Oracle® Solaris 11 보안 지침

부품 번호: E25818
2012년 3월

ORACLE

120410@25097

목차

머리말

이 설명서에서는 Oracle Solaris 운영 체제(Oracle Solaris OS)에 대한 보안 지침을 제공합니다. 첫째, 이 설명서에서는 엔터프라이즈 OS에서 해결해야 하는 보안 문제에 대해 설명합니다. 그런 다음 Oracle Solaris OS의 기본 보안 기능에 대해 설명합니다. 마지막으로 시스템 강화를 위해 수행해야 하는 구체적인 단계 및 Oracle Solaris 보안 기능을 사용하여 데이터 및 응용 프로그램을 보호하는 방법에 대해 설명합니다. 이 설명서의 권장 사항을 각 사이트 보안 정책에 맞게 사용자 정의할 수 있습니다.

대상

Oracle Solaris 11 보안 지침은 보안 관리자 및 다음 작업을 수행하는 기타 관리자를 대상으로 합니다.

- 보안 요구 사항 분석
- 소프트웨어의 사이트 보안 정책 구현
- Oracle Solaris OS 설치 및 구성
- 시스템 및 네트워크 보안 유지 관리

이 설명서를 사용하려면 일반적인 UNIX 관리 지식, 확고한 소프트웨어 보안 기초, 사이트 보안 정책에 대한 지식이 있어야 합니다.

Oracle Support에 액세스

Oracle 고객은 My Oracle Support를 통해 온라인 지원에 액세스할 수 있습니다. 자세한 내용은 `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info`를 참조하거나, 청각 장애가 있는 경우 `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs`를 방문하십시오.

활자체 규약

다음 표는 이 책에서 사용되는 활자체 규약에 대해 설명합니다.

표 P–1 활자체 규약

활자체	설명	예
`AaBbCc123`	명령 및 파일, 디렉토리 이름; 컴퓨터 화면에 출력되는 내용입니다.	`.login` 파일을 편집하십시오. 모든 파일 목록을 보려면 `ls -a` 명령을 사용하십시오. `machine_name% you have mail.`
`AaBbCc123`	사용자가 입력하는 내용으로 컴퓨터 화면의 출력 내용과 대조됩니다.	`machine_name%` **`su`** `Password:`
AaBbCc123	새로 나오는 용어, 강조 표시할 용어입니다. 명령줄 변수를 실제 이름이나 값으로 바꾸십시오.	`rm` *filename* 명령을 사용하여 파일을 제거합니다.
AaBbCc123	책 제목, 장, 절	**사용자 설명서**의 6장을 읽으십시오. **캐시**는 로컬로 저장된 복사본입니다. 파일을 저장하면 **안 됩니다**. **주:** 일부 강조된 항목은 온라인에서 굵은체로 나타납니다.

명령 예의 셸 프롬프트

다음 표에는 Oracle Solaris OS에 포함된 셸의 기본 UNIX 시스템 프롬프트 및 수퍼유저 프롬프트가 나와 있습니다. 명령 예제에 표시된 기본 시스템 프롬프트는 Oracle Solaris 릴리스에 따라 다릅니다.

표 P–2 셸 프롬프트

셸	프롬프트
Bash 셸, Korn 셸 및 Bourne 셸	`$`
수퍼유저용 Bash 셸, Korn 셸 및 Bourne 셸	`#`
C 셸	`machine_name%`
수퍼유저용 C 셸	`machine_name#`

◆ ◆ ◆ 1 장

1 Oracle Solaris 11 보안 개요

Oracle Solaris 11은 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 융통성은 엔터프라이즈 서버에서 데스크탑 클라이언트에 이르는 다양한 보안 목표를 만족시킬 수 있습니다. Oracle Solaris 11은 Oracle의 다양한 SPARC 및 x86 기반 시스템 및 타사 공급업체의 다른 하드웨어 플랫폼에서 완전히 테스트되었으며 지원됩니다.

Oracle Solaris 11 보안 보호

Oracle Solaris는 디스크에 저장된 데이터 및 이동 중인 데이터를 보호하여 회사 데이터 및 응용 프로그램에 대한 확고한 기반을 제공합니다. **리소스 관리**로 참조되는 Oracle Solaris Resource Manager 및 Oracle Solaris Zones는 응용 프로그램을 구분하고 오용되지 않도록 보호하는 기능을 제공합니다. 권한을 통해 구현되는 최소 권한 및 Oracle Solaris의 RBAC(Role-Based Access Control) 기능과 함께 이러한 제한을 통해 침입자 및 일반 사용자의 작업에 대한 보안 위험을 줄일 수 있습니다. IPsec(IP 보안)와 같은 인증되고 암호화된 프로토콜은 안전한 데이터 전달을 위해 LAN 또는 WAN뿐만 아니라 인터넷을 통한 VPN(가상 사설망)을 제공합니다. 또한 Oracle Solaris의 감사 기능은 레코드의 관심 작업을 최신 상태로 유지할 수 있게 해줍니다.

Oracle Solaris 11 보안 서비스는 시스템 및 네트워크에 대한 보호 계층을 제공하여 세부적인 방어 수단을 제공합니다. Oracle Solaris는 커널 유틸리티 내에서 해당 유틸리티가 수행할 수 있는 권한이 있는 작업을 제한하여 커널을 보호합니다. 기본 네트워크 구성은 시스템 및 유선상의 데이터 보호를 제공합니다. IPsec, Oracle Solaris의 IP 필터 및 Kerberos는 추가 보호를 제공할 수 있습니다.

Oracle Solaris 보안 서비스에는 다음이 포함됩니다.

- 커널 보호 - 커널 데몬 및 장치는 파일 권한 및 권한에 의해 보호됩니다.
- 로그인 보호 - 로그인에 암호가 필요합니다. 암호는 강력한 방식으로 암호화됩니다. 원격 로그인은 처음에 Oracle Solaris의 Secure Shell 기능을 통해 암호화되고 인증된 채널로 제한됩니다. `root` 계정은 직접 로그인할 수 없습니다.
- 데이터 보호 - 디스크의 데이터는 파일 권한에 의해 보호됩니다. 추가 보호 계층을 구성할 수 있습니다. 예를 들어, ACL(액세스 제어 목록)을 사용하고, 영역에 데이터를 배치하고, 파일을 암호화하고, Oracle Solaris ZFS 데이터 집합을 만들고, 파일 시스템을 마운트하여 `setuid` 프로그램 및 실행 파일을 실행할 수 없도록 할 수 있습니다.

Oracle Solaris 11 보안 기술

Oracle Solaris의 보안 기능은 사이트의 보안 정책을 구현하도록 구성할 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.

감사 서비스

감사는 시스템 리소스 사용에 대한 데이터의 모음입니다. 감사 데이터는 보안 관련 시스템 이벤트의 레코드를 제공합니다. 그런 다음 이 데이터를 사용하여 시스템에서 발생한 작업에 대한 책임을 지정할 수 있습니다.

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

자세한 내용은 다음을 참조하십시오.

- 감사 관련 매뉴얼 페이지 목록은 **Oracle Solaris 관리: 보안 서비스**의 29 장, "감사(참조)"를 참조하십시오.
- 자세한 내용은 33 페이지 "로그온/로그아웃 이외의 중요 감사 이벤트" 및 매뉴얼 페이지를 참조하십시오.
- 감사 개요는 **Oracle Solaris 관리: 보안 서비스**의 26 장, "감사(개요)"를 참조하십시오.
- 감사 작업은 **Oracle Solaris 관리: 보안 서비스**의 28 장, "감사 관리(작업)"를 참조하십시오.

기본 감사 보고 도구

Oracle Solaris의 BART(기본 감사 보고 도구)를 사용하면 시간 경과에 따른 시스템에 대한 파일 레벨 검사를 수행하여 시스템을 포괄적으로 검증할 수 있습니다. BART 매니페스트를 만들면 배치된 시스템에 설치된 소프트웨어 스택의 구성 요소에 대한 정보를 쉽고 안정적으로 수집할 수 있습니다.

BART는 한 시스템 또는 시스템 네트워크에서 무결성 관리를 위한 유용한 도구입니다.

자세한 내용은 다음을 참조하십시오.

- 선택한 매뉴얼 페이지에는 `bart(1M)`, `bart_rules(4)` 및 `bart_manifest(4)`가 포함됩니다.
- 자세한 내용은 46 페이지 "시스템의 BART 스냅샷 만들기", 49 페이지 "기본 감사 보고 도구 사용" 및 매뉴얼 페이지를 참조하십시오.
- BART 개요는 **Oracle Solaris 관리: 보안 서비스**의 6 장, "기본 감사 보고 도구 사용(작업)"을 참조하십시오.
- BART 사용 예를 보려면 **Oracle Solaris 관리: 보안 서비스**의 "BART 사용(작업)" 및 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. 다양한 PKI(공용 키 인프라)에 대한 다른 저장소 방식, 관리 유틸리티 및 프로그래밍 인터페이스에서는 KMF 인터페이스를 채택할 경우 통합 인터페이스를 사용할 수 있습니다.

암호화 프레임워크는 개별 명령, 사용자 레벨의 프로그래밍 인터페이스, 커널 프로그래밍 인터페이스 및 사용자 레벨/커널 레벨 프레임워크를 통해 사용자 및 응용 프로그램에 암호화 서비스를 제공합니다. 암호화 프레임워크는 이러한 암호화 서비스를 일반 사용자에게 효과적인 방식으로 응용 프로그램 및 커널 모듈에 제공합니다. 또한 파일에 대한 암호화 및 암호 해독과 같은 직접적인 암호화 서비스도 일반 사용자에게 제공합니다.

