos 네트워크 구성

Kerberos 서비스를 사용하여 네트워크를 보호할 수 있습니다. 클라이언트-서버 아키텍처는 네트워크에서 보안 트랜잭션을 제공합니다. 이 서비스는 무결성 및 프라이버시를 비롯하여 강력한 사용자 인증을 제공합니다. Kerberos 서비스를 사용하면 다른 시스템에 로그인하고, 명령을 실행하고, 데이터를 교환하고, 파일을 안전하게 전송할 수 있습니다. 또한 서비스를 통해 관리자가 서비스 및 시스템에 대한 액세스를 제한할 수 있습니다. Kerberos 사용자는 자신의 계정에 대한 다른 사용자의 액세스를 제한할 수 있습니다.

자세한 내용 및 절차를 보려면 다음을 참조하십시오.

- "Oracle Solaris 11.2의 Kerberos 및 기타 인증 서비스 관리 "의 3 장, "Kerberos 서비스 계획"
- "Oracle Solaris 11.2의 Kerberos 및 기타 인증 서비스 관리 "의 4 장, "Kerberos 서비스 구성"
- 선택한 매뉴얼 페이지에는 `kadmin`(1M), `pam_krb5`(5) 및 `kclient`(1M)가 포함됩니다.

# 레이블이 있는 다중 레벨 보안

Trusted Extensions는 레이블 기반의 MAC(필수 액세스 제어) 정책을 사용하여 Oracle Solaris 보안을 확장합니다. 민감도 레이블은 모든 데이터 소스(네트워크, 파일 시스템 및 창) 및 데이터 소비자(사용자 및 프로세스)에 자동으로 적용됩니다. 모든 데이터에 대한 액세스는 데이터 레이블(객체) 및 소비자(주체) 사이의 관계에 따라 제한됩니다. 계층화된 기능은 레이블을 인식하는 서비스 세트로 구성됩니다.

Trusted Extensions 서비스의 부분 목록에는 다음이 포함됩니다.

- 레이블이 있는 네트워킹
- 레이블 인식 파일 시스템 마운트 및 공유
- 레이블이 있는 데스크탑
- 레이블 구성 및 번역
- 레이블 인식 시스템 관리 도구
- 레이블 인식 장치 할당

`system/trusted` 및 `system/trusted/trusted-global-zone` 패키지는 다중 레벨 데스크탑이 필요하지 않은 서버 또는 헤드리스 시스템에 충분합니다. `system/trusted/trusted-`

`extensions` 패키지는 신뢰할 수 있는 Oracle Solaris 다중 레벨 데스크탑 환경을 제공합니다.

## Trusted Extensions 구성

Trusted Extensions 패키지를 설치한 후 시스템을 구성해야 합니다. `trusted-extensions` 패키지 설치 시 시스템에서는 랩탑 또는 워크스테이션과 같이 직접 연결된 비트맵 디스플레이를 사용하여 데스크탑을 실행할 수 있습니다. 다른 시스템과 통신하려면 네트워크 구성이 필요합니다.

자세한 내용 및 절차를 보려면 다음을 참조하십시오.

- “Trusted Extensions 구성 및 관리 ”의 제I부, “Trusted Extensions의 초기 구성”
- “Trusted Extensions 구성 및 관리 ”의 제II부, “Trusted Extensions 관리”

## 레이블이 있는 IPsec 구성

IPsec를 사용하여 레이블이 있는 패킷을 보호할 수 있습니다.

자세한 내용 및 절차를 보려면 다음을 참조하십시오.

- “Oracle Solaris 11.2의 네트워크 보안 ”의 6 장, “IP Security Architecture 정보”
- “Trusted Extensions 구성 및 관리 ”의 “레이블이 있는 IPsec 관리”
- “Trusted Extensions 구성 및 관리 ”의 “레이블이 있는 IPsec 구성”

♦ ♦ ♦ 3 장

# 3 Oracle Solaris 보안 유지 관리 및 모니터링

초기 설치 및 구성 후 다음 절차에 따라 시스템의 보안 체계를 유지 관리 및 모니터링할 수 있습니다.

- 정기적인 감사 레코드 검토
- 패키지 및 파일 무결성 검사 실행
- 네트워크 활동 모니터링
- 준수 검사 실행

## 시스템 보안 유지 관리 및 모니터링

다음은 시스템, 데이터 및 사이트의 보안 요구 사항 준수 여부에 대한 액세스 및 사용을 유지 관리 및 모니터링하는 작업입니다.

