



Solaris™ Security Toolkit

4.2 관리 지침서

Sun Microsystems, Inc.
www.sun.com

부품 번호: 819-3790-10
2005년 11월, 개정판 A

다음 사이트로 이 설명서에 대한 귀하의 의견을 보내주십시오: <http://www.sun.com/hwdocs/feedback>

Copyright 2005 Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, California 95054 U.S.A. All rights reserved. 모든 권리는 저작권자의 소유입니다.

Sun Microsystems, Inc.는 본 설명서에 나오는 제품에 구현된 기술과 관련한 지적 재산권을 보유합니다. 특히 이러한 지적 재산권에는 <http://www.sun.com/patents>에 나열된 하나 이상의 미국 특허와 미국 또는 기타 국가에서의 하나 이상의 추가 특허 또는 출원 중인 제품이 포함될 수 있습니다.

본 설명서 및 관련 제품은 사용, 복사, 배포 및 역컴파일을 제한하는 라이선스 하에서 배포됩니다. 본 제품 또는 설명서의 어떠한 부분도 Sun 및 Sun 소속 라이선스 부여자(있는 경우)의 사전 서면 승인 없이는 어떠한 형태나 수단으로도 재생산할 수 없습니다.

글꼴 기술을 포함한 타사 소프트웨어는 Sun 공급자에게 저작권이 있으며 사용 허가를 받았습니다.

이 제품의 일부는 University of California에서 승인된 Berkeley BSD 시스템에 기초합니다. UNIX는 미국 및 기타 국가의 등록 상표로서 X/Open Company, Ltd.를 통해 독점 사용권을 부여 받았습니다.

Sun, Sun Microsystems, Sun 로고, Sun BluePrints, Solaris, SunOS, Java, JumpStart, Sun4U, SunDocs 및 Solstice DiskSuite는 미국 및 기타 국가에 있는 Sun Microsystems, Inc.의 서비스 상표, 상표 또는 등록 상표입니다.

모든 SPARC 상표는 라이선스 하에서 사용되며 미국 및 기타 국가에서 SPARC International, Inc.의 상표 또는 등록 상표입니다. SPARC 상표가 부착된 제품은 Sun Microsystems, Inc.가 개발한 구조에 기초합니다. ORACLE은 Oracle Corporation의 등록 상표입니다.

OPEN LOOK과 Sun™ Graphical User Interface는 Sun Microsystems, Inc.가 사용자와 승인자를 위해 개발한 것입니다. Sun은 Xerox사의 컴퓨터 산업을 위한 비주얼 또는 그래픽 사용자 인터페이스의 개념 연구와 개발에 대한 선구적 업적을 높이 평가합니다. Sun은 Xerox와 Xerox Graphical User Interface에 대한 비독점적 사용권을 보유하고 있습니다. 이 권한은 OPEN LOOK GUI를 구현하는 Sun의 승인자에게도 해당되며 Sun의 서면 허가 계약에 기초합니다.

미국 정부의 권리—상용. 정부 사용자는 Sun Microsystems, Inc.의 표준 사용권 계약과 해당 FAR 규정 및 보충 규정을 준수해야 합니다.

이 출판물은 "있는 그대로" 제공되며 상업성, 특정 목적에 대한 적합성 또는 비침해성에 대한 모든 묵시적 보증을 포함하여 모든 명시적 또는 묵시적 조건, 표현 및 보증에 대해 어떠한 책임도 지지 않습니다. 이러한 보증 부인은 법적으로 허용된 범위 내에서만 적용됩니다.



재활용
가능



Adobe PostScript

목차

머리말 xvii

1. 서론 1

Solaris Security Toolkit 소프트웨어를 사용한 시스템 보안 1

JumpStart 모드 2

독립형 모드 2

소프트웨어 구성요소 이해 3

디렉토리 4

Audit 디렉토리 4

Documentation 디렉토리 5

man 디렉토리 5

Drivers 디렉토리 5

Files 디렉토리 8

Finish 디렉토리 9

OS 디렉토리 10

Packages 디렉토리 10

Patches 디렉토리 11

Profiles 디렉토리 11

Sysidcfg 디렉토리 11

데이터 저장소 12

	버전 제어 유지	12
	Solaris Security Toolkit 소프트웨어 구성 및 사용자 정의	13
	방침 및 요구사항	13
	지침	14
2.	시스템 보안: 방법론 적용	17
	계획 및 준비	17
	위험 및 수익 고려	18
	보안 방침, 표준 및 관련 문서 검토	19
	예 1	19
	예 2	20
	응용 프로그램 및 서비스 요구사항 판별	20
	응용프로그램 및 작동 서비스 목록 명세 식별	20
	서비스 요구사항 판별	21
	Solaris Security Toolkit 프로파일 개발 및 구현	29
	소프트웨어 설치	29
	설치 전 작업 수행	30
	데이터 백업	30
	시스템 안정성 확인	30
	설치 후 작업 수행	31
	응용프로그램 및 서비스 기능성 확인	31
	보안 프로파일 설치 확인	31
	응용 프로그램 및 서비스 기능성 확인	32
	시스템 보안 유지보수	32
3.	보안 소프트웨어 업그레이드, 설치 및 실행	35
	계획 및 설치 전 작업 수행	36
	소프트웨어 종속성	36
	사용할 모드 판별	36

독립형 모드	37
JumpStart 모드	37
업그레이드 절차	38
▼ Solaris Security Toolkit 소프트웨어 및 Solaris 운영체제 업그레이드	38
▼ Solaris Security Toolkit 소프트웨어만 업그레이드	39
Solaris OS만 업그레이드	40
보안 소프트웨어 다운로드	40
Solaris Security Toolkit 소프트웨어 다운로드	40
▼ pkg 버전 다운로드	41
Recommended Patch Cluster 소프트웨어 다운로드	42
▼ Recommended Patch Cluster 소프트웨어 다운로드	42
FixModes 소프트웨어 다운로드	43
▼ FixModes 소프트웨어 다운로드	44
OpenSSH 소프트웨어 다운로드	44
▼ OpenSSH 소프트웨어 다운로드	45
MD5 소프트웨어 다운로드	45
▼ MD5 소프트웨어 다운로드	46
보안 프로파일 사용자 정의	47
소프트웨어 설치 및 실행	47
독립형 모드에서 소프트웨어 실행	48
▼ 독립형 모드에서 소프트웨어 실행	51
감사 옵션	52
제거 옵션	52
도움말 표시 옵션	53
드라이버 옵션	54
전자 우편 통지 옵션	55
실행 내역 옵션	56
최근 실행 옵션	56

	출력 파일 옵션	57
	정숙 출력 옵션	57
	루트 디렉토리 옵션	57
	실행 취소 옵션	58
	JumpStart 모드에서 소프트웨어 실행	58
	▼ JumpStart 모드에서 소프트웨어 실행	58
	시스템 수정 검증	59
	서비스에 대한 QA 점검 수행	59
	구성의 보안 평가 수행	60
	보안 프로파일 검증	60
	설치 후 작업 수행	61
4.	시스템 변경 취소	63
	변경사항이 로깅되고 취소되는 방법 이해	63
	시스템 변경 실행 취소 요구사항	64
	변경을 실행 취소하도록 스크립트 사용자 정의	65
	수동으로 변경된 파일 점검	66
	실행 취소 기능에서 옵션 사용	67
	백업 옵션	68
	강제 옵션	68
	보존 옵션	68
	출력 파일 옵션	69
	정숙 출력 옵션	69
	전자 우편 통지 옵션	69
	시스템 변경 실행 취소	70
	▼ Solaris Security Toolkit 작업 실행 취소	70
5.	JumpStart 서버 구성 및 관리	77
	JumpStart 서버 및 환경 구성	78

▼ JumpStart 모드 구성	78
JumpStart 프로파일 템플릿 사용	80
core.profile	80
end-user.profile	81
developer.profile	81
entire-distribution.profile	81
oem.profile	81
minimal-SunFire_Domain*.profile	81
클라이언트 추가 및 제거	82
add-client 스크립트	82
rm-client 스크립트	84
6. 시스템 보안 감사	85
보안 유지	85
강화하기 전 시스템 검토	86
보안 감사 사용자 정의	86
보안 감사 준비	87
옵션 사용 및 감사 출력 제어	88
명령줄 옵션	88
도움말 표시 옵션	89
전자 우편 통지 옵션	90
출력 파일 옵션	91
정숙 옵션	91
상세 옵션	91
배너 및 메시지 출력	92
호스트 이름, 스크립트 이름 및 시간 소인 출력	95
보안 감사 수행	96
▼ 보안 감사 수행	96

7. 시스템 보안	101
계획 및 준비	101
가정 및 제한사항	102
시스템 환경	103
보안 요구사항	103
보안 프로파일 작성	103
소프트웨어 설치	104
보안 소프트웨어 다운로드 및 설치	104
▼ 보안 소프트웨어 다운로드 및 설치	104
패치 설치	105
▼ 패치 설치	105
OS Cluster 지정 및 설치	105
▼ OS 클러스터 지정 및 설치	106
JumpStart 서버 및 클라이언트 구성	107
기반구조 준비	107
▼ 기반구조 준비	107
Rules 파일 확인 및 검사	110
강화 구성 사용자 정의	111
FTP 서비스 사용	112
▼ FTP 서비스 사용	112
Secure Shell 소프트웨어 설치	113
▼ Secure Shell 설치	113
RPC 서버 사용	114
▼ RPC 사용	115
syslog.conf 파일 사용자 정의	115
▼ syslog.conf 파일 사용자 정의	115
클라이언트 설치	116
▼ 클라이언트 설치	117

품질 보증 검사 117

▼ 프로파일 설치 확인 117

▼ 응용 프로그램 및 서비스 기능 확인 118

용어 121

색인 129

그림

그림 1-1	소프트웨어 구성요소 구조	3
그림 1-2	드라이버 제어 흐름	7

표

표 1-1	사용자 정의 파일에 대한 이름 지정 표준	14
표 2-1	최근에 사용 중인 서비스 목록	27
표 3-1	<code>jass-execute</code> 와 함께 사용하는 명령줄 옵션	49
표 4-1	실행 취소 명령과 함께 명령줄 옵션 사용	67
표 5-1	JumpStart <code>add-client</code> 명령	83
표 5-2	JumpStart <code>rm-client</code> 명령	84
표 6-1	감사 명령과 함께 명령줄 옵션 사용	88
표 6-2	감사 상세 레벨	92
표 6-3	감사 출력에 배너 및 메시지 표시	93
표 6-4	호스트 이름, 스크립트 이름 및 시간 소인 감사 출력 표시	95

코드 예

코드 예 1-1	드라이버 제어 흐름 코드	8
코드 예 2-1	파일 시스템 개체에 대한 정보 획득	22
코드 예 2-2	실행 중 프로세스로부터 정보 수집	22
코드 예 2-3	동적으로 로드된 응용 프로그램 식별	23
코드 예 2-4	구성 파일을 사용 중인지 판별	24
코드 예 2-5	RPC를 사용하는 응용 프로그램 판별	25
코드 예 2-6	rusers 서비스 검증	26
코드 예 2-7	RPC를 사용하는 응용 프로그램을 판별하기 위한 대체 방법	27
코드 예 2-8	서비스 또는 응용 프로그램에 있는 포트 판별	28
코드 예 2-9	파일 및 포트를 사용 중인 프로세스 판별	28
코드 예 3-1	패치 파일을 /opt/SUNWjass/Patches 디렉토리로 이동	43
코드 예 3-2	독립형 모드의 명령줄 사용 예제	48
코드 예 3-3	독립형 모드에서 소프트웨어 실행	51
코드 예 3-4	예제 -c 옵션 출력	52
코드 예 3-5	예제 -h 옵션 출력	53
코드 예 3-6	예제 -d 드라이버 옵션 출력	55
코드 예 3-7	예제 -H 옵션 출력	56
코드 예 3-8	예제 -l 옵션 출력	56
코드 예 3-9	예제 -o 옵션 출력	57
코드 예 3-10	예제 -q 옵션 출력	57

코드 예 4-1	수동으로 변경된 파일의 예제 출력	66
코드 예 4-2	실행 취소할 수 있는 작업의 예제 출력	71
코드 예 4-3	복수 목록 파일 항목을 처리하는 실행 취소 작업의 예제 출력	72
코드 예 4-4	실행 취소 예외의 예제 출력	73
코드 예 4-5	실행 취소 중 백업 옵션 선택의 예제 출력	73
코드 예 4-6	실행 취소 중 항상 백업 옵션 선택의 예제 출력	75
코드 예 6-1	예제 -h 옵션 출력	90
코드 예 6-2	예제 -o 옵션 출력	91
코드 예 6-3	예제 -q 옵션 출력	91
코드 예 6-4	감사 실패만을 보고하는 예제 출력	93
코드 예 6-5	감사 로그 항목의 예제 출력	95
코드 예 6-6	감사 실행의 출력 예	98
코드 예 7-1	JumpStart 서버에 클라이언트 추가	107
코드 예 7-2	프로파일 작성	108
코드 예 7-3	수정된 스크립트의 출력 예제	109
코드 예 7-4	rules 파일의 정확성 검사	109
코드 예 7-5	rules 파일의 예제 출력	110
코드 예 7-6	잘못된 스크립트의 예제	111
코드 예 7-7	올바른 스크립트의 예제	111
코드 예 7-8	수정된 xsp-firewall-hardening.driver의 출력 예제	116
코드 예 7-9	보안 구성 평가	118

머리말

이 설명서에서는 Solaris™ Security Toolkit 소프트웨어의 이해 및 사용을 위한 참고 정보를 제공합니다. 이 설명서는 주로 Solaris Security Toolkit 소프트웨어를 사용하여 Solaris™ 운영체제(OS) 버전 8, 9 및 10 버전 및 관리자, 컨설턴트 및 새로운 Sun 시스템을 배포하거나 배포 시스템의 보안을 설정할 사용자를 대상으로 합니다. 이 지침은 JumpStart™ 모드 또는 독립형 모드에서 소프트웨어를 사용하는 데 적용됩니다.

본 설명서를 읽기 전에

사용자는 Solaris™에 대한 Sun 인증 시스템 관리자 또는 Solaris™ 운영체제에 대한 Sun 인증 네트워크 관리자여야 합니다. 또한 독립형 네트워크 프로토콜 및 토폴로지를 이해해야 합니다.

이 문서는 다양한 보안 경험이나 지식이 있는 사람에게 유용하도록 고안되었기 때문에 사용자의 경험과 지식이 이 문서를 사용하는 방법을 결정합니다.

이 설명서의 구성

이 설명서는 사용자 안내서로 사용됩니다. 각 장에는 시스템 보안을 위해 소프트웨어를 사용하기 위한 정보, 지시사항 및 지침이 들어있습니다. 이 문서는 다음과 같이 구성됩니다.

1 장은 Solaris Security Toolkit 소프트웨어의 설계 및 목적에 대해 설명합니다. 핵심 구성요소, 기능, 이점 및 지원 플랫폼을 다룹니다.

2 장은 시스템 보안 방법론에 대해 설명합니다. 이 소프트웨어를 사용하여 시스템의 보안을 설정하기 전에 Solaris Security Toolkit 프로세스를 적용할 수 있습니다.

3 장은 Solaris Security Toolkit 소프트웨어 및 기타 보안 관련 소프트웨어 다운로드, 설치 및 실행에 대한 지시사항을 제공합니다.

4 장은 강화 작업 중에 Solaris Security Toolkit 소프트웨어를 통해 수행된 변경사항의 역전(실행 취소)에 대한 정보 및 절차를 제공합니다.

5 장은 Solaris Security Toolkit 소프트웨어를 사용하기 위한 JumpStart 서버 구성 및 관리 정보를 제공합니다.

6 장은 Solaris Security Toolkit 소프트웨어를 사용하여 시스템의 보안을 감사(검증)하는 방법에 대해 설명합니다. 강화 후에 설정된 보안 프로파일 유지보수에 대해서는 이 장의 정보와 절차를 사용하십시오.

7 장은 새로운 시스템을 설치 및 보안하기 위해 이전 장에서 제공되는 정보와 전문 지식을 실현 가능한 시나리오에 적용하는 방법에 대해 설명합니다.

UNIX 명령어 사용

이 문서는 시스템 종료, 시스템 시동 및 장치 구성과 같은 기본 UNIX® 명령어 및 절차를 포함하지 않을 수도 있습니다. 이 정보에 대해서는 다음을 참조하십시오.

- 시스템과 함께 제공된 소프트웨어 설명서
- 다음 웹 사이트에서 나오는 Solaris 운영체제 설명서

<http://docs.sun.com>

셸 프롬프트

셸	프롬프트
C 셸	시스템이름%
C 셸 슈퍼유저	시스템이름#
Bourne 셸 및 Korn 셸	\$
Bourne 셸 및 Korn 셸 슈퍼유저	#

표기 규칙

서체 또는 기호*	의미	예
AaBbCc123	명령어 및 파일, 디렉토리 이름; 컴퓨터 화면에 출력되는 내용입니다.	.login 파일을 편집하십시오. 모든 파일 목록을 보려면 <code>ls -a</code> 명령어를 사용하십시오. % You have mail.
AaBbCc123	사용자가 입력하는 내용으로 컴퓨터 화면의 출력 내용과 반대입니다.	% su Password:
AaBbCc123	새로 나오는 용어, 강조 표시할 용어입니다. 명령줄 변수를 실제 이름이나 가치 값으로 바꾸십시오.	이는 <i>class</i> 옵션입니다. 이를 실행하기 위해서는 반드시 슈퍼유저여야 합니다. 파일 삭제 명령어는 rm filename 입니다.
AaBbCc123	책 제목, 장, 절	Solaris 사용자 설명서 6장 데이터 관리를 참조하시기 바랍니다.

* 사용자가 사용하는 브라우저의 설정과 이 설정이 다를 수 있습니다.

하드웨어 모델에 대한 일반 용어 사용

Sun Fire™ 최고급 시스템의 모델 번호는 다음과 같습니다.

- E25K
- E20K
- 15K
- 12K

Sun Fire™ 중급 시스템의 모델 번호는 다음과 같습니다.

- E6900
- E4900
- 6800
- 4810
- 4800
- 3800

Sun Fire™ 엔트리 레벨 시스템의 모델 번호는 다음과 같습니다.

- E2900
- Netra 1280
- V1280
- V890
- V880
- V490
- V480

지원되는 하드웨어 시스템

Solaris Security Toolkit 4.2 소프트웨어는 Solaris 10 OS를 실행하는 64비트 SPARC® 및 x86/x64 시스템을 지원합니다. Solaris Security Toolkit 4.2 소프트웨어는 Solaris 8 및 9에서 실행되는 SPARC 32 비트 시스템(예: Ultra 2 Creator 3D)을 지원하지 않습니다.

지원되는 Solaris OS 버전

Solaris Security Toolkit 소프트웨어에 대한 Sun의 지원은 Solaris 8, Solaris 9 및 Solaris 10 운영체제에서 사용할 때만 가능합니다.

참고 – Solaris Security Toolkit 4.2 소프트웨어를 실행하는 Solaris 10은 Sun Fire 최고급 시스템 도메인에서만 사용되며 시스템 제어기에서는 사용할 수 없습니다.

해당 소프트웨어가 Solaris 2.5.1, Solaris 2.6 및 Solaris 7 운영체제에서 사용될 경우, Sun 지원을 이용할 수 없습니다.

Solaris Security Toolkit 소프트웨어는 자동으로 설치된 Solaris 운영체제 소프트웨어의 버전을 감지한 후 운영체제 버전에 적합한 작업을 실행합니다.

이 설명서에 제공되는 예에서 스크립트가 OS 버전을 확인할 때, 해당 스크립트는 Solaris OS 버전인 2.x, 7, 8, 9 또는 10 대신에 SunOS™ 버전인 5.x를 확인합니다. 표 P-1은 SunOS와 Solaris OS 버전의 상호 관계를 나타냅니다.

표 P-1 SunOS와 Solaris OS 버전의 상호 관계

SunOS 버전	Solaris OS 버전
5.5.1	2.5.1
5.6	2.6
5.7	7
5.8	8
5.9	9
5.10	10

지원되는 SMS 버전

Sun Fire 최고급 시스템에 시스템 제어기(SC)를 실행할 때 SMS(System Management Services)를 사용하는 경우, Solaris Security Toolkit 4.2 소프트웨어는 Solaris 8 및 9 OS 버전에서 모두 지원됩니다(SMS 1.3, 1.4.1 및 1.5 버전과 함께 사용할 경우). Solaris Security Toolkit 2.4 소프트웨어가 설치된 Solaris 10 OS의 경우, 어떠한 버전의 SMS도 지원되지 않습니다.

참고 – Solaris Security Toolkit 4.2 소프트웨어를 실행하는 Solaris 10은 도메인에서만 사용되며 시스템 제어기에서는 사용할 수 없습니다.

관련 문서

온라인 설명서는 다음 주소에서 사용할 수 있습니다.

[http://www.sun.com/products-n-solutions/hardware/docs/
Software/enterprise_computing/systems_management/sst/index.html](http://www.sun.com/products-n-solutions/hardware/docs/Software/enterprise_computing/systems_management/sst/index.html)

적용 범위	제목	부품 번호	형식	위치
릴리스 노트	Solaris Security Toolkit 4.2 릴리스 노트	819-3797-10	PDF HTML	온라인
참조	Solaris Security Toolkit 4.2 Reference Manual	819-1503-10	PDF HTML	온라인
man 페이지	Solaris Security Toolkit 4.2 Man Page Guide	819-1505-10	PDF	온라인

설명서, 지원, 및 교육

Sun 제공 기능	URL	설명
Documentation	http://www.sun.com/documentation	PDF 및 HTML 문서 다운로드, 인쇄 문서 주문
지원	http://www.sun.com/blueprints	기술 지원 요구 및 패치 다운로드
교육	http://www.sun.com/blueprints	Sun 교육과정 소식

타사 웹 사이트

Sun은 이 설명서에 언급된 타사 웹 사이트의 이용 여부에 대해 책임지지 않습니다. Sun은 해당 사이트 또는 자원을 통해 사용 가능한 내용, 광고, 제품 또는 기타 자료에 대해 보증하거나 책임지지 않습니다. Sun은 그러한 사이트 또는 자원을 통해 사용 가능한 내용, 상품 또는 서비스의 사용이나 신뢰에 의해 야기되는 실질적 또는 주장된 손해나 손실에 대해 책임지지 않습니다.

Sun은 여러분의 의견을 환영합니다

Sun은 설명서의 내용 개선에 노력을 기울이고 있으며, 여러분의 의견과 제안을 환영합니다. 다음 웹 사이트에 여러분의 의견을 제출하여 주십시오.

<http://www.sun.com/hwdocs/feedback>

아래와 같이 설명서의 제목과 부품 번호를 함께 적어 보내주시기 바랍니다.

Solaris Security Toolkit 4.2 관리 지침서, 부품 번호 819-3790-10

서론

이 장은 Solaris Security Toolkit 소프트웨어의 설계 및 용도에 대해 설명합니다. 핵심 구성요소, 기능, 이점 및 지원 플랫폼을 다룹니다. 이 장에서는 수정 및 전개의 버전 제어 유지를 위한 지침을 제공하며, Solaris Security Toolkit 소프트웨어의 사용자 정의를 위한 중요 지침을 설명합니다.

이 장에서는 다음 주제를 다룹니다.

- 1페이지에 "Solaris Security Toolkit 소프트웨어를 사용한 시스템 보안"
- 3페이지에 "소프트웨어 구성요소 이해"
- 12페이지에 "버전 제어 유지"
- 13페이지에 "Solaris Security Toolkit 소프트웨어 구성 및 사용자 정의"

Solaris Security Toolkit 소프트웨어를 사용한 시스템 보안

Solaris Security Toolkit 소프트웨어는 약식으로는 JASS(JumpStart Architecture and Security Scripts) 도구 세트로 알려져 있으며 안전한 Solaris OS 시스템을 구축하고 유지보수하기 위한 자동화되고 확장 가능하며 계량 가능한 체계를 제공합니다. Solaris Security Toolkit 소프트웨어를 사용하면 시스템의 보안을 강화하고, 감사를 수행할 수 있습니다.

다음은 이 설명서를 이해하기 위해 필요한 중요 용어에 대한 설명입니다.

- 강화 - Solaris OS 구성을 수정하여 시스템 보안 개선
- 감사 - 시스템 구성이 사전 정의된 보안 프로파일을 준수하는지 판별

참고 - 감사라는 용어는 보안 상태를 사전 정의된 보안 프로파일과 비교하여 보안 상태를 검증하는 Solaris Security Toolkit 소프트웨어의 자동화된 프로세스를 설명합니다. 이 용어의 사용으로 인해 감사 옵션을 사용한 후 시스템이 완전한 안전을 보장받는 것은 아닙니다.

- 점수 - 감사가 실행되는 동안 적발된 실패의 수 어떤 종류의 실패도 발견되지 않을 경우, 결과 점수는 0입니다. Solaris Security Toolkit은 실패가 감지될 때마다 점수 (취약성 값이라고도 함)에 1점씩 증가시킵니다.

Solaris Security Toolkit 소프트웨어의 설치에는 두 가지 모드가 있습니다. 이에 대해서는 본 절의 마지막 부분에서 짧게 설명합니다.

- 2페이지에 "JumpStart 모드"
- 2페이지에 "독립형 모드"

시스템의 설치 방법과 관계 없이 Solaris Security Toolkit 소프트웨어를 사용하여 시스템을 강화하고 최소화할 수 있습니다. 그런 다음 주기적으로 Solaris Security Toolkit 소프트웨어를 사용하여 보안된 시스템의 보안 프로파일이 우발적 또는 악의적으로 수정되었는지 감사하십시오.

JumpStart 모드

시스템 설치 및 구성은 가능한 한(이상적으로는 100%) 자동화되어야 합니다. 이 지침에는 OS 설치 및 구성, 네트워크 구성, 사용자 계정, 응용프로그램 및 강화가 포함되어 있습니다. Solaris OS 설치를 자동화하기 위해 사용 가능한 한 가지 기술이 JumpStart 소프트웨어입니다. JumpStart 소프트웨어는 사람의 간섭이 거의 또는 전혀 필요 없이 네트워크를 통해 시스템을 설치하는 체계를 제공합니다. Solaris Security Toolkit 소프트웨어는 JumpStart 소프트웨어 기반 설치에서 Solaris OS 시스템 강화와 연관된 대부분의 작업을 구현하고 자동화하는 프레임워크 및 스크립트를 제공합니다. Solaris Security Toolkit의 강화를 지원하는 모듈을 포함하고 JumpStart 기반 설치를 도와주는 JumpStart Enterprise Toolkit(JET)을 구하려면 다음의 Sun Software Download 사이트를 방문하십시오.

<http://www.sun.com/download/>

JumpStart 기술에 대한 자세한 정보는 Sun BluePrints™ 설명서 JumpStart Technology: Effective Use in the Solaris Operating Environment를 참조하십시오.

독립형 모드

Solaris Security Toolkit 소프트웨어에는 독립형 모드가 있습니다. 이 모드는 JumpStart 모드에서와 동일한 모든 강화 기능을 수행하는 기능을 제공하지만 전개된 시스템에서만 작동합니다. 두 가지 모드 모두에서 보안 수정 사항은 시스템에 대한 보안 요구사항과 일치하도록 사용자 정의할 수 있으며 또한 그렇게 되어야 합니다.

시스템의 설치 방법과 관계 없이 처음에 Solaris Security Toolkit 소프트웨어를 사용하여 시스템을 강화할 수 있습니다. 그런 다음 주기적으로 Solaris Security Toolkit 소프트웨어를 사용하여 보안된 시스템의 구성이 우발적이거나 악의적으로 수정되지 않았는지 감사하십시오.

소프트웨어 구성요소 이해

이 절에서는 Solaris Security Toolkit 소프트웨어 구성요소 구조의 개요를 제공합니다. Solaris Security Toolkit 소프트웨어는 파일 및 디렉토리의 집합입니다. 그림 1-1은 해당 구조를 보여줍니다.

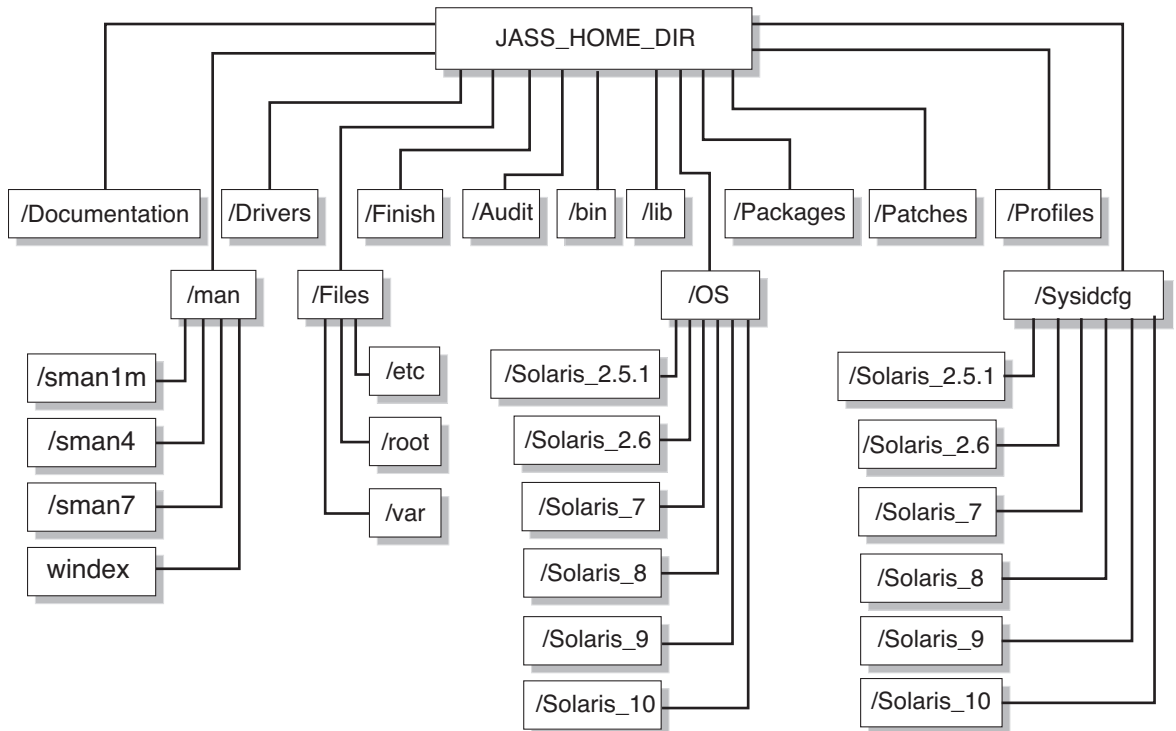


그림 1-1 소프트웨어 구성요소 구조

다음 프로그램 또는 명령 파일은 /bin 디렉토리에 포함되어 있습니다.

- add-client - JumpStart 환경에 클라이언트를 추가하기 위한 JumpStart 지원 프로그램

- `rm-client` - JumpStart 환경에서 클라이언트를 삭제하기 위한 JumpStart 지원 프로그램
- `make-jass-pkg` - 사용자 정의된 Solaris Security Toolkit 구성의 내부 분배를 단순화하기 위하여 Solaris Security Toolkit 디렉토리의 컨텐츠에서 Solaris OS 패키지를 생성할 수 있는 기능을 제공하는 명령
- `jass-check-sum` - Solaris Security Toolkit이 실행될 때마다 생성되는 체크섬을 기반으로 Solaris Security Toolkit 소프트웨어가 수정한 파일이 변경되었는지 판별하는 기능을 제공하는 명령
- `jass-execute` - Solaris Security Toolkit 소프트웨어의 대부분의 기능을 실행하는 명령

디렉토리

Solaris Security Toolkit 구조의 구성요소는 다음 디렉토리로 구성됩니다.

- /Audit
- /bin
- /Documentation
- /Drivers
- /Files
- /Finish
- /lib
- /man
- /OS
- /Packages
- /Patches
- /Profiles
- /Sysidcfg

이 절은 각 디렉토리에 대해 설명합니다. 적절한 위치에 각 스크립트, 구성 파일 또는 하위 디렉토리가 나열되며, 자세한 정보를 보기 위한 다른 장으로의 참조가 제공됩니다.

Solaris Security Toolkit 디렉토리 구조는 Sun BluePrints 설명서 *JumpStart Technology: Effective Use in the Solaris Operating Environment*를 참조하십시오.

Audit 디렉토리

이 디렉토리에는 시스템이 정의된 보안 프로파일 또는 감사 스크립트 세트를 준수하는지 평가하는 감사 스크립트가 들어있습니다. 이 디렉토리의 스트립트는 다음 범주로 구성됩니다.

- 사용 불가
- 사용 가능
- 설치

- 최소화
- 인쇄
- 제거
- 설정
- 업데이트

이러한 각 범주에 있는 스크립트의 상세한 목록과 각 스크립트의 설명에 대해서는 Solaris Security Toolkit 4.2 Reference Manual을 참조하십시오.

Documentation 디렉토리

이 디렉토리는 README, EOL_NOTICE 및 INSTALL 파일과 같은 사용자를 위한 정보 텍스트 파일을 포함합니다.

man 디렉토리

이 디렉토리에는 명령, 기능 및 드라이버에 대한 매뉴얼 페이지 절의 하위 디렉토리가 포함되어 있습니다. 이 디렉토리에는 특별히 제공된 명령 색인인 windex 파일도 포함되어 있습니다.

매뉴얼 페이지에 대한 자세한 정보는 실제 매뉴얼 페이지 또는 Solaris Security Toolkit 4.2 Man Page Guide를 참조하십시오.

Drivers 디렉토리

이 디렉토리에는 Solaris Security Toolkit 소프트웨어를 실행할 때 실행 및 설치되는 파일을 지정하는 구성 정보 파일이 들어있습니다. 이 디렉토리에는 드라이버, 스크립트 및 구성 파일이 포함되어 있습니다.

다음은 Drivers 디렉토리에 있는 드라이버 및 스크립트의 예입니다.

- audit_{private|public}.funcs
- common_{log|misc}.funcs
- {config|hardening|secure}.driver
- driver.{init|run}
- driver_{private|public}.funcs
- finish.init
- server-{config|hardening|secure}.driver
- suncluster3x-{config|hardening|secure}.driver
- sunfire_15k_sc-{config|hardening|secure}.driver
- undo.{funcs|init|run}
- user.init.SAMPLE
- user.run.SAMPLE

Solaris Security Toolkit과 함께 포함된 모든 드라이버는 각각 다음과 같은 세 개의 파일을 갖습니다.

- `name-{config|hardening|secure}.driver`

이 세 파일은 이전 목록에서 대괄호 안에 표시됩니다(예: `sunfire_15k_sc-{config|hardening|secure}.driver`). 이러한 파일은 완전성을 위해 나열됩니다. 드라이버를 실행하려는 경우에는 `secure.driver` 또는 `name-secure.driver` 만 사용하십시오. 해당 드라이버가 자동으로 관련 드라이버를 호출합니다.

Solaris Security Toolkit 구조는 실제 스크립트 자체를 수정하지 않지만 드라이버, 종료 및 감사 스크립트가 여러 환경에서 사용될 수 있도록 하는 구성 정보를 포함하고 있습니다. 종료 및 감사 스크립트에 사용되는 모든 변수는 구성 파일 세트에 유지됩니다. 드라이버는 이러한 구성 파일을 가져오며 변수를 호출하여 종료 및 감사 스크립트에서 사용할 수 있도록 합니다.

Solaris Security Toolkit 소프트웨어에는 다음과 같은 네 개의 기본 구성 파일이 있는데, 이 기본 구성 파일은 모두 `Drivers` 디렉토리에 저장됩니다.

- `driver.init`
- `finish.init`
- `user.init`
- `user.run`

`user.run` 파일은 있는 경우에 자동으로 사용되는 Solaris Security Toolkit 기능의 교체 또는 강화된 버전을 작성할 수 있는 위치를 제공합니다.



주의 - 반드시 `user.init` 구성 파일의 변수 정의만 변경하도록 합니다.
`driver.init` 및 `finish.init` 구성 파일의 변수 정의는 절대로 변경하지 마십시오.

드라이버가 호출하는 종료 스크립트는 `Finish` 디렉토리에 있습니다. 드라이버가 호출하는 감사 스크립트는 `Audit` 디렉토리에 있습니다. 드라이버가 설치하는 파일은 `Files` 디렉토리에서 읽습니다. 종료 스크립트에 대한 자세한 정보는 Solaris Security Toolkit 4.2 Reference Manual의 4장을 참조하십시오. 감사 스크립트에 대한 자세한 정보는 Solaris Security Toolkit 4.2 Reference Manual의 5장을 참조하십시오.

그림 1-2는 드라이버 제어 흐름의 흐름도를 보여줍니다.

