Solaris 10 11/06 및 Solaris 10 8/07 릴리스용 Solaris Trusted Extensions 설치 및 구성

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

부품 번호: 819–7610–13
2009년 4월

090318@21990

목차

그림

표

머리말

Solaris 10 11/06 및 Solaris 10 8/07 릴리스용 Solaris Trusted Extensions 설치 및 구성 설명서에서는 Solaris 운영 체제에서 Solaris™ Trusted Extensions를 구성하는 절차에 대해 설명합니다. 또한 Solaris Trusted Extensions의 보안 설치를 지원하도록 Solaris 시스템을 준비하는 방법에 대해서도 설명합니다.

주의 – 이 설명서는 Solaris 10 11/06 및 Solaris 10 8/07 릴리스 전용 Trusted Extensions를 설치하는 데 사용됩니다. Solaris Express Developer Edition 5/07 릴리스용으로도 사용할 수 있습니다.

이후 릴리스의 경우 이 설명서를 사용하지 **마십시오**. **Solaris Trusted Extensions 구성 안내서**를 사용하십시오.

주 – 이 Solaris 릴리스에서는 SPARC® 및 x86 제품군 프로세서 구조 UltraSPARC®, SPARC64, AMD64, Pentium 및 Xeon EM64T 시스템을 지원합니다. 지원되는 시스템은 **Solaris OS: Hardware Compatibility Lists**(`http://www.sun.com/bigadmin/hcl`)를 참조하십시오. 이 설명서에서는 플랫폼 유형에 따른 구현 차이가 있는 경우 이에 대하여 설명합니다.

이 문서에서 사용되는 x86 관련 용어의 의미는 다음과 같습니다.

- "x86"은 64비트 및 32비트 x86 호환 제품의 큰 제품군을 의미합니다.
- "x64"는 AMD64 또는 EM64T 시스템에 대한 특정 64비트 정보를 나타냅니다.
- "32비트 x86"은 x86 기반 시스템에 대한 특정 32비트 정보를 나타냅니다.

지원되는 시스템은 **Solaris OS: Hardware Compatibility Lists**를 참조하십시오.

본 설명서의 대상

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

사이트 보안 구현

사이트 보안과 일치하는 방식으로 시스템에 Trusted Extensions를 성공적으로 구성하려면 Trusted Extensions의 보안 기능과 사이트 보안 정책을 잘 알고 있어야 합니다. 소프트웨어를 구성할 때 사이트 보안을 보장하는 방법에 대한 자세한 내용을 보려면 Solaris Trusted Extensions 패키지를 설치하기 전에 1 장, "Trusted Extensions의 보안 계획"을 읽어 보십시오.

Trusted Extensions 및 Solaris 운영 체제

Trusted Extensions는 Solaris 운영 체제(Solaris OS)위에 설치됩니다. Trusted Extensions 소프트웨어는 Solaris OS를 수정할 수 있기 때문에 Trusted Extensions에서 Solaris 설치 옵션을 특수 설정할 수 있습니다. 자세한 내용은 3 장, "Solaris Trusted Extensions 소프트웨어 설치(작업)"를 참조하십시오. 또한 Trusted Extensions 설명서는 Solaris 설명서를 보완합니다. 사용자는 관리자로 Solaris 설명서 및 Trusted Extensions 설명서에 대한 액세스 권한이 필요합니다.

본 설명서의 구성

1 장, "Trusted Extensions의 보안 계획"에서는 하나 이상의 Solaris 시스템에서 Trusted Extensions 소프트웨어를 구성할 때 고려해야 할 보안 문제에 대해 설명합니다.

2 장, "Trusted Extensions 설치 및 구성 로드맵"에서는 Trusted Extensions 소프트웨어를 Solaris 시스템에 추가하기 위한 작업 맵이 포함되어 있습니다.

3 장, "Solaris Trusted Extensions 소프트웨어 설치(작업)"에서는 Trusted Extensions 소프트웨어에 대한 Solaris 시스템 준비 지침을 제공합니다. 또한 패키지 추가에 대한 지침도 포함됩니다.

4 장, "Trusted Extensions 구성(작업)"에서는 모니터가 있는 시스템에서 Trusted Extensions 소프트웨어를 구성하는 방법에 대한 지침을 제공합니다.

5 장, "Trusted Extensions에 대해 LDAP 구성(작업)"에서는 Trusted Extensions에 대해 LDAP를 구성하는 방법에 대한 지침을 제공합니다.

6 장, "Trusted Extensions로 헤드리스 시스템 구성(작업)"에서는 헤드리스 시스템에서 Trusted Extensions 소프트웨어를 구성 및 관리하는 방법에 대해 설명합니다.

부록 A, "사이트 보안 정책"에서는 사이트 보안 정책에 대해 설명하고 Trusted Extensions를 더 광범위한 조직 및 사이트 보안 컨텍스트 내에 배치합니다.

부록 B, "CDE 작업을 사용하여 Trusted Extensions에 영역 설치"에서는 Trusted CDE 작업을 사용하여 레이블이 있는 영역을 구성하는 방법에 대해 설명합니다.

부록 C, "Trusted Extensions 구성 검사 목록"에서는 설치 팀을 위한 구성 점검 목록을 제공합니다.

용어집에서는 본 설명서에서 사용된 어구와 선택된 용어를 정의합니다.

Solaris Trusted Extensions 설명서의 구성

Solaris Trusted Extensions 설명서 세트에는 Solaris 10 8/07 릴리스의 설명서를 보완하는 내용이 포함되어 있습니다. Solaris Trusted Extensions를 더 잘 이해하려면 두 설명서 세트를 모두 읽어 보십시오. Solaris Trusted Extensions 설명서 세트는 다음 책으로 구성되어 있습니다.

설명서 제목	내용	대상
Solaris Trusted Extensions Transition Guide	Trusted Solaris 8 소프트웨어, Solaris 10 8/07 소프트웨어 및 Solaris Trusted Extensions 소프트웨어 간의 차이점에 대한 개요를 제공합니다.	모든 사용자
Solaris Trusted Extensions Reference Manual	Solaris Trusted Extensions 매뉴얼 페이지를 제공합니다.	모든 사용자
Solaris Trusted Extensions 사용 설명서	Solaris Trusted Extensions의 기본 기능에 대해 설명합니다. 이 설명서에는 용어집도 포함되어 있습니다.	최종 사용자, 관리자 및 개발자
Solaris 10 11/06 및 Solaris 10 8/07 릴리스용 Solaris Trusted Extensions 설치 및 구성	Solaris Trusted Extensions의 계획, 설치 및 구성 방법에 대해 설명합니다.	관리자, 개발자
Solaris Trusted Extensions Administrator's Procedures	특정 관리 작업을 수행하는 방법에 대해 설명합니다.	관리자, 개발자
Solaris Trusted Extensions Developer's Guide	Solaris Trusted Extensions로 응용 프로그램을 개발하는 방법에 대해 설명합니다.	개발자, 관리자
Solaris 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

Sun Microsystems의 관련 설명서

다음 설명서에는 Solaris Trusted Extensions 소프트웨어를 설치할 때 유용한 정보가 포함되어 있습니다.

Solaris 설명서

Solaris 10 11/06 설치 설명서: 기본 설치 – Solaris OS에 관한 설치 옵션 지침을 제공합니다.

Solaris 10 11/06 설치 설명서: 사용자 정의 JumpStart 및 고급 설치 – 디스크 공간 요구사항, 설치 방법 및 구성 옵션에 관한 지침을 제공합니다.

System Administration Guide: Basic Administration – Solaris OS의 기본 관리 작업(예: Solaris Management Console 사용)에 대해 설명합니다.

System Administration Guide: Advanced Administration – Solaris OS의 고급 관리 작업(예: 인쇄 관리)에 대해 설명합니다.

System Administration Guide: IP Services – Solaris OS의 네트워크 구성 작업에 대해 설명합니다.

System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP) – Solaris OS의 이름 지정 서비스에 대해 설명합니다.

System Administration Guide: Security Services – Solaris OS의 보안 기능에 대해 설명합니다.

System Administration Guide: Solaris Containers-Resource Management and Solaris Zones – Solaris OS의 제약 기능에 대해 설명합니다.

외부 설명서

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

설명서, 지원 및 교육

Sun 웹 사이트에서는 다음 추가 자원에 대한 정보를 제공합니다.

- 설명서 (http://www.sun.com/documentation/)
- 지원 (http://www.sun.com/support/)
- 교육 (http://www.sun.com/training/)

Sun은 여러분의 의견을 환영합니다

Sun은 설명서의 내용 개선에 노력을 기울이고 있으며, 여러분의 의견과 제안을 환영합니다. 다음 사이트에 여러분의 의견을 제출하여 주십시오. 의견을 보내시려면 http://docs.sun.com에서 Feedback(피드백)을 누르십시오.

활자체 규약

다음 표는 이 책에서 사용되는 활자체 규약에 대해 설명합니다.

표 P–1 활자체 규약

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

명령 예의 쉘 프롬프트

다음 표에서는 C 쉘, Bourne 쉘 및 Korn 쉘에 대한 기본 UNIX® 시스템 프롬프트 및 수퍼유저 프롬프트를 보여 줍니다.

표 P–2 쉘 프롬프트

쉘	프롬프트
C 쉘	`machine_name%`
수퍼유저용 C 쉘	`machine_name#`
Bourne 쉘 및 Korn 쉘	`$`
수퍼유저용 Bourne 쉘 및 Korn 쉘	`#`

◆ ◆ ◆ 1 장

1 Trusted Extensions의 보안 계획

Solaris™ Trusted Extensions는 소프트웨어에서 사이트의 보안 정책 부분을 구현합니다. 이 장에서는 소프트웨어 구성의 보안 및 관리 측면에 대한 개요를 제공합니다.

Trusted Extensions의 보안 계획

이 절에서는 Trusted Extensions 소프트웨어를 설치 및 구성하기 전에 필요한 계획 수립에 대해 개략적으로 소개합니다.

Trusted Extensions 구성 작업에 대한 점검 목록은 부록 C, “Trusted Extensions 구성 검사 목록”을 참조하십시오. 사이트를 현지화하려면 20 페이지 “Trusted Extensions의 해외 고객”을 참조하십시오. 평가된 구성을 실행하려면 18 페이지 “사이트 보안 정책의 이해”를 참조하십시오.

Trusted Extensions의 이해

Trusted Extensions를 설치 및 구성하는 데에는 실행 파일 로드, 사이트 데이터 지정 및 구성 변수 설정 이상의 작업이 수반됩니다. 이러한 작업을 수행하려면 상당한 양의 배경 지식이 필요합니다. Trusted Extensions 소프트웨어는 다음과 같은 개념을 기반으로 하는 레이블이 있는 환경을 제공합니다.

- 대부분의 UNIX® 환경에서 수퍼유저에게 할당된 기능은 고유한 관리 역할에 사용할 수 있습니다.
- UNIX 사용 권한 이외에 특수 보안 태그를 통해서도 데이터 액세스가 제어됩니다. 이 태그를 **레이블**이라고 합니다. 레이블은 사용자, 프로세스 및 객체(예: 데이터 파일 및 디렉토리)에 할당됩니다.
- 보안 정책을 무효화하는 기능을 특정 사용자와 응용 프로그램에 할당할 수 있습니다.

사이트 보안 정책의 이해

Trusted Extensions를 사용하면 사이트의 보안 정책을 Solaris OS와 효율적으로 통합할 수 있습니다. 따라서 정책의 범위와 Trusted Extensions 소프트웨어에서 해당 정책을 수용하는 기능을 정확하게 이해해야 합니다. 체계적인 구성에서는 사이트 보안 정책과의 일관성 및 시스템에서 작업을 수행하는 사용자의 편의성이 균형있게 고려되어야 합니다.

Trusted Extensions는 기본적으로 다음과 같은 보호 프로필에 대해 Assurance Level EAL4에서 Common Criteria for Information Technology Security Evaluation(ISO/IEC 15408)을 준수하도록 구성되어 있습니다.

- 레이블이 있는 보안 보호 프로필
- 제어 액세스 보호 프로필
- 역할 기반 액세스 제어 보호 프로필

이 평가 수준을 충족하려면 LDAP를 이름 지정 서비스로 구성해야 합니다. 다음 중 하나를 수행하면 구성이 더 이상 평가와 일치하지 않을 수 있습니다.

- `/etc/system` 파일에서 커널 스위치 설정을 변경합니다.
- 감사 또는 장치 할당을 해제합니다.
- 다음 구성 가능 파일에서 기본 항목을 변경합니다.
  - `/usr/openwin/server/etc/*`
  - `/usr/dt/app-defaults/C/Dt`
  - `/usr/dt/app-defaults/C/Dtwm`
  - `/usr/dt/app-defaults/C/SelectionManager`
  - `/usr/dt/bin/Xsession`
  - `/usr/dt/bin/Xtsolsession`
  - `/usr/dt/bin/Xtsolusersession`

- /usr/dt/config/sel_config
- /usr/X11/lib/X11/xserver/TrustedExtensionsPolicy

자세한 내용은 Common Criteria 웹 사이트 (http://www.commoncriteriaportal.org/)를 참조하십시오.

Trusted Extensions에 대한 관리 전략 고안

root 사용자 또는 시스템 관리자 역할은 Solaris Trusted Extensions 설치 매체에서 패키지를 로드합니다. 역할을 만들어 여러 기능 영역 간에 관리 책임을 나눌 수 있습니다.

- 보안 관리자는 민감도 레이블 설정 및 할당, 감사 구성, 암호 정책 설정 등과 같은 보안 관련 작업을 담당합니다.
- 시스템 관리자는 설정, 유지 보수 및 일반 관리의 비보안 측면을 담당합니다.
- 주 관리자는 보안 및 시스템 관리자에게 충분한 권한이 없을 때 보안 관리자에 대한 권한 프로필 만들기 및 문제 해결을 담당합니다.
- 제한된 역할을 추가로 구성할 수 있습니다. 예를 들어, 운영자가 파일 백업을 담당할 수 있습니다.

관리 전략의 일부로 다음과 같은 의사 결정을 내려야 합니다.

- 관리 책임과 관리 책임을 처리하는 사용자
- 신뢰할 수 있는 응용 프로그램을 실행할 수 있는 관리자가 아닌 사용자, 즉 필요한 경우 보안 정책을 무효화하도록 허용된 사용자
- 데이터 그룹 및 데이터 그룹에 액세스할 수 있는 사용자

레이블 전략 고안

레이블을 계획하려면 시스템에서 민감도 수준 계층을 설정하고 정보를 범주화해야 합니다. 레이블 인코딩 파일에는 사이트에 대한 해당 유형의 정보가 포함되어 있습니다. Solaris Trusted Extensions 설치 매체에 제공된 label_encodings 파일 중 하나를 사용할 수 있습니다. 제공된 파일 중 하나를 수정하거나 사이트와 관련된 새 label_encodings 파일을 만들 수도 있습니다. 파일은 Sun 특정 로컬 확장명 중 적어도 COLOR NAMES 섹션을 반드시 포함해야 합니다.

주의 – label_encodings 파일을 제공하는 경우 최신 버전의 파일이 준비된 이후에 Solaris Trusted Extensions 패키지를 추가해야 합니다. 구성을 위해 시스템을 다시 부트하기 전에 파일이 추가됩니다. 파일은 이동식 매체에 있어야 합니다.

또한 레이블을 계획하려면 레이블 구성을 계획해야 합니다. 시스템에 Trusted Extensions 패키지를 추가한 후에는 시스템을 단일 레이블에서만 실행할 수 있는지, 아니면 여러

레이블에서 실행할 수 있는지를 결정해야 합니다. 관리자가 아닌 모든 사용자가 동일한 보안 레이블에서 작업할 수 있는 경우 단일 레이블 시스템을 선택합니다.

레이블이 표시되는지 여부 및 표시되는 레이블 이름 형식을 구성할 수도 있습니다. 자세한 내용은 **Solaris Trusted Extensions Label Administration**을 참조하십시오. 또한 **Compartmented Mode Workstation Labeling: Encodings Format**을 참조할 수도 있습니다.

Trusted Extensions의 해외 고객

해외 고객은 `label_encodings` 파일을 현지화할 경우 반드시 레이블 이름**만** 현지화해야 합니다. 관리 레이블 이름 `ADMIN_HIGH` 및 `ADMIN_LOW`는 현지화할 수 없습니다. 공급업체에서 연락하는 레이블이 있는 모든 호스트에는 `label_encodings` 파일에 있는 레이블 이름과 일치하는 레이블 이름이 있어야 합니다.

Trusted Extensions에서 지원하는 로켈 수는 Solaris OS보다 적습니다. Trusted Extensions가 지원하지 않는 로켈로 작업할 경우 레이블에 대한 오류 메시지와 같이 Trusted Extensions에 특정한 텍스트는 사용자의 로켈로 번역되지 않습니다. Solaris 소프트웨어는 사용자의 로켈로 계속 번역됩니다.

Trusted Extensions에 대한 시스템 하드웨어 및 용량 계획

시스템 하드웨어에는 시스템 자체와 시스템에 연결된 장치가 포함됩니다. 이러한 장치에는 테이프 드라이브, 마이크, CD-ROM 드라이브 및 디스크 팩이 포함됩니다. 하드웨어 용량에는 시스템 메모리, 네트워크 인터페이스 및 디스크 공간이 포함됩니다.

- **Solaris 10 11/06 설치 설명서: 기본 설치**의 "시스템 요구 사항 및 권장 사항"에 설명된 Solaris 릴리스 설치 권장 사항을 따르십시오. 이 요구 사항에 Trusted Extensions 기능을 추가할 수 있습니다.

  다음 시스템에는 제안된 최소값 이상의 메모리가 필요합니다.

  - 필수 관리 GUI인 Solaris Management Console을 실행하는 시스템
  - 두 개 이상의 민감도 레이블에서 실행되는 시스템
  - 관리 역할을 수락할 수 있는 사용자의 시스템

- 다음 시스템에는 추가 디스크 공간이 필요합니다.

  - 두 개 이상의 레이블에서 파일을 저장하는 시스템
  - 관리 역할을 수락할 수 있는 사용자의 시스템

신뢰할 수 있는 네트워크 계획

네트워크 하드웨어 계획에 대한 자세한 내용은 **System Administration Guide: IP Services**의 2 장, "Planning Your TCP/IP Network (Tasks)"를 참조하십시오.

클라이언트-서버 네트워크와 마찬가지로 기능별(서버 또는 클라이언트)로 호스트를 식별하고 소프트웨어를 적절하게 구성해야 합니다. 계획에 대한 자세한 내용은 **Solaris 10 11/06 설치 설명서: 사용자 정의 JumpStart 및 고급 설치**를 참조하십시오.

Trusted Extensions 소프트웨어에서는 두 개의 호스트 유형(레이블이 있는 호스트와 레이블이 없는 호스트)을 인식합니다. 표 1–1과 같이 각 호스트 유형에는 기본 보안 템플리트가 있습니다.

표 1–1 Trusted Extensions의 기본 호스트 템플리트

호스트 유형	템플리트 이름	목적
unlabeled	admin_low	초기 부트 시 전역 영역의 레이블을 지정합니다. 초기 부트 후 레이블이 지정되지 않은 패킷을 보내는 호스트를 식별합니다.
cipso	cipso	CIPSO 패킷을 보내는 호스트 또는 네트워크를 식별합니다. CIPSO 패킷에 레이블이 붙습니다.

네트워크를 다른 네트워크에 연결할 수 있는 경우 액세스 가능한 도메인과 호스트를 지정해야 합니다. 게이트웨이 역할을 담당할 Trusted Extensions 호스트를 식별해야 합니다. 이러한 게이트웨이에 대한 인정 범위 레이블과 다른 호스트의 데이터를 볼 수 있는 민감도 레이블을 식별해야 합니다.

각 호스트 유형에 대한 자세한 내용과 관련 예는 tnrhtp(4) 매뉴얼 페이지를 참조하십시오.

Trusted Extensions의 영역 계획

Trusted Extensions 소프트웨어가 전역 영역의 Solaris OS에 추가됩니다. 그런 다음 레이블이 있는 비전역 영역을 구성합니다. 레이블마다 하나씩 영역을 만들 필요가 없더라도 고유한 레이블마다 레이블이 있는 영역을 하나씩 만들 수 있습니다.

Trusted Extensions 영역 및 Solaris 10 영역

레이블이 있는 영역은 일반적인 Solaris 10 영역과 다릅니다. 레이블이 있는 영역은 주로 데이터를 분리하는 데 사용됩니다. Trusted Extensions에서 일반 사용자는 레이블이 있는 영역에 원격으로 로그인할 수 없습니다. 반드시 영역 콘솔을 사용하여 레이블이 있는 영역에 대화식 인터페이스를 통해 연결해야 합니다. 루트를 통해서만 영역 콘솔에 액세스할 수 있습니다.

Trusted Extensions의 영역 만들기

레이블이 있는 영역을 만들려면 전체 Solaris OS를 복사한 후 모든 영역에서 Solaris OS에 대한 서비스를 시작합니다. 이 프로세스에는 많은 시간이 소요될 수 있습니다. 하나의

영역을 만든 다음 해당 영역을 복사하거나 해당 영역의 내용을 복제하면 보다 빠르게 만들 수 있습니다. 다음 표에서는 Trusted Extensions에서 영역을 만들기 위해 필요한 옵션에 대해 설명합니다.

영역 생성 방법	필요 작업	이 방법의 특성
각 레이블이 있는 영역을 처음부터 만듭니다.	각 레이블이 있는 영역을 구성, 초기화, 설치, 사용자 정의 및 부트합니다.	■ 이 방법은 지원되며 하나 또는 두 개의 추가 영역을 만들 때 유용합니다. 영역을 업그레이드할 수 있습니다. ■ 이 방법은 많은 시간이 소요될 수 있습니다.
첫 번째 레이블이 있는 영역의 복사본에서 추가 레이블이 있는 영역을 만듭니다.	하나의 영역을 구성, 초기화, 설치 및 사용자 정의합니다. 이 영역을 레이블이 있는 추가 영역에 대한 템플리트로 사용합니다.	■ 이 방법은 지원되며 영역을 처음부터 새로 만드는 것보다 더 빠릅니다. 영역을 업그레이드할 수 있습니다. 영역 문제와 관련하여 Sun 지원의 도움을 받으려면 영역 복사 방법을 사용합니다. ■ 이 방법에서는 UFS를 사용합니다. UFS는 Solaris ZFS가 제공하는 영역에 대해 격리를 추가로 제공하지 않습니다.
레이블이 있는 첫 번째 영역의 ZFS 스냅샷으로부터 레이블이 있는 영역을 추가로 만듭니다.	Solaris 설치 중에 별도로 설정하는 분할 영역에서 ZFS 풀을 설정합니다. 하나의 영역을 구성, 초기화, 설치 및 사용자 정의합니다. 이 영역을 레이블이 있는 추가 영역에 대한 ZFS 스냅샷으로 사용합니다.	■ 이 방법은 Solaris ZFS를 사용하며 또한 제일 빠른 방법입니다. 이 방법은 모든 영역을 파일 시스템으로 만들기 때문에 UFS보다 더 많이 격리됩니다. ZFS에는 훨씬 적은 디스크 공간이 사용됩니다. ■ Trusted Extensions를 테스트하고 있고, 업그레이드하지 않아도 영역을 다시 설치할 수 있으면 이 방법을 선택하는 것이 좋습니다. 이 방법은 시스템을 사용 가능한 상태로 신속하게 다시 설치할 수 있기 때문에 휘발성 내용이 없는 시스템에 유용할 수 있습니다. ■ 이 방법은 지원되지 **않습니다**. 이 방법을 사용하여 만든 영역은 OS의 이후 버전이 릴리스될 때 **업그레이드할 수 없습니다**.

Solaris 영역은 패키지 설치와 패치에 영향을 줍니다. 자세한 내용은 다음을 참조하십시오.

- **Solaris 10 새로운 기능**의 3 장, "Solaris 10 8/07 릴리스의 새로운 기능"
- **Solaris 10 11/06 릴리스 노트**
- **System Administration Guide: Solaris Containers-Resource Management and Solaris Zones**의 24 장, "About Packages and Patches on a Solaris System With Zones Installed (Overview)"
- Solaris 영역 및 Solaris Container FAQ (`http://www.opensolaris.org/os/community/zones/faq`)

다중 레벨 액세스 계획

일반적으로 인쇄와 NFS는 다중 레벨 서비스로 구성됩니다. 다중 레벨 서비스에 액세스하려면 모든 영역에서 하나 이상의 네트워크 주소에 액세스할 수 있도록 시스템을 올바로 구성해야 합니다. 다중 레벨 서비스를 제공하는 구성은 다음과 같습니다.

- Solaris OS에서와 마찬가지로 전역 영역을 포함하여 모든 영역에 하나의 IP 주소가 할당됩니다. 각 영역에 별도의 네트워크 정보 카드(NIC)를 할당하면 이 구성이 구체화됩니다. 이러한 구성은 각 NIC에 연결되는 단일 레이블 네트워크를 물리적으로 구분하는 데 사용됩니다.
- 하나의 `all-zones` 주소가 할당됩니다. 하나 이상의 영역이 영역별 주소를 가질 수 있습니다.

다음 두 조건을 충족하는 시스템은 다중 레벨 서비스를 제공할 수 없습니다.

- 전역 영역과 레이블이 있는 영역이 공유하는 하나의 IP 주소가 할당됩니다.
- 영역별 주소가 할당되지 않습니다.

레이블이 있는 영역의 사용자에게 로컬 다중 레벨 프린터에 대한 액세스 권한이 없고 홈 디렉토리의 NFS 내보내기를 수행할 필요가 없는 경우 Trusted Extensions에서 구성하는 시스템에 하나의 IP 주소를 할당할 수 있습니다. 이러한 시스템에서는 다중 레벨 인쇄가 지원되지 않으며 홈 디렉토리를 공유할 수 없습니다. 이 구성은 일반적으로 노트북에서 사용됩니다.

Trusted Extensions의 LDAP 이름 지정 서비스 계획

레이블이 있는 시스템 네트워크를 설치하지 않으려면 이 절을 건너뛸 수 있습니다.

시스템 네트워크를 설치할 경우 LDAP가 Trusted Extensions에서 이름 지정 서비스로 사용됩니다. 시스템 네트워크를 구성할 경우 채워진 Sun Java™ System Directory

Server(LDAP 서버)가 필요합니다. 사이트에 기존 LDAP 서버가 있는 경우 서버를 Trusted Extensions 데이터베이스로 채울 수 있습니다. 서버에 액세스하려면 Trusted Extensions 시스템에서 LDAP 프록시를 설정합니다.

사이트에 기존 LDAP 서버가 없는 경우 Trusted Extensions 소프트웨어가 실행 중인 시스템에서 LDAP 서버를 만들도록 계획합니다. 이 절차는 5 장, “Trusted Extensions에 대해 LDAP 구성(작업)”을 참조하십시오.

Trusted Extensions의 감사 계획

기본적으로 Trusted Extensions를 설치하면 감사가 설정됩니다. 따라서 기본적으로 `root` 로그인과 `root` 로그아웃이 감사됩니다. 시스템을 구성 중인 사용자를 감사하려면 구성 프로세스의 초기에 역할을 만들 수 있습니다. 절차는 74 페이지 “Trusted Extensions의 역할 및 사용자 만들기”를 참조하십시오.

Trusted Extensions의 감사 계획은 Solaris OS와 동일합니다. 자세한 내용은 **System Administration Guide: Security Services**의 제 VII부, “Solaris Auditing”을 참조하십시오. Trusted Extensions에서 클래스, 이벤트 및 감사 토큰을 추가해도 감사를 관리하는 방법은 변경되지 않습니다. Trusted Extensions에서의 감사에 대한 추가 관련 정보는 **Solaris Trusted Extensions Administrator’s Procedures**의 18 장, “Trusted Extensions Auditing (Overview)”을 참조하십시오.

Trusted Extensions의 사용자 보안 계획

Trusted Extensions 소프트웨어는 사용자에 대한 적절한 보안 기본값을 제공합니다. 이러한 보안 기본값은 표 1–2를 참조하십시오. 나열된 두 값 중 첫 번째 값이 기본값입니다. 보안 관리자는 사이트의 보안 정책을 반영하여 이러한 값을 수정할 수 있습니다. 보안 관리자가 기본값을 설정한 후 시스템 관리자는 설정된 기본값을 상속하는 모든 사용자를 만들 수 있습니다. 이 기본값의 키워드 및 값에 대한 자세한 내용은 `label_encodings(4)`및`policy.conf(4)`매뉴얼 페이지를 참조하십시오.

표 1–2 사용자 계정에 대한 Trusted Extensions 보안 기본값

파일 이름	키워드	값
`/etc/security/policy.conf`	`IDLECMD`	`lock|logout`
	`IDLETIME`	`30`
	`LABELVIEW`	`showsl|hidesl`
	`CRYPT_ALGORITHMS_ALLOW`	`1,2a,md5`
	`CRYPT_DEFAULT`	`_unix_`

표 1–2 사용자 계정에 대한 Trusted Extensions 보안 기본값 (계속)

파일 이름	키워드	값
	LOCK_AFTER_RETRIES	no | yes
	PRIV_DEFAULT	basic
	PRIV_LIMIT	all
	AUTHS_GRANTED	solaris.device.cdrw
	PROFS_GRANTED	Basic Solaris User
/etc/security/tsol/label_encodings의 LOCAL DEFINITIONS 부분	Default User Clearance	CNF NEED TO KNOW
	Default User Sensitivity Label	PUBLIC

시스템 관리자는 모든 사용자에게 적합한 시스템 기본값을 설정하는 표준 사용자 템플리트를 설정할 수 있습니다. 예를 들어, 기본적으로 각 사용자의 초기 쉘은 Bourne 쉘입니다. 시스템 관리자는 각 사용자에게 C 쉘을 제공하는 템플리트를 설정할 수 있습니다. 자세한 내용은 사용자 계정에 대한 Solaris Management Console 온라인 도움말을 참조하십시오.

Trusted Extensions에 대한 설치 및 구성 전략 고안

Solaris OS에서와 마찬가지로 Trusted Extensions 소프트웨어는 root 사용자가 초기에 설치합니다. 그러나 root 사용자가 소프트웨어를 구성하도록 허용하는 것은 보안 전략이 아닙니다. 다음은 가장 안전한 전략에서 가장 안전하지 않은 전략까지의 설치 및 구성 전략에 대해 설명합니다.

- 두 명으로 구성된 설치 팀이 소프트웨어를 설치하고 구성합니다. 구성 프로세스는 감사됩니다.

  소프트웨어가 설치될 때 컴퓨터에는 두 명이 있습니다. 이 팀은 구성 프로세스의 초기에 로컬 사용자와 역할을 만듭니다. 또한 역할별로 실행되는 이벤트를 감사하도록 감사를 설정합니다. 사용자에게 역할이 할당되고 컴퓨터가 다시 부트되면 작업 부분이 역할별로 적용됩니다. 감사 증적에서는 구성 프로세스에 대한 레코드를 제공합니다. 보안 구성 프로세스에 대한 그림은 그림 1–1을 참조하십시오.

- 한 사람이 해당 역할을 수락하여 소프트웨어를 설치하고 구성합니다. 구성 프로세스는 감사됩니다.

  root 사용자는 구성 프로세스의 초기에 로컬 사용자와 역할을 만듭니다. 또한 역할별로 실행되는 이벤트를 감사하도록 감사를 설정합니다. 로컬 사용자에게 역할이 할당되고 컴퓨터가 다시 부트되면 작업 부분이 역할별로 적용됩니다. 감사 증적에서는 구성 프로세스에 대한 레코드를 제공합니다.

- 한 사람이 해당 역할을 수락하여 소프트웨어를 설치하고 구성합니다. 구성 프로세스는 감사되지 않습니다.

  이 전략을 사용하면 구성 프로세스에 대한 레코드가 보존되지 않습니다.

- root 사용자는 소프트웨어를 설치하고 구성합니다. 구성 프로세스는 감사됩니다.

  설치 팀은 구성 중에 root 사용자가 수행하는 모든 이벤트를 감사하도록 감사를 설정합니다. 팀에서는 이 전략을 사용하여 감사할 이벤트를 결정해야 합니다. root 역할을 하는 사용자의 이름은 감사 증적에 포함되지 않습니다.
- root 사용자는 소프트웨어를 설치하고 구성합니다.

다음 그림에는 역할별 작업의 배분이 표시됩니다. 보안 관리자는 다른 작업 간에 감사를 설정하고 파일 시스템을 보호하며, 장치 정책을 설정하고 실행 권한이 필요한 프로그램을 결정하고 사용자를 보호합니다. 시스템 관리자는 다른 작업 간에 파일 시스템을 공유 및 마운트하고 소프트웨어 패키지를 설치하며, 사용자를 만듭니다.

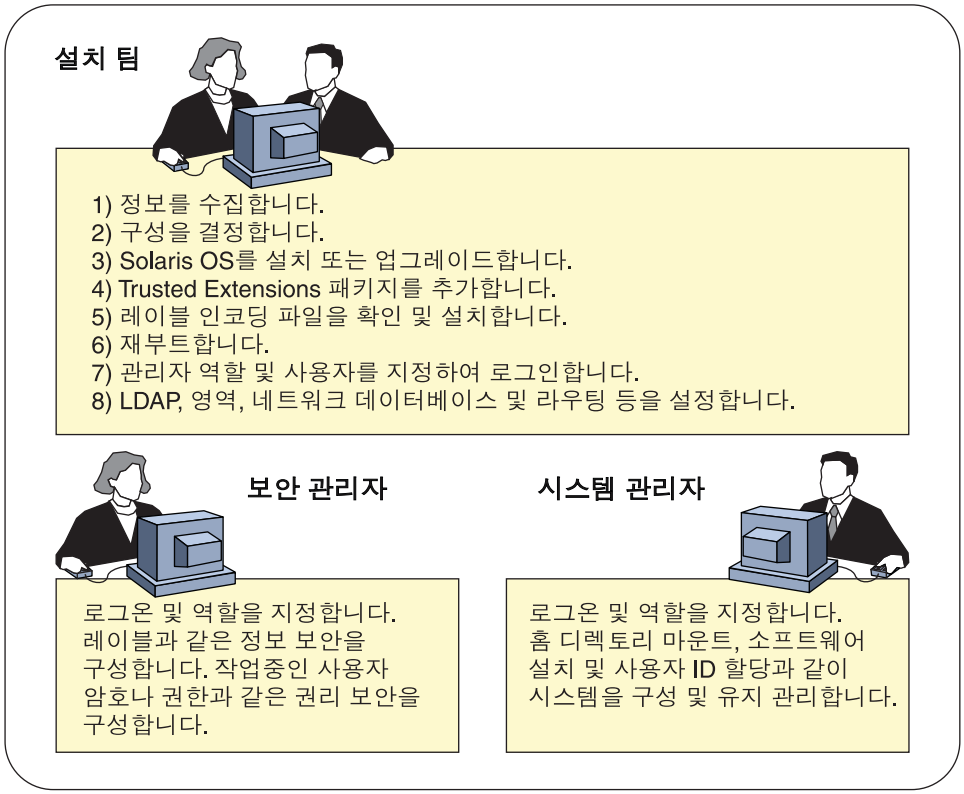


그림 1–1 Trusted Extensions 시스템 관리: 역할별 작업 부분

Trusted Extensions 설치 전 정보 수집

Solaris OS를 구성할 때처럼 Trusted Extensions를 구성하기 전에 시스템, 사용자, 네트워크 및 레이블 정보를 수집합니다. 자세한 내용은 39 페이지 “Trusted Extensions 설치 전 시스템 정보 수집”을 참조하십시오.

Trusted Extensions 설치 전 시스템 백업

시스템에 저장해야 할 파일이 있는 경우 Trusted Extensions 소프트웨어를 설치하기 전에 백업을 수행합니다. 파일을 백업하는 가장 안전한 방법은 레벨 0 덤프를 수행하는 것입니다. 해당 위치에 백업 절차가 없는 경우 현재 운영 체제의 관리자 설명서를 참조하십시오.

주 – Trusted Solaris 8 릴리스에서 마이그레이션할 경우 Trusted Extensions 레이블이 Trusted Solaris 8 레이블과 동일한 경우에만 데이터를 복원할 수 있습니다. Trusted Extensions는 다중 레벨 디렉토리를 만들지 않기 때문에 백업 매체의 각 파일과 디렉토리는 레이블이 백업의 파일 레이블과 동일한 영역에 복원됩니다. Trusted Extensions 릴리스를 설치하기 전에 백업을 **완료해야** 합니다.