KMF는 중앙에서 관리되는 공용 키 객체(예:X.509 인증서 및 공용/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)이 포함됩니다.
- 암호화 서비스에 대한 개요는 **Oracle Solaris 관리: 보안 서비스**의 11 장, "암호화 프레임워크(개요)" 및 **Oracle Solaris 관리: 보안 서비스**의 13 장, "키 관리 프레임워크"를 참조하십시오.
- 암호화 프레임워크에 대한 예는 **Oracle Solaris 관리: 보안 서비스**의 12 장, "암호화 프레임워크(작업)" 및 매뉴얼 페이지를 참조하십시오.

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 ZFS는 ACE(액세스 제어 항목)라고도 부르는 ACL(액세스 제어 목록)을 지원하여 파일 시스템 객체의 개별 항목 또는 그룹에 대한 액세스를 보다 세밀하게 제어합니다.

자세한 내용은 다음을 참조하십시오.

- ZFS에서 ACL 설정에 대한 자세한 내용은 chmod(1) 매뉴얼 페이지를 참조하십시오.
- 파일 권한에 대한 개요를 보려면 **Oracle Solaris 관리: 보안 서비스**의 "UNIX 사용 권한으로 파일 보호"을 참조하십시오.
- ZFS 파일 보호에 대한 개요 및 예를 보려면 **Oracle Solaris 관리: ZFS 파일 시스템**의 8 장, "ACL 및 속성을 사용하여 Oracle Solaris ZFS 파일 보호" 및 매뉴얼 페이지를 참조하십시오.

패킷 필터링

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

IP 필터

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.

- 선택한 매뉴얼 페이지에는 ipfilter(5), ipf(1M), ipnat(1M), svc.ipfd(1M) 및 ipf(4)가 포함됩니다.
- IP 필터에 대한 개요를 보려면 **Oracle Solaris 관리: IP 서비스**의 20 장, "Oracle Solaris의 IP 필터(개요)"를 참조하십시오.
- IP 필터 사용 예를 보려면 **Oracle Solaris 관리: IP 서비스**의 21 장, "IP 필터(작업)" 및 매뉴얼 페이지를 참조하십시오.
- IP 필터 정책 언어의 구문에 대한 자세한 내용 및 예를 보려면 ipnat(4) 매뉴얼 페이지를 참조하십시오.

TCP 래퍼

TCP 래퍼는 ACL에 대하여 특정 네트워크 서비스를 요청하는 호스트의 주소를 확인함으로써 액세스 제어를 구현하는 방식을 제공합니다. 요청은 이에 따라 허용 또는 거부됩니다. TCP 래퍼는 또한 유용한 모니터링 기능인 네트워크 서비스에 대한 호스트 요청을 기록합니다. Secure Shell 및 Oracle Solaris의 sendmail 기능은 TCP 래퍼를 사용하도록 구성됩니다. 액세스 제어하에 배치되는 네트워크 서비스에는 ftpd 및 rpcbind가 포함됩니다.

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.

자세한 내용은 다음을 참조하십시오.

- TCP 래퍼에 대한 자세한 내용은 **Oracle Solaris 관리: IP 서비스**의 "TCP 래퍼를 사용하여 TCP 서비스에 대한 액세스를 제어하는 방법"을 참조하십시오.
- TCP 래퍼의 액세스 제어 언어의 구문에 대한 자세한 내용 및 예를 보려면 hosts_access(4) 매뉴얼 페이지를 참조하십시오.

암호 및 암호 제약조건

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

Oracle Solaris에는 강력한 사용자 암호를 촉진하기 위해 사용할 수 있는 다양한 기능이 포함됩니다. 암호 길이, 내용, 변경 빈도, 수정 요구 사항을 설정하고 암호 기록을 유지할 수 있습니다. 사용하지 않아야 하는 암호에 대해서도 암호 사전이 제공됩니다. 일부 사용 가능한 암호 알고리즘도 제공됩니다.

자세한 내용은 다음을 참조하십시오.

- **Oracle Solaris 관리: 보안 서비스**의 "로그인 제어 유지 관리"
- **Oracle Solaris 관리: 보안 서비스**의 "로그인 및 암호 보안(작업)"

- 선택한 매뉴얼 페이지에는 passwd(1) 및 crypt.conf(4)가 포함됩니다.

플러그 가능한 인증 모듈

PAM(Pluggable Authentication Module) 프레임워크에서는 계정, 인증서, 세션 및 암호에 대한 사용자 인증 요구 사항을 조정하고 구성합니다.

PAM 프레임워크를 통해 조직은 계정, 세션 및 암호 관리 기능뿐만 아니라 사용자 인증 환경을 사용자 정의할 수 있습니다. login 및 ftp와 같은 시스템 입력 서비스는 PAM 프레임워크를 사용하여 시스템의 모든 입력 지점이 보안되도록 보장합니다. 이 아키텍처는 새로 발견된 취약점으로부터 시스템을 보호하기 위해 PAM 프레임워크를 사용하는 시스템 서비스를 변경하지 않고 필드에서 인증 모듈을 교체하거나 수정할 수 있게 해줍니다.

자세한 내용은 다음을 참조하십시오.

- **Oracle Solaris 관리: 보안 서비스**의 15 장, "PAM 사용"
- pam.conf(4) 매뉴얼 페이지

Oracle Solaris의 권한

권한은 커널에 강제 적용되는 프로세스에 대한 세밀하게 조정된 고유한 권한입니다. Oracle Solaris는 file_read와 같은 기본 권한에서부터 proc_clock_highres와 같은 보다 전문적인 권한까지 80개 이상의 권한을 정의합니다. 권한은 명령, 사용자, 역할 또는 시스템에 부여할 수 있습니다. 여러 Oracle Solaris 명령 및 데몬은 해당 작업을 수행하는 데 필요한 권한만 갖고 실행됩니다. 권한 사용은 **프로세스 권한 관리**라고도 부릅니다.

권한 인식 프로그램은 침입자가 프로그램 자체에서 사용하는 것보다 많은 권한을 부여하지 못하도록 방지합니다. 또한 권한을 통해 조직은 자신의 시스템에서 실행되는 서비스 및 프로세스에 부여되는 권한을 제한할 수 있습니다.

자세한 내용은 다음을 참조하십시오.

- **Oracle Solaris 관리: 보안 서비스**의 "권한(개요)"
- **Oracle Solaris 관리: 보안 서비스**의 "권한 사용(작업)"
- **Developer's Guide to Oracle Solaris 11 Security**의 2 장, "Developing Privileged Applications"
- 선택한 매뉴얼 페이지에는 ppriv(1) 및 privileges(5)가 포함됩니다.

원격 액세스

원격 액세스 공격은 시스템 및 네트워크를 손상시킬 수 있습니다. 현대의 인터넷 환경에서는 네트워크 액세스에 대한 보안이 필수적이며 WAN 및 LAN 환경에서도 네트워크 액세스 보안이 유용할 수 있습니다.

IPsec 및 IKE

IPsec(IP 보안)는 패킷을 인증 또는 암호화하거나, 두 가지를 모두 수행하여 IP 패킷을 보호합니다. Oracle Solaris는 IPv4 및 IPv6 모두에 대해 IPsec를 지원합니다. IPsec는 응용 프로그램 계층 아래에서 올바르게 구현되기 때문에 인터넷 응용 프로그램은 해당 코드를 수정할 필요 없이 IPsec를 활용할 수 있습니다.

IPsec 및 해당 키 교환 프로토콜인 IKE는 암호화 프레임워크의 알고리즘을 사용합니다. 또한 암호화 프레임워크는 메타 슬롯을 사용하는 응용 프로그램을 위해 softtoken 키 저장소를 제공합니다. IKE가 메타슬롯을 사용하도록 구성된 경우 조직에서는 키를 디스크, 연결된 하드웨어 키 저장소 또는 softtoken 키 저장소에 저장할 수 있습니다.

올바르게 관리할 경우 IPsec는 네트워크 보안 작업에 효과적으로 활용할 수 있습니다.

자세한 내용은 다음을 참조하십시오.

- **Oracle Solaris 관리: IP 서비스**의 14 장, "IP 보안 아키텍처(개요)"
- **Oracle Solaris 관리: IP 서비스**의 15 장, "IPsec 구성(작업)"
- **Oracle Solaris 관리: IP 서비스**의 17 장, "Internet Key Exchange(개요)"
- **Oracle Solaris 관리: IP 서비스**의 18 장, "IKE 구성(작업)"
- 선택한 매뉴얼 페이지에는 `ipsecconf(1M)` 및 `in.iked(1M)`이 포함됩니다.

Secure Shell

Oracle Solaris의 Secure Shell 기능을 사용하면 사용자 또는 서비스가 암호화된 통신 채널을 통해 원격 시스템 간에 파일을 액세스하거나 전송할 수 있습니다. Secure Shell에서는 모든 네트워크 트래픽이 암호화됩니다. Secure Shell는 또한 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. 기본적으로 Secure Shell는 새로 설치된 시스템에서 유일하게 활성화된 원격 액세스 방식입니다.

자세한 내용은 다음을 참조하십시오.

- **Oracle Solaris 관리: 보안 서비스**의 17 장, "Secure Shell 사용(작업)"
- 선택한 매뉴얼 페이지에는 `ssh(1)`, `sshd(1M)`, `sshd_config(4)` 및 `ssh_config(4)`가 포함됩니다.

