Trusted Extensions 관리자 절차

부품 번호: E38867
2013년 1월

ORACLE

130221@25097

목차

머리말 17

1 Trusted Extensions 관리 개념 23
Trusted Extensions 소프트웨어 및 Oracle Solaris OS 23
Trusted Extensions와 Oracle Solaris OS의 유사점 23
Trusted Extensions와 Oracle Solaris OS의 차이점 24
멀티헤디드 시스템 및 Trusted Extensions 데스크탑 25
Trusted Extensions의 기본 개념 26
Trusted Extensions 보호 26
Trusted Extensions 및 액세스 제어 27
역할 및 Trusted Extensions 28
Trusted Extensions 소프트웨어의 레이블 28

2 Trusted Extensions 관리 도구 33
Trusted Extensions용 관리 도구 33
`txzonemgr` 스크립트 35
Trusted CDE 작업 35
장치 할당 관리자 37
Solaris Management Console 도구 38
Solaris Management Console의 Trusted Extensions 도구 39
Solaris Management Console에서 클라이언트와 서버 간 통신 41
Solaris Management Console 설명서 42
Trusted Extensions의 레이블 구축기 43
Trusted Extensions의 명령줄 도구 44
Trusted Extensions에서 원격 관리 46

3 Trusted Extensions 관리자로 시작하기(작업) 47
Trusted Extensions의 새로운 기능 47
Trusted Extensions 관리 시 보안 요구 사항 48
Trusted Extensions에서 역할 만들기 49
Trusted Extensions에서 역할 맡기 49
Trusted Extensions 관리자로 시작하기(작업 맵) 49
▼ Trusted Extensions에서 전역 영역으로 들어가는 방법 51
▼ Trusted Extensions에서 전역 영역을 종료하는 방법 52
▼ Solaris Management Console에서 로컬 시스템을 관리하는 방법 52
▼ Trusted Extensions에서 CDE 관리 작업을 시작하는 방법 54
▼ Trusted Extensions에서 관리 파일을 편집하는 방법 54

4 Trusted Extensions 시스템의 보안 요구 사항(개요) 57
구성 가능한 Oracle Solaris 보안 기능 57
Trusted Extensions의 보안 기능 구성 인터페이스 57
Trusted Extensions를 통해 Oracle Solaris 보안 방식 확장 58
Trusted Extensions 보안 기능 58
보안 요구 사항 적용 59
사용자 및 보안 요구 사항 59
전자 메일 사용 59
암호 적용 60
정보 보호 60
암호 보호 61
그룹 관리 61
사용자 삭제 방법 61
데이터에 대한 보안 레벨 변경 규칙 62
`sel_config` 파일 64
Solaris Trusted Extensions(CDE) 사용자 정의 64
Front Panel(전면 패널) 사용자 정의 64
Workspace(작업 공간) 메뉴 사용자 정의 65

5 Trusted Extensions의 보안 요구 사항 관리(작업) 67
Trusted Extensions의 일반 작업(작업 맵) 67
▼ 선택한 편집기를 신뢰할 수 있는 편집기로 지정하는 방법 68
▼ root 암호를 변경하는 방법 69

▼ 데스크탑의 현재 포커스에 대한 컨트롤을 다시 얻는 방법 70
▼ 레이블에 해당하는 16진수를 얻는 방법 71
▼ 읽기 가능한 레이블을 해당 16진수 형식에서 얻는 방법 72
▼ 시스템 파일에서 보안 기본값을 변경하는 방법 73

6 Trusted Extensions의 사용자, 권한 및 역할(개요) 75
Trusted Extensions의 사용자 보안 기능 75
사용자에 대한 관리자 책임 76
사용자에 대한 시스템 관리자 책임 76
사용자에 대한 보안 관리자 책임 76
Trusted Extensions에서 사용자를 만들기 전에 결정할 사항 77
Trusted Extensions의 기본 사용자 보안 속성 77
`label_encodings` 파일 기본값 77
Trusted Extensions의 `policy.conf` 파일 기본값 78
Trusted Extensions에서 구성 가능한 사용자 속성 78
사용자에게 지정해야 하는 보안 속성 79
Trusted Extensions에서 사용자에게 보안 속성 지정 79
`.copy_files` 및 `.link_files` 파일 81

7 Trusted Extensions에서 사용자, 권한 및 역할 관리(작업) 83
보안을 위한 사용자 환경 사용자 정의(작업 맵) 83
▼ 기본 사용자 레이블 속성을 수정하는 방법 84
▼ `policy.conf` 기본값을 수정하는 방법 84
▼ Trusted Extensions에서 사용자의 시작 파일을 구성하는 방법 86
▼ Trusted Extensions에서 비상 안전 세션에 로그인하는 방법 88
Solaris Management Console에서 사용자 및 권한 관리(작업 맵) 89
▼ Solaris Management Console에서 사용자의 레이블 범위를 수정하는 방법 90
▼ 편리한 권한 부여를 위해 권한 프로파일을 만드는 방법 91
▼ 사용자의 권한 세트를 제한하는 방법 93
▼ 사용자에 대한 계정 잠금을 방지하는 방법 95
▼ 사용자가 데이터의 보안 레벨을 변경할 수 있게 하는 방법 96
▼ Trusted Extensions 시스템에서 사용자 계정을 삭제하는 방법 96
Solaris Management Console에서 기타 작업 처리(작업 맵) 97

8 Trusted Extensions에서 원격 관리(작업) 99
Trusted Extensions에서 보안 원격 관리 99
Trusted Extensions에서 원격 시스템을 관리하는 방법 100
Trusted Extensions에서 역할을 통한 원격 로그인 101
레이블이 없는 호스트에서 원격 역할 기반 관리 101
Trusted Extensions에서 원격 로그인 관리 101
원격으로 Trusted Extensions 관리(작업 맵) 102
▼ Trusted Extensions의 명령줄에서 원격으로 로그인하는 방법 103
▼ `dtappsession`을 사용하여 Trusted Extensions를 원격으로 관리하는 방법 103
▼ Trusted Extensions 시스템에서 Solaris Management Console을 사용하여 시스템을 원격으로 관리하는 방법 105
▼ 레이블이 없는 시스템에서 Solaris Management Console을 사용하여 시스템을 원격으로 관리하는 방법 106
▼ 특정 사용자가 Trusted Extensions의 전역 영역에 원격으로 로그인할 수 있게 설정하는 방법 108
▼ Xvnc를 사용하여 Trusted Extensions 시스템에 원격으로 액세스하는 방법 109

9 Trusted Extensions 및 LDAP(개요) 111
Trusted Extensions에서 이름 지정 서비스 사용 111
네트워크되지 않은 Trusted Extensions 시스템 112
Trusted Extensions LDAP 데이터베이스 112
Trusted Extensions에서 LDAP 이름 지정 서비스 사용 113

10 Trusted Extensions에서 영역 관리(작업) 117
Trusted Extensions의 영역 117
Trusted Extensions의 영역 및 IP 주소 118
영역 및 다중 레벨 포트 119
Trusted Extensions의 영역 및 ICMP 120
전역 영역 프로세스 및 레이블이 있는 영역 120
Trusted Extensions의 영역 관리 유틸리티 121
영역 관리(작업 맵) 122
▼ 준비 또는 실행 중인 영역을 표시하는 방법 123
▼ 마운트된 파일의 레이블을 표시하는 방법 124
▼ 레이블이 있는 영역에 일반적으로 표시되지 않는 파일을 루프백 마운트하는 방법 126
▼ 하위 레벨 파일의 마운트를 사용 안함으로 설정하는 방법 127

▼ 레이블이 있는 영역에서 ZFS 데이터 세트를 공유하는 방법 128
▼ 레이블이 있는 영역에서 파일의 레이블을 변경할 수 있게 설정하는 방법 130
▼ udp를 통해 NFSv3에 대한 다중 레벨 포트를 구성하는 방법 132
▼ 영역에 대한 다중 레벨 포트를 만드는 방법 132

11 Trusted Extensions에서 파일 관리 및 마운트(작업) 135
Trusted Extensions에서 파일 공유 및 마운트 135
Trusted Extensions에서 NFS 마운트 135
레이블이 있는 영역에서 파일 공유 137
Trusted Extensions에서 NFS 마운트된 디렉토리에 액세스 137
Trusted Extensions에서 홈 디렉토리 만들기 138
Trusted Extensions의 자동 마운트 변경 사항 139
Trusted Extensions 소프트웨어 및 NFS 프로토콜 버전 140
레이블이 있는 파일 백업, 공유 및 마운트(작업 맵) 141
▼ Trusted Extensions에서 파일을 백업하는 방법 142
▼ Trusted Extensions에서 파일을 복원하는 방법 142
▼ 레이블이 있는 영역에서 디렉토리를 공유하는 방법 142
▼ 레이블이 있는 영역에서 파일을 NFS 마운트하는 방법 144
▼ Trusted Extensions에서 마운트 실패 문제를 해결하는 방법 149

12 신뢰할 수 있는 네트워킹(개요) 151
신뢰할 수 있는 네트워크 151
Trusted Extensions 데이터 패킷 152
신뢰할 수 있는 네트워크 통신 152
Trusted Extensions의 네트워크 구성 데이터베이스 154
Trusted Extensions의 네트워크 명령 154
신뢰할 수 있는 네트워크 보안 속성 155
Trusted Extensions의 네트워크 보안 속성 156
보안 템플리트의 호스트 유형 및 템플리트 이름 157
보안 템플리트의 기본 레이블 158
보안 템플리트의 DOI 158
보안 템플리트의 레이블 범위 158
보안 템플리트의 보안 레이블 세트 159
신뢰할 수 있는 네트워크 폴백 방식 159
Trusted Extensions의 경로 지정 개요 161

경로 지정 배경 161
Trusted Extensions의 경로 지정 테이블 항목 161
Trusted Extensions 승인 검사 162
Trusted Extensions에서 경로 지정 관리 163
Trusted Extensions에서 라우터 선택 164
Trusted Extensions의 게이트웨이 165
Trusted Extensions의 경로 지정 명령 165

13 Trusted Extensions에서 네트워크 관리(작업) 167
신뢰할 수 있는 네트워크 관리(작업 맵) 167
신뢰할 수 있는 네트워크 데이터베이스 구성(작업 맵) 168
▼ 사이트별 보안 템플리트가 필요한지 여부를 확인하는 방법 169
▼ 신뢰할 수 있는 네트워킹 도구를 여는 방법 170
▼ 원격 호스트 템플리트를 작성하는 방법 170
▼ 시스템의 알려진 네트워크에 호스트를 추가하는 방법 175
▼ 호스트 또는 호스트 그룹에 보안 템플리트를 지정하는 방법 176
▼ 신뢰할 수 있는 네트워크에서 연결할 수 있는 호스트를 제한하는 방법 177
Trusted Extensions에서 경로 구성 및 네트워크 정보 확인(작업 맵) 181
▼ 보안 속성으로 경로를 구성하는 방법 182
▼ 신뢰할 수 있는 네트워크 데이터베이스의 구문을 확인하는 방법 183
▼ 신뢰할 수 있는 네트워크 데이터베이스 정보를 커널 캐시와 비교하는 방법 184
▼ 커널 캐시를 신뢰할 수 있는 네트워크 데이터베이스와 동기화하는 방법 185
신뢰할 수 있는 네트워크 문제 해결(작업 맵) 187
▼ 호스트의 인터페이스가 작동 중인지 확인하는 방법 187
▼ Trusted Extensions 네트워크를 디버깅하는 방법 188
▼ LDAP 서버에 대한 클라이언트 연결을 디버깅하는 방법 191

14 Trusted Extensions의 다중 레벨 메일(개요) 193
다중 레벨 메일 서비스 193
Trusted Extensions 메일 기능 193

15 레이블이 있는 인쇄 관리(작업) 195
레이블, 프린터 및 인쇄 195
Trusted Extensions에서 프린터 및 인쇄 작업 정보에 대한 액세스 제한 196

레이블이 있는 프린터 출력 196
보안 정보의 포스트스크립트 인쇄 199
Trusted Solaris 8 인쇄와 Trusted Extensions의 상호 운용성 201
Trusted Extensions 인쇄 인터페이스(참조) 202
Trusted Extensions에서 인쇄 관리(작업 맵) 203
레이블이 있는 인쇄 구성(작업 맵) 203
▼ 다중 레벨 인쇄 서버 및 해당 프린터를 구성하는 방법 204
▼ Sun Ray 클라이언트에 대해 네트워크 프린터를 구성하는 방법 206
▼ 레이블이 있는 시스템에서 계단식 인쇄를 구성하는 방법 209
▼ 영역의 단일 레이블 인쇄를 구성하는 방법 211
▼ Trusted Extensions 클라이언트가 프린터에 액세스할 수 있도록 설정하는 방법 213
▼ 프린터에 대해 제한된 레이블 범위를 구성하는 방법 215
Trusted Extensions에서 인쇄 제한 축소(작업 맵) 216
▼ 인쇄되는 출력에서 레이블을 제거하는 방법 216
▼ 레이블이 없는 인쇄 서버에 레이블을 지정하는 방법 217
▼ 모든 인쇄 작업에서 페이지 레이블을 제거하는 방법 218
▼ 특정 사용자가 페이지 레이블을 억제할 수 있도록 설정하는 방법 218
▼ 특정 사용자에 대해 배너 및 트레일러 페이지를 억제하는 방법 219
▼ Trusted Extensions에서 사용자가 포스트스크립트 파일을 인쇄할 수 있도록 설정하는 방법 219

16 Trusted Extensions의 장치(개요) 221
Trusted Extensions 소프트웨어로 장치 보호 221
장치 레이블 범위 222
장치의 레이블 범위 효과 222
장치 액세스 정책 223
Device-Clean 스크립트 223
Device Allocation Manager(장치 할당 관리자) GUI 223
Trusted Extensions에서 장치 보안 적용 225
Trusted Extensions의 장치(참조) 226

17 Trusted Extensions에 대한 장치 관리(작업) 227
Trusted Extensions에서 장치 취급(작업 맵) 227
Trusted Extensions에서 장치 사용(작업 맵) 228
Trusted Extensions에서 장치 관리(작업 맵) 228

▼ Trusted Extensions에서 장치를 구성하는 방법 229
▼ Trusted Extensions에서 장치를 해지하거나 재생 이용하는 방법 232
▼ Trusted Extensions에서 할당 불가능한 장치를 보호하는 방법 233
▼ 로그인을 위한 직렬 회선을 구성하는 방법 234
▼ Trusted CDE에서 사용할 오디오 플레이어 프로그램을 구성하는 방법 235
▼ 장치 할당 후 File Manager(파일 관리자)가 표시되지 않게 하는 방법 236
▼ Trusted Extensions에서 Device_Clean 스크립트를 추가하는 방법 237
Trusted Extensions에서 장치 권한 부여 사용자 정의(작업 맵) 237
▼ 새 장치 권한 부여를 만드는 방법 238
▼ Trusted Extensions에서 장치에 사이트별 권한 부여를 추가하는 방법 241
▼ 장치 권한 부여를 지정하는 방법 241

18 Trusted Extensions 감사(개요) 243
Trusted Extensions와 감사 243
Trusted Extensions에서 역할로 감사 관리 244
감사 관리를 위한 역할 설정 244
Trusted Extensions의 감사 작업 244
보안 관리자의 감사 작업 245
시스템 관리자의 감사 작업 245
Trusted Extensions 감사 참조 246
Trusted Extensions 감사 클래스 247
Trusted Extensions 감사 이벤트 247
Trusted Extensions 감사 토큰 248
Trusted Extensions 감사 정책 옵션 253
Trusted Extensions의 감사 명령에 대한 확장 253

19 Trusted Extensions에서 소프트웨어 관리(작업) 255
Trusted Extensions에 소프트웨어 추가 255
Oracle Solaris의 소프트웨어 보안 방식 256
소프트웨어의 보안 평가 257
윈도우 시스템의 신뢰할 수 있는 프로세스 259
Trusted CDE 작업 추가 259
Trusted Extensions에서 소프트웨어 관리(작업) 260
▼ Trusted Extensions에서 소프트웨어 패키지를 추가하는 방법 260
▼ Trusted Extensions에서 Java 아카이브 파일을 설치하는 방법 261

A Trusted Extensions 관리에 대한 빠른 참조 263
Trusted Extensions의 관리 인터페이스 263
Trusted Extensions에서 확장된 Oracle Solaris 인터페이스 265
Trusted Extensions의 강화된 보안 기본값 266
Trusted Extensions의 제한된 옵션 266

B Trusted Extensions 매뉴얼 페이지 목록 269
Trusted Extensions 매뉴얼 페이지(사전순) 269
Trusted Extensions에서 수정된 Oracle Solaris 매뉴얼 페이지 272

색인 275

그림

그림 1–1 Trusted Extensions 다중 레벨 CDE 데스크탑 27
그림 2–1 Trusted CDE의 Device Allocation Manager(장치 할당 관리자) 아이콘 37
그림 2–2 Device Allocation Manager(장치 할당 관리자) GUI 38
그림 2–3 Solaris Management Console의 일반적인 Trusted Extensions 도구 상자 39
그림 2–4 Solaris Management Console의 Computers and Networks(컴퓨터 및 네트워크) 도구 세트 40
그림 2–5 LDAP 서버를 사용하여 네트워크를 관리하는 Solaris Management Console 클라이언트 42
그림 2–6 네트워크의 개별 원격 시스템을 관리하는 Solaris Management Console 클라이언트 42
그림 12–1 일반적인 Trusted Extensions 경로 및 경로 지정 테이블 항목 165
그림 15–1 본문 페이지 맨 위와 아래에 인쇄된 작업의 레이블 197
그림 15–2 레이블이 있는 인쇄 작업의 일반적인 배너 페이지 198
그림 15–3 트레일러 페이지의 차이점 198
그림 16–1 사용자가 열어 놓은 Device Allocation Manager(장치 할당 관리자) 224
그림 17–1 Solaris Management Console의 Serial Ports(직렬 포트) 도구 235
그림 18–1 레이블이 있는 시스템의 일반적인 감사 레코드 구조 246
그림 18–2 `label` 토큰 형식 249
그림 18–3 `xcolormap`, `xcursor`, `xfont`, `xgc`, `xpixmap` 및 `xwindow` 토큰의 형식 250
그림 18–4 `xproperty` 토큰 형식 252
그림 18–5 `xselect` 토큰 형식 252

표

표 1–1 레이블 관계 예 29
표 2–1 Trusted Extensions 관리 도구 34
표 2–2 Trusted CDE의 관리 작업, 목적 및 연결된 권한 프로파일 35
표 2–3 Trusted CDE의 설치 작업, 목적 및 연결된 권한 프로파일 36
표 2–4 사용자 및 관리 Trusted Extensions 명령 44
표 2–5 Trusted Extensions에서 수정하는 사용자 및 관리 명령 45
표 4–1 파일을 새 레이블로 이동하기 위한 조건 62
표 4–2 선택 항목을 새 레이블로 이동하기 위한 조건 63
표 6–1 `policy.conf` 파일의 Trusted Extensions 보안 기본값 78
표 6–2 사용자를 만든 후 지정되는 보안 속성 79
표 12–1 `tnrhdb` 호스트 주소 및 폴백 방식 항목 160
표 15–1 `tsol_separator.ps` 파일의 구성 가능한 값 199
표 18–1 X 서버 감사 클래스 247
표 18–2 Trusted Extensions 감사 토큰 248
표 19–1 Trusted Extensions의 CDE 작업에 대한 제약 조건 260

머리말

Trusted Extensions 관리자 절차 설명서에서는 Oracle Solaris 운영 체제(Oracle Solaris OS)에서 Trusted Extensions를 구성하는 절차에 대해 설명합니다. 또한 Trusted Extensions 소프트웨어로 레이블이 지정된 사용자, 영역, 장치 및 호스트를 관리하는 절차에 대해 설명합니다.

주 – 본 Oracle Solaris 릴리스는 프로세서 아키텍처의 SPARC 및 x86 제품군을 사용하는 시스템을 지원합니다. 지원되는 시스템은 **Oracle Solaris OS: 하드웨어 호환성 목록**을 참조하십시오. 이 설명서에서는 플랫폼 유형에 따른 구현 차이가 있는 경우 이에 대하여 설명합니다.

이 문서에서 사용되는 x86 관련 용어의 의미는 다음과 같습니다.

- x86은 64비트 및 32비트 x86 호환 제품을 아우르는 큰 제품군을 의미합니다.
- x64는 특히 64비트 x86 호환 CPU와 관련됩니다.
- "32비트 x86"은 x86 기반 시스템에 대한 특정 32비트 정보를 나타냅니다.

지원되는 시스템은 **Oracle Solaris OS: 하드웨어 호환성 목록**을 참조하십시오.

본 설명서의 대상

이 설명서는 Trusted Extensions 소프트웨어를 구성하고 관리하는 지식이 풍부한 시스템 관리자 및 보안 관리자를 대상으로 합니다. 사이트 보안 정책에 필요한 신뢰 레벨과 전문 지식 레벨에 따라 구성 작업을 수행할 수 있는 사용자가 결정됩니다.

관리자는 Oracle Solaris 관리 방법에 대해 잘 알고 있어야 합니다. 또한 다음에 대한 이해가 필요합니다.

- Trusted Extensions의 보안 기능 및 사이트 보안 정책
- Trusted Extensions로 구성된 호스트 사용에 대한 기본 개념과 절차(**Trusted Extensions User's Guide** 참조)
- 사이트에서 역할 간에 관리 작업을 배분하는 방법

Trusted Extensions 설명서 구성 방식

다음 표에서는 Trusted Extensions 설명서에서 다루는 항목 및 각 설명서의 대상 사용자를 보여 줍니다.

설명서 제목	내용	대상
Trusted Extensions User's Guide	Trusted Extensions의 기본 기능에 대해 설명합니다. 이 설명서에는 용어집도 포함되어 있습니다.	최종 사용자, 관리자 및 개발자
Trusted Extensions Configuration Guide	Solaris 10 5/08 릴리스 이상 버전에서 Trusted Extensions를 사용으로 설정하고 초기 구성하는 방법에 대해 설명합니다. **Solaris Trusted Extensions Installation and Configuration for the Solaris 10 11/06 and Solaris 10 8/07 Releases**를 대체합니다.	관리자, 개발자
Trusted Extensions 관리자 절차	특정 관리 작업을 수행하는 방법에 대해 설명합니다.	관리자, 개발자
Trusted Extensions Developer's Guide	Trusted Extensions로 응용 프로그램을 개발하는 방법에 대해 설명합니다.	개발자, 관리자
Trusted Extensions Label Administration	레이블 인코딩 파일에서 레이블 구성 요소를 지정하는 방법에 대해 설명합니다.	관리자
Compartmented Mode Workstation Labeling: Encodings Format	레이블 인코딩 파일에 사용되는 구문에 대해 설명합니다. 구문을 통해 올바르게 구성된 시스템 레이블에 다양한 규칙이 적용됩니다.	관리자

관련 시스템 관리 설명서

다음 설명서에는 Trusted Extensions 소프트웨어를 준비하고 실행할 때 유용한 정보가 포함되어 있습니다.

설명서 제목	내용
Oracle Solaris 관리: 기본 관리	사용자 계정 및 그룹, 서버 및 클라이언트 지원, 시스템 종료 및 부팅, 서비스 관리, 소프트웨어 관리(패키지 및 패치)
시스템 관리 설명서: 고급 관리	터미널 및 모뎀, 시스템 리소스(디스크 쿼터, 계정, crontab), 시스템 프로세스, Solaris 소프트웨어 문제 해결
System Administration Guide: Devices and File Systems	이동식 매체, 디스크 및 장치, 파일 시스템, 데이터 백업 및 복원
Oracle Solaris 관리: IP 서비스	TCP/IP 네트워크 관리, IPv4 및 IPv6 주소 관리, DHCP, IPsec, IKE, Solaris IP 필터, 이동 IP, IPMP(IP Network Multipathing), IPQoS

설명서 제목	내용
System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)	DNS, NIS 및 LDAP 명명 규칙 및 디렉토리 서비스(NIS에서 LDAP으로의 전환, NIS+에서 LDAP으로의 전환 포함)
System Administration Guide: Network Services	웹 캐시 서버, 시간 관련 서비스, 네트워크 파일 시스템(NFS 및 Autofs), 메일, SLP, PPP
System Administration Guide: Security Services	감사, 장치 관리, 파일 보안, BART, Kerberos 서비스, PAM, Solaris Cryptographic Framework, 권한, RBAC, SASL, Solaris Secure Shell
시스템 관리 설명서: Oracle Solaris Containers-리소스 관리 및 Oracle Solaris 영역	리소스 관리 항목 프로젝트 및 작업, 확장 계정, 리소스 제어, FSS(Fair Share Scheduler), rcapd(Resource Capping Daemon)를 통한 물리적 메모리 제어, 리소스 풀, Solaris Zones 소프트웨어 분할 기술 및 lx 브랜드 영역을 통한 가상화
Oracle Solaris ZFS 관리 설명서	ZFS 저장소 풀 및 파일 시스템 만들기/관리, 스냅샷, 복제, 백업, ACL(액세스 제어 목록)을 통한 ZFS 파일 보호, 영역이 설치된 Solaris 시스템에서 ZFS 사용, 에뮬레이트된 볼륨, 문제 해결 및 데이터 복구
System Administration Guide: Printing	Solaris 인쇄 항목 및 작업, 서비스, 도구, 프로토콜 및 기술을 사용하여 인쇄 서비스와 프린터 설정 및 관리

관련 참조

사이트 보안 정책 문서 – 사이트의 보안 정책 및 보안 절차에 대해 설명합니다.

Solaris 공통 데스크탑 환경: 고급 사용자 및 시스템 관리자 안내서 – 공통 데스크탑 환경(Common Desktop Environment, CDE)에 대해 설명합니다.

현재 설치된 운영 체제에 대한 관리자 설명서 – 시스템 파일을 백업하는 방법에 대해 설명합니다.

타사 웹 사이트

이 문서에서 참조하는 타사 URL은 추가 관련 정보를 제공합니다.

주 – Oracle은 본 설명서에서 언급된 타사 웹 사이트의 가용성 여부에 대해 책임을 지지 않습니다. 또한 해당 사이트나 리소스를 통해 제공되는 내용, 알림, 제품 및 기타 자료에 대해 어떠한 보증도 하지 않으며 그에 대한 책임도 지지 않습니다. 따라서 타사 웹 사이트 또는 리소스의 내용, 제품 또는 서비스의 사용으로 인해 발생한 실제 또는 주장된 손상이나 피해에 대해서도 책임을 지지 않습니다.

Oracle Support에 액세스

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

활자체 규약

다음 표는 이 설명서에서 사용되는 활자체 규약에 대해 설명합니다.

표 P–1 활자체 규약

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

명령 예의 셸 프롬프트

다음 표에는 Oracle Solaris OS에 포함된 셸의 UNIX 시스템 프롬프트 및 수퍼유저 프롬프트가 나와 있습니다. 명령 예에서 셸 프롬프트는 명령을 일반 사용자가 실행해야 하는지 또는 권한 있는 사용자가 실행해야 하는지 나타냅니다.

표 P–2 셸 프롬프트

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

◆ ◆ ◆ 1 장

1 Trusted Extensions 관리 개념

이 장에서는 Trusted Extensions 소프트웨어로 구성된 시스템 관리를 소개합니다.

- 23 페이지 “Trusted Extensions 소프트웨어 및 Oracle Solaris OS”
- 26 페이지 “Trusted Extensions의 기본 개념”

Trusted Extensions 소프트웨어 및 Oracle Solaris OS

Trusted Extensions 소프트웨어는 Oracle Solaris OS(Solaris 운영 체제)를 실행 중인 시스템에 레이블을 추가합니다. 레이블은 MAC(**필수 액세스 제어**)를 구현합니다. MAC는 DAC(임의 액세스 제어)와 함께 시스템 주체(프로세스)와 객체(데이터)를 보호합니다. Trusted Extensions 소프트웨어는 레이블 구성, 레이블 지정 및 레이블 정책을 처리하는 인터페이스를 제공합니다.

Trusted Extensions와 Oracle Solaris OS의 유사점

Trusted Extensions 소프트웨어는 권한 프로파일, 역할, 감사 및 Oracle Solaris OS의 기타 보안 기능을 사용합니다. Trusted Extensions에서는 Oracle Solaris SSH(Secure Shell), BART, Oracle Solaris 암호화 프레임워크, IPsec 및 IP 필터를 사용할 수 있습니다.

- Oracle Solaris OS에서와 마찬가지로 사용자를 작업 수행에 필요한 응용 프로그램 사용으로 제한할 수 있습니다. 더 많은 작업을 수행할 수 있게 다른 사용자에게 권한을 부여할 수 있습니다.
- Oracle Solaris OS에서와 마찬가지로 이전에 수퍼유저에게 지정되었던 기능이 개별 "역할"에 지정됩니다.
- Oracle Solaris OS에서와 마찬가지로 권한을 통해 프로세스가 보호됩니다. 영역도 프로세스를 구분하는 데 사용됩니다.
- Oracle Solaris OS에서와 마찬가지로 시스템의 이벤트를 감사할 수 있습니다.
- Trusted Extensions에서는 Oracle Solaris OS의 시스템 구성 파일(예: `policy.conf` 및 `exec_attr`)을 사용합니다.

Trusted Extensions와 Oracle Solaris OS의 차이점

Trusted Extensions 소프트웨어는 Oracle Solaris OS를 확장합니다. 다음 목록은 개요 형식의 간략한 설명을 제공합니다. 빠른 참조는 부록 A, "Trusted Extensions 관리에 대한 빠른 참조"를 참조하십시오.

- Trusted Extensions에서는 **레이블**이라는 특수 보안 태그로 데이터에 대한 액세스를 제어합니다. 레이블은 MAC(**필수 액세스 제어**)를 제공합니다. UNIX 파일 사용 권한이나 DAC(임의 액세스 제어) 이외에 MAC 보호도 있습니다. 레이블은 사용자, 영역, 장치, 창 및 네트워크 끝점에 직접 지정됩니다. 레이블은 프로세스, 파일 및 기타 시스템 객체에 암시적으로 지정됩니다.

  일반 사용자는 MAC를 대체할 수 없습니다. Trusted Extensions에서 일반 사용자는 레이블이 있는 영역에서 작업해야 합니다. 기본적으로 레이블이 있는 영역의 사용자나 프로세스는 MAC를 대체할 수 없습니다.

  Oracle Solaris OS에서와 마찬가지로 보안 정책을 대체하는 기능은 MAC를 대체할 수 있을 때 특정 프로세서나 사용자에게 지정될 수 있습니다. 예를 들어, 파일의 레이블을 변경할 수 있게 사용자를 권한 부여할 수 있습니다. 이러한 작업은 해당 파일에서 정보의 민감도를 업그레이드하거나 다운그레이드합니다.
- Trusted Extensions는 기존 구성 파일 및 명령에 추가합니다. 예를 들어, Trusted Extensions에서는 감사 이벤트, 권한 부여, 권한 및 권한 프로파일을 추가합니다.
- Oracle Solaris 시스템에서는 선택 사항인 일부 기능이 Trusted Extensions 시스템에서는 필수 사항입니다. 예를 들어, Trusted Extensions로 구성된 시스템에서는 영역과 역할이 필수 사항입니다.
- Oracle Solaris 시스템에서는 선택 사항인 일부 기능이 Trusted Extensions 에서는 권장 사항입니다. 예를 들어, Trusted Extensions에서는 `root` 사용자가 `root` 역할로 변환되어야 합니다.
- Trusted Extensions에서는 Oracle Solaris OS의 기본 동작을 변경할 수 있습니다. 예를 들어, Trusted Extensions로 구성된 시스템에서는 감사가 기본적으로 사용으로 설정됩니다. 또한 장치를 할당해야 합니다.
- Oracle Solaris OS에서 사용할 수 있는 옵션을 Trusted Extensions에서 축소할 수 있습니다. 예를 들어, Trusted Extensions로 구성된 시스템에서는 NIS+ 이름 지정 서비스가 지원되지 않습니다. 또한 Trusted Extensions에서는 모든 영역이 레이블이 있는 영역입니다. Oracle Solaris OS와 달리 레이블이 있는 영역은 동일한 풀의 사용자 ID 및 그룹 ID를 사용해야 합니다. 또한 Trusted Extensions에서는 여러 레이블이 있는 영역이 하나의 IP 주소를 공유할 수 있습니다.
- Trusted Extensions에서는 두 데스크탑의 신뢰할 수 있는 버전을 제공합니다. 레이블이 있는 환경에서 작업하려면 Trusted Extensions의 데스크탑 사용자가 다음 두 데스크탑 중 하나를 사용해야 합니다.
  - **Solaris Trusted Extensions(CDE)** — CDE(Common Desktop Environment)의 신뢰할 수 있는 버전입니다. Trusted CDE로 줄여서 부르기도 합니다.
  - **Solaris Trusted Extensions(JDS)** – Java Desktop System, 릴리스 **번호**의 신뢰할 수 있는 버전입니다. Trusted JDS로 줄여서 부르기도 합니다.

- Trusted Extensions에서는 추가 GUI(그래픽 사용자 인터페이스)와 CLI(명령줄 인터페이스)를 제공합니다. 예를 들어, Trusted Extensions에서는 장치를 관리하는 Device Allocation Manager(장치 할당 관리자)를 제공합니다. 또한 `updatehome` 명령을 사용하여 모든 레이블의 일반 사용자 홈 디렉토리에 시작 파일을 넣을 수 있습니다.
- Trusted Extensions에서는 특정 GUI를 관리에 사용해야 합니다. 예를 들어, Trusted Extensions로 구성된 시스템에서는 Solaris Management Console을 사용하여 사용자, 역할 및 네트워크를 관리합니다. 마찬가지로 Trusted CDE에서는 관리 편집기를 사용하여 시스템 파일을 편집합니다.
- Trusted Extensions에서는 사용자에게 표시되는 항목이 제한됩니다. 예를 들어, 사용자가 할당할 수 없는 장치는 해당 사용자에게 표시되지 않습니다.
- Trusted Extensions에서는 사용자의 데스크탑 옵션을 제한합니다. 예를 들어, 사용자가 제한된 시간 동안 워크스테이션을 사용하지 않을 경우 화면이 잠깁니다.

멀티헤디드 시스템 및 Trusted Extensions 데스크탑

멀티헤디드 Trusted Extensions 시스템의 모니터가 수평으로 구성된 경우 신뢰할 수 있는 스트라이프가 모니터 전체로 늘어납니다. 모니터가 수직으로 구성된 경우 신뢰할 수 있는 스트라이프가 맨 아래 모니터에 나타납니다.

멀티헤디드 시스템의 모니터마다 다른 작업 공간이 표시되는 경우 Trusted CDE와 Trusted JDS에서 신뢰할 수 있는 스트라이프를 다르게 렌더링합니다.

- Trusted JDS 데스크탑에서는 각 모니터에 하나의 신뢰할 수 있는 스트라이프가 표시됩니다.
- Trusted CDE 데스크탑에서는 하나의 신뢰할 수 있는 스트라이프가 기본 모니터에 나타납니다.

주의 – 두번째의 신뢰할 수 있는 스트라이프가 Trusted CDE 멀티헤디드 시스템에 나타난 경우 해당 스트라이프는 운영 체제에 의해 생성되지 않습니다. 시스템에 허용되지 않은 프로그램이 있을 수 있습니다.

즉시 보안 관리자에게 문의하십시오. 올바른 신뢰할 수 있는 스트라이프를 확인하려면 70 페이지 “데스크탑의 현재 포커스에 대한 컨트롤을 다시 얻는 방법”을 참조하십시오.

Trusted Extensions의 기본 개념

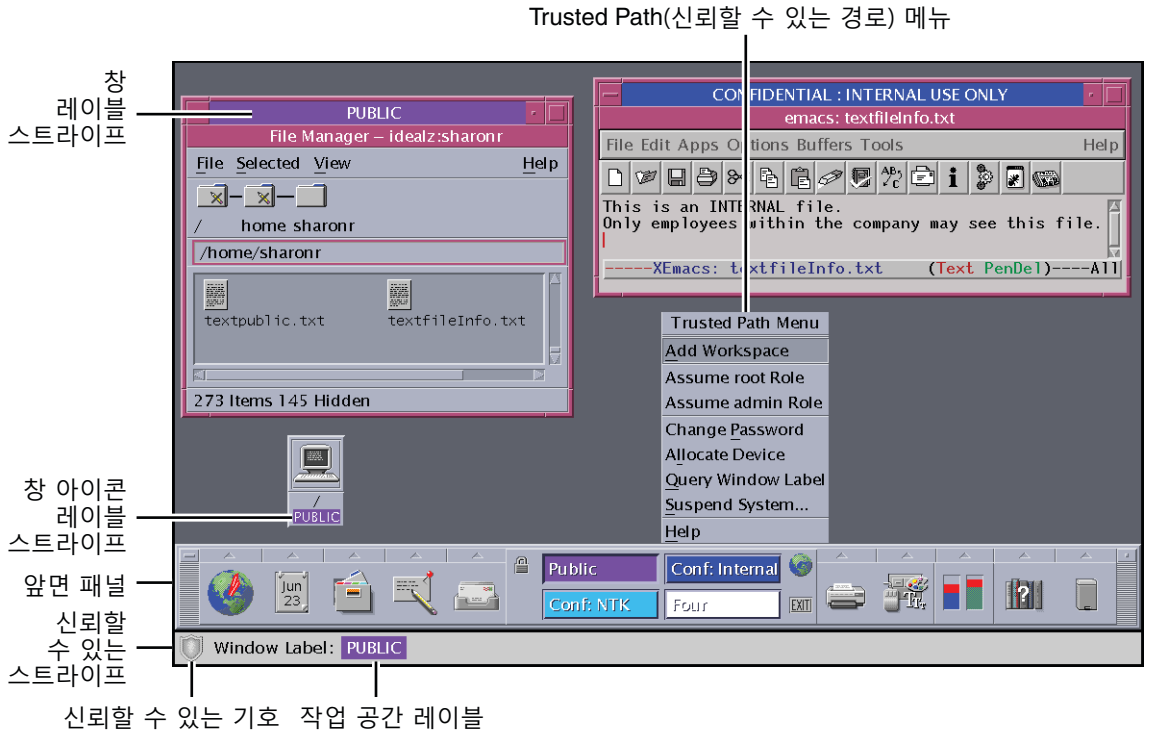
Trusted Extensions 소프트웨어는 Oracle Solaris 시스템에 레이블을 추가합니다. Label Builder(레이블 구축기) 및 Device Allocation Manager(장치 할당 관리자)와 같은 레이블이 있는 데스크탑과 신뢰할 수 있는 응용 프로그램도 추가됩니다. 여기서는 사용자와 관리자 모두가 Trusted Extensions를 이해하는 데 필요한 개념에 대해 설명합니다. 이러한 개념은 **Trusted Extensions User's Guide** 에 소개되어 있습니다.

Trusted Extensions 보호

Trusted Extensions 소프트웨어는 Oracle Solaris OS의 보호 기능을 강화합니다. Oracle Solaris OS에서는 암호가 필요한 사용자 계정으로 시스템에 대한 액세스를 보호합니다. 암호를 특정한 길이로 정기적으로 변경하도록 요구할 수 있습니다. 역할이 관리 작업을 수행하려면 추가 암호가 필요합니다. 역할은 로그인 계정으로 사용될 수 없기 때문에 추가 인증을 사용하면 루트 암호를 추측하려는 침입자에 의해 발생할 수 있는 피해를 제한할 수 있습니다. Trusted Extensions 소프트웨어는 사용자와 역할을 승인된 레이블 범위로 제한하여 보호 기능을 강화합니다. 이 레이블 범위에 따라 사용자와 역할이 액세스할 수 있는 정보가 제한됩니다.

Trusted Extensions 소프트웨어는 신뢰할 수 있는 스트라이프의 왼쪽에 나타나는 확실한 변조 방지 엠블럼인 Trusted Path(신뢰할 수 있는 경로) 기호를 표시합니다. Trusted CDE에서 스트라이프는 화면의 맨 아래에 있습니다. Trusted JDS에서 스트라이프는 화면의 맨 위에 있습니다. Trusted Path(신뢰할 수 있는 경로) 기호는 사용자가 시스템의 보안 관련 부분을 사용 중일 때 나타납니다. 사용자가 신뢰할 수 있는 응용 프로그램을 실행할 때 이 기호가 나타나지 않는 경우 응용 프로그램의 해당 버전이 인증되었는지 즉시 확인하십시오. 신뢰할 수 있는 스트라이프가 나타나지 않는 경우 해당 데스크탑을 신뢰할 수 없습니다. 샘플 데스크탑 표시는 그림 1–1을 참조하십시오.

그림 1–1 Trusted Extensions 다중 레벨 CDE 데스크탑



대부분의 보안 관련 소프트웨어 즉, TCB(Trusted Computing Base)는 전역 영역에서 실행됩니다. 일반 사용자는 전역 영역에 연결하거나 전역 영역의 리소스를 볼 수 없습니다. 사용자는 TCB 소프트웨어와 상호 작용(예: 암호 변경)할 수 있습니다. Trusted Path(신뢰할 수 있는 경로) 기호는 사용자가 TCB와 상호 작용할 때마다 표시됩니다.

Trusted Extensions 및 액세스 제어

Trusted Extensions 소프트웨어에서는 DAC(임의 액세스 제어) 및 MAC(필수 액세스 제어)를 통해 정보와 기타 리소스를 보호합니다. DAC는 소유자가 임의로 설정하는 일반 UNIX 권한 비트 및 액세스 제어 목록입니다. MAC는 시스템에서 자동으로 적용하는 방식입니다. MAC는 프로세스의 레이블과 트랜잭션 데이터를 확인하여 모든 트랜잭션을 제어합니다.

사용자의 **레이블**은 사용자가 작업할 수 있거나 작업하도록 선택하는 민감도 레벨을 나타냅니다. 일반 레이블은 `Secret` 또는 `Public`입니다. 레이블에 따라 사용자가 액세스할 수 있는 정보가 결정됩니다. MAC와 DAC는 모두 Oracle Solaris OS에 있는 특수 사용 권한으로 대체될 수 있습니다. **권한**은 프로세스에 허용될 수 있는 특수 사용 권한입니다. **권한 부여**는 관리자가 사용자와 역할에 부여할 수 있는 특수 사용 권한입니다.

관리자는 사이트의 보안 정책에 따라 사용자에게 적절한 파일 및 디렉토리 보안 절차를 교육해야 합니다. 또한 사용자가 적절한 시기에 레이블을 업그레이드하거나 다운그레이드할 수 있도록 알려 주어야 합니다.

역할 및 Trusted Extensions

Trusted Extensions 없이 Oracle Solaris 소프트웨어를 실행 중인 시스템에서 역할은 선택 사항입니다. Trusted Extensions로 구성된 시스템에서 역할은 필수 사항입니다. 시스템은 시스템 관리자 역할 및 보안 관리자 역할로 관리됩니다. `root` 역할이 사용되는 경우도 있습니다.

Oracle Solaris OS에서와 마찬가지로 권한 프로파일은 역할 기능의 기반입니다. Trusted Extensions에서는 Information Security와 User Security라는 두 가지 권한 프로파일을 제공합니다. 이 두 프로파일은 보안 관리자 역할을 정의합니다.

Trusted Extensions에서 역할이 사용할 수 있는 프로그램에는 **신뢰할 수 있는 경로 속성**이라는 특수 등록 정보가 있습니다. 이 속성은 프로그램이 TCB의 일부임을 나타냅니다. 신뢰할 수 있는 경로 속성은 프로그램이 전역 영역에서 시작되는 경우에 사용할 수 있습니다.

역할에 대한 자세한 내용은 **System Administration Guide: Security Services**의 제III부, "Roles, Rights Profiles, and Privileges"을 참조하십시오.

Trusted Extensions 소프트웨어의 레이블

레이블과 클리어런스는 Trusted Extensions에서 MAC(필수 액세스 제어)의 중앙에 있습니다. 레이블과 클리어런스에 따라 어느 사용자가 무슨 프로그램, 파일 및 디렉토리에 액세스할 수 있는지가 결정됩니다. 레이블과 클리어런스는 하나의 **분류** 구성 요소와 0개 이상의 **구획** 구성 요소로 구성됩니다. 분류 구성 요소는 보안 계층 레벨(예: `TOP SECRET` 또는 `CONFIDENTIAL`)을 나타냅니다. 구획 구성 요소는 정보의 일반 본문에 액세스해야 하는 사용자 그룹을 나타냅니다. 일반적인 유형의 구획으로는 프로젝트, 부서, 물리적 위치 등이 있습니다. 권한 부여된 사용자가 레이블을 읽을 수 있지만, 내부적으로는 레이블이 숫자로 조작됩니다. 숫자와 읽기 가능한 버전은 `label_encodings` 파일에 정의되어 있습니다.

Trusted Extensions에서는 시도되는 보안 관련 트랜잭션을 모두 중개합니다. 소프트웨어에서는 액세스하는 엔티티(일반적으로 프로세스)와 액세스 대상 엔티티(일반적으로 파일 시스템 객체)의 레이블을 비교합니다. 그런 다음 **지배적**인 레이블에 따라 트랜잭션을 허용하거나 거부합니다. 레이블은 다른 시스템 리소스(예: 할당 가능한 장치, 네트워크, 프레임 버퍼, 다른 호스트)에 대한 액세스 권한을 결정하는 데도 사용됩니다.

레이블 사이의 지배 관계

엔티티의 레이블이 다음과 같은 두 조건을 충족하는 경우 다른 레이블을 **지배**한다고 합니다.

- 첫번째 엔티티 레이블의 분류 구성 요소는 두번째 레이블의 분류보다 높거나 같습니다. 보안 관리자는 `label_encodings` 파일에서 분류에 번호를 지정합니다. 소프트웨어에서는 이 번호를 비교하여 지배 관계를 결정합니다.
- 첫번째 엔티티의 구획 세트에 두번째 엔티티의 모든 구획이 포함됩니다.

분류와 구획 세트가 동일한 경우 두 레이블이 **동일**하다고 합니다. 레이블이 동일한 경우 서로 지배 관계이므로 액세스가 허용됩니다.

한 레이블의 분류가 더 높거나 레이블의 분류가 동일하지만 한 레이블의 구획이 두번째 레이블 구획의 수퍼 세트인 경우 첫번째 레이블이 두번째 레이블을 **완전히 지배**한다고 합니다.

어떤 레이블도 다른 레이블을 지배하지 않는 경우 두 레이블은 **분리** 또는 **비교 불가**라고 합니다.

다음 표에서는 지배에 대한 레이블 비교의 예를 제공합니다. 예에서 `NEED_TO_KNOW`는 `INTERNAL`보다 더 높은 분류입니다. 이 예에는 Eng, Mkt, Fin의 세 가지 구획이 있습니다.

표 1–1 레이블 관계 예

레이블 1	관계	레이블 2
`NEED_TO_KNOW Eng Mkt`	(엄격한) 지배	`INTERNAL Eng Mkt`
`NEED_TO_KNOW Eng Mkt`	(엄격한) 지배	`NEED_TO_KNOW Eng`
`NEED_TO_KNOW Eng Mkt`	(엄격한) 지배	`INTERNAL Eng`
`NEED_TO_KNOW Eng Mkt`	지배(동등)	`NEED_TO_KNOW Eng Mkt`
`NEED_TO_KNOW Eng Mkt`	분리	`NEED_TO_KNOW Eng Fin`
`NEED_TO_KNOW Eng Mkt`	분리	`NEED_TO_KNOW Fin`
`NEED_TO_KNOW Eng Mkt`	분리	`INTERNAL Eng Mkt Fin`

관리 레이블

Trusted Extensions에서는 레이블이나 클리어런스로 사용되는 `ADMIN_HIGH` 및 `ADMIN_LOW`라는 두 가지 특수 관리 레이블을 제공합니다. 이 레이블은 시스템 리소스를 보호하는 데 사용되며 일반 사용자가 아닌 관리자용입니다.

`ADMIN_HIGH`는 최상위 레이블입니다. `ADMIN_HIGH`는 시스템의 다른 레이블을 모두 지배하며 시스템 데이터(예: 관리 데이터베이스, 감사 증적)를 읽지 못하도록 보호하는 데 사용됩니다. 레이블이 `ADMIN_HIGH`인 데이터를 보려면 전역 영역에 있어야 합니다.

ADMIN_LOW는 최하위 레이블입니다. ADMIN_LOW는 일반 사용자 레이블을 포함하여 시스템의 다른 모든 레이블의 지배를 받습니다. 필수 액세스 제어는 사용자가 자신의 레이블보다 낮은 레이블의 파일에 데이터를 쓰는 것을 허용하지 않습니다. 따라서 일반 사용자는 ADMIN_LOW 레이블의 파일을 읽을 수 있지만 수정할 수는 없습니다. ADMIN_LOW는 일반적으로 공유되는 공용 실행 파일(예: /usr/bin에 있는 파일)을 보호하는 데 사용됩니다.

레이블 인코딩 파일

시스템의 모든 레이블 구성 요소 즉, 분류, 구획 및 연결된 규칙은 ADMIN_HIGH 파일인 label_encodings 파일에 저장됩니다. 이 파일은 /etc/security/tsol 디렉토리에 있습니다. 보안 관리자는 사이트에 대한 label_encodings 파일을 설정합니다. 레이블 인코딩 파일에는 다음이 포함됩니다.

- **구성 요소 정의** – 분류, 구획, 레이블 및 클리어런스 정의(필요한 조합 및 제약 조건에 대한 규칙 포함)
- **승인 범위 정의** – 전체 시스템 및 일반 사용자에 대해 사용 가능한 레이블 세트를 정의하는 클리어런스 및 최소 레이블 지정
- **인쇄 사양** – 프린터 출력에 표시되는 인쇄 배너, 트레일러, 머리글, 바닥글 및 기타 보안 기능에 대한 식별 및 처리 정보
- **사용자 정의** – 로컬 정의(레이블 색상 코드 포함)와 기타 기본값

자세한 내용은 label_encodings(4) 매뉴얼 페이지를 참조하십시오. 자세한 내용은 **Trusted Extensions Label Administration** 및 **Compartmented Mode Workstation Labeling: Encodings Format** 을 참조하십시오.

레이블 범위

레이블 범위는 사용자가 작업할 수 있는 잠재적으로 사용 가능한 레이블의 세트입니다. 사용자와 리소스 모두 레이블 범위를 가집니다. 레이블 범위로 보호할 수 있는 리소스로는 할당 가능한 장치, 네트워크, 인터페이스, 프레임 버퍼, 명령, 작업 등이 있습니다. 레이블 범위는 범위의 맨 위에 있는 클리어런스와 맨 아래에 있는 최소 레이블로 정의됩니다.

최대 레이블과 최소 레이블 사이에 있는 모든 레이블 조합이 범위에 반드시 포함되어야 하는 것은 아닙니다. label_encodings 파일의 규칙에 따라 특정 조합이 무효화될 수 있습니다. 레이블이 범위에 포함되려면 **올바른 형식**이 되어야 합니다. 즉, 레이블 인코딩 파일의 적용 가능한 모든 규칙에서 레이블을 허용해야 합니다.

클리어런스는 올바른 형식이 아니어도 됩니다. 예를 들어, label_encodings 파일이 레이블에서 Eng, Mkt 및 Fin 구획의 모든 조합을 금지하는 경우 INTERNAL Eng Mkt Fin은 유효한 클리어런스지만 유효한 레이블은 아닙니다. 사용자는 이 조합을 클리어런스로 사용하여 레이블이 INTERNAL Eng, INTERNAL Mkt 및 INTERNAL Fin인 파일에 액세스할 수 있습니다.

계정 레이블 범위

사용자에게 클리어런스와 최소 레이블을 지정하면 사용자가 작업할 수 있는 **계정 레이블 범위**의 상한과 하한이 정의됩니다. 다음 방정식은 계정 레이블 범위를 보여줍니다. 여기서 ≤은 "지배됨 또는 동등"을 나타냅니다.

최소 레이블 ≤ 허용되는 레이블 ≤ 클리어런스

따라서 레이블이 최소 레이블을 지배하는 경우 사용자는 클리어런스의 지배를 받는 모든 레이블에서 작업할 수 있습니다. 사용자의 클리어런스와 최소 레이블이 명시적으로 설정되지 않은 경우 `label_encodings` 파일에 정의된 기본값이 적용됩니다.

두 개 이상의 레이블 또는 단일 레이블에서 작업할 수 있도록 사용자에게 클리어런스와 최소 레이블을 지정할 수 있습니다. 사용자의 클리어런스와 레이블이 동일할 경우 사용자는 하나의 레이블에서만 작업할 수 있습니다.

세션 범위

세션 범위는 사용자가 Trusted Extensions 세션 동안 사용할 수 있는 레이블 세트입니다. 세션 범위는 시스템에 대해 설정된 레이블 범위와 사용자의 계정 레이블 범위 내에 있어야 합니다. 로그인할 때 사용자가 단일 레이블 세션 모드를 선택하면 세션 범위는 해당 레이블로 제한됩니다. 사용자가 다중 레이블 모드를 선택하면 해당 레이블이 세션 클리어런스가 됩니다. 세션 클리어런스는 세션 범위의 상한을 정의합니다. 사용자의 최소 레이블은 하한을 정의합니다. 사용자는 최소 레이블의 작업 공간에서 세션을 시작합니다. 세션 동안 사용자는 세션 범위 내에 있는 모든 레이블의 작업 공간으로 전환할 수 있습니다.

레이블이 보호하는 항목 및 레이블이 표시되는 위치

레이블은 데스크탑과 데스크탑에서 실행되는 출력(예: 프린터 출력)에 표시됩니다.

- **응용 프로그램** – 응용 프로그램에서 프로세스를 시작합니다. 이러한 프로세스는 응용 프로그램이 시작되는 작업 공간의 레이블에서 실행됩니다. 파일과 같이 레이블이 있는 영역 내 응용 프로그램의 레이블은 해당 영역의 레이블에서 지정됩니다.
- **장치** – 장치를 통해 이동하는 데이터는 장치 할당 및 장치 레이블 범위를 통해 제어됩니다. 장치를 사용하려면 사용자가 장치의 레이블 범위 내에 있고 해당 장치를 할당할 수 있게 권한 부여되어야 합니다.
- **파일 시스템 마운트 지점** – 모든 마운트 지점에는 레이블이 있습니다. `getlabel` 명령을 사용하여 레이블을 볼 수 있습니다.
- **네트워크 인터페이스** – IP 주소(호스트)에는 해당 레이블 범위를 설명하는 템플리트가 있습니다. 레이블이 없는 호스트에도 기본 레이블이 있습니다.
- **프린터 및 인쇄** – 프린터에는 레이블 범위가 있습니다. 레이블은 본문 페이지에 인쇄됩니다. 레이블, 처리 정보 및 기타 보안 정보는 배너 및 트레일러 페이지에 인쇄됩니다. Trusted Extensions에서 인쇄를 구성하려면 15 장, “레이블이 있는 인쇄 관리(작업)” 및 **Trusted Extensions Label Administration**의 “Labels on Printed Output”을 참조하십시오.

- **프로세스** – 프로세스에는 레이블이 있습니다. 프로세스는 해당 프로세스가 시작된 작업 공간의 레이블에서 실행됩니다. 프로세스의 레이블은 `plabel` 명령을 사용하여 볼 수 있습니다.
- **사용자** – 사용자에게는 기본 레이블과 레이블 범위가 지정됩니다. 사용자의 작업 공간 레이블은 사용자의 프로세스 레이블을 나타냅니다.
- **창** – 레이블이 데스크탑 창의 맨 위에 표시됩니다. 또한 데스크탑의 레이블은 색상으로 표시됩니다. 색상은 데스크탑 스위치와 창 제목 표시줄 위에 나타납니다.

  창을 다른 레이블이 있는 작업 공간으로 이동해도 창의 원래 레이블이 유지됩니다.
- **영역** – 모든 영역에는 고유한 레이블이 있습니다. 영역에서 소유한 파일과 디렉토리는 영역의 레이블에 있습니다. 자세한 내용은 `getzonepath(1)` 매뉴얼 페이지를 참조하십시오.

◆ ◆ ◆ 2 장

2 Trusted Extensions 관리 도구

이 장에서는 Trusted Extensions에서 사용할 수 있는 도구, 도구의 위치 및 도구가 작업하는 데이터베이스에 대해 설명합니다.

- 33 페이지 “Trusted Extensions용 관리 도구”
- 35 페이지 “Trusted CDE 작업”
- 37 페이지 “장치 할당 관리자”
- 38 페이지 “Solaris Management Console 도구”
- 44 페이지 “Trusted Extensions의 명령줄 도구”
- 46 페이지 “Trusted Extensions에서 원격 관리”

Trusted Extensions용 관리 도구

Trusted Extensions로 구성된 시스템 관리에는 Oracle Solaris OS에서 사용 가능한 것과 동일한 여러 도구가 사용됩니다. Trusted Extensions에서는 보안이 강화된 도구도 제공합니다. 역할 작업 공간의 역할만 관리 도구를 사용할 수 있습니다.

역할 작업 공간 내에서 신뢰할 수 있는 명령, 작업, 응용 프로그램 및 스크립트에 액세스할 수 있습니다. 다음 표는 이러한 관리 도구를 요약한 것입니다.

표 2–1 Trusted Extensions 관리 도구

도구	설명	자세한 정보
`/usr/sbin/txzonemgr`	영역 만들기, 설치, 초기화 및 부트를 위한 메뉴 기반 마법사를 제공합니다. 이 스크립트는 영역을 관리하는 Trusted CDE 작업을 대신합니다. 스크립트는 네트워킹 옵션, 이름 서비스 옵션 및 기존 LDAP 서버에 대한 전역 영역 클라이언트화를 위한 메뉴 항목도 제공합니다. `txzonemgr`에서는 `zenity` 명령을 사용합니다.	**Trusted Extensions Configuration Guide**의 "Creating Labeled Zones" 참조 `zenity`(1) 매뉴얼 페이지도 참조하십시오.
Trusted CDE의 Application Manager 폴더 내 Trusted_Extensions 폴더의 작업	Solaris Management Console에서 관리하지 않는 로컬 파일(예: `/etc/system`)을 편집하는 데 사용됩니다. 영역 설치 작업과 같은 일부 작업에서는 스크립트를 실행합니다.	35 페이지 "Trusted CDE 작업" 및 54 페이지 "Trusted Extensions에서 CDE 관리 작업을 시작하는 방법"을 참조하십시오.
Trusted CDE의 Device Allocation Manager(장치 할당 관리자) Solaris Trusted Extensions(JDS)의 Device Manager(장치 관리자)	장치의 레이블 범위를 관리하고 장치를 할당하거나 할당 해제하는 데 사용됩니다.	37 페이지 "장치 할당 관리자" 및 227 페이지 "Trusted Extensions에서 장치 취급(작업 맵)"을 참조하십시오.
Solaris Management Console	사용자, 역할, 권한, 호스트, 영역 및 네트워크를 구성하는 데 사용됩니다. 이 도구는 로컬 파일이나 LDAP 데이터베이스를 업데이트할 수 있습니다. 또한 이 도구는 `dtappsession` 레거시 응용 프로그램을 실행할 수도 있습니다.	기본적인 기능은 **Oracle Solaris 관리: 기본 관리**의 2 장, "Solaris Management Console 작업(작업)"을 참조하십시오. Trusted Extensions에 대한 자세한 내용은 38 페이지 "Solaris Management Console 도구"를 참조하십시오.
Solaris Management Console 명령(예: `smuser` 및 `smtnzonecfg`)	Solaris Management Console용 명령줄 인터페이스입니다.	목록은 표 2–4를 참조하십시오.
레이블 구축기	사용자 도구이기도 합니다. 프로그램에서 레이블 선택을 요구할 때 나타납니다.	예는 90 페이지 "Solaris Management Console에서 사용자의 레이블 범위를 수정하는 방법"을 참조하십시오.
Trusted Extensions 명령	CDE 작업이나 Solaris Management Console 도구에서 다루지 않는 작업을 수행하는 데 사용됩니다.	관리 명령 목록은 표 2–5를 참조하십시오.

txzonemgr 스크립트

Solaris 10 5/08 릴리스부터 레이블이 있는 영역을 구성하는 데 txzonemgr 스크립트가 사용됩니다. 이 zenity(1) 스크립트는 Labeled Zone Manager(레이블이 있는 영역 관리자) 대화 상자를 표시합니다. 이 GUI는 레이블이 있는 영역의 현재 구성 상태에 대해 유효한 선택 항목만 표시하는 동적 메뉴입니다. 예를 들어, 영역에 레이블이 이미 있는 경우 Label(레이블) 메뉴 항목이 표시되지 않습니다.

Trusted CDE 작업

다음 표에는 Trusted Extensions에서 실행할 수 있는 CDE 작업이 나열되어 있습니다. 이러한 신뢰할 수 있는 CDE 작업은 Trusted_Extensions 폴더에서 사용할 수 있습니다. Trusted_Extensions 폴더는 CDE 데스크탑의 Application Manager 폴더에서 사용할 수 있습니다.

표 2–2 Trusted CDE의 관리 작업, 목적 및 연결된 권한 프로파일

작업 이름	작업 목적	기본 권한 프로파일
할당 가능한 장치 추가	장치 데이터베이스에 항목을 추가하여 장치를 만듭니다. add_allocatable(1M)을 참조하십시오.	Device Security
관리 편집기	지정된 파일을 편집합니다. 54 페이지 “Trusted Extensions에서 관리 파일을 편집하는 방법”을 참조하십시오.	Object Access Management
감사 클래스	audit_class 파일을 편집합니다. audit_class(4)를 참조하십시오.	Audit Control
감사 제어	audit_control 파일을 편집합니다. audit_control(4)을 참조하십시오.	Audit Control
감사 이벤트	audit_event 파일을 편집합니다. audit_event(4)를 참조하십시오.	Audit Control
감사 시작	audit_startup.sh 스크립트를 편집합니다. audit_startup(1M)을 참조하십시오.	Audit Control
인코딩 확인	지정된 인코딩 파일에 대해 chk_encodings 명령을 실행합니다. chk_encodings(1M)를 참조하십시오.	Object Label Management
TN 파일 확인	tnrhdb, tnrhtp 및 tnzonecfg 데이터베이스에 대해 tnchkdb 명령을 실행합니다. tnchkdb(1M)를 참조하십시오.	네트워크 관리
선택 확인 구성	/usr/dt/config/sel_config 파일을 편집합니다. sel_config(4)를 참조하십시오.	Object Label Management
LDAP 클라이언트 만들기	전역 영역을 기존 LDAP 디렉토리 서비스의 LDAP 클라이언트로 만듭니다.	Information Security

표 2–2 Trusted CDE의 관리 작업, 목적 및 연결된 권한 프로파일 *(계속)*

작업 이름	작업 목적	기본 권한 프로파일
인코딩 편집	지정된 `label_encodings` 파일을 편집하고 `chk_encodings` 명령을 실행합니다. `chk_encodings(1M)`를 참조하십시오.	Object Label Management
이름 서비스 스위치	`nsswitch.conf` 파일을 편집합니다. `nsswitch.conf(4)`를 참조하십시오.	네트워크 관리
DNS 서버 설정	`resolv.conf` 파일을 편집합니다. `resolv.conf(4)`를 참조하십시오.	네트워크 관리
일별 메시지 설정	`/etc/motd` 파일을 편집합니다. 로그인 시 이 파일의 내용이 Last Login(마지막 로그인) 대화 상자에 표시됩니다.	네트워크 관리
기본 경로 설정	기본 정적 경로를 지정합니다.	네트워크 관리
파일 시스템 공유	`dfstab` 파일을 편집합니다. `share` 명령을 실행하지 않습니다. `dfstab(4)`를 참조하십시오.	파일 시스템 관리

다음 작업은 영역을 만들 때 초기 설정 팀에서 사용합니다. 이러한 작업 중 일부는 유지 관리 및 문제 해결에 사용됩니다.

표 2–3 Trusted CDE의 설치 작업, 목적 및 연결된 권한 프로파일

작업 이름	작업 목적	기본 권한 프로파일
영역 복제	기존 영역의 ZFS 스냅샷에서 레이블이 있는 영역을 만듭니다.	Zone Management
영역 복사	기존 영역으로 레이블이 있는 영역을 만듭니다.	Zone Management
영역 구성	레이블을 영역 이름에 연결합니다.	Zone Management
LDAP 영역 초기화	LDAP 클라이언트로 부트를 위해 영역을 초기화합니다.	Zone Management
영역 설치	레이블이 있는 영역에 필요한 시스템 파일을 설치합니다.	Zone Management
영역 다시 시작	이미 부트된 영역을 다시 시작합니다.	Zone Management
논리적 인터페이스 공유	전역 영역에 대한 하나의 인터페이스를 설정하고, 공유할 레이블이 있는 영역에 대한 별도의 인터페이스를 설정합니다.	네트워크 관리
물리적 인터페이스 공유	전역 영역과 레이블이 있는 영역에서 공유하는 하나의 인터페이스를 설정합니다.	네트워크 관리
영역 종료	설치된 영역을 종료합니다.	Zone Management
영역 시작	설치된 영역을 부트하고 해당 영역에 대한 서비스를 시작합니다.	Zone Management
영역 터미널 콘솔	콘솔을 열어 설치된 영역의 프로세스를 봅니다.	Zone Management

장치 할당 관리자

장치는 컴퓨터에 연결된 물리적 주변 기기 또는 **의사 장치**라고 하는 소프트웨어 시뮬레이션 장치입니다. 장치는 시스템에서 데이터를 가져오고 내보내기 위한 수단을 제공하므로 적절한 데이터 보호를 위해 장치를 제어해야 합니다. Trusted Extensions에서는 장치 할당 및 장치 레이블 범위를 사용하여 장치를 통한 데이터 플로우를 제어합니다.

레이블 범위가 있는 장치의 예로는 프레임 버퍼, 테이프 드라이브, 디스켓 및 CD-ROM 드라이브, 프린터, USB 장치 등이 있습니다.

사용자는 Device Allocation Manager(장치 할당 관리자)를 통해 장치를 할당합니다. Device Allocation Manager(장치 할당 관리자)는 장치를 마운트하고, 정리 스크립트를 사용하여 장치를 준비하며, 할당을 수행합니다. 작업이 완료되면 사용자는 다른 정리 스크립트를 실행하고 장치를 마운트 해제 및 할당 해제하는 Device Allocation Manager(장치 할당 관리자)를 통해 장치를 할당 해제합니다.

그림 2–1 Trusted CDE의 Device Allocation Manager(장치 할당 관리자) 아이콘

Device Allocation Manager(장치 할당 관리자)에서 Device Administration(장치 관리) 도구를 사용하여 장치를 관리할 수 있습니다. 일반 사용자는 Device Administration(장치 관리) 도구에 액세스할 수 없습니다.

주 – Solaris Trusted Extensions(JDS)에서 이 GUI의 이름은 Device Manager(장치 관리자)이며, Device Administration(장치 관리) 버튼의 이름은 Administration(관리)입니다.

그림 2–2 Device Allocation Manager(장치 할당 관리자) GUI

Trusted Extensions에서 장치 보호에 대한 자세한 내용은 17 장, “Trusted Extensions에 대한 장치 관리(작업)”를 참조하십시오.

Solaris Management Console 도구

Solaris Management Console을 통해 GUI 기반 관리 도구의 도구 상자에 액세스할 수 있습니다. 이러한 도구를 사용하여 다양한 구성 데이터베이스에서 항목을 편집할 수 있습니다. Trusted Extensions에서 Solaris Management Console은 사용자, 역할 및 신뢰할 수 있는 네트워크 데이터베이스에 대한 관리 인터페이스입니다.

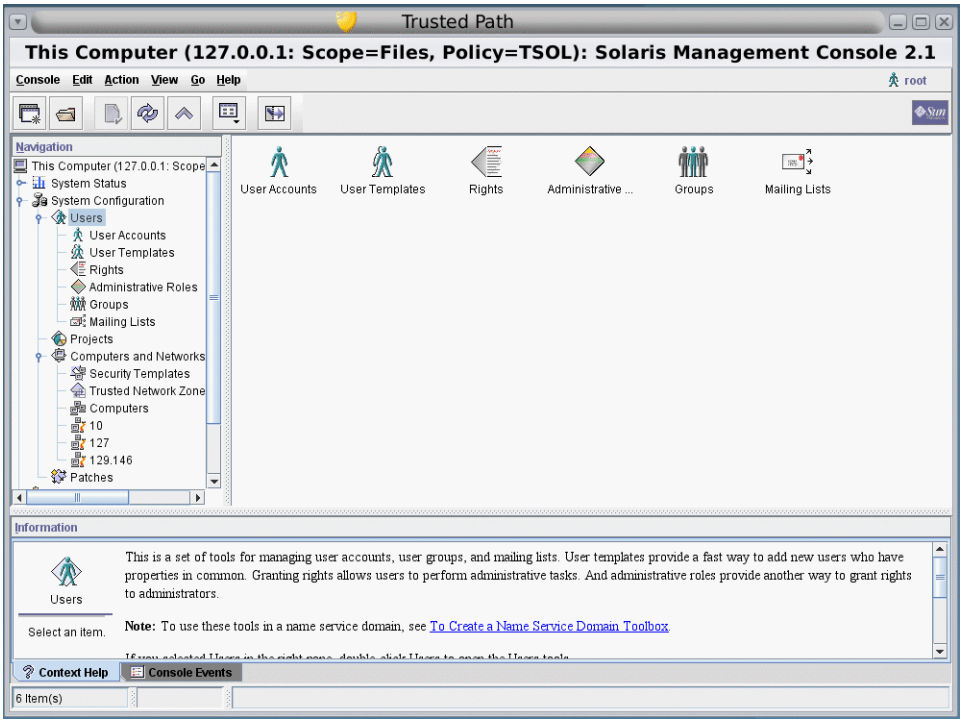
Trusted Extensions는 Solaris Management Console을 확장합니다.

- Trusted Extensions는 Solaris Management Console 사용자 도구 세트를 수정합니다. 도구 세트에 대한 소개는 **Oracle Solaris 관리: 기본 관리**의 2 장, “Solaris Management Console 작업(작업)”을 참조하십시오.
- Trusted Extensions는 Security Templates(보안 템플리트) 도구와 Trusted Network Zones(신뢰할 수 있는 네트워크 영역) 도구를 Computers and Networks(컴퓨터 및 네트워크) 도구 세트에 추가합니다.

Solaris Management Console 도구는 범위 및 보안 정책에 따라 **도구 상자**로 분류됩니다. Trusted Extensions 관리를 위해 Trusted Extensions는 `Policy=TSOL`인 도구 상자를 제공합니다. 범위, 즉 이름 지정 서비스를 통해 도구에 액세스할 수 있습니다. 사용 가능한 범위는 로컬 호스트와 LDAP입니다.

Solaris Management Console은 다음 그림에 나와 있습니다. `Scope=Files` Trusted Extensions 도구 상자가 로드되고 Users(사용자) 도구 세트가 열려 있습니다.

그림 2–3 Solaris Management Console의 일반적인 Trusted Extensions 도구 상자



Solaris Management Console의 Trusted Extensions 도구

Trusted Extensions는 구성 가능한 보안 속성을 다음 세 도구에 추가합니다.

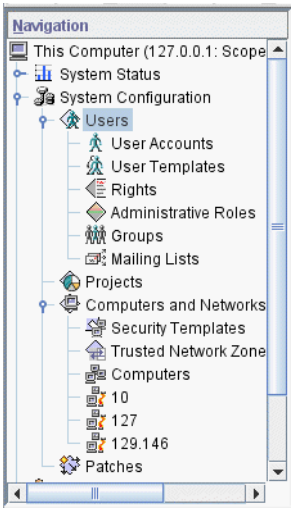
- **User Accounts(사용자 계정) 도구** – 사용자의 레이블 변경, 사용자의 레이블 보기 변경 및 계정 사용 제어를 위한 관리 인터페이스입니다.
- **Administrative Roles(관리 역할) 도구** – 사용자의 레이블 범위 및 유휴 상태일 때 화면 잠금 동작을 변경하기 위한 관리 인터페이스입니다.
- **Rights(권한) 도구** – 권한 프로파일에 지정할 수 있는 CDE 작업을 포함합니다. 이러한 작업에 보안 속성을 지정할 수 있습니다.

Trusted Extensions는 두 개의 도구를 Computers and Networks(컴퓨터 및 네트워크) 도구 세트에 추가합니다.

- **Security Templates(보안 템플리트) 도구** – 호스트 및 네트워크의 레이블 항목 관리를 위한 관리 인터페이스입니다. 이 도구는 `tnrhtp` 및 `tnrhdb` 데이터베이스를 수정하고, 구문 정확성을 적용하며, 변경 사항으로 커널을 업데이트합니다.
- **Trusted Network Zones(신뢰할 수 있는 네트워크 영역) 도구** – 영역의 레이블 항목 관리를 위한 관리 인터페이스입니다. 이 도구는 `tnzonecfg` 데이터베이스를 수정하고, 구문 정확성을 적용하며, 변경 사항으로 커널을 업데이트합니다.

그림 2–4는 사용자 도구 세트가 강조 표시된 파일 도구 상자를 나타냅니다. Trusted Extensions 도구는 Computers and Networks(컴퓨터 및 네트워크) 도구 세트 아래에 나타납니다.

그림 2–4 Solaris Management Console의 Computers and Networks(컴퓨터 및 네트워크) 도구 세트



Security Templates(보안 템플리트) 도구

보안 템플리트는 호스트 그룹에 지정할 수 있는 보안 속성 세트를 설명합니다. Security Templates(보안 템플리트) 도구를 사용하여 보안 속성의 특정 조합을 호스트 그룹에 편리하게 지정할 수 있습니다. 이러한 속성은 데이터가 패키징, 전송 및 해석되는 방법을 제어합니다. 템플리트에 지정된 호스트는 동일한 보안 설정을 가집니다.

호스트는 컴퓨터 도구에서 정의됩니다. 호스트의 보안 속성은 Security Templates(보안 템플리트) 도구에서 지정됩니다. Modify Template(템플리트 수정) 대화 상자에는 두 개의 탭이 있습니다.

- **General(일반) 탭** – 템플리트를 설명합니다. 이름, 호스트 유형, 기본 레이블, DOI(해석 도메인), 승인 범위 및 개별 민감도 레이블의 세트가 포함됩니다.
- **Hosts Assigned to Template(템플리트에 지정된 호스트) 탭** – 이 템플리트에 지정된 네트워크의 모든 호스트를 나열합니다.

신뢰할 수 있는 네트워킹 및 보안 템플리트는 12 장, “신뢰할 수 있는 네트워킹(개요)”에서 자세히 설명합니다.

Trusted Network Zones(신뢰할 수 있는 네트워크 영역) 도구

Trusted Network Zones(신뢰할 수 있는 네트워크 영역) 도구는 시스템의 영역을 식별합니다. 처음에는 전역 영역이 나열됩니다. 영역 및 해당 레이블을 추가하면 영역 이름이 창에 표시됩니다. 대개 시스템 구성 중에 영역이 만들어집니다. 레이블 지정, 다중 레벨 포트 구성 및 레이블 정책이 이 도구에서 구성됩니다. 자세한 내용은 10 장, “Trusted Extensions에서 영역 관리(작업)”를 참조하십시오.

Solaris Management Console에서 클라이언트와 서버 간 통신

일반적으로 Solaris Management Console 클라이언트는 시스템을 **원격으로** 관리합니다. LDAP을 이름 지정 서비스로 사용하는 네트워크에서 Solaris Management Console 클라이언트는 LDAP 서버에서 실행되는 Solaris Management Console 서버에 연결합니다. 다음 그림은 이 구성을 나타냅니다.

그림 2–5 LDAP 서버를 사용하여 네트워크를 관리하는 Solaris Management Console 클라이언트

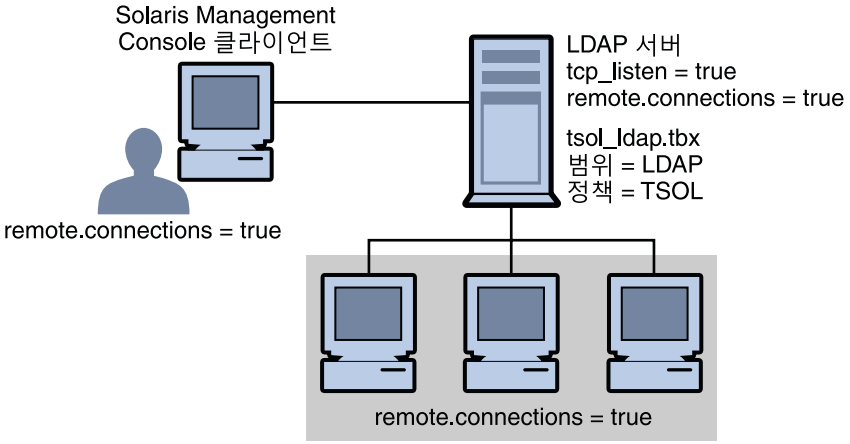
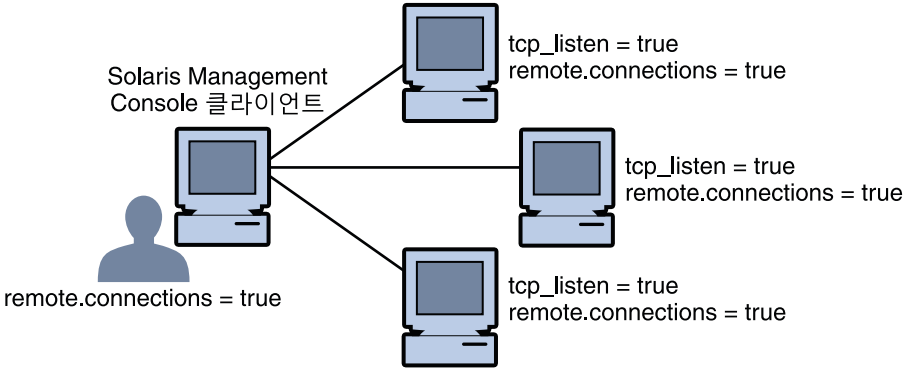


그림 2–6은 LDAP 서버로 구성되지 않은 네트워크를 나타냅니다. 관리자는 Solaris Management Console 서버에서 각 원격 시스템을 구성했습니다.

그림 2–6 네트워크의 개별 원격 시스템을 관리하는 Solaris Management Console 클라이언트

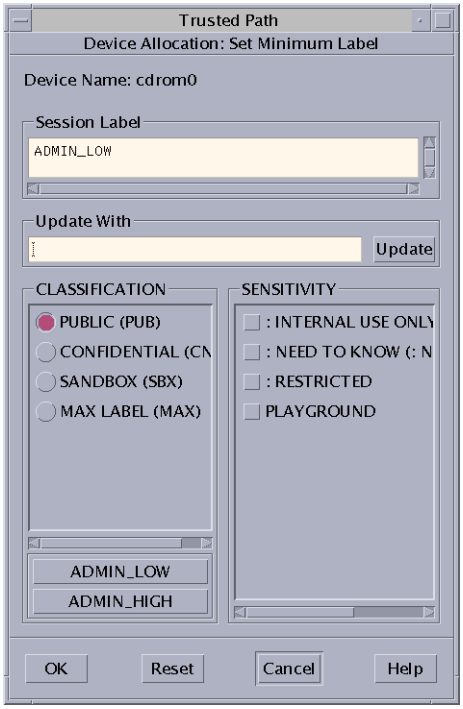


Solaris Management Console 설명서

Solaris Management Console 설명서의 주요 소스는 온라인 도움말입니다. 문맥에 따른 도움말이 현재 선택된 기능과 연결되어 있고 정보 창에 표시됩니다. 확장된 도움말 항목은 Help(도움말) 메뉴에서 보거나 문맥에 따른 도움말의 링크를 눌러 볼 수 있습니다. 추가 정보는 **Oracle Solaris 관리: 기본 관리**의 2 장, “Solaris Management Console 작업(작업)”에서 얻을 수 있습니다. 또한 **Oracle Solaris 관리: 기본 관리**의 “RBAC와 함께 Solaris 관리 도구 사용(작업 맵)”을 참조하십시오.

Trusted Extensions의 레이블 구축기

프로그램에서 레이블을 지정하도록 요구할 때 레이블 구축기 GUI를 통해 유효한 레이블이나 클리어런스를 선택할 수 있습니다. 예를 들어, 로그인 중에 레이블 구축기가 나타납니다(**Trusted Extensions User's Guide**의 2 장, "Logging In to Trusted Extensions (Tasks)" 참조). 작업 공간의 레이블을 변경하거나 Solaris Management Console에서 사용자, 영역 또는 네트워크 인터페이스에 레이블을 지정할 경우에도 레이블 구축기가 나타납니다. 레이블 범위를 새 장치에 지정할 때 다음 레이블 구축기가 나타납니다.