Solaris Trusted Extensions 소프트웨어 설치

Trusted Extensions 소프트웨어 설치는 Solaris 시스템에 패키지를 설치하는 것을 의미합니다. 보안상의 이유로 Solaris 설치에 사용할 수 있는 옵션 중 일부는 선택하지 마십시오. 자세한 내용은 35 페이지 “Trusted Extensions용 Solaris OS 설치 또는 업그레이드”를 참조하십시오.

관리자의 관점에서 Trusted Extensions 설치 결과

Trusted Extensions 소프트웨어를 설치하면 다음과 같은 보안 기능이 제공됩니다. 대부분의 기능은 보안 관리자가 구성할 수 있습니다.

- 감사가 활성화됩니다.
- Sun label_encodings 파일이 설치 및 구성됩니다.
- 두 개의 신뢰할 수 있는 데스크탑이 추가됩니다. Solaris Trusted Extensions(CDE)는 CDE의 신뢰할 수 있는 버전입니다. Solaris Trusted Extensions(JDS)는 Sun Java 데스크탑 시스템의 신뢰할 수 있는 버전입니다. 각 윈도우화 환경은 전역 영역에 신뢰할 수 있는 경로 작업 공간을 만듭니다.
- Solaris OS에서와 같이 역할의 권한 프로필이 정의됩니다. Solaris OS에서와 같이 역할이 정의되지 않습니다.

  Trusted Extensions를 관리하는 역할을 사용하려면 해당 역할을 만들어야 합니다. 구성하는 동안 보안 관리자 역할을 만듭니다.

- 세 개의 Trusted Extensions 네트워크 주소 `tnrhdb`, `tnrhtp` 및 `tnzonecfg`가 설치됩니다. Solaris Management Console에서 보안 템플리트 도구 및 신뢰할 수 있는 네트워크 영역 도구를 사용하여 데이터베이스를 관리합니다.
- Trusted Extensions에서는 시스템 관리를 위한 GUI를 제공합니다. 일부 GUI는 Solaris OS GUI에 대한 확장입니다.
  - Trusted CDE에서 관리 작업은 Trusted_Extensions 폴더에 제공됩니다. 이 작업 중 일부는 Trusted Extensions를 처음 구성할 때 사용됩니다. 도구에 대한 자세한 내용은 **Solaris Trusted Extensions Administrator's Procedures**의 2 장, "Trusted Extensions Administration Tools"를 참조하십시오.
  - 관리자는 신뢰할 수 있는 편집기를 사용하여 로컬 관리 파일을 수정할 수 있습니다. Trusted CDE에서 Admin Editor(관리 편집기) 작업은 신뢰할 수 있는 편집기를 호출합니다.
  - Device Allocation Manager(장치 할당 관리자)에서는 연결된 장치를 관리합니다.
  - Solaris Management Console은 로컬 및 네트워크 관리 데이터베이스를 관리할 수 있는 Java 기반 도구를 제공합니다. 이러한 도구는 신뢰할 수 있는 네트워크, 영역 및 사용자를 관리하는 데 사용됩니다.

◆ ◆ ◆ 2 장

2 Trusted Extensions 설치 및 구성 로드맵

이 장에서는 Solaris™ Trusted Extensions 소프트웨어 설치 및 구성 작업을 개략적으로 소개합니다.

작업 맵: Trusted Extensions에 대한 Solaris 시스템 준비

Trusted Extensions를 설치하는 Solaris OS가 사용하려고 하는 Trusted Extensions의 기능을 지원하는지 확인합니다. 다음 작업 맵에 설명된 두 작업 중 하나를 완료합니다.

작업	수행 방법
Trusted Extensions를 위한 기존 또는 업그레이드된 Solaris 설치를 준비합니다.	37 페이지 “Trusted Extensions 에 대해 설치된 Solaris 시스템 준비”
Trusted Extensions 기능을 사용하여 Solaris OS를 설치합니다.	36 페이지 “Trusted Extensions 지원을 위한 Solaris 시스템 설치”

작업 맵: Trusted Extensions 준비 및 설치

Trusted Extensions 시스템을 구성하기 전에 먼저 안전하게 설치하려면 다음 작업 맵에 설명된 작업을 완료합니다.

작업	수행 방법
Solaris 시스템 준비를 완료합니다.	29 페이지 “작업 맵: Trusted Extensions에 대한 Solaris 시스템 준비”

작업	수행 방법
시스템을 백업합니다.	Trusted Solaris 8 시스템의 경우 릴리스 설명서에 명시된 대로 시스템을 백업합니다. 레이블이 있는 백업을 레이블이 동일하게 지정된 각 영역에 복원할 수 있습니다.
	Solaris 시스템의 경우 **System Administration Guide: Basic Administration**을 참조하십시오.
시스템 및 Trusted Extensions 네트워크에 대한 정보를 수집하고 결정을 내립니다.	39 페이지 “Trusted Extensions 설치 전 정보 수집 및 의사 결정”
Trusted Extensions 소프트웨어 패키지를 설치합니다.	42 페이지 “Solaris Trusted Extensions 패키지 설치”
시스템을 구성합니다.	모니터가 있는 시스템의 경우 30 페이지 “작업 맵: Trusted Extensions 구성”을 참조하십시오.
	헤드리스 시스템의 경우 111 페이지 “Trusted Extensions에서 헤드리스 시스템 구성(작업 맵)”을 참조하십시오.
	Sun Ray™의 경우 Sun 설명서 웹 사이트 (`http://docs.sun.com`)에서 **Sun Ray Server Software 4.0 Installation and Configuration Guide for the Solaris Operating System**을 참조하십시오.
	노트북의 경우 OpenSolaris Community: Security 웹 페이지 (`http://opensolaris.org/os/community/security`)를 참조하십시오. Trusted Extensions를 누릅니다. Trusted Extensions 페이지의 Laptop Configurations(노트북 구성)에서 `Laptop instructions`를 누릅니다.
	네트워크를 전역 영역과 통신하지 못하게 하려면 `vni0` 인터페이스를 구성합니다. 예를 들어 `Laptop instructions`를 참조하십시오.

작업 맵: Trusted Extensions 구성

보안 설치의 경우 구성 프로세스의 초기에 역할을 만듭니다. 역할이 시스템을 구성할 때의 작업 순서는 다음 작업 맵을 참조하십시오.

1. 전역 영역을 구성합니다.

작업	수행 방법
하드웨어 설정을 변경하려면 암호를 입력하도록 요구하여 시스템 하드웨어를 보호합니다.	**System Administration Guide: Security Services**의 "Controlling Access to System Hardware"
레이블을 구성합니다. 사용자 사이트에 대한 레이블을 **반드시** 구성해야 합니다. 기본 `label_encodings` 파일을 사용하려면 이 작업을 건너뛸 수 있습니다.	46 페이지 "레이블 인코딩 파일 확인 및 설치"
IPv6 네트워크를 실행하는 경우 `/etc/system` 파일을 수정하여 IP가 레이블이 있는 패킷을 인식하도록 합니다.	49 페이지 "Trusted Extensions에서 IPv6 네트워크 사용"
Solaris ZFS 스냅샷을 사용하여 영역을 복제하려면 ZFS 풀을 만듭니다. ZFS는 "Zettabyte File System"에서 파생된 머리글자입니다.	49 페이지 "영역 복제를 위한 ZFS 풀 만들기 "
부트하여 레이블이 있는 환경을 활성화합니다. 로그인하면 사용자가 전역 영역에 있습니다. 시스템의 `label_encodings` 파일이 필수 액세스 제어(MAC)를 강제 시행합니다.	50 페이지 "Trusted Extensions 다시 부트 및 로그인"
Solaris Management Console을 초기화합니다. 이 GUI는 다른 작업 간에 영역 레이블을 지정하는 데 사용됩니다.	52 페이지 "Trusted Extensions에서 Solaris Management Console 서버 초기화"
보안 관리자 역할과 로컬로 사용할 기타 역할을 만듭니다. 이러한 역할은 Solaris OS에서와 같은 방식으로 만듭니다. 이 작업을 마지막까지 지연시킬 수 있습니다. 이 결과에 대해서는 25 페이지 "Trusted Extensions에 대한 설치 및 구성 전략 고안"을 참조하십시오.	74 페이지 "Trusted Extensions의 역할 및 사용자 만들기" 79 페이지 "Trusted Extensions 역할 작동 확인"

로컬 파일을 사용하여 시스템을 관리하려면 다음 일련의 작업을 건너뜁니다.

2. 이름 지정 서비스를 구성합니다.

작업	수행 방법
파일을 사용하여 Trusted Extensions를 관리하려면 다음 작업을 건너뛸 수 있습니다.	파일 이름 지정 서비스에 대해서는 구성할 필요가 없습니다.
기존 Sun Java™ System Directory Server(LDAP 서버)가 있는 경우 서버에 Trusted Extensions 데이터베이스를 추가합니다. 그런 다음 첫 번째 Trusted Extensions 시스템을 LDAP 서버의 프록시로 만듭니다. LDAP 서버가 없는 경우에는 첫 번째 시스템을 서버로 구성합니다.	5 장, “Trusted Extensions에 대해 LDAP 구성(작업)”
Solaris Management Console에 대한 LDAP 도구 상자를 수동으로 설정합니다. 도구 상자를 사용하여 네트워크 객체에 대한 Trusted Extensions 속성을 수정할 수 있습니다.	106 페이지 “LDAP에 대해 Solaris Management Console 구성(작업 맵)”
LDAP 서버 또는 프록시 서버가 아닌 시스템의 경우 해당 시스템을 LDAP 클라이언트로 만듭니다.	55 페이지 “Trusted Extensions에서 전역 영역을 LDAP 클라이언트로 만들기”
LDAP 범위 내에서 보안 관리자 역할과 사용할 기타 역할을 만듭니다. 이 작업을 마지막까지 지연시킬 수 있습니다. 이 결과에 대해서는 25 페이지 “Trusted Extensions에 대한 설치 및 구성 전략 고안”을 참조하십시오.	74 페이지 “Trusted Extensions의 역할 및 사용자 만들기” 79 페이지 “Trusted Extensions 역할 작동 확인”

3. 레이블이 있는 영역을 만듭니다.

작업	수행 방법
`txzonemgr` 명령을 실행합니다. 메뉴에 따라 네트워크 인터페이스를 구성한 다음 첫 번째 레이블이 있는 영역을 만들고 사용자 정의합니다. 모든 영역이 성공적으로 사용자 정의되면 레이블이 있는 영역에 영역별 네트워크 주소를 추가할 수 있습니다.	57 페이지 “레이블이 있는 영역 만들기”
또는 Trusted CDE 작업을 사용합니다.	부록 B, “CDE 작업을 사용하여 Trusted Extensions에 영역 설치”

다음 일련의 작업 중 대부분은 **Solaris Trusted Extensions Administrator's Procedures**에서 설명합니다.

4. 시스템 설정을 완료합니다.

작업	수행 방법
레이블, 하나 이상의 다중 레벨 포트 또는 서로 다른 제어 메시지 정책이 필요한 추가 원격 호스트를 식별합니다.	**Solaris Trusted Extensions Administrator's Procedures**의 "Configuring Trusted Network Databases (Task Map)"
다중 레벨 홈 디렉토리 서버를 만든 다음 설치된 영역을 자동 마운트합니다.	81 페이지 "Trusted Extensions에서 홈 디렉토리 만들기"
사용자가 시스템에 로그인하도록 하려면 감사를 구성하고, 파일 시스템을 마운트한 후 기타 작업을 수행합니다.	**Solaris Trusted Extensions Administrator's Procedures**
NIS 환경의 사용자를 LDAP 서버에 추가합니다.	84 페이지 "LDAP 서버에 NIS 사용자 추가"
호스트와 호스트의 레이블이 있는 영역을 LDAP 서버에 추가합니다.	**Solaris Trusted Extensions Administrator's Procedures**의 "Configuring Trusted Network Databases (Task Map)"

◆ ◆ ◆ 3 장

3 Solaris Trusted Extensions 소프트웨어 설치(작업)

이 장에서는 Solaris Trusted Extensions용 Solaris OS 설치 준비 방법에 대해 설명합니다. 또한 이 장에서는 Trusted Extensions 패키지를 설치하기 전에 필요한 정보에 대해서도 설명합니다. 패키지 설치 방법에 대한 지침도 제공됩니다.

설치 팀 책임

Trusted Extensions 소프트웨어는 각자 고유한 책임을 지니는 두 사람이 설치 및 구성하도록 설계되었습니다. 그러나 설치 프로그램은 이 두 역할 작업 부분을 적용하지 않습니다. 대신 작업 부분을 역할별로 적용합니다. 역할과 사용자는 설치가 끝날 때까지 만들어지지 않으므로 2명 이상의 설치 팀이 Trusted Extensions 소프트웨어 설치에 참여하는 것이 좋습니다.

Trusted Extensions용 Solaris OS 설치 또는 업그레이드

Solaris 설치 옵션 선택은 Trusted Extensions의 사용과 보안에 영향을 줄 수 있습니다.

- Trusted Extensions를 올바로 설치하려면 기본 Solaris OS를 안전하게 설치해야 합니다. Trusted Extensions에 영향을 주는 Solaris 설치 옵션은 36 페이지 "Trusted Extensions 지원을 위한 Solaris 시스템 설치"를 참조하십시오.
- Solaris OS를 사용하는 경우 현재 구성이 Trusted Extensions의 요구 사항에 맞는지 확인하십시오. Trusted Extensions에 영향을 주는 구성 옵션은 37 페이지 "Trusted Extensions 에 대해 설치된 Solaris 시스템 준비"를 참조하십시오.

▼ Trusted Extensions 지원을 위한 Solaris 시스템 설치

이 작업은 Solaris OS를 처음 설치할 때 적용됩니다. 업그레이드하려면 37 페이지 "Trusted Extensions 에 대해 설치된 Solaris 시스템 준비"를 참조하십시오.

- **Solaris OS를 설치하려면 다음 설치 옵션에 대한 권장 작업을 수행하십시오.**

  선택 옵션은 Solaris 설치 질문의 순서를 따릅니다. 다음 표에 언급되지 않은 설치 질문은 Trusted Extensions에 영향을 주지 않습니다.

Solaris 옵션	Trusted Extensions 동작	권장되는 작업
NIS 이름 지정 서비스 NIS+ 이름 지정 서비스	Trusted Extensions에서는 파일 및 LDAP의 이름 지정 서비스를 지원합니다. 호스트 이름 확인을 위해 DNS를 사용할 수 있습니다.	NIS 또는 NIS+를 선택하지 마십시오. None(없음)을 선택할 수 있습니다. 이는 파일에서도 동등합니다. 나중에 Trusted Extensions에서 작동하도록 LDAP를 구성할 수 있습니다.
업그레이드	Trusted Extensions에서는 특정 보안 특성을 사용하여 레이블이 있는 영역을 설치합니다.	업그레이드하는 경우 37 페이지 "Trusted Extensions 에 대해 설치된 Solaris 시스템 준비"를 참조하십시오.
`root` 암호	Trusted Extensions의 관리 도구에는 암호가 필요합니다. `root` 사용자에게 암호가 없는 경우 `root`는 시스템을 구성할 수 없습니다.	`root` 암호를 제공합니다. 기본 `crypt_unix` 암호의 암호화 방법을 변경하지 마십시오. 자세한 내용은 **System Administration Guide: Security Services**의 "Managing Password Information"을 참조하십시오.
개발자 그룹	Trusted Extensions에서는 Solaris Management Console을 사용하여 네트워크를 관리합니다. 최종 사용자 그룹과 소규모 그룹은 Solaris Management Console용 패키지를 설치하지 않습니다.	다른 시스템에서 관리하는 데 사용할 시스템에서는 최종 사용자, 코어 또는 축소 네트워크 그룹을 설치하지 마십시오.
제품 선택	이 화면에서 Java ES 소프트웨어를 설치할 수 있습니다.	Solaris 10 Extra Value 소프트웨어를 선택하지 마십시오. 나중에 42 페이지 "Solaris Trusted Extensions 패키지 설치(작업)"에서 Trusted Extensions 소프트웨어를 추가합니다.

Solaris 옵션	Trusted Extensions 동작	권장되는 작업
사용자 정의 설치	Trusted Extensions는 영역을 설치하기 때문에 기본 설치에서 제공하는 것보다 더 많은 디스크 공간이 분할 영역에 필요할 수 있습니다.	Custom Install(사용자 정의 설치)을 선택하고 분할 영역을 생성합니다. 역할에 대한 스왑 공간을 추가하는 것을 고려합니다. 영역을 복제하려면 ZFS 풀에 대해 2000 MB의 분할 영역을 만듭니다. 감사 파일의 경우 전용 분할 영역을 만드는 것이 좋습니다.

▼ Trusted Extensions에 대해 설치된 Solaris 시스템 준비

이 작업은 현재 사용 중이고 Trusted Extensions 패키지를 추가할 Solaris 시스템에 적용됩니다. 업그레이드된 Solaris 10 시스템에 Trusted Extensions를 설치하려면 다음 절차를 수행합니다. 설치된 Solaris 시스템을 수정하는 기타 작업은 Trusted Extensions 패키지를 추가한 이후에 수행할 수 있습니다.

시작하기 전에 다음과 같은 일부 Solaris 환경에서는 Trusted Extensions를 설치할 수 없습니다.

- 시스템이 클러스터의 일부인 경우 Trusted Extensions를 설치할 수 없습니다.
- 대체 부트 환경(BE)에서는 Trusted Extensions를 설치할 수 없습니다. Trusted Extensions는 현재 부트 환경에서만 설치할 수 있습니다.

  `live_upgrade` 도구를 사용하여 대체 BE에 Solaris OS를 설치한 경우 먼저 대체 BE를 활성화하고 새 BE에서 시스템을 부트한 다음 Trusted Extensions 패키지를 추가해야 합니다. 라이브 업그레이드 및 BE에 대한 자세한 내용은 `live_upgrade(5)` 매뉴얼 페이지를 참조하십시오.

1 시스템에 비전역 영역이 설치되어 있으면 제거합니다.

또는 Solaris OS를 다시 설치할 수 있습니다. Solaris OS를 다시 설치하려면 36 페이지 "Trusted Extensions 지원을 위한 Solaris 시스템 설치"의 지침을 따릅니다.

2 시스템에 `root` 암호가 없으면 암호를 만듭니다.

Trusted Extensions의 관리 도구에는 암호가 필요합니다. `root` 사용자에게 암호가 없는 경우 `root`는 시스템을 구성할 수 없습니다.

`root` 사용자의 경우 기본 `crypt_unix` 암호의 암호화 방법을 사용합니다. 자세한 내용은 **System Administration Guide: Security Services**의 "Managing Password Information"을 참조하십시오.

주 – 다른 사용자가 별도의 확인이나 설명 없이 사용자의 데이터에 액세스할 수 있으므로 다른 사용자에게 암호를 공개해서는 안 됩니다. 사용자가 고의적으로 자신의 암호를 다른 사용자에게 누설하여 직접적으로 암호가 공개될 수도 있고, 암호를 메모해 두거나 보안되지 않은 암호를 선택함으로써 간접적으로 암호가 공개될 수도 있습니다. Solaris OS는 보안되지 않은 암호에 대해 보호 기능을 제공하지만, 사용자가 자신의 암호를 공개하거나 메모하지 못하도록 막을 수는 없습니다.

3 이 시스템에서 사이트를 관리하려면 Solaris Management Console용 Solaris 패키지를 추가합니다.

Trusted Extensions에서는 Solaris Management Console을 사용하여 네트워크를 관리합니다. 최종 사용자 그룹 또는 소규모 그룹에서 시스템을 설치한 경우 시스템에는 Solaris Management Console용 패키지가 없습니다.

4 `xorg.conf` 파일을 만든 경우 이 파일을 수정해야 합니다.

`/etc/X11/xorg.conf` 파일에서 Module(모듈) 절의 끝에 다음 행을 추가합니다.

```
load "xtsol"
```

주 – 기본적으로 `xorg.conf` 파일은 존재하지 않습니다. 이 파일이 없으면 아무 작업도 수행하지 않습니다.

5 Solaris Trusted Extensions 시스템을 업그레이드하는 경우 시스템 설치 전 먼저 아래의 내용을 읽으십시오.

- **Solaris 10 새로운 기능**의 3 장, “Solaris 10 8/07 릴리스의 새로운 기능”
- **Solaris 10 11/06 릴리스 노트**

참고 – 적절한 관련 정보를 찾으시려면, `Trusted Extensions`를 검색하십시오.

6 영역을 복제하려면 ZFS 풀에 대한 분할 영역을 만듭니다.

영역 만들기 방법을 결정하려면 21 페이지 “Trusted Extensions의 영역 계획”을 참조하십시오.

7 레이블이 있는 영역을 이 시스템에 설치하려면 영역을 위한 충분한 디스크 공간이 분할 영역에 있는지 확인합니다.

Trusted Extensions을 통해 구성되는 대부분의 시스템은 레이블이 있는 영역을 설치합니다. 레이블이 있는 영역에는 설치된 시스템에서 별도로 확보해 둔 공간보다 더 많은 디스크 공간이 필요할 수 있습니다.

그러나 Trusted Extensions 시스템에 따라 레이블이 있는 영역을 설치할 필요가 없는 경우도 있습니다. 예를 들어 다중 레벨 인쇄 서버, 다중 레벨 LDAP 서버 또는 다중 레벨 LDAP 프록시 서버는 레이블이 있는 영역을 설치할 필요가 없습니다. 이러한 시스템에는 추가 디스크 공간이 필요하지 않습니다.

8 **(옵션) 역할에 대한 여분의 스왑 공간을 추가합니다.**

역할은 Trusted Extensions를 관리합니다. 역할 프로세스에 대한 여분의 스왑 추가를 고려합니다.

9 **(옵션) 감사 파일 전용 분할 영역을 설정합니다.**

Trusted Extensions는 기본적으로 감사를 활성화합니다. 감사 파일의 경우 전용 분할 영역을 만드는 것이 가장 좋습니다.

10 **(옵션) 강화된 구성을 실행하려면 `netservices limited` 명령을 실행한 후에 Trusted Extensions를 설치합니다.**

```
# netservices limited
```

Trusted Extensions 설치 전 정보 수집 및 의사 결정

Solaris Trusted Extensions를 구성할 각 시스템에 대해 일부 정보를 확인하고 구성과 관련된 몇 가지 사항을 결정해야 합니다. 예를 들어, 레이블이 있는 영역을 만들려고 하기 때문에 영역을 ZFS(Zettabyte File System)로 복제할 수 있는 별도의 디스크 공간을 확보하려고 할 수 있습니다. Solaris ZFS는 영역을 추가로 격리합니다.

▼ Trusted Extensions 설치 전 시스템 정보 수집

1 **시스템의 기본 호스트 이름과 IP 주소를 결정합니다.**

이 호스트 이름은 네트워크 상의 호스트 이름으로, 전역 영역입니다. Solaris 시스템에서 `getent` 명령은 호스트 이름을 다음과 같이 반환합니다.

```
# getent hosts machine1
192.168.0.11   machine1
```

2 **레이블이 있는 영역에 대한 IP 주소 할당을 결정합니다.**

IP 주소가 두 개인 시스템은 다중 레벨 서버 역할을 수행할 수 있습니다. IP 주소가 하나인 시스템에서 인쇄하거나 다중 레벨 작업을 수행하려면 다중 레벨 서버에 액세스해야 합니다. IP 주소 옵션에 대한 자세한 내용은 23 페이지 “다중 레벨 액세스 계획”을 참조하십시오.

대부분의 시스템은 레이블이 있는 영역을 위한 두 번째 IP 주소가 필요합니다. 예를 들어, 레이블이 있는 영역을 위한 두 번째 IP 주소가 있는 호스트는 다음과 같습니다.

```
# getent hosts machine1-zones
192.168.0.12   machine1-zones
```

3 **LDAP 구성 정보를 수집합니다.**

Trusted Extensions 소프트웨어를 실행하는 LDAP 서버의 경우 다음과 같은 정보가 필요합니다.

- LDAP 서버가 실행되는 Trusted Extensions 도메인의 이름
- LDAP 서버의 IP 주소
- 로드할 LDAP 프로필 이름

LDAP 프록시 서버의 경우 LDAP 프록시 암호도 설정해야 합니다.

▼ Trusted Extensions 설치 전 시스템 및 보안 사항 결정

Solaris Trusted Extensions를 구성할 각 시스템의 경우 패키지를 설치하려면 먼저 다음과 같이 구성과 관련된 의사 결정을 내립니다.

1 **시스템 하드웨어를 안전하게 보호해야 하는 방법을 결정합니다.**

안전한 사이트에서는 설치된 모든 Solaris 시스템에 대해 다음 단계를 수행해야 합니다.

- SPARC 시스템의 경우 PROM 보안 수준 및 암호가 제공되었습니다.
- x86 시스템의 경우 BIOS가 보호됩니다.
- 모든 시스템에서 `root`가 암호로 보호됩니다.

2 `label_encodings` **파일을 준비합니다.**

사이트별 `label_encodings` 파일이 있는 경우 해당 파일을 확인하여 설치한 이후에 다른 구성 작업을 시작할 수 있습니다. 사이트에 `label_encodings` 파일이 없는 경우 Sun에서 제공하는 기본 파일을 사용할 수 있습니다. 또한 `/etc/security/tsol` 디렉토리에서 찾을 수 있는 기타 `label_encodings` 파일도 제공합니다. Sun 파일은 데모용 파일입니다. 해당 파일은 생산 시스템에 적합하지 않을 수도 있습니다.

파일을 사이트에 맞게 사용자 정의하려면 **Solaris Trusted Extensions Label Administration**을 참조하십시오.

3 `label_encodings` **파일의 레이블 목록에서 사용자가 만들어야 하는 레이블이 있는 영역 목록을 작성합니다.**

기본 `label_encodings` 파일의 경우 레이블은 다음과 같으며 영역 이름은 다음과 유사할 수 있습니다.

레이블	영역 이름
PUBLIC	public
CONFIDENTIAL : INTERNAL	internal
CONFIDENTIAL : NEED TO KNOW	needtoknow
CONFIDENTIAL : RESTRICTED	restricted

NFS를 쉽게 마운트하려면 특정 레이블의 영역 이름이 모든 시스템에서 동일해야 합니다. 다중 레벨 인쇄 서버와 같은 일부 시스템에는 레이블이 있는 영역을 설치할 필요가 없습니다. 그러나 인쇄 서버에 레이블이 있는 영역을 설치할 경우 영역 이름은 네트워크에 있는 다른 시스템의 영역 이름과 동일해야 합니다.

4 역할을 만들 시기를 결정합니다.

사이트 보안 정책에 따라 역할을 수락하여 Trusted Extensions를 관리해야 할 수 있습니다. 평가된 구성에 대한 기준에 맞게 시스템을 구성하려면 구성 프로세스의 초기에 역할을 만들어야 합니다.

역할을 사용하여 시스템을 구성할 필요가 없는 경우 수퍼유저로 시스템을 구성하도록 선택할 수 있습니다. 이 구성 방법은 보안성이 떨어집니다. 감사 레코드는 구성하는 동안 수퍼유저였던 사용자를 표시하지 않습니다. 수퍼유저는 시스템에서 모든 작업을 수행할 수 있지만 역할은 수행 가능한 작업이 제한됩니다. 따라서 역할별로 수행할 때 보다 세부적으로 구성할 수 있습니다.

5 영역 생성 방법을 선택합니다.

영역을 처음부터 만들거나, 복사 또는 복제할 수 있습니다. 이러한 방법은 작성 속도, 디스크 공간 요구 사항 및 견고성이 서로 다릅니다. 각 방법의 장단점에 대한 자세한 내용은 21 페이지 “Trusted Extensions의 영역 계획”을 참조하십시오.

6 LDAP 구성을 계획합니다.

네트워크로 연결되지 않은 시스템의 경우 로컬 파일을 사용하여 관리하는 것이 좋습니다.

LDAP는 네트워크로 연결된 환경에 대한 이름 지정 서비스입니다. 여러 시스템을 구성할 경우 이름이 입력된 LDAP 서버가 필요합니다.

- 기존 Sun Java™ System Directory Server(LDAP 서버)가 있는 경우 Trusted Extensions를 실행 중인 시스템에서 LDAP 프록시 서버를 만들 수 있습니다. 다중 레벨 프록시 서버는 레이블이 없는 LDAP 서버와의 통신을 처리합니다.
- LDAP 서버가 없는 경우 Trusted Extensions 소프트웨어를 실행하는 시스템을 다중 레벨 LDAP 서버로 구성할 수 있습니다.

7 각 시스템 및 네트워크에 대한 기타 보안 문제를 결정합니다.

예를 들어 다음 보안 문제를 고려할 수 있습니다.

- 시스템에 연결하여 사용할 수 있는 장치를 결정합니다.
- 시스템에서 액세스할 수 있는 프린터와 해당 레이블을 식별합니다.
- 게이트웨이 시스템 또는 공개 키오스크와 같이 제한된 레이블 범위를 가진 시스템을 식별합니다.
- 레이블이 없는 특정 시스템과 통신할 수 있는 레이블이 있는 시스템을 식별합니다.

Solaris Trusted Extensions 패키지 설치(작업)

패키지를 설치하기 전에 35 페이지 “Trusted Extensions용 Solaris OS 설치 또는 업그레이드” 및 39 페이지 “Trusted Extensions 설치 전 정보 수집 및 의사 결정”의 작업을 완료해야 합니다.

▼ Solaris Trusted Extensions 패키지 설치

Java 마법사나 pkgadd 명령을 사용하여 패키지를 추가할 수 있습니다. pkgadd 명령 옵션을 보려면 pkgadd(1M) 매뉴얼 페이지를 참조하십시오.

1 Solaris 설치 매체를 드라이브에 넣습니다.

2 Trusted_Extensions 디렉토리로 이동합니다.

```
# cd Solaris_release-number/ExtraValue/CoBundled/Trusted_Extensions
```

3 모든 패키지를 로드합니다.

다음 옵션 중 하나를 선택합니다.

- **Java 마법사를 사용합니다.**

  ```
  # java wizard
  ```

  Java 설치 GUI에서 패키지를 설치하라는 메시지를 표시합니다.

- **Packages 디렉토리에서 pkgadd 명령을 사용합니다.**

  ```
  # cd Packages
  # pkgadd -d .
  ```

  a. **Enter 키를 눌러 모든 패키지를 로드합니다.**

  b. **모든 프롬프트에 y로 대답합니다.**

4 **적절한 패키지가 설치되었는지 확인합니다.**

- **Java 마법사에서 Details(세부 정보) 버튼을 누릅니다.**
- **명령줄에서 로그 전체를 스크롤합니다.**
  `/var/sadm/install/logs` 디렉토리로 이동하여 로그를 참조할 수도 있습니다.

참고 – 또한 `pkginfo` 명령을 사용하여 패키지가 설치되었는지 확인할 수 있습니다.

```
# pkginfo | grep Trust
system      SUNWdttshelp            Trusted Extensions, CDE Desktop Help
system      SUNWdttsr               Trusted Extensions, CDE Desktop, (Root)
system      SUNWdttsu               Trusted Extensions, CDE Desktop, (Usr)
system      SUNWmgts                Trusted Extensions, SMC
system      SUNWtsg                 Trusted Extensions global
system      SUNWtsman               Trusted Extensions Man Pages
application SUNWtsmc                Trusted Extensions SMC Server
system      SUNWtsr                 Trusted Extensions, (Root)
system      SUNWtsu                 Trusted Extensions, (Usr)
system      SUNWxwts                Trusted Extensions, X Window System
```

일반 오류 **Java 마법사 –** `Exception in thread "main" java.lang.NoClassDefFoundError: wizard` 메시지가 나타나면 잘못된 디렉토리에서 마법사를 호출한 것입니다.

다음 순서 Solaris Trusted Extensions 시스템을 업그레이드하는 경우 시스템 설치 전 먼저 아래의 내용을 읽으십시오.

Solaris 10 11/06 릴리스 노트

- **Solaris 10 새로운 기능**의 3 장, “Solaris 10 8/07 릴리스의 새로운 기능”
- **Solaris 10 11/06 릴리스 노트**

◆ ◆ ◆ 4 장

4 Trusted Extensions 구성(작업)

이 장에서는 모니터가 있는 시스템에서 Solaris™ Trusted Extensions를 구성하는 방법에 대해 설명합니다. Trusted Extensions 소프트웨어가 제대로 작동하려면 레이블, 영역, 네트워크, 역할 및 도구를 구성해야 합니다.

기타 구성 작업은 **Solaris Trusted Extensions Administrator's Procedures**를 참조하십시오.

Trusted Extensions의 전역 영역 설정

전역 영역을 설정하려면 먼저 구성에 대해 결정해야 합니다. 결정에 대한 자세한 내용은 39 페이지 “Trusted Extensions 설치 전 정보 수집 및 의사 결정”을 참조하십시오.

작업	설명	수행 방법
하드웨어를 보호합니다.	하드웨어 설정을 변경하려면 암호를 요구하여 하드웨어를 보호할 수 있습니다.	**System Administration Guide: Security Services**의 “Controlling Access to System Hardware”
레이블을 구성합니다.	사용자 사이트에 대한 레이블을 **반드시** 구성해야 합니다. 기본 `label_encodings` 파일을 사용하려면 이 단계를 건너뛸 수 있습니다.	46 페이지 “레이블 인코딩 파일 확인 및 설치”

작업	설명	수행 방법
IPv6의 경우 `/etc/system` 파일을 수정합니다.	IPv6 네트워크를 실행하는 경우 `/etc/system` 파일을 수정하여 IP가 레이블이 있는 패킷을 인식하도록 합니다.	49 페이지 “Trusted Extensions에서 IPv6 네트워크 사용”
Solaris ZFS 스냅샷을 위한 공간을 만듭니다.	Solaris ZFS 스냅샷을 사용하여 영역을 복제하려면 ZFS 풀을 만듭니다. ZFS는 "Zettabyte File System"에서 파생된 머리글자입니다. 첫 번째 영역을 복제하여 레이블이 있는 나머지 영역을 만들려면 이 작업을 수행합니다.	49 페이지 “영역 복제를 위한 ZFS 풀 만들기 ”
다시 부트하고 로그인합니다.	전역 영역으로 로그인됩니다. 전역 영역은 MAC(Mandatory Access Control)를 인식하고 실행하는 환경입니다.	50 페이지 “Trusted Extensions 다시 부트 및 로그인”
Solaris Management Console을 초기화합니다.	Trusted Extensions는 사용자, 역할, 영역 및 네트워크 관리를 위한 도구를 Solaris Management Console에 추가합니다.	52 페이지 “Trusted Extensions에서 Solaris Management Console 서버 초기화”
LDAP를 구성합니다.	LDAP 이름 지정 서비스를 사용하려면 LDAP 서비스를 설정합니다.	5 장, “Trusted Extensions에 대해 LDAP 구성(작업) ”
	LDAP 서비스를 설정한 경우 이 시스템을 LDAP 클라이언트로 지정합니다.	55 페이지 “Trusted Extensions에서 전역 영역을 LDAP 클라이언트로 만들기”

▼ 레이블 인코딩 파일 확인 및 설치

인코딩 파일은 통신하는 Trusted Extensions 호스트와 호환되어야 합니다.

주 – Trusted Extensions는 기본 `label_encodings` 파일을 설치합니다. 이 기본 파일은 데모용으로 유용합니다. 그러나 이 파일을 사용하지 않는 것이 좋습니다. 기본 파일을 사용하려면 이 절차를 건너뜁니다.

- 인코딩 파일에 대해 잘 알고 있는 경우 다음 절차를 사용할 수 있습니다.
- 인코딩 파일에 익숙하지 않은 경우 **Solaris Trusted Extensions Label Administration**에서 요구 사항, 절차 및 예를 참조하십시오.

주의 – 계속하려면 레이블을 **반드시** 설치해야 합니다. 그렇지 않으면 구성에 실패합니다.

시작하기 전에 사용자가 보안 관리자로 Trusted Extensions 패키지를 추가했으므로 이미 로그인된 것입니다.

보안 관리자는 label_encodings 파일의 편집, 확인 및 유지 관리를 담당합니다. label_encodings 파일을 편집하려면 파일 자체가 쓰기 가능한지 확인합니다. 자세한 내용은 label_encodings(4) 매뉴얼 페이지를 참조하십시오.

1 **label_encodings 파일이 들어 있는 매체를 해당 장치에 넣습니다.**

2 **label_encodings 파일을 디스크로 복사합니다.**

3 **새 레이블 인코딩 파일의 구문을 확인합니다.**

   a. **Trusted_Extensions 폴더를 엽니다.**
   배경에서 마우스 버튼 3을 누릅니다.

   b. **Workspace(작업 공간) 메뉴에서 Applications(응용 프로그램) → Application Manager(응용 프로그램 관리자)를 선택합니다.**

   c. **Trusted_Extensions 폴더 아이콘을 두 번 누릅니다.**

4 **Check Encodings(인코딩 확인) 작업을 두 번 누릅니다.**
대화 상자에 파일의 전체 경로 이름을 입력합니다.