Kerberos 서비스

Oracle Solaris의 커버로스 기능은 커버로스를 실행하는 이기종 네트워크에서도 Single Sign-On 및 보안 트랜잭션을 사용으로 설정합니다

커버로스는 MIT(Massachusetts Institute of Technology)에서 개발된 Kerberos V5 네트워크 인증 프로토콜을 기반으로 합니다. 커버로스 서비스는 네트워크에서 보안 트랜잭션을 제공하는 클라이언트-서버 구조입니다. 이 서비스는 무결성 및 프라이버시를 비롯하여

강력한 사용자 인증을 제공합니다. 커버로스 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 관리: 보안 서비스**의 제VI부, "Kerberos 서비스"
- 선택한 매뉴얼 페이지에는 `kerberos(5)` 및 `kinit(1)`이 포함됩니다.

역할 기반 액세스 제어

RBAC는 조직이 고유한 요구 및 요구 사항에 따라 사용자 또는 역할에 관리 권한을 선택적으로 부여할 수 있도록 함으로써 최소 권한의 원칙을 적용합니다.

Oracle Solaris의 RBAC(역할 기반 액세스 제어) 기능은 일반적으로는 `root` 역할로 제한되는 작업에 대한 사용자 액세스를 제어합니다. 프로세스 및 사용자에게 보안 속성을 제공하는 RBAC는 여러 관리자 간에 관리 권한을 분배할 수 있습니다. RBAC는 또한 **사용자 권한 관리**라고도 부릅니다.

자세한 내용은 다음을 참조하십시오.

- **Oracle Solaris 관리: 보안 서비스**의 제III부, "역할, 권한 프로파일 및 권한"
- 선택한 매뉴얼 페이지에는 `rbac(5)`, `roleadd(1M)`, `profiles(1)` 및 `user_attr(4)`가 포함됩니다.

Service Management Facility

Oracle Solaris의 SMF(Service Management Facility) 기능은 서비스 추가, 제거, 구성 및 관리를 위해 사용됩니다. SMF는 RBAC를 사용하여 시스템에서 Service Management Facility에 대한 액세스를 제어합니다. 특히 SMF는 권한을 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 관리: 일반 작업**의 6 장, "서비스 관리(개요)"
- **Oracle Solaris 관리: 일반 작업**의 7 장, "서비스 관리(작업)"
- 선택한 매뉴얼 페이지에는 `svcadm(1M)`, `svcs(1)` 및 `smf(5)`가 포함됩니다.

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 ACE 보호 파일 그리고 RBAC는 ZFS 데이터 집합에 대한 위임된 관리를 지원합니다.

자세한 내용은 다음을 참조하십시오.

- **Oracle Solaris 관리: ZFS 파일 시스템**의 1 장, "Oracle Solaris ZFS 파일 시스템(소개)"
- **Oracle Solaris 관리: ZFS 파일 시스템**의 3 장, "Oracle Solaris ZFS와 전통적인 파일 시스템의 차이"
- **Oracle Solaris 관리: ZFS 파일 시스템**의 6 장, "Oracle Solaris ZFS 파일 시스템 관리"
- 선택한 매뉴얼 페이지에는 `zfs(1M)` 및 `zfs(7FS)`가 포함됩니다.

Oracle Solaris Zones

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.

자세한 내용은 다음을 참조하십시오.

- **Oracle Solaris 관리: Oracle Solaris Zones, Oracle Solaris 10 Zones 및 리소스 관리**의 제II부, "Oracle Solaris Zones"
- 선택한 매뉴얼 페이지에는 `brands(5)`, `zoneadm(1M)` 및 `zonecfg(1M)`이 포함됩니다.

Trusted Extensions

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 흐름이 제한됩니다. 다른 다중 레벨 운영 체제와 달리 Trusted Extensions에는 다중 레벨 데스크탑이 포함됩니다.

Trusted Extensions는 공통 조건 LSPP(레이블이 있는 보안 보호 프로파일), RBACPP(역할 기반 액세스 보호 프로파일) 및 CAPP(제어 액세스 보호 프로파일)의 요구 사항을 충족합니다. 하지만 Trusted Extensions 구현은 호환성을 극대화하고 오버헤드를 최소화하면서 높은 보장성을 제공한다는 점에서 고유한 특성을 갖습니다.

자세한 내용은 다음을 참조하십시오.

- Trusted Extensions 구성 및 유지 관리에 대한 자세한 내용은 **Trusted Extensions 구성 및 관리**를 참조하십시오.
- 다중 레벨 데스크탑 사용에 대한 자세한 내용은 **Trusted Extensions 사용자 설명서**를 참조하십시오.
- 선택한 매뉴얼 페이지에는 `trusted_extensions(5)` 및 `labeld(1M)`이 포함됩니다.

Oracle Solaris 11 보안 기본값

설치 후 Oracle Solaris는 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. 두 계정의 암호는 처음에 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 1자 이상의 영문자와 숫자가 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 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 root로 가정 중인 사용자의 이름이 감사 증적에 추적됩니다. 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 및 데스크탑 응용 프로그램이 최소 권한, 권한 및 RBAC(역할 기반 액세스 제어)를 통해 보호됩니다.

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 umask는 022입니다. 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. 디렉토리 권한은 drwxr-xr-x(755)입니다. 파일 권한은 -rw-r--r--(644)입니다.

데스크탑 애플릿 – 데스크탑 애플릿은 RBAC로 보호됩니다. 예를 들어, 초기 사용자 또는 root 역할만 패키지 관리자 애플릿을 사용하여 새 패키지를 설치할 수 있습니다. 패키지 관리자는 사용 권한이 지정되지 않은 일반 사용자에게 표시되지 않습니다.

추가 보안 기능이 배치됨

Oracle Solaris 11은 사이트 보안 요구 사항을 충족시키도록 시스템 및 사용자를 구성하는 데 사용할 수 있는 보안 기능을 제공합니다.

- **RBAC(역할 기반 액세스 제어) –** Oracle Solaris는 다양한 인증, 권한 및 권한 프로파일을 제공합니다. root는 유일하게 정의된 역할입니다. 권한 프로파일은 사용자가 만드는 역할에 대한 효과적인 기준을 제공합니다. 또한 일부 관리 명령은 성공적으로 실행하기 위해 RBAC 인증이 필요합니다. 인증이 없는 사용자는 사용자에게 필요한 권한이 있더라도 해당 명령을 실행할 수 없습니다.

- **사용자 권한** – 20 페이지 “시스템 액세스가 제한되고 모니터됨”에 설명된 초기 사용자의 경우와 같이 사용자에게는 `/etc/security/policy.conf` 파일에서 기본적인 권한, 권한 프로파일 및 인증 집합이 지정됩니다. 사용자 로그인 시도는 제한되지 않지만 모든 실패한 로그인은 감사 서비스로 기록됩니다.
- **시스템 파일 보호** – 시스템 파일은 파일 권한에 의해 보호됩니다. `root` 역할만 시스템 구성 파일을 수정할 수 있습니다.

사이트 보안 정책 및 실행

보안 시스템 또는 시스템 네트워크를 위해서는 해당 정책을 지원하는 보안 실행과 함께 사이트에 보안 정책이 배치되어 있어야 합니다.

자세한 내용은 다음을 참조하십시오.

- **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 11 보안 구성

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

Oracle Solaris OS 설치

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 Oracle Solaris 대규모 서버 환경을 제공하는 `group/system/solaris-large-server` 그룹을 설치합니다.
- **Oracle Solaris 데스크탑** – 라이브 매체는 Oracle Solaris 11 데스크탑 환경을 제공하는 `group/system/solaris-desktop` 그룹을 설치합니다.

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

AI(자동 설치 프로그램)를 통한 자동 설치는 **Oracle Solaris 11 시스템**의 제III부, "설치 서버를 사용하여 설치"를 참조하십시오.

매체 선택 지침은 다음 설치 설명서를 참조하십시오.

- **Oracle Solaris 11 시스템**
- **사용자 정의 Oracle Solaris 11 설치 이미지 만들기**
- **Oracle Solaris 11 소프트웨어 패키지 추가 및 업데이트**

시스템 보안

다음 작업은 순서대로 수행하는 것이 가장 좋습니다. 현재 Oracle Solaris 11 OS가 설치되어 있고 root 역할을 소비할 수 있는 초기 사용자만 시스템에 액세스할 수 있습니다.

작업	설명	수행 방법
1. 시스템에서 패키지를 확인합니다.	설치 매체의 패키지가 설치된 패키지와 동일한지 확인합니다.	24 페이지 "패키지 확인"
2. 시스템에서 하드웨어 설정을 보호합니다.	하드웨어 설정을 변경하려면 암호를 입력하도록 요구하여 하드웨어를 보호합니다.	**Oracle Solaris 관리: 보안 서비스**의 "시스템 하드웨어에 대한 액세스 제어(작업)"
3. 필요하지 않은 서비스를 사용 안함으로 설정합니다.	시스템의 필수 기능에 포함되지 않는 프로세스가 실행되지 않도록 방지합니다.	25 페이지 "필요하지 않은 서비스를 사용 안함으로 설정"
4. 장치 할당을 요구합니다.	명시적인 인증 없이 이동식 매체 사용을 방지합니다. 장치에는 마이크, USB 드라이브 및 CD가 포함됩니다.	**Oracle Solaris 관리: 보안 서비스**의 "장치 할당을 사용으로 설정하는 방법"
5. 워크스테이션 소유자가 시스템 전원을 끄지 않도록 방지합니다.	콘솔 사용자가 시스템을 종료하거나 일시 중지하지 않도록 방지합니다.	25 페이지 "사용자에서 전원 관리 기능 제거"
6. 사이트의 보안 정책이 반영된 로그인 경고 메시지를 만듭니다.	사용자 및 잠재적인 공격자에게 시스템이 모니터되고 있음을 알립니다.	26 페이지 "배너 파일에 보안 메시지 배치" 27 페이지 "데스크탑 로그인 화면에 보안 메시지 배치"

▼ 패키지 확인

설치 후 바로 패키지를 확인하여 설치를 검증합니다.

