Trusted Extensions 구성 및 관리

부품 번호: E53982
2014년 7월

ORACLE

목차

그림

표

이 설명서 사용

- **개요** - 하나 이상의 시스템에서 Oracle Solaris의 Trusted Extensions 기능을 사용으로 설정, 구성 및 유지 관리하는 방법을 설명합니다.
- **대상** - 레이블이 있는 시스템 및 네트워크의 시스템 관리자
- **필요한 지식** - 보안 레이블 및 사이트 보안 요구 사항

제품 설명서 라이브러리

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

Oracle 지원 액세스

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

피드백

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

부 I

Trusted Extensions의 초기 구성

이 장에서는 Trusted Extensions 실행을 위해 Oracle Solaris 시스템을 준비하는 방법을 설명합니다. 이 장에서는 Trusted Extensions 설치 및 사용으로 설정 및 초기 구성 작업에 대한 내용을 다룹니다.

1장. Trusted Extensions의 보안 계획에서는 하나 이상의 Oracle Solaris 시스템에서 Trusted Extensions를 구성할 때 고려해야 할 보안 문제에 대해 설명합니다.

2장. Trusted Extensions용 로드맵 구성은 Oracle Solaris 시스템에서의 다양한 Trusted Extensions 구성에 대한 작업 맵을 제공합니다.

3장. Oracle Solaris에 Trusted Extensions 기능 추가에서는 Trusted Extensions에 대해 Oracle Solaris 시스템을 준비하기 위한 지침을 제공합니다. Trusted Extensions를 사용으로 설정하고 로그인하는 방법을 설명합니다.

4장. Trusted Extensions 구성은 모니터가 있는 시스템에서 Trusted Extensions를 구성하기 위한 지침을 제공합니다.

5장. Trusted Extensions에 대한 LDAP 구성은 Trusted Extensions 시스템에서 LDAP 이름 지정 서비스를 구성하기 위한 지침을 제공합니다.

♦ ♦ ♦ 1 장

1 Trusted Extensions의 보안 계획

Oracle Solaris의 Trusted Extensions 기능은 소프트웨어에서 사용자 사이트의 보안 정책 부분을 구현합니다. 이 장에서는 소프트웨어 구성의 보안 및 관리 측면에 대한 개요를 제공합니다.

Oracle Solaris 11.2에서 Trusted Extensions의 새로운 기능

이 절에서는 기존 고객들을 위해 이 릴리스에서 중요한 새로운 Trusted Extensions 기능에 대한 정보를 보여줍니다.

- Trusted Extensions는 재부트하지 않고 설치 및 구성할 수 있습니다. 자세한 내용은 `labeladm`(1M) 매뉴얼 페이지를 참조하십시오. 절차 정보는 Trusted Extensions 사용으로 설정 [36]을 참조하십시오.
- Trusted Extensions를 부트하기 전에 사용자 정의된 레이블 인코딩 파일을 쉽게 설치할 수 있습니다. 자세한 내용은 `labeladm`(1M) 매뉴얼 페이지를 참조하십시오. 예제 및 절차 정보는 레이블 인코딩 파일을 확인하고 설치하는 방법 [40]을 참조하십시오.
- Trusted Extensions는 `armor` 패키지에서 표준화된 역할의 ARMOR(Authorization Roles Managed on RBAC) 세트를 사용할 수 있습니다. ARMOR 및 Oracle Solaris의 기타 새로운 보안 기능에 대한 자세한 내용은 "Oracle Solaris 11.2의 사용자 및 프로세스 보안 "의 "Oracle Solaris 11.2 권한의 새로운 기능"을 참조하십시오.
- `txzonemgr` 명령은 네트워킹 인터페이스 지정을 위해 보다 빠르고 안정적으로 실행됩니다.

Trusted Extensions의 보안 계획

이 절에서는 Trusted Extensions 소프트웨어를 사용으로 설정 및 구성하기 전에 필요한 계획 수립에 대해 개략적으로 설명합니다.

Trusted Extensions 구성 작업에 대한 점검 목록은 부록 B. Trusted Extensions 구성 점검 목록을 참조하십시오. 사이트를 현지화하려면 “Trusted Extensions의 해외 고객” [20]을 참조하십시오. evaluated configuration(평가된 구성)을 실행하려면 “사이트 보안 정책의 이해” [18]를 참조하십시오.

Trusted Extensions 이해

Trusted Extensions를 사용으로 설정 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 두 Oracle Solaris 기능을 기반으로 하는 레이블이 있는 환경을 제공합니다.

- 대부분의 UNIX® 환경에서 `root`에게 지정된 기능은 몇 가지 관리 역할로 처리됩니다.
- 보안 정책을 대체하는 기능을 특정 사용자와 응용 프로그램에 지정할 수 있습니다.

Trusted Extensions에서 데이터에 대한 액세스는 특수한 보안 태그로 제어됩니다. 이 태그를 레이블이라고 합니다. 레이블은 사용자, 프로세스 및 객체(예: 데이터 파일 및 디렉토리)에 지정됩니다. 이러한 레이블은 UNIX 권한 또는 DAC(임의 액세스 제어) 이외에 mandatory access control(필수 액세스 제어)(MAC)를 제공합니다.

사이트 보안 정책의 이해

Trusted Extensions를 사용하면 사이트의 보안 정책을 Oracle Solaris OS와 효율적으로 통합할 수 있습니다. 따라서 정책의 범위와 Trusted Extensions 소프트웨어에서 해당 정책을 어떻게 구현할 수 있는지 정확하게 이해해야 합니다. 체계적인 구성에서는 사이트 보안 정책

과의 일관성 및 시스템에서 작업을 수행하는 사용자의 편의성이 균형있게 고려되어야 합니다.

Trusted Extensions는 다음 보호 프로파일에 대해 CCRA(Common Criteria Recognition Agreement) Assurance Level EAL4+를 준수하는 것으로 인증되었습니다.

- Advanced Management
- Extended Identification and Authentication
- Labeled Security
- Virtualization

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

Trusted Extensions를 구성할 사용자 계획

`root` 역할 또는 시스템 관리자 역할은 Trusted Extensions를 사용으로 설정하는 작업을 담당합니다. 역할을 만들어 여러 기능 영역 간에 관리 책임을 나눌 수 있습니다.

- security administrator(보안 관리자)는 민감도 레이블 설정 및 지정, 감사 구성, 암호 정책 설정 등과 같은 보안 관련 작업을 담당합니다.
- system administrator(시스템 관리자)는 설정, 유지 보수 및 일반 관리의 비보안 측면을 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 책임을 처리하는 사용자
- 신뢰할 수 있는 응용 프로그램을 실행할 수 있는 관리자가 아닌 사용자, 즉 필요한 경우 보안 정책을 대체하도록 허용된 사용자
- 데이터 그룹 및 데이터 그룹에 액세스할 수 있는 사용자

레이블 전략 고안

레이블을 계획하려면 시스템에서 민감도 레벨 계층을 설정하고 정보를 범주화해야 합니다. `label_encodings` 파일에는 사이트에 대한 해당 유형의 정보가 포함되어 있습니다. Trusted Extensions 소프트웨어와 함께 제공된 `label_encodings` 파일 중 하나를 사용할 수 있습니다. 제공된 파일 중 하나를 수정하거나 사이트와 관련된 새 `label_encodings` 파일을 만들 수도 있습니다. 파일은 Oracle 특정 로컬 확장명 중 적어도 `COLOR NAMES` 섹션을 반드시 포함해야 합니다.

또한 레이블을 계획하려면 레이블 구성을 계획해야 합니다. Trusted Extensions 서비스를 사용으로 설정한 후 시스템이 다중 레이블에서 로그인을 허용해야 하는지 또는 하나의 사용

자 레이블로만 시스템을 구성할 수 있는지 결정해야 합니다. 예를 들어, LDAP 서버는 하나의 레이블이 있는 영역을 가질 수 있는 좋은 대상입니다. 서버의 로컬 관리를 위해 최소 레벨에서 영역을 만듭니다. 시스템을 관리하려면 관리자가 특정 사용자로 로그인하고 사용자 작업 공간에서 적당한 역할로 전환합니다.

자세한 내용은 "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 이름만 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 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.

- "Oracle Solaris 11.2 시스템 설치 " 및 릴리스 노트 설치 절에 설명된 대로 Oracle Solaris 설치 권장 사항을 따릅니다.
- 이 권장 사항에 Trusted Extensions 기능을 추가할 수 있습니다.
  - 다음 시스템에는 제안된 최소값 이상의 메모리가 필요합니다.
    - 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 계획을 위한 지원 정보는 "Oracle Solaris 11.2의 네트워크 배치 계획 "을 참조하십시오.

Trusted Extensions 소프트웨어는 4개의 호스트 유형을 인식합니다. 표 1-1. “Trusted Extensions의 기본 호스트 템플리트”과 같이 각 호스트 유형에는 기본 보안 템플리트가 있습니다.

표 1-1 Trusted Extensions의 기본 호스트 템플리트

호스트 유형	템플리트 이름	용도
`unlabeled`	`admin_low`	전역 영역과 통신할 수 있는 신뢰할 수 없는 호스트를 식별합니다. 이러한 호스트는 레이블이 포함되지 않은 패킷을 보냅니다. 자세한 내용은 unlabeled system(레이블이 없는 시스템)을 참조하십시오.
`cipso`	`cipso`	CIPSO 패킷을 보내는 호스트 또는 네트워크를 식별합니다. CIPSO 패킷에 레이블이 붙습니다.
`netif`	`netif`	`adaptive` 호스트로부터 특정 네트워크 인터페이스에서 패킷을 수신하는 호스트를 식별합니다.
`adaptive`	`adapt`	레이블이 지정되지 않았지만 레이블이 없는 패킷을 `netif` 호스트의 특정 인터페이스로 전송하는 호스트 또는 네트워크를 식별합니다.

네트워크를 다른 네트워크에 연결할 수 있는 경우 액세스 가능한 도메인과 호스트를 지정해야 합니다. 게이트웨이 역할을 담당할 Trusted Extensions 호스트를 식별해야 합니다. 이러한 게이트웨이에 대한 accreditation range(승인 범위) 레이블과 다른 호스트의 데이터를 볼 수 있는 sensitivity label(민감도 레이블)을 식별해야 합니다.

호스트, 게이트웨이 및 네트워크의 레이블 지정은 16장. Trusted Extensions에서 네트워크 관리에 설명되어 있습니다. 원격 시스템에 레이블 지정은 초기 설정 이후 수행됩니다.

Trusted Extensions에서 레이블이 있는 영역 계획

Trusted Extensions 소프트웨어가 전역 영역의 Oracle Solaris에 추가됩니다. 그런 다음 레이블이 있는 비전역 영역을 구성합니다. `label_encodings` 파일에서 레이블마다 하나씩 영역을 만들 필요는 없지만 고유한 각 레이블에 대해 레이블이 있는 영역을 하나 이상 만들 수 있습니다. 제공된 스크립트를 사용하여 `label_encodings` 파일에서 기본 사용자 레이블 및 기본 사용자 클리어런스에 대한 두 개의 레이블이 있는 영역을 쉽게 만들 수 있습니다.

레이블이 있는 영역이 만들어진 후 일반 사용자는 구성된 시스템을 사용할 수 있지만 다른 시스템에는 연결할 수 없습니다. 동일한 레이블에서 실행되는 서비스를 추가로 격리하려면 보조 영역을 만들 수 있습니다. 자세한 내용은 “기본 및 보조 레이블이 있는 영역” [155]을 참조하십시오.

- Trusted Extensions에서 X 서버에 연결하기 위한 로컬 전송은 UNIX 도메인 소켓입니다. 기본적으로 X 서버는 TCP 연결을 수신하지 않습니다.
- 기본적으로 비전역 영역은 신뢰할 수 없는 호스트와 통신할 수 없습니다. 각 영역에서 접근할 수 있는 명시적인 원격 호스트 IP 주소 또는 네트워크 마스크를 지정해야 합니다.

Trusted Extensions 영역 및 Oracle Solaris 영역

Trusted Extensions 영역, 즉, 레이블이 있는 영역은 Oracle Solaris 영역의 브랜드입니다. 레이블이 있는 영역은 주로 데이터를 분리하는 데 사용됩니다. Trusted Extensions에서 일반 사용자는 다른 신뢰할 수 있는 시스템에서 동일하게 레이블이 있는 영역을 제외하고 레이블이 있는 영역에 원격으로 로그인할 수 없습니다. 권한이 부여된 관리자는 전역 영역에서 레이블이 있는 영역에 액세스할 수 있습니다. 영역 브랜드에 대한 자세한 내용은 `brands`(5) 매뉴얼 페이지를 참조하십시오.

Trusted Extensions의 영역 만들기

Trusted Extensions에서 영역 만들기는 Oracle Solaris에서 영역 만들기와 비슷합니다. Trusted Extensions는 프로세스를 단계별로 안내하는 `txzonemgr` 스크립트를 제공합니다. 스크립트에는 레이블이 있는 영역 만들기를 자동화할 수 있는 여러 명령줄 옵션이 있습니다. 자세한 내용은 `txzonemgr`(1M) 매뉴얼 페이지를 참조하십시오.

레이블이 있는 영역에 액세스

제대로 구성된 시스템에서 모든 영역은 네트워크 주소를 사용하여 동일 레이블을 공유하는 다른 시스템과 통신할 수 있어야 합니다. 다음 구성은 다른 레이블이 있는 영역에 대한 레이블이 있는 영역 액세스를 제공합니다.

- **all-zones 인터페이스** - 하나의 `all-zones` 주소가 지정됩니다. 이 기본 구성에서는 하나의 IP 주소만 필요합니다. 모든 영역(전역 영역 및 레이블이 있는 영역)이 이 공유 주소를 통해 원격 시스템의 레이블이 있는 영역과 동일하게 통신할 수 있습니다.

  독점적으로 사용할 전역 영역에 대한 두번째 IP 인스턴스를 만들면 이 구성이 구체화됩니다. 이 두번째 인스턴스는 `all-zones` 주소가 아닙니다. IP 인스턴스를 사용하여 다중 레벨 서비스를 호스트하거나 개인 서브넷에 대한 경로를 제공할 수 있습니다.
- **IP 인스턴스** - Oracle Solaris OS에서와 마찬가지로 전역 영역을 포함하여 모든 영역에 하나의 IP 주소가 지정됩니다. 영역은 IP 스택을 공유합니다. 가장 단순한 사례의 경우 모든 영역이 동일한 물리적 인터페이스를 공유합니다.

  각 영역에 별도의 네트워크 정보 카드(NIC)를 지정하면 이 구성이 구체화됩니다. 이러한 구성은 각 NIC에 연결되는 단일 레이블 네트워크를 물리적으로 구분하는 데 사용됩니다.

  영역당 하나의 IP 인스턴스와 함께 하나 이상의 `all-zones` 인터페이스를 사용하면 더욱 구체화됩니다. 이 구성은 `vni0`과 같은 내부 인터페이스를 사용하여 전역 영역에 접근하는 옵션을 제공하므로 원격 공격으로부터 전역 영역을 보호할 수 있습니다. 예를 들어, 전역 영역의 `vni0` 인스턴스에서 다중 레벨 포트를 바인드하는 권한이 있는 서비스는 공유 스택을 사용하는 영역에서만 내부적으로 접근할 수 있습니다.
- **배타적 IP 스택** - Oracle Solaris에서와 마찬가지로 전역 영역을 포함하여 모든 영역에 하나의 IP 주소가 지정됩니다. 각 레이블이 있는 영역에 대해 가상 네트워크 인터페이스 카드(VNIC)가 만들어집니다.

별도의 네트워크 인터페이스를 통해 각 VNIC를 만들면 이 구성이 구체화됩니다. 이러한 구성은 각 NIC에 연결되는 단일 레이블 네트워크를 물리적으로 구분하는 데 사용됩니다. 배타적 IP 스택으로 구성된 영역은 `all-zones` 인터페이스를 사용할 수 없습니다.

레이블이 있는 영역으로 제한된 응용 프로그램

기본적으로 레이블이 있는 영역은 전역 영역의 이름 서비스를 공유하며 `/etc/passwd` 및 `/etc/shadow` 파일을 비롯한 전역 영역 구성 파일의 읽기 전용 복사본을 포함합니다. 레이블이 있는 영역에서 레이블이 있는 영역에 응용 프로그램을 추가할 계획이고 패키지에서 사용자를 영역에 추가하는 경우 영역에 이러한 파일의 쓰기 가능한 복사본이 필요합니다.

`pkg:/service/network/ftp`와 같은 패키지는 사용자 계정을 만듭니다. 레이블이 있는 영역 내에서 `pkg` 명령을 실행하여 이 패키지를 설치하려면 영역에 별도의 `nscd` 데몬이 실행 중이고 영역에 배타적 IP 주소가 지정되어 있어야 합니다. 자세한 내용은 각 레이블이 있는 영역에 대해 별도의 이름 서비스를 구성하는 방법 [53]을 참조하십시오.

다중 레벨 서비스 계획

기본적으로 Trusted Extensions는 다중 레벨 서비스를 제공하지 않습니다. 대부분의 서비스는 영역 대 영역 서비스, 즉, 단일 레이블 서비스로 쉽게 구성할 수 있습니다. 예를 들어, 단일 레이블이 있는 영역은 레이블이 있는 영역의 레이블에서 실행되는 NFS 서버에 연결할 수 있습니다.

사이트에서 다중 레벨 서비스가 필요한 경우 이러한 서비스는 둘 이상의 IP 주소가 있는 시스템에서 가장 잘 구성됩니다. 다중 레벨 서비스에 필요한 다중 레벨 포트는 전역 영역과 연결된 IP 주소에 지정할 수 있습니다. `all-zones` 주소는 레이블이 있는 영역에서 서비스에 접근하는 데 사용할 수 있습니다.

작은 정보 - 레이블이 있는 영역의 사용자가 다중 레벨 서비스에 액세스하면 안 되는 경우 하나의 IP 주소를 시스템에 지정할 수 있습니다. 이 Trusted Extensions 구성은 일반적으로 랩탑에서 사용됩니다.

Trusted Extensions의 LDAP 이름 지정 서비스 계획

레이블이 있는 시스템 네트워크를 설치하지 않으려면 이 절을 건너뛸 수 있습니다. LDAP 사용을 계획 중인 경우 첫번째 레이블이 있는 영역을 추가하기 전에 시스템을 LDAP 클라이언트로 구성해야 합니다.

시스템 네트워크에서 Trusted Extensions를 실행하려면 이름 지정 서비스로 LDAP를 사용합니다. Trusted Extensions의 경우 시스템 네트워크를 구성할 경우 채워진 Oracle

Directory Server Enterprise Edition(LDAP 서버)이 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 만듭니다. 이 절차는 5장. Trusted Extensions에 대한 LDAP 구성을 참조하십시오.

Trusted Extensions의 감사 계획

기본적으로 감사가 사용으로 설정되어 있습니다. 따라서 기본적으로 `login/logout` 클래스의 모든 이벤트가 감사됩니다. 시스템을 구성 중인 사용자를 감사하려면 구성 프로세스의 초기에 역할을 만들 수 있습니다. 이러한 역할이 시스템을 구성할 경우 감사 레코드에는 이 역할을 맡는 로그인 사용자가 포함됩니다. “Trusted Extensions의 역할 및 사용자 만들기” [54]를 참조하십시오.

Trusted Extensions의 감사 계획은 Oracle Solaris OS에서와 동일합니다. 자세한 내용은 “Oracle Solaris 11.2의 감사 관리 ”를 참조하십시오. Trusted Extensions에서 클래스, 이벤트 및 감사 토큰을 추가해도 감사를 관리하는 방법은 변경되지 않습니다. Trusted Extensions에서의 감사에 대한 추가 관련 정보는 22장. Trusted Extensions와 감사를 참조하십시오.

Trusted Extensions의 사용자 보안 계획

Trusted Extensions 소프트웨어는 사용자에 대한 합리적인 보안 기본값을 제공합니다. 이러한 보안 기본값은 표 1-2. “사용자 계정에 대한 Trusted Extensions 보안 기본값”에 나열되어 있습니다. 나열된 두 값 중 첫번째 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	15
	CRYPT_ALGORITHMS_ALLOW	1,2a,md5,5,6
	CRYPT_DEFAULT	5(sha256)
	LOCK_AFTER_RETRIES	no | yes

파일 이름	키워드	값
	PRIV_DEFAULT	basic
	PRIV_LIMIT	all
	AUTHS_GRANTED	solaris.device.cdrw
	CONSOLE_USER	Console User
	PROFS_GRANTED	Basic Solaris User
/etc/security/tsol/label_encodings의 LOCAL DEFINITIONS 부분	기본 사용자 클리어런스	CNF INTERNAL USE ONLY
	기본 사용자 민감도 레이블	PUBLIC

참고 - IDLECMD 및 IDLETIME 변수는 로그인 사용자의 세션에 적용됩니다. 로그인 사용자가 역할을 맡을 경우 해당 사용자의 IDLECMD 및 IDLETIME 값이 해당 역할에 적용됩니다.

시스템 관리자는 모든 사용자에게 적합한 시스템 기본값을 설정하는 표준 사용자 템플리트를 설정할 수 있습니다. 예를 들어, 기본적으로 각 사용자의 초기 셸은 bash 셸입니다. 시스템 관리자는 각 사용자에게 pfbash 셸을 제공하는 템플리트를 설정할 수 있습니다.

Trusted Extensions의 설치 팀 구성

다음은 가장 안전한 전략에서 가장 안전하지 않은 전략까지 구성 전략에 대해 설명합니다.

- 2명으로 구성된 팀에서 소프트웨어를 구성합니다. 구성 프로세스는 감사됩니다.

  소프트웨어가 사용으로 설정될 때 컴퓨터에 두 명의 사용자가 있습니다. 구성 프로세스 초기에 이 팀은 관리 역할 및 이러한 역할로 전환할 수 있는 신뢰할 수 있는 사용자를 만듭니다. 또한 역할별로 실행되는 이벤트를 감사하도록 감사를 설정합니다. 역할이 사용자에게 지정되고 컴퓨터가 재부트되면 사용자가 로그인하고 관리 역할을 맡습니다. 소프트웨어는 역할별 작업 배분을 강제 적용합니다. 감사 증적에서는 구성 프로세스에 대한 레코드를 제공합니다. 보안 구성 프로세스에 대한 그림은 그림 1-1. “Trusted Extensions 시스템 관리: 역할별 작업 부분”을 참조하십시오.
- 한 사람이 해당 역할을 수락하여 소프트웨어를 사용으로 설정하고 구성합니다. 구성 프로세스는 감사됩니다.

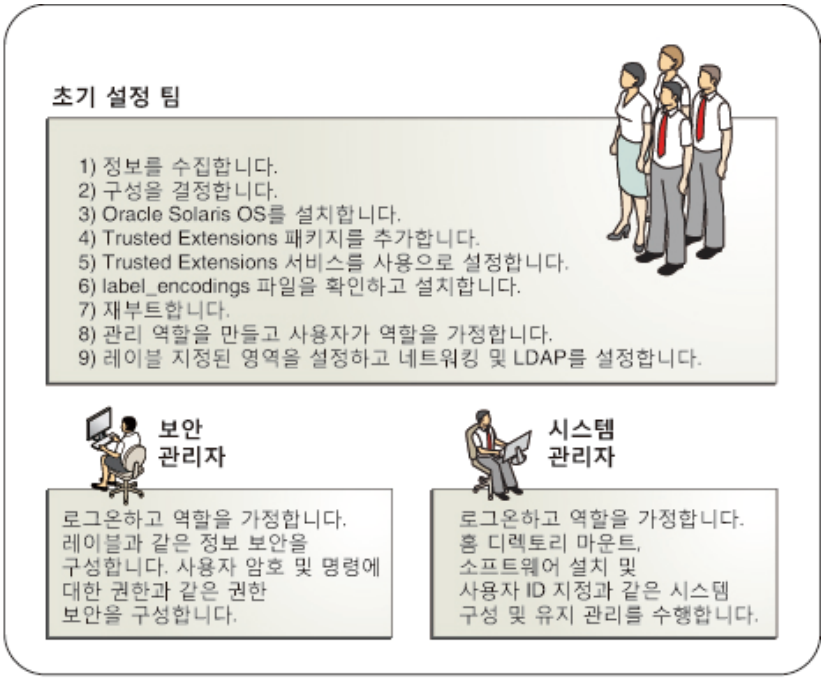
  구성 프로세스의 초기에 root 역할은 추가 역할을 만듭니다. 또한 root 역할은 역할별로 실행되는 이벤트를 감사하도록 감사를 설정합니다. 이러한 추가 역할이 초기 사용자에게 지정되고 컴퓨터가 재부트되면 사용자가 로그인하고 현재 작업에 알맞은 역할을 맡습니다. 감사 증적에서는 구성 프로세스에 대한 레코드를 제공합니다.
- 한 사람이 root 역할을 수락하여 소프트웨어를 사용으로 설정하고 구성합니다. 구성 프로세스는 감사되지 않습니다.