/full-pathname-of-label-encodings-file

chk_encodings 명령을 호출하여 파일의 구문을 확인합니다. 결과가 Check Encodings(인코딩 확인) 대화 상자에 표시됩니다.

5 **Check Encodings(인코딩 확인) 대화 상자의 내용을 읽습니다.**

6 **다음 중 한 가지를 수행합니다.**

계속	인코딩 확인 작업에서 오류를 보고하지 않는 경우 계속할 수 있습니다. 단계 7로 이동합니다.
오류 해결	인코딩 확인 작업에서 오류를 보고하는 경우 계속하려면 먼저 오류를 **해결해야** 합니다. 자세한 내용은 **Solaris Trusted Extensions Label Administration**의 3 장, “Making a Label Encodings File (Tasks)”을 참조하십시오.

7 **파일이 구문 검사를 통과하면 Yes(예)를 누릅니다.**
인코딩 확인 작업에서는 원본 파일의 백업 복사본을 만든 다음 확인된 버전을 /etc/security/tsol/label_encodings에 설치합니다. 그런 다음 레이블 데몬을 다시 시작합니다.

주의 – 계속하려면 레이블 인코딩 파일이 인코딩 확인 테스트를 **반드시** 통과해야 합니다.

예 4–1 명령줄에서 label_encodings 구문 검사

이 예에서는 관리자가 명령줄을 사용하여 여러 label_encodings 파일을 테스트합니다.

```
# /usr/sbin/chk_encodings /var/encodings/label_encodings1
No errors found in /var/encodings/label_encodings1
# /usr/sbin/chk_encodings /var/encodings/label_encodings2
No errors found in /var/encodings/label_encodings2
```

관리 과정에서 label_encodings2 파일을 사용하도록 결정하면 관리자는 파일의 구문 분석을 실행합니다.

```
# /usr/sbin/chk_encodings -a /var/encodings/label_encodings2
No errors found in /var/encodings/label_encodings2

---> VERSION = MYCOMPANY LABEL ENCODINGS  2.0 10/10/2006

---> CLASSIFICATIONS <---

   Classification 1: PUBLIC
   Initial Compartment bits: 10
   Initial Markings bits: NONE

---> COMPARTENTS AND MARKINGS USAGE ANALYSIS <---
...
---> SENSITIVITY LABEL to COLOR MAPPING <---
...
```

관리자는 기록을 위해 구문 분석 복사본을 인쇄한 후 해당 파일을 /etc/security/tsol 디렉토리로 이동합니다.

```
# cp /var/encodings/label_encodings2 /etc/security/tsol/label.encodings.10.10.06

# cd /etc/security/tsol
# cp label_encodings label_encodings.tx.orig
# cp label.encodings.10.10.06 label_encodings
```

마지막으로 관리자는 label_encodings 파일이 회사 파일인지 확인합니다.

```
# /usr/sbin/chk_encodings -a /etc/security/tsol/label_encodings | head -4
No errors found in /etc/security/tsol/label_encodings
```

```
---> VERSION = MYCOMPANY LABEL ENCODINGS  2.0 10/10/2006
```

▼ Trusted Extensions에서 IPv6 네트워크 사용

IPv6을 사용하지 않는 경우 Trusted Extensions에서 CIPSO 옵션을 사용하여 IPv6 패킷을 전달할 수 없습니다. Trusted Extensions에서 IPv6 네트워크를 사용하려면 `/etc/system` 파일에 항목을 추가해야 합니다.

- **`/etc/system` 파일에 다음 항목을 추가합니다.**

  ```
  set ip:ip6opt_ls = 0x0a
  ```

일반 오류

- 부트 중에 오류 메시지가 표시되면 IPv6 구성이 잘못된 것입니다.
  - 항목의 철자가 올바른지 확인합니다.
  - `/etc/system` 파일에 올바른 항목을 추가한 후에 시스템을 다시 부트했는지 확인합니다.
- 현재 IPv6을 사용하는 Solaris 시스템에 Trusted Extensions를 설치할 때 IP 항목을 `/etc/system`에 추가하지 않으면 다음과 같은 오류 메시지가 표시됩니다. `t_optmgmt: System error: Cannot assign requested address` *time-stamp*
- IPv6을 사용하지 않는 Solaris 시스템에 Trusted Extensions를 설치할 때 IP 항목을 `/etc/system`에 추가하지 않으면 다음과 같은 오류 메시지가 표시됩니다.
  - `WARNING: IPv6 not enabled via /etc/system`
  - `Failed to configure IPv6 interface(s): hme0`
  - `rpcbind: Unable to join IPv6 multicast group for rpc broadcast` *broadcast-number*

▼ 영역 복제를 위한 ZFS 풀 만들기

Solaris ZFS 스냅샷을 영역 템플리트로 사용하려면 ZFS 파일 또는 ZFS 장치에서 ZFS 풀을 만들어야 합니다. 이 풀에는 각 영역의 복제를 위한 스냅샷이 보관됩니다. ZFS 풀에 대해 `/zone` 장치를 사용합니다.

시작하기 전에 Solaris 설치 중에 ZFS 파일 시스템을 위한 별도의 디스크 공간을 확보해 두었습니다. 자세한 내용은 21 페이지 “Trusted Extensions의 영역 계획”을 참조하십시오.

1 **/zone 분할 영역을 마운트 해제합니다.**

설치하는 동안 충분한 디스크 공간(약 2000MB)이 있는 /zone 분할 영역을 만들었습니다.

```
# umount /zone
```

2 **/zone 마운트 지점을 제거합니다.**

```
# rmdir /zone
```

3 **vfstab 파일에서 /zone 항목을 주석 처리합니다.**

a. **/zone 항목을 읽지 못하도록 합니다.**

편집기에서 vfstab 파일을 엽니다. /zone 항목 앞에 주석 기호를 추가합니다.

```
#/dev/dsk/cntndnsn  /dev/dsk/cntndnsn  /zone  ufs  2  yes  -
```

b. **디스크 슬라이스, c*n* t*n*d*n* s*n*을 클립보드에 복사합니다.**

c. **파일을 저장하고 편집기를 닫습니다.**

4 **디스크 슬라이스를 사용하여 /zone을 ZFS 풀로 다시 만듭니다.**

```
# zpool create -f zone cntndnsn
```

예를 들어, /zone 항목에서 c0t0d0s5 디스크 슬라이스를 사용한 경우 명령은 다음과 같습니다.

```
# zpool create -f zone c0t0d0s5
```

5 **ZFS 풀이 정상인지 확인합니다.**

다음 명령 중 하나를 사용합니다.

```
# zpool status -x zone
pool 'zone' is healthy

# zpool list
NAME     SIZE     USED   AVAIL   CAP   HEALTH   ALTROOT
/zone    5.84G   80K    5.84G    7%   ONLINE   -
```

이 예에서는 설치 팀이 영역에 대해 6000MB의 분할 영역을 예약했습니다. 자세한 내용은 zpool(1M) 매뉴얼 페이지를 참조하십시오.

▼ Trusted Extensions 다시 부트 및 로그인

대부분의 사이트에는 시스템을 구성할 때 설치 팀 역할을 하는 두 명 이상의 관리자가 있습니다.

시작하기 전에 로그인하기 전에 먼저 Trusted Extensions의 데스크탑 및 레이블 옵션을 숙지하십시오. 자세한 내용은 **Solaris Trusted Extensions 사용 설명서**의 2 장, “Trusted Extensions에 로그인(작업)”를 참조하십시오.

1 시스템을 다시 부트합니다.

```
# /usr/sbin/reboot
```

시스템에 그래픽 디스플레이가 없는 경우 6 장, “Trusted Extensions로 헤드리스 시스템 구성(작업)”으로 이동합니다.

2 Solaris Trusted Extensions(CDE) 데스크탑에 수퍼유저로 로그인합니다.

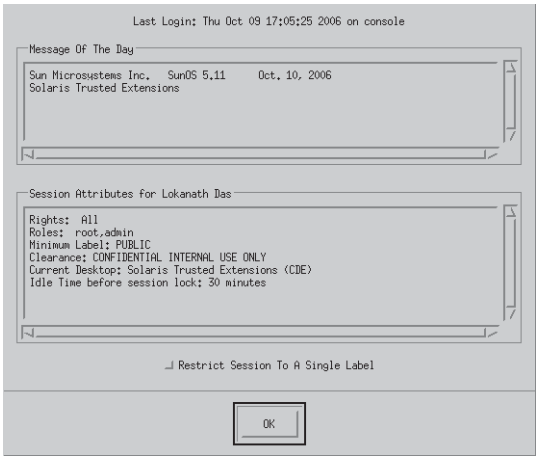
a. 로그인 창에서 Solaris Trusted Extensions(CDE)을 데스크탑으로 선택합니다.

이 Trusted CDE 데스크탑에는 시스템을 구성하는 데 유용한 작업이 포함되어 있습니다.

b. 로그인 대화 상자에서 root와 루트 암호를 입력합니다.

다른 사용자가 별도의 확인이나 설명 없이 사용자의 데이터에 액세스할 수 있으므로 다른 사용자에게 암호를 공개해서는 안 됩니다. 사용자가 고의적으로 자신의 암호를 다른 사용자에게 누설하여 직접적으로 암호가 공개될 수도 있고, 암호를 메모해 두거나 보안되지 않은 암호를 선택함으로써 간접적으로 암호가 공개될 수도 있습니다. Trusted Extensions 소프트웨어는 보안되지 않은 암호에 대해 보호 기능을 제공하지만, 사용자가 자신의 암호를 공개하거나 메모하지 못하도록 막을 수는 없습니다.

3 Last Login(마지막 로그인) 대화 상자의 정보를 읽어 보십시오.



그런 다음 OK(확인)를 눌러 상자를 없앱니다.

4 **Label Builder(레이블 구축기)를 읽습니다.**

OK(확인)를 눌러 기본 레이블을 적용합니다.

로그인 프로세스가 완료되면 Trusted Extensions 화면이 잠시 나타난 다음 네 개의 작업 공간이 있는 데스크탑 세션이 시작됩니다. `Trusted Path` 기호가 신뢰할 수 있는 스트라이프에 표시됩니다.

주 – 자리를 비우기 전에 반드시 로그오프하거나 화면을 잠가야 합니다. 그렇지 않으면 다른 사용자가 별도의 확인이나 설명 없이 식별 및 인증 과정을 거치지 않고 시스템에 액세스할 수 있습니다.

▼ Trusted Extensions에서 Solaris Management Console 서버 초기화

다음 절차에 따라 이 시스템에서 사용자, 역할, 호스트, 영역 및 네트워크를 관리할 수 있습니다. 구성하는 첫 번째 시스템에서는 `files` 범위만 사용할 수 있습니다.

시작하기 전에 사용자는 수퍼유저여야 합니다.

1 **Solaris Management Console을 시작합니다.**

```
# /usr/sbin/smc &
```

주 – 처음에 Solaris Management Console을 시작하면 몇 가지 등록 작업을 수행합니다. 이 작업에는 몇 분 정도의 시간이 소요될 수 있습니다.

---

2 **Solaris Management Console에 도구 상자 아이콘이 표시되지 않으면 다음 중 하나를 수행합니다.**

- **Navigation(탐색) 창이 표시되지 않는 경우**

  a. **표시되는 Open Toolbox(도구 상자 열기) 대화 상자의 Server(서버) 아래에서 이 시스템 이름 옆에 있는 Load(로드)를 누릅니다.**

  이 시스템에 권장된 양의 메모리 및 스왑이 없는 경우 도구 상자를 표시하는 데 몇 분 정도 걸릴 수 있습니다. 권장 사항은 35 페이지 “Trusted Extensions용 Solaris OS 설치 또는 업그레이드”를 참조하십시오.

b. 도구 상자 목록에서 `Policy=TSOL`인 도구 상자를 선택합니다.

그림 4–1은 이 컴퓨터(*this-host*: `Scope=Files, Policy=TSOL`) 도구 상자를 보여줍니다. Trusted Extensions은 System Configuration(시스템 구성) 노드에서 도구를 수정합니다.

주의 – 정책이 없는 도구 상자를 선택하면 안 됩니다. 나열된 정책이 없는 도구 상자는 Trusted Extensions를 지원하지 않습니다.

제어하려는 범위에 따라 선택하는 도구 상자가 달라집니다.

- 로컬 파일을 편집하려면 Files(파일) 범위를 선택합니다.
- LDAP 데이터베이스를 편집하려면 LDAP 범위를 선택합니다.

  108 페이지 “Solaris Management Console에서 LDAP 도구 상자 편집”을 완료한 후에 LDAP 범위를 사용할 수 있습니다.

c. Open(열기)을 누릅니다.

- **Navigation(탐색) 창이 표시되지만 도구 상자 아이콘이 중지 기호인 경우**

  a. Solaris Management Console을 종료합니다.

  b. Solaris Management Console을 다시 시작합니다.

  ```
  # /usr/sbin/smc &
  ```

3 아직 선택하지 않은 경우 `Policy=TSOL`인 도구 상자를 선택합니다.

다음 그림은 이 컴퓨터(*this-host*: `Scope=Files, Policy=TSOL`) 도구 상자를 보여줍니다. Trusted Extensions은 System Configuration(시스템 구성) 노드에서 도구를 수정합니다.

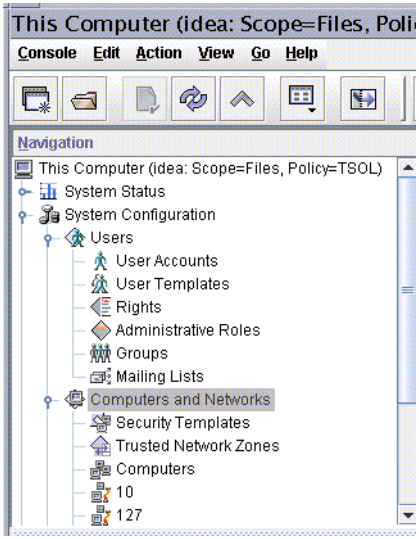


그림 4–1 Solaris Management Console의 Trusted Extensions 도구

4 **(옵션) 현재 도구 상자를 저장합니다.**

`Policy=TSOL` 도구 상자를 저장하면 기본적으로 Trusted Extensions 도구 상자를 로드할 수 있습니다. Preferences(기본 설정)는 역할별, 호스트별로 저장됩니다. 호스트는 Solaris Management Console 서버입니다.

a. **Console(콘솔) 메뉴에서 Preferences(기본 설정)를 선택합니다.**

Home(홈) 도구 상자가 선택됩니다.

b. **`Policy=TSOL` 도구 상자를 Home(홈) 도구 상자로 정의합니다.**

Use Current Toolbox(현재 도구 상자 사용) 버튼을 눌러 현재 도구 상자를 Location(위치) 필드에 넣습니다.

c. **OK(확인)를 눌러 기본 설정을 저장합니다.**

5 **Solaris Management Console을 종료합니다.**

참조 Solaris Management Console에 Trusted Extensions 추가에 대한 개요는 **Solaris Trusted Extensions Administrator's Procedures**의 "Solaris Management Console Tools"를 참조하십시오. Solaris Management Console을 사용하여 보안 템플리트를 만들려면 **Solaris Trusted Extensions Administrator's Procedures**의 "Configuring Trusted Network Databases (Task Map)"를 참조하십시오.

▼ Trusted Extensions에서 전역 영역을 LDAP 클라이언트로 만들기

LDAP의 경우 이 절차에서는 전역 영역에 대한 이름 지정 서비스 구성을 설정합니다. LDAP를 사용하지 않는 경우 이 절차를 건너뛸 수 있습니다.

시작하기 전에 Sun Java™ System Directory Server 즉, LDAP 서버가 있어야 합니다. 서버를 Trusted Extensions 데이터베이스로 채우고 이 시스템에서 서버에 연결할 수 있어야 합니다. 따라서 구성 중인 시스템에는 LDAP 서버의 `tnrhdb` 데이터베이스에 항목이 있어야 합니다. 또는 이 절차를 수행하기 전에 이 시스템을 와일드카드 항목에 포함시켜야 합니다.

Trusted Extensions로 구성되는 LDAP 서버가 없는 경우 이 절차를 수행하기 전에 5 장, “Trusted Extensions에 대해 LDAP 구성(작업)”의 절차를 완료해야 합니다.

1 원본 `nsswitch.ldap` 파일의 복사본을 저장합니다.

LDAP의 표준 이름 지정 서비스 전환 파일이 Trusted Extensions에 너무 제한적입니다.

```
# cd /etc
# cp nsswitch.ldap nsswitch.ldap.orig
```

2 DNS를 사용할 경우 다음 서비스에 대해 `nsswitch.ldap` 파일 항목을 변경합니다.

올바른 항목은 다음과 비슷합니다.

```
hosts:    files dns ldap

ipnodes:    files dns ldap

networks:   ldap files
protocols:  ldap files
rpc:        ldap files
ethers:     ldap files
netmasks:   ldap files
bootparams: ldap files
publickey:  ldap files

services:   files
```

Trusted Extensions는 다음 두 개의 항목을 추가합니다.

```
tnrhtp:    files ldap
tnrhdb:    files ldap
```

3 수정된 `nsswitch.ldap` 파일을 `nsswitch.conf`에 복사합니다.

```
# cp nsswitch.ldap nsswitch.conf
```

4 **Trusted CDE 작업 공간에서 Trusted_Extensions 폴더로 이동합니다.**

   a. **배경에서 마우스 버튼 3을 누릅니다.**

   b. **Workspace(작업 공간) 메뉴에서 Applications(응용 프로그램) → Application Manager(응용 프로그램 관리자)를 선택합니다.**

   c. **Trusted_Extensions 폴더 아이콘을 두 번 누릅니다.**
      이 폴더에는 인터페이스, LDAP 클라이언트 및 레이블이 있는 영역을 설정하는 작업이 포함되어 있습니다.

5 **Create LDAP Client(LDAP 클라이언트 만들기) 작업을 두 번 누릅니다.**
   다음 프롬프트에 응답합니다.

`Domain Name:`	*Type the domain name*
`Hostname of LDAP Server:`	*Type the name of the server*
`IP Address of LDAP Server:`	*Type the IP address*
`LDAP Proxy Password:`	*Type the password to the server*
`Profile Name:`	*Type the profile name*

6 **OK(확인)를 누릅니다.**
   다음 완료 메시지가 나타납니다.

```
global zone will be LDAP client of LDAP-server
System successfully configured.

*** Select Close or Exit from the window menu to close this window ***
```

7 **작업 창을 닫습니다.**

8 **서버에서 정보가 올바른지 확인합니다.**

   a. **단말기 창을 열고 LDAP 서버를 쿼리합니다.**

```
# ldapclient list
```

   출력은 다음과 유사합니다.

```
NS_LDAP_FILE_VERSION= 2.0
NS_LDAP_BINDDN= cn=proxyagent,ou=profile,dc=domain-name
...
NS_LDAP_BIND_TIME= number
```

b. 오류를 수정합니다.

오류가 발생하면 올바른 값을 사용하여 Create LDAP Client(LDAP 클라이언트 만들기) 작업을 실행합니다. 예를 들어, 다음 오류는 시스템에 LDAP 서버의 항목이 없음을 나타냅니다.

```
LDAP ERROR (91): Can't connect to the LDAP server.
Failed to find defaultSearchBase for domain domain-name
```

이 오류를 해결하려면 LDAP 서버를 확인해야 합니다.

레이블이 있는 영역 만들기

`txzonemgr` 스크립트는 레이블이 있는 영역을 구성하는 다음 작업 과정을 모두 안내합니다.

주의 – `txzonemgr` 절차를 사용하려면 Trusted Extensions의 Solaris 10 8/07 릴리스를 실행해야 합니다. 또는 이 릴리스에 대한 모든 패치를 설치해야 합니다.

현재 패치를 설치하지 않고 Solaris 10 11/06 릴리스를 실행할 경우 부록 B, "CDE 작업을 사용하여 Trusted Extensions에 영역 설치"의 절차에 따라 레이블이 있는 영역을 구성합니다.

이 절의 지침에서는 두 개 이하의 IP 주소가 할당된 시스템에서 레이블이 있는 영역을 구성합니다. 기타 옵션은 29 페이지 "작업 맵: Trusted Extensions 준비 및 설치"의 구성 옵션을 참조하십시오.

작업	설명	수행 방법
1. `txzonemgr` 스크립트를 실행합니다.	`txzonemgr` 스크립트는 영역을 구성할 때 적합한 작업을 나타내는 GUI를 만듭니다.	58 페이지 "`txzonemgr` 스크립트 실행"
2. 전역 영역에서 네트워크 인터페이스를 관리합니다.	전역 영역에서 인터페이스를 구성하거나 논리적 인터페이스를 만든 후 전역 영역에서 구성합니다.	59 페이지 "Trusted Extensions에서 네트워크 인터페이스 구성"
3. 영역의 이름과 레이블을 지정합니다.	레이블의 버전을 사용하여 영역의 이름을 지정하고 레이블을 할당합니다.	62 페이지 "영역의 이름 및 레이블 지정"
4. 영역을 설치하고 부트합니다.	영역에서 패키지를 설치합니다. 영역에서 서비스를 구성합니다. Zone Terminal Console(영역 터미널 콘솔)을 사용하여 영역에서 활동을 볼 수 있습니다.	65 페이지 "레이블이 있는 영역 설치" 66 페이지 "레이블이 있는 영역 부트"
5. 영역의 상태를 확인합니다.	레이블이 있는 영역이 실행 중이고 영역이 전역 영역과 통신할 수 있는지 확인합니다.	67 페이지 "영역 상태 확인"

작업	설명	수행 방법
6. 영역을 사용자 정의합니다.	원하지 않는 서비스를 영역에서 제거합니다. 이 영역을 사용하여 다른 영역을 만들려면 이 영역에만 해당하는 정보를 제거합니다.	68 페이지 “레이블이 있는 영역 사용자 정의”
7. 나머지 영역을 만듭니다.	두 번째 영역을 만들 때 선택한 방법을 사용합니다. 영역을 만드는 방법에 대한 설명은 21 페이지 “Trusted Extensions의 영역 계획”을 참조하십시오.	70 페이지 “Trusted Extensions에서 다른 영역 만들기”
8. (선택 사항) 영역별 네트워크 인터페이스를 추가합니다.	네트워크 격리를 적용하려면 레이블이 있는 영역에 하나 이상의 네트워크 인터페이스를 추가합니다. 일반적으로 이 구성은 레이블이 있는 서브넷을 격리시키는 데 사용됩니다.	72 페이지 “레이블이 있는 기존 영역에 네트워크 인터페이스 추가”

▼ txzonemgr 스크립트 실행

이 스크립트는 레이블이 있는 영역을 적절하게 구성, 설치, 초기화 및 부트하기 위한 작업 과정을 안내합니다. 스크립트에서 각 영역의 이름을 지정하고 이름을 레이블과 연결하며, 패키지를 설치하여 가상 OS를 만든 다음 영역을 부트하여 해당 영역에서 서비스를 시작합니다. 스크립트에는 영역 복사 및 영역 복제 작업이 포함되어 있습니다. 또한 영역을 정지하고 영역의 상태를 변경하며 영역별 네트워크 인터페이스를 추가할 수 있습니다.

이 스크립트는 현재 상황에 유효한 옵션만 표시하도록 동적으로 지정되는 메뉴를 제공합니다. 예를 들어, 영역의 상태를 구성할 경우 영역 설치 메뉴 항목은 표시되지 않습니다. 완료한 작업은 목록에 표시되지 않습니다.

시작하기 전에 사용자는 수퍼유저입니다.

영역을 복제하려는 경우 영역 복제 준비를 완료했습니다. 사용자 보안 템플리트를 사용하려는 경우 템플리트를 만들었습니다.

1 전역 영역에서 단말기 창을 엽니다.

2 txzonemgr 스크립트를 실행합니다.

```
# /usr/sbin/txzonemgr
```

이 스크립트로 Labeled Zone Manager 대화 상자가 열립니다. 이 zenity 대화 상자에는 현재의 설치 상태에 따라 해당 작업을 묻는 메시지가 표시됩니다.

작업을 수행하려면 메뉴 항목을 선택한 다음 Enter 키 또는 OK(확인)를 누릅니다. 텍스트를 입력하라는 메시지가 표시되면 텍스트를 입력한 다음 Enter 키 또는 OK(확인)를 누릅니다.

▼ Trusted Extensions에서 네트워크 인터페이스 구성

주 – DHCP를 사용하거나 네트워크가 전역 영역에 연결되지 않도록 시스템을 구성하려면 OpenSolaris Community: Security 웹 페이지 (`http://opensolaris.org/os/community/security`)의 Trusted Extensions 섹션에 있는 노트북 지침을 참조하십시오.

이 작업에서는 전역 영역에서 네트워크를 구성합니다. 정확히 한개 `all-zones` 인터페이스를 만들어야 합니다. `all-zones` 인터페이스가 레이블이 있는 영역과 전역 영역에 공유됩니다. 공유된 인터페이스는 레이블이 있는 영역과 전역 영역간의 트래픽 경로로 사용됩니다. 이 인터페이스를 구성하려면 다음 중 하나를 수행해야 합니다:

- 물리적 인터페이스에서 논리적 인터페이스를 만듭니다. 다음 물리적 인테페이스를 공유합니다.

  이 구성은 관리하기에 가장 간단합니다. 시스템에 두 개의 IP 주소가 할당된 경우 이 구성을 선택합니다. 이 절차에서 논리적 인터페이스가 전역 영역의 특정 주소로 되며 물리적 인터페이스가 전역 영역과 레이블이 있는 영역 사이에서 공유됩니다.

- 물리적 인터페이스 공유

  시스템에 하나의 IP 주소가 할당된 경우 이 구성을 선택합니다. 이 구성에서는 전역 영역과 레이블이 있는 영역이 물리적 인터페이스를 공유합니다.

- 가상 네트워크 인터페이스 공유, `vni0`

  DHCP를 구성하거나 또는 각 하위 네트워크가 다른 레이블상에 있을 때 이 구성을 선택합니다. 예제 절차는 OpenSolaris Community: Security 웹 페이지 (`http://opensolaris.org/os/community/security`)의 Trusted Extensions 섹션에 있는 노트북 지침을 참조하십시오.

영역별 네트워크 인터페이스를 추가하려면 영역 만들기를 마치고 이를 확인한 후에 인터페이스를 추가합니다. 절차는 72 페이지 “레이블이 있는 기존 영역에 네트워크 인터페이스 추가”를 참조하십시오.

시작하기 전에 사용자는 전역 영역의 수퍼유저입니다.

Labeled Zone Manager(레이블이 있는 영역 관리자)가 표시됩니다. 이 GUI를 열려면 58 페이지 “`txzonemgr` 스크립트 실행”을 참조하십시오.

1 **Labeled Zone Manager(레이블이 있는 영역 관리자)에서 Manage Network Interfaces(네트워크 인터페이스 관리)를 선택하고 OK(확인)를 누릅니다.**

인터페이스 목록이 표시됩니다.

주 – 이 예에서 물리적 인터페이스는 설치 중에 호스트 이름과 IP 주소로 할당됩니다.

2 **physical interface(물리적 인터페이스)를 선택.**

인터페이스가 하나인 시스템에는 다음과 비슷한 메뉴가 표시됩니다. 지원을 위해 주석이 추가됩니다.

```
vni0                          Down      Virtual Network Interface
eri0 global 10.10.9.9 cipso Up      Physical Interface
```

a. **eri0 인터페이스 선택.**

b. **OK(확인)를 누릅니다.**

3 **이 네트워크 인터페이스에 해당하는 작업을 선택합니다.**

세 가지 옵션이 제공됩니다.

```
View Template       Assign a label to the interface
Share       Enable the global zone and labeled zones to use this interface
Create Logical Interface       Create an interface to use for sharing
```

- **시스템이 한 개 IP 주소를 갖고 있다면 단계 4로 이동합니다.**
- **시스템이 두 개 IP 주소를 갖고 있다면 단계 6으로 이동합니다.**

4 **한 개 IP 주소를 갖고 있는 시스템에서 물리적 인터페이스를 공유합니다.**

이 구성에서는 호스트의 IP 주소가 모든 영역에 적용됩니다. 따라서 호스트의 주소가 `all-zones` 주소입니다. 이 호스트는 다중 레벨 서버로 사용되지 않습니다. 예를 들어, 사용자가 이 시스템에서 파일을 공유할 수 없습니다. 시스템이 LDAP 프록시 서버, NFS 홈 디렉토리 서버 또는 인쇄 서버가 될 수 없습니다.

a. **Share(공유)을 선택하고 OK(확인)를 누릅니다.**

b. **프롬프트에서 호스트 이름을 적용합니다.**

c. **네트마스크를 표시하는 대화 상자를 닫습니다.**

```
eri0  all-zones  10.10.9.8  cipso  Up
```

5 **다음 단계를 건너뜁니다.**

물리적 인터페이스가 `all-zones` 인터페이스인 경우 성공.

6 **두 개 IP 주소를 갖고 있는 시스템에서 논리적 인터페이스를 만듭니다.**

그런 다음 물리적 인터페이스를 공유합니다.

이 구성이 가장 간단한 Trusted Extensions 네트워크 구성입니다. 이 구성에서 기본 IP 주소는 다른 시스템에 사용되어 이 시스템상의 모든 영역에 도달할 수 있으며 논리적 인터페이스는 전역 영역에 대해 영역별입니다. 전역 영역은 다중 레벨 서버로 사용할수 있습니다.

a. **Create Logical Interface(논리적 인터페이스 작성)를 선택하고 ok(확인)를 누릅니다.**
   새로운 논리적 인터페이스 작성을 확인하는 대화 상자를 없앱니다.

b. **Set IP address(IP 주소 설정)를 선택하고 ok(확인)를 누릅니다.**

c. **프롬프트에서 논리적 인터페이스의 호스트 이름을 지정하고 ok(확인)를 누릅니다.**
   예를 들어 논리적 인터페이스의 호스트 이름을 `machine1-services` 로 지정합니다. 이름은 이 호스트가 다중 레벨 서비스를 제공한다는것을 나타냅니다.

d. **프롬프트에서 논리적 인터페이스의 IP 주소를 지정하고 ok(확인)를 누릅니다.**
   예를 들어 논리적 인터페이스의 IP 주소를 `10.10.9.2` 로 지정합니다.

e. **logical interface(논리적 인터페이스)를 다시 선택하고 ok(확인)를 누릅니다.**

f. **Bring Up(실행)를 선택하고 OK(확인)를 누릅니다.**
   인터페이스가 `Up`으로 표시됩니다.

```
eri0    global       10.10.9.1   cipso   Up
eri0:1  global       10.10.9.2   cipso   Up
```

g. **물리적 인터페이스를 공유합니다.**

   i. **physical interface(물리적 인터페이스)를 선택하고 ok(확인)를 누릅니다.**

   ii. **Share(공유)을 선택하고 OK(확인)를 누릅니다.**

```
eri0    all-zones    10.10.9.1   cipso   Up
eri0:1  global       10.10.9.2   cipso   Up
```

적어도 한개 인터페이스가 `all-zones` 인터페이스이면 성공.

예 4–2 공유된 논리적 인터페이스를 사용하여 시스템에서 /etc/hosts 파일 보기

전역 영역에 고유한 인터페이스가 있고 레이블이 있는 영역이 전역 영역과 두 번째 인터페이스를 공유하는 시스템에서 `/etc/hosts` 파일은 다음과 비슷합니다.

```
# cat /etc/hosts
...
127.0.0.1  localhost
192.168.0.11 machine1 loghost
192.168.0.12 machine1-services
```

기본 구성에서 tnrhdb 파일은 다음과 비슷합니다.

```
# cat /etc/security/tsol/tnrhdb
...
127.0.0.1:cipso
192.168.0.11:cipso
192.168.0.12:cipso
0.0.0.0:admin_low
```

all-zones 인터페이스가 tnrhdb 파일에 없는 경우 인터페이스는 기본적으로 cipso로 지정됩니다.

예 4–3 IP 주소가 하나인 Trusted Extensions 시스템에서 공유 인터페이스 표시

이 예에서 관리자는 시스템을 다중 레벨 서버로 사용하지 않습니다. IP 주소를 유지하기 위해 전역 영역은 레이블이 있는 모든 영역과 해당 IP 주소를 공유하도록 구성됩니다.

관리자는 시스템에서 hme0 인터페이스에 대해 Share(공유)를 선택합니다.
소프트웨어에서는 모든 영역이 논리적 NIC를 갖도록 구성합니다. 이러한 논리적 NIC는 전역 영역에서 한 개의 물리적 NIC를 공유합니다.

관리자는 **ifconfig -a** 명령을 실행하여 네트워크 인터페이스 192.168.0.11에서 물리적 인터페이스 hme0이 공유되는지 확인합니다. all-zones 값이 표시됩니다.

```
lo0: flags=2001000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4,VIRTUAL> mtu 8232 index 1
        inet 127.0.0.1 netmask ff000000
hme0: flags=1000843<BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        all-zones
        inet 192.168.0.11 netmask fffffe00 broadcast 192.168.0.255
```

또한 관리자는 /etc/hostname.hme0 파일의 내용을 검사합니다.

```
192.168.0.11 all-zones
```

▼ 영역의 이름 및 레이블 지정

label_encodings 파일의 모든 레이블에 대해 영역을 만들 필요는 없지만 그렇게 할 수는 있습니다. 관리 GUI는 이 시스템에서 영역을 만들 수 있는 레이블을 열거합니다.

시작하기 전에 사용자는 전역 영역의 수퍼유저입니다. Labeled Zone Manager(레이블이 있는 영역 관리자) 대화 상자가 표시됩니다. 이 GUI를 열려면 58 페이지 “txzonemgr 스크립트 실행”을 참조하십시오. 전역 영역에서 네트워크 인터페이스를 구성했습니다.

필요한 보안 템플리트를 만들었습니다. 보안 템플리트는 속성 중에서 네트워크 인터페이스에 할당할 수 있는 레이블 범위를 정의합니다. 기본 보안 템플리트는 사용자의 요구를 충족시킬 수 있습니다.

- 보안 템플리트에 대한 개요는 **Solaris Trusted Extensions Administrator's Procedures**의 "Network Security Attributes in Trusted Extensions"를 참조하십시오.
- Solaris Management Console을 사용하여 보안 템플리트를 만들려면 **Solaris Trusted Extensions Administrator's Procedures**의 "Configuring Trusted Network Databases (Task Map)"를 참조하십시오.

1 Labeled Zone Manager(레이블이 있는 영역 관리자)에서 Create a new zone(새 영역 만들기)을 선택하고 OK(확인)를 누릅니다.

이름을 묻는 메시지가 표시됩니다.

a. 영역의 이름을 입력합니다.

참고 – 영역에 해당 레이블과 비슷한 이름을 지정합니다. 예를 들어, 레이블이 `CONFIDENTIAL: RESTRICTED`인 영역의 이름은 `restricted`입니다.

예를 들어, 기본 `label_encodings` 파일에 다음과 같은 레이블이 포함되어 있습니다.

```
PUBLIC
CONFIDENTIAL: INTERNAL USE ONLY
CONFIDENTIAL: NEED TO KNOW
CONFIDENTIAL: RESTRICTED
SANDBOX: PLAYGROUND
MAX LABEL
```

레이블당 영역을 한 개씩 만들 수 있지만 다음과 같이 영역을 만드는 것을 고려해 보십시오.

- 모든 사용자용 시스템에서 `PUBLIC` 레이블에 대해 한 개의 영역을, `CONFIDENTIAL` 레이블에 대해 세 개의 영역을 만듭니다.
- 개발자용 시스템에서 `SANDBOX: PLAYGROUND` 레이블에 대해 영역을 만듭니다. `SANDBOX: PLAYGROUND`는 개발자용 분리 레이블로 정의되므로 개발자가 사용하는 시스템에만 이 레이블에 대해 영역이 필요합니다.
- 클리어런스로 정의되는 `MAX LABEL` 레이블에 대해서는 영역을 만들지 마십시오.

b. OK(확인)를 누릅니다.

대화 상자의 작업 목록 위에 *zone-name* `:configured`가 표시됩니다.