레이블 구축기에서 Classification(분류) 열의 구성 요소 이름은 `label_encodings` 파일의 `CLASSIFICATIONS` 구역에 해당합니다. Sensitivity(민감도) 열의 구성 요소 이름은 `label_encodings` 파일의 `WORDS` 구역에 해당합니다.

Trusted Extensions의 명령줄 도구

Trusted Extensions의 고유한 명령은 **Trusted Extensions Reference Manual**에 포함되어 있습니다. Trusted Extensions에서 수정하는 Oracle Solaris 명령은 **Oracle Solaris Reference Manual**에 포함되어 있습니다. `man` 명령은 모든 명령을 찾습니다.

다음 표에는 Trusted Extensions에 고유한 명령이 나열되어 있습니다. 명령은 매뉴얼 페이지 형식으로 나열되어 있습니다.

표 2–4 사용자 및 관리 Trusted Extensions 명령

매뉴얼 페이지	Trusted Extensions 수정	자세한 정보
`add_allocatable(1M)`	장치 할당 데이터베이스에 장치를 추가하여 할당할 수 있습니다. 기본적으로 분리 가능한 장치를 할당할 수 있습니다.	229 페이지 "Trusted Extensions에서 장치를 구성하는 방법"
`atohexlabel(1M)`	레이블을 16진수 형식으로 변환합니다.	71 페이지 "레이블에 해당하는 16진수를 얻는 방법"
`chk_encodings(1M)`	`label_encodings` 파일의 무결성을 검사합니다.	**Trusted Extensions Label Administration**의 "How to Debug a label_encodings File"
`dtappsession(1)`	Application Manager(응용 프로그램 관리자)를 사용하여 원격 Trusted CDE 세션을 엽니다.	8 장, "Trusted Extensions에서 원격 관리(작업)"
`getlabel(1)`	선택된 파일이나 디렉토리의 레이블을 표시합니다.	124 페이지 "마운트된 파일의 레이블을 표시하는 방법"
`getzonepath(1)`	특정 영역의 전체 경로 이름을 표시합니다.	**Trusted Extensions Developer's Guide**의 "Acquiring a Sensitivity Label"
`hextoalabel(1M)`	16진수 레이블을 읽을 수 있는 레이블로 변환합니다.	72 페이지 "읽기 가능한 레이블을 해당 16진수 형식에서 얻는 방법"
`plabel(1)`	현재 프로세스의 레이블을 표시합니다.	매뉴얼 페이지를 참조하십시오.
`remove_allocatable(1M)`	장치 할당 데이터베이스에서 해당 항목을 제거하여 장치의 할당을 막습니다.	229 페이지 "Trusted Extensions에서 장치를 구성하는 방법"
`setlabel(1)`	선택된 항목의 레이블을 재지정합니다. `solaris.label.file.downgrade` 또는 `solaris.label.file.upgrade` 권한 부여가 필요합니다. 이러한 권한 부여는 Object Label Management 권한 프로파일에 있습니다.	동일한 GUI 절차는 **Trusted Extensions User's Guide**의 "How to Move Files Between Labels in Trusted CDE"을 참조하십시오.
`smtnrhdb(1M)`	`tnrhdb` 데이터베이스의 항목을 로컬에서 또는 이름 지정 서비스 데이터베이스에서 관리합니다.	Solaris Management Console을 사용하는 동일한 절차는 168 페이지 "신뢰할 수 있는 네트워크 데이터베이스 구성(작업 맵)"을 참조하십시오.

표 2–4 사용자 및 관리 Trusted Extensions 명령 (계속)

매뉴얼 페이지	Trusted Extensions 수정	자세한 정보
smtnrhtp(1M)	tnrhtp 데이터베이스의 항목을 로컬에서 또는 이름 지정 서비스 데이터베이스에서 관리합니다.	매뉴얼 페이지를 참조하십시오.
smtnzonecfg(1M)	로컬 tnzonecfg 데이터베이스의 항목을 관리합니다.	Solaris Management Console을 사용하는 동일한 절차는 132 페이지 "영역에 대한 다중 레벨 포트를 만드는 방법"을 참조하십시오.
tnchkdb(1M)	tnrhdb 및 tnrhtp 데이터베이스의 무결성을 검사합니다.	183 페이지 "신뢰할 수 있는 네트워크 데이터베이스의 구문을 확인하는 방법"
tnctl(1M)	네트워크 정보를 커널에 캐시로 저장합니다.	185 페이지 "커널 캐시를 신뢰할 수 있는 네트워크 데이터베이스와 동기화하는 방법"
tnd(1M)	신뢰할 수 있는 네트워크 데몬을 실행합니다.	185 페이지 "커널 캐시를 신뢰할 수 있는 네트워크 데이터베이스와 동기화하는 방법"
tninfo(1M)	커널 레벨 네트워크 정보 및 통계를 표시합니다.	184 페이지 "신뢰할 수 있는 네트워크 데이터베이스 정보를 커널 캐시와 비교하는 방법"
updatehome(1M)	현재 레이블에 대한 .copy_files 및 .link_files를 업데이트합니다.	86 페이지 "Trusted Extensions에서 사용자의 시작 파일을 구성하는 방법"

다음 표에는 Trusted Extensions에서 수정하거나 확장하는 Oracle Solaris 명령이 나열되어 있습니다. 명령은 매뉴얼 페이지 형식으로 나열되어 있습니다.

표 2–5 Trusted Extensions에서 수정하는 사용자 및 관리 명령

매뉴얼 페이지	Trusted Extensions 수정	자세한 정보
allocate(1)	할당된 장치를 지우고 장치를 특정 영역에 할당하는 옵션을 추가합니다. Trusted Extensions에서 일반 사용자는 이 명령을 사용하지 않습니다.	**Trusted Extensions User's Guide**의 "How to Allocate a Device in Trusted Extensions"
deallocate(1)	장치를 지우고 장치를 특정 영역에서 할당 해제하는 옵션을 추가합니다. Trusted Extensions에서 일반 사용자는 이 명령을 사용하지 않습니다.	**Trusted Extensions User's Guide**의 "How to Allocate a Device in Trusted Extensions"
list_devices(1)	권한 부여 및 레이블과 같은 장치 속성을 표시하는 -a 옵션을 추가합니다. 할당된 장치 유형의 기본 속성을 표시하는 -d 옵션을 추가합니다. 레이블이 있는 영역에 할당할 수 있는 장치를 표시하는 -z 옵션을 추가합니다.	매뉴얼 페이지를 참조하십시오.

표 2–5 Trusted Extensions에서 수정하는 사용자 및 관리 명령 (계속)

매뉴얼 페이지	Trusted Extensions 수정	자세한 정보
tar(1)	레이블이 있는 파일 및 디렉토리를 아카이브하고 추출하는 -T 옵션을 추가합니다.	142 페이지 "Trusted Extensions에서 파일을 백업하는 방법" 및 142 페이지 "Trusted Extensions에서 파일을 복원하는 방법"
auditconfig(1M)	windata_down 및 windata_up 감사 정책 옵션을 추가합니다.	**System Administration Guide: Security Services**의 "How to Configure Audit Policy"
auditreduce(1M)	레이블로 감사 레코드를 선택하는 -l 옵션을 추가합니다.	**System Administration Guide: Security Services**의 "How to Select Audit Events From the Audit Trail"
automount(1M)	상위 레이블에서 영역 이름 및 영역 표시를 고려하여 auto_home 맵의 이름과 내용을 수정합니다.	139 페이지 "Trusted Extensions의 자동 마운트 변경 사항"
ifconfig(1M)	시스템의 모든 영역에서 인터페이스를 사용할 수 있게 하는 all-zones 옵션을 추가합니다.	187 페이지 "호스트의 인터페이스가 작동 중인지 확인하는 방법"
netstat(1M)	소켓 및 경로 지정 테이블 항목에 대한 확장 보안 속성을 표시하는 -R 옵션을 추가합니다.	188 페이지 "Trusted Extensions 네트워크를 디버깅하는 방법"
route(1M)	경로의 보안 속성인 cipso, doi, max_sl 및 min_sl을 표시하는 -secattr 옵션을 추가합니다.	182 페이지 "보안 속성으로 경로를 구성하는 방법"

Trusted Extensions에서 원격 관리

ssh 명령, dtappsession 프로그램 또는 Solaris Management Console을 사용하여 Trusted Extensions로 구성된 시스템을 원격으로 관리할 수 있습니다. 보안 정책에서 허용하는 경우 이로 인해 보안이 약화되더라도 Trusted Extensions가 아닌 호스트에서 로그인할 수 있게 Trusted Extensions 호스트를 구성할 수 있습니다. 자세한 내용은 8 장, "Trusted Extensions에서 원격 관리(작업)"를 참조하십시오.

◆ ◆ ◆ 3 장

3 Trusted Extensions 관리자로 시작하기(작업)

이 장에서는 Trusted Extensions를 사용하여 구성된 시스템을 관리하는 방법에 대해 소개합니다.

- 47 페이지 “Trusted Extensions의 새로운 기능”
- 48 페이지 “Trusted Extensions 관리 시 보안 요구 사항”
- 49 페이지 “Trusted Extensions 관리자로 시작하기(작업 맵)”

Trusted Extensions의 새로운 기능

Solaris 10 1/13 – 이 릴리스에서 Trusted Extensions는 인쇄 부속 시스템에 대한 감사 이벤트를 추가합니다. 신뢰할 수 있는 인쇄 이벤트 `AUE_print_request`, `AUE_print_request_ps`, `AUE_print_request_unlabeled` 및 `AUE_print_request_nobanner`의 정의는 `/etc/security/audit_event` 파일을 읽어보십시오.

Solaris 10 10/08 – 이 릴리스에서 Trusted Extensions는 다음과 같은 기능을 제공합니다.

- Trusted Extensions 공유 IP 스택을 사용하면 기본 경로를 통해 레이블이 있는 영역을 전역 영역과 서로 간에 격리시킬 수 있습니다.
- 루프백 인터페이스 `lo0`은 `all-zones` 인터페이스입니다.
- 역할별로 책임 구분을 적용할 수 있습니다. 시스템 관리자 역할은 사용자를 만들 수 있지만 암호를 지정할 수 없습니다. 보안 관리자 역할은 암호를 지정할 수 있지만 사용자를 만들 수 없습니다. 자세한 내용은 **Trusted Extensions Configuration Guide**의 “Create Rights Profiles That Enforce Separation of Duty”.
- 이 설명서의 부록 B, “Trusted Extensions 매뉴얼 페이지 목록”에 Trusted Extensions 매뉴얼 페이지 목록이 포함되어 있습니다.

Solaris 10 5/08 – 이 릴리스에서 Trusted Extensions는 다음과 같은 기능을 제공합니다.

- SMF(서비스 관리 기능)는 Trusted Extensions를 `svc:/system/labeld` 서비스로 관리합니다. 기본적으로 `labeld` 서비스는 사용 안함으로 설정되어 있습니다. 서비스가 사용으로 설정되면 시스템을 구성하고 재부트하여 Trusted Extensions 보안 정책을 적용해야 합니다.
- 시스템에서 사용되는 CIPSO DOI(Domain of Interpretation) 번호는 구성 가능합니다.
  - DOI에 대한 자세한 내용은 156 페이지 “Trusted Extensions의 네트워크 보안 속성”을 참조하십시오.
  - DOI를 기본값과 다르게 지정하려면 **Trusted Extensions Configuration Guide**의 “Configure the Domain of Interpretation”을 참조하십시오.
- Trusted Extensions는 NFS 버전 3(NFSv3)과 NFS 버전 4(NFSv4)가 마운트된 파일 시스템에서 CIPSO 레이블을 인식합니다. 따라서 Trusted Extensions 시스템에서 NFSv3 파일 시스템을 레이블이 있는 파일 시스템으로 마운트할 수 있습니다. udp를 NFSv3에서 다중 레벨 마운트에 대한 기본 프로토콜로 사용하려면 132 페이지 “udp를 통해 NFSv3에 대한 다중 레벨 포트를 구성하는 방법”을 참조하십시오.
- 이름 서비스 캐시 데몬 `nscd`를 레이블이 있는 모든 영역의 영역 레이블에서 실행하도록 구성할 수 있습니다.

Trusted Extensions 관리 시 보안 요구 사항

Trusted Extensions에서 역할은 시스템을 관리하는 일반적인 방법입니다. 일반적으로 수퍼유저는 사용되지 않습니다. 역할은 Oracle Solaris OS에서와 같은 방법으로 만들고, 대부분의 작업은 역할에 의해 수행됩니다. Trusted Extensions에서 `root` 사용자는 관리 작업을 수행하는 데 사용되지 않습니다.

Trusted Extensions 사이트의 일반적인 역할은 다음과 같습니다.

- `root` **역할** – 초기 설정 팀에서 만듭니다.
- **보안 관리자 역할** – 초기 설정 팀에서 초기 구성 중에 또는 초기 구성 후에 만듭니다.
- **시스템 관리자 역할** – 보안 관리자 역할이 만듭니다.

Oracle Solaris OS에서와 마찬가지로 기본 관리자 역할, 운영자 역할 등을 만들 수도 있습니다. `root` 역할을 제외하고 사용자가 만드는 역할은 이름 지정 서비스에서 관리할 수 있습니다.

Oracle Solaris OS에서와 마찬가지로 역할이 지정된 사용자만 해당 역할을 맡을 수 있습니다. Solaris Trusted Extensions(CDE)에서는 Trusted Path(신뢰할 수 있는 경로)라는 데스크탑 메뉴에서 역할을 맡을 수 있습니다. Solaris Trusted Extensions(JDS)에서는 신뢰할 수 있는 스트라이프에 사용자 이름이 표시된 경우에 역할을 맡을 수 있습니다. 사용자 이름을 누르면 역할 선택 옵션이 표시됩니다.

Trusted Extensions에서 역할 만들기

Trusted Extensions를 관리하려면 시스템 기능과 보안 기능을 나누는 역할을 만듭니다. 구성 중에 초기 설치 팀에서 보안 관리자 역할을 만들었습니다. 자세한 내용은 **Trusted Extensions Configuration Guide**의 "Create the Security Administrator Role in Trusted Extensions"를 참조하십시오.

Trusted Extensions에서 역할을 만드는 절차는 Oracle Solaris OS 프로세스와 동일합니다. 2장, "Trusted Extensions 관리 도구"에서 설명한 것처럼 Solaris Management Console은 Trusted Extensions에서 역할을 관리하는 데 사용되는 GUI입니다.

- 역할 만들기에 대한 개요는 **System Administration Guide: Security Services**의 10 장, "Role-Based Access Control (Reference)" 및 **System Administration Guide: Security Services**의 "Using RBAC (Task Map)"를 참조하십시오.
- 수퍼유저와 동등한 강력한 역할을 만들려면 **Oracle Solaris 관리: 기본 관리**의 "기본 관리자 역할 만들기"를 참조하십시오. Trusted Extensions를 사용하는 사이트에서 기본 관리자 역할이 보안 정책을 위반할 수 있습니다. 이러한 사이트에서는 `root`를 역할로 전환하여 보안 관리자 역할을 만듭니다.
- `root` 역할을 만들려면 **System Administration Guide: Security Services**의 "How to Make root User Into a Role"을 참조하십시오.
- Solaris Management Console을 사용하여 역할을 만들려면 **System Administration Guide: Security Services**의 "How to Create and Assign a Role by Using the GUI"를 참조하십시오.

Trusted Extensions에서 역할 맡기

Oracle Solaris OS와 달리 Trusted Extensions는 Trusted Path(신뢰할 수 있는 경로) 메뉴에서 Assume *Rolename* Role(Rolename 역할 맡기) 메뉴 항목을 제공합니다. 역할 암호를 확인하면 소프트웨어에서 신뢰할 수 있는 경로 속성을 사용하여 역할 작업 공간을 활성화합니다. 역할 작업 공간은 관리 작업 공간입니다. 이러한 작업 공간은 전역 영역에 있습니다.

Trusted Extensions 관리자로 시작하기(작업 맵)

Trusted Extensions를 관리하기 전에 다음 절차를 숙지하십시오.

작업	설명	수행 방법
로그인합니다.	안전하게 로그인합니다.	**Trusted Extensions User's Guide**의 "Logging In to Trusted Extensions"

작업	설명	수행 방법
데스크탑에서 일반적인 사용자 작업을 수행합니다.	작업은 다음과 같습니다. ■ 작업 공간 구성 ■ 다른 레이블에서 작업 공간 사용 ■ Trusted Extensions 매뉴얼 페이지 액세스 ■ Trusted Extensions 온라인 도움말 액세스	**Trusted Extensions User's Guide**의 "Working on a Labeled System"
신뢰할 수 있는 경로가 필요한 작업을 수행합니다.	작업은 다음과 같습니다. ■ 장치 할당 ■ 암호 변경 ■ 작업 공간의 레이블 변경	**Trusted Extensions User's Guide**의 "Performing Trusted Actions"
유용한 역할을 만듭니다.	사이트에 대한 관리 역할을 만듭니다. LDAP에서 역할 만들기는 일회성 작업입니다. 보안 관리자 역할은 유용한 역할입니다.	49 페이지 "Trusted Extensions에서 역할 만들기" **Trusted Extensions Configuration Guide**의 "Create the Security Administrator Role in Trusted Extensions"
(선택 사항) root를 역할로 만듭니다.	root에 의한 익명 로그인을 방지합니다. 이 작업은 시스템당 한 번만 수행됩니다.	**System Administration Guide: Security Services**의 "How to Make root User Into a Role"
역할을 수락합니다.	역할의 전역 영역으로 들어갑니다. 모든 관리 작업은 전역 영역에서 수행됩니다.	51 페이지 "Trusted Extensions에서 전역 영역으로 들어가는 방법"
역할 작업 공간을 종료하고 일반 사용자가 됩니다.	전역 영역에서 나옵니다.	52 페이지 "Trusted Extensions에서 전역 영역을 종료하는 방법"
사용자, 역할, 권한, 영역 및 네트워크를 로컬에서 관리합니다.	Solaris Management Console을 사용하여 분산 시스템을 관리합니다.	52 페이지 "Solaris Management Console에서 로컬 시스템을 관리하는 방법"
Trusted CDE 작업을 사용하여 시스템을 관리합니다.	Trusted_Extensions 폴더에서 관리 작업을 사용합니다.	54 페이지 "Trusted Extensions에서 CDE 관리 작업을 시작하는 방법"
관리 파일을 편집합니다.	신뢰할 수 있는 편집기에서 파일을 편집합니다.	54 페이지 "Trusted Extensions에서 관리 파일을 편집하는 방법"
장치 할당을 관리합니다.	Device Allocation Manager(장치 할당 관리자) – Device Administration GUI(장치 관리 GUI)를 사용합니다.	228 페이지 "Trusted Extensions에서 장치 관리(작업 맵)"

▼ Trusted Extensions에서 전역 영역으로 들어가는 방법

역할을 맡아서 Trusted Extensions에서 전역 영역으로 들어갑니다. 전체 시스템은 전역 영역에서만 관리할 수 있습니다. 수퍼유저 또는 역할만 전역 영역에 들어갈 수 있습니다.

역할을 맡으면 역할은 사용자 레이블에서 작업 공간을 만들어 레이블이 있는 영역에서 관리 파일을 편집할 수 있습니다.

문제 해결을 위해 Failsafe Session(비상 안전 세션)을 시작하여 전역 영역에 들어갈 수도 있습니다. 자세한 내용은 88 페이지 “Trusted Extensions에서 비상 안전 세션에 로그인하는 방법”을 참조하십시오.

시작하기 전에 하나 이상의 역할을 만들었거나 수퍼유저로 전역 영역에 들어가려고 합니다. 요약 내용은 49 페이지 “Trusted Extensions에서 역할 만들기”를 참조하십시오.

1 **신뢰할 수 있는 방식을 사용합니다.**

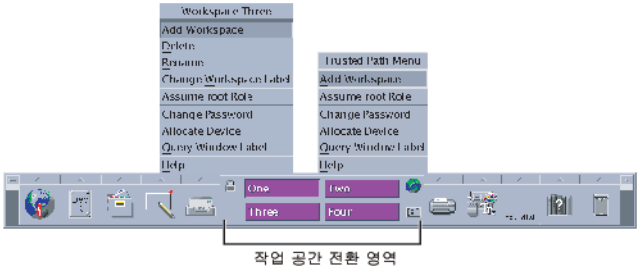
- **Solaris Trusted Extensions(JDS)의 신뢰할 수 있는 스트라이프에서 사용자 이름을 누르고 역할을 선택합니다.**

  역할이 지정된 경우 역할 이름이 목록에 표시됩니다.

  Trusted Extensions 데스크탑 기능의 위치와 중요성은 **Trusted Extensions User's Guide**의 4 장, “Elements of Trusted Extensions (Reference)”를 참조하십시오.

- **Solaris Trusted Extensions(CDE)에서는 Trusted Path(신뢰할 수 있는 경로) 메뉴를 엽니다.**

  a. **Workspace Switch Area(작업 공간 전환 영역)에서 마우스 버튼 3을 누릅니다.**



  b. **Trusted Path(신뢰할 수 있는 경로) 메뉴에서 Assume *rolename* Role(역할 이름 역할 맡기)을 선택합니다.**

2 **프롬프트에 역할 암호를 입력합니다.**

Trusted CDE에서 새 역할 작업 공간을 만들면 작업 공간 전환 버튼이 역할 데스크탑 색상으로 변경되고 각 창 위의 제목 표시줄에 `Trusted Path`가 표시됩니다. Trusted JDS에서는 현재 작업 공간이 역할 작업 공간으로 변경됩니다.

Trusted CDE에서 마우스로 일반 사용자 작업 공간을 선택하여 역할 작업 공간을 떠납니다. 마지막 역할 작업 공간을 삭제하여 역할을 종료할 수도 있습니다. Trusted JDS의 신뢰할 수 있는 스트라이프에서 역할 이름을 누르고 메뉴에서 다른 역할 또는 사용자를 선택합니다. 그러면 현재 작업 공간이 새 역할 또는 사용자의 프로세스로 변경됩니다.

▼ Trusted Extensions에서 전역 영역을 종료하는 방법

Trusted JDS와 Trusted CDE의 기존 역할에 대한 메뉴 위치는 서로 다릅니다.

시작하기 전에 사용자가 전역 영역에 있습니다.

- **두 데스크탑 모두의 Workspace Switch Area(작업 공간 전환 영역)에서 사용자 작업 공간을 누를 수 있습니다.**

  다음 중 하나를 수행하여 역할 작업 공간과 전역 영역을 종료할 수도 있습니다.

  - **Trusted JDS의 신뢰할 수 있는 스트라이프에서 역할 이름을 누릅니다.**

    역할 이름을 누르면 사용자 이름과 맡을 수 있는 역할 목록이 표시됩니다. 사용자 이름을 선택하면 해당 작업 공간에서 만드는 모든 후속 창이 선택한 이름으로 만들어집니다. 현재 데스크탑에서 이전에 만든 창은 해당 역할의 이름과 레이블로 계속 표시됩니다.

    다른 역할 이름을 선택하면 전역 영역에서 다른 역할로 유지됩니다.

  - **Trusted CDE에서 역할 작업 공간을 삭제합니다.**

    작업 공간 버튼에서 마우스 버튼 3을 누르고 Delete(삭제)를 선택합니다. 사용했던 마지막 작업 공간으로 돌아갑니다.

▼ Solaris Management Console에서 로컬 시스템을 관리하는 방법

시스템에서 Solaris Management Console을 처음으로 시작하는 경우 도구를 등록하고 다양한 디렉토리를 만드는 동안 지연 시간이 발생합니다. 이 지연은 일반적으로 시스템 구성 중에 발생합니다. 절차는 **Trusted Extensions Configuration Guide**의 "Initialize the Solaris Management Console Server in Trusted Extensions"를 참조하십시오.

원격 시스템을 관리하려면 102 페이지 "원격으로 Trusted Extensions 관리(작업 맵)"를 참조하십시오.

시작하기 전에 맡은 역할이 있어야 합니다. 자세한 내용은 51 페이지 “Trusted Extensions에서 전역 영역으로 들어가는 방법”을 참조하십시오.

1. **Solaris Management Console을 시작합니다.**

   Solaris Trusted Extensions(JDS)에서는 명령줄을 사용합니다.

   ```
   $ /usr/sbin/smc &
   ```

   Trusted CDE에서는 세 가지 선택 옵션이 있습니다.

   - **단말기 창에서 `smc` 명령을 사용합니다.**
   - **Front Panel(전면 패널)의 Tools(도구) 풀업 메뉴에서 Solaris Management Console 아이콘을 누릅니다.**
   - **Trusted_Extensions 폴더에서 Solaris Management Console 아이콘을 두 번 누릅니다.**

2. **Console(콘솔) -> Open Toolbox(도구 상자 열기)를 선택합니다.**

3. **목록에서 해당 범위의 Trusted Extensions 도구 상자를 선택합니다.**

   Trusted Extensions 도구 상자에 `Policy=TSOL`이 이름의 일부로 포함됩니다. Files(파일) 범위는 현재 시스템에 있는 로컬 파일을 업데이트합니다. LDAP 범위는 Oracle Directory Server Enterprise Edition에서 LDAP 디렉토리를 업데이트합니다. 도구 상자 이름이 다음과 비슷하게 표시됩니다.

   이 컴퓨터(*this-host*`: Scope=Files, Policy=TSOL`)
   이 컴퓨터(*ldap-server*`: Scope=LDAP, Policy=TSOL`)

4. **원하는 Solaris Management Console 도구로 이동합니다.**

   암호 프롬프트가 표시됩니다.

   Trusted Extensions에서 수정된 도구를 보려면 System Configuration(시스템 구성)을 누르십시오.

5. **암호를 입력합니다.**

   Solaris Management Console 도구에 대한 자세한 내용은 온라인 도움말을 참조하십시오. Trusted Extensions에서 수정하는 도구에 대한 소개 내용은 38 페이지 “Solaris Management Console 도구”를 참조하십시오.

6. **GUI를 닫으려면 Console(콘솔) 메뉴에서 Exit(종료)을 선택합니다.**

▼ Trusted Extensions에서 CDE 관리 작업을 시작하는 방법

1 **역할을 수락합니다.**

자세한 내용은 51 페이지 “Trusted Extensions에서 전역 영역으로 들어가는 방법”을 참조하십시오.

2 **Trusted CDE에서 Application Manager(응용 프로그램 관리자)를 불러옵니다.**

a. **배경을 마우스 버튼 3으로 눌러 Workspace(작업 공간) 메뉴를 불러옵니다.**

b. **Applications(응용 프로그램)를 누른 다음 Application Manager(응용 프로그램 관리자) 메뉴 항목을 누릅니다.**

Trusted_Extensions 폴더는 Application Manager(응용 프로그램 관리자)에 있습니다.

3 **Trusted_Extensions 폴더를 엽니다.**

4 **해당 아이콘을 두 번 누릅니다.**

관리 작업 목록은 35 페이지 “Trusted CDE 작업”을 참조하십시오.

▼ Trusted Extensions에서 관리 파일을 편집하는 방법

감사 기능이 통합된 신뢰할 수 있는 편집기를 사용하여 관리 파일을 편집합니다. 이 편집기를 사용하면 셸 명령을 실행하여 원래 파일을 다른 이름으로 저장할 수 없습니다.

1 **역할을 수락합니다.**

자세한 내용은 51 페이지 “Trusted Extensions에서 전역 영역으로 들어가는 방법”을 참조하십시오.

2 **신뢰할 수 있는 편집기를 엽니다.**

- **Solaris Trusted Extensions(CDE)에서 다음을 수행합니다.**

  a. **편집기를 불러오려면 배경을 마우스 버튼 3으로 눌러 Workspace(작업 공간) 메뉴를 불러옵니다.**

  b. **Applications(응용 프로그램)를 누른 다음 Application Manager(응용 프로그램 관리자) 메뉴 항목을 누릅니다.**

  Trusted_Extensions 폴더는 Application Manager(응용 프로그램 관리자)에 있습니다.

  c. **Trusted_Extensions 폴더를 엽니다.**

  d. **관리 편집기 작업을 두 번 누릅니다.**

  파일 이름을 제공하라는 메시지가 표시됩니다. 형식은 단계 3 및 단계 4를 참조하십시오.

- **Solaris Trusted Extensions(JDS)에서 다음을 수행합니다.**

  - **(옵션) `gedit`를 신뢰할 수 있는 편집기로 사용하려면 `EDITOR` 변수를 수정합니다.**

  자세한 내용은 68 페이지 “선택한 편집기를 신뢰할 수 있는 편집기로 지정하는 방법”을 참조하십시오.

  - **명령줄을 사용하여 신뢰할 수 있는 편집기를 불러옵니다.**

  ```
  # /usr/dt/bin/trusted_edit filename
  ```

  파일 이름 인수를 제공해야 합니다.

3 **새 파일을 만들려면 새 파일의 전체 경로 이름을 입력합니다.**

파일을 저장하면 편집기에서 임시 파일을 만듭니다.

4 **기존 파일을 편집하려면 기존 파일의 전체 경로 이름을 입력합니다.**

주 – 편집기에 Save As(다른 이름으로 저장) 옵션이 있는 경우 해당 옵션을 사용하지 마십시오. 편집기의 Save(저장) 옵션을 사용하여 파일을 저장합니다.

---

5 **파일을 지정된 경로 이름으로 저장하려면 편집기를 닫습니다.**

◆ ◆ ◆ 4 장

4 Trusted Extensions 시스템의 보안 요구 사항(개요)

이 장에서는 Trusted Extensions를 사용하여 구성된 시스템에서 구성 가능한 보안 기능에 대해 설명합니다.

- 57 페이지 "구성 가능한 Oracle Solaris 보안 기능"
- 59 페이지 "보안 요구 사항 적용"
- 62 페이지 "데이터에 대한 보안 레벨 변경 규칙"
- 64 페이지 "Solaris Trusted Extensions(CDE) 사용자 정의"

구성 가능한 Oracle Solaris 보안 기능

Trusted Extensions는 Oracle Solaris OS에서 제공하는 것과 동일한 보안 기능을 사용하며 일부 기능이 추가되었습니다. 예를 들어, Oracle Solaris OS는 `eeprom` 보호, 암호 요구 사항 및 강력한 암호 알고리즘, 사용자 잠금을 통한 시스템 보호, 키보드 종료를 통한 보호 기능을 제공합니다.

Trusted Extensions는 이러한 보안 기본값을 수정하는 데 사용되는 실제 절차가 Oracle Solaris OS에서와 다릅니다. Trusted Extensions에서는 일반적으로 역할을 맡아서 시스템을 관리합니다. 신뢰할 수 있는 편집기를 사용하여 로컬 설정을 수정합니다. 사용자, 역할 및 호스트의 네트워크에 적용되는 사항은 Solaris Management Console에서 변경합니다.

Trusted Extensions의 보안 기능 구성 인터페이스

Trusted Extensions에서 보안 설정을 수정하는 데 특정 인터페이스가 필요한 경우 이 문서에 절차가 제공됩니다. 이 인터페이스는 Oracle Solaris OS에서는 선택 사항입니다. Trusted Extensions에서 로컬 파일을 편집하기 위해 신뢰할 수 있는 편집기가 필요한 경우 이 문서에 별도의 절차가 제공되지 않습니다. 예를 들어, 95 페이지 "사용자에 대한 계정 잠금을 방지하는 방법" 절차에서는 Solaris Management Console를 사용하여 계정 잠금을 방지하도록 사용자 계정을 업데이트하는 방법에 대해 설명합니다. 하지만, 시스템

차원의 암호 잠금 정책을 설정하는 절차에 대해서는 본 문서에서 설명하지 않습니다. Oracle Solaris 지침을 따릅니다. 단, Trusted Extensions에서는 신뢰할 수 있는 편집기를 사용하여 시스템 파일을 수정합니다.

Trusted Extensions를 통해 Oracle Solaris 보안 방식 확장

Oracle Solaris OS에서와 마찬가지로 다음 Oracle Solaris 보안 방식은 Trusted Extensions에서 확장할 수 있습니다.

- **감사 이벤트 및 클래스** – 감사 이벤트 및 감사 클래스를 추가하는 방법은 **System Administration Guide: Security Services**의 30 장, "Managing Oracle Solaris Auditing (Tasks)"를 참조하십시오.
- **권한 프로파일** – 권한 프로파일을 추가하는 방법은 **System Administration Guide: Security Services**의 제III부, "Roles, Rights Profiles, and Privileges"를 참조하십시오.
- **역할** – 역할을 추가하는 방법은 **System Administration Guide: Security Services**의 제III부, "Roles, Rights Profiles, and Privileges"를 참조하십시오.
- **권한 부여** – 새 권한 부여를 추가하는 예는 237 페이지 "Trusted Extensions에서 장치 권한 부여 사용자 정의(작업 맵)"를 참조하십시오.

Oracle Solaris OS에서와 마찬가지로 권한은 확장할 수 없습니다.

Trusted Extensions 보안 기능

Trusted Extensions는 다음과 같은 고유한 보안 기능을 제공합니다.

- **레이블** – 주체와 객체에 레이블이 지정됩니다. 프로세스에 레이블이 지정됩니다. 영역과 네트워크에 레이블이 지정됩니다.
- **Device Allocation Manager(장치 할당 관리자)** – 기본적으로 장치는 할당 요구 사항에 의해 보호됩니다. Device Allocation Manager(장치 할당 관리자) GUI는 관리자와 일반 사용자를 위한 인터페이스입니다.
- **Change Password(암호 변경) 메뉴 항목** – Trusted Path(신뢰할 수 있는 경로) 메뉴를 사용하여 사용자 암호와 맡은 역할의 암호를 변경할 수 있습니다.

보안 요구 사항 적용

시스템 보안이 손상되지 않도록 관리자는 암호, 파일 및 감사 데이터를 보호해야 합니다. 사용자에게 각자 맡은 부분을 수행하도록 교육해야 합니다. 평가된 구성에 대해 요구 사항을 일관되게 유지하려면 이 섹션의 지침을 따르십시오.

사용자 및 보안 요구 사항

각 사이트의 보안 관리자는 사용자에게 보안 절차에 대해 교육해야 합니다. 보안 관리자는 신입 직원에게 다음 규칙에 대해 전달하고 기존 직원에게 해당 규칙에 대해 정기적으로 상기시켜야 합니다.

- 암호를 아무에게도 말하지 마십시오.

  다른 사람이 암호를 알고 있는 경우 책임을 지지 않고 사용자가 액세스할 수 있는 동일한 정보에 몰래 액세스할 수 있습니다.
- 암호를 기록해 두거나 전자 메일 메시지에 포함시키지 마십시오.
- 추측하기 어려운 암호를 선택하십시오.
- 암호를 다른 사람에게 전자 메일로 보내지 마십시오.
- 화면을 잠그거나 로그오프하지 않고 컴퓨터를 떠나지 마십시오.
- 관리자는 전자 메일을 통해 사용자에게 지침을 전달하지 않습니다. 따라서 관리자가 전자 메일로 보낸 지침은 따르지 말고 다시 한 번 관리자의 확인을 받으십시오.

  전자 메일의 보낸 사람 정보가 위조되었을 수 있습니다.
- 자신이 만든 파일과 디렉토리에 대한 액세스 권한은 사용자의 책임이므로 해당 파일과 디렉토리에 대한 사용 권한이 올바르게 설정되어 있는지 확인하십시오. 권한 부여되지 않은 사용자에게 파일 읽기, 파일 변경, 디렉토리 내용 보기 또는 디렉토리에 추가 권한을 허용하지 마십시오.

사이트에서 추가 제안 사항을 제공할 수 있습니다.

전자 메일 사용

전자 메일을 사용하여 사용자에게 수행할 작업을 지시하는 것은 안전한 방법이 아닙니다.

관리자가 보낸 지침이 포함된 전자 메일을 신뢰하지 않도록 사용자에게 지시하십시오. 그러면 스푸핑된 전자 메일 메시지를 통해 사용자를 속여서 암호를 특정 값으로 변경하거나 암호를 알려달라고 하여 해당 암호로 로그인한 다음 시스템을 손상시킬 수 있는 시도를 차단할 수 있습니다.

암호 적용

시스템 관리자 역할은 새 계정을 만들 때 고유한 사용자 이름과 사용자 ID를 지정해야 합니다. 새 계정에 대한 이름과 ID를 선택할 때 관리자는 사용자 이름과 관련 ID가 네트워크상에서 중복되지 않고 이전에 사용한 적이 없는지 확인해야 합니다.

보안 관리자 역할은 각 계정에 대한 원본 암호를 지정하고 새 계정의 사용자에게 암호를 전달할 책임이 있습니다. 암호를 관리할 때 다음 정보를 고려해야 합니다.

- 보안 관리자 역할을 맡을 수 있는 사용자에 대한 계정이 잠글 수 없도록 구성되어 있는지 확인합니다. 그러면 모든 다른 계정이 잠겨 있을 때 항상 최소 하나의 계정이 로그인하여 보안 관리자 역할을 맡은 다음 모든 사람의 계정을 다시 열 수 있습니다.
- 다른 사람이 암호를 도청할 수 없는 방법으로 새 계정의 사용자에게 암호를 전달합니다.
- 모르는 사람이 암호를 알아냈을 것 같은 의심이 드는 경우 계정 암호를 변경하십시오.
- 시스템 수명 기간 동안 사용자 이름 또는 사용자 ID를 다시 사용하지 마십시오.

  사용자 이름과 사용자 ID를 다시 사용하지 않으면 다음에 대한 혼동을 방지할 수 있습니다.

  - 감사 레코드를 분석할 때 어느 사용자가 어느 작업을 수행했는지 여부
  - 보관된 파일을 복원할 때 어느 파일이 어느 사용자의 소유인지 여부

정보 보호

관리자는 보안이 중요한 파일에 대한 DAC(임의 액세스 제어) 및 MAC(필수 액세스 제어) 보호를 올바르게 설정하여 유지 관리해야 할 책임이 있습니다. 중요한 파일은 다음과 같습니다.

- `shadow` **파일** – 암호화된 암호가 포함되어 있습니다. `shadow(4)`를 참조하십시오.
- `prof_attr` **데이터베이스** – 권한 프로파일의 정의가 포함되어 있습니다. `prof_attr(4)`를 참조하십시오.
- `exec_attr` **데이터베이스** – 권한 프로파일의 일부인 명령과 작업이 포함되어 있습니다. `exec_attr(4)`를 참조하십시오.
- `user_attr` **파일** – 로컬 사용자에게 지정된 권한 프로파일, 권한 및 권한 부여가 포함되어 있습니다. `user_attr(4)`를 참조하십시오.
- **감사 증적** – 감사 서비스에서 수집된 감사 레코드가 포함되어 있습니다. `audit.log(4)`를 참조하십시오.

주의 – LDAP 항목에 대한 보호 방식은 Trusted Extensions 소프트웨어에 의해 적용되는 액세스 제어 정책을 따르지 않으므로 기본 LDAP 항목을 확장하거나 액세스 규칙을 수정해서는 안됩니다.

암호 보호

로컬 파일의 암호는 DAC에 의해 보기가 방지되고 DAC와 MAC 모두에 의해 수정이 금지됩니다. 로컬 계정에 대한 암호는 수퍼유저만 읽을 수 있는 `/etc/shadow` 파일에서 유지 관리됩니다. 자세한 내용은 `shadow(4)` 매뉴얼 페이지를 참조하십시오.

그룹 관리

시스템 관리자 역할은 로컬 시스템과 네트워크에서 모든 그룹에 고유한 그룹 ID(GID)가 있는지 확인해야 합니다.

로컬 그룹을 시스템에서 삭제할 때 시스템 관리자 역할은 다음을 확인해야 합니다.

- 삭제된 그룹의 GID를 가진 모든 객체를 삭제하거나 다른 그룹에 지정해야 합니다.
- 삭제된 그룹을 기본 그룹으로 사용하는 모든 사용자를 다른 기본 그룹에 다시 지정해야 합니다.

사용자 삭제 방법

계정을 시스템에서 삭제할 때 시스템 관리자 역할과 보안 관리자 역할은 다음 작업을 수행해야 합니다.

- 모든 영역에서 계정의 홈 디렉토리를 삭제합니다.
- 삭제된 계정이 소유한 모든 프로세스 또는 작업을 삭제합니다.
  - 해당 계정이 소유한 모든 객체를 삭제하거나 소유권을 다른 사용자에게 지정합니다.
  - 사용자를 대신하여 예정된 모든 `at` 또는 `batch` 작업을 삭제합니다. 자세한 내용은 `at(1)` 및 `crontab(1)` 매뉴얼 페이지를 참조하십시오.
- 사용자(계정) 이름 또는 사용자 ID를 절대 다시 사용하지 마십시오.

데이터에 대한 보안 레벨 변경 규칙

기본적으로 일반 사용자는 파일과 선택 항목 모두에 대해 잘라내기 및 붙여넣기, 복사 및 붙여넣기, 끌어서 놓기 작업을 수행할 수 있습니다. 원본과 대상이 동일한 레이블에 있어야 합니다.

파일 레이블 또는 파일 내의 정보 레이블을 변경하려면 권한 부여가 필요합니다. 사용자가 데이터의 보안 레벨을 변경할 수 있게 권한 부여된 경우 Selection Manager(선택 관리자) 응용 프로그램에서 전송을 중재합니다. Trusted CDE에서는 `/usr/dt/config/sel_config` 파일이 파일 레이블 변경 작업과 정보를 잘라내어 다른 레이블에 붙여넣기 작업을 제어합니다. Trusted JDS에서는 `/usr/share/gnome/sel_config` 파일이 이러한 전송 작업을 제어합니다. Trusted CDE에서는 `/usr/dt/bin/sel_mgr` 응용 프로그램이 창 사이의 끌어서 놓기 작업을 제어합니다. 다음 표에 표시된 것처럼 선택 항목의 레이블 변경은 파일의 레이블 변경보다 더 제한적입니다.

다음 표에 파일 레이블 변경 규칙이 요약되어 있습니다. 규칙은 잘라내기 및 붙여넣기, 복사 및 붙여넣기, 끌어서 놓기 작업에 적용됩니다.

표 4–1 파일을 새 레이블로 이동하기 위한 조건

트랜잭션 설명	레이블 관계	소유자 관계	필요한 권한 부여
File Manager(파일 관리자) 간의 파일 복사 및 붙여넣기, 잘라내기 및 붙여넣기, 끌어서 놓기	동일한 레이블	동일한 UID	없음
	다운그레이드	동일한 UID	`solaris.label.file.downgrade`
	업그레이드	동일한 UID	`solaris.label.file.upgrade`
	다운그레이드	다른 UID	`solaris.label.file.downgrade`
	업그레이드	다른 UID	`solaris.label.file.upgrade`

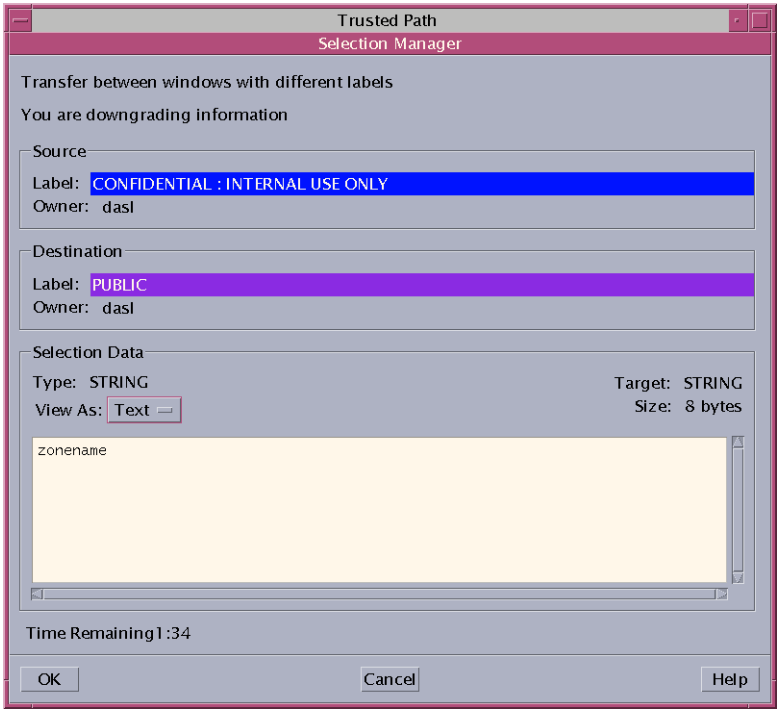
창 또는 파일 내의 선택에는 다른 규칙이 적용됩니다. **선택 항목** 끌어서 놓기는 항상 동일한 레이블과 소유권에만 적용됩니다. 창 사이의 끌어서 놓기는 `sel_config` 파일이 아니라 Selection Manager(선택 관리자) 응용 프로그램에서 중재합니다.

선택 항목의 레이블 변경 규칙에 대해서는 다음 표에 요약되어 있습니다.

표 4–2 선택 항목을 새 레이블로 이동하기 위한 조건

트랜잭션 설명	레이블 관계	소유자 관계	필요한 권한 부여
창 사이의 복사 및 붙여넣기 또는 잘라내기 및 붙여넣기	동일한 레이블	동일한 UID	없음
	다운그레이드	동일한 UID	`solaris.label.win.downgrade`
	업그레이드	동일한 UID	`solaris.label.win.upgrade`
	다운그레이드	다른 UID	`solaris.label.win.downgrade`
	업그레이드	다른 UID	`solaris.label.win.upgrade`
창 사이의 선택 항목 끌어서 놓기	동일한 레이블	동일한 UID	해당 없음

Trusted Extensions는 레이블 변경을 중재하는 선택 확인자를 제공합니다. 이 창은 권한이 부여된 사용자가 파일 또는 선택 항목의 레이블을 변경하려고 시도하면 표시됩니다. 사용자는 120초 동안 작업을 확인할 수 있습니다. 이 창을 표시하지 않고 데이터의 보안 레벨을 변경하려면 레이블 변경 권한 부여와 `solaris.label.win.noview` 권한 부여가 필요합니다. 다음 그림에는 창에 `zonename` 선택 항목이 표시되어 있습니다.



기본적으로 선택 확인자는 데이터를 다른 레이블로 전송할 때마다 표시됩니다. 선택 항목에 여러 전송 결정이 필요한 경우 자동 회신 방식을 사용하여 여러 전송 항목에 한 번에 회신할 수 있습니다. 자세한 내용은 sel_config(4) 매뉴얼 페이지와 다음 섹션을 참조하십시오.

sel_config 파일

작업에서 레이블을 업그레이드하거나 다운그레이드할 때 sel_config 파일을 확인하여 선택 확인자의 동작을 결정합니다.

sel_config 파일은 다음을 정의합니다.

- 자동 회신이 제공되는 선택 유형 목록
- 특정 유형의 작업을 자동으로 확인할 수 있는지 여부
- 선택 확인자 대화 상자가 표시되는지 여부

Trusted CDE에서 보안 관리자 역할은 Trusted_Extensions 폴더에서 선택 확인 구성 작업을 사용하여 기본값을 변경할 수 있습니다. 새 설정은 다음에 로그인할 때 적용됩니다. Solaris Trusted Extensions(JDS)에서는 CDE 작업을 사용할 수 없습니다. 기본값을 변경하려면 텍스트 편집기에서 /usr/share/gnome/sel_config 파일을 수정합니다.

Solaris Trusted Extensions(CDE) 사용자 정의

Solaris Trusted Extensions(CDE)에서 사용자는 Front Panel(전면 패널)에 작업을 추가하고 Workspace(작업 공간) 메뉴를 사용자 정의할 수 있습니다. Trusted Extensions 소프트웨어는 CDE에 프로그램과 명령을 추가할 수 있는 사용자 기능을 제한합니다.

Front Panel(전면 패널) 사용자 정의

모든 사용자는 Application Manager(응용 프로그램 관리자)에서 Front Panel(전면 패널)로 기존 작업을 끌어서 놓을 수 있습니다. 이때 수정하려는 계정의 프로파일에 해당 작업이 있어야 합니다. /usr/dt/ 또는 /etc/dt/ 디렉토리의 작업을 Front Panel(전면 패널)에 추가할 수 있지만, $HOME/.dt/appconfig 디렉토리의 응용 프로그램은 추가할 수 없습니다. 사용자는 작업 만들기 작업을 사용할 수 있지만, 시스템 차원의 작업이 저장되는 디렉토리에 쓸 수 없습니다. 따라서 일반 사용자는 사용 가능한 작업을 만들 수 없습니다.

Trusted Extensions에서 작업 검색 경로가 변경되었습니다. 개별 홈 디렉토리에 있는 작업이 처음이 아니라 마지막에 처리됩니다. 따라서 아무도 기존 작업을 사용자 정의할 수 없습니다.

보안 관리자 역할에 관리 편집기 작업이 지정되므로 필요에 따라 `/usr/dt/appconfig/types/C/dtwm.fp` 파일과 Front Panel(전면 패널)의 서브패널에 대한 다른 구성 파일을 수정할 수 있습니다.

Workspace(작업 공간) 메뉴 사용자 정의

Workspace(작업 공간) 메뉴는 작업 공간의 배경을 마우스 버튼 3으로 누르면 표시되는 메뉴입니다. 일반 사용자는 메뉴를 사용자 정의하고 메뉴에 항목을 추가할 수 있습니다.

사용자가 여러 레이블에서 작업할 수 있도록 허용되는 경우 다음과 같은 조건이 적용됩니다.

- 전역 영역에 사용자의 홈 디렉토리가 있어야 합니다.

  사용자 정의를 저장하려면 전역 영역의 프로세스가 올바른 레이블에서 사용자의 홈 디렉토리에 쓸 수 있어야 합니다. 전역 영역 프로세스에서 쓸 수 있는 사용자 홈 디렉토리의 영역 경로는 다음과 비슷합니다.

  `/zone/`*zone-name*`/home/`*username*
- 사용자는 일반 사용자 작업 공간에서 Customize Menu(메뉴 사용자 정의) 및 Add Item to Menu(메뉴에 항목 추가) 옵션을 사용해야 합니다. 사용자는 레이블마다 다른 사용자 정의를 만들 수 있습니다.
- 사용자가 역할을 맡으면 Workspace(작업 공간) 메뉴에 대한 변경 사항이 지속됩니다.
- Workspace(작업 공간) 메뉴에 대한 변경 사항은 현재 레이블에서 사용자의 홈 디렉토리에 저장됩니다. 사용자 정의된 메뉴 파일은 `.dt/wsmenu`입니다.
- 사용자의 권한 프로파일에서 사용자가 원하는 작업을 실행할 수 있도록 설정해야 합니다.

  Workspace(작업 공간) 메뉴에 추가되는 작업은 사용자의 권한 프로파일 중 하나에서 처리해야 합니다. 그렇지 않으면, 호출할 때 작업이 실패하고 오류 메시지가 표시됩니다.

  예를 들어, 실행 작업이 있는 사용자는 작업 또는 작업에서 호출되는 명령이 계정의 권한 프로파일 중 하나에 없더라도 실행 파일에 대한 아이콘을 두 번 눌러서 실행 파일을 실행할 수 있습니다. 기본적으로 역할에 실행 작업이 지정되지 않습니다. 따라서 역할이 실행 작업이 필요한 메뉴 항목을 실행할 경우 작업에 실패합니다.

◆ ◆ ◆ 5 장

5 Trusted Extensions의 보안 요구 사항 관리(작업)

이 장에는 Trusted Extensions로 구성된 시스템에서 일반적으로 수행하는 작업이 포함되어 있습니다.

Trusted Extensions의 일반 작업(작업 맵)

다음 작업 맵에서는 Trusted Extensions 관리자를 위한 작업 환경을 설정하는 절차를 설명합니다.

작업	설명	수행 방법
신뢰할 수 있는 편집기의 편집기 프로그램을 변경합니다.	관리 파일의 편집기를 지정합니다.	68 페이지 "선택한 편집기를 신뢰할 수 있는 편집기로 지정하는 방법"
root 암호를 변경합니다.	`root` 사용자나 `root` 역할의 새 암호를 지정합니다.	69 페이지 "root 암호를 변경하는 방법"
역할 암호를 변경합니다.	현재 역할의 새 암호를 지정합니다.	예 5–2
보안 키 조합을 사용합니다.	마우스나 키보드의 컨트롤을 가져옵니다. 또한 마우스나 키보드를 신뢰할 수 있는지 여부를 테스트합니다.	70 페이지 "데스크탑의 현재 포커스에 대한 컨트롤을 다시 얻는 방법"
레이블에 대한 16진수를 결정합니다.	텍스트 레이블에 대한 내부 표현을 표시합니다.	71 페이지 "레이블에 해당하는 16진수를 얻는 방법"
레이블에 대한 텍스트 표현을 결정합니다.	16진수 레이블에 대한 텍스트 표현을 표시합니다.	72 페이지 "읽기 가능한 레이블을 해당 16진수 형식에서 얻는 방법"
시스템 파일을 편집합니다.	안전하게 Oracle Solaris 또는 Trusted Extensions 시스템 파일을 편집합니다.	73 페이지 "시스템 파일에서 보안 기본값을 변경하는 방법"
장치를 할당합니다.	주변 기기를 사용하여 정보를 추가하거나 시스템에서 정보를 제거합니다.	**Trusted Extensions User's Guide**의 "How to Allocate a Device in Trusted Extensions"

작업	설명	수행 방법
호스트를 원격으로 관리합니다.	원격 호스트에서 Oracle Solaris 또는 Trusted Extensions 호스트를 관리합니다.	8 장, “Trusted Extensions에서 원격 관리(작업)”

▼ 선택한 편집기를 신뢰할 수 있는 편집기로 지정하는 방법

신뢰할 수 있는 편집기는 `$EDITOR` 환경 변수의 값을 자체 편집기로 사용합니다.

시작하기 전에 전역 영역에서 역할을 가진 사용자여야 합니다.

1. **`$EDITOR` 변수의 값을 결정합니다.**

   ```
   # echo $EDITOR
   ```

   가능한 편집기는 다음과 같습니다. `$EDITOR` 변수를 설정하지 않을 수도 있습니다.

   - `/usr/dt/bin/dtpad` – CDE에서 제공하는 편집기입니다.
   - `/usr/bin/gedit` – Java Desktop System, 릴리스 **번호**에서 제공하는 편집기입니다. Solaris Trusted Extensions(JDS)는 해당 데스크탑의 신뢰할 수 있는 버전입니다.
   - `/usr/bin/vi` – 영상 편집기입니다.

2. **`$EDITOR` 변수의 값을 설정합니다.**

   - **값을 영구적으로 설정하려면 역할에 대한 셸 초기화 파일에서 값을 수정합니다.**

     예를 들어, 역할의 홈 디렉토리에서 Korn 셸에 대한 `.kshrc` 파일과 C 셸에 대한 `.cshrc` 파일을 수정합니다.

   - **현재 셸에 대한 값을 설정하려면 터미널 창에서 값을 설정합니다.**

     예를 들어, Korn 셸에서는 다음 명령을 사용합니다.

     ```
     # setenv EDITOR=pathname-of-editor
     # export $EDITOR
     ```

     C 셸에서는 다음 명령을 사용합니다.

     ```
     # setenv EDITOR=pathname-of-editor
     ```

     Bourne 셸에서는 다음 명령을 사용합니다.

     ```
     # EDITOR=pathname-of-editor
     # export EDITOR
     ```

예 5–1 신뢰할 수 있는 편집기에 대한 편집기 지정

보안 관리자 역할은 시스템 파일을 편집할 때 vi를 사용하려고 합니다. 이 역할을 맡은 사용자는 역할의 홈 디렉토리에 있는 .kshrc 초기화 파일을 수정합니다.

```
$ cd /home/secadmin
$ vi .kshrc

## Interactive shell
set -o vi
...
export EDITOR=vi
```

다음에 어느 사용자가 보안 관리자 역할을 맡더라도 신뢰할 수 있는 편집기는 vi입니다.

▼ root 암호를 변경하는 방법

보안 관리자 역할은 Solaris Management Console을 사용하여 언제든지 계정의 암호를 변경할 수 있게 권한이 부여되었습니다. 그러나 Solaris Management Console에서는 시스템 계정의 암호를 변경할 수 없습니다. **시스템 계정**은 UID가 100 미만인 계정입니다. root는 UID가 0이기 때문에 시스템 계정입니다.

1. **수퍼유저가 됩니다.**
   사이트에서 수퍼유저를 root 역할로 만든 경우 root 역할을 맡습니다.

2. **Trusted Path(신뢰할 수 있는 경로) 메뉴에서 Change Password(암호 변경)를 선택합니다.**

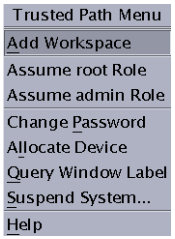
   - **Trusted JDS에서는 신뢰할 수 있는 스트라이프의 신뢰할 수 있는 기호를 누릅니다.**
     Trusted Path(신뢰할 수 있는 경로) 메뉴에서 Change Password(암호 변경)를 선택합니다.

   - **Solaris Trusted Extensions(CDE)에서는 Trusted Path(신뢰할 수 있는 경로) 메뉴를 엽니다.**

     a. **Workspace Switch Area(작업 공간 전환 영역)에서 마우스 버튼 3을 누릅니다.**

     b. **Trusted Path(신뢰할 수 있는 경로) 메뉴에서 Change Password(암호 변경)를 선택합니다.**



3 **암호를 변경하고 변경 내용을 확인합니다.**

예 5–2 역할의 암호 변경

LDAP에 정의된 역할을 맡을 수 있는 사용자는 Trusted Path(신뢰할 수 있는 경로) 메뉴를 사용하여 역할의 암호를 변경할 수 있습니다. 그러면 해당 역할을 맡으려고 하는 모든 사용자에 대해 LDAP에서 암호가 변경됩니다.

Oracle Solaris OS에서와 같이 기본 관리자 역할은 Solaris Management Console을 사용하여 역할의 암호를 변경할 수 있습니다. Trusted Extensions에서는 보안 관리자 역할이 Solaris Management Console을 사용하여 다른 역할의 암호를 변경할 수 있습니다.

▼ 데스크탑의 현재 포커스에 대한 컨트롤을 다시 얻는 방법

"보안" 키 조합을 사용하여 신뢰할 수 없는 응용 프로그램의 포인터 잡기나 키보드 잡기를 해제할 수 있습니다. 또한 이 키보드 조합을 사용하여 신뢰할 수 있는 응용 프로그램에서 포인터가 키보드를 잡았는지 확인할 수 있습니다. 여러 개의 신뢰할 수 있는 스트라이프를 표시하도록 스푸핑된 멀티헤디드 시스템에서 이 키 조합은 권한 부여된 신뢰할 수 있는 스트라이프로 포인터를 가져옵니다.

1 **Sun 키보드의 컨트롤을 다시 얻으려면 다음 키 조합을 사용하십시오.**

키를 동시에 눌러 현재 데스크탑 포커스에 대한 컨트롤을 다시 얻습니다. Sun 키보드에서 다이아몬드는 Meta 키입니다.

```
<Meta> <Stop>
```

포인터와 같은 잡기를 신뢰할 수 없는 경우 포인터가 스트라이프로 이동합니다. 신뢰할 수 있는 포인터는 신뢰할 수 있는 스트라이프로 이동하지 않습니다.

2 **Sun 키보드를 사용하지 않을 경우 다음 키 조합을 사용하십시오.**

```
<Alt> <Break>
```

키를 동시에 눌러 랩탑에서 현재 데스크탑 포커스에 대한 컨트롤을 다시 얻습니다.

예 5–3 암호 프롬프트를 신뢰할 수 있는지 테스트

Sun 키보드를 사용하는 x86 시스템에서는 사용자에게 암호를 묻는 프롬프트가 나타납니다. 커서가 잡혔으며 암호 대화 상자에 있습니다. 프롬프트를 신뢰할 수 있는지 확인하기 위해 사용자가 <Meta> <Stop> 키를 동시에 누릅니다. 포인터가 대화 상자에 남아 있으면 암호 프롬프트를 신뢰할 수 있는 것입니다.

그러나 포인터가 신뢰할 수 있는 스트라이프로 이동하면 암호 프롬프트를 신뢰할 수 없는 것이므로 관리자에게 문의해야 합니다.

예 5–4 포인터를 신뢰할 수 있는 스트라이프로 가져오기

이 예에서 사용자는 신뢰할 수 있는 프로세스를 실행하고 있지 않지만 마우스 포인터를 볼 수 없습니다. 포인터를 신뢰할 수 있는 스트라이프의 중앙으로 가져오기 위해 사용자는 <Meta> <Stop> 키를 동시에 누릅니다.

▼ 레이블에 해당하는 16진수를 얻는 방법

이 절차에서는 레이블의 내부 16진수 표현을 제공합니다. 이 표현은 공용 디렉토리에 저장하기에 안전합니다. 자세한 내용은 `atohexlabel(1M)` 매뉴얼 페이지를 참조하십시오.

시작하기 전에 전역 영역에서 보안 관리자 역할을 가진 사용자여야 합니다. 자세한 내용은 51 페이지 “Trusted Extensions에서 전역 영역으로 들어가는 방법”을 참조하십시오.

- **레이블에 대한 16진수 값을 얻으려면 다음 중 하나를 수행하십시오.**
  - **민감도 레이블에 대한 16진수 값을 얻으려면 명령에 레이블을 전달합니다.**

    ```
    $ atohexlabel "CONFIDENTIAL : NEED TO KNOW"
    0x0004-08-68
    ```

  - **클리어런스에 대한 16진수 값을 얻으려면 `-c` 옵션을 사용합니다.**

    ```
    $ atohexlabel -c "CONFIDENTIAL NEED TO KNOW"
    0x0004-08-68
    ```

주 – 사람이 읽을 수 있는 민감도 레이블과 클리어런스 레이블은 label_encodings 파일의 규칙에 따라 구성됩니다. 각 유형의 레이블은 이 파일의 개별 구역에 있는 규칙을 사용합니다. 민감도 레이블과 클리어런스 레이블 모두 동일한 기본 레벨의 민감도를 표현할 경우 두 레이블의 16진수 형식은 동일합니다. 그러나 사람이 읽을 수 있는 형식은 다를 수 있습니다. 사람이 읽을 수 있는 형식을 입력으로 받아들이는 시스템 인터페이스에서는 한 가지 유형의 레이블을 예상합니다. 레이블 유형에 대한 텍스트 문자열이 다를 경우 이들 텍스트 문자열을 혼용할 수 없습니다.

기본 label_encodings 파일에서 클리어런스 레이블에 해당하는 텍스트에는 콜론(:)이 포함되지 않습니다.

예 5–5 atohexlabel **명령 사용**

16진수 형식의 유효 레이블을 전달하면 명령에서 인수를 반환합니다.

```
$ atohexlabel 0x0004-08-68
0x0004-08-68
```

관리 레이블을 전달하면 명령에서 인수를 반환합니다.

```
$ atohexlabel admin_high
ADMIN_HIGH
atohexlabel admin_low
ADMIN_LOW
```

일반 오류 **위치 0의 <문자열>에서** atohexlabel **구문 분석 오류가 발생했습니다**는 오류 메시지는 atohexlabel에 전달한 **<문자열>** 인수가 유효 레이블이나 클리어런스가 아님을 나타냅니다. 입력 내용을 확인하고 설치한 label_encodings 파일에 레이블이 존재하는지 확인합니다.

▼ 읽기 가능한 레이블을 해당 16진수 형식에서 얻는 방법

이 절차에서는 내부 데이터베이스에 저장된 레이블을 복구하는 방법을 제공합니다. 자세한 내용은 hextoalabel(1M) 매뉴얼 페이지를 참조하십시오.

시작하기 전에 전역 영역에서 보안 관리자 역할을 가진 사용자여야 합니다.

- **레이블의 내부 표현에 해당하는 텍스트를 가져오려면 다음 중 하나를 수행하십시오.**
  - **민감도 레이블에 해당하는 텍스트를 가져오려면 레이블의 16진수 형식을 전달합니다.**

    ```
    $ hextoalabel 0x0004-08-68
    CONFIDENTIAL : NEED TO KNOW
    ```

- **클리어런스에 해당하는 텍스트를 가져오려면 -c 옵션을 사용합니다.**

```
$ hextoalabel -c 0x0004-08-68
CONFIDENTIAL NEED TO KNOW
```

▼ 시스템 파일에서 보안 기본값을 변경하는 방법

Trusted Extensions에서는 보안 관리자가 시스템의 기본 보안 설정을 변경하거나 액세스합니다.

보안 설정은 /etc/security 및 /etc/default 디렉토리의 파일에 있습니다. Oracle Solaris 시스템에서는 수퍼 유저가 이러한 파일을 편집할 수 있습니다. Oracle Solaris 보안에 대한 자세한 내용은 **System Administration Guide: Security Services**의 3 장, "Controlling Access to Systems (Tasks)"를 참조하십시오.

주의 – 사이트 보안 정책에서 허용하는 경우에만 시스템 보안 기본값을 완화하십시오.

시작하기 전에 전역 영역에서 보안 관리자 역할을 가진 사용자여야 합니다.

- **신뢰할 수 있는 편집기를 사용하여 시스템 파일을 편집합니다.**

  자세한 내용은 54 페이지 "Trusted Extensions에서 관리 파일을 편집하는 방법"을 참조하십시오.

  다음 표에는 보안 파일 및 해당 파일에서 변경할 보안 매개변수가 나열되어 있습니다.

파일	작업	자세한 정보
/etc/default/login	허용되는 암호 시도 횟수를 줄입니다.	**System Administration Guide: Security Services**의 "How to Monitor All Failed Login Attempts"에 있는 예를 참조하십시오. passwd(1) 매뉴얼 페이지
/etc/default/kbd	키보드 셧다운을 사용 안함으로 설정합니다.	**System Administration Guide: Security Services**의 "How to Disable a System's Abort Sequence" **주 –** 관리자가 디버깅에 사용하는 호스트에서 KEYBOARD_ABORT에 대한 기본 설정은 kadb 커널 디버거에 대한 액세스를 허용합니다. 디버거에 대한 자세한 내용은 kadb(1M) 매뉴얼 페이지를 참조하십시오.

파일	작업	자세한 정보
/etc/security/policy.conf	사용자 암호에 대한 보다 강력한 알고리즘을 필요로 합니다. 이 호스트의 모든 사용자에게서 기본 권한을 제거합니다. 이 호스트의 사용자를 Basic Solaris User(기본 Solaris 사용자) 권한 부여로 제한합니다.	policy.conf(4) 매뉴얼 페이지
/etc/default/passwd	사용자가 암호를 자주 변경해야 합니다. 사용자가 최대한 다른 암호를 만들어야 합니다. 보다 긴 사용자 암호를 요구합니다. 사전에서 찾을 수 없는 암호를 요구합니다.	passwd(1) 매뉴얼 페이지

◆ ◆ ◆ 6 장

6 Trusted Extensions의 사용자, 권한 및 역할(개요)

이 장에서는 일반 사용자를 만들기 전에 결정해야 하는 필수 사항을 설명하고, 사용자 계정 관리를 위한 추가 배경 정보를 제공합니다. 이 장에서는 초기 설정 팀이 역할 및 제한된 수의 사용자 계정을 설정했다고 가정합니다. 이러한 사용자는 Trusted Extensions를 구성하고 관리하는 데 사용되는 역할을 맡을 수 있습니다. 자세한 내용은 **Trusted Extensions Configuration Guide**의 "Creating Roles and Users in Trusted Extensions"를 참조하십시오.

- 75 페이지 "Trusted Extensions의 사용자 보안 기능"
- 76 페이지 "사용자에 대한 관리자 책임"
- 77 페이지 "Trusted Extensions에서 사용자를 만들기 전에 결정할 사항"
- 77 페이지 "Trusted Extensions의 기본 사용자 보안 속성"
- 78 페이지 "Trusted Extensions에서 구성 가능한 사용자 속성"
- 79 페이지 "사용자에게 지정해야 하는 보안 속성"

Trusted Extensions의 사용자 보안 기능

Trusted Extensions 소프트웨어는 사용자, 역할 또는 권한 프로파일에 다음 보안 기능을 추가합니다.

- 사용자는 시스템을 사용할 수 있는 레이블 범위를 가집니다.
- 역할은 관리 작업을 수행하는 데 사용할 수 있는 레이블 범위를 가집니다.
- Trusted Extensions 권한 프로파일에는 CDE 관리 작업이 포함될 수 있습니다. 명령과 마찬가지로 작업도 보안 속성을 가질 수 있습니다.
- Trusted Extensions 권한 프로파일의 명령 및 작업은 레이블 속성을 가집니다. 명령 또는 작업은 레이블 범위 내에서 또는 특정 레이블에서 수행되어야 합니다.
- Trusted Extensions 소프트웨어는 Oracle Solaris OS에서 정의한 권한 및 권한 부여 세트에 권한 및 권한 부여를 추가합니다.

사용자에 대한 관리자 책임

시스템 관리자 역할은 사용자 계정을 만듭니다. 보안 관리자 역할은 계정의 보안 속성을 설정합니다.

LDAP 이름 지정 서비스에 Oracle Directory Server Enterprise Edition를 사용하는 경우 초기 설정 팀에서 `tsol_ldap.tbx` 도구 상자를 구성했는지 확인하십시오. 절차는 **Trusted Extensions Configuration Guide**의 "Configuring the Solaris Management Console for LDAP (Task Map)"을 참조하십시오.

사용자 및 역할 설정에 대한 자세한 내용은 다음을 참조하십시오.

- **Oracle Solaris 관리: 기본 관리**의 "첫번째 역할(기본 관리자)을 만드는 방법"
- **Oracle Solaris 관리: 기본 관리**의 "사용자 계정 설정(작업 맵)"
- **System Administration Guide: Security Services**의 제III부, "Roles, Rights Profiles, and Privileges"

사용자에 대한 시스템 관리자 책임

Trusted Extensions에서 시스템 관리자 역할은 시스템에 액세스할 수 있는 사용자 결정을 담당합니다. 시스템 관리자는 다음 작업을 담당합니다.

- 사용자 추가 및 삭제
- 역할 추가 및 삭제
- 사용자 및 역할 구성 수정(보안 속성 제외)

사용자에 대한 보안 관리자 책임

Trusted Extensions에서 보안 관리자 역할은 사용자 또는 역할의 모든 보안 속성을 담당합니다. 보안 관리자는 다음 작업을 담당합니다.

- 사용자, 역할 또는 권한 프로파일의 보안 속성 지정 및 수정
- 권한 프로파일 만들기 및 수정
- 사용자 및 역할에 권한 프로파일 지정
- 사용자, 역할 또는 권한 프로파일에 권한 지정
- 사용자, 역할 또는 권한 프로파일에 권한 부여 지정
- 사용자, 역할 또는 권한 프로파일에서 권한 제거
- 사용자, 역할 또는 권한 프로파일에서 권한 부여 제거

일반적으로 보안 관리자 역할이 권한 프로파일을 만듭니다. 그러나 보안 관리자 역할에서 부여할 수 없는 기능이 프로파일에 필요한 경우 수퍼유저나 기본 관리자 역할에서 프로파일을 만들 수 있습니다.

권한 프로파일을 만들기 전에 보안 관리자는 새 프로파일의 명령이나 작업이 성공하기 위해 권한 또는 권한 부여가 필요한지 여부를 분석해야 합니다. 개별 명령에 대한 매뉴얼 페이지에는 필요할 수 있는 권한 및 권한 부여가 나열되어 있습니다. 권한 및 권한 부여가 필요한 작업의 예는 `exec_attr` 데이터베이스를 참조하십시오.

Trusted Extensions에서 사용자를 만들기 전에 결정할 사항

다음 결정 사항은 사용자가 Trusted Extensions에서 무엇을 수행할 수 있고 얼마나 많은 노력이 필요한지에 영향을 줍니다. 일부 결정 사항은 Oracle Solaris OS를 설치할 때 내리는 결정 사항과 동일합니다. 그러나 Trusted Extensions에 고유한 결정 사항은 사이트 보안 및 사용 편의성에 영향을 줄 수 있습니다.

- `policy.conf` 파일에서 기본 사용자 보안 속성을 변경할지 여부를 결정합니다. `label_encodings` 파일의 사용자 기본값은 초기 설정 팀에서 구성했습니다. 기본값에 대한 설명은 77 페이지 “Trusted Extensions의 기본 사용자 보안 속성”을 참조하십시오.
- 각 사용자의 최소 레이블 홈 디렉토리에서 사용자의 상위 레벨 홈 디렉토리로 복사하거나 링크할 시작 파일(있는 경우)을 결정합니다. 절차는 86 페이지 “Trusted Extensions에서 사용자의 시작 파일을 구성하는 방법”을 참조하십시오.
- 사용자가 마이크, CD-ROM 드라이브 및 JAZ 드라이브와 같은 주변 기기에 액세스할 수 있는지 여부를 결정합니다.

  일부 사용자에게 액세스가 허용된 경우 사이트 보안을 위해 사이트에서 추가 권한 부여를 필요로 하는지 여부를 결정합니다. 장치 관련 권한 부여의 기본 목록은 241 페이지 “장치 권한 부여를 지정하는 방법”을 참조하십시오. 더 세분화된 장치 권한 부여 설정은 237 페이지 “Trusted Extensions에서 장치 권한 부여 사용자 정의(작업 맵)”를 참조하십시오.

Trusted Extensions의 기본 사용자 보안 속성

`label_encodings` 및 `policy.conf` 파일의 설정에서 함께 사용자 계정에 대한 기본 보안 속성을 정의합니다. 사용자에 대해 명시적으로 설정하는 값은 이러한 시스템 값을 대체합니다. 이러한 파일에 설정된 몇몇 값은 역할 계정에도 적용됩니다. 명시적으로 설정할 수 있는 보안 속성은 78 페이지 “Trusted Extensions에서 구성 가능한 사용자 속성”을 참조하십시오.

`label_encodings` 파일 기본값

`label_encodings` 파일은 사용자의 최소 레이블, 클리어런스 및 기본 레이블 보기를 정의합니다. 파일에 대한 자세한 내용은 `label_encodings(4)` 매뉴얼 페이지를 참조하십시오. 사이트의 `label_encodings` 파일은 초기 설정 팀에서 설치했습니다. 이러한 결정은 **Trusted Extensions Configuration Guide**의 “Devising a Label Strategy” 및 **Trusted Extensions Label Administration** 의 예를 기준으로 합니다.

보안 관리자가 Solaris Management Console에서 개별 사용자에 대해 명시적으로 설정하는 레이블 값은 `label_encodings` 파일에서 파생됩니다. 명시적으로 설정된 값은 `label_encodings` 파일의 값보다 우선합니다.

Trusted Extensions의 `policy.conf` 파일 기본값

Oracle Solaris `/etc/security/policy.conf` 파일에는 시스템에 대한 기본 보안 설정이 들어 있습니다. Trusted Extensions는 이 파일에 두 개의 키워드를 추가합니다. 시스템 차원의 값을 변경하려는 경우 이러한 키워드=값 쌍을 파일에 추가할 수 있습니다. 이러한 키워드는 Trusted Extensions에 의해 적용됩니다. 다음 표에는 이러한 보안 설정의 가능한 값과 기본값이 나와 있습니다.

표 6–1 `policy.conf` 파일의 Trusted Extensions 보안 기본값

키워드	기본값	가능한 값	주
IDLECMD	LOCK	LOCK | LOGOUT	역할에 적용되지 않습니다.
IDLETIME	30	0 ~ 120분	역할에 적용되지 않습니다.

`policy.conf` 파일에 정의된 권한 부여 및 권한 프로파일은 개별 계정에 지정된 권한 부여 및 프로파일에 대한 **추가 사항**입니다. 기타 필드의 경우 개별 사용자의 값이 시스템 값을 대체합니다.

Trusted Extensions Configuration Guide의 "Planning User Security in Trusted Extensions"에 모든 `policy.conf` 키워드 표가 있습니다. `policy.conf(4)` 매뉴얼 페이지도 참조하십시오.

Trusted Extensions에서 구성 가능한 사용자 속성

Solaris Management Console 2.1은 사용자 계정을 만들고 수정하는 도구입니다. 둘 이상의 레이블에 로그인할 수 있는 사용자에 대해 각 사용자의 최소 레이블 홈 디렉토리에서 `.copy_files` 및 `.link_files` 파일을 설정할 수도 있습니다.

Solaris Management Console의 User Accounts(사용자 계정) 도구는 Oracle Solaris OS에서와 같이 작동하지만 두 가지 예외가 있습니다.

- Trusted Extensions는 사용자 계정에 속성을 추가합니다.
- 홈 디렉토리 서버 액세스를 위해서는 Trusted Extensions에서 관리가 필요합니다.
  - Oracle Solaris 시스템에서와 같은 방식으로 홈 디렉토리 서버 항목을 만듭니다.
  - 그런 다음 추가 단계를 수행하여 모든 사용자 레벨에서 홈 디렉토리를 마운트합니다.

Oracle Solaris 관리: 기본 관리의 "Solaris Management Console의 사용자 도구로 사용자를 추가하는 방법"에 설명된 대로 마법사를 사용하여 사용자 계정을 빠르게 만들 수 있습니다. 마법사를 사용한 후 사용자의 기본 Trusted Extensions 속성을 수정할 수 있습니다.

`.copy_files` 및 `.link_files` 파일에 대한 자세한 내용은 81 페이지 ".copy_files 및 .link_files 파일"을 참조하십시오.

사용자에게 지정해야 하는 보안 속성

보안 관리자 역할은 다음 표에 나온 대로 새로운 사용자에 대해 몇 가지 보안 속성을 지정해야 합니다. 기본값이 포함된 파일에 대한 자세한 내용은 77 페이지 "Trusted Extensions의 기본 사용자 보안 속성"을 참조하십시오. 다음 표에는 사용자에게 지정할 수 있는 보안 속성과 각 지정의 효과가 나와 있습니다.

표 6–2 사용자를 만든 후 지정되는 보안 속성

사용자 속성	기본값 위치	필요한 작업	작업 효과
Password	없음	필수	사용자가 암호를 가짐
역할	없음	선택 사항	사용자가 역할을 맡을 수 있음
권한 부여	`policy.conf` 파일	선택 사항	사용자가 추가 권한 부여를 가짐
권한 프로파일	`policy.conf` 파일	선택 사항	사용자가 추가 권한 프로파일을 가짐
레이블	`label_encodings` 파일	선택 사항	사용자가 다른 기본 레이블 또는 승인 범위를 가짐
권한	`policy.conf` 파일	선택 사항	사용자가 다른 권한 세트를 가짐
계정 사용	`policy.conf` 파일	선택 사항	사용자가 유휴 상태인 컴퓨터에 대해 다른 설정을 가짐
감사	`audit_control` 파일	선택 사항	사용자가 시스템 감사 설정과 다르게 감사됨

Trusted Extensions에서 사용자에게 보안 속성 지정

사용자 계정이 만들어진 후 보안 관리자 역할은 Solaris Management Console에서 사용자에게 보안 속성을 지정합니다. 올바른 기본값을 설정한 경우 다음 단계는 기본값에 대한 예외가 필요한 사용자에 대해서만 보안 속성을 지정하는 것입니다.

사용자에게 보안 속성을 지정할 때 보안 관리자는 다음 정보를 고려합니다.

암호 지정
계정이 만들어진 후 보안 관리자 역할은 사용자 계정에 암호를 지정합니다. 이 초기 지정 이후 사용자는 자신의 암호를 변경할 수 있습니다.

Oracle Solaris OS와 마찬가지로 사용자가 정기적으로 자신의 암호를 변경하도록 할 수 있습니다. 암호 만료일 옵션은 암호를 추측하거나 가로챌 수 있는 침입자가 시스템에 액세스할 수 있는 기간을 제한합니다. 또한 암호 변경 전에 경과해야 하는 최소 기간을 설정해 두면 새 암호로 변경한 사용자가 즉시 이전 암호로 되돌리지 못하게 됩니다. 자세한 내용은 `passwd(1)` 매뉴얼 페이지를 참조하십시오.

주 – 역할을 맡을 수 있는 사용자에 대한 암호는 암호 만료일 제약 조건의 적용을 받지 않습니다.

역할 지정
사용자에게 역할이 있을 필요는 없습니다. 사이트의 보안 정책에 부합한다면 단일 사용자에게 둘 이상의 역할을 지정할 수 있습니다.

권한 부여 지정
Oracle Solaris OS와 마찬가지로 사용자에게 직접 권한 부여를 지정하면 해당 권한 부여가 기존 권한 부여에 추가됩니다. Trusted Extensions에서는 권한 프로파일에 권한 부여를 추가한 다음 사용자에게 프로파일을 지정합니다.