  이 전략을 사용하면 구성 프로세스에 대한 레코드가 보존되지 않습니다.
- 초기 설정 팀은 root 역할을 사용자로 변경합니다.

  root로 활동하는 사용자 이름의 소프트웨어에는 레코드가 보관되지 않습니다. 이 설정은 헤드리스 시스템의 원격 관리에 필요할 수 있습니다.

다음 그림에는 역할별 작업의 배분이 표시됩니다. 보안 관리자는 다른 작업 간에 감사를 구성하고 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 Extensions를 사용으로 설정하기 전 추가 문제 해결

Trusted Extensions를 구성하기 전에 물리적으로 시스템을 보호하고, 영역에 추가할 레이블을 결정하며, 기타 보안 문제를 해결해야 합니다. 단계는 “Trusted Extensions 설치 전 보안 문제 해결” [33]을 참조하십시오.

Trusted Extensions 사용으로 설정 전 시스템 백업

시스템에 저장해야 할 파일이 있는 경우 Trusted Extensions 서비스를 사용으로 설정하기 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.

관리자의 관점에서 Trusted Extensions 사용으로 설정 결과

Trusted Extensions 소프트웨어가 사용으로 설정되고 시스템이 선택적으로 재부트되면 다음 보안 기능이 적용됩니다. 대부분의 기능은 보안 관리자가 구성할 수 있습니다.

- label_encodings file(label_encodings 파일)이 설치 및 구성됩니다.
- 세 개의 Trusted Extensions 네트워크 데이터베이스 `tnrhdb`, `tnrhtp` 및 `tnzonecfg`가 추가됩니다. `tncfg` 명령을 사용하여 관리자는 이러한 신뢰할 수 있는 데이터베이스를 보고 수정할 수 있습니다.
- 장치를 사용하려면 할당되어 있어야 합니다.
- 윈도우화 시스템을 설치할 경우 소프트웨어는 신뢰할 수 있는 데스크탑 Solaris Trusted Extensions (GNOME)를 만듭니다. 이 레이블이 있는 윈도우화 환경은 전역 영역에서 관리 작업 공간을 제공합니다. 이러한 작업 공간은 신뢰할 수 있는 스트라이프에서 볼 수 있는 신뢰할 수 있는 경로로 보호됩니다.

  또한 Trusted Extensions에서는 시스템 관리를 위한 GUI를 제공합니다. 목록은 7장. Trusted Extensions 관리 도구를 참조하십시오.

♦ ♦ ♦ 2 장

2 Trusted Extensions용 로드맵 구성

이 장에서는 Oracle Solaris의 Trusted Extensions 기능을 사용으로 설정하고 구성하기 위한 작업을 설명합니다.

주의 - 원격으로 Trusted Extensions를 사용으로 설정하고 구성하는 경우 Trusted Extensions 환경으로 부트하기 전에 12장. Trusted Extensions에서 원격 관리를 주의 깊게 검토하십시오.

작업 맵: Trusted Extensions 준비 및 사용으로 설정

시스템을 준비하고 Trusted Extensions를 사용으로 설정하려면 다음 작업을 완료하십시오.

작업	수행 방법
시스템 및 Trusted Extensions 네트워크에 대한 정보를 수집하고 결정을 내립니다.	"Trusted Extensions 설치 전 보안 문제 해결" [33]
Trusted Extensions를 사용으로 설정합니다.	Trusted Extensions 사용으로 설정 [36]

작업 맵: Trusted Extensions 구성 선택

다음 작업 맵에 나온 방법 중 하나를 사용하여 시스템에서 Trusted Extensions를 구성합니다.

작업	수행 방법
데모용 Trusted Extensions 시스템을 만듭니다.	"작업 맵: 제공된 기본값으로 Trusted Extensions 구성" [30]
엔터프라이즈 Trusted Extensions 시스템을 만듭니다.	"작업 맵: 사이트의 요구 사항에 맞게 Trusted Extensions 구성" [30]

작업	수행 방법
원격 시스템에서 Trusted Extensions를 구성합니다.	Trusted Extensions를 사용으로 설정하지만 재부트하지 마십시오. 12장. Trusted Extensions에서 원격 관리의 지침을 따릅니다. 그런 다음 모니터가 있는 시스템에 대한 지침을 계속 진행합니다.
Oracle의 Sun Ray 서버에서 Trusted Extensions를 구성합니다.	Sun Ray Products Documentation (http://www.oracle.com/technetwork/server-storage/sunrayproducts/docs/index.html) 웹 사이트를 참조하십시오. 초기 클라이언트-서버 통신을 구성하려면 “호스트 및 네트워크 레이블 지정” [199]을 참조하십시오.

작업 맵: 제공된 기본값으로 Trusted Extensions 구성

기본 구성의 경우 다음 작업을 순서대로 수행합니다.

작업	수행 방법
Trusted Extensions 패키지를 로드합니다.	Oracle Solaris 시스템에 Trusted Extensions 패키지 추가 [35]
Trusted Extensions를 사용으로 설정하고 재부트합니다.	Trusted Extensions 사용으로 설정 [36]
로그인합니다.	Trusted Extensions에 로그인 [37]
두 개의 레이블이 있는 영역을 만듭니다.	기본 Trusted Extensions 시스템을 만드는 방법 [44] 또는 레이블이 있는 영역을 대화식으로 만드는 방법 [44]
영역에 대해 레이블이 있는 작업 공간을 만듭니다.	두 영역 작업 공간에 레이블을 지정하는 방법 [47]

작업 맵: 사이트의 요구 사항에 맞게 Trusted Extensions 구성

작은 정보 - 보안 구성 프로세스의 경우 프로세스의 초기에 역할을 만듭니다.

작업 순서는 다음 작업 맵에 나와 있습니다.

- “레이블이 있는 영역 만들기” [43]의 작업은 필수입니다.
- 사이트의 요구 사항에 따라 기타 구성 작업을 수행합니다.

작업	수행 방법
전역 영역을 구성합니다.	“Trusted Extensions의 전역 영역 설정” [39]
레이블이 있는 영역을 구성합니다.	“레이블이 있는 영역 만들기” [43]
다른 시스템과 통신하려면 네트워킹을 설정합니다.	“ProductShort;에서 네트워크 인터페이스 구성” [48]

작업	수행 방법
LDAP 이름 지정 서비스를 구성합니다. **참고** - LDAP를 사용하지 않는 경우 건너뜁니다.	5장. Trusted Extensions에 대한 LDAP 구성
시스템 구성을 완료합니다.	Trusted Extensions 관리 [87]

♦ ♦ ♦ 3 장

3 Oracle Solaris에 Trusted Extensions 기능 추가

이 장에서는 Oracle Solaris 시스템에서 Trusted Extensions 서비스를 준비하고 사용으로 설정하는 방법을 설명합니다. 이 장에서는 다음 내용을 다룹니다.

초기 설정 팀 책임

Trusted Extensions 기능은 각자 고유한 책임을 지니는 두 사람이 구성하도록 설계되었습니다. 이 작업 배분은 역할별로 적용할 수 있습니다. 관리 역할과 추가 사용자는 설치가 끝날 때까지 만들어지지 않으므로 두 명 이상의 initial setup team(초기 설정 팀)이 Trusted Extensions 사용 설정과 구성에 참여하는 것이 좋습니다.

Trusted Extensions 설치 전 보안 문제 해결

Trusted Extensions를 구성할 각 시스템에 대해 몇 가지 구성 사항에 대한 결정을 내려야 합니다. 예를 들어, 기본 Trusted Extensions 구성을 설치할지 또는 구성을 사용자 정의할지 결정해야 합니다.

▼ Trusted Extensions를 사용으로 설정하기 전 시스템 하드웨어 보안 및 보안 사항 결정

Trusted Extensions를 구성할 각 시스템에 대해 소프트웨어를 사용으로 설정하려면 먼저 다음과 같이 구성과 관련된 사항을 결정해야 합니다.

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

   보안 사이트의 경우 이 단계는 모든 Oracle Solaris 시스템에서 수행됩니다.

   - SPARC 시스템의 경우 PROM 보안 레벨을 선택하고 암호를 제공합니다.
   - x86 시스템의 경우 BIOS 및 GRUB 메뉴를 보호합니다.
   - 모든 시스템에서는 `root`를 암호로 보호합니다.

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 Oracle에서 제공하는 기본 파일을 사용할 수 있습니다. 또한 `/etc/security/tsol` 디렉토리에서 찾을 수 있는 기타 `label_encodings` 파일도 제공합니다. Oracle 파일은 데모용 파일입니다. 해당 파일은 생산 시스템에 적합하지 않을 수도 있습니다.

   파일을 사이트에 맞게 사용자 정의하려면 "Trusted Extensions Label Administration "를 참조하십시오. 편집 지침은 레이블 인코딩 파일을 확인하고 설치하는 방법 [40]을 참조하십시오. Trusted Extensions를 사용으로 설정하고 재부트하기 전에 인코딩 파일을 설치하려면 Trusted Extensions 사용으로 설정 [36]을 참조하십시오.

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

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

전체 레이블 이름	권장되는 영역 이름
PUBLIC	public
CONFIDENTIAL: INTERNAL USE ONLY	internal
CONFIDENTIAL : NEED TO KNOW	needtoknow
CONFIDENTIAL : RESTRICTED	restricted

참고 - 자동 구성 방법에서는 `public` 및 `internal` 영역을 만듭니다.

4. **역할을 만들 시기를 결정합니다.**

   사이트의 보안 정책에 따라 역할을 전환하여 Trusted Extensions를 관리해야 할 수 있습니다. 그러한 경우, 이러한 역할을 구성 프로세스의 초기에 만들어야 합니다. 고유한 역할을 만들거나, 7개 역할이 포함된 `armor` 패키지를 설치하거나, ARMOR 역할 외에 추가 역할을 만들 수도 있습니다. ARMOR 역할에 대한 자세한 내용은 ARMOR standard 설명을 참조하십시오.

   역할을 사용하여 시스템을 구성할 필요가 없는 경우 `root` 역할로 시스템을 구성하도록 선택할 수 있습니다. 이 구성 방법은 보안성이 떨어집니다. `root` 역할은 시스템에서 모든 작업을 수행할 수 있는 반면, 기타 역할은 일반적으로 더욱 제한적인 작업을 수행합니다. 따라서 만든 역할로 구성을 수행하면 구성을 더욱 잘 제어할 수 있습니다.

5. **각 시스템 및 네트워크에 대한 기타 보안 문제를 결정합니다.**

   예를 들어 다음 보안 문제를 고려할 수 있습니다.

   - 시스템에 연결하여 사용하도록 할당할 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.

Trusted Extensions 설치 및 사용으로 설정

Oracle Solaris OS에서 Trusted Extensions 서비스 `svc:/system/labeld:default`는 기본적으로 사용 안함으로 설정됩니다.

`labeld` 서비스는 통신 끝점에 레이블을 연결합니다. 예를 들어 다음에 레이블이 있습니다.

- 모든 영역 및 각 영역에 있는 디렉토리와 파일
- 모든 네트워크 통신
- 창 프로세스가 포함된 모든 프로세스

▼ Oracle Solaris 시스템에 Trusted Extensions 패키지 추가

시작하기 전에 Software Installation 권한 프로파일이 지정되어야 합니다.

1. **초기 사용자로 로그인한 후 터미널 창에서 `root` 역할을 맡습니다.**

```
% su -
Enter Password: xxxxxxxx
#
```

2. **Trusted Extensions 패키지를 다운로드하고 설치합니다.**

   - **다중 레벨 데스크탑을 실행하는 시스템의 경우 다음 패키지를 설치합니다.**

     ```
     # pkg install system/trusted/trusted-extensions
     ```

   - **헤드리스 시스템 또는 다중 레벨 데스크탑이 필요하지 않은 서버의 경우 다음 패키지를 설치합니다.**

     ```
     # pkg install system/trusted
     ```

```
# pkg install system/trusted/trusted-global-zone
```

3. **신뢰할 수 있는 로케일을 설치하려면 로케일에 대한 단축명을 지정합니다.**
   예를 들어, 다음 명령은 일본어 로케일을 설치합니다.

   ```
   # pkg install system/trusted/locale/ja
   ```

▼ Trusted Extensions 사용으로 설정

시작하기 전에 전역 영역에서 `root` 역할을 가진 사용자여야 합니다.

1. **터미널 창에서 `labeld` 서비스를 사용으로 설정합니다.**

   참고 - `labeladm` 명령을 사용하여 `labeld` 서비스를 제어합니다. `labeld` 서비스를 직접 조작하지 마십시오. 자세한 내용은 `labeladm`(1M) 매뉴얼 페이지를 참조하십시오.

   ```
   # labeladm enable -r
   ```

   `labeladm` 명령은 서비스를 사용으로 설정할 때 몇 가지 옵션을 제공합니다.

`-i`	확인 프롬프트를 방지합니다.
`-m`	오류 메시지를 syslog 및 콘솔로 전송합니다.
`-n`	서비스를 사용으로 설정하지 않고 명령을 테스트합니다.
`-r`	서비스 사용으로 설정을 시스템을 재부트한 후로 지연합니다. 이 동작은 이전 릴리스와 동일합니다.

2. **서비스가 사용으로 설정되었는지 확인합니다.**

   ```
   # labeladm info
        Labeling status: pending enable on boot
             Latest log: "/var/user/root/trusted-extensions-install-log"
   Label encodings file: /etc/security/tsol/label_encodings
   ```

   주의 - 원격으로 Trusted Extensions를 사용으로 설정하고 구성하는 경우 12장. Trusted Extensions에서 원격 관리를 주의 깊게 검토하십시오. 원격 관리를 허용하도록 시스템을 구성할 때까지 재부트하지 마십시오. 원격 관리를 위해 Trusted Extensions 시스템을 구성하지 않을 경우 원격 시스템에서 접근하지 못하게 됩니다.

   ---

3. **사용자 정의된 레이블 인코딩 파일이 있으면 지금 설치합니다.**

   ```
   # labeladm encodings path-to-encodings-file
   ```

4. **시스템을 재부트합니다.**

-r 옵션을 사용한 경우 이 명령을 실행해야 합니다.

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

다음 순서 Trusted Extensions에 로그인 [37]을 계속 진행합니다.

▼ Trusted Extensions에 로그인

로그인하면 MAC(Mandatory Access Control)를 인식하고 실행하는 환경인 전역 영역으로 로그인됩니다.

대부분의 사이트에는 시스템을 구성할 때 initial setup team(초기 설정 팀) 역할을 하는 두 명 이상의 관리자가 있습니다.

시작하기 전에 Trusted Extensions 사용으로 설정 [36]을 완료했습니다.

- **Oracle Solaris 설치 중 만든 사용자 계정을 사용하여 로그인합니다.**
  로그인 대화 상자에서 *username*을 입력한 다음 암호를 입력합니다.

참고 - 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 Extensions는 보안되지 않은 암호에 대해 보호 기능을 제공하지만, 사용자가 자신의 암호를 공개하거나 메모하지 못하도록 막을 수는 없습니다.

- **데스크탑 패키지를 설치하지 않은 경우 터미널을 열고 `root` 역할로 전환합니다.**
- **데스크탑 패키지를 설치한 경우에는 다음 단계를 수행합니다.**

  a. **마우스를 사용하여 Status(상태) 창과 Clearance(클리어런스) 창을 없앱니다.**

  b. **`PUBLIC` 레이블에 일치하는 영역이 없다는 대화 상자를 없앱니다.**
     `root` 역할을 맡은 후 영역을 만들게 됩니다.

  c. **신뢰할 수 있는 스트라이프에서 사용자의 로그인 이름을 눌러서 `root` 역할로 전환합니다.**
     풀다운 메뉴에서 `root` 역할을 선택합니다.

보안 고려 사항

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

다음 순서 다음 중 하나의 작업을 계속합니다.

- 전역 영역을 구성하려면 "Trusted Extensions의 전역 영역 설정" [39]으로 이동합니다.
- 기본 시스템을 구성하려면 "레이블이 있는 영역 만들기" [43]로 이동합니다.
- 시스템에 그래픽 디스플레이가 없는 경우 12장. Trusted Extensions에서 원격 관리로 돌아갑니다.

♦ ♦ ♦ 4 장

4 Trusted Extensions 구성

이 장에서는 모니터가 있는 시스템에서 Trusted Extensions를 구성하는 방법에 대해 설명합니다. 제대로 작업하려면 Trusted Extensions 소프트웨어에 레이블 및 영역 구성이 필요합니다. 또한 네트워크 통신, 역할 및 역할을 맡을 수 있는 사용자를 구성할 수 있습니다.

기타 구성 작업은 Trusted Extensions 관리 [87]를 참조하십시오.

Trusted Extensions의 전역 영역 설정

Trusted Extensions 구성을 사용자 정의하려면 다음 작업 맵의 절차를 수행하십시오. 기본 구성을 설치하려면 "레이블이 있는 영역 만들기" [43]로 이동하십시오.

표 4-1 Trusted Extensions의 전역 영역 설정

작업	설명	수행 방법
하드웨어를 보호합니다.	하드웨어 설정을 변경하려면 암호를 입력하도록 요구하여 하드웨어를 보호합니다.	"Oracle Solaris 11.2에서 시스템 및 연결된 장치의 보안 "의 "시스템 하드웨어에 대한 액세스 제어"
레이블을 구성합니다.	사용자 사이트에 대한 레이블을 반드시 구성해야 합니다. 기본 `label_encodings` 파일을 사용하려면 이 단계를 건너뛸 수 있습니다.	레이블 인코딩 파일을 확인하고 설치하는 방법 [40]
IPv6 네트워크를 구성합니다.	Trusted Extensions IPv6 CIPSO 네트워크와의 호환성을 사용으로 설정합니다.	Trusted Extensions에서 IPv6 CIPSO 네트워크를 구성하는 방법 [42]
DOI를 변경합니다.	1이 아닌 DOI(Domain of Interpretation)를 지정합니다.	DOI(Domain of Interpretation)를 구성하는 방법 [42]
LDAP 서버를 구성합니다.	Trusted Extensions LDAP 디렉토리 서버를 구성합니다.	5장. Trusted Extensions에 대한 LDAP 구성

작업	설명	수행 방법
LDAP 클라이언트를 구성합니다.	이 시스템을 Trusted Extensions LDAP 디렉토리 서버의 클라이언트로 만듭니다.	Trusted Extensions에서 전역 영역을 LDAP 클라이언트로 만들기 [83]

▼ 레이블 인코딩 파일을 확인하고 설치하는 방법

인코딩 파일은 통신하는 Trusted Extensions 호스트와 호환되어야 합니다.

참고 - 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 "Trusted Extensions Label Administration "에서 요구 사항, 절차 및 예를 참조하십시오.

주의 - 계속하려면 레이블을 반드시 설치해야 합니다. 그렇지 않으면 구성에 실패합니다.

시작하기 전에 사용자는 보안 관리자입니다. security administrator(보안 관리자)는 `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.

`label_encodings` 파일을 편집하려면 `root` 역할을 가진 사용자여야 합니다.

1. **`label_encodings` 파일을 디스크로 복사합니다.**

   이동식 매체에서 복사하려면 Trusted Extensions에서 이동식 매체의 파일을 복사하는 방법 [69]을 참조하십시오.

2. **터미널 창에서 파일의 구문을 확인합니다.**

   a. **`chk_encodings` 명령을 실행합니다.**

   ```
   # /usr/sbin/chk_encodings /full-pathname-of-label-encodings-file
   ```

   b. **출력을 읽어본 후 다음 중 하나를 수행합니다.**

   - **오류를 해결합니다.**

     명령에서 오류를 보고하는 경우 계속하려면 먼저 오류를 해결해야 합니다. 자세한 내용은 "Trusted Extensions Label Administration "의 3 장, "Creating a Label Encodings File"를 참조하십시오.

- **파일을 활성 `label_encodings` 파일로 만듭니다.**

  ```
  # labeladm encodings full-pathname-of-label-encodings-file
  ```

주의 - 계속하려면 `label_encodings` 파일이 인코딩 확인 테스트를 통과해야 합니다.

예 4-1 명령줄에서 `label_encodings` 구문 검사

이 예에서는 관리자가 명령줄을 사용하여 여러 `label_encodings` 파일을 테스트합니다.

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

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

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

---> VERSION = MYCOMPANY LABEL ENCODINGS  3.0 10/10/2013

---> CLASSIFICATIONS <---

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

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

관리자가 아카이브에 대한 의미 분석 복사본을 인쇄한 후 파일을 설치합니다.

```
# labeladm encodings /tmp/encodings/label_encodings2
```

마지막으로 관리자는 `label_encodings` 파일이 회사 파일인지 확인합니다.

```
# labeladm
     Labeling status: disabled
          Latest log: ""
Label encodings file: /var/tsol/encodings/label-encodings-file
# /usr/sbin/chk_encodings -a /var/tsol/encodings/label-encodings-file | head -4
No errors found in /var/tsol/encodings/label-encodings-file

---> VERSION = MYCOMPANY LABEL ENCODINGS  3.0 10/10/2013
```

다음 순서 LDAP를 구성하거나 레이블이 있는 영역을 만들려면 먼저 시스템을 재부트해야 합니다.

▼ Trusted Extensions에서 IPv6 CIPSO 네트워크를 구성하는 방법

IPv6의 경우 Trusted Extensions는 CALIPSO(Common Architecture Label IPv6 Security Option)를 보안 레이블 지정 프로토콜로 사용합니다. 구성이 필요하지 않습니다. 오래된 Trusted Extensions IPv6 CIPSO 프로토콜을 실행하는 시스템과 통신해야 하는 경우 이 절차를 수행하십시오. 다른 CALIPSO 시스템과 통신하려면 이 절차를 수행하지 마십시오.

주의 - IPv6 프로토콜에 대해 CALIPSO를 사용하는 시스템은 프로토콜이 서로 호환되지 않으므로 오래된 TX IPv6 CIPSO 프로토콜을 사용하는 시스템과 통신할 수 없습니다.

오래된 Trusted Extensions IPv6 CIPSO 옵션에는 패킷의 IPv6 Option Type(IPv6 옵션 유형) 필드에서 사용할 IANA(Internet Assigned Numbers Authority) 번호가 없습니다. 이 절차에서 설정하는 항목은 로컬 네트워크에서 사용할 번호를 제공합니다.

시작하기 전에 독점이긴 하지만 오래된 Trusted Extensions IPv6 CIPSO 보안 레이블 지정 옵션을 사용하는 시스템과 통신해야 하는 경우 이 절차를 수행하십시오.

전역 영역에서 `root` 역할을 가진 사용자입니다.

- **`/etc/system` 파일에 다음 항목을 추가합니다.**

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

일반 오류 부트 중 IPv6 CIPSO 구성이 잘못되었다는 오류 메시지가 표시되면 항목을 수정합니다. 예를 들어 철자를 잘못 입력하면 `sorry, variable 'ip6opt_1d' is not defined in the 'ip' module. Verify that the entry is spelled correctly`라는 메시지가 표시됩니다.

- 항목을 수정합니다.
- `/etc/system` 파일에 올바른 항목을 추가한 후에 시스템을 재부트했는지 확인합니다.

다음 순서 LDAP를 구성하거나 레이블이 있는 영역을 만들려면 먼저 시스템을 재부트해야 합니다.

▼ DOI(Domain of Interpretation)를 구성하는 방법

사이트에서 DOI(Domain of Interpretation) `1`을 사용하지 않는 경우 모든 `security template`에서 security template(보안 템플리트) 값을 수정해야 합니다. 자세한 내용은 “보안 템플리트의 DOI” [188]를 참조하십시오.

시작하기 전에 전역 영역에서 `root` 역할을 가진 사용자입니다.

- **기본 보안 템플리트에서 DOI 값을 지정합니다.**

```
# tncfg -t cipso set doi=n
# tncfg -t admin_low set doi=n
```

참고 - 모든 보안 템플리트에서 DOI 값을 지정해야 합니다.

참조
- "Trusted Extensions의 네트워크 보안 속성" [186]
- 보안 템플리트를 만드는 방법 [202]

다음 순서 LDAP를 사용하려는 경우 5장. Trusted Extensions에 대한 LDAP 구성으로 이동합니다. 레이블이 있는 영역을 만들기 전에 LDAP를 구성해야 합니다.

그렇지 않은 경우 "레이블이 있는 영역 만들기" [43]를 계속 진행하십시오.