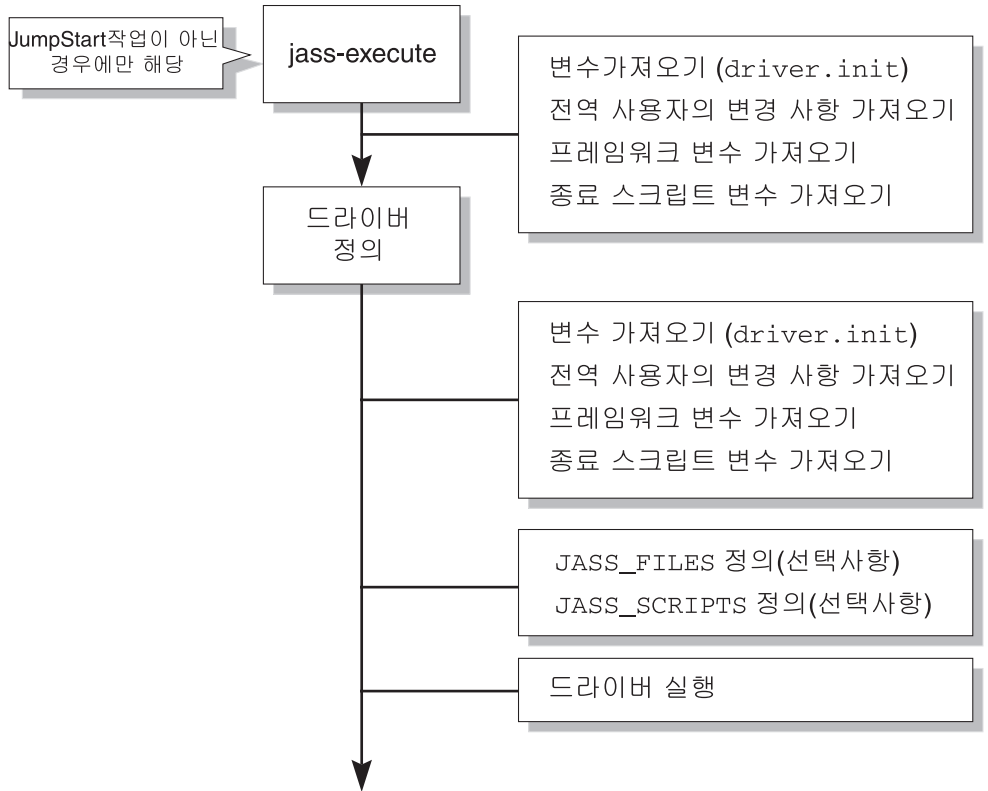


그림 1-2 드라이버 제어 흐름

1. JumpStart 실행이 아닌 경우, 드라이버는 `jass-execute` 명령을 실행합니다. JumpStart 실행의 경우에는 `jass-execute` 명령을 호출하지 않고 바로 드라이버를 호출합니다.
2. 드라이버가 명시적으로 변수를 설정할 수 있습니다.
3. 해당 드라이버는 여러 `.init` 파일에서 모든 환경 변수를 가져옵니다.
4. 해당 드라이버는 `JASS_FILES` 및 `JASS_SCRIPTS` 환경 변수를 정의합니다. 이 정의는 선택적입니다. 즉, 하나의 환경을 정의하거나 둘 다 정의하거나 둘 다 정의하지 않을 수 있습니다.

`JASS_FILES` 및 `JASS_SCRIPTS` 환경 변수 정의에 대한 자세한 내용은 Solaris Security Toolkit 4.2 Reference Manual 7장을 참조하십시오.
5. 드라이버는 `driver.run`을 호출하여 `JASS_FILE` 및 `JASS_SCRIPTS` 환경 변수에 의해 정의되는 작업을 수행합니다.

6. (선택사항) 드라이버는 특정 드라이버의 작동을 정의하며 이는 `finish.init` 또는 `user.init`의 시스템 기본 값을 겹쳐쓸 때 사용할 수 있습니다. 코드 예 1-1의 드라이버는 명시적으로 `JASS_PASS_HISTORY`를 4로 설정합니다.

코드 예 1-1은 드라이버 제어 흐름 코드를 보여줍니다.

코드 예 1-1 드라이버 제어 흐름 코드

```
DIR="`/bin/dirname $0`"
JASS_PASS_HISTORY="4"
export DIR
. ${DIR}/driver.init

JASS_FILES="
                                /etc/cron.d/cron.allow
                                /etc/default/ftpd
                                /etc/default/telnetd
"

JASS_SCRIPTS="
                                install-at-allow.fin
                                remove-unneeded-accounts.fin
"
. ${DIR}/driver.run
```

1. 이 코드 예제는 `DIR` 환경 변수를 설정하고 내보내서 드라이버가 시작 디렉토리를 인식하게 합니다.
2. 드라이버는 명시적으로 `JASS_PASS_HISTORY` 환경 변수를 4로 설정합니다.
3. 드라이버는 여러 개의 `.init` 파일을 읽습니다(`driver.init`부터 시작).
4. `JASS_FILES` 환경 변수가 클라이언트의 `JASS_HOME_DIR/Files` 디렉토리에서 복사되는 파일을 포함하도록 정의됩니다.
5. `JASS_SCRIPTS` 환경 변수가 Solaris Security Toolkit 소프트웨어에 의해 실행되는 종료 스크립트로 정의됩니다.
6. `driver.run` 드라이버를 호출하여 강화 작업의 실행이 시작됩니다. `driver.run`은 `JASS_FILES`에 의해 지정되는 파일을 복사하고, `JASS_SCRIPTS`로 지정되는 스크립트를 실행합니다.

Files 디렉토리

이 디렉토리는 `JASS_FILES` 환경변수 및 `driver.run` 스크립트에 의해 사용되어 JumpStart 클라이언트로 복사된 파일을 저장합니다.

이 디렉토리에 포함된 파일은 다음과 같습니다.

- /.cshrc
- /.profile
- /etc/default/sendmail
- /etc/dt/config/Xaccess
- /ftpd/banner.msg
- /etc/hosts.allow
- /etc/hosts.allow-15k_sc
- /etc/hosts.allow-server
- /etc/hosts.allow-suncluster
- /etc/hosts.deny
- /etc/init.d/klmmod
- /etc/init.d/nddconfig
- /etc/init.d/set-tmp-permissions
- /etc/init.d/sms_arpcnfig
- /etc/init.d/swapadd
- /etc/issue
- /etc/motd
- /etc/opt/ipf/ipf.conf
- /etc/opt/ipf/ipf.conf-15k_sc
- /etc/opt/ipf/ipf.conf-server
- /etc/security/audit_class+5.10
- /etc/security/audit_class+5.8
- /etc/security/audit_class+5.9
- /etc/security/audit_control
- /etc/security/audit_event+5.10
- /etc/security/audit_event+5.8
- /etc/security/audit_event+5.9
- /etc/sms_domain_arp
- /etc/sms_sc_arp
- /etc/syslog.conf
- /root/.cshrc
- /root/.profile
- /var/opt/SUNWjass/BART/rules
- /var/opt/SUNWjass/BART/rules-secure

Finish 디렉토리

이 디렉토리에는 실행 중에 시스템 수정 및 업데이트를 수행하는 종료 스크립트가 들어 있습니다. 이 디렉토리의 스크립트는 다음 범주로 구성됩니다.

- 사용 불가
- 사용 가능
- 설치
- 최소화
- 인쇄
- 제거

- 설정
- 업데이트

이러한 각 범주에 있는 스크립트의 상세한 목록과 각 스크립트의 설명에 대해서는 Solaris Security Toolkit 4.2 Reference Manual을 참조하십시오.

OS 디렉토리

이 디렉토리에는 Solaris OS 이미지만 들어있습니다. 이 이미지는 JumpStart 소프트웨어 설치 프로세스에서 클라이언트 설치를 위한 Solaris OS 소스로 사용됩니다. 이 디렉토리가 다음의 Solaris Security Toolkit OS 이름 지정 규칙을 따른다면, `add_client` 스크립트는 이 디렉토리에 포함된 Solaris OS 버전을 인수로서 사용합니다.

Solaris OS 이미지 로드 및 수정에 대한 자세한 정보는 Sun BluePrints 설명서 JumpStart Technology: Effective Use in the Solaris Operating Environment를 참조하십시오.

표준 설치 이름 지정 규칙을 따릅니다.

Solaris OS

Solaris OS의 경우 다음 이름 지정 표준 규칙을 사용하십시오.

`Solaris_os` 버전_CD 릴리스의 4자리 숫자 연도-2자리 숫자 월

예를 들어 2005년 5월자 Solaris 10 운영 환경 CD는 `Solaris_10_2005-03`의 디렉토리 이름을 갖습니다. Solaris OS의 업데이트와 릴리스를 구분하여 테스트 및 전개 목적으로 매우 정교한 제어를 유지할 수 있습니다.

x86/x64 플랫폼용 Solaris OS

x86/x64 플랫폼용 Solaris OS의 경우 아래의 디렉토리 이름 지정을 사용하십시오.

`Solaris_os` 버전_CD 릴리스의 4자리 숫자 연도-2자리 숫자 월_ia

예를 들어 x86/x64 플랫폼용 Solaris OS 릴리스가 2005년 4월자인 경우 디렉토리 이름은 `Solaris_10_2005-03_ia`입니다.

Packages 디렉토리

이 디렉토리에는 종료 스크립트로 설치하고 감사 스크립트로 검증할 수 있는 소프트웨어 패키지가 들어있습니다. 예를 들어, Open Secure Shell 소프트웨어 패키지는 Packages 디렉토리에 저장될 수 있으므로 올바른 종료 스크립트가 필요한 소프트웨어를 설치할 수 있습니다.

Solaris Security Toolkit 소프트웨어에 포함되어 있는 여러 종료 스크립트가 소프트웨어 설치, 기본 구성 및 검증 기능을 수행합니다. Packages 디렉토리에서 소프트웨어를 설치 및 검증하는 스크립트에는 다음이 포함됩니다.

- `install-fix-modes.{fin|aud}`
- `install-jass.{fin|aud}`
- `install-md5.{fin|aud}`
- `install-openssh.{fin|aud}`

Patches 디렉토리

이 디렉토리는 Solaris OS용 Recommended and Security Patch Clusters 저장을 위한 것입니다. 필수 패치를 이 디렉토리에 다운로드하고 압축을 풉니다.

이 디렉토리에 패치를 저장한 후 압축을 풀면 설치 능력을 올릴 수 있습니다. 패치의 압축이 이 디렉토리로 풀릴 때 Solaris Security Toolkit 소프트웨어의 패치 설치 스크립트가 설치를 자동화하므로 각 시스템 설치를 위해 패치 클러스터의 압축을 수동으로 풀 필요가 없게 됩니다.

사용되는 각 Solaris OS 버전에 대한 하위 디렉토리를 만듭니다. 예를 들어 Patches 디렉토리 안에 9_Recommended 및 10_Recommended 디렉토리를 만들 수 있습니다.

Solaris Security Toolkit 소프트웨어는 x86/x64 플랫폼용 Solaris OS 패치 클러스터를 지원합니다. 이러한 패치 클러스터에 지원되는 이름 지정 규칙은 SunSolve OnLineSM 서비스를 통해 사용 가능한 규칙과 동일합니다.

형식은 <release>_x86_Recommended입니다. x86/x64 플랫폼용 Solaris OS 패치 클러스터는 10_x86_Recommended라는 이름의 디렉토리에 있습니다.

Profiles 디렉토리

이 디렉토리에는 모든 JumpStart 프로파일이 들어있습니다. 이들 프로파일에는 설치할 Solaris OS 클러스터(예: 핵심, 일반 사용자, 개발자 또는 전체 배포), 디스크 배치 및 수행할 설치 유형(예: 독립형)을 판별하기 위해 JumpStart 소프트웨어가 사용하는 구성 정보가 들어있습니다.

JumpStart 프로파일은 특정 시스템 또는 시스템 그룹이 구축되는 방법을 정의하기 위해 rules 파일에 나열되고 사용됩니다.

Sysidcfg 디렉토리

Profiles 디렉토리와 비슷하게 Sysidcfg 디렉토리에는 JumpStart 모드 설치 중에만 사용되는 파일이 들어있습니다. 이 파일들은 필수 설치 정보를 제공하여 Solaris OS 설치를 자동화합니다. 별도의 디렉토리 트리가 정보를 운영체제별로 저장합니다.

각 Solaris OS는 개별 디렉토리를 갖습니다. 각 릴리스에 대해 Solaris_OS 버전으로 이름이 지정되는 디렉토리가 있습니다. Solaris Security Toolkit 소프트웨어에 Solaris OS 버전 2.5.1이상 10이하를 위한 예제 sysidcfg 파일이 포함되어 있습니다.

sysidcfg 예제 파일은 네트워크 또는 호스트 당 기타 유형으로 확장될 수 있습니다. Solaris Security Toolkit 소프트웨어는 임의의 sysidcfg 파일을 지원합니다.

sysidcfg 파일에 대한 추가 예제는 Sun BluePrints 설명서 JumpStart Technology: Effective Use in the Solaris Operating Environment를 참조하십시오.

데이터 저장소

JASS_HOME_DIR 디렉토리 구조에 포함되지 않는 데이터 저장소 또는 JASS_REPOSITORY 디렉토리는 Solaris Security Toolkit 실행 취소 작업을 지원하고 각 작업이 실행되는 방법에 대한 데이터, 소프트웨어가 수정한 파일의 목록 및 실행 로그 데이터를 저장합니다. 이 디렉토리는 /var/opt/SUNWjass/runs/시간소인에 위치합니다.

버전 제어 유지

Solaris Security Toolkit 소프트웨어가 사용하는 모든 파일 및 스크립트에 대한 버전 제어 유지는 다음 두 가지 이유 때문에 중요합니다.

1. 이 환경의 목표중 하나는 시스템 설치를 다시 작성할 수 있다는 것입니다. 이 목표는 설치 시 사용된 모든 파일 버전의 스냅샷이 없으면 불가능합니다.
2. 이 스크립트는 여러 조직에 중요한 보안 기능 프로세스를 수행하고 있으므로 꼭 필요하거나 테스트를 거친 변경만 수행하도록 매우 주의해야 합니다.

Source Code Control System(SCCS) 버전 제어 패키지가 Solaris OS SUNWsprout 패키지에서 제공됩니다. 프리웨어 및 상업용 제품으로 사용할 수 있는 기타 버전 제어 소프트웨어를 사용하여 버전 정보를 관리할 수 있습니다. 버전 제어 제품의 이름에 상관없이 업데이트를 관리하고 향후 시스템 재작성을 위해 버전 정보를 기록해두십시오.

버전 제어 이외에 무결성 관리 솔루션을 사용하여 파일의 내용이 수정되었는지 확인하십시오. 시스템 권한이 있는 사용자는 버전 제어 시스템을 우회할 수 있지만 원격 시스템에 무결성 데이터베이스를 유지하는 무결성 관리 시스템을 쉽게 우회할 수는 없습니다. 지역적으로 저장되는 데이터베이스는 악의적으로 수정될 수 있기 때문에 무결성 관리 솔루션은 중앙 집중될 때 최고의 성능을 갖습니다.

Solaris Security Toolkit 소프트웨어 구성 및 사용자 정의

Solaris Security Toolkit 소프트웨어에는 Sun BluePrints 설명서 Enterprise Security: Solaris Operating Environment Security Journal, Solaris Operating Environment Versions 2.5.1, 2.6, 7, and 8 및 보안 관련 Sun BluePrints OnLine 기사의 모든 보안 지침을 구현하는 스크립트, 프레임워크 기능 및 변수에 대한 기본값이 들어있습니다. 이러한 설정 값이 모든 시스템에 적합한 것은 아니므로, Solaris Security Toolkit 소프트웨어를 사용자 정의하여 사용 시스템의 보안 요구사항에 맞도록 합니다.

Solaris Security Toolkit 소프트웨어의 가장 중요한 특성 중 하나는 사용자의 환경, 시스템 및 보안 요구사항에 맞도록 쉽게 사용자 정의할 수 있다는 점입니다. Solaris Security Toolkit 소프트웨어를 사용자 정의하려면 드라이버, 종료 스크립트, 감사 스크립트, 프레임워크 기능, 환경 변수 및 파일 템플릿을 통해 소프트웨어의 활동을 조정하십시오.

대부분의 사용자는 Solaris Security Toolkit 코드를 수정할 필요가 없습니다. 사용자 환경에서 Solaris Security Toolkit 소프트웨어를 사용하기 위해 코드 수정이 절대적으로 필요한 경우, 코드를 `user.run`에 고유한 기능 이름으로 복사하여 14페이지에 "지침"에서와 같이 변경사항을 쉽게 추적할 수 있게 하십시오.

이 안내서에서는 Solaris Security Toolkit 소프트웨어 사용자 정의에 대한 안내 및 지침이 제공됩니다. 드라이버 사용자 정의에 대한 유용한 정보는 Solaris Security Toolkit 4.2 Reference Manual을 참조하십시오. 사용자 정의에는 파일 또는 변수 수정 및 작성이 포함됩니다.

이 안내서에서는 또한 Solaris Security Toolkit 소프트웨어 사용자 정의 예제를 제공합니다. 이 예제에서 Solaris Security Toolkit 소프트웨어를 사용자 정의할 수 있는 몇 가지 방법을 알려주지만, 그 이외에도 많은 방법이 있습니다.

다음 절은 Solaris Security Toolkit 소프트웨어의 사용자 정의 전에 명확히 이해해야 할 정보를 나타냅니다. 이 정보는 많은 전개에서 수집되는 공유된 경험을 바탕으로 하므로 일반적인 함정을 피할 수 있습니다.

방침 및 요구사항

Solaris Security Toolkit 소프트웨어를 사용자 정의 및 전개할 때 적합한 계획을 세우면 결과 플랫폼 구성이 올바르고 조직의 기대를 따를 수 있습니다.

계획 수립 단계에서 보안 방침 및 표준사항, 산업 규정 및 지침, 그리고 공급업체가 제공하는 바람직한 실례를 포함한 다양한 소스로부터 정보를 얻으십시오.

이 정보 외에 결과 구성이 플랫폼의 예정된 비즈니스 기능을 제공하는 능력에 영향을 주지 않도록 보장하기 위해 응용 프로그램 및 작업 요구사항을 고려해야 합니다.

지침

Solaris Security Toolkit 소프트웨어를 사용자 정의할 때 다음 지침을 고려하십시오. 이 지침을 이해하고 준수하면 전개를 유지하는 프로세스를 훨씬 더 쉽고 보다 효율적으로 만드는 데 도움이 됩니다.

- 일반적인 규칙으로서 Solaris Security Toolkit 소프트웨어와 함께 제공되는 어떤 원본 파일(드라이버, 스크립트, 파일 등)도 절대 수정하지 마십시오. 원본 파일을 변경하면 원본 파일에 대한 모든 변경이 파일의 새 버전에 의해 겹쳐 써질 수 있기 때문에 Solaris Security Toolkit 소프트웨어의 최신 버전으로 업그레이드하는 조직의 기능을 억제하고 제한합니다. (모든 사용자 정의 변경사항이 유실되고 시스템의 구성이 원하지 않는 방향으로 변경될 수 있습니다.)

파일을 사용자 정의하려면, 사본을 만든 후 원본은 그대로 두고 사본을 수정하십시오. 이 지침에는 다음과 같은 예외가 존재합니다.

- `sysidcfg` 파일
- Solaris Security Toolkit 4.2의 새로운 기능을 통해 `Files` 디렉토리의 템플릿에 키워드 접미어를 사용할 수 있습니다. 이렇게 하면 시스템 관리자가 Solaris Security Toolkit 4.2 소프트웨어에 포함된 어떤 기본 템플릿도 수정할 필요가 없어집니다. 적용 가능한 경우, 접미어를 사용하십시오.
- 드라이버 또는 스크립트의 사본에 이름을 지정하여 원본과 구별할 수 있게 하십시오. 스크립트의 목적을 표시하는 접두어나 키워드를 사용하십시오. 예를 들어 회사의 이름이나 증권 기호, 부서 식별자 심지어 플랫폼이나 응용 프로그램 유형을 포함하는 접두어가 모두 탁월한 이름 지정 표준입니다. 표 1-1은 몇 가지 이름 지정 표준의 예입니다.

표 1-1 사용자 정의 파일에 대한 이름 지정 표준

사용자 정의 파일	이름 지정 표준
<code>abccorp-secure.driver</code>	회사 접두어
<code>abcc-nj-secure.driver</code>	회사 증권 기호, 위치
<code>abbcorp-nj-webserver.driver</code>	회사, 위치, 응용프로그램 유형
<code>abc-nj-trading-webserver.driver</code>	회사, 위치, 조직, 응용프로그램 유형

- 다음 Solaris Security Toolkit 파일이 사용자 시스템에 적합한지 검토하십시오. 이 파일들을 사용자 정의하려면 사본의 이름을 `user.init` 및 `user.run`으로 바꾼 후 사본의 내용을 수정 또는 추가하십시오.

`Drivers/user.init.SAMPLE` 전역 매개변수 사용자 정의에 사용

`Drivers/user.run.SAMPLE` 전역 기능 사용자 정의에 사용

참고 - SUNWjass가 `pkgrm` 명령을 사용하여 제거되는 경우 `user.init` 및 `user.run` 파일은 작성된 경우에도 제거되지 않음을 명심하십시오. 이 작동은 또한 Solaris Security Toolkit 디렉토리 구조에 추가되고 최초 소프트웨어 분배에는 포함되지 않는 모든 고객 파일의 경우에 발생합니다.

참고 - Solaris Security Toolkit 4.2 소프트웨어에서는 새롭게 강화된 `pkgrm` 명령이 제공됩니다. 이 릴리스에서는 `pkgrm` 명령이 우선 배포판에 포함된 모든 파일의 무결성을 검사합니다. 다른 파일이 있을 경우, `pkgrm` 명령은 시스템 관리자에게 올바른 파일을 사용하거나 수정된 파일을 삭제하라는 오류 메시지를 표시하고 종료합니다.

시스템 보안: 방법론 적용

이 장은 시스템 보안 방법론을 제공합니다. 이 소프트웨어를 사용하여 시스템의 보안을 설정하기 전에 Solaris Security Toolkit 프로세스를 적용할 수 있습니다.

이 장에서는 다음 주제를 다룹니다.

- 17페이지에 "계획 및 준비"
- 29페이지에 "Solaris Security Toolkit 프로파일 개발 및 구현"
- 29페이지에 "소프트웨어 설치"
- 31페이지에 "응용프로그램 및 서비스 기능성 확인"
- 32페이지에 "시스템 보안 유지보수"

계획 및 준비

적절한 계획 수립은 Solaris Security Toolkit 소프트웨어를 사용하여 시스템을 성공적으로 보안하기 위한 핵심입니다. 계획 단계는 시스템의 응용 프로그램 및 작동 요구사항뿐만 아니라 조직의 보안 방침 및 표준을 기초로 하여 시스템을 위한 Solaris Security Toolkit 프로파일을 구성합니다. 이 단계는 다음 작업으로 구분됩니다.

- 18페이지에 "위험 및 수익 고려"
- 19페이지에 "보안 방침, 표준 및 관련 문서 검토"
- 20페이지에 "응용 프로그램 및 서비스 요구사항 판별"

이 설명서에서는 다루지 않지만 이 단계에 대한 기타 고려사항에는 위험 및 노출 이해, 기반구조 및 그의 보안 요구사항 이해 및 책임, 로깅 및 사용 감사가 포함될 수 있습니다.

위험 및 수익 고려

시스템을 강화할 때 Solaris Security Toolkit 소프트웨어가 구현된 후 시스템이 기능하도록 보장하기 위해 특별한 예방 조치를 취해야 합니다. 또한 모든 정지 시간을 가능한 최소화하기 위해 프로세스를 최적화하는 것도 중요합니다.

참고 - 전개된 시스템을 보안할 때에는 일부 경우에 조직이 시스템을 재구축하고 다시 설치할 때에 시스템을 강화한 후 작동에 필요한 모든 소프트웨어를 재로드하는 것이 훨씬 효과적일 수 있습니다.

이 절은 시스템을 보안하기 전에 명확하게 이해해야 하는 고려사항을 제공합니다. 위험과 수익을 주의깊게 검토하여 어떤 활동이 사용자 조직에 적합한지 판별하십시오.

1. 시스템에 대한 서비스 및 응용 프로그램의 요구사항을 이해하십시오.

Solaris Security Toolkit 소프트웨어를 실행하기 전에 시스템에서 실행 중인 서비스와 응용 프로그램을 식별해야 합니다. 서비스 및 응용 프로그램과 연관된 모든 종속성을 열거하여 Solaris Security Toolkit 소프트웨어의 구성을 충분히 조정할 수 있게 해야 합니다. 그렇게 하지 않으면 필요한 서비스를 사용할 수 없거나 시작하지 못할 수 있습니다. Solaris Security Toolkit 소프트웨어가 수행한 변경 사항이 대부분의 경우에 실행 취소될 수 있지만, 설치 전에 올바른 프로파일을 개발하면 Solaris Security Toolkit 소프트웨어 구현과 연관된 잠재적 정지 시간을 제한하게 됩니다.

2. 시스템을 오프라인한 후 재부팅해야 합니다.

Solaris Security Toolkit 소프트웨어 변경이 효력을 발생하려면 시스템을 재부팅해야 합니다. 시스템의 건전성, 시스템이 제공하는 서비스 및 유지보수 창고의 가용성에 따라서 조직은 소프트웨어 구현에 어려움을 겪을 수 있습니다. 보안을 강화하지 않았을 때의 위험에 대해 정지 시간의 비용을 신중히 평가하여 결정해야 합니다.

3. 기능성을 검증하기 위해 여러 번의 시스템 재부트가 필요할 수 있습니다.

가능할 경우, 임무 결정적 설정으로 시스템을 구현하기 전에 비생산 시스템에서 모든 변경을 수행하십시오. 이것이 항상 가능하지는 않습니다. 예를 들어 대상 환경을 효과적으로 미러링하는 충분한 하드웨어 또는 소프트웨어의 부족으로 인해 불가능할 수 있습니다. Solaris Security Toolkit 소프트웨어의 실행 전후에 테스트를 수행해야 합니다. 시스템이 강화된 후에 문제점 해결이 필요한 식별되지 않은 종속성이 여전히 존재할 수 있습니다. 대부분의 경우에 이들 문제는 이 장에서 설명하는 기법을 사용하여 상당히 빨리 해결할 수 있습니다. Solaris Security Toolkit 소프트웨어 실행 후에 기능성 문제점이 발견되는 경우 Solaris Security Toolkit 소프트웨어의 효과를 실행 취소하거나 누락된 기능성을 지원하고 활성화하는 시스템의 보안 구성을 더 변경하기 위해 추가로 플랫폼을 재부팅해야 할 수도 있습니다.

4. 플랫폼 보안은 단순한 강화 및 감사보다 많은 것을 요구합니다.

보안 상태를 향상시키기 위해 시스템 구성을 업데이트할 때, 플랫폼 강화 및 감사는 시스템, 서비스 및 데이터를 보호하기 위해 수행할 수 있고 수행해야 미소한 부분이라는 것을 알아야 합니다. 추가 대책 및 제어 처리는 이 문서의 범위를 벗어나지만,

계정 관리, 권한 관리, 파일 시스템과 데이터 무결성, 호스트 기반 액세스 제어, 침입 보호, 취약점 검색 및 분석 그리고 응용 프로그램 보안과 관련된 문제를 고려하는 것이 좋습니다.

5. 시스템이 이미 이용 가능한 취약점을 가지고 있거나 부당하게 이용되었을 수 있습니다.

강화될 플랫폼이 이미 공격자에 의해 부당하게 이용되었을 수 있습니다. Solaris Security Toolkit 소프트웨어가 너무 늦게 구현되어 부당하게 이용된 취약점에 대한 보호를 제공하지 못할 수 있습니다. 이용 가능한 취약점을 가지고 있는 경우에는 다음을 수행하십시오.

- a. 시스템을 다시 설치합니다.
- b. Solaris Security Toolkit 소프트웨어를 설치합니다.
- c. Solaris Security Toolkit 소프트웨어를 사용하여 보안을 강화합니다.

보안 방침, 표준 및 관련 문서 검토

시스템 보안에서의 첫 번째 작업은 조직의 관련 보안 방침, 표준 및 플랫폼 보안에 관한 지침을 이해하는 것입니다. 이 문서들이 조직의 모든 시스템에 대해 따라야 하는 요구 사항 및 관례를 전달하므로 이 문서들을 Solaris Security Toolkit 프로파일의 토대로 사용하십시오. 조직에 이런 문서가 없는 경우 해당 문서를 개발하는 것이 Solaris Security Toolkit 소프트웨어를 사용자 정의하는 능력을 향상시키는 데에 도움을 줄 것입니다.

참고 – 이러한 문서를 찾을 때 일부 자료는 최상의 용례나 다른 문서에 나열될 수 있음을 명심하십시오.

보안 방침에 대한 자세한 정보는 Sun BluePrints OnLine 기사 "Developing a Security Policy"를 참조하십시오. 이 문서를 사용하여 보안 방침이 조직의 보안 계획에서 수행하는 역할을 더욱 이해할 수 있습니다.

다음 두 예제는 방침 선언이 Solaris Security Toolkit 프로파일이 구성되는 방법에 직접적으로 영향을 미칠 수 있는 방법을 보여줍니다.

예 1

- 방침 – 조직에서는 전송 데이터의 암호화 및 사용자의 강력한 인증을 지원하는 관리 프로토콜을 사용해야 합니다.
- 프로파일 영향 – 텔넷, 파일 전송 프로토콜(FTP), SNMPv1(간이 망 관리 프로토콜 버전 1)등의 텍스트 제거 프로토콜을 사용해서는 안됩니다. Solaris Security Toolkit의 `secure.driver`는 이러한 서비스를 비활성화하므로 추가 구성은 필요하지 않습니다.

참고 - 텔넷 및 FTP 서비스는 둘 다 Kerberos 같은 확장을 사용하여 더욱 강력한 인증 및 암호화를 지원하도록 구성할 수 있습니다. 그러나 이 기본 구성은 추가된 보안 레벨을 지원하지 않습니다.

예 2

방침 - 모든 사용자는 30일마다 암호를 변경해야 합니다.

프로파일 영향 - 암호 사용 기간을 사용할 수 있도록 Solaris Security Toolkit 소프트웨어를 구성할 수 있습니다. 기본적으로 Solaris Security Toolkit 소프트웨어의 `secure.driver`는 최대 암호 사용 기간을 8주(56일)로 설정합니다. 이 방침을 준수하기 위해서 Solaris Security Toolkit 소프트웨어의 프로파일을 변경해야 합니다. Solaris Security Toolkit 4.2 Reference Manual을 참조하십시오.

Solaris Security Toolkit의 `secure.driver`는 시스템에서 실행하는 암호 사용 기간을 활성화하지만, 이 변경 사항은 기존 사용자가 그들의 암호를 변경할 때까지 기본 사용자에게 적용되지 않습니다. 기존 사용자에게 암호 사용 기간을 사용하려면 각 사용자 계정에서 `passwd(1)` 명령을 호출하십시오. 강제로 기본 사용자가 암호를 변경하도록 하려면, `passwd -f` 명령을 사용할 수 있습니다. `passwd(1)` 명령에 대한 자세한 정보는 Solaris 10 OS Reference Collection을 참조하십시오.

응용 프로그램 및 서비스 요구사항 판별

이 작업은 시스템이 강화된 후에도 서비스를 사용할 수 있도록 보장합니다. 이 작업은 다음 단계로 구성됩니다.

- 20페이지에 "응용프로그램 및 작동 서비스 목록 명세 식별"
- 21페이지에 "서비스 요구사항 판별"

응용프로그램 및 작동 서비스 목록 명세 식별

응용프로그램, 서비스 및 작동 또는 관리 기능의 목록을 작성하십시오. 이 목록은 시스템에서 실제로 사용되고 있는 소프트웨어를 판별하기 위해 필요합니다. 많은 경우 시스템은 실제 사용하는 것보다 많은 소프트웨어와 비즈니스 기능을 지원하지 않는 소프트웨어로 구성되어 있습니다.

시스템은 가능하면 항상 최소한으로 구성되어야 합니다. 즉 비즈니스 기능을 지원하기 위해 필요하지 않은 소프트웨어는 설치하지 않아야 합니다. 시스템에 있는 불필요한 소프트웨어 응용 프로그램은 공격자가 시스템을 부당하게 이용할 수 있는 기회를 높입니다. 또한 시스템에 소프트웨어가 많을수록 대개 적용해야 하는 패치도 많아집니다.

Solaris OS 최소화에 대해서는 Sun BluePrints OnLine 기사 "Minimizing the Solaris Operating Environment for Security"를 참조하십시오. Sun Fire 시스템 도메인 최소화

에 대한 자세한 내용은 Sun BluePrints Online 기사 "Part I: Minimizing Domains for Sun Fire V1280, 6800, 12K, and 15K Systems," 및 "Part II: Minimizing Domains for Sun Fire V1280, 6800, 12K, and 15K Systems"를 참조하십시오.

소프트웨어 목록을 구축할 때 반드시 시스템에 상주하는 응용 프로그램 외에 관리, 모니터링 및 백업 소프트웨어 같은 기반구조 구성요소를 포함시키십시오.

서비스 요구사항 판별

응용 프로그램 및 서비스 목록 작성을 완료한 후 임의의 구성요소가 강화 프로세스에 의 해 영향을 받을 수 있는 종속성을 갖는지 판별하십시오. 많은 타사 응용 프로그램은 Solaris OS가 제공하는 서비스를 직접 사용하지 않습니다. 해당 응용 프로그램에 대해 다음 절에서 도움이 되는 정보를 제공합니다.

- 21페이지에 "공유 라이브러리"
- 23페이지에 "구성 파일"
- 24페이지에 "서비스 프레임워크"

참고 – 이 절의 모든 예는 Solaris 9 OS에서 참조되었습니다.

공유 라이브러리

응용 프로그램을 지원하기 위해 필요한 라이브러리를 이해하는 것이 중요합니다. 이 지식은 디버깅 상황에서 가장 유용하지만 강화할 시스템을 준비할 때도 유용합니다. 시스템의 상태를 알 수 없을 때 소프트웨어 종속성 같은 문제를 명확히 이해하도록 가능한 많은 정보를 수집하십시오.

세가지 방법을 사용하여 설치하는 Solaris OS에 따라서 응용 프로그램이 사용하는 라이브러리를 판별할 수 있습니다. 이 절에서는 각 방법의 코드 예를 살펴봅니다.

- 방법 1 - 파일 시스템 객체에 대한 정보 얻기(예: 응용프로그램 이진 또는 라이브러리)(코드 예 2-1)
- 방법 2 - 프로세스를 실행하여 실행중인 응용프로그램을 분석하는 것에 대한 정보 수집(코드 예 2-2)
- 방법 3 - 동적으로 로드된 응용프로그램을 식별하여 시작된 프로그램 추적(코드 예 2-3)

방법 1

파일 시스템 개체에 대한 정보를 획득하려면 `/usr/bin/ldd` 명령을 사용하십시오.

예: DNS(Domain Name System) 서버 소프트웨어를 지원하는 데 필요한 라이브러리를 판별하십시오.

코드 예 2-1 파일 시스템 개체에 대한 정보 획득

```
# ldd /usr/sbin/in.named
libresolv.so.2 => /usr/lib/libresolv.so.2
libsocket.so.1 => /usr/lib/libsocket.so.1
libnsl.so.1 => /usr/lib/libnsl.so.1
libc.so.1 => /usr/lib/libc.so.1
libdl.so.1 => /usr/lib/libdl.so.1
libmp.so.2 => /usr/lib/libmp.so.2
/usr/platform/SUNW,Ultra-5_10/lib/libc_psr.so.1
```

방법 2

실행 중인 프로세스로부터 정보를 수집하려면 /usr/proc/bin/pldd 명령(Solaris OS 버전 8, 9 및 10에서 사용 가능)을 사용하십시오.

코드 예 2-2 실행 중 프로세스로부터 정보 수집

```
# pldd 20307
/usr/lib/libdl.so.1
/usr/lib/libmp.so.2
/usr/platform/sun4u/lib/libc_psr.so.1
/usr/lib/dns/dnssafe.so.1
/usr/lib/dns/cylink.so.1
```

방법 3

pldd 명령은 응용 프로그램이 링크되는 라이브러리 외에 응용 프로그램이 동적으로 로드하는 공유 라이브러리를 표시합니다. 이 정보는 다음 truss 명령을 사용하여 수집할 수도 있습니다.

참고 - 다음 출력은 간단하게 표시하기 위해 일부가 생략되었습니다.

코드 예 2-3 동적으로 로드된 응용 프로그램 식별

```
# truss -f -topen,open64 /usr/sbin/in.named
20357: open("/usr/lib/libresolv.so.2", O_RDONLY) = 3
20357: open("/usr/lib/libsocket.so.1", O_RDONLY) = 3
20357: open("/usr/lib/libnsl.so.1", O_RDONLY) = 3
20357: open("/usr/lib/libc.so.1", O_RDONLY) = 3
20357: open("/usr/lib/libdl.so.1", O_RDONLY) = 3
20357: open("/usr/lib/libmp.so.2", O_RDONLY) = 3
20357: open("/usr/lib/nss_files.so.1", O_RDONLY) = 4
20357: open("/usr/lib/nss_files.so.1", O_RDONLY) = 4
20357: open("/usr/lib/dns/dnssafe.so.1", O_RDONLY) = 4
20357: open("/usr/lib/dns/cylink.so.1", O_RDONLY) = 4
20357: open("/usr/lib/dns/sparcv9/cylink.so.1", O_RDONLY) = 4
```

이 출력 버전에는 시스템 호출의 반환값뿐 아니라 프로세스 ID, 시스템 호출(이 경우에 open) 및 그의 인수가 들어있습니다. 반환값을 사용하면 시스템 호출이 공유 라이브러리를 찾아서 여는 데 성공한 시기가 명백합니다.

공유 라이브러리 목록이 알려지면 다음 명령을 사용하여 해당 라이브러리가 속하는 Solaris OS 패키지를 판별하십시오.

```
# grep "/usr/lib/dns/cylink.so.1" /var/sadm/install/contents
/usr/lib/dns/cylink.so.1 f none 0755 root bin 63532 24346 \
1018126408 SUNWcs1
```

결과 출력은 이 공유 라이브러리가 SUNWcs1 (코어, 공유 라이브러리) 패키지에 속함을 표시합니다. 이는 응용 프로그램이나 서비스를 지원하기 위해 필요한 패키지를 식별하는데 도움이 되기 때문에 특히 플랫폼 최소화를 수행할 때 유용합니다.

구성 파일

요구사항을 수집하는 다른 방법은 구성 파일을 통하는 것입니다. 이 프로세스는 구성 파일을 제거하거나 이름을 바꾸어서 서비스를 비활성화 할 수 있기 때문에 시스템이 강화되는 방법에 더욱 직접적인 영향을 미칩니다. 자세한 정보는 Solaris Security Toolkit 4.2 Reference Manual을 참조하십시오.

구성 파일을 사용 중인지 판별하려면 `truss` 명령을 사용하십시오.

참고 - 다음 출력은 간단하게 표시하기 위해 일부가 생략되었습니다.