권한 프로파일 지정
Oracle Solaris OS와 마찬가지로 프로파일의 순서가 중요합니다. 프로파일 방식에서는 계정의 프로파일 세트에서 명령이나 작업의 첫번째 인스턴스를 사용합니다.

프로파일의 정렬 순서를 필요에 맞게 변경할 수 있습니다. 기존 프로파일의 명령에 대해 정의된 속성과 다른 보안 속성으로 명령을 실행하려는 경우 명령에 대해 선호하는 지정으로 새 프로파일을 만듭니다. 그런 다음 기존 프로파일 앞에 새 프로파일을 삽입합니다.

주 – 관리 작업이나 관리 명령이 포함된 권한 프로파일을 일반 사용자에게 지정하지 마십시오. 일반 사용자는 전역 영역에 들어갈 수 없으므로 프로파일이 작동하지 않습니다.

권한 기본값 변경
기본 권한 세트는 많은 사이트에서 너무 광범위할 수 있습니다. 시스템의 일반 사용자에 대한 권한 세트를 제한하려면 `policy.conf` 파일 설정을 변경합니다. 개별 사용자에 대한 권한 세트를 변경하려면 Solaris Management Console을 사용합니다. 예는 93 페이지 “사용자의 권한 세트를 제한하는 방법”을 참조하십시오.

레이블 기본값 변경
사용자의 레이블 기본값을 변경하면 `label_encodings` 파일에서 사용자 기본값에 대한 예외가 만들어집니다.

감사 기본값 변경
Oracle Solaris OS와 마찬가지로 사용자에게 감사 클래스를 지정하면 시스템의 `/etc/security/audit_control` 파일에서 지정된 감사 클래스에 대한 예외가

만들어집니다. 감사에 대한 자세한 내용은 18 장, “Trusted Extensions 감사(개요)”를 참조하십시오.

.copy_files 및 .link_files 파일

Trusted Extensions에서 파일은 골격 디렉토리에서 계정의 최소 레이블이 포함된 영역으로**만** 자동 복사됩니다. 상위 레이블의 영역에서 시작 파일을 사용할 수 있도록 하려면 사용자나 관리자가 `.copy_files` 및 `.link_files` 파일을 만들어야 합니다.

Trusted Extensions 파일 `.copy_files` 및 `.link_files`는 시작 파일을 계정 홈 디렉토리의 모든 레이블로 복사 또는 링크를 자동화하는 데 유용합니다. 사용자가 새 레이블에서 작업 공간을 만들 때마다 `updatehome` 명령이 계정의 최소 레이블에서 `.copy_files` 및 `.link_files`의 내용을 읽습니다. 그런 다음 나열된 모든 파일을 상위 레이블이 있는 작업 공간으로 복사하거나 링크합니다.

`.copy_files` 파일은 사용자가 다른 레이블에서 약간 다른 시작 파일을 원할 때 유용합니다. 예를 들어, 사용자가 다른 레이블에서 다른 메일 별칭을 사용할 경우 복사가 권장됩니다. `.link-files` 파일은 시작 파일이 호출된 모든 레이블에서 같아야 할 때 유용합니다. 예를 들어, 모든 레이블이 있는 인쇄 작업에 하나의 프린터가 사용되는 경우 링크가 권장됩니다. 예제 파일은 86 페이지 “Trusted Extensions에서 사용자의 시작 파일을 구성하는 방법”을 참조하십시오.

다음은 사용자가 상위 레이블로 링크하거나 복사할 수 있는 몇 가지 시작 파일의 목록입니다.

`.acrorc`
`.aliases`
`.cshrc`
`.dtprofile`
`.emacs`
`.login`
`.mailrc`
`.mime_types`
`.newsrc`
`.profile`
`.signature`
`.soffice`
`.Xdefaults`
`.Xdefaults-`*hostname*

◆ ◆ ◆ 7 장

7 Trusted Extensions에서 사용자, 권한 및 역할 관리(작업)

이 장에서는 사용자, 사용자 계정 및 권한 프로파일을 구성하고 관리하는 Trusted Extensions 절차를 제공합니다.

- 83 페이지 “보안을 위한 사용자 환경 사용자 정의(작업 맵)”
- 89 페이지 “Solaris Management Console에서 사용자 및 권한 관리(작업 맵)”
- 97 페이지 “Solaris Management Console에서 기타 작업 처리(작업 맵)”

보안을 위한 사용자 환경 사용자 정의(작업 맵)

다음 작업 맵에서는 모든 사용자에 대해 시스템을 사용자 정의하거나 개발 사용자의 계정을 사용자 정의할 때 수행할 수 있는 일반적인 작업을 설명합니다.

작업	설명	수행 방법
레이블 속성을 변경합니다.	사용자 계정에 대한 최소 레이블 및 기본 레이블 보기와 같은 레이블 속성을 수정합니다.	84 페이지 “기본 사용자 레이블 속성을 수정하는 방법”
시스템의 모든 사용자에 대한 Trusted Extensions 정책을 변경합니다.	`policy.conf` 파일을 변경합니다.	84 페이지 “`policy.conf` 기본값을 수정하는 방법”
	일정 시간이 경과한 후 화면 보호기를 켭니다. 시스템이 유휴 상태로 일정 시간이 경과한 후 사용자를 로그아웃합니다.	예 7–1
	시스템의 모든 일반 사용자에게서 불필요한 권한을 제거합니다.	예 7–2
	공개 키오스크에서 인쇄된 출력으로부터 레이블을 제거합니다.	예 7–3

작업	설명	수행 방법
사용자에 대한 초기화 파일을 구성합니다.	모든 사용자의 시작 파일(.cshrc, .copy_files, .soffice 등)을 구성합니다.	86 페이지 “Trusted Extensions에서 사용자의 시작 파일을 구성하는 방법”
비상 안전 세션에 로그인합니다.	잘못된 사용자 초기화 파일을 수정합니다.	88 페이지 “Trusted Extensions에서 비상 안전 세션에 로그인하는 방법”

▼ 기본 사용자 레이블 속성을 수정하는 방법

첫번째 시스템 구성 중에 기본 사용자 레이블 속성을 수정할 수 있습니다. 변경 사항을 모든 Trusted Extensions 호스트에 복사해야 합니다.

시작하기 전에 전역 영역에서 보안 관리자 역할을 가진 사용자여야 합니다. 자세한 내용은 51 페이지 “Trusted Extensions에서 전역 영역으로 들어가는 방법”을 참조하십시오.

1. **/etc/security/tsol/label_encodings 파일에서 기본 사용자 속성 설정을 검토합니다.**
   기본값은 77 페이지 “label_encodings 파일 기본값”을 참조하십시오.

2. **label_encodings 파일에서 사용자 속성 설정을 수정합니다.**
   신뢰할 수 있는 편집기를 사용합니다. 자세한 내용은 54 페이지 “Trusted Extensions에서 관리 파일을 편집하는 방법”을 참조하십시오. Trusted CDE에서도 레이블 인코딩 편집 작업을 사용할 수 있습니다. 자세한 내용은 54 페이지 “Trusted Extensions에서 CDE 관리 작업을 시작하는 방법”을 참조하십시오.

   label_encodings 파일은 모든 호스트에서 동일해야 합니다.

3. **파일 복사본을 모든 Trusted Extensions 호스트에 배포합니다.**

▼ policy.conf 기본값을 수정하는 방법

Trusted Extensions에서 policy.conf 기본값을 변경하는 것은 Oracle Solaris OS에서 보안 관련 시스템 파일을 변경하는 것과 유사합니다. Trusted Extensions에서는 신뢰할 수 있는 편집기를 사용하여 시스템 파일을 수정합니다.

시작하기 전에 전역 영역에서 보안 관리자 역할을 가진 사용자여야 합니다. 자세한 내용은 51 페이지 “Trusted Extensions에서 전역 영역으로 들어가는 방법”을 참조하십시오.

1. **/etc/security/policy.conf 파일에서 기본 설정을 검토합니다.**
   Trusted Extensions 키워드는 표 6–1을 참조하십시오.

2. **설정을 수정합니다.**

   신뢰할 수 있는 편집기를 사용하여 시스템 파일을 편집합니다. 자세한 내용은 54 페이지 “Trusted Extensions에서 관리 파일을 편집하는 방법”을 참조하십시오.

예 7–1 시스템의 유휴 설정 변경

이 예에서 보안 관리자는 유휴 시스템을 로그인 화면으로 되돌리려고 합니다. 기본값은 유휴 시스템을 잠그는 것입니다. 따라서 보안 관리자 역할은 IDLECMD 키워드=값 쌍을 /etc/security/policy.conf 파일에 다음과 같이 추가합니다.

```
IDLECMD=LOGOUT
```

또한 관리자는 시스템이 유휴 상태 이후 로그아웃되는 시간을 줄이려고 합니다. 따라서 보안 관리자 역할은 IDLETIME 키워드=값 쌍을 policy.conf 파일에 다음과 같이 추가합니다.

```
IDLETIME=10
```

이제 시스템은 10분 동안의 유휴 상태 이후 사용자를 로그아웃합니다.

예 7–2 모든 사용자의 기본 권한 세트 수정

이 예에서 Sun Ray 설치의 보안 관리자는 일반 사용자가 다른 Sun Ray 사용자의 프로세스를 볼 수 없게 하려고 합니다. 따라서 Trusted Extensions로 구성된 모든 시스템에서 관리자는 기본 권한 세트에서 proc_info를 제거합니다. /etc/policy.conf 파일의 PRIV_DEFAULT 설정은 다음과 같이 수정됩니다.

```
PRIV_DEFAULT=basic,!proc_info
```

예 7–3 시스템의 모든 사용자에게 인쇄 관련 권한 부여 지정

이 예에서 보안 관리자는 컴퓨터의 /etc/security/policy.conf 파일에 다음을 입력하여 공개 키오스크 컴퓨터에서 레이블 없이 인쇄할 수 있도록 합니다. 다음 부팅부터 이 키오스크에서 모든 사용자의 인쇄 작업은 페이지 레이블 없이 인쇄됩니다.

```
AUTHS_GRANTED= solaris.print.unlabeled
```

그런 다음 관리자는 용지 절약을 위해 배너 및 트레일러 페이지를 제거하기로 결정합니다. 먼저 인쇄 관리자에서 Always Print Banners(항상 배너 인쇄) 확인란이 선택되지 않았는지 확인합니다. 그리고 policy.conf 항목을 다음과 같이 수정하고 재부트합니다. 이제 모든 인쇄 작업은 레이블이 없으며 배너나 트레일러 페이지도 없습니다.

```
AUTHS_GRANTED= solaris.print.unlabeled,solaris.print.nobanner
```

▼ Trusted Extensions에서 사용자의 시작 파일을 구성하는 방법

사용자는 최소 민감도 레이블에서 해당하는 레이블의 .copy_files 파일 및 .link_files 파일을 홈 디렉토리에 넣을 수 있습니다. 또한 사용자의 최소 레이블에서 기존 .copy_files 및 .link_files 파일을 수정할 수 있습니다. 다음은 관리자 역할이 사이트에 대한 설정을 자동화하는 절차입니다.

시작하기 전에 전역 영역에서 시스템 관리자 역할을 가진 사용자여야 합니다. 자세한 내용은 51 페이지 "Trusted Extensions에서 전역 영역으로 들어가는 방법"을 참조하십시오.

1 두 Trusted Extensions 시작 파일을 만듭니다.

.copy_files 및 .link_files를 시작 파일 목록에 추가할 것입니다.

```
# cd /etc/skel
# touch .copy_files .link_files
```

2 .copy_files 파일을 사용자 정의합니다.

a. 신뢰할 수 있는 편집기를 시작합니다.

자세한 내용은 54 페이지 "Trusted Extensions에서 관리 파일을 편집하는 방법"을 참조하십시오.

b. .copy_files 파일의 전체 경로 이름을 입력합니다.

```
/etc/skel/.copy_files
```

c. 모든 레이블에서 사용자의 홈 디렉토리에 복사할 파일을 한 행에 하나씩 .copy_files에 입력합니다.

81 페이지 ".copy_files 및 .link_files 파일"을 참조하십시오. 샘플 파일은 예 7–4를 참조하십시오.

3 .link_files 파일을 사용자 정의합니다.

a. 신뢰할 수 있는 편집기에 .link_files 파일에 대한 전체 경로 이름을 입력합니다.

```
/etc/skel/.link_files
```

b. 모든 레이블에서 사용자의 홈 디렉토리에 링크할 파일을 한 행에 하나씩 .link_files에 입력합니다.

4 사용자에 대한 기타 시작 파일을 사용자 정의합니다.

- 시작 파일에 포함할 항목에 대한 자세한 내용은 **Oracle Solaris 관리: 기본 관리**의 "사용자 작업 환경 사용자 정의"를 참조하십시오.

- 자세한 내용은 **Oracle Solaris 관리: 기본 관리**의 "사용자 초기화 파일을 사용자가 정의하는 방법"을 참조하십시오.
- 예는 예 7–4를 참조하십시오.

5 **(옵션) 기본 셸이 프로파일 셸인 사용자에 대한 skelP 하위 디렉토리를 만듭니다.**

P는 프로파일 셸을 나타냅니다.

6 **사용자 정의된 시작 파일을 적절한 골격 디렉토리에 복사합니다.**

7 **사용자를 만들 때 적절한 skel*X* 경로 이름을 사용합니다.**

*X*는 셸 이름의 시작 문자를 나타냅니다(예: Bourne 셸의 경우 B, Korn 셸의 경우 K, C 셸의 경우 C, Profile 셸의 경우 P).

예 7–4 사용자의 시작 파일 사용자 정의

이 예에서 보안 관리자는 모든 사용자의 홈 디렉토리에 대한 파일을 구성합니다. 사용자가 로그인하기 전에 파일을 배치합니다. 파일은 사용자의 최소 레이블에 있습니다. 이 사이트에서 사용자의 기본 셸은 C 셸입니다.

보안 관리자는 신뢰할 수 있는 편집기에서 다음 내용으로 .copy_files 및 .link_files 파일을 만듭니다.

```
## .copy_files for regular users
## Copy these files to my home directory in every zone
.mailrc
.mozilla
.soffice
:wq

## .link_files for regular users with C shells
## Link these files to my home directory in every zone
.cshrc
.login
.Xdefaults
.Xdefaults-hostname
:wq

## .link_files for regular users with Korn shells
# Link these files to my home directory in every zone
.ksh
.profile
.Xdefaults
.Xdefaults-hostname
:wq
```

셸 초기화 파일에서 관리자는 사용자의 인쇄 작업이 레이블이 있는 프린터로 가도록 합니다.

```
## .cshrc file
setenv PRINTER conf-printer1
setenv LPDEST  conf-printer1

## .ksh file
export PRINTER conf-printer1
export LPDEST  conf-printer1
```

관리자는 `.Xdefaults-`*home-directory-server* 파일을 수정하여 `dtterm` 명령에서 새 터미널에 대해 `.profile` 파일을 소싱하도록 합니다.

```
## Xdefaults-HDserver
Dtterm*LoginShell: true
```

사용자 정의된 파일은 적절한 골격 디렉토리에 복사됩니다.

```
$ cp .copy_files .link_files .cshrc .login .profile \
.mailrc .Xdefaults .Xdefaults-home-directory-server \
/etc/skelC
$ cp .copy_files .link_files .ksh .profile \
.mailrc .Xdefaults .Xdefaults-home-directory-server \
/etc/skelK
```

일반 오류 가장 낮은 레이블에서 `.copy_files` 파일을 만든 다음 상위 영역으로 로그인하여 `updatehome` 명령을 실행하고 명령이 액세스 오류와 함께 실패할 경우 다음을 시도합니다.

- 상위 레벨 영역에서 하위 레벨 디렉토리를 볼 수 있는지 확인합니다.

  ```
  higher-level zone# ls /zone/lower-level-zone/home/username
  ACCESS ERROR: there are no files under that directory
  ```

- 디렉토리를 볼 수 없는 경우 상위 레벨 영역에서 자동 마운트 서비스를 다시 시작합니다.

  ```
  higher-level zone# svcadm restart autofs
  ```

홈 디렉토리에 대해 NFS 마운트를 사용하지 않는 경우 상위 레벨 영역의 자동 마운트는 `/zone/`*lower-level-zone*`/export/home/`*username*에서 `/zone/`*lower-level-zone*`/home/`*username*으로 루프백 마운트되어야 합니다.

▼ Trusted Extensions에서 비상 안전 세션에 로그인하는 방법

Trusted Extensions에서 비상 안전 로그인은 보호되어 있습니다. 일반 사용자가 셸 초기화 파일을 사용자 정의한 후 로그인할 수 없게 된 경우 비상 안전 로그인을 사용하여 사용자의 파일을 수정할 수 있습니다.

시작하기 전에 `root` 암호를 알고 있어야 합니다.

1. **Oracle Solaris OS와 마찬가지로 로그인 화면에서 Options(옵션) –> Failsafe Session(비상 안전 세션)을 선택합니다.**
2. **프롬프트에서 사용자가 사용자 이름과 암호를 제공하도록 합니다.**
3. **root 암호에 대한 프롬프트에서 root에 대한 암호를 제공합니다.**
   이제 사용자의 초기화 파일을 디버깅할 수 있습니다.

Solaris Management Console에서 사용자 및 권한 관리(작업 맵)

Trusted Extensions에서는 Solaris Management Console을 사용하여 사용자, 권한 부여, 권한 및 역할을 관리해야 합니다. 사용자 및 보안 속성을 관리하려면 보안 관리자 역할을 맡습니다. 다음 작업 맵에서는 레이블이 있는 환경에서 작업하는 사용자에 대해 수행하는 일반적인 작업을 설명합니다.

작업	설명	수행 방법
사용자의 레이블 범위를 수정합니다.	사용자가 작업할 수 있는 레이블을 수정합니다. 수정으로 `label_encodings` 파일에서 허용하는 범위를 제한하거나 확장할 수 있습니다.	90 페이지 “Solaris Management Console에서 사용자의 레이블 범위를 수정하는 방법”
편리한 권한 부여를 위해 권한 프로파일을 만듭니다.	일반 사용자에게 유용한 여러 권한이 있습니다. 이러한 권한 부여 자격을 갖춘 사용자에 대한 프로파일을 만듭니다.	91 페이지 “편리한 권한 부여를 위해 권한 프로파일을 만드는 방법”
사용자의 기본 권한 세트를 수정합니다.	사용자의 기본 권한 세트에서 권한을 제거합니다.	93 페이지 “사용자의 권한 세트를 제한하는 방법”
특정 사용자에 대한 계정 잠금을 방지합니다.	역할을 맡을 수 있는 사용자에 대해 계정 잠금을 해제해야 합니다.	95 페이지 “사용자에 대한 계정 잠금을 방지하는 방법”
사용자가 데이터 레이블을 재지정할 수 있도록 합니다.	사용자가 정보를 다운그레이드하거나 업그레이드할 수 있게 권한 부여합니다.	96 페이지 “사용자가 데이터의 보안 레벨을 변경할 수 있게 하는 방법”
시스템에서 사용자를 제거합니다.	사용자 및 사용자의 프로세스를 완전히 제거합니다.	96 페이지 “Trusted Extensions 시스템에서 사용자 계정을 삭제하는 방법”
기타 작업을 처리합니다.	Solaris Management Console을 사용하여 Trusted Extensions의 고유 작업이 아닌 작업을 처리합니다.	97 페이지 “Solaris Management Console에서 기타 작업 처리(작업 맵)”

▼ Solaris Management Console에서 사용자의 레이블 범위를 수정하는 방법

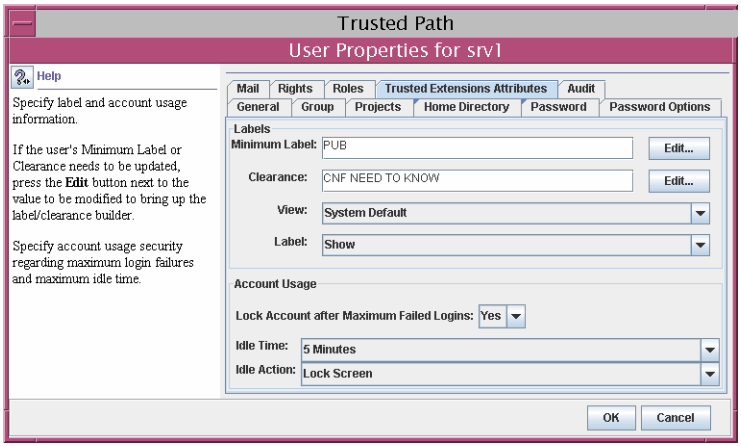
사용자에게 관리 응용 프로그램에 대한 읽기 액세스 권한을 부여하기 위해 사용자의 레이블 범위를 확장할 수 있습니다. 예를 들어, 전역 영역에 로그인할 수 있는 사용자는 Solaris Management Console을 실행할 수 있습니다. 사용자는 내용을 볼 수 있지만 변경할 수는 없습니다.

또는 사용자의 레이블 범위를 제한할 수도 있습니다. 예를 들어, guest 사용자는 하나의 레이블로 제한될 수 있습니다.

시작하기 전에 전역 영역에서 보안 관리자 역할을 가진 사용자여야 합니다.

1. **Solaris Management Console에서 Trusted Extensions 도구 상자를 엽니다.**
   적절한 범위의 도구 상자를 사용합니다. 자세한 내용은 **Trusted Extensions Configuration Guide**의 "Initialize the Solaris Management Console Server in Trusted Extensions"를 참조하십시오.
2. **System Configuration(시스템 구성)에서 User Accounts(사용자 계정)로 이동합니다.**
   암호 프롬프트가 표시될 수 있습니다.
3. **역할 암호를 입력합니다.**
4. **User Accounts(사용자 계정)에서 개별 사용자를 선택합니다.**

5 **Trusted Extensions Attributes(속성) 탭을 누릅니다.**



- **사용자의 레이블 범위를 확장하려면 더 상위의 클리어런스를 선택합니다.**
  최소 레이블을 낮출 수도 있습니다.
- **레이블 범위를 하나의 레이블로 제한하려면 클리어런스가 최소 레이블과 같아지도록 합니다.**

6 **변경 사항을 저장하려면 OK(확인)를 누릅니다.**

▼ 편리한 권한 부여를 위해 권한 프로파일을 만드는 방법

사이트 보안 정책에서 허용하는 경우 권한 부여가 필요한 작업을 수행할 수 있는 사용자에 대해 권한 부여가 포함된 권한 프로파일을 만들 수 있습니다. 특정 시스템의 모든 사용자가 권한 부여를 받도록 하려면 84 페이지 “policy.conf 기본값을 수정하는 방법”을 참조하십시오.

시작하기 전에 전역 영역에서 보안 관리자 역할을 가진 사용자여야 합니다.

1 **Solaris Management Console에서 Trusted Extensions 도구 상자를 엽니다.**
적절한 범위의 도구 상자를 사용합니다. 자세한 내용은 **Trusted Extensions Configuration Guide**의 “Initialize the Solaris Management Console Server in Trusted Extensions”를 참조하십시오.

2 **System Configuration(시스템 구성)에서 Rights(권한)로 이동합니다.**
암호 프롬프트가 표시될 수 있습니다.

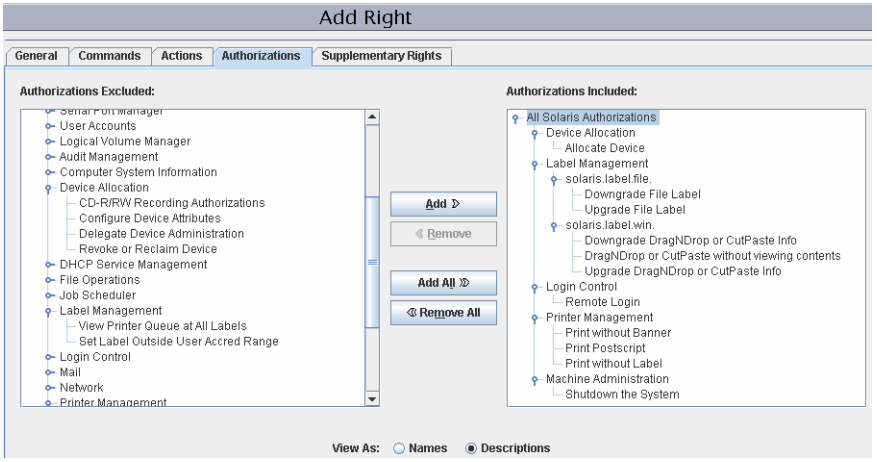
3 **역할 암호를 입력합니다.**

4 **권한 프로파일을 추가하려면 Action(작업) –> Add Right(권한 추가)를 누릅니다.**

5 **다음 권한 부여 중 하나 이상이 포함된 권한 프로파일을 만듭니다.**

단계별 절차는 **System Administration Guide: Security Services**의 "How to Create or Change a Rights Profile"을 참조하십시오.

다음 그림에서 Authorizations Included(포함된 권한 부여) 창에는 사용자에게 편리한 권한 부여가 표시되어 있습니다.



- Allocate Device(장치 할당) – 사용자가 마이크와 같은 주변 기기를 할당할 수 있게 권한을 부여합니다.

  기본적으로 Oracle Solaris 사용자는 CD-ROM을 읽고 쓸 수 있습니다. 그러나 Trusted Extensions에서는 장치를 할당할 수 있는 사용자만 CD-ROM 드라이브에 액세스할 수 있습니다. 사용할 드라이브를 할당하려면 권한 부여가 필요합니다. 따라서 Trusted Extensions에서 CD-ROM을 읽고 쓰려면 사용자에게 Allocate Device(장치 할당) 권한 부여가 필요합니다.

- Downgrade DragNDrop or CutPaste Info(DragNDrop 또는 CutPaste 정보 다운그레이드) – 사용자가 상위 레벨 파일에서 정보를 선택하고 하위 레벨 파일에 해당 정보를 넣을 수 있게 권한을 부여합니다.
- Downgrade File Label(파일 레이블 다운그레이드) – 사용자가 파일의 보안 레벨을 낮출 수 있게 권한을 부여합니다.
- DragNDrop or CutPaste without viewing contents(내용 보기 없이 DragNDrop 또는 CutPaste) – 사용자가 이동 중인 정보를 보지 않고 정보를 이동할 수 있게 권한을 부여합니다.
- Print Postscript(포스트스크립트 인쇄) – 사용자가 포스트스크립트 파일을 인쇄할 수 있게 권한을 부여합니다.

- Print without Banner(배너 없이 인쇄) - 사용자가 배너 페이지 없이 복사본을 인쇄할 수 있게 권한을 부여합니다.
- Print without Label(레이블 없이 인쇄) - 사용자가 레이블을 표시하지 않는 복사본을 인쇄할 수 있게 권한을 부여합니다.
- Remote Login(원격 로그인) – 사용자가 원격으로 로그인할 수 있게 권한을 부여합니다.
- Shutdown the System(시스템 종료) – 사용자가 시스템과 영역을 종료할 수 있게 권한을 부여합니다.
- Upgrade DragNDrop or CutPaste Info(DragNDrop 또는 CutPaste 정보 업그레이드) – 사용자가 하위 레벨 파일에서 정보를 선택하고 상위 레벨 파일에 해당 정보를 넣을 수 있게 권한을 부여합니다.
- Upgrade File Label(파일 레이블 업그레이드) – 사용자가 파일의 보안 레벨을 높일 수 있게 권한을 부여합니다.

6 **사용자 또는 역할에 권한 프로파일을 지정합니다.**

자세한 내용은 온라인 도움말을 참조하십시오. 단계별 절차는 **System Administration Guide: Security Services**의 "How to Change the RBAC Properties of a User"를 참조하십시오.

예 7–5 역할에 인쇄 관련 권한 부여 지정

다음 예에서 보안 관리자는 역할이 본문 페이지에 대한 레이블 없이 작업을 인쇄할 수 있도록 허용합니다.

Solaris Management Console에서 보안 관리자는 Administrative Roles(관리 역할)로 이동합니다. 특정 역할에 포함된 권한 프로파일을 보고, 인쇄 관련 권한 부여가 역할의 권한 프로파일 중 하나에 포함되어 있는지 확인합니다.

▼ 사용자의 권한 세트를 제한하는 방법

사이트 보안에 따라 사용자에게 기본적으로 지정되는 것보다 적은 수의 권한을 허용해야 할 수 있습니다. 예를 들어 Sun Ray 시스템에서 Trusted Extensions를 사용하는 사이트에서는 사용자가 Sun Ray 서버에서 다른 사용자의 프로세스를 보지 못하게 할 수 있습니다.

시작하기 전에 전역 영역에서 보안 관리자 역할을 가진 사용자여야 합니다.

1 **Solaris Management Console에서 Trusted Extensions 도구 상자를 엽니다.**

적절한 범위의 도구 상자를 사용합니다. 자세한 내용은 **Trusted Extensions Configuration Guide**의 "Initialize the Solaris Management Console Server in Trusted Extensions"를 참조하십시오.

2 **System Configuration(시스템 구성)에서 User Accounts(사용자 계정)로 이동합니다.**
암호 프롬프트가 표시될 수 있습니다.

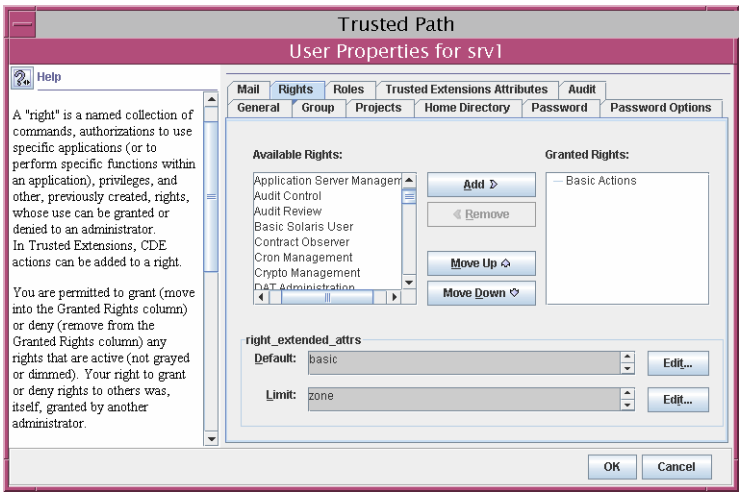
3 **역할 암호를 입력합니다.**

4 **사용자에 대한 아이콘을 두 번 누릅니다.**

5 **basic 세트에서 하나 이상의 권한을 제거합니다.**

a. **사용자에 대한 아이콘을 두 번 누릅니다.**

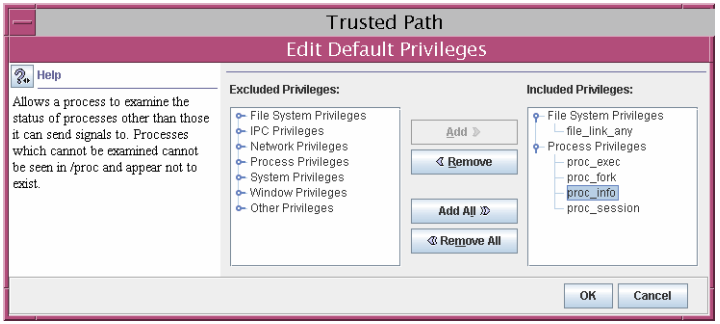
b. **Rights(권한) 탭을 누릅니다.**



c. **right_extended_attr 필드의 basic 세트 오른쪽에 있는 Edit(편집) 버튼을 누릅니다.**

d. **proc_session 또는 file_link_any를 제거합니다.**
proc_session 권한을 제거하면 사용자가 현재 세션 외부에 있는 프로세스를 볼 수 없게 됩니다. file_link_any 권한을 제거하면 사용자가 소유하고 있지 않은 파일에 대한 하드 링크를 만들 수 없게 됩니다.

주의 – proc_fork 또는 proc_exec 권한은 제거하지 마십시오. 이러한 권한이 없으면 사용자가 시스템을 사용할 수 없게 됩니다.



6 **변경 사항을 저장하려면 OK(확인)를 누릅니다.**

▼ 사용자에 대한 계정 잠금을 방지하는 방법

Trusted Extensions는 계정 잠금을 포함하도록 Solaris Management Console의 사용자 보안 기능을 확장합니다. 역할을 맡을 수 있는 사용자에 대한 계정 잠금을 해제합니다.

시작하기 전에 전역 영역에서 보안 관리자 역할을 가진 사용자여야 합니다.

1 **Solaris Management Console을 시작합니다.**

적절한 범위의 도구 상자를 사용합니다. 자세한 내용은 **Trusted Extensions Configuration Guide**의 "Initialize the Solaris Management Console Server in Trusted Extensions"를 참조하십시오.

2 **System Configuration(시스템 구성)에서 User Accounts(사용자 계정)로 이동합니다.**

암호 프롬프트가 표시될 수 있습니다.

3 **역할 암호를 입력합니다.**

4 **사용자에 대한 아이콘을 두 번 누릅니다.**

5 **Trusted Extensions Attributes(속성) 탭을 누릅니다.**

6 **Account Usage(계정 사용) 구역의 `Lock account after maximum failed logins`(최대 로그인 실패 횟수 이후 계정 잠금) 옆에 있는 풀다운 메뉴에서 `No`(아니오)를 선택합니다.**

7 **변경 사항을 저장하려면 OK(확인)를 누릅니다.**

▼ 사용자가 데이터의 보안 레벨을 변경할 수 있게 하는 방법

파일 및 디렉토리의 보안 레벨 또는 레이블을 변경할 수 있게 일반 사용자나 역할에 권한을 부여할 수 있습니다. 또한 두 개 이상의 레이블에서 작업할 수 있도록 사용자나 역할을 구성해야 합니다. 그리고 레이블 재지정을 허용하도록 레이블이 있는 영역을 구성해야 합니다. 절차는 130 페이지 "레이블이 있는 영역에서 파일의 레이블을 변경할 수 있게 설정하는 방법"을 참조하십시오.

주의 – 데이터의 보안 레벨 변경은 권한이 필요한 작업입니다. 이 작업은 신뢰할 수 있는 사용자만 수행해야 합니다.

시작하기 전에 전역 영역에서 보안 관리자 역할을 가진 사용자여야 합니다.

1. **91 페이지 "편리한 권한 부여를 위해 권한 프로파일을 만드는 방법"의 절차에 따라 권한 프로파일을 만듭니다.**

   다음 권한이 부여된 사용자는 파일 레이블을 재지정할 수 있습니다.

   - Downgrade File Label(파일 레이블 다운그레이드)
   - Upgrade File Label(파일 레이블 업그레이드)

   다음 권한이 부여된 사용자는 파일 내에서 정보 레이블을 재지정할 수 있습니다.

   - Downgrade DragNDrop or CutPaste Info(DragNDrop 또는 CutPaste 정보 다운그레이드)
   - DragNDrop or CutPaste Info Without Viewing(보기 없이 DragNDrop 또는 CutPaste 정보)
   - Upgrade DragNDrop or CutPaste Info(DragNDrop 또는 CutPaste 정보 업그레이드)

2. **Solaris Management Console을 사용하여 적절한 사용자 및 역할에 프로파일을 지정합니다.**

   자세한 내용은 온라인 도움말을 참조하십시오. 단계별 절차는 **System Administration Guide: Security Services**의 "How to Change the RBAC Properties of a User".

▼ Trusted Extensions 시스템에서 사용자 계정을 삭제하는 방법

사용자가 시스템에서 제거되면 해당 사용자의 홈 디렉토리 및 사용자가 소유한 모든 객체도 삭제되었는지 확인해야 합니다. 사용자가 소유한 객체를 삭제하는 대신 이러한 객체의 소유권을 유효한 사용자로 변경할 수도 있습니다.

또한 해당 사용자와 연결된 모든 배치 작업도 삭제되었는지 확인해야 합니다. 제거된 사용자에게 속하지 않은 객체나 프로세스는 시스템에 남겨 둘 수 있습니다.

시작하기 전에 시스템 관리자 역할을 가진 사용자여야 합니다.

1. **모든 레이블에서 사용자의 홈 디렉토리를 아카이브합니다.**
2. **모든 레이블에서 사용자의 메일 파일을 아카이브합니다.**
3. **Solaris Management Console에서 사용자 계정을 삭제합니다.**
   a. **Solaris Management Console에서 Trusted Extensions 도구 상자를 엽니다.**
      적절한 범위의 도구 상자를 사용합니다. 자세한 내용은 **Trusted Extensions Configuration Guide**의 "Initialize the Solaris Management Console Server in Trusted Extensions"를 참조하십시오.
   b. **System Configuration(시스템 구성)에서 User Accounts(사용자 계정)로 이동합니다.**
      암호 프롬프트가 표시될 수 있습니다.
   c. **역할 암호를 입력합니다.**
   d. **제거할 사용자 계정을 선택하고 Delete(삭제) 버튼을 누릅니다.**
      사용자의 홈 디렉토리 및 메일 파일을 삭제할지 묻는 프롬프트가 나타납니다. 프롬프트를 승인하면 사용자의 홈 디렉토리 및 메일 파일이 전역 영역에서만 삭제됩니다.
4. **모든 레이블이 있는 영역에서 사용자의 디렉토리 및 메일 파일을 수동으로 삭제합니다.**

주 – `/tmp` 디렉토리의 파일을 비롯하여 모든 레이블에서 사용자의 임시 파일을 찾아 삭제해야 합니다.

Solaris Management Console에서 기타 작업 처리(작업 맵)

Oracle Solaris 절차에 따라 Solaris Management Console에서 작업을 처리합니다. 사용자는 수퍼유저이거나 전역 영역에서 역할을 가진 사용자여야 합니다. 다음 작업 맵에서는 기본적인 Solaris Management Console 작업을 설명합니다.

작업	수행 방법
Solaris Management Console을 사용하여 관리 작업을 수행합니다.	**Oracle Solaris 관리: 기본 관리**의 2 장, "Solaris Management Console 작업(작업)"
사용자를 만듭니다.	**Oracle Solaris 관리: 기본 관리**의 "RBAC와 함께 Solaris 관리 도구 사용(작업 맵)"

작업	수행 방법
역할을 만듭니다.	**System Administration Guide: Security Services**의 "How to Create and Assign a Role by Using the GUI"
역할을 수정합니다.	**System Administration Guide: Security Services**의 "How to Change the Properties of a Role"
권한 프로파일을 만들거나 수정합니다.	**System Administration Guide: Security Services**의 "How to Create or Change a Rights Profile"
사용자의 기타 보안 속성을 변경합니다.	**System Administration Guide: Security Services**의 "How to Change the RBAC Properties of a User"
역할의 작업을 감사합니다.	**System Administration Guide: Security Services**의 "How to Audit Roles"
`smprofile list -D`*name-service-type*`:/`*server-name*`/`*domain-name* 을 사용하여 권한 프로파일을 나열합니다.	**System Administration Guide: Security Services**의 **9 장, Using Role-Based Access Control (Tasks)"** 또는 `smprofile`(1M) 매뉴얼 페이지

◆ ◆ ◆ 8 장

8 Trusted Extensions에서 원격 관리(작업)

이 장에서는 Trusted Extensions 관리 도구를 사용하여 원격 시스템을 관리하는 방법에 대해 설명합니다.

- 99 페이지 “Trusted Extensions에서 보안 원격 관리”
- 100 페이지 “Trusted Extensions에서 원격 시스템을 관리하는 방법”
- 101 페이지 “Trusted Extensions에서 역할을 통한 원격 로그인”
- 102 페이지 “원격으로 Trusted Extensions 관리(작업 맵)”

Trusted Extensions에서 보안 원격 관리

기본적으로 Trusted Extensions에서는 원격 관리를 허용하지 않습니다. 원격 관리를 허용하면 신뢰할 수 없는 원격 시스템의 사용자가 Trusted Extensions로 구성된 시스템을 관리할 수 있으므로 보안 위험이 커집니다. 따라서 처음에는 시스템이 원격 관리 옵션 없이 설치됩니다.

네트워크가 구성될 때까지 모든 원격 호스트에는 `admin_low` 보안 템플리트가 지정됩니다. 따라서 CIPSO 프로토콜은 연결에 사용되거나 허용되지 않습니다. 이 초기 상태에서 시스템은 다양한 방식을 통해 원격 공격으로부터 보호됩니다. 방식으로는 `netservices` 설정, 기본 로그인 정책, PAM 정책 등이 있습니다.

- `netservices` SMF(서비스 관리 기능) 프로파일을 `limited`로 설정하면 SSH만 사용으로 설정되고 다른 원격 서비스는 사용으로 설정되지 않습니다. 그러나 로그인 및 PAM 정책으로 인해 `ssh` 서비스는 원격 로그인에 사용할 수 없습니다.
- `/etc/default/login` 파일의 `CONSOLE`에 대한 기본 정책에서 `root`에 의한 원격 로그인을 금지하므로 `root` 계정을 원격 로그인에 사용할 수 없습니다.
- 원격 로그인에 적용되는 두 가지 PAM 설정이 있습니다.

  `pam_roles` 모듈은 `role` 유형 계정에서의 로컬 로그인을 항상 거부합니다. 기본적으로 이 모듈은 원격 로그인을 거부합니다. 그러나 시스템의 `pam.conf` 항목에서 `allow_remote`를 지정하여 원격 로그인을 허용하도록 시스템을 구성할 수 있습니다.

pam_tsol_account 모듈은 CIPSO 프로토콜을 사용하지 않을 경우 전역 영역으로의 원격 로그인을 거부합니다. 이 정책은 다른 Trusted Extensions 시스템에서 원격 관리를 수행하기 위한 것입니다.

원격 로그인 기능을 사용으로 설정하려면 두 시스템에서 모두 해당 피어 시스템을 CIPSO 보안 템플리트에 지정해야 합니다. 이 방법으로 효과가 없는 경우 pam.conf 파일에서 allow_unlabeled 옵션을 지정하여 네트워크 프로토콜 정책을 완화할 수 있습니다. 정책을 완화할 경우 임의의 시스템에서 전역 영역에 액세스할 수 없도록 기본 네트워크 템플리트를 변경해야 합니다. 와일드카드 주소 0.0.0.0이 기본값 ADMIN_LOW 레이블로 설정되지 않도록 가급적 admin_low 템플리트를 사용하지 않고 tnrhdb 데이터베이스를 수정해야 합니다. 자세한 내용은 102 페이지 "원격으로 Trusted Extensions 관리(작업 맵)" 및 177 페이지 "신뢰할 수 있는 네트워크에서 연결할 수 있는 호스트를 제한하는 방법"을 참조하십시오.

Trusted Extensions에서 원격 시스템을 관리하는 방법

일반적으로 관리자는 rlogin 및 ssh 명령을 사용하여 명령줄에서 원격 시스템을 관리합니다. Solaris Management Console도 사용할 수도 있습니다. Trusted CDE에서 dtappsession 프로그램은 Trusted CDE 작업을 원격으로 시작할 수 있습니다. Solaris 10 5/09 릴리스부터 가상 네트워킹 컴퓨터(VNC: Virtual Networking Computer)는 다중 레벨 데스크탑을 원격으로 표시하는 데 사용할 수 있습니다.

Trusted Extensions에서는 다음과 같은 방법으로 원격 관리를 수행할 수 있습니다.

- 루트 사용자가 터미널에서 원격 호스트로 로그인할 수 있습니다. 103 페이지 "Trusted Extensions의 명령줄에서 원격으로 로그인하는 방법"을 참조하십시오. 이 방법은 Oracle Solaris 시스템에서와 동일하게 작동합니다. 이 방법은 안전하지 않습니다.
- 역할이 역할 작업 공간의 터미널에서 원격 호스트에 로그인할 수 있습니다. 103 페이지 "Trusted Extensions의 명령줄에서 원격으로 로그인하는 방법"을 참조하십시오.
- 관리자가 원격 시스템에서 실행 중인 Solaris Management Console 서버를 시작할 수 있습니다. 105 페이지 "Trusted Extensions 시스템에서 Solaris Management Console을 사용하여 시스템을 원격으로 관리하는 방법"을 참조하십시오.
- dtappsession 명령을 사용하여 Trusted_Extensions 폴더의 작업을 원격으로 시작할 수 있습니다. 103 페이지 "dtappsession을 사용하여 Trusted Extensions를 원격으로 관리하는 방법"을 참조하십시오.
- 사용자는 VNC 클라이언트 프로그램으로 Trusted Extensions 시스템에서 Xvnc 서버에 연결하여 원격 다중 레벨 데스크탑에 로그인할 수 있습니다. 109 페이지 "Xvnc를 사용하여 Trusted Extensions 시스템에 원격으로 액세스하는 방법"을 참조하십시오.

Trusted Extensions에서 역할을 통한 원격 로그인

Oracle Solaris OS에서와 마찬가지로 각 호스트의 `/etc/default/login` 파일에서 원격 로그인을 허용하도록 설정을 변경해야 합니다. 또한 `pam.conf` 파일을 수정해야 할 수 있습니다. Trusted Extensions에서는 보안 관리자가 변경을 담당합니다. 절차는 **Trusted Extensions Configuration Guide**의 "Enable Remote Login by root User in Trusted Extensions" 및 **Trusted Extensions Configuration Guide**의 "Enable Remote Login by a Role in Trusted Extensions"을 참조하십시오.

Trusted Extensions 및 Oracle Solaris 호스트 모두에서 원격으로 로그인하려면 권한 부여가 필요할 수도 있습니다. 101 페이지 "Trusted Extensions에서 원격 로그인 관리"에서는 권한 부여가 필요한 로그인의 조건과 유형에 대해 설명합니다. 기본적으로 역할에는 Remote Login(원격 로그인) 권한 부여가 있습니다.

레이블이 없는 호스트에서 원격 역할 기반 관리

Trusted Extensions에서 사용자는 Trusted Path(신뢰할 수 있는 경로) 메뉴를 통해 역할을 맡습니다. 그러면 역할이 신뢰할 수 있는 작업 공간에서 작동합니다. 기본적으로 신뢰할 수 있는 경로를 벗어나서 역할을 맡을 수 없습니다. 사이트 정책에서 허용하는 경우 보안 관리자는 기본 정책을 변경할 수 있습니다. Solaris Management Console 2.1 클라이언트 소프트웨어를 실행 중인 레이블이 없는 호스트의 관리자는 신뢰할 수 있는 호스트를 관리할 수 있습니다.

- 기본 정책을 변경하려면 **Trusted Extensions Configuration Guide**의 "Enable Remote Login by a Role in Trusted Extensions"을 참조하십시오.
- 원격으로 시스템을 관리하려면 103 페이지 "Trusted Extensions의 명령줄에서 원격으로 로그인하는 방법"을 참조하십시오.

이 정책 변경은 원격 레이블이 없는 시스템의 사용자가 Trusted Extensions 호스트에 사용자 계정을 가지고 있는 경우에만 적용됩니다. Trusted Extensions 사용자는 관리 역할을 맡을 수 있어야 합니다. 그러면 역할이 Solaris Management Console을 사용하여 원격 시스템을 관리할 수 있습니다.

주의 – Trusted Extensions가 아닌 호스트에서 원격 관리가 사용으로 설정된 경우 Trusted Extensions 관리 작업 공간보다 관리 환경의 보호 수준이 낮습니다. 따라서 암호와 기타 보안 데이터를 입력할 때 주의하십시오. 또한 Solaris Management Console을 시작하기 전에 신뢰할 수 없는 응용 프로그램을 모두 종료하십시오.

Trusted Extensions에서 원격 로그인 관리

두 Trusted Extensions 호스트 간의 원격 로그인은 현재 로그인 세션의 확장으로 간주됩니다.

rlogin 명령 실행 시 암호를 묻지 않는 경우 권한 부여가 필요하지 않습니다. 원격 호스트의 사용자 홈 디렉토리에 있는 /etc/hosts.equiv 파일이나 .rhosts 파일에 원격 로그인을 시도 중인 호스트 또는 사용자 이름이 나열되어 있는 경우 암호가 필요하지 않습니다. 자세한 내용은 rhosts(4) 및 rlogin(1) 매뉴얼 페이지를 참조하십시오.

ftp 명령을 통한 로그인 등의 다른 모든 원격 로그인의 경우 Remote Login(원격 로그인) 권한 부여가 필요합니다.

Remote Login(원격 로그인) 권한 부여를 포함하는 권한 프로파일을 만들려면 89 페이지 “Solaris Management Console에서 사용자 및 권한 관리(작업 맵)”를 참조하십시오.

원격으로 Trusted Extensions 관리(작업 맵)

다음 작업 맵에서는 원격 Trusted Extensions 시스템을 관리하는 데 사용되는 작업에 대해 설명합니다.

작업	설명	수행 방법
root가 Trusted Extensions 시스템에 원격으로 로그인할 수 있게 허용합니다.	root 사용자가 레이블이 있는 시스템에서 원격으로 작업할 수 있게 허용합니다.	**Trusted Extensions Configuration Guide**의 “Enable Remote Login by root User in Trusted Extensions”
역할이 Trusted Extensions 시스템에 원격으로 로그인할 수 있게 허용합니다.	모든 역할이 레이블이 있는 시스템에서 원격으로 작업할 수 있습니다.	**Trusted Extensions Configuration Guide**의 “Enable Remote Login by a Role in Trusted Extensions”
레이블이 없는 시스템에서 Trusted Extensions 시스템으로의 원격 로그인을 허용합니다.	모든 사용자나 역할이 레이블이 없는 시스템에서 원격으로 작업할 수 있습니다.	**Trusted Extensions Configuration Guide**의 “Enable Remote Login From an Unlabeled System”
Trusted Extensions 시스템에 원격으로 로그인합니다.	Trusted Extensions 시스템에 역할로 로그인합니다.	103 페이지 “Trusted Extensions의 명령줄에서 원격으로 로그인하는 방법”
원격으로 시스템을 관리합니다.	dtappsession 명령을 사용하여 Trusted_Extensions 작업으로 원격 시스템을 관리합니다.	103 페이지 “dtappsession을 사용하여 Trusted Extensions를 원격으로 관리하는 방법”
	Trusted Extensions 시스템에서 Solaris Management Console을 사용하여 원격 호스트를 관리합니다.	105 페이지 “Trusted Extensions 시스템에서 Solaris Management Console을 사용하여 시스템을 원격으로 관리하는 방법”
	레이블이 없는 시스템에서 Solaris Management Console을 사용하여 원격 Trusted Extensions 호스트를 관리합니다.	106 페이지 “레이블이 없는 시스템에서 Solaris Management Console을 사용하여 시스템을 원격으로 관리하는 방법”

작업	설명	수행 방법
원격 시스템 관리 및 사용	클라이언트에서 원격 Trusted Extensions의 Xvnc 서버를 사용하여 클라이언트로 다시 연결되는 다중 레벨 세션을 표시합니다.	109 페이지 “Xvnc를 사용하여 Trusted Extensions 시스템에 원격으로 액세스하는 방법”
특정 사용자가 전역 영역에 로그인할 수 있도록 사용으로 설정합니다.	Solaris Management Console에서 사용자 및 네트워크 도구를 사용하여 특정 사용자가 전역 영역에 액세스할 수 있도록 허용합니다.	108 페이지 “특정 사용자가 Trusted Extensions의 전역 영역에 원격으로 로그인할 수 있게 설정하는 방법”

▼ Trusted Extensions의 명령줄에서 원격으로 로그인하는 방법

주 – `telnet` 명령은 기본 ID와 역할 ID를 `pam_roles` 모듈에 전달할 수 없으므로 원격 역할을 맡는 데 사용할 수 없습니다.

시작하기 전에 사용자와 역할이 로컬 시스템과 원격 시스템에 동일하게 정의되어 있어야 합니다.

역할에 Remote Login(원격 로그인) 권한 부여가 있어야 합니다. 기본적으로 이 권한 부여는 Remote Administration 프로파일과 Maintenance and Repair 권한 프로파일에 있습니다.

보안 관리자가 원격으로 관리할 수 있는 모든 시스템에서 **Trusted Extensions Configuration Guide**의 “Enable Remote Login by a Role in Trusted Extensions” 절차를 완료했습니다. 레이블이 없는 시스템에서 시스템을 관리할 수 있는 경우 **Trusted Extensions Configuration Guide**의 “Enable Remote Login From an Unlabeled System” 절차도 완료되었습니다.

- **역할을 맡을 수 있는 사용자의 작업 공간에서 원격 호스트에 로그인합니다.**

  `rlogin`, `ssh` 또는 `ftp` 명령을 사용합니다.

  - `rlogin -l` 또는 `ssh` 명령을 사용하여 로그인하는 경우 역할의 권한 프로파일에 있는 모든 명령을 사용할 수 있습니다.
  - `ftp` 명령을 사용하는 경우 사용 가능한 명령은 `ftp(1)` 매뉴얼 페이지를 참조하십시오.

▼ dtappsession을 사용하여 Trusted Extensions를 원격으로 관리하는 방법

관리자는 `dtappsession` 프로그램을 사용하여 CDE를 실행 중인 원격 시스템을 관리할 수 있습니다.

dtappsession은 원격 시스템에 모니터가 없는 경우 유용합니다. 예를 들어, dtappsession은 대규모 서버에서 도메인을 관리하는 데 많이 사용됩니다. 자세한 내용은 dtappsession(1) 매뉴얼 페이지를 참조하십시오.

시작하기 전에 레이블이 있는 시스템의 경우 전역 영역에서 관리 역할을 가진 사용자여야 합니다. 레이블이 없는 시스템의 경우 원격 시스템에 정의된 역할을 맡아야 합니다. 그런 다음 역할의 프로파일 셸에서 원격 로그인을 실행해야 합니다.

1. **(옵션) 원격 세션 전용 작업 공간을 만듭니다.**

   원격 CDE 응용 프로그램과 로컬 응용 프로그램 간의 혼동을 방지하기 위해 관리 역할 작업 공간을 이 절차 전용으로 사용합니다. 자세한 내용은 **Trusted Extensions User's Guide**의 "How to Add a Workspace at a Particular Label"을 참조하십시오.

2. **원격 호스트에 로그인합니다.**

   rlogin 또는 ssh 명령을 사용할 수 있습니다.

   ```
   $ ssh remote-host
   ```

3. **원격 관리를 시작합니다.**

   터미널 창에서 dtappsession 명령과 로컬 호스트 이름을 차례로 입력합니다.

   ```
   $ /usr/dt/bin/dtappsession local-host
   ```

   원격 호스트에서 실행 중인 Application Manager(응용 프로그램 관리자)가 로컬 호스트에 표시됩니다. Exit(종료) 대화 상자도 나타납니다.

4. **원격 호스트를 관리합니다.**

   Trusted CDE에서 원격 세션을 호출한 경우 Trusted_Extensions 폴더의 작업을 사용할 수 있습니다.

5. **작업이 끝나면 Exit(종료) 버튼을 누릅니다.**

주의 – Application Manager(응용 프로그램 관리자)를 닫아도 로그인 세션은 종료되지 않으므로 이 방법을 사용하지 않는 것이 좋습니다.

6 **터미널 창에서 원격 로그인 세션을 종료합니다.**

`hostname` 명령을 사용하여 로컬 호스트에 있는지 확인합니다.

```
$ exit
$ hostname
local-host
```

▼ Trusted Extensions 시스템에서 Solaris Management Console을 사용하여 시스템을 원격으로 관리하는 방법

Solaris Management Console에서는 사용자, 권한, 역할 및 네트워크를 관리할 수 있는 원격 관리 인터페이스를 제공합니다. 콘솔을 사용할 역할을 맡습니다. 이 절차에서는 로컬 시스템에서 콘솔을 실행하고 원격 시스템을 서버로 지정합니다.

시작하기 전에 다음 절차를 완료했습니다.

- 두 시스템 모두 – **Trusted Extensions Configuration Guide**의 "Initialize the Solaris Management Console Server in Trusted Extensions"
- 원격 시스템 – **Trusted Extensions Configuration Guide**의 "Enable Remote Login by a Role in Trusted Extensions" 및 **Trusted Extensions Configuration Guide**의 "Enable the Solaris Management Console to Accept Network Communications"
- LDAP 서버인 원격 시스템 – **Trusted Extensions Configuration Guide**의 "Configuring the Solaris Management Console for LDAP (Task Map)"

1 **로컬 시스템에서 원격 시스템에 동일하게 정의되어 있는 사용자로 로그인합니다.**

2 **시스템을 관리하는 데 사용할 역할을 맡습니다.**

3 **역할에서 Solaris Management Console을 시작합니다.**

자세한 내용은 **Trusted Extensions Configuration Guide**의 "Initialize the Solaris Management Console Server in Trusted Extensions"를 참조하십시오.

a. **Server(서버) 대화 상자에 원격 서버의 이름을 입력합니다.**

- **LDAP을 이름 지정 서비스로 사용 중인 경우 LDAP 서버의 이름을 입력합니다.**

  다음 범위 중 하나를 선택합니다.

  - **이름 지정 서비스에서 데이터베이스를 관리하려면 Scope=LDAP 도구 상자를 선택합니다.**

    이 컴퓨터(*ldap-server*: `Scope=LDAP, Policy=TSOL`)

- **LDAP 서버에서 로컬 파일을 관리하려면 Scope=Files 도구 상자를 선택합니다.**
  이 컴퓨터(*ldap-server*: Scope=Files, Policy=TSOL)
- **LDAP을 이름 지정 서비스로 사용하지 않을 경우 관리할 원격 시스템의 이름을 입력합니다.**
  그런 다음 Scope=Files 도구 상자를 선택합니다.
  이 컴퓨터(*remote-system*: Scope=Files, Policy=TSOL)

4 **System Configuration(시스템 구성)에서 도구를 선택합니다.**
User(사용자)와 같은 도구를 선택하면 대화 상자에 Solaris Management Console 서버 이름, 사용자 이름, 역할 이름, 역할 암호 입력란 등이 표시됩니다. 항목이 올바른지 확인하십시오.

5 **로컬 시스템과 원격 시스템에 동일하게 정의되어 있는 역할로 Solaris Management Console 서버에 로그인합니다.**
역할 암호를 입력하고 Login as Role(역할로 로그인)을 누릅니다. 이제 Solaris Management Console을 사용하여 시스템을 관리할 수 있습니다.

주 – Solaris Management Console을 사용하여 dtappsession을 실행할 수 있지만 dtappsession을 사용하는 가장 간단한 방법은 103 페이지 "dtappsession을 사용하여 Trusted Extensions를 원격으로 관리하는 방법"을 참조하십시오.

▼ 레이블이 없는 시스템에서 Solaris Management Console을 사용하여 시스템을 원격으로 관리하는 방법

이 절차에서는 원격 시스템에서 Solaris Management Console 클라이언트와 서버를 실행하고 로컬 시스템에 콘솔을 표시합니다.

시작하기 전에 Trusted Extensions 시스템에서 ADMIN_LOW 레이블을 로컬 시스템에 지정해야 합니다.

주 – CIPSO 프로토콜을 실행하지 않는 시스템(예: Trusted Solaris 시스템)은 Trusted Extensions 시스템의 관점에서 레이블이 없는 시스템입니다.

원격 연결을 수락하도록 원격 시스템의 Solaris Management Console 서버를 구성해야 합니다. 절차는 **Trusted Extensions Configuration Guide**의 "Enable the Solaris Management Console to Accept Network Communications"를 참조하십시오.

두 시스템 모두에서 Solaris Management Console을 사용할 수 있는 역할이 지정된 동일한 사용자가 있어야 합니다. 사용자의 범위는 일반 사용자의 레이블 범위일 수 있지만 역할의 범위는 ADMIN_LOW ~ ADMIN_HIGH이어야 합니다.

전역 영역에서 관리 역할을 가진 사용자여야 합니다.

1 로컬 X 서버에서 원격 Solaris Management Console을 표시할 수 있습니다.

```
# xhost + TX-SMC-Server
# echo $DISPLAY
:n.n
```

2 로컬 시스템에서 Solaris Management Console에 대한 역할을 맡을 수 있는 사용자가 됩니다.

```
# su - same-username-on-both-systems
```

3 해당 사용자로 원격 서버에 역할로 로그인합니다.

```
$ rlogin -l same-rolename-on-both-systems  TX-SMC-Server
```

4 Solaris Management Console에서 사용하는 환경 변수의 값이 올바른지 확인하십시오.

a. DISPLAY 변수 값을 설정합니다.

```
$ DISPLAY=local:n.n
$ export DISPLAY=local:n.n
```

b. LOGNAME 변수 값을 사용자 이름으로 설정합니다.

```
$ LOGNAME=same-username-on-both-systems
$ export LOGNAME=same-username-on-both-systems
```

c. USER 변수 값을 역할 이름으로 설정합니다.

```
$ USER=same-rolename-on-both-systems
$ export USER=same-rolename-on-both-systems
```

5 역할의 명령줄에서 Solaris Management Console을 시작합니다.

```
$ /usr/sbin/smc &
```

6 System Configuration(시스템 구성)에서 도구를 선택합니다.

User(사용자)와 같은 도구를 선택하면 대화 상자에 Solaris Management Console 서버 이름, 사용자 이름, 역할 이름, 역할 암호 입력란 등이 표시됩니다. 항목이 올바른지 확인하십시오.

7 역할로 서버에 로그인합니다.

역할 암호를 입력하고 Login as Role(역할로 로그인)을 누릅니다. 이제 Solaris Management Console을 사용하여 시스템을 관리할 수 있습니다.

주 – LDAP 서버가 아닌 시스템에서 네트워크 데이터베이스 정보에 액세스하려고 하는 경우 작업에 실패합니다. 콘솔에서 원격 호스트에 로그인하여 도구 상자를 열 수 있습니다. 그러나 정보에 액세스하거나 정보를 변경하려고 하는 경우 다음과 같은 오류 메시지가 표시되어 LDAP 서버가 아닌 시스템에서 `Scope=LDAP`를 선택했음을 나타냅니다.

```
Management server cannot perform the operation requested.
...
Error extracting the value-from-tool.
The keys received from the client were machine, domain, Scope.
Problem with Scope.
```

▼ 특정 사용자가 Trusted Extensions의 전역 영역에 원격으로 로그인할 수 있게 설정하는 방법

사용자의 기본 레이블 범위와 영역의 기본 동작이 역할 없이 원격으로 로그인할 수 있게 변경됩니다. 원격 레이블이 있는 시스템을 사용 중인 테스터를 위해 이 절차를 수행할 수 있습니다. 보안을 위해 테스터의 시스템에서 다른 사용자의 비연속 레이블을 실행하고 있어야 합니다.

시작하기 전에 이 사용자가 전역 영역에 로그인해야 하는 타당한 이유가 있어야 합니다.

전역 영역에서 보안 관리자 역할을 가진 사용자여야 합니다.

1 특정 사용자가 전역 영역에 로그인할 수 있게 하려면 해당 사용자에게 관리 레이블 범위를 지정합니다.

Solaris Management Console을 사용하여 `ADMIN_HIGH`의 클리어런스와 `ADMIN_LOW`의 최소 레이블을 각 사용자에게 지정합니다. 자세한 내용은 90 페이지 “Solaris Management Console에서 사용자의 레이블 범위를 수정하는 방법”을 참조하십시오.

사용자의 레이블이 있는 영역에서도 로그인을 허용해야 합니다.

2 레이블이 있는 영역에서 전역 영역으로 원격 로그인할 수 있게 하려면 다음을 수행하십시오.

a. 원격 로그인에 대한 다중 레벨 포트를 전역 영역에 추가합니다.

Solaris Management Console을 사용합니다. TCP 프로토콜을 통해 포트 513으로 원격 로그인할 수 있습니다. 예는 132 페이지 “영역에 대한 다중 레벨 포트를 만드는 방법”을 참조하십시오.

b. 커널에 대한 `tnzonecfg` 변경 사항을 확인합니다.

```
# tnctl -fz /etc/security/tsol/tnzonecfg
```

c. 원격 로그인 서비스를 다시 시작합니다.

```
# svcadm restart svc:/network/login:rlogin
```

▼ Xvnc를 사용하여 Trusted Extensions 시스템에 원격으로 액세스하는 방법

VNC(Virtual Network Computing) 기술은 클라이언트를 원격 서버에 연결한 다음 클라이언트의 창에 원격 서버의 데스크탑을 표시합니다. Xvnc는 표준 X 서버를 기반으로 하는 VNC의 UNIX 버전입니다. Trusted Extensions에서는 모든 플랫폼의 클라이언트가 Trusted Extensions 소프트웨어를 실행 중인 Xvnc에 연결하여 Xvnc 서버에 로그인한 다음 다중 레벨 데스크탑을 표시한 후 작업할 수 있습니다.

시작하기 전에 Xvnc 서버로 사용할 시스템에서 Trusted Extensions 소프트웨어를 설치하고 구성했습니다. 레이블이 있는 영역을 만들고 부트했습니다. Xvnc 서버에서 호스트 이름 또는 IP 주소로 VNC 클라이언트를 인식합니다.

Xvnc 서버로 사용할 시스템의 전역 영역에서 수퍼유저입니다.

1 Xvnc 서버를 구성합니다.

자세한 내용은 `Xvnc(1)` 및 `vncconfig(1)` 매뉴얼 페이지를 참조하십시오.

주의 – Solaris 10 10/08 또는 Solaris 10 5/08 릴리스를 실행 중인 경우 서버를 구성하기 전에 시스템을 패치해야 합니다. SPARC 시스템의 경우 패치 125719의 최신 버전을 설치합니다. x86 시스템의 경우 패치 125720의 최신 버전을 설치합니다.

a. Xservers 구성 디렉토리를 만듭니다.

```
# mkdir -p /etc/dt/config
```

b. /usr/dt/config/Xservers 파일을 /etc/dt/config 디렉토리에 복사합니다.

```
# cp /usr/dt/config/Xservers /etc/dt/config/Xservers
```

c. Xserver나 Xorg 대신 Xvnc 프로그램을 시작하도록 /etc/dt/config/Xservers 파일을 편집합니다.

이 예에서는 암호 없이 서버에 로그인하도록 항목이 구성됩니다. 데스크탑에 성공적으로 로그인하려면 로컬 UID가 `console`이 아니고 `none`이어야 합니다.

보기 좋게 항목이 나뉘었지만 실제로는 한 라인에 있어야 합니다.

```
#   :0  Local local_uid@console root /usr/X11/bin/Xserver :0 -nobanner
  :0  Local local_uid@none root /usr/X11/bin/Xvnc :0 -nobanner
  -AlwaysShared -SecurityTypes None -geometry 1024x768x24 -depth 24
```

주 – 안전한 구성을 위해 `-SecurityTypes VncAuth` 매개변수를 지정하여 암호를 사용하는 것이 좋습니다. `Xvnc(1)` 매뉴얼 페이지에서는 암호 요구 사항에 대해 설명합니다.

d. 서버를 재부트하거나 Xvnc 서버를 시작합니다.

```
# reboot
```

재부트한 후 Xvnc 프로그램이 실행 중인지 확인합니다.

```
# ps -ef | grep Xvnc
  root  2145  932  0  Jan 18 ?  6:15 /usr/X11/bin/Xvnc :0 -nobanner
  -AlwaysShared -SecurityTypes None -geometry 1024
```

2 Trusted Extensions Xvnc 서버의 모든 VNC 클라이언트에서 VNC 클라이언트 소프트웨어를 설치합니다.

클라이언트 시스템의 경우 소프트웨어를 선택할 수 있습니다. 이 예에서는 Sun VNC 소프트웨어를 사용합니다.

```
# cd SUNW-pkg-directory
# pkgadd -d . SUNWvncviewer
```

3 VNC 클라이언트의 터미널 창에서 서버에 연결합니다.

```
% /usr/bin/vncviewer Xvnc-server-hostname
```

4 표시되는 창에서 이름과 암호를 입력합니다.

로그인 절차를 계속합니다. 나머지 단계에 대한 자세한 설명은 **Trusted Extensions User's Guide**의 "Logging In to Trusted Extensions"을 참조하십시오.

서버에 수퍼유저로 로그인한 경우 서버를 즉시 관리할 수 있습니다. 서버에 사용자로 로그인한 경우 시스템을 관리하는 역할을 맡아야 합니다.

◆ ◆ ◆ 9 장

9 Trusted Extensions 및 LDAP(개요)

이 장에서는 Trusted Extensions를 사용하여 구성된 시스템에서 Oracle Directory Server Enterprise Edition(Directory Server)를 사용하는 것에 대해 설명합니다.

- 111 페이지 “Trusted Extensions에서 이름 지정 서비스 사용”
- 113 페이지 “Trusted Extensions에서 LDAP 이름 지정 서비스 사용”

Trusted Extensions에서 이름 지정 서비스 사용

여러 Trusted Extensions 시스템이 있는 보안 도메인에서 사용자, 호스트 및 네트워크 속성의 동일성을 유지하기 위해 대부분의 구성 정보 배포 시 이름 지정 서비스가 사용됩니다. LDAP은 이름 지정 서비스의 한 예입니다. `nsswitch.conf` 파일이 사용할 이름 지정 서비스를 결정합니다. Trusted Extensions에는 LDAP를 이름 지정 서비스로 사용하는 것이 좋습니다.

Directory Server는 Trusted Extensions 및 Oracle Solaris 클라이언트에 대한 LDAP 이름 지정 서비스를 제공할 수 있습니다. 서버에 Trusted Extensions 네트워크 데이터베이스가 포함되어야 하며, Trusted Extensions 클라이언트가 다중 레벨 포트를 통해 해당 서버에 연결되어야 합니다. Trusted Extensions를 구성할 때 보안 관리자가 다중 레벨 포트를 지정합니다.

Trusted Extensions는 LDAP 서버에 두 개의 신뢰할 수 있는 네트워크 데이터베이스, 즉 tnrhdb와 tnrhtp를 추가합니다. 이러한 데이터베이스는 Solaris Management Console의 Security Templates(보안 템플리트) 도구를 사용하여 관리합니다. Scope=LDAP, Policy=TSOL 도구 상자에 Directory Server의 구성 변경 사항이 보관됩니다.

- Oracle Solaris OS에서 LDAP 이름 지정 서비스를 사용하는 것에 대한 자세한 내용은 **System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)**를 참조하십시오.
- Trusted Extensions 클라이언트에 대한 디렉토리 서버 설정은 **Trusted Extensions Configuration Guide**에 설명되어 있습니다. Trusted Extensions 시스템은 Trusted Extensions를 사용하여 구성된 LDAP 프록시 서버를 사용하여 Oracle Solaris LDAP 서버의 클라이언트가 될 수 있습니다.

주 – Trusted Extensions를 사용하여 구성된 시스템은 NIS 또는 NIS+ 마스터의 클라이언트가 될 수 없습니다.

네트워크되지 않은 Trusted Extensions 시스템

사이트에서 이름 지정 서비스가 사용되지 않는 경우 관리자는 모든 호스트에서 사용자, 호스트 및 네트워크에 대한 구성 정보가 동일한지 확인해야 합니다. 한 호스트에서 정보를 변경하면 모든 호스트에서도 변경되어야 합니다.

네트워크되지 않은 Trusted Extensions 시스템에서 구성 정보는 /etc, /etc/security 및 /etc/security/tsol 디렉토리에서 유지 관리됩니다. Trusted_Extensions 폴더의 작업을 사용하여 일부 구성 정보를 수정할 수 있습니다. Solaris Management Console의 Security Templates(보안 템플리트) 도구를 사용하여 네트워크 데이터베이스 매개변수를 수정할 수 있습니다. 사용자, 역할 및 권한은 User Accounts(사용자 계정), Administrative Roles(관리 역할) 및 Rights(권한) 도구에서 수정합니다. 이 컴퓨터의 Scope=Files, Policy=TSOL 도구 상자에 구성 변경 사항이 로컬로 저장됩니다.

Trusted Extensions LDAP 데이터베이스

Trusted Extensions는 Directory Server의 스키마를 확장하여 tnrhdb 및 tnrhtp 데이터베이스를 수용합니다. Trusted Extensions는 ipTnetNumber 및 ipTnetTemplateName이라는 두 개의 새로운 속성과 ipTnetTemplate 및 ipTnetHost라는 두 개의 새로운 객체 클래스를 정의합니다.

속성 정의는 다음과 같습니다.

```
ipTnetNumber
   ( 1.3.6.1.1.1.1.34 NAME 'ipTnetNumber'
     DESC 'Trusted network host or subnet address'
     EQUALITY caseExactIA5Match
     SYNTAX 1.3.6.1.4.1.1466.115.121.1.26
     SINGLE-VALUE )
```

```
ipTnetTemplateName
   ( 1.3.6.1.1.1.1.35 NAME 'ipTnetTemplateName'
     DESC 'Trusted network template name'
     EQUALITY caseExactIA5Match
     SYNTAX 1.3.6.1.4.1.1466.115.121.1.26
     SINGLE-VALUE )
```

객체 클래스 정의는 다음과 같습니다.

```
ipTnetTemplate
   ( 1.3.6.1.1.1.2.18 NAME 'ipTnetTemplate' SUP top STRUCTURAL
     DESC 'Object class for Trusted network host templates'
     MUST ( ipTnetTemplateName )
     MAY ( SolarisAttrKeyValue ) )

ipTnetHost
   ( 1.3.6.1.1.1.2.19 NAME 'ipTnetHost' SUP top AUXILIARY
     DESC 'Object class for Trusted network host/subnet address
           to template mapping'
     MUST ( ipTnetNumber $ ipTnetTemplateName ) )
```

LDAP의 `cipso` 템플리트 정의는 다음과 유사합니다.

```
ou=ipTnet,dc=example,dc=example1,dc=exampleco,dc=com
 objectClass=top
 objectClass=organizationalUnit
 ou=ipTnet

 ipTnetTemplateName=cipso,ou=ipTnet,dc=example,dc=example1,dc=exampleco,dc=com
 objectClass=top
 objectClass=ipTnetTemplate
 ipTnetTemplateName=cipso
 SolarisAttrKeyValue=host_type=cipso;doi=1;min_sl=ADMIN_LOW;max_sl=ADMIN_HIGH;

 ipTnetNumber=0.0.0.0,ou=ipTnet,dc=example,dc=example1,dc=exampleco,dc=com
 objectClass=top
 objectClass=ipTnetTemplate
 objectClass=ipTnetHost
 ipTnetNumber=0.0.0.0
 ipTnetTemplateName=internal
```

Trusted Extensions에서 LDAP 이름 지정 서비스 사용

LDAP 이름 지정 서비스는 Oracle Solaris OS에서 관리되는 것처럼 Trusted Extensions에서 관리됩니다. 다음은 유용한 명령어의 예이며 자세한 정보를 알아 볼 수 있는 참조가 포함되어 있습니다.

- LDAP 구성 문제를 해결하기 위한 전략에 대해서는 **System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)**의 13 장, "LDAP Troubleshooting (Reference)"을 참조하십시오.
- 레이블로 인한 클라이언트-서버 LDAP 연결 문제를 해결하려면 191 페이지 "LDAP 서버에 대한 클라이언트 연결을 디버깅하는 방법"을 참조하십시오.

- 이외의 클라이언트-서버 LDAP 연결 문제를 해결하려면 **System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)**의 13 장, "LDAP Troubleshooting (Reference)"을 참조하십시오.
- LDAP 클라이언트에서 LDAP 항목을 표시하려면 다음을 입력하십시오.

```
$ ldaplist -l
$ ldap_cachemgr -g
```

- LDAP 서버에서 LDAP 항목을 표시하려면 다음을 입력하십시오.

```
$ ldap_cachemgr -g
$ idsconfig -v
```

- LDAP가 관리하는 호스트를 나열하려면 다음을 입력하십시오.

```
$ ldaplist -l hosts       Long listing
$ ldaplist hosts          One-line listing
```

- LDAP의 DIT(Directory Information Tree) 정보를 나열하려면 다음을 입력하십시오.

```
$ ldaplist -l services | more
dn: cn=apocd+ipServiceProtocol=udp,ou=Services,dc=exampleco,dc=com
  objectClass: ipService
  objectClass: top
  cn: apocd
  ipServicePort: 38900
  ipServiceProtocol: udp

...
$ ldaplist services name
dn=cn=name+ipServiceProtocol=udp,ou=Services,dc=exampleco,dc=com
```

- 클라이언트의 LDAP 서비스 상태를 표시하려면 다음을 입력하십시오.

```
# svcs -xv network/ldap/client
svc:/network/ldap/client:default (LDAP client)
 State: online since date
   See: man -M /usr/share/man -s 1M ldap_cachemgr
   See: /var/svc/log/network-ldap-client:default.log
Impact: None.
```

- LDAP 클라이언트를 시작 및 중지하려면 다음을 입력하십시오.

```
# svcadm enable network/ldap/client

# svcadm disable network/ldap/client
```

- Oracle Directory Server Enterprise Edition 소프트웨어 버전 5.2에서 LDAP 서버를 시작 및 중지하려면 다음을 입력하십시오.

```
# installation-directory/slap-LDAP-server-hostname/start-slapd
# installation-directory/slap-LDAP-server-hostname/stop-slapd
```

- Oracle Directory Server Enterprise Edition 소프트웨어 버전 6에서 LDAP 서버를 시작 및 중지하려면 다음을 입력하십시오.

```
# dsadm start /export/home/ds/instances/your-instance
# dsadm stop /export/home/ds/instances/your-instance
```

- Oracle Directory Server Enterprise Edition 소프트웨어 버전 6에서 프록시 LDAP 서버를 시작 및 중지하려면 다음을 입력하십시오.

```
# dpadm start /export/home/ds/instances/your-instance
# dpadm stop /export/home/ds/instances/your-instance
```

◆ ◆ ◆ 10장

10 Trusted Extensions에서 영역 관리(작업)

이 장에서는 Trusted Extensions로 구성된 시스템에서 비전역 영역이 어떻게 작동하는지 설명합니다. Trusted Extensions의 영역에 고유한 절차도 제공합니다.

- 117 페이지 "Trusted Extensions의 영역"
- 120 페이지 "전역 영역 프로세스 및 레이블이 있는 영역"
- 121 페이지 "Trusted Extensions의 영역 관리 유틸리티"
- 122 페이지 "영역 관리(작업 맵)"

Trusted Extensions의 영역

올바르게 구성된 Trusted Extensions 시스템은 운영 체제 인스턴스인 전역 영역과 레이블이 있는 하나 이상의 비전역 영역으로 구성됩니다. 구성하는 동안 Trusted Extensions에서 각 영역에 고유한 레이블을 연결하여 레이블이 있는 영역을 만듭니다. 레이블은 `label_encodings` 파일에서 가져옵니다. 관리자는 각 레이블에 대해 하나의 영역을 만들 수 있지만, 반드시 그래야 하는 것은 아닙니다. 시스템에 레이블이 있는 영역보다 레이블이 더 많을 수 있습니다. 레이블보다 레이블이 있는 영역이 더 많을 수는 없습니다.

Trusted Extensions 시스템에서 영역의 파일 시스템은 대개 루프백 파일 시스템(lofs)으로 마운트됩니다. 레이블이 있는 영역에서 모든 쓰기 가능한 파일과 디렉토리는 영역의 레이블에 있습니다. 기본적으로 사용자는 현재 레이블보다 하위 레이블에 있는 영역의 파일을 볼 수 있습니다. 이 구성을 통해 현재 작업 공간의 레이블보다 하위 레이블에 있는 홈 디렉토리를 볼 수 있습니다. 사용자는 하위 레이블에서 파일을 볼 수 있지만 수정할 수는 없습니다. 사용자는 파일과 동일한 레이블을 가진 프로세스에서만 파일을 수정할 수 있습니다.

Trusted Extensions에서 전역 영역은 관리 영역입니다. 레이블이 있는 영역은 일반 사용자용입니다. 사용자는 레이블이 승인 범위 내에 있는 영역에서 작업할 수 있습니다.

모든 영역에는 연결된 IP 주소와 보안 속성이 있습니다. MLP(다중 레벨 포트)로 영역을 구성할 수 있습니다. `ping`과 같은 ICMP(Internet Control Message Protocol) 브로드캐스트에 대한 정책으로 영역을 구성할 수도 있습니다.

레이블이 있는 영역에서 디렉토리를 공유하는 방법과 레이블이 있는 영역에서 원격으로 디렉토리를 마운트하는 방법은 11 장, “Trusted Extensions에서 파일 관리 및 마운트(작업)”를 참조하십시오.

Trusted Extensions의 영역은 Oracle Solaris 영역 제품을 기반으로 빌드됩니다. 자세한 내용은 **System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones**의 제II부, “Zones”를 참조하십시오. 특히 패치 및 패키지 설치 문제는 Trusted Extensions에 영향을 줍니다. 자세한 내용은 **System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones**의 25 장, “About Packages and Patches on an Oracle Solaris System With Zones Installed (Overview)” 및 **System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones**의 30 장, “Troubleshooting Miscellaneous Oracle Solaris Zones Problems”을 참조하십시오.