레이블이 있는 영역 만들기

이 섹션의 지침에 따라 레이블이 있는 영역을 구성합니다. 자동으로 두 개의 레이블이 있는 영역을 만들거나 수동으로 영역을 만들 수 있는 옵션이 있습니다.

참고 - LDAP를 사용하려는 경우 5장. Trusted Extensions에 대한 LDAP 구성으로 이동합니다. 레이블이 있는 영역을 만들기 전에 LDAP를 구성해야 합니다.

표 4-2 레이블이 있는 영역 만들기

작업	설명	수행 방법
1a. 기본 Trusted Extensions 구성을 만듭니다.	`txzonemgr -c` 명령은 `label_encodings` 파일에서 두 개의 레이블이 있는 영역을 만듭니다. 이 명령은 데스크탑이 없는 시스템에서 실행할 수 있습니다.	기본 Trusted Extensions 시스템을 만드는 방법 [44]
1b. GUI를 사용하여 기본 Trusted Extensions 구성을 만듭니다.	`txzonemgr` 스크립트는 시스템을 구성할 때 적합한 작업을 나타내는 GUI를 만듭니다.	레이블이 있는 영역을 대화식으로 만드는 방법 [44]
1c. 영역 만들기 단계를 수동으로 수행합니다.	`txzonemgr` 스크립트는 시스템을 구성할 때 적합한 작업을 나타내는 GUI를 만듭니다.	레이블이 있는 영역을 대화식으로 만드는 방법 [44]
영역 명령을 사용하여 레이블이 있는 영역을 만듭니다.	레이블이 있는 영역을 하나 만듭니다. 이 절차는 데스크탑이 없는 시스템에서 실행할 수 있습니다.	`zonecfg` 명령을 사용하여 레이블이 있는 영역을 만드는 방법 [48]
2. 레이블이 있는 작업 환경을 만듭니다.	기본 구성에서 두 작업 공간의 레이블을 `PUBLIC` 및 `INTERNAL USE ONLY`로 지정합니다. 이 절차는 데스크탑 시스템에서만 작동합니다.	두 영역 작업 공간에 레이블을 지정하는 방법 [47]
3. (선택 사항) 네트워크의 다른 시스템에 연결합니다.	레이블이 있는 영역 네트워크 인터페이스를 구성하고 전역 영역 및 레이블이 있는 영역을 다른 시스템에 연결합니다.	"ProductShort;에서 네트워크 인터페이스 구성" [48]

▼ 기본 Trusted Extensions 시스템을 만드는 방법

이 절차에서는 두 개의 레이블이 있는 영역과 함께 Trusted Extensions 작업 시스템을 만듭니다. 원격 호스트는 시스템의 보안 템플리트에 지정되지 않았으므로 이 시스템은 원격 호스트와 통신할 수 없습니다.

시작하기 전에 데스크탑이 없는 시스템의 전역 영역에 있거나, Trusted Extensions에 로그인 [37]을 완료하여 데스크탑에 로그인되어 있어야 합니다. `root` 역할을 맡았습니다.

1. **터미널 창을 엽니다.**

   데스크탑에서는 네번째 작업 공간을 사용할 수 있습니다.

2. **(옵션) `txzonemgr` 매뉴얼 페이지를 검토합니다.**

   ```
   # man txzonemgr
   ```

3. **기본 구성을 만듭니다.**

   ```
   # /usr/sbin/txzonemgr -c
   ```

   이 명령은 Oracle Solaris OS 및 Trusted Extensions 소프트웨어를 영역에 복사하고 영역의 스냅샷을 만든 후 원래 영역의 레이블을 지정한 다음 스냅샷을 사용하여 두번째 레이블이 있는 영역을 만듭니다. 영역이 부트됩니다.

   - 첫번째 레이블이 있는 영역은 `label_encodings` 파일의 `Default User Sensitivity Label`(기본 사용자 민감도 레이블) 값을 기준으로 합니다.
   - 두번째 레이블이 있는 영역은 `label_encodings` 파일의 `Default User Clearance`(기본 사용자 클리어런스) 값을 기준으로 합니다.

   이 단계는 약 20분이 소요될 수 있습니다. 영역을 설치하기 위해 스크립트는 레이블이 있는 영역에 대한 전역 영역의 root 암호를 사용합니다.

다음 순서 작업 공간에서 Trusted Extensions 레이블이 있는 영역에 액세스하려면 두 영역 작업 공간에 레이블을 지정하는 방법 [47]으로 이동합니다.

▼ 레이블이 있는 영역을 대화식으로 만드는 방법

`label_encodings` 파일의 모든 레이블에 대해 영역을 만들 필요는 없지만 그렇게 할 수는 있습니다. 관리 GUI는 이 시스템에서 영역을 만들 수 있는 레이블을 열거합니다. 이 절차에서는 두 개의 레이블이 있는 영역을 만듭니다. Trusted Extensions `label_encodings` 파일을 사용할 경우 기본 Trusted Extensions 구성을 만들게 됩니다.

시작하기 전에 Trusted Extensions에 로그인 [37]을 완료했습니다. `root` 역할을 맡았습니다.

아직 영역을 만들지 않았습니다.

1. **`txzonemgr` 명령을 옵션 없이 실행합니다.**

   ```
   # txzonemgr &
   ```

   이 스크립트로 `Labeled Zone Manager` 대화 상자가 열립니다. 이 `zenity` 대화 상자에는 현재의 구성 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.

   작은 정보 - 현재 영역 완료 상태를 보려면 Labeled Zone Manager(레이블이 있는 영역 관리자)에서 Return to Main Menu(주 메뉴로 돌아가기)를 누릅니다. 또는 Cancel(취소) 버튼을 누를 수 있습니다.

2. **다음 방법 중 하나를 선택하여 영역을 설치합니다.**

   - **두 개의 레이블이 있는 영역을 만들려면 대화 상자에서 `public and internal zones`(공용 및 내부 영역)를 선택합니다.**

     - 첫번째 레이블이 있는 영역은 `label_encodings` 파일의 `Default User Sensitivity` Label(기본 사용자 민감도 레이블) 값을 기준으로 합니다.
     - 두번째 레이블이 있는 영역은 `label_encodings` 파일의 `Default User` Clearance(기본 사용자 클리어런스) 값을 기준으로 합니다.

     a. **프롬프트에 응답하여 시스템을 식별합니다.**

        `public` 영역에서 배타적 IP 스택을 사용하거나 DNS에서 정의된 IP 주소를 가지고 있는 경우 DNS에서 정의된 호스트 이름을 사용합니다. 그렇지 않은 경우 시스템의 이름을 사용합니다.

     b. **root 암호에 대한 프롬프트에는 응답하지 마십시오.**

        root 암호는 시스템 설치 시 설정되었습니다. 이 프롬프트에 입력하면 실패합니다.

     c. **영역 로그인 프롬프트에서 사용자 이름과 암호를 입력합니다.**

        그런 다음 `svcs -x` 명령을 실행하여 모든 서비스가 구성되었는지 확인합니다. 표시되는 메시지가 없을 경우 모든 서비스가 구성된 것입니다.

     d. **영역에서 로그아웃하고 창을 닫습니다.**

        프롬프트에 exit을 입력하고 Zone Console(영역 콘솔)에서 Close window(창 닫기)를 선택합니다.

        다른 창에서 두번째 영역 설치가 완료됩니다. 이 영역은 스냅샷을 기반으로 하므로 빠르게 만들어집니다.

e. **두번째 영역 콘솔에 로그인하고 모든 서비스가 실행 중인지 확인합니다.**

```
# svcs -x
#
```

표시되는 메시지가 없을 경우 모든 서비스가 구성된 것입니다. Labeled Zone Manager(레이블이 있는 영역 관리자)가 표시됩니다.

f. **Labeled Zone Manager(레이블이 있는 영역 관리자)에서 내부 영역을 두 번 누릅니다.**

Reboot(재부트)를 선택한 다음 Cancel(취소) 버튼을 눌러 기본 화면으로 돌아갑니다. 모든 영역이 실행 중입니다. 레이블이 없는 스냅샷은 실행 중이 아닙니다.

- **영역을 수동으로 만들려면 Main Menu(주 메뉴)를 선택한 다음 Create a Zone(영역 만들기)을 선택합니다.**

  프롬프트를 따릅니다. GUI에서 영역 만들기를 단계별로 안내합니다.

  영역이 만들어지고 부트되면 전역 영역으로 돌아가서 더 많은 영역을 만들 수 있습니다. 이러한 영역은 스냅샷에서 만들어집니다.

예 4-2 다른 레이블이 있는 영역 만들기

이 예에서 관리자는 기본 `label_encodings` 파일에서 제한된 영역을 만듭니다.

먼저, 관리자는 대화식 모드에서 `txzonemgr` 스크립트를 엽니다.

```
# txzonemgr &
```

그런 다음 관리자는 전역 영역으로 이동하고 `restricted` 이름의 영역을 만듭니다.

```
Create a new zone:restricted
```

그런 다음 관리자는 올바른 레이블을 적용합니다.

```
Select label:CNF : RESTRICTED
```

목록에서 관리자는 Clone(복제) 옵션을 선택한 다음 `snapshot`을 새 영역에 대한 템플리트로 선택합니다.

`restricted` 영역이 사용 가능하게 된 후 관리자는 Boot(부트)를 눌러 두번째 영역을 부트합니다.

`restricted` 영역에 액세스할 수 있도록 관리자는 `label_encodings` 파일의 `Default User Clearance` 값을 `CNF RESTRICTED`로 변경합니다.

▼ 두 영역 작업 공간에 레이블을 지정하는 방법

이 절차에서는 두 개의 레이블이 있는 작업 공간을 만들고 각 레이블이 있는 작업 공간에서 레이블이 있는 창을 엽니다. 이 작업이 완료되면 네트워크에 연결되지 않은 Trusted Extensions 작업 시스템을 가지게 됩니다.

시작하기 전에 기본 Trusted Extensions 시스템을 만드는 방법 [44] 또는 레이블이 있는 영역을 대화식으로 만드는 방법 [44]을 완료했습니다.

사용자는 초기 사용자입니다.

1. **PUBLIC 작업 공간을 만듭니다.**
   PUBLIC 작업 공간의 레이블은 Default User Sensitivity Label(기본 사용자 민감도 레이블)에 해당합니다.

   a. **두번째 작업 공간으로 전환합니다.**

   b. **마우스 오른쪽 버튼을 누르고 Change Workspace Label(작업 공간 레이블 변경)을 선택합니다.**

   c. **PUBLIC을 선택하고 OK(확인)를 누릅니다.**

2. **프롬프트에 암호를 입력합니다.**
   이제 PUBLIC 작업 공간에 있습니다.

3. **터미널 창을 엽니다.**
   창의 레이블은 PUBLIC입니다.

4. **INTERNAL USE ONLY 작업 공간 만들기**
   사이트별 label_encodings 파일을 사용할 경우 Default User Clearance(기본 사용자 클리어런스) 값에서 작업 공간을 만들게 됩니다.

   a. **세번째 작업 공간으로 전환합니다.**

   b. **마우스 오른쪽 버튼을 누르고 Change Workspace Label(작업 공간 레이블 변경)을 선택합니다.**

   c. **INTERNAL USE ONLY를 선택하고 OK(확인)를 누릅니다.**

5. **프롬프트에 암호를 입력합니다.**
   이제 INTERNAL 작업 공간에 있습니다.

6. **터미널 창을 엽니다.**
   창의 레이블은 CONFIDENTIAL : INTERNAL USE ONLY입니다.

시스템이 사용할 준비가 되었습니다. 두 개의 사용자 작업 공간과 하나의 역할 작업 공간이 있습니다. 이 구성에서 레이블이 지정된 영역은 전역 영역과 동일한 IP 주소를 사용하여 다른 시스템과 통신합니다. 레이블이 있는 영역은 기본적으로 `all-zones` 인터페이스로 IP 주소를 공유하므로 이것이 가능합니다.

다음 순서 Trusted Extensions 시스템이 다른 시스템과 통신하도록 하려는 경우 "ProductShort;에서 네트워크 인터페이스 구성" [48]으로 이동하십시오.

▼ zonecfg 명령을 사용하여 레이블이 있는 영역을 만드는 방법

데스크탑에 있지 않은 경우에는 일반 영역 명령을 사용해서 레이블이 있는 영역을 만들어야 합니다. 데스크탑에 있는 경우에도 이 방식을 사용할 수 있습니다. `-t` 옵션은 영역의 브랜드를 지정합니다. 레이블은 명시적으로 설정되어야 합니다. 자세한 내용은 `brands`(5) 매뉴얼 페이지를 참조하십시오.

1. **`zonecfg` 명령을 실행하여 레이블이 있는 영역을 만듭니다.**

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

   이 예제는 이름이 `public`인 영역을 만듭니다.

   ```
   # zonecfg -t SYStsoldef -z public
   ```

2. **`tncfg` 명령을 사용하여 레이블을 설정합니다.**

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

   이 예제는 `public` 영역에 `public` 레이블을 지정합니다.

   ```
   # tncfg -z public set label=PUBLIC
   ```

3. **`zoneadm` 명령을 사용하여 영역을 설치합니다.**

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

   ```
   # zoneadm -z public install
   ```

ProductShort;에서 네트워크 인터페이스 구성

Trusted Extensions 시스템에는 비트맵 디스플레이가 직접 연결된 데스크탑(랩탑 또는 워크스테이션 등)을 실행하는 데 네트워크가 필요하지 않습니다. 하지만 다른 시스템과 통신하려면 네트워크 구성이 필요합니다. `txzonemgr` GUI를 사용하여 레이블이 있는 영역 및 전역 영역에서 다른 시스템에 연결하도록 쉽게 구성할 수 있습니다. 레이블이 있는 영역에 대한 구성

옵션 설명은 "레이블이 있는 영역에 액세스" [22]를 참조하십시오. 다음 작업 맵에서는 네트워크 구성 작업에 대한 설명과 해당 링크를 제공합니다.

표 4-3 Trusted Extensions에서 네트워크 인터페이스 구성 작업 맵

작업	설명	수행 방법
일반 사용자에 대한 기본 시스템을 구성합니다.	시스템에 하나의 IP 주소가 있고 `all-zones` 인터페이스를 사용하여 레이블이 있는 영역과 전역 영역 간에 통신합니다. 원격 시스템과 통신에도 동일한 IP 주소가 사용됩니다.	모든 영역에서 단일 IP 주소를 공유하는 방법 [49]
IP 주소를 전역 영역에 추가합니다.	시스템에 하나 이상의 IP 주소가 있고 전역 영역의 배타적 IP 주소를 사용하여 개인 서브넷에 접근합니다. 레이블이 있는 영역은 이 서브넷에 접근할 수 없습니다.	모든 영역에서 단일 IP 주소를 공유하는 방법 [49]
영역이 IP 스택을 공유하는 모든 영역에 IP 주소를 지정합니다.	시스템에 둘 이상의 IP 주소가 있습니다. 가장 단순한 사례의 경우 영역이 하나의 물리적 인터페이스를 공유합니다.	레이블이 있는 영역에 IP 인스턴스를 추가하는 방법 [50]
`all-zones` 인터페이스를 영역당 IP 인스턴스에 추가합니다.	시스템은 원격 공격으로부터 보호되는 권한이 있는 서비스를 레이블이 있는 영역에 제공할 수 있습니다.	레이블이 있는 영역에 IP 인스턴스를 추가하는 방법 [50]
IP 스택이 배타적인 모든 영역에 IP 주소를 지정합니다.	전역 영역을 포함하여 모든 영역에 하나의 IP 주소가 지정됩니다. 각 레이블이 있는 영역에 대해 VNIC가 만들어집니다.	가상 네트워크 인터페이스를 레이블이 있는 영역에 추가하는 방법 [51]
영역을 원격 영역에 연결합니다.	이 작업에서는 레이블이 있는 영역 및 전역 영역의 네트워크 인터페이스가 동일한 레이블에서 원격 시스템에 접근할 수 있도록 구성합니다.	Trusted Extensions 시스템을 다른 Trusted Extensions 시스템에 연결하는 방법 [52]
영역마다 별도의 `nscd` 데몬을 실행합니다.	각 서브넷에 고유의 이름 서버가 있는 환경에서 이 작업은 영역마다 하나의 `nscd` 데몬을 구성합니다.	각 레이블이 있는 영역에 대해 별도의 이름 서비스를 구성하는 방법 [53]

▼ 모든 영역에서 단일 IP 주소를 공유하는 방법

이 절차에서는 시스템의 모든 영역에서 하나의 IP 주소(전역 영역의 IP 주소)를 사용하여 동일하게 레이블이 지정된 다른 영역이나 호스트에 접근할 수 있도록 합니다. 이 구성은 기본값입니다. 네트워크 인터페이스를 다르게 구성하고 시스템을 기본 네트워크 구성으로 되돌리려는 경우 이 절차를 완료해야 합니다.

시작하기 전에 전역 영역에서 `root` 역할을 가진 사용자여야 합니다.

1. **`txzonemgr` 명령을 옵션 없이 실행합니다.**

   ```
   # txzonemgr &
   ```

   영역 목록이 Labeled Zone Manager(레이블이 있는 영역 관리자)에 표시됩니다. 이 GUI에 대한 자세한 내용은 레이블이 있는 영역을 대화식으로 만드는 방법 [44]을 참조하십시오.

2. **전역 영역을 두 번 누릅니다.**

3. **Configure Network Interfaces(네트워크 인터페이스 구성)를 두 번 누릅니다.**

   인터페이스 목록이 표시됩니다. 다음 특성을 가지는 인터페이스를 찾습니다.

- phys 유형
- 호스트 이름의 IP 주소
- up 상태

4. **호스트 이름에 해당하는 인터페이스를 선택합니다.**
5. **명령 목록에서 Share with Shared-IP Zones(공유 IP 영역과 공유)를 선택합니다.**
   모든 영역은 이 공유 IP 주소를 사용하여 자신의 레이블에서 원격 시스템과 통신할 수 있습니다.
6. **영역 명령 목록으로 돌아가려면 Cancel(취소)을 누릅니다.**

다음 순서 시스템의 외부 네트워크를 구성하려면 Trusted Extensions 시스템을 다른 Trusted Extensions 시스템에 연결하는 방법 [52]으로 이동합니다.

▼ 레이블이 있는 영역에 IP 인스턴스를 추가하는 방법

공유 IP 스택 및 영역별 주소를 사용하고 레이블이 있는 영역을 네트워크에서 다른 시스템의 레이블이 있는 영역에 연결하려는 경우 이 절차가 필요합니다.

이 절차에서는 하나 이상의 레이블이 있는 영역에 대해 하나의 IP 인스턴스, 즉 영역별 주소를 만듭니다. 레이블이 있는 영역은 자신의 영역별 주소를 사용하여 네트워크에서 동일하게 레이블이 지정된 영역과 통신합니다.

시작하기 전에 전역 영역에서 `root` 역할을 가진 사용자여야 합니다.

영역 목록이 Labeled Zone Manager(레이블이 있는 영역 관리자)에 표시됩니다. 이 GUI를 열려면 레이블이 있는 영역을 대화식으로 만드는 방법 [44]을 참조하십시오. 구성하려는 레이블이 있는 영역은 정지되어야 합니다.

1. **Labeled Zone Manager(레이블이 있는 영역 관리자)에서 IP 인스턴스를 추가할 레이블이 있는 영역을 두 번 누릅니다.**
2. **Configure Network Interfaces(네트워크 인터페이스 구성)를 두 번 누릅니다.**
   구성 옵션 목록이 표시됩니다.
3. **Add an IP instance(IP 인스턴스 추가)를 선택합니다.**
4. **시스템에 둘 이상의 IP 주소가 있을 경우 원하는 인터페이스가 있는 항목을 선택합니다.**
5. **이 레이블이 있는 영역의 경우 IP 주소와 접두어 수를 제공합니다.**
   예를 들어, `192.168.1.2/24`를 입력합니다. 접두어 수를 추가하지 않을 경우 넷마스크를 물어봅니다. 이 예에 해당하는 넷마스크는 `255.255.255.0`입니다.

6. **OK(확인)를 누릅니다.**

7. **기본 라우터를 추가하려면 방금 추가한 항목을 두 번 누릅니다.**
프롬프트에서 라우터의 IP 주소를 입력하고 OK(확인)를 누릅니다.

참고 - 기본 라우터를 제거하거나 수정하려면 항목을 제거한 다음 IP 인스턴스를 다시 만듭니다.

---

8. **영역 명령 목록으로 돌아가려면 Cancel(취소)을 누릅니다.**

다음 순서 시스템의 외부 네트워크를 구성하려면 Trusted Extensions 시스템을 다른 Trusted Extensions 시스템에 연결하는 방법 [52]으로 이동합니다.

▼ 가상 네트워크 인터페이스를 레이블이 있는 영역에 추가하는 방법

배타적 IP 스택 및 영역별 주소를 사용하고 레이블이 있는 영역을 네트워크에서 다른 시스템의 레이블이 있는 영역에 연결하려는 경우 이 절차가 필요합니다.

이 절차에서는 VNIC를 만들고 레이블이 있는 영역에 지정합니다.

시작하기 전에 전역 영역에서 `root` 역할을 가진 사용자여야 합니다.

영역 목록이 Labeled Zone Manager(레이블이 있는 영역 관리자)에 표시됩니다. 이 GUI를 열려면 레이블이 있는 영역을 대화식으로 만드는 방법 [44]을 참조하십시오. 구성하려는 레이블이 있는 영역은 정지되어야 합니다.

1. **Labeled Zone Manager(레이블이 있는 영역 관리자)에서 가상 인터페이스를 추가할 레이블이 있는 영역을 두 번 누릅니다.**

2. **Configure Network Interfaces(네트워크 인터페이스 구성)를 두 번 누릅니다.**
구성 옵션 목록이 표시됩니다.

3. **Add a virtual interface(VNIC, 가상 인터페이스 추가)를 두 번 누릅니다.**
시스템에 하나 이상의 VNIC 카드가 있을 경우 하나 이상의 선택 항목이 표시됩니다. 원하는 인터페이스가 있는 항목을 선택합니다.

4. **호스트 이름을 지정하거나 IP 주소와 접두어 수를 지정합니다.**
예를 들어, `192.168.1.2/24`를 입력합니다. 접두어 수를 추가하지 않을 경우 넷마스크를 물어봅니다. 이 예에 해당하는 넷마스크는 `255.255.255.0`입니다.

5. **기본 라우터를 추가하려면 방금 추가한 항목을 두 번 누릅니다.**
프롬프트에서 라우터의 IP 주소를 입력하고 OK(확인)를 누릅니다.

참고 - 기본 라우터를 제거하거나 수정하려면 항목을 제거한 다음 VNIC를 다시 만듭니다.

6. **영역 명령 목록으로 돌아가려면 Cancel(취소)을 누릅니다.**
   VNIC 항목이 표시됩니다. 시스템이 `internal_0`과 같이 *zonename* *_n* 이름을 지정합니다.

다음 순서 시스템의 외부 네트워크를 구성하려면 Trusted Extensions 시스템을 다른 Trusted Extensions 시스템에 연결하는 방법 [52]으로 이동합니다.

▼ Trusted Extensions 시스템을 다른 Trusted Extensions 시스템에 연결하는 방법

이 절차에서는 Trusted Extensions 시스템이 연결할 수 있는 원격 호스트를 추가하여 Trusted Extensions 네트워크를 정의합니다.

시작하기 전에 Labeled Zone Manager(레이블이 있는 영역 관리자)가 표시됩니다. 이 GUI를 열려면 레이블이 있는 영역을 대화식으로 만드는 방법 [44]을 참조하십시오. 전역 영역에서 `root` 역할을 가진 사용자입니다.

1. **Labeled Zone Manager(레이블이 있는 영역 관리자)에서 전역 영역을 두 번 누릅니다.**
2. **Add Multilevel Access to Remote Host(원격 호스트에 다중 레벨 액세스 추가)를 선택합니다.**
   a. **다른 Trusted Extensions 시스템의 IP 주소를 입력합니다.**
   b. **다른 Trusted Extensions 시스템에서 해당하는 명령을 실행합니다.**
3. **영역 명령 목록으로 돌아가려면 Cancel(취소)을 누릅니다.**
4. **Labeled Zone Manager(레이블이 있는 영역 관리자)에서 레이블이 있는 영역을 두 번 누릅니다.**
5. **Add Access to Remote Host(원격 호스트에 액세스 추가)를 선택합니다.**
   a. **다른 Trusted Extensions 시스템에서 동일하게 레이블이 지정된 영역의 IP 주소를 입력합니다.**
   b. **다른 Trusted Extensions 시스템의 영역에서 해당하는 명령을 실행합니다.**

참조
- 15장. 신뢰할 수 있는 네트워킹
- “호스트 및 네트워크 레이블 지정” [199]

▼ 각 레이블이 있는 영역에 대해 별도의 이름 서비스를 구성하는 방법

이 절차에서는 각 레이블이 있는 영역에 별도의 이름 서비스 데몬(nscd)을 구성합니다. 이 구성에서는 각 영역이 해당 영역 레이블에서 실행되는 서브넷에 연결되고 서브넷에는 해당 레이블에 대한 고유 이름 지정 서버가 있는 환경을 지원합니다. 레이블이 있는 영역에서 해당 레이블의 사용자 계정이 필요한 패키지를 설치하려는 경우 영역별로 별개의 이름 서비스를 구성할 수 있습니다. 배경 정보는 "레이블이 있는 영역으로 제한된 응용 프로그램" [23] 및 "Trusted Extensions에서 사용자를 만들기 전에 결정할 사항" [122]을 참조하십시오.