시작하기 전에 root 역할을 가진 사용자여야 합니다.

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

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

2. **로그에서 오류를 검토합니다.**

3. **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.

▼ 필요하지 않은 서비스를 사용 안함으로 설정

이 절차를 사용하여 시스템 목적에 따라 필요하지 않은 서비스를 사용 안함으로 설정합니다.

시작하기 전에 root 역할을 가진 사용자여야 합니다.

1. **온라인 서비스를 나열합니다.**

   ```
   # svcs | grep network
   online         Sep_07   svc:/network/loopback: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 관리: 일반 작업**의 6 장, "서비스 관리(개요)" 및 svcs(1) 매뉴얼 페이지를 참조하십시오.

▼ 사용자에서 전원 관리 기능 제거

이 절차에 따라 시스템 사용자가 시스템을 일시 중지하거나 전원을 끄지 않도록 방지합니다.

시작하기 전에 root 역할을 가진 사용자여야 합니다.

1 **콘솔 사용자 권한 프로파일의 내용을 검토합니다.**

```
% getent prof_attr | grep Console
Console User:RO::Manage System as the Console User:
profiles=Desktop Removable Media User,Suspend To RAM,Suspend To Disk,
Brightness,CPU Power Management,Network Autoconf User;
auths=solaris.system.shutdown;help=RtConsUser.html
```

2 **사용자가 보존하게 하려는 콘솔 사용자 프로파일의 모든 권한이 포함된 권한 프로파일을 만듭니다.**

자세한 내용은 **Oracle Solaris 관리: 보안 서비스**의 "감사 프로파일을 만들거나 변경하는 방법"을 참조하십시오.

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

```
#CONSOLE_USER=Console User
```

4 **단계 2에서 만든 권한 프로파일을 사용자에게 지정합니다.**

```
# usermod -P +new-profile username
```

참조 자세한 내용은 **Oracle Solaris 관리: 보안 서비스**의 "policy.conf 파일" 및 `policy.conf(4)` 및 `usermod(1M)` 매뉴얼 페이지를 참조하십시오.

▼ 배너 파일에 보안 메시지 배치

이 절차를 수행하여 사이트의 보안 정책이 반영된 경고 메시지를 만듭니다. 로컬 및 원격 로그인 시 해당 파일의 내용이 표시됩니다.

주 – 이 절차의 샘플 메시지는 미국 정부 요구 사항을 충족하지 않으며 사용자의 보안 정책을 충족하지도 않습니다.

시작하기 전에 `root` 역할을 가진 사용자여야 합니다. 보안 메시지 내용에 대해서는 회사의 법률 전문가와 상의하는 것이 가장 좋습니다.

1 **/etc/issue 파일에 보안 메시지를 입력합니다.**

```
# vi /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.
```

자세한 내용은 `issue(4)` 매뉴얼 페이지를 참조하십시오.

telnet 프로그램은 /etc/issue 파일의 내용을 로그인 메시지에 표시합니다. 다른 응용 프로그램에서 이 파일을 사용하는 방법은 36 페이지 "ssh 및 ftp 사용자에게 보안 메시지 표시" 및 27 페이지 "데스크탑 로그인 화면에 보안 메시지 배치"를 참조하십시오.

2 **/etc/motd 파일에 보안 메시지를 추가합니다.**

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

▼ 데스크탑 로그인 화면에 보안 메시지 배치

로그인 시 사용자가 검토할 보안 메시지를 만들 수 있는 여러 가지 방법 중에서 선택합니다.

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.

주 – 이 절차의 샘플 메시지는 미국 정부 요구 사항을 충족하지 않으며 사용자의 보안 정책을 충족하지도 않습니다.

시작하기 전에 root 역할을 가진 사용자여야 합니다. 보안 메시지 내용에 대해서는 회사의 법률 전문가와 상의하는 것이 가장 좋습니다.

- **데스크탑 로그인 화면에 보안 메시지를 배치합니다.**

  여러 옵션이 있습니다. 대화 상자를 만드는 옵션은 26 페이지 "배너 파일에 보안 메시지 배치"의 단계 1에서 /etc/issue 파일을 사용합니다.

  - **옵션 1: 로그인 시 대화 상자에 보안 메시지를 표시하는 데스크탑 파일을 만듭니다.**

    ```
    # vi /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/issue
    OnlyShowIn=GNOME;
    X-GNOME-Autostart-Phase=Application
    ```

    로그인 창에서 인증이 완료되면 대화 상자를 닫아야만 작업 공간에 연결할 수 있습니다. zenity 명령 옵션은 zenity(1) 매뉴얼 페이지를 참조하십시오.

- **옵션 2: 대화 상자에 보안 메시지가 표시되도록 GDM 초기화 스크립트를 수정합니다.**

  /etc/gdm 디렉토리에는 데스크탑 로그인 전, 데스크탑 로그인 도중 또는 데스크탑 로그인 직후 보안 메시지를 표시하는 세 가지 초기화 스크립트가 포함되어 있습니다. 이러한 스크립트는 Oracle Solaris 10 릴리스에서도 사용할 수 있습니다.

  - **로그인 화면이 나타나기 전에 보안 메시지를 표시합니다.**

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

  - **인증 후 로그인 화면에 보안 메시지를 표시합니다.**

    이 스크립트는 사용자 작업 공간이 나타나기 전에 실행됩니다. 이 스크립트는 Default.sample 스크립트를 수정하여 만듭니다.

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

  - **인증 후 사용자의 초기 작업 공간에 보안 메시지를 표시합니다.**

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

    주 – 사용자 작업 공간에 여러 창이 표시된 경우 대화 상자가 가려질 수 있습니다.

- **옵션 3: 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.

  주 – 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) 로그인 창 GUI를 수정한 후 복사본을 저장합니다.

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

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.

```
# vi /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.

작업	설명	수행 방법
강력한 암호를 사용하고 암호를 자주 변경해야 합니다.	각 시스템에서 기본 암호 제약 조건을 강화합니다.	30 페이지 “강력한 암호 제약 조건 설정”
일반 사용자에 대해 제한적인 파일 권한을 구성합니다.	일반 사용자의 파일 권한에 대해 022보다 제한적인 값을 설정합니다.	32 페이지 “일반 사용자에 대해 보다 제한적인 umask 값 설정”.
일반 사용자에 대한 계정 잠금을 설정합니다.	관리에 사용되지 않는 시스템에서 시스템 차원의 계정 잠금을 설정하고 잠금을 활성화하는 로그인 수를 줄입니다.	31 페이지 “일반 사용자에 대한 계정 잠금”

작업	설명	수행 방법
추가 감사 클래스를 미리 선택합니다.	시스템의 잠재적 위협에 대해 보다 효과적인 모니터링 및 레코딩 기능을 제공합니다.	33 페이지 "로그온/로그아웃 이외의 중요 감사 이벤트"
감사 이벤트에 대한 텍스트 요약을 `syslog` 유틸리티에 전송합니다.	로그인 및 로그인 시도와 같은 중요한 감사 이벤트를 실시간으로 기록합니다.	33 페이지 "실시간으로 `lo` 이벤트 모니터링"
역할을 만듭니다.	한 명의 사용자가 시스템을 손상시킬 수 없도록 여러 신뢰할 수 있는 사용자에게 고유한 관리 작업을 분배합니다.	**Oracle Solaris 관리: 일반 작업**의 "사용자 계정 설정" **Oracle Solaris 관리: 보안 서비스**의 "역할을 만드는 방법" **Oracle Solaris 관리: 보안 서비스**의 "역할을 할당하는 방법".
사용자의 데스크탑에만 허용된 응용 프로그램을 표시합니다.	사용자가 자신에게 사용 권한이 없는 응용 프로그램을 보거나 사용할 수 없도록 방지합니다.	**Trusted Extensions 구성 및 관리**의 "사용자를 데스크탑 응용 프로그램으로 제한하는 방법"을 참조하십시오.
사용자의 권한을 제한합니다.	사용자에게 필요하지 않은 기본 권한을 제거합니다.	34 페이지 "사용자에게서 필요하지 않은 기본 권한 제거"

▼ 강력한 암호 제약 조건 설정

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

시작하기 전에 기본값을 변경하기 전에 변경 사항에 따라 모든 사용자가 해당 응용 프로그램에 인증할 수 있고 네트워크의 다른 시스템에도 인증할 수 있는지 확인하십시오.

`root` 역할을 가진 사용자여야 합니다.