코드 예 2-4 구성 파일을 사용 중인지 판별

```
# truss -f -topen,open64 /usr/sbin/in.named 2>&1 | \
grep -v "/usr/lib/.*.so.*"

20384: open("/etc/resolv.conf", O_RDONLY) = 3
20384: open("/dev/console", O_WRONLY) = 3
20384: open("/usr/share/lib/zoneinfo/US/Eastern", O_RDONLY) = 4
20384: open("/var/run/syslog_door", O_RDONLY) = 4
20384: open("/etc/nsswitch.conf", O_RDONLY) = 4
20384: open("/etc/services", O_RDONLY) = 4
20384: open("/etc/protocols", O_RDONLY) = 4
20384: open("/etc/named.conf", O_RDONLY) = 4
20384: open("named.ca", O_RDONLY) = 5
20384: open("named.local", O_RDONLY) = 5
20384: open("db.192.168.1", O_RDONLY) = 5
20384: open("db.internal.net", O_RDONLY) = 5
```

이 예제에서 DNS 서비스가 `/etc/named.conf` 같은 구성 파일을 사용합니다. 이전 예제에서와 같이 서비스의 반환값이 오류를 표시하는 경우 문제점이 있을 수 있습니다. 강화 전후의 결과를 주의하여 문서화하는 것이 전체 검증 프로세스를 가속화하는 데 도움이 됩니다.

서비스 프레임워크

이 범주는 더 크고 더 복잡한 응용 프로그램이 구축되는 프레임워크 또는 메타서비스를 포함합니다. 이 범주에 포함되는 프레임워크의 일반적인 유형은 다음과 같습니다.

- 이름 지정 서비스 - 예: NIS (Network Information Services), NIS+ 및 LDAP (Lightweight Directory Access Protocol)
- 인증 서비스 - 예: Kerberos 및 LDAP
- 유틸리티 서비스 - 원격 프로시저 호출(RPC) 기능이 사용하는 포트 매핑 프로그램 등

응용 프로그램이 이런 유형의 서비스에 종속할 때가 항상 명확하지는 않습니다. Kerberos 영역에 추가하는 작업과 같이 응용 프로그램을 구성하기 위해 특별한 조정이 필요한 경우 종속성이 알려집니다. 그러나 응용 프로그램 종속성이 항상 추가 작업을 필요로 하지는 않으며 공급 업체가 실제 종속성을 문서화하지 않을 수 있습니다.

이러한 예 중의 하나가 RPC 포트 매핑 프로그램입니다. Solaris Security Toolkit 소프트웨어의 `secure.driver`는 RPC 포트 매핑 프로그램을 비활성화합니다. 이 조치가 이 서비스에 의존하는 다른 서비스에서 예기치 않은 작동을 유발할 수 있습니다. 과거 경험을 토대로, 응용 프로그램 코드가 예외 사례를 얼마나 잘 다루도록 작성되는지에 따라서 서비스가 취소, 중단 또는 실패합니다. 응용프로그램이 RPC 포트 매핑 프로그램을 사용 중인지 확인하려면 `rpcinfo` 명령을 사용하십시오. 예:

코드 예 2-5 RPC를 사용하는 응용 프로그램 판별

```
# rpcinfo -p
100000 3 tcp 111 rpcbind
100000 4 udp 111 rpcbind
100000 2 udp 111 rpcbind
100024 1 udp 32777 status
100024 1 tcp 32772 status
100133 1 udp 32777
100133 1 tcp 32772
100021 1 udp 4045 nlockmgr
100021 2 udp 4045 nlockmgr
100021 3 udp 4045 nlockmgr
100021 4 udp 4045 nlockmgr
100021 1 tcp 4045 nlockmgr
```

서비스 열은 `/etc/rpc` 파일의 정보 또는 LDAP 같이 구성된 이름 지정 서비스로 채워집니다.

타사 제품에 대한 경우에서 종종 그런 것처럼 이 파일에 서비스에 대한 항목이 없는 경우 서비스 필드가 비어 있을 수도 있습니다. 이로 인해 다른 응용 프로그램으로 등록된 응용 프로그램을 식별하기가 어렵습니다.

예를 들어 `rusers` 명령을 고려하십시오. 이 명령은 RPC 포트 매핑 서비스에 의존합니다. RPC 포트 매핑 프로그램이 실행하지 않는 경우 `rusers` 명령은 중지한 것으로 나타납니다. 프로그램은 결국 다음 오류 메시지와 함께 시간 초과됩니다.

```
# rusers -a localhost
localhost: RPC: Rpcbnd failure
```

이 문제점은 프로그램이 서비스와 통신할 수 없기 때문에 발생합니다. 그러나 /etc/init.d/rpc로부터 RPC 포트 매핑 서비스를 시작한 후 프로그램이 즉시 결과를 산출합니다.

또 다른 예로서, RPC 포트 매핑 서비스가 실행 중이고 rusers 서비스가 실행하도록 구성되지 않은 경우를 고려하십시오. 이 경우에 완전히 다른 응답이 생성되며 상대적으로 검증하기 쉽습니다.

코드 예 2-6 rusers 서비스 검증

```
# rusers -a localhost
localhost: RPC: Program not registered
# grep rusers /etc/rpc
rusersd          100002  rusers
# rpcinfo -p | grep rusers
<No output generated>
```

rpcinfo 명령이 rusers 서비스에 대한 레지스트리를 갖지 않는 경우 서비스가 실행하도록 구성되지 않았다고 가정하는 것이 안전합니다. 이 가정은 /etc/inet/inetd.conf에서 서비스 항목을 조사하여 검증됩니다.

```
# grep rusers /etc/inet/inetd.conf
# rusersd/2-3  tli      rpc/datagram_v,circuit_v  wait root
/usr/lib/netsvc/rusers/rpc.rusersd  rpc.rusersd
```

서비스 행의 시작부에 있는 주석 표시(#)는 rusers 서비스를 사용할 수 없음을 표시합니다. 서비스를 활성화 하려면 행의 주석 표시를 제거하고 다음과 같이 SIGHUP 신호를 /usr/sbin/inetd 프로세스로 보내십시오.

```
# pkill -HUP inetd
```

참고 - pkill 명령은 Solaris OS 버전 7에서 10까지에서만 사용 가능합니다. 다른 버전의 경우, ps 및 kill 명령을 각각 사용하여 프로세스를 찾고 신호하십시오.

응용 프로그램이 RPC 기능을 사용하는지 판별하는 또 다른 방법은 앞에서 설명한 ldd 명령을 사용하는 것입니다.

코드 예 2-7 RPC를 사용하는 응용 프로그램을 판별하기 위한 대체 방법

```
# ldd /usr/lib/netshvc/rusers/rpc.rusersd
libnsl.so.1 => /usr/lib/libnsl.so.1
librpcsvc.so.1 => /usr/lib/librpcsvc.so.1
libc.so.1 => /usr/lib/libc.so.1
libdl.so.1 => /usr/lib/libdl.so.1
libmp.so.2 => /usr/lib/libmp.so.2
/usr/platform/SUNW,Ultra-250/lib/libc_psr.so.1
```

librpcsvc.so.1에 대한 항목은 파일 이름과 함께 이 서비스가 RPC 포트 매핑 서비스에 의존함을 나타냅니다.

RPC 포트 매핑 프로그램 외에, 응용 프로그램이 FTP, SNMP 또는 NFS(네트워크 파일 시스템)와 같은 다른 일반 OS 서비스에 의존할 수 있습니다. 비슷한 방법을 사용하여 이들 서비스를 디버그하고 해당 서비스가 비즈니스 기능을 지원하기 위해 실제로 필요한지 판별할 수 있습니다. 한 가지 방법은 다음과 같이 netstat 명령을 사용하는 것입니다.

```
# netstat -a | egrep "ESTABLISHED|TIME_WAIT"
```

이 명령은 최근에 사용 중이거나 사용 중인 서비스의 목록을 반환합니다. 예를 들어,

표 2-1 최근에 사용 중인 서비스 목록

localhost.32827	localhost.32828	49152	0	49152	0
ESTABLISHED					
localhost.35044	localhost.32784	49152	0	49152	0
ESTABLISHED					
localhost.32784	localhost.35044	49152	0	49152	0
ESTABLISHED					
localhost.35047	localhost.35046	49152	0	49152	0
ESTABLISHED					
localhost.35046	localhost.35047	49152	0	49152	0
ESTABLISHED					
filefly.ssh	192.168.0.3.2969	17615	1	50320	0
ESTABLISHED					

이 예제에서 많은 서비스를 사용 중이지만 어떤 서비스나 응용 프로그램에 어떤 포트가 있는지 명확하지 않습니다. 이 정보는 `pfiles(1)` 명령(Solaris OS 버전 8, 9 및 10에서 사용 가능)을 사용하는 프로세스를 조사하여 수집할 수 있습니다. `pfiles` 명령은 각 프로세스에서 열린 모든 파일에 대한 정보를 보고합니다.

코드 예 2-8 서비스 또는 응용 프로그램에 있는 포트 판별

```
# for pid in `ps -a eo pid | grep -v PID`; do
> pfiles ${pid} | egrep "^${pid}:|sockname:"
> done
```

이러한 종속성을 판별하는 보다 효과적이고 효율적인 방법은 `list open files(lsof)` 명령을 사용하는 것입니다.

다음 주소에서 `lsof` 소스 코드를 다운로드 합니다.

<ftp://lsof.itap.purdue.edu/pub/tools/unix/lsof/>

다음 주소에서 `lsof` 이진을 다운로드 합니다.

<http://www.sunfreeware.com>

`lsof` 명령은 어떤 프로세스가 어떤 파일 및 포트를 사용 중인지 판별합니다. 예를 들어 이전 예제에서 어떤 프로세스가 포트 35047을 사용 중인지 판별하려면 다음 명령을 사용하십시오.

코드 예 2-9 파일 및 포트를 사용 중인 프로세스 판별

```
# ./lsof -i | grep 35047

ttsession    600 root 9u  IPv4 0x3000b4d47e8      0t1  TCP
localhost:35047->localhost:35046 (ESTABLISHED)

dtexec       5614 root 9u  IPv4 0x3000b4d59e8      0t0  TCP
localhost:35046->localhost:35047 (ESTABLISHED)
```

`lsof`의 출력은 포트 35047이 `dtexec`와 `ttsession` 프로세스 사이의 통신에 사용 중임을 나타냅니다.

`lsof` 프로그램을 사용할 때 파일 시스템 또는 네트워크 사용이 필요한 시스템간 또는 응용 프로그램간 종속성을 훨씬 더 빨리 판별할 수 있습니다. `lsof` 프로그램의 다양한 옵션을 사용하여 이 절에서 다루는 거의 모든 것을 캡처할 수 있습니다.

참고 - 종속성 판별을 설명하는 방법이 드물게 사용되는 항목은 찾지 못할 수 있습니다. 이 방법을 사용하는 것 외에 Sun 문서 및 공급 업체 문서를 검토하십시오.

Solaris Security Toolkit 프로파일 개발 및 구현

계획 및 준비 단계를 완료한 후 보안 프로파일을 개발 및 구현하십시오. 보안 프로파일은 구성, 강화 및 보안 드라이버 (예: `name- {config|hardening|secure}.driver`) 및 사이트 특정 보안 정책을 구현하기 위한 관련 드라이버, 스크립트 및 파일로 구성됩니다.

Solaris Security Toolkit 소프트웨어와 함께 제공되는 보안 프로파일 중 하나를 사용자 정의하거나 고유한 프로파일을 개발하십시오. 각 조직의 방침, 표준 및 응용 프로그램 요구사항은 아주 조금일지라도 서로 다릅니다.

보안 프로파일을 사용자 정의하려면 종료 스크립트, 감사 스크립트, 환경 변수, 프레임워크 기능 및 파일 템플릿을 통해 프로파일의 작동을 조정하십시오.

자세한 정보는 다음 장을 참조하십시오.

- 소프트웨어 사용자 정의에 대한 중요한 지침은 1 장, 13페이지에 "Solaris Security Toolkit 소프트웨어 구성 및 사용자 정의"를 참조하십시오.
- 보안 프로파일이 작성되는 예제 시나리오에 대해서는 7 장, 103페이지에 "보안 프로파일 작성"을 참조하십시오.
- 드라이버 사용자 정의에 대해서는 Solaris Security Toolkit 4.2 Reference Manual을 참조하십시오.

필요할 때마다 스크립트, 프레임워크 기능, 환경 변수 및 파일에 대한 정보는 Solaris Security Toolkit 4.2 Reference Manual 장을 참조하십시오. 사용자 정의할 수 있는 두 개의 핵심 환경 변수는 `JASS_FILES`와 `JASS_SCRIPTS`입니다.

플랫폼 고유의 차이를 고려하면서 대다수의 플랫폼에서 표준을 집행하려면 내포 또는 계층 구조 보안 프로파일이라고 부르는 방법을 사용하십시오. 자세한 정보는 Solaris Security Toolkit 4.2 Reference Manual을 참조하십시오. 결과 보안 프로파일을 조직의 방침, 표준 및 요구사항과 비교하여 우발적으로 또는 오류가 있는 변경이 작성되지 않도록 하십시오.

소프트웨어 설치

Solaris Security Toolkit 소프트웨어의 설치 전개된 시스템 및 설치되고 있는 모든 새 시스템에 대해 동일합니다. 자세한 지침은 3 장을 참조하십시오.

전개된 시스템의 경우 소수의 특별한 경우가 이 프로세스를 더 간단하고 빠르게 만들 수 있습니다. 이러한 경우는 강화 프로세스에서 집중되지 않지만 설치 전 및 설치 후 작업에 집중됩니다.

설치 전 작업 수행

전개된 시스템을 강화하기 전에, 다음 두 가지 중요 작업을 고려하고 계획하십시오.

- 백업
- 검증

이들 작업은 배포된 시스템의 상태를 판별하고 시스템이 강화되기 전에 모든 잠재적 구성 문제점을 해결하는 데 도움이 됩니다.

데이터 백업

이 작업은 긴급 대책 계획에 집중합니다. 문제점이 있는 경우 시스템의 구성 및 데이터가 어떤 양식으로 보존되도록 보장하는 것이 필요합니다. 다음을 반드시 수행해야 합니다.

- 시스템을 백업합니다.
- 백업 매체를 읽을 수 있는지 확인합니다.
- 내용이 저장될 수 있는지 검증합니다.

시스템의 구성에 어떤 중대한 변경을 수행하기 전에 이 단계를 수행하십시오.

시스템 안정성 확인

검증 작업은 백업 작업 만큼이나 중요합니다. 검증은 강화 프로세스에 의한 변경과 같이 모든 구성 변경의 구현 전에 시스템이 안정하고 작동 중인 상태에 있음을 보장합니다. 이 검증 프로세스는 다음과 관련됩니다.

- 재부팅
- 모든 응용프로그램 또는 서비스의 테스트 성공

올바르게 정의된 테스트 및 승인 계획이 우선적이지만 계획이 항상 가능하지는 않습니다. 그런 경우에는 시스템의 사용 방법에 기초하여 합리적인 방법으로 시스템을 테스트하십시오. 이 노력의 목표는 실행 중인 구성이 사실상 저장된 구성과 일치하도록 보장하는 것입니다.

시스템이 시동하거나 응용프로그램이 시작할 때 표시되는 모든 오류 메시지나 경고를 조사하십시오. 오류를 정정할 수 없는 경우 강화 프로세스 중에 문제점의 잠재적인 원인으로 포함되지 않도록 오류를 기록하십시오. 로그 파일을 조사할 때 다음과 같은 시스템, 서비스 및 응용 프로그램 로그를 포함하십시오.

- /var/adm/messages

- /var/adm/sulog
- /var/log/syslog
- /var/cron/log

이 작업은 오류 또는 경고 메시지가 발생하지 않거나 알 수 없는 오류 또는 경고(알려진 모든 오류나 경고는 문서화됨)가 발생하지 않고 시스템을 다시 시작할 수 있을 때 완료됩니다. 시스템은 알려지고 안정한 상태로 다시 시작해야 합니다. 검증 과정 중에 시스템의 실행 중인 구성 및 저장된 구성이 다르다는 것을 발견하는 경우 조직의 변경 제어 방침 및 프로세스를 다시 평가하여 해당 상태를 유발하는 차이를 식별하십시오.

설치 후 작업 수행

설치 후 작업은 설치 전 작업의 확장입니다. 작업의 목적은 강화 프로세스가 시스템이나 응용 프로그램에 어떤 새 결함도 초래하지 않도록 확인하는 것입니다. 이 작업은 주로 시스템 및 응용 프로그램 로그 파일을 검토하여 수행됩니다. 강화 및 후속 재부트 후에 작성되는 로그 파일은 시스템이 강화되기 전에 수집된 로그 파일과 비슷해야 합니다. 어떤 경우에는 더 적은 서비스가 시작되기 때문에 더 적은 메시지가 있을 수 있습니다. 가장 중요한 것은 새로운 오류 또는 경고 메시지가 없어야 합니다.

로그 파일 검토 외에, 일부 응용 프로그램은 로그 항목을 생성하지 않고 실패할 수 있기 때문에 기능을 테스트하십시오. 자세한 검증 정보에 대해서는 다음 절을 참조하십시오.

응용프로그램 및 서비스 기능성 확인

시스템 보안 프로세스의 마지막 작업은 시스템이 제공하는 응용 프로그램 및 서비스가 올바르게 기능하고 있는지 확인하는 것입니다. 이 작업은 또한 보안 프로파일이 보안 방침의 요구사항을 성공적으로 구현했음을 확인합니다. 모든 비정상 또는 문제점을 감지하고 바로 정정하려면 강화된 플랫폼의 재부트 후에 이 작업을 즉각 철저히 수행하십시오. 이 작업은 보안 프로파일 설치 확인 및 응용프로그램과 서비스 기능성 확인이라는 두 하위 작업으로 구분됩니다.

보안 프로파일 설치 확인

Solaris Security Toolkit 소프트웨어가 보안 프로파일을 오류 없이 올바르게 설치했는지 확인하기 위해 설치 로그 파일 `jass-install-log.txt`를 검토하십시오. 이 파일은 각 강화 또는 감사 작업(실행 시작 시간)에 대한 고유 디렉토리의 하위인 `/var/opt/SUWWjass/runs`에 설치되어 있습니다.

참고 – Solaris Security Toolkit 소프트웨어가 시스템에 수행한 작업을 이해하기 위해 이 로그 파일을 참조하십시오. 시스템의 각 실행에 대한 실행 시작 시간을 기초로 새 로그 파일이 디렉토리에 저장됩니다.

프로파일의 설치를 확인하는 것 외에, 시스템의 보안 구성을 평가하십시오. 수동 검사를 수행하거나 도구를 사용하여 프로세스를 자동화하십시오.

응용 프로그램 및 서비스 기능성 확인

프로세스 응용프로그램 및 서비스를 검증하기 위해 올바르게 정의된 테스트 및 승인 계획을 실행하십시오. 이 계획은 시스템 또는 응용 프로그램의 다양한 구성요소를 사용하여 해당 구성요소가 사용 가능하며 작업 순서대로 있는지 판별합니다. 이러한 계획이 사용 불가능할 경우, 시스템의 사용 방법을 기초로 시스템을 합리적으로 검사하십시오. 이 작업의 목적은 강화 프로세스가 자체 기능을 수행하는 응용 프로그램 또는 서비스 기능에 전혀 영향을 미치지 않음을 확인하는 것입니다.

시스템이 강화된 후 응용 프로그램 또는 서비스가 제대로 작동하지 않는 경우 응용 프로그램 로그 파일을 검토하여 문제점을 판별하십시오. 대부분의 경우, `truss` 명령을 사용하여 응용 프로그램의 문제점이 있는 위치를 판별하십시오. 이 위치가 알려진 후에 해당 문제점을 대상으로 하여 Solaris Security Toolkit 소프트웨어가 변경한 내용을 다시 추적할 수 있습니다.

시스템 보안 유지보수

많은 조직의 공통적인 실수는 설치 중에만 보안에 신경 쓰고 그 후에는 거의 또는 전혀 다시 확인하지 않는 것입니다. 보안 유지보수는 지속적인 프로세스입니다. 주기적으로 시스템 보안을 검토하고 확인해야 합니다.

임의의 시스템에 대한 보안 구성이 시간이 지남에 따라 점차 허술해지기 때문에 보안 시스템 유지보수는 경계가 필요합니다. 예를 들어 시스템 취약점이 더욱 알려지게 됩니다.

다음 기본 지침은 시스템 보안 유지에 대한 개요를 제공합니다.

- 패치를 설치하기 전과 후에 시스템의 보안 상태를 검토하십시오. 또한 항상 시스템을 최신 패치로 업데이트하는 것이 중요합니다.

Solaris OS 패치는 설치의 일부로서 추가 소프트웨어 패키지를 설치할 수 있으며 시스템 구성 파일을 겹쳐 쓸 수 있습니다. Solaris Security Toolkit 소프트웨어가 한 시스템에서의 반복적인 실행을 지원하기 때문에 패치를 설치한 후 시스템을 보안할 수 있도록 사용자의 패치 적용을 도와줄 수 있습니다. 모든 패치 설치 후에 적용 가능한 드라이버와 함께 소프트웨어를 실행하여 구성이 정의된 보안 방침과 일관성을 유지

하는지 확인하십시오. 또한 사용되는 Solaris Security Toolkit 소프트웨어의 버전이 설치된 패치에 의해 추가된 새로운 기능을 지원하지 않을 수 있기 때문에 시스템을 수동으로 검토하십시오.

- 지속적으로 시스템을 모니터링하여 허가되지 않은 작동이 발생하지 않도록 하십시오. 시스템 계정, 암호 및 액세스 패턴을 검토하십시오. 시스템에서 발생하고 있는 사항에 대한 많은 정보를 제공할 수 있습니다.
- 중앙 집중된 syslog 저장소를 전개하고 유지 보수하여 syslog 메시지를 수집하고 분석하십시오. 이들 로그를 수집하고 검토하여 가치있는 정보를 얻을 수 있습니다.
- 포괄적인 취약점 및 감사 전략을 설정하여 시스템 구성을 모니터링하고 유지 보수하십시오. 이 요구사항은 특히 시간에 따라 시스템을 안전한 구성으로 유지 보수한다는 점에서 중요합니다.
- Solaris Security Toolkit 소프트웨어의 최신 버전으로 시스템을 주기적으로 업데이트하십시오.

Solaris Security Toolkit 소프트웨어에는 시작점으로 사용할 수 있는 기본 보안 프로파일도 포함되어 있습니다.

보안 소프트웨어 업그레이드, 설치 및 실행

이 장은 Solaris Security Toolkit 소프트웨어 및 기타 보안 관련 소프트웨어 다운로드, 업그레이드 또는 설치 및 실행에 대한 지침을 제공합니다. 독립형 또는 JumpStart 모드에 맞게 환경을 구성하고 지원을 얻기 위한 지시가 포함됩니다.

소프트웨어를 업그레이드 또는 설치, 구성 및 실행하려면 이 절에 제공되는 지침 및 프로세스를 따르십시오. 이들 지시에는 추가 보안 소프트웨어, 도움이 되는 예제 및 안내서 다운로드가 포함됩니다.

Solaris Security Toolkit 소프트웨어가 독립형 제품이지만 다운로드할 수 있도록 제공되는 추가 보안 소프트웨어와 함께 사용될 때 가장 효과적입니다. 이 소프트웨어에는 SunSolve OnLine의 Recommended and Security Patch Cluster, 포함되지 않은 Solaris OS용 Secure Shell 소프트웨어, Solaris OS 및 타사 소프트웨어 사용 권한을 강화하기 위한 사용 권한 및 소유권 수정 소프트웨어 및 Sun 파일 및 실행 파일의 무결성을 검증하기 위한 무결성 검증 이진이 포함됩니다.

이 장에서는 다음 작업을 다룹니다.

- 36페이지에 "계획 및 설치 전 작업 수행"
- 36페이지에 "소프트웨어 종속성"
- 36페이지에 "사용할 모드 판별"
- 38페이지에 "업그레이드 절차"
- 40페이지에 "보안 소프트웨어 다운로드"
- 47페이지에 "보안 프로파일 사용자 정의"
- 47페이지에 "소프트웨어 설치 및 실행"
- 59페이지에 "시스템 수정 검증"

계획 및 설치 전 작업 수행

적절한 계획 수립은 Solaris Security Toolkit 소프트웨어를 사용하여 시스템을 성공적으로 보안하기 위한 핵심입니다. 소프트웨어를 설치하기 전의 계획 수립에 대한 자세한 정보는 2 장을 참조하십시오.

전개된 시스템에 소프트웨어를 설치하는 경우, 전개된 시스템에 소프트웨어를 설치하기 전에 설치 전 작업 수행에 대해 30페이지에 "설치 전 작업 수행"을 참조하십시오.

소프트웨어 종속성

Solaris Security Toolkit 4.2 소프트웨어는 SUNWloc 패키지에 의존합니다. 이 패키지가 없을 경우 Solaris Security Toolkit은 작동하지 않게 됩니다.

Solaris 운영체제의 지원 버전에 대한 자세한 정보는 xx페이지에 "지원되는 Solaris OS 버전"을 참조하십시오.

시스템 관리 서비스 소프트웨어의 지원 버전에 대한 자세한 정보는 xxi페이지에 "지원되는 SMS 버전"을 참조하십시오.

사용할 모드 판별

시스템이 보안되지 않은 상태에 있는 동안 공격에 노출될 수 있는 기간을 제한하기 위해 OS 설치 중 또는 직후에 시스템을 강화하십시오. Solaris Security Toolkit 소프트웨어를 사용하여 시스템을 보안하기 전에 사용자 환경에서 제대로 실행하도록 Solaris Security Toolkit 소프트웨어를 구성하십시오.

Solaris Security Toolkit 소프트웨어는 모듈형 프레임워크를 갖고 있습니다. JumpStart 제품을 사용하지 않을 경우 Solaris Security Toolkit 소프트웨어 프레임워크의 유연성으로 나중에 JumpStart를 사용하도록 효율적으로 준비할 수 있습니다. JumpStart를 사용하는 경우 기존 JumpStart 기반구조에 통합하는 Solaris Security Toolkit 소프트웨어의 기능이 유용합니다.

다음 절은 독립형 및 JumpStart 모드에 대해 설명합니다.

독립형 모드

Solaris Security Toolkit 소프트웨어는 독립형 모드에서 Solaris OS 셸 프롬프트에서 직접 실행합니다. 이 모드로 보안 수정이나 업데이트가 필요하지만 아직 스크래치로부터 OS를 다시 설치하기 위해 서비스를 받을 수 없는 시스템에서 Solaris Security Toolkit 소프트웨어를 사용할 수 있습니다. 그러나 가능하면 보안 설정 전에 운영체제를 스크래치로부터 다시 설치하지 않도록 합니다.

독립형 모드는 특히 패치 또는 타사 소프트웨어를 설치한 후 시스템을 강화할 때 유용합니다. 오류 없이 한 시스템에 Solaris Security Toolkit 소프트웨어를 여러 번 실행할 수 있습니다. 패치가 Solaris Security Toolkit 소프트웨어가 수정한 파일을 겹쳐 쓰거나 수정할 수 있습니다. Solaris Security Toolkit 소프트웨어를 다시 실행하여 패치 설치에 의해 무효가 된 모든 보안 수정을 다시 구현할 수 있습니다.

참고 - 생산 환경에서는 활동 중인 환경에 패치를 설치하기 전에 테스트 및 개발 환경에서 패치를 계획하십시오.

독립형 모드는 전개된 시스템을 가능한 빨리 강화하는 최상의 옵션 중 하나입니다. 40 페이지에 "보안 소프트웨어 다운로드"에 제공된 다운로드 및 설치 지시의 단계 외에 Solaris Security Toolkit 소프트웨어를 JumpStart가 없는 구조에 통합하기 위해 특별한 단계가 필요하지는 않습니다.

JumpStart 모드

Sun의 네트워크 기반 Solaris OS 설치 체계인 JumpStart 기술은 설치 프로세스 중에 Solaris Security Toolkit 스크립트를 실행할 수 있습니다. 이 책에서는 사용자가 JumpStart 기술에 익숙하고 기존 JumpStart 환경을 사용할 수 있다고 가정합니다. JumpStart 기술에 대한 자세한 정보는 Sun BluePrints 설명서 *JumpStart Technology: Effective Use in the Solaris Operating Environment*를 참조하십시오.

Solaris Security Toolkit 4.2 패키지는 재배치가 가능하기 때문에 `pkgadd` 명령에 올바른 옵션을 사용하여 원하는 디렉토리에 설치할 수 있습니다. `JASS_HOME_DIR`이 JumpStart 서버의 기본 디렉토리가 됩니다.

Solaris Security Toolkit 소프트웨어를 JumpStart 구조에 통합하기 위해서는 몇 개의 단계만 필요합니다. JumpStart 서버 구성 방법에 대한 지시는 5 장을 참조하십시오.

업그레이드 절차

이 절에서는 Solaris Security 4.0 및 4.1 소프트웨어를 Solaris Security Toolkit 4.2 소프트웨어로 업그레이드하는 방법을 설명합니다. Solaris 운영체제의 Solaris Security Toolkit 소프트웨어를 사용하여 시스템을 강화할 수 있습니다. 4.0과 4.1 버전의 업그레이드 절차는 동일합니다. 이 절차를 미리 수행하면 사전 사용자 정의 사항을 겹쳐쓰지 않도록 할 수 있습니다.



주의 - Solaris Security Toolkit은 한번에 단 하나만 설치할 수 있습니다.

Solaris Security Toolkit 4.2 소프트웨어에서는 새롭게 강화된 `pkgrm` 명령이 제공됩니다. 이 릴리스에서는 `pkgrm` 명령이 우선 배포판에 포함된 모든 파일의 무결성을 검사합니다. 다른 파일이 있을 경우, `pkgrm` 명령은 시스템 관리자에게 올바른 파일을 사용하거나 수정된 파일을 삭제하라는 오류 메시지를 표시하고 종료합니다.

해당 드라이버는 Solaris Security Toolkit이 설치된 Drivers 하위 디렉토리에 저장되어 있습니다. 사용자가 작성한 드라이버도 위 디렉토리에 있습니다. `pkgrm` 명령으로 `SUNWjass`를 제거하면, Solaris Security Toolkit 제공 드라이버 및 사용자가 수정한 드라이버는 제거되고, 사용자정의 드라이버는 Solaris Security Toolkit 제공 드라이버와 다른 이름을 가지고 있다는 가정하에 사용자가 추가한 사용자정의 드라이버는 제거되지 않습니다.



주의 - 드라이버가 수정되는 경우, 해당 드라이버를 업그레이드하기 전에 반드시 저장해야 합니다. Solaris Security Toolkit 소프트웨어와 함께 배포된 원본 파일을 절대로 수정하지 마십시오. 드라이버 파일을 수정하는 대신, 해당 드라이버를 새 파일에 복사한 후 새 파일을 수정하십시오.

▼ Solaris Security Toolkit 소프트웨어 및 Solaris 운영체제 업그레이드

1. **Solaris** 업그레이드를 사용하거나 백업을 수행하여 시스템을 업그레이드하려면 다음 사용 용례를 따르십시오.
2. 이전 버전의 **Solaris Security Toolkit** 소프트웨어를 제거합니다.
3. **Solaris Security Toolkit 4.2** 소프트웨어를 설치합니다.

4. 이전 **Solaris Security Toolkit** 드라이버 및 사용자 지정 드라이버를 사용하여 업그레이드한 시스템의 감사 모드에서 **Solaris Security Toolkit 4.2** 소프트웨어를 실행합니다.
사용자 지정 드라이버는 `Drivers` 디렉토리에 있어야 합니다. 해당 드라이버가 `Drivers` 디렉토리에 있는 경우, 이 드라이버를 `jass-execute` 또는 강화 작업에 지정할 수 있습니다.
5. 다음 중 하나를 수행하십시오.
 - a. 오류가 발생하지 않으면 **6**단계로 이동합니다.
 - b. 해당 작업을 수행하는 도중에 오류가 생성되면 (예: **A non-installed run control script is modified.** 또는 **A service should be controlled using an FMRI.**) 오류를 수정하고 더 이상의 오류가 발생하지 않을 때까지 **4**단계 및 **5**단계를 반복합니다.
6. 사용자정의 드라이버와 `secure.driver` 드라이버를 비교하여 사용자정의 드라이버에 새로운 종료 또는 감사 스크립트를 추가해야 할지를 결정합니다.
7. 다음 중 하나를 수행하십시오.
 - a. 누락된 스크립트가 없으면 **8**단계로 이동합니다.
 - b. 누락된 스크립트가 있는 경우에는 누락된 스크립트를 추가한 후 필요한 모든 스크립트가 포함될 때까지 **4 - 7**단계를 반복합니다.
8. 강화 모드에서 **Solaris Security Toolkit 4.2**를 실행합니다.
9. 감사 모드에서 **Solaris Security Toolkit 4.2**를 실행한 후 오류가 있는지 확인합니다.
10. 보안 구성 및 시스템의 상태를 검토하여 보안상의 요구사항을 충족하는지 판별합니다.
11. 다음 중 하나를 수행하십시오.
 - a. 시스템이 요구사항을 충족하는 경우, **12**단계로 이동합니다.
 - b. 요구사항을 충족하지 않는 경우, 사용중인 드라이버를 업데이트하고 **8**단계로 돌아갑니다.
12. 전체 시스템을 테스트하여 필수 네트워크 서비스와 모든 응용프로그램이 올바르게 작동하고 있는지 확인합니다.
13. 오류가 발생하는 경우, 사용중인 드라이버를 업데이트하고 **8**단계로 돌아갑니다.
이제 업그레이드가 완료됩니다.

▼ Solaris Security Toolkit 소프트웨어만 업그레이드

1. 이전 버전의 **Solaris Security Toolkit** 소프트웨어를 제거합니다.
2. **Solaris Security Toolkit 4.2** 소프트웨어를 설치합니다.

3. 4단계, 38페이지에 "Solaris Security Toolkit 소프트웨어 및 Solaris 운영체제 업그레이드"로 이동합니다.

Solaris OS만 업그레이드

Solaris Security Toolkit 4.2 소프트웨어가 설치되어 있고 Solaris OS만 업그레이드하려는 경우(예: Solaris 8 OS에서 10 OS로 업그레이드), Solaris Security Toolkit 4.2 소프트웨어를 제거할 필요가 없습니다. Solaris OS 업그레이드를 종료한 후, 감사 모드에서 Solaris Security Toolkit 4.2를 실행하고 시스템 보안 구성을 검토하여 오류가 있는지 확인합니다.

보안 소프트웨어 다운로드

시스템 강화의 첫 번째 단계에서는 보안하려는 시스템으로 추가 소프트웨어 보안 패키지를 다운로드해야 합니다. 이 절에서는 다음 작업을 다룹니다.

- 40페이지에 "Solaris Security Toolkit 소프트웨어 다운로드"
- 42페이지에 "Recommended Patch Cluster 소프트웨어 다운로드"
- 43페이지에 "FixModes 소프트웨어 다운로드"
- 44페이지에 "OpenSSH 소프트웨어 다운로드"
- 45페이지에 "MD5 소프트웨어 다운로드"

참고 - 이 절에서 설명하는 소프트웨어 중에서 Solaris Security Toolkit 소프트웨어, Recommended and Security Patch Cluster, FixModes 및 MD5(message-digest 5) 알고리즘 소프트웨어는 필수입니다. OpenSSH 대신 다양한 공급 업체에서 구할 수 있는 Secure Shell의 상업용 버전으로 대체할 수 있습니다. 모든 시스템에 Secure Shell 제품을 설치하고 사용하십시오. Solaris 9 또는 10 OS의 경우는 함께 제공된 SSH(Secure Shell) 버전을 사용하십시오. Solaris 10 OS를 사용하는 경우, MD5 체크섬에 포함된 /usr/bin/digest 명령을 사용합니다.

Solaris Security Toolkit 소프트웨어 다운로드

Solaris Security Toolkit 소프트웨어는 Solaris OS 패키지 형식으로 배포됩니다. 먼저 Solaris Security Toolkit 소프트웨어를 다운로드한 후 독립형 모드에서 Solaris Security Toolkit 소프트웨어를 사용하려는 서버나 JumpStart 모드의 경우 JumpStart 서버에 설치하십시오.

참고 - 다음 지시는 버전 번호를 참조하지 않는 파일 이름을 사용합니다. 항상 웹 사이트에서 최신 버전을 다운로드하십시오.

이 안내서 전체에서 `JASS_HOME_DIR` 환경 변수는 Solaris Security Toolkit 소프트웨어의 루트 디렉토리를 의미합니다(기본값은 `/opt/SUNWjass`입니다).

▼ pkg 버전 다운로드

1. 소프트웨어 배포 파일(`SUNWjass-n.n.pkg.tar.Z`)을 다운로드합니다.
소스 파일은 다음 위치에 있습니다.
<http://www.sun.com/security/jass>

참고 - 소프트웨어 다운로드 중에 어려움이 있는 경우 브라우저의 Save As 옵션을 사용하십시오.

2. `uncompress` 명령을 사용하여 소프트웨어 배포 파일의 압축을 서버의 디렉토리에 풉니다.

```
# uncompress SUNWjass-n.n.pkg.tar.Z
```

3. 다음과 같이 `tar` 명령을 사용하여 소프트웨어 배포 패키지의 압축을 풉니다.

```
# tar -xvf SUNWjass-n.n.pkg.tar
```

4. 아래에 표시된 것처럼 `pkgadd` 명령을 사용하여 서버의 디렉토리에 소프트웨어 배포 파일을 설치합니다.

```
# pkgadd -d SUNWjass-n.n.pkg SUNWjass
```

여기서 `n.n`은 다운로드하려는 최신 버전입니다.

이 명령을 실행하면 `/opt`에 `SUNWjass` 디렉토리가 작성됩니다. 이 하위 디렉토리에는 모든 Solaris Security Toolkit 디렉토리 및 연관된 파일이 들어있습니다.

Recommended Patch Cluster 소프트웨어 다운로드

패치는 Sun에서 성능, 안정성, 기능성 및 보안을 위한 Solaris OS 수정사항을 제공하기 위해 릴리스됩니다. 가장 최신의 패치 클러스터가 설치되는 것이 시스템 보안에 아주 중요합니다. 최신 Solaris OS Recommended and Security Patch Cluster가 시스템에 설치되도록 보장하기 위해 이 절에서 최신 패치 클러스터를 다운로드하는 방법에 대해 설명합니다.