시작하기 전에 Labeled Zone Manager(레이블이 있는 영역 관리자)가 표시됩니다. 이 GUI를 열려면 레이블이 있는 영역을 대화식으로 만드는 방법 [44]을 참조하십시오. 전역 영역에서 root 역할을 가진 사용자입니다.

1. **Labeled Zone Manager(레이블이 있는 영역 관리자)에서 Configure per-zone name service(영역별 이름 서비스 구성)를 선택하고 OK(확인)를 누릅니다.**

   참고 - 이 옵션은 초기 시스템 구성 중 한 번 사용됩니다.

2. **각 영역의 nscd 서비스를 구성합니다.**

   자세한 내용은 nscd(1M) 매뉴얼 페이지를 참조하십시오.

3. **시스템을 재부트합니다.**

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

   재부트 후 Step 1에서 레이블이 있는 영역 관리자를 실행할 1단계 역할을 맡은 사용자 계정이 각 영역에 구성됩니다. 레이블이 있는 영역과 관련된 다른 계정은 영역에 수동으로 추가해야 합니다.

   참고 - LDAP 저장소에 저장된 계정은 전역 영역에서 계속 관리됩니다.

4. **모든 영역에 대해 경로와 이름 서비스 데몬을 확인합니다.**

   a. **Zone Console(영역 콘솔)에서 nscd 서비스를 나열합니다.**

   ```
   zone-name # svcs -x name-service/cache
   svc:/system/name-service/cache:default (name service cache)
   State: online since September 10, 2012  10:10:12 AM PDT
   See: nscd(1M)
   See: /var/svc/log/system-name-service-cache:default.log
   Impact: None.
   ```

   b. **하위 네트워크에 대한 경로를 확인합니다.**

```
zone-name # netstat -rn
```

예 4-3 각 레이블이 있는 영역에서 이름 서비스 캐시 제거

영역당 하나의 이름 서비스 데몬을 테스트한 후 시스템 관리자는 레이블이 있는 영역에서 이름 서비스 데몬을 제거하고 전역 영역에서만 데몬을 실행하기로 결정합니다. 시스템을 기본 이름 서비스 구성으로 되돌리기 위해 관리자는 `txzonemgr` GUI를 열고 전역 영역을 선택한 후 `Unconfigure per-zone name service`(영역별 이름 서비스 구성 해제)를 선택하고 OK(확인)를 누릅니다. 이렇게 하면 레이블이 있는 모든 영역에서 `nscd` 데몬이 제거됩니다. 그런 다음 관리자는 시스템을 재부트합니다.

다음 순서 각 영역에 대해 사용자 및 역할 계정을 구성할 때 세 가지 옵션이 있습니다.

- 다중 레벨 LDAP 디렉토리 서버에서 LDAP 계정을 만들 수 있습니다.
- 별도의 LDAP 디렉토리 서버(레이블당 하나의 서버)에서 LDAP 계정을 만들 수 있습니다.
- 로컬 계정을 만들 수 있습니다.

각 레이블이 있는 영역에서 이름 서비스 데몬을 별도로 구성하면 모든 사용자가 암호를 가지게 됩니다. 사용자는 자신을 인증함으로써 자신의 기본 레이블에 해당하는 영역을 포함하여 레이블이 있는 영역에 대한 액세스 권한을 얻어야 합니다. 또한 관리자가 각 영역에서 로컬로 계정을 만들거나 영역이 LDAP 클라이언트인 LDAP 디렉토리에 계정이 있어야 합니다.

전역 영역의 계정이 Labeled Zone Manager(레이블이 있는 영역 관리자) `txzonemgr`를 실행하는 특수한 경우 계정 정보가 레이블이 있는 영역에 복사되므로 적어도 해당 계정은 각 영역에 로그인할 수 있습니다. 기본적으로 이 계정은 초기 사용자 계정입니다.

Trusted Extensions의 역할 및 사용자 만들기

Trusted Extensions의 역할 만들기는 Oracle Solaris의 역할 만들기와 동일합니다.

표 4-4 Trusted Extensions에서 역할 및 사용자 만들기 작업 맵

작업	설명	수행 방법
ARMOR 역할을 설치합니다.	ARMOR 표준으로 정의된 7개 역할을 만들고 이를 지정합니다.	"Oracle Solaris 11.2의 사용자 및 프로세스 보안 "의 "역할 만들기"의 첫번째 예제
Security Administrator(보안 관리자) 역할을 만듭니다.	보안 관련 작업을 처리할 역할을 만듭니다.	Trusted Extensions에서 보안 관리자 역할을 만드는 방법 [55]
시스템 관리자 역할을 만듭니다.	보안과 관련 없는 시스템 관리 작업을 처리할 역할을 만듭니다.	시스템 관리자 역할을 만드는 방법 [56]
관리자 역할을 수락할 사용자를 만듭니다.	역할을 수락할 수 있는 한 명 이상의 사용자를 만듭니다.	Trusted Extensions에서 역할을 맡을 수 있는 사용자를 만드는 방법 [57]

작업	설명	수행 방법
역할이 해당 작업을 수행할 수 있는지 확인합니다.	역할을 테스트합니다.	Trusted Extensions 역할이 작동하는지 확인하는 방법 [59]
레이블이 있는 영역에 사용자가 로그인할 수 있게 합니다.	일반 사용자가 로그인할 수 있도록 zones 서비스를 시작합니다.	사용자가 레이블이 있는 영역에 로그인할 수 있도록 설정하는 방법 [60]

▼ Trusted Extensions에서 보안 관리자 역할을 만드는 방법

시작하기 전에 전역 영역에서 root 역할을 가진 사용자입니다.

1. **역할을 만들려면 roleadd 명령을 사용합니다.**

   명령에 대한 자세한 내용은 roleadd(1M) 매뉴얼 페이지를 참조하십시오.

   참고 - ARMOR 역할을 사용하려면 "Oracle Solaris 11.2의 사용자 및 프로세스 보안 "의 "역할 만들기" 절에서 ARMOR 예제를 참조하십시오.

   다음 정보에 따라 작업을 수행합니다.

   - 역할 이름 - secadmin
   - -c Local Security Officer

     고유의 정보를 제공하지 마십시오.
   - -m *home-directory*
   - -u *role-UID*
   - -S *repository*
   - -K *key=value*

     Information Security 및 User Security 권한 프로파일을 지정합니다.

   참고 - 모든 관리 역할에 대해 레이블 범위의 관리 레이블을 사용하고, 관리 명령의 사용을 감사하며, lock_after_retries=no를 설정하고, 암호 만료 날짜는 설정하지 않습니다.

   ```
   # roleadd -c "Local Security Officer" -m \
   -u 110 -K profiles="Information Security,User Security" -S files \
   -K lock_after_retries=no -K audit_flags=cusa:no secadmin
   ```

2. **역할에 대한 초기 암호를 제공합니다.**

   ```
   # passwd -r files secadmin
   New Password: xxxxxxxx
   Re-enter new Password: xxxxxxxx
   passwd: password successfully changed for secadmin
   #
   ```

6자 이상의 영숫자로 구성된 암호를 지정합니다. 악의적인 사용자가 암호를 추측하여 무단으로 액세스하지 못하도록 보안 관리자 역할의 암호와 모든 암호를 추측하기 어렵게 지정해야 합니다.

3. **다른 역할을 만들 때 보안 관리자 역할을 기준으로 사용합니다.**

   사용 가능한 역할은 다음과 같습니다.

   - admin 역할 - `System Administrator` 권한 프로파일
   - oper 역할 - `Operator` 권한 프로파일

예 4-4 LDAP에서 보안 관리자 역할 만들기

첫번째 시스템을 로컬 보안 관리자 역할로 구성한 후 관리자는 LDAP 저장소에서 보안 관리자 역할을 만듭니다. 이 시나리오에서 LDAP 클라이언트는 LDAP에서 정의된 보안 관리자 역할로 관리할 수 있습니다.

```
# roleadd -c "Site Security Officer" -d server1:/rpool/pool1/BayArea/secadmin
-u 111 -K profiles="Information Security,User Security" -S ldap \
-K lock_after_retries=no -K audit_flags=cusa:no secadmin
```

관리자는 역할에 대한 초기 암호를 제공합니다.

```
# passwd -r ldap secadmin
New Password: xxxxxxxx
Re-enter new Password: xxxxxxxx
passwd: password successfully changed for secadmin
#
```

다음 순서 로컬 역할을 로컬 사용자에게 지정하려면 Trusted Extensions에서 역할을 맡을 수 있는 사용자를 만드는 방법 [57]을 참조하십시오.

▼ 시스템 관리자 역할을 만드는 방법

시작하기 전에 전역 영역에서 `root` 역할을 가진 사용자입니다.

1. **System Administrator 권한 프로파일을 역할에 지정합니다.**

   ```
   # roleadd -c "Local System Administrator" -m -u 111  -K audit_flags=cusa:no\
   -K profiles="System Administrator" -K lock_after_retries=no sysadmin
   ```

2. **역할에 대한 초기 암호를 제공합니다.**

   ```
   # passwd -r files sysadmin
   New Password: xxxxxxxx
   Re-enter new Password: xxxxxxxx
   passwd: password successfully changed for sysadmin
   ```

#

▼ Trusted Extensions에서 역할을 맡을 수 있는 사용자를 만드는 방법

사이트 보안 정책에 따라 둘 이상의 관리 역할을 수락할 수 있는 사용자를 만들도록 선택할 수 있습니다.

보안 사용자를 만드는 경우 시스템 관리자 역할에서 사용자를 만든 후 초기 암호를 지정하고, 보안 관리자 역할에서 역할과 같은 보안 관련 속성을 지정합니다.

시작하기 전에 전역 영역에서 `root` 역할을 가진 사용자여야 합니다. 또는 책임 구분이 적용된 경우 보안 관리자 및 시스템 관리자의 고유 역할을 맡을 수 있는 사용자가 존재하고 이 절차에서 해당하는 단계를 수행해야 합니다.

1. **사용자를 만듭니다.**

   `root` 역할 또는 시스템 관리자 역할이 이 단계를 수행합니다.

   주석에 고유 정보를 추가하지 마십시오.

   ```
   # useradd -c "Second User" -u 1201 -d /home/jdoe jdoe
   ```

2. **사용자를 만든 후 사용자의 보안 속성을 수정합니다.**

   `root` 역할 또는 보안 관리자 역할이 이 단계를 수행합니다.

   참고 - 역할을 맡을 수 있는 사용자에 대해 계정 잠금을 해제하고 암호 만료 날짜를 설정하지 않습니다. `pfexec` 명령 사용을 감사합니다. `root` 역할만 사용자당 기준에 따라 감사 플래그를 설정할 수 있습니다.

   ```
   # usermod -K lock_after_retries=no -K idletime=5 -K idlecmd=lock \
   -K audit_flags=lo,ex:no jdoe
   ```

   참고 - `idletime` 및 `idlecmd`에 대한 값은 사용자가 역할을 맡을 경우 계속 유효합니다. 자세한 내용은 "Trusted Extensions의 `policy.conf` 파일 기본값" [124]을 참조하십시오.

3. **6자 이상의 영숫자로 구성된 암호를 지정합니다.**

   ```
   # passwd jdoe
   New Password: xxxxxxxx
   Re-enter new Password: xxxxxxxx
   ```

   참고 - 초기 설정 팀은 암호를 선택할 때 악의적인 사용자가 암호를 추측하여 무단으로 액세스하지 못하도록 추측하기 어려운 암호를 선택해야 합니다.

4. **사용자에게 역할을 지정합니다.**
   root 역할 또는 보안 관리자 역할이 이 단계를 수행합니다.

   ```
   # usermod -R oper jdoe
   ```

5. **사용자 환경을 사용자 정의합니다.**

   a. **편리한 권한 부여를 지정합니다.**
      사이트 보안 정책을 확인한 후 첫번째 사용자에게 Convenient Authorizations(편리한 권한 부여) 권한 프로파일을 부여할 수 있습니다. 이 프로파일을 가진 사용자는 장치 할당, 레이블 없이 인쇄, 원격 로그인 및 시스템 종료를 수행할 수 있습니다. 프로파일을 만들려면 편리한 권한 부여를 위해 권한 프로파일을 만드는 방법 [136]을 참조하십시오.

   b. **사용자 초기화 파일을 사용자 정의하기**
      "보안을 위한 사용자 환경 사용자 정의" [129]를 참조하십시오.

   c. **다중 레벨 복사본을 만들고 파일을 연결합니다.**
      다중 레벨 시스템에서는 다른 레이블에 복사하거나 연결할 사용자 초기화 파일을 나열하는 파일을 사용하여 사용자와 역할을 설정할 수 있습니다. 자세한 내용은 ".copy_files 및 .link_files 파일" [126]을 참조하십시오.

예 4-5 useradd 명령을 사용하여 로컬 사용자 만들기

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

이 사용자는 기본 레이블 범위보다 넓은 레이블 범위를 가지게 됩니다. 따라서 root 역할은 16진수 형식의 사용자 최소 레이블 및 클리어런스 레이블을 결정합니다.

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

다음으로 root 역할은 표 1-2, "사용자 계정에 대한 Trusted Extensions 보안 기본값"를 참조한 후에 사용자를 만듭니다. 관리자는 사용자의 홈 디렉토리를 기본값인 /export/home 대신 /export/home1에 둡니다.

```
# useradd -c "Local user for Security Admin" -d /export/home1/jandoe -K
 audit_flags=lo,ex:no \
-K  idletime=8 -K idlecmd=lock -K lock_after_retries=no \
-K min_label=0x0002-08-08 -K clearance=0x0004-08-78 jandoe
```

그런 다음 root 역할은 초기 암호를 제공합니다.

```
# passwd -r files jandoe
```

```
New Password: xxxxxxxx
Re-enter new Password: xxxxxxxx
passwd: password successfully changed for jandoe
#
```

마지막으로 root 역할은 사용자 정의에 보안 관리자 역할을 추가합니다. 역할은 Trusted Extensions에서 보안 관리자 역할을 만드는 방법 [55]에서 만들었습니다.

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

▼ Trusted Extensions 역할이 작동하는지 확인하는 방법

각 역할을 확인하려면 역할을 수락합니다. 그런 다음 해당 역할만 수행할 수 있는 작업을 수행하고 해당 역할이 수행할 수 없는 작업을 시도합니다.

시작하기 전에 DNS 또는 경로 지정을 구성한 경우 역할을 만들고 재부트한 후에 작동 여부를 확인해야 합니다.

1. **각 역할에 대해 역할을 수락할 수 있는 사용자로 로그인합니다.**
2. **역할을 전환합니다.**

   ■ **다중 레벨 데스크탑을 실행하지 않는 시스템에서는 터미널 창을 엽니다.**

   a. **해당 역할로 전환합니다.**

   ```
   % su - rolename
   ```

   b. **PRIV_PFEXEC 플래그가 적용되었는지 확인합니다.**

   ```
   # ppriv $$
   ...
   flags = PRIV_PFEXEC
   ...
   ```

   ■ **다중 레벨 데스크탑에서는 해당 역할로 전환합니다.**
   다음 신뢰할 수 있는 스트라이프에서 사용자 이름은 tester입니다.

   a. **신뢰할 수 있는 스트라이프에서 사용자 이름을 누릅니다.**

   b. **사용자에게 지정된 역할 목록에서 역할을 선택합니다.**

3. **역할을 테스트합니다.**

   사용자 등록 정보를 변경하는 데 필요한 권한 부여는 passwd(1) 매뉴얼 페이지를 참조하십시오.

   - 시스템 관리자 역할은 사용자를 만들고 사용자의 로그인 셸과 같이 `solaris.user.manage` 권한 부여가 필요한 사용자 등록 정보를 수정할 수 있어야 합니다. 시스템 관리자 역할은 `solaris.account.setpolicy` 권한 부여가 필요한 사용자 등록 정보를 변경할 수 없어야 합니다.
   - 보안 관리자 역할은 `solaris.account.setpolicy` 권한 부여가 필요한 사용자 등록 정보를 변경할 수 있어야 합니다. 보안 관리자는 사용자를 만들거나 사용자의 로그인 셸을 변경할 수 없어야 합니다.

▼ 사용자가 레이블이 있는 영역에 로그인할 수 있도록 설정하는 방법

시스템이 재부트되면 장치와 기본 저장소 간의 연결을 다시 설정해야 합니다.

시작하기 전에 레이블이 있는 영역을 한 개 이상 만들었습니다. 시스템을 구성한 후 재부트했습니다. `root` 역할을 맡을 수 있습니다.

1. **로그인하고 `root` 역할을 맡습니다.**

2. **영역 서비스의 상태를 확인합니다.**

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

3. **서비스를 다시 시작합니다.**

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

4. **로그아웃합니다.**

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

Trusted Extensions에서 중앙 홈 디렉토리 만들기

Trusted Extensions에서 사용자는 작업하는 모든 레이블에서 홈 디렉토리에 액세스할 수 있어야 합니다. 기본적으로 홈 디렉토리는 각 영역에서 실행 중인 자동 마운트에 의해 자동으로

만들어집니다. 하지만 NFS 서버를 사용하여 홈 디렉토리를 중앙 집중화하는 경우 사용자에 대한 모든 레이블에서 홈 디렉토리 액세스를 사용으로 설정해야 합니다.

▼ Trusted Extensions에서 홈 디렉토리 서버를 만드는 방법

시작하기 전에 전역 영역에서 `root` 역할을 가진 사용자입니다.

1. **Trusted Extensions 소프트웨어를 홈 디렉토리 서버에 추가하고 레이블이 있는 영역을 구성합니다.**

   사용자는 로그인할 수 있는 모든 레이블에서 홈 디렉토리가 필요하므로 모든 사용자 레이블에서 홈 디렉토리 서버를 만듭니다. 예를 들어, 기본 구성을 만드는 경우 `PUBLIC` 레이블에 대한 홈 디렉토리 서버와 `INTERNAL` 레이블에 대한 서버를 만듭니다.

2. **레이블이 있는 모든 영역에 대해 레이블이 있는 영역에서 파일을 NFS 마운트하는 방법 [178]에 나와 있는 자동 마운트 절차를 수행합니다. 그런 다음 이 절차로 돌아갑니다.**

3. **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.**

4. **홈 디렉토리 서버에서 로그아웃합니다.**

▼ 사용자가 각 NFS 서버에 로그인하여 모든 레이블에서 원격 홈 디렉토리에 액세스할 수 있도록 설정하는 방법

이 절차에서는 사용자가 각 홈 디렉토리 서버에 직접 로그인하여 각 레이블에서 홈 디렉토리를 만들 수 있도록 허용합니다. 중앙 서버에 각 홈 디렉토리를 만들면 사용자는 어느 시스템에서나 자신의 홈 디렉토리에 액세스할 수 있습니다.

또는 관리자가 스크립트를 실행한 다음 자동 마운트를 수정하여 각 홈 디렉토리 서버에 마운트 지점을 만들 수 있습니다. 이 방법은 각 서버에서 자동 마운트를 구성하여 사용자가 원격 홈 디렉토리에 액세스할 수 있도록 설정하는 방법 [62]을 참조하십시오.

시작하기 전에 Trusted Extensions 도메인에 대한 홈 디렉토리 서버가 구성됩니다.

- **사용자가 각 홈 디렉토리 서버에 직접 로그인할 수 있도록 합니다.**
  일반적으로 레이블당 하나의 NFS 서버를 만듭니다.

  a. **각 사용자에게 서버의 레이블에서 각 NFS 서버에 로그인하도록 지시합니다.**

  b. **로그인을 성공하면 사용자에게 서버에서 로그아웃하도록 지시합니다.**
  로그인을 성공하면 사용자에 대한 홈 디렉토리를 서버의 레이블에서 사용할 수 있습니다.

  c. **일반 워크스테이션에서 로그인하도록 지시합니다.**
  기본 레이블에 대한 홈 디렉토리는 홈 디렉토리 서버에서 사용할 수 있습니다. 사용자가 세션의 레이블을 변경하거나 다른 레이블에 작업 공간을 추가한 경우 해당 레이블에 대한 사용자의 홈 디렉토리가 마운트됩니다.

다음 순서 사용자는 로그인 중 레이블 구축기에서 다른 레이블을 선택하여 기본 레이블과 다른 레이블에서 로그인할 수 있습니다.

▼ 각 서버에서 자동 마운트를 구성하여 사용자가 원격 홈 디렉토리에 액세스할 수 있도록 설정하는 방법

이 절차에서는 각 NFS 서버에서 홈 디렉토리에 대한 마운트 지점을 만드는 스크립트를 실행합니다. 그런 다음 마운트 지점을 추가할 서버의 레이블에서 `auto_home` 항목을 수정합니다. 그러면 사용자가 로그인할 수 있습니다.

시작하기 전에 Trusted Extensions 도메인에 대한 홈 디렉토리 서버가 LDAP 클라이언트로 구성됩니다. 사용자 계정은 `useradd` 명령과 함께 `-S ldap` 옵션을 사용하여 LDAP 서버에 만들어졌습니다. `root` 역할을 가진 사용자여야 합니다.

1. **모든 사용자에 대해 홈 디렉토리 마운트 지점을 만드는 스크립트를 작성합니다.**
   샘플 스크립트에서는 다음 사항을 가정합니다.

   - LDAP 서버가 NFS 홈 디렉토리 서버와 다른 서버입니다.
   - 클라이언트 시스템도 다른 시스템입니다.
   - `hostname` 항목은 영역의 외부 IP 주소, 즉 해당 레이블에 대한 NFS 홈 디렉토리 서버를 지정합니다.

- 스크립트는 해당 레이블에서 클라이언트를 서비스하는 영역의 NFS 서버에서 실행됩니다.

```
#!/bin/sh
hostname=$(hostname)
scope=ldap

for j in $(getent passwd|tr ' ' _); do
uid=$(echo $j|cut -d: -f3)
if [ $uid -ge 100 ]; then
home=$(echo $j|cut -d: -f6)
if [[ $home == /home/* ]]; then
user=$(echo $j|cut -d: -f1)
echo Updating home directory for $user
homedir=/export/home/$user
usermod -md ${hostname}:$homedir -S $scope $user
mp=$(mount -p|grep  " $homedir zfs" )
dataset=$(echo $mp|cut -d" " -f1)
if [[ -n $dataset ]]; then
zfs set sharenfs=on $dataset
fi
fi
fi
done
```

2. **각 NFS 서버에서, 해당 레이블에서 클라이언트를 서비스하는 레이블이 있는 영역에서 위의 스크립트를 실행합니다.**

Trusted Extensions 구성 문제 해결

데스크탑을 잘못 구성하면 시스템을 사용하지 못할 수 있습니다.

▼ 데스크탑 패널을 화면 하단으로 이동하는 방법

참고 - 데스크탑 패널을 화면 위쪽으로 이동한 경우 패널이 Trusted Extensions 신뢰할 수 있는 스트라이프로 가려집니다. 패널은 작업 공간의 측면이나 하단에 있어야 합니다. 기본 작업 공간에는 두 개의 데스크탑 패널이 있습니다.

시작하기 전에 시스템의 데스크탑 패널 위치를 변경하려면 `root` 역할을 가진 사용자여야 합니다.

1. **화면 하단에 하나의 데스크탑 패널이 표시되어 있는 경우 다음 작업 중 하나를 수행합니다.**

   - **마우스 오른쪽 버튼을 사용하여 애플릿을 표시된 패널에 추가합니다.**

- **다음 단계를 수행하여 숨겨진 두번째 데스크탑 패널을 화면 하단으로 이동합니다.**

2. **그렇지 않으면 자신의 로그인에 대해서만 또는 시스템의 모든 사용자에 대해 하단 데스크탑 패널을 만듭니다.**

   - **자신의 로그인에 대해서만 패널을 이동하려면 홈 디렉토리에서 `top_panel_screen`*n* 파일을 편집합니다.**

     a. **패널 위치를 정의하는 파일이 포함된 디렉토리로 변경합니다.**

     ```
     % cd $HOME/.gconf/apps/panel/toplevels
     % ls
     %gconf.xml    bottom_panel_screen0/   top_panel_screen0/
     % cd top_panel_screen0
     % ls
     %gconf.xml             top_panel_screen0/
     ```

     b. **상단 패널의 위치를 정의하는 `%gconf.xml` 파일을 편집합니다.**

     ```
     % vi %gconf.xml
     ```

     c. **모든 방향 행을 찾아 `top` 문자열을 `bottom`으로 바꿉니다.**
     예를 들어, 방향 행은 다음과 유사하게 나타납니다.