**표 3-1** 시스템 유지 관리 및 모니터링 작업 맵

| 작업 | 설명 | 수행 방법 |
|---|---|---|
| 시스템에서 패키지를 확인합니다. | 업데이트 후 패키지가 소스 패키지와 동일한지 여부를 확인합니다. | 패키지 확인 방법 [30] |
| 파일 무결성을 확인합니다. | 구성 후 정기적으로 BART 매니페스트를 비교하여 변경해야 할 파일만 변경되었는지 확인합니다. | “BART를 사용하여 파일 무결성 확인” [52] |
| 허위 파일을 찾습니다. | 프로그램에서 무단 사용의 가능성이 있는 `setuid` 및 `setgid` 권한을 찾습니다. | “Oracle Solaris 11.2의 파일 보안 및 파일 무결성 확인 ”의 “특수 파일 사용 권한이 있는 파일을 찾는 방법” |
| 정기적으로 감사 로그를 검토합니다. | 비정상적인 시스템 액세스 및 사용을 찾습니다. | “감사 서비스 사용” [52] |
| 로그인 및 로그아웃 이벤트에 대한 감사 로그를 실시간으로 검토합니다. | 침해 시도가 발생한 경우 즉시 이를 식별합니다. | “실시간으로 감사 레코드 모니터링” [53] |
| 준수 테스트를 실행합니다. | 시스템에서 보안 벤치마크를 준수하는지 평가합니다. | “Oracle Solaris 11.2 보안 적합성 안내서 ” 및 `compliance`(1M) 매뉴얼 페이지 |

# BART를 사용하여 파일 무결성 확인

BART는 암호화 강도 해시 및 파일 시스템 메타 데이터를 사용하여 변경 사항을 보고하는 규칙 기반 파일 무결성 검사 및 보고 도구입니다.

자세한 내용 및 절차를 보려면 다음을 참조하십시오.

- "Oracle Solaris 11.2의 파일 보안 및 파일 무결성 확인 "의 "BART 정보"
- "Oracle Solaris 11.2의 파일 보안 및 파일 무결성 확인 "의 "BART 사용 정보"
- "Oracle Solaris 11.2의 파일 보안 및 파일 무결성 확인 "의 "BART 매니페스트, 규칙 파일 및 보고서"

설치된 시스템에 대한 변경 사항을 추적하기 위한 자세한 지침은 "Oracle Solaris 11.2의 파일 보안 및 파일 무결성 확인 "의 "시간에 따라 동일 시스템에 대한 매니페스트를 비교하는 방법"을 참조하십시오.

# 감사 서비스 사용

감사는 시스템 사용 방법에 대한 레코드를 유지 합니다. 감사 서비스에는 감사 데이터 분석을 도와주는 도구가 포함됩니다.

감사 서비스에 대해서는 "Oracle Solaris 11.2의 감사 관리 "에 설명되어 있습니다. 매뉴얼 페이지 목록과 링크는 "Oracle Solaris 11.2의 감사 관리 "의 "감사 서비스 매뉴얼 페이지"를 참조하십시오.

다음 감사 서비스 절차는 다양한 보안 환경에 유용합니다.

- 감사를 구성하고, 감사 서비스를 시작 및 중지하기 위한 역할을 개별적으로 만드십시오. 신뢰할 수 있는 사용자에게 역할을 지정합니다.

  감사 구성, 감사 검토 및 감사 제어 권한 프로파일을 자신의 역할에 대한 기본값으로 사용하십시오.

  역할을 만들거나 미리 정의된 ARMOR 역할을 사용하려면 "Oracle Solaris 11.2의 사용자 및 프로세스 보안 "의 "사용자에게 권한 지정"을 참조하십시오.
- `cusa` 감사 클래스로 모든 관리자를 감사합니다.

  `cusa` 감사 클래스의 이벤트에는 시스템의 보안 체계에 영향을 주는 관리 작업이 포함되어 있습니다. 자세한 설명은 `/etc/security/audit_class` 파일을 참조하십시오. 절차는 로그인/로그아웃 이외의 중요 이벤트를 감사하는 방법 [41]을 참조하십시오.
- 감사 레코드를 중앙 서버로 전송합니다.
  - ARS(감사 원격 서버)와 함께 사용할 수 있도록 감사를 구성합니다.

    "Oracle Solaris 11.2의 감사 관리 "의 "원격 저장소에 감사 파일을 보내는 방법"을 참조하십시오.
  - 개별 ZFS 풀에서 감사 검토 파일 시스템에 전체 감사 파일을 안전하게 전송하도록 일정을 잡습니다.

- `syslog` 유틸리티에서 선택된 감사 이벤트에 대한 텍스트 요약을 모니터링합니다.

  `audit_syslog` 플러그인을 활성화하고 보고된 이벤트를 모니터합니다.

  "Oracle Solaris 11.2의 감사 관리 "의 "syslog 감사 로그를 구성하는 방법"을 참조하십시오.
- 감사 파일 크기를 제한합니다.