참고 – 패치를 설치하기 전에 비생산 시스템에서 또는 예정된 유지보수 기간 중에 패치를 평가하고 테스트하십시오.

▼ Recommended Patch Cluster 소프트웨어 다운로드

패치 클러스터를 설치하기 전에 개별 패치 README 파일 및 기타 제공되는 정보를 검토하십시오. 이 정보에는 종종 패치 클러스터를 설치하기 전에 알아야 하는 제안과 정보가 들어있습니다.

1. 다음 주소의 **SunSolve OnLine** 웹 사이트에서 최신 패치 클러스터를 다운로드합니다.
<http://sunsolve.sun.com>
2. 우측의 탐색 도구에서 **Patches and Updates** 링크를 누릅니다.
3. **Recommended Patch Clusters** 링크를 누릅니다.
4. **Recommended Solaris Patch Clusters** 상자에서 적합한 **Solaris OS** 버전을 선택합니다.
이 예제에서는 Solaris 10 OS를 선택하겠습니다.
5. 연결된 라디오 버튼으로 적합한 다운로드 옵션(**HTTP** 또는 **FTP**)을 선택하고 **Go**를 누릅니다.
브라우저 창에 다른 이름으로 저장 대화 상자가 표시됩니다.
6. 파일을 로컬에 저장합니다.
7. 강화될 시스템으로 해당 파일을 안전하게 이동합니다.
보안 복사 명령인 `scp(1)`를 사용하거나 보안 파일 전송을 제공하는 다른 방법을 사용하십시오.
다음과 같이 `scp` 명령을 사용하십시오.

```
# scp 10_Recommended.zip target01:
```

8. 파일을 /opt/SUNWjass/Patches 디렉토리로 이동하고 압축을 풉니다.
예를 들면,

코드 예 3-1 패치 파일을 /opt/SUNWjass/Patches 디렉토리로 이동

```
# cd /opt/SUNWjass/Patches
# mv /directory in which file was saved/10_Recommended.zip .
# unzip 10_Recommended.zip
Archive:      10_Recommended.zip
  creating: 10_Recommended/
  inflating: 10_Recommended/CLUSTER_README
  inflating: 10_Recommended/copyright
  inflating: 10_Recommended/install_cluster
[. . .]
```

다른 보안 패키지를 다운로드하고 Solaris Security Toolkit 소프트웨어를 실행하면 패치 클러스터 소프트웨어가 자동으로 설치됩니다.

참고 – Recommended and Security Patch Cluster 소프트웨어를

/opt/SUNWjass/Patches 디렉토리에 저장하지 않은 경우, Solaris Security Toolkit 소프트웨어를 실행할 때 경고 메시지가 표시됩니다. OS의 새 릴리스에서 가끔 발생하는 것처럼 적용된 패치 클러스터가 없는 경우 이 메시지를 무시해도 안전합니다.

FixModes 소프트웨어 다운로드

FixModes는 기본 Solaris OS 디렉토리 및 파일 사용 권한을 강화하는 소프트웨어 패키지입니다. 이러한 사용 권한을 강화하면 전체 보안을 크게 개선할 수 있습니다. 사용 권한을 제한할 수록 악의에 찬 사용자가 시스템에 대한 권한을 얻기가 더 어렵습니다.

참고 – Solaris 10 OS 릴리스는 FixModes 소프트웨어에 의해 사전 변경된 객체의 기본 사용 권한을 개선할 수 있도록 변경되어 해당 소프트웨어는 더 이상 필요하지 않게 되었습니다. 그러므로 install-fixmodes 종료 및 감사 스크립트는 Solaris 10 OS를 실행하는 시스템에서 사용할 수 없습니다.

▼ FixModes 소프트웨어 다운로드

1. 다음 위치에서 사전에 이진 코드로 컴파일된 **FixModes** 소프트웨어를 다운로드합니다.

<http://www.sun.com/security/jass>

FixModes 소프트웨어는 Solaris OS 시스템용으로 형식화된 사전 컴파일되고 압축된 패키지 버전 파일로서 배포됩니다. 파일 이름은 SUNBEfixm.pkg.Z입니다.

2. scp 명령이나 안전한 파일 전송을 제공하는 다른 방법을 사용하여 강화될 시스템으로 해당 파일을 안전하게 이동합니다.

다음과 같이 scp 명령을 사용하십시오.

```
# scp SUNBEfixm.pkg.Z target01:
```

3. 다음 명령으로 /opt/SUNWjass/Packages의 **Solaris Security Toolkit Packages** 디렉토리에 SUNBEfixm.pkg.Z 파일을 압축을 풀고 저장합니다.

```
# uncompress SUNBEfixm.pkg.Z
# mv SUNBEfixm.pkg /opt/SUNWjass/Packages/
```

나중에 다른 모든 보안 패키지를 다운로드하고 Solaris Security Toolkit 소프트웨어를 실행하면 FixModes 소프트웨어가 자동으로 설치됩니다.

OpenSSH 소프트웨어 다운로드

보안된 환경에서 사용자 대화식 세션을 보호하려면 철저하게 인증되는 암호를 사용해야 합니다. 최소한 네트워크 액세스를 암호화해야 합니다.

암호화를 구현하기 위해 가장 일반적으로 사용되는 도구는 Secure Shell 소프트웨어로서 Solaris OS와 함께 번들로 제공되는 버전이나 타사의 상업용 버전 또는 프리웨어 버전을 사용합니다. Solaris Security Toolkit 소프트웨어가 수행하는 모든 보안 수정 사항을 적용하려면, Secure Shell 소프트웨어 제품이 있어야 합니다.

참고 – Solaris 9 또는 10 OS를 사용하는 경우, 운영체제와 함께 제공된 Secure Shell 버전을 사용하십시오. 이 버전의 Secure Shell은 Sun의 지원 조직에 의한 지원뿐 아니라 BSM(Basic Security Module) 같은 다른 Solaris OS 보안 기능과 통합합니다.

Solaris Security Toolkit 소프트웨어를 실행하면 시스템의 암호화되지 않은 사용자 대화식 서비스 및 데몬(특히 in.telnetd, in.ftpd, in.rshd 및 in.rlogind)이 모두 비활성화됩니다.

Secure Shell을 사용하면 텔넷과 FTP를 사용하는 경우와 마찬가지로 시스템에 액세스할 수 있습니다.

▼ OpenSSH 소프트웨어 다운로드

참고 - 서버가 Solaris 9 또는 10 OS를 실행 중인 경우 번들로 제공되는 Secure Shell 소프트웨어를 사용하고 이 절의 OpenSSH 설치 단계를 생략할 수 있습니다.

install-ssh 종료 및 감사 스크립트는 Solaris 10 OS를 실행하는 시스템에서 사용할 수 없습니다.

- 다음 **Sun BluePrints Online** 기사 또는 **Sun BluePrints** 설명서에서 소프트웨어 다운로드에 대한 지침을 얻을 수 있습니다.
 - OpenSSH 컴파일 및 전개 방법에 대한 Sun BluePrints OnLine 기사, "Building and Deploying OpenSSH on the Solaris Operating Environment"는 다음 위치에서 찾을 수 있습니다.
<http://www.sun.com/blueprints>
 - Sun BluePrints 참고 서적 *Secure Shell in the Enterprise*는 서점에서 구할 수 있습니다.

다른 모든 보안 패키지를 다운로드하고 Solaris Security Toolkit 소프트웨어를 실행한 후 OpenSSH 소프트웨어가 자동으로 설치됩니다.



주의 - 강화될 시스템에서 OpenSSH를 컴파일하지 말고 강화될 시스템에 컴파일러를 설치하지 마십시오. 동일한 Solaris OS 버전, 구조 및 모드를 실행하는 별도의 Solaris OS 시스템(예: Solaris 8 OS, Sun4U™ (sun4u) 및 64비트)을 사용하여 OpenSSH를 컴파일하십시오. 상업용 SSH 버전을 구현하는 경우 컴파일이 필요 없습니다. 잠재적인 침입자에 대한 컴파일러 기능을 제한하는 것이 목적입니다. 그러나 시스템에 지역적으로 컴파일러를 설치하지 않는다 해도 여전히 사전에 컴파일된 도구를 설치할 수 있기 때문에 의도적인 공격자에 대해서까지 보호할 수는 없습니다.

MD5 소프트웨어 다운로드

MD5 소프트웨어는 강화되는 시스템에 MD5 디지털 지문을 생성합니다. 디지털 지문을 생성한 후, 이를 Sun이 올바르다고 공개한 것과 비교하여 허가받지 않은 사용자에 의해 변경되거나 안전해 보이는 것 안에 숨겨진(악성 코드가 삽입된) 시스템 이진을 감지하십시오. 공격자는 시스템 이진을 수정하여 시스템에 대한 백도어 액세스를 확보합니다. 즉, 자신의 존재를 숨기고 시스템을 불안정하게 작동시킬 수 있습니다.

참고 - 서버에서 Solaris 10 OS가 실행되고 있는 경우, /usr/bin/digest 명령 세트를 사용하여 이 절의 MD5 설치 단계를 생략할 수 있습니다.

▼ MD5 소프트웨어 다운로드

참고 - 이 절차의 설명과 같이 Solaris 10 시스템의 Solaris Security Toolkit은 MD5 소프트웨어의 설치를 감사하거나 설치하지 않습니다. digest(1M) 명령이 MD5 기능을 포함하므로 Solaris 10 OS를 실행하는 시스템에는 MD5가 필요하지 않습니다.

1. 다음 웹 사이트에서 **MD5** 이진을 다운로드합니다.

`http://www.sun.com/security/jass`

MD5 프로그램은 압축 패키지 버전 파일로서 배포됩니다.

2. `scp` 명령이나 안전한 파일 전송을 제공하는 다른 방법을 사용하여 `SUNBEmd5.pkg.Z` 파일을 안전하게 강화될 시스템으로 이동합니다.

다음과 같이 `scp` 명령을 사용하십시오.

```
# scp SUNBEmd5.pkg.Z target01:
```

3. 다음과 비슷한 명령을 사용하여 파일을 /opt/SUNWjass/Packages의 **Solaris Security Toolkit Packages** 디렉토리에 압축을 풀고 이동합니다.

```
# uncompress SUNBEmd5.pkg.Z
# mv SUNBEmd5.pkg /opt/SUNWjass/Packages/
```

MD5 소프트웨어가 /opt/SUNWjass/Packages 디렉토리에 저장된 후 Solaris Security Toolkit 소프트웨어를 실행하면 해당 소프트웨어가 설치됩니다.

MD5 이진이 설치된 후 이를 사용하여 Solaris 지문 데이터베이스를 통해 시스템에 있는 실행 파일의 무결성을 검증할 수 있습니다. Solaris 지문 데이터베이스에 대한 자세한 정보는 Sun BluePrints OnLine 기사 "The Solaris Fingerprint Database — A Security Tool for Solaris Software and Files"에 있습니다.

4. (선택사항) 다음 위치의 **Sun BluePrint** 웹 사이트에서 **Solaris Fingerprint Database Companion** 및 **Solaris Fingerprint Database Sidekick** 소프트웨어를 다운로드하고 설치합니다.

`http://www.sun.com/blueprints/tools`

참고 - 4단계는 선택사항이지만 모든 운영체제에서 매우 유익하게 사용할 수 있습니다.

이러한 선택 도구를 MD5 소프트웨어와 함께 설치하고 사용하십시오. 이들 도구는 MD5 체크섬의 데이터베이스에 대해 시스템 이진을 검증하는 프로세스를 간단하게 만듭니다. 이러한 도구를 자주 사용하여 보안된 시스템의 Solaris OS 이진 및 파일의 무결성을 검증하십시오.

이들 도구 및 다운로드 지침은 Sun BluePrints OnLine 기사 "The Solaris Fingerprint Database — A Security Tool for Solaris Software and Files"에 있습니다.

다운로드한 보안 도구의 무결성을 확인해야 합니다. Solaris Security Toolkit 소프트웨어 및 추가 보안 소프트웨어를 설치하고 실행하기 전에 MD5 체크섬을 사용하여 무결성을 검증하십시오. Solaris Security Toolkit의 다운로드 페이지에서 MD5 체크섬을 구할 수 있습니다.

보안 프로파일 사용자 정의

다양한 보안 프로파일 템플릿이 Solaris Security Toolkit 소프트웨어 배포에 드라이버로서 포함되어 있습니다. 이러한 드라이버로부터 구현되는 보안 프로파일은 불필요한 서비스를 비활성화하고 `secure.driver`로부터 비활성화된 선택적 보안 기능을 활성화합니다. 이전 장에서 언급한 것처럼 기본 보안 프로파일 및 이들 드라이버로 작성된 변경이 사용자 시스템에 적합하지 않을 수 있습니다.

Solaris Security Toolkit 소프트웨어를 실행하기 전에 기본 보안 프로파일을 검토하고 사용자 환경에 맞게 사용자 정의하거나 새 프로파일을 개발하십시오. 보안 프로파일 사용자 정의에 대한 방법과 지침은 Solaris Security Toolkit 4.2 Reference Manual에 있습니다.

소프트웨어 설치 및 실행

Solaris Security Toolkit 소프트웨어를 실행하기 전에 다음 예비 작업을 완료하는 것이 중요합니다. 대부분의 강화는 Solaris Security Toolkit 소프트웨어를 실행할 때 자동으로 완료됩니다.

- 강화하려는 시스템이나 JumpStart 서버에 추가 보안 소프트웨어와 Solaris Security Toolkit 소프트웨어를 다운로드하십시오. 40페이지에 "보안 소프트웨어 다운로드"를 참조하십시오.
- 시스템을 독립형 또는 JumpStart 모드로 구성하십시오. 36페이지에 "사용할 모드 판별"을 참조하십시오.

- 필요한 경우, 사용 환경에 맞게 Solaris Security Toolkit 소프트웨어를 사용자 정의하십시오.
- Solaris Security Toolkit 소프트웨어 및 추가 보안 소프트웨어를 설치하고 실행하기 전에 MD5 체크섬을 사용하여 무결성을 검증하십시오.

명령줄에서 직접 또는 JumpStart 서버에서 Solaris Security Toolkit 소프트웨어를 실행할 수 있습니다.

명령줄 옵션 및 소프트웨어 실행에 대한 기타 정보는 다음 중 하나를 참조하십시오.

- 48페이지에 "독립형 모드에서 소프트웨어 실행"
- 58페이지에 "JumpStart 모드에서 소프트웨어 실행"

독립형 모드에서 소프트웨어 실행

코드 예 3-2는 독립형 모드에서 명령줄 사용법의 예를 보여줍니다.

코드 예 3-2 독립형 모드의 명령줄 사용 예제

```
# ./jass-execute -h

usage:

To apply this Toolkit to a system, using the syntax:
jass-execute [-r root_directory -p os_version ]
             [ -q | -o output_file ] [ -m e-mail_address ]
             [ -V [3|4] ] [ -d ] driver

To undo a previous application of the Toolkit from a system:
jass-execute -u [ -b | -f | -k ] [ -q | -o output_file ]
             [ -m e-mail_address ] [ -V [3|4] ]

To audit a system against a pre-defined profile:
jass-execute -a driver [ -V [0-4] ] [ -q | -o output_file ]
             [ -m e-mail_address ]

To remove saved files from a previous run of the Toolkit:
jass-execute -c [ -q | -o output_file ]
             [ -m e-mail_address ] [ -V [3|4] ]

To display the history of Toolkit applications on a system:
jass-execute -H

To display the last application of the Toolkit on a system:
jass-execute -l

To display this help message:
```


코드 예 3-2 독립형 모드의 명령줄 사용 예제 (계속)

```
jass-execute -h
jass-execute -?

To display version information for this program:
jass-execute -v

#
```

표 3-1은 사용 가능한 명령줄 옵션을 나열하고 각 옵션에 대해 설명합니다.

표 3-1 jass-execute와 함께 사용하는 명령줄 옵션

옵션	설명
-a 드라이버	시스템이 보안 프로파일을 준수하는지 판별합니다. -b, -k, -f, -c, -d, -h, -H, -l, -p, -r 또는 -u 옵션과 함께 사용하지 마십시오.
-b	최종 강화 작업 이후에 수동으로 변경된 모든 파일을 백업한 후 시스템을 원래 상태로 복원합니다. -u 옵션만 함께 사용하십시오.
-c	제거 옵션을 지정합니다. 이전 Solaris Security Toolkit 작업에서 저장된 파일을 삭제합니다.
-d 드라이버	독립형 모드에서 실행될 드라이버를 지정합니다. -a, -b, -c, -f, -h, -H, -k 또는 -u 옵션과 함께 사용하지 마십시오.
-f	파일이 강화 작업 후에 수동으로 변경된 경우에도 사용자에게 예외에 대해 알리지 않고 강화 작업 중에 작성된 변경을 취소합니다. -u 옵션만 함께 사용하십시오.
-H	시스템에서 Solaris Security Toolkit 소프트웨어의 내역을 표시합니다.
-h -?	사용 가능한 옵션의 개요를 제공하는 jass-execute 도움말 메시지를 표시합니다. 따로 사용하십시오. -h -?에 추가로 지정된 모든 옵션은 무시됩니다.
-k	강화 작업 후에 파일에 작성한 모든 수동 변경을 보존합니다. -u 옵션만 함께 사용하십시오.
l	시스템에 설치된 Solaris Security Toolkit의 최종 작업을 표시합니다.
-m 전자우편_주소	사내 지원을 위한 전자우편 주소를 지정합니다.
-o 출력_파일	출력 파일과 출력 파일에 대한 전체 경로를 지정합니다.
-p os_버전	Solaris OS 버전을 지정합니다. 형식은 <code>uname -r</code> 과 동일합니다. -r 루트_디렉토리 옵션과 함께 사용해야 합니다.
-q	정숙 모드를 설정합니다. 이 명령을 실행하는 동안에는 어떤 메시지도 표시되지 않습니다. 출력 결과는 JASS_REPOSITORY/에 저장됩니다.

표 3-1 jass-execute와 함께 사용하는 명령줄 옵션 (계속)

옵션	설명										
-r 루트_디렉토리	jass-execute 실행 중에 사용되는 루트 디렉토리를 지정합니다. 이 루트 디렉토리는 /이며 Solaris Security Toolkit 환경 변수 JASS_ROOT_DIR에 의해 정의됩니다. 보안되는 Solaris OS는 /를 통해 사용 가능합니다. 예를 들어 /mnt에 임시로 마운트되는 별도의 OS 디렉토리를 보안하려는 경우 -r 옵션을 사용하여 /mnt를 지정합니다. -p os_버전 옵션과 반드시 함께 사용해야 합니다.										
-u	예외가 발생했을 때 사용자가 취하고자 하는 활동을 묻는 대화식 프롬프트와 함께 해당 실행 취소 옵션을 실행합니다. -a, -c, -d, -h, -l, -p, -r 또는 -H 옵션과 함께 사용하지 마십시오.										
-v 상세_레벨	감사 실행에 대한 상세 (verbosity) 레벨을 지정합니다. 상세 레벨에는 5 단계 (0-4)가 있습니다. <table border="0" style="margin-left: 20px;"> <tr> <td style="padding-right: 20px;">0</td> <td>통과 또는 실패를 나타내는 단일 행.</td> </tr> <tr> <td>1</td> <td>각 스크립트에 대해 통과 또는 실패를 나타내는 단일 행 및 모든 스크립트 행 아래에 있는 하나의 총 점수 행.</td> </tr> <tr> <td>2</td> <td>각 스크립트에 대해 모든 점검 결과를 제공합니다.</td> </tr> <tr> <td>3</td> <td>배너 및 헤더 메시지를 포함하여 전체 출력을 제공하는 여러 행. 이것은 기본값입니다.</td> </tr> <tr> <td>4</td> <td>여러 행 (레벨 3에서 제공되는 모든 데이터) 및 logDebug 로깅 기능에 의해 생성되는 모든 항목. 이 레벨은 디버깅용입니다.</td> </tr> </table>	0	통과 또는 실패를 나타내는 단일 행.	1	각 스크립트에 대해 통과 또는 실패를 나타내는 단일 행 및 모든 스크립트 행 아래에 있는 하나의 총 점수 행.	2	각 스크립트에 대해 모든 점검 결과를 제공합니다.	3	배너 및 헤더 메시지를 포함하여 전체 출력을 제공하는 여러 행. 이것은 기본값입니다.	4	여러 행 (레벨 3에서 제공되는 모든 데이터) 및 logDebug 로깅 기능에 의해 생성되는 모든 항목. 이 레벨은 디버깅용입니다.
0	통과 또는 실패를 나타내는 단일 행.										
1	각 스크립트에 대해 통과 또는 실패를 나타내는 단일 행 및 모든 스크립트 행 아래에 있는 하나의 총 점수 행.										
2	각 스크립트에 대해 모든 점검 결과를 제공합니다.										
3	배너 및 헤더 메시지를 포함하여 전체 출력을 제공하는 여러 행. 이것은 기본값입니다.										
4	여러 행 (레벨 3에서 제공되는 모든 데이터) 및 logDebug 로깅 기능에 의해 생성되는 모든 항목. 이 레벨은 디버깅용입니다.										
-v	이 프로그램의 버전 정보를 표시합니다.										

독립형 모드에서 jass-execute 명령과 함께 사용 가능한 옵션에 대한 자세한 정보는 다음 절을 참조하십시오.

- 52페이지에 "감사 옵션"
- 52페이지에 "제거 옵션"
- 53페이지에 "도움말 표시 옵션"
- 54페이지에 "드라이버 옵션"
- 55페이지에 "전자 우편 통지 옵션"
- 56페이지에 "실행 내역 옵션"
- 56페이지에 "최근 실행 옵션"
- 57페이지에 "출력 파일 옵션"
- 57페이지에 "정숙 출력 옵션"
- 57페이지에 "루트 디렉토리 옵션"
- 58페이지에 "실행 취소 옵션"

사용 가능한 드라이버의 전체 목록은 5페이지에 "Drivers 디렉토리"를 참조하십시오. 소프트웨어의 최신 버전에 추가 드라이버가 있을 수 있습니다.

▼ 독립형 모드에서 소프트웨어 실행

1. 다음과 같이 `secure.driver`(또는 `sunfire_15k_sc-secure.driver` 같은 제품 특정 스크립트)를 실행합니다.

코드 예 3-3 독립형 모드에서 소프트웨어 실행

```
# ./jass-execute -d secure.driver

[NOTE] The following prompt can be disabled by setting
JASS_NOVICE_USER to 0.
[WARN] Depending on how the Solaris Security Toolkit is configured,
it is both possible and likely that by default all remote shell
and file transfer access to this system will be disabled upon
reboot effectively locking out any user without console access to
the system.

Are you sure that you want to continue? (YES/NO) [NO]
Y

[NOTE] Executing driver, secure.driver

=====
secure.driver: Driver started.
=====

=====
Solaris Security Toolkit Version: 4.2.0
Node name:                        ufudu
Zone name:                        global
Host ID:                          8085816e
Host address:                     10.8.31.115
MAC address:                      8:0:20:85:81:6e
OS version:                       5.10
Date:                             Tue Jul 5 16:28:24 EST 2005
=====
[...]
```

사용 가능한 드라이버의 전체 목록은 5페이지에 "Drivers 디렉토리"를 참조하십시오. 소프트웨어의 최신 버전에 추가 드라이버가 있을 수 있습니다.

2. 시스템에서 **Solaris Security Toolkit** 소프트웨어를 실행한 후, 시스템을 재부팅하면 변경사항이 적용됩니다.

강화 작업 중에 클라이언트의 구성이 다양하게 수정됩니다. 이러한 수정에는 서비스용 시작 스크립트 사용 불가, 서비스용 옵션 사용 불가 및 패치를 통한 새 이진 또는 라이브러리 설치가 포함될 수 있습니다. 클라이언트가 다시 시작될 때까지 이들 수정은 활성화되지 않을 수 있습니다.

3. 시스템을 재부팅한 후 수정의 정확성과 완전성을 검증합니다.
59페이지에 "시스템 수정 검증"을 참조하십시오.
4. 오류가 발생하는 경우 오류를 수정하고 독립형 모드에서 **Solaris Security Toolkit** 소프트웨어를 다시 실행합니다.

감사 옵션

Solaris Security Toolkit 소프트웨어는 `-a` 옵션을 통해 감사 실행을 수행하여 시스템이 보안 프로파일을 준수하는지 판별할 수 있습니다. 이 실행은 작성된 시스템 파일 수정이 여전히 활동하는지 여부뿐 아니라 이전에 사용 불가능하게 된 프로세스가 실행 중인지 아니면 제거된 소프트웨어 패키지가 다시 설치되었는지를 검증합니다. 이 기능에 대한 자세한 정보는 6 장을 참조하십시오.

보안 프로파일에 대해 시스템을 감사하는 명령줄 사용 개요:

```
# jass-execute -a 드라이버 [ -v [0-4] ] [ -q | -o 출력파일 ]
[ -m 전자우편주소 ]
```

제거 옵션

`-c` 옵션은 이전 Solaris Security Toolkit 작업에서 저장된 파일을 삭제합니다. 제거 옵션과 함께 정숙(`-q`), 출력(`-o`), 전송(`-m`) 및 상세(`-v`) 옵션을 사용할 수 있습니다.

코드 예 3-4는 다음과 유사한 출력 결과를 생성하는 `-c` 옵션 사용의 예를 보여줍니다.

코드 예 3-4 예제 `-c` 옵션 출력

```
# bin/jass-execute -c
Executing driver, clean.driver

Please select Solaris Security Toolkit runs to clean:
1. July 15, 2005 at 11:41:02 (/var/opt/SUNWjass/run/20050715114102)
2. July 15, 2005 at 11:44:03 (/var/opt/SUNWjass/run/20050715114403)
Choice ('q' to exit)? 2
[NOTE] Cleaning previous run from /var/opt/SUNWjass/run/20050715114403

=====
clean.driver: Driver started.
=====

=====
Toolkit Version: 4.2.0
Node name:      sstzone
```

코드 예 3-4 예제 -c 옵션 출력 (계속)

```
Zone name:      sstzone
Host ID:        80cb346c
Host address:   10.8.28.45
MAC address:    8:0:20:cb:34:6c
OS version:     5.10
Date:          Fri Jul 15 11:44:58 PDT 2005

=====
clean.driver: Performing CLEANUP of /var/opt/SUNWjass/run/20050715114403.
=====

=====
clean.driver: Driver finished.
=====

=====
[SUMMARY] Results Summary for CLEAN run of clean.driver
[SUMMARY] The run completed with a total of 1 script run.
[SUMMARY] There were Failures in 0 Scripts
[SUMMARY] There were Errors in 0 Scripts
[SUMMARY] There were Warnings in 0 Scripts
[SUMMARY] There was a Note in 1 Script
[SUMMARY] Notes Scripts listed in:
           /var/opt/SUNWjass/run/20050715114403/jass-clean-script-notes.txt
=====
```

도움말 표시 옵션

-h 옵션은 사용 가능한 옵션의 개요를 제공하는 jass-execute 도움말 메시지를 표시합니다.

-h 옵션은 다음과 비슷한 출력을 작성합니다.

코드 예 3-5 예제 -h 옵션 출력

```
# ./jass-execute -h
To apply this Toolkit to a system, using the syntax:
  jass-execute [-r root_directory -p os_version ]
                [ -q | -o output_file ] [ -m e-mail_address ]
                [ -V [3|4] ] [ -d ] driver

To undo a previous application of the Toolkit from a system:
  jass-execute -u [ -b | -f | -k ] [ -q | -o output_file ]
                [ -m e-mail_address ] [ -V [3|4] ]

To audit a system against a pre-defined profile:
```

코드 예 3-5 예제 -h 옵션 출력 (계속)

```
jass-execute -a driver [ -V [0-4] ] [ -q | -o output_file ]  
[ -m e-mail_address ]
```

To remove saved files from a previous run of the Toolkit:

```
jass-execute -c [ -q | -o output_file ]  
[ -m e-mail_address ] [ -V [3|4] ]
```

To display the history of Toolkit applications on a system:

```
jass-execute -H
```

To display the last application of the Toolkit on a system:

```
jass-execute -l
```

To display this help message:

```
jass-execute -h  
jass-execute -?
```

To display version information for this program:

```
jass-execute -v
```

Note that just the driver name should be specified when using the `-d` or `-a` options. A path need not be specified as the script is assumed to exist in the Drivers directory.

The `-u` undo option is mutually exclusive with the `-d` and `-a` options. The default undo behavior is to ask the user what to do if a file to be restored has been modified as the checksum is incorrect.

The `-u` option can be combined with the `-k`, `-b`, or `-f` to override the default interactive behavior. The use of one of these options is required when run in quiet mode (`-q`).

The `-k` option can be used to always keep the current file and backup if checksum is incorrect. The `-b` can be used to backup the current file and restore original if the checksum is incorrect. The `-f` option will always overwrite the original if the checksum is incorrect, without saving the modified original.

드라이버 옵션

-d 드라이버 옵션은 독립형 모드에서 실행될 드라이버를 지정합니다.

-d 옵션과 함께 드라이버를 지정해야 합니다. Solaris Security Toolkit 소프트웨어는 추가된 스크립트의 이름 앞에 Drivers/를 붙입니다. 명령줄에는 스크립트 이름만 입력하면 됩니다.

참고 - `-d` option with the `-a`, `-b`, `-c`, `-f`, `-H`, `-h`, `-k` 또는 `-u` 옵션과 함께 사용하지 마십시오.

`-d` 드라이버 옵션을 사용한 `jass-execute` 강화 작업은 다음과 비슷한 출력을 생성합니다.

코드 예 3-6 예제 `-d` 드라이버 옵션 출력

```
# ./jass-execute -d secure.driver
[...]
[NOTE] Executing driver, secure.driver

=====
secure.driver: Driver started.
=====

=====
Solaris Security Toolkit Version: 4.2.0
Node name:                ufudu
Zone name:                global
Host ID:                  8085816e
Host address:             10.8.31.115
MAC address:              8:0:20:85:81:6e
OS version:               5.10
Date:                    Tue Jul 5 16:28:24 EST 2005
=====
[...]
```

전자 우편 통지 옵션

`-m` 전자우편_주소 옵션은 실행이 완료될 때 독립형 강화, 감사, 제거 및 실행 취소 출력이 Solaris Security Toolkit 소프트웨어에 의해 자동으로 전자 우편을 통해 보내질 수 있는 체계를 제공합니다. 전자우편 보고는 기타 옵션을 사용하여 시스템에서 생성된 모든 기록과 Solaris Security Toolkit 소프트웨어에서 생성된 로컬 로그와 더불어 추가 작동합니다.

전자 우편 옵션을 사용하여 `sunfire_15k_sc-config.driver`를 호출하는 Solaris Security Toolkit 실행은 다음과 비슷합니다.

```
# ./jass-execute -m root -d sunfire_15k_sc-config.driver
[...]
```

실행 내역 옵션

-H 옵션은 Solaris Security Toolkit 소프트웨어가 한 시스템에서 실행된 횟수를 판별하는 간단한 체계를 제공합니다. 실행 취소되었는지 여부와 상관없이 모든 실행이 나열됩니다.

-H 옵션은 다음과 비슷한 출력을 작성합니다.

코드 예 3-7 예제 -H 옵션 출력

```
# ./jass-execute -H
Note: This information is only applicable for applications of
      the Solaris Security Toolkit starting with version 0.3.

The following is a listing of the applications of the Solaris
Security Toolkit on this system. This list is provided in
reverse chronological order:

1.   June 31, 2004 at 12:20:19 (20040631122019) (UNDONE)
2.   June 31, 2004 at 12:10:29 (20040631121029)
3.   June 31, 2004 at 12:04:15 (20040631120415)
```

이 출력은 Solaris Security Toolkit 소프트웨어가 이 시스템에서 세 번 실행되었고 최근의 실행이 취소되었음을 나타냅니다.

최근 실행 옵션

-l 옵션은 최근 실행을 판별하는 체계를 제공합니다. 이것은 또한 항상 -H 옵션에 의해 나열되는 마지막 실행입니다.

-l 옵션은 다음과 비슷한 출력을 제공합니다.

코드 예 3-8 예제 -l 옵션 출력

```
# ./jass-execute -l
Note: This information is only applicable for applications of
      the Solaris Security Toolkit starting with version 4.2.0.

The last application of the Solaris Security Toolkit was:

1.   June 31, 2005 at 12:20:19 (20040631122019) (UNDONE)
```


출력 파일 옵션

-o 출력_파일 옵션은 jass-execute 실행의 콘솔 출력을 별개의 출력_파일로 재지정합니다. 출력_파일에 대한 정규식 이름을 지정할 수 있습니다.

이 옵션은 JASS_REPOSITORY 디렉토리에 보존되는 로그에는 아무 영향도 주지 않습니다. 이 옵션은 특히 느린 터미널 연결을 통해 수행될 때 유용합니다. 지정한 상세 레벨에 따라 Solaris Security Toolkit 실행으로부터 매우 많은 양의 출력이 생성될 수 있습니다.

이 옵션은 -a, -d 또는 -u 옵션과 함께 사용할 수 있습니다.

-o 옵션은 다음과 비슷한 출력을 표시합니다.

코드 예 3-9 예제 -o 옵션 출력

```
# ./jass-execute -o /var/tmp/root/jass-output.txt -d secure.driver
[NOTE] Executing driver, secure.driver
[NOTE] Recording output to /var/tmp/root/jass-output.txt
```

정숙 출력 옵션

-q 옵션은 강화 작업 중에 Solaris Security Toolkit 출력이 콘솔로 이동하는 것을 비활성화합니다.

이 옵션은 JASS_REPOSITORY 디렉토리에 보존되는 로그에는 아무 영향도 주지 않습니다. -o 옵션과 비슷하게, 이 옵션은 특히 cron 작업 또는 느린 네트워크 연결을 통해 Solaris Security Toolkit 소프트웨어를 실행할 때 도움이 됩니다.

이 옵션은 -a, -c, -d 또는 -u 옵션과 함께 사용할 수 있습니다.

-q 옵션은 다음과 비슷한 출력을 작성합니다.

코드 예 3-10 예제 -q 옵션 출력

```
# ./jass-execute -q -d secure.driver
[NOTE] Executing driver, secure.driver
```

루트 디렉토리 옵션

-r 루트디렉토리 옵션은 jass-execute 실행 중에 사용되는 루트 디렉토리를 지정하기 위한 것입니다. -r 옵션 사용은 또한 -p 옵션을 사용하여 플랫폼(OS) 버전을 지정해야 합니다. -p 옵션의 형식은 uname -r에 의해 작성되는 형식과 동등합니다.

이 루트 디렉토리는 /이며 Solaris Security Toolkit 환경 변수 JASS_ROOT_DIR에 의해 정의됩니다. 보안되는 Solaris OS는 /를 통해 사용 가능합니다. 예를 들어 /mnt에 임시로 마운트되는 별도의 OS 디렉토리를 보안하려는 경우 -r 옵션을 사용하여 /mnt를 지정합니다. 모든 스크립트가 해당 OS 이미지에 적용됩니다.

실행 취소 옵션

-u 옵션을 통해 Solaris Security Toolkit 소프트웨어가 강화 중에 수행되는 시스템 수정 사항을 실행 취소할 수 있습니다. 각 종료 스크립트는 -u 옵션으로 실행 취소할 수 있습니다. 또한 Solaris Security Toolkit의 실행 취소 능력은 각 실행 중에 생성되는 체크섬과 밀접하게 통합됩니다. 이 기능에 대한 자세한 정보는 4 장을 참조하십시오.

-u 옵션과 함께 사용할 수 있는 세 가지 옵션은 다음과 같습니다.

- -b(백업) 옵션 - 최종 강화 작업 이후에 수동으로 변경된 모든 파일을 백업한 후 시스템을 원래 상태로 복원합니다.
- -f(강제) 옵션 - 파일이 강화 작업 후에 수동으로 변경된 경우에도 사용자에게 예외에 대해 알리지 않고 강화 작업 중에 작성된 변경을 취소합니다.
- -k(보존) 옵션 - 최종 강화 작업 이후에 수동으로 변경한 내용을 보존합니다.

실행 취소 명령의 명령줄 사용 개요:

```
# jass-execute -u [ -b | -f | -k ] [ -q | -o 출력_파일 ]  
[ -m 전자우편_주소 ] [ -v [3|4] ]
```

JumpStart 모드에서 소프트웨어 실행

JumpStart 모드는 JumpStart 서버의 rules 파일에 삽입된 Solaris Security Toolkit 드라이버에 의해 제어됩니다.

JumpStart 모드를 사용하도록 환경을 구성하지 않은 경우 5 장을 참조하십시오.

JumpStart 기술에 대한 자세한 정보는 Sun BluePrints 설명서 JumpStart Technology: Effective Use in the Solaris Operating Environment를 참조하십시오.

▼ JumpStart 모드에서 소프트웨어 실행

JumpStart 모드에서 Solaris Security Toolkit 소프트웨어를 실행하려면 JumpStart 환경에 통합되고 JumpStart 설치와 연관된 종료 스크립트의 일부로서 호출되어야 합니다. Solaris Security Toolkit 소프트웨어를 사용자 환경에 통합하는 방법에 대해서는 5 장을 참조하십시오.

1. 드라이버에 모든 필수 수정 사항을 적용한 후, **JumpStart** 기반 구조를 사용하여 클라이언트를 설치합니다.

이 작업은 클라이언트의 ok 프롬프트에서 다음 명령을 사용하여 수행됩니다.

```
ok> boot net - install
```

설치가 완료된 후 시스템이 **JumpStart** 소프트웨어에 의해 재부팅됩니다.

시스템이 올바른 구성 상태에 있어야 합니다. 강화 작업 중에 클라이언트의 구성이 다양하게 수정됩니다. 이러한 수정에는 서비스용 시작 스크립트 사용 불가, 서비스용 옵션 사용 불가 및 패치를 통한 새 이진 또는 라이브러리 설치가 포함될 수 있습니다. 클라이언트가 다시 시작될 때까지 이들 수정은 효력을 갖지 않습니다.

2. 시스템이 재부팅된 후 수정 사항이 제대로 올바르게 적용되었는지 검증합니다.
59페이지에 "시스템 수정 검증"을 참조하십시오.
3. 오류가 발생하는 경우 오류를 수정하고 클라이언트 **OS**를 다시 설치합니다.