     ```
     /toplevels/orientation" type="string">
     <stringvalue>bottom</stringvalue>
     ```

   - **시스템의 모든 사용자에 대해 패널을 이동하려면 데스크탑 구성을 수정합니다.**
     `root` 역할의 터미널 창에서 다음 명령을 수행합니다.

     ```
     # export SETUPPANEL="/etc/gconf/schemas/panel-default-setup.entries"
     # export TMPPANEL="/tmp/panel-default-setup.entries"
     # sed 's/<string>top<\/string>/<string>bottom<\/string>/' $SETUPPANEL > $TMPPANEL
     # cp $TMPPANEL $SETUPPANEL
     # svcadm restart gconf-cache
     ```

3. **시스템에서 로그아웃하고 다시 로그인합니다.**
   둘 이상의 데스크탑 패널이 있는 경우 패널은 화면 하단에 쌓입니다.

추가 Trusted Extensions 구성 작업

다음 작업은 요구 사항에 맞게 Trusted Extensions 시스템을 구성할 때 유용할 수 있습니다. 마지막 작업에서는 Oracle Solaris에서 Trusted Extensions 기능 제거를 사용으로 설정합니다.

표 4-5 추가 Trusted Extensions 구성 작업 맵

작업	설명	수행 방법
사용자에게 사이트 보안에 대해 알립니다.	로그인 시 보안 메시지를 표시합니다.	"Oracle Solaris 11 보안 지침 "의 "배너 파일에 보안 메시지를 배치하는 방법" "Oracle Solaris 11 보안 지침 "의 "데스크탑 로그인 화면에 보안 메시지를 배치하는 방법"
기존 영역과 동일한 레이블에서 작동되는 서비스를 포함하는 레이블이 있는 영역을 만듭니다.	기본 영역과 동일한 레이블에 보조 영역을 만듭니다.	보조 레이블이 있는 영역을 만드는 방법 [65]
모든 레이블의 디렉토리 및 파일을 보유할 데이터 세트를 만듭니다.	최소 오버헤드로 파일의 레이블을 다시 지정할 수 있는 데이터 세트를 만들고 마운트합니다.	다중 레벨 데이터 세트를 만들고 공유하는 방법 [66]
모든 레이블에서 홈 디렉토리 서버를 만듭니다.	각 레이블에 하나씩 여러 홈 디렉토리 서버를 만듭니다. 또는 다중 레벨 홈 디렉토리 서버를 만듭니다.	Trusted Extensions에서 홈 디렉토리 서버를 만드는 방법 [61]
역할을 맡을 수 있는 초기 사용자를 만듭니다.	역할을 맡는 경우 시스템을 관리할 신뢰할 수 있는 사용자를 만듭니다.	Trusted Extensions에서 역할을 맡을 수 있는 사용자를 만드는 방법 [57]
Trusted Extensions를 제거합니다.	시스템에서 Trusted Extensions 및 모든 신뢰할 수 있는 데이터를 제거합니다. 또한 Oracle Solaris 시스템에서 Trusted Extensions 실행을 준비합니다.	시스템에서 Trusted Extensions를 제거하는 방법 [70]

▼ 보조 레이블이 있는 영역을 만드는 방법

보조 레이블이 있는 영역은 서비스를 다른 영역에 격리하면서도 동일한 레이블에서 실행할 수 있도록 하는 데 유용합니다. 자세한 내용은 "기본 및 보조 레이블이 있는 영역" [155]을 참조하십시오.

시작하기 전에 기본 영역은 반드시 있어야 합니다. 보조 영역에는 배타적 IP 주소가 있어야 하며 데스크탑이 필요하면 안 됩니다.

전역 영역에서 `root` 역할을 가진 사용자여야 합니다.

1. **보조 영역을 만듭니다.**

   명령줄이나 레이블이 있는 영역 GUI `txzonemgr`을 사용할 수 있습니다.

   ■ **명령줄 사용**

   ```
   # tncfg -z secondary-label-service primary=no
   # tncfg -z secondary-label-service label=public
   ```

   ■ **`txzonemgr` 사용**

   ```
   # txzonemgr &
   ```

Create a new zone(새 영역 만들기)으로 이동하고 프롬프트를 따릅니다.

참고 - 넷마스크는 접두어 형식으로 입력해야 합니다. 예를 들어, `255.255.254.0` 넷마스크에 상응하는 접두어는 `/23`입니다.

2. **영역이 보조 영역인지 확인합니다.**

```
# tncfg -z zone info primary
primary=no
```

예 4-6 공용 스크립트를 위한 영역 만들기

이 예에서 관리자는 스크립트 및 일괄 처리 작업을 실행하기 위한 공용 영역을 격리합니다.

```
# tncfg -z public-scripts primary=no
# tncfg -z public-scripts label=public
```

▼ 다중 레벨 데이터 세트를 만들고 공유하는 방법

다중 레벨 데이터 세트는 정보를 다운그레이드하거나 업그레이드할 때 유용한 컨테이너입니다. 자세한 내용은 "파일의 레이블 다시 지정을 위한 다중 레벨 데이터 세트" [170]를 참조하십시오. 다중 레벨 데이터 세트는 여러 레이블에서 여러 NFS 클라이언트에 파일을 제공하는 다중 레벨 NFS 파일 서버에도 유용합니다.

시작하기 전에 다중 레벨 데이터 세트를 만들려면 전역 영역에서 `root` 역할이어야 합니다.

1. **다중 레벨 데이터 세트를 만듭니다.**

```
# zfs create -o mountpoint=/multi -o multilevel=on rpool/multi
```

`rpool/multi`는 전역 영역에서 `/multi`에 마운트되는 다중 레벨 데이터 세트입니다.

데이터 세트의 상위 레이블 범위를 제한하려면 예 4-7. "ADMIN_HIGH 아래의 최상위 레이블로 다중 레벨 데이터 세트 만들기"을 참조하십시오.

2. **다중 레벨 데이터 세트가 마운트되어 있고 마운트 지점에 ADMIN_LOW 레이블이 있는지 확인합니다.**

```
# getlabel /multi
/multi: ADMIN_LOW
```

3. **상위 파일 시스템을 보호합니다.**

풀의 모든 파일 시스템에 대해 ZFS 등록 정보를 `off`로 설정됩니다.

```
# zfs set devices=off rpool/multi
```

```
# zfs set exec=off rpool/multi
# zfs set setuid=off rpool/multi
```

4. **(옵션) 풀의 압축 등록 정보를 설정합니다.**

   일반적으로 압축은 ZFS의 파일 시스템 레벨에서 설정됩니다. 하지만 이 풀의 모든 파일 시스템은 데이터 파일이므로 압축은 풀의 최상위 레벨 데이터 세트에서 설정됩니다.

   ```
   # zfs set compression=on rpool/multi
   ```

   또한 "Oracle Solaris 11.2의 ZFS 파일 시스템 관리 "의 "ZFS 압축, 중복 제거 및 암호화 등록 정보 간의 상호 작용"을 참조하십시오.

5. **다중 레벨 데이터 세트에 필요한 각 레이블에 대한 최상위 디렉토리를 만듭니다.**

   ```
   # cd /multi
   # mkdir public internal
   # chmod 777 public internal
   # setlabel PUBLIC public
   # setlabel "CNF : INTERNAL" internal
   ```

6. **액세스하도록 승인된 모든 레이블이 있는 영역에서 LOFS를 사용하여 다중 레벨 데이터 세트를 마운트합니다.**

   예를 들어 다음 일련의 `zonecfg` 명령은 `public` 영역에서 데이터 세트를 마운트합니다.

   ```
   # zonecfg -z public
   zonecfg:public> add fs
   zonecfg:public:fs> set dir=/multi
   zonecfg:public:fs> set special=/multi
   zonecfg:public:fs> set type=lofs
   zonecfg:public:fs> end
   zonecfg:public> exit
   ```

   다중 레벨 데이터 세트는 마운트 영역과 동일한 레이블에서 파일 쓰기 및 하위 레벨 파일 읽기를 허용합니다. 마운트된 파일의 레이블을 보고 설정할 수 있습니다.

7. **NFS를 사용하여 다른 시스템과 다중 레벨 데이터 세트를 공유하려면 다음을 수행합니다.**

   a. **전역 영역에서 NFS 서비스를 다중 레벨 서비스로 만듭니다.**

      ```
      # tncfg -z global add mlp_private=2049/tcp
      # tncfg -z global add mlp_private=111/udp
      # tncfg -z global add mlp_private=111/tcp
      ```

   b. **NFS 서비스를 다시 시작합니다.**

      ```
      # svcadm restart nfs/server
      ```

   c. **다중 레벨 데이터 세트를 공유합니다.**

      ```
      # share /multi
      ```

NFS 마운트된 다중 레벨 데이터 세트는 마운트 영역과 동일한 레이블에서 파일 쓰기 및 하위 레벨 파일 읽기를 허용합니다. 마운트된 파일의 레이블을 안정적으로 보거나 설정할 수 없습니다. 자세한 내용은 "다른 시스템에서 다중 레벨 데이터 세트 마운트" [171]를 참조하십시오.

예 4-7 ADMIN_HIGH 아래의 최상위 레이블로 다중 레벨 데이터 세트 만들기

이 예에서 관리자는 기본값인 ADMIN_HIGH보다 낮은 상한 또는 최상위 레이블로 다중 데이터 세트를 만듭니다. 데이터 세트 생성 시 관리자는 mslabel 등록 정보에 레이블 상한을 지정합니다. 이 상한은 전역 영역 프로세스에서 다중 레벨 데이터 세트에 파일 또는 디렉토리를 만들지 못하게 합니다. 레이블이 있는 영역 프로세스만 데이터 세트에 디렉토리 및 파일을 만들 수 있습니다. multilevel 등록 정보가 on이므로 mslabel 등록 정보는 단일 레이블 데이터 세트에 대한 레이블이 아니라 상한을 설정합니다.

```
# zfs create -o mountpoint=/multiIUO -o multilevel=on \
   -o mlslabel="CNF : INTERNAL" rpool/multiIUO
```

그런 다음 관리자는 각 레이블이 있는 영역에 로그인하여 마운트된 데이터 세트에 해당 레이블의 디렉토리를 만듭니다.

```
# zlogin public
# mkdir /multiIUO
# chmod 777 /multiIUO
# zlogin internal
# mkdir /multiIUO
# chmod 777 /multiIUO
```

영역이 재부트된 후 다중 레벨 데이터 세트는 마운트 영역의 레이블에서 권한이 부여된 사용자에게 표시됩니다.

다음 순서 사용자가 파일의 레이블을 다시 지정할 수 있도록 설정하려면 레이블이 있는 영역에서 파일의 레이블을 재지정할 수 있게 설정하는 방법 [162]을 참조하십시오.

파일의 레이블 다시 지정에 대한 자세한 내용은 "Trusted Extensions 사용자 설명서 "의 "다중 레벨 데이터 세트에서 데이터를 업그레이드하는 방법" 및 "Trusted Extensions 사용자 설명서 "의 "다중 레벨 데이터 세트에서 데이터를 다운그레이드하는 방법"을 참조하십시오.

▼ Trusted Extensions에서 이동식 매체에 파일을 복사하는 방법

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

참고 - Trusted Extensions 구성 중 root 역할은 이동식 매체를 사용하여 label_encodings 파일을 모든 시스템에 전송할 수 있습니다. 매체 레이블을 Trusted Path로 지정합니다.

시작하기 전에 관리 파일을 복사하려면 전역 영역에서 `root` 역할을 가진 사용자여야 합니다.

1. **해당 장치를 할당합니다.**
   예를 들어, 다음 명령은 JAZ 또는 ZIP 드라이브나 USB 핫 플러그 가능 매체와 같은 이동식 디스크를 할당합니다.

   ```
   # allocate rmdisk0
   ```

   윈도우화 시스템에서는 장치 관리자를 사용할 수 있습니다. 2개의 파일 브라우저를 열고 장치에서 디스크로 파일을 끕니다. 자세한 내용은 "Trusted Extensions 사용자 설명서 "의 "Trusted Extensions에서 장치를 할당하는 방법"을 참조하십시오.

2. **장치를 할당 해제합니다.**

   ```
   # deallocate rmdisk0
   ```

   장치 관리자를 사용하여 장치를 할당 해제하려면 "Trusted Extensions 사용자 설명서 "의 "Trusted Extensions에서 장치를 할당 해제하는 방법"을 참조하십시오.

참고 - 복사된 파일의 민감도 레이블을 사용하여 매체에 레이블을 물리적으로 추가합니다.

예 4-8 구성 파일을 모든 시스템에서 동일하게 유지

시스템 관리자는 모든 시스템을 동일한 설정으로 구성하려고 합니다. 따라서 구성되는 첫번째 시스템에서 관리자는 재부트 중에 삭제할 수 없는 디렉토리를 만듭니다. 관리자는 모든 시스템에서 동일하거나 유사해야 하는 파일을 해당 디렉토리에 넣습니다.

예를 들어, 관리자는 `policy.conf` 파일과 이 사이트에 대한 기본 `login` 및 `passwd` 파일을 수정합니다. 따라서 관리자는 다음 파일을 영구 디렉토리에 복사합니다.

```
# mkdir /export/commonfiles
# cp  /etc/security/policy.conf \
# cp  /etc/default/login \
# cp  /etc/default/passwd \
/export/commonfiles
```

관리자가 CD-ROM 드라이브에 CD를 삽입하고 할당합니다.

```
# allocate cdrom0
```

파일을 CD에 전송한 후 관리자가 `Trusted Path` 레이블을 붙입니다.

▼ Trusted Extensions에서 이동식 매체의 파일을 복사하는 방법

파일을 바꾸기 전에 원본 Trusted Extensions 파일의 이름을 바꾸는 것이 좋습니다. 시스템을 구성할 때 `root` 역할은 관리 파일의 이름을 변경하고 이 파일을 복사합니다.

시작하기 전에 관리 파일을 복사하려면 전역 영역에서 `root` 역할을 가진 사용자여야 합니다.

1. **해당 장치를 할당합니다.**

   ```
   # allocate cdrom0
   ```

   윈도우화 시스템에서는 장치 관리자를 사용할 수 있습니다. 자세한 내용은 "Trusted Extensions 사용자 설명서 "의 "Trusted Extensions에서 장치를 할당하는 방법"을 참조하십시오.

2. **시스템에 동일한 이름을 가진 파일이 있는 경우 원본 파일을 새 이름으로 복사합니다.**

   예를 들어, `.orig`를 원본 파일의 끝에 추가합니다.

   ```
   # cp /etc/security/policy.conf /etc/security/policy.conf.orig
   ```

3. **할당된 매체의 파일을 디스크의 위치로 복사한 후 전송합니다.**

   예를 들어, `policy.conf` 파일을 전송합니다.

   ```
   # cp /dev/rdsk/cdrom0/trusted/* /tmp
   # cp /tmp/policy.conf /etc/security/policy.conf
   ```

4. **장치를 할당 해제합니다.**

   ```
   # deallocate cdrom0
   ```

   장치 관리자에서 할당 해제하려면 "Trusted Extensions 사용자 설명서 "의 "Trusted Extensions에서 장치를 할당 해제하는 방법"을 참조하십시오.

5. **매체를 꺼내고 분리합니다.**

   ```
   # eject cdrom0
   ```

▼ 시스템에서 Trusted Extensions를 제거하는 방법

Oracle Solaris 시스템에서 Trusted Extensions 기능을 제거하려면 특정 단계를 수행합니다.

시작하기 전에 전역 영역에서 `root` 역할을 가진 사용자입니다.

1. **보관할 레이블이 있는 영역의 데이터를 아카이브합니다.**

   이동식 매체의 경우 각 아카이브된 영역에 영역의 민감도 레이블이 적힌 스티커를 붙입니다.

2. **레이블이 있는 영역을 시스템에서 제거합니다.**

   자세한 내용은 "Oracle Solaris 영역 만들기 및 사용 "의 "비전역 영역 제거 방법"을 참조하십시오.

3. **Trusted Extensions 서비스를 사용 안함으로 설정합니다.**

   ```
   # labeladm disable -r
   ```

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

4. **(옵션) 시스템을 재부트합니다.**

5. **시스템을 구성합니다.**

   기본 네트워킹, 이름 지정 서비스 및 파일 시스템 마운트와 같은 다양한 서비스를 Oracle Solaris 시스템에 대해 구성해야 할 수 있습니다.

♦ ♦ ♦ 5 장

5 Trusted Extensions에 대한 LDAP 구성

이 장에서는 Trusted Extensions에 사용하도록 Oracle Directory Server Enterprise Edition(LDAP 서버)을 구성하는 방법을 다룹니다. LDAP 서버는 LDAP 서비스를 제공합니다. LDAP는 Trusted Extensions에서 지원되는 이름 지정 서비스입니다. 마지막 섹션 "Trusted Extensions LDAP 클라이언트 만들기" [83]에서는 LDAP 클라이언트를 구성하는 방법을 다룹니다.

LDAP 서버를 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.

LDAP 서버를 구성하려면 다음 작업 맵 중 하나의 지시를 따릅니다.

Trusted Extensions 네트워크에서 LDAP 구성

표 5-1 Trusted Extensions 네트워크에서 LDAP 구성 작업 맵

작업	설명	수행 방법
Trusted Extensions LDAP 서버를 설정합니다.	기존 Oracle Directory Server Enterprise Edition가 없는 경우 첫번째 Trusted Extensions 시스템을 LDAP 서버로 만듭니다. 이 시스템에는 레이블이 있는 영역이 없습니다. 다른 Trusted Extensions 시스템은 이 서버의 클라이언트입니다.	LDAP 서버에 대한 정보 수집 [74] Oracle Directory Server Enterprise Edition 설치 [75] Oracle Directory Server Enterprise Edition 용 로그 구성 [78]
Trusted Extensions 데이터베이스를 서버에 추가합니다.	LDAP 서버를 Trusted Extensions 시스템 파일의 데이터로 채웁니다.	Oracle Directory Server Enterprise Edition 채우기 [80]
다른 모든 Trusted Extensions 시스템을 이 서버의 클라이언트로 구성합니다.	다른 시스템을 Trusted Extensions와 함께 구성할 때는 시스템을 이 LDAP 서버의 클라이언트로 만듭니다.	Trusted Extensions에서 전역 영역을 LDAP 클라이언트로 만들기 [83]

Trusted Extensions 시스템에서 LDAP 프록시 서버 구성

Oracle Solaris 시스템에서 실행 중인 기존 Oracle Directory Server Enterprise Edition이 있는 경우 이 작업 맵을 사용합니다.

표 5-2 Trusted Extensions 시스템에서 LDAP 프록시 서버 구성 작업 맵

작업	설명	수행 방법
Trusted Extensions 데이터베이스를 서버에 추가합니다.	Trusted Extensions 네트워크 데이터베이스 `tnrhdb` 및 `tnrhtp`를 LDAP 서버에 추가해야 합니다.	Oracle Directory Server Enterprise Edition 채우기 [80]
LDAP 프록시 서버를 설정합니다.	하나의 Trusted Extensions 시스템을 다른 Trusted Extensions 시스템에 대한 프록시 서버로 만듭니다. 다른 시스템에서는 이 프록시 서버를 사용하여 LDAP 서버에 연결합니다.	LDAP 프록시 서버 만들기 [82]
LDAP용 다중 레벨 포트를 포함하도록 프록시 서버를 구성합니다.	특정 레이블에서 LDAP 서버와 통신하도록 Trusted Extensions 프록시 서버를 사용으로 설정합니다.	Oracle Directory Server Enterprise Edition용 다중 레벨 포트 구성 [80]
다른 모든 Trusted Extensions 시스템을 LDAP 프록시 서버의 클라이언트로 구성합니다.	다른 시스템을 Trusted Extensions와 함께 구성할 때는 시스템을 이 LDAP 프록시 서버의 클라이언트로 만듭니다.	Trusted Extensions에서 전역 영역을 LDAP 클라이언트로 만들기 [83]

Trusted Extensions 시스템에서 Oracle Directory Server Enterprise Edition 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 Oracle Directory Server Enterprise Edition(Directory Server)을 구성합니다.

사이트에서 이미 LDAP 서버가 실행되고 있는 경우 서버에 Trusted Extensions 데이터베이스를 추가해야 합니다. Directory Server에 액세스하려면 시스템에 LDAP 프록시를 설정합니다.

참고 - 이 LDAP 서버를 NFS 서버나 Sun Ray 클라이언트의 서버로 사용하지 않는 경우 이 서버에 레이블이 있는 영역을 설치할 필요가 없습니다.

▼ LDAP 서버에 대한 정보 수집

- **다음 항목의 값을 결정합니다.**

항목은 System Install Wizard(시스템 설치 마법사)에 표시되는 순서대로 나열됩니다.

설치 마법사 프롬프트	작업 또는 정보
Oracle Directory Server Enterprise Edition *version*	
Administrator User ID(관리자 아이디)	기본값은 `admin`입니다.
Administrator Password(관리자 암호)	`admin123`과 같은 암호를 만듭니다.
Directory Manager DN(디렉토리 관리자 DN)	기본값은 `cn=Directory Manager`입니다.
Directory Manager Password(디렉토리 관리자 암호)	`dirmgr89`와 같은 암호를 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 제안되는 규칙은 *software-version* x `1000`입니다. 소프트웨어 버전 `5.2`의 경우 이 규칙의 결과는 포트 `5200`이 됩니다.

▼ Oracle Directory Server Enterprise Edition 설치

Directory Server 패키지는 Oracle 웹 사이트 (http://www.oracle.com/technetwork/middleware/id-mgmt/overview/index-085178.html)에서 제공됩니다.

시작하기 전에 Trusted Extensions 시스템에 전역 영역이 있으며, 레이블이 있는 영역이 없습니다. 전역 영역에서 `root` 역할을 가진 사용자여야 합니다.

Trusted Extensions LDAP 서버는 암호 작업 및 암호 정책을 결정하는 클라이언트에 대해 구성됩니다. 특히, LDAP 서버에서 설정된 정책은 사용되지 않습니다. 클라이언트에서 설정

할 수 있는 암호 매개변수는 "Oracle Solaris 11.2에서 시스템 및 연결된 장치의 보안 "의 "암호 정보 관리"를 참조하십시오. 또한 pam.conf(4) 매뉴얼 페이지를 참조하십시오.

참고 - LDAP 클라이언트에서 Trusted Extensions에 대해 pam_ldap를 사용하는 것은 평가된 구성이 아닙니다.

---

1. **Directory Server 패키지를 설치하기 전에 먼저 시스템의 호스트 이름 항목에 FQDN을 추가합니다.**

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

   ```
   # pfedit /etc/hosts
   ...
   192.168.5.5 myhost myhost.example-domain.com
   ```

2. **Oracle 웹 사이트 (http://www.oracle.com/technetwork/middleware/id-mgmt/overview/index-085178.html)에서 Oracle Directory Server Enterprise Edition 패키지를 다운로드합니다.**

   해당 플랫폼에 적합한 최신 소프트웨어를 선택합니다.

3. **Directory Server 패키지를 설치합니다.**

   LDAP 서버에 대한 정보 수집 [74]의 정보를 사용하여 질문에 답합니다. 질문, 기본값 및 권장 응답에 대한 전체 목록은 "Oracle Solaris 11.2의 이름 지정 및 디렉토리 서비스 작업: LDAP "의 4 장, "LDAP 클라이언트를 사용하여 Oracle Directory Server Enterprise Edition 설정" 및 "Oracle Solaris 11.2의 이름 지정 및 디렉토리 서비스 작업: LDAP "의 5 장, "LDAP 클라이언트 설정"을 참조하십시오.