Trusted Extensions의 영역 및 IP 주소

초기 설치 팀이 전역 영역과 레이블이 있는 영역에 IP 주소를 지정했습니다. 세 가지 구성 유형 **Trusted Extensions Configuration Guide**의 “Creating Labeled Zones”에 설명되어 있습니다.

- 시스템에 전역 영역과 레이블이 있는 모든 영역에 대한 IP 주소가 하나 있습니다.

  이 구성은 DHCP 소프트웨어를 사용하여 해당 IP 주소를 얻는 시스템에 유용합니다. 사용자가 로그인할 수 없는 경우 LDAP 서버에서 이 구성을 사용할 수 있습니다.

- 시스템에 전역 영역에 대한 IP 주소와 전역 영역을 포함한 모든 영역에서 공유되는 IP 주소가 하나씩 있습니다. 모든 영역에서 고유 주소와 공유 주소를 조합하여 사용할 수 있습니다.

  이 구성은 일반 사용자가 로그인하는 시스템에 유용합니다. 프린터나 NFS 서버에도 이 구성을 사용할 수 있습니다. 이 구성은 IP 주소를 절약합니다.

- 시스템에 전역 영역에 대한 IP 주소가 하나 있고 레이블이 있는 영역마다 고유 IP 주소가 있습니다.

  이 구성은 단일 레벨 시스템의 개별 물리적 네트워크에 액세스하는 데 유용합니다. 일반적으로 각 영역에는 다른 레이블이 있는 영역과 구별되는 물리적 네트워크상의 IP 주소가 있습니다. 이 구성은 단일 IP 인스턴스로 구현되기 때문에 전역 영역은 물리적 인터페이스를 제어하고 전역 리소스(예: 경로 테이블)를 관리합니다.

비전역 영역에 대한 배타적 IP 인스턴스를 도입하여 Oracle Solaris OS에서 네번째 유형의 구성을 사용할 수 있습니다. Solaris 10 8/07 릴리스부터 비전역 영역은 자체 IP 인스턴스를 지정받고 자체 물리적 인터페이스를 관리할 수 있습니다. 이 구성에서 각 영역은 고유

시스템처럼 작동합니다. 자세한 내용은 **System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones**의 "Zone Network Interfaces"를 참조하십시오.

그러나 이 구성에서 각 레이블이 있는 영역은 고유한 단일 레이블이 있는 시스템처럼 작동합니다. Trusted Extensions의 다중 레벨 네트워킹 기능은 공유 IP 스택의 기능을 사용합니다. Trusted Extensions의 관리 절차에서는 전역 영역에서 네트워킹을 완전히 제어하는 것으로 가정합니다. 따라서 초기 설치 팀에서 배타적 IP 인스턴스로 레이블이 있는 영역을 설치한 경우 사이트별 설명서를 제공하거나 알려줘야 합니다.

영역 및 다중 레벨 포트

기본적으로 영역 간에는 패킷을 보내고 받을 수 없습니다. 포트의 특정 서비스에서 MLP(다중 레벨 포트)를 사용하여 레이블 범위나 레이블 세트에서 요청을 받을 수 있습니다. 이 권한 있는 서비스에서는 요청 레이블에 응답할 수 있습니다. 예를 들어, 모든 레이블을 수신할 수 있지만 레이블에 의해 응답이 제한되는 권한 있는 웹 브라우저 포트를 만들 수 있습니다. 기본적으로 레이블이 있는 영역에는 MLP가 없습니다.

MLP가 받을 수 있는 패킷을 제한하는 레이블 범위나 레이블 세트는 영역의 IP 주소를 기반으로 합니다. IP 주소에 `tnrhdb` 데이터베이스의 원격 호스트 템플리트가 지정됩니다. 원격 호스트 템플리트의 레이블 범위나 레이블 세트는 MLP가 받을 수 있는 패킷을 제한합니다.

- 다른 IP 주소 구성에 대한 MLP 제약 조건은 다음과 같습니다.
- 전역 영역에 IP 주소가 하나 있고 레이블이 있는 영역마다 고유한 IP 주소가 있는 시스템의 경우 특정 서비스에 대한 MLP를 모든 영역에 추가할 수 있습니다. 예를 들어, TCP 포트 22를 통한 `ssh` 서비스를 전역 영역과 레이블이 있는 모든 영역의 MLP로 사용하도록 시스템을 구성할 수 있습니다.
- 일반적인 구성에서는 전역 영역에 하나의 IP 주소가 지정되고 레이블이 있는 영역에서 두번째 IP 주소를 전역 영역과 공유합니다. MLP를 공유 인터페이스에 추가하면 MLP가 정의된 레이블이 있는 영역으로 서비스 패킷이 경로 지정됩니다. 레이블이 있는 영역에 대한 원격 호스트 템플리트에 패킷 레이블이 포함되어 있는 경우에만 패킷이 수락됩니다. 범위가 `ADMIN_LOW ~ ADMIN_HIGH`이면 모든 패킷이 수락됩니다. 보다 좁은 범위를 사용하면 범위에 포함되지 않는 패킷은 무시됩니다.

  일반적으로 한 영역에서 특정 포트를 공유 인터페이스에 대한 MLP로 정의할 수 있습니다. `ssh` 포트가 비전역 영역의 공유 MLP로 구성된 앞의 시나리오에서 다른 영역은 공유 주소에 대한 `ssh` 연결을 수신할 수 없습니다. 그러나 전역 영역에서는 `ssh` 포트를 영역별 주소에 대한 연결을 수신할 수 있는 개인 MLP로 정의할 수 있습니다.
- 전역 영역과 레이블이 있는 영역이 IP 주소를 공유하는 시스템에서는 `ssh` 서비스에 대한 MLP를 한 영역에 추가할 수 있습니다. `ssh`에 대한 MLP를 전역 영역에 추가하면 레이블이 있는 영역에서는 `ssh` 서비스에 대한 MLP를 추가할 수 없습니다. 마찬가지로 `ssh` 서비스에 대한 MLP를 레이블이 있는 영역에 추가하면 `ssh` MLP로 전역 영역을 구성할 수 없습니다.

MLP를 레이블이 있는 영역에 추가하는 예는 예 13–16을 참조하십시오.

Trusted Extensions의 영역 및 ICMP

네트워크에서 브로드캐스트 메시지를 전송하고 ICMP 패킷을 네트워크상의 시스템에 보냅니다. 다중 레벨 시스템의 경우 모든 레이블의 시스템이 이러한 전송으로 가득 찰 수 있습니다. 기본적으로 레이블이 있는 영역에 대한 네트워크 정책에 따라 일치하는 레이블에서만 ICMP 패킷을 수신해야 합니다.

전역 영역 프로세스 및 레이블이 있는 영역

Trusted Extensions에서는 전역 영역의 프로세스를 포함한 모든 프로세스에 MAC 정책이 적용됩니다. 전역 영역의 프로세스는 ADMIN_HIGH 레이블에서 실행됩니다. 전역 영역에서 공유되는 파일은 ADMIN_LOW 레이블에서 공유됩니다. MAC에서는 상위 레이블이 있는 프로세스에서 하위 레이블 객체를 수정하지 못하므로 일반적으로 전역 영역에서 NFS 마운트된 시스템에 쓸 수 없습니다.

드물기는 하지만 레이블이 있는 영역에서 작업하기 위해 전역 영역 프로세스에서 해당 영역의 파일을 수정해야 하는 경우가 있습니다.

전역 영역 프로세스에서 읽기/쓰기 권한을 사용하여 원격 파일 시스템을 마운트하려면 레이블이 원격 파일 시스템의 레이블과 일치하는 영역의 영역 경로 아래에 마운트해야 합니다. 이때 영역의 루트 경로 아래에 마운트할 수는 없습니다.

- 마운팅 시스템에는 원격 파일 시스템과 동일한 레이블에 영역이 있어야 합니다.
- 시스템에서 동일한 레이블이 있는 영역의 영역 경로 아래에 원격 파일 시스템을 마운트해야 합니다.

  시스템에서 동일한 레이블이 있는 영역의 **영역 루트 경로** 아래에 원격 파일 시스템을 마운트할 수는 **없습니다**.

PUBLIC 레이블에 이름이 public인 영역이 있다고 가정합니다. **영역 경로**는 /zone/public/입니다. 영역 경로 아래의 모든 디렉토리는 PUBLIC 레이블에 있습니다. 예를 들면 다음과 같습니다.

```
/zone/public/dev
/zone/public/etc
/zone/public/home/username
/zone/public/root
/zone/public/usr
```

영역 경로 아래의 디렉토리 중에서 /zone/public/root 아래에 있는 파일만 공용 영역에 표시됩니다. PUBLIC 레이블에 있는 모든 다른 디렉토리와 파일은 전역 영역에서만 액세스할 수 있습니다. /zone/public/root 경로는 **영역 루트 경로**입니다.

공용 영역 관리자의 관점에서 영역 루트 경로는 /로 표시됩니다. 마찬가지로 공용 영역 관리자는 영역 경로의 사용자 홈 디렉토리인 /zone/public/home/*username* 디렉토리에 액세스할 수 없습니다. 이 디렉토리는 전역 영역에서만 표시됩니다. 공용 영역에서는 영역 루트 경로의 이 디렉토리를 /home/ *username*으로 마운트합니다. 전역 영역의 관점에서 이 마운트는 /zone/public/root/home/*username*으로 표시됩니다.

공용 영역 관리자는 /home/*username*을 수정할 수 있습니다. 사용자의 홈 디렉토리에서 파일을 수정해야 하는 경우 전역 영역 프로세스에서는 해당 경로를 사용하지 않습니다. 전역 영역에서는 영역 경로의 사용자 홈 디렉토리인 /zone/public/home/*username*을 사용합니다.

- /zone/*zonename*/ 영역 경로 아래에 있지만 영역 루트 경로인 /zone/*zonename*/root 디렉토리 아래에는 없는 파일과 디렉토리는 ADMIN_HIGH 레이블에서 실행되는 전역 영역 프로세스를 통해 수정할 수 있습니다.
- /zone/public/root 영역 루트 경로 아래에 있는 파일과 디렉토리는 레이블이 있는 영역 관리자가 수정할 수 있습니다.

예를 들어, 공용 영역에서 장치를 할당하면 ADMIN_HIGH 레이블에서 실행되는 전역 영역 프로세스에서 영역 경로의 dev 디렉토리(/zone/public/dev)를 수정합니다. 마찬가지로 사용자가 데스크탑 구성을 저장하면 /zone/public/home/*username*의 전역 영역 프로세스에서 데스크탑 구성 파일을 수정합니다. 마지막으로, 레이블이 있는 영역에서 파일을 공유하기 위해 전역 영역 관리자가 /zone/public/etc/dfs/dfstab 영역 경로에 dfstab 구성 파일을 만듭니다. 레이블이 있는 영역 관리자는 이 파일에 액세스할 수 없으므로 레이블이 있는 영역에서 파일을 공유할 수 없습니다. 레이블이 있는 디렉토리를 공유하려면 142 페이지 “레이블이 있는 영역에서 디렉토리를 공유하는 방법”을 참조하십시오.

Trusted Extensions의 영역 관리 유틸리티

명령줄에서 몇 가지 영역 관리 작업을 수행할 수 있습니다. 그러나 영역을 관리하는 가장 간단한 방법은 Trusted Extensions에서 제공하는 GUI를 사용하는 것입니다.

- 영역 보안 속성은 Solaris Management Console의 Trusted Network Zones(신뢰할 수 있는 네트워크 영역) 도구를 사용하여 구성합니다. 도구에 대한 자세한 내용은 41 페이지 “Trusted Network Zones(신뢰할 수 있는 네트워크 영역) 도구”를 참조하십시오. 영역 구성 및 만들기 예는 **Trusted Extensions Configuration Guide**의 4장, “Configuring Trusted Extensions (Tasks)” 및 132 페이지 “영역에 대한 다중 레벨 포트를 만드는 방법”을 참조하십시오.
- /usr/sbin/txzonemgr 셸 스크립트는 영역 만들기, 설치, 초기화 및 부트를 위한 메뉴 기반 마법사를 제공합니다. Solaris Trusted Extensions(JDS)에서 영역을 관리할 경우 Trusted CDE 작업 대신 txzonemgr 스크립트를 사용하십시오. txzonemgr에서는 zenity 명령을 사용합니다. 자세한 내용은 zenity(1) 매뉴얼 페이지를 참조하십시오.

- Trusted CDE에서는 Trusted_Extensions 폴더에서 영역 구성 및 만들기 작업을 수행할 수 있습니다. 작업에 대한 자세한 내용은 35 페이지 “Trusted CDE 작업”을 참조하십시오. 작업을 사용하는 절차는 54 페이지 “Trusted Extensions에서 CDE 관리 작업을 시작하는 방법”을 참조하십시오.

영역 관리(작업 맵)

다음 작업 맵에서는 Trusted Extensions에 특정한 영역 관리 작업을 설명합니다. 또한 이 맵은 Oracle Solaris 시스템과 Trusted Extensions에서 수행되는 공통 절차를 알려줍니다.

작업	설명	수행 방법
모든 영역을 봅니다.	모든 레이블에서 현재 영역의 지배를 받는 영역을 봅니다.	123 페이지 “준비 또는 실행 중인 영역을 표시하는 방법”
마운트된 디렉토리를 봅니다.	모든 레이블에서 현재 레이블의 지배를 받는 디렉토리를 봅니다.	124 페이지 “마운트된 파일의 레이블을 표시하는 방법”
일반 사용자가 `/etc` 파일을 볼 수 있게 합니다.	루프백에서는 레이블이 있는 영역에 기본적으로 표시되지 않는 디렉토리 또는 파일을 전역 영역에서 마운트합니다.	126 페이지 “레이블이 있는 영역에 일반적으로 표시되지 않는 파일을 루프백 마운트하는 방법”
일반 사용자가 상위 레이블에서 하위 레벨 홈 디렉토리를 보지 못하게 합니다.	기본적으로 하위 레벨 디렉토리는 상위 레벨 영역에서 표시됩니다. 한 하위 레벨 영역의 마운트를 사용 안함으로 설정하면 하위 레벨 영역의 모든 마운트가 사용 안함으로 설정됩니다.	127 페이지 “하위 레벨 파일의 마운트를 사용 안함으로 설정하는 방법”
파일에서 레이블을 변경할 수 있도록 영역을 구성합니다.	레이블이 있는 영역은 제한된 권한을 가집니다. 기본적으로 레이블이 있는 영역에는 권한 부여된 사용자가 파일 레이블을 변경하게 할 수 있는 권한이 없습니다. 영역 구성을 수정하여 권한을 추가합니다.	130 페이지 “레이블이 있는 영역에서 파일의 레이블을 변경할 수 있게 설정하는 방법”
레이블이 있는 영역의 내부 또는 외부로 파일이나 디렉토리를 이동합니다.	파일이나 디렉토리의 레이블을 변경하여 해당 보안 레벨을 변경합니다.	**Trusted Extensions User's Guide**의 “How to Move Files Between Labels in Trusted CDE”
ZFS 데이터 세트를 레이블이 있는 영역에 연결하고 공유합니다.	레이블이 있는 영역에서 읽기/쓰기 권한으로 ZFS 데이터 세트를 마운트하고 상위 영역과 읽기 전용으로 공유합니다.	128 페이지 “레이블이 있는 영역에서 ZFS 데이터 세트를 공유하는 방법”

작업	설명	수행 방법
새 영역을 구성합니다.	이 시스템에서 영역의 레이블을 지정하는 데 현재 사용되고 있지 않은 레이블에서 영역을 만듭니다.	**Trusted Extensions Configuration Guide**의 "Name and Label the Zone"을 참조하십시오. 그런 다음 초기 설치 팀에서 다른 영역을 만드는 데 사용한 절차를 따릅니다. 작업 단계는 **Trusted Extensions Configuration Guide**의 "Creating Labeled Zones"를 참조하십시오.
응용 프로그램에 대한 다중 레벨 포트를 만듭니다.	다중 레벨 포트는 레이블이 있는 영역에 대한 다중 레벨 피드를 필요로 하는 프로그램에 유용합니다.	132 페이지 "udp를 통해 NFSv3에 대한 다중 레벨 포트를 구성하는 방법" 132 페이지 "영역에 대한 다중 레벨 포트를 만드는 방법"
NFS 마운트 및 액세스 문제를 해결합니다.	마운트 및 영역에 대한 일반 액세스 문제를 디버깅합니다.	149 페이지 "Trusted Extensions에서 마운트 실패 문제를 해결하는 방법"
레이블이 있는 영역을 제거합니다.	레이블이 있는 영역을 시스템에서 완전히 제거합니다.	**System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones**의 "How to Remove a Non-Global Zone"

▼ 준비 또는 실행 중인 영역을 표시하는 방법

이 절차에서는 현재 영역과 현재 영역에서 지배하는 모든 영역의 레이블을 표시하는 셸 스크립트를 만듭니다.

시작하기 전에 전역 영역에서 시스템 관리자 역할을 가진 사용자여야 합니다.

1 신뢰할 수 있는 편집기를 사용하여 `getzonelabels` 스크립트를 만듭니다.

자세한 내용은 54 페이지 "Trusted Extensions에서 관리 파일을 편집하는 방법"을 참조하십시오.

스크립트에 경로 이름(예: `/usr/local/scripts/getzonelabels`)을 제공합니다.

2 다음 내용을 추가하고 파일을 저장합니다.

```
#!/bin/sh
#
echo "NAME\t\tSTATUS\t\tLABEL"
echo "====\t\t======\t\t====="
myzone=‘zonename‘
for i in ‘/usr/sbin/zoneadm list -p‘ ; do
        zone=‘echo $i | cut -d ":" -f2‘
        status=‘echo $i | cut -d ":" -f3‘
        path=‘echo $i | cut -d ":" -f4‘
        if [ $zone != global ]; then
```

```
                if [ $myzone = global ]; then
                        path=$path/root/tmp
                else
                        path=$path/export/home
                fi
        fi
        label=‘/usr/bin/getlabel -s $path |cut -d ":" -f2-9‘
        if [ ‘echo $zone|wc -m‘ -lt 8 ]; then
                echo "$zone\t\t$status\t$label"
        else
                echo "$zone\t$status\t$label"
        fi
done
```

3 전역 영역에서 스크립트를 테스트합니다.

```
# getzonelabels
NAME            STATUS          LABEL
====            ======          =====
global          running         ADMIN_HIGH
needtoknow      running         CONFIDENTIAL : NEED TO KNOW
restricted      ready           CONFIDENTIAL : RESTRICTED
internal        running         CONFIDENTIAL : INTERNAL
public          running         PUBLIC
```

스크립트를 전역 영역에서 실행하면 준비되거나 실행 중인 모든 영역의 레이블이 표시됩니다. 다음은 기본 `label_encodings` 파일에서 만든 영역에 대한 전역 영역 출력입니다.

예 10–1 준비 또는 실행 중인 모든 영역의 레이블 표시

다음 예에서는 `internal` 영역에서 `getzonelabels` 스크립트를 실행합니다.

```
# getzonelabels
NAME            STATUS          LABEL
====            ======          =====
internal        running         CONFIDENTIAL : INTERNAL
public          running         PUBLIC
```

▼ 마운트된 파일의 레이블을 표시하는 방법

이 절차에서는 현재 영역의 마운트된 파일 시스템을 표시하는 셸 스크립트를 만듭니다. 이 스크립트를 전역 영역에서 실행하면 모든 영역의 마운트된 모든 파일 시스템의 레이블이 표시됩니다.

시작하기 전에 전역 영역에서 시스템 관리자 역할을 가진 사용자여야 합니다.

1 신뢰할 수 있는 편집기를 사용하여 `getmounts` 스크립트를 만듭니다.

자세한 내용은 54 페이지 “Trusted Extensions에서 관리 파일을 편집하는 방법”을 참조하십시오.

스크립트에 경로 이름(예: /usr/local/scripts/getmounts)을 제공합니다.

2 다음 내용을 추가하고 파일을 저장합니다.

```
#!/bin/sh
#
for i in `/usr/sbin/mount -p | cut -d " " -f3` ; do
        /usr/bin/getlabel $i
done
```

3 전역 영역에서 스크립트를 테스트합니다.

```
# /usr/local/scripts/getmounts
/:      ADMIN_LOW
/dev:   ADMIN_LOW
/kernel:        ADMIN_LOW
/lib:   ADMIN_LOW
/opt:   ADMIN_LOW
/platform:      ADMIN_LOW
/sbin:  ADMIN_LOW
/usr:   ADMIN_LOW
/var/tsol/doors:        ADMIN_LOW
/zone/needtoknow/export/home:   CONFIDENTIAL : NEED TO KNOW
/zone/internal/export/home:     CONFIDENTIAL : INTERNAL USE ONLY
/zone/restricted/export/home:   CONFIDENTIAL : RESTRICTED
/proc:  ADMIN_LOW
/system/contract:       ADMIN_LOW
/etc/svc/volatile:      ADMIN_LOW
/etc/mnttab:    ADMIN_LOW
/dev/fd:        ADMIN_LOW
/tmp:           ADMIN_LOW
/var/run:       ADMIN_LOW
/zone/public/export/home:  PUBLIC
/root:          ADMIN_LOW
```

예 10–2 restricted 영역의 파일 시스템 레이블 표시

일반 사용자가 레이블이 있는 영역에서 getmounts 스크립트를 실행하면 해당 영역에 마운트된 모든 파일 시스템의 레이블이 표시됩니다. 시스템에서 기본 label_encodings 파일의 모든 레이블에 대해 영역을 만든 경우 restricted 영역에서 다음 내용이 출력됩니다.

```
# /usr/local/scripts/getmounts
/:      CONFIDENTIAL : RESTRICTED
/dev:   CONFIDENTIAL : RESTRICTED
/kernel:        ADMIN_LOW
/lib:   ADMIN_LOW
/opt:   ADMIN_LOW
/platform:      ADMIN_LOW
/sbin:  ADMIN_LOW
/usr:   ADMIN_LOW
/var/tsol/doors:        ADMIN_LOW
/zone/needtoknow/export/home:   CONFIDENTIAL : NEED TO KNOW
/zone/internal/export/home:     CONFIDENTIAL : INTERNAL USE ONLY
/proc:  CONFIDENTIAL : RESTRICTED
/system/contract:       CONFIDENTIAL : RESTRICTED
```

```
/etc/svc/volatile:      CONFIDENTIAL : RESTRICTED
/etc/mnttab:    CONFIDENTIAL : RESTRICTED
/dev/fd:        CONFIDENTIAL : RESTRICTED
/tmp:   CONFIDENTIAL : RESTRICTED
/var/run:       CONFIDENTIAL : RESTRICTED
/zone/public/export/home:       PUBLIC
/home/gfaden:   CONFIDENTIAL : RESTRICTED
```

▼ 레이블이 있는 영역에 일반적으로 표시되지 않는 파일을 루프백 마운트하는 방법

이 절차에서는 지정된 레이블이 있는 영역의 사용자가 전역 영역에서 기본적으로 내보내지 않는 파일을 볼 수 있도록 설정합니다.

시작하기 전에 전역 영역에서 시스템 관리자 역할을 가진 사용자여야 합니다.

1 구성을 변경할 영역을 중지합니다.

```
# zoneadm -z zone-name halt
```

2 파일이나 디렉토리를 루프백 마운트합니다.

예를 들어, 일반 사용자가 `/etc` 디렉토리에서 파일을 볼 수 있도록 허용합니다.

```
# zonecfg -z zone-name
 add filesystem
 set special=/etc/filename
 set directory=/etc/filename
 set type=lofs
 add options [ro,nodevices,nosetuid]
 end
 exit
```

주 – 시스템에서 사용되지 않는 파일은 루프백 마운트해도 효과가 없습니다. 예를 들어, 레이블이 있는 영역의 `/etc/dfs/dfstab` 파일은 Trusted Extensions 소프트웨어에서 확인되지 않습니다. 자세한 내용은 137 페이지 “레이블이 있는 영역에서 파일 공유”를 참조하십시오.

---

3 영역을 시작합니다.

```
# zoneadm -z zone-name boot
```

예 10–3 `/etc/passwd` 파일 루프백 마운트

이 예에서 보안 관리자는 테스터와 프로그래머가 로컬 암호가 설정되었는지 확인할 수 있도록 합니다. `sandbox` 영역이 중지된 후 `passwd` 파일을 루프백 마운트하도록 구성됩니다. 그런 다음 영역이 다시 시작됩니다.

```
# zoneadm -z sandbox halt
# zonecfg -z sandbox
 add filesystem
    set special=/etc/passwd
    set directory=/etc/passwd
    set type=lofs
    add options [ro,nodevices,nosetuid]
 end
 exit
# zoneadm -z sandbox boot
```

▼ 하위 레벨 파일의 마운트를 사용 안함으로 설정하는 방법

기본적으로 사용자는 하위 레벨 파일을 볼 수 있습니다. 특정 영역에서 모든 하위 레벨 파일을 보지 못하도록 net_mac_aware 권한을 제거합니다. net_mac_aware 권한에 대한 자세한 내용은 privileges(5) 매뉴얼 페이지를 참조하십시오.

시작하기 전에 전역 영역에서 시스템 관리자 역할을 가진 사용자여야 합니다.

1 구성을 변경할 영역을 중지합니다.

```
# zoneadm -z zone-name halt
```

2 하위 레벨 파일을 보지 못하도록 영역을 구성합니다.

영역에서 net_mac_aware 권한을 제거합니다.

```
# zonecfg -z zone-name
 set limitpriv=default,!net_mac_aware
 exit
```

3 영역을 다시 시작합니다.

```
# zoneadm -z zone-name boot
```

예 10–4 사용자가 하위 레벨 파일을 보지 못하도록 금지

이 예에서 보안 관리자는 특정 시스템의 사용자가 혼돈을 일으키지 않게 하려고 합니다. 그 결과, 사용자는 자신이 작업 중인 레이블의 파일만 볼 수 있습니다. 따라서 보안 관리자는 모든 하위 레벨 파일 보기를 금지합니다. 이 시스템에서 사용자는 PUBLIC 레이블에서 작업 중인 경우가 아니면 공개적으로 사용 가능한 파일을 볼 수 없습니다. 또한 영역 레이블의 파일만 NFS 마운트할 수 있습니다.

```
# zoneadm -z restricted halt
# zonecfg -z restricted
 set limitpriv=default,!net_mac_aware
 exit
# zoneadm -z restricted boot
```

```
# zoneadm -z needtoknow halt
# zonecfg -z needtoknow
 set limitpriv=default,!net_mac_aware
 exit
# zoneadm -z needtoknow boot

# zoneadm -z internal halt
# zonecfg -z internal
 set limitpriv=default,!net_mac_aware
 exit
# zoneadm -z internal boot
```

PUBLIC은 최하위 레이블이므로 보안 관리자는 PUBLIC 영역에 대해 명령을 실행하지 않습니다.

▼ 레이블이 있는 영역에서 ZFS 데이터 세트를 공유하는 방법

이 절차에서는 레이블이 있는 영역에서 읽기/쓰기 권한으로 ZFS 데이터 세트를 마운트합니다. 모든 명령은 전역 영역에서 실행되므로 전역 영역 관리자는 레이블이 있는 영역에 대한 ZFS 데이터 세트 추가를 제어합니다.

데이터 세트를 공유하려면 최소한 레이블이 있는 영역이 ready 상태에 있어야 합니다. 영역이 running 상태일 수 있습니다.

시작하기 전에 데이터 세트로 영역을 구성하려면 영역을 중지합니다.

1 ZFS 데이터 세트를 만듭니다.

```
# zfs create datasetdir/subdir
```

데이터 세트의 이름에 디렉토리(예: zone/data)가 포함될 수 있습니다.

2 전역 영역에서 레이블이 있는 영역을 중지합니다.

```
# zoneadm -z labeled-zone-name halt
```

3 데이터 세트의 마운트 지점을 설정합니다.

```
# zfs set mountpoint=legacy datasetdir/subdir
```

ZFS mountpoint 등록 정보를 설정하면 마운트 지점이 레이블이 있는 영역과 일치하는 경우 마운트 지점의 레이블이 설정됩니다.

4 데이터 세트를 영역에 파일 시스템으로 추가합니다.

```
# zonecfg -z labeled-zone-name
# zonecfg:labeled-zone-name> add fs
# zonecfg:labeled-zone-name:dataset> set dir=/subdir
# zonecfg:labeled-zone-name:dataset> set special=datasetdir/subdir
# zonecfg:labeled-zone-name:dataset> set type=zfs
```

```
# zonecfg:labeled-zone-name:dataset> end
# zonecfg:labeled-zone-name> exit
```

데이터 세트를 파일 시스템으로 추가하면 dfstab 파일이 해석되기 전에 데이터 세트가 영역의 /data에 마운트됩니다. 이 단계를 수행하면 영역이 부팅되기 전에 데이터 세트가 마운트되지 않습니다. 즉, 영역이 부트되고, 데이터 세트가 마운트된 다음 dfstab 파일이 해석됩니다.

5 데이터 세트를 공유합니다.

/zone/*labeled-zone-name*/etc/dfs/dfstab 파일에 데이터 세트 파일 시스템에 대한 항목을 추가합니다. 또한 이 항목은 */subdir* 경로 이름을 사용합니다.

```
share  -F nfs  -d "dataset-comment"  /subdir
```

6 레이블이 있는 영역을 부트합니다.

```
# zoneadm -z labeled-zone-name boot
```

영역이 부팅되면 데이터 세트가 *labeled-zone-name* 영역 레이블을 사용하여 *labeled-zone-name* 영역에서 읽기/쓰기 마운트 지점으로 자동으로 마운트됩니다.

예 10–5 레이블이 있는 영역에서 ZFS 데이터 세트 공유 및 마운트

이 예에서 관리자는 ZFS 데이터 세트를 needtoknow 영역에 추가하여 공유합니다. zone/data 데이터 세트는 /mnt 마운트 지점에 지정되어 있습니다. restricted 영역의 사용자는 이 데이터 세트를 볼 수 있습니다.

먼저 관리자가 영역을 중지합니다.

```
# zoneadm -z needtoknow halt
```

데이터 세트가 다른 마운트 지점에 지정되어 있으므로 관리자는 이전 지정을 제거한 다음 새 마운트 지점을 설정합니다.

```
# zfs set zoned=off zone/data
# zfs set mountpoint=legacy zone/data
```

그런 다음 zonecfg 대화형 인터페이스에서 관리자는 데이터 세트를 needtoknow 영역에 명시적으로 추가합니다.

```
# zonecfg -z needtoknow
# zonecfg:needtoknow> add fs
# zonecfg:needtoknow:dataset> set dir=/data
# zonecfg:needtoknow:dataset> set special=zone/data
# zonecfg:needtoknow:dataset> set type=zfs
# zonecfg:needtoknow:dataset> end
# zonecfg:needtoknow> exit
```

관리자는 데이터 세트를 공유하도록 /zone/needtoknow/etc/dfs/dfstab 파일을 수정한 다음 needtoknow 영역을 부트합니다.

```
## Global zone dfstab file for needtoknow zone
share  -F nfs  -d "App Data on ZFS"  /data

# zoneadm -z needtoknow boot
```

이제 데이터 세트를 액세스할 수 있습니다.

needtoknow 영역을 지배하는 restricted 영역의 사용자는 /data 디렉토리로 변경하여 마운트된 데이터 세트를 볼 수 있습니다. 또한 전역 영역의 관점에서 마운트된 데이터 세트의 전체 경로를 사용합니다. 이 예에서 machine1은 레이블이 있는 영역을 포함하는 시스템의 호스트 이름입니다. 관리자가 호스트 이름을 공유되지 않는 IP 주소에 지정했습니다.

```
# cd /net/machine1/zone/needtoknow/root/data
```

일반 오류 상위 레이블에서 데이터 세트에 연결할 때 not found(찾을 수 없음) 또는 No such file or directory(해당 파일 또는 디렉토리 없음) 오류가 표시되는 경우 관리자는 svcadm restart autofs 명령을 실행하여 자동 마운트 서비스를 다시 시작해야 합니다.

▼ 레이블이 있는 영역에서 파일의 레이블을 변경할 수 있게 설정하는 방법

이 절차를 수행해야 사용자가 파일의 레이블을 바꿀 수 있습니다.

시작하기 전에 전역 영역에서 보안 관리자 역할을 가진 사용자여야 합니다.

1 구성을 변경할 영역을 중지합니다.

```
# zoneadm -z zone-name halt
```

2 레이블을 바꿀 수 있게 영역을 구성합니다.

영역에 적절한 권한을 추가합니다. 창 권한을 사용하면 끌어서 놓기 및 잘라내기/붙여넣기 작업을 수행할 수 있습니다.

- **다운그레이드를 사용으로 설정하려면 영역에 file_downgrade_sl 권한을 추가합니다.**

```
# zonecfg -z zone-name
 set limitpriv=default,win_dac_read,win_mac_read,win_dac_write,
 win_mac_write,win_selection,file_downgrade_sl
 exit
```

- **업그레이드를 사용으로 설정하려면 영역에 sys_trans_label 및 file_upgrade_sl 권한을 추가합니다.**

```
# zonecfg -z zone-name
 set limitpriv=default,win_dac_read,win_mac_read,win_dac_write,
 win_mac_write,win_selection,sys_trans_label,file_upgrade_sl
 exit
```

- **업그레이드와 다운그레이드를 모두 사용으로 설정하려면 세 권한을 영역에 모두 추가합니다.**

```
# zonecfg -z zone-name
 set limitpriv=default,win_dac_read,win_mac_read,win_dac_write,
 win_mac_write,win_selection,sys_trans_label,file_downgrade_sl,
 file_upgrade_sl
 exit
```

3 영역을 다시 시작합니다.

```
# zoneadm -z zone-name boot
```

레이블 바꾸기를 허용하는 사용자 및 프로세스 요구 사항은 setflabel(3TSOL) 매뉴얼 페이지를 참조하십시오. 파일 레이블을 바꿀 수 있게 사용자를 권한 부여하려면 96 페이지 “사용자가 데이터의 보안 레벨을 변경할 수 있게 하는 방법”을 참조하십시오.

예 10–6 internal 영역에서 업그레이드 사용

이 예에서 보안 관리자는 시스템의 권한이 부여된 사용자가 파일을 업그레이드할 수 있게 하려고 합니다. 사용자가 정보를 업그레이드할 수 있게 함으로써 관리자는 높은 보안 레벨로 정보를 보호할 수 있습니다. 전역 영역에서 관리자는 다음 영역 관리 명령을 실행합니다.

```
# zoneadm -z internal halt
# zonecfg -z internal
 set limitpriv=default,sys_trans_label,file_upgrade_sl
 exit
# zoneadm -z internal boot
```

권한이 부여된 사용자는 이제 internal 정보를 internal 영역에서 restricted 영역으로 업그레이드할 수 있습니다.

예 10–7 restricted 영역에서 다운그레이드 사용

이 예에서 보안 관리자는 시스템의 권한이 부여된 사용자가 파일을 다운그레이드할 수 있게 하려고 합니다. 관리자가 영역에 창 권한을 추가하지 않았기 때문에 권한이 부여된 사용자는 File Manager(파일 관리자)를 사용하여 파일의 레이블을 바꿀 수 없습니다. 사용자가 파일의 레이블을 바꾸려면 setlabel 명령을 사용합니다.

사용자가 정보를 다운그레이드할 수 있게 설정하여 관리자는 사용자에게 낮은 보안 레벨로 파일에 액세스할 수 있게 허용합니다. 전역 영역에서 관리자는 다음 영역 관리 명령을 실행합니다.

```
# zoneadm -z restricted halt
# zonecfg -z restricted
 set limitpriv=default,file_downgrade_sl
 exit
# zoneadm -z restricted boot
```

권한이 부여된 사용자는 이제 setlabel 명령을 사용하여 restricted 정보를 restricted 영역에서 internal 또는 public 영역으로 다운그레이드할 수 있습니다.

▼ udp를 통해 NFSv3에 대한 다중 레벨 포트를 구성하는 방법

이 절차는 udp를 통해 NFSv3 하위 읽기(read-down) 마운트를 사용으로 설정하는 데 사용됩니다. Solaris Management Console은 MLP를 추가하는 데 사용됩니다.

시작하기 전에 전역 영역에서 보안 관리자 역할을 가진 사용자여야 합니다.

1. **Solaris Management Console을 시작합니다.**
   자세한 내용은 52 페이지 “Solaris Management Console에서 로컬 시스템을 관리하는 방법”을 참조하십시오.
2. **Files(파일) 도구 상자를 선택합니다.**
   도구 상자 제목에 `Scope=Files, Policy=TSOL`이 포함됩니다.
3. **영역과 MLP를 구성합니다.**
   a. **Trusted Network Zones(신뢰할 수 있는 네트워크 영역) 도구로 이동합니다.**
   b. **전역 영역을 두 번 누릅니다.**
   c. **UDP 프로토콜에 대해 다중 레벨 포트를 추가합니다.**
      i. **Add for the Multilevel Ports for Zone's IP Addresses(영역 IP 주소에 대해 다중 레벨 포트 추가)를 누릅니다.**
      ii. **포트 번호로 2049를 입력하고 OK(확인)를 누릅니다.**
   d. **OK(확인)를 눌러 설정을 저장합니다.**
4. **Solaris Management Console을 닫습니다.**
5. **커널을 업데이트합니다.**

```
# tnctl -fz /etc/security/tsol/tnzonecfg
```

▼ 영역에 대한 다중 레벨 포트를 만드는 방법

레이블이 있는 영역에서 실행되는 응용 프로그램에 영역과의 통신을 위한 MLP(다중 레벨 포트)가 필요한 경우 이 절차를 사용합니다. 이 절차에서 웹 프록시는 영역과 통신합니다. Solaris Management Console은 MLP를 추가하는 데 사용됩니다.

시작하기 전에 전역 영역에서 보안 관리자 역할을 가진 사용자여야 합니다. 레이블이 있는 영역이 존재해야 합니다. 자세한 내용은 **Trusted Extensions Configuration Guide**의 "Creating Labeled Zones"를 참조하십시오.

1 **Solaris Management Console을 시작합니다.**

자세한 내용은 52 페이지 "Solaris Management Console에서 로컬 시스템을 관리하는 방법"을 참조하십시오.

2 **Files(파일) 도구 상자를 선택합니다.**

도구 상자 제목에 `Scope=Files, Policy=TSOL`이 포함됩니다.

3 **프록시 호스트와 웹 서비스 호스트를 컴퓨터 목록에 추가합니다.**

a. **System Configuration(시스템 구성)에서 Computers and Networks(컴퓨터 및 네트워크) 도구로 이동합니다.**

b. **Computers(컴퓨터) 도구에서 Action(작업) 메뉴를 누르고 Add Computer(컴퓨터 추가)를 선택합니다.**

c. **프록시 호스트에 대한 호스트 이름과 IP 주소를 추가합니다.**

d. **변경 사항을 저장합니다.**

e. **웹 서비스 호스트에 대한 호스트 이름과 IP 주소를 추가합니다.**

f. **변경 사항을 저장합니다.**

4 **영역과 MLP를 구성합니다.**

a. **Trusted Network Zones(신뢰할 수 있는 네트워크 영역) 도구로 이동합니다.**

b. **레이블이 있는 영역을 선택합니다.**

c. **MLP Configuration for Local IP Addresses(로컬 IP 주소에 대한 MLP 구성) 구역에서 적절한 포트/프로토콜 필드를 지정합니다.**

d. **변경 사항을 저장합니다.**

5 **영역에 대해 다음 단계를 수행하여 템플리트를 사용자 정의합니다.**

a. **Security Templates(보안 템플리트) 도구로 이동합니다.**

Action(작업) 메뉴를 누르고 Add Template(템플리트 추가)를 선택합니다.

b. 템플리트 이름에 대해 호스트 이름을 사용합니다.

c. Host Type(호스트 유형)으로 CIPSO를 지정합니다.

d. Minimum Label(최소 레이블) 및 Maximum Label(최대 레이블)로 영역의 레이블을 사용합니다.

e. 보안 레이블 세트에 영역 레이블을 지정합니다.

f. Hosts Explicitly Assigned(명시적으로 지정된 호스트) 탭을 선택합니다.

g. Add an Entry(항목 추가) 구역에서 영역에 연결된 IP 주소를 추가합니다.

h. 변경 사항을 저장합니다.

6 Solaris Management Console을 닫습니다.

7 영역을 시작합니다.

```
# zoneadm -z zone-name boot
```

8 전역 영역에서 새 주소에 대한 경로를 추가합니다.

예를 들어, 영역에 공유 IP 주소가 있는 경우 다음을 수행합니다.

```
# route add proxy labeled-zones-IP-address
# route add webservice labeled-zones-IP-address
```

◆ ◆ ◆ 11장

11 Trusted Extensions에서 파일 관리 및 마운트(작업)

이 장에서는 Trusted Extensions로 구성된 시스템에서 LOFS 및 NFS 마운트가 어떻게 작동하는지 설명합니다. 이 장에서는 파일을 백업하고 복원하는 방법도 다룹니다.

- 135 페이지 “Trusted Extensions에서 파일 공유 및 마운트”
- 135 페이지 “Trusted Extensions에서 NFS 마운트”
- 137 페이지 “레이블이 있는 영역에서 파일 공유”
- 137 페이지 “Trusted Extensions에서 NFS 마운트된 디렉토리에 액세스”
- 140 페이지 “Trusted Extensions 소프트웨어 및 NFS 프로토콜 버전”
- 141 페이지 “레이블이 있는 파일 백업, 공유 및 마운트(작업 맵)”

Trusted Extensions에서 파일 공유 및 마운트

Trusted Extensions 소프트웨어는 Oracle Solaris OS와 동일한 파일 시스템 및 파일 시스템 관리 명령을 지원합니다. Trusted Extensions는 비전역 영역에서 파일을 공유하는 기능을 추가합니다. 또한 Trusted Extensions는 모든 비전역 영역에 고유한 레이블을 붙입니다. 해당 영역에 속하는 모든 파일과 디렉토리는 영역의 레이블에 마운트됩니다. 기타 영역 또는 NFS 서버에 속하는 공유 파일 시스템은 소유자의 레이블에 마운트됩니다. Trusted Extensions는 레이블 지정에 대한 MAC(필수 액세스 제어) 정책을 위반하는 모든 마운트를 금지합니다. 예를 들어, 영역의 레이블은 마운트된 파일 시스템 레이블을 모두 지배해야 하고, 동일한 레이블의 파일 시스템만 읽기/쓰기 권한으로 마운트될 수 있습니다.

Trusted Extensions에서 NFS 마운트

Trusted Extensions에서 NFS 마운트는 Oracle Solaris 마운트와 유사합니다. 차이는 Trusted Extensions에서 레이블이 있는 영역을 마운트할 때 영역 루트 경로 이름 사용과 MAC 정책 적용에서 나타납니다.

Trusted Extensions에서 NFS 공유는 전역 영역에서 Oracle Solaris 공유와 유사합니다. 그러나 다중 레벨 시스템의 레이블이 있는 영역에서 파일 공유는 Trusted Extensions에 고유합니다.

- **전역 영역에서 공유 및 마운트** – Trusted Extensions 시스템의 전역 영역에서 파일 공유 및 마운트는 Oracle Solaris OS의 절차와 거의 동일합니다. 파일 마운트의 경우 자동 마운트, `vfstab` 파일 및 `mount` 명령을 사용할 수 있습니다. 파일 공유의 경우 `dfstab` 파일이 사용됩니다.
- **레이블이 있는 영역에서 마운트** – Trusted Extensions의 레이블이 있는 영역에서 파일 마운트는 Oracle Solaris OS의 비전역 영역에서 파일 마운트와 거의 동일합니다. 파일 마운트의 경우 자동 마운트, `vfstab` 파일 및 `mount` 명령을 사용할 수 있습니다. Trusted Extensions에는 각 레이블이 있는 영역마다 고유한 `automount_home_`*label* 구성 파일이 있습니다.
- **레이블이 있는 영역에서 공유** – 레이블이 있는 영역의 파일은 영역의 레이블에 있지만 전역 영역에만 표시되는 `dfstab` 파일을 사용하여 영역의 레이블에서 공유할 수 있습니다. 따라서 파일 공유를 위한 레이블이 있는 영역의 구성은 전역 영역에서 전역 영역 관리자가 수행합니다. 이 구성 파일은 레이블이 있는 영역에서 볼 수 없습니다. 자세한 내용은 120 페이지 “전역 영역 프로세스 및 레이블이 있는 영역”을 참조하십시오.

레이블에 따라 마운트할 수 있는 파일이 달라집니다. 파일은 특정 레이블에서 공유되고 마운트됩니다. Trusted Extensions 클라이언트에서 NFS 마운트된 파일에 쓰려면 파일이 읽기/쓰기 권한으로 마운트**되고** 클라이언트와 동일한 레이블에 있어야 합니다. 두 Trusted Extensions 호스트 사이에 파일을 마운트하는 경우 서버와 클라이언트는 `cipso` 유형의 호환되는 원격 호스트 템플리트를 가지고 있어야 합니다. Trusted Extensions 호스트와 레이블이 없는 호스트 사이에 파일을 마운트하는 경우 `tnrhdb` 파일에서 레이블이 없는 호스트에 지정된 단일 레이블의 파일을 마운트할 수 있습니다. LOFS로 마운트된 파일은 볼 수 있지만 수정할 수는 없습니다. NFS 마운트에 대한 자세한 내용은 137 페이지 “Trusted Extensions에서 NFS 마운트된 디렉토리에 액세스”를 참조하십시오.

또한 레이블에 따라 볼 수 있는 디렉토리와 파일이 달라집니다. 기본적으로 하위 레벨 객체는 사용자의 환경에서 사용할 수 있습니다. 따라서 기본 구성에서 일반 사용자는 사용자의 현재 레벨보다 하위 레벨의 영역에 있는 파일을 볼 수 있습니다. 예를 들어, 사용자는 상위 레이블의 하위 레벨 홈 디렉토리를 볼 수 있습니다. 자세한 내용은 138 페이지 “Trusted Extensions에서 홈 디렉토리 만들기”를 참조하십시오.

사이트 보안에서 하위 레벨 객체 보기를 금지하는 경우 사용자가 하위 레벨 디렉토리를 볼 수 없게 할 수 있습니다. 자세한 내용은 127 페이지 “하위 레벨 파일의 마운트를 사용 안함으로 설정하는 방법”을 참조하십시오.

Trusted Extensions의 마운트 정책에는 MAC 대체가 없습니다. 하위 레이블에서 표시되는 마운트된 파일은 상위 레이블 프로세스에서 수정할 수 없습니다. 이 MAC 정책은 전역 영역에도 적용됩니다. 전역 영역 `ADMIN_HIGH` 프로세스는 `PUBLIC` 파일 또는 `ADMIN_LOW` 파일과 같은 하위 레이블의 NFS 마운트된 파일을 수정할 수 없습니다. MAC 정책은 기본 구성을 적용하며 일반 사용자에게 표시되지 않습니다. 일반 사용자는 MAC 액세스 권한이 없으면 객체를 볼 수 없습니다.

레이블이 있는 영역에서 파일 공유

Oracle Solaris OS에서 비전역 영역은 해당 영역에서 디렉토리를 공유할 수 없습니다. 그러나 Trusted Extensions에서는 레이블이 있는 영역에서 디렉토리를 공유할 수 있습니다. 레이블이 있는 영역에서 공유 가능한 디렉토리의 지정은 영역의 `root` 경로 외부에 있는 디렉토리를 사용하여 전역 영역에서 수행됩니다. 자세한 내용은 120 페이지 "전역 영역 프로세스 및 레이블이 있는 영역"을 참조하십시오.

`/zone/`*labeled-zone*`/`*directories*	영역 경로라고도 합니다. 전역 영역에서 레이블이 있는 영역으로의 경로입니다. *labeled-zone* 아래의 모든 디렉토리에는 영역과 동일한 레이블이 지정됩니다.
`/zone/`*labeled-zone*`/root/`*directories*	영역 루트 경로라고도 합니다. 전역 영역의 관점에서 레이블이 있는 영역의 `root` 경로입니다. 레이블이 있는 영역의 관점에서는 영역의 루트인 `/` 디렉토리입니다. 이 경로는 전역 영역에서 영역을 관리하는 데 사용되지 않습니다.

레이블이 있는 영역에서 디렉토리를 공유하려면 전역 영역 관리자가 영역 경로의 `/etc` 디렉토리에서 `dfstab` 파일을 만들고 수정합니다.

`/zone/`*labeled-zone*`/etc/dfs/dfstab`

`/etc` 디렉토리는 레이블이 있는 영역에서 볼 수 없습니다. 이 디렉토리는 영역에서 볼 수 있는 `/etc` 디렉토리와 다릅니다.

```
Global zone view: /zone/labeled-zone/root/etc
Labeled zone view of the same directory: /etc
```

이 경로의 `dfstab` 파일을 통해 레이블이 있는 디렉토리를 공유할 수 없습니다.

레이블이 있는 영역의 상태가 `ready` 또는 `running`인 경우 `/zone/`*labeled-zone*`/etc/dfs/dfstab` 파일에 나열된 파일은 영역의 레이블에서 공유됩니다. 절차는 142 페이지 "레이블이 있는 영역에서 디렉토리를 공유하는 방법"을 참조하십시오.

Trusted Extensions에서 NFS 마운트된 디렉토리에 액세스

기본적으로 NFS 마운트된 파일 시스템은 내보낸 파일 시스템의 레이블에서 표시됩니다. 파일 시스템을 읽기/쓰기 권한으로 내보낸 경우 해당 레이블의 사용자는 파일에 쓸 수 있습니다. 사용자의 현재 세션보다 낮은 레이블에 있는 NFS 마운트는 사용자에게 표시되지만 쓸 수는 없습니다. 파일 시스템이 읽기/쓰기 권한으로 공유되더라도 마운트 시스템은 마운트의 레이블에 있는 파일 시스템에만 쓸 수 있습니다.

NFS 마운트된 하위 레벨 디렉토리가 상위 레벨 영역의 사용자에게 표시되도록 하려면 NFS 서버에서 전역 영역의 관리자가 상위 디렉토리를 내보내야 합니다. 상위 디렉토리는 해당 레이블에서 내보내집니다. 클라이언트 측에서 각 영역에 `net_mac_aware` 권한이 있어야 합니다. 기본적으로 레이블이 있는 영역에는 `limitpriv` 세트의 `net_mac_aware` 권한이 포함됩니다.

- **서버 구성** – NFS 서버에서 `dfstab` 파일로 상위 디렉토리를 내보냅니다. 상위 디렉토리가 레이블이 있는 영역에 있는 경우 상위 디렉토리의 레이블이 있는 영역에서 `dfstab` 파일을 수정해야 합니다. 레이블이 있는 영역에 대한 `dfstab` 파일은 전역 영역에서만 볼 수 있습니다. 절차는 142 페이지 “레이블이 있는 영역에서 디렉토리를 공유하는 방법”을 참조하십시오.
- **클라이언트 구성** – `net_mac_aware` 권한이 초기 영역 구성 중 사용된 영역 구성 파일에 지정되어야 합니다. 따라서 모든 하위 레벨 홈 디렉토리를 볼 수 있는 사용자에게는 최하위 영역을 제외한 모든 영역에서 `net_mac_aware` 권한이 있어야 합니다. 예는 144 페이지 “레이블이 있는 영역에서 파일을 NFS 마운트하는 방법”을 참조하십시오.

예 11–1 하위 레벨 홈 디렉토리에 대한 액세스 제공

홈 디렉토리 서버에서 관리자는 모든 레이블이 있는 영역에서 `/zone/`*`labeled-zone`*`/etc/dfs/dfstab` 파일을 만들고 수정합니다. `dfstab` 파일은 `/export/home` 디렉토리를 읽기/쓰기 권한으로 내보냅니다. 따라서 디렉토리가 동일한 레이블에 마운트되면 홈 디렉토리에 쓸 수 있습니다. `PUBLIC`의 `/export/home` 디렉토리를 내보내기 위해 관리자는 홈 디렉토리 서버에서 `PUBLIC` 레이블에서 작업 공간을 만들고, 전역 영역에서 `/zone/public/etc/dfs/dfstab` 파일을 수정합니다.

클라이언트에서 전역 영역의 관리자는 최하위 레이블을 제외한 모든 레이블이 있는 영역에 `net_mac_aware` 권한이 있는지 확인합니다. 이 권한이 마운트를 허용합니다. 이 권한은 영역 구성 중 `zonecfg` 명령을 사용하여 지정할 수 있습니다. 하위 레벨 홈 디렉토리만 볼 수 있습니다. MAC는 디렉토리의 파일이 수정되는 것을 방지합니다.

Trusted Extensions에서 홈 디렉토리 만들기

홈 디렉토리는 Trusted Extensions에서 특수한 경우입니다. 사용자가 사용할 수 있는 모든 영역에서 홈 디렉토리가 만들어졌는지 확인해야 합니다. 또한 홈 디렉토리 마운트 지점이 사용자 시스템의 영역에서 만들어져야 합니다. NFS 마운트된 홈 디렉토리가 제대로 작동하려면 디렉토리에 대한 기본 위치인 `/export/home`이 사용되어야 합니다. Trusted Extensions에서는 모든 영역 즉, 모든 레이블의 홈 디렉토리를 처리할 수 있도록 자동 마운트가 수정되었습니다. 자세한 내용은 139 페이지 “Trusted Extensions의 자동 마운트 변경 사항”을 참조하십시오.

사용자가 만들어질 때 홈 디렉토리가 만들어집니다. Trusted Extensions에서는 사용자를 만드는 데 Solaris Management Console(콘솔)이 사용되므로 콘솔에서 홈 디렉토리를

만듭니다. 그러나 콘솔은 홈 디렉토리 서버의 전역 영역에 홈 디렉토리를 만듭니다. 해당 서버에서 디렉토리는 LOFS로 마운트됩니다. 홈 디렉토리는 LOFS 마운트로 지정된 경우 자동 마운트에서 자동으로 만들어집니다.

주 – 콘솔을 사용하여 사용자를 삭제할 경우 전역 영역에 있는 사용자의 홈 디렉토리만 삭제됩니다. 레이블이 있는 영역에 있는 사용자의 홈 디렉토리는 삭제되지 않습니다. 레이블이 있는 영역의 홈 디렉토리 아카이브 및 삭제는 사용자가 결정해야 합니다. 절차는 96 페이지 “Trusted Extensions 시스템에서 사용자 계정을 삭제하는 방법”을 참조하십시오.

그러나 자동 마운트는 원격 NFS 서버에 홈 디렉토리를 자동으로 만들 수 없습니다. 사용자가 먼저 NFS 서버에 로그인해야 하거나 관리자 작업이 필요합니다. 사용자를 위한 홈 디렉토리를 만들려면 **Trusted Extensions Configuration Guide**의 “Enable Users to Access Their Home Directories in Trusted Extensions”을 참조하십시오.

Trusted Extensions의 자동 마운트 변경 사항

Trusted Extensions에서는 레이블마다 별도의 홈 디렉토리 마운트를 필요로 합니다. 이러한 레이블이 있는 자동 마운트를 처리하도록 `automount` 명령이 수정되었습니다. 각 영역에 대해 자동 마운트인 `autofs`는 `auto_home_` *zone-name* 파일을 마운트합니다. 예를 들어, 다음은 `auto_home_global` 파일에서 전역 영역에 대한 항목입니다.

```
+auto_home_global
*       -fstype=lofs    :/export/home/&
```

하위 레벨 영역의 마운트를 허용하는 영역이 부팅될 때 다음이 수행됩니다. 하위 레벨 영역의 홈 디렉토리가 `/zone/<`*zone-name*`>/export/home`에서 읽기 전용으로 마운트됩니다. `auto_home_<`*zone-name*`>` 맵은 `lofs`에 대한 소스 디렉토리가 `/zone/<`*zone-name*`>/home/<`*username*`>`으로 다시 마운트될 때 `/zone` 경로를 지정합니다.

예를 들어, 다음은 상위 레벨 영역에서 생성되는 `auto_home_`*zone-at-higher-label* 맵의 `auto_home_public` 항목입니다.

```
+auto_home_public
*       -fstype=lofs    :/zone/public/export/home/&
```

다음은 공용 영역의 해당하는 항목입니다.

```
auto_home_public
*       -fstype=lofs    :/export/home/&
```

홈 디렉토리가 참조되고 이름이 auto_home_<*zone-name*> 맵의 항목과 일치하지 않을 경우 맵은 이 루프백 마운트 사양과 일치하는 항목을 찾으려고 합니다. 다음 두 조건이 충족될 때 소프트웨어에서 홈 디렉토리를 만듭니다.

1. 맵이 루프백 마운트 사양과 일치하는 항목을 찾습니다.
2. 아직 *zone-name*에 존재하지 않는 유효한 사용자와 홈 디렉토리 이름이 일치합니다.

자동 마운트의 변경 사항에 대한 자세한 내용은 automount(1M) 매뉴얼 페이지를 참조하십시오.

Trusted Extensions 소프트웨어 및 NFS 프로토콜 버전

Solaris 10 11/06 및 Solaris 10 8/07 릴리스에서 Trusted Extensions는 NFS 버전 4(NFSv4)의 다중 레벨 레이블만 인식합니다. Solaris 10 5/08 릴리스부터 Trusted Extensions 소프트웨어는 NFS 버전 3(NFSv3)과 NFSv4의 레이블을 인식합니다. 다음 마운트 옵션 세트 중 하나를 사용할 수 있습니다.

```
vers=4 proto=tcp
vers=3 proto=tcp
vers=3 proto=udp
```

Trusted Extensions에는 tcp 프로토콜을 통한 마운트 제한 사항이 없습니다. NFSv3 및 NFSv4에서는 동일 레이블(same-label) 마운트와 하위 읽기(read-down) 마운트에 tcp 프로토콜을 사용할 수 있습니다. 하위 읽기 마운트에는 다중 레벨 포트(MLP)가 필요합니다.

NFSv3의 경우 Trusted Extensions는 Oracle Solaris OS와 같이 동작합니다. udp 프로토콜은 NFSv3의 기본값이지만, udp는 초기 마운트 작업에만 사용됩니다. 이후 NFS 작업에는 시스템에서 tcp를 사용합니다. 따라서 하위 읽기 마운트는 기본 구성의 NFSv3에 대해 작동합니다.

드물지만 초기 및 이후 NFS 작업에 udp 프로토콜을 사용하도록 NFSv3 마운트를 제한한 경우 udp 프로토콜을 사용하는 NFS 작업에 대해 MLP를 만들어야 합니다. 절차는 132 페이지 “udp를 통해 NFSv3에 대한 다중 레벨 포트를 구성하는 방법”을 참조하십시오.

Trusted Extensions로 구성된 호스트는 자체 파일 시스템을 레이블이 없는 호스트와 공유할 수도 있습니다. 레이블이 없는 호스트로 내보낸 파일이나 디렉토리는 해당 레이블이 신뢰할 수 있는 네트워킹 데이터베이스 항목의 원격 호스트와 연결된 레이블과 같을 경우 **쓰기 가능**합니다. 레이블이 없는 호스트로 내보낸 파일이나 디렉토리는 해당 레이블이 원격 호스트와 연결된 레이블의 지배를 받는 경우에만 **읽기 가능**합니다.

Trusted Solaris 소프트웨어 릴리스를 실행 중인 시스템과의 통신은 단일 레이블에서만 가능합니다. Trusted Extensions 시스템 및 Trusted Solaris 시스템은 레이블이 없는 호스트 유형의 템플리트를 다른 시스템에 지정해야 합니다. 레이블이 없는 호스트 유형은

동일한 단일 레이블을 지정해야 합니다. Trusted Solaris 서버의 레이블이 없는 NFS 클라이언트로서 클라이언트의 레이블은 ADMIN_LOW일 수 없습니다.

사용되는 NFS 프로토콜은 로컬 파일 시스템의 유형에 독립적입니다. 오히려 프로토콜은 공유 컴퓨터의 운영 체제 유형에 따라 달라집니다. 원격 파일 시스템에 대해 mount 명령 또는 vfstab 파일에 지정되는 파일 시스템 유형은 항상 NFS입니다.

레이블이 있는 파일 백업, 공유 및 마운트(작업 맵)

다음 작업 맵에서는 레이블이 있는 파일 시스템에서 데이터를 백업 및 복원하고, 레이블이 있는 디렉토리와 파일을 공유 및 마운트하는 데 사용되는 일반적인 작업을 설명합니다.

작업	설명	수행 방법
파일을 백업합니다.	데이터를 백업하여 보호합니다.	142 페이지 “Trusted Extensions에서 파일을 백업하는 방법”
데이터를 복원합니다.	백업에서 데이터를 복원합니다.	142 페이지 “Trusted Extensions에서 파일을 복원하는 방법”
레이블이 있는 영역에서 디렉토리의 내용을 공유합니다.	레이블이 있는 디렉토리의 내용을 사용자 간에 공유할 수 있습니다.	142 페이지 “레이블이 있는 영역에서 디렉토리를 공유하는 방법”
레이블이 있는 영역에서 공유된 디렉토리의 내용을 마운트합니다.	디렉토리의 내용을 읽기/쓰기를 위한 동일한 레이블의 영역에 마운트할 수 있습니다. 상위 레벨 영역에서 공유 디렉토리를 마운트하는 경우 디렉토리는 읽기 전용으로 마운트됩니다.	144 페이지 “레이블이 있는 영역에서 파일을 NFS 마운트하는 방법”
홈 디렉토리 마운트 지점을 만듭니다.	모든 레이블의 모든 사용자를 위한 마운트 지점을 만듭니다. 이 작업을 통해 사용자는 NFS 홈 디렉토리 서버가 아닌 시스템에서 홈 디렉토리에 액세스할 수 있습니다.	**Trusted Extensions Configuration Guide**의 “Enable Users to Access Their Home Directories in Trusted Extensions”
상위 레이블에서 작업하는 사용자에게서 하위 레벨 정보를 숨깁니다.	상위 레벨 창에서 하위 레벨 정보를 볼 수 없도록 합니다.	127 페이지 “하위 레벨 파일의 마운트를 사용 안함으로 설정하는 방법”
파일 시스템 마운트 문제를 해결합니다.	파일 시스템 마운트 문제를 해결합니다.	149 페이지 “Trusted Extensions에서 마운트 실패 문제를 해결하는 방법”

▼ Trusted Extensions에서 파일을 백업하는 방법

1 **운영자 역할을 맡습니다.**

이 역할에는 Media Backup 권한 프로파일이 포함됩니다.

2 **다음 백업 방법 중 하나를 사용합니다.**

- 대규모 백업의 경우 `/usr/lib/fs/ufs/ufsdump`
- 소규모 백업의 경우 `/usr/sbin/tar cT`
- 이러한 명령을 호출하는 스크립트

  예를 들어, Budtool 백업 응용 프로그램은 `ufsdump` 명령을 호출합니다. `ufsdump(1M)` 매뉴얼 페이지를 참조하십시오. `tar` 명령의 `T` 옵션에 대한 자세한 내용은 `tar(1)` 매뉴얼 페이지를 참조하십시오.

▼ Trusted Extensions에서 파일을 복원하는 방법

1 **루트가 되어야 합니다.**

2 **다음 방법 중 하나를 사용합니다.**

- 대규모 복원의 경우 `/usr/lib/fs/ufs/ufsrestore`
- 소규모 복원의 경우 `/usr/sbin/tar xT`
- 이러한 명령을 호출하는 스크립트

`tar` 명령의 `T` 옵션에 대한 자세한 내용은 `tar(1)` 매뉴얼 페이지를 참조하십시오.

주의 – 이러한 명령만 레이블을 보존합니다.

▼ 레이블이 있는 영역에서 디렉토리를 공유하는 방법

Oracle Solaris OS에서와 마찬가지로 Solaris Management Console의 마운트 및 공유 도구를 사용하여 전역 영역에서 파일을 공유하고 마운트합니다. 이 도구는 레이블이 있는 영역의 디렉토리를 마운트하거나 공유하는 데 사용할 수 없습니다. 영역의 레이블에서 `dfstab` 파일을 만든 다음 영역을 다시 시작하여 레이블이 있는 디렉토리를 공유합니다.

주의 – 공유 파일 시스템에 대해 독점적 이름을 사용하지 마십시오. 공유 파일 시스템의 이름은 모든 사용자에게 표시됩니다.

시작하기 전에 사용자는 수퍼유저이거나 파일 서버의 전역 영역에서 시스템 관리자 역할을 가진 사용자여야 합니다.

1 공유할 디렉토리의 레이블에서 작업 공간을 만듭니다.

자세한 내용은 **Trusted Extensions User's Guide**의 "How to Add a Workspace at a Particular Label"을 참조하십시오.

2 해당 영역의 레이블에서 `dfstab` 파일을 만듭니다.

디렉토리를 공유할 각 영역에 대해 다음 단계를 반복합니다.

a. 영역에서 `/etc/dfs` 디렉토리를 만듭니다.

```
# mkdir -p /zone/zone-name/etc/dfs
```

b. 신뢰할 수 있는 편집기를 엽니다.

자세한 내용은 54 페이지 "Trusted Extensions에서 관리 파일을 편집하는 방법"을 참조하십시오.

c. `dfstab` 파일의 전체 경로 이름을 편집기에 입력합니다.

```
# /zone/zone-name/etc/dfs/dfstab
```

d. 해당 영역에서 디렉토리를 공유할 항목을 추가합니다.

항목은 영역 루트 경로의 관점에서 디렉토리를 설명합니다. 예를 들어, 다음 항목은 포함하는 영역의 레이블에서 응용 프로그램의 파일을 공유합니다.

```
share -F nfs -o ro /viewdir/viewfiles
```

3 각 영역에 대해 영역을 시작하여 디렉토리를 공유합니다.

전역 영역에서 각 영역에 대해 다음 명령 중 하나를 실행합니다. 각 영역은 이러한 방식으로 디렉토리를 공유할 수 있습니다. 실제 공유는 각 영역이 `ready` 또는 `running` 상태가 될 때 이루어집니다.

- **영역이 `running` 상태가 아니고 사용자가 영역의 레이블에서 서버에 로그인하지 못하게 하려는 경우 영역 상태를 `ready`로 설정합니다.**

  ```
  # zoneadm -z zone-name ready
  ```

- **영역이 `running` 상태가 아니고 사용자가 영역의 레이블에서 서버에 로그인할 수 있는 경우 영역을 부팅합니다.**

  ```
  # zoneadm -z zone-name boot
  ```

- **영역이 이미 실행 중인 경우 영역을 재부팅합니다.**

  ```
  # zoneadm -z zone-name reboot
  ```

4 시스템에서 공유된 디렉토리를 표시합니다.

```
# showmount -e
```

5 **클라이언트에서 내보낸 파일을 마운트할 수 있게 하려면 144 페이지 "레이블이 있는 영역에서 파일을 NFS 마운트하는 방법"을 참조하십시오.**

예 11–2 PUBLIC 레이블에서 /export/share 디렉토리 공유

PUBLIC 레이블에서 실행되는 응용 프로그램의 경우 시스템 관리자는 사용자가 public 영역의 /export/share 디렉토리에 있는 문서를 읽도록 할 수 있습니다. 이름이 public인 영역은 PUBLIC 레이블에서 실행됩니다.

우선 관리자가 public 작업 공간을 만들고 dfstab 파일을 편집합니다.

```
# mkdir -p /zone/public/etc/dfs
# /usr/dt/bin/trusted_edit /zone/public/etc/dfs/dfstab
```

관리자가 파일에 다음 항목을 추가합니다.

```
## Sharing PUBLIC user manuals
share -F nfs -o ro /export/appdocs
```

관리자는 public 작업 공간에서 나와 Trusted Path(신뢰할 수 있는 경로) 작업 공간으로 돌아갑니다. 사용자는 이 시스템에 로그인할 수 없으므로 관리자가 영역을 ready 상태로 설정하여 파일을 공유합니다.

```
# zoneadm -z public ready
```

디렉토리가 사용자의 시스템에 마운트되면 사용자는 공유 디렉토리에 액세스할 수 있습니다.

▼ 레이블이 있는 영역에서 파일을 NFS 마운트하는 방법

Trusted Extensions에서 레이블이 있는 영역은 해당 영역의 파일 마운트를 관리합니다.

레이블이 없는 호스트 및 레이블이 있는 호스트의 파일은 Trusted Extensions 레이블이 있는 호스트에 마운트할 수 있습니다.

- 단일 레이블 호스트에서 파일을 읽기/쓰기로 마운트하려면 원격 호스트의 지정된 레이블이 파일이 마운트되는 영역과 동일해야 합니다.
- 상위 레벨 영역에서 마운트된 파일은 읽기 전용입니다.
- Trusted Extensions에서 auto_home 구성 파일은 영역별로 사용자 정의됩니다. 파일은 영역 이름을 따라 지정됩니다. 예를 들어, 전역 영역과 공용 영역이 있는 시스템에는 두 개의 auto_home 파일인 auto_home_global과 auto_home_public이 있습니다.

Trusted Extensions에서는 Oracle Solaris OS와 동일한 마운트 인터페이스를 사용합니다.

- 부트 시 파일을 마운트하려면 레이블이 있는 영역의 `/etc/vfstab` 파일을 사용합니다.
- 동적으로 파일을 마운트하려면 레이블이 있는 영역의 `mount` 명령을 사용합니다.
- 홈 디렉토리를 자동 마운트하려면 `auto_home_`*zone-name* 파일을 사용합니다.
- 다른 디렉토리를 자동 마운트하려면 표준 자동 마운트 맵을 사용합니다. 자동 마운트 맵이 LDAP에 있을 경우 LDAP 명령을 사용하여 관리합니다.

시작하기 전에 마운트하려는 파일의 레이블 영역에서 클라이언트 시스템에 있어야 합니다. 자동 마운트를 사용하지 않는 경우 사용자는 수퍼유저이거나 시스템 관리자 역할을 가진 사용자여야 합니다. 하위 레벨 서버에서 마운트하려면 영역이 `net_mac_aware` 권한으로 구성되어야 합니다.

● **레이블이 있는 영역에서 파일을 NFS 마운트하려면 다음 절차를 따릅니다.**

대부분의 절차에는 특정 레이블에서 작업 공간 만들기가 포함됩니다. 작업 공간을 만들려면 **Trusted Extensions User's Guide**의 "How to Add a Workspace at a Particular Label"을 참조하십시오.

- **파일을 동적으로 마운트합니다.**

  레이블이 있는 영역에서 `mount` 명령을 사용합니다. 동적으로 파일을 마운트하는 예는 예 11–3을 참조하십시오.

- **영역이 부트될 때 파일을 마운트합니다**

  레이블이 있는 영역에서 마운트를 `vfstab` 파일에 추가합니다.

  레이블이 있는 영역이 부트될 때 파일을 마운트하는 예는 예 11–4와 예 11–5를 참조하십시오.

- **LDAP으로 관리되는 시스템에 대한 홈 디렉토리를 마운트합니다.**

  a. **모든 레이블에서 사용자 사양을 `auto_home_`*zone-name* 파일에 추가합니다.**

  b. **그런 다음 이 파일을 사용하여 LDAP 서버의 `auto_home_`*zone-name* 데이터베이스를 채웁니다.**

  예는 예 11–6을 참조하십시오.

- **파일로 관리되는 시스템에 대한 홈 디렉토리를 마운트합니다.**

  a. **`/export/home/auto_home_`*lowest-labeled-zone-name* 파일을 만들고 채웁니다.**

  b. **새로 채워진 파일을 가리키도록 `/etc/auto_home_`*lowest-labeled-zone-name* 파일을 편집합니다.**

c. 단계 a에서 만든 파일을 가리키도록 모든 상위 영역의 /etc/auto_home_*lowest-labeled-zone-name* 파일을 수정합니다.

예는 예 11–7을 참조하십시오.

예 11–3 mount 명령을 사용하여 레이블이 있는 영역에서 파일 마운트

이 예에서 시스템 관리자는 공용 영역에서 원격 파일 시스템을 마운트합니다. 공용 영역은 다중 레벨 서버에 있습니다.

시스템 관리자 역할을 맡은 후 관리자는 작업 공간을 PUBLIC 레이블에서 만듭니다. 해당 작업 공간에서 관리자는 mount 명령을 실행합니다.

```
# zonename
public
# mount -F nfs remote-sys:/zone/public/root/opt/docs  /opt/docs
```

PUBLIC 레이블의 단일 레이블 파일 서버에도 마운트할 문서가 포함되어 있습니다.

```
# mount -F nfs public-sys:/publicdocs  /opt/publicdocs
```

remote-sys 파일 서버의 공용 영역이 ready 또는 running 상태인 경우 remote-sys 파일이 이 시스템에서 성공적으로 마운트됩니다. public-sys 파일 서버가 실행 중인 경우 파일이 성공적으로 마운트됩니다.

예 11–4 vfstab 파일을 수정하여 레이블이 있는 영역에서 파일을 읽기/쓰기로 마운트

이 예에서 시스템 관리자는 공용 영역이 부트될 때 로컬 시스템의 공용 영역에 PUBLIC 레이블의 두 원격 파일 시스템을 마운트합니다. 한 파일 시스템은 다중 레벨 시스템에서 마운트되고, 다른 파일 시스템은 단일 레이블 시스템에서 마운트됩니다.

시스템 관리자 역할을 맡은 후 관리자는 작업 공간을 PUBLIC 레이블에서 만듭니다. 해당 작업 공간에서 관리자는 해당 영역의 vfstab 파일을 수정합니다.

```
## Writable books directories at PUBLIC
remote-sys:/zone/public/root/opt/docs  - /opt/docs  nfs  no  yes  rw
public-sys:/publicdocs    - /opt/publicdocs  nfs no yes rw
```

다중 레벨 시스템의 원격 레이블이 있는 영역의 파일에 액세스하기 위해 vfstab 항목은 원격 시스템 공용 영역의 영역 루트 경로인 /zone/public/root를 마운트할 디렉토리의 디렉토리 경로 이름으로 사용합니다. 단일 레이블 시스템의 경로는 Oracle Solaris 시스템에서 사용되는 경로와 동일합니다.

PUBLIC 레이블의 터미널 창에서 관리자가 파일을 마운트합니다.

```
# mountall
```

예 11–5 vfstab 파일을 수정하여 레이블이 있는 영역에서 하위 레벨 파일 마운트

이 예에서 시스템 관리자는 로컬 시스템 내부 영역의 공용 영역에서 원격 파일 시스템을 마운트합니다. 시스템 관리자 역할을 맡은 후 관리자는 작업 공간을 INTERNAL 레이블에서 만든 다음 해당 영역에서 vfstab 파일을 수정합니다.

```
## Readable books directory at PUBLIC
## ro entry indicates that PUBLIC docs can never be mounted rw in internal zone
remote-sys:/zone/public/root/opt/docs  - /opt/docs  nfs  no  yes  ro
```

원격 레이블이 있는 영역의 파일에 액세스하려면 vfstab 항목은 원격 시스템 공용 영역의 영역 루트 경로인 /zone/public/root를 마운트할 디렉토리의 디렉토리 경로 이름으로 사용합니다.

내부 영역의 사용자 관점에서 파일은 /opt/docs에서 액세스할 수 있습니다.

INTERNAL 레이블의 터미널 창에서 관리자가 파일을 마운트합니다.

```
# mountall
```

예 11–6 LDAP을 사용하여 관리되는 네트워크에서 레이블이 있는 홈 디렉토리 마운트

이 예에서 시스템 관리자는 새로운 사용자인 ikuk가 모든 레이블에서 자신의 홈 디렉토리에 액세스할 수 있게 합니다. 이 사이트는 두 개의 홈 디렉토리 서버를 사용하며 LDAP으로 관리됩니다. 두번째 서버에는 jdoe 및 pkai 사용자에 대한 홈 디렉토리가 포함되어 있습니다. 새로운 사용자가 이 목록에 추가됩니다.

먼저 시스템 관리자 역할을 맡은 후 관리자는 두번째 홈 디렉토리 서버에 새로운 사용자가 포함되도록 전역 영역의 /etc 디렉토리에 있는 auto_home_*zone-name* 파일을 수정합니다.

```
## auto_home_global file
jdoe   homedir2-server:/export/home/jdoe
pkai   homedir2-server:/export/home/pkai
ikuk   homedir2-server:/export/home/ikuk
*      homedir-server:/export/home/&

## auto_home_internal file
## Mount the home directory from the internal zone of the NFS server
jdoe   homedir2-server:/export/home/jdoe
pkai   homedir2-server:/export/home/pkai
ikuk   homedir2-server:/export/home/ikuk
*      homedir-server:/export/home/&

## auto_home_public
## Mount the home directory from the public zone of the NFS server
jdoe   homedir2-server:/export/home/jdoe
pkai   homedir2-server:/export/home/pkai
ikuk   homedir2-server:/export/home/ikuk
*      homedir-server:/export/home/&
```

그런 다음 사용자가 모든 레이블에서 로그인할 수 있도록 관리자는 모든 레이블의 auto_home_*zone-name* 파일에 대해 이러한 편집 작업을 반복합니다.

마지막으로 이 시스템의 모든 auto_home_*zone-name* 파일을 수정한 후 관리자가 이러한 파일을 사용하여 항목을 LDAP 데이터베이스에 추가합니다.

Oracle Solaris OS와 마찬가지로 /etc/auto_home_*zone-name* 파일의 +auto_home_public 항목은 자동 마운트를 LDAP 항목으로 지정합니다. 네트워크의 다른 시스템에 있는 auto_home_*zone-name* 파일은 LDAP 데이터베이스에서 업데이트됩니다.

예 11–7 파일을 사용하여 관리되는 시스템에서 하위 레벨 홈 디렉토리 마운트

이 예에서 시스템 관리자는 사용자가 모든 레이블에서 자신의 디렉토리에 액세스할 수 있게 합니다. 사이트의 레이블은 PUBLIC, INTERNAL 및 NEEDTOKNOW입니다. 이 사이트는 두 개의 홈 디렉토리 서버를 사용하며 파일로 관리됩니다. 두번째 서버에는 jdoe 및 pkai 사용자에 대한 홈 디렉토리가 포함되어 있습니다.

이 작업을 위해 시스템 관리자는 public 영역에서 공용 영역 NFS 홈 디렉토리를 정의하고, internal 및 needtoknow 영역과 이 구성을 공유합니다.

먼저 시스템 관리자 역할을 맡은 후 관리자는 PUBLIC 레이블에서 작업 공간을 만듭니다. 이 작업 공간에서 관리자는 새 파일인 /export/home/auto_home_public을 만듭니다. 이 파일에는 모든 사용자 정의된 사용자별 NFS 지정 항목이 포함됩니다.

```
## /export/home/auto_home_public file at PUBLIC label
jdoe   homedir2-server:/export/home/jdoe
pkai   homedir2-server:/export/home/pkai
*      homedir-server:/export/home/&
```

두번째로 관리자는 이 새 파일을 가리키도록 /etc/auto_home_public 파일을 수정합니다.

```
## /etc/auto_home_public file in the public zone
## Use /export/home/auto_home_public for the user entries
## +auto_home_public
+ /export/home/auto_home_public
```

이 항목은 자동 마운트가 로컬 파일의 내용을 사용하도록 지정합니다.

세번째로 관리자는 internal 및 needtoknow 영역에서 /etc/auto_home_public 파일을 유사하게 수정합니다. 관리자는 internal 및 needtoknow 영역에서 볼 수 있는 public 영역의 경로 이름을 사용합니다.

```
## /etc/auto_home_public file in the internal zone
## Use /zone/public/export/home/auto_home_public for PUBLIC user home dirs
## +auto_home_public
+ /zone/public/export/home/auto_home_public

## /etc/auto_home_public file in the needtoknow zone
## Use /zone/public/export/home/auto_home_public for PUBLIC user home dirs
## +auto_home_public
+ /zone/public/export/home/auto_home_public
```

관리자가 새로운 사용자인 ikuk을 추가하면 PUBLIC 레이블에서 /export/home/auto_home_public 파일에 추가됩니다.

```
## /export/home/auto_home_public file at PUBLIC label
jdoe    homedir2-server:/export/home/jdoe
pkai    homedir2-server:/export/home/pkai
ikuk    homedir2-server:/export/home/ikuk
*       homedir-server:/export/home/&
```

상위 레벨 영역은 하위를 읽어 하위 레벨 공용 영역에서 사용자별 홈 디렉토리를 가져옵니다.

▼ Trusted Extensions에서 마운트 실패 문제를 해결하는 방법

시작하기 전에 마운트하려는 파일의 레이블 영역에 있어야 합니다. 수퍼유저이거나 시스템 관리자 역할을 가진 사용자여야 합니다.

1 NFS 서버의 보안 속성을 확인합니다.

해당 범위에서 Solaris Management Console의 보안 템플리트 도구를 사용합니다. 자세한 내용은 **Trusted Extensions Configuration Guide**의 "Initialize the Solaris Management Console Server in Trusted Extensions"를 참조하십시오.

a. NFS 서버의 IP 주소가 보안 템플리트 중 하나에서 지정된 호스트인지 확인합니다.