시스템 수정 검증

시스템을 재부팅한 후, 다음 절에서 설명하는 것처럼 수정사항의 정확성과 완전성을 검증하십시오.

서비스에 대한 QA 점검 수행

시스템 보안에 관련되는 중대한 도전 중 하나는 시스템이 제대로 기능하기 위해 계속 사용 가능해야 하는 OS 서비스를 판별하는 것입니다. Solaris OS 서비스는 시스템에 로그인하기 위해 직접 사용되기 때문에(예: Secure Shell) 필요할 수 있습니다. 또는 타사 소프트웨어 관리 도구의 그래픽 사용자 인터페이스(GUI)용으로 RPC 데몬을 사용하는 것처럼 간접적으로 사용할 수 있습니다.

이들 요구사항의 대부분은 Solaris Security Toolkit 소프트웨어를 실행하기 전에 판별되어야 합니다. (21페이지에 "서비스 요구사항 판별"을 참조하십시오.) 그러나 유일하게 결정적인 체계는 시스템을 설치 및 보안한 후 품질 보장(QA) 테스트를 통한 필수 기능성의 철저한 테스트를 수행하는 것입니다. 시스템이 강화된 후 전개되는 모든 새로운 시스템에 대해 QA 계획이 실행되어야 합니다. 비슷하게 강화될 전개된 시스템의 경우 모든 필수 및 예상 기능이 존재하는지 확인하기 위해 철저한 테스트를 수행해야 합니다.

QA 프로세스가 어떤 모순도 적발하지 않는 경우 다음을 수행하십시오.

1. 2 장의 지침을 기초로 문제 영역을 판별합니다.
2. 응용프로그램이 수정된 구성에서 실행하는지 검증합니다.
3. Solaris Security Toolkit의 실행을 취소합니다.
4. 문제점 해결에 근거하여 보안 프로파일(드라이버)을 수정합니다.
5. Solaris Security Toolkit 소프트웨어를 다시 실행합니다.

종료 결과가 어떤 필수 기능에도 부정적으로 영향을 주지 않고 시스템에서 실행될 수 있는 보안 프로파일이어야 합니다.

구성의 보안 평가 수행

시스템이 모든 필수 기능을 수행하는지 검증하는 동안 보안 구성을 평가하여 시스템이 원하는 레벨로 보안되는지 판별하십시오. 시스템에 수행된 강화 또는 최소화에 따라서 이것이 다른 측면과 관련될 수 있습니다.

최소한 다음 방법으로 시스템의 구성을 검토해야 합니다.

- 필요한 Security and Recommended Patches가 모두 설치되었는지 확인합니다.
- 필수 및 중요한 프로세스만이 실행 중이고 이들이 올바른 인수와 함께 실행 중인지 확인합니다.
- 필수 데몬만이 실행 중이고 이들이 올바른 인수와 함께 실행 중인지 확인합니다.
- 지역적으로(예를 들어 `netstat -a`) 및 네트워크 인터페이스에서 사용 가능한 포트를 판별할 수 있는 Nmap 같은 포트 스캐너를 사용하여 원격으로 점검하여 시스템에 필수 포트만이 열려있는지 확인합니다.
- 시스템이 최소화된 경우 필수 Solaris OS 패키지만 설치되었는지 확인합니다.

이 검토가 새로 구축되고 보안된 시스템에 대한 최소로 고려되어야 합니다. 레거시 시스템을 강화할 때 허가되지 않은 수정이 있었는지 판별하기 위해 기초 OS를 검증해야 합니다. 이런 종류의 무결성 점검은 시스템의 파일 시스템을 읽기 전용 모드로 마운트 하고 알려진 OS 인스턴스로부터 무결성 점검 소프트웨어를 실행하여 가장 잘 수행됩니다. Sun BluePrints OnLine 기사 “The Solaris Fingerprint Database—A Security Tool for Solaris Software and Files”에 설명되는 도구가 이 시나리오에 유용합니다.

보안 프로파일 검증

시스템이 보안되고 사용자가 시스템의 필수 서비스 및 능력을 검증한 후 감사 기능을 사용하여 보안 프로파일이 제대로 완벽하게 적용되었는지 확인하십시오. 이 작업은 두 가지 이유 때문에 중요합니다. 첫 번째는 시스템이 필요한 대로 강화되는지 확인하는 것입니다. 두 번째는 시스템에 대해 정의된 보안 프로파일이 Solaris Security

Toolkit 구성에 적절히 반영되도록 보장하는 것입니다. 이 점검은 구성 정보가 시스템의 전체 전개 수명 동안 시스템의 보안 프로파일을 유지 보수하는 데 사용되기 때문에 중요합니다.

감사 기능에 대한 자세한 정보는 6 장을 참조하십시오.

설치 후 작업 수행

전개된 시스템에 소프트웨어를 설치한 경우, 설치 후 작업 수행에 대한 정보는 31페이지에 "설치 후 작업 수행"을 참조하십시오.

시스템 변경 취소

이 장은 강화 작업 중에 Solaris Security Toolkit 소프트웨어를 통해 수행된 변경사항의 역전(실행 취소)에 대한 정보 및 절차를 제공합니다. 이 옵션은 시스템을 Solaris Security Toolkit 강화 작업 또는 일련의 작업 이전의 상태로 되돌릴 수 있는 자동화 체계를 제공합니다.

이 장에서는 다음 주제를 다룹니다.

- 63페이지에 "변경사항이 로깅되고 취소되는 방법 이해"
- 64페이지에 "시스템 변경 실행 취소 요구사항"
- 65페이지에 "변경을 실행 취소하도록 스크립트 사용자 정의"
- 66페이지에 "수동으로 변경된 파일 점검"
- 67페이지에 "실행 취소 기능에서 옵션 사용"
- 70페이지에 "시스템 변경 실행 취소"

변경사항이 로깅되고 취소되는 방법 이해

각 Solaris Security Toolkit 강화 작업은 JASS_REPOSITORY에 작업 디렉토리를 작성합니다. 이들 디렉토리의 이름은 작업이 시작되는 날짜 및 시간을 토대로 합니다. 출력을 화면에 표시하는 것 외에 Solaris Security Toolkit 소프트웨어는 변경을 추적하고 조작을 로깅하는 파일 세트를 디렉토리에 작성합니다.

이 디렉토리에 저장되는 파일이 시스템에 수행된 수정사항을 추적하고 실행 취소 기능이 작동할 수 있게 합니다.



주의 - 관리자는 JASS_REPOSITORY 디렉토리에 있는 파일의 내용을 절대로 수정해서는 안됩니다. 파일을 수정하면 내용이 손상되고 실행 취소 기능을 사용할 때 예기치 않은 오류 또는 시스템 손상이 유발될 수 있습니다.

JumpStart 모드나 독립형 모드에서 Solaris Security Toolkit 소프트웨어를 사용하여 시스템을 강화할 때 소프트웨어는 JASS_REPOSITORY/jass-manifest.txt 파일에 변경을 로깅합니다. 이 파일은 undo 기능이 변경을 실행 취소하는 데 사용하는 조작을 나열합니다. 이 파일에는 작성, 복사, 이동 또는 제거된 파일을 포함하여 Solaris Security Toolkit 소프트웨어에 의해 구현되는 강화 조작에 대한 정보가 들어있습니다. 또한 이 파일은 소프트웨어 패키지 설치와 같은 더 복잡한 변경을 취소할 때 필요한 표준 및 사용자 정의 항목을 포함할 수 있습니다. 각 강화 작업에 대해 별도의 jass-manifest.txt 파일이 작성됩니다.

참고 – Solaris Security Toolkit 소프트웨어 undo 기능은 목록 파일에 항목이 있는 변경만 취소합니다.

undo 작업은 Solaris Security Toolkit 작업 중에 생성되고 JASS_REPOSITORY에 저장되는 목록 파일을 조사합니다. 해당 작업을 실행하면 백업, 강제 또는 보존 옵션 중 어떤 옵션을 선택하는지에 따라 백업 파일을 원래의 위치로 복원합니다. 백업, 강제 및 보존 옵션에 대한 자세한 정보는 다음을 참조하십시오.

- 68페이지에 "백업 옵션"
- 68페이지에 "강제 옵션"
- 68페이지에 "보존 옵션"

JASS_SAVE_BACKUP 변수가 user.init 파일에 0으로 정의되었거나 -c 옵션이 사용된 경우, 강화가 실행되는 동안 파일이 백업되지 않았다면, 실행 취소 기능을 사용할 수 없습니다. 자세한 내용은 64페이지에 "시스템 변경 실행 취소 요구사항"을 참조하십시오.

Solaris Security Toolkit 작업의 실행 취소 시 연결된 디렉토리는 제거되지 않습니다. 대신 JASS_REPOSITORY 디렉토리에 다음 두 파일 jass-undo-log.txt 및 reverse-jass-manifest.txt가 작성됩니다. 그 후, 다음에 jass-execute -u가 실행될 때 실행 취소된 작업이 나열되지 않습니다. 강화 작업은 한 번만 실행 취소할 수 있습니다.

시스템 변경 실행 취소 요구사항

Solaris Security Toolkit 소프트웨어의 실행 취소 기능 사용에 대한 다음 한계 및 요구사항을 알고 있어야 합니다.

- Solaris Security Toolkit 버전 0.3에서 4.2까지 독립형 또는 JumpStart 모드에서 시작된 실행에 대해 실행 취소 기능을 사용할 수 있습니다. 그러나 독립형 모드에서만 변경을 실행 취소할 수 있습니다. JumpStart 설치 중에는 실행 취소 기능을 사용할 수 없습니다.

- JumpStart 또는 독립형 모드를 통해 백업 파일을 작성하지 않는 Solaris Security Toolkit 옵션을 선택하는 경우 실행 취소 기능을 사용할 수 없습니다. 백업 파일 사본의 작성은 JASS_SAVE_BACKUP 매개변수를 0으로 설정하여 비활성화 됩니다.
- 작업은 한 번만 실행 취소할 수 있습니다.
- 새로운 종료 스크립트를 개발하는 경우, 반드시 Solaris Security Toolkit 프레임워크 기능을 사용하십시오. add_to_manifest 스크립트를 사용하여 대응하는 감사 스크립트를 작성하고 해당 항목을 목록 파일에 추가해야 합니다. 그렇지 않으면 Solaris Security Toolkit이 사용자 정의 개발에 대해 알 수 있는 방법이 없습니다.
- 어떤 상황에서도 JASS_REPOSITORY 디렉토리의 내용을 수정하지 마십시오. 파일을 수정하면 내용이 손상되고 실행 취소 기능을 사용할 때 예기치 않은 오류 또는 시스템 손상이 유발될 수 있습니다.

변경을 실행 취소하도록 스크립트 사용자 정의

Solaris Security Toolkit 프레임워크는 종료 스크립트 설계 및 구축에 대한 유연성을 제공합니다. 이 프레임워크를 사용하면 Solaris Security Toolkit 소프트웨어의 능력을 확장하여 시스템의 수명 동안 시스템 구성을 잘 관리하는 데 도움을 주면서도 조직의 수요에 더 잘 대응할 수 있습니다.

스크립트를 사용자 정의할 때 사용자가 취하는 조치가 실행 취소 기능에 영향을 줄 수 있는 방법을 이해하는 것이 중요합니다. 스크립트 사용자 정의를 단순화하기 위해 지원 프로그램 기능이 목록 파일을 올바르게 변경합니다. (undo 기능은 강화 작업을 취소하기 위해 목록 파일의 내용에 의존합니다.) 대부분의 경우 이들 지원 프로그램 기능이 조직에 맞게 스크립트를 사용자 정의하기 위해 필요한 것을 제공합니다.

지원 프로그램 기능의 목록과 해당 기능의 사용에 대한 정보는 Solaris Security Toolkit 4.2 Reference Manual을 참조하십시오. 실행 취소 작업이 목록 파일의 관련 항목을 참조할 수 있도록 시스템 명령 대조물 대신 이들 지원 프로그램 기능을 사용하십시오.

어떤 경우에는 지원 프로그램 기능이 없는 기능을 수행해야 할 수 있습니다. 이러한 경우에는 add_to_manifest라는 특수 기능을 사용하십시오. 이 기능을 사용하여 지원 프로그램 기능 중 하나를 호출할 필요 없이 수동으로 목록 파일에 항목을 삽입할 수 있습니다. 이 특수 기능을 주의해서 사용하여 시스템 및 Solaris Security Toolkit 저장소의 무결성을 보호하십시오. 이 특수 기능을 사용할 수 있는 시기의 예는 Sun의 pkg 형식이 아닌 소프트웨어 패키지를 추가할 때입니다. 이 예제에서는 undo 기능에 강화 작업 중에 다른 형식으로 추가된 패키지를 제거하는 방법을 지시해야 합니다.

지원 프로그램 기능과 특수 add_to_manifest 기능을 사용하여 Solaris Security Toolkit 소프트웨어는 스크립트를 사용자 정의하고 변경사항이 실행 취소 작업으로 확장되게 하는 간단하고 유연성 있는 방법을 제공합니다.

이러한 기능을 사용하지 않고 종료 스크립트의 작동을 변경할 경우, Solaris Security Toolkit 소프트웨어는 변경사항이 발생했는지 알 수 없습니다. 그러므로 목록 파일에 참조되지 않은 모든 변경사항을 수동으로 실행 취소해야 합니다.

다른 예제에서는, 시스템의 파일을 수정하기 전에 파일의 원래 버전을 먼저 저장해야 합니다. Solaris Security Toolkit 소프트웨어의 컨텍스트 밖에서, 일반적으로 사용자는 `/usr/bin/cp` 명령을 사용하여 이 작업을 수행합니다. 그러나 Solaris Security Toolkit 소프트웨어의 컨텍스트 내에서 이 명령을 직접 사용할 경우, Solaris Security Toolkit 소프트웨어는 목록 항목의 작성 여부를 알 수 없습니다. `cp` 명령 대신 `backup_file` 지원 프로그램 기능을 사용하십시오. 이 기능은 `JASS_SUFFIX`의 접미어와 함께 원본 파일의 사본을 저장하고 Solaris Security Toolkit 소프트웨어에 파일의 사본이 작성되었음을 알리는 목록 항목을 추가합니다. 이 기능으로 인해 파일 체크섬이 계산됩니다. 파일 체크섬은 `jass-check-sum` 명령 및 실행 취소 기능에 의해 사용됩니다.

수동으로 변경된 파일 점검

`jass-execute -u` 명령이 강화 작업 후에 수동으로 변경된 파일을 자동으로 점검하지 만, 때로는 `jass-check-sum` 명령을 사용하여 변경된 파일을 나열하고 검토하는 것이 유용할 수 있습니다.

이 명령을 사용하면 `JASS_REPOSITORY` 디렉토리의 내용을 검토하고 목록 파일에 나열되는 모든 파일에 대해 체크섬을 수행하여 나열된 파일이 체크섬이 강화 작업 중에 기록된 이후에 변경되었는지 판별할 수 있습니다. 강제 실행 취소 작업을 계속하기 전에 이 점검을 수행하는 것이 많은 불필요한 문제 해결 시간을 저장할 수 있는 가치 있는 정보를 제공합니다.

다음은 예제 출력입니다.

코드 예 4-1 수동으로 변경된 파일의 예제 출력

# ./jass-check-sum		
File Name	Saved CkSum	Current CkSum
- - - - -	- - - - -	- - - - -
/etc/inet/inetd.con	1643619259:6883	2801102257:6879
/etc/logadm.conf	2362963540:1042	640364414:1071
/etc/default/inetd	3677377803:719	2078997873:720

이 출력은 강화 작업이 완료된 후에 3개의 파일이 변경되었음을 나타냅니다.

실행 취소 기능에서 옵션 사용

이 절에서는 실행 취소 작업을 실행할 때 사용할 수 있는 `jass-execute -u` 명령 및 옵션에 대해 설명합니다.

참고 - 실행 취소 기능과 함께 `-c`, `-d`, `-a`, `-h`, `-l` 또는 `-H` 옵션을 사용할 수 없습니다. 정숙 모드에서 `undo` 명령을 실행할 때에는 `-b`, `-k` 또는 `-f` 옵션 중 하나를 제공해야 합니다.

`jass-execute -u` 명령은 `undo` 작업 실행을 위한 표준 방법입니다. 이 명령은 마지막 강화 작업 이후 수동으로 수정된 모든 파일을 자동으로 발견합니다. Solaris Security Toolkit 소프트웨어가 강화 실행 후 수동으로 변경된 파일을 발견할 경우, 응답을 선택하도록 요청합니다.

1. 원본(강화 작업 전에 존재했던 파일)을 복원하기 전에 최신 파일을 백업합니다.
2. 최신 파일을 보존하고 원본 파일을 복원하지 않습니다.
3. 수동으로 변경된 모든 파일을 강제로 겹쳐 쓰고(데이터를 유실할 수 있음) 원본 파일을 복원합니다.
4. 원본(강화 작업 전에 존재했던 파일)을 복원하기 전에 항상 최신 파일을 백업합니다.
5. 최신 파일을 항상 보존하고 원본 파일은 복원하지 않습니다.
6. 수동으로 변경된 모든 파일은 항상 강제로 겹쳐 쓰고(데이터를 유실할 수 있음) 원본 파일을 복원합니다.

강화 작업을 수행한 후에 수정된 모든 파일을 처리할 수 있는 실행 취소 명령을 정의하려는 경우, 백업(`-b`), 보존(`-k`) 또는 강제(`-f`) 옵션을 사용하십시오.

표 4-1은 실행 취소와 함께 사용할 수 있는 명령줄 옵션을 나열합니다. 각 옵션에 대한 자세한 정보는 다음 절을 참조하십시오.

표 4-1 실행 취소 명령과 함께 명령줄 옵션 사용

옵션	설명
<code>-b</code>	최종 강화 작업 이후에 수동으로 변경된 모든 파일을 백업한 후 시스템을 원래 상태로 복원합니다.
<code>-f</code>	파일이 강화 작업 후에 수동으로 변경된 경우에도 사용자에게 예외에 대해 알리지 않고 강화 작업 중에 작성된 변경을 취소합니다.
<code>-k</code>	강화 작업 후에 파일에 작성한 모든 수동 변경을 보존합니다.
<code>-m</code>	출력을 전자 우편 주소로 보냅니다.

표 4-1 실행 취소 명령과 함께 명령줄 옵션 사용 (계속)

옵션	설명
-o	출력을 파일로 보냅니다.
-q	화면에 대한 출력 표시를 금지합니다. 또한 정숙 옵션이라고도 합니다. 출력이 JASS_REPOSITORY/jass-undo-log.txt에 저장됩니다.
-V	실행 취소 작업에 대한 상세(verbosity) 레벨을 지정합니다.

백업 옵션

-b 옵션은 최종 강화 작업 이후에 수동으로 변경된 모든 파일을 자동으로 백업한 후 파일을 강화 작업 전의 원래 상태로 복원합니다. 수동 변경을 구현하기 위해 반드시 복원된 파일을 백업된 파일과 비교하고 그 차이를 수동으로 조정해야 합니다. 파일이 이 옵션을 사용하여 백업되는 경우 다음 예제와 비슷하게 나타납니다.

```
/etc/motd.BACKUP.JASS_SUFFIX
```

강제 옵션

-f 옵션은 파일이 강화 작업 후에 수동으로 변경된 경우에도 예외 없이 강화 작업 중에 작성된 변경사항을 취소합니다. 실행 취소 작업은 저장된 파일 체크섬을 파일의 현재 버전에 비교하지 않습니다. 결국 강화 작업 후에 파일을 수동으로 변경한 경우 실행 취소 작업 후에 변경사항이 겹쳐 써지고 유실됩니다.

실행 취소 작업이 완료된 후 변경사항을 수동으로 다시 구현해야 할 수 있습니다. 게다가 작성된 변경의 유형에 따라서 파일의 그룹 사이의 차이를 조정해야 할 수도 있습니다.

참고 - 이런 문제점을 막으려면 `jass-check-sum` 명령이나 이전에 언급된 `-b` 명령줄 옵션을 사용하십시오.

보존 옵션

-k 옵션은 원본 파일을 복원하는 대신 강화 작업 후 파일에 작성한 모든 수동 변경사항을 자동으로 보존합니다. -k 옵션은 파일의 모든 불일치를 발견하고 주의사항을 생성하고 기록하며 파일을 원본으로 겹쳐 쓰지 않습니다. 취소되는 유일한 변경사항은 저장된 체크섬이 유효한 변경사항입니다.

이 옵션에는 단점이 있습니다. 예를 들어 종료 스크립트에 의해 수정된 파일의 서브셋이 나중에 수정되는 경우 시스템이 일치하지 않는 상태가 될 수 있습니다.

`remove-unneeded-accounts.fin` 종료 스크립트를 고려하십시오. 이 스크립트는 시스템의 `/etc/passwd` 및 `/etc/shadow` 파일을 모두 수정합니다. 사용자가 강화 작업이 종료된 후 수동으로 암호를 변경하는 경우 `/etc/shadow` 파일과 연관된 체크섬이 Solaris Security Toolkit 소프트웨어에 의해 저장된 값과 일치하지 않습니다. 결국, 보존 옵션이 사용되는 경우 `/etc/passwd` 파일만이 원래 상태로 다시 복사됩니다. `/etc/shadow` 파일은 현재 양식으로 유지됩니다. 두 파일은 더 이상 일치하지 않습니다.

출력 파일 옵션

`-o /complete/path/to/output_file` 옵션은 `jass-execute` 작업의 콘솔 출력을 개별 출력_파일로 재지정합니다.

이 옵션은 `JASS_REPOSITORY` 디렉토리에 보존되는 로그에는 아무 영향도 주지 않습니다. 이 옵션은 특히 느린 터미널 연결을 통해 수행될 때 Solaris Security Toolkit 실행 취소 실행에 의해 생성되는 상당한 양의 출력이 있기 때문에 유용합니다.

정숙 출력 옵션

참고 - 정숙 모드에서 `undo` 명령을 실행할 때에는 `-b`, `-k` 또는 `-f` 옵션 중 하나를 제공해야 합니다.

`-q` 옵션은 Solaris Security Toolkit 소프트웨어가 화면에 출력을 표시하지 않게 합니다. 이 옵션은 `JASS_REPOSITORY` 디렉토리에 보존되는 로그에는 아무 영향도 주지 않습니다. `-o` 옵션과 비슷하게, 이 옵션은 특히 `cron` 작업을 통하거나 느린 네트워크 연결을 통해 Solaris Security Toolkit을 실행할 때 도움이 됩니다.

전자 우편 통지 옵션

`-m` 전자우편_주소 옵션은 Solaris Security Toolkit 소프트웨어에 완료된 작업의 사본을 지정된 전자 우편 주소로 보내도록 지시합니다. 전자 우편 보고서는 다른 옵션을 사용하여 시스템에 생성되는 모든 로그에 추가로 작성됩니다.

시스템 변경 실행 취소

때로는 하나 또는 복수의 Solaris Security Toolkit 강화 작업 중에 작성된 변경사항을 취소해야 합니다. 강화 작업 중에 작성된 변경이 시스템에 부정적인 영향을 주는 경우 변경사항을 실행 취소 하십시오.

예를 들어 강화 작업 후 SVM(Solaris Volume Manager)과 같은 필수 서비스가 사용 불가능함을 발견하는 경우 다음을 수행하십시오.

1. 강화 작업을 실행 취소합니다.
2. 사용자 정의된 드라이버를 생성합니다.
드라이버 사용자 정의에 대한 자세한 내용은 Solaris Security Toolkit 4.2 Reference Manual 4장 "드라이버 사용자 정의"를 참조하십시오.
3. JASS_SVCS_ENABLE 환경 변수를 통해 사용할 SVM 서비스를 활성화합니다.
JASS_SVCS_ENABLE을 사용하는 방법은 Solaris Security Toolkit 4.2 Reference Manual 7장 "JASS_SVCS_ENABLE"을 참조하십시오.
4. 강화 작업을 반복합니다.

이 절은 하나 또는 복수 강화 작업 중에 작성된 변경을 취소하기 위한 지시를 제공합니다. 강화 작업을 효과적으로 취소하기 위한 한계 및 요구사항이 있음을 주의하십시오. 64페이지에 "시스템 변경 실행 취소 요구사항"을 참조하십시오.

▼ Solaris Security Toolkit 작업 실행 취소

1. 시스템을 백업하고 재부팅합니다.
시스템이 알려지고 작동 중인 상태로 되돌아가거나 되돌아갈 수 있도록 각 실행 취소 작업 전에 시스템을 백업하고 재부팅하십시오.
2. `jass-execute -u` 명령과 함께 사용하려는 옵션을 판별합니다.
67페이지에 "실행 취소 기능에서 옵션 사용"을 참조하십시오.
다음 지시는 `jass-execute -u` 명령을 사용 중이라고 가정합니다.

3. 표준 `-u` 옵션을 사용하여 하나 이상의 강화 작업을 실행 취소 하려면 `JASS_HOME_DIR/bin`에서 다음 명령을 입력하십시오.

```
# ./jass-execute -u
```

Solaris Security Toolkit 소프트웨어는 `JASS_REPOSITORY`에 있는 모든 목록 파일을 찾아서 각 강화 작업에 대한 정보를 수집합니다. 목록 파일이 비어 있거나 존재하지 않는 경우 실행 취소 할 변경이 없고 작업이 생략되었다고 가정합니다. 또한 `jass-undo-log.txt`라는 파일이 목록 파일과 동일한 디렉토리에 존재하는 경우 작업이 이미 취소 되었으므로 해당 작업이 생략되었다고 가정합니다. 수집 프로세스가 완료된 후 그 결과가 표시됩니다. 다음은 출력의 예입니다.

코드 예 4-2 실행 취소할 수 있는 작업의 예제 출력

```
# ./jass-execute -u
[NOTE] Executing driver, undo.driver
Please select a JASS run to restore through:
1. January 24, 2003 at 13:57:27
   (/var/opt/SUNWjass/run/20030124135727)
2. January 24, 2003 at 13:44:18
   (/var/opt/SUNWjass/run/20030124134418)
3. January 24, 2003 at 13:42:45
   (/var/opt/SUNWjass/run/20030124134245)
4. January 24, 2003 at 12:57:30
   (/var/opt/SUNWjass/run/20030124125730)

Choice? ('q' to exit)?
```

이 예제에서 4개의 개별 강화 작업이 발견됩니다. 이들 작업이 시스템에 변경을 작성했고 실행 취소되지 않았습니다. 강화 작업의 목록은 항상 연대기 역순으로 표시됩니다. 목록의 첫 번째 항목은 가장 최근의 강화 작업입니다.

4. 출력을 검토하여 실행 취소하려는 작업을 판별한 후 대응하는 번호를 입력합니다.

임의의 선택된 항목에 대해 Solaris Security Toolkit 소프트웨어는 선택된 값보다 작거나 같은 색인 번호를 갖는 각 작업을 취소합니다. 즉, 실행 취소 작업이 가장 최근의 강화 작업으로 시작하여 사용자가 선택한 작업까지 계속해서 변경이 원래 작성된 역순으

로 변경사항을 실행 취소 합니다. 앞의 예제를 지침으로 사용하여 작업 3을 선택하는 경우 실행 취소 작업은 먼저 작업 1에 대한 변경을 취소한 후 작업 2에 대한 변경을 취소하려 이동하고 작업 3에 대한 변경을 취소하여 종료합니다.

코드 예 4-3은 실행 취소 작업이 두 개의 목록 파일 항목을 처리할 때 생성되는 출력을 보여줍니다.

코드 예 4-3 복수 목록 파일 항목을 처리하는 실행 취소 작업의 예제 출력

```
[...]  
  
=====undo.driver: Performing UNDO of  
//var/opt/SUNWjass/run/20050715145837.  
=====br/>  
[...]  
  
=====undo.driver: Undoing Finish Script: update-cron-allow.fin  
=====br/>  
[NOTE] Undoing operation COPY.  
cp -p /etc/cron.d/cron.allow.JASS.20050715145906  
/etc/cron.d/cron.allow  
rm -f /etc/cron.d/cron.allow.JASS.20050715145906  
  
[NOTE] Removing a Solaris Security Toolkit-created file.  
rm -f /etc/cron.d/cron.allow  
  
[...]
```

이 예제에서 Solaris Security Toolkit 소프트웨어는 복사 조작을 실행 취소하고 강화 작업 중에 추가된 파일을 제거합니다. 실행 취소 작업의 출력은 시스템을 복원하기 위한 실제 명령을 문서화하므로, 시스템 구성의 문제를 해결해야 할 경우 프로세스를 명확히 이해하고 참조할 수 있습니다.

Solaris Security Toolkit이 마지막 강화 작업을 수행한 이후에 수정된 파일의 확인을 성공적으로 완료하면, 실행 취소 작업은 모든 작업 및 해당 목록 파일이 처리되고 변경이 취소될 때까지 계속됩니다.

JASS_REPOSITORY에 위치한 모든 목록 파일을 찾아서 각 강화 작업에 대한 정보를 수집하는 Solaris Security Toolkit 소프트웨어 외에, Solaris Security Toolkit 소프트웨어는 다음을 수행합니다.

- a. 수정된 각 파일의 체크섬을 비교합니다.
- b. 체크섬 파일의 불일치에 대한 알림을 생성 및 기록합니다.
- c. 이 파일에 어떤 조치를 취할지 묻습니다.

5. 실행 취소 작업이 예외(강화 작업 후 변경된 파일)를 발견하는 경우 옵션 중 하나를 입력합니다.

참고 – Solaris Security Toolkit 소프트웨어는 특정 예외 파일에 대해 선택한 백업, 보존 및 강제 옵션을 기억하므로 파일이 실행 취소 작업의 예외가 되는 다음 번에는 해당 파일에 대해 또다시 옵션을 선택할 필요가 없습니다.

다음은 예외 및 예외 처리용 선택사항을 보여주는 예제 출력입니다.

코드 예 4-4 실행 취소 예외의 예제 출력

```
[...]

=====
undo.driver: Undoing Finish Script: enable-process-accounting.fin
=====

[NOTE] Undoing operation COPY.
[WARN] Checksum of current file does not match the saved value.
[WARN] filename = /var/spool/cron/crontabs/adm
[WARN] current = db27341e3e1f0f27d371d2e13e6f47ce
[WARN] saved = a7f95face84325cddc23ec66d59374b0

Select your course of action:
1. Backup - Save the current file, BEFORE restoring original.
2. Keep - Keep the current file, making NO changes.
3. Force - Ignore manual changes, and OVERWRITE current file.

NOTE: The following additional options are applied to this and ALL
subsequent files:
4. ALWAYS Backup.
5. ALWAYS Keep.
6. ALWAYS Force.

Enter 1, 2, 3, 4, 5, or 6:
```

이 예제에서 항목 1을 선택하는 경우 다음 출력이 표시됩니다.

코드 예 4-5 실행 취소 중 백업 옵션 선택의 예제 출력

```
Enter 1, 2, 3, 4, 5, or 6: 1

[WARN] Creating backup copies of some files may cause unintended
effects.
[WARN] This is particularly true of /etc/hostname.[interface]
files as well as crontab files in /var/spool/cron/crontabs.

[NOTE] BACKUP specified, creating backup copy of
```

코드 예 4-5 실행 취소 중 백업 옵션 선택의 예제 출력 (계속)

```
/var/spool/cron/crontabs/adm.  
[NOTE] File to be backed up is from an undo operation.  
[NOTE] Copying /var/spool/cron/crontabs/adm to  
/var/spool/cron/crontabs/adm.BACKUP.JASS.20050715151817  
cp -p /var/spool/cron/crontabs.JASS/adm.JASS.20050715151719  
/var/spool/cron/crontabs/adm  
rm -f /var/spool/cron/crontabs.JASS/adm.JASS.20050715151719  
  
[NOTE] Undoing operation COPY.  
cp -p /var/spool/cron/crontabs.JASS/root.JASS.20050715151717  
/var/spool/cron/crontabs/root  
rm -f /var/spool/cron/crontabs.JASS/root.JASS.20050715151717  
  
[NOTE] Undoing operation MAKE DIRECTORY.  
rmdir /var/spool/cron/crontabs.JASS  
  
[NOTE] Undoing operation SYMBOLIC LINK.  
rm -f /etc/rc3.d/S22acct  
  
[NOTE] Undoing operation SYMBOLIC LINK.  
rm -f /etc/rc0.d/K22acct
```

항목 4를 선택하는 경우 다음 출력이 표시됩니다.

코드 예 4-6 실행 취소 중 항상 백업 옵션 선택의 예제 출력

```
Enter 1, 2, 3, 4, 5, or 6: 4
[NOTE] Always do BACKUP selected.  Overriding JASS_UNDO_TYPE with
BACKUP.

[WARN] Creating backup copies of some files may cause unintended
effects.
[WARN] This is particularly true of /etc/hostname.[interface]
files as well as crontab files in /var/spool/cron/crontabs.

[NOTE] BACKUP specified, creating backup copy of
/var/spool/cron/crontabs/adm.
[NOTE] File to be backed up is from an undo operation.
[NOTE] Copying /var/spool/cron/crontabs/adm to
/var/spool/cron/crontabs/adm.BACKUP.JASS.20050715152126
cp -p /var/spool/cron/crontabs.JASS/adm.JASS.20050715151953
/var/spool/cron/crontabs/adm
rm -f /var/spool/cron/crontabs.JASS/adm.JASS.20050715151953

[NOTE] Undoing operation COPY.
[WARN] Checksum of current file does not match the saved value.
[WARN]     filename = /var/spool/cron/crontabs/root
[WARN]     current  = 741af21a62ea7a9e7abe6ba04855aa76
[WARN]     saved   = bcf180f45c65ceff3bf61012cb2b4982
[WARN] Creating backup copies of some files may cause unintended
effects.
[WARN] This is particularly true of /etc/hostname.[interface]
files as well as crontab files in /var/spool/cron/crontabs.
[NOTE] BACKUP specified, creating backup copy of
/var/spool/cron/crontabs/root.
[NOTE] File to be backed up is from an undo operation.
[NOTE] Copying /var/spool/cron/crontabs/root to
/var/spool/cron/crontabs/root.BACKUP.JASS.20050715152127
cp -p /var/spool/cron/crontabs.JASS/root.JASS.20050715151951
/var/spool/cron/crontabs/root
rm -f /var/spool/cron/crontabs.JASS/root.JASS.20050715151951

[NOTE] Undoing operation MAKE DIRECTORY.
rmdir /var/spool/cron/crontabs.JASS

[NOTE] Undoing operation SYMBOLIC LINK.
rm -f /etc/rc3.d/S22acct

[NOTE] Undoing operation SYMBOLIC LINK.
rm -f /etc/rc0.d/K22acct
```

Solaris Security Toolkit이 선택한 실행 취소 작업을 완료하면, 강화로 인해 변경된 것으로 플래그된 해당 파일을 검토하고 필요한 시스템 수정을 수행해야 합니다. 이 변경 사항이 시스템을 일치하지 않는 상태로 남겨두었다고 수동으로 검토될 때 까지 시스템을 재부팅하지 마십시오.

참고 - 이 예제에서 수정된 파일은 다음의 새 이름으로 저장됩니다.
/etc/.login.BACKUP.JASS.20050715151817. 실행 취소 작업이 완료된 후 해당 파일을 /etc/.login에 비교하여 추가 조정이 필요한지 판별하십시오.

6. 계속하기 전에 모든 예외를 조정합니다.
7. 모든 예외를 조정한 후 시스템을 재부팅합니다.
시스템을 재부팅해야만 Solaris OS 구성에 변경한 사항이 적용됩니다.



주의 - JumpStart 모드에서 Solaris Security Toolkit을 실행하면 root 암호를 설정합니다. 실행 취소 작업이 나중에 수행되는 경우, root 암호는 이전의 설정(암호 없음)으로 복귀합니다. 이는 누구나 암호를 입력하지 않고 root 계정으로 로그인할 수 있음을 의미합니다. 실행 취소 작업을 실행한 후에는 passwd(1) 명령으로 root 암호를 재설정하십시오. 또한 Solaris Security Toolkit 4.2 소프트웨어는 시스템이 이러한 상태에 있을 때 경고 메시지를 표시합니다.

JumpStart 서버 구성 및 관리

이 장은 Solaris Security Toolkit 소프트웨어를 사용하기 위한 JumpStart 서버 구성 및 관리 정보를 제공합니다. Sun의 네트워크 기반 Solaris OS 설치 체계인 JumpStart 기술은 설치 프로세스 중에 Solaris Security Toolkit 소프트웨어를 실행할 수 있습니다.

Solaris Security Toolkit의 JumpStart 모드는 버전 2.1 이후의 Solaris OS 제품에 사용 가능한 JumpStart 기술을 기초로 합니다. JumpStart 기술은 Solaris OS 및 시스템 소프트웨어 설치, 시스템의 정확성 및 표준화 촉진을 완전히 자동화하여 복잡성을 관리하는데 도움을 줍니다. 시스템을 빨리 설치 및 전개하는 요구사항을 충족시키는 방법을 제공합니다.

JumpStart 기술 사용의 장점은 시스템 보안 영역에서 두드러집니다. Solaris Security Toolkit 소프트웨어에 JumpStart 기술을 사용하여 자동화된 Solaris OS 설치시 시스템을 보안할 수 있습니다. 이 기술은 시스템 설치시 시스템 보안이 표준화되고 주소화되도록 도와줍니다. Solaris Security Toolkit의 강화를 지원하는 모듈을 포함하고 JumpStart 기반 설치를 도와주는 JumpStart Enterprise Toolkit(JET)을 구하려면 다음의 Sun Software Download 사이트를 방문하십시오.

<http://www.sun.com/download/>

JumpStart 기술에 대한 자세한 정보는 Sun BluePrints 설명서 *JumpStart Technology: Effective Use in the Solaris Operating Environment*를 참조하십시오.

이 장에서는 다음 주제를 다룹니다.

- 78페이지에 "JumpStart 서버 및 환경 구성"
- 80페이지에 "JumpStart 프로파일 템플릿 사용"
- 82페이지에 "클라이언트 추가 및 제거"

JumpStart 서버 및 환경 구성

JumpStart 환경에서 사용하기 위해, /opt/SUNWjass(pkg 다운로드용)의 Solaris Security Toolkit 소스를 JumpStart 서버의 기본 디렉토리에 설치합니다. 기본 디렉토리는 JumpStart 서버의 /jumpstart입니다. 이 작업이 완료된 후 JASS_HOME_DIR이 JumpStart 서버의 기본 디렉토리가 됩니다.