- **`/etc/default/passwd` 파일을 편집합니다.**

  a. **사용자가 3주~1개월 사이에 암호를 변경하도록 요구합니다.**

  ```
  ## /etc/default/passwd
  ##
  MAXWEEKS=
  MINWEEKS=
  MAXWEEKS=4
  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 제한하는 변수 목록은 `/etc/default/passwd` 파일을 참조하십시오. 기본값은 파일에 표시되어 있습니다.
- 설치 후 적용되는 암호 제약 조건은 20 페이지 "시스템 액세스가 제한되고 모니터됨"을 참조하십시오.
- `passwd(1)` 매뉴얼 페이지

▼ 일반 사용자에 대한 계정 잠금

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

주 – 사용자가 역할을 잠글 수 있으므로 역할을 가정할 수 있는 다른 사용자에 대해 계정 잠금을 설정하지 마십시오.

시작하기 전에 `root` 역할을 가진 사용자여야 합니다. 관리 작업을 수행하기 위해 사용하는 시스템에서 이 시스템 차원의 보호를 설정하지 마십시오.

1 LOCK_AFTER_RETRIES 보안 속성을 YES로 설정합니다.

- **시스템 차원 설정**

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

- **사용자별 설정**

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

2 **RETRIES 보안 속성을 3으로 설정합니다.**

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

참조
- 사용자 및 역할 보안 속성에 대한 자세한 내용은 **Oracle Solaris 관리: 보안 서비스**의 10 장, "Oracle Solaris의 보안 속성(참조)"을 참조하십시오.
- 선택한 매뉴얼 페이지에 `policy.conf(4)` 및 `user_attr(4)`가 포함됩니다.

▼ 일반 사용자에 대해 보다 제한적인 umask 값 설정

기본값인 umask 값 022가 충분히 제한적이지 않으면 이 절차에 따라 보다 제한적인 마스크를 설정합니다.

시작하기 전에 root 역할을 가진 사용자여야 합니다.

● **여러 셸의 골격 디렉토리에 있는 로그인 프로파일에서 umask 값을 수정합니다.**

Oracle Solaris는 관리자가 사용자 셸 기본값을 사용자 정의할 수 있는 디렉토리를 제공합니다. 이러한 골격 디렉토리에는 `.profile`, `.bashrc`, `.kshrc`와 같은 파일이 포함되어 있습니다.

다음 값 중 하나를 선택합니다.

- umask 027 – 중간 수준의 파일 보호를 제공합니다.

  (740) – 그룹의 경우 w, 기타의 경우 rwx입니다.
- umask 026 – 조금 더 엄격한 파일 보호를 제공합니다.

  (741) – 그룹의 경우 w, 기타의 경우 rw입니다.
- umask 077 – 완전한 파일 보호를 제공합니다.

  (700) – 그룹 및 기타에 대한 액세스 권한이 제공되지 않습니다.

참조 자세한 내용은 다음을 참조하십시오.
- **Oracle Solaris 관리: 일반 작업**의 "사용자 계정 설정"
- **Oracle Solaris 관리: 보안 서비스**의 "기본 umask 값"
- 선택한 매뉴얼 페이지에 `usermod(1M)` 및 `umask(1)`가 포함됩니다.

▼ 로그온/로그아웃 이외의 중요 감사 이벤트

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

주 – 이 절차의 예로는 사용자의 보안 정책을 만족시키는 데 충분하지 않을 수 있습니다.

시작하기 전에 root 역할을 가진 사용자여야 합니다. 감사와 관련하여 사이트의 보안 정책을 구현합니다.

1. **사용자 및 역할별로 사용되는 권한이 있는 명령을 모두 감사합니다.**

   모든 사용자 및 역할에 대해 해당 사전 선택 마스크에 AUE_PFEXEC 감사 이벤트를 추가합니다.

   ```
   # usermod -K audit_flags=lo,ps:no username

   # rolemod -K audit_flags=lo,ps:no rolename
   ```

2. **인수를 감사된 명령에 기록합니다.**

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

3. **감사된 명령이 실행되는 환경을 기록합니다.**

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

참조

- 감사 정책에 대한 자세한 내용은 **Oracle Solaris 관리: 보안 서비스**의 "감사 정책"를 참조하십시오.
- 감사 플래그 설정 예는 **Oracle Solaris 관리: 보안 서비스**의 "감사 서비스 구성(작업)" 및 **Oracle Solaris 관리: 보안 서비스**의 "감사 서비스 문제 해결(작업)"을 참조하십시오.
- 감사를 구성하려면 auditconfig(1M) 매뉴얼 페이지를 참조하십시오.

▼ 실시간으로 lo 이벤트 모니터링

이 절차에 따라 이벤트가 발생할 때 모니터링하려는 이벤트에 대해 audit_syslog 플러그인을 활성화합니다.

시작하기 전에 syslog.conf 파일을 수정하려면 사용자가 root 역할이어야 합니다. 기타 단계에서는 사용자에게 감사 구성 권한 프로파일이 지정되어야 합니다.

1. **audit_syslog 플러그인에 lo 클래스를 전송하고 플러그인을 활성화합니다.**

   ```
   # auditconfig -setplugin audit_syslog active p_flags=lo
   ```

2 **syslog.conf 파일에 audit.notice 항목을 추가합니다.**

기본 항목에는 로그 파일 위치가 포함됩니다.

```
# cat /etc/syslog.conf
...
audit.notice       /var/adm/auditlog
```

3 **로그 파일을 만듭니다.**

```
# touch /var/adm/auditlog
```

4 **syslog 서비스에 대한 구성 정보를 새로 고칩니다.**

```
# svcadm refresh system/system-log
```

5 **감사 서비스를 새로 고칩니다.**

감사 서비스는 새로 고쳐질 때 감사 플러그인 변경 사항을 읽습니다.

```
# audit -s
```

참조

- 감사 요약을 다른 시스템으로 전송하려면 **Oracle Solaris 관리: 보안 서비스**의 "syslog 감사 로그를 구성하는 방법" 예를 참조하십시오.
- 감사 서비스는 확장 출력을 생성할 수 있습니다. 로그를 관리하려면 logadm(1M) 매뉴얼 페이지를 참조하십시오.
- 출력을 모니터하려면 50 페이지 "audit_syslog 감사 요약 모니터링"을 참조하십시오.

▼ 사용자에게서 필요하지 않은 기본 권한 제거

특정 환경에서는 일반 사용자의 기본 집합에서 세 가지 기본 권한 중 하나 이상을 제거할 수 있습니다.

- file_link_any – 프로세스가 해당 프로세스의 유효 UID와 다른 UID로 소유되는 파일에 대해 하드 링크를 만들 수 있도록 허용합니다.
- proc_info – 프로세스가 신호를 보낼 수 있는 프로세스 이외의 다른 프로세스 상태를 검사할 수 있도록 허용합니다. 조사할 수 없는 프로세스는 /proc에서 볼 수 없고 존재하지 않는 것으로 표시됩니다.
- proc_session – 프로세스가 세션 외부에서 신호를 보내거나 프로세스를 추적할 수 있도록 허용합니다.

시작하기 전에 root 역할을 가진 사용자여야 합니다.

1 **사용자가 소유하지 않는 파일에 사용자가 연결하지 못하도록 방지합니다.**

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

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

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

3 **사용자의 현재 세션으로부터 ssh 세션을 시작하는 것과 같이 사용자가 두번째 세션을 시작하지 못하도록 방지합니다.**

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

4 **사용자의 기본 집합에서 세 가지 모든 권한을 제거합니다.**

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

참조 자세한 내용은 **Oracle Solaris 관리: 보안 서비스**의 8 장, "역할 및 권한 사용(개요)" 및 `privileges(5)` 매뉴얼 페이지를 참조하십시오.

커널 보안

이 때, 역할을 가정할 수 있는 사용자를 만들고 역할을 만들었을 수 있습니다. `root` 역할만 시스템 파일을 수정할 수 있습니다.

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 관리: 보안 서비스**의 "보안 손상으로부터 실행 파일 보호"
중요한 정보가 포함될 수 있는 코어 파일을 보호합니다.	코어 파일 전용의 액세스가 제한된 디렉토리를 만듭니다.	**Oracle Solaris 관리: 일반 작업**의 "전역 코어 파일 경로를 사용으로 설정하는 방법" **Oracle Solaris 관리: 일반 작업**의 "코어 파일 관리(작업 맵)"

네트워크 구성

이 때, 역할을 가정할 수 있는 사용자를 만들고 역할을 만들었을 수 있습니다. `root` 역할만 시스템 파일을 수정할 수 있습니다.

다음 네트워크 작업에서 사이트 요구 사항에 따라 추가 보안을 제공하는 작업을 수행합니다. 이러한 네트워크 작업은 원격으로 로그인한 사용자에게 시스템이 보호되고 있음을 알리고 IP, ARP 및 TCP 프로토콜을 강화합니다.

작업	설명	수행 방법
사이트의 보안 정책이 반영된 경고 메시지를 표시합니다.	사용자 및 잠재적인 공격자에게 시스템이 모니터되고 있음을 알립니다.	36 페이지 "ssh 및 ftp 사용자에게 보안 메시지 표시"

작업	설명	수행 방법
네트워크 라우팅 데몬을 사용 안함으로 설정합니다.	잠재적인 네트워크 스니퍼에 의한 시스템 액세스를 제한합니다.	37 페이지 “네트워크 라우팅 데몬 사용 안함”
네트워크 토폴로지 정보에 대한 배포를 방지합니다.	패킷 브로드캐스트를 방지합니다.	38 페이지 “브로드캐스트 패킷 전달 사용 안함”
	브로드캐스트 에코 요청 및 멀티캐스트 에코 요청에 대한 응답을 방지합니다.	38 페이지 “에코 요청에 대한 응답 사용 안함”
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.	39 페이지 “엄격한 다중 홈 지정 설정”
완전하지 않은 시스템 연결 개수를 제한하여 DOS 공격을 방지합니다.	TCP 리스너에 대해 완전하지 않은 TCP 연결의 허용 가능한 개수를 제한합니다.	40 페이지 “완전하지 않은 TCP 연결의 최대 개수 설정”
허용된 수신 연결 개수를 제한하여 DOS 공격을 방지합니다.	TCP 리스너에 대한 보류 중인 TCP 연결의 기본 최대 개수를 지정합니다.	40 페이지 “보류 중인 TCP 연결의 최대 개수 설정”
초기 TCP 연결에 대한 높은 수준의 난수를 생성합니다.	RFC 1948에 의해 지정된 시퀀스 번호 생성 값을 준수합니다.	41 페이지 “초기 TCP 연결에 대한 높은 수준의 난수 지정”
네트워크 매개변수를 해당 보안 기본값으로 반환합니다.	관리 작업으로 줄어든 보안을 늘립니다.	41 페이지 “네트워크 매개변수를 보안 값으로 재설정”
네트워크 서비스에 TCP 래퍼를 추가하여 응용 프로그램을 적합한 사용자로 제한합니다.	네트워크 서비스에 대해 액세스가 허용되는 시스템을 지정합니다(예: FTP). **Oracle Solaris 관리: 네트워크 서비스**의 “sendmail 버전 8.12의 TCP 래퍼에 대한 지원”에 설명된 것처럼 기본적으로 `sendmail` 응용 프로그램은 TCP 래퍼로 보호됩니다.	모든 `inetd` 서비스에 대해 TCP 래퍼를 사용으로 설정하려면 **Oracle Solaris 관리: IP 서비스**의 “TCP 래퍼를 사용하여 TCP 서비스에 대한 액세스를 제어하는 방법”을 참조하십시오. FTP 네트워크 서비스를 보호하는 TCP 예를 보려면 **Oracle Solaris 관리: 네트워크 서비스**의 “SMF를 사용하여 FTP 서버를 시작하는 방법”을 참조하십시오.

▼ ssh 및 ftp 사용자에게 보안 메시지 표시

다음 절차는 원격 로그인 및 파일 전송 시 경고를 표시하는 방법입니다.

시작하기 전에 `root` 역할을 가진 사용자여야 합니다. `/etc/issue` 파일은 26 페이지 “배너 파일에 보안 메시지 배치”의 단계 1에서 이미 만들었습니다.

1 **ssh를 사용하여 로그인 중인 사용자에게 보안 메시지를 표시하려면 다음을 수행합니다.**

a. **/etc/sshd_config 파일에서 배너 지시어의 주석을 해제합니다.**