2 **영역의 레이블을 지정하려면 다음 중 하나를 선택합니다.**

- **사용자 정의된** `label_encodings` **파일을 사용할 경우 Trusted Network Zones(신뢰할 수 있는 네트워크 영역) 도구를 사용하여 영역의 레이블을 지정합니다.**

  a. **Solaris Management Console에서 Trusted Network Zones(신뢰할 수 있는 네트워크 영역) 도구를 엽니다.**

     i. **Solaris Management Console을 시작합니다.**

     ```
     # /usr/sbin/smc &
     ```

     ii. **로컬 시스템의 Trusted Extensions 도구 상자를 엽니다.**

     Console(콘솔) → Open Toolbox(도구 상자 열기)를 선택합니다.

     이 컴퓨터(*this-host*: `Scope=Files, Policy=TSOL`)라는 도구 상자를 선택합니다.

     Open(열기)을 누릅니다.

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

     암호를 입력하라는 메시지가 나타나면 암호를 제공합니다.

     iv. **Trusted Network Zones(신뢰할 수 있는 네트워크 영역) 도구를 두 번 누릅니다.**

  b. **각 영역에 대해 해당 레이블을 영역 이름과 연결합니다.**

     i. **Action(작업) → Add Zone Configuration(영역 구성 추가)을 선택합니다.**

     대화 상자에 할당된 레이블이 없는 영역의 이름이 표시됩니다.

     ii. **영역 이름을 확인한 다음 Edit(편집)를 누릅니다.**

     iii. **레이블 구축기에서 영역 이름에 해당하는 레이블을 누릅니다.**

     잘못된 레이블을 누른 경우 레이블을 다시 눌러 선택을 해제한 다음 올바른 레이블을 누릅니다.

     iv. **할당을 저장합니다.**

     레이블 구축기에서 OK(확인)를 누른 다음 Trusted Network Zones Properties(신뢰할 수 있는 네트워크 영역 등록 정보) 대화 상자에서 OK(확인)를 누릅니다.

원하는 모든 영역이 패널에 표시되어 있으면 작업이 완료된 것이며, 그렇지 않은 경우 Add Zone Configuration(영역 구성 추가) 메뉴 항목이 Zone Name(영역 이름)에 값이 없는 대화 상자를 엽니다.

- **기본 `label_encodings` 파일을 사용할 경우 Labeled Zone Manager(레이블이 있는 영역 관리자)를 사용합니다.**

  Select Label(레이블 선택) 메뉴 항목을 누르고 OK(확인)를 눌러 사용 가능한 레이블 목록을 표시합니다.

  a. **영역에 대한 레이블을 선택합니다.**

     영역의 이름이 `public`인 경우 목록에서 `PUBLIC` 레이블을 선택합니다.

  b. **OK(확인)를 누릅니다.**

     작업 목록이 표시됩니다.

▼ 레이블이 있는 영역 설치

시작하기 전에 사용자는 전역 영역의 수퍼유저입니다. 영역이 설치되고 네트워크 인터페이스가 영역에 할당됩니다.

부제가 *zone-name*:`configured`인 Labeled Zone Manager(레이블이 있는 영역 관리자) 대화 상자가 표시됩니다. 이 GUI를 열려면 58 페이지 “`txzonemgr` 스크립트 실행”을 참조하십시오.

1 **Labeled Zone Manager(레이블이 있는 영역 관리자)에서 Install(설치)을 선택하고 OK(확인)를 누릅니다.**

주의 – 이 프로세스는 완료하는 데 시간이 약간 걸립니다. 이 작업을 완료하는 동안에는 다른 작업을 수행하지 마십시오.

패키지를 전역 영역에서 비전역 영역으로 복사합니다. 이 작업에서는 레이블이 있는 가상 운영 체제를 영역에 설치합니다. 이 예를 계속하려면 이 작업에서 `public` 영역을 설치합니다. GUI 표시 출력은 다음과 비슷합니다.

```
# Labeled Zone Manager: Installing zone-name zone
Preparing to install zone <zonename>
Creating list of files to copy from the global zone
Copying <total> files to the zone
Initializing zone product registry
Determining zone package initialization order.
Preparing to initialize <subtotal> packages on the zone.
Initializing package <number> of <subtotal>: percent complete: percent
```

```
Initialized <subtotal> packages on zone.
Zone <zonename> is initialized.
The file /zone/internal/root/var/sadm/system/logs/install_log
contains a log of the zone installation.
```

설치가 완료되면 호스트의 이름을 묻는 메시지가 표시됩니다. 이름이 제공됩니다.

2 호스트의 이름을 그대로 사용합니다.

대화 상자의 작업 목록 위에 *zone-name*:installed가 표시됩니다.

일반 오류 Installation of these packages generated errors: SUNW*pkgname*과 비슷한 경고가 표시될 경우 설치 로그를 확인하고 패키지 설치를 마칩니다.

▼ 레이블이 있는 영역 부트

시작하기 전에 사용자는 전역 영역의 수퍼유저입니다. 영역이 설치되고 네트워크 인터페이스가 영역에 할당됩니다.

부제가 *zone-name*:installed인 Labeled Zone Manager(레이블이 있는 영역 관리자) 대화 상자가 표시됩니다. 이 GUI를 열려면 58 페이지 “txzonemgr 스크립트 실행”을 참조하십시오.

1 Labeled Zone manager(레이블이 있는 영역 관리자)에서 Zone Console(영역 콘솔)을 선택하고 OK(확인)를 누릅니다.

현재 레이블이 있는 영역에 대한 개별 콘솔 창이 나타납니다.

2 Boot(부트)를 선택합니다.

Zone Terminal Console(영역 터미널 콘솔)에서 영역의 부트 진행률을 추적합니다. 영역을 처음부터 만들 경우 다음과 비슷한 메시지가 콘솔에 표시됩니다.

```
[Connected to zone 'public' console]

[NOTICE: Zone booting up]
...
Hostname: zone-name
Loading smf(5) service descriptions: number/total
Creating new rsa public/private host key pair
Creating new dsa public/private host key pair

rebooting system due to change(s) in /etc/default/init

[NOTICE: Zone rebooting]
```

주의 – 이 작업을 완료하는 동안에는 다른 작업을 수행하지 마십시오.

일반 오류 오류 메시지가 표시되고 영역이 다시 부트되지 않는 경우도 있습니다. Zone Terminal Console(영역 터미널 콘솔)에서 Enter 키를 누릅니다. 다시 부트하기 위해 y를 입력하라는 메시지가 표시되면 y를 입력하고 Enter 키를 누릅니다. 영역이 다시 부트됩니다.

다음 순서 이 영역이 다른 영역에서 복사 또는 복제된 경우 67 페이지 "영역 상태 확인"을 계속합니다.

이 영역이 첫 번째 영역이면 68 페이지 "레이블이 있는 영역 사용자 정의"를 계속합니다.

▼ 영역 상태 확인

주 – X 서버가 전역 영역에서 실행됩니다. X 서버를 사용하려면 레이블이 있는 각 영역에서 전역 영역에 연결할 수 있어야 합니다. 따라서 영역을 사용하려면 영역 네트워크가 작동해야 합니다. 자세한 내용은 23 페이지 "다중 레벨 액세스 계획"을 참조하십시오.

1 영역이 완전히 시작되었는지 확인합니다.

a. *zone-name*: **Zone Terminal Console(영역 터미널 콘솔)에서 루트로 로그인합니다.**

```
hostname console login: root
Password:       Type root password
```

b. Zone Terminal Console(영역 터미널 콘솔)에서 중요한 서비스를 실행하고 있는지 확인합니다.

```
# svcs -xv
svc:/application/print/server:default (LP print server)
 State: disabled since Tue Oct 10 10:10:10 2006
Reason: Disabled by an administrator.
   See: http://sun.com/msg/SMF-8000-05
   See: lpsched(1M)
...
```

`sendmail` 및 `print` 서비스는 중요한 서비스가 아닙니다.

c. 영역에 유효한 IP 주소가 있는지 확인합니다.

```
# ifconfig -a
```

예를 들어, 다음 출력에는 hme0 인터페이스에 대한 IP 주소가 표시됩니다.

```
# ...
 hme0: flags=1000843<BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
         all-zones
         inet 192.168.0.11 netmask fffffe00 broadcast 192.168.0.255
```

d. (옵션) 영역이 전역 영역과 통신할 수 있는지 확인합니다.

i. DISPLAY 변수가 X 서버를 가리키도록 설정합니다.

```
# DISPLAY=global-zone-hostname:n.n
# export DISPLAY
```

ii. 단말기 창에서 GUI를 표시합니다.

예를 들어, 클럭을 표시합니다.

```
# /usr/openwin/bin/xclock
```

영역 레이블에 클럭이 나타나지 않는 경우 영역 네트워크가 잘못 구성된 것입니다. 디버깅 제안 사항은 87 페이지 "레이블이 있는 영역에서 X 서버에 액세스할 수 없음"을 참조하십시오.

iii. 계속하려면 먼저 GUI를 닫습니다.

2 전역 영역에서 레이블이 있는 영역의 상태를 확인합니다.

```
# zoneadm list -v
ID NAME         STATUS         PATH                BRAND   IP
 0 global       running        /                   native  shared
 3 internal     running        /zone/internal      native  shared
 4 needtoknow   running        /zone/needtoknow    native  shared
 5 restricted   running        /zone/restricted    native  shared
```

▼ 레이블이 있는 영역 사용자 정의

영역을 복제하거나 복사하려면 이 절차에서 영역을 다른 영역에 대한 템플리트로 구성합니다. 또한 이 절차에서 사용할 템플리트에서 만들어지지 않은 영역을 구성합니다.

시작하기 전에 사용자는 전역 영역의 수퍼유저입니다. 67 페이지 "영역 상태 확인"을 완료했습니다.

1 **Zone Terminal Console(영역 터미널 콘솔)의 레이블이 있는 영역에서 불필요한 서비스를 비활성화합니다.**

이 영역을 복사 또는 복제하는 경우에는 비활성화한 서비스가 새 영역에서 비활성화됩니다. 시스템에 온라인 상태로 유지되는 서비스는 영역에 대한 서비스 매니페스트에 따라 달라집니다. `netservices limited` 명령을 사용하여 레이블이 있는 영역에서 불필요한 서비스를 해제합니다.

a. **불필요한 서비스들을 제거합니다.**

```
# netservices limited
```

b. **나머지 서비스를 나열합니다.**

```
# svcs
...
STATE          STIME      FMRI
online         13:05:00   svc:/application/graphical-login/cde-login:default
...
```

c. **그래픽 로그인을 비활성화합니다.**

```
# svcadm disable svc:/application/graphical-login/cde-login
# svcs cde-login
STATE          STIME      FMRI
disabled       13:06:22   svc:/application/graphical-login/cde-login:default
```

서비스 관리 프레임워크에 대한 자세한 내용은 `smf(5)` 매뉴얼 페이지를 참조하십시오.

2 **Labeled Zone Manager(레이블이 있는 관리자)에서 Halt(정지)를 선택하여 영역을 정지시킵니다.**

3 **계속하기 전에 먼저 영역이 종료되었는지 확인합니다.**

zone-name: Zone Terminal Console(영역 터미널 콘솔)에서 다음 메시지는 영역이 종료되었음을 나타냅니다.

```
[ NOTICE: Zone halted]
```

이 영역을 복사 또는 복제하지 않는 경우에는 첫 번째 영역을 만든 방법으로 나머지 영역을 만듭니다. 그렇지 않은 경우 다음 단계를 계속합니다.

4 **이 영역을 다른 영역에 대한 템플리트로 사용하는 경우에는 다음을 수행합니다.**

a. `auto_home_`*zone-name* **파일을 제거합니다.**

전역 영역의 터미널 창에서 이 파일을 *zone-name* 영역에서 제거합니다.

```
# cd /zone/zone-name/root/etc
# ls auto_home*
auto_home  auto_home_zone-name
# rm auto_home_zone-name
```

예를 들어, public 영역이 다른 영역의 복제를 위한 템플리트인 경우 auto_home_public 파일을 제거합니다.

```
# cd /zone/public/root/etc
# rm auto_home_public
```

b. **이 영역을 복제하려면 다음 단계에서 ZFS 스냅샷을 만든 다음 70 페이지 "Trusted Extensions에서 다른 영역 만들기"를 계속합니다.**

c. **이 영역을 복사하려면 단계 6을 완료한 다음 70 페이지 "Trusted Extensions에서 다른 영역 만들기"를 계속합니다.**

5 **나머지 영역을 복제하기 위한 영역 템플리트를 만들려면 Create Snapshot(스냅샷 만들기)을 선택한 다음 OK(확인)를 누릅니다.**

주의 – 스냅샷 영역이 ZFS 파일 시스템에 있어야 합니다. 49 페이지 "영역 복제를 위한 ZFS 풀 만들기 "에서 영역에 대한 ZFS 파일 시스템을 만들었습니다.

6 **사용자 정의된 영역을 계속 사용할 수 있는지 확인하려면 Labeled Zone Manager(레이블이 있는 영역 관리자)에서 Boot(부트)를 선택합니다.**

Zone Terminal Console(영역 터미널 콘솔)에서 영역의 부트 진행률을 추적합니다. 콘솔에 다음과 유사한 메시지가 나타납니다.

```
[Connected to zone 'public' console]

[NOTICE: Zone booting up]
...
Hostname: zonename
```

로그인 프롬프트에서 Enter 키를 누릅니다. root로 로그인할 수 있습니다.

▼ Trusted Extensions에서 다른 영역 만들기

다음과 같은 세 가지 옵션이 있습니다.

- 첫 번째 영역을 복사할 수 있습니다.
- 첫 번째 영역을 만드는 데 사용했던 단계를 반복할 수 있습니다.
- 첫 번째 영역을 복제할 수 있습니다.

시작하기 전에 68 페이지 "레이블이 있는 영역 사용자 정의"를 완료했습니다.

Labeled Zone Manager(레이블이 있는 영역 관리자) 대화 상자가 표시됩니다. 이 GUI를 열려면 58 페이지 "txzonemgr 스크립트 실행"을 참조하십시오.

1 **영역의 이름과 레이블을 지정합니다.**
자세한 내용은 62 페이지 "영역의 이름 및 레이블 지정"을 참조하십시오.

2 **다음 방법 중 하나를 선택하여 영역 만들기 전략을 계속합니다.**
모든 새 영역에 대해 이 단계를 반복합니다.

- **모든 영역을 처음부터 만듭니다.**
  a. **65 페이지 "레이블이 있는 영역 설치"를 완료합니다.**
  b. **66 페이지 "레이블이 있는 영역 부트"를 완료합니다.**
  c. **67 페이지 "영역 상태 확인"을 완료합니다.**
  d. **68 페이지 "레이블이 있는 영역 사용자 정의"를 완료합니다.**
- **레이블이 있는 영역을 복사합니다.**
  a. **Labeled Zone Manager(레이블이 있는 영역 관리자)에서 Copy(복사)를 선택하고 OK(확인)를 누릅니다.**
  b. **영역 템플리트를 선택하고 OK(확인)를 누릅니다.**
  창에 복사 프로세스가 표시됩니다. 프로세스가 완료되면 영역이 설치됩니다.
  Labeled Zone Manager(레이블이 있는 영역 관리자)에 *zone-name* `:configured`가 표시되면 다음 단계를 계속합니다. 그렇지 않으면 단계 e를 계속합니다.
  c. **Select another zone(다른 영역 선택) 메뉴 항목을 선택하고 OK(확인)를 누릅니다.**
  d. **새로 설치된 영역을 선택하고 OK(확인)를 누릅니다.**
  e. **66 페이지 "레이블이 있는 영역 부트"를 완료합니다.**
  f. **67 페이지 "영역 상태 확인"을 완료합니다.**
- **레이블이 있는 영역을 복제합니다.**
  a. **Labeled Zone Manager(레이블이 있는 영역 관리자)에서 Clone(복제)을 선택하고 OK(확인)를 누릅니다.**
  b. **목록에서 ZFS 스냅샷을 선택하고 OK(확인)를 누릅니다.**
  예를 들어, `public`에서 스냅샷을 만든 경우 `zone/public@snapshot`을 선택합니다.

복제 프로세스가 완료되면 영역이 설치됩니다. Labeled Zone Manager(레이블이 있는 영역 관리자)에 *zone-name* :configured가 표시되면 다음 단계를 계속합니다. 그렇지 않으면 단계 e를 계속합니다.

c. Select another zone(다른 영역 선택) 메뉴 항목을 선택하고 OK(확인)를 누릅니다.

d. 새로 설치된 영역을 선택하고 OK(확인)를 누릅니다.

e. 66 페이지 "레이블이 있는 영역 부트"를 완료합니다.

f. 67 페이지 "영역 상태 확인"을 완료합니다.

다음 순서

- 모든 영역에 대해 67 페이지 "영역 상태 확인"을 완료한 상태에서 각 영역을 별도의 물리적 네트워크에 지정하려면 72 페이지 "레이블이 있는 기존 영역에 네트워크 인터페이스 추가"를 계속합니다.
- 역할을 아직 만들지 않은 경우 74 페이지 "Trusted Extensions의 역할 및 사용자 만들기"를 계속합니다.
- 역할을 이미 만든 경우 81 페이지 "Trusted Extensions에서 홈 디렉토리 만들기"를 계속합니다.

▼ 레이블이 있는 기존 영역에 네트워크 인터페이스 추가

이 절차에서는 레이블이 있는 기존 영역에 영역별 네트워크 인터페이스를 추가합니다. 이 구성은 각 영역이 별도의 물리적 네트워크에 연결되는 환경을 지원합니다.

주 – 전역 영역은 비전역 영역 주소를 구성한 모든 서브넷의 IP 주소를 구성해야 합니다.

시작하기 전에 사용자는 전역 영역의 수퍼유저입니다. 67 페이지 "영역 상태 확인"을 성공적으로 완료했습니다.

1 전역 영역에서 추가 네트워크 인터페이스의 IP 주소와 호스트 이름을 /etc/hosts 파일에 입력합니다.

호스트의 이름에 *-zone-name* 을 추가 하는것과 같은 표준 이름 지정 규약을 사용하십시오.

```
## /etc/hosts in global zone
10.10.8.2    hostname-zone-name1
10.10.8.3    hostname-global-name1
10.10.9.2    hostname-zone-name2
10.10.9.3    hostname-global-name2
```

2 **네트워크의 각 인터페이스에 대해 /etc/netmasks 파일에 항목을 추가합니다.**

```
## /etc/netmasks in global zone
10.10.8.0 255.255.255.0
10.10.9.0 255.255.255.0
```

자세한 내용은 netmasks(4) 매뉴얼 페이지를 참조하십시오.

3 **전역 영역에서 영역별 물리적 인터페이스를 연결합니다.**

a. **이미 연결한 물리적 인터페이스를 식별합니다.**

```
# ifconfig -a
```

b. **각 인터페이스에 전역 영역 주소를 구성합니다.**

```
# ifconfig interface-nameN1 plumb
# ifconfig interface-nameN1 10.10.8.3 up
# ifconfig interface-nameN2 plumb
# ifconfig interface-nameN2 10.10.9.3 up
```

c. **각 전역 영역 주소에 대해서 hostname. *interface-nameN* 파일을 만듭니다.**

```
# /etc/hostname.interface-nameN1
10.10.8.3
# /etc/hostname.interface-nameN2
10.10.9.3
```

전역 영역 주소는 시스템 시작에서 즉시 구성됩니다. 영역이 부트될 때 영역별 주소가 구성됩니다.

4 **각 영역별 네트워크 인터페이스에 보안 템플리트를 할당합니다.**

네트워크에 대한 게이트웨이에 레이블이 구성되지 않은 경우 admin_low 보안 템플리트를 할당합니다. 네트워크에 대한 게이트웨이에 레이블이 구성된 경우 cipso 보안 템플리트를 할당합니다.

모든 네트워크의 레이블을 반영하는 호스트 유형 cipso의 보안 템플리트를 구성할 수 있습니다. 템플리트를 만들거나 할당 절차를 보시려면 **Solaris Trusted Extensions Administrator's Procedures**의 "Configuring Trusted Network Databases (Task Map)"를 참조하십시오.

5 **영역별 인터페이스를 추가할 레이블이 있는 모든 영역을 정지합니다.**

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

6 **Labeled Zone Manager(레이블이 있는 영역 관리자)를 시작합니다.**

```
# /usr/sbin/txzonemgr
```

7 영역별 인터페이스를 추가할 각 영역에 대해 다음을 수행합니다.

a. 영역을 선택합니다.

b. Add Network(네트워크 추가)를 선택합니다.

c. 네트워크 인터페이스의 이름을 지정합니다.

d. 인터페이스의 IP 주소를 입력합니다.

8 Labeled Zone Manager(레이블이 있는 영역 관리자)에서 완료된 모든 영역에 대해 Zone Console(영역 콘솔)을 선택합니다.

9 Boot(부트)를 선택합니다.

10 Zone Console(영역 콘솔)에서 인터페이스가 만들어졌는지 확인합니다.

```
# ifconfig -a
```

11 영역에 서브넷에 대한 게이트웨이 경로가 있는지 확인합니다.

```
# netstat -rn
```

일반 오류 영역 구성을 디버깅하려면 다음을 참조하십시오.

- **System Administration Guide: Solaris Containers-Resource Management and Solaris Zones**의 29 장, "Troubleshooting Miscellaneous Solaris Zones Problems"
- 86 페이지 "Trusted Extensions 구성 문제 해결 "
- **Solaris Trusted Extensions Administrator's Procedures**의 "Troubleshooting the Trusted Network (Task Map)"

Trusted Extensions의 역할 및 사용자 만들기

관리 역할을 이미 사용 중인 경우 보안 관리자 역할을 추가할 수 있습니다. 역할을 아직 구현하지 않은 사이트의 경우 역할을 만드는 절차는 Solaris OS의 절차와 비슷합니다. Trusted Extensions에서는 보안 관리자 역할을 추가하고 Solaris Management Console을 사용하여 Trusted Extensions 도메인을 관리해야 합니다.

▼ Trusted Extensions의 보안 관리자 역할 만들기

Trusted Extensions의 역할 만들기는 Solaris OS의 역할 만들기와 동일합니다. 그러나 Trusted Extensions에는 Security Administrator(보안 관리자) 역할이 필요합니다. 로컬 보안 관리자 역할을 만들려면 예 4–4에서와 같이 명령줄 인터페이스를 사용할 수도 있습니다.

시작하기 전에 사용자가 수퍼유저이거나 root 역할 또는 Primary Administrator(주 관리자) 역할에 속해야 합니다.

네트워크에서 역할을 만들려면 106 페이지 “LDAP에 대해 Solaris Management Console 구성(작업 맵)”을 완료해야 합니다.

1. **Solaris Management Console을 시작합니다.**

   ```
   # /usr/sbin/smc &
   ```

2. **적절한 도구 상자를 선택합니다.**

   - **역할을 로컬로 만들려면 이 컴퓨터(*this-host*: Scope=Files, Policy=TSOL)를 사용합니다.**
   - **LDAP 서비스에서 역할을 만들려면 이 컴퓨터(*this-host*: Scope=LDAP, Policy=TSOL)를 사용합니다.**

3. **System Configuration(시스템 구성), Users(사용자)를 차례로 누릅니다.**
   암호를 입력하라는 메시지가 표시됩니다.

4. **적절한 암호를 입력합니다.**

5. **Administrative Roles(관리 역할)를 두 번 누릅니다.**

6. **Action(작업) 메뉴에서 Add Administrative Role(관리 역할 추가)을 선택합니다.**

7. **보안 관리자 역할을 만듭니다.**
   다음 정보에 따라 작업을 수행합니다.

   - Role name(역할 이름) – secadmin
   - Full name(전체 이름) – Security Administrator
   - Description(설명) – Site Security Officer(사이트 보안 관리자) **여기에는 소유 정보가 없습니다.**
   - Role ID Number(역할 ID 번호) – ≥100
   - Role Shell(역할 쉘) – 관리자의 Bourne(프로필 쉘)
   - Create A Role Mailing List(역할 메일링 목록 만들기) – 확인란을 선택한 상태로 둡니다.
   - Password And Confirm(암호 및 확인) – 6자 이상의 영숫자로 구성된 암호를 지정합니다.

     악의적인 사용자가 암호를 추측하여 무단으로 액세스하지 못하도록 보안 관리자 역할의 암호와 모든 암호를 추측하기 어렵게 지정해야 합니다.

주 – 모든 관리 역할에 대해 계정을 Always Available(항상 사용 가능)로 지정하고 암호 만료 날짜를 설정하지 않습니다.

- Available and Granted Rights(사용 가능 및 허용된 권한) – 정보 보안, 사용자 보안
- Home Directory Server(홈 디렉토리 서버) – *home-directory-server*
- Home Directory Path(홈 디렉토리 경로) – */mount-path*
- Assign Users(사용자 할당) – 사용자에게 역할을 할당하면 이 필드가 자동으로 채워집니다.

8 역할을 만든 후 설정이 올바른지 확인합니다.

역할을 선택하고 두 번 누릅니다.

다음 필드 값을 검토합니다.

- Available Groups(사용 가능한 그룹) – 필요한 경우 그룹을 추가합니다.
- Trusted Extensions Attributes(Trusted Extensions 속성) – 기본값이 올바릅니다.

  레이블을 표시하면 안되는 단일 레이블 시스템의 경우 Hide for Label(레이블 숨기기): Show(표시) 또는 Hide(숨기기)를 선택합니다.
- Audit Excluded and Included(감사 제외 및 포함) – 역할의 감사 플래그가 `audit_control` 파일의 시스템 설정에 대한 예외인 경우에만 감사 플래그를 설정합니다.

9 다른 역할을 만들려면 Security Administrator(보안 관리자) 역할을 참조하십시오.

관련 예는 **System Administration Guide: Security Services**의 "How to Create and Assign a Role by Using the GUI"를 참조하십시오. 각 역할에 고유한 ID를 제공하고 해당 역할에 올바른 권한 프로필을 할당합니다. 사용 가능한 역할은 다음과 같습니다.

- admin Role(admin 역할) – `System Administrator` 권한 부여
- primaryadmin Role(primaryadmin 역할) – `Primary Administrator` 권한 부여
- oper Role(oper 역할) – `Operator` 권한 부여

예 4–4 `roleadd` 명령을 사용하여 로컬 보안 관리자 역할 만들기

이 예에서 `root` 사용자는 `roleadd` 명령을 사용하여 로컬 시스템에 Security Administrator(보안 관리자) 역할을 추가합니다. 자세한 내용은 `roleadd(1M)` 매뉴얼 페이지를 참조하십시오. `root` 사용자는 역할을 만들기 전에 표 1–2를 참조하십시오.

```
# roleadd -c "Local Security Administrator" -d /export/home1 \
-u 110 -P "Information Security,User Security" -K lock_after_retries=no \
-K idletime=5 -K idlecmd=lock -K labelview=showsl \
-K min_label=ADMIN_LOW -K clearance=ADMIN_HIGH secadmin
```

`root` 사용자가 해당 역할에 대한 초기 암호를 제공합니다.

```
# passwd -r files secadmin
New Password:             <Type password>
Re-enter new Password:      <Retype password>
passwd: password successfully changed for secadmin
#
```

로컬 사용자에게 역할을 할당하려면 예 4–5를 참조하십시오.

▼ Trusted Extensions에서 역할을 수락할 수 있는 사용자 만들기

로컬 사용자를 만들려면 다음 절차를 수행하는 대신 예 4–5에서와 같이 명령줄 인터페이스를 사용할 수 있습니다. 사이트 보안 정책에 따라 둘 이상의 관리 역할을 수락할 수 있는 사용자를 만들도록 선택할 수 있습니다.

보안 사용자를 만드는 경우 System Administrator(시스템 관리자) 역할에서 사용자를 만들고 Security Administrator(보안 관리자) 역할에서 암호와 같은 보안 관련 속성을 할당합니다.

시작하기 전에 사용자는 수퍼유저, `root` 역할, Security Administrator(보안 관리자) 역할 또는 Primary Administrator(주 관리자) 역할이어야 합니다. Security Administrator(보안 관리자) 역할에는 사용자를 만드는 데 필요한 최소의 권한이 있습니다.

Solaris Management Console이 표시됩니다. 자세한 내용은 74 페이지 “Trusted Extensions의 보안 관리자 역할 만들기”를 참조하십시오.

1. **Solaris Management Console에서 User Accounts(사용자 계정)를 두 번 누릅니다.**
2. **Action(작업) 메뉴에서 Add User(사용자 추가) → Use Wizard(마법사 사용)를 선택합니다.**

주의 – 역할 및 사용자의 이름과 ID는 동일한 풀에서 가져옵니다. 추가하는 사용자에 대해서는 ID 기존 이름 또는 ID를 사용하지 마십시오.

3. **온라인 도움말을 따릅니다.**

   System Administration Guide: Basic Administration의 “How to Add a User With the Solaris Management Console’s Users Tool” 절차를 따를 수도 있습니다.

4. **사용자를 만든 후에 해당 사용자를 두 번 눌러 설정을 수정합니다.**

주 – 역할을 수락할 수 있는 사용자의 경우 사용자 계정을 Always Available(항상 사용 가능)로 지정하고 암호 만료 날짜를 설정하지 않습니다.

다음 필드가 올바르게 설정되어 있는지 확인합니다.

- Description(설명) – 고유 정보가 없습니다.
- Password And Confirm(암호 및 확인) – 6자 이상의 영숫자로 구성된 암호를 지정합니다.

주 – 설치 팀은 암호를 선택할 때 악의적인 사용자가 암호를 추측하여 무단으로 액세스하지 못하도록 추측하기 어려운 암호를 선택해야 합니다.

- Account Availability(계정 가용성) – Always Available(항상 가능)입니다.
- Trusted Extensions Attributes(Trusted Extensions 속성) – 기본값이 올바릅니다.

  레이블을 표시하면 안되는 단일 레이블 시스템의 경우 Hide for Label(레이블 숨기기): Show(표시) 또는 Hide(숨기기)를 선택합니다.
- Account Usage(계정 사용) – 유휴 시간과 유휴 작업을 설정합니다.

  Lock account(계정 잠금) – 역할을 수락할 수 있는 모든 사용자에 대해 No(아니오)를 설정합니다.

5 사용자 환경을 사용자 정의합니다.

- **Assign Convenient Authorizations(편리한 권한 부여 할당)**

  사이트 보안 정책을 확인한 후 첫 번째 사용자에게 Convenient Authorizations(편리한 권한 부여) 권한 프로필을 부여할 수 있습니다. 이 권한을 가진 사용자는 장치 할당, PostScript™ 파일 인쇄, 레이블 없이 인쇄, 원격 로그인 및 시스템 종료를 수행할 수 있습니다.

- **Customize user initialization files(사용자 초기화 파일 사용자 정의)**

  Solaris Trusted Extensions Administrator's Procedures의 7 장, "Managing Users, Rights, and Roles in Trusted Extensions (Tasks)"를 참조하십시오.

  Solaris Trusted Extensions Administrator's Procedures의 "Managing Users and Rights With the Solaris Management Console (Task Map)"을 참조하십시오.

- **Create Multilabel Copy And Link Files(다중 레이블 복사본 만들기 및 파일 연결)**

  다중 레이블 시스템에서는 다른 레이블에 복사하거나 연결할 사용자 초기화 파일을 나열하는 파일을 사용하여 사용자와 역할을 설정할 수 있습니다. 자세한 내용은 **Solaris Trusted Extensions Administrator's Procedures**의 ".copy_files and .link_files Files"를 참조하십시오.

예 4–5 useradd 명령을 사용하여 로컬 사용자 만들기

이 예에서 root 사용자는 Security Administrator(보안 관리자) 역할을 수락할 수 있는 로컬 사용자를 만듭니다. 자세한 내용은 useradd(1M) 및 atohexlabel(1M) 매뉴얼 페이지를 참조하십시오.

먼저 root 사용자는 16진수 형식의 사용자 최소 레이블 및 클리어런스 레이블을 결정합니다.

```
# atohexlabel public
0x0002-08-08
# atohexlabel -c "confidential restricted"
0x0004-08-78
```

다음으로 root 사용자는 표 1–2를 참조한 후에 사용자를 만듭니다.

```
# useradd -c "Local user for Security Admin" -d /export/home1 \
-K  idletime=10 -K idlecmd=logout -K lock_after_retries=no
-K min_label=0x0002-08-08 -K clearance=0x0004-08-78 -K labelview=showsl jandoe
```

그런 다음 root 사용자는 초기 암호를 제공합니다.

```
# passwd -r files jandoe
New Password:          <Type password>
Re-enter new Password:      <Retype password>
passwd: password successfully changed for jandoe
#
```

마지막으로 root 사용자는 사용자 정의에 Security Administrator(보안 관리자) 역할을 추가합니다. 역할은 74 페이지 “Trusted Extensions의 보안 관리자 역할 만들기”에서 만들었습니다.

```
# usermod -R secadmin jandoe
```

▼ Trusted Extensions 역할 작동 확인

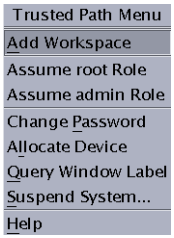
각 역할을 확인하려면 역할을 수락합니다. 그런 다음 해당 역할만 수행할 수 있는 작업을 수행합니다.

시작하기 전에 DNS 또는 라우팅을 구성한 경우 역할을 만들고 다시 부트한 후에 작동 여부를 확인해야 합니다.

1 각 역할에 대해 역할을 수락할 수 있는 사용자로 로그인합니다.

2 **Trusted Path(신뢰할 수 있는 경로) 메뉴를 엽니다.**

- **Trusted CDE에서 작업 공간 전환 영역을 누릅니다.**
- **Trusted JDS에서 신뢰할 수 있는 기호를 누릅니다.**



3 **메뉴에서 역할을 수락합니다.**

4 **역할 작업 공간에서 Solaris Management Console을 시작합니다.**

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

5 **테스트할 역할의 적절한 범위를 선택합니다.**

6 **System Services(시스템 서비스)를 누르고 Users(사용자)로 이동합니다.**
암호를 입력하라는 메시지가 표시됩니다.

a. **역할 암호를 입력합니다.**

b. **User Accounts(사용자 계정)를 두 번 누릅니다.**

7 **사용자를 누릅니다.**

- System Administrator(시스템 관리자) 역할은 General(일반), Home Directory(홈 디렉토리) 및 Group(그룹) 탭에서 필드를 수정할 수 있어야 합니다.
- Security Administrator(보안 관리자) 역할은 모든 탭에서 필드를 수정할 수 있어야 합니다.
- Primary Administrator(주 관리자) 역할은 모든 탭에서 필드를 수정할 수 있어야 합니다.

▼ 레이블이 있는 영역에 대한 사용자 로그인 허용

호스트가 다시 부트되면 장치와 기본 저장소 간의 연결을 다시 설정해야 합니다.

시작하기 전에 레이블이 있는 영역을 한 개 이상 만들었습니다. 해당 영역은 복제에 사용되지 않습니다.

1. **시스템을 다시 부트합니다.**
2. **root 사용자로 로그인합니다.**
3. **영역 서비스를 다시 시작합니다.**

```
# svcs zones
STATE          STIME    FMRI
offline        -        svc:/system/zones:default

# svcadm restart svc:/system/zones:default
```

4. **로그아웃합니다.**

   이제 일반 사용자가 로그인할 수 있습니다. 세션이 레이블이 있는 영역에 있습니다.

Trusted Extensions에서 홈 디렉토리 만들기

Trusted Extensions에서 사용자는 작업하는 모든 레이블에서 홈 디렉토리에 액세스할 수 있어야 합니다. 사용자가 모든 홈 디렉토리를 사용할 수 있게 하려면 다중 레벨 홈 디렉토리 서버를 만들고, 서버에서 자동 마운터를 실행한 다음 홈 디렉토리를 내보내야 합니다. 클라이언트 측에서 스크립트를 실행하여 각 사용자의 모든 영역에 대한 홈 디렉토리를 찾거나 사용자가 홈 디렉토리 서버에 로그인하도록 허용할 수 있습니다.

▼ Trusted Extensions에서 홈 디렉토리 서버 만들기

시작하기 전에 사용자가 수퍼유저이거나 root 역할 또는 Primary Administrator(주 관리자) 역할에 속해야 합니다.

1. **Trusted Extensions 소프트웨어를 사용하여 홈 디렉토리 서버를 설치하고 구성합니다.**
   - 영역을 복제하려면 비어 있는 홈 디렉토리가 있는 Solaris ZFS 스냅샷을 사용해야 합니다.
   - 사용자가 로그인할 수 있는 모든 레이블에는 홈 디렉토리가 필요하기 때문에 사용자가 로그인할 수 있는 모든 영역을 만듭니다. 예를 들어, 기본 label_encodings 파일을 사용할 경우 PUBLIC 레이블에 대한 영역을 만듭니다.