4. **(옵션) Directory Server에 대한 환경 변수를 사용자 경로에 추가합니다.**

   ```
   # $PATH
   /usr/sbin:.../opt/SUNWdsee/dsee6/bin:/opt/SUNWdsee/dscc6/bin:/opt/SUNWdsee/ds6/bin:
   /opt/SUNWdsee/dps6/bin
   ```

5. **(옵션) Directory Server 매뉴얼 페이지를 MANPATH에 추가합니다.**

   ```
   /opt/SUNWdsee/dsee6/man
   ```

6. **cacaoadm 프로그램을 사용으로 설정하고 해당 프로그램이 사용으로 설정되었는지 확인합니다.**

   ```
   # /usr/sbin/cacaoadm enable
   # /usr/sbin/cacaoadm start
   start: server (pid n) already running
   ```

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

   Directory Server용 SMF 서비스 템플리트는 Oracle Directory Server Enterprise Edition 패키지에 있습니다.

- **Trusted Extensions 디렉토리 서버에 대해 서비스를 사용으로 설정합니다.**

  ```
  # dsadm stop /export/home/ds/instances/your-instance
  # dsadm enable-service -T SMF /export/home/ds/instances/your-instance
  # dsadm start /export/home/ds/instances/your-instance
  ```

  dsadm 명령에 대한 자세한 내용은 dsadm(1M) 매뉴얼 페이지를 참조하십시오.

- **프록시 Directory Server에 대해 서비스를 사용으로 설정합니다.**

  ```
  # dpadm stop /export/home/ds/instances/your-instance
  # dpadm enable-service -T SMF /export/home/ds/instances/your-instance
  # dpadm start /export/home/ds/instances/your-instance
  ```

  dpadm 명령에 대한 자세한 내용은 dpadm(1M) 매뉴얼 페이지를 참조하십시오.

8. **설치를 확인합니다.**

```
# dsadm info /export/home/ds/instances/your-instance
Instance Path:          /export/home/ds/instances/your-instance
Owner:                  root(root)
Non-secure port:        389
Secure port:            636
Bit format:             32-bit
State:                  Running
Server PID:             298
DSCC url:               -
SMF application name:   ds--export-home-ds-instances-your-instance
Instance version:       D-A00
```

일반 오류 LDAP 구성 문제를 해결하기 위한 전략은 “Oracle Solaris 11.2의 이름 지정 및 디렉토리 서비스 작업: LDAP ”의 6 장, “LDAP 문제 해결”을 참조하십시오.

▼ LDAP 서버용 LDAP 클라이언트 만들기

이 클라이언트를 사용하여 LDAP용 LDAP 서버를 채울 수 있습니다. LDAP 서버를 채우기 전에 먼저 이 작업을 수행해야 합니다.

Trusted Extensions Directory Server에 클라이언트를 임시로 만든 다음 해당 서버에서 클라이언트를 제거하거나 독립 클라이언트를 만들 수 있습니다.

시작하기 전에 전역 영역에서 root 역할을 가진 사용자입니다.

1. **Trusted Extensions 소프트웨어를 시스템에 추가합니다.**

   Trusted Extensions LDAP 서버를 사용하거나 Trusted Extensions를 별도의 시스템에 추가할 수 있습니다. 자세한 내용은 3장. Oracle Solaris에 Trusted Extensions 기능 추가를 참조하십시오.

2. **클라이언트의 `name-service/switch` 서비스에서 LDAP를 구성합니다.**

   a. **현재 구성을 표시합니다.**

   ```
   # svccfg -s name-service/switch listprop config
   config                      application
   config/value_authorization  astring      solaris.smf.value.name-service.switch
   config/default              astring      "files ldap"
   config/host                 astring      "files dns"
   config/netgroup             astring      ldap
   config/printer              astring      "user files ldap"
   ```

   b. **다음 등록 정보를 기본값에서 변경합니다.**

   ```
   # svccfg -s name-service/switch setprop config/host = astring: "files ldap dns"
   ```

3. **전역 영역에서 `ldapclient init` 명령을 실행합니다.**
   이 예에서 LDAP 클라이언트는 `example-domain.com` 도메인에 있습니다. 서버의 IP 주소는 `192.168.5.5`입니다.

   ```
   # ldapclient init -a domainName=example-domain.com -a profileName=default \
   > -a proxyDN=cn=proxyagent,ou=profile,dc=example-domain,dc=com \
   > -a proxyDN=cn=proxyPassword={NS1}ecc423aad0 192.168.5.5
   System successfully configured
   ```

4. **서버의 `enableShadowUpdate` 매개변수를 `TRUE`로 설정합니다.**

   ```
   # ldapclient -v mod -a enableShadowUpdate=TRUE \
   > -a adminDN=cn=admin,ou=profile,dc=example-domain,dc=com
   System successfully configured
   ```

   `enableShadowUpdate` 매개변수에 대한 자세한 내용은 "Oracle Solaris 11.2의 이름 지정 및 디렉토리 서비스 작업: LDAP "의 "enableShadowUpdate 스위치" 및 `ldapclient`(1M) 매뉴얼 페이지를 참조하십시오.

▼ Oracle Directory Server Enterprise Edition용 로그 구성

이 절차에서는 3가지 로그 유형인 액세스 로그, 감사 로그 및 오류 로그를 구성합니다. 다음 기본 설정은 변경되지 않습니다.

- 모든 로그는 사용으로 설정되고 버퍼됩니다.
- 로그는 해당 `/export/home/ds/instances/` *your-instance*`/logs/`*LOG_TYPE* 디렉토리에 배치됩니다.
- 이벤트는 로그 레벨 256에서 기록됩니다.
- 로그는 `600`개의 파일 사용 권한으로 보호됩니다.

- 액세스 로그는 일별로 회전됩니다.
- 오류 로그는 주별로 회전됩니다.

이 절차에 있는 설정은 다음 요구 사항을 충족합니다.

- 감사 로그는 일별로 회전됩니다.
- 3개월이 지난 오래된 로그 파일은 만료됩니다.
- 모든 로그 파일은 최대 20,000MB의 디스크 공간을 사용합니다.
- 로그 파일 수는 최대 100개로 유지되며, 각 파일의 크기는 최대 500MB를 넘지 않도록 합니다.
- 빈 디스크 공간이 500MB 미만이 되면 가장 오래된 로그가 삭제됩니다.
- 추가 정보는 오류 로그에서 수집됩니다.

시작하기 전에 전역 영역에서 `root` 역할을 가진 사용자여야 합니다.

1. **액세스 로그를 구성합니다.**
   액세스용 *LOG_TYPE*은 ACCESS입니다. 로그 구성 구문은 다음과 같습니다.

   ```
   dsconf set-log-prop LOG_TYPE property:value
   ```

   ```
   # dsconf set-log-prop ACCESS max-age:3M
   # dsconf set-log-prop ACCESS max-disk-space-size:20000M
   # dsconf set-log-prop ACCESS max-file-count:100
   # dsconf set-log-prop ACCESS max-size:500M
   # dsconf set-log-prop ACCESS min-free-disk-space:500M
   ```

2. **감사 로그를 구성합니다.**

   ```
   # dsconf set-log-prop AUDIT max-age:3M
   # dsconf set-log-prop AUDIT max-disk-space-size:20000M
   # dsconf set-log-prop AUDIT max-file-count:100
   # dsconf set-log-prop AUDIT max-size:500M
   # dsconf set-log-prop AUDIT min-free-disk-space:500M
   # dsconf set-log-prop AUDIT rotation-interval:1d
   ```

   기본적으로 감사 로그의 회전 간격은 1주입니다.

3. **오류 로그를 구성합니다.**
   이 구성에서 오류 로그에서 수집할 추가 데이터를 지정할 수 있습니다.

   ```
   # dsconf set-log-prop ERROR max-age:3M
   # dsconf set-log-prop ERROR max-disk-space-size:20000M
   # dsconf set-log-prop ERROR max-file-count:30
   # dsconf set-log-prop ERROR max-size:500M
   # dsconf set-log-prop ERROR min-free-disk-space:500M
   # dsconf set-log-prop ERROR verbose-enabled:on
   ```

4. **(옵션) 로그를 좀 더 자세히 구성합니다.**
   각 로그에 대해 다음 설정을 구성할 수도 있습니다.

```
# dsconf set-log-prop LOG_TYPE rotation-min-file-size:undefined
# dsconf set-log-prop LOG_TYPE rotation-time:undefined
```

dsconf 명령에 대한 자세한 내용은 dsconf(1M) 매뉴얼 페이지를 참조하십시오.

▼ Oracle Directory Server Enterprise Edition용 다중 레벨 포트 구성

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

시작하기 전에 전역 영역에서 root 역할을 가진 사용자여야 합니다.

1. **터미널 창에서 txzonemgr을 시작합니다.**

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

2. **TCP 프로토콜에 대한 다중 레벨 포트를 전역 영역에 추가합니다.**
   포트 번호는 389입니다.

3. **UDP 프로토콜에 대한 다중 레벨 포트를 전역 영역에 추가합니다.**
   포트 번호는 389입니다.

▼ Oracle Directory Server Enterprise Edition 채우기

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

시작하기 전에 전역 영역에서 root 역할을 가진 사용자여야 합니다. 섀도우 업데이트가 사용으로 설정된 LDAP 클라이언트에 있습니다. 필수 조건에 대해서는 LDAP 서버용 LDAP 클라이언트 만들기 [77]를 참조하십시오.

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 networks netmasks protocols /setup/files
   # cp rpc services auto_master /setup/files
   ```

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

주의 - *attr 파일은 복사하지 않습니다. 대신 사용자, 역할 및 권한 프로파일을 LDAP 저장소에 추가하는 명령에 -S ldap 옵션을 사용합니다. 이러한 명령은 user_attr, auth_attr, exec_attr 및 prof_attr 데이터베이스에 대한 항목을 추가합니다. 자세한 내용은 user_attr(4) 및 useradd(1M) 매뉴얼 페이지를 참조하십시오.

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

4. **단계화 영역에서 영역 자동맵을 만듭니다.**

```
# cp /zone/public/root/etc/auto_home_public /setup/files
# cp /zone/internal/root/etc/auto_home_internal /setup/files
# cp /zone/needtoknow/root/etc/auto_home_needtoknow /setup/files
# cp /zone/restricted/root/etc/auto_home_restricted /setup/files
```

다음 자동맵 목록에서 각 쌍의 첫번째 행에는 파일 이름이 표시됩니다. 각 쌍의 두번째 행에는 파일 내용이 표시됩니다. 영역 이름은 Trusted Extensions 소프트웨어와 함께 제공된 기본 label_encodings 파일에서 레이블을 식별합니다.

- 사용자의 영역 이름이 이 행의 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/&
```

5. **ldapaddent 명령을 사용하여 LDAP 서버를 스테이징 영역의 모든 파일로 채웁니다.**
예를 들어, 다음 명령은 스테이징 영역의 hosts 파일로 서버를 채웁니다.

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

6. **Trusted Extensions Directory Server에 대해 ldapclient 명령을 실행한 경우 해당 시스템에서 클라이언트를 사용 안함으로 설정합니다.**
전역 영역에서 ldapclient uninit 명령을 실행합니다. 상세 정보 출력을 사용하여 시스템이 더 이상 LDAP 클라이언트가 아닌지 확인합니다.

```
# ldapclient -v uninit
```

자세한 내용은 ldapclient(1M) 매뉴얼 페이지를 참조하십시오.

7. **Trusted Extensions 네트워크 데이터베이스를 LDAP에 채우려면 `tncfg` 명령을 `-S ldap` 옵션과 함께 사용합니다.**
   지침은 "호스트 및 네트워크 레이블 지정" [199]을 참조하십시오.

기존 Oracle Directory Server Enterprise Edition에 대한 Trusted Extensions 프록시 만들기

먼저 Trusted Extensions 데이터베이스를 Oracle Solaris 시스템의 기존 LDAP 서버에 추가해야 합니다. 그런 다음 Trusted Extensions 시스템에서 LDAP 서버에 액세스할 수 있도록 사용으로 설정한 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 `enableShadowUpdate` 매개변수를 `TRUE`로 설정하도록 수정된 클라이언트에서 LDAP 서버를 채웠습니다. 요구 사항은 LDAP 서버용 LDAP 클라이언트 만들기 [77]를 참조하십시오.

또한, `enableShadowUpdate` 매개변수가 `TRUE`로 설정된 클라이언트에서 Trusted Extensions 정보가 포함된 데이터베이스를 LDAP 서버에 추가했습니다. 자세한 내용은 Oracle Directory Server Enterprise Edition 채우기 [80]를 참조하십시오.

전역 영역에서 `root` 역할을 가진 사용자여야 합니다.

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

   참고 - 두 가지 `ldapclient` 명령을 실행해야 합니다. `ldapclient init` 명령을 실행한 경우 `ldapclient modify` 명령을 실행하여 `enableShadowUpdate` 매개 변수를 `TRUE`로 설정합니다.

   다음은 샘플 명령입니다. `ldapclient init` 명령은 프록시 값을 정의합니다.

```
# ldapclient init \
  -a proxyDN=cn=proxyagent,ou=profile,dc=west,dc=example,dc=com \
  -a domainName=west.example.com \
  -a profileName=pit1 \
  -a proxyPassword=test1234 192.168.0.1
System successfully configured
```

   `ldapclient mod` 명령은 섀도우 업데이트를 사용으로 설정합니다.

```
# ldapclient mod -a enableShadowUpdate=TRUE \
```

```
  -a adminDN=cn=admin,ou=profile,dc=west,dc=example,dc=com \
  -a adminPassword=admin-password
System successfully configured
```

자세한 내용은 “Oracle Solaris 11.2의 이름 지정 및 디렉토리 서비스 작업: LDAP ”의 5 장, “LDAP 클라이언트 설정”을 참조하십시오.

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

```
# ldaplist -l database
```

일반 오류 LDAP 구성 문제를 해결하기 위한 전략은 “Oracle Solaris 11.2의 이름 지정 및 디렉토리 서비스 작업: LDAP ”의 6 장, “LDAP 문제 해결”을 참조하십시오.

Trusted Extensions LDAP 클라이언트 만들기

다음 절차에서는 기존 Trusted Extensions 디렉토리 서버에 대한 LDAP 클라이언트를 만듭니다.

▼ Trusted Extensions에서 전역 영역을 LDAP 클라이언트로 만들기

이 절차에서는 LDAP 클라이언트의 전역 영역에 대한 LDAP 이름 지정 서비스 구성을 설정합니다.

`txzonemgr` 스크립트를 사용합니다.

참고 - 레이블이 있는 각 영역에서 이름 서버를 설정하려는 경우 사용자가 해당 영역에 대한 LDAP 클라이언트 연결을 설정해야 합니다.

시작하기 전에 Oracle Directory Server Enterprise Edition 즉, LDAP 서버가 있어야 합니다. 서버를 Trusted Extensions 데이터베이스로 채우고 이 클라이언트 시스템에서 서버에 연결할 수 있어야 합니다. 따라서 LDAP 서버에서 보안 템플리트를 이 클라이언트에 지정해야 합니다. 특정 지정은 필요하지 않으며, 와일드카드 지정이면 충분합니다.

전역 영역에서 `root` 역할을 가진 사용자여야 합니다.

1. **DNS를 사용하는 경우 `dns`를 `name-service/switch` 구성에 추가합니다.**
LDAP의 표준 이름 지정 서비스 전환 파일이 Trusted Extensions에 너무 제한적입니다.

   a. **현재 구성을 표시합니다.**

```
# svccfg -s name-service/switch listprop config
```

```
config                      application
config/value_authorization  astring      solaris.smf.value.name-service.switch
config/default              astring      files ldap
config/netgroup             astring      ldap
config/printer              astring      "user files ldap"
```

b. **dns를 host 등록 정보에 추가하고 서비스를 새로 고칩니다.**

```
# svccfg -s name-service/switch setprop config/host = astring: "files dns ldap"
# svccfg -s name-service/switch:default refresh
```

c. **새 구성을 확인합니다.**

```
# svccfg -s name-service/switch listprop config
config                      application
config/value_authorization  astring      solaris.smf.value.name-service.switch
config/default              astring      files ldap
config/host                 astring      files dns ldap
config/netgroup             astring      ldap
config/printer              astring      "user files ldap"
```

Trusted Extensions 데이터베이스는 기본 구성 `files ldap`을 사용하므로 나열되지 않습니다.

2. **LDAP 클라이언트를 만들려면 txzonemgr 명령을 옵션 없이 실행합니다.**

```
# txzonemgr &
```

a. **전역 영역을 두 번 누릅니다.**

b. **Create LDAP Client(LDAP 클라이언트 만들기)를 선택합니다.**

c. **다음 프롬프트에 응답한 다음 각 응답 후 OK(확인)를 누릅니다.**

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

d. **표시된 값을 확인하거나 취소합니다.**

```
Proceed to create LDAP Client?
```

확인하면 `txzonemgr` 스크립트가 `ldapclient init` 명령을 실행합니다.

3. **섀도우 업데이트를 사용으로 설정하여 클라이언트 구성을 완료합니다.**

```
# ldapclient -v mod -a enableShadowUpdate=TRUE \
> -a adminDN=cn=admin,ou=profile,dc=domain,dc=suffix
```

```
System successfully configured
```

4. **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 발생하는 경우 2단계부터 4단계까지 다시 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.

부 II

Trusted Extensions 관리

이 장에서는 Trusted Extensions를 관리하는 방법을 설명합니다.

6장. Trusted Extensions 관리 개념에서는 Trusted Extensions 기능을 소개합니다.

7장. Trusted Extensions 관리 도구에서는 Trusted Extensions에 고유한 관리 프로그램을 설명합니다.

8장. Trusted Extensions 시스템의 보안 요구 사항 정보는 Trusted Extensions에서 확정된 보안 요구 사항과 구성 가능한 보안 요구 사항을 설명합니다.

9장. Trusted Extensions의 일반 작업에서는 Trusted Extensions 관리를 소개합니다.

10장. Trusted Extensions의 사용자, 권한 및 역할 정보는 Trusted Extensions의 RBAC(역할 기반 액세스 제어)를 소개합니다.

11장. Trusted Extensions에서 사용자, 권한 및 역할 관리에서는 Trusted Extensions의 일반 사용자 관리에 대한 지침을 제공합니다.

12장. Trusted Extensions에서 원격 관리에서는 Trusted Extensions를 원격으로 관리하기 위한 지침을 제공합니다.

13장. Trusted Extensions에서 영역 관리에서는 레이블이 있는 영역 관리에 대한 지침을 제공합니다.

14장. Trusted Extensions에서 파일 관리 및 마운트에서는 Trusted Extensions에서 마운트 관리, 시스템 백업 및 기타 파일 관련 작업에 대한 지침을 제공합니다.

15장. 신뢰할 수 있는 네트워킹에서는 Trusted Extensions의 네트워크 데이터베이스 및 경로 지정에 대한 개요를 제공합니다.

16장. Trusted Extensions에서 네트워크 관리에서는 Trusted Extensions의 네트워크 데이터베이스 및 경로 지정 관리에 대한 지침을 제공합니다.

17장. Trusted Extensions 및 LDAP 정보에서는 Trusted Extensions의 메일 관련 문제에 대해 설명합니다.

18장. Trusted Extensions의 다중 레벨 메일 정보는 Trusted Extensions의 메일 관련 문제를 설명합니다.

19장. 레이블이 있는 인쇄 관리에서는 Trusted Extensions에서 인쇄 처리에 대한 지침을 제공합니다.

20장. Trusted Extensions의 장치 정보는 Trusted Extensions가 Oracle Solaris에서 장치 보호를 위해 제공하는 확장 기능을 설명합니다.

21장. Trusted Extensions에 대한 장치 관리에서는 장치 관리자를 사용하여 장치를 관리하기 위한 지침을 제공합니다.

22장. Trusted Extensions와 감사는 감사에 대한 Trusted Extensions 특정 정보를 제공합니다.

23장. Trusted Extensions에서 소프트웨어 관리에서는 Trusted Extensions 시스템에서 응용 프로그램을 관리하는 방법을 설명합니다.

♦ ♦ ♦ 6 장

6 Trusted Extensions 관리 개념

이 장에서는 Trusted Extensions 기능으로 구성된 시스템을 관리하는 방법에 대해 소개합니다.

Trusted Extensions 및 Oracle Solaris OS

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

Trusted Extensions와 Oracle Solaris OS의 유사점

Trusted Extensions 소프트웨어는 권한 프로파일, 역할, 감사 및 Oracle Solaris의 기타 보안 기능을 사용합니다. Trusted Extensions에서는 Secure Shell, BART, 암호화 프레임워크, IPsec 및 IP 필터를 사용할 수 있습니다. 스냅샷, 암호화 및 저장소를 포함한 ZFS 파일 시스템의 모든 기능을 Trusted Extensions에서 사용할 수 있습니다.

Trusted Extensions와 Oracle Solaris OS의 차이점

Trusted Extensions 소프트웨어는 Oracle Solaris OS를 확장합니다. 다음 목록은 개요 형식의 간략한 설명을 제공합니다. 부록 C. Trusted Extensions 관리에 대한 빠른 참조도 참조하십시오.

- Trusted Extensions에서는 레이블이라는 특수 보안 태그로 데이터에 대한 액세스를 제어합니다. 레이블은 MAC(필수 액세스 제어)를 제공합니다. UNIX 파일 사용 권한이나

DAC(임의 액세스 제어) 이외에 MAC 보호도 있습니다. 레이블은 사용자, 영역, 장치, 창 및 네트워크 끝점에 직접 지정됩니다. 레이블은 프로세스, 파일 및 기타 시스템 객체에 암시적으로 지정됩니다.

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

Oracle Solaris OS에서와 마찬가지로 보안 정책을 대체하는 기능은 MAC를 대체할 수 있을 때 특정 프로세서나 사용자에게 지정될 수 있습니다. 예를 들어, 파일의 레이블을 변경할 수 있게 사용자를 권한 부여할 수 있습니다. 이러한 작업은 해당 파일에서 정보의 민감도를 업그레이드하거나 다운그레이드합니다.

- Trusted Extensions는 기존 구성 파일 및 명령에 추가합니다. 예를 들어, Trusted Extensions에서는 감사 이벤트, 권한 부여, 권한 및 권한 프로파일을 추가합니다.
- Oracle Solaris 시스템에서는 선택 사항인 일부 기능이 Trusted Extensions 시스템에서는 필수 사항입니다. 예를 들어, Trusted Extensions로 구성된 시스템에서는 영역과 역할이 필수 사항입니다.
- Oracle Solaris 시스템에서는 선택 사항인 일부 기능이 Trusted Extensions 시스템에서는 사용으로 설정됩니다. 예를 들어, Trusted Extensions를 구성하는 많은 사이트에서 사용자를 만들고 보안 속성을 지정할 때 separation of duty(책임 구분)이 필요합니다.
- Trusted Extensions는 Oracle Solaris의 기본 동작을 변경할 수 있습니다. 예를 들어, Trusted Extensions로 구성된 시스템에서 장치 할당은 필수입니다.
- Oracle Solaris에서 사용할 수 있는 옵션을 Trusted Extensions에서 축소할 수 있습니다. 예를 들어, Trusted Extensions에서는 모든 영역이 레이블이 있는 영역입니다. Oracle Solaris와 달리 레이블이 있는 영역은 동일한 풀의 사용자 ID 및 그룹 ID를 사용해야 합니다. 또한 Trusted Extensions에서는 여러 레이블이 있는 영역이 하나의 IP 주소를 공유할 수 있습니다.
- Trusted Extensions는 Oracle Solaris 데스크탑 Solaris Trusted Extensions (GNOME)의 다중 레벨 버전을 제공합니다. 이 이름은 Trusted GNOME로 줄여서 부르기도 합니다.
- Trusted Extensions에서는 추가 GUI(그래픽 사용자 인터페이스)와 CLI(명령줄 인터페이스)를 제공합니다. 예를 들어, Trusted Extensions에서는 장치를 관리하는 Device Manager(장치 할당 관리자) GUI를 제공합니다. 또한 `updatehome` CLI를 사용하여 모든 레이블의 사용자 홈 디렉토리에 시작 파일을 넣을 수 있습니다.
- 윈도우화 환경에서 Trusted Extensions는 관리용 GUI를 제공합니다. 예를 들어, `zonecfg` 명령 외에도 Labeled Zone Manager(레이블이 있는 영역 관리자)는 레이블이 있는 영역을 관리하는 데 사용됩니다.
- Trusted Extensions에서는 사용자에게 표시되는 항목이 제한됩니다. 예를 들어, 사용자가 할당할 수 없는 장치는 해당 사용자에게 표시되지 않습니다.
- Trusted Extensions에서는 사용자의 데스크탑 옵션을 제한합니다. 예를 들어, 사용자가 제한된 시간 동안 워크스테이션을 사용하지 않을 경우 화면이 잠깁니다. 기본적으로 사용자는 시스템을 종료할 수 없습니다.

멀티헤디드 시스템 및 Trusted Extensions 데스크탑

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

그러나 서로 다른 작업 공간이 멀티헤디드 시스템의 모니터에 표시될 경우 Trusted GNOME은 각 모니터에 신뢰할 수 있는 스트라이프를 표시합니다.