주소는 직접 지정되거나 와일드카드 방식을 통해 간접적으로 지정될 수 있습니다. 주소는 레이블이 있는 템플리트 또는 레이블이 없는 템플리트에 있을 수 있습니다.

b. 템플리트가 NFS 서버에 지정하는 레이블을 확인합니다.

레이블은 파일을 마운트하려는 레이블과 일관성이 있어야 합니다.

2 현재 영역의 레이블을 확인합니다.

레이블이 마운트된 파일 시스템의 레이블보다 상위인 경우 원격 파일 시스템을 읽기/쓰기 권한으로 내보내더라도 마운트에 쓸 수 없습니다. 마운트의 레이블에서 마운트된 파일 시스템에만 쓸 수 있습니다.

3 이전 버전의 Trusted Solaris 소프트웨어를 실행하는 NFS 서버에서 파일 시스템을 마운트하려면 다음을 수행합니다.

- **Trusted Solaris 1 NFS 서버의 경우 `mount` 명령에 `vers=2` 및 `proto=udp` 옵션을 사용합니다.**
- **Trusted Solaris 2.5.1 NFS 서버의 경우 `mount` 명령에 `vers=2` 및 `proto=udp` 옵션을 사용합니다.**

- **Trusted Solaris 8 NFS 서버의 경우 `mount` 명령에 `vers=3` 및 `proto=udp` 옵션을 사용합니다.**

이러한 서버에서 파일 시스템을 마운트하려면 레이블이 없는 템플리트에 서버가 지정되어야 합니다.

◆ ◆ ◆ 12 장

12 신뢰할 수 있는 네트워킹(개요)

이 장에서는 Trusted Extensions의 신뢰할 수 있는 네트워크 개념과 방식에 대해 설명합니다.

- 151 페이지 “신뢰할 수 있는 네트워크”
- 156 페이지 “Trusted Extensions의 네트워크 보안 속성”
- 159 페이지 “신뢰할 수 있는 네트워크 폴백 방식”
- 161 페이지 “Trusted Extensions의 경로 지정 개요”
- 163 페이지 “Trusted Extensions에서 경로 지정 관리”

신뢰할 수 있는 네트워크

Trusted Extensions는 영역, 호스트 및 네트워크에 보안 속성을 지정합니다. 이러한 속성은 네트워크에 다음과 같은 보안 기능이 적용되도록 합니다.

- 네트워크 통신에서 데이터의 레이블이 적절히 지정됩니다.
- 로컬 네트워크를 통해 데이터를 보내거나 받을 때 그리고 파일 시스템을 마운트할 때 MAC(필수 액세스 제어) 규칙이 적용됩니다.
- 원거리 네트워크로 데이터를 경로 지정할 때 MAC 규칙이 적용됩니다.
- 영역으로 데이터를 경로 지정할 때 MAC 규칙이 적용됩니다.

Trusted Extensions에서 네트워크 패킷은 MAC로 보호됩니다. 레이블은 MAC 결정에 사용됩니다. 민감도 레이블에 따라 데이터의 레이블이 명시적 또는 암시적으로 지정됩니다. 레이블에는 ID 필드, 분류 또는 "레벨" 필드 및 구획 또는 "범주" 필드가 있습니다. 데이터는 승인 검사를 통과해야 합니다. 이 검사에서는 레이블이 올바른 형식이고 받는 호스트의 승인 범위 내에 있는지 확인합니다. 받는 호스트의 승인 범위 내에 있는 올바른 형식의 패킷은 액세스가 승인됩니다.

신뢰할 수 있는 시스템 간에 교환되는 IP 패킷의 레이블을 지정할 수 있습니다. Trusted Extensions는 CIPSO(Commercial IP Security Option) 레이블을 지원합니다. 패킷의 CIPSO 레이블은 IP 패킷을 분류, 분리 및 경로를 지정하는 데 사용됩니다. 경로 지정 결정에서는 데이터의 민감도 레이블을 대상 레이블과 비교합니다.

일반적으로 신뢰할 수 있는 네트워크에서 레이블은 전송 호스트에 의해 생성되고 받는 호스트에 의해 처리됩니다. 또한 신뢰할 수 있는 라우터는 신뢰할 수 있는 네트워크에서 패킷을 전달하는 동안 레이블을 추가하거나 제거할 수 있습니다. 민감도 레이블은 전송하기 전에 CIPSO 레이블에 매핑됩니다. CIPSO 레이블은 IP 패킷에 포함됩니다. 일반적으로 패킷을 보낸 사람과 받는 사람은 동일한 레이블에서 작업합니다.

신뢰할 수 있는 네트워킹 소프트웨어는 주체(프로세스)와 객체(데이터)가 서로 다른 호스트에 있는 경우 Trusted Extensions 보안 정책이 적용되도록 합니다. Trusted Extensions 네트워킹은 분산된 응용 프로그램 전체에서 MAC를 유지합니다.

Trusted Extensions 데이터 패킷

Trusted Extensions 데이터 패킷은 CIPSO 레이블 옵션을 포함합니다. IPv4 또는 IPv6 네트워크를 통해 데이터 패킷을 보낼 수 있습니다.

표준 IPv4 형식에서는 IPv4 헤더와 옵션, TCP, UDP 또는 SCTP 헤더, 실제 데이터의 순서로 표시됩니다. Trusted Extensions 버전의 IPv4 패킷에서는 보안 속성에 대한 IP 헤더에 CIPSO 옵션을 사용합니다.

CIPSO 옵션이 있는 IPv4 헤더	TCP, UDP 또는 SCTP	데이터

표준 IPv6 형식에서는 IPv6 헤더와 확장, TCP, UDP 또는 SCTP 헤더, 실제 데이터의 순서로 표시됩니다. Trusted Extensions IPv6 패킷에는 확장이 있는 헤더에 다중 레벨 보안 옵션이 포함되어 있습니다.

확장이 있는 IPv6 헤더	TCP, UDP 또는 SCTP	데이터

신뢰할 수 있는 네트워크 통신

Trusted Extensions는 신뢰할 수 있는 네트워크에서 레이블이 있는 호스트와 레이블이 없는 호스트를 지원합니다. LDAP은 완벽하게 지원되는 이름 지정 서비스입니다. 다양한 명령과 GUI를 사용하여 네트워크를 관리할 수 있습니다.

Trusted Extensions 소프트웨어를 실행하는 시스템은 Trusted Extensions 호스트와 다음 유형의 시스템 간 네트워크 통신을 지원합니다.

- Trusted Extensions를 실행 중인 다른 시스템
- 보안 속성을 인식하지 않지만 TCP/IP를 지원하는 운영 체제를 실행 중인 시스템(예: Oracle Solaris 시스템), 기타 UNIX 시스템, Microsoft Windows 및 Macintosh OS 시스템
- CIPSO 레이블을 인식하는 다른 신뢰할 수 있는 운영 체제를 실행 중인 시스템

Oracle Solaris OS에서와 마찬가지로 이름 지정 서비스를 통해 Trusted Extensions 네트워크 통신과 서비스를 관리할 수 있습니다. Trusted Extensions는 Oracle Solaris 네트워크 인터페이스에 다음과 같은 인터페이스를 추가합니다.

- Trusted Extensions는 세 가지 네트워크 구성 데이터베이스인 `tnzonecfg`, `tnrhdb` 및 `tnrhtp`를 추가합니다. 자세한 내용은 154 페이지 "Trusted Extensions의 네트워크 구성 데이터베이스"를 참조하십시오.
- Trusted Extensions 버전의 이름 지정 서비스 전환 파일인 `nsswitch.conf`에는 `tnrhtp` 및 `tnrhdb` 데이터베이스에 대한 항목이 포함되어 있습니다. 이 항목을 각 사이트의 구성에 맞게 수정할 수 있습니다.

  Trusted Extensions는 LDAP 이름 지정 서비스를 사용하여 호스트, 네트워크 및 사용자를 정의하는 구성 파일을 중앙에서 관리합니다. LDAP 이름 지정 서비스의 신뢰할 수 있는 네트워크 데이터베이스에 대한 기본 `nsswitch.conf` 항목은 다음과 같습니다.

  ```
  # Trusted Extensions
  tnrhtp: files ldap
  tnrhdb: files ldap
  ```

  Oracle Directory Server Enterprise Edition의 LDAP 이름 지정 서비스는 Trusted Extensions에서 완벽하게 지원되는 유일한 이름 지정 서비스입니다. Trusted Extensions로 구성된 시스템에서 LDAP 사용에 대한 자세한 내용은 9 장, "Trusted Extensions 및 LDAP(개요)"를 참조하십시오.
- Trusted Extensions는 Solaris Management Console에 도구를 추가합니다. 콘솔은 영역, 호스트 및 네트워크를 중앙에서 관리하는 데 사용됩니다. 38 페이지 "Solaris Management Console 도구"에 네트워크 도구가 설명되어 있습니다.

  Trusted Extensions Configuration Guide에서는 네트워크를 구성할 때 영역과 호스트를 정의하는 방법에 대해 설명합니다. 자세한 내용은 13 장, "Trusted Extensions에서 네트워크 관리(작업)"를 참조하십시오.
- Trusted Extensions는 신뢰할 수 있는 네트워킹을 관리하는 명령을 추가합니다. 또한 Trusted Extensions는 Oracle Solaris 네트워크 명령에 대한 옵션을 추가합니다. 이러한 명령에 대한 자세한 내용은 154 페이지 "Trusted Extensions의 네트워크 명령"을 참조하십시오.

Trusted Extensions의 네트워크 구성 데이터베이스

Trusted Extensions는 네트워크 구성 데이터베이스를 커널로 로드합니다. 이러한 데이터베이스는 호스트 간에 데이터를 전송할 때 승인 검사에 사용됩니다.

- `tnzonecfg` – 이 로컬 데이터베이스는 보안과 관련된 영역 속성을 저장합니다. 각 영역에 대한 속성은 영역 레이블과 단일 레벨 및 다중 레벨 호스트에 대한 영역의 액세스 권한을 지정합니다. 다른 속성은 `ping`과 같은 제어 메시지에 대한 응답을 처리합니다. 영역에 대한 레이블은 `label_encodings` 파일에 정의되어 있습니다. 자세한 내용은 `label_encodings(4)` 및 `smtnzonecfg(1M)` 매뉴얼 페이지를 참조하십시오. 다중 레벨 포트에 대한 자세한 내용은 119 페이지 “영역 및 다중 레벨 포트”를 참조하십시오.
- `tnrhtp` – 이 데이터베이스는 호스트 및 게이트웨이의 보안 속성을 설명하는 템플리트를 저장합니다. `tnrhtp`는 로컬 데이터베이스거나 LDAP 서버에 저장할 수 있습니다. 호스트와 게이트웨이는 트래픽을 전송할 때 대상 호스트와 다음 홉 게이트웨이의 속성을 사용하여 MAC를 적용합니다. 트래픽을 받을 때는 보낸 사람의 속성을 사용합니다. 보안 속성에 대한 자세한 내용은 155 페이지 “신뢰할 수 있는 네트워크 보안 속성”을 참조하십시오. 자세한 내용은 `smtnrhtp(1M)` 매뉴얼 페이지를 참조하십시오.
- `tnrhdb` – 이 데이터베이스는 통신이 허용된 모든 호스트에 해당하는 IP 주소와 네트워크 접두어(폴백 방식)를 저장합니다. `tnrhdb`는 로컬 데이터베이스거나 LDAP 서버에 저장할 수 있습니다. 각 호스트 또는 네트워크 접두어에는 `tnrhtp` 데이터베이스의 보안 템플리트가 지정됩니다. 템플리트의 속성은 지정된 호스트의 속성을 정의합니다. 자세한 내용은 `smtnrhdb(1M)` 매뉴얼 페이지를 참조하십시오.

Trusted Extensions에서 이러한 데이터베이스를 처리하도록 Solaris Management Console이 확장되었습니다. 자세한 내용은 38 페이지 “Solaris Management Console 도구”를 참조하십시오.

Trusted Extensions의 네트워크 명령

Trusted Extensions는 신뢰할 수 있는 네트워킹을 관리하는 다음 명령을 추가합니다.

- `tnchkdb` – 이 명령은 신뢰할 수 있는 네트워크 데이터베이스의 정확성을 확인하는 데 사용됩니다. `tnchkdb` 명령은 보안 템플리트(`tnrhtp`), 보안 템플리트 지정(`tnrhdb`) 또는 영역 구성(`tnzonecfg`)을 변경할 때마다 사용됩니다. 데이터베이스가 수정되면 Solaris Management Console 도구에서 이 명령을 자동으로 실행합니다. 자세한 내용은 `tnchkdb(1M)` 매뉴얼 페이지를 참조하십시오.
- `tnctl` – 이 명령을 사용하여 커널에서 신뢰할 수 있는 네트워크 정보를 업데이트할 수 있습니다. `tnctl`은 시스템 서비스이기도 합니다. `svcadm restart /network/tnctl` 명령으로 다시 시작하면 로컬 시스템의 신뢰할 수 있는 네트워크 데이터베이스에서 커널 캐시를 새로 고쳐집니다. Files(파일) 범위 내에서 데이터베이스가 수정되면 Solaris Management Console 도구에서 이 명령을 자동으로 실행합니다. 자세한 내용은 `tnctl(1M)` 매뉴얼 페이지를 참조하십시오.

- `tnd` – 이 데몬은 LDAP 디렉토리 및 로컬 파일에서 `tnrhdb` 및 `tnrhtp` 정보를 끌어옵니다. `nsswitch.conf` 파일 내의 순서에 따라 이름 지정 서비스에서 정보가 로드됩니다. 부팅하는 동안 `svc:/network/tnd` 서비스에 의해 `tnd` 데몬이 시작됩니다. 이 서비스는 `svc:/network/ldap/client`에 종속됩니다.

  `tnd` 명령은 폴링 간격을 변경하거나 디버깅하는 데도 사용될 수 있습니다. 자세한 내용은 `tnd(1M)` 매뉴얼 페이지를 참조하십시오.

- `tninfo` – 이 명령은 신뢰할 수 있는 네트워크 커널 캐시의 현재 상태에 대한 세부 정보를 표시합니다. 호스트 이름, 영역 또는 보안 템플리트별로 출력을 필터링할 수 있습니다. 자세한 내용은 `tninfo(1M)` 매뉴얼 페이지를 참조하십시오.

Trusted Extensions는 다음 Oracle Solaris 네트워크 명령에 옵션을 추가합니다.

- `ifconfig` – 이 명령에 대한 `all-zones` 인터페이스 플래그는 지정된 인터페이스를 시스템의 모든 영역에서 사용할 수 있게 합니다. 데이터에 연결된 레이블에 따라 데이터를 전달할 적절한 영역이 결정됩니다. 자세한 내용은 `ifconfig(1M)` 매뉴얼 페이지를 참조하십시오.
- `netstat` – `-R` 옵션은 Oracle Solaris `netstat` 사용을 확장하여 경로 지정 테이블 항목 및 다중 레벨 소켓에 대한 보안 속성 등의 Trusted Extensions 관련 정보를 표시합니다. 확장된 보안 속성에는 소켓이 한 영역에 특정한지 아니면 여러 영역에서 사용 가능한지와 피어의 레이블이 포함됩니다. 자세한 내용은 `netstat(1M)` 매뉴얼 페이지를 참조하십시오.
- `route` – `-secattr` 옵션은 Oracle Solaris `route` 사용을 확장하여 경로의 보안 속성을 표시합니다. 옵션 값의 형식은 다음과 같습니다.

  `min_sl=`*label*`,max_sl=`*label*`,doi=`*integer*`,cipso`

  `cipso` 키워드는 선택 사항이며 기본적으로 설정됩니다. 자세한 내용은 `route(1M)` 매뉴얼 페이지를 참조하십시오.
- `snoop` – Oracle Solaris OS에서와 마찬가지로 이 명령에 대한 `-v` 옵션을 사용하여 IP 헤더를 자세히 표시할 수 있습니다. Trusted Extensions에서는 헤더에 레이블 정보가 포함됩니다.

신뢰할 수 있는 네트워크 보안 속성

Trusted Extensions에서 네트워크 관리는 보안 템플리트를 기반으로 합니다. 보안 템플리트는 공통 프로토콜과 동일한 보안 속성을 사용하는 호스트 세트에 대해 설명합니다.

보안 속성은 템플리트를 통해 호스트 시스템과 라우터 시스템 모두에 관리용으로 지정됩니다. 보안 관리자는 템플리트를 관리하고 시스템에 지정합니다. 시스템에 지정된 템플리트가 없는 경우 해당 시스템과 통신할 수 없습니다.

템플리트마다 이름이 있으며 다음을 포함합니다.

- Unlabeled(레이블 없는) 또는 CIPSO 호스트 유형. 네트워크 통신에 사용되는 프로토콜은 템플리트의 호스트 유형에 의해 결정됩니다.

  호스트 유형은 CIPSO 옵션의 사용 여부를 결정하는 데 사용되며 MAC에 영향을 줍니다. 자세한 내용은 157 페이지 "보안 템플리트의 호스트 유형 및 템플리트 이름"을 참조하십시오.
- 각 호스트 유형에 적용되는 보안 속성 세트.

호스트 유형 및 보안 속성에 대한 자세한 내용은 156 페이지 "Trusted Extensions의 네트워크 보안 속성"을 참조하십시오.

Trusted Extensions의 네트워크 보안 속성

Trusted Extensions는 기본 보안 템플리트 세트와 함께 설치됩니다. 템플리트가 호스트에 지정되면 템플리트의 보안 값이 호스트에 적용됩니다. Trusted Extensions에서는 템플리트를 통해 네트워크의 레이블이 없는 호스트와 레이블이 있는 호스트 모두에 보안 속성이 지정됩니다. 보안 템플리트가 지정되지 않은 호스트에는 연결할 수 없습니다. 템플리트는 로컬로 저장하거나 Oracle Directory Server Enterprise Edition의 LDAP 이름 지정 서비스에 저장할 수 있습니다.

템플리트를 호스트에 직접 또는 간접적으로 지정할 수 있습니다. 직접 지정에서는 템플리트를 특정 IP 주소에 지정합니다. 간접 지정에서는 호스트가 포함된 네트워크 주소에 템플리트를 지정합니다. 보안 템플리트가 없는 호스트는 Trusted Extensions로 구성된 호스트와 통신할 수 없습니다. 직접 지정과 간접 지정에 대한 자세한 내용은 159 페이지 "신뢰할 수 있는 네트워크 폴백 방식"을 참조하십시오.

Solaris Management Console의 Security Templates(보안 템플리트) 도구를 사용하여 템플리트를 수정하거나 만듭니다. Security Templates(보안 템플리트) 도구는 템플리트의 필수 필드를 모두 작성하도록 합니다. 필수 필드는 호스트 유형을 기반으로 합니다.

호스트 유형마다 추가 필수 및 선택적 보안 속성이 있습니다. 보안 템플리트에서 지정되는 보안 속성은 다음과 같습니다.

- **호스트 유형** – CIPSO 보안 레이블을 사용하여 패킷의 레이블을 지정할지 아니면 레이블을 아예 지정하지 않을지 여부를 정의합니다.
- **기본 레이블** – 레이블이 없는 호스트의 신뢰 레벨을 정의합니다. 레이블이 없는 호스트에서 보내는 패킷은 받는 Trusted Extensions 호스트 또는 게이트웨이가 이 레이블에서 읽습니다.

  기본 레이블 속성은 레이블이 없는 호스트 유형에만 한정됩니다. 자세한 내용은 `smtnrhtp(1M)` 매뉴얼 페이지와 다음 섹션을 참조하십시오.

- **DOI** – DOI를 식별하는 0이 아닌 양의 정수입니다. DOI는 네트워크 통신 또는 네트워크 엔티티에 적용되는 레이블 인코딩 세트를 나타내는 데 사용됩니다. 다른 항목이 동일하더라도 DOI가 다른 레이블은 서로 분리됩니다. 레이블이 없는 호스트의 경우 DOI가 기본 레이블에 적용됩니다. Trusted Extensions에서 기본값은 1입니다.
- **최소 레이블** – 레이블 승인 범위의 하한을 정의합니다. 호스트 및 다음 홉 게이트웨이가 템플리트에 지정된 최소 레이블보다 낮은 패킷을 받지 않습니다.
- **최대 레이블** – 레이블 승인 범위의 상한을 정의합니다. 호스트 및 다음 홉 게이트웨이가 템플리트에 지정된 최대 레이블보다 높은 패킷을 받지 않습니다.
- **보안 레이블 세트** – 선택 사항입니다. 보안 템플리트에 대해 별개의 보안 레이블 세트를 지정합니다. 최대 레이블과 최소 레이블에 의해 결정되는 승인 범위 이외에 보안 레이블 세트를 통해 템플리트에 지정되는 호스트는 레이블 세트의 레이블 중 하나와 일치하는 패킷을 보내고 받을 수 있습니다. 지정할 수 있는 최대 레이블 수는 4개입니다.

보안 템플리트의 호스트 유형 및 템플리트 이름

Trusted Extensions는 신뢰할 수 있는 네트워크 데이터베이스에서 두 가지 호스트 유형을 지원하고 두 개의 기본 템플리트를 제공합니다.

- **CIPSO 호스트 유형** – 신뢰할 수 있는 운영 체제를 실행하는 호스트용입니다. Trusted Extensions는 이 호스트 유형에 대해 `cipso` 템플리트를 제공합니다.

  CIPSO(Common IP Security Option) 프로토콜은 IP 옵션 필드로 전달되는 보안 레이블을 지정하는 데 사용됩니다. CIPSO 레이블은 데이터 레이블에서 자동으로 파생됩니다. 태그 유형 1은 CIPSO 보안 레이블을 전달하는 데 사용됩니다. 그런 다음 이 레이블은 IP 레벨에서 보안 검사를 수행하고 네트워크 패킷에서 데이터의 레이블을 지정하는 데 사용됩니다.
- **레이블이 없는 호스트 유형** - 표준 네트워킹 프로토콜을 사용하지만 CIPSO 옵션을 지원하지 않는 호스트용입니다. Trusted Extensions는 이 호스트 유형에 대해 `admin_low` 템플리트를 제공합니다.

  이 호스트 유형은 Oracle Solaris OS 또는 레이블이 없는 다른 운영 체제를 실행하는 호스트에 지정됩니다. 이 호스트 유형은 레이블이 없는 호스트와의 통신에 적용할 기본 클리어런스와 기본 레이블을 제공합니다. 또한 패킷을 레이블이 없는 게이트웨이로 보내서 전달할 수 있도록 레이블 범위나 개별 레이블 세트를 지정할 수 있습니다.

주의 – `admin_low` 템플리트는 사이트별 레이블로 레이블이 없는 템플리트를 구성하는 예를 제공합니다. `admin_low` 템플리트는 Trusted Extensions를 설치하는 데 필요하지만 보안 설정은 일반 시스템 작업에 적합하지 않을 수 있습니다. 시스템 유지 보수 및 지원을 위해 제공된 템플리트를 수정하지 않고 그대로 유지하십시오.

보안 템플리트의 기본 레이블

레이블이 없는 호스트 유형에 대한 템플리트는 기본 레이블을 지정합니다. 이 레이블은 운영 체제에서 레이블을 인식하지 못하는 호스트(예: Oracle Solaris 시스템)와의 통신을 제어하는 데 사용됩니다. 지정되는 기본 레이블은 호스트와 해당 사용자에 적합한 신뢰 레벨을 반영합니다.

레이블이 없는 호스트와의 통신은 기본 레이블로 제한되기 때문에 이러한 호스트를 **단일 레이블 호스트**라고도 합니다.

보안 템플리트의 DOI

동일한 DOI(Domain of Interpretation)를 사용하는 조직 간에는 레이블 정보와 기타 보안 속성을 동일한 방법으로 해석한다는 동의가 있습니다. Trusted Extensions에서 레이블 비교를 수행할 때 DOI가 같은지 여부를 검사합니다.

Trusted Extensions 시스템에서는 하나의 DOI 값에 레이블 정책을 적용합니다. Trusted Extensions 시스템의 모든 영역이 동일한 DOI에서 작동해야 합니다. Trusted Extensions 시스템은 다른 DOI를 사용하는 시스템에서 받은 패킷에 대한 예외 처리를 제공하지 않습니다.

사이트에서 기본값과 다른 DOI 값을 사용하는 경우 이 값을 `/etc/system` 파일에 추가하고 모든 보안 템플리트에서 값을 변경해야 합니다. 초기 절차는 **Trusted Extensions Configuration Guide**의 "Configure the Domain of Interpretation"을 참조하십시오. 모든 보안 템플리트에서 DOI를 구성하려면 예 13–1을 참조하십시오.

보안 템플리트의 레이블 범위

최소 레이블 및 최대 레이블 속성은 레이블이 있는 호스트와 레이블이 없는 호스트에 대한 레이블 범위를 설정하는 데 사용됩니다. 이러한 속성을 사용하여 다음을 수행할 수 있습니다.

- 원격 CIPSO 호스트와 통신할 때 사용할 수 있는 레이블 범위 설정

  패킷을 대상 호스트로 보내려면 패킷의 레이블이 해당 호스트에 대한 보안 템플리트에서 대상 호스트에 지정된 레이블 범위에 속해야 합니다.
- CIPSO 게이트웨이 또는 레이블이 없는 게이트웨이를 통해 전달되는 패킷에 대한 레이블 범위 설정

  레이블이 없는 호스트 유형에 대한 템플리트에 레이블 범위를 지정할 수 있습니다. 레이블 범위를 사용하면 호스트에서 호스트 레이블에 없어도 되지만 지정된 레이블 범위 내에 있는 패킷을 전달할 수 있습니다.

보안 템플리트의 보안 레이블 세트

보안 레이블 세트는 원격 호스트에서 패킷을 수락, 전달 또는 전송할 수 있는 4개 이하의 개별 레이블을 정의합니다. 이 속성은 선택 사항입니다. 기본적으로 보안 레이블 세트는 정의되어 있지 않습니다.

신뢰할 수 있는 네트워크 폴백 방식

`tnrhdb` 데이터베이스는 특정 호스트에 보안 템플리트를 직접 또는 간접적으로 지정할 수 있습니다. 직접 지정에서는 템플리트를 호스트 IP 주소에 지정합니다. 간접 지정은 폴백 방식에 의해 처리됩니다. 신뢰할 수 있는 네트워크 소프트웨어에서 먼저 호스트의 IP 주소를 템플리트에 지정하는 항목을 찾습니다. 소프트웨어에서 호스트에 대한 특정 항목을 찾을 수 없는 경우 "일치하는 비트의 가장 긴 접두어"를 찾습니다. 호스트의 IP 주소가 고정 접두어 길이를 가진 IP 주소의 "일치하는 비트의 가장 긴 접두어" 내에 속하면 호스트를 보안 템플리트에 간접적으로 지정할 수 있습니다.

IPv4에서는 서브넷에서 간접 지정을 수행할 수 있습니다. 4, 3, 2 또는 1 후행 제로(0) 옥테트를 사용하여 간접 지정을 수행하면 소프트웨어에서 접두어 길이를 각각 0, 8, 16 또는 24로 계산합니다. 표 12–1의 3 – 6 항목은 이 폴백 방식을 보여줍니다.

슬래시(/)와 고정 비트 수를 추가하여 고정 접두어 길이를 설정할 수도 있습니다. IPv4 네트워크 주소의 가능한 접두어 길이는 1 – 32입니다. IPv6 네트워크 주소의 가능한 접두어 길이는 1 – 128입니다.

다음 표에는 폴백 주소와 호스트 주소의 예가 나와 있습니다. 폴백 주소 세트 내의 한 주소가 간접적으로 지정되는 경우 해당 주소에 폴백 방식이 사용되지 않습니다.

표 12–1 tnrhdb 호스트 주소 및 폴백 방식 항목

IP 버전	tnrhdb 항목	포함된 주소
IPv4	192.168.118.57:cipso	192.168.118.57
	192.168.118.57/32:cipso	/32는 접두어 길이를 32 고정 비트로 설정합니다.
	192.168.118.128/26:cipso	192.168.118.0 - 192.168.118.63
	192.168.118.0:cipso	192.168.118. 네트워크의 모든 주소
	192.168.118.0/24:cipso	
	192.168.0.0/24:cipso	192.168.0. 네트워크의 모든 주소
	192.168.0.0:cipso	192.168. 네트워크의 모든 주소
	192.168.0.0/16:cipso	
	192.0.0.0:cipso	192. 네트워크의 모든 주소
	192.0.0.0/8:cipso	
	192.168.0.0/32:cipso	네트워크 주소 192.168.0.0. 와일드카드 주소 아님
	192.168.118.0/32:cipso	네트워크 주소 192.168.118.0. 와일드카드 주소 아님
	192.0.0.0/32:cipso	네트워크 주소 192.0.0.0. 와일드카드 주소 아님
	0.0.0.0/32:cipso	호스트 주소 0.0.0.0. 와일드카드 주소 아님
	0.0.0.0:cipso	모든 네트워크의 모든 주소
IPv6	2001\:DB8\:22\:5000\:\:21f7:cipso	2001:DB8:22:5000::21f7
	2001\:DB8\:22\:5000\:\:0/52:cipso	2001:DB8:22:5000::0 ~ 2001:DB8:22:5fff:ffff:ffff:ffff:ffff
	0\:\:0/0:cipso	모든 네트워크의 모든 주소

0.0.0.0/32 주소는 특정 주소 0.0.0.0과 일치합니다. tnrhdb 항목 0.0.0.0/32:admin_low는 리터럴 주소 0.0.0.0이 소스 IP 주소로 사용되는 시스템에서 유용합니다. 예를 들어, DHCP 클라이언트는 서버가 클라이언트에 IP 주소를 제공하기 전에 DHCP 서버에 0.0.0.0으로 연결합니다.

DHCP 클라이언트를 처리하는 Sun Ray 서버에서 tnrhdb 항목을 만들려면 예 13–13을 참조하십시오. 0.0.0.0:admin_low는 기본 와일드카드 항목이므로 이 기본값을 제거하거나 변경하기 전에 고려해야 할 사항은 177 페이지 “신뢰할 수 있는 네트워크에서 연결할 수 있는 호스트를 제한하는 방법”을 참조하십시오.

IPv4 및 IPv6 주소의 접두어 길이에 대한 자세한 내용은 **Oracle Solaris 관리: IP 서비스**의 "CIDR IPv4 주소 지정 체계 설계" 및 **Oracle Solaris 관리: IP 서비스**의 "IPv6 주소 지정 개요"를 참조하십시오.

Trusted Extensions의 경로 지정 개요

Trusted Extensions에서는 서로 다른 네트워크에 있는 호스트 간의 경로 지정 시 각 전송 단계에서 보안이 유지되어야 합니다. Trusted Extensions는 Oracle Solaris OS의 경로 지정 프로토콜에 확장된 보안 속성을 추가합니다. Oracle Solaris OS와 달리 이 Trusted Extensions 릴리스는 동적 경로 지정을 지원하지 않습니다. 정적 경로 지정에 대한 자세한 내용은 `route(1M)` 매뉴얼 페이지의 `-p` 옵션을 참조하십시오.

게이트웨이와 라우터는 패킷을 경로 지정합니다. 이 항목에서는 용어 "게이트웨이"와 "라우터"가 같은 의미로 사용됩니다.

동일한 서브넷에 있는 호스트 간 통신에서는 라우터가 사용되지 않으므로 끝점에서만 승인 검사가 수행됩니다. 레이블 범위 검사는 소스에서 수행됩니다. 받는 호스트에서 Trusted Extensions 소프트웨어를 실행 중인 경우 대상에서도 레이블 범위 검사가 수행됩니다.

소스 호스트와 대상 호스트가 서로 다른 서브넷에 있는 경우 패킷은 소스 호스트에서 게이트웨이로 전송됩니다. 대상과 첫번째 홉 게이트웨이의 레이블 범위는 경로 선택 시 소스에서 검사됩니다. 게이트웨이는 대상 호스트가 연결되는 네트워크에 패킷을 전달합니다. 패킷은 대상에 도달하기 전에 여러 게이트웨이를 통과할 수 있습니다.

경로 지정 배경

Trusted Extensions 게이트웨이에서는 특정한 경우에만 레이블 범위 검사가 수행됩니다. 레이블이 없는 두 호스트 사이에서 패킷을 경로 지정하는 Trusted Extensions 시스템은 소스 호스트의 기본 레이블을 대상 호스트의 기본 레이블과 비교합니다. 레이블이 없는 호스트가 기본 레이블을 공유하는 경우 패킷이 경로 지정됩니다.

각 게이트웨이는 모든 대상에 대한 경로 목록을 유지합니다. 표준 Oracle Solaris 경로 지정은 경로를 최적화하는 선택 사항을 만듭니다. Trusted Extensions는 경로 선택 사항에 적용되는 보안 요구 사항을 검사하는 추가 소프트웨어를 제공합니다. 보안 요구 사항을 충족하지 않는 Oracle Solaris 선택 사항은 건너뜁니다.

Trusted Extensions의 경로 지정 테이블 항목

Trusted Extensions의 경로 지정 테이블 항목은 보안 속성을 통합할 수 있습니다. 보안 속성은 `cipso` 키워드를 포함할 수 있으며 보안 속성은 최대 레이블, 최소 레이블 및 DOI를 포함해야 합니다.

항목에서 보안 속성을 제공하지 않는 경우 게이트웨이의 보안 템플리트에 있는 속성이 사용됩니다.

Trusted Extensions 승인 검사

Trusted Extensions 소프트웨어에서는 보안을 위해 경로의 적합성을 결정합니다. 이 소프트웨어는 소스 호스트, 대상 호스트 및 중간 게이트웨이에서 **승인 검사**라는 일련의 테스트를 실행합니다.

주 – 다음 설명에서 레이블 범위에 대한 승인 검사는 보안 레이블 세트에 대한 검사를 의미하기도 합니다.

승인 검사에서는 레이블 범위와 CIPSO 레이블 정보를 확인합니다. 경로에 대한 보안 속성은 경로 지정 테이블 항목에서 가져오며, 항목에 보안 속성이 없는 경우 게이트웨이의 보안 템플리트에서 가져오기도 합니다.

받는 통신의 경우 Trusted Extensions 소프트웨어에서는 가능하면 패킷 자체에서 레이블을 가져옵니다. 레이블을 지원하는 시스템에서 메시지를 보내는 경우에만 패킷에서 레이블을 가져올 수 있습니다. 패킷에서 레이블을 사용할 수 없는 경우 신뢰할 수 있는 네트워킹 데이터베이스 파일의 메시지에 기본 레이블이 지정됩니다. 그러면 승인 검사 중에 이러한 레이블이 사용됩니다. Trusted Extensions는 나가는 메시지, 전달된 메시지 및 받는 메시지에 대해 여러 가지 검사를 수행합니다.

소스 승인 검사

보내는 프로세스 또는 보내는 영역에서 다음과 같은 승인 검사가 수행됩니다.

- 모든 대상에 대해 데이터 레이블이 경로의 다음 홉 즉, 첫번째 홉의 레이블 범위 내에 있어야 합니다. 또한 레이블이 첫번째 홉 게이트웨이의 보안 속성에 포함되어야 합니다.
- 모든 대상에 대해 나가는 패킷의 DOI가 대상 호스트의 DOI와 일치해야 합니다. 또한 DOI가 첫번째 홉 게이트웨이를 포함하여 경로를 따라 모든 홉의 DOI와 일치해야 합니다.
- 대상 호스트가 레이블이 없는 호스트인 경우 다음 조건 중 하나를 충족해야 합니다.
  - 보내는 호스트의 레이블이 대상 호스트의 기본 레이블과 일치해야 합니다.
  - 보내는 호스트가 교차 레이블 통신을 수행할 권한이 있고 보낸 사람의 레이블이 대상의 기본 레이블을 지배합니다.
  - 보내는 호스트에 레이블 간 통신을 수행할 권한이 있고 보낸 사람의 레이블이 `ADMIN_LOW`입니다. 즉, 보낸 사람이 전역 영역에서 보내고 있습니다.

주 – 게이트웨이를 통해 한 네트워크의 호스트에서 다른 네트워크의 호스트로 메시지를 보낼 때 첫번째 홉 검사가 수행됩니다.

게이트웨이 승인 검사

Trusted Extensions 게이트웨이 시스템에서 다음 홉 게이트웨이에 대해 다음과 같은 승인 검사가 수행됩니다.

- 받는 패킷에 레이블이 없는 경우 해당 패킷은 `tnrhdb` 항목에서 소스 호스트의 기본 레이블을 상속합니다. 그렇지 않으면, 표시된 CIPSO 레이블을 받습니다.
- 패킷 전달 검사는 소스 승인과 비슷하게 진행됩니다.
  - 모든 대상에 대해 데이터의 레이블이 다음 홉의 레이블 범위 내에 있어야 합니다. 또한 레이블이 다음 홉 호스트의 보안 속성에 포함되어야 합니다.
  - 모든 대상에 대해 나가는 패킷의 DOI가 대상 호스트의 DOI와 일치해야 합니다. 또한 DOI가 다음 홉 호스트의 DOI와 일치해야 합니다.
  - 레이블이 없는 패킷의 레이블이 대상 호스트의 기본 레이블과 일치해야 합니다.
  - CIPSO 패킷의 레이블이 대상 호스트의 레이블 범위 내에 있어야 합니다.

대상 승인 검사

Trusted Extensions 호스트에서 데이터를 받으면 소프트웨어에서 다음과 같은 검사를 수행합니다.

- 받는 패킷에 레이블이 없는 경우 해당 패킷은 `tnrhdb` 항목에서 소스 호스트의 기본 레이블을 상속합니다. 그렇지 않으면, 표시된 CIPSO 레이블을 받습니다.
- 패킷의 레이블과 DOI가 대상 영역 또는 대상 프로세스의 레이블 및 DOI와 일치해야 합니다. 프로세스가 다중 레벨 포트에서 수신 대기하는 경우는 예외입니다. 수신 프로세스에 레이블 간 통신을 수행할 권한이 있고, 프로세스가 전역 영역 내에 있거나 프로세스에 패킷의 레이블을 지배하는 레이블이 있는 경우 프로세스에서 패킷을 받을 수 있습니다.

Trusted Extensions에서 경로 지정 관리

Trusted Extensions는 네트워크 간의 통신을 경로 지정하는 다양한 방법을 지원합니다. 보안 관리자 역할로 사이트의 보안 정책에서 요구하는 수준의 보안을 적용하는 경로를 설정할 수 있습니다.

예를 들어, 사이트에서 로컬 네트워크 외부 통신을 단일 레이블로 제한할 수 있습니다. 이 레이블은 공개적으로 사용 가능한 정보에 적용됩니다. UNCLASSIFIED 또는 PUBLIC과 같은 레이블은 공용 정보를 나타낼 수 있습니다. 제한을 적용하기 위해 이러한 사이트에서는 외부 네트워크에 연결되는 네트워크 인터페이스에 단일 레이블 템플리트를 지정합니다. TCP/IP 및 경로 지정에 대한 자세한 내용은 다음을 참조하십시오.

- **Oracle Solaris 관리: IP 서비스**의 "네트워크의 라우터 계획"
- **Oracle Solaris 관리: IP 서비스**의 "로컬 네트워크의 시스템 구성"
- **Oracle Solaris 관리: IP 서비스**의 "주요 TCP/IP 관리 작업(작업 맵)"
- **Oracle Solaris 관리: IP 서비스**의 "DHCP 서비스용 네트워크 준비(작업 맵)"

Trusted Extensions에서 라우터 선택

Trusted Extensions 호스트는 가장 높은 수준의 신뢰를 라우터로 제공합니다. 다른 유형의 라우터는 Trusted Extensions 보안 속성을 인식할 수 없습니다. 관리 작업 없이 MAC 보안 보호를 제공하지 않는 라우터를 통해 패킷을 경로 지정할 수 있습니다.

- CIPSO 라우터는 IP 옵션 구역에서 올바른 유형의 정보를 찾을 수 없는 패킷을 삭제합니다. 예를 들어, CIPSO 라우터는 옵션이 필수 항목일 때 IP 옵션에서 CIPSO 옵션을 찾을 수 없거나 IP 옵션의 DOI가 대상의 승인과 일치하지 않는 경우 패킷을 삭제합니다.
- Trusted Extensions 소프트웨어를 실행하지 않는 다른 유형의 라우터는 패킷을 전달하거나 CIPSO 옵션을 포함하는 패킷을 삭제하도록 구성할 수 있습니다. Trusted Extensions에서 제공하는 CIPSO 인식 게이트웨이에서만 CIPSO IP 옵션의 내용을 사용하여 MAC를 적용할 수 있습니다.

신뢰할 수 있는 경로 지정을 지원하기 위해 Trusted Extensions 보안 속성을 포함하도록 Solaris 10 경로 지정 테이블이 확장되었습니다. 속성에 대한 자세한 내용은 161 페이지 "Trusted Extensions의 경로 지정 테이블 항목"을 참조하십시오. Trusted Extensions는 관리자가 경로 지정 테이블 항목을 수동으로 만드는 정적 경로 지정을 지원합니다. 자세한 내용은 route(1M) 매뉴얼 페이지의 -p 옵션을 참조하십시오.

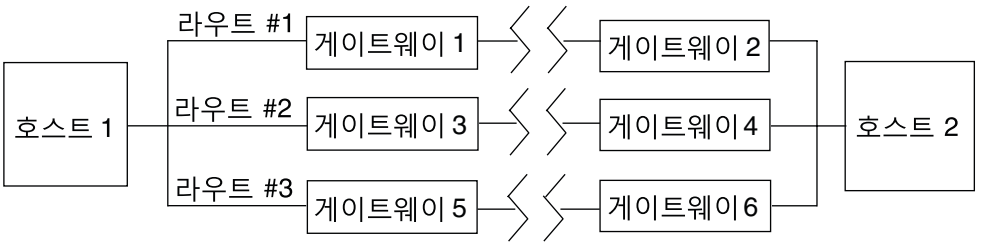
경로 지정 소프트웨어는 경로 지정 테이블에서 대상 호스트로 가는 경로를 찾으려고 합니다. 호스트 이름이 명시적으로 지정되지 않은 경우 경로 지정 소프트웨어는 호스트가 있는 하위 네트워크에 대한 항목을 찾습니다. 호스트와 호스트가 있는 네트워크가 모두 정의되지 않은 경우 호스트는 기본 게이트웨이(정의된 경우)로 패킷을 보냅니다. 여러 기본 게이트웨이를 정의할 수 있으며 각 기본 게이트웨이는 동일하게 처리됩니다.

이 Trusted Extensions 릴리스에서 보안 관리자는 경로를 수동으로 설정한 다음 조건이 변경될 경우 경로 지정 테이블을 수동으로 변경합니다. 예를 들어, 많은 사이트에서 단일 게이트웨이를 사용하여 외부 세계와 통신합니다. 이 경우 단일 게이트웨이를 네트워크의 각 호스트에 대한 **기본값**으로 정적으로 정의할 수 있습니다. 동적 경로 지정 지원은 향후 Trusted Extensions 릴리스에서 제공될 예정입니다.

Trusted Extensions의 게이트웨이

다음은 Trusted Extensions의 경로 지정 예입니다. 다이어그램과 표는 Host 1과 Host 2 사이의 세 가지 잠재적 경로를 보여줍니다.

그림 12–1 일반적인 Trusted Extensions 경로 및 경로 지정 테이블 항목



경로	첫번째 홉 게이트웨이	최소 레이블	최대 레이블	DOI
#1	게이트웨이 1	CONFIDENTIAL	SECRET	1
#2	게이트웨이 3	ADMIN_LOW	ADMIN_HIGH	1
#3	게이트웨이 5			

- 경로 #1은 CONFIDENTIAL ~ SECRET 레이블 범위 내의 패킷을 전송할 수 있습니다.
- 경로 #2는 ADMIN_LOW ~ ADMIN_HIGH의 패킷을 전송할 수 있습니다.
- 경로 #3은 경로 지정 정보를 지정하지 않습니다. 따라서 게이트웨이 5에 대한 tnrhtp 데이터베이스의 템플리트에서 보안 속성이 파생됩니다.

Trusted Extensions의 경로 지정 명령

소켓에 대한 레이블 및 확장 보안 속성을 표시하기 위해 Trusted Extensions는 다음 Oracle Solaris 네트워크 명령을 수정합니다.

- netstat -rR 명령은 경로 지정 테이블 항목의 보안 속성을 표시합니다.
- netstat -aR 명령은 소켓에 대한 보안 속성을 표시합니다.
- add 또는 delete 옵션이 있는 route -p 명령은 경로 지정 테이블 항목을 변경합니다.

자세한 내용은 netstat(1M) 및 route(1M) 매뉴얼 페이지를 참조하십시오.

예는 182 페이지 “보안 속성으로 경로를 구성하는 방법”을 참조하십시오.

◆ ◆ ◆ 13장

13 Trusted Extensions에서 네트워크 관리(작업)

이 장에서는 Trusted Extensions 네트워크 보안을 위한 구현 세부 정보와 절차를 제공합니다.

- 167 페이지 “신뢰할 수 있는 네트워크 관리(작업 맵)”
- 168 페이지 “신뢰할 수 있는 네트워크 데이터베이스 구성(작업 맵)”
- 181 페이지 “Trusted Extensions에서 경로 구성 및 네트워크 정보 확인(작업 맵)”
- 187 페이지 “신뢰할 수 있는 네트워크 문제 해결(작업 맵)”

신뢰할 수 있는 네트워크 관리(작업 맵)

다음 표는 일반적인 신뢰할 수 있는 네트워킹 절차에 대한 작업 맵을 보여줍니다.

작업	설명	수행 방법
네트워크 데이터베이스를 구성합니다.	원격 호스트 템플리트를 만들고 호스트를 템플리트에 지정합니다.	168 페이지 “신뢰할 수 있는 네트워크 데이터베이스 구성(작업 맵)”
경로를 구성하고, 커널의 네트워크 데이터베이스와 네트워크 정보를 확인합니다.	레이블이 있는 패킷이 레이블이 있는 게이트웨이와 레이블이 없는 게이트웨이를 통해 대상에 도달할 수 있도록 정적 경로를 구성합니다. 또한 네트워크의 상태를 표시합니다.	181 페이지 “Trusted Extensions에서 경로 구성 및 네트워크 정보 확인(작업 맵)”
네트워킹 문제를 해결합니다.	레이블이 있는 패킷의 네트워크 문제를 진단할 때 수행하는 단계입니다.	187 페이지 “신뢰할 수 있는 네트워크 문제 해결(작업 맵)”

신뢰할 수 있는 네트워크 데이터베이스 구성(작업 맵)

Trusted Extensions 소프트웨어에는 `tnrhtp` 및 `tnrhdb` 데이터베이스가 포함되어 있습니다. 이러한 데이터베이스는 시스템에 연결하는 원격 호스트에 대한 레이블을 제공합니다. Solaris Management Console은 이러한 데이터베이스를 관리하는 데 사용하는 GUI를 제공합니다.

다음 작업 맵에서는 보안 템플리트를 만들어서 호스트에 할당하는 작업을 설명합니다.

작업	설명	수행 방법
사이트에 사용자 정의된 보안 템플리트가 필요한지 여부를 확인합니다.	사이트의 보안 요구 사항에 대해 기존 템플리트를 평가합니다.	169 페이지 "사이트별 보안 템플리트가 필요한지 여부를 확인하는 방법"
Solaris Management Console에서 Security Templates(보안 템플리트) 도구에 액세스합니다.	신뢰할 수 있는 네트워크 데이터베이스를 수정하는 도구에 액세스합니다.	170 페이지 "신뢰할 수 있는 네트워킹 도구를 여는 방법"
보안 템플리트를 수정합니다.	신뢰할 수 있는 네트워크 데이터베이스를 수정하여 신뢰할 수 있는 네트워크의 보안 속성 정의를 수정합니다.	170 페이지 "원격 호스트 템플리트를 작성하는 방법"
	DOI를 1 이외의 값으로 변경합니다.	예 13–1
	다른 호스트 간의 통신을 단일 레이블로 제한하는 레이블이 있는 호스트에 대한 보안 템플리트를 만듭니다.	예 13–2
	단일 레이블 게이트웨이로 작동하는 레이블이 없는 호스트에 대한 보안 템플리트를 만듭니다.	예 13–3
	레이블 범위가 제한된 호스트에 대한 보안 템플리트를 만듭니다.	예 13–4
	레이블 범위에서 고유의 레이블 세트를 지정하는 호스트에 대한 보안 템플리트를 만듭니다.	예 13–5
	레이블이 없는 시스템 및 네트워크에 대한 보안 템플리트를 만듭니다.	예 13–6
	두 개발자 시스템에 대한 보안 템플리트를 만듭니다.	예 13–7
알려진 네트워크에 호스트를 추가합니다.	신뢰할 수 있는 네트워크에 시스템과 네트워크를 추가합니다.	175 페이지 "시스템의 알려진 네트워크에 호스트를 추가하는 방법"

작업	설명	수행 방법
와일드카드 항목을 사용하여 원격 호스트 액세스를 제공합니다.	각 호스트를 동일한 보안 템플리트에 간접적으로 지정하여 IP 주소 범위 내에 있는 호스트가 시스템과 통신할 수 있도록 합니다.	예 13–8 예 13–9 예 13–10
tnrhdb 파일에서 admin_low 와일드카드 항목을 변경합니다.	와일드카드 항목을 호스트가 부트 시 연결하는 특정 주소로 바꾸어 보안을 강화합니다.	177 페이지 "신뢰할 수 있는 네트워크에서 연결할 수 있는 호스트를 제한하는 방법"
	와일드카드 항목을 레이블이 있는 호스트의 네트워크(기본값)로 바꾸어 보안을 강화합니다.	예 13–11
호스트 주소 0.0.0.0에 대한 항목을 만듭니다.	원격 클라이언트의 초기 연결을 수락하도록 Sun Ray 서버를 구성합니다.	예 13–13
보안 템플리트를 지정합니다.	템플리트를 IP 주소나 연속 IP 주소 목록과 연결합니다.	176 페이지 "호스트 또는 호스트 그룹에 보안 템플리트를 지정하는 방법"

▼ 사이트별 보안 템플리트가 필요한지 여부를 확인하는 방법

시작하기 전에 전역 영역에서 보안 관리자 역할을 가진 사용자여야 합니다.

1. **Trusted Extensions 템플리트를 익힙니다.**

   로컬 호스트의 tnrhtp 파일을 읽습니다. 파일의 주석을 활용할 수 있습니다. Solaris Management Console에서 Security Templates(보안 템플리트) 도구의 보안 속성 값을 볼 수도 있습니다.

   - 기본 템플리트는 모든 설치에서 동일합니다. 각 템플리트에 대한 레이블 범위는 ADMIN_LOW ~ ADMIN_HIGH입니다.
   - cipso 템플리트는 DOI가 1인 CIPSO 호스트 유형을 정의합니다. 템플리트에 대한 레이블 범위는 ADMIN_LOW ~ADMIN_HIGH입니다.
   - admin_low 템플리트는 DOI가 1인 레이블이 없는 호스트를 정의합니다. 템플리트의 기본 레이블은 ADMIN_LOW입니다. 템플리트에 대한 레이블 범위는 ADMIN_LOW ~ADMIN_HIGH입니다. 기본 구성에서는 0.0.0.0 주소가 이 템플리트에 지정됩니다. 따라서 CIPSO가 아닌 호스트는 모두 ADMIN_LOW 보안 레이블에서 작동하는 호스트로 처리됩니다.

2. **기본 템플리트를 유지합니다.**

   지원을 위해 기본 템플리트를 삭제하거나 수정하지 마십시오. 이러한 기본 템플리트가 지정된 호스트는 변경할 수 있습니다. 예는 177 페이지 "신뢰할 수 있는 네트워크에서 연결할 수 있는 호스트를 제한하는 방법"을 참조하십시오.

3 **다음과 같은 작업을 수행하려는 경우 새 템플리트를 만듭니다.**

- 호스트 또는 호스트 그룹의 레이블 범위를 제한합니다.
- 단일 레이블 호스트를 만듭니다.
- 일부 고유 레이블을 인식하는 호스트를 만듭니다.
- 1 이외의 다른 DOI를 사용합니다.
- 레이블이 없는 호스트에 대해 `ADMIN_LOW` 이외의 기본 레이블이 필요합니다.

예는 170 페이지 "원격 호스트 템플리트를 작성하는 방법"을 참조하십시오.

▼ 신뢰할 수 있는 네트워킹 도구를 여는 방법

시작하기 전에 전역 영역에서 네트워크 보안을 수정할 수 있는 역할을 가진 사용자여야 합니다. 예를 들어, Information Security 또는 Network Security 권한 프로파일이 지정된 역할은 보안 설정을 수정할 수 있습니다. 보안 관리자 역할에는 이러한 프로파일이 포함됩니다.

LDAP 도구 상자를 사용하려면 **Trusted Extensions Configuration Guide**의 "Configuring the Solaris Management Console for LDAP (Task Map)"을 완료해야 합니다.

1 **Solaris Management Console을 시작합니다.**

자세한 내용은 **Trusted Extensions Configuration Guide**의 "Initialize the Solaris Management Console Server in Trusted Extensions"를 참조하십시오.

2 **적절한 도구를 사용합니다.**

- 템플리트를 수정하려면 Security Templates(보안 템플리트) 도구를 사용합니다.

  현재 정의된 모든 템플리트가 오른쪽 창에 표시됩니다. 템플리트를 선택하거나 만들 때 왼쪽 창에서 온라인 도움말을 사용할 수 있습니다.
- 호스트를 템플리트에 지정하려면 Security Templates(보안 템플리트) 도구를 사용합니다.
- 템플리트에 지정할 수 있는 호스트를 만들려면 Computers and Networks(컴퓨터 및 네트워크) 도구를 사용합니다.
- 영역에 레이블을 지정하려면 Trusted Network Zones(신뢰할 수 있는 네트워크 영역) 도구를 사용합니다. Trusted Extensions의 영역에 대한 자세한 내용은 10 장, "Trusted Extensions에서 영역 관리(작업)"를 참조하십시오.

▼ 원격 호스트 템플리트를 작성하는 방법

시작하기 전에 전역 영역에서 네트워크 보안을 수정할 수 있는 역할을 가진 사용자여야 합니다. 예를 들어, Information Security 또는 Network Security 권한 프로파일이 지정된 역할은 보안 설정을 수정할 수 있습니다. 보안 관리자 역할에는 이러한 프로파일이 포함됩니다.

1. **Solaris Management Console에서 Security Templates(보안 템플리트) 도구로 이동합니다.**
   단계는 170 페이지 "신뢰할 수 있는 네트워킹 도구를 여는 방법"을 참조하십시오.

2. **Computers and Networks(컴퓨터 및 네트워크)에서 Security Templates(보안 템플리트)를 두 번 누릅니다.**
   기존 템플리트가 View(보기) 창에 표시됩니다. 이러한 템플리트는 이 시스템이 연결할 수 있는 호스트에 대한 보안 속성을 설명합니다. 이러한 호스트에는 Trusted Extensions를 실행하는 CIPSO 호스트 및 레이블이 없는 호스트가 포함됩니다.

3. **`cipso` 템플리트를 검사합니다.**
   이 템플리트가 이미 지정된 호스트와 네트워크를 확인합니다.

4. **`admin_low` 템플리트를 검사합니다.**
   이 템플리트가 이미 지정된 호스트와 네트워크를 확인합니다.

5. **템플리트를 만듭니다.**
   제공된 템플리트가 이 시스템과 통신할 수 있는 호스트를 충분히 설명하지 않는 경우 Action(작업) 메뉴에서 Add Template(템플리트 추가)를 선택합니다.

   자세한 내용은 온라인 도움말을 참조하십시오. 호스트를 템플리트에 지정하기 전에 사이트에 필요한 모든 템플리트를 만듭니다.

6. **(옵션) 기본 템플리트가 아닌 기존 템플리트를 수정합니다.**
   템플리트를 두 번 누르고 온라인 도움말을 참조합니다. 지정된 호스트나 네트워크를 변경할 수 있습니다.

예 13–1 다른 DOI 값으로 보안 템플리트 만들기

이 예에서 보안 관리자의 네트워크에는 값이 1이 아닌 DOI가 있습니다. 처음에 시스템을 구성한 팀에서 **Trusted Extensions Configuration Guide**의 "Configure the Domain of Interpretation"을 완료했습니다.

먼저 보안 관리자는 `/etc/system` 파일에서 DOI의 값을 확인합니다.

```
# grep doi /etc/system
set default_doi = 4
```

그런 다음 Security Templates(보안 템플리트) 도구에서 관리자가 만드는 모든 템플리트에 대해 `doi`의 값을 `4`로 설정합니다. 예 13–2에 설명된 단일 레이블 시스템의 경우 보안 관리자는 다음 템플리트를 만듭니다.

```
template: CIPSO_PUBLIC
host_type: CIPSO
doi: 4
min_sl: PUBLIC
max_sl: PUBLIC
```

예 13–2 단일 레이블을 가진 보안 템플리트 만들기

이 예에서 보안 관리자는 단일 레이블인 PUBLIC에서만 패킷을 전달할 수 있는 게이트웨이를 만들려고 합니다. 관리자가 Solaris Management Console에서 Security Templates(보안 템플리트) 도구로 템플리트를 만들어 게이트웨이 호스트를 템플리트에 지정합니다.

먼저 게이트웨이 호스트와 IP 주소를 Computers and Networks(컴퓨터 및 네트워크) 도구에 추가합니다.

```
gateway-1
192.168.131.75
```

그런 다음 Security Templates(보안 템플리트) 도구에서 템플리트를 만듭니다. 다음은 템플리트의 값입니다.

```
template: CIPSO_PUBLIC
host_type: CIPSO
doi: 1
min_sl: PUBLIC
max_sl: PUBLIC
```

도구는 PUBLIC에 대한 16진수 값인 0X0002-08-08을 제공합니다.

마지막으로 gateway-1 호스트가 해당 이름과 IP 주소로 템플리트에 지정됩니다.

```
gateway-1
192.168.131.75
```

로컬 호스트에서 tnrhtp 항목은 다음과 비슷합니다.

```
cipso_public:host_type=cipso;doi=1;min_sl=0X0002-08-08;max_sl=0X0002-08-08;
```

로컬 호스트에서 tnrhdb 항목은 다음과 비슷합니다.

```
# gateway-1
192.168.131.75:cipso_public
```

예 13–3 레이블이 없는 라우터에 대한 보안 템플리트 만들기

라우터에서 명시적으로 레이블을 지원하지 않더라도 모든 IP 라우터는 CIPSO 레이블로 메시지를 전달할 수 있습니다. 이러한 레이블이 없는 라우터에는 대개 라우터 관리를 위한 라우터 연결을 처리해야 하는 레벨을 정의하기 위한 기본 레이블이 필요합니다. 이 예에서 보안 관리자는 어느 레이블에서나 트래픽을 전달할 수 있는 라우터를 만들지만, 라우터와의 모든 직접 통신은 기본 레이블인 PUBLIC에서 처리됩니다.

Solaris Management Console에서 관리자는 템플리트를 만들고 게이트웨이 호스트를 템플리트에 지정합니다.

먼저 라우터와 해당 IP 주소를 Computers and Networks(컴퓨터 및 네트워크) 도구에 추가합니다.

```
router-1
192.168.131.82
```

그런 다음 Security Templates(보안 템플리트) 도구에서 템플리트를 만듭니다. 다음 값이 템플리트에 있습니다.

```
Template Name: UNL_PUBLIC
Host Type: UNLABELED
DOI: 1
Default Label: PUBLIC
Minimum Label: ADMIN_LOW
Maximum Label: ADMIN_HIGH
```

도구에서 레이블에 대한 16진수 값을 제공합니다.

마지막으로 `router-1` 라우터가 해당 이름과 IP 주소로 템플리트에 지정됩니다.

```
router-1
192.168.131.82
```

예 13–4 제한된 레이블 범위를 가진 보안 템플리트 만들기

이 예에서 보안 관리자는 패킷을 좁은 레이블 범위로 제한하는 게이트웨이를 만들려고 합니다. Solaris Management Console에서 관리자는 템플리트를 만들고 게이트웨이 호스트를 템플리트에 지정합니다.

먼저 호스트와 해당 IP 주소를 Computers and Networks(컴퓨터 및 네트워크) 도구에 추가합니다.

```
gateway-ir
192.168.131.78
```

그런 다음 Security Templates(보안 템플리트) 도구에서 템플리트를 만듭니다. 다음 값이 템플리트에 있습니다.

```
Template Name: CIPSO_IUO_RSTRCT
Host Type: CIPSO
DOI: 1
Minimum Label: CONFIDENTIAL : INTERNAL USE ONLY
Maximum Label: CONFIDENTIAL : RESTRICTED
```

도구에서 레이블에 대한 16진수 값을 제공합니다.

마지막으로 `gateway-ir` 게이트웨이가 해당 이름과 IP 주소로 템플리트에 지정됩니다.

```
gateway-ir
192.168.131.78
```

예 13–5 보안 레이블 세트를 가진 보안 템플리트 만들기

이 예에서 보안 관리자는 두 레이블만 인식하는 보안 템플리트를 만들려고 합니다. Solaris Management Console에서 관리자는 템플리트를 만들고 게이트웨이 호스트를 템플리트에 지정합니다.

먼저 이 템플리트를 사용할 각 호스트 및 IP 주소를 Computers and Networks(컴퓨터 및 네트워크) 도구에 추가합니다.

```
host-slset1
192.168.132.21

host-slset2
192.168.132.22

host-slset3
192.168.132.23

host-slset4
192.168.132.24
```

그런 다음 Security Templates(보안 템플리트) 도구에서 템플리트를 만듭니다. 다음 값이 템플리트에 있습니다.

```
Template Name: CIPSO_PUB_RSTRCT
Host Type: CIPSO
DOI: 1
Minimum Label: PUBLIC
Maximum Label: CONFIDENTIAL : RESTRICTED
SL Set: PUBLIC, CONFIDENTIAL : RESTRICTED
```

도구에서 레이블에 대한 16진수 값을 제공합니다.

마지막으로 와일드카드 버튼 및 접두어를 사용하여 IP 주소 범위가 템플리트에 지정됩니다.

```
192.168.132.0/17
```

예 13–6 PUBLIC 레이블에서 레이블이 없는 템플리트 만들기

이 예에서 보안 관리자는 Oracle Solaris 시스템의 하위 네트워크가 신뢰할 수 있는 네트워크에서 PUBLIC 레이블을 가지도록 허용합니다. 템플리트는 다음 값을 가집니다.

```
Template Name: public
Host Type: Unlabeled
Default Label: Public
Minimum Label: Public
Maximum Label: Public
DOI: 1

Wildcard Entry: 10.10.0.0
Prefix: 16
```

10.10.0.0 하위 네트워크의 모든 시스템은 PUBLIC 레이블에서 처리됩니다.

예 13–7 개발자에 대한 레이블이 있는 템플리트 만들기

이 예에서 보안 관리자는 SANDBOX 템플리트를 만듭니다. 이 템플리트는 신뢰할 수 있는 소프트웨어의 개발자가 사용하는 시스템에 지정됩니다. 이 템플리트가 지정된 두 시스템은 레이블이 있는 프로그램을 만들고 테스트합니다. 그러나 SANDBOX 레이블은 네트워크의 다른 레이블과 떨어져 있으므로 이러한 테스트는 다른 레이블이 있는 시스템에 영향을 주지 않습니다.

```
Template Name: cipso_sandbox
Host Type: CIPSO
Minimum Label: SANDBOX
Maximum Label: SANDBOX
DOI: 1

Hostname: DevMachine1
IP Address: 196.168.129.129

Hostname: DevMachine2
IP Address: 196.168.129.102
```

이러한 시스템을 사용하는 개발자는 SANDBOX 레이블에서 서로 통신할 수 있습니다.

▼ 시스템의 알려진 네트워크에 호스트를 추가하는 방법

Solaris Management Console의 Computers(컴퓨터) 도구는 Oracle Solaris OS의 Computers(컴퓨터) 도구와 동일합니다. 여기에서 이 절차는 사용자의 편의를 위해 제공됩니다. 호스트가 알려졌으면 호스트를 보안 템플리트에 지정합니다.

시작하기 전에 사용자는 네트워크를 관리할 수 있는 관리자여야 합니다. 예를 들어, Network Management 또는 System Administrator 권한 프로파일을 포함하는 역할이 네트워크를 관리할 수 있습니다.

1. **Solaris Management Console에서 Computers(컴퓨터) 도구로 이동합니다.**
   자세한 내용은 170 페이지 “신뢰할 수 있는 네트워킹 도구를 여는 방법”을 참조하십시오.
2. **Computers(컴퓨터) 도구에서 네트워크의 모든 컴퓨터를 보려고 하는지 확인합니다.**
3. **이 시스템이 연결할 수 있는 호스트를 추가합니다.**
   정적 라우터 및 감사 서버를 포함하여 이 시스템이 연결할 수 있는 모든 호스트를 추가해야 합니다.
   a. **Action(작업) 메뉴에서 Add Computer(컴퓨터 추가)를 선택합니다.**

b. 이름 및 IP 주소로 호스트를 식별합니다.

c. (옵션) 호스트에 대한 추가 정보를 제공합니다.

d. 호스트를 추가하려면 Apply(적용)를 누릅니다.

e. 입력이 완료되면 OK(확인)를 누릅니다.

4 이 시스템이 연결할 수 있는 호스트 그룹을 추가합니다.
온라인 도움말을 참조하여 네트워크 IP 주소로 호스트 그룹을 추가합니다.

▼ 호스트 또는 호스트 그룹에 보안 템플리트를 지정하는 방법

시작하기 전에 전역 영역에서 보안 관리자 역할을 가진 사용자여야 합니다.

템플리트에 지정하려고 하는 모든 호스트는 Computers and Networks(컴퓨터 및 네트워크) 도구에 있어야 합니다. 자세한 내용은 175 페이지 "시스템의 알려진 네트워크에 호스트를 추가하는 방법"을 참조하십시오.

1 Solaris Management Console에서 Security Templates(보안 템플리트) 도구로 이동합니다.
자세한 내용은 170 페이지 "신뢰할 수 있는 네트워킹 도구를 여는 방법"을 참조하십시오.

2 적절한 템플리트 이름을 두 번 누릅니다.

3 Hosts Assigned to Template(템플리트에 지정된 호스트) 탭을 누릅니다.

4 단일 호스트에 템플리트를 지정하려면 다음을 수행합니다.

a. Hostname(호스트 이름) 필드에 호스트의 이름을 입력합니다.

b. IP Address(IP 주소) 필드에 호스트의 주소를 입력합니다.

c. 추가 버튼을 누릅니다.

d. 변경 사항을 저장하려면 OK(확인)를 누릅니다.

5 연속 주소를 사용하는 호스트 그룹에 템플리트를 지정하려면 다음을 수행합니다.

a. Wildcard(와일드카드)를 누릅니다.

b. IP Address(IP 주소) 필드에 IP 주소를 입력합니다.

c. **Prefix(접두어) 필드에 연속 주소의 그룹을 설명하는 접두어를 입력합니다.**

d. **추가 버튼을 누릅니다.**

e. **변경 사항을 저장하려면 OK(확인)를 누릅니다.**

예 13–8 와일드카드 항목으로 IPv4 네트워크 추가

다음 예에서 보안 관리자는 여러 IPv4 하위 네트워크를 동일한 보안 템플리트에 지정합니다. Hosts Assigned to Template(템플리트에 지정된 호스트) 탭에서 관리자는 다음 와일드카드 항목을 추가합니다.

```
IP Address: 192.168.113.0
IP address: 192.168.75.0
```

예 13–9 와일드카드 항목으로 IPv4 호스트 목록 추가

이 예에서 보안 관리자는 옥테트 경계를 따르지 않는 연속 IPv4 주소를 동일한 보안 템플리트에 지정합니다. Hosts Assigned to Template(템플리트에 지정된 호스트) 탭에서 관리자는 다음 와일드카드 항목을 추가합니다.

```
IP Address: 192.168.113.100
Prefix Length: 25
```

이 와일드카드 항목은 `192.168.113.0` ~ `192.168.113.127`의 주소 범위를 포함합니다. 주소에는 `192.168.113.100`이 포함됩니다.

예 13–10 와일드카드 항목으로 IPv6 호스트 목록 추가

다음 예에서 보안 관리자는 연속 IPv6 주소를 동일한 보안 템플리트에 지정합니다. Hosts Assigned to Template(템플리트에 지정된 호스트) 탭에서 관리자는 다음 와일드카드 항목을 추가합니다.

```
IP Address: 2001:a08:3903:200::0
Prefix Length: 56
```

이 와일드카드 항목은 `2001:a08:3903:200::0` ~ `2001:a08:3903:2ff:ffff:ffff:ffff:ffff`의 주소 범위를 포함합니다. 주소에는 `2001:a08:3903:201:20e:cff:fe08:58c`가 포함됩니다.

▼ 신뢰할 수 있는 네트워크에서 연결할 수 있는 호스트를 제한하는 방법

다음은 임의의 레이블이 없는 호스트가 레이블이 있는 호스트에 연결하지 못하게 하는 절차입니다. Trusted Extensions가 설치되면 이 기본 템플리트는 네트워크의 모든 호스트를 정의합니다. 이 절차를 사용하여 레이블이 없는 특정 호스트를 열거합니다.

각 시스템의 로컬 tnrhdb 파일은 부트 시 네트워크에 연결하는 데 사용됩니다. 기본적으로 CIPSO 템플리트가 제공되지 않은 모든 호스트는 admin_low 템플리트로 정의됩니다. 이 템플리트는 다르게 정의되지 않은 모든 시스템(0.0.0.0)을 기본 레이블 admin_low의 레이블이 없는 시스템이 되도록 지정합니다.

주의 – 기본 admin_low 템플리트는 Trusted Extensions 네트워크에서 보안상 위험할 수 있습니다. 사이트 보안에 강력한 보호가 요구되는 경우 보안 관리자는 시스템이 설치된 후 0.0.0.0 와일드카드 항목을 제거할 수 있습니다. 항목은 시스템이 부트 중 연결하는 모든 호스트에 대한 항목으로 바뀌어야 합니다.

예를 들어, 0.0.0.0 와일드카드 항목이 제거된 후 DNS 서버, 홈 디렉토리 서버, 감사 서버, 브로드캐스트/멀티캐스트 주소 및 라우터가 로컬 tnrhdb 파일에 있어야 합니다.

응용 프로그램에서 처음으로 호스트 주소 0.0.0.0의 클라이언트를 인식할 경우 0.0.0.0/32:admin_low 호스트 항목을 tnrhdb 데이터베이스에 추가해야 합니다. 예를 들어 잠재적 Sun Ray 클라이언트에서 초기 연결 요청을 받으려면 Sun Ray 서버에 다음 항목을 포함해야 합니다. 그러면 서버에서 클라이언트를 인식할 때 클라이언트에 IP 주소가 제공되고 CIPSO 클라이언트로 연결됩니다.

시작하기 전에 전역 영역에서 보안 관리자 역할을 가진 사용자여야 합니다.

부트 시 연결해야 하는 모든 호스트가 Computers and Networks(컴퓨터 및 네트워크) 도구에 있어야 합니다.

1 **Solaris Management Console에서 Files(파일) 범위에 있는 Security Templates(보안 템플리트) 도구로 이동합니다.**

Files(파일) 범위는 부트 중 시스템을 보호합니다. Security Templates(보안 템플리트) 도구에 액세스하려면 170 페이지 “신뢰할 수 있는 네트워킹 도구를 여는 방법”을 참조하십시오.

2 **admin_low 템플리트에 지정된 호스트를 수정합니다.**

a. **admin_low 템플리트를 두 번 누릅니다.**

추가된 모든 호스트는 부트 중 ADMIN_LOW 레이블에서 연결할 수 있습니다.

b. **Hosts Assigned to Template(템플리트에 지정된 호스트) 탭을 누릅니다.**

추가된 모든 호스트는 부트 중 ADMIN_LOW 레이블에서 연결할 수 있습니다.

c. **부트 시 연결해야 하는 각 레이블이 없는 호스트를 추가합니다.**

자세한 내용은 176 페이지 “호스트 또는 호스트 그룹에 보안 템플리트를 지정하는 방법”을 참조하십시오.

Trusted Extensions를 실행하지 않는 모든 온-링크 라우터를 포함합니다. 이 라우터를 통해 이 호스트가 통신해야 합니다.

d. 부트 시 연결해야 하는 호스트의 범위를 추가합니다.

e. `0.0.0.0` 항목을 제거합니다.

3 `cipso` 템플리트에 지정된 호스트를 수정합니다.

a. `cipso` 템플리트를 두 번 누릅니다.
추가된 모든 호스트는 부트 중 연결할 수 있습니다.

b. Hosts Assigned to Template(템플리트에 지정된 호스트) 탭을 누릅니다.
추가된 모든 호스트는 부트 중 `ADMIN_LOW` 레이블에서 연결할 수 있습니다.

c. 부팅 시 연결해야 하는 각 레이블이 있는 호스트를 추가합니다.
자세한 내용은 176 페이지 "호스트 또는 호스트 그룹에 보안 템플리트를 지정하는 방법"을 참조하십시오.

- LDAP 서버를 포함합니다.
- Trusted Extensions를 실행하는 모든 온-링크 라우터를 포함합니다. 이 라우터를 통해 이 호스트가 통신해야 합니다.
- 모든 네트워크 인터페이스가 템플리트에 지정되었는지 확인합니다.
- 브로드캐스트 주소를 포함합니다.

d. 부트 시 연결해야 하는 호스트의 범위를 추가합니다.

4 호스트 지정에서 시스템 부팅을 허용하는지 확인합니다.

예 13–11 0.0.0.0 `tnrhdb` 항목의 레이블 변경

이 예에서 보안 관리자는 공용 게이트웨이 시스템을 만듭니다. 관리자는 `admin_low` 템플리트에서 `0.0.0.0` 항목을 제거하고 레이블이 없는 `public` 템플리트에 항목을 지정합니다. 그러면 시스템은 `tnrhdb` 파일에 나열되지 않은 모든 시스템을 `public` 보안 템플리트의 보안 속성을 가진 레이블이 없는 시스템으로 인식합니다.

다음은 공용 게이트웨이용으로 특별히 만들어진 레이블이 없는 템플리트를 설명합니다.

```
Template Name: public
Host Type: Unlabeled
Default Label: Public
Minimum Label: Public
Maximum Label: Public
DOI: 1
```

예 13–12 tnrhdb 데이터베이스에서 부트 중 연결할 컴퓨터 열거

다음 예는 두 네트워크 인터페이스를 가진 LDAP 클라이언트에 대한 항목이 있는 로컬 tnrhdb 데이터베이스를 나타냅니다. 클라이언트는 다른 네트워크 및 라우터와 통신합니다.

```
127.0.0.1:cipso             Loopback address
192.168.112.111:cipso       Interface 1 of this host
192.168.113.111:cipso       Interface 2 of this host
10.6.6.2:cipso              LDAP server
192.168.113.6:cipso         Audit server
192.168.112.255:cipso       Subnet broadcast address
192.168.113.255:cipso       Subnet broadcast address
192.168.113.1:cipso         Router
192.168.117.0:cipso         Another Trusted Extensions network
192.168.112.12:public       Specific network router
192.168.113.12:public       Specific network router
224.0.0.2:public            Multicast address
255.255.255.255:admin_low       Broadcast address
```

예 13–13 호스트 주소 0.0.0.0을 유효한 tnrhdb 항목으로 만들기

이 예에서 보안 관리자는 Sun Ray 서버가 잠재적 클라이언트의 초기 연결 요청을 받아들이도록 구성합니다. 서버는 전용 토폴로지와 기본값을 사용합니다.

```
# utadm -a bge0
```

먼저 관리자가 Solaris Management Console 도메인 이름을 확인합니다.

```
SMCserver # /usr/sadm/bin/dtsetup scopes
Getting list of managable scopes...
Scope 1 file:/machine1.ExampleCo.COM/machine1.ExampleCo.COM
```

그런 다음 관리자는 클라이언트 초기 연결에 대한 항목을 Sun Ray 서버의 tnrhdb 데이터베이스에 추가합니다. 관리자가 테스트 중이므로 기본 와일드카드 주소는 여전히 모든 알 수 없는 주소에 사용됩니다.

```
SunRayServer # /usr/sadm/bin/smtnrhdb \
add -D file:/machine1.ExampleCo.COM/machine1.ExampleCo.COM \
-- -w 0.0.0.0 -p 32 -n admin_low
Authenticating as user: root

Please enter a string value for: password ::
... from machine1.ExampleCo.COM was successful.
```

이 명령 후 tnhrdb 데이터베이스는 다음과 비슷합니다. smtnrhdb 명령의 결과가 강조 표시되어 있습니다.

```
## tnrhdb database
## Sun Ray server address
       192.168.128.1:cipso
```

```
## Sun Ray client addresses on 192.168.128 network
       192.168.128.0/24:admin_low
## Initial address for new clients
       0.0.0.0/32:admin_low
## Default wildcard address
0.0.0.0:admin_low
     Other addresses to be contacted at boot
```

```
# tnchkdb -h /etc/security/tsol/tnrhdb
```

이 테스트 단계가 성공한 후 관리자는 기본 와일드카드 주소를 제거하여 구성을 더욱 안전하게 만들고 `tnrhdb` 데이터베이스의 구문을 검사한 후 다시 테스트합니다. 최종 `tnhrdb` 데이터베이스는 다음과 비슷합니다.

```
## tnrhdb database
## Sun Ray server address
       192.168.128.1:cipso
## Sun Ray client addresses on 192.168.128 network
       192.168.128.0/24:admin_low
## Initial address for new clients
       0.0.0.0/32:admin_low
## 0.0.0.0:admin_low - no other systems can enter network at admin_low
     Other addresses to be contacted at boot
```

Trusted Extensions에서 경로 구성 및 네트워크 정보 확인(작업 맵)

다음 작업 맵에서는 네트워크를 구성하고 구성을 확인하는 작업을 설명합니다.

작업	설명	수행 방법
정적 경로를 구성합니다.	호스트 간의 가장 적절한 경로를 수동으로 설명합니다.	182 페이지 "보안 속성으로 경로를 구성하는 방법"
로컬 네트워크 데이터베이스의 정확성을 확인합니다.	`tnchkdb` 명령을 사용하여 로컬 네트워크 데이터베이스의 구문 유효성을 확인합니다.	183 페이지 "신뢰할 수 있는 네트워크 데이터베이스의 구문을 확인하는 방법"
네트워크 데이터베이스 항목을 커널 캐시의 항목과 비교합니다.	`tninfo` 명령을 사용하여 커널 캐시가 최신 데이터베이스 정보로 업데이트되었는지 여부를 확인합니다.	184 페이지 "신뢰할 수 있는 네트워크 데이터베이스 정보를 커널 캐시와 비교하는 방법"
커널 캐시를 네트워크 데이터베이스와 동기화합니다.	`tnctl` 명령을 사용하여 실행 중인 시스템의 최신 네트워크 데이터베이스 정보로 커널 캐시를 업데이트합니다.	185 페이지 "커널 캐시를 신뢰할 수 있는 네트워크 데이터베이스와 동기화하는 방법"

▼ 보안 속성으로 경로를 구성하는 방법

시작하기 전에 전역 영역에서 보안 관리자 역할을 가진 사용자여야 합니다.

1. **신뢰할 수 있는 네트워크를 통한 패킷 경로에 사용하고 있는 모든 대상 호스트 및 게이트웨이를 추가합니다.**

   주소는 로컬 `/etc/hosts` 파일 또는 LDAP 서버의 해당 파일에 추가됩니다. Solaris Management Console의 Computers and Networks(컴퓨터 및 네트워크) 도구를 사용합니다. Files(파일) 범위는 `/etc/hosts` 파일을 수정합니다. LDAP 범위는 LDAP 서버의 항목을 수정합니다. 자세한 내용은 175 페이지 "시스템의 알려진 네트워크에 호스트를 추가하는 방법"을 참조하십시오.

2. **각 대상 호스트, 네트워크 및 게이트웨이를 보안 템플리트에 지정합니다.**

   주소는 로컬 `/etc/security/tsol/tnrhdb` 파일 또는 LDAP 서버의 해당 파일에 추가됩니다. Solaris Management Console의 Security Templates(보안 템플리트) 도구를 사용합니다. 자세한 내용은 176 페이지 "호스트 또는 호스트 그룹에 보안 템플리트를 지정하는 방법"을 참조하십시오.

3. **경로를 설정합니다.**

   터미널 창에서 `route add` 명령을 사용하여 경로를 지정합니다.