2 **UFS를 사용하고 Solaris ZFS는 사용하지 않을 경우 NFS 서버를 사용합니다.**

a. **전역 영역에서 `nsswitch.conf` 파일의 `automount` 항목을 수정합니다.**
신뢰할 수 있는 편집기를 사용하여 `/etc/nsswitch.conf` 파일을 편집합니다. 자세한 내용은 **Solaris Trusted Extensions Administrator's Procedures**의 "How to Edit Administrative Files in Trusted Extensions"를 참조하십시오.

```
automount: files
```

b. **전역 영역에서 `automount` 명령을 실행합니다.**

3 **레이블이 있는 모든 영역에 대해 Solaris Trusted Extensions Administrator's Procedures의 "How to NFS Mount Files in a Labeled Zone"에서 자동 마운트 절차를 수행합니다. 그런 다음 이 절차로 돌아갑니다.**

4 **홈 디렉토리가 만들어졌는지 확인합니다.**

a. **홈 디렉토리 서버에서 로그아웃합니다.**

b. **일반 사용자로 홈 디렉토리 서버에 로그인합니다.**

c. **로그인 영역에서 터미널을 엽니다.**

d. **단말기 창에서 사용자의 홈 디렉토리가 있는지 확인합니다.**

e. **사용자가 작업할 수 있는 모든 영역에 대해 작업 공간을 만듭니다.**

f. **각 영역에서 단말기 창을 열어 사용자의 홈 디렉토리가 있는지 확인합니다.**

5 **홈 디렉토리 서버에서 로그아웃합니다.**

▼ Trusted Extensions에서 사용자의 홈 디렉토리 액세스 허용

사용자는 처음에 홈 디렉토리 서버에 로그인하여 다른 시스템과 공유할 홈 디렉토리를 만들 수 있습니다.. 모든 레이블에서 홈 디렉토리를 만들려면 각 사용자는 모든 레이블에서 홈 디렉토리 서버에 로그인해야 합니다.

또는 관리자로 사용자가 처음 로그인하기 전에 각 사용자의 홈 시스템에서 홈 디렉토리에 대한 마운트 지점을 만들 스크립트를 작성할 수 있습니다. 스크립트는 사용자에게 작업이 허용되는 모든 레이블에서 마운트 지점을 만듭니다.

시작하기 전에 Trusted Extensions 도메인에 대한 홈 디렉토리 서버가 구성됩니다.

- **서버에 대한 직접 로그인을 허용할지, 아니면 스크립트를 실행할지 여부를 선택합니다.**
  - **사용자가 홈 디렉토리 서버에 직접 로그인할 수 있도록 합니다.**
    a. **각 사용자에게 홈 디렉토리 서버에 로그인하도록 지시합니다.**
       로그인한 후에 사용자는 로그아웃해야 합니다.
    b. **다시 로그인하고 이번에는 다른 로그인 레이블을 선택하도록 각 사용자에게 지시합니다.**
       사용자는 레이블 구축기를 사용하여 다른 로그인 레이블을 선택합니다. 로그인한 후에 사용자는 로그아웃해야 합니다.
    c. **사용이 허용된 모든 레이블에 대해 로그인 프로세스를 반복하도록 각 사용자에게 지시합니다.**
    d. **일반 워크스테이션에서 로그인하도록 지시합니다.**
       기본 레이블의 홈 디렉토리를 사용할 수 있습니다. 사용자가 세션의 레이블을 변경하거나 다른 레이블에 작업 공간을 추가한 경우 해당 레이블에 대한 사용자의 홈 디렉토리가 마운트됩니다.
  - **모든 사용자에 대해 홈 디렉토리 마운트 지점을 만드는 스크립트를 작성하고 스크립트를 실행합니다.**

```
#!/bin/sh
#
for zoneroot in `/usr/sbin/zoneadm list -p | cut -d ":" -f4` ; do
    if [ $zoneroot != / ]; then
        prefix=$zoneroot/root/export

        for j in `getent passwd|tr ' ' _` ; do
            uid=`echo $j|cut -d ":" -f3`
            if [ $uid -ge 100 ]; then
                gid=`echo $j|cut -d ":" -f4`
                homedir=`echo $j|cut -d ":" -f6`
                mkdir -m 711 -p $prefix$homedir
                chown $uid:$gid $prefix$homedir
            fi
        done
    fi
done
```

    a. **전역 영역의 NFS 서버에서 이 스크립트를 실행합니다.**
    b. **그런 다음 사용자가 로그인할 모든 다중 레벨 데스크탑에서 이 스크립트를 실행합니다.**

사용자 및 호스트를 기존의 신뢰할 수 있는 네트워크에 추가

NIS 맵에 정의된 사용자가 있는 경우에는 이 사용자를 네트워크에 추가할 수 있습니다.

호스트와 레이블을 호스트에 추가하려면 다음 절차를 참조하십시오.

- 호스트를 추가하려면 Solaris Management Console에 설정된 Computers and Networks(컴퓨터 및 네트워크) 도구를 사용합니다. 자세한 내용은 **Solaris Trusted Extensions Administrator's Procedures**의 "How to Add Hosts to the System's Known Network"를 참조하십시오.

  LDAP 서버에 호스트를 추가하는 경우 호스트와 연관된 모든 IP 주소를 추가합니다. 레이블이 있는 영역에 대한 주소를 포함하여 모든 영역 주소를 LDAP 서버에 추가해야 합니다.
- 호스트의 레이블을 지정하려면 **Solaris Trusted Extensions Administrator's Procedures**의 "How to Assign a Security Template to a Host or a Group of Hosts"를 참조하십시오.

▼ LDAP 서버에 NIS 사용자 추가

시작하기 전에 사용자가 수퍼유저이거나 `root` 역할 또는 Primary Administrator(주 관리자) 역할에 속해야 합니다.

1 NIS 데이터베이스에서 필요한 정보를 수집합니다.

a. `aliases` 데이터베이스의 사용자 항목에서 파일을 만듭니다.

```
% ypcat -k aliases | grep login-name > aliases.name
```

b. `passwd` 데이터베이스의 사용자 항목에서 파일을 만듭니다.

```
% ypcat -k passwd | grep "Full Name" > passwd.name
```

c. `auto_home_` 데이터베이스의 사용자 항목에서 파일을 만듭니다.

```
% ypcat -k auto_home | grep login-name > auto_home_label
```

2 LDAP 및 Trusted Extensions 정보를 재포맷합니다.

a. `sed` 명령을 사용하여 `aliases` 항목을 다시 포맷합니다.

```
% sed 's/ /:/g' aliases.login-name > aliases
```

b. `nawk` 명령을 사용하여 `passwd` 항목을 다시 포맷합니다.

```
% nawk -F: '{print $1":x:"$3":"$4":"$5":"$6":"$7}' passwd.name > passwd
```

c. `nawk` 명령을 사용하여 `shadow` 항목을 재포맷합니다.

```
% nawk -F: '{print $1":"$2":6445::::::"}' passwd.name > shadow
```

d. nawk 명령을 사용하여 user_attr 항목을 만듭니다.

```
% nawk -F: '{print $1"::::lock_after_retries=yes-or-no;profiles=user-profile, ...;
labelview=int-or-ext,show-or-hide;min_label=min-label;
clearance=max-label;type=normal;roles=role-name,...;
auths=auth-name,..."}' passwd.name > user_attr
```

3 수정된 파일을 LDAP 서버의 /tmp 디렉토리에 복사합니다.

```
# cp aliases auto_home_internal passwd shadow user_attr /tmp/name
```

4 단계 3의 파일 항목을 LDAP 서버의 데이터베이스에 추가합니다.

```
# /usr/sbin/ldapaddent -D "cn=directory manager" -w DM-password \
-a simple -f /tmp/name/aliases aliases
# /usr/sbin/ldapaddent -D "cn=directory manager" -w DM-password \
-a simple -f /tmp/name/auto_home_internal auto_home_internal
# /usr/sbin/ldapaddent -D "cn=directory manager" -w DM-password \
-a simple -f /tmp/name/passwd passwd
# /usr/sbin/ldapaddent -D "cn=directory manager" -w DM-password \
-a simple -f /tmp/name/shadow shadow
# /usr/sbin/ldapaddent -D "cn=directory manager" -w DM-password \
-a simple -f /tmp/name/user_attr user_attr
```

예 4–6 NIS 데이터베이스에서 LDAP 서버로 사용자 추가

다음 예에서는 관리자가 신뢰할 수 있는 네트워크에 새 사용자를 추가합니다. 사용자의 정보는 원래 NIS 데이터베이스에 저장됩니다. LDAP 서버 암호를 보호하려면 관리자가 ldapaddent 명령을 서버에서 실행합니다.

Trusted Extensions에서 새 사용자는 장치를 할당하고 Operator(운영자) 역할을 수락합니다. 사용자가 역할을 수락할 수 있기 때문에 사용자 계정은 잠기지 않습니다. 사용자의 최소 레이블은 PUBLIC입니다. 사용자가 작업하는 레이블은 INTERNAL이므로 jan이 auto_home_internal 데이터베이스에 추가됩니다. auto_home_internal 데이터베이스는 읽기/쓰기 권한으로 jan의 홈 디렉토리를 자동 마운트합니다.

- LDAP 서버에서 관리자는 NIS 데이터베이스에서 사용자 정보를 추출합니다.

```
# ypcat -k aliases | grep jan.doe > aliases.jan
# ypcat passwd | grep "Jan Doe" > passwd.jan
# ypcat -k auto_home | grep jan.doe > auto_home_internal
```

- 그런 다음 관리자는 LDAP에 대한 항목을 다시 포맷합니다.

```
# sed 's/ /:/g' aliases.jan > aliases
# nawk -F: '{print $1":x:"$3":"$4":"$5":"$6":"$7}' passwd.jan > passwd
# nawk -F: '{print $1":"$2":6445::::::"}' passwd.jan > shadow
```

- 그런 다음 관리자는 Trusted Extensions에 대한 user_attr 항목을 만듭니다.

```
# nawk -F: '{print $1"::::lock_after_retries=no;profiles=Media User;
labelview=internal,showsl;min_label=0x0002-08-08;
clearance=0x0004-08-78;type=normal;roles=oper;
auths=solaris.device.allocate"}' passwd.jan > user_attr
```

- 그런 다음 관리자는 파일을 /tmp/jan 디렉토리에 복사합니다.

```
# cp aliases auto_home_internal passwd shadow user_attr /tmp/jan
```

- 마지막으로 관리자는 서버를 /tmp/jan 디렉토리의 파일로 채웁니다.

```
# /usr/sbin/ldapaddent -D "cn=directory manager" -w a2b3c4d5e6 \
-a simple -f /tmp/jan/aliases aliases
# /usr/sbin/ldapaddent -D "cn=directory manager" -w a2b3c4d5e6 \
-a simple -f /tmp/jan/auto_home_internal auto_home_internal
# /usr/sbin/ldapaddent -D "cn=directory manager" -w a2b3c4d5e6 \
-a simple -f /tmp/jan/passwd passwd
# /usr/sbin/ldapaddent -D "cn=directory manager" -w a2b3c4d5e6 \
-a simple -f /tmp/jan/shadow shadow
# /usr/sbin/ldapaddent -D "cn=directory manager" -w a2b3c4d5e6 \
-a simple -f /tmp/jan/user_attr user_attr
```

Trusted Extensions 구성 문제 해결

Trusted Extensions에서 레이블이 있는 영역은 전역 영역을 통해 X 서버와 통신합니다. 따라서 레이블이 있는 영역은 전역 영역에 대해 사용 가능한 경로가 있어야 합니다. 또한 Solaris 설치 중에 선택한 옵션으로 인해 Trusted Extensions에서 전역 영역에 대한 인터페이스를 사용하지 못할 수 있습니다.

Trusted Extensions 설치 후 netservices limited가 실행됨

설명:

Trusted Extensions 패키지를 추가하기 전에 netservices limited 명령을 실행하는 대신 패키지를 추가한 후에 전역 영역에서 명령을 실행했습니다. 따라서 레이블이 있는 영역에서 전역 영역의 X 서버에 연결할 수 없습니다.

해결 방법:

다음 명령을 실행하여 Trusted Extensions에서 영역 간의 통신에 필요한 서비스를 엽니다.

```
# svccfg -s x11-server setprop options/tcp_listen = true
# svcadm enable svc:/network/rpc/rstat:default
```

레이블이 있는 영역에서 콘솔 창을 열 수 없음

설명:

레이블이 있는 영역에서 콘솔 창을 열려고 시도하면 대화 상자에 다음과 같은 오류가 표시됩니다.

```
Action:DttermConsole,*,*,*,0 [Error]
Action not authorized.
```

해결 방법:

`/etc/security/exec_attr` 파일의 각 영역 항목에 다음 두 줄이 있는지 확인합니다.

```
All Actions:solaris:act:::*;*;*;*;*:
All:solaris:act:::*;*;*;*;*:
```

이 줄이 없는 경우 해당 항목을 추가하는 Trusted Extensions 패키지가 레이블이 있는 영역에 설치되어 있지 않은 것입니다. 이 경우에는 레이블이 있는 영역을 다시 만듭니다. 절차는 57 페이지 "레이블이 있는 영역 만들기"를 참조하십시오.

레이블이 있는 영역에서 X 서버에 액세스할 수 없음

설명:

레이블이 있는 영역에서 X 서버에 액세스할 수 없는 경우 다음과 같은 메시지가 표시될 수 있습니다.

- `Action failed. Reconnect to Solaris Zone?(`**작업에 실패했습니다. Solaris 영역에 다시 연결하시겠습니까?**`)`
- `No route available(`**사용 가능한 경로 없음**`)`
- `Cannot reach globalzone(`**전역 영역에 연결할 수 없음**`)-`*hostname* `:0`

원인:

레이블이 있는 영역에서 X 서버에 액세스할 수 없는 원인은 다음과 같습니다.

- 영역이 초기화되지 않고 `sysidcfg` 프로세스가 완료될 때까지 대기하고 있습니다.
- 레이블이 있는 영역의 호스트 이름이 전역 영역에서 실행되는 이름 지정 서비스에서 인식되지 않습니다.
- `all-zones`로 지정된 인터페이스가 없습니다.
- 레이블이 있는 영역의 네트워크 인터페이스의 작동이 중지되었습니다.
- LDAP 이름을 조회하지 못했습니다.
- NFS 마운트가 작동하지 않습니다.

해결 단계:

다음을 수행합니다.

1. 영역에 로그인합니다.

   `zlogin` 명령 또는 Zone Terminal Console(영역 터미널 콘솔) 작업을 사용할 수 있습니다.

   ```
   # zlogin -z zone-name
   ```

   수퍼유저로 로그인할 수 없는 경우 `zlogin -S` 명령을 사용하여 인증을 생략합니다.
2. 영역이 실행 중인지 확인합니다.

   ```
   # zoneadm list
   ```

   영역이 `running` 상태인 경우에는 해당 영역에서 하나 이상의 프로세스가 실행되고 있는 것입니다.
3. 레이블이 있는 영역에서 X 서버에 액세스하지 못하게 하는 모든 문제를 해결합니다.
   - `sysidcfg` 프로세스를 완료하여 영역을 초기화합니다.

     `sysidcfg` 프로그램을 대화식으로 실행합니다. `zlogin` 명령을 실행했던 단말기 창 또는 Zone Terminal Console(영역 터미널 콘솔)에서 프롬프트에 응답합니다.

     `sysidcfg` 프로세스를 비대화식으로 실행하기 위해 다음 중 하나를 수행할 수 있습니다.
     - `/usr/sbin/txzonemgr` 스크립트에서 Initialize(초기화) 항목을 지정합니다.

       Initialize(초기화) 항목을 사용하여 `sysidcfg` 질문에 기본값을 입력할 수 있습니다.
     - 사용자가 직접 `sysidcfg` 스크립트를 작성합니다.

       자세한 내용은 `sysidcfg(4)` 매뉴얼 페이지를 참조하십시오.
   - 영역에서 X 서버를 사용할 수 있는지 확인합니다.

     레이블이 있는 영역에 로그인합니다. `DISPLAY` 변수가 X 서버를 가리키도록 설정하고 창을 엽니다.

     ```
     # DISPLAY=global-zone-hostname:n.n
     # export DISPLAY
     # /usr/openwin/bin/xclock
     ```

     레이블이 있는 창이 나타나지 않으면 해당 레이블이 있는 영역에 대한 영역 네트워킹이 제대로 구성되지 않은 것입니다.
   - 이름 지정 서비스를 사용하여 영역의 호스트 이름을 구성합니다.

영역의 로컬 /etc/hosts 파일이 사용되고 있지 않습니다. 대신 전역 영역 또는 LDAP 서버에서 관련 정보를 지정해야 합니다. 정보에는 영역에 할당되는 호스트 이름의 IP 주소가 포함되어야 합니다.

- all-zones로 지정된 인터페이스가 없습니다.

  모든 영역이 전역 영역과 동일한 서브넷의 IP 주소를 사용하는 경우가 아니면 all-zones(공유) 인터페이스를 구성해야 할 수 있습니다. 이 구성을 사용하면 레이블이 있는 영역에서 전역 영역의 X 서버에 연결할 수 있습니다. 전역 영역 X 서버에 대한 원격 연결을 제한하려면 vni0을 all-zones 주소로 사용할 수 있습니다.

  all-zones 인터페이스를 구성하지 **않으려면** 각 영역에 대해 전역 영역 X 서버의 경로를 제공해야 합니다. 이 경로는 전역 영역에서 구성해야 합니다.
- 레이블이 있는 영역의 네트워크 인터페이스의 작동이 중지되었습니다.

  ```
  # ifconfig -a
  ```

  ifconfig 명령을 사용하여 레이블이 있는 영역의 네트워크 인터페이스가 UP 및 RUNNING 상태인지 확인합니다.
- LDAP 이름을 조회하지 못했습니다.

  ldaplist 명령을 사용하여 각 영역에서 LDAP 서버 또는 LDAP 프록시 서버와 통신할 수 있는지 확인합니다. LDAP 서버에서 영역이 tnrhdb 데이터베이스에 나열되는지 확인합니다.
- NFS 마운트가 작동하지 않습니다.

  수퍼유저로 영역에서 automount를 다시 시작합니다. 또는 crontab 항목을 추가하여 automount 명령을 5분마다 실행합니다.

추가 Trusted Extensions 구성 작업

다음 두 작업을 수행하여 구성 파일의 정확한 복사본을 사이트의 모든 Trusted Extensions 시스템에 전송할 수 있습니다. 마지막 작업에서는 Solaris 시스템에서 Trusted Extensions 사용자 정의를 제거할 수 있습니다.

▼ Trusted Extensions에서 이동식 매체에 파일을 복사하는 방법

이동식 매체에 복사할 경우 정보의 민감도 레이블을 사용하여 매체의 레이블을 지정합니다.

주 – 설치하는 동안 수퍼유저 또는 이와 동등한 역할의 사용자가 이동식 매체로 또는 이동식 매체에서 관리 파일을 복사합니다. 매체 레이블을 `Trusted Path`로 지정합니다.

시작하기 전에 관리 파일을 복사하려면 사용자가 수퍼유저이거나 전역 영역의 역할에 속해야 합니다.

1. **해당 장치를 할당합니다.**

   Device Allocation Manager(장치 할당 관리자)를 사용하고 손상되지 않은 매체를 넣습니다. 자세한 내용은 **Solaris Trusted Extensions 사용 설명서**의 "Trusted Extensions에서 장치를 할당하는 방법"를 참조하십시오.

   - Solaris Trusted Extensions(CDE)에서 *File Manager(***파일 관리자***)*에 이동식 매체의 내용이 표시됩니다.
   - Solaris Trusted Extensions(JDS)에서 *File Browser(***파일 브라우저***)*에 내용이 표시됩니다.

   이 절차에서 File Manager(파일 관리자)는 이 GUI를 참조하는 데 사용됩니다.

2. **두 번째 File Manager(파일 관리자)를 엽니다.**

3. **복사할 파일이 있는 폴더로 이동합니다.**

   예를 들어, 파일을 `/export/clientfiles` 폴더에 복사했을 수 있습니다.

4. **각 파일에 대해서 다음을 수행합니다.**

   a. **파일에 대한 아이콘을 강조 표시합니다.**

   b. **파일을 이동식 매체에 대한 File Manager(파일 관리자)로 끕니다.**

5. **장치를 할당 해제합니다.**

   자세한 내용은 **Solaris Trusted Extensions 사용 설명서**의 "Trusted Extensions에서 장치를 할당 해제하는 방법"를 참조하십시오.

6. **이동식 매체에 대한 File Manager(파일 관리자)의 File(파일) 메뉴에서 Eject(꺼내기)를 선택합니다.**

주 – 복사된 파일의 민감도 레이블을 사용하여 매체에 레이블을 물리적으로 추가합니다.

예 4–7 구성 파일을 모든 시스템에서 동일하게 유지

시스템 관리자는 모든 시스템을 동일한 설정으로 구성하려고 합니다. 따라서 구성되는 첫 번째 시스템에서는 재부트 중에 삭제할 수 없는 디렉토리를 만듭니다. 관리자는 모든 시스템에서 동일하거나 유사한 파일을 해당 디렉토리에 넣습니다.

예를 들어, Solaris Management Console에서 LDAP 범위 `/var/sadm/smc/toolboxes/tsol_ldap/tsol_ldap.tbx`에 사용하는 Trusted Extensions 도구 상자를 복사합니다. `tnrhtp` 파일에서 원격 호스트 템플리트를 사용자 정의했으며, DNS 서버 목록과 감사 구성 파일이 있습니다. 또한 사이트에 대한 `policy.conf` 파일을 수정했습니다. 따라서 파일을 영구 디렉토리에 복사합니다.

```
# mkdir /export/commonfiles
# cp  /etc/security/policy.conf \
/etc/security/audit_control \
/etc/security/audit_startup \
/etc/security/tsol/tnrhtp \
/etc/resolv.conf \
/etc/nsswitch.conf \
/export/commonfiles
```

Device Allocation Manager(장치 할당 관리자)를 사용하여 전역 영역에서 디스켓을 할당하고 이 파일을 디스켓으로 전송합니다. 레이블이 `ADMIN_HIGH`인 개별 디스켓에 사이트에 대한 `label_encodings` 파일을 넣습니다.

파일을 시스템에 복사할 때 해당 시스템의 `/etc/security/audit_control` 파일에서 `dir:` 항목을 수정합니다.

▼ Trusted Extensions에서 이동식 매체의 파일을 복사하는 방법

파일을 바꾸기 전에 원본 Trusted Extensions 파일의 이름을 변경해도 안전합니다. 시스템을 구성할 때 `root` 역할은 관리 파일의 이름을 변경하고 이 파일을 복사합니다.

시작하기 전에 관리 파일을 복사하려면 사용자가 수퍼유저이거나 전역 영역의 역할에 속해야 합니다.

1. **해당 장치를 할당합니다.**

   자세한 내용은 **Solaris Trusted Extensions 사용 설명서**의 "Trusted Extensions에서 장치를 할당하는 방법"를 참조하십시오.

   - Solaris Trusted Extensions(CDE)에서 *File Manager(***파일 관리자***)*에 이동식 매체의 내용이 표시됩니다.
   - Solaris Trusted Extensions(JDS)에서 *File Browser(***파일 브라우저***)*에 내용이 표시됩니다.

   이 절차에서 File Manager(파일 관리자)는 이 GUI를 참조하는 데 사용됩니다.

2. **관리 파일이 들어 있는 매체를 삽입합니다.**

3. **시스템에 동일한 이름을 가진 파일이 있는 경우 원본 파일을 새 이름으로 복사합니다.**
   예를 들어, `.orig`를 원본 파일의 끝에 추가합니다.

   ```
   # cp /etc/security/tsol/tnrhtp /etc/security/tsol/tnrhtp.orig
   ```

4. **File Manager(파일 관리자)를 엽니다.**

5. **원하는 대상 디렉토리(예: `/etc/security/tsol`)로 이동합니다.**

6. **복사할 각 파일에 대해 다음을 수행합니다.**

   a. **마운트된 매체의 File Manager(파일 관리자)에서 해당 파일의 아이콘을 강조 표시합니다.**

   b. **그런 다음 파일을 두 번째 File Manager(파일 관리자)의 대상 디렉토리로 끕니다.**

7. **장치를 할당 해제합니다.**
   자세한 내용은 **Solaris Trusted Extensions 사용 설명서**의 "Trusted Extensions에서 장치를 할당 해제하는 방법"를 참조하십시오.

8. **메시지가 표시되면 매체를 꺼내서 제거합니다.**

예 4–8 Trusted Extensions에서 감사 구성 파일 로드

이 예에서는 역할이 시스템에서 아직 구성되어 있지 않습니다. `root` 사용자는 구성 파일을 이동식 매체에 복사해야 합니다. 그러면 매체의 내용이 다른 시스템에 복사됩니다. 이 파일은 Trusted Extensions 소프트웨어에서 구성되는 각 시스템에 복사됩니다.

`root` 사용자는 Device Allocation Manager(장치 할당 관리자)에서 `floppy_0` 장치를 할당하고 마운트 쿼리에 `yes`로 응답합니다. 그런 다음 `root` 사용자는 구성 파일이 있는 디스켓을 넣고 해당 파일을 디스크에 복사합니다. 디스켓의 레이블이 `Trusted Path`로 지정됩니다.

매체에서 읽으려면 `root` 사용자는 수신 호스트에서 장치를 할당하고 내용을 다운로드합니다.

구성 파일이 테이프에 있는 경우 `root` 사용자는 `mag_0` 장치를 할당합니다. 구성 파일이 CD-ROM에 있는 경우 `root` 사용자는 `cdrom_0` 장치를 할당합니다.

▼ 시스템에서 Trusted Extensions를 제거하는 방법

Solaris 시스템에서 Trusted Extensions를 제거하려면 특정 단계를 수행하여 Solaris 시스템에서 Trusted Extensions 사용자 정의를 제거합니다.

1. **Solaris OS에서와 같이 레이블이 있는 영역에서 보관할 데이터를 모두 아카이브합니다.**

2. **레이블이 있는 영역을 시스템에서 제거합니다.**

   자세한 내용은 **System Administration Guide: Solaris Containers-Resource Management and Solaris Zones**의 "How to Remove a Non-Global Zone"을 참조하십시오.

3. **시스템에서 Trusted Extensions 패키지를 제거합니다.**

   - **설치 마법사를 사용하여 Trusted Extensions 패키지를 추가한 경우 제거 마법사를 사용합니다.**

     마법사는 `/var/sadm/tx` 디렉토리에 있습니다.

     ```
     # cd /var/sadm/tx
     # java uninstall_Solaris_Trusted_Extensions
     ```

     또한 `prodreg` 명령을 사용할 수 있습니다. 자세한 내용은 `prodreg(1M)` 명령을 참조하십시오.

   - **`pkgadd` 명령을 사용하여 Trusted Extensions 패키지를 추가한 경우 `pkgrm` 명령을 사용합니다.**

     자세한 내용은 `pkgrm(1M)` 매뉴얼 페이지를 참조하십시오.

4. **`bsmunconv` 명령을 실행합니다.**

   이 명령으로 인한 결과는 `bsmunconv(1M)` 매뉴얼 페이지를 참조하십시오.

5. **(옵션) 시스템을 다시 부트합니다.**

6. **시스템을 구성합니다.**

   Solaris 시스템에 대한 다양한 서비스를 구성해야 할 수 있습니다. 대상 서비스에는 감사, 기본 네트워크, 이름 지정 서비스 및 파일 시스템 마운트가 포함됩니다.

◆ ◆ ◆ 5 장

5 Trusted Extensions에 대해 LDAP 구성(작업)

이 장에서는 Solaris Trusted Extensions와 함께 사용하기 위해 Sun Java™ System Directory Server 및 Solaris Management Console을 구성하는 방법에 대해 설명합니다. Directory Server는 LDAP 서비스를 제공합니다. LDAP는 Trusted Extensions에서 지원되는 이름 지정 서비스입니다. Solaris Management Console은 로컬 및 LDAP 데이터베이스의 관리 GUI입니다.

Directory Server를 구성하는 경우에는 두 가지 옵션이 있습니다. Trusted Extensions 시스템에서 LDAP 서버를 구성할 수도 있고, Trusted Extensions 프록시 서버를 통해 기존 서버에 연결함으로써 기존 서버를 사용할 수도 있습니다. 다음 작업 맵 중 **하나**의 지침을 따릅니다.

- 96 페이지 “Trusted Extensions 호스트에서 LDAP 서버 구성(작업 맵)”
- 96 페이지 “Trusted Extensions 호스트에서 LDAP 프록시 서버 구성(작업 맵)”

Trusted Extensions 호스트에서 LDAP 서버 구성(작업 맵)

작업	설명	수행 방법
Trusted Extensions LDAP 서버를 설정합니다.	기존 Sun Java System Directory Server가 없는 경우 첫 번째 Trusted Extensions 시스템을 Directory Server로 만듭니다. 다른 Trusted Extensions 시스템은 이 서버의 클라이언트입니다.	97 페이지 “LDAP용 Directory Server에 대한 정보 수집” 98 페이지 “Sun Java System Directory Server 설치” 100 페이지 “Sun Java System Directory Server의 액세스 로그 보호” 102 페이지 “Sun Java System Directory Server의 오류 로그 보호” 103 페이지 “Sun Java System Directory Server용 다중 레벨 포트 구성”
Trusted Extensions 데이터베이스를 서버에 추가합니다.	LDAP 서버를 Trusted Extensions 시스템 파일의 데이터로 채웁니다.	104 페이지 “Sun Java System Directory Server 채우기”
Directory Server와 작동하도록 Solaris Management Console을 구성합니다.	Solaris Management Console에 대한 LDAP 도구 상자를 수동으로 설정합니다. 도구 상자를 사용하여 네트워크 객체에 대한 Trusted Extensions 속성을 수정할 수 있습니다.	106 페이지 “LDAP에 대해 Solaris Management Console 구성(작업 맵)”
다른 모든 Trusted Extensions 시스템을 이 서버의 클라이언트로 구성합니다.	다른 시스템을 Trusted Extensions와 함께 구성할 때는 시스템을 이 LDAP 서버의 클라이언트로 만듭니다.	55 페이지 “Trusted Extensions에서 전역 영역을 LDAP 클라이언트로 만들기”

Trusted Extensions 호스트에서 LDAP 프록시 서버 구성(작업 맵)

Solaris 시스템에서 실행 중인 기존 Sun Java System Directory Server가 있는 경우 이 작업 맵을 사용합니다.

작업	설명	수행 방법
Trusted Extensions 데이터베이스를 서버에 추가합니다.	Trusted Extensions 네트워크 데이터베이스 `tnrhdb` 및 `tnrhtp`를 LDAP 서버에 추가해야 합니다.	104 페이지 “Sun Java System Directory Server 채우기”

작업	설명	수행 방법
LDAP 프록시 서버를 설정합니다.	하나의 Trusted Extensions 시스템을 다른 Trusted Extensions 시스템에 대한 프록시 서버로 만듭니다. 다른 Trusted Extensions 시스템에서는 이 프록시 서버를 사용하여 LDAP 서버에 연결합니다.	106 페이지 “LDAP 프록시 서버 만들기”
LDAP용 다중 레벨 포트를 포함하도록 프록시 서버를 구성합니다.	특정 레이블에서 LDAP 서버와 통신하도록 Trusted Extensions 프록시 서버를 활성화합니다.	103 페이지 “Sun Java System Directory Server용 다중 레벨 포트 구성”
LDAP 프록시 서버에서 작동하도록 Solaris Management Console을 구성합니다.	Solaris Management Console에 대해 LDAP 도구 상자를 수동으로 설정합니다. 도구 상자를 사용하여 네트워크 객체에 대한 Trusted Extensions 속성을 수정할 수 있습니다.	106 페이지 “LDAP에 대해 Solaris Management Console 구성(작업 맵)”
다른 모든 Trusted Extensions 시스템을 LDAP 프록시 서버의 클라이언트로 구성합니다.	다른 시스템을 Trusted Extensions와 함께 구성할 때는 시스템을 이 LDAP 프록시 서버의 클라이언트로 만듭니다.	55 페이지 “Trusted Extensions에서 전역 영역을 LDAP 클라이언트로 만들기”

Trusted Extensions 시스템에서 Sun Java System Directory Server 구성

LDAP 이름 지정 서비스는 Trusted Extensions에서 지원되는 이름 지정 서비스입니다. 사이트에서 아직 LDAP 이름 지정 서비스가 실행되고 있지 않은 경우 Trusted Extensions로 구성된 시스템에서 Sun Java System Directory Server(Directory Server)를 구성합니다. 사이트에서 이미 Directory Server가 실행되고 있는 경우 서버에 Trusted Extensions 데이터베이스를 추가해야 합니다. Directory Server에 액세스하려면 시스템에 LDAP 프록시를 설정합니다.

주 – 이 LDAP 서버를 NFS 서버 또는 Sun Ray™ 클라이언트에 대한 서버로 사용하지 않는 경우 이 서버에 레이블이 있는 영역을 설치할 필요가 없습니다.

▼ LDAP용 Directory Server에 대한 정보 수집

- **다음 항목의 값을 결정합니다.**

  항목은 Sun Java Enterprise System Install Wizard에 나타나는 순서대로 나열됩니다.

설치 마법사 프롬프트	작업 또는 정보
Sun Java System Directory Server *version*	
Administrator User ID(관리자 아이디)	기본값은 `admin`입니다.
Administrator Password(관리자 비밀번호)	`admin123`과 같은 비밀번호를 만듭니다.
Directory Manager DN(디렉토리 관리자 DN)	기본값은 `cn=Directory Manager`입니다.
Directory Manager Password(디렉토리 관리자 비밀번호)	`dirmgr89`와 같은 비밀번호를 만듭니다.
Directory Server Root(디렉토리 서버 루트)	기본값은 `/var/Sun/mps`입니다. 프록시 소프트웨어가 설치된 경우 이 경로는 나중에도 사용됩니다.
Server Identifier(서버 식별자)	기본값은 로컬 시스템입니다.
Server Port(서버 포트)	Directory Server를 사용하여 클라이언트 시스템에 대한 표준 LDAP 이름 지정 서비스를 제공하려면 기본값 `389`를 사용합니다. Directory Server를 사용하여 이후의 프록시 서버 설치를 지원하려면 `10389`와 같은 비표준 포트를 입력합니다.
Suffix(접미어)	`dc=example-domain,dc=com`에서와 같이 도메인 구성 요소를 포함합니다.
Administration Domain(관리 도메인)	`example-domain.com`에서와 같이 Suffix(접미어)에 일치하도록 구성합니다.
System User(시스템 사용자)	기본값은 `root`입니다.
System Group(시스템 그룹)	기본값은 `root`입니다.
Data Storage Location(데이터 저장소 위치)	기본값은 `Store configuration data on this server`(**구성 데이터를 이 서버에 저장합니다**)입니다.
Data Storage Location(데이터 저장소 위치)	기본값은 `Store user data and group data on this server`(**사용자 데이터와 그룹 데이터를 이 서버에 저장합니다**)입니다.
Administration Port(관리 포트)	기본값은 Server Port(서버 포트)입니다. 기본값 변경을 위해 제안된 규칙은 `software-version TIMES 1000`입니다. 소프트웨어 버전 5.2의 경우 이 규칙은 포트 `5200`이 됩니다.

▼ Sun Java System Directory Server 설치

Directory Server 패키지는 Sun Software Gateway 웹 사이트 (`http://www.sun.com/software/solaris`)에서 구할 수 있습니다.

1 **Sun 웹 사이트에서 Sun Java System Directory Server 패키지를 찾습니다.**

   a. **Sun Software Gateway (`http://www.sun.com/software/solaris`) 페이지에서 Get It(얻기) 탭을 누릅니다.**

   b. **Sun Java Identity Management Suite(Sun Java Identity Management 제품군)의 확인란을 누릅니다.**

   c. **Submit(제출) 버튼을 누릅니다.**

   d. **등록하지 않은 경우 등록합니다.**

   e. **로그인하여 소프트웨어를 다운로드합니다.**

   f. **화면 왼쪽 위에서 Download Center(다운로드 센터)를 누릅니다.**

   g. **Identity Management 아래에서 사용자의 플랫폼에 맞는 최신 소프트웨어를 다운로드합니다.**

2 **`/etc/hosts` 파일에서 시스템의 호스트 이름 항목에 FQDN을 추가합니다.**

   FQDN은 Fully Qualified Domain Name(정규화된 도메인 이름)의 약어로 다음과 같이 호스트 이름과 관리 도메인의 조합입니다.