Trusted Extensions의 기본 개념

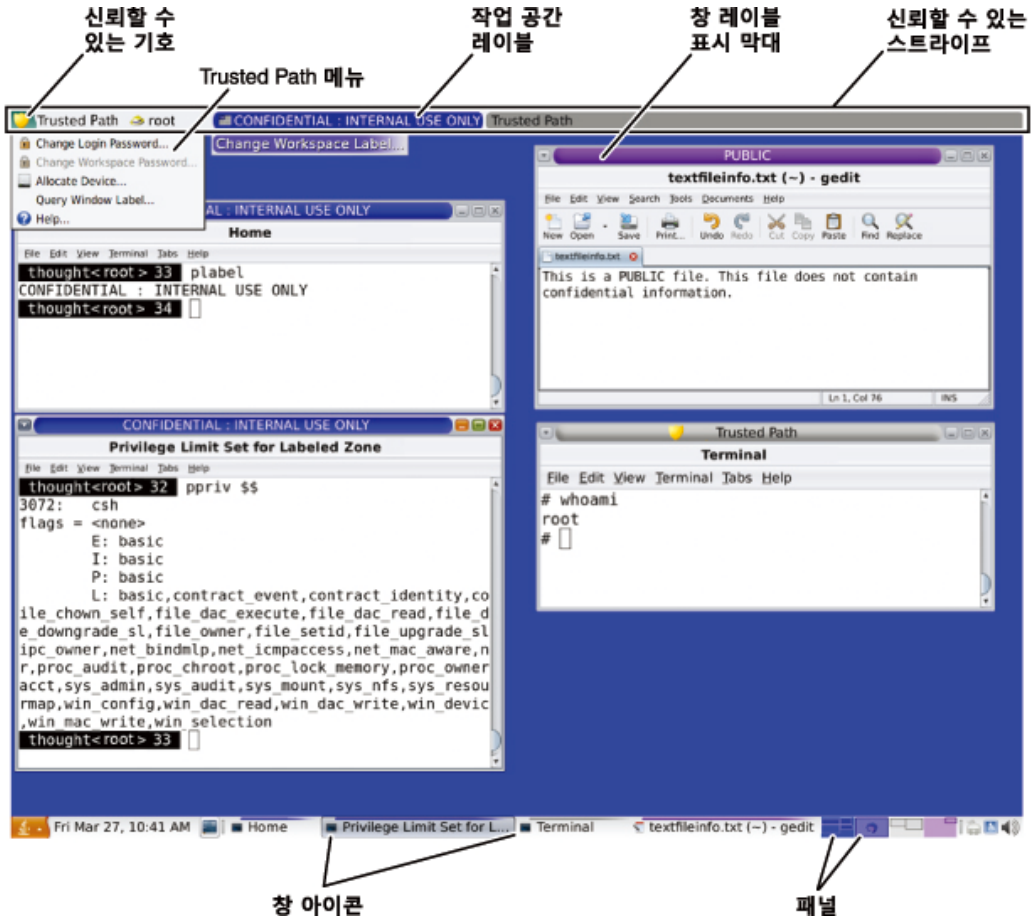
Trusted Extensions 소프트웨어는 Oracle Solaris 시스템에 레이블을 추가합니다. Label Builder(레이블 구축기) 및 Device Manager(장치 할당 관리자)와 같은 레이블이 있는 작업 공간과 신뢰할 수 있는 응용 프로그램도 추가됩니다. 여기서는 사용자와 관리자 모두가 Trusted Extensions를 이해하는 데 필요한 개념에 대해 설명합니다. 이러한 개념은 “Trusted Extensions 사용자 설명서 ”에 소개되어 있습니다.

Trusted Extensions 보호

Trusted Extensions 소프트웨어는 Oracle Solaris OS에 대한 보호를 개선합니다. Trusted Extensions는 사용자 및 역할을 승인된 레이블 범위로 제한합니다. 이 레이블 범위에 따라 사용자와 역할이 액세스할 수 있는 정보가 제한됩니다.

Trusted Extensions는 신뢰할 수 있는 스트라이프의 왼쪽에 나타나는 확실한 변조 방지 엠블럼인 Trusted Path(신뢰할 수 있는 경로) 기호를 표시합니다. Trusted GNOME에서 스트라이프는 화면의 맨 위에 있습니다. Trusted Path(신뢰할 수 있는 경로) 기호는 사용자가 시스템의 보안 관련 부분을 사용 중일 때 나타납니다. 사용자가 신뢰할 수 있는 응용 프로그램을 실행할 때 이 기호가 나타나지 않는 경우 응용 프로그램의 해당 버전이 인증되었는지 즉시 확인하십시오. 신뢰할 수 있는 스트라이프가 나타나지 않는 경우 해당 데스크탑을 신뢰할 수 없습니다. 샘플 데스크탑 표시는 그림 6-1. “Trusted Extensions 다중 레벨 데스크탑”을 참조하십시오.

그림 6-1 Trusted Extensions 다중 레벨 데스크탑



대부분의 보안 관련 소프트웨어 즉, TCB(Trusted Computing Base)는 전역 영역에서 실행됩니다. 일반 사용자는 전역 영역에 연결하거나 전역 영역의 리소스를 볼 수 없습니다. 사용자는 암호를 변경할 때와 같이 TCB 소프트웨어의 영향을 받습니다. Trusted Path(신뢰할 수 있는 경로) 기호는 사용자가 TCB와 상호 작용할 때마다 표시됩니다.

Trusted Extensions 및 액세스 제어

Trusted Extensions 소프트웨어에서는 DAC(임의 액세스 제어) 및 MAC(필수 액세스 제어)를 통해 정보와 기타 리소스를 보호합니다. DAC는 소유자가 임의로 설정하는 일반 UNIX

권한 비트 및 액세스 제어 목록입니다. MAC는 시스템에서 자동으로 적용하는 방식입니다. MAC는 프로세스의 레이블과 트랜잭션 데이터를 확인하여 모든 트랜잭션을 제어합니다.

사용자의 레이블은 사용자가 작업할 수 있거나 작업하도록 선택하는 민감도 레벨을 나타냅니다. 일반 레이블은 `Secret` 및 `Public`입니다. 레이블에 따라 사용자가 액세스할 수 있는 정보가 결정됩니다. MAC 및 DAC는 모두 Oracle Solaris에서 제공하는 *privileges* 및 *authorizations*의 특수 권한으로 대체될 수 있습니다. 권한 은 프로세스에 허용될 수 있는 특수 사용 권한입니다. 권한 부여 는 관리자가 사용자와 역할에 부여할 수 있는 특수 사용 권한입니다.

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

Trusted Extensions 소프트웨어의 레이블

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

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

레이블 사이의 지배 관계

엔티티의 레이블이 다음과 같은 두 조건을 충족하는 경우 다른 레이블을 지배한다고 합니다.

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

분류와 구획 세트가 동일한 경우 두 레이블이 동일하다고 합니다. 레이블이 동일한 경우 서로 지배 관계이므로 액세스가 허용됩니다.

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

어떤 레이블도 다른 레이블을 지배하지 않는 경우 두 레이블은 분리 또는 비교 불가라고 합니다.

다음 표에서는 지배에 대한 레이블 비교의 예를 제공합니다. 예에서 NEED_TO_KNOW는 INTERNAL보다 더 높은 분류입니다. 이 예에는 Eng, Mkt, Fin의 세 가지 구획이 있습니다.

표 6-1 레이블 관계 예

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

관리 레이블

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

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

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

레이블 인코딩 파일

시스템의 모든 레이블 구성 요소 즉, 분류, 구획 및 연결된 규칙은 ADMIN_HIGH 파일인 label_encodings 파일에 저장됩니다. 원본 파일은 /etc/security/tsol 디렉토리에 있습니다. Trusted Extensions가 사용으로 설정된 다음에는 파일 위치가 labeld 서비스의 등록 정보로 저장됩니다. 보안 관리자는 사이트에 대한 label_encodings 파일을 구성합니다. 레이블 인코딩 파일에는 다음이 포함됩니다.

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

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

레이블 범위

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

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

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

계정 레이블 범위

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

minimum-label ≤ *permitted-label* ≤ *clearance*

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

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

세션 범위

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

레이블이 보호하는 항목 및 레이블이 표시되는 위치

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

- **응용 프로그램** - 응용 프로그램에서 프로세스를 시작합니다. 이러한 프로세스는 응용 프로그램이 시작되는 작업 공간의 레이블에서 실행됩니다. 파일과 같이 레이블이 있는 영역 내 응용 프로그램의 레이블은 해당 영역의 레이블에서 지정됩니다.
- **장치** - 장치를 통해 이동하는 데이터는 장치 할당 및 장치 레이블 범위를 통해 제어됩니다. 장치를 사용하려면 사용자가 장치의 레이블 범위 내에 있고 해당 장치를 할당할 수 있게 권한 부여되어야 합니다.
- **파일 시스템 마운트 지점** - 모든 마운트 지점에는 레이블이 있습니다. `getlabel` 명령을 사용하여 레이블을 볼 수 있습니다.
- **IPsec 및 IKE** - IPsec 보안 연결 및 IKE 규칙에는 레이블이 있습니다.
- **네트워크 인터페이스** - IP 주소(호스트)에는 해당 레이블 범위를 설명하는 보안 템플리트가 지정됩니다. 레이블이 없는 호스트에도 통신하는 Trusted Extensions 시스템에 의해 기본 레이블이 지정됩니다.
- **프린터 및 인쇄** - 프린터에는 레이블 범위가 있습니다. 레이블은 본문 페이지에 인쇄됩니다. 레이블, 처리 정보 및 기타 보안 정보는 배너 및 트레일러 페이지에 인쇄됩니다. Trusted Extensions에서 인쇄를 구성하려면 19장. 레이블이 있는 인쇄 관리 및 “Trusted Extensions Label Administration ”의 “Labels on Printed Output”을 참조하십시오.
- **프로세스** - 프로세스에는 레이블이 있습니다. 프로세스는 해당 프로세스가 시작된 작업 공간의 레이블에서 실행됩니다. 프로세스의 레이블은 `plabel` 명령을 사용하여 볼 수 있습니다.
- **사용자** - 사용자에게는 기본 레이블과 레이블 범위가 지정됩니다. 사용자의 작업 공간 레이블은 사용자의 프로세스 레이블을 나타냅니다.
- **창** - 레이블이 데스크탑 창의 맨 위에 표시됩니다. 또한 데스크탑의 레이블은 색상으로 표시됩니다. 그림 6-1. “Trusted Extensions 다중 레벨 데스크탑”에 나온 대로 작업 공간 패널과 창 제목 표시줄 위에 색상이 나타납니다.

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

역할 및 Trusted Extensions

Trusted Extensions 없이 Oracle Solaris 소프트웨어를 실행 중인 시스템에서 역할은 선택 사항입니다. Trusted Extensions로 구성된 시스템에서는 `root` 이외의 일부 역할로 시스템이 관리됩니다. 일반적으로 시스템 관리자 역할 및 보안 관리자 역할은 대부분의 관리 기능을 수행합니다. 일부 경우에는 초기 설정 후에 `root` 역할로 관리를 수행할 수 있습니다. 데스크탑 시스템에서 작업 공간은 사용자가 특정 역할로 전환할 때 해당 역할의 작업 공간으로 변경됩니다.

Trusted Extensions의 한 역할에 제공되는 프로그램은 신뢰할 수 있는 경로 속성이라는 특별한 등록 정보를 포함합니다. 이 속성은 프로그램이 TCB의 일부임을 나타냅니다. 신뢰할 수 있는 경로 속성은 프로그램이 전역 영역에서 시작되는 경우에 사용할 수 있습니다.

Oracle Solaris에서와 마찬가지로 권한 프로파일은 역할 기능의 기반입니다. 권한 프로파일 및 역할에 대한 자세한 내용은 “Oracle Solaris 11.2의 사용자 및 프로세스 보안 ”의 1 장, “권한을 사용하여 사용자 및 프로세스 제어 정보”를 참조하십시오.

♦ ♦ ♦ 7 장

7 Trusted Extensions 관리 도구

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

Trusted Extensions용 관리 도구

Trusted Extensions로 구성된 시스템 관리에는 Oracle Solaris OS에서 사용 가능한 것과 동일한 여러 도구가 사용됩니다. Trusted Extensions에서는 보안이 강화된 도구도 제공합니다. 관리 도구는 역할에만 제공됩니다.

역할 작업 공간의 데스크탑 시스템에서 신뢰할 수 있는 명령, 응용 프로그램 및 스크립트에 액세스할 수 있습니다. 다음 표는 이러한 관리 도구를 요약한 것입니다. 데스크탑을 실행 중이 아닌 시스템에서 명령줄 도구를 사용할 수 있습니다.

표 7-1 Trusted Extensions 관리 도구

도구	설명	자세한 정보
`/usr/sbin/labeladm`	Trusted Extensions를 사용 및 사용 안함으로 설정합니다. 레이블 인코딩 파일을 설치하는 데에도 사용됩니다.	"Trusted Extensions 설치 및 사용으로 설정" [35], 레이블 인코딩 파일을 확인하고 설치하는 방법 [40] 및 `labeladm`(1M) 매뉴얼 페이지를 참조하십시오.
`/usr/sbin/txzonemgr`	네트워킹을 포함하여 레이블이 있는 영역을 만들고 구성하기 위한 Labeled Zone Manager(레이블이 있는 영역 관리자) GUI를 만듭니다.	"레이블이 있는 영역 만들기" [43] 및 `txzonemgr`(1M) 매뉴얼 페이지를 참조하십시오. `txzonemgr`은 `zenity` (1) 스크립트입니다.

도구	설명	자세한 정보
	명령줄 옵션을 사용하여 사용자 이름 지정 영역을 자동으로 만들 수 있습니다.	
Device Manager(장치 할당 관리자)	장치의 레이블 범위를 관리하고 장치를 할당하거나 할당 해제하는 데 사용됩니다.	"장치 관리자" [100] 및 "Trusted Extensions에서 장치 취급" [265]을 참조하십시오.
레이블 구축기	사용자 도구이기도 합니다. 프로그램에서 레이블 선택을 요구할 때 나타납니다.	예는 사용자의 레이블 범위를 수정하는 방법 [135]을 참조하십시오.
Selection Manager(선택 관리자)	데이터의 보안 레벨을 변경할 수 있는 권한이 부여된 사용자를 위한 도구입니다. 데이터의 보안 레벨을 변경해야 하는 경우 나타납니다.	사용자에게 권한을 부여하려면 사용자가 데이터의 보안 레벨을 변경할 수 있게 하는 방법 [138]을 참조하십시오. 그림은 "Trusted Extensions 사용자 설명서 "의 "다른 레이블의 창 간에 데이터를 이동하는 방법"을 참조하십시오.
Trusted Extensions 명령	관리 작업을 수행하는 데 사용됩니다.	관리 명령 및 구성 파일 목록은 부록 D. Trusted Extensions 매뉴얼 페이지 목록을 참조하십시오.

txzonemgr 스크립트

/usr/sbin/txzonemgr 명령은 두 가지 모드를 제공하는 영역 및 네트워크 구성 도구입니다.

- CLI에서 이 명령은 레이블이 있는 영역을 만듭니다. -c 명령 옵션과 함께 실행하면 CLI는 두 레이블이 있는 영역을 만들고 부트합니다. -d 옵션은 모든 영역을 하나씩 삭제하라는 프롬프트를 표시합니다.
- GUI로 스크립트는 Labeled Zone Manager(레이블이 있는 영역 관리자)라는 대화 상자를 표시합니다. 이 GUI는 레이블이 있는 영역 만들기 및 부트를 안내합니다. 스크립트에는 스냅샷을 만들기 위한 영역 복제가 포함되어 있습니다. 또한 GUI는 네트워킹, 이름 지정 서비스 및 LDAP 구성 메뉴를 제공합니다. 이 스크립트는 IPv4 및 IPv6 주소를 처리합니다.

txzonemgr 명령은 zenity(1) 스크립트를 실행합니다. Labeled Zone Manager(레이블이 있는 영역 관리자) 대화 상자는 레이블이 있는 영역의 현재 구성 상태에 대해 유효한 선택 항목만 표시합니다. 예를 들어, 영역에 레이블이 이미 있는 경우 Label(레이블) 메뉴 항목이 표시되지 않습니다.

장치 관리자

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

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

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

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

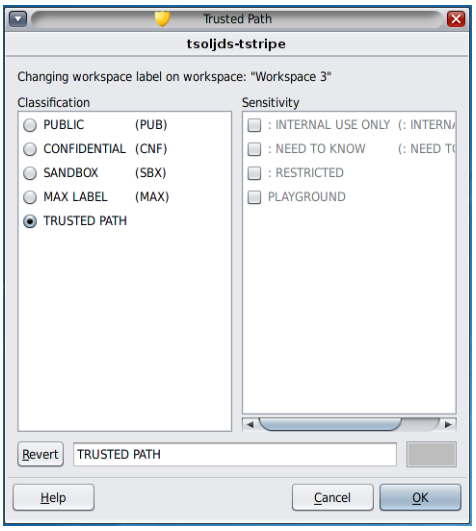
Trusted Extensions에서 장치 보호에 대한 자세한 내용은 21장. Trusted Extensions에 대한 장치 관리를 참조하십시오.

Trusted Extensions의 Selection Manager(선택 관리자)

객체 또는 선택 항목의 레이블을 변경하려고 할 때 Selection Manager(선택 관리자) GUI가 나타납니다. 자세한 내용은 “데이터에 대한 보안 레벨 변경 규칙” [110]을 참조하십시오.

Trusted Extensions의 레이블 구축기

프로그램에서 레이블을 지정하도록 요구할 때 레이블 구축기 GUI를 통해 유효한 레이블이나 클리어런스를 선택할 수 있습니다. 예를 들어, 로그인 중에 레이블 구축기가 나타납니다(“Trusted Extensions 사용자 설명서 ”의 2 장, “Trusted Extensions에 로그인” 참조). 작업 공간의 레이블을 변경하거나 사용자, 영역 또는 네트워크 인터페이스에 레이블을 지정할 경우에도 레이블 구축기가 나타납니다. 레이블 범위를 새 장치에 지정할 때 다음 레이블 구축기가 나타납니다.



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

개발자는 `tgnome-selectlabel` 명령을 사용하여 자신의 응용 프로그램에 대한 레이블 구축기를 만들 수 있습니다. 온라인 도움말을 표시하려면 `tgnome-selectlabel -h`를 입력하십시오. 또한 "Trusted Extensions Developer's Guide "의 6 장, "Label Builder GUI"를 참조하십시오.

Trusted Extensions의 명령줄 도구

Trusted Extensions에 고유한 명령 및 Trusted Extensions에서 수정된 명령은 *Oracle Solaris Reference Manual*에 나와 있습니다. `man` 명령은 모든 명령을 찾습니다. 명령에 대한 설명, Trusted Extensions 설명서의 예에 대한 링크 및 매뉴얼 페이지에 대한 링크는 부록 D. Trusted Extensions 매뉴얼 페이지 목록을 참조하십시오.

Trusted Extensions의 구성 파일

`/etc/inet/ike/config` 파일은 Trusted Extensions에서 확장되어 레이블 정보를 포함합니다. `ike.config`(4) 매뉴얼 페이지에서는 `label_aware` 전역 매개변수와 세 개의 단계 1 변환 매개변수인 `single_label`, `multi_label` 및 `wire_label`을 설명합니다.

참고 - IKE 구성 파일에는 단계 1 IKE 규칙을 고유하게 만드는 데 사용되는 `label` 키워드가 포함됩니다. IKE 키워드 `label`은 Trusted Extensions 레이블과 구분됩니다.

♦ ♦ ♦ 8 장

8 Trusted Extensions 시스템의 보안 요구 사항 정보

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

구성 가능한 보안 기능

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

Trusted Extensions는 사용자가 일반적으로 제한된 역할을 맡아 시스템을 관리한다는 점에서 Oracle Solaris와 다릅니다.

Trusted Extensions의 역할

Trusted Extensions에서 역할은 시스템을 관리하는 일반적인 방법입니다. 수퍼유저는 `root` 역할이며 감사 플래그 설정, 계정의 암호 변경, 시스템 파일 편집 등의 작업에 필요합니다. 역할은 Oracle Solaris와 마찬가지로 만들어집니다.

Trusted Extensions 사이트의 일반적인 역할은 다음과 같습니다.

- `root` **역할** - Oracle Solaris 설치 시 만들어집니다.
- **보안 관리자 역할** - 초기 설정 팀에서 초기 구성 중에 또는 초기 구성 후에 만듭니다.
- **시스템 관리자 역할** - 초기 설정 팀에서 초기 구성 중에 또는 초기 구성 후에 만듭니다.

Trusted Extensions에서 역할 만들기

Trusted Extensions를 관리하려면 시스템 기능과 보안 기능을 나누는 역할을 만듭니다.

Trusted Extensions에서 역할을 만드는 절차는 Oracle Solaris 프로세스와 동일합니다. 기본적으로 역할에는 `ADMIN_HIGH` ~ `ADMIN_LOW` 범위의 관리 레이블이 지정됩니다.

- 역할 만들기에 대한 개요는 "Oracle Solaris 11.2의 사용자 및 프로세스 보안 "의 "사용자에게 권한 지정"을 참조하십시오.
- 역할을 만들려면 "Trusted Extensions의 역할 및 사용자 만들기" [54]를 참조하십시오.

Trusted Extensions에서 역할 맡기

신뢰할 수 있는 데스크탑의 신뢰할 수 있는 스트라이프에서 역할 선택을 위한 사용자 이름을 눌러 지정된 역할을 맡을 수 있습니다. 역할 암호를 확인하면 현재 작업 공간이 역할 작업 공간으로 변경됩니다. 역할 작업 공간은 전역 영역에 있으며 신뢰할 수 있는 경로 속성을 가집니다. 역할 작업 공간은 관리 작업 공간입니다.

Trusted Extensions의 보안 기능 구성 인터페이스

Trusted Extensions에서는 기존 보안 기능을 확장할 수 있습니다. 또한 Trusted Extensions는 고유한 보안 기능도 제공합니다.

Trusted Extensions로 Oracle Solaris 보안 기능 확장

Oracle Solaris에서 제공하는 다음 보안 방식은 Oracle Solaris에서와 마찬가지로 Trusted Extensions에서 확장 가능합니다.

- **감사 클래스** - 감사 클래스 추가는 "Oracle Solaris 11.2의 감사 관리 "의 3 장, "감사 서비스 관리"를 참조하십시오.

참고 - 감사 이벤트를 추가하고자 하는 공급업체는 Oracle Solaris 담당자에게 연락하여 이벤트 번호를 예약하고 감사 인터페이스에 대한 액세스 권한을 얻어야 합니다.

- **역할 및 권한 프로파일** - 역할 및 권한 프로파일 추가는 "Oracle Solaris 11.2의 사용자 및 프로세스 보안 "의 3 장, "Oracle Solaris에서 권한 지정"을 참조하십시오.
- **권한 부여** - 새 권한 부여를 추가하는 예는 "Trusted Extensions에서 장치 권한 부여 사용자 정의" [273]를 참조하십시오.

Oracle Solaris에서와 마찬가지로 권한은 확장할 수 없습니다.

고유한 Trusted Extensions 보안 기능

Trusted Extensions는 다음과 같은 고유한 보안 기능을 제공합니다.

- **레이블** - 주체와 객체에 레이블이 지정됩니다. 프로세스에 레이블이 지정됩니다. 영역과 네트워크에 레이블이 지정됩니다. 작업 공간 및 해당 객체가 레이블 지정됩니다.
- **Device Manager(장치 할당 관리자)** - 기본적으로 장치는 할당 요구 사항에 의해 보호됩니다. Device Manager(장치 할당 관리자) GUI는 관리자와 일반 사용자를 위한 인터페이스입니다.
- **Change Password(암호 변경) 메뉴** - 이 메뉴를 사용하여 사용자 또는 역할 암호를 변경할 수 있습니다.
- **Change Workspace Label(작업 공간 레이블 변경) 메뉴** - 다중 레벨 세션의 사용자가 작업 공간 레이블을 변경할 수 있습니다. 다른 레이블의 작업 공간에 들어갈 때 사용자는 암호를 제공해야 합니다.
- **Selection Manager(선택 관리자) 대화 상자** - 다중 레벨 세션에서 권한이 부여된 사용자는 정보를 다른 레이블로 업그레이드하거나 다운그레이드할 수 있습니다.
- **TrustedExtensionsPolicy 파일** - 관리자는 Trusted Extensions에 고유한 X 서버 확장자에 대한 정책을 변경할 수 있습니다. 자세한 내용은 `TrustedExtensionsPolicy(4)` 매뉴얼 페이지를 참조하십시오.