   첫번째 항목은 기본 경로를 설정합니다. 항목은 호스트 또는 패킷의 대상에 대해 정의된 특정 경로가 없을 때 사용할 게이트웨이의 주소로 `192.168.113.1`을 지정합니다.

   ```
   # route add default 192.168.113.1  -static
   ```

   자세한 내용은 `route`(1M) 매뉴얼 페이지를 참조하십시오.

4. **하나 이상의 네트워크 항목을 설정합니다.**

   `-secattr` 플래그를 사용하여 보안 속성을 지정합니다.

   다음 명령 목록에서 두번째 라인은 네트워크 항목을 나타냅니다. 세번째 라인은 레이블 범위가 `PUBLIC ~ CONFIDENTIAL : INTERNAL USE ONLY`인 네트워크 항목을 나타냅니다.

   ```
   # route add default 192.168.113.36
   # route add -net 192.168.102.0 gateway-101
   # route add -net 192.168.101.0 gateway-102 \
   -secattr min_sl="PUBLIC",max_sl="CONFIDENTIAL : INTERNAL USE ONLY",doi=1
   ```

5. **하나 이상의 호스트 항목을 설정합니다.**

   새로운 네번째 라인은 단일 레이블 호스트인 `gateway-pub`에 대한 호스트 항목을 나타냅니다. `gateway-pub`의 레이블 범위는 `PUBLIC ~ PUBLIC`입니다.

   ```
   # route add default 192.168.113.36
   # route add -net 192.168.102.0 gateway-101
   # route add -net 192.168.101.0 gateway-102 \
   -secattr min_sl="PUBLIC",max_sl="CONFIDENTIAL : INTERNAL USE ONLY",doi=1
   # route add -host 192.168.101.3 gateway-pub \
   -secattr min_sl="PUBLIC",max_sl="PUBLIC",doi=1
   ```

예 13–14 레이블 범위가 CONFIDENTIAL : INTERNAL USE ONLY ~ CONFIDENTIAL : RESTRICTED인 경로 추가

다음 route 명령은 192.168.115.0 및 192.168.118.39의 호스트를 경로 지정 테이블에 게이트웨이로 추가합니다. 레이블 범위는 CONFIDENTIAL : INTERNAL USE ONLY ~ CONFIDENTIAL : RESTRICTED이며, DOI는 1입니다.

```
$ route add -net 192.168.115.0 192.168.118.39 \
-secattr min_sl="CONFIDENTIAL : INTERNAL USE ONLY",max_sl="CONFIDENTIAL : RESTRICTED",doi=1
```

추가된 호스트의 결과는 netstat -rR 명령으로 표시됩니다. 다음 발췌 부분에서 기타 경로는 말줄임표(...)로 바뀌었습니다.

```
$ netstat -rRn
...
192.168.115.0        192.168.118.39        UG       0      0
        min_sl=CNF : INTERNAL USE ONLY,max_sl=CNF : RESTRICTED,DOI=1,CIPSO
...
```

▼ 신뢰할 수 있는 네트워크 데이터베이스의 구문을 확인하는 방법

tnchkdb 명령은 각 네트워크 데이터베이스의 구문이 정확한지 검사합니다. Solaris Management Console에서는 Security Templates(보안 템플리트) 도구나 Trusted Network Zones(신뢰할 수 있는 네트워크 영역) 도구를 사용할 때 이 명령을 자동으로 실행합니다. 일반적으로 이 명령을 실행하여 나중에 사용하도록 구성하는 데이터베이스 파일의 구문을 검사합니다.

시작하기 전에 전역 영역에서 네트워크 설정을 확인할 수 있는 역할을 가진 사용자여야 합니다. 보안 관리자 역할 및 시스템 관리자 역할이 이러한 설정을 확인할 수 있습니다.

- **터미널 창에서 tnchkdb 명령을 실행합니다.**

```
$ tnchkdb [-h tnrhdb-path] [-t tnrhtp-path] [-z tnzonecfg-path]
checking /etc/security/tsol/tnrhtp ...
checking /etc/security/tsol/tnrhdb ...
checking /etc/security/tsol/tnzonecfg ...
```

예 13–15 시험 네트워크 데이터베이스의 구문 테스트

이 예에서 보안 관리자는 네트워크 데이터베이스 파일의 사용 가능성을 테스트합니다. 처음에 관리자는 잘못된 옵션을 사용합니다. 확인 결과는 tnrhdb 파일에 대한 라인에 출력됩니다.

```
$ tnchkdb -h /opt/secfiles/trial.tnrhtp
checking /etc/security/tsol/tnrhtp ...
checking /opt/secfiles/trial.tnrhtp ...
```

```
line 12: Illegal name: min_sl=ADMIN_LOW;max_sl=ADMIN_HIGH
line 14: Illegal name: min_sl=ADMIN_LOW;max_sl=ADMIN_HIGH
checking /etc/security/tsol/tnzonecfg ...
```

보안 관리자가 `-t` 옵션을 사용하여 파일을 검사할 때 명령은 시험 `tnrhtp` 데이터베이스의 구문이 정확한지 확인합니다.

```
$ tnchkdb -t /opt/secfiles/trial.tnrhtp
checking /opt/secfiles/trial.tnrhtp ...
checking /etc/security/tsol/tnrhdb ...
checking /etc/security/tsol/tnzonecfg ...
```

▼ 신뢰할 수 있는 네트워크 데이터베이스 정보를 커널 캐시와 비교하는 방법

네트워크 데이터베이스에는 커널에 캐시되지 않은 정보가 포함될 수 있습니다. 이 절차에서는 정보가 동일한지 확인합니다. Solaris Management Console을 사용하여 네트워크를 업데이트하면 커널 캐시가 네트워크 데이터베이스 정보로 업데이트됩니다. `tninfo` 명령은 테스트 및 디버깅에 유용하게 사용할 수 있습니다.

시작하기 전에 전역 영역에서 네트워크 설정을 확인할 수 있는 역할을 가진 사용자여야 합니다. 보안 관리자 역할 및 시스템 관리자 역할이 이러한 설정을 확인할 수 있습니다.

- **터미널 창에서 `tninfo` 명령을 실행합니다.**
  - `tninfo -h` *hostname*은 지정된 호스트에 대한 IP 주소와 템플리트를 표시합니다.
  - `tninfo -t` *templatename*은 다음 정보를 표시합니다.

    ```
    template: template-name
    host_type: either CIPSO or UNLABELED
    doi: 1
    min_sl: minimum-label
    hex: minimum-hex-label
    max_sl: maximum-label
    hex:maximum-hex-label
    ```

  - `tninfo -m` *zone-name*은 영역의 다중 레벨 포트(MLP) 구성을 표시합니다.

예 13–16 호스트의 다중 레벨 포트 표시

이 예에서 시스템은 레이블이 있는 여러 영역으로 구성되어 있습니다. 모든 영역은 동일한 IP 주소를 공유합니다. 또한 일부 영역은 영역별 주소로 구성되어 있습니다. 이 구성에서 웹 브라우징을 위한 TCP 포트인 `8080` 포트는 공용 영역의 공유 인터페이스에서 MLP입니다. 또한 관리자는 `telnet`용 TCP 포트 `23`이 공용 영역에서 MLP가 되도록 설정했습니다. 이러한 두 MLP는 공유 인터페이스에 있으므로 전역 영역을 비롯한 다른 영역에서는 공유 인터페이스의 `8080` 및 `23` 포트에서 패킷을 받을 수 없습니다.

또한 ssh에 대한 TCP 포트인 22 포트는 공용 영역에서 영역별 MLP입니다. 공용 영역의 ssh 서비스는 주소의 레이블 범위 내에 있는 영역별 주소에서 패킷을 수신할 수 있습니다.

다음 명령은 공용 영역에 대한 MLP를 보여줍니다.

```
$ tninfo -m public
private: 22/tcp
shared:  23/tcp;8080/tcp
```

다음 명령은 전역 영역에 대한 MLP를 보여줍니다. 전역 영역은 공용 영역과 동일한 주소를 공유하므로 23 및 8080 포트는 전역 영역에서 MLP가 될 수 없습니다.

```
$ tninfo -m global
private: 111/tcp;111/udp;514/tcp;515/tcp;631/tcp;2049/tcp;
         6000-6003/tcp;38672/tcp;60770/tcp;
shared:  6000-6003/tcp
```

▼ 커널 캐시를 신뢰할 수 있는 네트워크 데이터베이스와 동기화하는 방법

커널이 신뢰할 수 있는 네트워크 데이터베이스 정보로 업데이트되지 않은 경우 커널 캐시를 업데이트할 수 있는 몇 가지 방법이 있습니다. Solaris Management Console에서는 Security Templates(보안 템플리트) 도구나 Trusted Network Zones(신뢰할 수 있는 네트워크 영역) 도구를 사용할 때 이 명령을 자동으로 실행합니다.

시작하기 전에 전역 영역에서 보안 관리자 역할을 가진 사용자여야 합니다.

- **커널 캐시를 네트워크 데이터베이스와 동기화하려면 다음 명령 중 하나를 실행합니다.**
  - **tnctl 서비스를 다시 시작합니다.**

    주의 – LDAP 서버에서 신뢰할 수 있는 네트워크 데이터베이스 정보를 가져오는 시스템에서는 이 방법을 사용하지 마십시오. 로컬 데이터베이스 정보가 LDAP 서버에서 가져온 정보를 덮어씁니다.

    ```
    $ svcadm restart  svc:/network/tnctl
    ```

    이 명령은 신뢰할 수 있는 로컬 네트워크 데이터베이스의 모든 정보를 커널로 읽어옵니다.

  - **최근에 추가된 항목에 대한 커널 캐시를 업데이트합니다.**

    ```
    $ tnctl -h hostname
    ```

    이 명령은 선택한 옵션의 정보만 커널로 읽어옵니다. 옵션에 대한 자세한 내용은 예 13–17 및 tnctl(1M) 매뉴얼 페이지를 참조하십시오.

- **tnd 서비스를 수정합니다.**

  주 – tnd 서비스는 ldap 서비스가 실행 중인 경우에만 실행됩니다.

  - **tnd 폴링 간격을 변경합니다.**

    이로 인해 커널 캐시가 업데이트되지는 않습니다. 그러나 폴링 간격을 줄여서 커널 캐시를 더 자주 업데이트할 수 있습니다. 자세한 내용은 tnd(1M) 매뉴얼 페이지의 예를 참조하십시오.

  - **tnd를 새로 고칩니다.**

    이 SMF(서비스 관리 기능) 명령은 신뢰할 수 있는 네트워크 데이터베이스에 대한 최근 변경 사항으로 커널 즉시 업데이트를 트리거합니다.

    ```
    $ svcadm refresh svc:/network/tnd
    ```

  - **SMF를 사용하여 tnd를 다시 시작합니다.**

    ```
    $ svcadm restart svc:/network/tnd
    ```

주의 – tnd 다시 시작을 위해 tnd 명령을 실행하지는 마십시오. 이 명령으로 인해 현재 진행 중인 통신이 중단될 수 있습니다.

예 13–17 최신 tnrhdb 항목으로 커널 업데이트

이 예에서 관리자는 3개의 주소를 로컬 tnrhdb 데이터베이스에 추가했습니다. 먼저 관리자는 0.0.0.0 와일드카드 항목을 제거했습니다.

```
$ tnctl -d -h 0.0.0.0:admin_low
```

그런 다음 관리자는 /etc/security/tsol/tnrhdb 데이터베이스에 있는 최종 3개 항목의 형식을 봅니다.

```
$ tail /etc/security/tsol/tnrhdb
#\:\:0:admin_low
127.0.0.1:cipso
#\:\:1:cipso
192.168.103.5:admin_low
192.168.103.0:cipso
0.0.0.0/32:admin_low
```

그런 다음 관리자는 커널 캐시를 업데이트합니다.

```
$ tnctl -h 192.168.103.5
tnctl -h 192.168.103.0
tnctl -h 0.0.0.0/32
```

마지막으로 관리자는 커널 캐시가 업데이트되었는지 확인합니다. 첫번째 항목에 대한 출력은 다음과 유사합니다.

```
$ tninfo -h 192.168.103.5
IP Address: 192.168.103.5
Template: admin_low
```

예 13–18 커널에서 네트워크 정보 업데이트

이 예에서 관리자는 신뢰할 수 있는 네트워크를 공용 인쇄 서버로 업데이트한 다음 커널 설정이 올바른지 확인합니다.

```
$ tnctl -h public-print-server
$ tninfo -h public-print-server
IP Address: 192.168.103.55
Template: PublicOnly
$ tninfo -t PublicOnly
================================
Remote Host Template Table Entries
--------------------------------
template: PublicOnly
host_type: CIPSO
doi: 1
min_sl: PUBLIC
hex: 0x0002-08-08
max_sl: PUBLIC
hex: 0x0002-08-08
```

신뢰할 수 있는 네트워크 문제 해결(작업 맵)

다음 작업 맵에서는 네트워크 디버깅 작업을 설명합니다.

작업	설명	수행 방법
두 호스트가 통신할 수 없는 이유를 확인합니다.	단일 시스템의 인터페이스가 작동 중인지 확인합니다.	187 페이지 “호스트의 인터페이스가 작동 중인지 확인하는 방법”
	두 호스트가 서로 통신할 수 없을 때 디버깅 도구를 사용합니다.	188 페이지 “Trusted Extensions 네트워크를 디버깅하는 방법”
LDAP 클라이언트가 LDAP 서버에 연결할 수 없는 이유를 확인합니다.	LDAP 서버와 클라이언트 간의 연결 끊김 문제를 해결합니다.	191 페이지 “LDAP 서버에 대한 클라이언트 연결을 디버깅하는 방법”

▼ 호스트의 인터페이스가 작동 중인지 확인하는 방법

시스템이 다른 호스트와 예상한 대로 통신하지 않을 경우 이 절차를 사용합니다.

시작하기 전에 전역 영역에서 네트워크 설정을 확인할 수 있는 역할을 가진 사용자여야 합니다. 보안 관리자 역할 및 시스템 관리자 역할이 이러한 설정을 확인할 수 있습니다.

1 **시스템의 네트워크 인터페이스가 작동 중인지 확인합니다.**

다음 출력은 시스템에 2개의 네트워크 인터페이스(hme0 및 hme0:3)가 있음을 나타냅니다. 두 인터페이스 모두 작동하고 있지 않습니다.

```
# ifconfig -a
...
hme0: flags=1000843<BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
         inet 192.168.0.11 netmask ffffff00 broadcast 192.168.0.255
hme0:3 flags=1000843<BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
         inet 192.168.0.12 netmask ffffff00 broadcast 192.168.0.255
```

2 **인터페이스가 작동 중이 아닐 경우 인터페이스를 호출한 다음 작동 중인지 확인합니다.**

다음 출력은 두 인터페이스가 모두 작동 중임을 나타냅니다.

```
# ifconfig hme0 up
# ifconfig -a
...
hme0: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,...
hme0:3 flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,..
```

▼ Trusted Extensions 네트워크를 디버깅하는 방법

통신 중이 아닌 두 호스트를 디버깅하려면 Trusted Extensions 및 Solaris 디버깅 도구를 사용합니다. 예를 들어, snoop 및 netstat와 같은 Oracle Solaris 네트워크 디버깅 명령을 사용할 수 있습니다. 자세한 내용은 snoop(1M) 및 netstat(1M) 매뉴얼 페이지를 참조하십시오. Trusted Extensions에 대한 특정 명령은 표 2–4를 참조하십시오.

- 레이블이 있는 영역에 대한 연결 문제는 122 페이지 “영역 관리(작업 맵)”를 참조하십시오.
- NFS 마운트 디버깅은 149 페이지 “Trusted Extensions에서 마운트 실패 문제를 해결하는 방법”을 참조하십시오.
- LDAP 통신 디버깅은 191 페이지 “LDAP 서버에 대한 클라이언트 연결을 디버깅하는 방법”을 참조하십시오.

시작하기 전에 전역 영역에서 네트워크 설정을 확인할 수 있는 역할을 가진 사용자여야 합니다. 보안 관리자 역할 또는 시스템 관리자 역할이 이러한 설정을 확인할 수 있습니다.

1 **tnd 데몬 문제를 해결하려면 폴링 간격을 변경하고 디버깅 정보를 수집합니다.**

주 – tnd 서비스는 ldap 서비스가 실행 중인 경우에만 실행됩니다.

자세한 내용은 tnd(1M) 매뉴얼 페이지를 참조하십시오.

2 통신할 수 없는 호스트가 동일한 이름 지정 서비스를 사용 중인지 확인합니다.

a. 각 호스트에서 `nsswitch.conf` 파일을 확인합니다.

i. `nsswitch.conf` 파일에서 Trusted Extensions 데이터베이스에 대한 값을 확인합니다.

예를 들어, LDAP을 사용하여 네트워크를 관리하는 사이트에서 항목은 다음과 유사합니다.

```
# Trusted Extensions
tnrhtp: files ldap
tnrhdb: files ldap
```

ii. 값이 다를 경우 `nsswitch.conf` 파일을 수정합니다.

이러한 항목을 수정하려면 시스템 관리자가 이름 서비스 스위치 작업을 사용합니다. 자세한 내용은 54 페이지 “Trusted Extensions에서 CDE 관리 작업을 시작하는 방법”을 참조하십시오. 이 작업은 필요한 DAC 및 MAC 파일 권한을 유지합니다.

b. LDAP 이름 지정 서비스가 구성되었는지 확인합니다.

```
$ ldaplist -l
```

c. 두 호스트가 모두 LDAP 이름 지정 서비스에 있는지 확인합니다.

```
$ ldaplist -l hosts | grep hostname
```

3 각 호스트가 올바르게 정의되었는지 확인합니다.

a. Solaris Management Console을 사용하여 정의를 확인합니다.

- Security Templates(보안 템플리트) 도구에서 각 호스트가 다른 호스트의 보안 템플리트와 호환되는 보안 템플리트에 지정되었는지 확인합니다.
- 레이블이 없는 시스템의 경우 기본 레이블 지정이 올바른지 확인합니다.
- Trusted Network Zones(신뢰할 수 있는 네트워크 영역) 도구에서 다중 레벨 포트(MLP)가 올바르게 구성되었는지 확인합니다.

b. 명령줄을 사용하여 커널의 네트워크 정보가 최신 정보인지 확인합니다.

각 호스트 커널 캐시의 지정이 네트워크의 지정 및 다른 호스트의 지정과 일치하는지 확인합니다.

소스, 대상 및 게이트웨이 호스트에 대한 보안 정보를 얻으려면 `tninfo` 명령을 사용합니다.

- **해당 호스트에 대한 IP 주소 및 지정된 보안 템플리트를 표시합니다.**

```
$ tninfo -h hostname
IP Address: IP-address
Template: template-name
```

- **템플리트 정의를 표시합니다.**

  ```
  $ tninfo -t template-name
  template: template-name
  host_type: one of CIPSO or UNLABELED
  doi: 1
  min_sl: minimum-label
  hex: minimum-hex-label
  max_sl: maximum-label
  hex: maximum-hex-label
  ```

- **영역에 대한 MLP를 표시합니다.**

  ```
  $ tninfo -m zone-name
  private: ports-that-are-specific-to-this-zone-only
  shared: ports-that-the-zone-shares-with-other-zones
  ```

4 잘못된 정보를 수정합니다.

- 네트워크 보안 정보를 변경하거나 확인하려면 Solaris Management Console 도구를 사용합니다. 자세한 내용은 170 페이지 “신뢰할 수 있는 네트워킹 도구를 여는 방법”을 참조하십시오.
- 커널 캐시를 업데이트하려면 정보가 오래된 호스트에서 `tnctl` 서비스를 다시 시작합니다. 이 프로세스가 완료될 때까지 기다립니다. 그런 다음 `tnd` 서비스를 새로 고칩니다. 새로 고침에 실패할 경우 `tnd` 서비스를 다시 시작해 봅니다. 자세한 내용은 185 페이지 “커널 캐시를 신뢰할 수 있는 네트워크 데이터베이스와 동기화하는 방법”을 참조하십시오.

주 – `tnd` 서비스는 `ldap` 서비스가 실행 중인 경우에만 실행됩니다.

재부트하면 커널 캐시가 지워집니다. 부팅 시 캐시는 데이터베이스 정보로 채워집니다. `nsswitch.conf` 파일은 커널을 채우는 데 로컬 데이터베이스나 LDAP 데이터베이스가 사용되는지 결정합니다.

5 전송 정보를 수집하면 디버깅에 도움이 됩니다.

- **경로 지정 구성을 확인합니다.**

  `route` 명령에 대한 `get` 하위 명령을 사용합니다.

  ```
  $ route get [ip] -secattr sl=label,doi=integer
  ```

  자세한 내용은 `route(1M)` 매뉴얼 페이지를 참조하십시오.

- **패킷의 레이블 정보를 봅니다.**

  `snoop -v` 명령을 사용합니다.

  `-v` 옵션은 레이블 정보를 포함한 패킷 헤더의 세부 사항을 표시합니다. 이 명령은 많은 세부 사항을 제공하므로 명령이 검사하는 패킷을 제한하는 것이 좋습니다. 자세한 내용은 `snoop(1M)` 매뉴얼 페이지를 참조하십시오.

- **경로 지정 테이블 항목 및 소켓의 보안 속성을 봅니다.**

  `netstat -a|-r` 명령과 함께 `-R` 옵션을 사용합니다.

  `-aR` 옵션은 소켓에 대한 확장 보안 속성을 표시합니다. `-rR` 옵션은 경로 지정 테이블 항목을 표시합니다. 자세한 내용은 `netstat(1M)` 매뉴얼 페이지를 참조하십시오.

▼ LDAP 서버에 대한 클라이언트 연결을 디버깅하는 방법

LDAP 서버에서 클라이언트 항목을 잘못 구성하면 클라이언트가 서버와 통신하지 못할 수 있습니다. 마찬가지로 클라이언트에서 파일을 잘못 구성해도 통신에 방해가 될 수 있습니다. 클라이언트와 서버 간 통신 문제를 디버깅할 때 다음 항목과 파일을 확인하십시오.

시작하기 전에 LDAP 클라이언트의 전역 영역에서 보안 관리자 역할을 가진 사용자여야 합니다.

1. **LDAP 서버에 대한 원격 호스트 템플리트 및 LDAP 서버의 게이트웨이에 대한 원격 호스트 템플리트가 올바른지 확인합니다.**

   ```
   # tninfo -h LDAP-server
   # route get LDAP-server
   # tninfo -h gateway-to-LDAP-server
   ```

   원격 호스트 템플리트 지정이 올바르지 않을 경우 Solaris Management Console에서 Security Templates(보안 템플리트) 도구를 사용하여 올바른 템플리트에 호스트를 지정합니다.

2. **`/etc/hosts` 파일을 확인하고 수정합니다.**

   시스템, 시스템의 레이블이 있는 영역에 대한 인터페이스, LDAP 서버에 대한 게이트웨이 및 LDAP 서버가 파일에 나열되어야 합니다. 추가 항목이 있을 수도 있습니다.

   중복된 항목을 찾습니다. 다른 시스템의 레이블이 있는 영역인 항목을 제거합니다. 예를 들어, `Lserver`가 LDAP 서버의 이름이고 `LServer-zones`가 레이블이 있는 영역에 대한 공유 인터페이스인 경우 `/etc/hosts`에서 `LServer-zones`를 제거합니다.

3. **DNS를 사용하는 경우 `resolv.conf` 파일에서 항목을 확인하고 수정합니다.**

   ```
   # more resolv.conf
   search list of domains
   domain domain-name
   nameserver IP-address

   ...
   nameserver IP-address
   ```

4. **`nsswitch.conf` 파일의 `tnrhdb` 및 `tnrhtp` 항목이 정확한지 확인합니다.**

5 **클라이언트가 서버에서 올바르게 구성되었는지 확인합니다.**

```
# ldaplist -l tnrhdb client-IP-address
```

6 **레이블이 있는 영역에 대한 인터페이스가 LDAP 서버에서 올바르게 구성되었는지 확인합니다.**

```
# ldaplist -l tnrhdb client-zone-IP-address
```

7 **현재 실행 중인 모든 영역에서 LDAP 서버를 핑(ping)할 수 있는지 확인합니다.**

```
# ldapclient list
...
NS_LDAP_SERVERS= LDAP-server-address
# zlogin zone-name1 ping LDAP-server-address
LDAP-server-address is alive
# zlogin zone-name2 ping LDAP-server-address
LDAP-server-address is alive
...
```

8 **LDAP를 구성하고 재부팅합니다.**

a. **절차는 Trusted Extensions Configuration Guide의 "Make the Global Zone an LDAP Client in Trusted Extensions"를 참조하십시오.**

b. **모든 레이블이 있는 영역에서 LDAP 서버의 클라이언트로 영역을 재설정합니다.**

```
# zlogin zone-name1
# ldapclient init \
-a profileName=profileName \
-a domainName=domain \
-a proxyDN=proxyDN \
-a proxyPassword=password LDAP-Server-IP-Address
# exit
# zlogin zone-name2 ...
```

c. **모든 영역을 중지하고 파일 시스템을 잠근 다음 재부트합니다.**

Oracle Solaris ZFS를 사용하는 경우 재부트하기 전에 영역을 중지하고 파일 시스템을 잠급니다. ZFS를 사용하지 않는 경우 위의 과정을 생략하고 재부트할 수 있습니다.

```
# zoneadm list
# zoneadm -z zone-name halt
# lockfs -fa
# reboot
```

◆ ◆ ◆ 14 장

14 Trusted Extensions의 다중 레벨 메일(개요)

이 장에서는 Trusted Extensions를 사용하여 구성된 시스템의 보안 및 다중 레벨 메일러에 대해 설명합니다.

- 193 페이지 “다중 레벨 메일 서비스”
- 193 페이지 “Trusted Extensions 메일 기능”

다중 레벨 메일 서비스

Trusted Extensions는 모든 메일 응용 프로그램에 대해 다중 레벨 메일을 제공합니다. 일반 사용자가 해당 메일러를 시작하면 사용자의 현재 레이블에서 응용 프로그램이 열립니다. 사용자가 다중 레벨 시스템에서 작업 중인 경우 해당 메일러 초기화 파일을 연결하거나 복사해야 할 수 있습니다. 자세한 내용은 86 페이지 “Trusted Extensions에서 사용자의 시작 파일을 구성하는 방법”을 참조하십시오.

Trusted Extensions 메일 기능

Trusted Extensions에서 시스템 관리자 역할은 Oracle Solaris **시스템 관리 설명서: 고급 관리** 및 **Oracle Solaris 관리: IP 서비스**의 지침에 따라 메일 서버를 설정하고 관리합니다. 또한 보안 관리자는 Trusted Extensions 메일 기능 구성 방법을 결정합니다.

메일 관리에 대한 다음 내용은 Trusted Extensions에만 해당됩니다.

- `.mailrc` 파일은 사용자의 최소 레이블에 있습니다.

  따라서 여러 레이블에서 작업하는 사용자는 최소 레이블 디렉토리에서 각 상위 디렉토리로 `.mailrc` 파일을 복사하거나 연결하지 않는 한 상위 레이블에 `.mailrc` 파일이 없습니다.

  보안 관리자 역할이나 개별 사용자는 `.mailrc` 파일을 `.copy_files` 또는 `.link_files` 중 하나에 추가할 수 있습니다. 이러한 파일에 대한 설명은 `updatehome`(1M) 매뉴얼 페이지를 참조하십시오. 구성 제안은 81 페이지 “`.copy_files` 및 `.link_files` 파일”을 참조하십시오.

- 메일 판독기는 시스템의 모든 레이블에서 실행할 수 있습니다. 메일 클라이언트를 서버에 연결하려면 일부 구성이 필요합니다.

  예를 들어 다중 레벨 메일에 Mozilla 메일을 사용하려면 각 레이블에서 Mozilla 메일 클라이언트를 구성하여 메일 서버를 지정해야 합니다. 각 레이블에 대해 메일 서버가 동일하거나 다를 수 있지만 서버는 반드시 지정해야 합니다.

- Solaris Management Console의 Mailing Lists(메일링 목록) 도구는 메일 별칭을 관리합니다.

  선택된 Solaris Management Console 도구 상자의 범위에 따라 로컬 `/etc/aliases` 파일이나 Oracle Directory Server Enterprise Edition의 LDAP 항목을 업데이트할 수 있습니다.

- Trusted Extensions 소프트웨어는 메일을 보내거나 전달하기 전에 호스트 및 사용자 레이블을 확인합니다.
  - 이 소프트웨어는 해당 메일이 호스트의 승인 범위 내에 있는지 확인합니다. 확인에 대한 내용은 이 목록 및 13 장, “Trusted Extensions에서 네트워크 관리(작업)”에 설명되어 있습니다.
  - 이 소프트웨어는 해당 메일이 계정의 클리어런스 및 최소 레이블 사이에 있는지 확인합니다.
  - 사용자는 인정 범위 내에서 수신된 전자 메일을 읽을 수 있습니다. 세션 중에 사용자는 현재 레이블에서만 메일을 읽을 수 있습니다.

    전자 메일을 사용하여 일반 사용자와 연락하려면 사용자가 읽을 수 있는 레이블에 있는 작업 공간에서 관리 역할이 메일을 보내야 합니다. 일반적으로 사용자의 기본 레이블을 선택하는 것이 좋습니다.

◆ ◆ ◆ 15 장

15 레이블이 있는 인쇄 관리(작업)

이 장에서는 Trusted Extensions 소프트웨어를 사용하여 레이블이 있는 인쇄를 구성하는 방법에 대해 설명합니다. 레이블 지정 옵션 없이 인쇄 작업을 구성하는 방법도 설명합니다.

- 195 페이지 “레이블, 프린터 및 인쇄”
- 203 페이지 “Trusted Extensions에서 인쇄 관리(작업 맵)”
- 203 페이지 “레이블이 있는 인쇄 구성(작업 맵)”
- 216 페이지 “Trusted Extensions에서 인쇄 제한 축소(작업 맵)”

레이블, 프린터 및 인쇄

Trusted Extensions 소프트웨어는 레이블을 사용하여 프린터 액세스를 제어합니다. 프린터 및 대기열의 인쇄 작업 정보에 대한 액세스를 제어하는 데 레이블이 사용됩니다. 이 소프트웨어는 인쇄되는 출력에도 레이블을 지정합니다. 본문 페이지에 레이블이 지정되고 필수 배너와 트레일러 페이지에 레이블이 지정됩니다. 배너와 트레일러 페이지에는 처리 지침도 포함될 수 있습니다.

시스템 관리자는 기본적인 프린터 관리 작업을 수행합니다. 보안 관리자 역할은 프린터 보안을 관리하며 여기에는 레이블 및 레이블이 있는 출력의 처리 방법이 포함됩니다. 관리자는 기본적인 Oracle Solaris 프린터 관리 절차를 따른 다음 인쇄 서버와 프린터에 레이블을 지정합니다.

Trusted Extensions 소프트웨어는 단일 레벨과 다중 레벨 인쇄를 모두 지원합니다. 다중 레벨 인쇄는 전역 영역에서만 구현됩니다. 전역 영역의 인쇄 서버를 사용하려면 레이블이 있는 영역이 전역 영역과는 다른 호스트 이름을 가지고 있어야 합니다. 별개의 호스트 이름을 얻는 방법 중 하나는 레이블이 있는 영역에 IP 주소를 지정하는 것입니다. 이 주소는 전역 영역의 IP 주소와 다릅니다.

Trusted Extensions에서 프린터 및 인쇄 작업 정보에 대한 액세스 제한

Trusted Extensions 소프트웨어를 사용하여 구성된 시스템의 사용자 및 역할은 해당 세션의 레이블에서 인쇄 작업을 만듭니다. 인쇄 작업은 해당 레이블을 인식하는 프린터에서만 인쇄할 수 있습니다. 레이블은 프린터의 레이블 범위에 있어야 합니다.

사용자와 역할은 세션의 레이블과 동일한 레이블을 가진 인쇄 작업을 볼 수 있습니다. 전역 영역의 경우 역할은 영역의 레이블에 의해 지배되는 레이블을 가진 작업을 볼 수 있습니다.

Trusted Extensions 소프트웨어를 사용하여 구성된 프린터는 프린터 출력에 레이블을 인쇄합니다. 레이블이 없는 인쇄 서버에서 관리하는 프린터는 프린터 출력에 레이블을 인쇄하지 않습니다. 이러한 프린터는 레이블이 없는 서버와 동일한 레이블을 가집니다. 예를 들어 Oracle Solaris 인쇄 서버에는 LDAP 이름 지정 서비스의 `tnrhdb` 데이터베이스에서 임의의 레이블이 지정될 수 있습니다. 그러면 사용자는 Oracle Solaris 프린터의 임의의 레이블에서 작업을 인쇄할 수 있습니다. Trusted Extensions 프린터처럼 이러한 Oracle Solaris 프린터도 해당 인쇄 서버에 지정된 레이블에서 작업하는 사용자의 인쇄 작업만을 승인할 수 있습니다.

레이블이 있는 프린터 출력

Trusted Extensions는 본문 페이지와 배너 및 트레일러 페이지에 보안 정보를 인쇄합니다. 정보는 `label_encodings` 파일과 `tsol_separator.ps` 파일에서 가져옵니다.

보안 관리자는 다음을 수행하여 레이블 설정 기본값을 수정하고 프린터 출력에 처리 지침을 추가할 수 있습니다.

- 배너와 트레일러 페이지의 텍스트 지역화 또는 사용자 정의
- 배너와 트레일러 페이지의 여러 필드 또는 본문 페이지에 인쇄할 대체 레이블 지정
- 원하는 텍스트나 레이블 변경 또는 생략

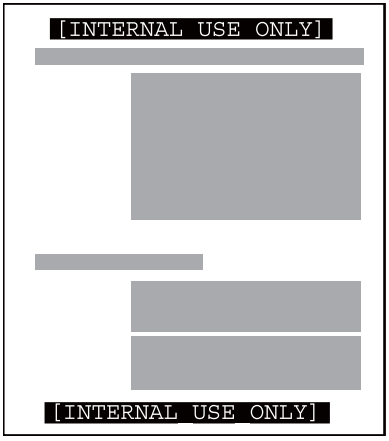
보안 관리자는 출력에 레이블을 인쇄하지 않는 프린터를 사용하도록 사용자 계정을 구성할 수도 있습니다. 사용자가 프린터 출력에 배너 또는 레이블을 선택적으로 인쇄하지 않을 수 있게 권한이 부여될 수도 있습니다.

레이블이 있는 본문 페이지

기본적으로 "Protect As" 분류가 모든 본문 페이지의 맨 위와 맨 아래에 인쇄됩니다. "Protect As" 분류는 작업 레이블의 분류가 `minimum protect as classification`과 비교될 때 지배 분류입니다. `minimum protect as classification`은 `label_encodings` 파일에서 정의됩니다.

예를 들어 사용자가 Internal Use Only 세션에 로그인하면 사용자의 인쇄 작업은 해당 레이블에 있습니다. `label_encodings` 파일의 `minimum protect as classification`이 Public이면 본문 페이지에 Internal Use Only 레이블이 인쇄됩니다.

그림 15–1 본문 페이지 맨 위와 아래에 인쇄된 작업의 레이블



레이블이 있는 배너 및 트레일러 페이지

다음 그림에서는 기본 배너 페이지 및 이 페이지와 기본 트레일러 페이지의 차이점을 보여 줍니다. 콜아웃은 다양한 섹션을 식별합니다. 트레일러 페이지에서는 윤곽선을 사용합니다.

인쇄 작업에서 표시되는 텍스트, 레이블 및 경고를 구성할 수 있습니다. 지역화를 위해 텍스트를 다른 언어의 텍스트로 바꿀 수도 있습니다.

그림 15–2 레이블이 있는 인쇄 작업의 일반적인 배너 페이지

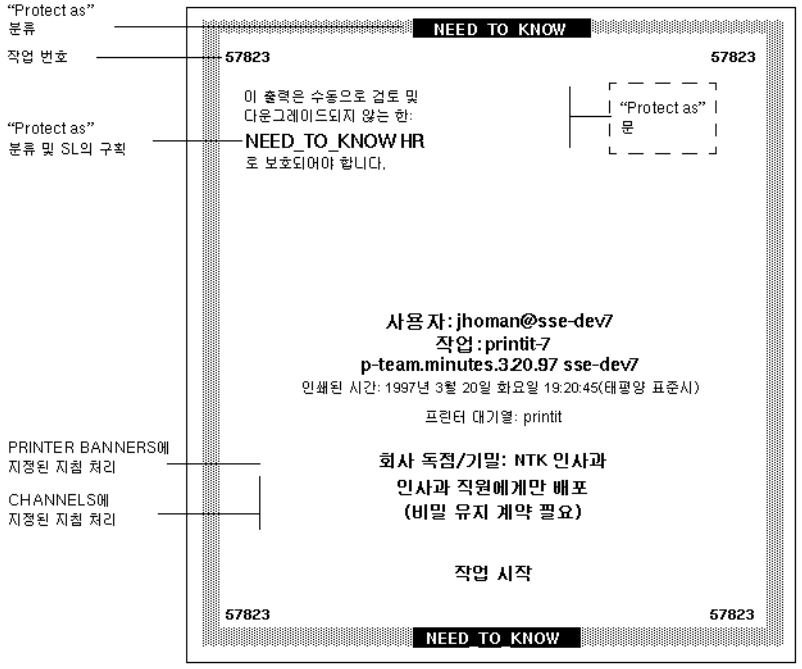
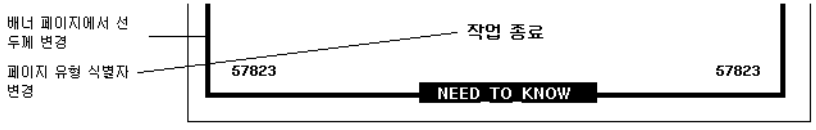


그림 15–3 트레일러 페이지의 차이점



다음 표는 보안 관리자가 `/usr/lib/lp/postscript/tsol_separator.ps` 파일을 수정하여 변경할 수 있는 신뢰할 수 있는 인쇄의 내용을 보여 줍니다.

주 – 인쇄되는 출력을 현지화 또는 국제화하려면 `tsol_separator.ps` 파일의 설명을 참조하십시오.

표 15–1 tsol_separator.ps 파일의 구성 가능한 값

출력	기본값	정의되는 방식	변경 방법
PRINTER BANNERS	/Caveats Job_Caveats	/Caveats Job_Caveats	**Trusted Extensions Label Administration**의 "Specifying Printer Banners"을 참조하십시오.
CHANNELS	/Channels Job_Channels	/Channels Job_Channels	**Trusted Extensions Label Administration**의 "Specifying Channels"을 참조하십시오.
배너 및 트레일러 페이지 맨 위의 레이블	/HeadLabel Job_Protect def	/PageLabel 설명을 참조하십시오.	/PageLabel을 변경하는 것과 같습니다. 또한 **Trusted Extensions Label Administration**의 "Specifying the Protect As Classification"을 참조하십시오.
본문 페이지 맨 위와 아래의 레이블	/PageLabel Job_Protect def	작업 레이블을 label_encodings 파일의 minimum protect as classification과 비교합니다. 더 지배적인 분류를 인쇄합니다. 인쇄 작업의 레이블에 구획이 있는 경우 구획을 포함합니다.	/PageLabel 정의를 변경하여 다른 값을 지정합니다. 또는 선택한 문자열을 입력합니다. 또는 아무것도 인쇄하지 않습니다.
"Protect as" 분류 문의 텍스트 및 레이블	/Protect Job_Protect def /Protect_Text1 () def /Protect_Text2 () def	/PageLabel 설명을 참조하십시오. 레이블 위에 표시할 텍스트입니다. 레이블 아래에 표시할 텍스트입니다.	/PageLabel을 변경하는 것과 동일합니다. Protect_Text1 및 Protect_Text2의 ()를 텍스트 문자열로 바꿉니다.

보안 정보의 포스트스크립트 인쇄

Trusted Extensions의 레이블이 있는 인쇄는 Solaris 인쇄 기능에 의존합니다. Oracle Solaris OS에서는 프린터 모델 스크립트가 배너 페이지 생성을 처리합니다. 레이블 지정을 구현하기 위해 먼저 프린터 모델 스크립트가 인쇄 작업을 포스트스크립트 파일로 변환합니다. 그런 다음 포스트스크립트 파일을 조작하여 본문 페이지에 레이블을 삽입하고 배너와 트레일러 페이지를 만듭니다.

Solaris 프린터 모델 스크립트는 포스트스크립트를 프린터의 고유 언어로 변환할 수도 있습니다. 프린터에서 포스트스크립트 입력을 허용하면 Oracle Solaris 소프트웨어에서 프린터로 작업을 보냅니다. 프린터에서 포스트스크립트 입력을 허용하지 않으면 이

소프트웨어는 포스트스크립트 형식을 래스터 이미지로 변환합니다. 그런 다음 래스터 이미지가 해당 프린터 형식으로 변환됩니다.

레이블 정보를 인쇄하기 위해 포스트스크립트 소프트웨어가 사용되므로 사용자는 기본적으로 포스트스크립트 파일을 인쇄할 수 없습니다. 이러한 제한으로 인해 숙련된 포스트스크립트 프로그래머라도 프린터 출력에서 레이블을 수정하는 포스트스크립트 파일을 만들 수 없습니다.

보안 관리자 역할은 역할 계정 및 신뢰할 수 있는 사용자에게 `Print Postscript`(포스트스크립트 인쇄) 권한 부여를 지정하여 이 제한을 대체할 수 있습니다. 이 권한 부여는 해당 계정이 프린터 출력의 레이블을 도용하지 않을 것으로 신뢰할 수 있는 경우에만 지정됩니다. 또한 사용자의 포스트스크립트 파일 출력을 허용하는 것이 해당 사이트의 보안 정책과 일치해야 합니다.

프린터 모델 스크립트

프린터 모델 스크립트를 사용하여 특정 모델의 프린터에 배너 및 트레일러 페이지를 제공할 수 있습니다. Trusted Extensions는 다음과 같은 4가지 스크립트를 제공합니다.

- `tsol_standard` - 직접 연결된 포스트스크립트 프린터용(예: 병렬 포트로 연결된 프린터)
- `tsol_netstandard` - 네트워크 액세스 가능 포스트스크립트 프린터용
- `tsol_standard_foomatic` - 포스트스크립트 형식을 인쇄하지 않는 직접 연결된 프린터용
- `tsol_netstandard_foomatic` - 포스트스크립트 형식을 인쇄하지 않는 네트워크 액세스 가능 프린터용

프린터 드라이버 이름이 `Foomatic`으로 시작하는 경우 `foomatic` 스크립트가 사용됩니다. Foomatic 드라이버는 PPD(포스트스크립트 프린터 드라이버)입니다.

주 – 레이블이 있는 영역에 프린터를 추가하면 Print Manager(인쇄 관리자)에서 기본적으로 "Use PPD(PPD 사용)"가 지정됩니다. 그러면 PPD를 사용하여 배너와 트레일러 페이지를 프린터의 언어로 변환합니다.

추가 변환 필터

변환 필터는 텍스트 파일을 포스트스크립트 형식으로 변환합니다. 필터의 프로그램은 프린터 데몬에 의해 실행되는 신뢰할 수 있는 프로그램입니다. 설치된 필터 프로그램에 의해 포스트스크립트 형식으로 변환되는 파일은 인증된 레이블과 배너 및 트레일러 페이지 텍스트를 포함하는 것으로 신뢰할 수 있습니다.

Oracle Solaris 소프트웨어는 사이트에서 필요로 하는 대부분의 변환 필터를 제공합니다. 사이트의 시스템 관리자 역할은 추가 필터를 설치할 수 있습니다. 그러면 이러한 필터는 인증된 레이블과 배너 및 트레일러 페이지를 포함하는 것으로 신뢰할 수 있습니다. 변환

필터를 추가하려면 **System Administration Guide: Printing**의 7 장, “Customizing LP Printing Services and Printers (Tasks)”를 참조하십시오.

Trusted Solaris 8 인쇄와 Trusted Extensions의 상호 운용성

호환 가능한 `label_encodings` 파일이 있고 CIPSO 템플리트를 사용하여 서로를 식별하는 Trusted Solaris 8 및 Trusted Extensions 시스템은 원격 인쇄에 서로를 사용할 수 있습니다. 다음 표에는 인쇄를 설정하기 위해 시스템을 설정하는 방법이 설명되어 있습니다. 기본적으로 사용자는 다른 OS의 원격 인쇄 서버에 있는 인쇄 작업을 나열하거나 취소할 수 없습니다. 선택적으로 사용자가 이를 수행할 수 있도록 권한을 부여할 수 있습니다.

시작 시스템	인쇄 서버 시스템	작업	결과
Trusted Extensions	Trusted Solaris 8	인쇄 구성 – Trusted Extensions `tnrhdb`에서 적절한 레이블 범위를 사용하여 템플리트를 Trusted Solaris 8 인쇄 서버에 지정합니다. 레이블은 CIPSO이거나 레이블이 없을 수 있습니다.	Trusted Solaris 8 프린터는 프린터의 레이블 범위 내에서 Trusted Extensions 시스템의 작업을 인쇄할 수 있습니다.
Trusted Extensions	Trusted Solaris 8	사용자 권한 부여 – Trusted Extensions 시스템에서 필요한 권한 부여를 추가하는 프로파일을 만듭니다. 사용자에게 프로파일을 지정합니다.	Trusted Extensions 사용자가 Trusted Solaris 8 프린터로 보내는 인쇄 작업을 나열하거나 취소할 수 있습니다. 사용자는 다른 레이블에 있는 작업을 보거나 제거할 수 없습니다.
Trusted Solaris 8	Trusted Extensions	인쇄 구성 – Trusted Solaris 8 `tnrhdb`에서 적절한 레이블 범위를 사용하여 템플리트를 Trusted Extensions 인쇄 서버에 지정합니다. 레이블은 CIPSO이거나 레이블이 없을 수 있습니다.	Trusted Extensions 프린터는 프린터의 레이블 범위 내에서 Trusted Solaris 8 시스템의 작업을 인쇄할 수 있습니다.

시작 시스템	인쇄 서버 시스템	작업	결과
Trusted Solaris 8	Trusted Extensions	사용자 권한 부여 – Trusted Solaris 8 시스템에서 필요한 권한 부여를 추가하는 프로파일을 만듭니다. 사용자에게 프로파일을 지정합니다.	Trusted Solaris 8 사용자가 Trusted Extensions 프린터로 보내는 인쇄 작업을 나열하거나 취소할 수 있습니다. 사용자는 다른 레이블에 있는 작업을 보거나 제거할 수 없습니다.

Trusted Extensions 인쇄 인터페이스(참조)

다음과 같은 사용자 명령이 Trusted Extensions 보안 정책에 맞게 확장되었습니다.

- `cancel` – 호출자가 인쇄 작업의 레이블과 동일해야만 작업을 취소할 수 있습니다. 기본적으로 일반 사용자는 자신의 작업만을 취소할 수 있습니다.
- `lp` – Trusted Extensions는 `-o nolabels` 옵션을 추가합니다. 사용자가 레이블 없이 인쇄할 수 있게 권한이 부여되어야 합니다. 마찬가지로 `-o nobanner` 옵션을 사용할 수 있게 권한이 부여되어야 합니다.
- `cancel` – 호출자가 인쇄 작업의 레이블과 동일해야만 작업의 상태를 가져올 수 있습니다. 기본적으로 일반 사용자는 자신의 인쇄 작업만을 볼 수 있습니다.

다음과 같은 관리 명령이 Trusted Extensions 보안 정책에 맞게 확장되었습니다. Oracle Solaris OS에서와 마찬가지로 이러한 명령은 Printer Management 권한 프로파일을 포함하는 역할만 실행할 수 있습니다.

- `cancel` – 호출자가 인쇄 작업의 레이블과 동일해야만 작업을 이동할 수 있습니다. 기본적으로 일반 사용자는 자신의 인쇄 작업만 이동할 수 있습니다.
- `lpadmin` – 전역 영역에서 이 명령은 모든 작업에 사용할 수 있습니다. 레이블이 있는 영역에서는 호출자가 인쇄 작업의 레이블을 지배해야만 작업을 볼 수 있고 레이블과 동일해야만 작업을 변경할 수 있습니다.

  Trusted Extensions는 `-m` 옵션에 프린터 모델 스크립트를 추가합니다. Trusted Extensions는 `-o nolabels` 옵션을 추가합니다.
- `lpsched` – 전역 영역에서 이 명령은 항상 올바로 실행됩니다. Oracle Solaris OS에서와 마찬가지로 `svcadm` 명령을 사용하여 인쇄 서비스를 사용/사용 안함으로 설정하거나, 시작하거나, 다시 시작할 수 있습니다. 레이블이 있는 영역에서는 호출자가 인쇄 서비스의 레이블과 동일해야만 인쇄 서비스를 변경할 수 있습니다. 서비스 관리 기능에 대한 자세한 내용은 `smf(5)`, `svcadm(1M)` 및 `svcs(1)` 매뉴얼 페이지를 참조하십시오.

Trusted Extensions는 Printer Management 권한 프로파일에 `solaris.label.print` 권한 부여를 추가합니다. 레이블 없이 본문 페이지를 인쇄하려면 `solaris.print.unlabeled` 권한 부여가 필요합니다.

Trusted Extensions에서 인쇄 관리(작업 맵)

인쇄 구성을 위한 Trusted Extensions 절차는 Oracle Solaris 프린터 설정을 완료한 후에 수행됩니다. 다음 작업 맵은 레이블이 있는 인쇄를 관리하는 주요 작업을 알려 줍니다.

작업	설명	수행 방법
레이블이 있는 출력을 위해 프린터를 구성합니다.	사용자가 Trusted Extensions 프린터에 인쇄할 수 있도록 설정합니다. 인쇄 작업이 레이블을 사용하여 표시됩니다.	203 페이지 “레이블이 있는 인쇄 구성(작업 맵)”
프린터 출력에서 표시되는 레이블을 제거합니다.	사용자가 특정 레이블에서 Oracle Solaris 프린터로 인쇄할 수 있도록 설정합니다. 인쇄 작업이 레이블을 사용하여 표시되지 않습니다. 또는 레이블이 Trusted Extensions 프린터에서 인쇄되지 않도록 합니다.	216 페이지 “Trusted Extensions에서 인쇄 제한 축소(작업 맵)”

레이블이 있는 인쇄 구성(작업 맵)

다음 작업 맵은 레이블이 있는 인쇄와 관련된 일반적인 구성 절차를 설명합니다.

주 – 프린터 클라이언트는 Trusted Extensions 인쇄 서버의 레이블 범위 내에서만 작업을 인쇄할 수 있습니다.

작업	설명	수행 방법
전역 영역에서 인쇄를 구성합니다.	전역 영역에서 다중 레벨 인쇄 서버를 만듭니다.	204 페이지 “다중 레벨 인쇄 서버 및 해당 프린터를 구성하는 방법”
시스템 네트워크에 대한 인쇄를 구성합니다.	전역 영역에서 다중 레벨 인쇄 서버를 만들고 레이블이 있는 영역에서 프린터를 사용할 수 있도록 설정합니다.	206 페이지 “Sun Ray 클라이언트에 대해 네트워크 프린터를 구성하는 방법”
레이블이 있는 시스템과 동일한 서브넷에서 레이블이 없는 시스템에 대한 인쇄를 구성합니다.	레이블이 없는 시스템이 네트워크 프린터를 사용할 수 있도록 설정합니다.	209 페이지 “레이블이 있는 시스템에서 계단식 인쇄를 구성하는 방법”
레이블이 있는 영역의 인쇄를 구성합니다.	레이블이 있는 영역에 대해 단일 레이블 인쇄 서버를 만듭니다.	211 페이지 “영역의 단일 레이블 인쇄를 구성하는 방법”
다중 레벨 인쇄 클라이언트를 구성합니다.	Trusted Extensions 호스트를 프린터에 연결합니다.	213 페이지 “Trusted Extensions 클라이언트가 프린터에 액세스할 수 있도록 설정하는 방법”

작업	설명	수행 방법
프린터의 레이블 범위를 제한합니다.	Trusted Extensions 프린터를 좁은 레이블 범위로 제한합니다.	215 페이지 "프린터에 대해 제한된 레이블 범위를 구성하는 방법"

▼ 다중 레벨 인쇄 서버 및 해당 프린터를 구성하는 방법

Trusted Extensions 인쇄 서버에서 관리하는 프린터는 본문 페이지, 배너 페이지 및 트레일러 페이지에 레이블을 인쇄합니다. 이러한 프린터는 인쇄 서버의 레이블 범위 내에서 작업을 인쇄할 수 있습니다. 인쇄 서버에 연결할 수 있는 Trusted Extensions 호스트는 해당 서버에 연결된 프린터를 사용할 수 있습니다.

시작하기 전에 Trusted Extensions 네트워크에 대한 인쇄 서버를 결정합니다. 전역 영역에서 이 인쇄 서버의 시스템 관리자 역할을 가진 사용자여야 합니다.

1. **Solaris Management Console을 시작합니다.**
   자세한 내용은 52 페이지 "Solaris Management Console에서 로컬 시스템을 관리하는 방법"을 참조하십시오.

2. **Files(파일) 도구 상자를 선택합니다.**
   도구 상자 제목에 `Scope=Files, Policy=TSOL`이 포함됩니다.

3. **인쇄 서버 포트 515/tcp를 사용하여 전역 영역을 구성하여 다중 레벨 인쇄를 설정합니다.**
   포트를 전역 영역에 추가하여 인쇄 서버에 대한 MLP(다중 레벨 포트)를 만듭니다.

   a. **Trusted Network Zones(신뢰할 수 있는 네트워크 영역) 도구로 이동합니다.**

   b. **영역 IP 주소의 다중 레벨 포트에 515/tcp를 추가합니다.**

   c. **OK(확인)를 누릅니다.**

4. **연결된 모든 프린터의 특성을 정의합니다.**
   명령줄 사용 Print Manager(인쇄 관리자) GUI는 전역 영역에서 사용할 수 없습니다.

   ```
   # lpadmin -p printer-name -v /dev/null \
   -o protocol=tcp -o dest=printer-IP-address:9100 -T PS -I postscript
   # accept printer-name
   # enable printer-name
   ```

5. **프린터 모델 스크립트를 인쇄 서버에 연결된 각 프린터에 지정합니다.**
   모델 스크립트는 지정된 프린터에 대해 배너 및 트레일러 페이지를 활성화합니다.

스크립트에 대한 설명은 200 페이지 “프린터 모델 스크립트”를 참조하십시오. 프린터 드라이버 이름이 Foomatic으로 시작하면 foomatic 모델 스크립트 중 하나를 지정합니다. 한 라인에서 다음 명령을 사용합니다.

```
$ lpadmin -p printer \
 -m { tsol_standard | tsol_netstandard |
      tsol_standard_foomatic | tsol_netstandard_foomatic }
```

ADMIN_LOW에서 ADMIN_HIGH의 기본 프린터 레이블 범위가 모든 프린터에 대해 허용되면 레이블 구성이 완료됩니다.

6 인쇄가 허용되는 레이블이 있는 모든 영역에서 프린터를 구성합니다.

전역 영역에 대해 all-zones IP 주소를 인쇄 서버로 사용합니다.

a. 레이블이 있는 영역의 영역 콘솔에 root로 로그인합니다.

```
# zlogin -C labeled-zone
```

b. 프린터를 영역에 추가합니다.

```
# lpadmin -p printer-name -s all-zones-IP-address
```

c. (옵션) 이 프린터를 기본 프린터로 설정합니다.

```
# lpadmin -d printer-name
```

7 모든 영역에서 프린터를 테스트합니다.

주 – Solaris 10 7/10 릴리스부터 ADMIN_HIGH 또는 ADMIN_LOW 관리 레이블이 있는 파일은 인쇄 출력의 본문에 ADMIN_HIGH를 인쇄합니다. 배너 및 트레일러 페이지에 label_encodings 파일에 있는 최상위 레이블과 구획을 사용하여 레이블이 지정됩니다.

---

root 및 일반 사용자로 다음 단계를 수행합니다.

a. 명령줄에서 일반 파일을 인쇄합니다.

b. Beehive, 브라우저, 편집기 등의 응용 프로그램에서 파일을 인쇄합니다.

c. 배너 페이지, 트레일러 페이지 및 보안 배너가 제대로 인쇄되는지 확인합니다.

참조
- **프린터 레이블 범위 제한 –** 215 페이지 “프린터에 대해 제한된 레이블 범위를 구성하는 방법”
- **레이블이 있는 출력 방지 –** 216 페이지 “Trusted Extensions에서 인쇄 제한 축소(작업 맵)”
- **이 영역을 인쇄 서버로 사용 –** 213 페이지 “Trusted Extensions 클라이언트가 프린터에 액세스할 수 있도록 설정하는 방법”

▼ Sun Ray 클라이언트에 대해 네트워크 프린터를 구성하는 방법

이 절차는 단일 `all-zones` 인터페이스가 있는 Sun Ray 서버에서 포스트스크립트 프린터를 구성합니다. 이 서버의 모든 Sun Ray 클라이언트 사용자가 프린터를 사용할 수 있게 됩니다. 초기 구성은 전역 영역에서 수행됩니다. 전역 영역을 구성한 후 레이블이 있는 각 영역에서 프린터를 사용할 수 있도록 구성합니다.

시작하기 전에 Trusted CDE의 다중 레벨 세션으로 로그인해야 합니다.

1. **전역 영역에서 네트워크 프린터에 IP 주소를 지정합니다.**

   지침은 **System Administration Guide: Printing**의 5 장, “Setting Up Printers by Using LP Print Commands (Tasks)”를 참조하십시오.

2. **Solaris Management Console을 시작합니다.**

   - 지침은 **Trusted Extensions Configuration Guide**의 “Initialize the Solaris Management Console Server in Trusted Extensions”를 참조하십시오.
   - `Scope=Files, Policy=TSOL` 도구 상자를 선택하고 로그인합니다.

3. **`admin_low` 템플리트에 프린터를 지정합니다.**

   a. **Computers and Networks(컴퓨터 및 네트워크) 도구에서 Security Templates(보안 템플리트)를 두 번 누릅니다.**

   b. **`admin_low`를 두 번 누릅니다.**

   c. **Hosts Assigned to Template(템플리트에 지정된 호스트) 탭에서 프린터의 IP 주소를 추가합니다.**

      자세한 내용은 왼쪽 창의 온라인 도움말을 참조하십시오.

4. **프린터 포트를 전역 영역의 공유 인터페이스에 추가합니다.**

   a. **Computers and Networks(컴퓨터 및 네트워크) 도구에서 Trusted Network Zones(신뢰할 수 있는 네트워크 영역)를 두 번 누릅니다.**

   b. **`global`을 두 번 누릅니다.**

   c. **Multilevel Ports for Shared IP Addresses(공유 IP 주소의 다중 레벨 포트) 목록에 포트 515, 프로토콜 `tcp`를 추가합니다.**

5 Solaris Management Console 지정이 커널에 있는지 확인합니다.

```
# tninfo -h printer-IP-address
   IP address= printer-IP-address
   Template = admin_low

# tninfo -m global
   private: 111/tcp;111/udp;513/tcp;515/tcp;631/tcp;2049/tcp;6000-6050/tcp;
7007/tcp;7010/tcp;7014/tcp;7015/tcp;32771/tcp;32776/ip
   shared: 515/tcp;6000-6050/tcp;7007/tcp;7010/tcp;7014/tcp;7015/tcp
```

주 – 6055, 7007 등의 추가 개인 및 공유 MLP(다중 레벨 포트)는 Sun Ray 요구 사항을 지원합니다.

---

6 전역 영역에 인쇄 서비스가 설정되어 있는지 확인합니다.

```
# svcadm enable print/server
# svcadm enable rfc1179
```

7 netservices limited를 사용하여 시스템이 설치되어 있는 경우 프린터가 네트워크에 연결되도록 설정합니다.

rfc1179 서비스에서 localhost 이외의 주소를 수신 대기해야 합니다. LP 서비스는 명명된 파이프에서만 수신 대기합니다.

```
# inetadm -m svc:/application/print/rfc1179:default bind_addr=''
# svcadm refresh rfc1179
```

주 – netservices open을 실행하는 경우 이전의 명령은 다음과 같은 오류를 생성합니다. **오류**: "inetd" **특성 그룹이 없습니다**.

---

8 모든 사용자가 포스트스크립트를 인쇄할 수 있도록 설정합니다.

신뢰할 수 있는 편집기에서 /etc/default/print 파일을 만들고 다음 라인을 추가합니다.

```
PRINT_POSTSCRIPT=1
```

Beehive, gedit 등의 응용 프로그램은 포스트스크립트 출력을 만듭니다.

9 인쇄 서비스에 모든 LP 필터를 추가합니다.

전역 영역에서 다음 C-셸 스크립트를 실행합니다.

```
csh
    cd /etc/lp/fd/
    foreach a (*.fd)
        lpfilter -f $a:r -F $a
    end
```

10 전역 영역에 프린터를 추가합니다.

명령줄 사용 Print Manager(인쇄 관리자) GUI는 전역 영역에서 사용할 수 없습니다.

```
# lpadmin -p printer-name -v /dev/null -m tsol_netstandard \
-o protocol=tcp -o dest=printer-IP-address:9100 -T PS -I postscript
```

```
# accept printer-name
# enable printer-name
```

11 (옵션) 이 프린터를 기본 프린터로 설정합니다.

```
# lpadmin -d printer-name
```

12 레이블이 있는 모든 영역에서 프린터를 구성합니다.

전역 영역에 대해 `all-zones` IP 주소를 인쇄 서버로 사용합니다. `all-zones` NIC가 vni(가상 네트워크 인터페이스)인 경우 vni에 대한 IP 주소를 `-s` 옵션에 대한 인수로 사용합니다.

a. 레이블이 있는 영역의 영역 콘솔에 root로 로그인합니다.

```
# zlogin -C labeled-zonename
```

b. 프린터를 영역에 추가합니다.

```
# lpadmin -p printer-name -s global-zone-shared-IP-address
```

c. (옵션) 이 프린터를 기본 프린터로 설정합니다.

```
# lpadmin -d printer-name
```

13 모든 영역에서 프린터를 테스트합니다.

주 – Solaris 10 7/10 릴리스부터 `ADMIN_HIGH` 또는 `ADMIN_LOW` 관리 레이블이 있는 파일은 인쇄 출력의 본문에 `ADMIN_HIGH`를 인쇄합니다. 배너 및 트레일러 페이지에 `label_encodings` 파일에 있는 최상위 레이블과 구획을 사용하여 레이블이 지정됩니다.

`root` 및 일반 사용자로 다음 단계를 수행합니다.

a. 명령줄에서 일반 파일을 인쇄합니다.

b. Beehive, 브라우저, 편집기 등의 응용 프로그램에서 파일을 인쇄합니다.

c. 배너 페이지, 트레일러 페이지 및 보안 배너가 제대로 인쇄되는지 확인합니다.

예 15–1 네트워크 프린터의 프린터 상태 확인

이 예에서는 관리자가 전역 영역과 레이블이 있는 영역의 네트워크 프린터 상태를 확인합니다.

```
global # lpstat -t
    scheduler is running
    system default destination: math-printer
    system for _default: trusted1 (as printer math-printer)
    device for math-printer: /dev/null
    character set
    default accepting requests since Feb 28 00:00 2008
```

```
    lex accepting requests since Feb 28 00:00 2008
    printer math-printer is idle. enabled since Feb 28 00:00 2008. available.

Solaris1# lpstat -t
   scheduler is not running
   system default destination: math-printer
   system for _default: 192.168.4.17 (as printer math-printer)
   system for math-printer: 192.168.4.17
   default accepting requests since Feb 28 00:00 2008
   math-printer accepting requests since Feb 28 00:00 2008
   printer _default is idle. enabled since Feb 28 00:00 2008. available.
   printer math-printer is idle. enabled since Feb 28 00:00 2008. available.
```

▼ 레이블이 있는 시스템에서 계단식 인쇄를 구성하는 방법

계단식 인쇄는 Windows 데스크탑 세션에서 Trusted Extensions 레이블이 있는 영역 인터페이스로 인쇄할 수 있는 기능을 제공합니다. 이 경우 물리적 인터페이스의 영역 IP 주소가 인쇄 스풀러로 작동합니다. 물리적 인터페이스의 영역 IP 주소에 있는 MLP(다중 레벨 포트) listener는 Trusted Extensions 인쇄 부속 시스템에 지시를 보내 해당 레이블이 있는 헤더와 트레일러 시트를 사용하여 파일을 인쇄합니다.

이 절차를 통해 레이블이 있는 시스템과 동일한 서브넷에 있는 레이블이 없는 시스템에서 레이블이 있는 네트워크 프린터를 사용할 수 있게 됩니다. `rfc1179` 서비스에서 계단식 인쇄를 처리합니다. 계단식 인쇄가 허용된 레이블이 있는 모든 영역에서 이 절차를 수행해야 합니다.

시작하기 전에 206 페이지 “Sun Ray 클라이언트에 대해 네트워크 프린터를 구성하는 방법”을 완료합니다.

1 레이블이 있는 영역의 영역 콘솔에 root 로 로그인합니다.

```
# zlogin -C labeled-zonename
```

2 인쇄/서버 서비스에서 `rfc1179` 서비스의 종속성을 제거합니다.

```
labeled-zone # cat <<EOF | svccfg
      select application/print/rfc1179
      delpg lpsched
      end
   EOF

labeled-zone # svcadm refresh application/print/rfc1179
```

3 `rfc1179` 서비스가 설정되어 있는지 확인합니다.

```
labeled-zone # svcadm enable rfc1179
```

4 netservices limited를 사용하여 레이블이 있는 영역이 설치되어 있는 경우 프린터가 네트워크에 연결되도록 설정합니다.

rfc1179 서비스에서 localhost 이외의 주소를 수신 대기해야 합니다. LP 서비스는 명명된 파이프에서만 수신 대기합니다.

```
# inetadm -m svc:/application/print/rfc1179:default bind_addr=''
# svcadm refresh rfc1179
```

주 – netservices open을 실행하는 경우 이전의 명령은 다음과 같은 메시지를 생성합니다. **오류**: "inetd" **특성 그룹이 없습니다**.

---

5 레이블이 있는 영역의 계단식 인쇄를 구성합니다.

labeled-zone # lpset -n system -a spooling-type=cascade *printer-name*

이 명령은 영역의 /etc/printers.conf 파일을 업데이트합니다.

6 이 레이블이 있는 영역과 동일한 서브넷에 있는 Oracle Solaris 시스템을 테스트합니다.

예를 들어 Solaris1 시스템을 테스트합니다. 이 시스템은 internal 영역과 동일한 서브넷에 있습니다. 구성 매개변수는 다음과 같습니다.

- math-printer IP 주소는 192.168.4.6입니다.
- Solaris1 IP 주소는 192.168.4.12입니다.
- internal 영역 IP 주소는 192.168.4.17입니다.

```
Solaris1# uname -a
SunOS Solaris1 Generic_120011-11 sun4u sparc SUNW,Sun-Blade-1000
Solaris1# lpadmin -p math-printer -s 192.168.4.17
Solaris1# lpadmin -d math-printer

Solaris1# lpstat -t
   scheduler is not running
   system default destination: math-printer
   system for _default: 192.168.4.17 (as printer math-printer)
   system for math-printer: 192.168.4.17
   default accepting requests since Feb 28 00:00 2008
   math-printer accepting requests since Feb 28 00:00 2008
   printer _default is idle. enabled since Feb 28 00:00 2008. available.
   printer math-printer is idle. enabled since Feb 28 00:00 2008. available.
```

- **lp 명령을 테스트합니다.**

  ```
  Solaris1# lp /etc/hosts
     request id is math-printer-1 (1 file)
  ```

- **Beehive, 브라우저 등의 응용 프로그램에서 인쇄를 테스트합니다.**

7 이 레이블이 있는 영역과 동일한 서브넷에 있는 Windows 2003 Server를 테스트합니다.

a. Windows Server에서 프린터를 설정합니다.

시작 메뉴->설정->프린터 및 팩스 GUI를 사용합니다.

다음과 같이 프린터 구성을 지정합니다.

- 프린터 추가
- 이 컴퓨터에 연결된 로컬 프린터
- 새 포트 만들기 – 표준 TCP/IP 포트
- 프린터 이름 또는 IP 주소 – 192.168.4.17(즉, 레이블이 있는 영역의 IP 주소)
- 포트 이름 – 기본값 사용
- 포트 정보가 추가로 필요합니다. – 기본값 사용
  - 장치 유형 = 사용자 정의
  - 설정 – 프로토콜 = LPR
  - LPR 설정 – 대기열 이름 = math-printer(즉, UNIX 대기열 이름)
  - LPR 바이트 계산 사용

제조사, 모델, 드라이버 및 기타 프린터 매개변수를 지정하여 프린터 설정을 마칩니다.

8 응용 프로그램에서 프린터를 선택하여 해당 프린터를 테스트합니다.

예를 들어 `internal` 영역과 동일한 서브넷에 있는 `winserver` 시스템을 테스트합니다. 구성 매개변수는 다음과 같습니다.

- `math-printer` IP 주소는 192.168.4.6입니다.
- `winserver` IP 주소는 192.168.4.200입니다.
- `internal` 영역 IP 주소는 192.168.4.17입니다.

```
winserver C:/> ipconfig
Windows IP Configuration
   Ethernet adapter TP-NIC:
      Connection-specific DNS Suffix  . :
      IP Address. . . . . . . . . . . . : 192.168.4.200
      Subnet Mask . . . . . . . . . . . : 255.255.255.0
      Default Gateway . . . . . . . . . : 192.168.4.17
```

▼ 영역의 단일 레이블 인쇄를 구성하는 방법

시작하기 전에 영역에서 전역 영역과 IP 주소를 공유하지 않아야 합니다. 전역 영역에서 시스템 관리자 역할을 가진 사용자여야 합니다.

1 작업 공간을 추가합니다.

자세한 내용은 **Trusted Extensions User's Guide**의 "How to Add a Workspace at a Particular Label"을 참조하십시오.

2 새 작업 공간의 레이블을 해당 레이블의 인쇄 서버가 될 영역의 레이블로 변경합니다.

자세한 내용은 **Trusted Extensions User's Guide**의 "How to Change the Label of a Workspace"을 참조하십시오.

3 연결된 프린터의 특성을 정의합니다.

a. 영역의 레이블에서 Print Manager(인쇄 관리자)를 시작합니다.

기본적으로 "Use PPD(PPD 사용)" 확인란이 선택됩니다. 시스템에서 프린터에 적합한 드라이버를 찾습니다.

b. (옵션) 다른 프린터 드라이버를 지정하려면 다음을 수행합니다.

i. "Use PPD(PPD 사용)" 선택을 취소합니다.

ii. 다른 드라이버를 사용하는 프린터 제품과 모델을 정의합니다.

Print Manager(인쇄 관리자)에서 처음 두 필드의 값을 제공하면 Print Manager(인쇄 관리자)에서 드라이버 이름을 제공합니다.

```
Printer Make        manufacturer
Printer Model       manufacturer-part-number
Printer Driver      automatically filled in
```

4 프린터 모델 스크립트를 영역에 연결된 각 프린터에 지정합니다.

모델 스크립트는 지정된 프린터에 대해 배너 및 트레일러 페이지를 활성화합니다.

스크립트 선택에 대해서는 200 페이지 “프린터 모델 스크립트”를 참조하십시오. 프린터 드라이버 이름이 `Foomatic`으로 시작하면 foomatic 모델 스크립트 중 하나를 지정합니다. 다음 명령을 사용합니다.

```
$ lpadmin -p printer -m model
```

연결된 프린터는 영역의 레이블에서만 작업을 인쇄할 수 있습니다.

5 프린터를 테스트합니다.

주 – Solaris 10 7/10 릴리스부터 `ADMIN_HIGH` 또는 `ADMIN_LOW` 관리 레이블이 있는 파일은 인쇄 출력의 본문에 `ADMIN_HIGH`를 인쇄합니다. 배너 및 트레일러 페이지에 `label_encodings` 파일에 있는 최상위 레이블과 구획을 사용하여 레이블이 지정됩니다.

`root` 및 일반 사용자로 다음 단계를 수행합니다.

a. 명령줄에서 일반 파일을 인쇄합니다.

b. Beehive, 브라우저, 편집기 등의 응용 프로그램에서 파일을 인쇄합니다.

c. 배너 페이지, 트레일러 페이지 및 보안 배너가 제대로 인쇄되는지 확인합니다.

참조 레이블이 있는 출력 방지 – 216 페이지 “Trusted Extensions에서 인쇄 제한 축소(작업 맵)”

▼ Trusted Extensions 클라이언트가 프린터에 액세스할 수 있도록 설정하는 방법

처음에는 인쇄 서버가 구성된 영역만 해당 인쇄 서버의 프린터에 인쇄할 수 있습니다. 다른 영역 및 시스템에 대해서는 시스템 관리자가 명시적으로 이러한 프린터에 대한 액세스를 추가해야 합니다. 가능한 설정은 다음과 같습니다.

- 전역 영역의 경우 다른 시스템의 전역 영역에 연결되어 있는 프린터에 대한 액세스를 추가합니다.
- 레이블이 있는 영역의 경우 해당 시스템의 전역 영역에 연결되어 있는 프린터에 대한 액세스를 추가합니다.
- 레이블이 있는 영역의 경우 동일한 레이블에 있는 원격 영역에 구성되어 있는 프린터에 대한 액세스를 추가합니다.
- 레이블이 있는 영역의 경우 다른 시스템의 전역 영역에 연결되어 있는 프린터에 대한 액세스를 추가합니다.

시작하기 전에 레이블 범위 또는 단일 레이블을 사용하여 인쇄 서버를 구성하고 여기에 연결된 프린터 구성을 완료합니다. 자세한 내용은 다음을 참조하십시오.

- 204 페이지 “다중 레벨 인쇄 서버 및 해당 프린터를 구성하는 방법”
- 211 페이지 “영역의 단일 레이블 인쇄를 구성하는 방법”
- 217 페이지 “레이블이 없는 인쇄 서버에 레이블을 지정하는 방법”

전역 영역에서 시스템 관리자 역할을 가진 사용자이거나 이 역할을 맡을 수 있어야 합니다.

1 시스템에서 프린터에 액세스할 수 있도록 설정하는 절차를 완료합니다.

- **인쇄 서버가 아닌 시스템에서 전역 영역을 구성하여 프린터 액세스에 다른 시스템의 전역 영역을 사용하도록 합니다.**

  a. 프린터 액세스 권한이 없는 시스템에서 시스템 관리자 역할을 맡습니다.

  b. Trusted Extensions 인쇄 서버에 연결된 프린터에 대한 액세스를 추가합니다.

  ```
  $ lpadmin -s printer
  ```

- **레이블이 있는 영역을 구성하여 프린터 액세스에 해당 전역 영역을 사용하도록 합니다.**

  a. 역할 작업 공간의 레이블을 레이블이 있는 영역의 레이블로 변경합니다.

  자세한 내용은 **Trusted Extensions User’s Guide**의 “How to Change the Label of a Workspace”을 참조하십시오.

b. 프린터에 대한 액세스를 추가합니다.

```
$ lpadmin -s printer
```

- **레이블이 있는 영역을 구성하여 프린터 액세스에 다른 시스템의 레이블이 있는 영역을 사용하도록 합니다.**

  영역의 레이블이 동일해야 합니다.

  a. 프린터 액세스 권한이 없는 시스템에서 시스템 관리자 역할을 맡습니다.

  b. 역할 작업 공간의 레이블을 레이블이 있는 영역의 레이블로 변경합니다.

  자세한 내용은 **Trusted Extensions User's Guide**의 "How to Change the Label of a Workspace"을 참조하십시오.

  c. 레이블이 있는 원격 영역의 인쇄 서버에 연결된 프린터에 대한 액세스를 추가합니다.

  ```
  $ lpadmin -s printer
  ```

- **레이블이 있는 영역을 구성하여 프린터 액세스에 레이블이 없는 인쇄 서버를 사용하도록 합니다.**

  영역의 레이블이 인쇄 서버의 레이블과 동일해야 합니다.

  a. 프린터 액세스 권한이 없는 시스템에서 시스템 관리자 역할을 맡습니다.

  b. 역할 작업 공간의 레이블을 레이블이 있는 영역의 레이블로 변경합니다.

  자세한 내용은 **Trusted Extensions User's Guide**의 "How to Change the Label of a Workspace"을 참조하십시오.

  c. 임의의 레이블이 있는 인쇄 서버에 연결된 프린터에 대한 액세스를 추가합니다.

  ```
  $ lpadmin -s printer
  ```

2 프린터를 테스트합니다.

Solaris 10 7/10 릴리스부터 `ADMIN_HIGH` 또는 `ADMIN_LOW` 관리 레이블이 있는 파일은 인쇄 출력의 본문에 `ADMIN_HIGH`를 인쇄합니다. 배너 및 트레일러 페이지에 `label_encodings` 파일에 있는 최상위 레이블과 구획을 사용하여 레이블이 지정됩니다.

모든 클라이언트에서 전역 영역의 `root` 및 역할, 레이블이 있는 영역의 `root`, 역할 및 일반 사용자에 대해 인쇄가 가능한지 테스트합니다.

a. 명령줄에서 일반 파일을 인쇄합니다.

b. Beehive, 브라우저, 편집기 등의 응용 프로그램에서 파일을 인쇄합니다.

c. 배너 페이지, 트레일러 페이지 및 보안 배너가 제대로 인쇄되는지 확인합니다.

▼ 프린터에 대해 제한된 레이블 범위를 구성하는 방법

기본 프린터 레이블 범위는 ADMIN_LOW에서 ADMIN_HIGH입니다. 이 절차는 Trusted Extensions 인쇄 서버에서 제어하는 프린터의 레이블 범위를 좁힙니다.

시작하기 전에 전역 영역에서 보안 관리자 역할을 가진 사용자여야 합니다.

1. **Device Allocation Manager(장치 할당 관리자)를 시작합니다.**
   - **Trusted Path(신뢰할 수 있는 경로) 메뉴에서 Allocate Device(장치 할당) 옵션을 선택합니다.**
   - **Trusted CDE에서 Front Panel(전면 패널)의 Tools(도구) 서브패널에서 Device Allocation Manager(장치 할당 관리자) 작업을 시작합니다.**
2. **Device Administration(장치 관리) 버튼을 눌러 Device Allocation: Administration(장치 할당: 관리) 대화 상자를 표시합니다.**
3. **새 프린터의 이름을 입력합니다.**
   프린터가 사용자의 시스템에 연결되어 있는 경우 프린터의 이름을 찾습니다.
4. **Configure(구성) 버튼을 눌러 Device Allocation: Configuration(장치 할당: 구성) 대화 상자를 표시합니다.**
5. **프린터의 레이블 범위를 변경합니다.**
   a. **Min Label(최소 레이블) 버튼을 눌러 최소 레이블을 변경합니다.**
      레이블 구축기에서 레이블을 선택합니다. 레이블 구축기에 대한 자세한 내용은 43 페이지 "Trusted Extensions의 레이블 구축기"를 참조하십시오.
   b. **Max Label(최대 레이블) 버튼을 눌러 최대 레이블을 변경합니다.**
6. **변경 사항을 저장합니다.**
   a. **Configuration(구성) 대화 상자에서 OK(확인)를 누릅니다.**
   b. **Administration(관리) 대화 상자에서 OK(확인)를 누릅니다.**
7. **Device Allocation Manager(장치 할당 관리자)를 닫습니다.**

Trusted Extensions에서 인쇄 제한 축소(작업 맵)

다음 작업은 선택 사항입니다. 이러한 작업은 소프트웨어가 설치되어 있을 때 Trusted Extensions에서 기본적으로 제공하는 인쇄 보안을 축소합니다.