   ```
   192.168.5.5 myhost myhost.example-domain.com
   ```

3 **Directory Server 패키지를 설치합니다.**

   97 페이지 “LDAP용 Directory Server에 대한 정보 수집”의 정보를 사용하여 질문에 답합니다.

4 **부트할 때마다 Directory Server가 시작되는지 확인합니다.**

   a. **`init.d` 스크립트를 추가합니다.**

      다음 예에서는 `SERVER_ROOT` 및 `SERVER_INSTANCE` 변수를 사용자의 설치에 맞게 변경합니다.

      ```
      /etc/init.d/ldap.directory-myhost
      ---------------------------------------
      #!/sbin/sh

      SERVER_ROOT=/var/Sun/mps
      SERVER_INSTANCE=myhost

      case "$1" in
      start)
      ${SERVER_ROOT}/slapd-${SERVER_INSTANCE}/start-slapd
      ;;
      ```

```
stop)

${SERVER_ROOT}/slapd-${SERVER_INSTANCE}/stop-slapd
;;
*)

echo "Usage: $0 { start | stop }"
exit 1
esac
exit 0
```

b. init.d 스크립트를 rc2.d 디렉토리에 연결합니다.

```
/usr/bin/ln \
/etc/init.d/ldap.directory-myhost \
/etc/rc2.d/S70ldap.directory-myhost
```

5 설치를 확인합니다.

a. 설치 디렉토리를 검사합니다.

이름이 slapd-*server-hostname*인 하위 디렉토리가 있어야 합니다.

b. Directory Server를 시작할 수 있어야 합니다.

```
# installation-directory/slapd-server-hostname/restart-slapd
```

c. slapd 프로세스가 있는지 확인합니다.

```
# ps -ef | grep slapd
./ns-slapd -D installation-directory/slapd-server-instance -i
installation-directory/slapd-server-instance/
```

일반 오류 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.

▼ Sun Java System Directory Server의 액세스 로그 보호

이 절차를 통해 작성되는 LDIF 스크립트는 액세스 로그에 대해 다음 규칙을 설정합니다.

- 로그 수준 256의 로그 이벤트로, 버퍼 로그를 작성합니다(기본값).
- 로그는 매일 회전됩니다.
- 로그 파일 수를 최대 100개로 유지하고각 파일의 크기는 최대 500MB를 넘지 않도록 합니다.
- 3개월 이상 된 로그 파일은 만료됩니다.
- 빈 디스크 공간이 500MB 미만이 되면 가장 오래된 로그를 삭제합니다.

- 모든 로그 파일은 최대 20,000MB의 디스크 공간을 사용합니다.

1 스크립트를 만들어 액세스 로그를 관리합니다.

다음 내용이 있는 /var/tmp/logs-access.ldif 파일을 만듭니다.

```
dn: cn=config
changetype: modify
replace: nsslapd-accesslog-logging-enabled
nsslapd-accesslog-logging-enabled: on
-
replace: nsslapd-accesslog-level
nsslapd-accesslog-level: 256
-
replace: nsslapd-accesslog-logbuffering
nsslapd-accesslog-logbuffering: on
-
replace: nsslapd-accesslog-logrotationtime
nsslapd-accesslog-logrotationtime: 1
-
replace: nsslapd-accesslog-logrotationtimeunit
nsslapd-accesslog-logrotationtimeunit: day
-
replace: nsslapd-accesslog-maxlogsize
nsslapd-accesslog-maxlogsize: 500
-
replace: nsslapd-accesslog-maxlogsperdir
nsslapd-accesslog-maxlogsperdir: 100
-
replace: nsslapd-accesslog-logexpirationtime
nsslapd-accesslog-logexpirationtime: 3
-
replace: nsslapd-accesslog-logexpirationtimeunit
nsslapd-accesslog-logexpirationtimeunit: month
-
replace: nsslapd-accesslog-logmaxdiskspace
nsslapd-accesslog-logmaxdiskspace: 20000
-
replace: nsslapd-accesslog-logminfreediskspace
nsslapd-accesslog-logminfreediskspace: 500
```

2 스크립트를 실행합니다.

```
# ldapmodify -h localhost -D 'cn=directory manager' \
-f /var/tmp/logs-access.ldif
```

3 비밀번호를 입력합니다.

```
Enter bind password:      Type the appropriate password
modifying entry cn=config
```

▼ Sun Java System Directory Server의 오류 로그 보호

이 절차로 작성되는 LDIF 스크립트는 오류 로그에 대해 다음 규칙을 설정합니다.

- 로그는 매주 회전됩니다.
- 로그 파일 수를 최대 30개로 유지하고각 파일의 크기는 최대 500MB를 넘지 않도록 합니다.
- 3개월 이상 된 로그 파일은 만료됩니다.
- 빈 디스크 공간이 500MB 미만이 되면 가장 오래된 로그를 삭제합니다.
- 모든 로그 파일은 최대 20,000MB의 디스크 공간을 사용합니다.

1 스크립트를 만들어 오류 로그를 관리합니다.

다음 내용이 있는 `/var/tmp/logs-error.ldif` 파일을 만듭니다.

```
dn: cn=config
changetype: modify
replace: nsslapd-errorlog-logging-enabled
nsslapd-errorlog-logging-enabled: on
-
replace: nsslapd-errorlog-logexpirationtime
nsslapd-errorlog-logexpirationtime: 3
-
replace: nsslapd-errorlog-logexpirationtimeunit
nsslapd-errorlog-logexpirationtimeunit: month
-
replace: nsslapd-errorlog-logrotationtime
nsslapd-errorlog-logrotationtime: 1
-
replace: nsslapd-errorlog-logrotationtimeunit
nsslapd-errorlog-logrotationtimeunit: week
-
replace: nsslapd-errorlog-maxlogsize
nsslapd-errorlog-maxlogsize: 500
-
replace: nsslapd-errorlog-maxlogsperdir
nsslapd-errorlog-maxlogsperdir: 30
-
replace: nsslapd-errorlog-logmaxdiskspace
nsslapd-errorlog-logmaxdiskspace: 20000
-
replace: nsslapd-errorlog-logminfreediskspace
nsslapd-errorlog-logminfreediskspace: 500
```

2 스크립트를 실행합니다.

```
# ldapmodify -h localhost -D 'cn=directory manager' -f
/var/tmp/logs-error.ldif
```

3 **프롬프트에 대답합니다.**

```
Enter bind password:      Type the appropriate password
modifying entry cn=config
```

▼ Sun Java System Directory Server용 다중 레벨 포트 구성

Trusted Extensions에서 작업하려면 Directory Server의 서버 포트가 전역 영역에서 다중 레벨 포트(MLP)로 구성되어야 합니다.

1 **Solaris Management Console을 시작합니다.**

```
# /usr/sbin/smc &
```

2 **이 컴퓨터(*this-host*: `Scope=Files, Policy=TSOL`) 도구 상자를 선택합니다.**

3 **System Configuration(시스템 구성)을 누른 다음 Computers and Networks(컴퓨터 및 네트워크)를 누릅니다.**

암호를 입력하라는 메시지가 표시됩니다.

4 **적절한 암호를 입력합니다.**

5 **Trusted Network Zones(신뢰할 수 있는 네트워크 영역)를 두 번 누릅니다.**

6 **전역 영역을 두 번 누릅니다.**

7 **TCP 프로토콜에 대해 다중 레벨 포트를 추가합니다.**

a. **Add for the Multilevel Ports for Zone's IP Addresses(영역 IP 주소에 대해 다중 레벨 포트 추가)를 누릅니다.**

b. **포트 번호로 389를 입력하고 OK(확인)를 누릅니다.**

8 **UDP 프로토콜에 대해 다중 레벨 포트를 추가합니다.**

a. **Add for the Multilevel Ports for Zone's IP Addresses(영역 IP 주소에 대해 다중 레벨 포트 추가)를 누릅니다.**

b. **포트 번호로 389를 입력합니다.**

c. **udp 프로토콜을 선택하고 OK(확인)를 누릅니다.**

9 **확인을 눌러 설정을 저장합니다.**

10 커널을 업데이트합니다.

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

▼ Sun Java System Directory Server 채우기

몇 개의 LDAP 데이터베이스가 레이블 구성, 사용자 및 원격 시스템에 대한 Trusted Extensions 데이터를 보관할 수 있도록 작성되거나 수정되었습니다. 이 절차에서는 Directory Server 데이터베이스에 Trusted Extensions 정보를 채웁니다.

1 이름 지정 서비스 데이터베이스를 채우는 데 사용할 파일의 스테이징 영역을 만듭니다.

```
# mkdir -p /setup/files
```

2 샘플 /etc 파일을 스테이징 영역에 복사합니다.

```
# cd /etc
# cp aliases group hosts networks netmasks protocols /setup/files
# cp rpc services auto_master /setup/files

# cd /etc/security
# cp auth_attr prof_attr exec_attr /setup/files/
#
# cd /etc/security/tsol
# cp tnrhdb tnrhtp /setup/files
```

패치 없이 Solaris 10 11/06 릴리스를 실행하는 경우 ipnodes 파일을 복사합니다.

```
# cd /etc/inet
# cp ipnodes /setup/files
```

3 /setup/files/auto_master 파일에서 +auto_master 항목을 제거합니다.

4 ?:::::? 항목을 /setup/files/auth_attr 파일에서 제거합니다.

5 :::: 항목을 /setup/files/prof_attr 파일에서 제거합니다.

6 단계화 영역에서 영역 자동맵을 만듭니다.

다음 자동맵 목록에서 각 쌍의 첫 번째 줄에는 파일 이름이 표시됩니다. 각 쌍의 두 번째 줄에는 파일 내용이 표시됩니다. 영역 이름은 Trusted Extensions 소프트웨어와 함께 제공된 기본 label_encodings 파일에서 레이블을 식별합니다.

- 사용자의 영역 이름이 이 줄의 영역 이름을 대체합니다.
- *myNFSserver*는 홈 디렉토리에 대한 NFS 서버를 식별합니다.

```
/setup/files/auto_home_public
 * myNFSserver_FQDN:/zone/public/root/export/home/&
```

```
/setup/files/auto_home_internal
 * myNFSserver_FQDN:/zone/internal/root/export/home/&

/setup/files/auto_home_needtoknow
 * myNFSserver_FQDN:/zone/needtoknow/root/export/home/&

/setup/files/auto_home_restricted
 * myNFSserver_FQDN:/zone/restricted/root/export/home/&
```

7 네트워크의 모든 시스템을 /setup/files/tnrhdb 파일에 추가합니다.

이 파일에는 와일드카드 메커니즘을 사용할 수 없습니다. 레이블이 있는 영역의 IP 주소를 포함하여 연결하는 모든 시스템의 IP 주소가 이 파일에 **있어야 합니다**.

a. 신뢰할 수 있는 편집기를 열고 /setup/files/tnrhdb를 편집합니다.

b. Trusted Extensions 도메인에서 레이블이 있는 시스템의 모든 IP 주소를 추가합니다.

레이블이 있는 시스템은 cipso 유형입니다. 또한 레이블이 있는 시스템의 보안 템플리트 이름은 cipso입니다. 따라서 기본 구성에서 cipso 항목은 다음과 비슷합니다.

```
192.168.25.2:cipso
```

주 – 이 목록에는 전역 영역과 레이블이 있는 영역의 IP 주소가 포함됩니다.

---

c. 도메인이 통신할 수 있는 레이블이 없는 모든 시스템을 추가합니다.

레이블이 없는 시스템 unlabeled 유형입니다. 레이블이 없는 시스템의 보안 템플리트 이름은 admin_low입니다. 따라서 기본 구성에서 레이블이 없는 시스템의 항목은 다음과 비슷합니다.

```
192.168.35.2:admin_low
```

d. 파일을 저장하고 편집기를 종료합니다.

e. 파일 구문을 확인합니다.

```
# tnchkdb -h /setup/files/tnrhdb
```

f. 계속하기 전에 오류를 수정합니다.

8 /setup/files/tnrhdb 파일을 /etc/security/tsol/tnrhdb 파일로 복사합니다.

9 ldapaddent 명령을 사용하여 스테이징 영역의 모든 파일을 채웁니다.

```
# /usr/sbin/ldapaddent -D "cn=directory manager" \
-w dirmgr123 -a simple -f /setup/files/hosts hosts
```

기존 Sun Java System Directory Server에 대한 Trusted Extensions 프록시 만들기

먼저 Trusted Extensions 데이터베이스를 Solaris 시스템의 기존 Directory Server에 추가해야 합니다. 그런 다음 Trusted Extensions 시스템에서 Directory Server에 액세스할 수 있도록 활성화한 후 하나의 Trusted Extensions 시스템을 LDAP 프록시 서버로 설정합니다.

▼ LDAP 프록시 서버 만들기

사이트에 이미 LDAP 서버가 있는 경우 Trusted Extensions 시스템에서 프록시 서버를 만듭니다.

시작하기 전에 Trusted Extensions 정보가 포함된 데이터베이스를 LDAP 서버에 추가했습니다. 자세한 내용은 104 페이지 "Sun Java System Directory Server 채우기"를 참조하십시오.

1. **Trusted Extensions로 구성된 시스템에서 프록시 서버를 만듭니다.**

   자세한 내용은 **System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)**의 12 장, "Setting Up LDAP Clients (Tasks)"를 참조하십시오.

2. **프록시 서버에서 Trusted Extensions 데이터베이스를 볼 수 있는지 확인합니다.**

   ```
   # ldaplist -l database
   ```

일반 오류 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.

LDAP에 대해 Solaris Management Console 구성(작업 맵)

Solaris Management Console은 Trusted Extensions가 실행되고 있는 시스템의 네트워크를 관리하기 위한 GUI입니다.

작업	설명	수행 방법
Solaris Management Console을 초기화합니다.	Solaris Management Console을 초기화합니다. 이 절차는 전역 영역에서 시스템당 한 번 수행됩니다.	52 페이지 "Trusted Extensions에서 Solaris Management Console 서버 초기화"
자격 증명을 등록합니다.	LDAP 서버에서 Solaris Management Console을 인증합니다.	107 페이지 "Solaris Management Console에 LDAP 자격 증명 등록"

작업	설명	수행 방법
시스템에서 LDAP 관리를 활성화합니다.	기본적으로, LDAP 관리는 설치할 때 해제되어 있습니다. 특정 시스템이 LDAP 관리 시스템이 되도록 명시적으로 활성화합니다.	108 페이지 “LDAP 클라이언트에서 LDAP 관리 활성화”
LDAP 도구 상자를 만듭니다.	Solaris Management Console에서 Trusted Extensions용 LDAP 도구 상자를 만듭니다.	108 페이지 “Solaris Management Console에서 LDAP 도구 상자 편집”
통신을 확인합니다.	Trusted Extensions 호스트가 LDAP 클라이언트가 될 수 있는지 확인합니다.	55 페이지 “Trusted Extensions에서 전역 영역을 LDAP 클라이언트로 만들기”

▼ Solaris Management Console에 LDAP 자격 증명 등록

시작하기 전에 Trusted Extensions가 실행되고 있는 LDAP 서버의 `root` 사용자여야 합니다. 프록시 서버를 서버로 사용할 수 있습니다.

Sun Java System Directory Server를 구성해야 합니다. 다음 구성 중 하나를 완료했습니다.

- 96 페이지 “Trusted Extensions 호스트에서 LDAP 서버 구성(작업 맵)”
- 96 페이지 “Trusted Extensions 호스트에서 LDAP 프록시 서버 구성(작업 맵)”

1 LDAP 관리 자격 증명을 등록합니다.

```
# /usr/sadm/bin/dtsetup storeCred
Administrator DN:       Type the value for cn on your system
Password:       Type the Directory Manager password
Password (confirm):       Retype the password
```

2 Directory Server와의 통신을 확인합니다.

```
# /usr/sadm/bin/dtsetup scopes
Getting list of manageable scopes...
Scope 1 file:       Displays name of file scope
Scope 2 ldap:       Displays name of ldap scope
```

LDAP 서버 설정에 따라 나열되는 LDAP 범위가 결정됩니다. 서버를 등록한 후에는 LDAP 도구 상자를 편집한 다음 사용할 수 있습니다.

예 5–1 LDAP 자격 증명 등록

이 예에서 LDAP 서버의 이름은 `LDAP1`이고 LDAP 클라이언트의 이름은 `myhost`이며, `cn`의 값은 기본값인 `Directory Manager`입니다.

```
# /usr/sadm/bin/dtsetup storeCred
Administrator DN:cn=Directory Manager
Password:abcde1;!
Password (confirm):abcde1;!
# /usr/sadm/bin/dtsetup scopes
```

```
Getting list of manageable scopes...
Scope 1 file:/myhost/myhost
Scope 2 ldap:/myhost/cd=myhost,dc=example,dc=com
```

▼ LDAP 클라이언트에서 LDAP 관리 활성화

기본적으로 시스템은 보안 위험이 있는 포트는 수신하지 않도록 설치됩니다. 따라서 LDAP 서버와의 네트워크 통신을 명시적으로 설정해야 합니다. 이 절차는 시스템 및 사용자의 네트워크를 관리하려고 하는 시스템에서만 수행합니다.

시작하기 전에 사용자는 수퍼유저이거나 전역 영역에서 보안 관리자 역할을 가진 사용자여야 합니다.

- **시스템에서 LDAP를 관리하도록 활성화합니다.**

  ```
  # svccfg -s wbem setprop options/tcp_listen=true
  ```

  LDAP 도구 상자를 보려면 108 페이지 “Solaris Management Console에서 LDAP 도구 상자 편집”을 완료해야 합니다.

▼ Solaris Management Console에서 LDAP 도구 상자 편집

시작하기 전에 사용자는 수퍼유저여야 합니다. Solaris Management Console에 LDAP 자격 증명을 반드시 등록해야 하며,`/usr/sadm/bin/dtsetup scopes` 명령 출력을 꼭 알아야 합니다. 자세한 내용은 107 페이지 “Solaris Management Console에 LDAP 자격 증명 등록”을 참조하십시오.

1. **LDAP 도구 상자를 찾습니다.**

   ```
   # cd /var/sadm/smc/toolboxes/tsol_ldap
   # ls *tbx
   tsol_ldap.tbx
   ```

2. **LDAP 서버 이름을 제공합니다.**

   a. **신뢰할 수 있는 편집기를 엽니다.**

   b. **`tsol_ldap.tbx` 도구 상자의 전체 경로 이름을 복사하여 편집기에 인수로 붙여 넣습니다.**

      예를 들어 다음 경로는 LDAP 도구 상자의 기본 위치입니다.

      ```
      /var/sadm/smc/toolboxes/tsol_ldap/tsol_ldap.tbx
      ```

c. 범위 정보를 교체합니다.

<Scope> 및 </Scope> 태그 사이의 server 태그를 ldap:/..... 라인(/usr/sadm/bin/dtsetup scopes 명령)의 출력으로 교체합니다.

```
<Scope>ldap:/<myhost>/<dc=domain,dc=suffix></Scope>
```

d. <?server?> 또는 <?server ?>의 모든 인스턴스를 LDAP 서버로 교체합니다.

```
<Name> ldap-server-name: Scope=ldap, Policy=TSOL</Name>
services and configuration of ldap-server-name.</Description>
and configuring ldap-server-name.</Description>
<ServerName>ldap-server-name</ServerName>
<ServerName>ldap-server-name</ServerName>
```

e. 파일을 저장하고 편집기를 종료합니다.

3 wbem 서비스를 중지한 후 시작합니다.

smc 데몬은 wbem 서비스에서 제어합니다.

```
# svcadm disable wbem
# svcadm enable wbem
```

예 5–2 LDAP 도구 상자 구성

이 예에서 LDAP 서버의 이름은 LDAP1입니다. 도구 상자를 구성하려면 관리자는 server의 인스턴스를 LDAP1로 바꿉니다.

```
<Name>LDAP1: Scope=ldap, Policy=TSOL</Name>
services and configuration of LDAP1.</Description>
and configuring LDAP1.</Description>
<ServerName>LDAP1</ServerName>
<ServerName>LDAP1</ServerName>
```

▼ Solaris Management Console에 Trusted Extensions 정보가 포함되는지 확인

시작하기 전에 관리 역할 또는 수퍼유저로 LDAP 클라이언트에 로그인해야 합니다. 시스템을 LDAP 클라이언트로 만들려면 55 페이지 “Trusted Extensions에서 전역 영역을 LDAP 클라이언트로 만들기”를 참조하십시오.

LDAP 도구 상자를 사용하려면 108 페이지 “Solaris Management Console에서 LDAP 도구 상자 편집” 및 52 페이지 “Trusted Extensions에서 Solaris Management Console 서버 초기화”를 완료해야 합니다.

1 Solaris Management Console을 시작합니다.

```
# /usr/sbin/smc &
```

2 **Trusted Extensions 도구 상자를 엽니다.**

Trusted Extensions 도구 상자에 `Policy=TSOL` 값이 있습니다.

- **로컬 파일에 액세스할 수 있는지 확인하려면 이 컴퓨터(*this-host*:`Scope=Files, Policy=TSOL`) 도구 상자를 엽니다.**
- **LDAP 서버의 데이터베이스에 액세스할 수 있는지 확인하려면 이 컴퓨터(*this-host*:`Scope=LDAP, Policy=TSOL`) 도구 상자를 엽니다.**

3 **System Configuration(시스템 구성) 아래에서 Computers and Networks(컴퓨터 및 네트워크)로 이동한 다음 Security Templates(보안 템플리트)로 이동합니다.**

4 **올바른 템플리트와 레이블이 원격 시스템에 적용되었는지 확인합니다.**

일반 오류 LDAP 구성 문제를 해결하려면 **System Administration Guide: Naming and Directory Services (DNS, NIS, and LDAP)**의 13 장, "LDAP Troubleshooting (Reference)"을 참조하십시오.

◆ ◆ ◆ 6 장

6 Trusted Extensions로 헤드리스 시스템 구성(작업)

Netra™ 시리즈와 같은 헤드리스 시스템에서 Solaris Trusted Extensions 소프트웨어를 구성하고 관리하려면 모니터가 있는 시스템에서 같은 작업을 수행할 때와는 다른 절차가 필요합니다. Trusted Extensions 소프트웨어는 관리 책임을 역할로 나누며, 이러한 역할은 원격으로 수락할 수 없습니다. 이 소프트웨어는 관리 GUI도 제공합니다. 직렬 라인에서는 GUI가 표시되지 않습니다.

주 – 헤드리스 시스템에 필요한 구성 방법은 평가된 구성의 조건을 만족시키지 않습니다. 자세한 내용은 18 페이지 “사이트 보안 정책의 이해”를 참조하십시오.

Trusted Extensions에서 헤드리스 시스템 구성(작업 맵)

헤드리스 시스템에서 직렬 라인을 통해 콘솔을 터미널 에뮬레이터 창에 연결합니다. 이 라인은 일반적으로 `tip` 명령을 통해 고정됩니다. 사용 가능한 두 번째 시스템의 유형에 따라 다음 방법 중 하나를 사용하여 헤드리스 시스템을 구성할 수 있습니다. 다음 표의 작업 3에는 가장 선호되는 방법부터 순서대로 나열되어 있습니다.

작업	설명	수행 방법
1. 헤드리스 시스템을 `cipso` 시스템으로 식별합니다.	헤드리스 시스템을 구성할 데스크탑 시스템이 Trusted Extensions와 함께 구성된 경우 헤드리스 시스템의 호스트 유형을 `cipso`로 만듭니다.	신뢰할 수 있는 네트워크의 헤드리스 시스템 부분을 아직 만들지 않은 경우 적절한 보안 템플리트를 시스템에 할당합니다. **Solaris Trusted Extensions Administrator’s Procedures**의 “How to Assign a Security Template to a Host or a Group of Hosts”를 참조하십시오.
2. 원격 로그인을 사용 가능하게 합니다.	수퍼유저가 헤드리스 시스템에 원격으로 로그인할 수 있게 합니다.	112 페이지 “Trusted Extensions에서 원격 로그인 활성화”

작업	설명	수행 방법
3. 헤드리스 시스템을 설정할 구성 및 관리 방법을 선택합니다. 헤드리스 시스템과 통신하는 두 번째 시스템에서 사용할 수 있는 하드웨어와 소프트웨어를 기반으로 선택합니다. 선택 사항은 간편성 및 보안에 따라 내림차순으로 나열됩니다.	rlogin 명령을 사용하여 한 역할 내에서 원격 시스템을 관리합니다.	원격 시스템을 관리하는 역할을 수락하려면 114 페이지 "rlogin 명령을 사용하여 Trusted Extensions에서 헤드리스 시스템에 로그인"으로 이동합니다.
	ssh 명령을 사용하여 수퍼유저로 원격 시스템을 관리합니다.	원격 시스템을 수퍼유저로 관리하려면 116 페이지 "ssh 명령을 사용하여 Trusted Extensions에서 헤드리스 시스템에 로그인"으로 이동합니다.
	윈도우화 시스템이 없으면 직렬 로그인을 사용할 수 있습니다. 이 절차는 안전하지 않습니다.	직렬 로그인을 사용하여 헤드리스 시스템을 구성하고 관리하려면 117 페이지 "Trusted Extensions에서 직렬 로그인으로 관리 설정"으로 이동합니다.
4. 헤드리스 시스템에서 Trusted Extensions를 구성합니다.	로그인되면 모니터 있는 시스템에서 하는 것과 동일하게 구성을 계속합니다.	4 장, "Trusted Extensions 구성(작업)"을 참조하고 선택한 로그인 방법에 따라 가능한 방법을 사용합니다.

▼ Trusted Extensions에서 원격 로그인 활성화

rlogin 또는 ssh 명령을 사용하여 헤드리스 시스템을 관리해야 하는 **경우에만** 이 절차를 수행하십시오. 이 절차는 안전하지 않습니다.

구성 오류는 원격으로 디버그할 수 있습니다.

시작하기 전에 보안 정책을 검토하여 사이트에서 허용되는 원격 로그인 방법을 결정합니다. 데스크탑 시스템 및 헤드리스 시스템은 동일한 보안 템플리트를 사용하는 것으로 서로를 식별해야 합니다.

1. **콘솔 장치를 통해 root 계정에 로그인합니다.**
2. **원격 로그인의 다음 방법 중 하나 이상을 활성화하도록 선택합니다.**
   - **root 사용자의 원격 로그인을 사용 가능하게 합니다.**
     a. **/etc/default/login 파일의 CONSOLE= 행을 주석 처리합니다.**

        ```
        #CONSOLE=/dev/console
        ```

     b. **ssh 서비스에 대해 root 사용자 로그인을 허용합니다.**

        /etc/ssh/sshd_config 파일을 수정합니다. 기본적으로 ssh는 Solaris 시스템에서 활성화되어 있습니다.

        ```
        PermitRootLogin yes
        ```

- **역할이 rlogin 서비스를 사용하여 로그인하도록 허용합니다.**
  root가 역할인 경우 root 역할로 원격 로그인하려면 이러한 수정이 필요합니다.

  a. **텍스트 편집기에서 pam.conf 파일을 엽니다.**

     ```
     # vi /etc/pam.conf
     ```

  b. **파일 끝으로 이동하면서 other account requisite를 찾습니다.**

  c. **allow_remote를 역할 모듈에 추가합니다.**
     필드 사이를 이동할 때는 Tab 키를 사용합니다.

     ```
     other account requisite      pam_roles.so.1        allow_remote
     ```

     편집 후 이 섹션은 다음과 유사합니다.

     ```
     other account requisite      pam_roles.so.1        allow_remote
     other account required       pam_unix_account.so.1
     other account required       pam_tsol_account.so.1
     ```

- **레이블이 없는 호스트에서 전역 영역으로 원격 로그인을 활성화합니다.**

  a. **텍스트 편집기에서 pam.conf 파일을 엽니다.**

     ```
     # vi /etc/pam.conf
     ```

  b. **파일 끝으로 이동하면서 other account requisite를 찾습니다.**

  c. **allow_unlabeled를 tsol_account 모듈에 추가합니다.**
     필드 사이를 이동할 때는 Tab 키를 사용합니다.

     ```
     other account required       pam_tsol_account.so.1 allow_unlabeled
     ```

     편집 후 이 섹션은 다음과 유사합니다.

     ```
     other account requisite      pam_roles.so.1        allow_remote
     other account required       pam_unix_account.so.1
     other account required       pam_tsol_account.so.1 allow_unlabeled
     ```

- **특정 사용자가 전역 영역에 로그인할 수 있도록 활성화합니다.**
  이러한 사용자에게 관리 레이블 범위를 할당합니다. 데스크탑의 사용자 이름은 헤드리스 시스템의 사용자 이름과 같아야 합니다.

  ```
  # usermod -R root -K min_label=ADMIN_LOW -K clearance=ADMIN_LOW username
  ```

3 **헤드리스 시스템에서 데스크탑의 호스트 유형을 정의합니다.**

데스크탑 시스템의 호스트 유형과 헤드리스 시스템의 호스트 유형은 일치해야 합니다. 이 임시 정의를 만들려면 `tnctl` 명령을 사용합니다. 자세한 내용은 `tnctl(1M)` 매뉴얼 페이지를 참조하십시오.

- **레이블이 있는 데스크탑 시스템에 대해 호스트 유형을 `cipso`로 정의합니다.**

  ```
  # tnctl -h desktop-IP-address:cipso
  ```

- **레이블이 없는 데스크탑 시스템의 경우 호스트 유형을 `ADMIN_LOW`에서 실행되는 레이블이 없는 시스템으로 정의합니다.**

  ```
  # tnctl -h desktop-IP-address:admin_low
  ```

▼ `rlogin` 명령을 사용하여 Trusted Extensions에서 헤드리스 시스템에 로그인

이 절차에서는 역할 수락을 통해 명령줄 및 Trusted Extensions GUI를 사용하여 헤드리스 시스템을 관리할 수 있습니다.

시작하기 전에 헤드리스 시스템에는 Solaris Management Console을 사용할 충분한 메모리가 있어야 합니다. 요구 사항은 Solaris OS의 요구 사항과 같습니다. 자세한 내용은 **Solaris 10 11/06 설치 설명서: 기본 설치**의 "시스템 요구 사항 및 권장 사항"를 참조하십시오.

관리자의 데스크탑 시스템이 Trusted Extensions와 함께 구성되어 있는 경우 헤드리스 시스템은 데스크탑 시스템에서 CIPSO 시스템으로 식별됩니다. 자세한 내용은 **Solaris Trusted Extensions Administrator's Procedures**의 "How to Assign a Security Template to a Host or a Group of Hosts"를 참조하십시오.

112 페이지 "Trusted Extensions에서 원격 로그인 활성화"를 완료했습니다.

사용자는 헤드리스 시스템에 로그인할 수 있는 사용자입니다.

1 **데스크탑 시스템에서 헤드리스 시스템의 프로세스가 표시되도록 합니다.**

a. **헤드리스 시스템이 X 서버에 액세스할 수 있도록 합니다.**

```
desktop $ xhost + headless-host
```

b. **데스크탑의 `DISPLAY` 변수 값을 확인합니다.**

```
desktop $ echo $DISPLAY
:n.n
```

2 Trusted Extensions 데스크탑 시스템에서 Trusted Path(신뢰할 수 있는 경로) 작업 공간을 엽니다.

- **사용자 계정에 전역 영역에 대한 직접 액세스 권한이 있는 경우 Trusted Path(신뢰할 수 있는 경로) 작업 공간을 만들고 터미널 창을 엽니다.**
- **사용자 계정에 전역 영역에 대한 직접 액세스 권한이 없는 경우 역할을 수락한 다음 터미널 창을 엽니다.**

3 이 터미널 창에서 헤드리스 시스템에 원격으로 로그인합니다.

desktop `# rlogin` *headless*
`Password:` *Type the headless user's password*

4 역할을 수락합니다.

헤드리스 시스템에 권한 없는 사용자로 로그인한 경우 관리 권한이 있는 역할을 수락합니다. 같은 터미널 창을 사용합니다. 예를 들어 `root` 역할을 수락합니다.

headless `$ su - root`
`Password:` *Type the root password*

이제 사용자가 전역 영역에 있습니다.

5 헤드리스 시스템의 프로세스가 데스크탑 시스템에 표시될 수 있도록 합니다.

headless `$ setenv DISPLAY` *desktop*`:`*n*`.`*n*
headless `$ export DISPLAY=`*n*`:`*n*

이제 Trusted Extensions GUI를 사용하여 헤드리스 시스템을 관리할 수 있습니다.

6 헤드리스 시스템을 관리합니다.

- **Solaris Management Console을 시작합니다.**

  headless `$` **`/usr/sbin/smc &`**

  Solaris Management Console이 데스크탑 시스템에 표시됩니다. 도구 상자 목록에서 헤드리스 시스템에 대해 `Scope=Files`, `Policy=TSOL`을 선택합니다.

- `txzonemgr`**을 시작합니다.**

  headless `$` **`/usr/sbin/txzonemgr`**

- **Trusted CDE 작업에 액세스합니다.**

  headless `# /usr/dt/bin/dtappsession` *desktop*
  `Password:` *Type the remote password*

▼ ssh 명령을 사용하여 Trusted Extensions에서 헤드리스 시스템에 로그인

이 절차에서는 명령줄을 사용하여 수퍼유저로 헤드리스 시스템을 관리할 수 있습니다. Trusted Extensions GUI를 사용하려면 114 페이지 "rlogin 명령을 사용하여 Trusted Extensions에서 헤드리스 시스템에 로그인"에서 원격 표시를 위한 단계를 완료합니다.

시작하기 전에 헤드리스 시스템에는 Solaris Management Console을 사용할 충분한 메모리가 있어야 합니다. 요구 사항은 Solaris OS의 요구 사항과 같습니다. 자세한 내용은 **Solaris 10 11/06 설치 설명서: 기본 설치**의 "시스템 요구 사항 및 권장 사항"를 참조하십시오.

관리자의 데스크탑 시스템이 Trusted Extensions와 함께 구성되어 있는 경우 헤드리스 시스템은 데스크탑 시스템에서 CIPSO 시스템으로 식별됩니다. 자세한 내용은 **Solaris Trusted Extensions Administrator's Procedures**의 "How to Assign a Security Template to a Host or a Group of Hosts"를 참조하십시오.

112 페이지 "Trusted Extensions에서 원격 로그인 활성화"를 완료했습니다.

사용자는 헤드리스 시스템에 로그인할 수 있는 사용자입니다.

1. **Trusted Extensions 데스크탑 시스템에서 Trusted Path(신뢰할 수 있는 경로) 작업 공간을 엽니다.**

   - **사용자 계정에 전역 영역에 대한 직접 액세스 권한이 있는 경우 Trusted Path(신뢰할 수 있는 경로) 작업 공간을 만들고 터미널 창을 엽니다.**
   - **사용자 계정에 전역 영역에 대한 직접 액세스 권한이 없는 경우 역할을 수락한 다음 터미널 창을 엽니다.**

2. **이 터미널 창에서 헤드리스 시스템에 원격으로 로그인합니다.**

   ```
   desktop $ ssh -l username-on-headless  headless
   Password:       Type the headless user's password
   headless $
   ```

   이제 터미널 창에 헤드리스 시스템의 작업이 표시됩니다.

3. **수퍼유저가 됩니다.**

   헤드리스 시스템에서 전역 영역에 있지 않은 경우 같은 터미널 창에서 사용자를 root로 전환합니다.

   ```
   headless $ su - root
   Password:       Type the root password
   ```

   이제 명령줄을 사용하여 헤드리스 시스템을 관리할 수 있습니다.

관리 GUI를 사용하여 시스템을 관리하려면 헤드리스 시스템의 프로세스가 데스크탑에 표시되도록 합니다. 자세한 내용은 114 페이지 “rlogin 명령을 사용하여 Trusted Extensions에서 헤드리스 시스템에 로그인”을 참조하십시오.

예 6–1 헤드리스 시스템의 원격 관리 설정

이 예제에서 관리자는 레이블이 있는 데스크탑 시스템에서 레이블이 없는 헤드리스 시스템을 설정합니다. Solaris OS에서처럼 관리자는 X 서버가 데스크탑 시스템에 액세스할 수 있도록 하고 헤드리스 시스템에서 DISPLAY 변수를 설정합니다.

```
TXdesk1 $ xhost + TXnohead4
TXdesk1 $ whoami
config1
TXdesk1 $ uname -n ; echo $DISPLAY
TXdesk1
:1.0

TXdesk1 $ ssh -l install1 TXnohead4
Password: Ins1PwD1
TXnohead4 $
```

전역 영역에서 관리자는 DISPLAY 변수를 설정합니다.

```
TXnohead4 # su -
Password: abcd1EFG
TXnohead4 # setenv DISPLAY TXdesk1:1.0
TXnohead4 # export DISPLAY=TXdesk1:1.0
```

그런 다음 관리자는 Solaris Management Console을 시작합니다.

```
TXnohead4 # /usr/sbin/smc &
```

마지막으로 관리자는 This Computer (TXnohead: Scope=Files, Policy=TSOL) 도구 상자를 선택합니다.