```
# vi /etc/ssh/sshd_config
# Banner to be printed before authentication starts.
Banner /etc/issue
```

b. **ssh 서비스를 새로 고칩니다.**

```
# svcadm refresh ssh
```

자세한 내용은 issue(4) 및 sshd_config(4) 매뉴얼 페이지를 참조하십시오.

2 **ftp를 사용하여 로그인 중인 사용자에게 보안 메시지를 표시하려면 다음을 수행합니다.**

a. **DisplayConnect 지시어를 proftpd.conf 파일에 추가합니다.**

```
# vi /etc/proftpd.conf
# Banner to be printed before authentication starts.
DisplayConnect /etc/issue
```

b. **ftp 서비스를 다시 시작합니다.**

```
# svcadm restart ftp
```

자세한 내용은 ProFTPD (http://www.proftpd.org/) 웹 사이트를 참조하십시오.

▼ 네트워크 라우팅 데몬 사용 안함

이 절차에 따라 기본 라우터를 지정하여 설치한 후 네트워크 라우팅을 방지합니다. 그렇지 않으면 라우팅을 수동으로 구성한 후 이 절차를 수행하십시오.

주 – 여러 네트워크 구성 절차에서는 라우팅 데몬을 사용 안함으로 설정해야 합니다. 따라서 대규모 구성 절차에서는 이 데몬이 사용 안함으로 설정되었을 수 있습니다.

시작하기 전에 네트워크 관리 권한 프로파일을 지정해야 합니다.

1 **라우팅 데몬이 실행 중인지 확인합니다.**

```
# svcs -x svc:/network/routing/route:default
svc:/network/routing/route:default (in.routed network routing daemon)
 State: online since April 10, 2011 05:15:35 AM PDT
   See: in.routed(1M)
   See: /var/svc/log/network-routing-route:default.log
Impact: None.
```

서비스가 실행 중이 아니면 여기에서 중지할 수 있습니다.

2. **라우팅 데몬을 사용 안함으로 설정합니다.**

```
# routeadm -d ipv4-forwarding -d ipv6-forwarding
# routeadm -d ipv4-routing -d ipv6-routing
# routeadm -u
```

3. **라우팅 데몬이 사용 안함으로 설정되었는지 확인합니다.**

```
# svcs -x routing/route:default
svc:/network/routing/route:default (in.routed network routing daemon)
 State: disabled since April 11, 2011 10:10:10 AM PDT
Reason: Disabled by an administrator.
   See: http://sun.com/msg/SMF-8000-05
   See: in.routed(1M)
Impact: This service is not running.
```

참조 routeadm(1M) 매뉴얼 페이지

▼ 브로드캐스트 패킷 전달 사용 안함

기본적으로 Oracle Solaris는 브로드캐스트 패킷을 전달합니다. 사이트 보안 정책에 따라 브로드캐스트 범람 가능성을 줄여야 하는 경우 이 절차를 사용하여 기본값을 변경하십시오.

주 – _forward_directed_broadcasts 네트워크 등록 정보를 사용 안함으로 설정하면 브로드캐스트 핑이 사용 안함으로 설정됩니다.

시작하기 전에 네트워크 관리 권한 프로파일을 지정해야 합니다.

1. **IP 패킷에 대해 브로드캐스트 패킷 전달 등록 정보를 0으로 설정합니다.**

```
# ipadm set-prop -p _forward_directed_broadcasts=0 ip
```

2. **현재 값을 확인합니다.**

```
# ipadm show-prop -p _forward_directed_broadcasts ip
PROTO  PROPERTY                  PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ip     _forward_directed_broadcasts  rw   0         --           0         0,1
```

참조 ipadm(1M) 매뉴얼 페이지

▼ 에코 요청에 대한 응답 사용 안함

이 절차를 사용하여 네트워크 토폴로지에 대한 정보 배포를 방지합니다.

시작하기 전에 네트워크 관리 권한 프로파일을 지정해야 합니다.

1. **브로드캐스트 에코 요청 등록 정보에 대한 응답을 IP 패킷에 대해 0으로 설정하고 현재 값을 확인합니다.**

```
# ipadm set-prop -p _respond_to_echo_broadcast=0 ip

# ipadm show-prop -p _respond_to_echo_broadcast ip
PROTO  PROPERTY                 PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ip     _respond_to_echo_broadcast rw   0         --           1         0,1
```

2. **멀티캐스트 에코 요청 등록 정보에 대한 응답을 IP 패킷에 대해 0으로 설정하고 현재 값을 확인합니다.**

```
# ipadm set-prop -p _respond_to_echo_multicast=0 ipv4
# ipadm set-prop -p _respond_to_echo_multicast=0 ipv6

# ipadm show-prop -p _respond_to_echo_multicast ipv4
PROTO  PROPERTY                 PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv4   _respond_to_echo_multicast rw   0         --           1         0,1
# ipadm show-prop -p _respond_to_echo_multicast ipv6
PROTO  PROPERTY                 PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv6   _respond_to_echo_multicast rw   0         --           1         0,1
```

참조 자세한 내용은 **Oracle Solaris 조정 가능 매개변수 참조 설명서**의 "_respond_to_echo_broadcast 및 _respond_to_echo_multicast (ipv4 or ipv6)" 및 `ipadm`(1M) 매뉴얼 페이지를 참조하십시오.

▼ 엄격한 다중 홈 지정 설정

다른 시스템에 대한 게이트웨이인 시스템(예: 방화벽 또는 VPN 노드)의 경우 이 절차를 사용하여 엄격한 다중 홈 지정을 설정합니다.

Oracle Solaris 11 릴리스에는 IPv4 및 IPv6에 대한 새로운 등록 정보인 `hostmodel`이 도입되었습니다. 이 등록 정보는 다중 홈 지정 시스템에 대한 IP 패킷의 전송 및 수신 동작을 제어합니다.

시작하기 전에 네트워크 관리 권한 프로파일을 지정해야 합니다.

1. **`hostmodel` 등록 정보를 IP 패킷에 대해 `strong`으로 설정합니다.**

```
# ipadm set-prop -p hostmodel=strong ipv4
# ipadm set-prop -p hostmodel=strong ipv6
```

2. **현재 값을 확인하고 가능한 값을 적어 둡니다.**

```
# ipadm show-prop -p hostmodel ip
PROTO  PROPERTY    PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv6   hostmodel   rw   strong    strong       weak      strong,src-priority,weak
ipv4   hostmodel   rw   strong    strong       weak      strong,src-priority,weak
```

참조 자세한 내용은 **Oracle Solaris 조정 가능 매개변수 참조 설명서**의 "hostmodel (ipv4 or ipv6)" 및 `ipadm`(1M) 매뉴얼 페이지를 참조하십시오.

엄격한 다중 홈 지정 사용에 대한 자세한 내용은 **Oracle Solaris 관리: IP 서비스**의 "터널 모드에서 IPsec를 사용하여 VPN을 보호하는 방법"를 참조하십시오.

▼ 완전하지 않은 TCP 연결의 최대 개수 설정

이 절차에 따라 완전하지 않은 보류 중인 연결 개수를 제어하여 서비스 거부(DOS) 공격을 방지합니다.

시작하기 전에 네트워크 관리 권한 프로파일을 지정해야 합니다.

1 수신 중인 연결의 최대 개수를 설정합니다.

```
# ipadm set-prop -p _conn_req_max_q0=4096 tcp
```

2 현재 값을 확인합니다.

```
# ipadm show-prop -p _conn_req_max_q0 tcp
PROTO  PROPERTY         PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
tcp    _conn_req_max_q0 rw   4096      --           128       1-4294967295
```

참조 자세한 내용은 **Oracle Solaris 조정 가능 매개변수 참조 설명서**의 "_conn_req_max_q0" 및 ipadm(1M) 매뉴얼 페이지를 참조하십시오.

▼ 보류 중인 TCP 연결의 최대 개수 설정

이 절차에 따라 허용된 수신 중인 연결 개수를 제어하여 DOS 공격을 방지합니다.

시작하기 전에 네트워크 관리 권한 프로파일을 지정해야 합니다.

1 수신 중인 연결의 최대 개수를 설정합니다.