작업	설명	수행 방법
레이블을 출력하지 않도록 프린터를 구성합니다.	본문 페이지에 보안 정보가 인쇄되는 것을 방지하고 배너 및 트레일러 페이지를 제거합니다.	216 페이지 "인쇄되는 출력에서 레이블을 제거하는 방법"
레이블이 있는 출력 없이 단일 레이블에서 프린터를 구성합니다.	사용자가 특정 레이블에서 Oracle Solaris 프린터로 인쇄할 수 있도록 설정합니다. 인쇄 작업이 레이블을 사용하여 표시되지 않습니다.	217 페이지 "레이블이 없는 인쇄 서버에 레이블을 지정하는 방법"
본문 페이지에 표시되는 레이블을 제거합니다.	`tsol_separator.ps` 파일을 수정하여 Trusted Extensions 호스트에서 보내는 모든 인쇄 작업에서 레이블이 있는 본문 페이지가 인쇄되지 않도록 합니다.	218 페이지 "모든 인쇄 작업에서 페이지 레이블을 제거하는 방법"
배너 및 트레일러 페이지를 억제합니다.	특정 사용자가 배너 및 트레일러 페이지 없이 작업을 인쇄할 수 있도록 권한이 부여됩니다.	219 페이지 "특정 사용자에 대해 배너 및 트레일러 페이지를 억제하는 방법"
신뢰할 수 있는 사용자가 레이블 없이 작업을 인쇄할 수 있도록 설정합니다.	특정 사용자 또는 특정 시스템의 모든 사용자가 레이블 없이 작업을 인쇄할 수 있도록 권한이 부여됩니다.	218 페이지 "특정 사용자가 페이지 레이블을 억제할 수 있도록 설정하는 방법"
포스트스크립트 파일 인쇄를 설정합니다.	특정 사용자 또는 특정 시스템의 모든 사용자가 포스트스크립트 파일을 인쇄할 수 있도록 권한이 부여됩니다.	219 페이지 "Trusted Extensions에서 사용자가 포스트스크립트 파일을 인쇄할 수 있도록 설정하는 방법"
인쇄 권한 부여를 지정합니다.	사용자가 기본 인쇄 제한을 무시할 수 있도록 설정합니다.	91 페이지 "편리한 권한 부여를 위해 권한 프로파일을 만드는 방법" 84 페이지 "`policy.conf` 기본값을 수정하는 방법"

▼ 인쇄되는 출력에서 레이블을 제거하는 방법

Trusted Extensions 프린터 모델 스크립트가 없는 프린터는 레이블이 있는 배너나 트레일러 페이지를 인쇄하지 않습니다. 본문 페이지에도 레이블이 포함되지 않습니다.

시작하기 전에 전역 영역에서 보안 관리자 역할을 가진 사용자여야 합니다.

- **해당 레이블에서 다음 중 하나를 수행합니다.**
  - **인쇄 서버에서 배너 인쇄를 완전히 중지합니다.**

    ```
    $ lpadmin -p printer -o nobanner=never
    ```

본문 페이지에는 여전히 레이블이 있습니다.

- **프린터 모델 스크립트를 Oracle Solaris 스크립트로 설정합니다.**

```
$ lpadmin -p printer  \
-m { standard | netstandard | standard_foomatic | netstandard_foomatic }
```

인쇄되는 출력에 레이블이 표시되지 않습니다.

▼ 레이블이 없는 인쇄 서버에 레이블을 지정하는 방법

Oracle Solaris 인쇄 서버는 해당 레이블의 프린터에 액세스하는 Trusted Extensions에 대해 레이블을 지정할 수 있는 레이블이 없는 인쇄 서버입니다. 레이블이 없는 인쇄 서버에 연결된 프린터는 해당 인쇄 서버에 지정된 레이블에서만 작업을 인쇄할 수 있습니다. 작업은 레이블이나 트레일러 페이지 없이 인쇄되며 배너 페이지 없이 인쇄될 수도 있습니다. 작업이 배너 페이지와 함께 인쇄되는 경우 해당 페이지에는 보안 정보가 포함되지 않습니다.

레이블이 없는 인쇄 서버에서 관리되는 프린터에 작업을 보내도록 Trusted Extensions 시스템을 구성할 수 있습니다. 사용자는 보안 관리자가 해당 인쇄 서버에 지정한 레이블에서 레이블이 없는 프린터를 통해 작업을 인쇄할 수 있습니다.

시작하기 전에 전역 영역에서 보안 관리자 역할을 가진 사용자여야 합니다.

1. **해당 범위에서 Solaris Management Console을 엽니다.**

   자세한 내용은 **Trusted Extensions Configuration Guide**의 "Initialize the Solaris Management Console Server in Trusted Extensions"를 참조하십시오.

2. **System Configuration(시스템 구성)에서 Computers and Networks(컴퓨터 및 네트워크) 도구로 이동합니다.**

   암호를 입력하라는 메시지가 나타나면 암호를 제공합니다.

3. **레이블이 없는 템플리트를 인쇄 서버에 지정합니다.**

   자세한 내용은 176 페이지 "호스트 또는 호스트 그룹에 보안 템플리트를 지정하는 방법"을 참조하십시오.

   레이블을 선택합니다. 이 레이블에서 작업하는 사용자는 인쇄 서버의 해당 레이블에서 Oracle Solaris 프린터로 인쇄 작업을 보낼 수 있습니다. 페이지에 레이블이 인쇄되지 않으며 배너 및 트레일러 페이지도 인쇄 작업의 일부가 아닙니다.

예 15–2 레이블이 없는 프린터에 공용 인쇄 작업 보내기

일반 대중이 사용할 수 있는 파일은 레이블이 없는 프린터에서 인쇄하기에 적합합니다. 이 예에서는 마케팅 담당자가 페이지의 맨 위와 맨 아래에 레이블을 인쇄하지 않는 문서를 생성하려고 합니다.

보안 관리자가 레이블이 없는 호스트 유형 템플리트를 Oracle Solaris 인쇄 서버에 지정합니다. 이 템플리트는 예 13–6에 설명되어 있습니다. 이 템플리트의 임의의 레이블은 PUBLIC입니다. 프린터 pr-nolabel1이 이 인쇄 서버에 연결되어 있습니다. PUBLIC 영역 사용자의 인쇄 작업이 pr-nolabel1 프린터에서 레이블 없이 인쇄됩니다. 프린터 설정에 따라 작업에 배너 페이지가 포함되거나 포함되지 않을 수 있습니다. 배너 페이지에는 보안 정보가 포함되지 않습니다.

▼ 모든 인쇄 작업에서 페이지 레이블을 제거하는 방법

이 절차는 Trusted Extensions 프린터의 모든 인쇄 작업에 대해 인쇄 작업의 본문 페이지에 레이블을 표시하지 않도록 합니다.

시작하기 전에 전역 영역에서 보안 관리자 역할을 가진 사용자여야 합니다.

1. **/usr/lib/lp/postscript/tsol_separator.ps 파일을 편집합니다.**
   신뢰할 수 있는 편집기를 사용합니다. 자세한 내용은 54 페이지 “Trusted Extensions에서 관리 파일을 편집하는 방법”을 참조하십시오.

2. **/PageLabel의 정의를 찾습니다.**
   다음 라인을 찾습니다.

   ```
   %% To eliminate page labels completely, change this line to
   %% set the page label to an empty string: /PageLabel () def
   /PageLabel Job_PageLabel def
   ```

   주 – 사용자 사이트에서는 Job_PageLabel 값이 다를 수 있습니다.

3. **/PageLabel의 값을 일련의 빈 괄호로 대체합니다.**

   ```
   /PageLabel () def
   ```

▼ 특정 사용자가 페이지 레이블을 억제할 수 있도록 설정하는 방법

이 절차를 통해 권한이 부여된 사용자 또는 역할은 Trusted Extensions 프린터에서 각 본문 페이지의 맨 위와 맨 아래에 레이블을 표시하지 않고 작업을 인쇄할 수 있습니다. 사용자가 작업할 수 있는 모든 레이블에 대해 페이지 레이블이 억제됩니다.

시작하기 전에 전역 영역에서 보안 관리자 역할을 가진 사용자여야 합니다.

1. **페이지 레이블 없이 작업을 인쇄할 수 있도록 허용되는 사용자를 결정합니다.**

2. **이러한 사용자 및 역할이 페이지 레이블 없이 작업을 인쇄할 수 있도록 권한을 부여합니다.**

   Print without Label(레이블 없이 인쇄) 권한 부여를 포함하는 권한 프로파일을 이러한 사용자와 역할에 지정합니다. 자세한 내용은 91 페이지 "편리한 권한 부여를 위해 권한 프로파일을 만드는 방법"을 참조하십시오.

3. **사용자 또는 역할에 다음 `lp` 명령을 사용하여 인쇄 작업을 제출하도록 지시합니다.**

```
% lp -o nolabels staff.mtg.notes
```

▼ 특정 사용자에 대해 배너 및 트레일러 페이지를 억제하는 방법

시작하기 전에 전역 영역에서 보안 관리자 역할을 가진 사용자여야 합니다.

1. **Print without Banner(배너 없이 인쇄) 권한 부여를 포함하는 권한 프로파일을 만듭니다.**

   이 프로파일을 배너 및 트레일러 페이지 없이 인쇄할 수 있도록 허용되는 각 사용자 또는 역할에 지정합니다.

   자세한 내용은 91 페이지 "편리한 권한 부여를 위해 권한 프로파일을 만드는 방법"을 참조하십시오.

2. **사용자 또는 역할에 다음 `lp` 명령을 사용하여 인쇄 작업을 제출하도록 지시합니다.**

```
% lp -o nobanner staff.mtg.notes
```

▼ Trusted Extensions에서 사용자가 포스트스크립트 파일을 인쇄할 수 있도록 설정하는 방법

시작하기 전에 전역 영역에서 보안 관리자 역할을 가진 사용자여야 합니다.

- **다음 세 가지 방법 중 하나를 사용하여 사용자가 포스트스크립트 파일을 인쇄할 수 있도록 설정합니다.**

  - **시스템에서 포스트스크립트 인쇄를 사용으로 설정하려면 `/etc/default/print` 파일을 수정합니다.**

    a. **`/etc/default/print` 파일을 만들거나 수정합니다.**

       신뢰할 수 있는 편집기를 사용합니다. 자세한 내용은 54 페이지 "Trusted Extensions에서 관리 파일을 편집하는 방법"을 참조하십시오.

    b. **다음 항목을 입력합니다.**

```
PRINT_POSTSCRIPT=1
```

c. **파일을 저장하고 편집기를 닫습니다.**

- **모든 사용자가 시스템에서 포스트스크립트 파일을 인쇄할 수 있도록 권한을 부여하려면 `/etc/security/policy.conf` 파일을 수정합니다.**

  a. **`policy.conf` 파일을 수정합니다.**

  신뢰할 수 있는 편집기를 사용합니다. 자세한 내용은 54 페이지 “Trusted Extensions에서 관리 파일을 편집하는 방법”을 참조하십시오.

  b. **`solaris.print.ps` 권한 부여를 추가합니다.**

  `AUTHS_GRANTED=`*other-authorizations*`,solaris.print.ps`

  c. **파일을 저장하고 편집기를 닫습니다.**

- **사용자나 역할이 어떤 시스템에서나 포스트스크립트 파일을 인쇄할 수 있도록 설정하려면 이러한 사용자와 역할에 해당 권한을 부여하면 됩니다.**

  `Print Postscript`(포스트스크립트 인쇄) 권한 부여를 포함하는 프로파일을 이러한 사용자와 역할에 지정합니다. 자세한 내용은 91 페이지 “편리한 권한 부여를 위해 권한 프로파일을 만드는 방법”을 참조하십시오.

예 15–3 공용 시스템에서 포스트스크립트 인쇄 설정

다음 예에서 보안 관리자는 공개 키오스크가 `PUBLIC` 레이블에서 작동하도록 제한합니다. 또한 이 시스템에는 관심 있는 항목을 여는 몇 개의 아이콘이 있습니다. 이러한 항목을 인쇄할 수 있습니다.

보안 관리자는 해당 시스템에서 `/etc/default/print` 파일을 만듭니다. 이 파일에는 포스트스크립트 파일 인쇄를 설정할 수 있는 하나의 항목이 있습니다. 어떤 사용자도 `Print Postscript`(포스트스크립트 인쇄) 권한 부여가 필요하지 않습니다.

```
# vi /etc/default/print

# PRINT_POSTSCRIPT=0
PRINT_POSTSCRIPT=1
```

◆ ◆ ◆ 16장

16 Trusted Extensions의 장치(개요)

이 장에서는 Trusted Extensions에서 장치 보호에 제공하는 확장에 대해 설명합니다.

- 221 페이지 “Trusted Extensions 소프트웨어로 장치 보호”
- 223 페이지 “Device Allocation Manager(장치 할당 관리자) GUI”
- 225 페이지 “Trusted Extensions에서 장치 보안 적용”
- 226 페이지 “Trusted Extensions의 장치(참조)”

Trusted Extensions 소프트웨어로 장치 보호

Oracle Solaris 시스템에서는 할당과 권한 부여로 장치를 보호할 수 있습니다. 기본적으로 일반 사용자가 권한 부여 없이 장치를 사용할 수 있습니다. Trusted Extensions 기능으로 구성된 시스템에서는 Oracle Solaris OS의 장치 보호 방식을 사용합니다.

그러나 기본적으로 Trusted Extensions에서는 사용할 장치를 할당해야 하며 사용자는 장치를 사용할 수 있게 권한 부여되어야 합니다. 또한 장치는 레이블로 보호됩니다. Trusted Extensions에서는 관리자가 장치를 관리하는 데 사용할 수 있는 그래픽 사용자 인터페이스(GUI)를 제공합니다. 사용자가 장치를 할당하는 데도 동일할 인터페이스가 사용됩니다.

주 – Trusted Extensions에서는 사용자가 `allocate` 및 `deallocate` 명령을 사용할 수 없습니다. 사용자는 Device Allocation Manager(장치 할당 관리자)를 사용해야 합니다. Solaris Trusted Extensions(JDS)에서 GUI의 제목은 Device Manager(장치 관리자)입니다.

Oracle Solaris에서 장치 보호에 대한 자세한 내용은 **System Administration Guide: Security Services**의 4 장, “Controlling Access to Devices (Tasks)”를 참조하십시오.

Trusted Extensions로 구성된 시스템에서는 두 역할이 장치를 보호합니다.

- 시스템 관리자 역할은 주변 기기에 대한 액세스를 제어합니다.

  시스템 관리자는 장치를 할당 가능으로 설정합니다. 시스템 관리자가 할당 불가능으로 설정하는 장치는 누구도 사용할 수 없습니다. 할당 가능한 장치는 권한 부여된 사용자만이 할당할 수 있습니다.
- 보안 관리자 역할은 장치에 액세스할 수 있는 레이블을 제한하고 장치 정책을 설정합니다. 보안 관리자는 장치를 할당할 수 있게 권한 부여된 사용자를 결정합니다.

다음은 Trusted Extensions 소프트웨어를 사용한 주요 장치 제어 기능입니다.

- 기본적으로 Trusted Extensions 시스템에서 권한이 부여되지 않은 사용자는 테이프 드라이브, CD-ROM 드라이브 또는 디스켓 드라이브 등의 장치를 할당할 수 없습니다.

  Allocate Device(장치 할당) 권한이 있는 일반 사용자는 장치를 할당하는 레이블의 정보를 가져오거나 내보낼 수 있습니다.
- 사용자가 직접 로그인한 경우 Device Allocation Manager(장치 할당 관리자)를 사용하여 장치를 할당합니다. 사용자가 원격으로 장치를 할당하려면 전역 영역에 액세스할 수 있어야 합니다. 일반적으로 역할만 전역 영역에 액세스할 수 있습니다.
- 보안 관리자가 각 장치의 레이블 범위를 제한할 수 있습니다. 일반 사용자는 레이블 범위에 해당 사용자가 작업할 수 있는 레이블이 포함된 장치에만 액세스할 수 있습니다. 장치의 기본 레이블 범위는 `ADMIN_LOW` ~ `ADMIN_HIGH`입니다.
- 할당 가능한 장치와 할당 불가능한 장치 모두에 대해 레이블 범위를 제한할 수 있습니다. 할당 불가능한 장치는 프레임 버퍼와 포인터 등의 장치입니다.

장치 레이블 범위

사용자가 민감한 정보를 복사하지 못하도록 할당 가능한 장치마다 레이블 범위가 있습니다. 할당 가능한 장치를 사용하려면 사용자가 해당 장치의 레이블 범위 내에 있는 레이블에서 작업 중이어야 합니다. 그렇지 않으면 할당이 거부됩니다. 장치가 사용자에게 할당된 동안 가져오거나 내보내는 데이터에는 사용자의 현재 레이블이 적용됩니다. 장치 할당이 해제될 때 내보낸 데이터의 레이블이 표시됩니다. 사용자가 내보낸 데이터가 들어 있는 매체에 물리적인 표시를 해야 합니다.

장치의 레이블 범위 효과

콘솔을 통해 직접 로그인 액세스를 제한하려면 보안 관리자가 프레임 버퍼에 제한된 레이블 범위를 설정합니다.

예를 들어, 제한된 레이블 범위를 지정하여 공용으로 액세스 가능한 시스템으로 액세스를 제한할 수 있습니다. 레이블 범위는 사용자가 프레임 버퍼의 레이블 범위 내에 있는 레이블의 시스템에만 액세스할 수 있게 합니다.

호스트에 로컬 프린터가 있는 경우 프린터의 제한된 레이블 범위에 의해 해당 프린터에서 인쇄할 수 있는 작업이 제한됩니다.

장치 액세스 정책

Trusted Extensions는 Oracle Solaris와 동일한 장치 정책을 따릅니다. 보안 관리자가 기본 정책을 변경하고 새 정책을 정의할 수 있습니다. `getdevpolicy` 명령은 장치 정책에 대한 정보를 검색하고 `update_drv` 명령은 장치 정책을 변경합니다. 자세한 내용은 **System Administration Guide: Security Services**의 "Configuring Device Policy (Task Map)"를 참조하십시오. `getdevpolicy(1M)` 및 `update_drv(1M)` 매뉴얼 페이지도 참조하십시오.

Device-Clean 스크립트

device-clean 스크립트는 장치가 할당되거나 할당 해제될 때 실행됩니다. Oracle Solaris에서는 테이프 드라이브, CD-ROM 및 디스켓 드라이브에 대한 스크립트를 제공합니다. 사이트에서 시스템에 할당 가능한 장치 유형을 추가할 경우 추가된 장치에 스크립트가 필요할 수 있습니다. 기존 스크립트를 보려면 `/etc/security/lib` 디렉토리로 이동합니다. 자세한 내용은 **System Administration Guide: Security Services**의 "Device-Clean Scripts"를 참조하십시오.

Trusted Extensions 소프트웨어의 경우에는 device-clean 스크립트가 특정 요구 사항을 충족해야 합니다. 이 요구 사항은 `device_clean(5)` 매뉴얼 스크립트에 설명되어 있습니다.

Device Allocation Manager(장치 할당 관리자) GUI

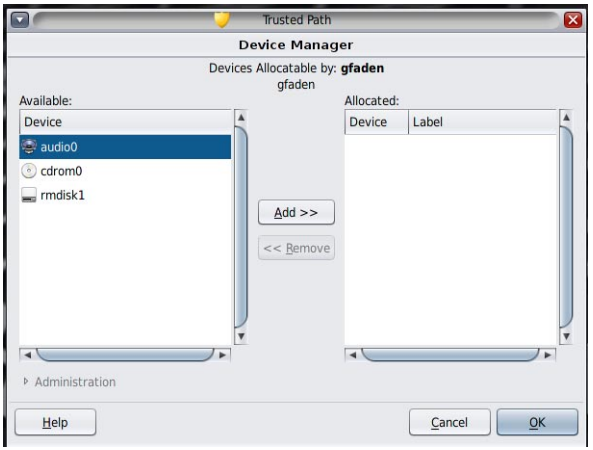
Device Allocation Manager(장치 할당 관리자)는 관리자가 할당 가능한 장치와 할당 불가능한 장치를 관리하는 데 사용됩니다. 일반 사용자가 장치를 할당하고 할당 해제하는 데도 Device Allocation Manager(장치 할당 관리자)가 사용됩니다. 사용자에게 장치 할당 권한이 있어야 합니다. Solaris Trusted Extensions(CDE) 작업 공간에서는 전면 패널에서 Device Allocation Manager(장치 할당 관리자)를 엽니다. 다음과 같은 아이콘을 사용합니다.

장치 할당 

Solaris Trusted Extensions(JDS) 작업 공간에서는 GUI를 Device Manager(장치 관리자)라고 합니다. Trusted Path(신뢰할 수 있는 경로) 메뉴에서 Allocate Device(장치 할당)를 선택하여 이 GUI를 시작합니다. Trusted CDE에서도 Trusted Path(신뢰할 수 있는 경로)

메뉴에서 GUI를 시작할 수 있습니다. 다음 그림은 audio 장치를 할당할 수 있는 사용자가 열어 놓은 Device Allocation Manager(장치 할당 관리자)를 보여줍니다.

그림 16–1 사용자가 열어 놓은 Device Allocation Manager(장치 할당 관리자)



장치를 할당할 수 있게 권한 부여되지 않은 사용자의 경우 빈 목록이 표시됩니다. 할당 가능한 장치가 현재 다른 사용자에 의해 할당되거나 오류 상태일 때도 빈 목록이 표시됩니다. Available Devices(사용 가능한 장치) 목록에 장치가 표시되지 않는 경우 담당 관리자에게 문의해야 합니다.

Device Administration(장치 관리) 기능은 장치 관리에 필요한 권한 부여가 하나 이상 있는 역할만 사용할 수 있습니다. 관리 권한 부여는 Configure Device Attributes(장치 속성 구성)와 Revoke or Reclaim Device(장치 해지 또는 재생 이용)입니다. 다음 그림은 Device Allocation Administration(장치 할당 관리) 대화 상자를 보여줍니다.

Solaris Trusted Extensions(JDS)에서는 Device Administration(장치 관리) 버튼을 Administration(관리)이라고 합니다.

Trusted Extensions에서 장치 보안 적용

보안 관리자가 장치를 할당할 수 있는 사용자를 결정하고, 장치를 사용할 수 있게 권한 부여된 사용자가 교육을 받았는지 확인합니다. 이러한 사용자는 다음을 수행할 수 있는 것으로 간주됩니다.

- 민감한 정보를 내보낸 경우 다른 사용자가 무단으로 보지 못하도록 해당 정보가 들어 있는 매체에 적절히 라벨을 붙이고 매체를 처리할 수 있습니다.

  예를 들어, NEED TO KNOW ENGINEERING 레이블의 정보가 디스켓에 저장된 경우 이 정보를 내보내는 사용자는 디스크에 NEED TO KNOW ENGINEERING이라는 물리적인 표시를 해야 합니다. 디스켓은 해당 엔지니어링 그룹의 구성원만 액세스할 수 있는 곳에 보관해야 합니다.
- 이러한 장치의 매체에서 가져오거나 읽는 모든 정보에 대해 레이블을 적절히 유지 관리해야 합니다.

  권한 부여된 사용자는 가져오는 정보의 레이블과 일치하는 레이블의 장치를 할당해야 합니다. 예를 들어, 사용자가 PUBLIC의 디스켓 드라이브를 할당하는 경우 사용자는 PUBLIC이라는 레이블의 정보만 가져와야 합니다.

보안 관리자는 이러한 보안 요구 사항을 준수하게 하는 역할도 담당합니다.

Trusted Extensions의 장치(참조)

Trusted Extensions 장치 보호에서는 Oracle Solaris 인터페이스와 Trusted Extensions 인터페이스를 사용합니다.

Oracle Solaris 명령줄 인터페이스는 **System Administration Guide: Security Services**의 "Device Protection (Reference)"을 참조하십시오.

Device Allocation Manager(장치 할당 관리자)에 액세스할 수 없는 관리자는 명령줄을 사용하여 할당 가능한 장치를 관리할 수 있습니다. `allocate` 및 `deallocate` 명령에는 관리 옵션이 있습니다. 예는 **System Administration Guide: Security Services**의 "Forcibly Allocating a Device"와 **System Administration Guide: Security Services**의 "Forcibly Deallocating a Device"를 참조하십시오.

Trusted Extensions 명령줄 인터페이스는 `add_allocatable(1M)` 및 `remove_allocatable(1M)` 매뉴얼 페이지를 참조하십시오.

◆ ◆ ◆ 17장

17 Trusted Extensions에 대한 장치 관리(작업)

이 장에서는 Trusted Extensions로 구성된 시스템에서 장치를 관리하고 사용하는 방법을 설명합니다.

- 227 페이지 “Trusted Extensions에서 장치 취급(작업 맵)”
- 228 페이지 “Trusted Extensions에서 장치 사용(작업 맵)”
- 228 페이지 “Trusted Extensions에서 장치 관리(작업 맵)”
- 237 페이지 “Trusted Extensions에서 장치 권한 부여 사용자 정의(작업 맵)”

Trusted Extensions에서 장치 취급(작업 맵)

다음 작업 맵에서는 관리자 및 사용자가 주변 기기를 취급하기 위한 작업 맵에 대한 링크를 제공합니다.

작업	설명	수행 방법
장치를 사용합니다.	역할이나 일반 사용자로 장치를 사용합니다.	228 페이지 “Trusted Extensions에서 장치 사용(작업 맵)”
장치를 관리합니다.	일반 사용자에 대해 장치를 구성합니다.	228 페이지 “Trusted Extensions에서 장치 관리(작업 맵)”
장치 권한 부여를 사용자 정의합니다.	보안 관리자 역할은 새 권한 부여를 만들어 장치에 추가한 후 권한 프로파일에 넣고 이 프로파일을 사용자에게 지정합니다.	237 페이지 “Trusted Extensions에서 장치 권한 부여 사용자 정의(작업 맵)”

Trusted Extensions에서 장치 사용(작업 맵)

Trusted Extensions의 모든 역할은 장치를 할당할 수 있게 권한 부여됩니다. 사용자와 같이 역할도 Device Allocation Manager(장치 할당 관리자)를 사용해야 합니다. Oracle Solaris `allocate` 명령은 Trusted Extensions에서 작동하지 않습니다. 다음 작업 맵에서는 Trusted Extensions에서 장치 사용을 위한 사용자 절차에 대한 링크를 제공합니다.

작업	수행 방법
장치를 할당하고 할당 해제합니다.	**Trusted Extensions User's Guide**의 "How to Allocate a Device in Trusted Extensions" **Trusted Extensions User's Guide**의 "Workspace Switch Area"
휴대용 매체를 사용하여 파일을 전송합니다.	**Trusted Extensions Configuration Guide**의 "How to Copy Files From Portable Media in Trusted Extensions" **Trusted Extensions Configuration Guide**의 "How to Copy Files to Portable Media in Trusted Extensions"

Trusted Extensions에서 장치 관리(작업 맵)

다음 작업 맵에서는 사이트에서 장치를 보호하는 절차를 설명합니다.

작업	설명	수행 방법
장치 정책을 설정하거나 수정합니다.	장치에 액세스하는 데 필요한 권한을 변경합니다.	**System Administration Guide: Security Services**의 "Configuring Device Policy (Task Map)"
장치를 할당할 수 있는 권한 부여를 사용자에게 부여합니다.	보안 관리자 역할은 Allocate Device(장치 할당) 권한이 있는 권한 프로파일을 사용자에게 지정합니다.	**System Administration Guide: Security Services**의 "How to Authorize Users to Allocate a Device"
	보안 관리자 역할은 사이트별 권한이 있는 프로파일을 사용자에게 지정합니다.	237 페이지 "Trusted Extensions에서 장치 권한 부여 사용자 정의(작업 맵)"
장치를 구성합니다.	장치를 보호하기 위한 보안 기능을 선택합니다.	229 페이지 "Trusted Extensions에서 장치를 구성하는 방법"
장치를 해지하거나 재생 이용합니다.	Device Allocation Manager(장치 할당 관리자)로 장치를 사용할 수 있게 만듭니다.	232 페이지 "Trusted Extensions에서 장치를 해지하거나 재생 이용하는 방법"
	Oracle Solaris 명령으로 장치를 사용할 수 있게 만들거나 사용할 수 없게 만듭니다.	**System Administration Guide: Security Services**의 "Forcibly Allocating a Device" **System Administration Guide: Security Services**의 "Forcibly Deallocating a Device"

작업	설명	수행 방법
할당 가능한 장치에 대한 액세스를 금지합니다.	장치에 대한 세분화된 액세스 제어를 제공합니다.	예 17–4
	할당 가능한 장치에 대한 모든 사용자의 액세스를 거부합니다.	예 17–1
프린터와 프레임 버퍼를 보호합니다.	할당 불가능한 장치를 할당할 수 없게 합니다.	233 페이지 “Trusted Extensions에서 할당 불가능한 장치를 보호하는 방법”
직렬 로그인 장치를 구성합니다.	직렬 포트로 로그인을 사용으로 설정합니다.	234 페이지 “로그인을 위한 직렬 회선을 구성하는 방법”
CD 플레이어 프로그램이 사용되게 사용으로 설정합니다.	음악 CD를 넣으면 오디오 플레이어 프로그램이 자동으로 열리게 사용으로 설정합니다.	235 페이지 “Trusted CDE에서 사용할 오디오 플레이어 프로그램을 구성하는 방법”
File Manager(파일 관리자)가 표시되지 않게 합니다.	장치가 할당된 후 File Manager(파일 관리자)가 표시되지 않게 합니다.	236 페이지 “장치 할당 후 File Manager(파일 관리자)가 표시되지 않게 하는 방법”
새 device-clean 스크립트를 사용합니다.	적당한 위치에 새 스크립트를 넣습니다.	237 페이지 “Trusted Extensions에서 Device_Clean 스크립트를 추가하는 방법”

▼ Trusted Extensions에서 장치를 구성하는 방법

기본적으로 할당 가능한 장치는 `ADMIN_LOW` ~ `ADMIN_HIGH`의 레이블 범위를 가지며 사용하도록 할당되어야 합니다. 또한 장치를 할당할 수 있는 권한 부여가 사용자에게 있어야 합니다. 이러한 기본값은 변경할 수 있습니다.

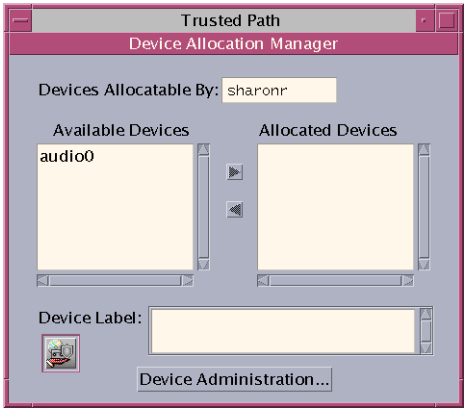
다음 장치를 사용하도록 할당할 수 있습니다.

- `audio`*n* – 마이크로폰 및 스피커를 나타냅니다.
- `cdrom`*n* – CD-ROM 드라이브를 나타냅니다.
- `floppy`*n* – 디스켓 드라이브를 나타냅니다.
- `mag_tape`*n* – 테이프 드라이브(스트리밍)를 나타냅니다.
- `rmdisk`*n* – 이동식 디스크(예: JAZ 또는 ZIP 드라이브) 또는 USB 핫플러그 가능 매체를 나타냅니다.

시작하기 전에 전역 영역에서 보안 관리자 역할을 가진 사용자여야 합니다.

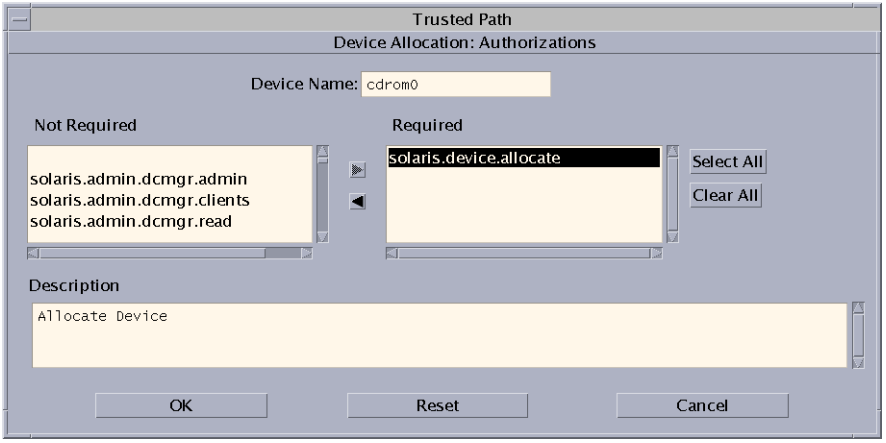
1 **Trusted Path(신뢰할 수 있는 경로) 메뉴에서 Allocate Device(장치 할당)를 선택합니다.**

Device Allocation Manager(장치 할당 관리자)가 나타납니다.



2 **기본 보안 설정을 확인합니다.**

Device Administration(장치 관리)을 누르고 장치를 강조 표시합니다. 다음 그림은 `root` 역할이 보고 있는 오디오 장치를 보여줍니다.



3 **(옵션) 장치의 레이블 범위를 제한합니다.**

a. **최소 레이블을 설정합니다.**

Min Label(최소 레이블) 버튼을 누릅니다. 레이블 구축기에서 최소 레이블을 선택합니다. 레이블 구축기에 대한 자세한 내용은 43 페이지 “Trusted Extensions의 레이블 구축기”를 참조하십시오.

b. 최대 레이블을 설정합니다.

Max Label(최대 레이블)... 버튼을 누릅니다. 레이블 구축기에서 최대 레이블을 선택합니다.

4 장치를 로컬로 할당할 수 있는지 여부를 지정합니다.

Device Allocation Configuration(장치 할당 구성) 대화 상자의 For Allocations From Trusted Path(신뢰할 수 있는 경로에서 할당)에 있는 Allocatable By(가능한 할당자) 목록에서 옵션을 선택합니다. 기본적으로 Authorized Users(권한 부여된 사용자) 옵션이 선택되어 있습니다. 따라서 장치는 할당 가능하며 사용자가 권한 부여되어야 합니다.

- **장치를 할당할 수 없게 하려면 No Users(사용자 없음)를 누릅니다.**

  할당할 수 없어야 하는 프린터, 프레임 버퍼 또는 기타 장치를 구성할 때 No Users(사용자 없음)를 선택합니다.

- **권한 부여 없이도 장치를 할당할 수 있게 하려면 All Users(모든 사용자)를 누릅니다.**

5 장치를 원격으로 할당할 수 있는지 여부를 지정합니다.

For Allocations From Non-Trusted Path(신뢰할 수 없는 경로에서 할당) 구역에 있는 Allocatable By(가능한 할당자) 목록에서 옵션을 선택합니다. 기본적으로 Same As Trusted Path(신뢰할 수 있는 경로와 같음) 옵션이 선택되어 있습니다.

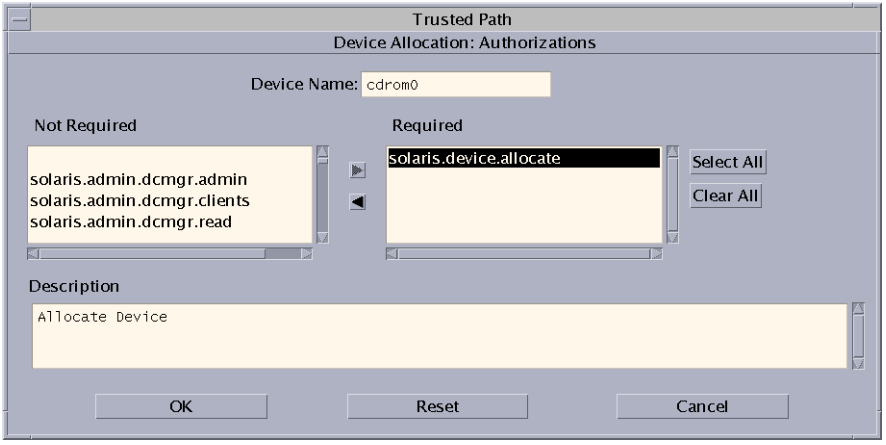
- **사용자 권한 부여가 필요하도록 하려면 Allocatable by Authorized Users(권한 부여된 사용자가 할당 가능)를 선택합니다.**

- **원격 사용자가 장치를 할당할 수 없게 하려면 No Users(사용자 없음)를 선택합니다.**

- **누구나 장치를 할당할 수 있게 하려면 All Users(모든 사용자)를 선택합니다.**

6 **장치를 할당할 수 있고 사이트에서 새 장치 권한 부여를 만든 경우 적당한 권한 부여를 선택합니다.**

다음 대화 상자는 `cdrom0` 장치를 할당하려면 `solaris.device.allocate` 권한 부여가 필요함을 나타냅니다.



사이트별 장치 권한 부여를 만들고 사용하려면 237 페이지 “Trusted Extensions에서 장치 권한 부여 사용자 정의(작업 맵)”를 참조하십시오.

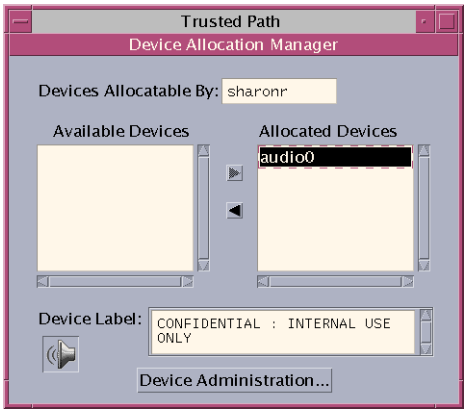
7 **변경 사항을 저장하려면 OK(확인)를 누릅니다.**

▼ Trusted Extensions에서 장치를 해지하거나 재생 이용하는 방법

장치가 Device Allocation Manager(장치 할당 관리자)에 나열되지 않을 경우 이미 할당되었거나 할당 오류 상태일 수 있습니다. 시스템 관리자는 사용할 장치를 복구할 수 있습니다.

시작하기 전에 전역 영역에서 시스템 관리자 역할을 가진 사용자여야 합니다. 이 역할에는 `solaris.device.revoke` 권한 부여가 포함됩니다.

1. **Trusted Path(신뢰할 수 있는 경로) 메뉴에서 Allocate Device(장치 할당)를 선택합니다.**
   다음 그림에서는 오디오 장치가 이미 사용자에게 할당되었습니다.



2. **Device Administration(장치 관리) 버튼을 누릅니다.**

3. **장치의 상태를 확인합니다.**
   장치 이름을 선택하고 State(상태) 필드를 확인합니다.

   - **State(상태) 필드가 Allocate Error State(할당 오류 상태)인 경우 Reclaim(재생 이용) 버튼을 누릅니다.**
   - **State(상태) 필드가 Allocated(할당됨)인 경우 다음 중 하나를 수행합니다.**
     - **Owner(소유자) 필드의 사용자에게 장치를 할당 해제하도록 요청합니다.**
     - **Revoke(해지) 버튼을 눌러 장치를 강제로 할당 해제합니다.**

4. **Device Allocation Manager(장치 할당 관리자)를 닫습니다.**

▼ Trusted Extensions에서 할당 불가능한 장치를 보호하는 방법

Device Configuration(장치 구성) 대화 상자의 Allocatable By(가능한 할당자) 구역에 있는 No Users(사용자 없음) 옵션은 사용을 위해 할당할 필요가 없는 프레임 버퍼와 프린터에 가장 자주 사용됩니다.

시작하기 전에 전역 영역에서 보안 관리자 역할을 가진 사용자여야 합니다.

1. **Trusted Path(신뢰할 수 있는 경로) 메뉴에서 Allocate Device(장치 할당)를 선택합니다.**

2 **Device Allocation Manager(장치 할당 관리자)에서 Device Administration(장치 관리) 버튼을 누릅니다.**

3 **새 프린터나 프레임 버퍼를 선택합니다.**

a. **장치를 할당할 수 없게 하려면 No Users(사용자 없음)를 누릅니다.**

b. **(옵션) 장치의 레이블 범위를 제한합니다.**

i. **최소 레이블을 설정합니다.**

Min Label(최소 레이블)... 버튼을 누릅니다. 레이블 구축기에서 최소 레이블을 선택합니다. 레이블 구축기에 대한 자세한 내용은 43 페이지 “Trusted Extensions의 레이블 구축기”를 참조하십시오.

ii. **최대 레이블을 설정합니다.**

Max Label(최대 레이블)... 버튼을 누릅니다. 레이블 구축기에서 최대 레이블을 선택합니다.

예 17–1 오디오 장치의 원격 할당 금지

Allocatable By(가능한 할당자) 구역의 No Users(사용자 없음) 옵션은 원격 사용자가 원격 시스템 주변의 대화를 들을 수 없도록 합니다.

보안 관리자는 Device Allocation Manager(장치 할당 관리자)에서 오디오 장치를 다음과 같이 구성합니다.

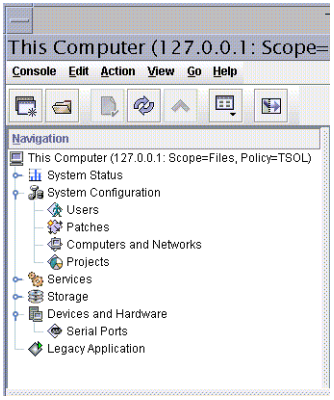
```
Device Name: audio
For Allocations From: Trusted Path
Allocatable By: Authorized Users
Authorizations: solaris.device.allocate

Device Name: audio
For Allocations From: Non-Trusted Pathh
Allocatable By: No Users
```

▼ 로그인을 위한 직렬 회선을 구성하는 방법

시작하기 전에 전역 영역에서 보안 관리자 역할을 가진 사용자여야 합니다.

1 **Files(파일) 범위에서 Solaris Management Console을 엽니다.**

그림 17–1 Solaris Management Console의 Serial Ports(직렬 포트) 도구



2 **Devices and Hardware(장치 및 하드웨어)에서 Serial Ports(직렬 포트)로 이동합니다.**
암호를 입력하라는 메시지가 나타나면 암호를 제공합니다. 온라인 도움말에 따라 직렬 포트를 구성합니다.

3 **기본 레이블 범위를 변경하려면 Device Allocation Manager(장치 할당 관리자)를 엽니다.**
기본 레이블 범위는 `ADMIN_LOW` ~ `ADMIN_HIGH`입니다.

예 17–2 직렬 포트의 레이블 범위 제한

직렬 로그인 장치를 만든 후 보안 관리자는 직렬 포트의 레이블 범위를 단일 레이블인 `Public`으로 제한합니다. 관리자는 Device Administration(장치 관리) 대화 상자에서 다음 값을 설정합니다.

```
Device Name: /dev/term/[a|b]
Device Type: tty
Clean Program: /bin/true
Device Map: /dev/term/[a|b]
Minimum Label: Public
Maximum Label: Public
Allocatable By: No Users
```

▼ Trusted CDE에서 사용할 오디오 플레이어 프로그램을 구성하는 방법

다음은 사용자가 음악 CD를 넣으면 Trusted CDE 작업 공간에서 오디오 플레이어가 자동으로 열리게 하는 절차입니다. 사용자의 절차는 **Trusted Extensions User's Guide**의 "How to Allocate a Device in Trusted Extensions"에 나와 있는 예를 참조하십시오.

주 – 사용자는 신뢰할 수 없는 작업 공간에서 휴대용 매체의 동작을 지정할 때와 같이 Trusted JDS 작업 공간에서 해당 동작을 지정합니다.

시작하기 전에 전역 영역에서 시스템 관리자 역할을 가진 사용자여야 합니다.

1. **`/etc/rmmount.conf` 파일을 편집합니다.**
   신뢰할 수 있는 편집기를 사용합니다. 자세한 내용은 54 페이지 “Trusted Extensions에서 관리 파일을 편집하는 방법”을 참조하십시오.
2. **사이트의 CD 플레이어 프로그램을 파일의 `cdrom` 작업에 추가합니다.**
   `action` *media* `action_`*program*`.so` *path-to-program*

예 17–3 **사용할 오디오 플레이어 프로그램 구성**

다음 예에서 시스템 관리자는 시스템의 모든 사용자가 `workman` 프로그램을 사용할 수 있도록 합니다. `workman` 프로그램은 오디오 플레이어 프로그램입니다.

```
# /etc/rmmount.conf file
action cdrom action_workman.so /usr/local/bin/workman
```

▼ 장치 할당 후 File Manager(파일 관리자)가 표시되지 않게 하는 방법

기본적으로 장치가 마운트되면 File Manager(파일 관리자)가 표시됩니다. 파일 시스템이 있는 장치를 마운트하지 않는 경우 File Manager(파일 관리자)가 표시되지 않도록 할 수 있습니다.

시작하기 전에 전역 영역에서 시스템 관리자 역할을 가진 사용자여야 합니다.

1. **`/etc/rmmount.conf` 파일을 편집합니다.**
   신뢰할 수 있는 편집기를 사용합니다. 자세한 내용은 54 페이지 “Trusted Extensions에서 관리 파일을 편집하는 방법”을 참조하십시오.
2. **다음 `filemgr` 작업을 찾습니다.**

   ```
   action cdrom action_filemgr.so
   action floppy action_filemgr.so
   ```
3. **해당하는 작업을 주석 처리합니다.**
   다음 예에서는 `cdrom` 및 `diskette` 장치에 대한 `action_filemgr.so` 작업이 주석 처리되었습니다.

   ```
   # action cdrom action_filemgr.so
   # action floppy action_filemgr.so
   ```

CDROM이나 디스켓이 할당될 때는 File Manager(파일 관리자)가 표시되지 않습니다.

▼ Trusted Extensions에서 Device_Clean 스크립트를 추가하는 방법

장치가 만들어질 때 `device_clean` 스크립트를 지정하지 않을 경우 기본 스크립트인 `/bin/true`가 사용됩니다.

시작하기 전에 물리적 장치에서 사용 가능한 데이터를 모두 비우고 성공 시 `0`을 반환하는 스크립트를 준비합니다. 휴대용 매체가 있는 장치의 경우 사용자가 매체를 꺼내지 않으면 스크립트에서 매체 꺼내기를 시도합니다. 매체가 꺼내지지 않을 경우 스크립트는 장치를 할당 오류 상태로 설정합니다. 요구 사항에 대한 자세한 내용은 `device_clean(5)` 매뉴얼 페이지를 참조하십시오.

전역 영역에서 `root` 역할을 가진 사용자여야 합니다.

1. **스크립트를 `/etc/security/lib` 디렉토리에 복사합니다.**
2. **Device Administration(장치 관리) 대화 상자에서 스크립트의 전체 경로를 지정합니다.**
   a. **Device Allocation Manager(장치 할당 관리자)를 엽니다.**
   b. **Device Administration(장치 관리) 버튼을 누릅니다.**
   c. **장치의 이름을 선택하고 Configure(구성) 버튼을 누릅니다.**
   d. **Clean Program(정리 프로그램) 필드에 스크립트의 전체 경로를 지정합니다.**
3. **변경 사항을 저장합니다.**

Trusted Extensions에서 장치 권한 부여 사용자 정의(작업 맵)

다음 작업 맵에서는 사이트에서 장치 권한 부여를 변경하는 절차를 설명합니다.

작업	설명	수행 방법
새 장치 권한 부여를 만듭니다.	사이트별 권한 부여를 만듭니다.	238 페이지 “새 장치 권한 부여를 만드는 방법”
장치에 권한 부여를 추가합니다.	선택한 장치에 사이트별 권한 부여를 추가합니다.	241 페이지 “Trusted Extensions에서 장치에 사이트별 권한 부여를 추가하는 방법”

작업	설명	수행 방법
사용자와 역할에 장치 권한 부여를 지정합니다.	사용자와 역할이 새 권한 부여를 사용할 수 있도록 합니다.	241 페이지 "장치 권한 부여를 지정하는 방법"

▼ 새 장치 권한 부여를 만드는 방법

장치에 권한 부여가 필요하지 않은 경우 기본적으로 모든 사용자가 장치를 사용할 수 있습니다. 권한 부여가 필요한 경우에는 기본적으로 권한이 부여된 사용자만 장치를 사용할 수 있습니다.

할당 가능한 장치에 대한 모든 액세스를 거부하려면 예 17–1을 참조하십시오.

시작하기 전에 전역 영역에서 보안 관리자 역할을 가진 사용자여야 합니다.

1. **`auth_attr` 파일을 편집합니다.**
   신뢰할 수 있는 편집기를 사용합니다. 자세한 내용은 54 페이지 "Trusted Extensions에서 관리 파일을 편집하는 방법"을 참조하십시오.

2. **새 권한 부여에 대한 머리글을 만듭니다.**
   조직의 인터넷 도메인 이름을 역순으로 사용하고 선택적으로 추가 임의 구성 요소(회사 이름 등)를 붙입니다. 점으로 구성 요소를 구분합니다. 머리글 이름은 점으로 끝냅니다.

   domain-suffix`.`*domain-prefix*`.`*optional*`.:::`*Company* `Header::help=`*Company*`.html`

3. **새 권한 부여 항목을 추가합니다.**
   한 라인에 하나씩 권한 부여를 추가합니다. 라인은 표시 목적으로 나뉩니다. 권한 부여에는 관리자가 새 권한 부여를 지정할 수 있게 하는 `grant` 권한 부여가 포함됩니다.

   ```
   domain-suffix.domain-prefix.grant:::Grant All Company Authorizations::
   help=CompanyGrant.html
   domain-suffix.domain-prefix.grant.device:::Grant Company Device Authorizations::
   help=CompanyGrantDevice.html
   domain-suffix.domain-prefix.device.allocate.tape:::Allocate Tape Device::
   help=CompanyTapeAllocate.html
   domain-suffix.domain-prefix.device.allocate.floppy:::Allocate Floppy Device::
   help=CompanyFloppyAllocate.html
   ```

4. **파일을 저장하고 편집기를 닫습니다.**

5. **LDAP을 이름 지정 서비스로 사용하는 경우 Oracle Directory Server Enterprise Edition(디렉토리 서버)에서 `auth_attr` 항목을 업데이트합니다.**
   자세한 내용은 `ldapaddent(1M)` 매뉴얼 페이지를 참조하십시오.

6 **적절한 권한 프로파일에 새 권한 부여를 추가합니다. 그런 다음 프로파일을 사용자와 역할에 지정합니다.**

Solaris Management Console을 사용합니다. 보안 관리자 역할을 맡고 Oracle Solaris 절차인 **System Administration Guide: Security Services**의 "How to Create or Change a Rights Profile"을 따릅니다.

7 **권한 부여를 사용하여 테이프 및 디스켓 드라이브에 대한 액세스를 제한합니다.**

Device Allocation Manager(장치 할당 관리자)에서 필수 권한 부여 목록에 새권한 부여를 추가합니다. 절차는 241 페이지 "Trusted Extensions에서 장치에 사이트별 권한 부여를 추가하는 방법"을 참조하십시오.

예 17–4 세분화된 장치 권한 부여 만들기

NewCo의 보안 관리자는 회사를 위한 세분화된 장치 권한 부여를 만들어야 합니다.

먼저 관리자는 다음 도움말 파일을 작성하여 `/usr/lib/help/auths/locale/C` 디렉토리에 넣습니다.

```
Newco.html
NewcoGrant.html
NewcoGrantDevice.html
NewcoTapeAllocate.html
NewcoFloppyAllocate.html
```

그런 다음 `auth_attr` 파일에서 `newco.com`에 대한 모든 권한 부여의 머리글을 추가하고,

```
# auth_attr file
com.newco.:::NewCo Header::help=Newco.html
```

권한 부여 항목을 파일에 추가합니다.

```
com.newco.grant:::Grant All NewCo Authorizations::
help=NewcoGrant.html
com.newco.grant.device:::Grant NewCo Device Authorizations::
help=NewcoGrantDevice.html
com.newco.device.allocate.tape:::Allocate Tape Device::
help=NewcoTapeAllocate.html
com.newco.device.allocate.floppy:::Allocate Floppy Device::
help=NewcoFloppyAllocate.html
```

라인은 표시 목적으로 나눕니다.

`auth_attr` 항목이 다음 권한 부여를 만듭니다.

- 모든 NewCo의 권한을 부여할 수 있는 권한 부여
- NewCo의 장치 권한을 부여할 수 있는 권한 부여
- 테이프 드라이브를 할당할 수 있는 권한 부여
- 디스켓 드라이브를 할당할 수 있는 권한 부여

예 17–5 신뢰할 수 있는 경로 및 신뢰할 수 없는 경로 권한 부여 만들기

기본적으로 Allocate Device(장치 할당) 권한 부여를 통해 신뢰할 수 있는 경로와 그 외부에서 할당이 가능합니다.

다음 예의 사이트 보안 정책에서는 원격 CD-ROM 할당 제한을 요구합니다. 보안 관리자는 `com.someco.device.cdrom.local` 권한 부여를 만듭니다. 이 권한 부여는 신뢰할 수 있는 경로를 사용하여 할당된 CD-ROM 드라이브용입니다. `com.someco.device.cdrom.remote` 권한 부여는 신뢰할 수 있는 경로 외부에서 CD-ROM 드라이브를 할당할 수 있는 일부 사용자용입니다.

보안 관리자는 도움말 파일을 만든 후 권한 부여를 `auth_attr` 데이터베이스에 추가하고 권한 부여를 장치에 추가한 다음 권한 부여를 권한 프로파일에 넣습니다. 프로파일은 장치 할당이 허용된 사용자에게 할당됩니다.

- 다음은 `auth_attr` 데이터베이스 항목입니다.

```
com.someco.:::SomeCo Header::help=Someco.html
com.someco.grant:::Grant All SomeCo Authorizations::
help=SomecoGrant.html
com.someco.grant.device:::Grant SomeCo Device Authorizations::
help=SomecoGrantDevice.html
com.someco.device.cdrom.local:::Allocate Local CD-ROM Device::
help=SomecoCDAllocateLocal.html
com.someco.device.cdrom.remote:::Allocate Remote CD-ROM Device::
help=SomecoCDAllocateRemote.html
```

- 다음은 Device Allocation Manager(장치 할당 관리자) 할당입니다.

  신뢰할 수 있는 경로를 통해 권한이 부여된 사용자는 로컬 CD-ROM 드라이브를 할당할 때 Device Allocation Manager(장치 할당 관리자)를 사용할 수 있습니다.

```
Device Name: cdrom_0
For Allocations From: Trusted Path
Allocatable By: Authorized Users
Authorizations: com.someco.device.cdrom.local
```

  신뢰할 수 없는 경로를 통해 사용자는 `allocate` 명령을 사용하여 원격으로 장치를 할당할 수 있습니다.

```
Device Name: cdrom_0
For Allocations From: Non-Trusted Path
Allocatable By: Authorized Users
Authorizations: com.someco.device.cdrom.remote
```

- 다음은 권한 프로파일 항목입니다.

```
# Local Allocator profile
com.someco.device.cdrom.local

# Remote Allocator profile
com.someco.device.cdrom.remote
```

- 다음은 권한이 부여된 사용자에 대한 권한 프로파일입니다.

```
# List of profiles for regular authorized user
Local Allocator Profile
...
```

```
# List of profiles for role or authorized user
Remote Allocator Profile
...
```

▼ Trusted Extensions에서 장치에 사이트별 권한 부여를 추가하는 방법

시작하기 전에 보안 관리자 역할이나 장치 속성 구성 권한 부여를 포함하는 역할을 가진 사용자여야 합니다. 238 페이지 "새 장치 권한 부여를 만드는 방법"에 설명된 대로 사이트별 권한 부여를 만들어 놓아야 합니다.

1. **229 페이지 "Trusted Extensions에서 장치를 구성하는 방법" 절차를 따릅니다.**
   a. **새 권한 부여로 보호해야 하는 장치를 선택합니다.**
   b. **Device Administration(장치 관리) 버튼을 누릅니다.**
   c. **Authorizations(권한 부여) 버튼을 누릅니다.**
      새 권한 부여가 Not Required(필수 아님) 목록에 표시됩니다.
   d. **새 권한 부여를 Required(필수) 권한 부여 목록에 추가합니다.**
2. **변경 사항을 저장하려면 OK(확인)를 누릅니다.**

▼ 장치 권한 부여를 지정하는 방법

Allocate Device(장치 할당) 권한 부여를 통해 사용자는 장치를 할당할 수 있습니다. Allocate Device(장치 할당) 권한 부여와 Revoke or Reclaim Device(장치 해지 또는 재생 이용) 권한 부여는 관리 역할에 적합합니다.

시작하기 전에 전역 영역에서 보안 관리자 역할을 가진 사용자여야 합니다.

기존 프로파일이 적당하지 않은 경우 보안 관리자는 새 프로파일을 만들 수 있습니다. 예는 91 페이지 "편리한 권한 부여를 위해 권한 프로파일을 만드는 방법"을 참조하십시오.

- **Allocate Device(장치 할당) 권한 부여가 포함된 권한 프로파일을 사용자에게 할당합니다.**
  자세한 내용은 온라인 도움말을 참조하십시오. 단계별 절차는 **System Administration Guide: Security Services**의 "How to Change the RBAC Properties of a User"를 참조하십시오.

다음 권한 프로파일을 통해 역할이 장치를 할당할 수 있습니다.

- All Authorizations
- 장치 관리
- Media Backup
- Object Label Management
- Software Installation

다음 권한 프로파일을 통해 역할이 장치를 해지하거나 재생 이용할 수 있습니다.

- All Authorizations
- 장치 관리

다음 권한 프로파일을 통해 역할이 장치를 만들거나 구성할 수 있습니다.

- All Authorizations
- Device Security

예 17–6 새 장치 권한 부여 지정

이 예에서 보안 관리자는 시스템에 대한 새 장치 권한 부여를 구성하고 새 권한 부여가 포함된 권한 프로파일을 신뢰할 수 있는 사용자에게 지정합니다. 보안 관리자는 다음 작업을 수행합니다.

1. 238 페이지 “새 장치 권한 부여를 만드는 방법”에 설명된 대로 새 장치 권한 부여를 만듭니다.
2. Device Allocation Manager(장치 할당 관리자)에서 새 장치 권한 부여를 테이프 및 디스켓 드라이브에 추가합니다.
3. 새 권한 부여를 NewCo Allocation 권한 프로파일에 넣습니다.
4. 테이프 및 디스켓 드라이브를 할당할 수 있게 권한이 부여된 사용자 및 역할 프로파일에 NewCo Allocation 권한 프로파일을 추가합니다.

이제 권한이 부여된 사용자와 역할이 이 시스템에서 테이프 드라이브와 디스켓 드라이브를 사용할 수 있습니다.

◆ ◆ ◆ 18장

18 Trusted Extensions 감사(개요)

이 장에서는 Trusted Extensions에서 제공하는 감사에 추가된 기능에 대해 설명합니다.

- 243 페이지 “Trusted Extensions와 감사”
- 244 페이지 “Trusted Extensions에서 역할로 감사 관리”
- 246 페이지 “Trusted Extensions 감사 참조”

Trusted Extensions와 감사

Trusted Extensions 소프트웨어로 구성된 시스템의 감사는 Oracle Solaris 시스템의 감사와 유사하게 구성되고 관리됩니다. 그러나 다음과 같은 몇 가지 차이점이 있습니다.

- Trusted Extensions 소프트웨어는 시스템에 감사 클래스, 감사 이벤트, 감사 토큰 및 감사 정책 옵션을 추가합니다.
- Trusted Extensions 소프트웨어에는 기본적으로 감사가 사용으로 설정되어 있습니다.
- Oracle Solaris 영역별 감사가 지원되지 않습니다. Trusted Extensions에서는 모든 영역이 동일하게 감사됩니다.
- Trusted Extensions에서는 사용자의 감사 특징을 관리하고 감사 파일을 편집하는 관리 도구를 제공합니다.
- Trusted Extensions에서는 시스템 관리자와 보안 관리자라는 두 가지 역할로 감사를 구성하고 관리합니다.

  보안 관리자는 감사 대상 및 사이트별 이벤트와 클래스 간 매핑을 계획합니다. Oracle Solaris OS에서와 같이 시스템 관리자는 감사 파일에 필요한 디스크 공간을 계획하고, 감사 관리 서버를 만들고, 감사 구성 파일을 설치합니다.

Trusted Extensions에서 역할로 감사 관리

Trusted Extensions의 감사에는 Oracle Solaris OS의 감사와 동일한 계획이 필요합니다. 계획에 대한 자세한 내용은 **System Administration Guide: Security Services**의 29 장, “Planning for Oracle Solaris Auditing”을 참조하십시오.

감사 관리를 위한 역할 설정

Trusted Extensions에서는 두 가지 역할이 감사를 담당합니다. 시스템 관리자 역할은 감사 저장소의 디스크와 네트워크를 설정하며, 보안 관리자 역할은 감사 대상을 결정하고 감사 구성 파일의 정보를 지정합니다. Oracle Solaris OS에서와 마찬가지로 소프트웨어에서 역할을 만듭니다. 이 두 역할에 대한 권한 프로파일이 제공됩니다. 첫 구성 시 초기 설치 팀에서 보안 관리자 역할을 만들었습니다. 자세한 내용은 **Trusted Extensions Configuration Guide**의 “Create the Security Administrator Role in Trusted Extensions”를 참조하십시오.

주 – 시스템에서 기록하도록 감사 구성 파일에 설정된 보안 관련 이벤트만 기록됩니다. 즉, 이벤트의 기록 여부는 사전 선택 내용에 의해 결정됩니다. 따라서 후속 감사 검토에서는 기록된 이벤트만 고려할 수 있습니다. 이를 잘못 구성하면 시스템 보안을 침해하려는 시도가 감지되지 않거나 이를 시도한 사용자를 관리자가 찾아낼 수 없습니다. 관리자는 정기적으로 감사 증적을 분석하여 보안 침해가 있는지 확인해야 합니다.

Trusted Extensions의 감사 작업

Trusted Extensions의 감사를 구성하고 관리하는 절차는 Oracle Solaris 절차와 약간 다릅니다.

- 두 관리 권한 중 하나로 전역 영역에서 감사 구성이 수행됩니다. 그러면 시스템 관리자가 전역 영역에서 레이블이 있는 모든 영역으로 특정 사용자 정의 감사 파일을 복사합니다. 이 절차에 따라 사용자 작업이 전역 영역과 레이블이 있는 영역에서 동일하게 감사됩니다.

  자세한 내용은 245 페이지 “보안 관리자의 감사 작업” 및 245 페이지 “시스템 관리자의 감사 작업”을 참조하십시오.

- Trusted Extensions 관리자는 신뢰할 수 있는 편집기를 사용하여 감사 구성 파일을 편집합니다. Trusted CDE, Trusted Extensions에서는 관리자가 CDE 작업을 사용하여 신뢰할 수 있는 편집기를 호출합니다. 작업 목록은 35 페이지 “Trusted CDE 작업”을 참조하십시오.

- Trusted Extensions 관리자는 Solaris Management Console을 사용하여 특정 사용자를 구성합니다. 이 도구에서 사용자별 감사 특징을 지정할 수 있습니다. 사용자의 감사 특징이 사용자가 작업 중인 시스템의 감사 특징과 다를 경우에만 사용자 특징 지정이 필요합니다. 도구 소개는 38 페이지 "Solaris Management Console 도구"를 참조하십시오.

보안 관리자의 감사 작업

다음은 보안 관리자가 담당하는 보안 관련 작업입니다. Oracle Solaris 지침을 따르지만 Trusted Extensions 관리 도구를 사용하십시오.

작업	Oracle Solaris 지침	Trusted Extensions 차이점
감사 파일을 구성합니다.	**System Administration Guide: Security Services**의 "Configuring Audit Files (Task Map)"	신뢰할 수 있는 편집기를 사용합니다. 자세한 내용은 54 페이지 "Trusted Extensions에서 관리 파일을 편집하는 방법"을 참조하십시오.
(선택 사항) 기본 감사 정책을 변경합니다.	**System Administration Guide: Security Services**의 "How to Configure Audit Policy"	신뢰할 수 있는 편집기를 사용합니다.
감사를 사용 안함으로 설정하고 다시 사용으로 설정합니다.	**System Administration Guide: Security Services**의 "How to Disable the Audit Service"	감사 기능은 기본적으로 사용으로 설정됩니다.
감사를 관리합니다.	**System Administration Guide: Security Services**의 "Oracle Solaris Auditing (Task Map)"	신뢰할 수 있는 편집기를 사용합니다. 영역별 감사 작업을 무시합니다.

시스템 관리자의 감사 작업

다음은 시스템 관리자가 담당하는 작업입니다. Oracle Solaris 지침을 따르지만 Trusted Extensions 관리 도구를 사용하십시오.

작업	Oracle Solaris 지침	Trusted Extensions 차이점
파일 감사 전용 ZFS 파일 시스템을 만듭니다. `audit_warn` 별명을 만듭니다.	**System Administration Guide: Security Services**의 "Managing Audit Records" **System Administration Guide: Security Services**의 "How to Configure the audit_warn Email Alias"	전역 영역에서 모든 관리를 수행합니다. 신뢰할 수 있는 편집기를 사용합니다.

작업	Oracle Solaris 지침	Trusted Extensions 차이점
레이블이 있는 영역으로 사용자 정의 감사 파일을 복사하거나 루프백 마운트합니다.	**System Administration Guide: Security Services**의 "Configuring the Audit Service in Zones (Tasks)"	레이블이 있는 영역이 모두 생성된 후 해당 영역으로 파일을 루프백 마운트하거나 복사합니다. 레이블이 있는 첫번째 영역으로 파일을 복사한 다음 해당 영역을 복사합니다.
(선택 사항) 감사 구성 파일을 배포합니다.	지침 없음	**Trusted Extensions Configuration Guide**의 "How to Copy Files From Portable Media in Trusted Extensions"을 참조하십시오.
감사를 관리합니다.	**System Administration Guide: Security Services**의 "Oracle Solaris Auditing (Task Map)"	영역별 감사 작업을 무시합니다.
레이블로 감사 레코드를 선택합니다.	**System Administration Guide: Security Services**의 "How to Select Audit Events From the Audit Trail"	레이블로 레코드를 선택하려면 `-l` 옵션과 함께 `auditreduce` 명령을 사용합니다.

Trusted Extensions 감사 참조

Trusted Extensions 소프트웨어는 Oracle Solaris OS에 감사 클래스, 감사 이벤트, 감사 토큰 및 감사 정책 옵션을 추가합니다. 몇 가지 감사 명령이 레이블을 처리하도록 확장되었습니다. 다음 그림은 일반적인 Trusted Extensions 커널 감사 레코드 및 사용자 레벨 감사 레코드를 보여줍니다.

그림 18–1 레이블이 있는 시스템의 일반적인 감사 레코드 구조

Trusted Extensions 감사 클래스

다음 표에는 Trusted Extensions 소프트웨어에서 Oracle Solaris OS에 추가하는 감사 클래스가 사전순으로 나열되어 있습니다. 클래스는 /etc/security/audit_class 파일에 나열되어 있습니다. 감사 클래스에 대한 자세한 내용은 audit_class(4) 매뉴얼 페이지를 참조하십시오.

표 18–1 X 서버 감사 클래스

짧은 이름	긴 이름	감사 마스크
xc	X - 객체 만들기/완전 삭제	0x00800000
xp	X - 권한 있는/관리 작업	0x00400000
xs	X - 잘못된 경우 항상 자동으로 실패하는 작업	0x01000000
xx	X - xc, xp 및 xs 클래스의 모든 X 이벤트(메타 클래스)	0x01c00000

다음 조건에 따라 X 서버 감사 이벤트가 이들 클래스에 매핑됩니다.

- **xc –** 이 클래스는 서버 객체 만들기나 삭제에 대해 감사합니다. 예를 들어, 이 클래스는 CreateWindow()를 감사합니다.
- **xp –** 이 클래스는 권한 사용에 대해 감사합니다. 권한 사용은 성공 또는 실패일 수 있습니다. 예를 들어, 클라이언트가 다른 클라이언트 창의 속성을 변경하려고 하면 ChangeWindowAttributes()가 감사됩니다. 이 클래스에는 SetAccessControl() 등의 관리 루틴도 포함됩니다.
- **xs –** 이 클래스는 보안 속성으로 인한 오류 발생 시 클라이언트에게 이에 대한 X 오류 메시지를 반환하지 않는 루틴을 감사합니다. 예를 들어, GetImage()는 권한이 부족하여 창에서 읽을 수 없는 경우 BadWindow 오류를 반환하지 않습니다.

  이러한 이벤트는 성공 시에만 감사하도록 선택해야 합니다. 실패에 대해 xs 이벤트를 감사하도록 선택하면 감사 증적이 관계없는 레코드로 채워집니다.
- **xx –** 이 클래스에는 모든 X 감사 클래스가 포함됩니다.

Trusted Extensions 감사 이벤트

Trusted Extensions 소프트웨어에서 시스템에 감사 이벤트를 추가합니다. 새로운 감사 이벤트와 해당 이벤트가 속한 감사 클래스는 /etc/security/audit_event 파일에 나열되어 있습니다. Trusted Extensions에 대한 감사 이벤트 번호는 9000에서 10000 사이입니다. 감사 이벤트에 대한 자세한 내용은 audit_event(4) 매뉴얼 페이지를 참조하십시오.

Trusted Extensions 감사 토큰

다음 표에는 Trusted Extensions 소프트웨어에서 Oracle Solaris OS에 추가하는 감사 토큰이 사전순으로 나열되어 있습니다. 이러한 토큰은 audit.log(4) 매뉴얼 페이지에도 나열되어 있습니다.

표 18–2 Trusted Extensions 감사 토큰

토큰 이름	설명
248 페이지 “label 토큰”	민감도 레이블
249 페이지 “xatom 토큰”	X 창 기본 단위 식별
249 페이지 “xclient 토큰”	X 클라이언트 식별
250 페이지 “xcolormap 토큰”	X 창 색상 정보
250 페이지 “xcursor 토큰”	X 창 커서 정보
250 페이지 “xfont 토큰”	X 창 글꼴 정보
251 페이지 “xgc 토큰”	X 창 그래픽 문맥 정보
251 페이지 “xpixmap 토큰”	Xwindow 픽셀 매핑 정보
251 페이지 “xproperty 토큰”	X 창 등록 정보 정보
252 페이지 “xselect 토큰”	X 창 데이터 정보
252 페이지 “xwindow 토큰”	X 창 창 정보

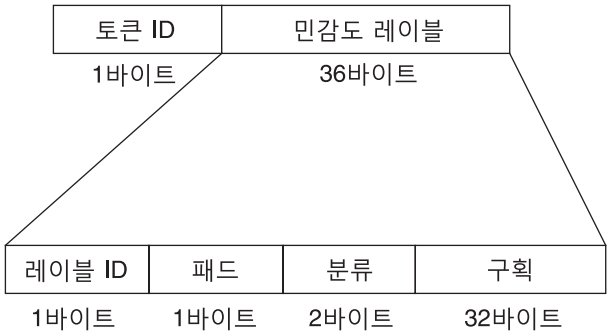
label 토큰

label 토큰에는 민감도 레이블이 있습니다. 이 토큰에는 다음 필드가 포함됩니다.

- 토큰 ID
- 민감도 레이블

다음 그림은 토큰 형식을 보여줍니다.

그림 18–2 label 토큰 형식



label 토큰은 다음과 같이 praudit 명령으로 표시됩니다.

```
sensitivity label,ADMIN_LOW
```

xatom 토큰

xatom 토큰에는 X 기본 단위에 대한 정보가 포함됩니다. 이 토큰에는 다음 필드가 포함됩니다.

- 토큰 ID
- 문자열 길이
- 기본 단위를 식별하는 텍스트 문자열

xatom 토큰은 다음과 같이 praudit로 표시됩니다.

```
X atom,_DT_SAVE_MODE
```

xclient 토큰

xclient 토큰에는 X 클라이언트에 대한 정보가 포함됩니다. 이 토큰에는 다음 필드가 포함됩니다.

- 토큰 ID
- 클라이언트 ID

xclient 토큰은 다음과 같이 praudit로 표시됩니다.

```
X client,15
```

xcolormap 토큰

xcolormap 토큰에는 색상맵에 대한 정보가 포함됩니다. 이 토큰에는 다음 필드가 포함됩니다.

- 토큰 ID
- X 서버 식별자
- 작성자의 사용자 ID

다음 그림은 토큰 형식을 보여줍니다.

그림 18–3 xcolormap, xcursor , xfont, xgc, xpixmap 및 xwindow 토큰의 형식

토큰 ID	XID	작성자 UID
1바이트	4바이트	4바이트

xcolormap 토큰은 다음과 같이 praudit로 표시됩니다.

```
X color map,0x08c00005,srv
```

xcursor 토큰

xcursor 토큰에는 커서에 대한 정보가 포함됩니다. 이 토큰에는 다음 필드가 포함됩니다.

- 토큰 ID
- X 서버 식별자
- 작성자의 사용자 ID

그림 18–3은 토큰 형식을 보여줍니다.

xcursor 토큰은 다음과 같이 praudit로 표시됩니다.

```
X cursor,0x0f400006,srv
```

xfont 토큰

xfont 토큰에는 글꼴에 대한 정보가 포함됩니다. 이 토큰에는 다음 필드가 포함됩니다.

- 토큰 ID
- X 서버 식별자
- 작성자의 사용자 ID

그림 18–3은 토큰 형식을 보여줍니다.

xfont 토큰은 다음과 같이 praudit로 표시됩니다.

```
X font,0x08c00001,srv
```

xgc 토큰

xgc 토큰에는 xgc에 대한 정보가 포함됩니다. 이 토큰에는 다음 필드가 포함됩니다.

- 토큰 ID
- X 서버 식별자
- 작성자의 사용자 ID

그림 18–3은 토큰 형식을 보여줍니다.

xgc 토큰은 다음과 같이 praudit로 표시됩니다.

```
Xgraphic context,0x002f2ca0,srv
```

xpixmap 토큰

xpixmap 토큰에는 픽셀 매핑에 대한 정보가 포함됩니다. 이 토큰에는 다음 필드가 포함됩니다.

- 토큰 ID
- X 서버 식별자
- 작성자의 사용자 ID

그림 18–3은 토큰 형식을 보여줍니다.

xpixmap 토큰은 다음과 같이 praudit로 표시됩니다.

```
X pixmap,0x08c00005,srv
```

xproperty 토큰

xproperty 토큰에는 창의 다양한 특성에 대한 정보가 포함됩니다. 이 토큰에는 다음 필드가 포함됩니다.

- 토큰 ID
- X 서버 식별자
- 작성자의 사용자 ID
- 문자열 길이
- 기본 단위를 식별하는 텍스트 문자열

다음 그림은 xproperty 토큰 형식을 보여줍니다.

그림 18–4 xproperty 토큰 형식

토큰 ID	XID	작성자 UID	문자열 길이	문자열(기본 단위 이름)
1바이트	4바이트	4바이트	2바이트	N바이트

xproperty 토큰은 다음과 같이 praudit로 표시됩니다.

```
X property,0x000075d5,root,_MOTIF_DEFAULT_BINDINGS
```

xselect 토큰

xselect 토큰에는 창 간에 이동되는 데이터가 포함됩니다. 이 데이터는 간주할 내부 구조와 등록 정보 문자열이 없는 바이트 스트림입니다. 이 토큰에는 다음 필드가 포함됩니다.

- 토큰 ID
- 특성 문자열의 길이
- 등록 정보 문자열
- 특성 유형의 길이
- 특성 유형 문자열
- 데이터의 바이트 수를 제공하는 길이 필드
- 데이터를 포함하는 바이트 문자열

다음 그림은 토큰 형식을 보여줍니다.

그림 18–5 xselect 토큰 형식

토큰 ID	특성 길이	특성 문자열	특성 유형 길이	특성 유형	데이터 길이	창 데이터
1바이트	2바이트	N바이트	2바이트	N바이트	2바이트	N바이트

xselect 토큰은 다음과 같이 praudit로 표시됩니다.

```
X selection,entryfield,halogen
```

xwindow 토큰

xwindow 토큰에는 창에 대한 정보가 포함됩니다. 이 토큰에는 다음 필드가 포함됩니다.

- 토큰 ID
- X 서버 식별자
- 작성자의 사용자 ID

그림 18–3은 토큰 형식을 보여줍니다.

xwindow 토큰은 다음과 같이 praudit로 표시됩니다.

```
X window,0x07400001,srv
```

Trusted Extensions 감사 정책 옵션

Trusted Extensions는 기존 Oracle Solaris 감사 정책 옵션에 두 가지 감사 정책 옵션을 추가합니다. 추가 사항을 보려면 정책을 나열하십시오.

```
$ auditconfig -lspolicy
...
windata_down Include downgraded window information in audit records
windata_up   Include upgraded window information in audit records
...
```

Trusted Extensions의 감사 명령에 대한 확장

Trusted Extensions 정보를 처리하도록 `auditconfig`, `auditreduce` 및 `bsmrecord` 명령이 확장되었습니다.

- `auditconfig` 명령에 Trusted Extensions 감사 정책이 포함됩니다. 자세한 내용은 `auditconfig(1M)` 매뉴얼 페이지를 참조하십시오.
- `auditreduce` 명령이 레이블로 레코드 필터링을 위한 `-l` 옵션을 추가합니다. 자세한 내용은 `auditreduce(1M)` 매뉴얼 페이지를 참조하십시오.
- `bsmrecord` 명령에 Trusted Extensions 감사 이벤트가 포함됩니다. 자세한 내용은 `bsmrecord(1M)` 매뉴얼 페이지를 참조하십시오.

◆ ◆ ◆ 19 장

19 Trusted Extensions에서 소프트웨어 관리(작업)

이 장에서는 Trusted Extensions를 사용하여 구성된 시스템에서 타사 소프트웨어를 신뢰할 수 있는 방법으로 실행하는 방법을 설명합니다.

- 255 페이지 "Trusted Extensions에 소프트웨어 추가"
- 259 페이지 "윈도우 시스템의 신뢰할 수 있는 프로세스"
- 260 페이지 "Trusted Extensions에서 소프트웨어 관리(작업)"

Trusted Extensions에 소프트웨어 추가

Oracle Solaris 시스템에 추가할 수 있는 모든 소프트웨어는 Trusted Extensions를 사용하여 구성된 시스템에 추가할 수 있습니다. 또한 Trusted Extensions API를 사용하는 프로그램도 추가할 수 있습니다. Trusted Extensions 시스템에 소프트웨어를 추가하는 방법은 비전역 영역을 실행 중인 Oracle Solaris 시스템에 소프트웨어를 추가하는 방법과 비슷합니다.

예를 들어, 패키지 문제는 비전역 영역을 설치한 시스템에 영향을 줍니다. 패키지 매개변수는 다음을 정의합니다.

- **패키지의 영역 범위** – 범위에 따라 특정 패키지를 설치할 수 있는 영역의 유형이 결정됩니다.
- **패키지의 표시 여부** – 표시 여부에 따라 패키지를 설치해야 하는지 및 패키지가 모든 영역에서 동일해야 하는지가 결정됩니다.
- **패키지 제한** – 한 가지 제한은 패키지를 현재 영역에만 설치해야 하는지 여부입니다.

Trusted Extensions에서 프로그램은 일반적으로 레이블이 있는 영역에서 일반 사용자가 사용하도록 전역 영역에 설치됩니다. 영역에 패키지를 설치하는 방법에 대한 자세한 내용은 **System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones**의 25 장, "About Packages and Patches on an Oracle Solaris System With Zones Installed (Overview)"를 참조하십시오. 또한 `pkgadd(1M)` 매뉴얼 페이지를 참조하십시오.

Trusted Extensions 사이트에서 시스템 관리자와 보안 관리자가 함께 작업하여 소프트웨어를 설치합니다. 보안 관리자는 소프트웨어 추가가 보안 정책을 준수하는지 평가합니다. 소프트웨어 사용에 권한 또는 권한 부여가 필요한 경우 보안 관리자 역할은 해당 소프트웨어 사용자에게 적절한 권한 프로파일을 지정합니다.

이동식 매체에서 소프트웨어를 가져오려면 권한 부여가 필요합니다. Allocate Device(장치 할당) 권한이 있는 계정은 이동식 매체에서 데이터를 가져오거나 내보낼 수 있습니다. 데이터는 실행 코드를 포함할 수 있습니다. 일반 사용자는 사용자의 클리어런스 내에 있는 레이블에서만 데이터를 가져올 수 있습니다.

시스템 관리자 역할은 보안 관리자가 승인한 프로그램을 추가할 책임이 있습니다.

Oracle Solaris의 소프트웨어 보안 방식

Trusted Extensions는 Oracle Solaris OS와 동일한 보안 방식을 사용합니다. 방식에는 다음이 포함됩니다.

- **권한 부여** – 프로그램 사용자에게 특정 권한 부여가 요구될 수 있습니다. 권한 부여에 대한 자세한 내용은 **System Administration Guide: Security Services**의 "Oracle Solaris RBAC Elements and Basic Concepts"를 참조하십시오. 또한 `auth_attr(4)` 및 `getauthattr(3SECDB)` 매뉴얼 페이지를 참조하십시오.
- **권한** – 프로그램 및 프로세스에 권한이 지정될 수 있습니다. 권한에 대한 자세한 내용은 **System Administration Guide: Security Services**의 8 장, "Using Roles and Privileges (Overview)"를 참조하십시오. 또한 `privileges(5)` 매뉴얼 페이지를 참조하십시오.