이 절에서는 사용자가 JumpStart 기술에 익숙하고 기존 JumpStart 환경을 사용할 수 있다고 가정합니다.

Solaris Security Toolkit 소프트웨어를 JumpStart 구조에 통합하기 위해서는 몇 개의 단계만 필요합니다.

▼ JumpStart 모드 구성

1. JumpStart 서버의 루트 디렉토리에 Solaris Security Toolkit 소스를 설치합니다.

다음 예와 같이, Solaris Security Toolkit은 JASS_REPOSITORY(이 경우에는 /jumpstart)에 설치될 수 있습니다.

```
# pwd
/opt/SUNWjass
# pkgadd -R /jumpstart -d . SUNWjass
```

일반적으로 Solaris Security Toolkit 소프트웨어는 보통은 JASS_HOME_DIR이기도 한 JumpStart 서버의 SI_CONFIG_DIR에 설치됩니다.

2. Solaris 2.5.1 OS sysidcfg 파일을 수정하는 경우 해당 수정사항을 JASS_HOME_DIR/Sysidcfg/Solaris_2.5.1 디렉토리의 하나로 만듭니다.
Solaris 2.5.1 OS를 사용 중인 경우, JASS_HOME_DIR/Sysidcfg/Solaris_2.5.1의 sysidcfg 파일은 직접 사용할 수 없습니다. 이 Solaris 버전은 SI_CONFIG_DIR에 있고 별도의 하위 디렉토리에 있지 않은 sysidcfg 파일만 지원하기 때문입니다. Solaris 2.5.1 OS에서 이 제한을 다루기 위해 Solaris Security Toolkit 소프트웨어에는 SI_CONFIG_DIR/sysidcfg이 있으며, 이것은 JASS_HOME_DIR/Sysidcfg/Solaris_2.5.1/sysidcfg 파일에 링크됩니다.
3. 다음 명령으로 JASS_HOME_DIR/Drivers/user.init.SAMPLE를 JASS_HOME_DIR/Drivers/user.init로 복사합니다.

```
# pwd
/jumpstart/opt/SUNWjass/Drivers
# cp user.init.SAMPLE user.init
```

4. **JumpStart** 설치 시 대상 시스템에 **Solaris Security Toolkit** 패키지를 설치하려는 경우, `user.init` 파일에 정의된 `JASS_PACKAGE_MOUNT` 디렉토리에 해당 패키지를 저장해야 합니다. 예:

```
# cp /해당경로//SUNWjass.pkg JASS_HOME_DIR/Packages
```

5. 멀티홈 **JumpStart** 서버에 문제점이 있는 경우 `JASS_PACKAGE_MOUNT` 및 `JASS_PATCH_MOUNT`에 대한 두 항목을 `JASS_HOME_DIR/Patches` 및 `JASS_HOME_DIR/Packages` 디렉토리에 대한 올바른 경로로 수정합니다.
6. `SI_CONFIG_DIR/path/to/JASS` 같이 `SI_CONFIG_DIR`의 하위 디렉토리에 **Solaris Security Toolkit** 소프트웨어를 설치하려는 경우 `user.init` 파일에 다음을 추가합니다.

```
if [ -z "${JASS_HOME_DIR}" ]; then
    if [ "${JASS_STANDALONE}" = 0 ]; then
        JASS_HOME_DIR="${SI_CONFIG_DIR}/path/to/JASS"
    fi
fi
export JASS_HOME_DIR
```

7. **Solaris Security Toolkit** 드라이버(예: 기본 `secure.driver`)를 선택하거나 작성합니다.
- `hardening.driver` 및 `config.driver`에 나열되는 모든 스크립트가 사용되어야 하는 경우 `Drivers/secure.driver` 경로를 `rules` 파일에 추가하십시오.
 - 선택된 스크립트만이 사용될 경우 해당 파일을 복사한 후 사본을 수정하십시오. 드라이버 복사 및 수정에 대한 자세한 내용은 **Solaris Security Toolkit 4.2 Reference Manual** 4장 "드라이버 사용자 정의"를 참조하십시오.



주의 – Solaris Security Toolkit 소프트웨어에 포함된 원본 스크립트를 절대 수정하지 마십시오. Solaris Security Toolkit 소프트웨어의 새 릴리스로의 효율적인 마이그레이션을 허용하기 위해 원본 파일과 사용자 정의 파일을 개별적으로 유지하십시오.

8. 드라이버를 완료한 후 `rules` 파일에 올바른 항목을 작성합니다.
항목은 다음과 비슷해야 합니다.

```
hostname imbulu - Profiles/core.profile Drivers/secure-abc.driver
```

Solaris Security Toolkit 소프트웨어를 성공적으로 기존 **JumpStart** 환경에 통합하기 위해 또 다른 수정이 필요할 수 있습니다.

9. Solaris Security Toolkit 소프트웨어와 함께 제공되는 `sysidcfg` 파일을 사용하여 **JumpStart** 클라이언트 설치를 자동화하려는 경우 적용 가능한지 검토합니다.

JumpStart 서버에서 `sysidcfg` 파일을 구문 분석하는 중에 오류가 발생하는 경우 파일의 전체 내용이 무시됩니다.

이 절에 있는 모든 구성 단계를 완료한 후 JumpStart 기술을 사용하여 클라이언트에 Solaris OS를 설치하고 설치 프로세스 중에 OS를 강화하거나 최소화할 수 있습니다.

JumpStart 프로파일 템플릿 사용

JumpStart 프로파일 템플릿은 JumpStart 모드에서만 사용되는 파일입니다. 프로파일의 필수 및 선택적 내용은 Sun BluePrints 설명서 *JumpStart Technology: Effective Use in the Solaris Operating Environment*를 참조하십시오.

JumpStart 프로파일 템플릿을 개별 사이트 수정을 수행하는 예제로 사용하십시오. 프로파일을 검토하여 사용자 환경에서 사용해야 하는 변경 사항(있는 경우)을 판별하십시오.

프로파일의 사본을 작성한 후 사이트에 맞게 수정하십시오. Solaris Security Toolkit 소프트웨어에 대한 업데이트가 사용자 정의를 겹쳐 쓸 수 있으므로 원본을 수정하지 마십시오.

다음 JumpStart 프로파일이 Solaris Security Toolkit 소프트웨어에 포함되어 있습니다.

- `core.profile`
- `end-user.profile`
- `developer.profile`
- `entire-distribution.profile`
- `oem.profile`
- `minimal-SunFire_Domain*.profile`

다음 하위 절은 이러한 프로파일에 대해 설명합니다.

`core.profile`

이 JumpStart 프로파일은 가장 작은 Solaris OS 클러스터인 SUNWCreq를 설치합니다. 디스크의 분할이 루트 및 스왑 파티션을 포함하도록 지정하는 것 외에 다른 구성 수정은 하지 않습니다.

end-user.profile

이 JumpStart 프로파일은 End User Solaris OS 클러스터인 SUNWCuser 및 프로세스 회계가 제대로 작동하기 위해 필요한 두 개의 Solaris OS 패키지를 설치합니다. 또한 루트 및 스왑 파티션만 포함하도록 디스크 분할이 정의됩니다.

developer.profile

이 JumpStart 프로파일은 Developer Solaris OS 클러스터 SUNWCprog 및 프로세스 회계가 제대로 작동하기 위해 필요한 두 개의 Solaris OS 패키지를 설치합니다. core.profile 정의에서와 같이 Solaris OS 클러스터 외에 작성된 유일한 다른 구성 정의는 디스크 분할이 루트 및 스왑을 포함하는 것입니다.

entire-distribution.profile

이 JumpStart 프로파일은 Entire Distribution Solaris OS 클러스터 SUNWCa11을 설치합니다. 다른 프로파일에서와 같이 루트 및 스왑 파티션을 포함하도록 디스크 분할이 정의됩니다.

oem.profile

이 JumpStart 프로파일은 OEM Solaris OS 클러스터 SUNWCXa11을 설치합니다. 이 클러스터는 Entire Distribution 클러스터의 슈퍼세트이며 OEM으로 제공되는 소프트웨어를 설치합니다.

minimal-SunFire_Domain*.profile

주 - 이 프로파일은 Solaris OS 8 및 9 버전을 실행하는 시스템에서만 사용하십시오.

아래의 모든 프로파일은 Sun BluePrints OnLine 기사 [Minimizing Domains for Sun Fire V1280, 12K, and 15K Systems](#)를 기초로 합니다. 다음 JumpStart 프로파일은 이 기사의 참조 내용과 동일합니다.

- minimal-SunFire_Domain-Apps-Solaris8.profile
- minimal-SunFire_Domain-Apps-Solaris9.profile
- minimal-SunFire_Domain-NoX-Solaris8.profile
- minimal-SunFire_Domain-NoX-Solaris9.profile
- minimal-SunFire_Domain-X-Solaris8.profile

클라이언트 추가 및 제거

add-client 및 rm-client 스크립트가 서버를 구성할 때 사용되며 서버는 JumpStart 소프트웨어를 사용하여 클라이언트의 네트워크 기반 설치를 수행할 수 있습니다. 해당 스크립트는 JASS_HOME_DIR/bin 디렉토리에 저장되어 있습니다. JumpStart 모드는 JumpStart 서버의 rules 파일에 삽입된 Solaris Security Toolkit 드라이버에 의해 제어됩니다.

JumpStart 모드를 사용하도록 환경을 구성하지 않은 경우 78페이지에 "JumpStart 서버 및 환경 구성"을 참조하십시오.

SPARC 기반 시스템의 경우, add-client 명령이 Solaris Security Toolkit에 필요한 JumpStart 클라이언트 및 구성 정보를 설치합니다. 해당 명령은 JumpStart 서버로부터 실행됩니다.

DHCP(동적 호스트 구성 프로토콜)클라이언트가 필요한 x86/x64 시스템의 경우, Solaris (Install) Media에 제공되는 add_install_client를 사용해야 합니다.

add-client 스크립트

JumpStart 서버로부터 클라이언트 추가를 단순화하려면 Solaris Security Toolkit 소프트웨어에 포함되어 있는 이 스크립트를 사용하십시오. 명령과 옵션은 다음 문단에 설명되어 있지만 기초 JumpStart 기술은 설명되지 않습니다. Sun BluePrints 설명서 JumpStart Technology: Effective Use in the Solaris Operating Environment를 참조하십시오.

add-client 스크립트는 add_install_client 명령 주위의 랩퍼이며 다음 인수를 승인합니다.

다음은 add-client 명령의 개요입니다.

```
# add-client -c 클라이언트 -i 서버 -m 클라이언트-클래스 -o 클라이언트-OS  
-s sysidcfg
```

표 5-1은 add-client 명령에 대한 올바른 입력을 설명합니다.

표 5-1 JumpStart add-client 명령

옵션	설명
-c 클라이언트	JumpStart 클라이언트의 해석 가능한 호스트 이름.
-h -?	사용 정보 표시 다른 옵션 없이 사용합니다. 모든 추가 옵션은 무시됩니다.
-i 서버	이 JumpStart 클라이언트에 대한 JumpStart 서버 인터페이스의 IP 주소 또는 해석 가능한 호스트 이름. 값을 지정하지 않으면 로컬 호스트에서 사용할 수 있는 인터페이스 목록이 표시됩니다.
-m 클라이언트-클래스	JumpStart 클라이언트의 기계 클래스. 이 값은 uname -m 명령의 출력과 동일한 형식으로 되어 있습니다.
-o 클라이언트-OS	JASS_HOME_DIR/OS 디렉토리에서 사용 가능하며 클라이언트에 설치될 Solaris OS의 버전 값을 지정하지 않으면 JASS_HOME_DIR/OS 디렉토리의 사용 가능한 Solaris OS 버전 목록이 표시됩니다.
-s sysidcfg	시스템 식별 및 구성에 사용하려는 sysidcfg 파일이 들어있는 대체 디렉토리에 대한 선택적 경로 이름. 기본적으로, 이 값은 JASS_HOME_DIR/Sysidcfg/Solaris_버전/ 디렉토리에 설정되어 있습니다. Solaris-버전은 사용했던 필수 -o 인수로부터 추출됩니다. 선택적인 경로 이름을 지정하는 경우, JASS_HOME_DIR 디렉토리와 관련된 경로 이름을 사용합니다. sysidcfg 파일에 대한 경로만 지정하십시오.
-V	이 프로그램의 버전 정보 모든 추가 옵션은 무시됩니다.

기본 값을 사용하여 eng1이라는 JumpStart 클라이언트를 추가하려면 다음을 수행하십시오.

```
# /opt/SUNWjass/bin/add-client -c eng1 -m sun4u
Selecting default operating system, Solaris_ver.
Selecting default system interface, IP_address.
cleaning up preexisting install client "eng1"
removing eng1 from bootparams
updating /etc/bootparams
```

Solaris 9 OS(12/03) 및 -s sysidcfg 옵션을 사용하여 eng1이라는 JumpStart 클라이언트를 jumpserve1이라는 JumpStart 서버에 추가하려면, 다음을 수행하십시오.

```
# /opt/SUNWjass/bin/add-client -c eng1 -i jumpserve1 -m sun4u -o Solaris_9_2003-12 -s Hosts/alpha
cleaning up preexisting install client "eng1"
removing eng1 from bootparams
updating /etc/bootparams
```

rm-client 스크립트

JumpStart 서버로부터 클라이언트 제거를 단순화하려면 Solaris Security Toolkit 소프트웨어에 포함되어 있는 이 스크립트를 사용하십시오. 명령과 옵션은 다음 문단에 설명되어 있지만 기초 JumpStart 기술은 설명되지 않습니다. JumpStart 기술에 대한 정보는 *JumpStart Technology: Effective Use in the Solaris Operating Environment* 를 참조하십시오.

rm-client 스크립트는 add-client와 동일한 rm_install_client 명령 주위의 래퍼입니다.

사용 예제: **rm-client** [-c] 클라이언트

여기서 클라이언트는 JumpStart 클라이언트의 해석 가능한 호스트 이름입니다.

표 5-2는 rm-client 명령에 대한 올바른 입력을 설명합니다.

표 5-2 JumpStart rm-client 명령

옵션	설명
-c 클라이언트	JumpStart 클라이언트의 해석 가능한 호스트 이름.
-h -?	사용 정보 표시 다른 옵션 없이 사용합니다. 모든 추가 옵션은 무시됩니다.
-v	이 프로그램의 버전 정보 모든 추가 옵션은 무시됩니다.

eng1이라는 JumpStart 클라이언트를 제거하려면 다음 rm-client 명령을 사용하십시오.

```
# ./rm-client -c eng1  
removing eng1 from bootparams
```

시스템 보안 감사

이 장은 Solaris Security Toolkit 소프트웨어를 사용하여 시스템의 보안을 감사(검증)하는 방법에 대해 설명합니다. 강화 후에 설정된 보안 프로파일 유지보수에 대해서는 이 장의 정보와 절차를 사용하십시오. 이미 전개된 시스템의 경우 이 장에 있는 정보를 사용하여 강화하기 전에 보안을 평가할 수 있습니다.

참고 - 감사라는 용어는 이 장과 설명서에서 보안 상태를 사전 정의된 보안 프로파일과 비교하여 보안 상태를 검증하는 Solaris Security Toolkit 소프트웨어의 자동화된 프로세스를 정의하는 데 사용됩니다. 그러나, 이 용어의 사용이 감사 옵션 사용후 시스템이 완벽하게 안전함을 보장하는 것은 아닙니다.

이 장에서는 다음 주제를 다룹니다.

- 85페이지에 "보안 유지"
 - 86페이지에 "강화하기 전 시스템 검토"
 - 86페이지에 "보안 감사 사용자 정의"
 - 87페이지에 "보안 감사 준비"
 - 88페이지에 "옵션 사용 및 감사 출력 제어"
 - 96페이지에 "보안 감사 수행"
-

보안 유지

보안 유지는 주기적으로 검토하고 확인해야 하는 진행 중 프로세스입니다. 시스템에 대한 기본 보안 구성이 시간이 지남에 따라 점차 열리기 때문에 보안 시스템 유지보수는 경계가 필요합니다. (보안 유지에 대한 자세한 정보는 32페이지에 "시스템 보안 유지보수"를 참조하십시오.)

Solaris Security Toolkit은 특정 보안 프로파일로 준수 레벨을 결정하여 시스템의 보안 상태를 감사하는 자동화된 방법을 제공합니다.

참고 - 이 방법은 `jass-execute -a` 명령을 사용하여 독립형 모드에서만 사용할 수 있으며 JumpStart 설치 중에는 사용할 수 없습니다.

수동 또는 자동으로(예를 들어 `a cron` 작업이나 `rc` 스크립트를 통해) 주기적으로 시스템의 보안 상태를 감사하십시오. 예를 들어 새로운 설치를 강화한 후 5일 후에 Solaris Security Toolkit 소프트웨어 감사 명령(`jass-execute -a` 드라이버이름)을 실행하여 시스템 보안이 보안 프로파일에 의해 정의된 상태에서 변경되었는지 판별하십시오.

보안을 감사하는 빈도는 환경의 중요성과 보안 방침에 따라 달라집니다. 일부 사용자는 매 시간마다, 매일 또는 1개월에 한 번만 감사를 실행합니다. 일부 사용자는 매 시간마다 소형 스캔(제한된 수의 검사)을 실행하고 하루에 한 번 전체 스캔(가능한 모든 검사 사용)을 실행합니다. 규칙적으로 실행되는 감사 및 시스템 재부팅 후에는 반드시 사용자의 보안 상태를 점검해야 합니다.

필수 구성요소를 감사하여 전개된 시스템의 보안 상태를 유지하십시오. 보안 상태를 주기적으로 감사하지 않는 경우 원하는 보안 상태를 모르거나 또는 악의적으로 변경하는 엔트로피 또는 수정으로 인해 구성이 종종 시간에 따라서 변화합니다. 주기적 검토가 없으면 이들 변경은 검출되지 않고 수정되지 않습니다. 결과적으로 시스템은 덜 안정적이고 더 취약하게 됩니다.

주기적 감사 외에, 업그레이드, 패치 설치 및 기타 중요한 시스템 구성 변경 후에 감사를 수행하십시오.

강화하기 전 시스템 검토

경우에 따라, 전개된 시스템을 강화하기 전에 해당 시스템의 보안 상태를 검토하는 것이 유용함을 알 수 있습니다. 예를 들어 다른 사람이 관리한 전개된 시스템에 대한 책임을 지는 경우 시스템 상태를 파악하고 필요한 경우 다른 시스템에서 사용되는 동일한 보안 프로파일을 준수하게 만들 수 있도록 시스템의 상태를 조사하십시오.

보안 감사 사용자 정의

감사 옵션은 시스템 상태 평가를 위한 높은 융통성과 확장성을 갖는 체계를 제공합니다. 강화 스크립트에서와 같이 감사 스크립트의 조치를 사용자 정의할 수 있습니다. 예를 들어 환경 변수를 사용자 정의하고 프레임워크와 지원 프로그램 기능을 사용자 정의하고 새로운 점검을 추가하고 감사 프레임워크에 기능을 추가할 수 있습니다.

대체로 표준 및 제품 특정 감사 스크립트는 해당 환경에 대한 감사를 사용자 정의할 템플릿으로 적합합니다. 이 시나리오의 경우 드라이버, 종료 스크립트, 환경 변수 및 파일 템플릿을 통해 감사 스크립트 조치를 사용자 정의하십시오. 이러한 사용자 정의 변경은 아주 간단하며 코드를 수정하지 않고도 가능합니다. 강화를 위해 수행하는 모든 변경 사항은 사용자가 감사를 수행할 때 Solaris Security Toolkit 소프트웨어에 의해 자동으로 알려집니다.

일부 사용자는 완전히 새로운 독점적 또는 사이트에 고유한 드라이버와 스크립트를 작성해야 합니다. 새로운 드라이버 및 스크립트를 코드화할 때 템플릿과 예제를 지침으로 사용하십시오. 감사 옵션을 사용할 때 사이트 특정 드라이버, 종료 스크립트, 변수 및 기능이 Solaris Security Toolkit 소프트웨어에 자동으로 알려지지 않음을 주의하십시오. 예를 들어 사이트에 고유한 종료 스크립트인 `abcc-nj-install-foo.fin`이 들어있는 `abcc-nj-secure.driver`라는 사이트 특정 드라이버를 추가하는 경우 사이트 특정 감사 스크립트 `abcc-nj-install-foo.aud`를 작성해야 합니다. 이와 유사하게 감사 스크립트만으로 시작하는 경우 대응하는 종료 스크립트를 작성해야 합니다.

때때로 Solaris Security Toolkit 소프트웨어가 제공하지 않은 검사나 기능을 추가할 필요가 있을 수도 있습니다. 이 시나리오의 경우 감사 스크립트에 검사나 새 기능을 추가하십시오. (대응하는 종료 스크립트에서 관련된 변경을 수행할 수도 있습니다.) `user.run` 파일을 통해 코드 추가 및 수정을 수행할 때 버그 및 실패가 발생하지 않도록 주의하십시오.

새로운 드라이버, 스크립트, 변수 및 기능을 사용자 정의하거나 작성하려면 Solaris Security Toolkit 4.2 Reference Manual을 참조하십시오.

예를 들어 Solaris Security Toolkit 소프트웨어가 설치하지 않은 패치를 추가할 필요가 있을 수 있습니다. 표준 또는 제품 특정 템플릿 중 하나를 확장하거나 고유한 것을 작성할 수 있습니다. 고유 템플릿을 작성하는 경우, 종료 스크립트를 작성하여 패치를 추가한 후 그에 대응하는 감사 스크립트를 작성하여 패치 설치를 점검합니다. 기존의 종료 (.fin) 및 감사(.aud) 스크립트를 템플릿으로 사용할 경우에는 이 두 가지 스크립트를 고유한 이름을 갖는 새 파일에 복사해야 합니다.

보안 감사 준비

이 장의 지시 및 지침을 사용하려면 보안 프로파일이 필요합니다. 보안 프로파일 개발 및 구현에 대한 정보는 2 장을 참조하십시오.

다양한 보안 프로파일이 Solaris Security Toolkit 배포판에 드라이버로 포함되어 있습니다. 이 설명서의 앞에서 언급한 것처럼 기본 보안 프로파일 및 해당 드라이버로 작성된 변경이 사용자 시스템에 적합하지 않을 수 있습니다. 일반적으로 구현되는 보안 프로파일은 보안을 위한 “최고 수위선”입니다. 이는 불필요한 서비스를 비활성화 하고 `secure.driver`에 의해 비활성화된 선택적 보안 기능을 활성화 함을 의미합니다.

많은 Solaris Security Toolkit 소프트웨어 사용자는 표준 및 제품 특정 보안 프로파일이 해당 환경에 적용할 수 있음을 발견합니다. 이 경우에 해당하는 경우 어떤 보안 프로파일이 사용자가 원하는 보안 상태에 가장 가까운지를 판별하고 시스템 평가 및 강화에 사용하십시오.

사용자 환경에 대해 보안 프로파일 템플릿을 검토 및 사용자 정의하거나 새로 개발하십시오. 보안 프로파일 사용자 정의에 대한 방법과 지침은 Solaris Security Toolkit 4.2 Reference Manual에 포함되어 있습니다. 이 접근법은 사용자 조직에 맞는 보안 상태를 제공하며, 보안 평가 중에 반환되는 거짓 오류의 수를 최소화합니다. 예를 들어 텔넷을 사용해야 함을 알고 있는 경우 보안 평가를 수행할 때 소프트웨어가 텔넷을 취약점으로 고려하지 않도록 보안 프로파일을 사용자 정의할 수 있습니다. 이렇듯, 인증 및 암호화를 위해 Telnet with Kerberos를 사용하는 사이트는 텔넷 사용을 취약점으로 간주하지 않습니다.

옵션 사용 및 감사 출력 제어

이 절에서는 감사 실행 실행에 사용 가능한 옵션과 출력 제어용 옵션에 대해 설명합니다. 이 절은 다음 항목으로 구성됩니다.

- 88페이지에 "명령줄 옵션"
- 92페이지에 "배너 및 메시지 출력"
- 95페이지에 "호스트 이름, 스크립트 이름 및 시간 소인 출력"

명령줄 옵션

다음 명령줄 개요는 보안 프로파일에 대한 시스템 감사 방법을 보여줍니다.

```
# jass-execute -a 드라이버 [ -v [0-4] ] [ -q | -o 출력_파일 ] [ -m 전자우편_주소 ]
```

Solaris Security Toolkit 소프트웨어 감사 명령을 실행할 때 표 6-1에 나열된 다음 옵션을 사용할 수 있습니다.

표 6-1 감사 명령과 함께 명령줄 옵션 사용

옵션	설명
-a 드라이버	시스템이 보안 프로파일을 준수하는지 판별합니다.
-m 전자우편_주소	사내 지원을 위한 전자우편 주소를 지정합니다.

표 6-1 감사 명령과 함께 명령줄 옵션 사용 (계속)

옵션	설명
-o 출력_파일	Solaris Security Toolkit의 출력에 대한 파일 이름을 지정합니다.
-q	정숙 모드(Quiet Mode)를 설정합니다. 이 명령을 실행하는 동안에는 어떤 메시지도 표시되지 않습니다. 출력 결과는 JASS_REPOSITORY/에 저장됩니다.
-V 상세_레벨	감사 실행에 대한 상세(verbosity) 레벨(0-4)을 지정합니다.

jass-execute -a 명령과 함께 사용할 수 있는 옵션에 대한 자세한 정보는 다음 절을 참조하십시오.

- 89페이지에 "도움말 표시 옵션"
- 90페이지에 "전자 우편 통지 옵션"
- 91페이지에 "출력 파일 옵션"
- 91페이지에 "정숙 옵션"
- 91페이지에 "상세 옵션"

도움말 표시 옵션

-h 옵션은 사용 가능한 옵션의 개요를 제공하는 jass-execute 도움말 메시지를 표시합니다.

-h 옵션은 다음과 비슷한 출력을 작성합니다.

코드 예 6-1 예제 -h 옵션 출력

```
# ./jass-execute -h

To apply this Toolkit to a system, using the syntax:
jass-execute [-r root_directory -p os_version ]
[ -q | -o output_file ] [ -m e-mail_address ]
[ -V [3|4] ] [ -d ] driver

To undo a previous application of the Toolkit from a system:
jass-execute -u [ -b | -f | -k ] [ -q | -o output_file ]
[ -m e-mail_address ] [ -V [3|4] ]

To audit a system against a pre-defined profile:
jass-execute -a driver [ -V [0-4] ] [ -q | -o output_file ]
[ -m e-mail_address ]

To display the history of Toolkit applications on a system:
jass-execute -H

To display the last application of the Toolkit on a system:
jass-execute -l

To display this help message:
jass-execute -h
jass-execute -?

To display version information for this program:
jass-execute -v
```

전자 우편 통지 옵션

-m 전자우편주소 옵션은 실행이 완료될 때 출력이 Solaris Security Toolkit 소프트웨어에 의해 자동으로 전자 우편을 통해 보내질 수 있는 체계를 제공합니다. 전자 우편 보고서는 다른 옵션을 사용하여 시스템에 생성되는 모든 로그에 추가로 작성됩니다.

전자 우편 옵션을 사용하여 sunfire_15k_sc-config.driver를 호출하는 Solaris Security Toolkit 실행은 다음과 비슷합니다.

```
# ./jass-execute -m root -a sunfire_15k_sc-config.driver
[...]
```

출력 파일 옵션

-o 출력파일 옵션은 jass-execute 실행의 콘솔 출력을 별개 파일인 출력파일로 재지정합니다.

이 옵션은 JASS_REPOSITORY 디렉토리에 보존되는 로그에는 아무 영향도 주지 않습니다. 이 옵션은 Solaris Security Toolkit 실행에 의해 생성되는 상당한 양의 출력이 있기 때문에 특히 느린 터미널 연결을 통해 수행될 때 유용합니다.

이 옵션은 -d, -u 또는 -a 옵션 중 하나와 함께 사용할 수 있습니다.

-o 옵션은 다음과 비슷한 출력을 표시합니다.

코드 예 6-2 예제 -o 옵션 출력

```
# ./jass-execute -o jass-output.txt -a secure.driver
[NOTE] Executing driver, secure.driver
[NOTE] Recording output to jass-output.txt
#
```

정숙 옵션

-q 옵션은 강화 작업 중에 표준 입출력(stdio) 스트림에 대한 Solaris Security Toolkit 출력을 비활성화 합니다.

이 옵션은 JASS_REPOSITORY 디렉토리에 보존되는 로그에는 아무 영향도 주지 않습니다. -o 옵션과 비슷하게, 이 옵션은 특히 cron 작업 또는 느린 네트워크 연결을 통해 Solaris Security Toolkit 소프트웨어를 실행할 때 도움이 됩니다.

이 옵션은 -d, -u 또는 -a 옵션 중 하나와 함께 사용할 수 있습니다.

-q 옵션은 다음과 비슷한 출력을 작성합니다.

코드 예 6-3 예제 -q 옵션 출력

```
# ./jass-execute -q -a secure.driver
[NOTE] Executing driver, secure.driver
```

상세 옵션

-v 옵션은 감사 실행에 대한 상세(verbosity) 레벨을 지정합니다. 이 옵션은 감사에만 사용할 수 있습니다. 상세 레벨은 감사 실행의 결과를 표시하는 용통성이 높은 방법을 제공합니다. 예를 들어 100대의 시스템을 감사하는 경우 각 시스템에 대해 출력을 하나의 행으로 제한하여 어느 시스템이 감사를 통과하는지 간단히 판별할 수도 있습니다. 그런 다음 실패하는 시스템에 대해 문제점 영역에 집중하기 위해 확장된 출력을 생성하는 감사를 실행할 수 있습니다.

5가지 상세 레벨(0 - 4)이 -v 옵션으로 제어됩니다. 레벨이 올라갈수록 어떤 점검이 통과하고 어느 것이 실패하는지 보다 완전하게 이해하기 위해 사용할 수 있는 추가 세부 사항을 제공합니다. 표 6-2에 상세 레벨이 설명되어 있습니다.

표 6-2 감사 상세 레벨

레벨	출력
0	통과 또는 실패를 나타내는 단일 행.
1	각 스크립트에 대해 통과 또는 실패를 나타내는 단일 행 및 모든 스크립트 행 아래에 있는 하나의 총 점수 행.
2	각 스크립트에 대해 모든 점검 결과를 제공합니다.
3	배너 및 헤더 메시지를 포함하여 전체 출력을 제공하는 여러 행 이것은 기본값입니다.
4	여러 행(레벨 3에서 제공되는 모든 데이터) 및 logDebug 로깅 기능에 의해 생성되는 모든 항목. 이 레벨은 디버깅용입니다.

참고 - `jass-execute -v` 명령에 대한 기본 상세 레벨은 3입니다.

감사 상세 레벨의 전체 설명을 보려면 Solaris Security Toolkit 4.2 Reference Manual 7장 “JASS_VERBOSITY” 또는 `jass-execute man` 페이지를 참조하십시오.

배너 및 메시지 출력

배너 및 메시지를 보고하거나 생략하도록 Solaris Security Toolkit 감사 옵션을 구성할 수 있습니다. `JASS_LOG_BANNER` 변수는 상세 레벨 0-2로 사용할 수 없습니다. 이런 출력 옵션은 상세 레벨 3과 4에 적용합니다. 예를 들어, (`JASS_LOG_FAILURE` 변수)만을 보고하고 집중할 수 있도록 출력에서 통과 메시지(`JASS_LOG_SUCCESS` 변수)를 제거할 수 있습니다.

표 6-3은 로깅 변수를 통해 제어할 수 있는 배너 및 메시지 목록입니다. 로깅 변수에 대한 자세한 내용은 Solaris Security Toolkit 4.2 Reference Manual 7장 “JASS_LOG_BANNER”를 참조하십시오. 감사 상세 레벨에 대한 자세한 내용은 Solaris Security Toolkit 4.2 Reference Manual 7장 “JASS_VERBOSITY” 또는 `jass-execute man` 페이지를 참조하십시오. 로깅 변수가 0으로 설정되면 해당 유형의 메시지에 대해

출력이 생성되지 않습니다. 반대로 로깅 변수가 1로 설정되면 메시지가 표시됩니다. 이러한 각 변수에 대한 기본 조치는 출력을 표시하는 것입니다. 표 6-3에서 로깅 변수에 대해 설명합니다.

표 6-3 감사 출력에 배너 및 메시지 표시

로깅 변수	로그 접두어	설명
JASS_LOG_BANNER	모든 배너 출력	이 매개변수는 배너 메시지의 표시를 제어합니다. 이들 메시지는 대개 등호(=) 또는 하이픈(-) 문자 중 하나를 포함하는 분리자로 둘러싸입니다.
JASS_LOG_ERROR	[ERR]	이 매개변수는 오류 메시지의 표시를 제어합니다. 0으로 설정되면 오류 메시지가 생성되지 않습니다.
JASS_LOG_FAILURE	[FAIL]	이 매개변수는 실패 메시지의 표시를 제어합니다. 0으로 설정되면 실패 메시지가 생성되지 않습니다.
JASS_LOG_NOTICE	[NOTE]	이 매개변수는 알림 메시지의 표시를 제어합니다. 0으로 설정되면 알림 메시지가 생성되지 않습니다.
JASS_LOG_SUCCESS	[PASS]	이 매개변수는 성공 또는 통과 상태 메시지의 표시를 제어합니다. 0으로 설정되면 성공 메시지가 생성되지 않습니다.
JASS_LOG_SUMMARY	[SUMMARY]	이 매개변수는 요약 메시지의 표시를 제어합니다. 0으로 설정되면 어떤 요약 메시지도 표시되지 않습니다.
JASS_LOG_WARNING	[WARN]	이 매개변수는 경고 메시지의 표시를 제어합니다. 0으로 설정되면 경고 메시지가 생성되지 않습니다.

이 옵션은 특정 메시지만을 보고자 할 경우에 매우 유용합니다. 이들 옵션을 설정하여 중요하다고 생각하는 영역에 집중하면서도 출력을 최소화할 수 있습니다. 예를 들어 JASS_LOG_FAILURE(기본값인 1로 그대로 둠)를 제외한 모든 로깅 변수를 0으로 설정하면 감사가 logFailure에 의해 생성되는 실패에 대해서만 보고합니다.

코드 예 6-4 감사 실패만을 보고하는 예제 출력

```
# JASS_LOG_FAILURE=1
# export JASS_LOG_FAILURE
# JASS_LOG_BANNER=0
# JASS_LOG_ERROR=0
# JASS_LOG_NOTICE=0
# JASS_LOG_SUCCESS=0
# JASS_LOG_SUMMARY=0
# JASS_LOG_WARNING=0
# export JASS_LOG_BANNER JASS_LOG_ERROR
# export JASS_LOG_NOTICE JASS_LOG_SUCCESS
# export JASS_LOG_WARNING
# bin/jass-execute -a abc.driver -V2
update-at-deny      [FAIL] User adm is not listed in /etc/cron.d/at.deny.
```

코드 예 6-4 감사 실패만을 보고하는 예제 출력 (계속)

```
update-at-deny      [FAIL] User zz999999 is not listed in /etc/cron.d/at.deny.
update-at-deny      [FAIL] User gdm is not listed in /etc/cron.d/at.deny.
update-at-deny      [FAIL] User lp is not listed in /etc/cron.d/at.deny.
update-at-deny      [FAIL] User nobody4 is not listed in /etc/cron.d/at.deny.
update-at-deny      [FAIL] User root is not listed in /etc/cron.d/at.deny.
update-at-deny      [FAIL] User smmsp is not listed in /etc/cron.d/at.deny.
update-at-deny      [FAIL] User sys is not listed in /etc/cron.d/at.deny.
update-at-deny      [FAIL] User uucp is not listed in /etc/cron.d/at.deny.
update-at-deny      [FAIL] User webserverd is not listed in /etc/cron.d/at.deny.
update-at-deny      [FAIL] Script Total: 10 Errors
update-inetd-conf   [FAIL] Service svc:/network/telnet:default was enabled.
update-inetd-conf   [FAIL] Service svc:/network/ftp:default was enabled.
update-inetd-conf   [FAIL] Service svc:/network/finger:default was enabled.
update-inetd-conf   [FAIL] Service svc:/network/login:rlogin was enabled.
update-inetd-conf   [FAIL] Service svc:/network/shell:default was enabled.
update-inetd-conf   [FAIL] Service svc:/network/login:eklogin was enabled.
update-inetd-conf   [FAIL] Service svc:/network/login:klogin was enabled.
update-inetd-conf   [FAIL] Service svc:/network/shell:kshell was enabled.
update-inetd-conf   [FAIL] Service svc:/application/font/stfsloader:default was
enabled.
update-inetd-conf   [FAIL] Service svc:/network/security/ktkt_warn:default was
enabled.
update-inetd-conf   [FAIL] Service svc:/network/rpc/smsserver:default was
enabled.
update-inetd-conf   [FAIL] Service svc:/network/rpc/rstat:default was enabled.
update-inetd-conf   [FAIL] Service svc:/network/rpc/rusers:default was enabled.
update-inetd-conf   [FAIL] Service svc:/network/nfs/rquota:default was enabled.
update-inetd-conf   [FAIL] Service svc:/network/rpc/gss:default was enabled.
update-inetd-conf   [FAIL] Service 100235 is enabled in /etc/inet/inetd.conf.
update-inetd-conf   [FAIL] Service 100083 is enabled in /etc/inet/inetd.conf.
update-inetd-conf   [FAIL] Service 100068 is enabled in /etc/inet/inetd.conf.
update-inetd-conf   [FAIL] Script Total: 18 Errors
abc.driver          [FAIL] Driver Total: 28 Errors
abc.driver          [FAIL] Grand Total: 28 Errors
#
```

호스트 이름, 스크립트 이름 및 시간 소인 출력

상세 레벨 0 - 2에 대한 호스트 이름, 스크립트 이름 및 시간 소인 정보를 포함하도록 Solaris Security Toolkit 감사 옵션을 구성할 수 있습니다. 예를 들어, 감사할 시스템이 여러 개인 경우, 출력 결과를 호스트 이름, 스크립트 이름 또는 시간 소인으로 정렬하고자 할 수 있습니다. 표 6-4는 변수의 목록입니다.