```
# ipadm set-prop -p _conn_req_max_q=1024 tcp
```

2 현재 값을 확인합니다.

```
# ipadm show-prop -p _conn_req_max_q tcp
PROTO  PROPERTY         PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
tcp    _conn_req_max_q  rw   1024      --           128       1-4294967295
```

참조 자세한 내용은 **Oracle Solaris 조정 가능 매개변수 참조 설명서**의 "_conn_req_max_q" 및 ipadm(1M) 매뉴얼 페이지를 참조하십시오.

▼ 초기 TCP 연결에 대한 높은 수준의 난수 지정

이 절차에서는 RFC 1948 (http://www.ietf.org/rfc/rfc1948.txt)을 준수하는 TCP 초기 시퀀스 번호 생성 매개변수를 설정합니다.

시작하기 전에 시스템 파일을 수정하려면 사용자가 root 역할이어야 합니다.

- **TCP_STRONG_ISS 변수에 대한 기본값을 변경합니다.**

```
# vi /etc/default/inetinit
# TCP_STRONG_ISS=1
TCP_STRONG_ISS=2
```

▼ 네트워크 매개변수를 보안 값으로 재설정

기본적으로 보안되는 여러 네트워크 매개변수는 튜닝 가능하므로 변경될 수 있습니다. 사이트 조건에서 허용하는 경우 다음과 같은 튜닝 가능한 매개변수를 해당 기본값으로 반환합니다.

시작하기 전에 네트워크 관리 권한 프로파일을 지정해야 합니다. 매개변수의 현재 값이 기본값보다 보안이 낮습니다.

1. **IP 패킷에 대해 소스 패킷 전달 등록 정보를 0으로 설정한 후 현재 값을 확인하십시오.**

   기본값은 허위로 제공된 패킷으로부터의 DOS 공격을 방지합니다.

```
# ipadm set-prop -p _forward_src_routed=0 ipv4
# ipadm set-prop -p _forward_src_routed=0 ipv6
# ipadm show-prop -p _forward_src_routed ipv4
PROTO  PROPERTY             PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv4   _forward_src_routed   rw   0         --           0         0,1
# ipadm show-prop -p _forward_src_routed ipv6
PROTO  PROPERTY             PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv6   _forward_src_routed   rw   0         --           0         0,1
```

   자세한 내용은 **Oracle Solaris 조정 가능 매개변수 참조 설명서**의 "forwarding (ipv4 or ipv6)"을 참조하십시오.

2. **IP 패킷에 대해 netmask 응답 등록 정보를 0으로 설정한 후 현재 값을 확인하십시오.**

   기본값은 네트워크 토폴로지 정보의 배포를 방지합니다.

```
# ipadm set-prop -p _respond_to_address_mask_broadcast=0 ip
# ipadm show-prop -p _respond_to_address_mask_broadcast ip
PROTO PROPERTY                          PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ip    _respond_to_address_mask_broadcast rw   0         --           0         0,1
```

3 **IP 패킷에 대해 타임스탬프 응답 등록 정보를 0으로 설정한 후 현재 값을 확인하십시오.**

기본값은 시스템에서 추가 CPU 요구를 제거하고 네트워크 정보의 배포를 방지합니다.

```
# ipadm set-prop -p _respond_to_timestamp=0 ip
# ipadm show-prop -p _respond_to_timestamp ip
PROTO  PROPERTY                       PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ip     _respond_to_timestamp          rw   0         --           0         0,1
```

4 **IP 패킷에 대해 브로드캐스트 타임스탬프 응답 등록 정보를 0으로 설정한 후 현재 값을 확인하십시오.**

기본값은 시스템에서 추가 CPU 요구를 제거하고 네트워크 정보의 배포를 방지합니다.

```
# ipadm set-prop -p _respond_to_timestamp_broadcast=0 ip
# ipadm show-prop -p _respond_to_timestamp_broadcast ip
PROTO  PROPERTY                       PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ip     _respond_to_timestamp_broadcast rw  0         --           0         0,1
```

5 **IP 패킷에 대해 재지정 무시 등록 정보를 0으로 설정한 후 현재 값을 확인하십시오.**

기본값은 시스템에서 추가 CPU 요구를 방지합니다.

```
# ipadm set-prop -p _ignore_redirect=0 ipv4
# ipadm set-prop -p _ignore_redirect=0 ipv6
# ipadm show-prop -p _ignore_redirect ipv4
PROTO  PROPERTY         PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv4   _ignore_redirect  rw   0         --           0         0,1
# ipadm show-prop -p _ignore_redirect ipv6
PROTO  PROPERTY         PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv6   _ignore_redirect  rw   0         --           0         0,1
```

6 **IP 소스 라우팅을 방지합니다.**

진단 목적을 위해 IP 소스 라우팅이 필요한 경우 이 네트워크 매개변수를 사용 안함으로 설정하지 마십시오.

```
# ipadm set-prop -p _rev_src_routes=0 tcp
# ipadm show-prop -p _rev_src_routes tcp
PROTO  PROPERTY         PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
tcp    _rev_src_routes   rw   0         --           0         0,1
```

자세한 내용은 **Oracle Solaris 조정 가능 매개변수 참조 설명서**의 "_rev_src_routes"를 참조하십시오.

7 **IP 패킷에 대해 재지정 무시 등록 정보를 0으로 설정한 후 현재 값을 확인하십시오.**

기본값은 시스템에서 추가 CPU 요구를 방지합니다. 잘 구성된 네트워크에서는 일반적으로 재지정이 필요하지 않습니다.