▼ Trusted Extensions에서 직렬 로그인으로 관리 설정

헤드리스 시스템을 구성하는 데 사용할 데스크탑 시스템이 없는 **경우에만** 이 절차를 수행하십시오. 이 절차는 안전하지 않습니다.

시작하기 전에 헤드리스 시스템의 단일 사용자 모드에서 수퍼유저여야 합니다. 어느 정도 보안을 유지하려면 시스템을 구성하는 동안 두 사람이 있어야 합니다.

1 직렬 포트를 할당합니다.

자세한 내용은 **Solaris Trusted Extensions Administrator’s Procedures**의 “Managing Devices in Trusted Extensions (Task Map)”를 참조하십시오.

2 수퍼유저로 시스템을 관리합니다.

◆ ◆ ◆ 부 록 A

사이트 보안 정책

이 부록에서는 사이트 보안 정책 문제를 설명하고 자세한 내용을 볼 수 있는 참조 서적 및 웹 사이트를 소개합니다.

보안 정책 생성 및 관리

각 Solaris Trusted Extensions 사이트는 고유하며 자체 보안 정책을 결정해야 합니다. 보안 정책을 만들고 관리할 때 다음 작업을 수행합니다.

- 보안 팀을 구축합니다. 보안 팀은 최고 경영진, 인력 관리 부서, 컴퓨터 시스템 관리 부서 및 관리자, 시설 관리 부서 등의 대표로 구성되어야 합니다. 보안 팀은 Trusted Extensions 관리자의 정책과 절차를 검토하고 모든 시스템 사용자에게 적용되는 일반 보안 정책을 권장해야 합니다.
- 경영진 및 관리 담당자를 대상으로 사이트 보안 정책에 대한 교육을 실시합니다. 사이트 관리와 관련된 모든 직원을 대상으로 보안 정책에 대한 교육을 실시해야 합니다. 보안 정책 정보에는 컴퓨터 시스템 보안과 직접적으로 관련된 내용이 포함되어 있으므로 이 보안 정책을 일반 사용자에게 공개하지 마십시오.

- 사용자를 대상으로 Trusted Extensions 소프트웨어 및 보안 정책에 대한 교육을 실시합니다. 모든 사용자는 **Solaris Trusted Extensions 사용 설명서**의 내용을 숙지해야 합니다. 시스템이 정상적으로 작동하지 않는 경우 대개 사용자가 가장 먼저 알게 되므로 사용자는 시스템에 익숙해져야 하고 시스템 관리자에게 모든 문제를 보고해야 합니다. 안전한 환경을 위해서 사용자는 다음과 같은 문제를 발견하는 즉시 시스템 관리자에게 알려야 합니다.
  - 각 세션을 시작할 때 보고되는 마지막 로그인 시간이 일치하지 않음
  - 파일 데이터가 비정상적으로 변경됨
  - 사람이 판독 가능한 인쇄 출력이 손실되거나 도난됨
  - 사용자 기능을 작동할 수 없음
- 보안 정책을 적용합니다. 보안 정책을 따르지 않거나 적용하지 않으면 Trusted Extensions로 구성된 시스템에 포함된 데이터가 보안되지 않습니다. 모든 문제 및 문제 해결을 위해 수행한 조치를 기록하기 위한 절차를 설정해야 합니다.
- 보안 정책을 주기적으로 검토합니다. 보안 팀은 보안 정책을 정기적으로 검토하고 마지막 검토 이후 발생한 모든 문제를 정기적으로 검토해야 합니다. 정책을 조정하여 보안을 강화할 수 있습니다.

사이트 보안 정책 및 Trusted Extensions

보안 관리자는 사이트의 보안 정책을 기반으로 Trusted Extensions 네트워크를 설계해야 합니다. 보안 정책은 다음과 같은 구성 관련 의사 결정을 제어합니다.

- 모든 사용자에 대해 수행되는 감사의 정도 및 감사가 수행되는 이벤트 클래스
- 역할 내의 사용자에 대해 수행되는 감사의 정도 및 감사가 수행되는 이벤트 클래스
- 감사 데이터 관리, 아카이브 및 검토 방법
- 시스템에 사용되는 레이블 및 일반 사용자에게 `ADMIN_LOW` 및 `ADMIN_HIGH` 레이블을 표시할지 여부
- 개인에게 할당되는 사용자 클리어런스
- 할당할 수 있는 장치(있는 경우) 및 할당을 수행할 수 있는 일반 사용자
- 시스템, 프린터 및 기타 장치에 대해 정의된 레이블 범위
- Trusted Extensions가 평가된 구성에서 사용되는지 여부

컴퓨터 보안 권장 사항

사이트의 보안 정책을 개발할 때 다음 지침 목록을 고려하십시오.

- Trusted Extensions로 구성된 시스템의 최대 레이블이 사이트에서 수행되는 작업의 최대 보안 수준을 넘지 않도록 할당합니다.
- 시스템 재부트, 전원 장애 및 종료를 사이트 로그에 수동으로 기록합니다.
- 파일 시스템 손상을 문서화하고 영향을 받는 모든 파일에 대해 잠재적인 보안 정책 위반을 분석합니다.
- 작동 설명서 및 관리자 설명서는 해당 정보에 대한 액세스가 필요한 개인에게만 액세스를 허용합니다.
- Trusted Extensions 소프트웨어의 비정상적이거나 예기치 않은 동작을 보고 및 문서화하며 원인을 파악합니다.
- 가능한 경우 Trusted Extensions로 구성된 관리자 시스템에 최소 두 명의 개인을 할당합니다. 한 사람에게는 보안과 관련한 의사 결정을 위한 보안 관리자 권한을 할당합니다. 다른 사람에게는 시스템 관리 작업을 위한 시스템 관리 권한을 할당합니다.
- 정기 백업 루틴을 설정합니다.
- 권한은 해당 권한이 필요하고 적절하게 사용할 것으로 신뢰할 수 있는 사람에게만 할당합니다.
- 프로그램에서 해당 작업을 수행하는 데 권한이 필요하고 프로그램의 권한 사용에 대한 신뢰성을 검토하여 입증된 경우에만 프로그램에 권한을 할당합니다. 기존 Trusted Extensions 프로그램에 대한 권한을 검토하여 새 프로그램에 대한 권한 설정의 지침으로 사용합니다.
- 감사 정보를 정기적으로 검토 및 분석합니다. 불규칙적인 이벤트는 조사를 통해 이벤트의 원인을 파악합니다.
- 관리 ID의 수를 최소화합니다.
- setuid 및 setgid 프로그램의 수를 최소화합니다. 이러한 프로그램은 보호된 하위 시스템에서만 사용해야 합니다.
- 관리자는 정기적으로 일반 사용자에게 유효한 로그인 쉘이 있는지 확인해야 합니다.
- 관리자는 일반 사용자에게 시스템 관리 ID 값이 아닌 유효한 사용자 ID 값이 있는지 정기적으로 확인해야 합니다.

물리적 보안 권장 사항

사이트의 보안 정책을 개발할 때 다음 지침 목록을 고려하십시오.

- Trusted Extensions로 구성된 시스템에 대한 액세스를 제한합니다. 일반적으로 가장 안전한 위치는 1층을 제외한 실내 공간입니다.
- Trusted Extensions로 구성된 시스템에 대한 액세스를 모니터 및 문서화합니다.
- 컴퓨터 장비를 테이블이나 책상 등의 대형 물체에 고정하여 도난을 방지합니다. 장비를 목재품에 고정할 경우 금속판을 추가하여 목재품의 내구력을 높입니다.
- 민감한 정보의 경우 이동식 저장 매체를 고려합니다. 사용하지 않는 모든 이동식 매체를 잠급니다.
- 시스템 백업 및 아카이브는 시스템 위치에서 떨어진 안전한 위치에 보관합니다.
- 시스템에 대한 액세스 제한과 동일한 방식으로 백업 및 아카이브 매체에 대한 물리적 액세스를 제한합니다.
- 온도가 제조업체의 사양 범위를 벗어날 경우 알려주는 고온 경보를 컴퓨터 시설에 설치합니다. 권장 범위는 10°C-32°C(50°F-90°F)입니다.
- 바닥, 바닥 밑 공간 및 천장의 수분을 나타내는 수분 감지 경보를 설치합니다.
- 화재를 알리는 화재 경보기를 설치하고 방화 시스템을 설치합니다.
- 습도가 너무 높거나 너무 낮을 경우 알려주는 습도 경보를 설치합니다.
- 시스템에 TEMPEST 차폐를 고려합니다. TEMPEST 차폐는 시설 벽, 바닥 및 천장에 적합합니다.
- 전자기 방사선을 차폐하려면 인증된 기술자만 TEMPEST 장비를 열고 닫아야 합니다.
- 컴퓨터 장비가 있는 시설이나 공간으로 들어갈 수 있는 물리적 간격을 점검합니다. 바닥의 돌출부, 천장의 돌출부, 지붕 환기 장비 및 원물과 부차적인 추가물 사이의 인접 벽에 틈이 있는지 확인합니다.
- 컴퓨터 시설 내 또는 컴퓨터 장비 근처에서 식사, 음주 및 흡연을 금지합니다. 컴퓨터 장비에 해를 주지 않고 이런 활동을 할 수 있는 영역을 설정합니다.
- 컴퓨터 시설의 구조 도면 및 도표를 보호합니다.
- 건물 도표, 평면도 및 컴퓨터 장비 사진의 사용을 제한합니다.

담당자 보안 권한 사항

사이트의 보안 정책을 개발할 때 다음 지침 목록을 고려하십시오.

- 보안 사이트를 출입하는 패키지, 문서 및 저장 매체를 검사합니다.
- 모든 직원 및 방문객은 항상 신분증이나 배지를 착용해야 합니다.
- 복사하거나 위조하기 어려운 신분증이나 배지를 사용합니다.
- 방문객 통제 영역을 설정하고 명확히 표시합니다.
- 항상 방문자와 동행합니다.

일반 보안 위반

완벽하게 안전한 컴퓨터는 없기 때문에 컴퓨터 시설을 사용하는 사람에 의해 안전도가 결정됩니다. 대부분의 보안 위반 활동은 사용자의 주의나 추가 장비를 통해 쉽게 해결됩니다. 그러나 다음과 같은 문제가 발생할 수 있습니다.

- 시스템에 액세스해서는 안되는 다른 개인에게 암호를 제공합니다.
- 적어둔 암호를 분실하거나 안전하지 않은 장소에 둡니다.
- 쉽게 추측할 수 있는 단어나 이름으로 암호를 설정합니다.
- 다른 사용자가 암호를 입력하는 것을 보고 암호를 알아냅니다.
- 권한 없는 사용자가 하드웨어를 제거, 교체 또는 물리적으로 변경합니다.
- 화면을 잠그지 않고 자리를 비웁니다.
- 다른 사용자가 파일을 읽을 수 있도록 파일에 대한 권한을 변경합니다.
- 다른 사용자가 파일을 읽을 수 있도록 파일의 레이블을 변경합니다.
- 중요한 하드카피 문서를 파쇄하지 않고 폐기하거나 안전하지 않은 장소에 방치합니다.
- 출입문을 잠그지 않은 상태로 방치합니다.
- 사용자 열쇠를 분실합니다.
- 이동식 저장 매체를 잠그지 않습니다.
- 외부 창을 통해 컴퓨터 화면을 볼 수 있습니다.
- 네트워크 케이블이 도청됩니다.
- 전자 도청을 통해 컴퓨터 장비에서 방출된 신호를 캡처합니다.
- 정전, 서지 및 스파이크로 인해 데이터가 삭제됩니다.
- 지진, 홍수, 태풍이나 번개로 인해 데이터가 삭제됩니다.
- 태양 흑점 활동과 같은 외부 전자기 방사선 간섭으로 인해 파일이 손상됩니다.

추가 보안 참조

정부 발행물에서는 컴퓨터 보안과 관련된 표준, 정책, 방법 및 용어를 자세히 설명합니다. 여기에 나열된 기타 발행물은 UNIX® 시스템의 시스템 관리자를 위한 지침이며 UNIX 보안 문제 및 솔루션을 완벽하게 이해하는 데 매우 유용합니다.

또한 웹을 통해서도 자원이 제공됩니다. 특히 CERT (`http://www.cert.org`) 웹 사이트에서는 기업과 사용자에게 소프트웨어의 보안상 취약성을 경고합니다. SANS 협회 (`http://www.sans.org/index.php`)에서는 교육, 광범위한 용어집 및 인터넷의 주요 위협 요인에 대한 최신 목록을 제공합니다.

미국 정부 발행물

미국 정부는 웹을 통해 여러 발행물을 제공합니다. NIST(National Institute of Standards and Technology)의 CSRC(Computer Security Resource Center)에서는 컴퓨터 보안에 대한 기사를 발행합니다. NIST 사이트 (`http://csrc.nist.gov/index.html`)에서 다운로드할 수 있는 발행물 샘플은 다음과 같습니다.

- **An Introduction to Computer Security: The NIST Handbook**. SP 800-12, October 1995.
- **Standard Security Label for Information Transfer**. FIPS-188, September 1994.
- Swanson, Marianne 및 Barbara Guttman. **Generally Accepted Principles and Practices for Securing Information Technology Systems**. SP 800-14, September 1996.
- Tracy, Miles, Wayne Jensen 및 Scott Bisker. **Guidelines on Electronic Mail Security**. SP 800-45, September 2002. Section E.7 메일용 LDAP의 보안 구성 내용 포함.
- Wilson, Mark 및 Joan Hash. **Building an Information Technology Security Awareness and Training Program**. SP 800-61, January 2004. 유용한 용어 포함.
- Grace, Tim, Karen Kent 및 Brian Kim. **Computer Security Incident Handling Guidelines**. SP 800-50, September 2002. Section E.7 메일용 LDAP의 보안 구성 내용 포함.
- Souppaya, Murugiah, John Wack 및 Karen Kent. **Security configuration Checklists Program for IT Products**. SP 800-70, May 2005.

UNIX 보안 발행물

Chirillo, John 및 Edgar Danielyan. **Sun™ Certified Security Administration for Solaris™ 9 & 10 Study Guide**. McGraw-Hill/Osborne, 2005.

Garfinkel, Simson, Gene Spafford 및 Alan Schwartz. **Practical UNIX and Internet Security, 3rd Edition**. O'Reilly & Associates, Inc, Sebastopol, CA, 2006.

일반 컴퓨터 보안 발행물

Brunette, Glenn M. 및 Christoph L. **Toward Systemically Secure IT Architectures**. Sun Microsystems, Inc, June 2005.

Kaufman, Charlie, Radia Perlman 및 Mike Speciner. **Network Security: Private Communication in a Public World, 2nd Edition**. Prentice-Hall, 2002.

Pfleeger, Charles P. 및 Shari Lawrence Pfleeger. **Security in Computing**. Prentice Hall PTR, 2006.

Privacy for Pragmatists: A Privacy Practitioner's Guide to Sustainable Compliance. Sun Microsystems, Inc, August 2005.

Rhodes-Ousley, Mark, Roberta Bragg 및 Keith Strassberg. **Network Security: The Complete Reference**. McGraw-Hill/Osborne, 2004.

Stoll, Cliff. **The Cuckoo's Egg**. Doubleday, 1989.

일반 UNIX 발행물

Bach, Maurice J. **The Design of the UNIX Operating System**. Prentice Hall, Englewood Cliffs, NJ, 1986.

Nemeth, Evi, Garth Snyder 및 Scott Seebas. **UNIX System Administration Handbook**. Prentice Hall, Englewood Cliffs, NJ, 1989.

◆ ◆ ◆ 부 록 B

CDE 작업을 사용하여 Trusted Extensions에 영역 설치

이 부록에서는 Trusted CDE 작업을 사용하여 Solaris Trusted Extensions에 레이블이 있는 영역을 구성하는 방법에 대해 설명합니다. 패치 없이 Solaris 10 11/06 릴리스를 실행 중이거나 이러한 작업에 익숙한 경우 Trusted CDE 작업을 사용합니다. `txzonemgr` 스크립트를 사용하려면 57 페이지 “레이블이 있는 영역 만들기”를 참조하십시오.

CDE 작업을 사용하여 네트워크 인터페이스와 영역 연결(작업 맵)

다음 작업 중 하나만 수행합니다. 교환 조건에 대한 자세한 내용은 23 페이지 “다중 레벨 액세스 계획”을 참조하십시오.

작업	설명	수행 방법
논리적 인터페이스를 공유합니다.	전역 영역을 한 IP 주소에 연결하고 레이블이 있는 영역을 다른 IP 주소에 연결합니다.	127 페이지 “CDE 작업을 사용하여 시스템에 두 개의 IP 주소 지정”
물리적 인터페이스를 공유합니다.	모든 영역을 하나의 IP 주소에 매핑합니다.	129 페이지 “CDE 작업을 사용하여 시스템에 하나의 IP 주소 지정”

▼ CDE 작업을 사용하여 시스템에 두 개의 IP 주소 지정

이 구성에서는 호스트 주소가 전역 영역에만 적용됩니다. 레이블이 있는 영역은 두 번째 IP 주소를 전역 영역과 공유합니다.

시작하기 전에 사용자는 전역 영역의 수퍼유저입니다. 시스템에 이미 두 개의 IP 주소가 할당되어 있으며 사용자는 Trusted CDE 작업 공간에 있습니다.

1 Trusted_Extensions 폴더로 이동합니다.

a. 배경에서 마우스 버튼 3을 누릅니다.

b. Workspace(작업 공간) 메뉴에서 Applications(응용 프로그램) → Application Manager(응용 프로그램 관리자)를 선택합니다.

c. Trusted_Extensions 폴더 아이콘을 두 번 누릅니다.
이 폴더에는 인터페이스, LDAP 클라이언트 및 레이블이 있는 영역을 설정하는 작업이 포함되어 있습니다.

2 Share Logical Interface(논리적 인터페이스 공유) 작업을 두 번 누르고 프롬프트에 응답합니다.

주 – 시스템에 두 개의 IP 주소가 할당되어 있어야 합니다. 이 작업의 경우 두 번째 주소와 해당 주소의 호스트 이름을 제공합니다. 두 번째 주소는 공유 주소입니다.

```
Hostname:       Type the name for your labeled zones interface
IP Address:     Type the IP address for the interface
```

이 작업은 두 개 이상의 IP 주소가 있는 호스트를 구성합니다. 전역 영역의 IP 주소는 호스트의 이름입니다. 레이블이 있는 영역의 IP 주소에는 다른 호스트 이름이 있습니다. 또한 레이블이 있는 영역의 IP 주소는 전역 영역과 공유됩니다. 이 구성을 사용하면 레이블이 있는 영역에서 네트워크 프린터에 연결할 수 있습니다.

참고 – 레이블이 있는 영역에 표준 이름 지정 규약을 사용합니다. 예를 들어 호스트 이름에 `-zones`를 추가합니다.

---

3 (옵션) 터미널 창에서 작업 결과를 확인합니다.

```
# ifconfig -a
```

예를 들어 다음 출력은 레이블이 있는 영역에 대한 `192.168.0.12` 네트워크 인터페이스의 공유 논리적 인터페이스 `hme0:3`을 보여 줍니다. `hme0` 인터페이스는 전역 영역의 고유 IP 주소입니다.

```
lo0: flags=2001000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4,VIRTUAL> mtu 8232 index 1
        inet 127.0.0.1 netmask ff000000
        ether 0:0:00:00:00:0
hme0: flags=1000843<BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        inet 192.168.0.11 netmask fffffe00 broadcast 192.168.0.255
hme0:3 flags=1000843<BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
```

```
all-zones
inet 192.168.0.12 netmask fffffe00 broadcast 192.168.0.255
```

▼ CDE 작업을 사용하여 시스템에 하나의 IP 주소 지정

이 구성에서는 호스트 주소가 레이블이 있는 영역을 포함한 모든 영역에 적용됩니다.

시작하기 전에 사용자는 전역 영역의 수퍼유저입니다. 사용자는 Trusted CDE 작업 공간에 있습니다.

1 Trusted_Extensions 폴더로 이동합니다.

a. 배경에서 마우스 버튼 3을 누릅니다.

b. Workspace(작업 공간) 메뉴에서 Applications(응용 프로그램) → Application Manager(응용 프로그램 관리자)를 선택합니다.

c. Trusted_Extensions 폴더 아이콘을 두 번 누릅니다.
이 폴더에는 인터페이스, LDAP 클라이언트 및 레이블이 있는 영역을 설정하는 작업이 포함되어 있습니다.

2 Share Physical Interface(물리적 인터페이스 공유) 작업을 두 번 누릅니다.
이 작업은 호스트를 하나의 IP 주소로 구성합니다. 전역 영역에는 고유한 주소가 없습니다. 이 시스템은 다중 레벨 인쇄 서버나 NFS 서버로 사용할 수 없습니다.

3 (옵션) 터미널 창에서 작업 결과를 확인합니다.

```
# ifconfig -a
```

물리적 인터페이스 공유 작업은 모든 영역이 논리적 NIC를 가지도록 구성합니다. 이러한 논리적 NIC는 전역 영역에서 한 개의 물리적 NIC를 공유합니다.

예를 들어 다음 출력은 모든 영역에 대한 `192.168.0.11` 네트워크 인터페이스의 공유 물리적 인터페이스 `hme0`을 보여 줍니다.

```
lo0: flags=2001000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4,VIRTUAL> mtu 8232 index 1
       inet 127.0.0.1 netmask ff000000
       ether 0:0:00:00:00:0
hme0: flags=1000843<BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
       all-zones
       inet 192.168.0.11 netmask fffffe00 broadcast 192.168.0.255
```

CDE 작업을 사용하여 영역 만들기 준비(작업 맵)

다음 작업 맵은 영역을 만들기 위해 시스템을 준비하는 작업을 설명합니다. 영역을 만드는 방법에 대한 설명은 21 페이지 "Trusted Extensions의 영역 계획"을 참조하십시오.

작업	설명	수행 방법
1. 각 영역에 이름을 지정하고 영역 이름을 영역 레이블에 연결합니다.	레이블이 있는 각 영역에 레이블 버전을 사용하여 이름을 지정한 다음 이름을 Solaris Management Console의 레이블과 연결합니다.	130 페이지 "CDE 작업을 사용하여 영역 이름 및 영역 레이블 지정"
2. 영역을 만들기 전에 네트워크를 구성합니다.	모든 호스트의 네트워크 인터페이스에 레이블을 할당하고 추가 구성을 합니다.	**Solaris Trusted Extensions Administrator's Procedures**의 "Configuring Trusted Network Databases (Task Map)"

▼ CDE 작업을 사용하여 영역 이름 및 영역 레이블 지정

`label_encodings` 파일의 모든 레이블에 대해 영역을 만들 필요는 없지만 그렇게 할 수는 있습니다. `tnzonecfg` 데이터베이스는 이 시스템에 영역을 만들 수 있는 레이블을 열거합니다.

1 Trusted_Extensions 폴더로 이동합니다.

a. 배경에서 마우스 버튼 3을 누릅니다.

b. Workspace(작업 공간) 메뉴에서 Applications(응용 프로그램) → Application Manager(응용 프로그램 관리자)를 선택합니다.

c. Trusted_Extensions 폴더 아이콘을 두 번 누릅니다.

2 모든 영역에 대해 영역 이름을 지정합니다.

a. Configure Zone(영역 구성) 작업을 두 번 누릅니다.

b. 프롬프트에서 이름을 제공합니다.

참고 – 영역의 레이블과 비슷한 이름을 영역에 지정합니다. 예를 들어 레이블이 `CONFIDENTIAL : INTERNAL USE ONLY`인 영역의 이름은 `internal`일 수 있습니다.

---

3 모든 영역에 대해 Configure Zone(영역 구성) 작업을 반복합니다.

예를 들어, 기본 `label_encodings` 파일에 다음과 같은 레이블이 포함되어 있습니다.

```
PUBLIC
CONFIDENTIAL: INTERNAL USE ONLY
CONFIDENTIAL: NEED TO KNOW
CONFIDENTIAL: RESTRICTED
SANDBOX: PLAYGROUND
MAX LABEL
```

Configure Zone(영역 구성) 작업을 여섯 번 실행하여 레이블당 영역을 하나씩 만들 수도 있지만 영역을 다음과 같이 만드는 것이 좋습니다.

- 모든 사용자용 시스템에서 `PUBLIC` 레이블에 대해 한 개의 영역을, `CONFIDENTIAL` 레이블에 대해 세 개의 영역을 만듭니다.
- 개발자용 시스템에서 `SANDBOX: PLAYGROUND` 레이블에 대해 영역을 만듭니다. `SANDBOX: PLAYGROUND`는 개발자용 분리 레이블로 정의되므로 개발자가 사용하는 시스템에만 이 레이블에 대해 영역이 필요합니다.
- 클리어런스로 정의되는 `MAX LABEL` 레이블에 대해서는 영역을 만들지 마십시오.

4 Trusted Network Zones(신뢰할 수 있는 네트워크 영역) 도구를 엽니다.

Solaris Management Console의 도구는 사용자 오류를 방지하도록 설계되었습니다. 이러한 도구는 구문 오류를 검사하고 자동으로 명령을 올바른 순서로 실행하여 데이터베이스를 업데이트합니다.

a. Solaris Management Console을 시작합니다.

```
# /usr/sbin/smc &
```

b. 로컬 시스템의 Trusted Extensions 도구 상자를 엽니다.

i. Console(콘솔) → Open Toolbox(도구 상자 열기)를 선택합니다.

ii. 이 컴퓨터(*this-host*: `Scope=Files, Policy=TSOL`)라는 도구 상자를 선택합니다.

iii. Open(열기)을 누릅니다.

c. System Configuration(시스템 구성)에서 Computers and Networks(컴퓨터 및 네트워크)로 이동합니다.

암호를 입력하라는 메시지가 나타나면 암호를 제공합니다.

d. Trusted Network Zones(신뢰할 수 있는 네트워크 영역) 도구를 두 번 누릅니다.

5 **각 영역에 대해 적절한 레이블을 영역 이름에 연결합니다.**

a. **Action(작업) → Add Zone Configuration(영역 구성 추가)을 선택합니다.**
대화 상자에 할당된 레이블이 없는 영역의 이름이 표시됩니다.

b. **영역 이름을 확인한 다음 Edit(편집)를 누릅니다.**

c. **레이블 구축기에서 영역 이름에 해당하는 레이블을 누릅니다.**
잘못된 레이블을 누른 경우 레이블을 다시 눌러 선택을 해제한 다음 올바른 레이블을 누릅니다.

d. **할당을 저장합니다.**
레이블 구축기에서 OK(확인)를 누른 다음 Trusted Network Zones Properties(신뢰할 수 있는 네트워크 영역 등록 정보) 대화 상자에서 OK(확인)를 누릅니다.

원하는 모든 영역이 패널에 표시되어 있으면 작업이 완료된 것이며, 그렇지 않은 경우 Add Zone Configuration(영역 구성 추가) 메뉴 항목이 Zone Name(영역 이름)에 값이 없는 대화 상자를 엽니다.

일반 오류 사용자가 만들려고 하는 영역이 Trusted Network Zones Properties(신뢰할 수 있는 네트워크 영역 등록 정보) 대화 상자에 표시되지 않으면 영역 네트워크 구성 파일이 없거나 파일을 이미 만든 경우입니다.

- 영역 네트워크 구성 파일이 있는지 확인합니다. 패널에서 이름을 찾습니다.
- 파일이 없으면 Configure Zone(영역 구성) 작업을 실행하여 영역 이름을 제공합니다. 그런 다음 단계 5를 반복하여 파일을 만듭니다.

CDE 작업을 사용하여 레이블이 있는 영역 만들기(작업 맵)

Trusted Network Zone Configuration(신뢰할 수 있는 네트워크 영역 구성) 데이터베이스의 모든 항목에 대해 하나의 영역을 만들 수 있습니다. Configure Zone(영역 구성) 작업을 실행하여 130 페이지 “CDE 작업을 사용하여 영역 이름 및 영역 레이블 지정”에서 항목을 만들었습니다.

Application Manager(응용 프로그램 관리자)의 Trusted_Extensions 폴더에는 레이블이 있는 영역을 만드는 다음과 같은 작업이 포함되어 있습니다.

- Configure Zone(영역 구성) – 모든 영역 이름에 대한 영역 구성 파일을 만듭니다.
- Install Zone(영역 설치) – 영역에 올바른 패키지와 파일 시스템을 추가합니다.
- Zone Terminal Console(영역 터미널 콘솔) – 영역의 이벤트를 보는 창을 제공합니다.
- Initialize Zone for LDAP(LDAP에 대해 영역 초기화) – 영역을 LDAP 클라이언트로 만들고 부트할 영역을 준비합니다.

- Start Zone(영역 시작) – 영역을 부트한 다음 모든 서비스 관리 프레임워크(service management framework, SMF) 서비스를 시작합니다.
- Shut Down Zone(영역 종료) – 영역의 상태를 Started(시작됨)에서 Halted(중지됨)로 변경합니다.

작업은 다음 순서로 완료됩니다.

작업	설명	수행 방법
1. 영역 하나를 설치하고 부트합니다.	첫 번째 레이블이 있는 영역을 만듭니다. 패키지를 설치하고 영역을 LDAP 클라이언트로 만든 다음 영역의 모든 서비스를 시작합니다.	133 페이지 “CDE 작업을 사용하여 레이블이 있는 영역 설치, 초기화 및 부트”
2. 영역을 사용자 정의합니다.	원하지 않는 서비스를 제거합니다. 영역을 복사 또는 복제하려면 영역 관련 정보를 제거합니다.	136 페이지 “Trusted Extensions에서 부트된 영역 사용자 정의”
3. 다른 영역을 만듭니다.	다음 방법 중 하나를 사용하여 다른 영역을 만듭니다. 40 페이지 “Trusted Extensions 설치 전 시스템 및 보안 사항 결정”에서 방법을 선택했습니다.	
	각 영역을 처음부터 만듭니다.	133 페이지 “CDE 작업을 사용하여 레이블이 있는 영역 설치, 초기화 및 부트” 136 페이지 “Trusted Extensions에서 부트된 영역 사용자 정의”
	첫 번째 레이블이 있는 영역을 다른 레이블로 복사합니다. 모든 영역에 대해 반복합니다.	138 페이지 “Trusted Extensions에서 영역 복사 방법 사용”
	ZFS 스냅샷을 사용하여 첫 번째 레이블이 있는 영역에서 다른 영역을 복제합니다.	139 페이지 “Trusted Extensions에서 영역 복제 방법 사용”

▼ CDE 작업을 사용하여 레이블이 있는 영역 설치, 초기화 및 부트

영역을 만들려면 전체 운영 체제를 복사해야 하므로 프로세스에 시간이 많이 소요됩니다. 이 프로세스를 좀더 빨리 수행하려면 영역을 하나 만들고 이 영역을 다른 영역에 대한 템플리트로 만든 다음 해당 영역 템플리트를 복사하거나 복제할 수 있습니다.

시작하기 전에 130 페이지 “CDE 작업을 사용하여 영역 이름 및 영역 레이블 지정”을 완료했습니다.

LDAP를 이름 지정 서비스로 사용 중인 경우에는 55 페이지 “Trusted Extensions에서 전역 영역을 LDAP 클라이언트로 만들기”을 완료했습니다.

영역을 복제하려는 경우 49 페이지 “영역 복제를 위한 ZFS 풀 만들기 ”를 완료했습니다. 다음 절차에서는 준비한 영역을 설치합니다.

1 **Trusted_Extensions 폴더에서 Install Zone(영역 설치) 작업을 두 번 누릅니다.**

   a. **설치할 영역 이름을 입력합니다.**

      이 작업은 레이블이 있는 가상 운영 체제를 만듭니다. 이 단계를 완료하려면 어느 정도 시간이 소요됩니다. Install Zone(영역 설치)을 실행하는 동안 시스템에서 다른 작업을 수행하지 마십시오.

```
# zone-name: Install Zone
Preparing to install zone <zone-name>
Creating list of files to copy from the global zone
Copying <total> files to the zone
Initializing zone product registry
Determining zone package initialization order.
Preparing to initialize <subtotal> packages on the zone.
Initializing package <number> of <subtotal>: percent complete: percent

Initialized <subtotal> packages on zone.
Zone <zone-name> is initialized.
The file /zone/internal/root/var/sadm/system/logs/install_log
contains a log of the zone installation.

*** Select Close or Exit from the window menu to close this window ***
```

   b. **콘솔을 열어 설치된 영역에서 이벤트를 모니터합니다.**

      i. **Zone Terminal Console(영역 터미널 콘솔) 작업을 두 번 누릅니다.**

      ii. **방금 설치한 영역의 이름을 입력합니다.**

2 **영역을 초기화합니다.**

   - **LDAP를 사용하는 경우 Initialize Zone for LDAP(LDAP에 대해 영역 초기화) 작업을 두 번 누릅니다.**

```
Zone name:                  Type the name of the installed zone
Host name for the zone:     Type the host name for this zone
```

     예를 들어 공유 논리적 인터페이스가 있는 시스템에서는 값이 다음과 비슷합니다.

```
Zone name:              public
Host name for the zone: machine1-zones
```

     이 작업은 레이블이 있는 영역을 전역 영역을 제공하는 같은 LDAP 서버의 LDAP 클라이언트로 만듭니다. 작업이 완료되면 다음 정보가 표시됩니다.

```
zone-name zone will be  LDAP client of IP-address
zone-name is ready for booting
Zone label is LABEL
```

```
*** Select Close or Exit from the window menu to close this window ***
```

- **LDAP를 사용하고 있지 않을 때는 다음 단계 중 하나를 수행하여 영역을 수동으로 초기화합니다.**

  Trusted Extensions의 수동 절차는 Solaris OS에 대한 절차와 동일합니다. 시스템에 `all-zones` 인터페이스가 하나 이상 있는 경우에는 모든 영역에 대한 호스트 이름이 전역 영역의 호스트 이름과 일치해야 합니다. 일반적으로 영역 초기화 중 나타나는 질문에 대한 응답은 전역 영역에 대한 응답과 동일합니다.

  다음 중 하나를 수행하여 호스트 정보를 제공합니다.

  - **단계 3에서 영역을 시작한 후 Zone Terminal Console(영역 터미널 콘솔)에서 시스템 특성에 대한 질문에 응답합니다.**

    응답은 영역의 `sysidcfg` 파일을 채우는 데 사용됩니다.

  - **단계 3에서 영역을 부트하려면 먼저 영역의 `/etc` 디렉토리에 사용자 정의 `sysidcfg` 파일을 넣습니다.**

3. **Start Zone(영역 시작) 작업을 두 번 누릅니다.**

   프롬프트에 대답합니다.

   `Zone name:` *Type the name of the zone that you are configuring*

   이 작업은 영역을 부트한 다음 영역에서 실행되는 모든 서비스를 시작합니다. 서비스에 대한 자세한 내용은 `smf(5)` 매뉴얼 페이지를 참조하십시오.

   Zone Terminal Console(영역 터미널 콘솔)에서 영역의 부트 진행률을 추적합니다. 콘솔에 다음과 유사한 메시지가 나타납니다.

```
[Connected to zone 'public' console]

[NOTICE: Zone booting up]
...
Hostname: zonename
Loading smf(5) service descriptions: number/total
Creating new rsa public/private host key pair
Creating new dsa public/private host key pair

rebooting system due to change(s) in /etc/default/init

[NOTICE: Zone rebooting]
```

4 콘솔 출력을 모니터합니다.

136 페이지 "Trusted Extensions에서 부트된 영역 사용자 정의"로 진행하기 전에 영역이 재부트되었는지 확인합니다. 다음 콘솔 로그인 프롬프트는 영역이 재부트되었음을 나타냅니다.

hostname `console login:`

일반 오류 Install Zone(영역 설치)의 경우: 다음과 비슷한 경고가 표시될 경우 `Installation of these packages generated errors: SUNW`*pkgname*(패키지 설치 중 오류 발생: SUNWpkgname)과 비슷한 경고가 표시될 경우 설치 로그를 확인하고 패키지 설치를 마칩니다.

▼ Trusted Extensions에서 부트된 영역 사용자 정의

영역을 복제하려는 경우 이 절차는 영역을 다른 영역의 템플리트가 되도록 구성합니다. 또한 이 절차는 영역을 사용하도록 구성합니다.

1 해당 영역이 완전히 시작했는지 확인합니다.

a. *zone-name*: **Zone Terminal Console(영역 터미널 콘솔)에서 루트로 로그인합니다.**

```
hostname console login: root
Password:       Type root password
```

b. 영역이 실행 중인지 확인합니다.