표 6-4 호스트 이름, 스크립트 이름 및 시간 소인 감사 출력 표시

변수 이름	변수 설명
JASS_DISPLAY_HOSTNAME	이 매개변수를 1로 설정하면 Solaris Security Toolkit 소프트웨어가 각 로그 항목 앞에 시스템의 호스트 이름을 첨부합니다. 이 정보는 JASS_HOSTNAME 매개변수에 기초합니다. 기본적으로 이 매개변수는 비어 있으므로 Toolkit은 이 정보를 표시하지 않습니다.
JASS_DISPLAY_SCRIPTNAME	기본적으로 이 매개변수는 1로 설정되므로 Solaris Security Toolkit 소프트웨어가 각 로그 항목 앞에 현재 실행되고 있는 감사 스크립트의 이름을 첨부합니다. 이 매개변수를 다른 값으로 설정하면 Toolkit은 이 정보를 표시하지 않습니다.
JASS_DISPLAY_TIMESTAMP	이 매개변수를 1로 설정하면 Solaris Security Toolkit 소프트웨어가 각 로그 항목 앞에 감사 실행과 연관된 시간 소인을 첨부합니다. 이 정보는 JASS_TIMESTAMP 매개변수에 기초합니다. 기본적으로 이 매개변수는 비어 있으므로 해당 소프트웨어는 이 정보를 표시하지 않습니다.

호스트, 스크립트 및 시간 소인 정보를 앞에 첨부하도록 Solaris Security Toolkit 소프트웨어를 구성함으로써 단일 시스템이나 시스템 그룹의 많은 감사 실행을 결합하고 핵심 데이터를 기초로 정렬할 수 있습니다. 이 정보를 사용하여 여러 시스템에 걸쳐있거나 전개 프로세스의 증상인 문제점을 찾을 수 있습니다. 예를 들어 관리자는 이 방식으로 정보를 사용하여 주어진 프로세스를 사용하는 모든 시스템 구축에 항상 동일한 실패한 검사가 있는지 알 수 있습니다.

JASS_DISPLAY_TIMESTAMP 매개변수를 1로 설정하고 JASS_DISPLAY_SCRIPTNAME 값을 0으로 설정하면 다음과 비슷한 출력이 생성됩니다.

코드 예 6-5 감사 로그 항목의 예제 출력

```
# JASS_DISPLAY_TIMESTAMP=1
# JASS_DISPLAY_SCRIPTNAME=0
# export JASS_DISPLAY_TIMESTAMP JASS_DISPLAY_SCRIPTNAME
# bin/jass-execute -a abc.driver -V2
20050716132908 [FAIL] User adm is not listed in /etc/cron.d/at.deny.
20050716132908 [PASS] User bin is listed in /etc/cron.d/at.deny.
20050716132908 [FAIL] User zz999999 is not listed in /etc/cron.d/at.deny.
...
```

```
...
...
20050716132908 [FAIL] Script Total: 18 Errors
20050716132908 [FAIL] Driver Total: 28 Errors
20050716132908 [FAIL] Grand Total: 28 Errors
20050716132908 [SUMMARY] Results Summary for AUDIT run of dan.driver
20050716132908 [SUMMARY] The run completed with a total of 2 scripts run.
20050716132908 [SUMMARY] There were Failures in 2 Scripts
20050716132908 [SUMMARY] There were Errors in 0 Scripts
20050716132908 [SUMMARY] There were Warnings in 0 Scripts
20050716132908 [SUMMARY] There was a Note in 1 Script
20050716132908 [SUMMARY] Failure Scripts listed in:
/var/opt/SUNWjass/run/20050716132908/jass-script-failures.txt
20050716132908 [SUMMARY] Notes Scripts listed in:
/var/opt/SUNWjass/run/20050716132908/jass-script-notes.txt
#
```

보안 감사 수행

시스템에 대해 보안 평가를 주기적으로 수행하면 사용자가 구현한 보안 프로파일에 대해 시스템이 얼마나 가깝게 일치하는지의 벤치마크를 얻게 됩니다. 보안 평가 수행에 대한 가장 일반적인 시나리오는 새로운 설치를 수행한 후 보안 유지 작업으로 수행하는 것입니다. 보안 평가 옵션은 단순히 시스템을 강화하는 데 사용했던 동일한 강화 드라이버를 실행하도록 설계되었지만, 이제는 -a 옵션을 사용하여 강화 중에 구현된 보안 프로파일과 비교한 현재 상태를 점검합니다. 이 설계 방식은 복잡하지 않은 유연함을 제공합니다. 예를 들어 보안 프로파일을 업데이트할 때 후속 보안 평가는 업데이트된 보안 프로파일을 사용합니다.

또 다른 가능한 시나리오에서 사용자는 이미 전개된 시스템 보안의 책임자일 수도 있습니다. 해당 시스템을 강화하기 전에 보안 평가를 수행하고자 합니다. 이 시나리오에서는 사용자 고유의 보안 프로파일을 정의하거나 Solaris Security Toolkit 보안 프로파일 템플릿을 사용자 정의하거나 보안 프로파일 템플릿 중 하나를 있는 그대로 사용합니다.

▼ 보안 감사 수행

감사를 수행하기 전에 보안 프로파일을 정의 또는 선택해야 합니다. 자세한 정보는 87 페이지에 "보안 감사 준비"를 참조하십시오.



주의 - 이전에 강화하지 않은 전개된 시스템에 대해 보안 평가를 수행하려는 경우 먼저 시스템을 백업하고 재부팅하여 시스템이 알려지고 작동 중이며 일관성 있는 구성 상태에 있는지 확인하십시오. 보안 평가를 계속하기 전에 이 예비 재부팅 중에 검출되는 모든 오류나 경고를 정정하거나 기록해야 합니다.

1. 사용하려는 보안 프로파일(강화 드라이버)을 선택합니다.
 - 이전에 시스템을 강화한 경우 동일한 보안 프로파일을 사용하십시오.
예를 들면 `secure.driver`.
 - 시스템을 강화한 적이 없는 경우 표준 보안 프로파일이나 자체 프로파일 중 하나를 사용하십시오.
예를 들면 `secure.driver` 또는 `abccorp-secure.driver`.

사용 가능한 표준 및 제품별 드라이버의 최신 목록 및 전체 정보를 보려면 Solaris Security Toolkit 4.2 Reference Manual 4장 또는 `security_drivers` 매뉴얼 페이지를 참조하십시오.
2. 원하는 명령줄 옵션과 출력 제어 방법을 결정합니다.
88페이지에 "옵션 사용 및 감사 출력 제어"을 참조하십시오.

3. `jass-execute -a` 명령, 보안 프로파일의 이름 및 원하는 옵션을 입력합니다.
다음은 `abc-secure.driver`를 사용한 감사 실행의 예입니다.

코드 예 6-6 감사 실행의 출력 예

```
# ./jass-execute -a abc-secure.driver
[NOTE] Executing driver, abc-secure.driver

[...]

=====
abc-secure.driver: Audit script: enable-rfc1948.aud
=====

#-----
# RFC 1948 Sequence Number Generation
#
# Rationale for Verification Check:
#
# The purpose of this script is to verify that the system is
# configured and is in fact using RFC 1948 for its TCP sequence
# number generation algorithm (unique-per-connection ID). This is
# configured by setting the 'TCP_STRONG_ISS' parameter to '2' in
# the /etc/default/inetinit file.
#
# Determination of Compliance:
#
[...]
#-----

[PASS] TCP_STRONG_ISS is set to '2' in /etc/default/inetinit.
[PASS] System is running with tcp_strong_iss=2.

# The following is the vulnerability total for this audit script.

[PASS] Audit Check Total : 0 Error(s)

=====

# The following is the vulnerability total for this driver profile.

[PASS] Driver Total : 0 Error(s)

=====
abc-secure.driver: Driver finished.
=====
```

코드 예 6-6 감사 실행의 출력 예 (계속)

```
# The following is the vulnerability grand total for this run.  
  
[PASS] Grand Total : 0 Error(s)
```

감사 실행이 시작될 때 Solaris Security Toolkit 소프트웨어는 JASS_HOME_DIR/Audit 디렉토리의 파일에 액세스합니다. JASS_HOME_DIR/Audit 및 JASS_HOME_DIR/Finish 디렉토리에 있는 파일이 동일한 기본 파일 이름을 공유하지만 서로 다른 파일 이름 접미어를 갖습니다. driver.run 스크립트는 JASS_SCRIPTS 변수로 정의된 종료 스크립트의 접미사를 .fin에서 .aud로 변경하여 실행하는 동안 각 경고 레벨에서 생성된 모든 메시지가 포함된 포인터 및 파일을 따라 자동으로 감사 스크립트로 해석합니다.

감사 실행이 시작하고 Solaris Security Toolkit 소프트웨어의 상태를 초기화합니다. 실행 중에 액세스되는 각 드라이버가 모든 파일 템플릿 및 감사 스크립트의 상태를 평가합니다. 각 검사 결과는 각각 0이거나 0이 아닌 취약성 값으로 표시되는 성공 또는 실패 상태로 나타납니다. 대부분의 경우 실패는 숫자 1로 표시됩니다. 실행되는 각 스크립트가 스크립트에 들어있는 각 검사의 총 취약성 값을 토대로 총 보안 점수를 작성합니다. 각 드라이버에 대한 총 취약성 값 결과가 드라이버 평가 완료 시에 표시됩니다. 모든 점수의 총계는 작업이 종료할 때 제시됩니다.

보안 평가 옵션은 평가 작업이 시작되는 시점에서 시스템 상태의 포괄적인 보기를 제공합니다. Solaris Security Toolkit 소프트웨어는 구성 파일을 조사하여 시스템의 저장된 상태를 점검하고 프로세스 테이블 정보, 장치 드라이버 정보 등을 조사하여 시스템의 실행 중 상태를 점검합니다. Solaris Security Toolkit 소프트웨어는 각 파일이나 서비스의 존재 여부를 점검하고 서비스와 연관된 소프트웨어가 설치, 구성, 사용 가능 및 실행 중인지 점검합니다. 이 접근 방식은 시스템의 현재 상태에 대한 정확한 스냅샷을 작성합니다.

시스템 보안

이 장은 새로운 Solaris 8 또는 9 OS의 설치 및 보안에 대해 이전 장에서 제공된 정보와 전문 지식을 실현 가능한 시나리오에 적용하는 방법에 대해 설명합니다. 이 장은 Solaris 8 OS용 Check PointFirewall-1 NG를 갖는 Solaris Security Toolkit 소프트웨어를 전개하는 방법에 대해 설명합니다.

이 장에 있는 정보를 새로운 시스템 및 응용 프로그램 보안을 위한 지침 및 사례 시나리오로 사용하십시오.

Sun BluePrint 설명서와 온라인 기사는 많은 Sun 시스템의 최소화 및 강화 프로세스 과정을 이해하는데 유용합니다. 최신 제품 관련 설명서 및 기사는 다음 웹사이트를 참조하십시오.

<http://www.sun.com/blueprints>

이 장에서는 다음 주제를 다룹니다.

- 101페이지에 "계획 및 준비"
- 103페이지에 "보안 프로파일 작성"
- 104페이지에 "소프트웨어 설치"
- 107페이지에 "JumpStart 서버 및 클라이언트 구성"
- 111페이지에 "강화 구성 사용자 정의"
- 116페이지에 "클라이언트 설치"
- 117페이지에 "품질 보증 검사"

계획 및 준비

이 사례 연구에서 설명된 것처럼 최소화 및 보안된 시스템을 효과적으로 그리고 효율적으로 전개하려면 계획과 준비가 중요합니다. 기초적인 네트워크 기반구조, 방침 및 절차가 제대로 준비되어 있어야 합니다. 또한, 시스템의 지원 및 유지에 대해 정의하고 이해

해야 합니다. 계획 및 준비에 대한 자세한 정보는 2 장을 참조하십시오. 이 장에 설명된 시나리오는 시스템 관리자(SA)가 방화벽 시스템을 위해 Solaris OS 이미지의 최소화 및 강화를 위해 수행할 과정 및 작업에 대해 상세히 설명합니다.

이 시나리오에서, 시스템 관리자는 고객에게 방화벽 서비스를 제공려는 서비스 제공자를 위해 Check Point Firewall-1 NG 시스템을 구축 및 전개하기 위한 자동화되고 확장 가능한 솔루션을 만드는 작업을 합니다. 이 시나리오의 경우, 서비스 제공자의 요구사항과 고려사항은 다음과 같습니다.

- 서비스 제공자는 이러한 시스템을 많이 전개할 계획이므로 각 시스템을 구축하고 전개하는 시간은 매우 중요하며 능률적으로 수행해야 합니다.
- 시스템은 각 시스템의 내부 이더넷 인터페이스에 연결된 전용 관리 네트워크를 사용하여 설치됩니다. 서비스 제공자 직원만이 이 네트워크를 사용하며 가입자는 사용하지 않습니다.
- 다른 모든 네트워크는 분리된 물리적 네트워크 인터페이스에 있으며 필터링됩니다.
- 관리 네트워크의 보안은 전개된 방화벽 시스템의 전체 보안에 매우 중요합니다.

이러한 요구사항에 근거하여 시스템 관리자는 JumpStart 기술과 Solaris Security Toolkit 소프트웨어를 사용하여 OS 이미지의 설치, 최소화 및 강화를 자동화하기로 결정합니다.

가정 및 제한사항

이 장은 이미 작동 중인 Solaris Security Toolkit 소프트웨어와 JumpStart 기술 설치를 사용 중이라고 가정합니다. 3 장에서는 해당 소프트웨어 설치에 대한 안내 및 지침을 제공합니다.

또한 이 장에서는 특정 응용 프로그램의 최소화 및 강화를 위해 사용자 정의 구성을 개발 중이라고 가정합니다. Solaris Security Toolkit 소프트웨어에는 해당 응용 프로그램에 대한 드라이버나 JumpStart 프로파일이 없습니다. 따라서, 이 응용 프로그램에 대해 사용자 정의된 드라이버 및 프로파일을 작성해야 합니다. 이 작업은 기존 드라이버와 프로파일을 복사한 후, 응용 프로그램에 맞게 수정하면 됩니다.

이 사례 시나리오의 경우 시스템 관리자(SA)의 기술 레벨은 다음과 같습니다.

- OS 및 응용 프로그램 구성에 대한 충분한 지식과 경험이 있습니다.
- 구성을 테스트하고 조정하는 방법을 알고 있습니다.
- 클라이언트 시스템이 설치되는 JumpStart 환경을 구축하는 방법을 알고 있습니다. 자세한 내용은 Sun BluePrint 설명서 *JumpStart Technology: Effective Use in the Solaris Operating Environment*를 참조하십시오.
- OS 최소화 기술에 익숙합니다. *Enterprise Security: Solaris Operating Environment Security Journal*, *Solaris Operating Environment Versions 2.5.1, 2.6, 7, and 8*을 참조하십시오.

- Solaris Security Toolkit 소프트웨어에 대한 기본 지식이 있고, 최소화와 강화 기술 및 지침을 모두 사용하여 사용자 정의된 구성을 구축하려고 합니다. 1 장을 참조하십시오.

시스템 환경

예제 시나리오는 다음 하드웨어 및 소프트웨어 환경을 기초로 합니다.

- Check PointFirewall-1 NG
- Solaris 8 OS
- JumpStart 기술
- Solaris OS 클러스터(SUNWCreg)
- Solaris Security Toolkit 소프트웨어
- SPARC 기술에 기초를 둔 플랫폼
- 적어도 두 개의 이더넷 인터페이스

보안 요구사항

이 시나리오의 경우, 높은 레벨의 요구사항 및 소프트웨어 패키지가 확인되었으나, 모든 패키지의 특정 구성요소 및 서비스가 확인되어야 합니다. 또한, 시스템을 관리하기 위해 필요한 Solaris OS 기능이 확인되어야 합니다.

다음 목록은 소프트웨어 구성요소가 사용된 방법에 대한 자세한 보기를 제공합니다.

- 원격 관리를 위한 Secure Shell
- 원격 파일을 다운로드하는 FTP 클라이언트
- 파일을 복사하는 scp 및 sftp

이 목록에서 보안 프로파일을 개발할 수 있습니다. 보안 프로파일 개발과 프로파일 템플릿 사용에 대한 자세한 정보는 29페이지에 "Solaris Security Toolkit 프로파일 개발 및 구현"을 참조하십시오.

보안 프로파일 작성

보안 프로파일은 Solaris Security Toolkit 소프트웨어가 시스템의 보안 구성을 강화하고 최소화할 때 수행하는 보안 수정사항을 정의합니다. Solaris Security Toolkit에 포함된 표준 보안 프로파일 또는 드라이버는 최소화된 Check PointFirewall-1 NG 시스템에 대한 요구사항에 부합되지 않습니다. 따라서, 사용자 정의 보안 프로파일을 작성하여 필요한 시스템 수정사항을 적용해야 합니다.

이 시나리오의 경우, 보안 프로파일을 작성하는 프로세스가 이 장에 여러 절로 설명되어 있습니다. 첫 번째, 기존 드라이버에 기초하여 새 드라이버 파일을 작성합니다. 그런 다음 이전에 요약된 보안 요구사항을 준수하도록 새 드라이버를 수정합니다. 최소화는 104페이지에 "소프트웨어 설치"에서 설명되고 강화 수정은 111페이지에 "강화 구성 사용자 정의"에서 설명됩니다.

소프트웨어 설치

이 절은 소프트웨어 설치 프로세스를 설명합니다. 예제 시나리오를 위해 모든 예외사항 또는 시나리오 관련 지침을 제공합니다. 소프트웨어 설치에 대한 일반 지침을 보려면 3장을 참조하십시오.

참고 – 다음 지침을 관련 상황을 취급하기 위한 템플릿으로 사용할 수 있습니다.

이 절에는 다음 작업이 포함됩니다.

- 104페이지에 "보안 소프트웨어 다운로드 및 설치"
- 105페이지에 "패치 설치"
- 105페이지에 "OS Cluster 지정 및 설치"

보안 소프트웨어 다운로드 및 설치

아래와 같이 JumpStart 서버에 Solaris Security Toolkit과 패치를 포함한 추가 보안 소프트웨어를 다운로드 및 설치하십시오.

▼ 보안 소프트웨어 다운로드 및 설치

1. **Solaris Security Toolkit** 소프트웨어와 추가 보안 소프트웨어를 다운로드 및 설치하십시오.
(40페이지에 "보안 소프트웨어 다운로드" 참조)
2. 다운로드한 **Solaris Security Toolkit** 소프트웨어와 추가 보안 소프트웨어를 설치하십시오.
(47페이지에 "소프트웨어 설치 및 실행" 참조)



주의 – 아직 Solaris Security Toolkit 소프트웨어를 실행하지 마십시오. 우선 다음 절에 설명되어 있는 추가 구성 및 사용자 정의를 수행하십시오.

패치 설치

OS 패치는 보안 취약성, 가용성 문제, 성능 관련 사항 또는 시스템의 다른 측면을 다룰 수 있습니다. 새로운 OS를 설치하는 동안, 그리고 설치 후에는 필요한 패치가 설치되었는지 지속적으로 확인하십시오.

Solaris Security Toolkit 소프트웨어는 SunSolve Online에서 이용 가능한 Recommended and Security Patch Cluster의 설치 방법을 제공합니다. OS 관련 클러스터 패치에는 가장 일반적으로 사용되는 패치가 들어있습니다.

▼ 패치 설치

1. 최소한 **Recommended and Security Patch Cluster**를 Patches 디렉토리에 다운로드 하고 압축을 해제합니다.

`install-recommended-patches.fin` 스크립트가 강화 드라이버에 포함되는 경우 해당 패치 클러스터가 자동으로 설치됩니다.

Check PointFirewall-1 NG에 추가 문제점이 있습니다. 이 응용프로그램에는 Recommended and Security Patch Cluster에 들어있지 않은 특정 패치가 필요합니다. Check PointFirewall-1 NG는 다음 패치를 필요로 합니다.

- 108434
- 108435

2. 패치 **108434** 및 **108435**의 설치를 자동화하기 위해, **SunSolve OnLine**에서 최신 버전을 다운로드하여 Patches 디렉토리에 저장합니다.
3. 각 패치의 이름과 함께 `add_patch` 지원 프로그램 기능을 호출하는 새로운 종료 스크립트(예: `fw1-patch-install.fin`)를 작성합니다.

이 종료 스크립트는 두 개의 Check PointFirewall-1 NG 필수 패치 ID와 함께 올바른 지원 프로그램 기능을 호출합니다. 예를 들면,

```
# !/bin/sh

# add_patch 108434-10

# add_patch 108435-10
```

OS Cluster 지정 및 설치

OS 설치를 위한 디스크 레이아웃을 정의한 후, 설치할 Solaris OS 클러스터를 지정합니다. Solaris OS와 함께 사용 가능한 다섯 개의 설치 클러스터 `SUNWCreg`, `SUNWCuser`, `SUNWCprog`, `SUNWCall` 및 `SUNWCXall` 중 하나를 선택하십시오.

▼ OS 클러스터 지정 및 설치

1. 설치할 OS 클러스터를 지정합니다.

이 사례 시나리오의 목표가 최소화 및 전용 방화벽 디바이스를 구축하는 것이기 때문에 사용 가능한 Solaris OS 클러스터 중 가장 작은 SUNWCreq(Core라고도 함)를 선택합니다.

이 클러스터는 상대적으로 적은 수의 패키지를 포함하므로 다른 패키지가 필요할 수도 있습니다. 이러한 다른 필수 패키지가 Solaris OS 클러스터 정의가 있는 프로파일에 반드시 포함되어야 합니다.

기준 프로파일 정의는 다음을 이전에 정의된 프로파일에 추가합니다.

cluster	SUNWCreq
---------	----------

SUNWCreq 설치 클러스터는 방화벽 Sun 서버가 올바르게 기능하기 위해 불필요한 패키지를 포함합니다. 작업 기준을 정한 후 이러한 여분의 패키지를 제거하십시오. Sun BluePrints OnLine 기사 “Minimizing the Solaris Operating Environment for Security: Updated for the Solaris 9 Operating Environment” 를 참조하십시오.

2. 정의된 보안 프로파일과 함께 설치를 실행하여 패키지 종속 문제가 있는지 판별하십시오.

일부 패키지 종속성이 설치 시 발생되었고, 다음 Solaris OS 패키지가 Check PointFirewall-1 NG에 필요하다고 결정하였습니다.

- SUNWter - 터미널 정보
- SUNWadmc - 시스템 관리 코어 라이브러리
- SUNWadmfw - 시스템 및 네트워크 관리 프레임워크
- SUNWlibc 및 SUNWlibcX - Check PointNG 응용프로그램에 필요

프로파일의 전체 패키지 목록은 다음과 같습니다..

cluster	SUNWCreq	
package	SUNWter	add
package	SUNWlibc	add
package	SUNWlibcX	add
package	SUNWadmc	add
package	SUNWadmfw	add

참고 - 이 목록은 본 사례 연구에는 완벽하지만, 이 구성이 전개될 실제 환경에 따라 추가 패키지를 추가 또는 제거해야 할 수 있습니다.

117페이지에 "품질 보증 검사"에 설명된 것처럼 시스템이 기능 및 보안 측면 모두에서 검증될 때까지 패키지의 최종 목록은 수정이 필요할 수 있습니다. 수정이 필요한 경우 프로파일을 수정하고 시스템을 다시 설치한 후 테스트를 반복하십시오.

- 이전 두 단계의 패키지 종속성을 기초로 `minimize-firewall.fin` 스크립트를 작성합니다.

JumpStart 서버 및 클라이언트 구성

이 절은 최소화를 위해 사용자 정의 보안 프로파일을 사용하도록 JumpStart 서버 및 클라이언트를 구성하는 방법에 대해 설명합니다. JumpStart 환경에서 Solaris Security Toolkit 소프트웨어 사용에 대한 자세한 정보는 5 장을 참조하십시오.

이 절에는 다음 작업이 포함됩니다.

- 107페이지에 "기반구조 준비"
- 110페이지에 "Rules 파일 확인 및 검사"

기반구조 준비

기반구조를 준비하려면 다음 작업을 수행하십시오. 다음 작업은 기존 드라이버, 프로파일 및 종료 스크립트를 사용하는 클라이언트를 위한 기준 구성 작성 프로세스를 설명합니다. 이 기준이 적용된 후, 제대로 작동하는지 확인하고 선택된 응용 프로그램에 맞게 사용자 정의하십시오.

▼ 기반구조 준비

1. **JumpStart** 서버 및 환경을 구성합니다.
자세한 지침은 5 장을 참조하십시오.
2. `add-client` 명령을 사용하여 **JumpStart** 서버에 클라이언트를 추가합니다.

코드 예 7-1 JumpStart 서버에 클라이언트 추가

```
# pwd
/jumpstart
# bin/add-client -c jordan -o Solaris_8_2002-02 -m sun4u
-s nomex-jumpstart
cleaning up preexisting install client "jordan"
removing jordan from bootparams
updating /etc/bootparams
```

3. 올바른 **JumpStart** 프로파일 및 종료 스크립트를 지정하여 클라이언트를 위한 rules 파일 항목을 작성합니다. 예를 들면,

```
hostname jordan - Profiles/xsp-minimal-firewall.profile \  
Drivers/xsp-firewall-secure.driver
```

4. **Solaris Security Toolkit** 소프트웨어와 함께 제공된 파일을 복사하여 xsp-minimal-firewall.profile이라는 프로파일 파일 및 xsp-firewall-secure.driver라는 드라이버 파일을 작성합니다.

이러한 파일을 작성해야 다음 단계를 성공적으로 완료할 수 있습니다. 처음에 이러한 파일은 Solaris Security Toolkit 소프트웨어와 함께 배포된 파일의 사본일 수 있습니다.

참고 – Solaris Security Toolkit 소프트웨어와 함께 배포된 원본 파일을 절대 수정하지 마십시오.

다음 예제는 파일을 작성하는 방법을 보여줍니다.

코드 예 7-2 프로파일 작성

```
# pwd  
/jumpstart/Drivers  
# cp install-Sun_ONE-WS.driver xsp-firewall-secure.driver  
# cp hardening.driver xsp-firewall-hardening.driver  
[...]  
# pwd  
/jumpstart/Profiles  
# cp minimal-Sun_ONE-WS-Solaris8-64bit.profile \  
xsp-minimal-firewall.profile
```

이 예제는 전용 방화벽을 개발하기 좋은 기준선이므로 전용 웹 서버 구성을 기준으로 합니다.

5. 프로파일 및 드라이버 파일을 작성한 후 다음과 같이 파일을 수정합니다.
 - a. hardening.driver에 대한 xsp-firewall-secure.driver 참조를 xsp-firewall-hardening.driver로 교체합니다.

- b. JASS_SCRIPTS에 정의된 두 종료 스크립트를 minimize-firewall.fin에 대한 참조 및 사용자의 종료 스크립트(예: fw1-patch-install.fin)로 교체합니다. 수정된 스크립트는 다음과 유사해야 합니다.

코드 예 7-3 수정된 스크립트의 출력 예제

```
DIR="/bin/dirname $0`"  
export DIR  
. ${DIR}/driver.init  
. ${DIR}/config.driver  
JASS_SCRIPTS="  
                minimize-firewall.fin  
                fw1-patch-install.fin"  
. ${DIR}/driver.run  
. ${DIR}/xsp-firewall-hardening.driver
```

6. 다음 명령을 사용하여 rules 파일 항목이 올바른지 확인하십시오.

코드 예 7-4 rules 파일의 정확성 검사

```
# pwd  
/jumpstart  
# ./check  
Validating rules...  
Validating profile Profiles/end-user.profile...  
Validating profile Profiles/xsp-minimal-firewall.profile...  
Validating profile Profiles/test.profile...  
Validating profile Profiles/entire-distribution.profile...  
Validating profile Profiles/oem.profile...  
The custom JumpStart configuration is ok.
```

이 시점에서, 이 예제의 jordan 클라이언트에서 JumpStart 설치를 시작하는 것이 가능해야 합니다. 작성한 JumpStart 구성과 Solaris Security Toolkit 드라이버, 종료 스크립트 및 프로파일을 사용합니다.

7. rules 파일을 검사할 때 문제점이 발생하는 경우 110페이지에 "Rules 파일 확인 및 검사"를 참조하십시오.

8. 클라이언트의 ok 프롬프트에서 다음 명령을 입력하여 **JumpStart** 기반구조를 사용하는 클라이언트를 설치합니다.

```
ok> boot net - install
```

클라이언트가 설치되지 않는 경우 구성을 검토하여 적절히 동작할 때까지 구성을 수정하십시오. 이 절에서 JumpStart 구성의 모든 부분이 언급되지는 않습니다. 자세한 내용은 Sun BluePrint 설명서 JumpStart Technology: Effective Use in the Solaris Operating Environment를 참조하십시오.

rules 파일의 올바른 실행을 달성하고 패치가 제대로 설치되었음을 확인한 다음, 클라이언트 시스템의 기본 레벨 설치 및 그의 최소화 및 강화를 시작할 수 있습니다.

Rules 파일 확인 및 검사

rules 파일의 정확성을 확인할 때, 다양한 문제점이 발생할 수 있습니다. 일반적인 문제 몇 가지가 이 절에서 언급됩니다.

rules 파일을 처음 실행하면 다음 출력이 나타납니다.

코드 예 7-5 rules 파일의 예제 출력

```
# pwd
/jumpstart
# ./check
Validating rules...
Validating profile Profiles/xsp-minimal-firewall.profile...
Error in file "rules", line 20
hostname jordan - Profiles/xsp-minimal-firewall.profile
Drivers/xsp-firewall-secure.driver
오류: Profile missing:
  Profiles/xsp-minimal-firewall.profile
```

이 예제에서, jordan에 대한 rules 항목에 지정된 프로파일이 존재하지 않습니다. xsp-minimal-firewall.profile Profiles은 profiles 디렉토리에 존재하지 않았습니다. 일반적으로 이 오류는 파일 이름의 잘못된 철자, 프로파일의 올바른 디렉토리 지정 생략 또는 프로파일을 작성하지 않은 이유로 발생합니다. 문제점을 수정하고 검사를 재실행하십시오.

두 번째 실행은 두 거자 다른 문제점을 표시합니다. 첫 번째 문제점은 xsp-firewall-secure.driver에서 호출되는 드라이버입니다. xsp-firewall-hardening.driver를 호출하는 대신, xsp-firewall-secure.driver가 여전히 hardening.driver를 호출하고 있습니다.

두 번째 문제점은 JASS_SCRIPTS 변수가 minimize-firewall.fin 대신에 minimize-Sun_ONE-WS.fin으로 잘못 설정된다는 것입니다.

다음은 잘못된 스크립트입니다.

코드 예 7-6 잘못된 스크립트의 예제

```
#!/bin/sh
DIR="/bin/dirname $0`"
export DIR
. ${DIR}/driver.init
. ${DIR}/config.driver
JASS_SCRIPTS="minimize-Sun_ONE-WS.fin"
. ${DIR}/driver.run
. ${DIR}/hardening.driver
```

다음은 올바른 스크립트의 예제입니다.

코드 예 7-7 올바른 스크립트의 예제

```
#!/bin/sh
DIR="/bin/dirname $0`"
export DIR
. ${DIR}/driver.init
. ${DIR}/config.driver
JASS_SCRIPTS="
minimize-firewall.fin"
. ${DIR}/driver.run
. ${DIR}/xsp-firewall-hardening.driver
```

강화 구성 사용자 정의

제안된 방화벽의 강화 구성은 사용자 정의되고 정교하게 조절될 준비가 되었습니다. 초기 스크립트는 hardening.driver를 기초로 합니다. 이것은 시스템이 "warm-brick" 상태가 됨을 의미합니다. 즉 모든 서비스가 사용 불가능합니다.

Solaris 8 OS에 Secure Shell 클라이언트가 포함되어 있지 않으므로, 방화벽의 원격 네트워크 기반 관리가 가능하도록 수정해야 합니다. 이 사례 시나리오의 방화벽의 경우, FTP 서비스가 사용 가능 상태로 남아있고 원격 관리를 위해 Secure Shell 클라이언트를 설치해야 합니다. 이들 서비스를 모두 개인 관리 네트워크만으로 제한함으로써 다른 네

트위크 인터페이스에서 접속하지 못하도록 하십시오. 이러한 서비스 제한에 대한 정보에 대해서는, Sun BluePrints OnLine 기사 "Solaris Operating Environment Security: Updated for Solaris 9 Operating Environment"를 참조하십시오.

이들 두 서비스를 사용 가능한 상태로 두는 것 외에, 디스크 미러링을 위해 Sostice DiskSuite를 구성하는 데 Solstice DiskSuite GUI를 사용할 수 있도록 RPC 서비스를 사용 가능한 상태로 두십시오. Solstice DiskSuite GUI를 사용하지 않을 경우, RPC 서비스는 필요하지 않습니다. 이 예제에서는 GUI가 필요하므로 RPC 서비스는 사용 가능한 상태로 남아있습니다. Solstice DiskSuite의 설치 및 구성은 이 설명서에서 다루지 않습니다.

이 클라이언트에 필요한 최종 수정은 xSP(서비스 제공자)의 중앙 집중된 SYSLOG 서버를 사용하는 사용자 정의된 syslog.conf가 정교하게 만들어지는 것입니다. 이 사용자 정의된 syslog.conf 파일이 각 방화벽 시스템에 설치되어야 합니다.

이 수정을 위해서는 Solaris Security Toolkit의 구성 옵션을 변경해야 합니다. 필요한 각 수정사항이 다음 절에서 상세히 설명됩니다.

- 112페이지에 "FTP 서비스 사용"
- 113페이지에 "Secure Shell 소프트웨어 설치"
- 114페이지에 "RPC 서버 사용"
- 115페이지에 "syslog.conf 파일 사용자 정의"

FTP 서비스 사용

이 사례 시나리오의 방화벽의 경우 FTP 서비스를 사용 가능하게 하십시오.

▼ FTP 서비스 사용

1. FTP를 사용 가능한 상태로 두기 위해, JASS_SVCS_DISABLE 및 JASS_SVCS_ENABLE 변수를 설정하여 update-inetd-conf.fin 파일의 기본 동작을 수정합니다.

FTP를 제외한 모든 표준 Solaris OS 서비스를 사용 불가능하게 하려는 경우, 본 사례 시나리오에 대한 최선의 방법은 JASS_SVCS_DISABLE이 finish.init 스크립트에서 받은 기본값으로 남아있는지 확인하면서 JASS_SVCS_ENABLE이 ftp가 되도록 정의하는 것입니다. Solaris Security Toolkit 4.2 Reference Manual을 참조하십시오.

2. 환경 변수를 통해 변경을 구현하기 위해 xsp-firewall-hardening.driver에 대한 호출 전에 다음과 비슷한 항목을 xsp-firewall-secure.driver에 추가합니다.

```
JASS_SVCS_ENABLE="ftp"
```


3. 방화벽 소프트웨어를 통해 구현하여 **FTP가 xSP의 관리 네트워크에서만 사용 가능한지** 확인합니다.

언급된 기타 요구사항 중 하나는 Secure Shell이 **xSP의 관리 네트워크에서만 사용 가능**해야 한다는 것이었습니다. Solaris 8 OS에서 TCP 랩퍼를 시스템에 통합함으로써 또는 방화벽 소프트웨어 자체를 통해서 이 요구사항을 수행할 수 있습니다. 이 사례 시나리오에서는 방화벽 소프트웨어를 통해서 수행하십시오.

Secure Shell 소프트웨어 설치

참고 – 이 지침은 Solaris 8 OS가 실행되는 시스템에만 적용됩니다. 사용하는 시스템에서 Solaris 9 또는 10 OS가 실행되는 경우, Solaris OS와 함께 배포된 Secure Shell 소프트웨어를 사용하여 이 절의 OpenSSH 설치 단계를 생략할 수 있습니다.

Solaris 8 OS에는 Secure Shell 클라이언트가 포함되지 않습니다. 그러므로 시스템에 Solaris 8 OS가 실행되는 경우에는 원격 관리를 위해 Secure Shell 클라이언트를 설치해야 합니다.

Solaris Security Toolkit 소프트웨어를 구성하여 OpenSSH 도구를 설치할 수 있습니다. `xsp-firewall-secure.driver`에 의해 사용된 `config.driver` 파일에 나열되는 `install-openssh.fin` 스크립트를 사용하십시오.

▼ Secure Shell 설치

1. 기본 `config.driver`를 `xsp-firewall-config.driver`에 복사합니다.
2. 파일 사본에서 `install-openssh.fin`에 대한 항목을 주석으로 처리합니다.
3. `xsp-firewall-config.driver`에서 `config.driver`를 호출하는 항목을 수정하여 대신 `xsp-firewall-secure.driver`를 호출합니다.
4. **OpenSSH의 최신 버전을 구합니다.**
패치 및 OS 릴리스의 경우와 마찬가지로 OpenSSH의 최신 버전을 사용하십시오. 최신 릴리스 정보는 다음 OpenSSH 웹 페이지를 참조하십시오.
<http://www.openssh.org>
5. **OpenSSH** 패키지를 컴파일하고 이름을 지정한 후 Packages 디렉토리에 설치합니다.
이 패키지에 대한 자세한 정보는, Sun BluePrints 온라인 기사 “Configuring OpenSSH for the Solaris Operating Environment” 를 참조하십시오.

- 올바른 **OpenSSH** 패키지 이름을 반영하도록 `install-openssh.fin` 스크립트를 업데이트합니다.

`install-openssh.fin` 스크립트를 수정해야 하는 경우가 있습니다. 이 스크립트는 **OpenSSH** 패키지의 패키지 이름을 다음과 유사하게 형식화되도록 정의합니다.

```
OBSDssh-3.5p1-sparc-sun4u-5.8.pkg
```

여기서 패키지 이름은 버전 번호(3.5p1), 구조(sparc), 구조의 버전(sun4u), 패키지가 컴파일되는 대상 OS(5.8) 및 pkg 접미어의 형식을 따릅니다.

- 방화벽 소프트웨어를 통해 구현하여 **SSH**가 **xSP**의 관리 네트워크에서만 사용 가능하게 합니다.