  `audit_binfile` 플러그인에 대한 `p_fsize` 속성을 유용한 크기로 설정합니다. 여러 요소들 중에서도 일정, 디스크 공간 및 `cron` 작업 빈도를 검토하십시오.

  예를 들어 "Oracle Solaris 11.2의 감사 관리 "의 "감사 추적에 대한 감사 공간을 지정하는 방법"을 참조하십시오.
- 개별 ZFS 풀에서 감사 검토 파일 시스템에 전체 감사 파일을 안전하게 전송하도록 일정을 잡습니다.
- 감사 검토 파일 시스템에서 전체 감사 파일을 검토합니다.

## 실시간으로 감사 레코드 모니터링

`audit_syslog` 플러그인을 사용하면 미리 선택한 감사 이벤트에 대한 요약을 기록할 수 있습니다. 다음과 비슷한 명령을 실행하여 생성되는 감사 요약을 터미널 창에 표시하려면 다음을 수행합니다.

```
# tail -0f  /var/adm/auditlog
```

감사 로그를 구성하려면 "Oracle Solaris 11.2의 감사 관리 "의 "syslog 감사 로그를 구성하는 방법"을 참조하십시오.

## 감사 로그 검토 및 아카이브

감사 레코드는 텍스트 형식으로 보거나 브라우저에 XML 형식으로 볼 수 있습니다.

자세한 내용 및 절차를 보려면 다음을 참조하십시오.

- "Oracle Solaris 11.2의 감사 관리 "의 "감사 로그"
- "Oracle Solaris 11.2의 감사 관리 "의 "감사 추적 오버플로우 방지"
- "Oracle Solaris 11.2의 감사 관리 "의 "감사 추적 데이터 표시"

♦ ♦ ♦ 부 록 A

# Oracle Solaris 보안 문서 목록

다음 참조 자료에는 Oracle Solaris 시스템에 대한 유용한 보안 정보가 포함되어 있습니다. Oracle Solaris의 이전 릴리스의 보안 정보에는 일부 유용한 정보와 오래된 정보가 포함됩니다.

## Oracle 기술 네트워크에 대한 보안 참조

Oracle Solaris 11 시스템의 보안에 대한 설명은 Oracle Technology Network 웹 사이트의 다음 서적 및 문서를 참조하십시오.

- “Oracle Solaris 11.2에서 시스템 및 연결된 장치의 보안 ”
- “Oracle Solaris 11.2의 파일 보안 및 파일 무결성 확인 ”
- “Oracle Solaris 11.2의 네트워크 보안 ”
- “Oracle Solaris 11.2의 사용자 및 프로세스 보안 ”
- “Oracle Solaris 11.2의 암호화 및 인증서 관리 ”
- “Oracle Solaris 11.2의 감사 관리 ”
- “Oracle Solaris 11.2의 Kerberos 및 기타 인증 서비스 관리 ”
- “Oracle Solaris 11.2의 보안 셸 액세스 관리 ”
- “Oracle Solaris 11.2 보안 적합성 안내서 ”
- “Using a FIPS 140 Enabled System in Oracle Solaris 11.2 ”

## 타사 발행물의 Oracle Solaris 보안 참조

Oracle Solaris 11 시스템의 보안에 대한 설명은 다음 서적을 참조하십시오.

- *Security Configuration Benchmark For Solaris 11 11/11 Version 1.0.0 June 11th, 2012*

  이 보안 벤치마크는 보안 커뮤니티용으로 CIS(Center for Internet Security)http://cisecurity.org/에서 출간되었습니다. 이 설명서에서는 Oracle Solaris 운영 체제에 대한 보안 설정을 권장합니다. 이 문서는 시스템 및 응용 프로그램 관리자, 보안 전문가, 감사자, 지원 엔지니어 및 Oracle Solaris용 보안 솔루션을 개발, 설치, 평가 또는 제공하

는 설치자 또는 개발자를 대상으로 합니다. 사본을 얻으려면 CIS Security Benchmarks (http://benchmarks.cisecurity.org/)를 방문하십시오.

- *Oracle Solaris 11 System Administration: The Complete Reference*. Michael Jang, Harry Foxwell, Christine Tran 및 Alan Formy-Duval. 2012. McGraw-Hill. ISBN 978007179042.

  이 서적에는 Oracle Solaris의 보안 범위가 포함되어 있습니다.
- *Oracle Solaris 11: First Look*. Philip P. Brown. 2013. Packt Publishing. ISBN 9781849688307.

  이 서적에서는 Oracle Solaris 관리자 및 해당 보안을 소개합니다.
- *Oracle Solaris 11 System Administration*, Bill Calkins. 2013. Prentice Hall. ISBN 9780133007114.

  이 서적에서는 보안 기능을 포함하여 Oracle Solaris의 새로운 기능을 다룹니다.