상태가 `running`이면 하나 이상의 프로세스가 영역에서 실행되고 있음을 나타냅니다.

```
# zoneadm list -v
ID NAME         STATUS         PATH
 2 public       running        /
```

c. 해당 영역이 전역 영역과 통신할 수 있는지 확인합니다.

X 서버가 전역 영역에서 실행됩니다. 이 서비스를 사용하려면 레이블이 있는 각 영역이 전역 영역에 연결할 수 있어야 합니다. 따라서 영역을 사용할 수 있으려면 영역 네트워킹이 작동해야 합니다. 도움이 필요한 경우 87 페이지 "레이블이 있는 영역에서 X 서버에 액세스할 수 없음"을 참조하십시오.

2 Zone Terminal Console(영역 터미널 콘솔)의 레이블이 있는 영역에서 불필요한 서비스를 비활성화합니다.

이 영역을 복사 또는 복제하는 경우에는 비활성화한 서비스가 새 영역에서 비활성화됩니다. 시스템에 온라인 상태로 유지되는 서비스는 영역에 대한 서비스 매니페스트에 따라 달라집니다. `netservices limited` 명령을 사용하여 레이블이 있는 영역에서 불필요한 서비스를 해제합니다.

a. 불필요한 서비스들을 제거합니다.

```
# netservices limited
```

b. 나머지 서비스를 나열합니다.

```
# svcs
...
STATE          STIME      FMRI
online         13:05:00   svc:/application/graphical-login/cde-login:default
...
```

c. 그래픽 로그인을 비활성화합니다.

```
# svcadm disable svc:/application/graphical-login/cde-login
# svcs cde-login
STATE          STIME      FMRI
disabled       13:06:22   svc:/application/graphical-login/cde-login:default
```

서비스 관리 프레임워크에 대한 자세한 내용은 `smf(5)` 매뉴얼 페이지를 참조하십시오.

3 영역을 종료합니다.

다음 방법 중 하나를 선택합니다.

- **Shut Down Zone(영역 종료) 작업을 실행합니다.**

  영역 이름을 제공합니다.

- **전역 영역의 터미널 창에서 `zlogin` 명령을 사용합니다.**

  ```
  # zlogin zone-name init 0
  ```

  자세한 내용은 `zlogin(1)` 매뉴얼 페이지를 참조하십시오.

4 영역이 종료되었는지 확인합니다.

zone-name: Zone Terminal Console(영역 터미널 콘솔)에 다음 메시지가 표시되면 영역이 종료되었음을 나타냅니다.

```
[ NOTICE: Zone halted]
```

이 영역을 복사 또는 복제하지 않는 경우에는 첫 번째 영역을 만든 방법으로 나머지 영역을 만듭니다.

5 이 영역을 다른 영역에 대한 템플리트로 사용하는 경우에는 다음을 수행합니다.

a. auto_home_*zone-name* 파일을 제거합니다.

전역 영역의 터미널 창에서 이 파일을 *zone-name* 영역에서 제거합니다.

```
cd /zone/zone-name/root/etc
# ls auto_home*
auto_home  auto_home_zone-name
# rm auto_home_zone-name
```

예를 들어 public 영역을 기초로 다른 영역을 복제하는 경우에는 auto_home 파일을 제거합니다.

```
# cd /zone/public/root/etc
# rm auto_home_public
```

다음 순서

- 영역을 복사하는 경우 138 페이지 "Trusted Extensions에서 영역 복사 방법 사용"으로 이동합니다.
- 영역을 복제하는 경우 139 페이지 "Trusted Extensions에서 영역 복제 방법 사용"으로 이동합니다.

▼ Trusted Extensions에서 영역 복사 방법 사용

시작하기 전에

- 130 페이지 "CDE 작업을 사용하여 영역 이름 및 영역 레이블 지정"을 완료했습니다.
- 132 페이지 "CDE 작업을 사용하여 레이블이 있는 영역 만들기(작업 맵)"에서 복제에 대한 템플리트로 사용되는 영역을 사용자 정의했습니다.
- 복제에 대한 템플리트로 사용되는 영역을 실행하고 있지 않습니다.
- Trusted_Extensions 폴더가 표시됩니다.

1 만들려고 하는 모든 영역에 대해 Copy Zone(영역 복사) 작업을 두 번 누릅니다.

프롬프트에 대답합니다.

```
New Zone Name:          Type name of target zone
From Zone Name:         Type name of source zone
```

주의 – 이 작업을 완료하는 동안에는 다른 작업을 수행하지 마십시오.

2 영역이 만들어지면 모든 영역의 상태를 확인합니다.

a. Zone Terminal Console(영역 터미널 콘솔) 작업을 두 번 누릅니다.

b. 각 영역에 로그인합니다.

c. 67 페이지 "영역 상태 확인"을 완료합니다.

▼ Trusted Extensions에서 영역 복제 방법 사용

시작하기 전에

- 130 페이지 "CDE 작업을 사용하여 영역 이름 및 영역 레이블 지정"을 완료했습니다.
- 49 페이지 "영역 복제를 위한 ZFS 풀 만들기 "를 완료했습니다.
- 49 페이지 "영역 복제를 위한 ZFS 풀 만들기 "를 완료하여 영역 템플리트를 만들었습니다.
- 132 페이지 "CDE 작업을 사용하여 레이블이 있는 영역 만들기(작업 맵)"에서 복제에 대한 템플리트로 사용되는 영역을 사용자 정의했습니다.
- 복제에 대한 템플리트로 사용되는 영역이 종료되었습니다.
- Trusted_Extensions 폴더가 표시됩니다.

1 영역 템플리트의 Solaris ZFS 스냅샷을 만듭니다.

```
# cd /
# zfs snapshot zone/zone-name@snapshot
```

이 스냅샷을 사용하여 나머지 영역을 복제합니다. 구성된 영역의 이름이 `public`인 경우 스냅샷 명령은 다음과 같습니다.

```
# zfs snapshot zone/public@snapshot
```

2 만들려고 하는 모든 영역에 대해 Clone Zone(영역 복제) 작업을 두 번 누릅니다.

프롬프트에 대답합니다.

```
New Zone Name:          Type name of source zone
ZFS Snapshot:             Type name of snapshot
```

3 대화 상자의 정보를 읽습니다.

```
Zone label is <LABEL>
zone-name is ready for booting

*** Select Close or Exit from the window menu to close this window ***
```

4 각 영역에 대해 Start Zone(영역 시작) 작업을 실행합니다.

다른 영역에 대해 작업을 실행하기 전에 각 영역을 시작합니다.

5 영역을 만든 후 모든 영역의 상태를 확인합니다.

a. Zone Terminal Console(영역 터미널 콘솔) 작업을 두 번 누릅니다.

b. 67 페이지 "영역 상태 확인"을 완료합니다.

◆ ◆ ◆ 부 록 C

Trusted Extensions 구성 검사 목록

이 검사 목록에서는 Solaris Trusted Extensions에 대한 주요 구성 작업의 전체적인 보기를 제공합니다. 세부 작업은 주요 작업에서 개략적으로 설명합니다. 검사 목록은 이 설명서의 다음 단계를 대체하지 않습니다.

Trusted Extensions 구성 검사 목록

다음은 사이트에 Trusted Extensions를 설치 및 구성하는 데 필요한 사항을 요약한 목록입니다. 다른 책에서 다루는 작업은 상호 참조됩니다.

1. 참조.
   - **Solaris Trusted Extensions Administrator's Procedures**의 처음 다섯 장을 참조하십시오.
   - 사이트 보안 요구 사항을 이해합니다.
   - 120 페이지 "사이트 보안 정책 및 Trusted Extensions"를 참조하십시오.
2. 준비.
   - **루트** 암호를 결정합니다.
   - PROM 또는 BIOS 보안 레벨을 결정합니다.
   - PROM 또는 BIOS 암호를 결정합니다.
   - 주변기기 연결이 허용되는지 결정합니다.
   - 원격 프린터에 대한 액세스가 허용되는지 결정합니다.
   - 레이블이 없는 네트워크에 대한 액세스가 허용되는지 결정합니다.
   - 영역 생성 방법을 결정합니다.
3. Trusted Extensions 설치.
   a. Solaris OS를 설치합니다.
      - 원격 관리의 경우 Developer Group(개발자 그룹) 이상의 Solaris 패키지를 설치합니다.
      - Clone Zone(영역 복제) 생성 방법의 경우 Custom Install(사용자 정의 설치)를 선택한 다음 `/zone` 분할 영역을 레이아웃합니다.

b. Trusted Extensions 패키지를 추가합니다.

4. IPv6을 사용하는 경우 Trusted Extensions에 대해 IPv6 활성화.
5. (선택 사항) 영역 복제를 위한 ZFS 풀 생성.
6. 레이블을 구성합니다.
   a. 사이트의 `label_encodings` 파일을 완료합니다.
   b. 파일을 확인 및 설치합니다.
   c. 다시 부트합니다.
7. 전역 영역 및 레이블이 있는 영역을 위한 인터페이스 구성.
8. Solaris Management Console 구성.
9. 이름 지정 서비스 구성.
   - 구성이 필요하지 않은 파일 이름 지정 서비스를 사용합니다.
   - 또는, LDAP 구성
     a. Trusted Extensions 프록시 서버 또는 Trusted Extensions LDAP 서버를 생성합니다.
     b. Solaris Management Console을 LDAP에 등록합니다.
     c. Solaris Management Console용 LDAP 도구 상자를 생성합니다.
10. LDAP에 대한 네트워크 연결 구성.
    - 원격 호스트 템플리트의 `cipso` 호스트 유형에 LDAP 서버 또는 프록시 서버를 할당합니다.
    - 원격 호스트 템플리트의 `cipso` 호스트 유형에 로컬 시스템을 할당합니다.
    - 로컬 시스템을 LDAP 서버의 클라이언트로 만듭니다.
11. 레이블이 있는 영역 생성.
    - 옵션 1: txzonemgr 스크립트를 사용합니다.
    - 옵션 2: Trusted CDE 작업을 사용합니다.
      a. 레이블이 있는 영역을 구성합니다.
         i. Solaris Management Console에서 영역 이름을 특정 레이블과 연결합니다.
         ii. Configure Zone(영역 구성) 작업을 실행합니다.
      b. Install Zone(영역 설치) 작업을 실행합니다.
      c. Initialize for LDAP(LDAP용으로 초기화) 작업을 실행합니다.
      d. Start Zone(영역 시작) 작업을 실행합니다.
      e. 실행 중인 영역을 사용자 정의합니다.
      f. Shut Down Zone(영역 종료) 작업을 실행합니다.
      g. 영역을 종료하는 동안 영역을 사용자 정의합니다.
      h. (선택 사항) ZFS 스냅샷을 생성합니다.

i. 처음부터 또는 Copy Zone(영역 복사) 또는 Clone Zone(영역 복제) 작업을 사용하여 나머지 영역을 생성합니다.

12. 네트워크 구성. **Solaris Trusted Extensions Administrator's Procedures**의 "Configuring Trusted Network Databases (Task Map)"를 참조하십시오.
    - 단일 레이블 호스트 및 제한된 범위 호스트를 식별합니다.
    - 레이블이 없는 호스트에서 수신되는 데이터에 적용할 레이블을 결정합니다.
    - 원격 호스트 템플리트를 사용자 정의합니다.
    - 개별 호스트를 템플리트에 할당합니다.
    - 서브넷을 템플리트에 할당합니다.
13. 정적 라우팅 설정. **Solaris Trusted Extensions Administrator's Procedures**의 "Configuring Routes and Checking Network Information in Trusted Extensions (Task Map)"를 참조하십시오.
14. 로컬 사용자 및 로컬 관리 역할 구성.
    - 보안 관리자 역할을 만듭니다.
    - 보안 관리자 역할을 수락할 수 있는 로컬 사용자를 생성합니다.
    - 다른 역할 및 이러한 역할을 수락할 수 있는 다른 로컬 사용자를 생성합니다.
15. NFS 서버에 홈 디렉토리 생성.
    - 사용자가 액세스할 수 있는 모든 레이블에서 각 사용자의 홈 디렉토리를 생성합니다.
    - (선택 사항) 사용자가 하위 수준의 홈 디렉토리를 읽지 못하도록 합니다.
16. 인쇄 구성. **Solaris Trusted Extensions Administrator's Procedures**의 "Managing Printing in Trusted Extensions (Task Map)"를 참조하십시오.
17. 장치 구성. **Solaris Trusted Extensions Administrator's Procedures**의 "Handling Devices in Trusted Extensions (Task Map)"를 참조하십시오.
    a. 역할에 Device Management(장치 관리) 프로필 또는 System ADministrator(시스템 관리자) 프로필을 할당합니다.
    b. 장치를 사용 가능하게 하려면 다음 중 하나를 수행합니다.
        - 시스템에 따라 장치를 할당 가능하게 합니다.
        - 선택한 사용자 및 역할에 Allocate Device(장치 할당) 권한을 할당합니다.
18. Solaris 기능 구성.
    - 감사를 구성합니다.
    - 보안 설정을 구성합니다.
    - 특정 LDAP 클라이언트를 LDAP 관리 시스템으로 사용 가능하게 합니다.
    - LDAP에서 사용자를 구성합니다.
    - LDAP에서 네트워크 역할의 구성합니다.

- 파일 시스템을 마운트 및 공유합니다. **Solaris Trusted Extensions Administrator's Procedures**의 11 장, "Managing and Mounting Files in Trusted Extensions (Tasks)"를 참조하십시오.

용어집

CDE 공통 데스크탑 환경을 참조하십시오.

CIPSO 레이블 Common IP Security Option(공통 IP 보안 옵션)입니다. CIPSO는 Trusted Extensions에서 구현되는 레이블 표준입니다.

.copy_files 파일 다중 레이블 시스템의 선택적 설치 파일. 이 파일에는 시스템 또는 응용 프로그램이 제대로 작동하기 위해 사용자 환경이나 사용자 응용 프로그램에 필요한 `.cshrc` 또는 `.mozilla` 등의 시작 파일 목록이 포함되어 있습니다. `.copy_files`에 나열된 파일은 해당 디렉토리를 만들 때 상위 레이블의 사용자 홈 디렉토리로 **복사됩니다**. .link_files 파일을 참조하십시오.

DAC 임의의 액세스 제어를 참조하십시오.

GFI Government Furnished Information의 약자입니다. 이 설명서에서는 미국 정부에서 제공하는 label_encodings 파일을 가리킵니다. Trusted Extensions 소프트웨어에서 GFI를 사용하려면 GFI의 끝에 Sun 고유의 `LOCAL DEFINITIONS` 섹션을 추가해야 합니다. 자세한 내용은 **Solaris Trusted Extensions Label Administration**의 5 장, “Customizing LOCAL DEFINITIONS”를 참조하십시오.

IP 주소 인터넷 프로토콜 주소입니다. 인터넷 프로토콜을 통해 통신할 수 있도록 네트워크에 연결된 시스템을 식별하는 고유 번호입니다. IPv4에서 주소는 마침표로 구분된 네 개의 숫자로 구성됩니다. 대부분의 경우 IP 주소의 각 부분은 0부터 225 사이의 숫자입니다. 그러나 첫 번째 숫자는 224보다 작아야 하고 마지막 숫자는 0이 될 수 없습니다.

IP 주소는 논리적으로 네트워크와 네트워크에 있는 시스템으로 나뉩니다. 네트워크 번호는 지역 번호와 유사합니다. 네트워크에 대해 시스템 번호는 전화 번호와 유사합니다.

label_encodings 파일 인정 범위, 레이블 보기, 기본 레이블 가시성, 기본 사용자 클리어런스 및 레이블의 기타 측면과 같은 전체 민감도 레이블이 정의되어 있는 파일입니다.

.link_files 파일 다중 레이블 시스템의 선택적 설치 파일. 이 파일에는 시스템 또는 응용 프로그램이 제대로 작동하기 위해 사용자 환경이나 사용자 응용 프로그램에 필요한 `.cshrc` 또는 `.mozilla` 등의 시작 파일 목록이 포함되어 있습니다. `.link_files`에 나열된 파일은 해당 디렉토리를 만들 때 상위 레이블의 사용자 홈 디렉토리로 **연결됩니다**. .copy_files 파일을 참조하십시오.

MAC 필수 액세스 제어를 참조하십시오.

Solaris Management Console 관리 프로그램의 도구 상자가 들어 있는 Java 기반 관리 GUI입니다. Trusted CDE에서 이 GUI는 Application Manager(응용 프로그램 관리자)에서 시작할 수 있습니다. 대부분의 시스템, 네트워크 및 사용자 관리는 Console(콘솔) 도구 상자를 사용하여 수행합니다.

tnrhdb 데이터베이스 신뢰할 수 있는 네트워크 원격 호스트 데이터베이스입니다. 이 데이터베이스는 원격 호스트에 레이블 특성 집합을 할당합니다. 데이터베이스는 /etc/security/tsol/tnrhdb의 파일로 액세스하거나 LDAP 서버에서 액세스할 수 있습니다.

tnrhtp 데이터베이스 신뢰할 수 있는 네트워크 원격 호스트 템플리트입니다. 이 데이터베이스는 원격 호스트에 할당할 수 있는 레이블 특성 집합을 정의합니다. 데이터베이스는 /etc/security/tsol/tnrhtp의 파일로 액세스하거나 LDAP 서버에서 액세스할 수 있습니다.

txzonemgr 스크립트 /usr/sbin/txzonemgr 스크립트는 레이블이 있는 영역을 관리하기 위한 간단한 GUI를 제공합니다. 스크립트는 적절한 선택 항목이 있는 문맥에 맞는 메뉴를 제공합니다. txzonemgr은 전역 영역에서 루트에 의해 실행됩니다.

개방형 네트워크 다른 네트워크에 물리적으로 연결되어 있으며 Trusted Extensions 소프트웨어를 사용하여 비 Trusted Extensions 호스트와 통신하는 Solaris Trusted Extensions 호스트의 네트워크입니다. 폐쇄형 네트워크와 반대입니다.

공통 데스크탑 환경 Trusted Extensions 소프트웨어를 관리하기 위한 기록 윈도우화 환경입니다. Trusted Extensions는 환경을 수정하여 Trusted CDE를 만듭니다. 또한 Sun Java™ 데스크탑 시스템을 수정해야 Trusted JDS를 만들 수 있습니다.

관리 역할 역할의 한 유형으로, 필요한 권한 부여, 권한 있는 명령, 권한 있는 작업 및 Trusted Path(신뢰할 수 있는 경로)의 보안 속성을 제공하여 해당 역할이 관리 작업을 수행할 수 있도록 합니다. 역할은 백업 또는 감사와 같은 Solaris 수퍼유저 기능의 일부를 수행합니다.

권한 명령을 실행 중인 프로세스에 부여되는 권한입니다. 기본 기능부터 관리 기능까지 시스템의 모든 기능을 설명하는 전체 권한 집합입니다. 시스템의 클럭 설정과 같이 보안 정책을 우회하는 권한은 사이트의 보안 관리자가 부여할 수 있습니다.

권한 부여 작업을 수행하도록 사용자 또는 역할에게 부여되는 권한으로, 이러한 권한 없이는 보안 정책에 따라 해당 작업을 수행할 수 없습니다. 권한 부여는 권한 프로필에서 부여됩니다. 특정 명령의 경우 사용자가 이 명령을 성공적으로 실행하려면 특정 권한 부여가 필요합니다. 예를 들어 PostScript 파일을 인쇄하려면 Print Postscript(Postscript 인쇄) 권한이 있어야 합니다.

권한 비트 파일 또는 디렉토리를 읽거나 쓰거나 실행할 수 있는 사람을 나타내는 비트 집합을 소유자가 지정하는 임의의 액세스 제어 유형입니다. 각 파일이나 디렉토리에 세 가지 사용 권한 집합이 할당됩니다. 집합 하나는 소유자에 대한 권한이고, 다른 하나는 소유자의 그룹에 대한 권한, 나머지 하나는 기타 모든 사용자에 대한 권한입니다.

권한 프로필 명령과 CDE 작업 및 이러한 실행 파일에 할당된 보안 속성에 대한 번들 메커니즘입니다. 권한 프로필을 사용하여 Solaris 관리자는 각 명령을 실행할 수 있는 사용자를 제어하고 명령 실행 시 명령의 속성을 제어할 수 있습니다. 사용자가 로그인하면 해당 사용자에게 할당된 모든 권한이 적용되며, 사용자는 해당 사용자의 모든 권한 프로필에 할당된 모든 명령, CDE 작업 및 권한 부여에 액세스할 수 있습니다.

네트워크로 연결된 시스템 하드웨어 및 소프트웨어를 통해 연결된 시스템 그룹이며 로컬 영역 네트워크(LAN)라고도 합니다. 시스템이 네트워크에 연결되면 일반적으로 하나 이상의 서버가 필요합니다.

네트워크에 연결되지 않은 시스템 네트워크에 연결되지 않았거나 다른 호스트에 의존하지 않는 컴퓨터입니다.

도구 상자 Solaris Management Console의 프로그램 모음입니다. Trusted Extensions 호스트의 경우 관리자는 `Policy=TSOL` 도구 상자를 사용합니다. 각 도구 상자에는 도구 상자 범위 내에서 사용할 수 있는 프로그램이 있습니다. 예를 들어 시스템의 `tnzonecfg` 데이터베이스를 처리하는 Trusted Network Zones(신뢰할 수 있는 네트워크 영역) 도구는 그 범위가 항상 로컬이기 때문에 `Files(파일)` 도구 상자에만 있습니다. User Accounts(사용자 계정) 프로그램은 모든 도구 상자에 있습니다. 관리자는 로컬 사용자를 만들려면 `Files` 도구 상자를 사용하고 네트워크 사용자를 만들려면 `LDAP` 도구 상자를 사용합니다.

도메인 인터넷 이름 지정 계층의 일부입니다. 관리 파일을 공유하는 로컬 네트워크의 시스템 그룹을 나타냅니다.

도메인 이름 로컬 네트워크의 시스템 그룹에 대한 식별 정보입니다. 도메인 이름은 마침표로 구분되는 구성 요소 이름의 시퀀스로 구성됩니다(예: `example1.town.state.country.org`). 도메인 이름을 왼쪽에서 오른쪽으로 읽음에 따라 구성 요소 이름은 관리 기관의 보다 일반적인(일반적으로 원격) 영역을 식별합니다.

레이블 객체에 할당된 보안 식별자입니다. 레이블은 객체를 보호해야 하는 정보의 레벨을 기반으로 합니다. 보안 관리자가 사용자를 구성한 방법에 따라 사용자는 민감도 레이블을 볼 수 있거나 전혀 레이블을 볼 수 없습니다. 레이블은 label_encodings 파일에서 정의합니다.

레이블 구성 Trusted Extensions 설치 시 선택할 수 있는 민감도 레이블(단일 레이블 또는 다중 레이블)입니다. 대부분의 환경에서 레이블 구성은 사이트의 모든 시스템에서 동일합니다.

레이블 범위 명령, 영역 및 할당 가능 장치에 할당되는 민감도 레이블 집합입니다. 범위는 최대 레이블 및 최소 레이블을 통해 지정됩니다. 명령의 경우 최소 및 최대 레이블은 명령이 실행될 수 있는 레이블을 제한합니다. 레이블을 인식하지 않는 원격 호스트에는 단일 민감도 레이블이 할당되며 보안 관리자가 단일 레이블로 제한하고자 하는 다른 호스트도 마찬가지입니다. 레이블 범위는 장치가 할당될 수 있는 레이블을 제한하며 장치 사용 시 정보를 저장하거나 처리할 수 있는 레이블을 제한합니다.

레이블 집합 보안 레이블 집합을 참조하십시오.

레이블이 없는 호스트 Solaris OS를 실행하는 시스템과 같이 레이블이 없는 네트워크 패킷을 보내는 시스템입니다.

레이블이 있는 호스트 레이블이 있는 호스트는 CIPSO 레이블을 붙여 네트워크 패킷을 전송합니다. 모든 Trusted Extensions 호스트는 레이블이 있는 호스트입니다.

민감도 레이블 객체 또는 프로세스에 할당된 보안 레이블입니다. 레이블은 포함된 데이터의 보안 레벨에 따라 액세스를 제한하는 데 사용됩니다.

보안 관리자 민감한 정보를 보호해야 하는 조직에서 사이트의 보안 정책을 정의하고 적용하는 사람입니다. 이러한 사용자는 사이트에서 처리되는 모든 정보에 액세스할 수 있습니다. 소프트웨어에서 보안 관리자 관리 역할은 적절한 클리어런스를 가진 한 명 이상의 사용자에게 할당됩니다. 이러한 관리자는 소프트웨어가 사이트의 보안 정책을 적용하도록 모든 사용자와 호스트의 보안 속성을 구성합니다. 시스템 관리자와 비교해 보십시오.

보안 레이블 집합 tnrhtp 데이터베이스 항목에 대해 별개의 보안 레이블 집합을 지정합니다. 보안 레이블이 설정된 템플리트에 할당된 호스트는 레이블 집합에서 임의의 레이블에 일치하는 패킷을 보내고 받을 수 있습니다.

보안 속성 Trusted Extensions 보안 정책을 적용하는 데 사용되는 속성입니다. 프로세스, 사용자, 영역, 호스트, 할당 가능 장치 및 기타 객체에 다양한 보안 속성 집합이 할당됩니다.

보안 정책 Trusted Extensions 호스트에서 정보에 액세스하는 방법을 정의하는 DAC, MAC 및 레이블 지정 규칙 집합입니다. 고객 사이트에서, 사이트에서 처리되는 정보의 민감도를 정의하고 인증되지 않은 액세스로부터 정보를 보호하는 데 사용되는 대책을 정의하는 규칙 집합입니다.

사용자 인정 범위 일반 사용자가 시스템에서 작업할 수 있는 가능한 모든 레이블의 집합입니다. 사이트의 보안 관리자가 label_encodings 파일에서 범위를 지정합니다. 시스템 인정 범위가 파일의 ACCREDITATION RANGE 섹션 값(상한, 하한, 제약 사항 및 기타 제한의 조합)에 의해 추가적으로 제한된다는 것을 정의하는 올바른 형식의 레이블에 대한 규칙입니다.

사용자 클리어런스 사용자가 언제든지 작업할 수 있는 레이블 집합의 상한을 설정하며 보안 관리자가 할당하는 클리어런스입니다. 사용자는 기본값을 사용할 수도 있고 특정 로그인 세션 중 해당 클리어런스를 더 제한할 수도 있습니다.

설치 팀 Solaris Trusted Extensions 소프트웨어의 설치와 구성을 함께 감독하는 두 명 이상으로 구성된 팀입니다. 팀 구성원 중 한 명은 보안 의사 결정을 담당하고 다른 한 명은 시스템 관리 의사 결정을 담당합니다.

시스템 컴퓨터의 일반 이름입니다. 설치 후 네트워크의 시스템을 호스트라고도 합니다.

시스템 관리자 Trusted Extensions에서 사용자 계정의 비보안 부분을 설정하는 것처럼 표준 시스템 관리 작업을 담당하는 사용자에게 할당되는 신뢰할 수 있는 역할입니다. 보안 관리자와 비교해 보십시오.

시스템 인정 범위 보안 관리자가 label_encodings 파일에 정의한 규칙에 따라 만들어진 모든 유효한 레이블 집합과 Trusted Extensions로 구성된 모든 시스템에서 사용되는 두 개의 관리 레이블입니다. 관리 레이블은 ADMIN_LOW와 ADMIN_HIGH입니다.

신뢰할 수 있는 네트워크 데이터베이스 신뢰할 수 있는 네트워크 원격 호스트 템플리트 tnrhtp와 신뢰할 수 있는 네트워크 원격 호스트 데이터베이스 tnrhdb는 Trusted Extensions 시스템이 통신할 수 있는 원격 호스트를 정의합니다.

신뢰할 수 있는 스트라이프 스푸핑할 수 없는 영역입니다. Trusted CDE에서 신뢰할 수 있는 스트라이프는 화면 하단에 있고 Trusted JDS에서는 스트라이프가 상단에 있을 수 있습니다. 스트라이프는 윈도우 시스템 상태에 대한 시각적 피드백인 신뢰할 수 있는 경로 표시기 및 윈도우 민감도 레이블을 제공합니다. 민감도 레이블이 사용자에게 보이지 않도록 구성된 경우 신뢰할 수 있는 스트라이프는 신뢰할 수 있는 경로 표시기만 보여 주는 아이콘으로 축소됩니다.

신뢰할 수 있는 역할 관리 역할을 참조하십시오.

역할 역할은 로그인할 수 없는 점을 제외하고 사용자와 비슷합니다. 일반적으로 역할은 관리 기능을 할당하는 데 사용되며 특정 명령 및 CDE 작업 집합에 대해서만 사용할 수 있습니다. 관리 역할을 참조하십시오.

원격 호스트 로컬 시스템과 다른 시스템입니다. 원격 호스트는 레이블이 없는 호스트이거나 레이블이 있는 호스트일 수 있습니다.

응용 프로그램 검색 경로 CDE에서 시스템은 검색 경로를 사용하여 응용 프로그램과 특정 구성 정보를 찾습니다. 응용 프로그램 검색 경로는 신뢰할 수 있는 역할에 의해 제어됩니다.

이름 지정 서비스 시스템 간에 서로 통신할 수 있도록 네트워크상의 모든 시스템에 대한 주요 시스템 정보를 포함하는 분산 네트워크 데이터베이스입니다. 이름 지정 서비스를 사용하여 네트워크상에서 시스템 정보를 유지, 관리 및 액세스할 수 있습니다. Sun은 LDAP 이름 지정 서비스를 지원합니다. 이러한 서비스가 없으면 각 시스템이 로컬 `/etc` 파일에 자체 시스템 정보 복사본을 유지해야 합니다.

인정 범위 사용자 또는 자원 클래스에 대해 승인된 민감도 레이블의 집합입니다. 유효한 레이블 집합입니다. 시스템 인정 범위 및 사용자 인정 범위를 참조하십시오.

임의의 액세스 제어 파일이나 디렉토리 소유자가 임의로 허용하거나 거부하는 액세스 유형입니다. Solaris Trusted Extensions에서는 UNIX 권한 비트와 ACL 등 두 종류의 임의 액세스 제어(DAC)를 제공합니다.

장치 장치에는 프린터, 컴퓨터, 테이프 드라이브, 플로피 드라이브, CD-ROM 드라이브, DVD 드라이브, 오디오 장치 및 내부 의사 터미널 장치가 포함됩니다. 장치에는 read equal write equal MAC 정책이 적용됩니다. DVD 드라이브와 같은 이동식 장치에 대한 액세스는 장치 할당에 의해 제어됩니다.

장치 할당 장치를 할당한 사용자 이외의 사용자가 할당 가능 장치 정보에 액세스하는 것을 방지하기 위한 메커니즘입니다. 장치 할당이 해제될 때까지는 장치를 할당한 사용자만 장치 관련 정보에 액세스할 수 있습니다. 사용자가 장치를 할당하려면 보안 관리자가 해당 사용자에게 Device Allocation(장치 할당) 권한을 부여해야 합니다.

주 관리자 조직의 권한 프로필을 새로 만들 수 있으며 보안 관리자 및 시스템 관리자의 권한 범위를 넘어서는 시스템 문제를 해결할 수 있는 것으로 신뢰되는 사용자입니다. 이 역할은 매우 제한적으로 수락됩니다. 사이트를 보다 안전하게 구축하려면 초기 보안 구성 후 이 역할을 만들지 않고 주 관리자 프로필에 아무런 역할도 할당하지 않을 수 있습니다.

초기 레이블 사용자나 역할에 할당된 최소 레이블 및 사용자의 초기 작업 공간의 레이블입니다. 초기 레이블은 사용자나 역할이 작업할 수 있는 가장 낮은 레이블입니다.

최소 레이블 사용자 민감도 레이블의 하한 및 시스템 민감도 레이블의 하한입니다. 사용자의 보안 속성을 지정할 때 보안 관리자가 설정하는 최소 레이블은 최초 로그인 시 사용자의 첫 번째 작업 공간의 민감도 레이블입니다. 보안 관리자가 `label_encodings` 파일에서 최소 레이블 필드에 지정하는 민감도 레이블은 시스템의 하한을 설정합니다.

클라이언트 네트워크에 연결된 시스템입니다.

클리어런스 사용자가 작업할 수 있는 레이블 집합의 상한입니다. 하한은 보안 관리자가 할당한 최소 레이블입니다. 클리어런스 유형은 세션 클리어런스 또는 사용자 클리어런스 중 하나입니다.

파일 시스템 논리적 계층 구조로 설정할 때 체계적이고 구조화된 정보 집합을 구성하는 파일 및 디렉토리의 모음입니다. 파일 시스템은 로컬 시스템 또는 원격 시스템에서 마운트할 수 있습니다.

평가된 구성

인증 기관에 의해 특정 기준을 충족하는 것으로 인증된 구성에서 실행 중인 하나 이상의 Trusted Extensions 호스트입니다. 미국에서는 TCSEC가 기준으로 적용됩니다. 평가 및 인증 기관은 NSA입니다. Solaris Trusted Extensions 소프트웨어는 Common Criteria v2.1 [August 1999](ISO 표준), Evaluation Assurance Level (EAL) 4 및 다양한 보호 프로필에 대해 인증됩니다.

Common Criteria v2(CCv2) 및 보호 프로필은 이전 TCSEC U.S. 표준을 폐기하고 B1+ 레벨로 대체합니다. 미국, 영국, 캐나다, 덴마크, 네덜란드, 독일 및 프랑스에서 CCv2에 대한 상호 인정 협정에 서명했습니다.

Trusted Extensions 구성 대상은 TCSEC C2 및 B1 레벨과 비슷한 기능을 제공하며 몇 가지 추가 기능이 있습니다.

평가된 구성 외부

평가된 구성의 조건을 만족시키는 것으로 입증된 소프트웨어가 보안 조건을 만족시키지 않는 설정으로 구성된 경우 소프트웨어가 *outside the evaluated configuration*에 있다고 합니다.

폐쇄형 네트워크

Trusted Extensions를 통해 구성된 시스템 네트워크입니다. 이 네트워크는 비Trusted Extensions 호스트에서 연결이 끊깁니다. 회선이 Trusted Extensions 네트워크 범위 이상으로 확장되지 않아 물리적으로 연결이 끊길 수도 있고 Trusted Extensions 호스트가 Trusted Extensions 호스트만 인식하기 때문에 소프트웨어적으로 연결이 끊길 수도 있습니다. 네트워크 외부에서 데이터를 입력하려면 Trusted Extensions 호스트에 연결된 주변 기기를 통해서만 가능합니다. 개방형 네트워크와 반대입니다.

프로세스

명령을 호출한 사용자를 대신하여 명령을 실행하는 작업입니다. 프로세스는 사용자 ID(UID), 그룹 ID(GID), 보완 그룹 목록 및 사용자의 감사 ID(AUID)를 포함하여 사용자로부터 여러 보안 속성을 수신합니다. 프로세스가 수신하는 보안 속성에는 실행 중인 명령에 사용 가능한 권한과 현재 작업 공간의 민감도 레이블이 포함됩니다.

프로필 쉘

권한을 인식하는 특수 쉘입니다. 프로필 쉘은 일반적으로 사용자들이 적은 수의 명령만 실행할 수 있게 제한하지만 권한이 있는 경우 이러한 명령을 실행할 수 있도록 허용할 수 있습니다. 프로필 쉘은 신뢰할 수 있는 역할의 기본 쉘입니다.

필수 액세스 제어

파일, 디렉토리 또는 장치의 민감도 레이블을 여기에 액세스하려고 하는 프로세스의 민감도 레이블과 비교하는 액세스 제어입니다. 한 레이블의 프로세스가 하위 레이블의 파일을 읽으려고 할 때 read equal–read down MAC 규칙이 적용됩니다. 한 레이블의 프로세스가 다른 레이블의 디렉토리에 쓰려고 할 때는 write equal-read down MAC 규칙이 적용됩니다.

할당

장치에 대한 액세스를 제어하는 메커니즘입니다. 장치 할당을 참조하십시오.

호스트 이름

네트워크의 다른 시스템에 알려진 시스템 이름입니다. 이 이름은 해당 도메인 내에서 모든 시스템 사이에 고유해야 합니다. 일반적으로 도메인은 단일 조직을 식별합니다. 호스트 이름은 문자, 숫자 및 음수 기호(–)를 조합하여 지정할 수 있지만 음수 기호로 시작하거나 끝날 수 없습니다.

색인

N

R

S

T

U

X

Z

감

결

계

관