언급된 기타 요구사항 중 하나는 **Secure Shell**이 **xSP**의 관리 네트워크에서만 사용 가능해야 한다는 것이었습니다. **Solaris 8 OS**에서는 **TCP 램퍼**를 시스템에 통합함으로써 또는 방화벽 소프트웨어 자체를 통해 이 요구사항을 구현할 수 있습니다. 이 사례 시나리오의 경우, 방화벽 소프트웨어를 통해 구현합니다. 이 요구사항은 또한 **Secure Shell** 서버의 구성을 수정하여 구현할 수 있음을 주의하십시오.

RPC 서버 사용

RPC가 필요한 디스크 미러링을 위해 **Solaris DiskSuite**를 사용할 수 있도록 **RPC** 서비스를 사용 가능한 상태로 두십시오.

이 수정은 특정 종료 스크립트인 `disable-rpc.fin`가 **Solaris Security Toolkit** 실행 중에 **RPC** 서비스를 사용 불가능하게 할 수 있기 때문에 비교적 간단합니다.

참고 - 시스템의 **RPC** 서비스에 원격으로 액세스하는 것은 시스템의 방화벽 구성에 의해 명시적으로 거부되어야 합니다.

▼ RPC 사용

- `xsp-firewall-hardening.driver`에서 `disable-rpc.fin`에 대한 항목을 주석으로 처리합니다.

스크립트를 제거하는 대신 주석으로 처리하여 드라이버에서 스크립트를 사용할 수 없도록 합니다. 주석의 경우, 특정 조합만 허용되므로 `JASS_SCRIPTS` 정의의 항목을 주석으로 처리할 때 주의하십시오.

다음은 Solaris Security Toolkit 소프트웨어가 `JASS_SCRIPTS` 정의에서 주석 표시기로서 허용하는 것에 대해 `driver.funcs script`에 들어있는 주석입니다.

```
#Very rudimentary comment handler. This code will only recognize
#comments where a single '#' is placed before the file name
#(separated by white space or not). It then will only skip the
#very next argument.
```

syslog.conf 파일 사용자 정의

이 클라이언트에 필요한 최종 수정은 xSP(서비스 제공자)의 중앙 집중된 SYSLOG 서버를 사용하는 사용자 정의된 `syslog.conf`가 정교하게 만들어지는 것입니다. 이 사용자 정의된 `syslog.conf` 파일이 각 방화벽 시스템에 설치되어야 합니다.

▼ syslog.conf 파일 사용자 정의

1. xSP 표준 `syslog.conf` 파일을 복사한 후 `syslog.conf.jordan`로 이름을 바꾸고 `Files/etc` 디렉토리에 저장합니다.

Solaris Security Toolkit 소프트웨어는 다양한 파일 복사 모드를 지원합니다. 이 구성에 가장 적합한 옵션은 `syslog.conf` 파일이 `jordan`에만 복사되도록 시스템의 호스트 이름을 파일에 접미어로 추가하는 것으로, 그것이 고유한 방화벽 특정 수정사항을 갖기 때문입니다. 이 경우, 클라이언트를 `jordan`이라고 하므로 `Files/etc`에 사용된 실제 파일 이름은 `syslog.conf.jordan`입니다. `JASS_FILES` 정의는 이 접미어가 추가되지 않아야 한다는 것을 주의하십시오. 접미어에 대한 자세한 정보는, Solaris Security Toolkit 4.2 Reference Manual을 참조하십시오.

2. xSP 표준 `syslog.conf` 파일을 사용할 수 없는 경우 다음과 같이 사용자 정의 `syslog.conf` 파일을 작성합니다.
 - a. Solaris Security Toolkit 소프트웨어에 포함된 `syslog.conf` 파일을 복사하여 `syslog.conf.jordan`으로 이름을 바꾼 다음 `Files/etc` 디렉토리에 저장합니다.
 - b. SYSLOG에 대해 xSP 표준을 준수하도록 `syslog.conf.jordan`을 수정합니다.

3. /etc/syslog.conf 파일이 xsp-firewall-hardening.driver의 JASS_FILES 정의에 나열되는지 확인합니다.

기본적으로 xsp-firewall-hardening.driver의 수정된 JASS_FILE 정의는 다음과 같이 나타납니다.

코드 예 7-8 수정된 xsp-firewall-hardening.driver의 출력 예제

```
JASS_FILES="
                /etc/dt/config/Xaccess
                /etc/init.d/inetsvc
                /etc/init.d/nddconfig
                /etc/init.d/set-tmp-permissions
                /etc/issue
                /etc/motd
                /etc/notrouter
                /etc/rc2.d/S00set-tmp-permissions
                /etc/rc2.d/S07set-tmp-permissions
                /etc/rc2.d/S70nddconfig
                /etc/syslog.conf
"
```

이제 모든 필수 수정사항이 만들어졌습니다. OS의 설치, 최소화 및 강화는 특정 응용 프로그램에 맞게 사용자 정의되고 완전히 자동화되었습니다. 완전히 자동화되지 않은 유일한 프로세스는 방화벽 소프트웨어와 Solstice DiskSuite의 구성 및 설치입니다. JumpStart 기술을 사용하여 이러한 구성을 수행할 수도 있지만, 이 책에서는 다루지 않습니다. Sun BluePrints 설명서 JumpStart Technology: Effective Use in the Solaris Operating Environment를 참조하십시오.

클라이언트 설치

드라이버에 대한 모든 수정사항을 작성한 뒤 이 절에서 설명한 것처럼 클라이언트를 설치하십시오.

▼ 클라이언트 설치

1. 드라이버에 대한 모든 필수 수정사항을 작성한 후, **JumpStart** 기반구조를 사용하여 클라이언트를 설치합니다.

클라이언트의 `ok` 프롬프트에서 다음 명령을 사용합니다.

```
ok> boot net - install
```

2. 오류가 발생하는 경우 오류를 수정하고 클라이언트 **OS**를 다시 설치합니다.

품질 보증 검사

프로세스의 마지막 작업은 시스템이 제공하는 응용프로그램 및 서비스가 올바르게 기능하고 있는지 확인하는 것입니다. 또한, 이 작업은 보안 프로파일이 필수 수정사항을 성공적으로 이행하고 있는지 확인합니다.

모든 이상 징후나 문제점이 감지되고 신속히 정정되도록 하려면, 강화 및 최소화된 플랫폼을 재부팅한 다음 이 작업을 신속하고 꼼꼼하게 수행해야 합니다. 이 프로세스는 프로파일 설치 확인 및 응용 프로그램과 서비스 기능성 확인의 두 작업으로 구분됩니다.

▼ 프로파일 설치 확인

Solaris Security Toolkit 소프트웨어가 보안 프로파일을 오류 없이 올바르게 설치했는지 확인하기 위해 다음을 검토하고 평가하십시오.

1. 설치 로그 파일을 검토합니다.

이 파일은 `JASS_REPOSITORY/jass-install-log.txt`에 설치됩니다.

참고 – 이 로그 파일은 Solaris Security Toolkit 소프트웨어가 시스템에 수행한 작업을 이해하기 위한 참조로서 사용될 수 있습니다. 각 시스템에 대한 실행의 시작 시간을 기초로 새 로그 파일이 디렉토리에 저장됩니다. 이들 파일과 `JASS_REPOSITORY` 디렉토리의 다른 모든 파일은 절대 직접 수정해서는 안됩니다.

2. 감사 옵션을 사용하여 시스템의 보안 구성을 평가합니다.

감사 옵션에 대한 자세한 정보는 6 장을 참조하십시오. 이 시나리오의 경우, 클라이언트에서 Solaris Security Toolkit 소프트웨어가 설치된 디렉토리에서 다음 명령을 사용합니다.

코드 예 7-9 보안 구성 평가

```
# ./jass-execute -a xsp-firewall-secure.driver
[NOTE] Executing driver, xsp-firewall-secure.driver
=====
xsp-firewall-secure.driver: Driver started.
=====

=====
Solaris Security Toolkit Version: 4.2.0
[...]
```

Solaris Security Toolkit 검증 실행시 불일치가 발견되면, 해당 불일치는 기록됩니다. 실행 완료시 발견된 총 불일치 수가 요약에서 보고됩니다. 실행의 전체 출력은 JASS_REPOSITORY 디렉토리에 있습니다.

▼ 응용 프로그램 및 서비스 기능 확인

응용 프로그램 및 서비스에 대한 확인 프로세스에는 잘 정의된 테스트 및 허용 계획의 실행이 포함됩니다. 이 계획은 시스템 또는 응용 프로그램의 다양한 구성요소를 조사하여 구성요소가 사용 가능한 상태 및 작업 명령 상태에 있는지 판별하는데 사용됩니다. 이러한 계획을 사용할 수 없는 경우, 시스템의 사용 방법을 기초로 시스템을 합리적으로 검사하십시오. 강화 프로세스는 해당 기능을 수행하기 위해 응용 프로그램 및 서비스 기능에 영향을 미치지 않음을 확인하는 것이 중요합니다.

1. 시스템이 강화된 후 응용 프로그램이나 서비스가 제대로 작동하지 않음을 발견하는 경우 2 장에 설명된 기법을 사용하여 문제점을 판별하십시오.

예를 들어, `truss` 명령을 사용하십시오. 이 명령은 응용 프로그램에 문제가 발생하는 지점을 결정하는데 사용될 수 있습니다. 이 지점을 찾으려면 이 문제에 대해 Solaris Security Toolkit 소프트웨어로 작업한 변경사항을 다시 추적할 수 있습니다.

참고 – Solaris Security Toolkit 소프트웨어를 전개한 여러 사용자의 경험을 토대로 이 설명서에 나오는 접근 방식을 사용하면 대다수의 문제점을 해결할 수 있습니다.

2. 유사한 방법으로 **Check PointFirewall-1 NG** 소프트웨어를 검사하고, **Solaris Security Toolkit** 소프트웨어 수정으로 인한 모든 문제점을 다시 추적하고, 문제를 정정합니다.

3. 패키지의 최종 목록에 수정이 필요한 경우, 프로파일을 수정하고 시스템을 다시 설치한 후 검사를 반복하십시오.

용어

본 목록은 Solaris Security Toolkit에 나오는 축약어 및 두문자어를 정의합니다.

A

- ab2 AnswerBook2
- ABI 응용프로그램 이진 인터페이스
- ARP 주소 결정 프로토콜
- ASPPP 비동기식 점대점 프로토콜

B

- BART 기본 감사 및 보고 도구
- BIND 버클리 인터넷 네임 도메인
- BSD 캘리포니아 대학교 버클리 분교에서 개발한 유닉스(UNIX) 시스템 버전
- BSM 기본 보안 모델(*Solaris*)

C

- CD 콤팩트 디스크

CD-ROM 콤팩트 디스크 - 읽기 전용 메모리
CDE 공통 데스크탑 환경
cp(1) 파일 복사 명령
cron(1M) 클럭 데몬 명령

D

DHCP 동적 호스트 구성 프로토콜
DMI 데스크탑 관리 인터페이스
DMTF 분산 관리 작업 단체
DNS 도메인 네임 시스템

E

EEPROM 전자식 소거 및 프로그램 가능 읽기용 메모리

F

FACE 프레임 액세스 명령 환경
FMRI 결함 관리 자원 식별자
FTP 파일 전송 프로토콜

G

GID 그룹 식별자
GUI 그래픽 사용자 인터페이스

H

- HSFS** 고급 Sierra 파일 시스템
- HTTP** 하이퍼텍스트 전송 프로토콜

I

- ID** ID
- IETF** 인터넷 엔지니어링 태스크 포스
- INETD** 인터넷 서비스 데몬
 - IP** 인터넷 프로토콜
 - IPF** 인터넷 프로토콜 필터
- ISA** 명령어 집합 아키텍처

J

- JASS** JumpStart 구조 및 보안 스크립트, 현재의 경우 Solaris Security Toolkit

K

- KDC** Kerberos 키 배포

L

- LDAP** 경량 디렉토리 액세스 프로토콜
- lp(1)** 프린터 입력 명령 (프린트 요청 제출)

M

- MAN** 네트워크 관리 (*Sun Fire* 최고급 시스템 내부 *I1* 네트워크)
- MD5** 메시지 요약 5 알고리즘
- MIP** 이동식 인터넷 프로토콜
- MSP** 미드프레임 서비스 처리 장치
- mv(1)** 파일 이동 명령

N

- NFS** 네트워크 파일 시스템
- NG** 차세대
- NGZ** 비전역 영역
- NIS, NIS+** 네트워크 정보 서비스
- NP** 암호 없음
- NSCD** 이름 서비스 캐쉬 데몬

O

- OEM** 주문자 상표 부착 생산
- OS** 운영체제

P

- PAM** 플러그 가능한 인증 모듈
- PDF** 휴대용 문서 형식
- Perl** Practical Extraction and Report Language

PICL 플랫폼 정보 및 제어 라이브러리
PPP 점대점 프로토콜
PROM 프로그램 가능한 읽기 전용 메모리

Q

QA 품질 보증

R

RBAC 역할 기반 액세스 제어
rc 실행 제어 (파일 또는 스크립트)
rlogin(1) 원격 로그인 명령
RFC 원격 기능 호출
RPC 원격 절차 호출
rsh(1) 원격 셸 명령

S

SA 시스템 관리자
SC 시스템 제어 (*Sun Fire* 고급 및 중급 시스템)
scp(1) 보안 복사(원격 파일 복사 프로그램)
SCCS 원시 코드 제어 시스템
SLP 서비스 지역 프로토콜
SMA 시스템 관리 에이전트
SMC Solaris 관리 콘솔
SMF 서비스 관리 기능
SMS 시스템 관리 서비스

SNMP	간이 망 관리 프로토콜
SP	서비스 제공자
SPARC	스파크
SPC	SunSoft Print Client
SSH	Secure Shell (Solaris 9 및 10 OS)
SVM	Solaris Volume Manager

T

TCP	전송 제어 프로토콜
tftp(1)	단순 파일 전송 프로그램
ttl	time-to-live

U

UDP	사용자 다이어그램 프로토콜
UFS	Unix 파일 시스템
UID	사용자 식별자
UUCP	UNIX 시스템간 복사

V

VOLD	볼륨 관리 데몬
-------------	----------

W

WBEM 웹 기반 기업 관리

색인

심볼

/usr/bin/ldd 명령, 21

A

add_install_client 명령, 82

add_to_manifest 기능, 65

add-client 스크립트, 3, 82

B

-b 옵션, 실행 취소, 68

backup_file 지원 프로그램 기능, 66

Basic Security Module(BSM), 44

BSM, 44

C

Check Point Firewall-1 NG, 101

core.profile, 80

cp 명령, 66

cron 작업

 감사 실행, 86

 정숙 출력 옵션 사용, 69

D

-d 드라이버 옵션 제한사항, 55

Developer Solaris OE 클러스터, SUNWCprog, 81

developer.profile, 81

DNS 서비스, 24

documentation 디렉토리, 5

driver 디렉토리, 5

driver.init 파일

 개요, 6

drivers 디렉토리, 5

dtexec 프로세스, 28

E

End User Solaris OE 클러스터, SUNWCuser, 81

end-user.profile, 81

Entire Distribution Solaris OE 클러스터,

 SUNWCall, 81

entire-distribution.profile, 81

F

-f 옵션, 실행 취소, 68

files 디렉토리, 8

finish 디렉토리, 9

finish.init 파일

 드라이버 플로우, 6

FixModes

FixModes.tar.z 파일, 44
소프트웨어, 다운로드, 43

FTP

기본 구성, 20
서비스, 사용 가능성, 사례 시나리오, 112

J

JASS, 1

JASS_DISPLAY_HOSTNAME 변수, 95
JASS_DISPLAY_SCRIPTNAME 변수, 95
JASS_DISPLAY_TIMESTAMP 변수, 95
JASS_HOME_DIR 환경 변수, 정의, 41
JASS_LOG_BANNER 환경 변수, 92, 93
JASS_LOG_ERROR 환경 변수, 93
JASS_LOG_FAILURE 환경 변수, 93
JASS_LOG_SUCCESS 환경 변수, 93
JASS_LOG_WARNING 환경 변수, 93
JASS_REPOSITORY
내용 검토, 66
내용 수정, 63
실행 취소 작업, 63

jass-check-sum 명령, 66
jass-check-sum 프로그램, 4
jass-execute -a 명령, 98
jass-execute -a 명령 옵션, 89
jass-execute -u 명령, 67
jass-execute 명령 옵션, 50
jass-manifest.txt 파일, 64
jass-undo-log.txt 파일, 71

JumpStart Architecture and Security
Scripts(JASS), 1

JumpStart 구조, Solaris Security Toolkit 통합, 78

JumpStart 기술, 37, 77

JumpStart 기술, 지원되는 OS 버전, 77

JumpStart 모드

sysidcfg 수정, 78
sysidcfg 파일 구문 분석 중 오류, 80
구성, 37, 78
모든 스크립트 사용, 79
선택된 스크립트 사용, 79

설치, sysidcfg 디렉토리, 11

JumpStart 서버

구성 및 관리, 77
구성, 사례 시나리오, 107
멀티홈, 79

JumpStart 클라이언트

구축되지 않음, 사례 시나리오, 110
추가, 사례 시나리오, 107
클라이언트 설치, 사례 시나리오, 116
파일, 저장, 8

JumpStart 클라이언트 추가, 사례 시나리오, 107

JumpStart 프로파일, 80

디렉토리, 11
템플릿, 80

K

-k 옵션, 실행 취소, 68

Kerberos, 20

kill 명령, 26

L

LDAP, 24

ldd 명령, 27

librpcsvc.so.1 항목, 27

list open files 프로그램, 28

lsof 프로그램, 28

lsof 프로그램, 확보, 28

M

-m 옵션

감사, 90
실행 취소, 69

make-jass-pkg 프로그램, 4

man 디렉토리, 5

MD5 소프트웨어

md5.tar.z 파일, 46
다운로드, 45

MD5 이진, 46

N

netstat 명령, 27

NFS

의존하는 응용 프로그램, 27

NIS, 24

O

-o 옵션, 감사, 91

-o 옵션, 실행 취소, 69

OEM Solaris OE 클러스터, SUNWCXall, 81

oem.profile, 81

OpenSSH

구축 및 전개, 45

소프트웨어, 다운로드, 45

컴파일, 45

OS

디렉토리, 10

OS 이미지, 10

OS 클러스터 지정 및 설치, 사례 시나리오, 106

OS 클러스터, 지정 및 설치, 사례 시나리오, 106

P

packages 디렉토리, 10

pfiles 명령, 28

pkgadd 명령, 41

pkill 명령, 26

pldd 명령, 22

ps 명령, 26

Q

-q 옵션, 감사, 91

-q 옵션, 실행 취소, 69

R

rc 스크립트, 감사 실행, 86

Recommended and Security Patch Clusters

다운로드, 42

저장, 11

reverse-jass-manifest.txt 파일, 64

rm_install_client 명령, 84

rm-client 스크립트, 4, 84

RPC

rpcinfo 명령, 25, 26

서비스, 112

포트 매핑 프로그램, 25

rules 파일

JumpStart 서버, 79, 82

검사, 사례 시나리오, 109

rusers 명령, 25

rusers 서비스, 검증, 26

S

SCCS, 12

scp 명령, 42

Secure Shell

구축 및 전개, 45

상업용 버전, 컴파일, 45

설치, 사례 시나리오, 113

소프트웨어, 다운로드, 44

제품 요구사항, 40

secure.driver, 실행, 51

SI_CONFIG_DIR, 하위 디렉토리에 소프트웨어 설치, 79

SIGHUP 신호, 26

SNMP, 27

Solaris Fingerprint Database Companion, 46

Solaris Fingerprint Database Sidekick, 46

Solaris OS

서비스, 점검, 59

수정사항, 42

이름 지정 표준, 10

이미지, 10

클러스터, SUNWCreg, 80

패키지 형식, 40

Solaris Security Toolkit

JumpStart 모드용 설치, 79

소프트웨어, 다운로드, 40

- Solaris Security Toolkit 실행, 48
- Solaris 지문 데이터베이스, 46
- Solstice DiskSuite, 103
- Source Code Control System(SCCS), 12
- sun4u, 45
- SunSolve OnLine 웹 사이트, 42
- SUNWjass 디렉토리, 41
- SUNWjass-*n.n*.pkg, 41
- sysidcfg
 - 디렉토리, 11
 - 파일, 80
 - 파일 예제, 12
 - 파일, JumpStart 모드용 수정, 78
 - 파일, 버전 제한, 78
- syslog
 - syslog.conf 파일, 사용자 정의, 115
 - 메시지, 로깅, 33
 - 저장소, 33

T

- TCP 랩퍼, 114
- truss 명령, 22, 32
- ttssession 프로세스, 28

U

- uncompress 명령, 41
- undo-log.txt 파일, 64
- user.init 파일, 6
- user.init.SAMPLE, 목적, 15
- user.run.SAMPLE, 목적, 15

W

- warm-brick, 111

ㄱ

- 가장 최근 실행 옵션, 56

- 가정 및 제한사항, 사례 시나리오, 102

감사

- 결과 표시, 91
- 로그 항목, 예제, 95
- 메시지, 92
- 명령, 88
- 배너, 92
- 백업, 주의, 97
- 보고서 구성, 95
- 보안 평가, 96
- 사례 시나리오, 118
- 사용자 정의, 86
- 소형 스캔, 86
- 실패만 보고, 93
- 옵션, 88
- 자동화, 85
- 전자 우편 옵션, 90
- 정숙 옵션, 91
- 주기적, 86
- 출력 옵션, 91
- 출력 정렬, 95
- 출력 제어, 88
- 프로세스, 99
- 호스트 이름, 스크립트 이름 및 시간 소인 정보, 95

감사 스크립트

- 대응하는 드라이버, 65
- 독점적, 87
- 디렉토리, 4
- 사용자 정의, 87

감사 옵션, 52

감사 전략, 33

감사 출력 정렬, 95

감사, 정의, 85

감사, 한계, 2

강력한 인증, 44

강제 옵션, 68

강화 작업

- Solaris Security Toolkit 실행, 47

- 변경 취소, 70

- 실행 취소 목록, 71

개인 관리 네트워크, 111

검사

- 실패, 95

- 추가, 87
- 검증
 - 기능성, 여러 번의 재부트, 18
 - 보안 프로파일 설치, 31
 - 시스템 안정성, 30
 - 응용 프로그램 및 서비스 기능성, 31
- 검증 프로세스, 24
- 검증, 설치 전, 30
- 결과 문서화, 24
- 결과, 문서화, 24
- 결합, 31
- 경고 메시지
 - Solaris Security Toolkit 소프트웨어 실행, 43
 - 시스템 시동 또는 응용 프로그램 시작 시에 표시, 30
- 계속 사용 가능할 OS 서비스 판별, 59
- 계획 단계, 17
- 계획 및 준비, 사례 시나리오, 101
- 계획, 설치, 36
- 고장, 32
- 공유 라이브러리, 21
- 관련 자원, xviii
- 관리 소프트웨어, 목록 작성, 21
- 관리 프로토콜, 방침 예, 19
- 구성
 - JumpStart 모드, 78
 - JumpStart 서버, 77
 - JumpStart 서버, 사례 시나리오, 107
 - 감사, 86
 - 감사 보고, 95
 - 검토 지침, 60
 - 모니터링 및 유지보수, 33
 - 보안 평가, 60
 - 사용자 정의, 사례 시나리오, 102, 111
 - 스크립트, 11
 - 실행 중인 구성 대 저장된 구성의 차이, 31
 - 자동화, 2
 - 정보, 드라이버, 5
 - 지침, 2
 - 평가, 사례 시나리오, 118
 - 환경 구성, 35
- 구성 파일

- JumpStart 프로파일, 11
- 기본, 6
- 사용 증인지 판별, 24
- 조사, 99
- 구조, Solaris Security Toolkit 소프트웨어, 4
- 구조, 소프트웨어, 3
- 권한 관리, 19
- 권한, 보호, 43
- 기능성
 - 문제점, 18
 - 추가, 87
 - 테스트, 31
 - 패치, 42
- 기능성 테스트, 31
- 기반구조, 17
- 기반구조 구성요소, 21
- 기반구조, 준비, 사례 시나리오, 107
- 기본값
 - 구성, FTP 및 Telnet, 20
 - 보안 프로파일, 33

L

- 내역 옵션, 56
- 내포 또는 계층 구조 보안 프로파일, 29
- 네트워크 액세스, 보호, 44
- 느린 네트워크 연결, 정숙 출력 사용, 69

□

- 더욱 강력한 인증, 20
- 데몬, 사용 불가, 44
- 데이터 무결성, 19
- 도구, 선택적, 47
- 도움말 표시 옵션, 53
- 도움말 표시 옵션, 감사, 89
- 독립형 모드, 37
 - 사용, 50
 - 실행, 51
- 독립형 모드에서 소프트웨어 실행, 51

- 독점적 드라이버 및 스크립트, 87
- 동적으로 로드된 응용 프로그램 식별, 23
- 드라이버
 - 구성 정보, 5
 - 디렉토리, 5
 - 이름 지정, 14
- 드라이버 옵션, 54
- 드라이버 제어 흐름, 6
- 드라이버, JumpStart 서버, 79
- 디렉토리
 - JumpStart 프로파일, 11
 - man, 5
 - OS, 10
 - sysidcfg, 11
 - 감사 스크립트, 4
 - 구조, 4
 - 드라이버, 5
 - 목록, 4
 - 소프트웨어 패키지, 10
 - 시작, 8
 - 작업, 63
 - 종료 스크립트, 9
 - 파일, 8
 - 패치, 11
- 디버깅 서비스, 27
- 디지털 지문, 45

ㄹ

- 라이브러리, 공유, 21
- 로그 파일
 - 검토, 31
 - 설치, 31
- 로그 파일 검토, 31
- 로깅
 - 고려, 17
 - 조작, 63
- 루트
 - 디렉토리, 41
 - 옵션, 57

ㅁ

- 멀티홈 JumpStart 서버, 79
- 메시지, 감사, 92
- 메타서비스, 24
- 명령줄 옵션
 - jass-execute 명령, 49
 - 가장 최근 실행, 56
 - 감사, 52, 88
 - 감사, 도움말, 89
 - 내역, 56
 - 도움말, 53
 - 드라이버, 54
 - 루트, 57
 - 실행 취소, 58, 67
 - 전자 우편 통지, 55
 - 정숙, 57
 - 출력 파일, 57
- 모니터링 소프트웨어, 목록 작성, 21
- 모드, 37
- 모순, 찾기, 59
- 목록 파일, 64
- 목록 파일 항목
 - 복수 처리, 72
- 무결성
 - 데이터, 19
 - 소프트웨어 다운로드, 47
 - 실행 파일, 검증, 46
 - 이진, 점검, 45
 - 파일 시스템, 19
- 무결성 관리 솔루션, 12
- 문제 해결, 18
 - 시스템 수정, 59
 - 실행 취소 작업, 66

ㅂ

- 반환값, 23
- 방법론, 시스템 보안, 17
- 백도어 액세스, 이진, 45
- 백업
 - 감사, 97
 - 설치 전, 30

- 작업 실행 취소 전 요구사항, 70
- 백업 소프트웨어, 목록 작성, 21
- 백업 파일
 - 기본 조치, 65
- 버그 수정사항, 패치, 42
- 버전 제어, 12
- 버전 제어 유지, 12
- 변경 제어 방침, 31
- 변경 추적, 63
- 변경 취소, 64
- 보고서, 전자 우편 통지, 69
- 보안
 - 요구사항, 17
 - 구성, 평가, 32
 - 모니터링, 33
 - 방침
 - 개발, 19
 - 검토, 19
 - 표준, 17
 - 상태
 - 감사, 86
 - 검토, 86
 - 상태 검토, 86
 - 소프트웨어 다운로드, 40
 - 소프트웨어, 다운로드, 40
 - 유지, 32, 85
 - 평가
 - 구성, 60
 - 수행, 96
 - 프로파일
 - 검증, 60
 - 기본값, 33
 - 내포 또는 계층 구조, 29
 - 설치 확인, 사례 시나리오, 117
 - 작성, 사례 시나리오, 103
 - 템플릿, 87
 - 프로파일 검증, 60, 85
 - 프로파일 작성, 사례 시나리오, 103
 - 모니터링, 33
 - 유지, 32, 85
 - 보존 옵션, 68

- 부당하게 이용된 시스템, 19

人

- 사례 시나리오, 101
- 사용 감사, 17
- 사용 권한
 - 오브젝트. 기본값, 43
- 사용자 대화식 서비스, 사용 불가, 44
- 사용자 대화식 세션, 보호, 44
- 사용자 정의
 - Solaris Security Toolkit, 13
 - syslog.conf 파일, 115
 - 방침 및 요구사항, 13
 - 보안 감사, 86
 - 지침, 14
- 사용자 정의 구성, 사례 시나리오, 102
- 사이트 특정 드라이버, 대응하는 감사 스크립트, 87
- 상세 레벨, 91
- 서비스
 - RPC, 112
 - 목록 작성, 20
 - 식별, 18
 - 요구사항, 18
 - 제한, 112
 - 최근에 사용된, 판별, 27
 - 취소, 중지 또는 실패, 25
 - 필수인지 판별, 27
- 서비스 요구사항, 판별, 21
- 서비스 제한, 112
- 서비스 프레임워크, 24
- 설계, Solaris Security Toolkit 소프트웨어, 1
- 설치
 - Solaris OS 자동화, 11
 - 검증, 30
 - 계획, 36
 - 로그 파일, 31
 - 백업, 30
 - 새 시스템, 사례 시나리오, 101
 - 설치 전 작업, 30
 - 소프트웨어, 29
 - 소프트웨어, 사례 시나리오, 104

- 시스템 강화, 36
- 자동화, 2, 77
- 지침, 2
- 클라이언트, 사례 시나리오, 116
- 패치, 11
- 패치 자동화, 11
- 표준화, 77
- 후 감사, 96
- 설치 전 작업, 30
- 성능
 - Solaris OS 패치, 42
- 소프트웨어 구성요소, 3
- 소프트웨어 설치, 스크립트, 11
- 소프트웨어 패키지
 - pkg 형식이 아닌 패키지 추가, 65
 - 디렉토리, 10
- 손상된 내용, 파일, 63, 65
- 수동 검토, 보안, 32
- 수동 변경, 실행 취소 중 보존, 68
- 수명, 보안 유지, 61
- 수정
 - 코드, 13
 - 프로파일 파일, 80
- 수정사항, 검증, 59
- 수정사항, 추적, 63
- 스크립트
 - 목록, 5
 - 수정, 주의, 79
 - 이름 지정, 14
- 시간 초과, 프로그램, 26
- 시나리오, 시스템 보안, 101
- 시스템
 - 구성, 모니터링 및 유지보수, 33
 - 상태, 21
 - 손상, 63, 65
 - 시동, 메시지, 30
 - 안정성, 검증, 30
 - 요구사항, 사례 시나리오, 103
 - 이진, 검증, 47
 - 취약점, 32
 - 호출, 23
- 시스템 감사, 85

- 시스템 보안, 방법론, 17
- 시스템 설치 표준화, 77
- 시스템 전개, 77
- 시스템 평가, 86
- 시스템의 신속한 강화, 37
- 시작 디렉토리, 8
- 실패, 응용 프로그램, 31
- 실패한 검사, 95
- 실행 취소
 - 강제 옵션, 68
 - 대화식 실행, 67
 - 명령줄 옵션, 58
 - 백업 옵션, 68
 - 변경 로깅 및 역전, 64
 - 보존 옵션, 68
 - 사용 불가능, 65
 - 사용에 필요한 정보, 64
 - 수동으로 변경사항 실행 취소, 66
 - 옵션, 67
 - 작업 선택, 예제 출력, 71
 - 작업 실행 취소, 70
 - 작업, 목록, 71
 - 전자 우편 옵션, 69
 - 정숙 옵션, 69
 - 제한, 64
 - 출력 옵션, 69
 - 한계, 64

O

- 안정성, 42
- 암호
 - passwd(1) 명령, 20
 - 방침 예, 20
- 암호화, 20
- 암호화 소프트웨어, 44
- 액세스 권한, 보호, 43
- 예기치 않은 작동, 25
- 예방 조치, 18
- 예제, 프로파일 파일, 80
- 오류
 - sysidcfg 파일 구문 분석 중, JumpStart 모드, 80

- 메시지 또는 경고, 30
- 손상된 내용, 63, 65
- 시스템 손상, 63, 65
- 오프라인, 시스템 보안, 18
- 옵션
 - jass-execute 명령, 49
 - 가장 최근 실행, 56
 - 감사, 52, 88
 - 감사, 도움말, 89
 - 내역, 56
 - 도움말, 53
 - 드라이버, 54
 - 루트, 57
 - 백업, 실행 취소, 68
 - 실행 취소 명령, 67
 - 전자 우편 통지, 55
 - 전자 우편, 감사, 90
 - 전자 우편, 실행 취소, 69
 - 정숙, 57
 - 정숙, 감사, 91
 - 정숙, 실행 취소, 69
 - 출력 파일, 57
- 요구사항
 - 강화 작업 실행 취소, 64
 - 보안, 19
 - 서비스, 18
 - 서비스, 판별, 21
 - 수집, 23
 - 응용 프로그램, 18
- 용도, Solaris Security Toolkit 소프트웨어, 1
- 원본 파일 변경, 14
- 위험 및 수익, 고려, 18
- 유지보수 창, 18
- 응용 프로그램
 - RPC 포트 매핑 프로그램이 사용중인지 판별, 25
 - 동적으로 로드된 식별, 23
 - 식별, 18
 - 요구사항, 18
 - 확인, 사례 시나리오, 117
- 응용 프로그램 보안, 19
- 응용 프로그램 시작, 메시지, 30
- 응용 프로그램
 - 목록 작성, 20
 - 이더넷 인터페이스, 사례 시나리오, 103
 - 이름 지정 서비스, 24
 - 이름 지정 표준
 - Solaris OS, 10
 - 사용자 정의 파일, 14
 - 설치, 10
 - 이진, 검증, 47
 - 인증
 - 강력한, 44
 - 더욱 강력한, 20
 - 서비스, 24
 - 일치하지 않는 상태, 69
- ㅈ
 - 자동 감사, 85
 - 작동 또는 관리 기능, 목록 작성, 20
 - 작업 디렉토리, 63
 - 재부트, 시스템 보안, 18
 - 저장된 상태, 99
 - 전개된 시스템
 - 보안, 18
 - 소프트웨어 설치, 29
 - 전개된 시스템 보안, 18
 - 전자 우편 통지 옵션, 55
 - 정보 수집, 실행 중 프로세스, 22
 - 정숙 옵션, 57
 - 정지 시간, 18
 - 종료 스크립트
 - 신규 작성, 65
 - 실행 취소 기능, 65
 - 종속성
 - 식별되지 않은, 18
 - 판별, 28
 - 주기적 감사, 86
 - 주석 처리기, 115
 - 주석 표시(#), 26
 - 주의사항, 실행 취소 중 생성, 68
 - 중앙 집중된 syslog 저장소, 33
 - 지원 프로그램 기능, 65

ㄸ

- 책임, 17
- 체크섬, 66
- 최소화 및 보안된 시스템 전개, 101
- 최소화, Solaris 운영체제, 20
- 출력
 - 감사 정렬, 95
 - 사용 불가, 57
 - 예제 감사 실행, 98
 - 최소화, 93
- 출력 옵션
 - 감사, 91
 - 실행 취소, 69
 - 파일, 57
- 출력 최소화, 93
- 취약점
 - 값, 정의, 99
 - 검색, 19
 - 분석, 19
 - 전략, 33
- 침입 보호, 19

ㅋ

- 컴파일러 제한, 45
- 컴파일러, 설치 경고, 45
- 컴파일러, 제한, 45
- 클라이언트
 - JumpStart 서버에서 제거, 84
 - JumpStart 서버에서 추가, 82
- 클라이언트 제거, JumpStart 서버로부터, 84
- 클라이언트 추가, JumpStart 서버로부터, 82
- 클라이언트가 구축되지 않음, 사례 시나리오, 110

ㅌ

- 테스트 및 승인 계획, 32
- 테스트, 비생산 시스템에서, 42
- 텔넷, 사용 가능, 88
- 템플릿, 프로파일 파일, 80
- 트로이, 정의, 45

ㅍ

파일

- JumpStart 클라이언트, 저장, 8
- 디렉토리, 8
- 변경 나열 및 검토, 66
- 사용 판별, 28
- 손상된 내용, 63, 65
- 수동으로 변경된 파일 검토, 66
- 수정, 14
- 이름 지정 표준, 14
- 일치하지 않는, 69
- 프로파일, 80
- 파일 시스템
 - 무결성, 19
- 파일 시스템 개체
 - 정보 획득, 21
- 파일 예제, sysidcfg, 12
- 파일 이름, 41
- 파일 이름 지정, 표준, 14
- 파일 체크섬, 66
- 패치, 42
 - README 파일, 42
 - 구성 파일 겹쳐 쓰기, 32
 - 디렉토리, 11
 - 디렉토리 이름 지정, 11
 - 설치, 11
 - 설치 후 시스템 재강화, 37
 - 설치되지 않은 패치 추가, 87
 - 압축 풀기, 11
 - 파일 이동, 42
 - 하위 디렉토리 만들기, 11
- 패치 압축 풀기, 11
- 패치 적용, 32
- 패치 파일 이동, 42
- 패키지 이름, 사례 시나리오, 114
- 패키지, pkg 형식이 아닌 패키지 추가, 65
- 포트, 사용 판별, 28
- 표준, 보안 방침, 19
- 표준, 플랫폼에 대해 집행, 29
- 품질 보장(QA) 테스트, 59
- 프레임워크, Solaris Security Toolkit 사용자 정의, 65
- 프레임워크, 서비스, 24

프로세스
 ID, 23
 파일 및 포트를 사용 중인 것 판별, 28

프로파일
 JumpStart, 11, 80
 계획 및 준비, 17
 디렉토리, 11
 수정, 80
플랫폼 최소화, 23
필수 소프트웨어, 40

응
핵심 구성요소, 1
핵심 환경 변수, 29
호스트 기반 액세스 제어, 19
확장, 20
환경 변수
 가져오기, 7
환경, 구성, 36