  `ppriv` 명령은 디버깅 유틸리티를 제공합니다. 자세한 내용은 `ppriv(1)` 매뉴얼 페이지를 참조하십시오. 비전역 영역에서 작동하는 프로그램에서 이 유틸리티를 사용하는 방법은 **System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones**의 "Using the ppriv Utility"를 참조하십시오.
- **권한 프로파일** – 권한 프로파일은 한 곳에서 사용자 또는 역할에 지정할 보안 속성을 수집합니다. 권한 프로파일에 대한 자세한 내용은 **System Administration Guide: Security Services**의 "RBAC Rights Profiles"를 참조하십시오. Trusted Extensions는 보안 속성이 지정될 수 있는 실행 파일의 유형에 CDE 작업을 추가합니다.
- **신뢰할 수 있는 라이브러리** – `setuid`, `setgid` 및 권한 있는 프로그램에서 사용하는 동적 공유 라이브러리는 신뢰할 수 있는 디렉토리에서만 로드할 수 있습니다. Oracle Solaris OS에서와 마찬가지로 `crle` 명령은 신뢰할 수 있는 디렉토리 목록에 권한 있는 프로그램의 공유 라이브러리 디렉토리를 추가하는 데 사용됩니다. 자세한 내용은 `crle(1)` 매뉴얼 페이지를 참조하십시오.

소프트웨어의 보안 평가

소프트웨어에 권한이 지정되거나 소프트웨어를 대체 사용자 ID 또는 그룹 ID로 실행하면 **신뢰할 수 있는** 소프트웨어가 됩니다. 신뢰할 수 있는 소프트웨어는 Trusted Extensions 보안 정책을 무시할 수 있습니다. 소프트웨어를 신뢰할 만하지 않은 경우에도 신뢰할 수 있는 소프트웨어로 지정할 수 있습니다. 보안 관리자는 세부 조사를 통해 소프트웨어에서 신뢰할 수 있는 방법으로 권한을 사용한다는 사실이 확인될 때까지 기다렸다가 소프트웨어에 권한을 부여해야 합니다.

프로그램은 신뢰할 수 있는 시스템에서 세 가지 범주로 분류됩니다.

- **보안 속성이 필요하지 않은 프로그램** – 일부 프로그램은 단일 레벨에서 실행되므로 권한이 필요하지 않습니다. 이러한 프로그램은 공용 디렉토리(예: `/usr/local`)에 설치할 수 있습니다. 액세스하려면 사용자 및 역할의 권한 프로파일에 있는 명령으로 프로그램을 지정합니다.
- **root로 실행되는 프로그램** – 일부 프로그램은 `setuid 0`으로 실행됩니다. 이러한 프로그램에는 권한 프로파일에서 유효 UID `0`이 지정될 수 있습니다. 그러면 보안 관리자는 프로파일을 관리 역할에 지정합니다.

  참고 – 응용 프로그램에서 권한을 신뢰할 수 있는 방법으로 사용할 수 있는 경우 응용 프로그램에 필요한 권한을 지정하고 프로그램을 `root`로 실행하지 마십시오.

- **권한이 필요한 프로그램** – 일부 프로그램은 분명하지 않은 이유로 인해 권한이 필요할 수 있습니다. 프로그램에서 시스템 보안 정책을 위반할 것 같은 기능을 수행하고 있지 않더라도, 해당 프로그램이 보안을 위반하는 기능을 내부적으로 수행할 수 있습니다. 예를 들어, 프로그램에서 공유 로그 파일을 사용하거나 프로그램이 `/dev/kmem`에서 읽을 수 있습니다. 보안 문제에 대한 자세한 내용은 `mem(7D)` 매뉴얼 페이지를 참조하십시오.

  내부 정책을 대체해도 응용 프로그램의 올바른 작동에 특별히 영향을 미치지 않는 경우도 있습니다. 오히려 내부 정책을 대체하면 사용자가 기능을 보다 편리하게 수행할 수 있습니다.

  조직에서 소스 코드에 액세스할 수 있는 경우 응용 프로그램의 성능에 영향을 주지 않고 정책을 대체해야 하는 작업을 제거할 수 있는지 여부를 확인합니다.

신뢰할 수 있는 프로그램을 만들 때의 개발자 책임

프로그램 개발자가 소스 코드에서 권한 세트를 조작할 수 있더라도 보안 관리자가 프로그램에 필요한 권한을 지정하지 않은 경우에는 프로그램이 실패합니다. 따라서 신뢰할 수 있는 프로그램을 만들 때는 개발자와 보안 관리자가 상호 협력해야 합니다.

신뢰할 수 있는 프로그램을 작성하는 개발자는 다음을 수행해야 합니다.

1. 프로그램에서 작업을 수행하는 데 권한이 필요한 경우를 파악합니다.
2. 프로그램에서 권한을 안전하게 사용할 수 있도록 권한 분류 등과 같은 기술을 확인하여 따라야 합니다.
3. 프로그램에 권한을 지정할 때 보안에 미치는 영향에 유의합니다. 프로그램이 보안 정책을 위반하지 않아야 합니다.
4. 신뢰할 수 있는 디렉토리에서 프로그램에 연결되는 공유 라이브러리를 사용하여 프로그램을 컴파일합니다.

   자세한 내용은 **Developer's Guide to Oracle Solaris 10 Security**를 참조하십시오. Trusted Extensions에 대한 코드 예제는 **Trusted Extensions Developer's Guide** 를 참조하십시오.

신뢰할 수 있는 프로그램에 대한 보안 관리자 책임

보안 관리자는 새 소프트웨어를 테스트하고 평가해야 할 책임이 있습니다. 신뢰할 수 있는 소프트웨어인지 확인한 후 보안 관리자는 프로그램에 대한 권한 프로파일과 기타 보안 관련 속성을 구성합니다.

보안 관리자의 책임은 다음과 같습니다.

1. 프로그래머와 프로그램 배포 프로세스가 신뢰할 수 있는지 확인합니다.
2. 다음 중 한 가지 방법으로 프로그램에 필요한 권한을 확인합니다.
   - 프로그래머에게 질문합니다.
   - 소스 코드에서 프로그램에 사용할 권한을 검색합니다.
   - 소스 코드에서 프로그램에서 사용자에게 요구하는 권한 부여를 검색합니다.
   - `ppriv` 명령에 대한 디버깅 옵션을 사용하여 권한 사용을 검색합니다. 예제는 `ppriv(1)`매뉴얼 페이지를 참조하십시오.
3. 소스 코드를 조사하여 프로그램을 작동하는 데 필요한 권한과 관련하여 코드가 신뢰할 수 있는 방법으로 작동하는지 확인합니다.

   프로그램에서 신뢰할 수 있는 방법으로 권한을 사용하지 못하는 경우 프로그램의 소스 코드를 수정할 수 있으면 코드를 수정합니다. 보안에 대해 잘 알고 있는 보안 컨설턴트 또는 개발자는 코드를 수정할 수 있습니다. 권한 분류, 권한 부여 확인 등을 수정할 수 있습니다.

   권한은 수동으로 지정해야 합니다. 권한이 부족하여 실패하는 프로그램에 권한을 지정할 수 있습니다. 또는 보안 관리자가 권한이 필요하지 않도록 유효한 UID 또는 GID를 지정할 수 있습니다.

윈도우 시스템의 신뢰할 수 있는 프로세스

Solaris Trusted Extensions(CDE)에서 신뢰할 수 있는 윈도우 시스템 프로세스는 다음과 같습니다.

- Front Panel(전면 패널)
- Front Panel(전면 패널)의 서브패널
- Workspace(작업 공간) 메뉴
- File Manager(파일 관리자)
- Application Manager(응용 프로그램 관리자)

윈도우 시스템의 신뢰할 수 있는 프로세스는 모든 사용자가 사용할 수 있지만 관리 작업에 대한 액세스는 전역 영역에 있는 역할로 제한됩니다.

File Manager(파일 관리자)에서 작업이 계정의 프로파일 중 하나에 없는 경우 작업 아이콘이 표시되지 않습니다. Workspace(작업 공간) 메뉴에서 작업이 계정의 프로파일 중 하나에 없는 경우 작업이 표시되지만 작업을 호출하면 오류가 표시됩니다.

Trusted CDE에서 창 관리자 `dtwm`은 `Xtsolusersession` 스크립트를 호출합니다. 이 스크립트는 창 관리자에서 실행되어 윈도우 시스템에서 시작되는 작업을 호출합니다. `Xtsolusersession` 스크립트는 계정에서 작업을 실행하려고 시도할 때 계정의 권한 프로파일을 확인합니다. 어느 경우든 작업이 지정된 권한 프로파일에 있는 경우 프로파일에 지정된 보안 속성으로 작업이 실행됩니다.

Trusted CDE 작업 추가

Trusted Extensions에서 CDE 작업을 만들어서 사용하는 절차는 Oracle Solaris OS의 절차와 비슷합니다. 작업을 추가하는 방법은 **Solaris Common Desktop Environment: Advanced User's and System Administrator's Guide**의 4 장, "Adding and Administering Applications"를 참조하십시오.

Oracle Solaris OS에서와 마찬가지로 작업 사용은 권한 프로파일 방식에 의해 제어될 수 있습니다. Trusted Extensions에서는 관리 역할의 권한 프로파일에서 여러 작업에 보안 속성이 지정되었습니다. 보안 관리자는 Rights(권한) 도구를 사용하여 새 작업에 보안 속성을 지정할 수도 있습니다.

다음 표에 작업을 만들어 사용할 때의 Oracle Solaris 시스템과 Trusted Extensions 시스템 사이의 주요 차이점이 요약되어 있습니다.

표 19–1 Trusted Extensions의 CDE 작업에 대한 제약 조건

Oracle Solaris CDE 작업	Trusted CDE 작업
개발자의 홈 디렉토리에 있는 모든 사용자가 새 작업을 만들 수 있습니다.	작업이 사용자에게 지정된 권한 프로파일에 있는 경우에만 작업을 사용할 수 있습니다. 작업 검색 경로가 다릅니다. 사용자의 홈 디렉토리에 있는 작업이 처음이 아니라 마지막에 처리됩니다. 따라서 아무도 기존 작업을 사용자 정의할 수 없습니다.
작성자는 자동으로 새 작업을 사용할 수 있습니다.	사용자는 홈 디렉토리에서 새 작업을 만들 수 있지만 작업을 사용할 수 없습니다. All(모든) 프로파일을 가진 사용자는 자신이 만든 작업을 사용할 수 있습니다. 그렇지 않으면, 보안 관리자가 계정의 권한 프로파일 중 하나에 새 작업의 이름을 추가해야 합니다. 작업을 시작하려면 사용자가 File Manager(파일 관리자)를 사용합니다. 시스템 관리자는 작업을 공용 디렉토리에 넣을 수 있습니다.
작업을 끌어서 Front Panel(전면 패널)에 놓을 수 있습니다.	Front Panel(전면 패널)이 신뢰할 수 있는 경로의 일부입니다. 창 관리자는 `/usr/dt` and `/etc/dt` 하위 디렉토리에 있는 관리적으로 추가된 작업만 인식합니다. All(모든) 프로파일이 있는 경우에도 사용자가 새 작업을 Front Panel(전면 패널)로 끌어 놓을 수 없습니다. 사용자의 홈 디렉토리에 있는 작업은 창 관리자에서 인식되지 않습니다. 관리자는 공용 디렉토리만 확인합니다.
작업은 `root`로 실행되는 경우 권한 있는 작업을 수행할 수 있습니다.	사용자에게 지정된 권한 프로파일에서 작업에 권한이 지정된 경우 작업은 권한 있는 작업을 수행할 수 있습니다.
작업이 Solaris Management Console에서 관리되지 않습니다.	작업은 Solaris Management Console의 Rights(권한) 도구에서 권한 프로파일에 지정됩니다. 새 작업이 추가되면 보안 관리자는 새 작업을 사용할 수 있도록 설정할 수 있습니다.

Trusted Extensions에서 소프트웨어 관리(작업)

Trusted Extensions에서 소프트웨어를 관리하는 방법은 비전역 영역을 설치한 Oracle Solaris 시스템에서 소프트웨어를 관리하는 방법과 비슷합니다. 영역에 대한 자세한 내용은 **System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones**의 제II부, “Zones”를 참조하십시오.

▼ Trusted Extensions에서 소프트웨어 패키지를 추가하는 방법

시작하기 전에 장치를 할당할 수 있는 역할에 속해야 합니다.

1 적절한 작업 공간에서 시작합니다.

- **전역 영역에서 소프트웨어 패키지를 설치하려면 전역 영역에 있습니다.**

- **레이블이 있는 영역에서 소프트웨어 패키지를 추가하려면 해당 레이블에서 작업 공간을 만듭니다.**

  자세한 내용은 **Trusted Extensions User's Guide**의 "How to Change the Label of a Workspace"을 참조하십시오.

2. **CD-ROM 드라이브를 할당합니다.**

   자세한 내용은 **Trusted Extensions User's Guide**의 "How to Allocate a Device in Trusted Extensions"을 참조하십시오.

3. **소프트웨어를 설치합니다.**

   자세한 내용은 **Oracle Solaris 관리: 기본 관리**의 "소프트웨어 관리 작업 검색 위치"를 참조하십시오.

4. **작업을 마친 후 장치를 할당 해제합니다.**

   자세한 내용은 **Trusted Extensions User's Guide**의 "How to Allocate a Device in Trusted Extensions"을 참조하십시오.

▼ Trusted Extensions에서 Java 아카이브 파일을 설치하는 방법

이 절차에서는 JAR(Java 아카이브) 파일을 전역 영역에 다운로드합니다. 전역 영역에서 관리자는 해당 파일을 일반 사용자가 사용할 수 있도록 설정할 수 있습니다.

시작하기 전에 보안 관리자가 Java 프로그램의 소스가 신뢰할 수 있고 전달 방법이 안전하며 프로그램을 신뢰할 수 있는 방법으로 실행할 수 있다는 것을 확인했습니다.

사용자는 전역 영역에서 시스템 관리자 역할에 속합니다. Trusted CDE에서 Software Installation 권한 프로파일에 Java 코드에 대한 열기 작업이 포함되어 있습니다.

1. **JAR 파일을 `/tmp` 디렉토리로 다운로드합니다.**

   예를 들어, `http://www.sunfreeware.com`에서 소프트웨어를 선택할 경우 사이트의 "Solaris `pkg-get` 도구" 지침을 사용합니다.

2. **File Manager(파일 관리자)를 열고 `/tmp` 디렉토리로 이동합니다.**

3. **다운로드한 파일을 두 번 누릅니다.**

4. **소프트웨어를 설치하려면 대화 상자의 질문에 답합니다.**

5. **설치 로그를 확인합니다.**

예 19–1 사용자 레이블에 JAR 파일 다운로드

보안 위험을 제한하기 위해 시스템 관리자는 일반 사용자의 승인 범위 내 단일 레이블에 소프트웨어를 다운로드합니다. 그러면 보안 관리자는 해당 레이블에서 JAR 파일을 테스트합니다. 소프트웨어가 테스트를 통과하면 보안 관리자는 레이블을 ADMIN_LOW로 다운그레이드할 수 있습니다. 시스템 관리자는 NFS 서버에 소프트웨어를 설치하여 모든 사용자가 사용할 수 있도록 합니다.

1. 먼저 시스템 관리자는 사용자 레이블에서 작업 공간을 만듭니다.
2. 이 작업 공간에서 JAR 파일을 다운로드합니다.
3. 해당 레이블에서 보안 관리자는 파일을 테스트합니다.
4. 그런 다음 보안 관리자는 파일의 레이블을 ADMIN_LOW로 변경합니다.
5. 마지막으로 시스템 관리자는 레이블이 ADMIN_LOW인 NFS 서버로 파일을 복사합니다.

◆ ◆ ◆ 부 록 A

Trusted Extensions 관리에 대한 빠른 참조

Trusted Extensions 인터페이스는 Oracle Solaris OS를 확장합니다. 이 부록을 참조하여 차이점을 빠르게 확인할 수 있습니다. 라이브러리 루틴, 시스템 호출을 비롯한 자세한 인터페이스 목록은 부록 B, "Trusted Extensions 매뉴얼 페이지 목록"을 참조하십시오.

Trusted Extensions의 관리 인터페이스

Trusted Extensions에서는 소프트웨어에 대한 인터페이스를 제공합니다. 다음 인터페이스는 Trusted Extensions 소프트웨어를 실행 중인 경우에만 사용할 수 있습니다.

`txzonemgr` 스크립트	레이블이 있는 영역을 만들고 설치, 초기화 및 부팅하는 메뉴 기반의 마법사를 제공합니다. 메뉴 제목은 Labeled Zone Manager(레이블이 있는 영역 관리자)입니다. 이 스크립트는 네트워킹 옵션, 이름 서비스 옵션 및 기존 LDAP 서버에 대한 전역 영역 클라이언트화를 위한 메뉴 항목도 제공합니다.
Trusted CDE 작업	Trusted CDE의 Workspace Menu(작업 공간 메뉴) -> Application Manager(응용 프로그램 관리자) -> Trusted_Extensions에는 파일을 구성하고, 영역을 설치 및 부트하고, 기타 Trusted Extensions 작업을 간소화하는 CDE 작업이 있습니다. 이러한 작업에 대한 자세한 내용은 35 페이지 "Trusted CDE 작업"을 참조하십시오. Trusted CDE 온라인 도움말에도 이러한 작업이 설명되어 있습니다.
관리 편집기	이 신뢰할 수 있는 편집기는 시스템 파일을 편집하는 데 사용됩니다. Trusted CDE에서 Workspace Menu(작업 공간 메뉴) ->

	Application Manager(응용 프로그램 관리자) –> Trusted_Extensions –> 관리 편집기를 선택하여 관리 편집기를 호출합니다. Trusted JDS의 명령줄에서 편집기를 호출합니다. 다음과 같이 편집할 파일을 인수로 제공합니다. `/usr/dt/bin/trusted_edit` *filename*
장치 할당 관리자	Trusted Extensions에서 이 GUI는 장치를 관리하는 데 사용됩니다. Device Administration(장치 관리) 대화 상자는 관리자가 장치를 구성하는 데 사용됩니다. Device Allocation Manager(장치 할당 관리자)는 역할 및 일반 사용자가 장치를 할당하는 데 사용됩니다. GUI는 Trusted Path(신뢰할 수 있는 경로) 메뉴에서 사용할 수 있습니다.
레이블 구축기	이 응용 프로그램은 사용자가 레이블 또는 클리어런스를 선택할 수 있을 때 호출됩니다. 이 응용 프로그램은 역할이 장치, 영역, 사용자 또는 역할에 레이블이나 레이블 범위를 지정할 때도 나타납니다.
선택 관리자	이 응용 프로그램은 권한 부여된 사용자나 역할이 정보를 업그레이드하거나 다운그레이드하려고 할 때 호출됩니다.
Trusted Path(신뢰할 수 있는 경로) 메뉴	이 메뉴는 TCB(Trusted Computing Base)와의 상호 작용을 처리합니다. 예를 들어, 이 메뉴에는 Change Password(암호 변경) 메뉴 항목이 있습니다. Trusted CDE의 작업 공간 전환 영역에서 Trusted Path(신뢰할 수 있는 경로) 메뉴에 액세스합니다. Trusted JDS에서는 신뢰할 수 있는 스트라이프 왼쪽의 신뢰할 수 있는 기호를 눌러서 Trusted Path(신뢰할 수 있는 경로) 메뉴에 액세스합니다.
관리 명령	Trusted Extensions에서는 레이블을 가져오고 기타 작업을 수행하는 명령을 제공합니다. 명령 목록은 44 페이지 “Trusted Extensions의 명령줄 도구”를 참조하십시오.

Trusted Extensions에서 확장된 Oracle Solaris 인터페이스

Trusted Extensions에서 기존 Oracle Solaris 구성 파일, 명령 및 GUI에 다음 사항을 추가합니다.

관리 명령	Trusted Extensions에서 선택된 Oracle Solaris 명령에 옵션을 추가합니다. 목록은 표 2–5를 참조하십시오.
구성 파일	Trusted Extensions에서 `net_mac_aware`와 `net_mlp`라는 두 가지 권한을 추가합니다. `net_mac_aware` 권한을 사용할 경우 137 페이지 “Trusted Extensions에서 NFS 마운트된 디렉토리에 액세스”를 참조하십시오. Trusted Extensions에서 `auth_attr` 데이터베이스에 권한 부여를 추가합니다. Trusted Extensions에서 `exec_attr` 데이터베이스에 CDE 작업을 포함한 실행 파일을 추가합니다. Trusted Extensions에서 `prof_attr` 데이터베이스의 기존 권한 프로파일을 수정합니다. 또한 데이터베이스에 프로파일을 추가합니다. Trusted Extensions에서 `exec_attr` 데이터베이스에서 권한을 부여할 수 있는 실행 파일에 CDE 작업을 추가합니다. Trusted Extensions에서 `policy.conf` 데이터베이스에 필드를 추가합니다. 필드는 78 페이지 “Trusted Extensions의 `policy.conf` 파일 기본값”을 참조하십시오. Trusted Extensions에서 감사 토큰, 감사 이벤트, 감사 클래스 및 감사 정책 옵션을 추가합니다. 목록은 246 페이지 “Trusted Extensions 감사 참조”를 참조하십시오.
Solaris Management Console	Trusted Extensions에서 Computers and Networks(컴퓨터 및 네트워크) 도구 세트에 Security Templates(보안 템플리트) 도구를 추가합니다. Trusted Extensions에서 Computers and Networks(컴퓨터 및 네트워크) 도구 세트에 Trusted Network Zones(신뢰할 수 있는 네트워크 영역) 도구를 추가합니다. Trusted Extensions에서는 Users(사용자) 도구 및 Administrative Roles(관리 역할) 도구에 Trusted Extensions Attributes(Trusted Extensions 속성) 탭을 추가합니다.

영역의 공유 디렉토리 Trusted Extensions에서는 레이블이 있는 영역의 디렉토리를 공유할 수 있습니다. 전역 영역에서 `/etc/dfs/dfstab` 파일을 만들어 영역의 레이블에서 디렉토리를 공유합니다.

Trusted Extensions의 강화된 보안 기본값

Trusted Extensions에서는 Oracle Solaris OS보다 보안 기본값이 강화되었습니다.

감사 기본적으로 감사가 사용으로 설정되어 있습니다.

관리자가 감사를 해제할 수 있습니다. 그러나 Trusted Extensions를 설치하는 사이트에는 일반적으로 감사가 필요합니다.

장치 기본적으로 장치 할당이 사용으로 설정되어 있습니다.

기본적으로 장치 할당에는 권한 부여가 필요합니다. 따라서 기본적으로 일반 사용자는 이동식 매체를 사용할 수 없습니다.

관리자는 권한 부여 요구 사항을 제거할 수 있습니다. 그러나 Trusted Extensions를 설치하는 사이트에는 일반적으로 장치 할당이 필요합니다.

인쇄 일반 사용자는 프린터의 레이블 범위에 사용자의 레이블이 포함되어 있는 프린터로만 인쇄할 수 있습니다.

기본적으로 인쇄된 출력에는 트레일러 페이지와 배너 페이지가 있습니다. 이들 페이지와 본문 페이지에는 인쇄 작업의 레이블이 포함됩니다.

기본적으로 사용자는 PostScript 파일을 인쇄할 수 없습니다.

역할 Oracle Solaris OS에서는 역할을 사용할 수 있지만 선택 사항입니다. Trusted Extensions에서는 역할이 적절한 관리를 위한 필수 사항입니다.

Oracle Solaris OS에서는 `root` 사용자를 역할로 지정할 수 있습니다. Trusted Extensions에서는 수퍼유저 역할을 하는 사용자를 효율적으로 감사하기 위해 `root` 사용자를 역할로 지정합니다.

Trusted Extensions의 제한된 옵션

Trusted Extensions에서는 Oracle Solaris 구성 옵션 범위를 축소합니다.

데스크탑 Trusted Extensions에서는 Solaris Trusted Extensions(CDE)와 Solaris Trusted Extensions(JDS)의 두 가지 데스크탑을 제공합니다.

	Trusted Extensions에서는 Solaris Trusted Extensions (GNOME) 데스크탑을 제공합니다.
이름 지정 서비스	LDAP 이름 지정 서비스가 지원됩니다. 하나의 이름 지정 서비스로 모든 영역을 관리해야 합니다.
영역	전역 영역은 관리 영역입니다. `root` 사용자 또는 역할만 전역 영역에 들어갈 수 있습니다. 따라서 일반 Trusted Extensions 사용자는 일반 Oracle Solaris 사용자가 사용할 수 있는 관리 인터페이스를 사용할 수 없습니다. 예를 들어, Trusted Extensions에서 사용자는 Solaris Management Console을 불러올 수 없습니다. 비전역 영역은 레이블이 있는 영역입니다. 사용자는 레이블이 있는 영역에서 작업합니다.

◆ ◆ ◆ 부 록 B

Trusted Extensions 매뉴얼 페이지 목록

Trusted Extensions는 Oracle Solaris OS의 구성입니다. 이 부록에서는 Trusted Extensions 정보가 들어 있는 Oracle Solaris 매뉴얼 페이지에 대해 간략하게 설명합니다.

Trusted Extensions 매뉴얼 페이지(사전순)

다음은 Oracle Solaris 시스템의 Trusted Extensions 소프트웨어에 대해 설명하는 매뉴얼 페이지로서 Trusted Extensions로 구성된 시스템에만 해당됩니다.

Oracle Solaris 매뉴얼 페이지	요약
add_allocatable(1M)	할당 데이터베이스에 항목 추가
atohexlabel(1M)	사람이 읽을 수 있는 레이블을 해당 내부 텍스트로 변환
blcompare(3TSOL)	이진 레이블 비교
blminmax(3TSOL)	두 레이블의 범위 결정
chk_encodings(1M)	레이블 인코딩 파일 구문 확인
dtappsession(1)	새 Application Manager(응용 프로그램 관리자) 세션 시작
fgetlabel(2)	파일의 레이블 가져오기
getlabel(1)	파일의 레이블 표시
getlabel(2)	파일의 레이블 가져오기
getpathbylabel(3TSOL)	영역 경로 이름 가져오기
getplabel(3TSOL)	프로세스 레이블 가져오기
getuserrange(3TSOL)	사용자의 레이블 범위 가져오기

getzoneidbylabel(3TSOL)	영역 레이블에서 영역 ID 가져오기
getzonelabelbyid(3TSOL)	영역 ID에서 영역 레이블 가져오기
getzonelabelbyname(3TSOL)	영역 이름에서 영역 레이블 가져오기
getzonepath(1)	지정된 레이블에 해당하는 영역의 루트 경로 표시
getzonerootbyid(3TSOL)	영역 루트 ID에서 영역 루트 경로 이름 가져오기
getzonerootbylabel(3TSOL)	영역 레이블에서 영역 루트 경로 이름 가져오기
getzonerootbyname(3TSOL)	영역 이름에서 영역 루트 경로 이름 가져오기
hextoalabel(1M)	내부 텍스트 레이블을 사람이 읽을 수 있는 해당 레이블로 변환
labelbuilder(3TSOL)	유효한 레이블 또는 클리어런스를 대화식으로 구축하는 Motif 기반의 사용자 인터페이스 만들기
labelclipping(3TSOL)	이진 레이블을 변환하고 지정된 폭으로 잘라내기
label_encodings(4)	레이블 인코딩 파일 설명
label_to_str(3TSOL)	레이블을 사람이 읽을 수 있는 문자열로 변환
labels(5)	Trusted Extensions 레이블 속성 설명
libtsnet(3LIB)	Trusted Extensions 네트워크 라이브러리
libtsol(3LIB)	Trusted Extensions 라이브러리
m_label(3TSOL)	새 레이블에 대한 리소스 할당 및 비우기
pam_tsol_account(5)	레이블에 따른 계정 제한 확인
plabel(1)	프로세스 레이블 가져오기
remove_allocatable(1M)	할당 데이터베이스에서 항목 제거
sel_config(4)	복사, 잘라내기, 붙여넣기 및 끌어서 놓기 작업에 대한 선택 규칙
setflabel(3TSOL)	파일을 해당 민감도 레이블의 영역으로 이동
smtnrhdb(1M)	Trusted Extensions 네트워킹 데이터베이스의 항목 관리
smtnrhtp(1M)	Trusted Extensions 네트워킹에 대한 템플리트 데이터베이스에서 항목 관리

smtnzonecfg(1M)	비전역 영역의 Trusted Extensions 네트워킹에 대한 구성 데이터베이스에서 항목 관리
str_to_label(3TSOL)	사람이 읽을 수 있는 문자열을 레이블로 구문 분석
tnctl(1M)	Trusted Extensions 네트워크 매개변수 구성
tnd(1M)	신뢰할 수 있는 네트워크 데몬
tninfo(1M)	커널 레벨 Trusted Extensions 네트워크 정보 및 통계 표시
trusted_extensions(5)	Trusted Extensions 소개
TrustedExtensionsPolicy(4)	Trusted Extensions X 서버 확장에 대한 구성 파일
tsol_getrhtype(3TSOL)	Trusted Extensions 네트워크 정보에서 호스트 유형 가져오기
updatehome(1M)	현재 레이블에 대한 홈 디렉토리 복사 및 링크 파일 업데이트
XTSOLgetClientAttributes(3XTSOL)	X 클라이언트의 레이블 속성 가져오기
XTSOLgetPropAttributes(3XTSOL)	창 등록 정보의 레이블 속성 가져오기
XTSOLgetPropLabel(3XTSOL)	창 등록 정보의 레이블 가져오기
XTSOLgetPropUID(3XTSOL)	창 등록 정보의 UID 가져오기
XTSOLgetResAttributes(3XTSOL)	창 또는 픽스맵의 모든 레이블 속성 가져오기
XTSOLgetResLabel(3XTSOL)	창, 픽스맵 또는 색상맵의 레이블 가져오기
XTSOLgetResUID(3XTSOL)	창 또는 픽스맵의 UID 가져오기
XTSOLgetSSHeight(3XTSOL)	화면 스트라이프의 높이 가져오기
XTSOLgetWorkstationOwner(3XTSOL)	워크스테이션의 소유권 가져오기
XTSOLIsWindowTrusted(3XTSOL)	신뢰할 수 있는 클라이언트가 창을 만들었는지 확인
XTSOLMakeTPWindow(3XTSOL)	이 창을 Trusted Path(신뢰할 수 있는 경로) 창으로 설정
XTSOLsetPolyInstInfo(3XTSOL)	다중 인스턴스화 정보 설정
XTSOLsetPropLabel(3XTSOL)	창 등록 정보의 레이블 설정
XTSOLsetPropUID(3XTSOL)	창 등록 정보의 UID 설정
XTSOLsetResLabel(3XTSOL)	창 또는 픽스맵의 레이블 설정

XTSOLsetResUID(3XTSOL)	창, 픽스맵 또는 색상맵의 UID 설정
XTSOLsetSessionHI(3XTSOL)	세션의 높은 민감도 레이블을 창 서버로 설정
XTSOLsetSessionLO(3XTSOL)	세션의 낮은 민감도 레이블을 창 서버로 설정
XTSOLsetSSHeight(3XTSOL)	화면 스트라이프의 높이 설정
XTSOLsetWorkstationOwner(3XTSOL)	워크스테이션의 소유권 설정

Trusted Extensions에서 수정된 Oracle Solaris 매뉴얼 페이지

Trusted Extensions에서는 다음 Oracle Solaris 매뉴얼 페이지에 정보를 추가합니다.

Oracle Solaris 매뉴얼 페이지	Trusted Extensions 수정
allocate(1)	영역에서 장치 할당과 창 환경에서 장치 정리를 지원하는 옵션 추가
auditconfig(1M)	레이블이 있는 정보에 대한 창 정책 추가
audit_class(4)	X 서버 감사 클래스 추가
audit_event(4)	감사 이벤트 추가
auditreduce(1M)	레이블 선택기 추가
auth_attr(4)	레이블 권한 부여 추가
automount(1M)	마운트 기능 즉, 하위 레벨 홈 디렉토리 보기 기능 추가
cancel(1)	사용자의 인쇄 작업 취소 기능에 대한 레이블 제한 추가
deallocate(1)	영역에서 장치 할당 취소, 창 환경에서 장치 정리 및 할당 취소할 장치 유형 지정을 지원하는 옵션 추가
device_clean(5)	Trusted Extensions에서 기본적으로 호출됨
exec_attr(4)	CDE 작업을 프로파일 객체 유형으로 추가
getpflags(2)	NET_MAC_AWARE 및 NET_MAC_AWARE_INHERIT 프로세스 플래그 인증
getsockopt(3SOCKET)	소켓의 필수 액세스 제어 상태인 SO_MAC_EXEMPT 가져오기
getsockopt(3XNET)	소켓의 필수 액세스 제어 상태인 SO_MAC_EXEMPT 가져오기
ifconfig(1M)	all-zones 인터페이스 추가
is_system_labeled(3C)	시스템이 Trusted Extensions로 구성되었는지 여부 확인

ldaplist(1)	Trusted Extensions 네트워크 데이터베이스 추가
list_devices(1)	장치에 연결된 속성(예: 레이블) 추가
lp(1)	-nolabels 옵션 추가
lpadmin(1M)	관리자의 인쇄 관리 기능에 레이블 제한 추가
lpmove(1M)	관리자의 인쇄 작업 이동 기능에 대한 레이블 제한 추가
lpq(1B)	인쇄 대기열 정보 표시에 대한 레이블 제한 추가
lprm(1B)	호출자의 인쇄 요청 제거 기능에 대한 레이블 제한 추가
lpsched(1M)	관리자의 인쇄 서비스 중지 및 다시 시작 기능에 대한 레이블 제한 추가
lpstat(1)	인쇄 서비스 상태 표시에 대한 레이블 제한 추가
netstat(1M)	확장 보안 속성을 표시하는 -R 옵션 추가
privileges(5)	Trusted Extensions 권한(예: PRIV_FILE_DOWNGRADE_SL) 추가
prof_attr(4)	권한 프로파일(예: Object Label Management) 추가
route(1M)	경로에 확장 보안 속성을 추가하는 -secattr 옵션 추가
setpflags(2)	NET_MAC_AWARE 프로세스별 플래그 설정
setsockopt(3SOCKET)	SO_MAC_EXEMPT 옵션 설정
setsockopt(3XNET)	소켓에 필수 액세스 제어인 SO_MAC_EXEMPT 설정
smexec(1M)	CDE 작업 유형을 지원하는 옵션 추가
smrole(1M)	역할 레이블을 지원하는 옵션 추가
smuser(1M)	사용자 레이블 및 기타 보안 속성을 지원하는 옵션 추가(예: 허용된 유휴 시간)
socket.h(3HEAD)	레이블이 없는 피어에 대한 SO_MAC_EXEMPT 옵션 지원
tar(1)	tar 파일에 레이블 포함 및 레이블에 따른 추출 기능 추가
tar.h(3HEAD)	레이블이 있는 tar 파일에 사용되는 속성 유형 추가
ucred_getlabel(3C)	사용자 자격 증명에서 레이블 값 가져오기 기능 추가
user_attr(4)	Trusted Extensions의 특정 사용자 보안 속성 추가

색인

A

add_allocatable 명령, 44
ADMIN_HIGH 레이블, 29
ADMIN_LOW 레이블
  관리 파일 보호, 61
  최하위 레이블, 30
Administrative Roles(관리 역할) 도구, 39
Allocate Device(장치 할당) 권한 부여, 241–242, 242
allocate 명령, 45
Assume Role(역할 맡기) 메뉴 항목, 51–52
atohexlabel 명령, 44, 71–72
audit_class 파일, 편집 작업, 35
audit_control 파일, 편집 작업, 35
audit_event 파일, 35
audit_startup 명령, 편집 작업, 35
auditconfig 명령, 46
auditreduce 명령, 46
automount 명령, 46

C

CD-ROM 드라이브
  액세스, 222
  음악 자동 재생, 235–236
CDE 작업, "작업"참조
Change Password(암호 변경) 메뉴 항목
  root 암호 변경에 사용, 69–70
  설명, 58
chk_encodings 명령, 44
  호출 작업, 35
Computers and Networks(컴퓨터 및 네트워크) 도구
  tnrhdb 데이터베이스 수정, 168–181
  알려진 호스트 추가, 175–176, 176–177
Computers and Networks(컴퓨터 및 네트워크) 도구
  세트, 40
.copy_files 파일
  사용자에 대한 설정, 87–88
  사용자의 시작 파일, 86–88
  설명, 81
  시작 파일, 45

D

DAC, "DAC(임의 액세스 제어)"참조
DAC(임의 액세스 제어), 27
deallocate 명령, 45
/dev/kmem 커널 이미지 파일, 보안 위반, 257
Device Allocation Manager(장치 할당 관리자)
  관리 도구, 34
  설명, 223–225
device-clean 스크립트
  요구 사항, 223
  장치에 추가, 237
Device Manager(장치 관리자)
  관리 도구, 34
  관리자가 사용, 229–232
dfstab 파일
  public 영역, 138
  편집 작업, 36
DNS 서버 설정 작업, 36
DOI, 원격 호스트 템플리트, 157

Downgrade DragNDrop or CutPaste Info(DragNDrop 또는 CutPaste 정보 다운그레이드) 권한 부여, 91–93
Downgrade File Label(파일 레이블 다운그레이드) 권한 부여, 91–93
dtappsession 명령, 44
dtsession 명령, updatehome 실행, 81
dtterm 터미널, .profile의 강제 소싱, 88
dtwm 명령, 259

E

/etc/default/kbd 파일, 편집 방법, 73–74
/etc/default/login 파일, 편집 방법, 73–74
/etc/default/passwd 파일, 편집 방법, 73–74
/etc/default/print 파일, 219
/etc/dfs/dfstab 파일, 36
/etc/dt/config/sel_config 파일, 64
/etc/hosts 파일, 175–176, 176–177
/etc/motd 파일, 편집 작업, 36
/etc/nsswitch.conf 파일, 36
/etc/resolv.conf 파일, 36
/etc/rmmount.conf 파일, 235–236, 236–237
/etc/security/audit_class 파일, 35
/etc/security/audit_control 파일, 35
/etc/security/audit_event 파일, 35
/etc/security/audit_startup 파일, 35
/etc/security/policy.conf 파일
  기본값, 78
  수정, 84–85
  편집 방법, 73–74
  포스트스크립트 인쇄 설정, 220
/etc/security/tsol/label_encodings 파일, 30

F

File Manager(파일 관리자), 장치 할당 후 표시 금지, 236–237

G

getlabel 명령, 44
getmounts 스크립트, 125
getzonelabels 스크립트, 123
getzonepath 명령, 44

H

hextoalabel 명령, 44, 72–73

I

IDLECMD 키워드, 기본값 변경, 85
IDLETIME 키워드, 기본값 변경, 85
ifconfig 명령, 46, 155
IP 주소
  tnrhdb 데이터베이스, 168–181
  tnrhdb 파일 내, 168–181
  tnrhdb의 폴백 방식, 159

J

JAR(Java 아카이브) 파일, 설치, 261–262

K

kmem 커널 이미지 파일, 257

L

label_encodings 파일
  내용, 30
  레이블이 있는 인쇄에 대한 참조, 196–199
  승인 범위의 소스, 30
  편집 및 확인 작업, 36
label 감사 토큰, 248–249
LDAP
  Trusted Extensions 데이터베이스, 111
  Trusted Extensions에 대한 이름 지정 서비스, 111–113
  문제 해결, 191–192
  시작, 114

LDAP *(계속)*
  이름 지정 서비스 관리, 113–115
  전역 영역 클라이언트 만들기 작업, 35
  중지, 114
  항목 표시, 114
LDAP 영역 초기화 작업, 36
LDAP 클라이언트 만들기 작업, 35
`.link_files` 파일
  사용자에 대한 설정, 86–88
  설명, 81
  시작 파일, 45
`list_devices` 명령, 45
`lp` 명령에 대한 `-o nobanner` 옵션, 219

M

MAC, "MAC(필수 액세스 제어)"참조
MAC(Mandatory Access Control), 네트워크에 적용, 151–156
MAC(필수 액세스 제어), Trusted Extensions, 27
MLP, "MLP(다중 레벨 포트)"참조
MLP(다중 레벨 포트)
  NFSv3 MLP 예, 132
  웹 프록시 MLP의 예, 132
`motd` 파일, 편집 작업, 36

N

`net_mac_aware` 권한, 127–128
`netstat` 명령, 46, 155, 188
NFS 마운트
  전역 및 레이블이 있는 영역에서, 135–136
  하위 레벨 디렉토리에 액세스, 137–140
`nsswitch.conf` 파일, 편집 작업, 36

O

Oracle Solaris OS
  Trusted Extensions 감사와의 유사점, 243
  Trusted Extensions 감사와의 차이점, 243
  Trusted Extensions와의 유사점, 23
  Trusted Extensions와의 차이점, 24–25

P

`plabel` 명령, 44
`policy.conf` 파일
  Trusted Extensions 키워드 변경, 85
  기본값, 78
  기본값 변경, 73–74
  편집 방법, 84–85
Print Postscript(포스트스크립트 인쇄) 권한 부여, 91–93, 199–201, 219–220
Print without Banner(배너 없이 인쇄) 권한 부여, 91–93, 219
`proc_info` 권한, 기본 세트에서 제거, 85
`public` 영역에 대한 `/etc/dfs/dfstab` 파일, 138

R

Remote Login(원격 로그인) 권한 부여, 91–93
`remove_allocatable` 명령, 44
`resolv.conf` 파일, 편집 작업, 36
Revoke or Reclaim Device(장치 해지 또는 재생 이용) 권한 부여, 241–242, 242
Rights(권한) 도구, 39
`rmmount.conf` 파일, 235–236, 236–237
root UID, 응용 프로그램에 필요, 257
root 역할, `device_clean` 스크립트 추가, 237
root의 실제 UID, 응용 프로그램에 필요, 257
`route` 명령, 46, 155

S

Security Templates(보안 템플리트) 도구, 40
  `tnrhdb` 수정, 168–181
  사용, 170
  템플리트 지정, 176–177
`sel_config` 파일, 64
  선택 항목 전송 규칙 구성, 64
  편집 작업, 35
`sel_mgr` 응용 프로그램, 62–64
Selection Manager(선택 관리자), 선택 확인자에 대한 규칙 구성, 64
Selection Manager(선택 관리자) 응용 프로그램, 62–64
`setlabel` 명령, 44

SMF(서비스 관리 기능), Trusted Extensions
서비스, 47–48
smtnrhdb 명령, 44
smtnrhtp 명령, 45
smtnzonecfg 명령, 45
snoop 명령, 155, 188
Solaris Management Console
Computers and Networks(컴퓨터 및 네트워크) 도구, 175–176
Security Templates(보안 템플리트) 도구, 40–41, 170
Trusted Network Zones(신뢰할 수 있는 네트워크 영역) 도구, 41
도구 및 도구 상자 설명, 38–42
도구 상자, 38
사용자 관리, 89–97
시작, 52–53
신뢰할 수 있는 네트워크 관리, 168–181
Solaris Management Console에서 기타 작업 처리(작업 맵), 97–98
Solaris Management Console에서 사용자 및 권한 관리(작업 맵), 89–97
solaris.print.nobanner 권한 부여, 85, 219
solaris.print.ps 권한 부여, 219–220
solaris.print.unlabeled 권한 부여, 85
Stop-A, 사용으로 설정, 73–74
Sun Ray 시스템
네트워크 프린터 구성, 206–209
사용자가 다른 사용자의 프로세스를 볼 수 없게 하기, 85
클라이언트 연결을 위한 tnrhdb 주소, 178
클라이언트와 서버 간 초기 연결 사용, 180

T

tar 명령, 46
TN 파일 확인 작업, 35
tnchkdb 명령
설명, 154
요약, 45
확인 작업, 35
tnctl 명령
사용, 187
설명, 154
tnctl 명령 *(**계속**)*
요약, 45
커널 캐시 업데이트, 185
tnd 명령
설명, 155
요약, 45
tninfo 명령
사용, 189, 191
설명, 155
요약, 45
tnrhdb 데이터베이스
0.0.0.0 와일드카드 주소, 178
0.0.0.0 호스트 주소, 160, 178
Sun Ray 서버에 대한 항목, 178
관리 도구, 40–41
구성, 168–181
와일드카드 주소, 168–181
추가, 176–177
폴백 방식, 159, 168–181
확인 작업, 35
tnrhtp 데이터베이스
관리 도구, 40–41
추가, 170–175
확인 작업, 35
trusted_edit 신뢰할 수 있는 편집기, 54–55
Trusted Extensions
Oracle Solaris OS와의 유사점, 23
Oracle Solaris OS와의 차이점, 24–25
Oracle Solaris 감사와의 유사점, 243
Oracle Solaris 감사와의 차이점, 243
관리에 대한 빠른 참조, 263–267
매뉴얼 페이지 빠른 참조, 269–273
Trusted Extensions DOI, 1이 아닌 DOI 사용으로 설정, 47–48
Trusted Extensions 관리자로 시작하기(작업 맵), 49–55
Trusted_Extensions 폴더
관리 편집기 사용, 54–55
위치, 34
작업 사용, 54
Trusted Extensions를 실행 중인 Xvnc 시스템, 원격 액세스, 109–110
Trusted Extensions를 실행하는 Xvnc 시스템, 원격 액세스, 100

Trusted Extensions에 대한 감사 이벤트, 목록, 247
Trusted Extensions에 대한 감사 클래스, 새 X 감사 클래스 목록, 247
Trusted Extensions에 대한 감사 토큰
label 토큰, 248–249
xatom 토큰, 249
xclient 토큰, 249
xcolormap 토큰, 250
xcursor 토큰, 250
xfont 토큰, 250
xgc 토큰, 251
xpixmap 토큰, 251
xproperty 토큰, 251–252
xselect 토큰, 252
xwindow 토큰, 252–253
목록, 248–253
Trusted Extensions에서 경로 구성 및 네트워크 정보 확인(작업 맵), 181–187
Trusted Extensions에서 소프트웨어 관리(작업), 260–262
Trusted Extensions에서 인쇄 관리(작업 맵), 203
Trusted Extensions에서 인쇄 제한 축소(작업 맵), 216–220
Trusted Extensions에서 장치 관리(작업 맵), 228–237
Trusted Extensions에서 장치 권한 부여 사용자 정의(작업 맵), 237–242
Trusted Extensions에서 장치 사용(작업 맵), 228
Trusted Extensions에서 장치 취급(작업 맵), 227
Trusted Extensions의 감사
Oracle Solaris 감사와의 차이점, 243
X 감사 클래스, 247
관리를 위한 역할, 244–246
기존 감사 명령에 대한 추가 사항, 253
보안 관리자 작업, 245
시스템 관리자 작업, 245–246
작업, 244–245
참조, 243–253
추가 감사 이벤트, 247
추가 감사 정책, 253
추가 감사 토큰, 248–253
Trusted Extensions의 감사 레코드, 정책, 253
Trusted Extensions의 감사 정책, 253
Trusted Extensions의 일반 작업(작업 맵), 67–74
Trusted Network Zones(신뢰할 수 있는 네트워크 영역) 도구
다중 레벨 인쇄 서버 구성, 204–205
다중 레벨 포트 구성, 132
다중 레벨 포트 만들기, 132
설명, 40, 41
Trusted Network(신뢰할 수 있는 네트워크) 도구, 설명, 40
Trusted Path(신뢰할 수 있는 경로) 메뉴, Assume Role(역할 맡기), 51–52
tsol_separator.ps 파일
구성 가능 값, 198
레이블이 있는 인쇄 사용자 정의, 196–199

U

updatehome 명령, 45, 81
Upgrade DragNDrop or CutPaste Info(DragNDrop 또는 CutPaste 정보 업그레이드) 권한 부여, 91–93
Upgrade File Label(파일 레이블 업그레이드) 권한 부여, 91–93
User Accounts(사용자 계정) 도구, 39
/usr/dt/bin/sel_mgr 응용 프로그램, 62–64
/usr/dt/bin/trusted_edit 신뢰할 수 있는 편집기, 54–55
/usr/dt/config/sel_config 파일, 64
/usr/lib/lp/postscript/tsol_separator.ps 파일, 프린터 출력 레이블 지정, 196–199
/usr/local/scripts/getmounts 스크립트, 125
/usr/local/scripts/getzonelabels 스크립트, 123
/usr/sbin/txzonemgr 스크립트, 34, 121
/usr/share/gnome/sel_config 파일, 64
utadm 명령, 기본 Sun Ray 서버 구성, 180

V

VNC(Virtual Network Computing), “Trusted Extensions를 실행 중인 Xvnc 시스템”참조

X

X 감사 클래스, 247
xatom 감사 토큰, 249
xc 감사 클래스, 247
xclient 감사 토큰, 249
xcolormap 감사 토큰, 250
xcursor 감사 토큰, 250
xfont 감사 토큰, 250
xgc 감사 토큰, 251
xp 감사 클래스, 247
xpixmap 감사 토큰, 251
xproperty 감사 토큰, 251–252
xs 감사 클래스, 247
xselect 감사 토큰, 252
Xtsolusersession 스크립트, 259
xwindow 감사 토큰, 252–253
xx 감사 클래스, 247

Z

ZFS
  레이블이 있는 영역에 데이터 세트 추가, 128–130
  레이블이 있는 영역에서 읽기/쓰기 권한으로 데이터 세트 마운트, 128–130
  상위 레벨 영역에서 마운트된 데이터 세트를 읽기 전용으로 보기, 129–130
/zone/public/etc/dfs/dfstab 파일, 138

가

가져오기, 소프트웨어, 255

감

감사 검토 프로파일, 감사 레코드 검토, 246
감사 시작 작업, 35
감사 이벤트 작업, 35
감사 제어 작업, 35
감사 클래스 작업, 35

개

개발자 책임, 258

게

게이트웨이
  승인 검사, 163
  예, 165

경

경로 지정, 161
  route 명령 사용, 182–183
  Trusted Extensions의 명령, 165
  개념, 163
  보안 속성이 있는 정적, 182–183
  승인 검사, 162–163
  예, 165
  테이블, 161–162, 164

계

계단식 인쇄, 209–211
계정
  "사용자"참조
  "역할"참조
계정 잠금, 방지, 95

공

공유, 레이블이 있는 영역에서 ZFS 데이터 세트, 128–130

관

관리
  "관리"참조
  dtappsession을 사용하여 원격으로, 103–105
  LDAP, 111–115

관리 *(계속)*
Solaris Management Console에서
원격으로, 105–106, 106–108
Sun Ray 인쇄, 206–209
Trusted Extensions에서 인쇄, 203
Trusted Extensions의 감사, 244–246
Trusted Extensions의 네트워크, 167–192
Trusted JDS의 영역, 121
Trusted Solaris 8과의 인쇄 상호 운용성, 201–202
계정 잠금, 95
관리자를 위한 빠른 참조, 263–267
다중 레벨 포트, 184–185
레이블이 없는 인쇄, 216–220
레이블이 있는 인쇄, 195–220
로그인을 위한 직렬 회선, 234–235
메일, 193–194
명령줄에서 원격으로, 103
보안 속성으로 경로 지정, 182–183
사용자, 77, 83–98
사용자 권한, 93–95
사용자에 대한 편리한 권한 부여, 91–93
사용자의 네트워크, 89–97
사용자의 시작 파일, 86–88
시스템 파일, 73–74
신뢰할 수 있는 네트워크 데이터베이스, 168–181
신뢰할 수 있는 네트워킹, 167–192
영역, 122–134
원격, 99–110
원격 호스트 데이터베이스, 176–177
원격 호스트 템플리트, 170–175
음악을 재생할 오디오 장치, 235–236
장치, 227–242
장치 권한 부여, 238–241
장치 권한 부여 할당, 241–242
장치 할당, 241–242
전역 영역에서, 51–52
정보의 레이블 변경, 96
타사 소프트웨어, 255–262
파일
백업, 142
복원, 142
파일 시스템
개요, 135
마운트, 144–149
관리, 파일 시스템 *(계속)*
문제 해결, 149–150
파일 시스템 공유, 142–144
포스트스크립트 인쇄, 219–220
관리 도구
Device Allocation Manager(장치 할당 관리자), 37–38
Labeled Zone Manager(레이블이 있는 영역 관리자), 35
Solaris Management Console, 38–42, 52–53
Trusted CDE 작업, 35–37
Trusted_Extensions 폴더에서, 54
`txzonemgr` 스크립트, 35
레이블 구축기, 43
명령, 44–46
설명, 33–46
액세스, 49–55
관리 레이블, 29
관리 역할, "역할"참조
관리 작업
"작업"참조
CDE, 35–37
Trusted_Extensions 폴더에서, 54
신뢰할 수 있는, 259
신뢰할 수 있는 CDE 목록, 35–37
액세스, 54–55
원격으로 시작, 105–106, 106–108
관리 편집기 작업, 35
열기, 54–55

구

구성
감사, 245
레이블이 있는 인쇄, 203–215
로그인을 위한 직렬 회선, 234–235
보안 속성으로 경로 지정, 182–183
사용자의 시작 파일, 86–88
신뢰할 수 있는 네트워크, 167–192
음악을 재생할 오디오 장치, 235–236
장치, 229–232
장치에 대한 권한 부여, 238–241
구성 요소 정의, `label_encodings` 파일, 30
구획 레이블 구성 요소, 29

국
국제화, “현지화”참조

권
권한
  “권한 프로파일”참조
  기본 세트에서 proc_info 제거, 85
  명령을 실행할 때, 51–52
  사용자 제한, 93–95
  사용자에 대한 기본값 변경, 80
  필요한 이유가 분명하지 않음, 257
권한 부여
  Allocate Device(장치 할당), 241–242, 242
  Revoke or Reclaim Device(장치 해지 또는 재생 이용), 241–242, 242
  solaris.print.nobanner, 219
  solaris.print.ps, 219–220
  레이블이 없는 인쇄, 216–220
  로컬 및 원격 장치 권한 부여 만들기, 240–241
  부여, 27
  사용자 또는 역할이 레이블을 변경할 수 있게 권한 부여, 96
  사용자 정의된 장치 권한 부여 만들기, 239
  사용자에 대한 편리, 91–93
  새 장치 권한 부여 추가, 238–241
  장치 권한 부여 할당, 241–242
  장치 속성 구성, 242
  장치 할당, 222, 241–242
  장치 할당 권한 부여가 포함된 프로파일, 242
  장치에 대한 사용자 정의, 241
  지정, 80
  포스트스크립트 인쇄, 199–201, 216–220
권한 프로파일
  Allocate Device(장치 할당) 권한 부여 포함, 241, 242
  새 장치 권한 부여 포함, 240–241
  작업 사용 제어, 259
  지정, 80
  편리한 권한 부여, 91–93

그
그룹
  보안 요구 사항, 61
  삭제 예방 조치, 61

금
금지
  “보호”참조
  임의의 레이블이 없는 호스트에서 레이블이 있는 호스트 연결, 177–181
  임의의 호스트에서 액세스, 177–181
  하위 레벨의 파일 액세스, 127–128

기
기본 경로 설정 작업, 36

내
내보내기, “공유”참조
내용 보기 없이 DragNDrop 또는 CutPaste 권한 부여, 91–93

네
네트워크, “신뢰할 수 있는 네트워크”참조
네트워크 데이터베이스
  LDAP, 111
  설명, 154
  확인 작업, 35
네트워크 패킷, 152
네트워킹 개념, 152–153

논
논리적 인터페이스 공유 작업, 36

다

다중 레벨 마운트, NFS 프로토콜 버전, 140–141
다중 레벨 인쇄
  Sun Ray 클라이언트, 209–211
  구성, 204–205
  인쇄 클라이언트를 통해 액세스, 213–214
다중 레벨 포트(MLP), 관리, 184–185

단

단일 레이블 인쇄, 영역에 대해 구성, 211–212
단일 레이블 작업, 31
단축 키, 데스크탑 포커스에 대한 컨트롤 다시 얻기, 70–71

데

데스크탑
  비상 안전 세션에 로그인, 88–89
  원격으로 다중 레벨 액세스, 109–110
  작업 공간 색상 변경, 52
데스크탑 포커스에 대한 컨트롤 다시 얻기, 70–71
데스크탑 포커스에 대한 컨트롤 복원, 70–71
데이터 세트, "ZFS"참조
데이터베이스
  LDAP, 111
  신뢰할 수 있는 네트워크, 154
  장치, 35

도

도구, "관리 도구"참조
도구 상자, 정의, 38
도구 서브패널, Device Allocation Manager(장치 할당 관리자), 223–225

디

디렉토리
  공유, 142–144
  마운트, 142–144
디렉토리 *(**계속**)*
  사용자 또는 역할이 레이블을 변경할 수 있게 권한 부여, 96
  하위 레벨에 액세스, 117
디버깅, "문제 해결"참조
디스켓, 액세스, 222

레

레이블
  "레이블 범위"참조
  16진수로 표시, 71–72
  개요, 28
  관계, 29–30
  구획 구성 요소, 29
  내부 데이터베이스에서 복구, 72–73
  다운그레이드 및 업그레이드, 64
  레이블 변경 규칙 구성, 64
  레이블이 있는 영역의 파일 시스템 레이블 표시, 125–126
  문제 해결, 72–73
  분류 구성 요소, 29
  사용자 또는 역할이 데이터의 레이블을 변경할 수 있게 권한 부여, 96
  사용자 프로세스, 31
  설명, 27
  올바른 형식, 30
  원격 호스트 템플리트의 기본값, 156
  지배, 29–30
  페이지 레이블 없이 인쇄, 218
  프로세스, 31–32
  프린터 출력, 196–199
  해당하는 텍스트 결정, 72–73
레이블 권한 부여 없이 인쇄, 91–93
레이블 다운그레이드, 선택 확인자에 대한 규칙 구성, 64
레이블 범위
  프레임 버퍼에 설정, 222–223
  프린터 레이블 범위 제한, 215
  프린터에 설정, 222–223
레이블 업그레이드, 선택 확인자에 대한 규칙 구성, 64
레이블에 해당하는 텍스트, 결정, 72–73
레이블의 지배, 29–30

레이블이 없는 인쇄, 구성, 216–220
레이블이 있는 영역, "영역"참조
레이블이 있는 인쇄
  Sun Ray 클라이언트, 206–209
  레이블 제거, 91–93
  배너 페이지, 197–199
  배너 페이지 없이, 91–93, 219
  본문 페이지, 196–197
  포스트스크립트 제한 제거, 91–93
  포스트스크립트 파일, 219–220
레이블이 있는 인쇄 구성(작업 맵), 203–215
레이블이 있는 파일 백업, 공유 및 마운트(작업 맵), 141–150

로

로그아웃, 필요, 85
로그인
  역할별, 48–49
  역할을 통한 원격, 101–102
  직렬 회선 구성, 234–235

마

마운트
  NFSv3 파일 시스템, 47–48
  개요, 135–136
  레이블이 있는 영역의 ZFS 데이터 세트, 128–130
  루프백 마운트하여 파일, 126
  문제 해결, 149–150
  파일 시스템, 142–144

만

만들기
  장치에 대한 권한 부여, 238–241
  홈 디렉토리, 138–139

맡

맡기, 역할, 51–52

매

매뉴얼 페이지, Trusted Extensions 관리자를 위한 빠른 참조, 269–273

멀

멀티헤디드 시스템, 신뢰할 수 있는 스트라이프, 25

메

메일
  Trusted Extensions의 구현, 193–194
  관리, 193–194
  다중 레벨, 193

명

명령
  `trusted_edit` 신뢰할 수 있는 편집기, 54–55
  권한으로 실행, 51–52
  네트워킹 문제 해결, 188

문

문제 해결
  LDAP, 191–192
  내부 데이터베이스에서 레이블 복구, 72–73
  네트워크, 187–192
  로그인 실패, 88–89
  마운트된 파일 시스템, 149–150
  신뢰할 수 있는 네트워크, 188–191
  인터페이스가 작동 중인지 확인, 187–188
  장치 재생 이용, 232–233
  하위 레벨 영역에 마운트된 ZFS 데이터 세트 보기, 130

물

물리적 인터페이스 공유 작업, 36

배
배너 페이지
  레이블 없이 인쇄, 219
  레이블이 있음에 대한 설명, 197–199
  일반, 197
  트레일러 페이지의 차이, 197–198

번
번역, "현지화"참조

변
변경
  IDLETIME 키워드, 85
  권한 부여된 사용자의 레이블, 96
  데이터의 보안 레벨, 96
  레이블 변경 규칙, 64
  사용자 권한, 93–95
  선택 확인자 기본값, 64
  시스템 보안 기본값, 73–74

보
보기, "액세스"참조
보안, 키 조합, 70–71
보안 관리자, "보안 관리자 역할"참조
보안 관리자 역할
  감사 작업, 245
  로그인을 위한 직렬 회선 구성, 234–235
  보안 설정, 225
  사용자에게 권한 부여 지정, 91–93
  사용자의 네트워크 관리, 89–97
  장치 구성, 229–232
  창 구성 파일 수정, 65
  편리한 권한 부여 권한 프로파일 만들기, 91–93
  포스트스크립트 제한 관리, 200
  프린터 보안 관리, 195
  할당 불가능한 장치 보호, 233–234
보안 레이블 세트, 원격 호스트 템플리트, 157
보안 방식
  Oracle Solaris, 256
보안 방식 (**계속**)
  확장 가능, 58
보안 속성, 161–162
  경로에서 사용, 182–183
  모든 사용자에 대한 기본값 수정, 84–85
  사용자 기본값 수정, 84
  원격 호스트에 대해 설정, 170–175
보안 정보, 프린터 출력, 196–199
보안 정책
  감사, 253
  사용자 교육, 59
  사용자 및 장치, 225
보안 템플리트, "원격 호스트 템플리트"참조
보안을 위한 사용자 환경 사용자 정의(작업 맵), 83–89
보호
  레이블이 있는 정보, 31–32
  비독점적 이름을 사용하는 파일 시스템, 142
  원격 할당 장치, 234
  장치, 37–38, 221–223
  할당 불가능한 장치, 233–234

복
복구, 내부 데이터베이스에서 레이블, 72–73

본
본문 페이지
  레이블이 있음에 대한 설명, 196–197
  모든 사용자에 대해 레이블 없이, 218
  특정 사용자에 대해 레이블 없이, 218–219

분
분류 레이블 구성 요소, 29

비
비상 안전 세션, 로그인, 88–89

사

사용, 1이 아닌 DOI, 47–48
사용으로 설정, 키보드 셧다운, 73–74
사용자
  Change Password(암호 변경) 메뉴 항목, 58
  .copy_files 파일 사용, 86–88
  .link_files 파일 사용, 86–88
  계정 잠금 방지, 95
  계획, 77
  골격 디렉토리 설정, 86–88
  권한 부여, 91–93
  권한 부여 지정, 80
  권한 지정, 80
  기본 권한 변경, 80
  다른 사용자의 프로세스를 볼 수 없게 하기, 85
  데스크탑 포커스에 대한 컨트롤 복원, 70–71
  레이블 지정, 80
  만들기, 76
  모든 사용자에 대한 보안 기본값 수정, 84–85
  보안 교육, 59, 61, 225
  보안 기본값 수정, 84
  보안 예방 조치, 61
  비상 안전 세션에 로그인, 88–89
  삭제 예방 조치, 61
  세션 범위, 31
  시작 파일, 86–88
  암호 지정, 79
  역할 지정, 80
  인쇄, 195–202
  일부 권한 제거, 93–95
  장치 사용, 228
  장치에 액세스, 221–223
  전역 영역에 원격으로 로그인, 108–109
  프로세스 레이블, 31
  프린터 액세스, 195–202
  환경 사용자 정의, 83–89
사용자 정의
  label_encodings 파일, 30
  레이블이 없는 인쇄, 216–220
  사용자 계정, 83–89
  장치 권한 부여, 241

상

상용 응용 프로그램, 평가, 258
상호 운용성, Trusted Solaris 8 및 인쇄, 201–202

색

색상, 작업 공간의 레이블 표시, 32

선

선택
  "선택"참조
  레이블로 감사 레코드, 246
선택 확인 구성 작업, 35
선택 확인자, 기본값 변경, 64

세

세션, 비상 안전, 88–89
세션 범위, 31

소

소프트웨어
  Java 프로그램 설치, 261–262
  가져오기, 255
  타사 관리, 255–262

수

수정, sel_config 파일, 64

스

스크립트
  getmounts, 125
  getzonelabels, 123
  /usr/sbin/txzonemgr, 34, 121

승

승인 검사, 162–163
승인 범위, label_encodings 파일, 30

시

시스템 관리자 역할
  File Manager(파일 관리자) 표시 금지, 236–237
  감사 레코드 검토, 246
  감사 작업, 245–246
  공용 시스템에서 레이블이 없는 본문 페이지 사용으로 설정, 85
  음악이 자동으로 재생되도록 설정, 235–236
  인쇄 변환 필터 추가, 200
  장치 재생 이용, 232–233
  프린터 관리, 195
시스템 관리자의 감사 작업, 245–246
시스템 파일
  Oracle Solaris /etc/default/print, 219
  Oracle Solaris policy.conf, 220
  Trusted Extensions sel_config, 64
  Trusted Extensions tsol_separator.ps, 218
  편집, 54–55, 73–74
시작 파일, 사용자 정의 절차, 86–88

신

신뢰할 수 있는 경로 속성, 사용 가능한 경우, 28
신뢰할 수 있는 네트워크
  0.0.0.0 tnrhdb 항목, 177–181
  Solaris Management Console에서 관리, 168–181
  개념, 151–165
  경로 지정 예, 165
  기본 경로 설정 작업, 36
  기본 레이블, 162
  레이블 및 MAC 설정, 151–156
  로컬 파일 편집, 168–181
  템플리트 사용, 168–181
  파일의 구문 확인, 183
  호스트 유형, 157–158
신뢰할 수 있는 네트워크 데이터베이스 구성(작업 맵), 168–181
신뢰할 수 있는 네트워크 도구, 사용, 170
신뢰할 수 있는 네트워크 문제 해결(작업 맵), 187–192
신뢰할 수 있는 네트워킹 관리(작업 맵), 167
신뢰할 수 있는 스트라이프
  멀티헤디드 시스템, 25
  포인터 가져오기, 71
신뢰할 수 있는 응용 프로그램, 역할 작업 공간, 33
신뢰할 수 있는 작업, CDE, 35–37
신뢰할 수 있는 잡기, 키 조합, 70–71
신뢰할 수 있는 편집기
  시작, 54–55
  즐겨 찾는 편집기 지정, 68–69
신뢰할 수 있는 프로그램, 257–258
  정의, 257–258
  추가, 257–258
신뢰할 수 있는 프로세스
  윈도우 시스템에서, 259–260
  작업 시작, 259

아

아이콘 표시 여부
  File Manager(파일 관리자)에서, 259
  Workspace(작업 공간) 메뉴에서, 259

암

암호
  Change Password(암호 변경) 메뉴 항목, 58, 69–70
  root에 대해 변경, 69–70
  사용자 암호 변경, 58
  암호 프롬프트를 신뢰할 수 있는지 테스트, 71
  저장소, 61
  지정, 79

액

액세스
  "컴퓨터 액세스"참조
  Solaris Management Console, 52–53
  Trusted CDE 작업, 54
  관리 도구, 49–55

액세스 *(계속)*
관리 편집기 작업, 54–55
레이블로 감사 레코드, 246
상위 레벨 영역에서 하위 레벨 영역에 마운트된 ZFS 데이터 세트, 129–130
원격 다중 레벨 데스크탑, 109–110
장치, 221–223
전역 영역, 51–52
프린터, 195–202
홈 디렉토리, 117
액세스 정책
DAC(임의 액세스 제어), 23, 24–25
MAC(필수 액세스 제어), 24
장치, 223

역

역할
감사 관리, 244
권한 지정, 80
레이블이 없는 호스트의 역할 맡기, 101
만들기, 49
맡기, 48–49, 51–52
신뢰할 수 있는 응용 프로그램 액세스, 33
역할 작업 공간 떠나기, 52
원격 로그인, 101–102
원격으로 관리, 105–106, 106–108
작업 공간, 48–49
역할 작업 공간, 전역 영역, 48–49

영

영역
MLP 만들기, 132
net_mac_aware 권한, 144–149
NFSv3용 MLP 만들기, 132
Trusted Extensions에서, 117–134
Trusted JDS에서 관리, 121
관리, 117–134
구성 작업, 36
논리적 인터페이스 공유 작업, 36
다시 시작 작업, 36
레이블 지정 도구, 41
영역 *(계속)*
물리적 인터페이스 공유 작업, 36
복사 작업, 36
복제 작업, 36
상태 표시, 123
설치 작업, 36
시작 작업, 36
전역, 117
종료 작업, 36
초기화 작업, 36
콘솔에서 보기 작업, 36
파일 시스템 레이블 표시, 125–126
영역 관리(작업 맵), 122–134
영역 구성 작업, 36
영역 다시 시작 작업, 36
영역 복사 작업, 36
영역 복제 작업, 36
영역 설치 작업, 36
영역 시작 작업, 36
영역 종료 작업, 36
영역 터미널 콘솔 작업, 36

오

오디오 장치
오디오 플레이어 자동 시작, 235–236
원격 할당 금지, 234

올

올바른 형식의 레이블, 30

와

와일드카드 주소, “폴백 방식”참조

원

원격 관리
기본값, 99–100
방법, 100

원격 다중 레벨 데스크탑, 액세스, 109–110
원격 호스트, tnrhdb에서 폴백 방식 사용, 159
원격 호스트 템플리트
  관리 도구, 40–41
  만들기, 170–175
  지정, 168–181
  호스트에 지정, 176–177
원격으로 Trusted Extensions 관리(작업 맵), 102–110

윈
윈도우 시스템, 신뢰할 수 있는 프로세스, 259–260

유
유사점
  Trusted Extensions 및 Oracle Solaris OS, 23
  Trusted Extensions 및 Oracle Solaris 감사, 243

응
응용 프로그램
  보안 평가, 258
  설치, 260–262
  신뢰할 수 있는, 257–258

이
이동식 매체, 마운트, 260–261
이름 서비스 스위치 작업, 36, 189
이름 지정 서비스
  LDAP, 111–115
  LDAP 관리, 113–115
  Trusted Extensions에 고유한 데이터베이스, 111

인
인쇄
  Oracle Solaris 인쇄 서버 레이블 지정, 217–218
  Oracle Solaris 인쇄 서버 사용, 217–218
인쇄 *(**계속**)*
  Oracle Solaris 인쇄 서버의 공용 작업, 217–218
  Sun Ray 클라이언트에 대해 구성, 206–209
  Trusted Extensions의 포스트스크립트
    제한, 199–201
  Trusted Solaris 8과의 상호 운용성, 201–202
  공용 시스템에서 레이블이 없는 출력에 대한
    권한 부여, 85
  공용 인쇄 작업 구성, 217–218
  관리, 195–202
  다중 레벨 레이블이 있는 출력 구성, 204–205
  레이블 및 텍스트 구성, 198
  레이블 범위 제한, 215
  레이블이 있는 배너 또는 트레일러 없이, 91–93
  레이블이 있는 배너 및 트레일러 없이, 219
  레이블이 있는 영역 구성, 211–212
  레이블이 있는 출력 국제화, 198
  레이블이 있는 출력 현지화, 198
  모델 스크립트, 200
  및 label_encodings 파일, 30
  변환 필터 추가, 200–201
  인쇄 클라이언트에 대해 구성, 213–214
  출력에 레이블 인쇄 방지, 216–217
  페이지 레이블 없이, 91–93, 218
  포스트스크립트 제한 제거, 91–93
  포스트스크립트 파일, 219–220
  현지 언어로, 198
인코딩 편집 작업, 36
인코딩 확인 작업, 35
인터페이스
  보안 템플리트에 지정, 176–177
  작동 중인지 확인, 187–188

일
일반 사용자, "사용자"참조
일별 메시지 설정 작업, 36

작
작업
  "이름별 개별 작업"참조
  CDE와 Trusted CDE 사이의 사용 차이점, 259

작업 *(계속)*
Device Allocation Manager(장치 할당 관리자), 223–225
관리 편집기, 54–55
권한 프로파일에 의해 제한되는, 259
새 Trusted CDE 작업 추가, 259–260
신뢰할 수 있는 CDE 목록, 35–37
이름 서비스 스위치, 189
작업 공간
레이블을 나타내는 색상, 32
색상 변경, 52
전역 영역, 48–49
작업 및 작업 맵
Solaris Management Console에서 기타 작업 처리(작업 맵), 97–98
Solaris Management Console에서 사용자 및 권한 관리, 89–97
Trusted Extensions 관리자로 시작하기(작업 맵), 49–55
Trusted Extensions에서 경로 구성 및 네트워크 정보 확인(작업 맵), 181–187
Trusted Extensions에서 소프트웨어 관리(작업), 260–262
Trusted Extensions에서 인쇄 관리(작업 맵), 203
Trusted Extensions에서 인쇄 제한 축소(작업 맵), 216–220
Trusted Extensions에서 장치 관리(작업 맵), 228–237
Trusted Extensions에서 장치 권한 부여 사용자 정의(작업 맵), 237–242
Trusted Extensions에서 장치 사용(작업 맵), 228
Trusted Extensions에서 장치 취급(작업 맵), 227
Trusted Extensions의 일반 작업(작업 맵), 67–74
레이블이 있는 인쇄 구성(작업 맵), 203–215
레이블이 있는 파일 백업, 공유 및 마운트(작업 맵), 141–150
보안 관리자의 감사 작업, 245
보안을 위한 사용자 환경 사용자 정의(작업 맵), 83–89
시스템 관리자의 감사 작업, 245–246
신뢰할 수 있는 네트워크 데이터베이스 구성(작업 맵), 168–181
신뢰할 수 있는 네트워크 문제 해결(작업 맵), 187–192
작업 및 작업 맵 *(계속)*
신뢰할 수 있는 네트워킹 관리(작업 맵), 167
영역 관리(작업 맵), 122–134
원격으로 Trusted Extensions 관리(작업 맵), 102–110

잘

잘라내기 및 붙여넣기
레이블 변경 규칙 구성, 64
및 레이블, 62–64

장

장치
`device_clean` 스크립트 추가, 237
Device Manager(장치 관리자)로 관리, 229–232
Trusted Extensions, 221–226
관리, 227–242
문제 해결, 232–233
보호, 37–38
사용, 228
사용자 정의된 권한 부여 추가, 241
새 권한 부여 만들기, 238–241
액세스, 223–225
액세스 정책, 223
오디오 설정, 235–236
오디오 플레이어 자동 시작, 235–236
오디오의 원격 할당 금지, 234
장치 구성, 229–232
재생 이용, 232–233
정책 기본값, 223
정책 설정, 223
직렬 회선 구성, 234–235
할당, 221–223
할당 불가능한 장치 보호, 233–234
할당 불가능한 장치에 대한 레이블 범위 설정, 222–223
장치 권한 부여 할당, 91–93
장치 데이터베이스, 편집 작업, 35
장치 속성 구성 권한 부여, 242
장치 할당
File Manager(파일 관리자) 표시 금지, 236–237

장치 할당 *(계속)*
개요, 221–223
권한 부여, 241–242
할당 권한 부여가 포함된 프로파일, 242
장치 할당 권한 부여, 222

전
전면 패널, Device Allocation Manager(장치 할당 관리자), 223–225
전역 영역
들어가기, 51–52
레이블이 있는 영역과의 차이점, 117
사용자로 원격 로그인, 108–109
종료, 52

절
절차, "작업 및 작업 맵"참조

정
정보 레이블 재지정, 96

제
제거, 프린터 출력의 레이블, 216–217
제어, "제한"참조
제한
권한 프로파일별 작업, 259
네트워크에서 정의된 호스트, 177–181
레이블을 기준으로 컴퓨터에 대한 액세스, 222–223
레이블을 사용하여 프린터 액세스, 196
레이블을 사용하여 프린터에 액세스, 196
원격 액세스, 99–100
장치에 대한 액세스, 221–223
전역 영역에 액세스, 49
프린터 레이블 범위, 215
하위 레벨 파일에 액세스, 127–128
하위 레벨 파일의 마운트, 127–128

종
종료 권한 부여, 91–93

지
지정
권한 프로파일, 80
사용자에게 권한, 80
편집기를 신뢰할 수 있는 편집기로, 68–69

직
직렬 회선, 로그인을 위한 구성, 234–235

차
차이, Oracle Solaris 인터페이스 확장, 265–266
차이점
Trusted Extensions 및 Oracle Solaris 감사, 243
Trusted Extensions와 Oracle Solaris OS, 24–25
Trusted Extensions의 관리 인터페이스, 263–264
Trusted Extensions의 기본값, 266
Trusted Extensions의 제한된 옵션, 266–267

창
창 관리자, 259

찾
찾기
레이블에 해당하는 16진수, 71–72
레이블에 해당하는 텍스트 형식의 항목, 72–73

최
최대 레이블, 원격 호스트 템플리트, 157
최소 레이블, 원격 호스트 템플리트, 157

컴
컴퓨터 액세스
  관리자 책임, 60–61
  제한, 222–223

클
클리어런스, 레이블 개요, 28

키
키 조합, 잡기를 신뢰할 수 있는지 테스트, 70–71
키보드 셧다운, 사용으로 설정, 73–74

테
테이프 장치, 액세스, 222

트
트레일러 페이지, "배너 페이지"참조

파
파일
  .copy_files, 45, 81, 86–88
  /etc/default/kbd, 73–74
  /etc/default/login, 73–74
  /etc/default/passwd, 73–74
  /etc/default/print, 219
  /etc/dfs/dfstab, 36
  /etc/dt/config/sel_config, 64
  /etc/motd, 36
  /etc/nsswitch.conf, 36
  /etc/resolv.conf, 36
  /etc/rmmount.conf, 235–236
  /etc/security/audit_class, 35
  /etc/security/audit_control, 35
  /etc/security/audit_event, 35
  /etc/security/audit_startup, 35
파일 *(계속)*
  /etc/security/policy.conf, 78, 84–85, 220
  /etc/security/tsol/label_encodings, 36
  getmounts, 125
  getzonelabels, 123
  .link_files, 45, 81, 86–88
  policy.conf, 73–74
  sel_config 파일, 64
  /usr/dt/bin/sel_mgr, 62–64
  /usr/dt/config/sel_config, 35, 64
  /usr/lib/lp/postscript/tsol_separator.ps, 196–199
  /usr/sbin/txzonemgr, 34, 121
  /usr/share/gnome/sel_config, 64
  레이블 바꾸기 권한, 130
  루프백 마운트, 126
  백업, 142
  복원, 142
  사용자 또는 역할이 레이블을 변경할 수 있게 권한 부여, 96
  시작, 86–88
  신뢰할 수 있는 편집기로 편집, 54–55
  지배하는 레이블에서 액세스, 124–126
  지배하는 레이블에서 액세스 금지, 127–128
  포스트스크립트, 219–220
파일 및 파일 시스템
  공유, 142–144
  마운트, 142–144
  이름 지정, 142
파일 시스템
  NFS 마운트, 135–136
  NFSv3, 47–48
  공유, 135
  전역 및 레이블이 있는 영역에서 공유, 135–136
  전역 및 레이블이 있는 영역에서 마운트, 135–136
파일 시스템 공유 작업, 36
파일 시스템의 이름, 142

패
패키지, 매체 액세스, 260–261

편
편집
  시스템 파일, 73–74
  신뢰할 수 있는 편집기 사용, 54–55

포
포스트스크립트
  Trusted Extensions의 인쇄 제한, 199–201
  인쇄 설정, 219–220

폴
폴백 방식
  tnrhdb, 159
  네트워크 구성에 사용, 168–181
  원격 호스트, 168–181

표
표시
  레이블이 있는 영역의 파일 시스템 레이블, 125–126
  모든 영역의 상태, 123

프
프로그램, "응용 프로그램"참조
프로그램의 보안 평가, 257–258
프로세스
  레이블, 31–32
  사용자 프로세스의 레이블, 31
  사용자가 다른 사용자의 프로세스를 볼 수 없게 하기, 85
프로파일, "권한 프로파일"참조
프린터, 레이블 범위 설정, 222–223
프린터 출력, "인쇄"참조

플
플로피, "디스켓"참조
플로피 디스크, "디스켓"참조

할
할당, Device Allocation Manager(장치 할당 관리자) 사용, 223–225
할당 가능한 장치 추가 작업, 35
할당 불가능한 장치
  레이블 범위, 222–223
  보호, 233–234
할당 오류 상태, 수정, 232–233
할당 해제, 강제, 232–233

현
현지화, 레이블이 있는 프린터 출력 변경, 198

호
호스트
  네트워크 파일에 입력, 175–176
  네트워킹 개념, 152–153
  보안 템플리트에 지정, 176–177
  템플리트 지정, 168–181
호스트 유형
  네트워킹, 152, 157–158
  원격 호스트 템플리트, 156
  템플리트 및 프로토콜 표, 157–158

홈
홈 디렉토리
  만들기, 138–139
  액세스, 117

확

확인
네트워크 데이터베이스의 구문, 183
인터페이스 작동 중, 187–188