```
# ipadm set-prop -p _ignore_redirect=0 ipv4
# ipadm set-prop -p _ignore_redirect=0 ipv6
# ipadm show-prop -p _ignore_redirect ipv4
PROTO  PROPERTY           PERM  CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv4   _ignore_redirect   rw    0         --           0         0,1
# ipadm show-prop -p _ignore_redirect ipv6
PROTO  PROPERTY           PERM  CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv6   _ignore_redirect   rw    0         --           0         0,1
```

참조 ipadm(1M) 매뉴얼 페이지

파일 시스템 및 파일 보호

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

다음 작업을 통해 Oracle Solaris의 기본 파일 시스템인 ZFS에서 사용 가능한 보호 수단에 대한 개괄적으로 이해할 수 있습니다. 자세한 내용은 **Oracle Solaris 관리: ZFS 파일 시스템**의 "ZFS 쿼터 및 예약 설정" 및 zfs(1M) 매뉴얼 페이지를 참조하십시오.

작업	설명	수행 방법
디스크 공간을 관리 및 보존하여 DOS 공격을 방지합니다.	사용자나 그룹 또는 프로젝트별로 파일 시스템의 디스크 공간 사용을 지정합니다.	**Oracle Solaris 관리: ZFS 파일 시스템**의 "ZFS 쿼터 및 예약 설정"
데이터 집합 및 해당 종속 요소에 최소한의 디스크 공간을 보장합니다.	파일 시스템, 사용자나 그룹 또는 프로젝트별로 디스크 공간을 보장합니다.	**Oracle Solaris 관리: ZFS 파일 시스템**의 "ZFS 파일 시스템에 대한 예약 설정"
파일 시스템에서 데이터를 암호화합니다.	데이터베이스를 만들 때 데이터 집합에 액세스하기 위한 passphrase 및 암호화를 사용하여 데이터 집합을 보호합니다.	**Oracle Solaris 관리: ZFS 파일 시스템**의 "ZFS 파일 시스템 암호화" **Oracle Solaris 관리: ZFS 파일 시스템**의 "ZFS 파일 시스템 암호화의 예"
일반 UNIX 파일 권한보다 세부적인 수준으로 파일을 보호하려면 ACL을 지정합니다.	확장된 보안 속성은 파일을 보호하는 데 유용할 수 있습니다. 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)

파일 보호 및 수정

root 역할만 시스템 파일을 수정할 수 있습니다.

작업	설명	수행 방법
일반 사용자에 대해 제한적인 파일 권한을 구성합니다.	일반 사용자의 파일 권한에 대해 022보다 제한적인 값을 설정합니다.	32 페이지 "일반 사용자에 대해 보다 제한적인 umask 값 설정"
시스템 파일을 허위 파일로 교체할 수 없도록 방지합니다.	스크립트 또는 BART를 사용하여 허위 파일을 찾습니다.	**Oracle Solaris 관리: 보안 서비스**의 "특수 파일 사용 권한이 있는 파일을 찾는 방법"

응용 프로그램 및 서비스 보안

Oracle Solaris 보안 기능을 사용하여 응용 프로그램을 보호할 수 있습니다.

중요 응용 프로그램을 포함하기 위한 영역 만들기

영역은 프로세스를 구분하는 컨테이너입니다. 영역은 응용 프로그램 및 응용 프로그램의 일부에 대한 유용한 컨테이너입니다. 예를 들어, 영역을 사용하여 웹 사이트의 데이터베이스를 사이트의 웹 서버와 구분할 수 있습니다.

자세한 내용 및 절차를 보려면 다음을 참조하십시오.

- **Oracle Solaris 관리: Oracle Solaris Zones, Oracle Solaris 10 Zones 및 리소스 관리**의 15 장, "Oracle Solaris Zones 소개"
- **Oracle Solaris 관리: Oracle Solaris Zones, Oracle Solaris 10 Zones 및 리소스 관리**의 "기능별 영역 요약"
- **Oracle Solaris 관리: Oracle Solaris Zones, Oracle Solaris 10 Zones 및 리소스 관리**의 "비전역 영역에서 제공하는 기능"
- **Oracle Solaris 관리: Oracle Solaris Zones, Oracle Solaris 10 Zones 및 리소스 관리**의 "시스템에서 영역 설정(작업 맵)".
- **Oracle Solaris 관리: Oracle Solaris Zones, Oracle Solaris 10 Zones 및 리소스 관리**의 16 장, "비전역 영역 구성(개요)".
- **Oracle Solaris 보안 기술로 Oracle Database 강화** (`http://www.oracle.com/technetwork/server-storage/solaris/solaris-security-hardening-db-167784.pdf`)

영역에서 리소스 관리

영역은 영역 리소스 관리를 위한 다양한 도구를 제공합니다.

자세한 내용 및 절차를 보려면 다음을 참조하십시오.

- **Oracle Solaris 관리: Oracle Solaris Zones, Oracle Solaris 10 Zones 및 리소스 관리**의 14 장, "리소스 관리 구성 예"
- **Oracle Solaris 관리: Oracle Solaris Zones, Oracle Solaris 10 Zones 및 리소스 관리**의 제I부, "Oracle Solaris 리소스 관리"

IPsec 및 IKE 구성

IPsec 및 IKE는 IPsec 및 IKE를 사용하여 공동으로 구성된 노드와 네트워크 사이의 네트워크 전송을 보호합니다.

자세한 내용 및 절차를 보려면 다음을 참조하십시오.

- **Oracle Solaris 관리: IP 서비스**의 14 장, "IP 보안 아키텍처(개요)"
- **Oracle Solaris 관리: IP 서비스**의 17 장, "Internet Key Exchange(개요)"
- **Oracle Solaris 관리: IP 서비스**의 15 장, "IPsec 구성(작업)"
- **Oracle Solaris 관리: IP 서비스**의 18 장, "IKE 구성(작업)"

IP 필터 구성

IP 필터 기능은 방화벽을 제공합니다.

자세한 내용 및 절차를 보려면 다음을 참조하십시오.

- **Oracle Solaris 관리: IP 서비스**의 20 장, "Oracle Solaris의 IP 필터(개요)"
- **Oracle Solaris 관리: IP 서비스**의 21 장, "IP 필터(작업)"

Kerberos 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 관리: 보안 서비스**의 20 장, "Kerberos 서비스 계획"
- **Oracle Solaris 관리: 보안 서비스**의 21 장, "Kerberos 서비스 구성(작업)"
- 선택한 매뉴얼 페이지에는 `kadmin`(1M), `pam_krb5`(5) 및 `kclient`(1M)가 포함됩니다.

레거시 서비스에 SMF 추가

Oracle Solaris의 SMF(Service Management Facility) 기능에 응용 프로그램을 추가하여 신뢰할 수 있는 사용자 또는 역할로 응용 프로그램 구성을 제한할 수 있습니다.

자세한 내용 및 절차를 보려면 다음을 참조하십시오.

- **Oracle Solaris 관리: 보안 서비스**의 "RBAC 등록 정보를 레거시 응용 프로그램에 추가하는 방법"
- Securing MySQL using SMF - the Ultimate Manifest (`http://blogs.oracle.com/bobn/entry/securing_mysql_using_smf_the`).
- 선택한 매뉴얼 페이지에는 `smf(5)`, `smf_security(5)`, `svcadm(1M)` 및 `svccfg(1M)`이 포함됩니다.

시스템의 BART 스냅샷 만들기

시스템을 구성한 후 하나 이상의 BART 매니페스트를 만들 수 있습니다. 이러한 매니페스트는 시스템에 대한 스냅샷을 제공합니다. 그런 다음 일반 스냅샷 및 비교에 대한 일정을 잡을 수 있습니다. 자세한 내용은 49 페이지 "기본 감사 보고 도구 사용"을 참조하십시오.

다중 레벨(레이블 지정) 보안 추가

Trusted Extensions는 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 집합으로 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

`group/feature/trusted-desktop` 패키지는 Oracle Solaris의 신뢰할 수 있는 다중 레벨 데스크탑 환경을 제공합니다.

Trusted Extensions 구성

Trusted Extensions 패키지를 설치한 후 시스템을 구성해야 합니다. 패키지 설치 후 시스템은 랩탑 또는 워크스테이션과 같이 직접 연결된 비트맵 지연 표시를 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 관리: IP 서비스**의 14 장, "IP 보안 아키텍처(개요)"
- **Trusted Extensions 구성 및 관리**의 "레이블이 있는 IPsec 관리"
- **Trusted Extensions 구성 및 관리**의 "레이블이 있는 IPsec 구성(작업 맵)"

◆ ◆ ◆ 3 장

3 Oracle Solaris 11 보안 모니터링 및 유지 관리

Oracle Solaris는 보안 모니터링을 위한 두 가지 시스템 도구인 BART(기본 감사 보고 도구) 기능 및 감사 서비스를 제공합니다. 개별 프로그램 및 응용 프로그램에서도 액세스 및 사용 로그를 만들 수 있습니다.

기본 감사 보고 도구 사용

BART 매니페스트는 시스템에 설치된 정적 레코드를 제공합니다. 시간이 경과된 후 그리고 시스템 간에 BART 매니페스트를 비교하여 설치된 시스템에 대한 변경 사항을 추적하고 시스템 간의 차이점을 추적할 수 있습니다.

자세한 내용 및 절차를 보려면 다음을 참조하십시오.

- **Oracle Solaris 관리: 보안 서비스**의 "기본 감사 보고 도구(개요)"
- **Oracle Solaris 관리: 보안 서비스**의 "BART 사용(작업)"
- **Oracle Solaris 관리: 보안 서비스**의 "BART 매니페스트, 규칙 파일 및 보고서(참조)"

설치된 시스템에 대한 변경 사항을 추적하기 위한 자세한 지침은 **Oracle Solaris 관리: 보안 서비스**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 서비스는 **Oracle Solaris 관리: 보안 서비스**의 제VII부, "Oracle Solaris에서 감사"를 참조하십시오.

- **Oracle Solaris 관리: 보안 서비스**의 26 장, "감사(개요)"
- **Oracle Solaris 관리: 보안 서비스**의 27 장, "감사 계획"
- **Oracle Solaris 관리: 보안 서비스**의 28 장, "감사 관리(작업)"
- **Oracle Solaris 관리: 보안 서비스**의 29 장, "감사(참조)"

  매뉴얼 페이지 목록 및 링크는 **Oracle Solaris 관리: 보안 서비스**의 "감사 서비스 매뉴얼 페이지"를 참조하십시오.

사이트 요구 사항을 충족하려면 다음 감사 서비스 절차를 수행하면 됩니다.

- 감사를 구성하고, 감사 서비스를 시작 및 중지하기 위한 역할을 개별적으로 만드십시오.

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

  역할을 만들려면 **Oracle Solaris 관리: 보안 서비스**의 "역할을 만드는 방법"을 참조하십시오.
- `syslog` 유틸리티에서 감사 이벤트에 대한 텍스트 요약을 모니터합니다.

  `audit_syslog` 플러그인을 활성화하고 보고된 이벤트를 모니터합니다.

  Oracle Solaris 관리: 보안 서비스의 "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 관리: 보안 서비스**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.

audit_syslog 감사 요약 모니터링

`audit_syslog` 플러그인을 사용하면 미리 선택한 감사 이벤트에 대한 요약을 기록할 수 있습니다.

다음과 비슷한 명령을 실행하여 생성되는 감사 요약을 터미널 창에 표시할 수 있습니다.

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

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 관리: 보안 서비스**의 "감사 로그"
- **Oracle Solaris 관리: 보안 서비스**의 "감사 추적 오버플로우를 막는 방법"
- **Oracle Solaris 관리: 보안 서비스**의 "로컬 시스템에서 감사 레코드 관리(작업)"

허위 파일 찾기

프로그램에서 인증되지 않은 방식으로 사용되었을 수 있는 `setuid` 및 `setgid` 권한을 찾을 수 있습니다. 의심스러운 실행 파일은 시스템 계정이 아닌 사용자에게 소유권을 부여할 수 있습니다(예: `root` 또는 `bin`).

절차 및 예를 보려면 **Oracle Solaris 관리: 보안 서비스**의 "특수 파일 사용 권한이 있는 파일을 찾는 방법"을 참조하십시오.

◆ ◆ ◆ 부 록 A

Oracle Solaris 보안 문서 목록

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

Oracle Solaris 11 참조

다음 서적 및 문서에는 Oracle Solaris 11 시스템에 대한 보안 설명이 포함됩니다.

- **Oracle Solaris 관리: 보안 서비스**

  이 보안 설명서는 Oracle Solaris 11 관리자용으로 Oracle에서 출간했습니다. 이 설명서는 Oracle Solaris의 보안 기능과 시스템 구성 시 사용 방법을 설명합니다. 서문에는 보안 정보가 포함되었을 수 있는 다른 Oracle Solaris 시스템 관리 설명서에 대한 링크가 들어 있습니다.

- **Oracle Solaris Security: Oracle Solaris Express (`http://www.oracle.com/technetwork/articles/servers-storage-admin/os11esecurity-186797.pdf`)**

  이 문서에서는 이 릴리스의 2010년 11월 버전에 대한 Oracle Solaris 보안 기능의 스냅샷을 제공합니다.

- ORACLE SOLARIS 11 EXPRESS 2010.11 (`http://www.oracle.com/technetwork/server-storage/solaris11/documentation/solaris-express-whatsnew-201011-175308.pdf`)

  이 문서에서는 이 릴리스의 2010년 11월 버전에 대한 Oracle Solaris 기능의 스냅샷을 제공합니다.

유용한 Oracle Solaris 10 참조 자료를 보려면 **Oracle Solaris 10 Security Guidelines**을 참조하십시오.