보안 요구 사항 적용

시스템 보안이 손상되지 않도록 관리자는 암호, 파일 및 감사 데이터를 보호해야 합니다. 사용자도 해당 파트를 수행하도록 교육해야 합니다. 평가된 구성에 대해 요구 사항을 일관되게 유지하려면 이 섹션의 지침을 따르십시오.

사용자 및 보안 요구 사항

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

- 암호를 아무에게도 말하지 마십시오.

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

전자 메일의 보낸 사람 정보가 위조되었을 수 있습니다.

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

사이트에서 추가 제안 사항을 제공할 수 있습니다.

전자 메일 사용 지침

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

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

암호 적용

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

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

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

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

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

정보 보호

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

- `shadow` **파일** - 암호화된 암호가 포함되어 있습니다. shadow(4) 매뉴얼 페이지를 참조하십시오.
- `auth_attr` **파일** - 사용자 정의 권한 부여가 포함되어 있습니다. auth_attr(4) 매뉴얼 페이지를 참조하십시오.
- `prof_attr` **파일** - 사용자 정의 권한 프로파일이 포함되어 있습니다. prof_attr(4) 매뉴얼 페이지를 참조하십시오.
- `exec_attr` **파일** - 사이트에서 권한 프로파일에 추가한 보안 속성을 가진 명령이 포함되어 있습니다. exec_attr(4) 매뉴얼 페이지를 참조하십시오.
- **감사 추적** - 감사 서비스에서 수집된 감사 레코드가 포함되어 있습니다. audit.log(4) 매뉴얼 페이지를 참조하십시오.

암호 보호

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

그룹 관리 방법

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

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

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

사용자 삭제 방법

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

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

데이터에 대한 보안 레벨 변경 규칙

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

파일 레이블 또는 파일 내의 정보 레이블을 변경하려면 권한 부여가 필요합니다. 사용자가 데이터의 보안 레벨을 변경할 수 있게 권한 부여된 경우 Selection Manager(선택 관리자) 응용 프로그램에서 전송을 중재합니다.

- `/usr/share/gnome/sel_config` 파일은 파일 레이블 변경 작업과 정보를 잘라내어 다른 레이블에 붙여넣기 작업을 제어합니다. 자세한 내용은 "`sel_config` 파일" [111] 및 `sel_config`(4) 매뉴얼 페이지를 참조하십시오.
- `/usr/bin/tsoljdsselmgr` 응용 프로그램은 창 사이에 끌어서 놓기 작업을 제어합니다. 다음 표에 표시된 것처럼 선택 항목의 레이블 변경은 파일의 레이블 변경보다 더 제한적입니다.

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

표 8-1 파일을 새 레이블로 이동하기 위한 조건

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

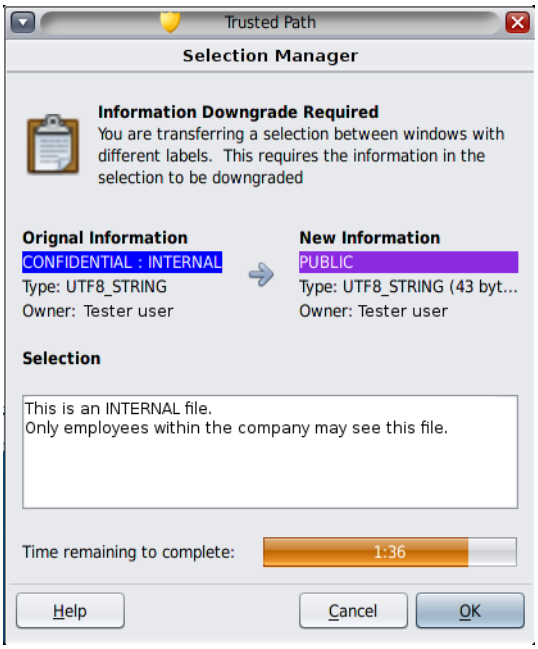
창 또는 파일 내의 선택에는 다른 규칙이 적용됩니다. 선택 항목 끌어서 놓기는 항상 동일한 레이블과 소유권에만 적용됩니다. 창 사이의 끌어서 놓기는 `sel_config` 파일이 아니라 Selection Manager(선택 관리자) 응용 프로그램에서 중재합니다.

선택 항목의 레이블 변경 규칙에 대해서는 다음 표에 요약되어 있습니다.

표 8-2 선택 항목을 새 레이블로 이동하기 위한 조건

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

윈도우화 시스템에서 Trusted Extensions는 레이블 변경을 중재하는 Selection Manager(선택 관리자)를 제공합니다. 이 대화 상자는 권한이 있는 사용자가 파일 또는 선택 항목의 레이블을 변경하려고 시도하면 표시됩니다. 사용자는 120초 동안 작업을 확인할 수 있습니다. 이 창을 표시하지 않고 데이터의 보안 레벨을 변경하려면 레이블 변경 권한 부여와 `solaris.label.win.noview` 권한 부여가 필요합니다. 다음 그림에는 창에 두 행의 선택 항목이 표시되어 있습니다.



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

`sel_config` 파일

레이블 업그레이드 또는 다운그레이드 작업을 수행할 때 `/usr/share/gnome/sel_config` 파일을 확인하여 Selection Manager(선택 관리자)의 동작을 결정합니다.

`sel_config` 파일은 다음을 정의합니다.

- 자동 회신이 제공되는 선택 유형 목록
- 특정 유형의 작업을 자동으로 확인할 수 있는지 여부
- Selection Manager(선택 관리자) 대화 상자가 표시되는지 여부

♦ ♦ ♦ 9 장

9 Trusted Extensions의 일반 작업

이 장에서는 Trusted Extensions 시스템 관리 및 이러한 시스템에서 일반적으로 수행되는 작업에 대해 소개합니다.

데스크탑 시스템에서 Trusted Extensions 관리자로 시작하기

Trusted Extensions를 관리하기 전에 다음 절차를 숙지하십시오.

표 9-1 Trusted Extensions 데스크탑 로그인 및 사용

작업	설명	수행 방법
Trusted Extensions 시스템에 로그인합니다.	안전하게 로그인합니다.	“Trusted Extensions 사용자 설명서 ”의 “Trusted Extensions에 로그인”
데스크탑에서 일반적인 사용자 작업을 수행합니다.	작업은 다음과 같습니다. ■ 작업 공간 구성 ■ 다른 레이블에서 작업 공간 사용 ■ Trusted Extensions 매뉴얼 페이지 사용	“Trusted Extensions 사용자 설명서 ”의 “레이블이 있는 시스템에서의 작업”
신뢰할 수 있는 경로가 필요한 작업을 수행합니다.	작업은 다음과 같습니다. ■ 장치 할당 ■ 암호 변경 ■ 작업 공간의 레이블 변경	“Trusted Extensions 사용자 설명서 ”의 “신뢰할 수 있는 작업 수행”
역할을 전환합니다.	역할의 전역 영역에 둡니다. 모든 관리 작업은 전역 영역에서 수행됩니다.	Trusted Extensions에서 전역 영역으로 들어가는 방법 [114]
사용자 작업 공간을 선택합니다.	전역 영역에서 나옵니다.	Trusted Extensions에서 전역 영역을 종료하는 방법 [114]

▼ Trusted Extensions에서 전역 영역으로 들어가는 방법

역할을 맡아서 Trusted Extensions에서 전역 영역으로 들어갑니다. 전체 시스템은 전역 영역에서만 관리할 수 있습니다.

문제 해결을 위해 Failsafe Session(비상 안전 세션)을 시작하여 전역 영역에 들어갈 수도 있습니다. 자세한 내용은 Trusted Extensions에서 비상 안전 세션에 로그인하는 방법 [134]을 참조하십시오.

시작하기 전에 관리 역할이 지정됩니다. 요약 내용은 "Trusted Extensions에서 역할 만들기" [106]를 참조하십시오.

1. **신뢰할 수 있는 스트라이프의 *account-name*을 누릅니다.**
   목록에서 역할을 선택합니다.
   Trusted Extensions 데스크탑 기능의 위치는 그림 6-1. "Trusted Extensions 다중 레벨 데스크탑"을 참조하십시오. 이러한 기능에 대한 설명은 "Trusted Extensions 사용자 설명서 "의 4 장, "Trusted Extensions의 요소"를 참조하십시오.
2. **프롬프트에 역할 암호를 입력합니다.**
   인증 후, 현재 작업 공간이 역할 작업 공간으로 변경됩니다.

▼ Trusted Extensions에서 전역 영역을 종료하는 방법

시작하기 전에 사용자가 전역 영역에 있습니다.

1. **화면 하단의 데스크탑 패널에서 사용자 작업 공간을 선택합니다.**
2. **또는 신뢰할 수 있는 스트라이프에서 역할 이름을 누른 다음 사용자 이름을 선택합니다.**
   현재 작업 공간이 사용자 작업 공간으로 변경됩니다. 이 작업 공간에서 만드는 이후의 모든 창은 사용자의 사용자 레이블에서 만들어집니다.
   역할 작업 공간에서 만든 창은 계속해서 역할 레이블에서 프로세스를 지원합니다. 이러한 창에서 시작된 프로세스는 관리 권한으로 전역 영역에서 실행됩니다.
   자세한 내용은 "Trusted Extensions 사용자 설명서 "의 "레이블이 있는 시스템에서의 작업"을 참조하십시오.

Trusted Extensions에서 일반 작업 수행

다음 작업 맵에서는 Trusted Extensions의 일반적인 관리 절차를 설명합니다.

표 9-2 Trusted Extensions에서 일반 관리 작업 수행 작업 맵

작업	설명	수행 방법
root 암호를 변경합니다.	root 역할에 대한 새 암호를 지정합니다.	데스크탑 시스템에서 root에 대한 암호 변경 방법 [115]
레이블이 있는 영역에서 암호 변경 사항을 반영합니다.	영역을 재부트하여 암호가 변경된 영역을 업데이트합니다.	레이블이 있는 영역에서 새 로컬 사용자 암호를 강제 적용하는 방법 [116]
보안 키 조합을 사용합니다.	마우스나 키보드의 컨트롤을 가져옵니다. 또한 마우스나 키보드를 신뢰할 수 있는지 여부를 테스트합니다.	데스크탑의 현재 포커스에 대한 컨트롤을 다시 얻는 방법 [117]
레이블에 대한 16진수를 결정합니다.	텍스트 레이블에 대한 내부 표현을 표시합니다.	레이블에 해당하는 16진수를 얻는 방법 [117]
레이블에 대한 텍스트 표현을 결정합니다.	16진수 레이블에 대한 텍스트 표현을 표시합니다.	읽기 가능한 레이블을 해당 16진수 형식에서 얻는 방법 [119]
장치를 할당합니다.	사용자가 장치를 할당할 수 있도록 합니다. 주변 기기를 사용하여 정보를 추가하거나 시스템에서 정보를 제거합니다.	"Oracle Solaris 11.2에서 시스템 및 연결된 장치의 보안 "의 "장치를 할당할 수 있도록 사용자에게 권한을 부여하는 방법" "Trusted Extensions 사용자 설명서 "의 "Trusted Extensions에서 장치를 할당하는 방법"
시스템 구성 파일을 변경합니다.	기본 Trusted Extensions 및 Oracle Solaris 보안 값을 변경합니다.	시스템 파일에서 보안 기본값을 변경하는 방법 [119]
원격으로 시스템을 관리합니다.	원격 시스템에서 Trusted Extensions 시스템을 관리합니다.	12장. Trusted Extensions에서 원격 관리

▼ 데스크탑 시스템에서 root에 대한 암호 변경 방법

Trusted Extensions에서는 암호 변경을 위한 GUI를 제공합니다.

1. **root 역할을 맡습니다.**
   단계는 Trusted Extensions에서 전역 영역으로 들어가는 방법 [114]을 참조하십시오.

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

3. **Change Login Password(로그인 암호 변경)를 선택합니다.**
   영역마다 별도의 암호가 만들어진 경우 Change Workspace Password(작업 공간 암호 변경) 메뉴가 나타날 수도 있습니다.

4. **암호를 변경하고 변경 내용을 확인합니다.**

▼ 레이블이 있는 영역에서 새 로컬 사용자 암호를 강제 적용하는 방법

다음 조건에서는 레이블이 있는 영역을 재부트해야 합니다.

- 한 명 이상의 로컬 사용자가 암호를 변경했습니다.
- 모든 영역에서 단일 인스턴스의 이름 지정 서비스 캐시 데몬(nscd)을 사용합니다.
- 시스템이 LDAP가 아닌 파일로 관리됩니다.

시작하기 전에 Zone Security 권한 프로파일이 지정되어 있어야 합니다.

- **암호 변경 사항을 강제 적용하려면 사용자가 액세스할 수 있는 레이블이 있는 영역을 재부트합니다.**
  다음 방법 중 하나를 사용합니다.

  - **`txzonemgr` GUI를 사용합니다.**

    ```
    # txzonemgr &
    ```

    Labeled Zone Manager(레이블이 있는 영역 관리자)에서 레이블이 있는 영역으로 이동하고 명령 목록에서 Halt(정지)를 선택한 다음 Boot(부트)를 선택합니다.

  - **전역 영역의 터미널 창에서 영역 관리 명령을 사용합니다.**
    시스템을 종료하거나 정지하도록 선택할 수 있습니다.

    - `zlogin` 명령은 영역을 완전히 종료합니다.

      ```
      # zlogin labeled-zone shutdown -i 0
      # zoneadm -z labeled-zone boot
      ```

    - `halt` 하위 명령은 종료 스크립트를 건너뜁니다.

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

일반 오류 레이블이 있는 영역에 대한 사용자 암호를 자동으로 업데이트하려면 LDAP를 구성하거나 영역마다 하나의 이름 지정 서비스를 구성해야 합니다. 둘 다 구성할 수도 있습니다.

- LDAP를 구성하려면 5장. Trusted Extensions에 대한 LDAP 구성을 참조하십시오.
- 영역마다 하나의 이름 지정 서비스를 구성하려면 고급 네트워킹 기술이 필요합니다. 절차는 각 레이블이 있는 영역에 대해 별도의 이름 서비스를 구성하는 방법 [53]을 참조하십시오.

▼ 데스크탑의 현재 포커스에 대한 컨트롤을 다시 얻는 방법

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

1. **Sun 키보드의 컨트롤을 다시 얻으려면 다음 키 조합을 사용하십시오.**
   키를 동시에 눌러 현재 데스크탑 포커스에 대한 컨트롤을 다시 얻습니다. Sun 키보드에서 다이아몬드는 Meta 키입니다.

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

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

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

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

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

예 9-1 암호 프롬프트를 신뢰할 수 있는지 테스트

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

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

예 9-2 포인터를 신뢰할 수 있는 스트라이프로 가져오기

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

▼ 레이블에 해당하는 16진수를 얻는 방법

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

시작하기 전에 전역 영역에서 보안 관리자 역할을 가진 사용자여야 합니다. 자세한 내용은 Trusted Extensions에서 전역 영역으로 들어가는 방법 [114]을 참조하십시오.

- **레이블에 대한 16진수 값을 얻으려면 다음 중 하나를 수행하십시오.**

  - **민감도 레이블에 대한 16진수 값을 얻으려면 명령에 레이블을 전달합니다.**

    ```
    # atohexlabel "CONFIDENTIAL : INTERNAL USE ONLY"
    0x0004-08-48
    ```

    문자열은 대소문자를 구분하지 않지만 공백은 정확해야 합니다. 예를 들어, 다음 따옴표로 묶인 문자열은 16진수 레이블을 반환합니다.

    - `"CONFIDENTIAL : INTERNAL USE ONLY"`
    - `"cnf : Internal"`
    - `"confidential : internal"`

    다음 따옴표로 묶인 문자열은 구문 분석 오류를 반환합니다.

    - `"confidential:internal"`
    - `"confidential: internal"`

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

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

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

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

예 9-3 `atohexlabel` 명령 사용

16진수 형식의 유효 레이블을 전달하면 명령에서 인수를 반환합니다.

```
# atohexlabel 0x0004-08-68
0x0004-08-68
```

관리 레이블을 전달하면 명령에서 인수를 반환합니다.

```
# atohexlabel admin_high
```

```
ADMIN_HIGH
atohexlabel admin_low
ADMIN_LOW
```

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

▼ 읽기 가능한 레이블을 해당 16진수 형식에서 얻는 방법

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

시작하기 전에 전역 영역에서 보안 관리자 역할을 가진 사용자여야 합니다.

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

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

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

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

▼ 시스템 파일에서 보안 기본값을 변경하는 방법

보안 값은 /etc/security 및 /etc/default 디렉토리의 파일에 있습니다. 자세한 내용은 "Oracle Solaris 11.2에서 시스템 및 연결된 장치의 보안 "의 3 장, "시스템에 대한 액세스 제어"를 참조하십시오.

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

시작하기 전에 전역 영역에 있고 solaris.admin.edit/*filename* 권한 부여가 지정되었습니다. 기본적으로 root 역할에는 이 권한 부여가 있습니다.

- **시스템 파일을 편집합니다.**

  다음 표에는 보안 파일 및 해당 파일에서 변경할 수 있는 보안 값이 나열되어 있습니다. 처음 두 개 파일은 Trusted Extensions에 고유합니다.

파일	작업	자세한 정보
/usr/share/gnome/의 sel_config	정보가 다른 레이블로 이동될 때 시스템이 작동하는 방식을 지정합니다.	sel_config(4) 매뉴얼 페이지
/usr/lib/xorg/의 TrustedExtensionsPolicy	X 서버에서 레이블 구분에 대한 SUN_TSOL 보안 정책 시행을 수정합니다.	TrustedExtensionsPolicy(4) 매뉴얼 페이지
/etc/default/login	허용되는 암호 시도 횟수를 줄입니다.	passwd(1) 매뉴얼 페이지
/etc/default/kbd	키보드 종료를 사용 안함으로 설정합니다.	"Oracle Solaris 11.2에서 시스템 및 연결된 장치의 보안 "의 "시스템 중단 시퀀스를 사용 안함으로 설정하는 방법" **참고** - 관리자가 디버깅에 사용하는 호스트에서 KEYBOARD_ABORT에 대한 기본 설정은 kadb 커널 디버거에 대한 액세스를 허용합니다. kadb(1M) 매뉴얼 페이지
/etc/security/policy.conf	사용자 암호에 대한 보다 강력한 알고리즘을 필요로 합니다. 이 호스트의 모든 사용자에게서 기본 권한을 제거합니다. 이 호스트의 사용자를 Basic Solaris User(기본 Solaris 사용자) 권한 부여로 제한합니다.	policy.conf(4) 매뉴얼 페이지
/etc/default/passwd	사용자가 암호를 자주 변경해야 합니다. 사용자가 최대한 다른 암호를 만들어야 합니다. 보다 긴 사용자 암호를 요구합니다. 사전에서 찾을 수 없는 암호를 요구합니다.	passwd(1) 매뉴얼 페이지

♦ ♦ ♦ 10 장

10 Trusted Extensions의 사용자, 권한 및 역할 정보

이 장에서는 일반 사용자를 만들기 전에 결정해야 하는 필수 사항을 설명하고, 사용자 계정 관리를 위한 추가 배경 정보를 제공합니다. 이 장에서는 초기 설정 팀이 역할 및 제한된 수의 사용자 계정을 설정했다고 가정합니다. 이러한 사용자는 Trusted Extensions를 구성하고 관리하는 데 사용되는 역할을 맡을 수 있습니다. 자세한 내용은 "Trusted Extensions의 역할 및 사용자 만들기" [54]를 참조하십시오.

Trusted Extensions의 사용자 보안 기능

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

- 사용자는 시스템을 사용할 수 있는 레이블 범위를 가집니다.
- 역할은 관리 작업을 수행하는 데 사용할 수 있는 레이블 범위를 가집니다.
- Trusted Extensions 권한 프로파일의 명령은 레이블 속성을 가집니다. 명령은 레이블 범위 내에서 또는 특정 레이블에서 수행되어야 합니다.
- Trusted Extensions 소프트웨어는 Oracle Solaris에서 정의한 권한 및 권한 부여 세트에 권한 및 권한 부여를 추가합니다.

사용자에 대한 관리자 책임

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

사용자 및 역할 설정에 대한 자세한 내용은 다음을 참조하십시오.

- “Oracle Solaris 11.2의 사용자 계정 및 사용자 환경 관리 ”의 “CLI를 사용하여 사용자 계정을 설정 및 관리하기 위한 작업 맵”
- “Oracle Solaris 11.2의 사용자 및 프로세스 보안 ”

사용자에 대한 시스템 관리자 책임

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

- 사용자 추가 및 삭제
- 역할 추가 및 삭제
- 초기 암호 지정
- 사용자 및 역할 등록 정보 수정(보안 속성 제외)

사용자에 대한 보안 관리자 책임

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

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

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

권한 프로파일을 만들기 전에 보안 관리자는 새 프로파일의 명령이 성공하기 위해 권한 또는 권한 부여가 필요한지 여부를 분석해야 합니다. 개별 명령에 대한 매뉴얼 페이지에는 필요할 수 있는 권한 및 권한 부여가 나열되어 있습니다.

Trusted Extensions에서 사용자를 만들기 전에 결정할 사항

다음 결정 사항은 사용자가 Trusted Extensions에서 수행할 수 있는 작업 및 필요한 노력에 영향을 줍니다. 일부 결정 사항은 Oracle Solaris OS를 설치할 때 내리는 결정 사항과 동일합니다. 그러나 Trusted Extensions에 고유한 결정 사항은 사이트 보안 및 사용 편의성에 영향을 줄 수 있습니다.

- `policy.conf` 파일에서 기본 사용자 보안 속성을 변경할지 여부를 결정합니다. `label_encodings` 파일의 사용자 기본값은 원래 초기 설정 팀에서 구성했습니다. 기본값에 대한 설명은 "Trusted Extensions의 기본 사용자 보안 속성" [123]을 참조하십시오.
- 각 사용자의 최소 레이블 홈 디렉토리에서 사용자의 상위 레벨 홈 디렉토리로 복사하거나 링크할 시작 파일(있는 경우)을 결정합니다. 절차는 Trusted Extensions에서 사용자의 시작 파일을 구성하는 방법 [132]을 참조하십시오.
- 사용자가 마이크, CD-ROM 드라이브 및 USB 장치와 같은 주변 기기에 액세스할 수 있는지 여부를 결정합니다.

  일부 사용자에게 액세스가 허용된 경우 사이트 보안을 위해 사이트에서 추가 권한 부여를 필요로 하는지 여부를 결정합니다. 장치 관련 권한 부여의 기본 목록은 장치 권한 부여를 지정하는 방법 [277]을 참조하십시오. 더 세분화된 장치 권한 부여를 만들려면 "Trusted Extensions에서 장치 권한 부여 사용자 정의" [273]를 참조하십시오.
- 레이블이 있는 영역에서 사용자 계정을 별도로 만들어야 하는지 결정합니다.

  기본적으로 레이블이 있는 영역은 전역 영역의 이름 서비스 구성을 공유합니다. 따라서 전역 영역에서는 모든 영역에 대해 사용자 계정이 생성됩니다. 레이블이 있는 영역의 `/etc/passwd` 및 `/etc/shadow` 파일은 전역 영역 파일에 대한 읽기 전용 뷰입니다. 마찬가지로 LDAP 데이터베이스는 레이블이 있는 영역에서 읽기 전용입니다.

  영역 내에서 영역에 설치하는 응용 프로그램에서 사용자 계정을 만들어야 합니다(예: `pkg:/service/network/ftp`). 영역 관련 응용 프로그램에서 사용자 계정을 만들 수 있도록 설정하려면 각 레이블이 있는 영역에 대해 별도의 이름 서비스를 구성하는 방법 [53]에 설명된 대로 영역별 이름 서비스 데몬을 구성해야 합니다. 이러한 응용 프로그램이 레이블이 있는 영역에 추가하는 사용자 계정은 영역 관리자가 수동으로 관리해야 합니다.

참고 - LDAP에 저장된 계정은 전역 영역에서 계속 관리됩니다.

Trusted Extensions의 기본 사용자 보안 속성

`label_encodings` 및 `policy.conf` 파일의 설정에서 함께 사용자 계정에 대한 기본 보안 속성을 정의합니다. 사용자에 대해 명시적으로 설정하는 값은 이러한 시스템 값을 대체합니다. 이러한 파일에 설정된 몇몇 값은 역할 계정에도 적용됩니다. 명시적으로 설정할 수 있는 보안 속성은 "Trusted Extensions에서 구성 가능한 사용자 속성" [124]을 참조하십시오.

`label_encodings` 파일 기본값

`label_encodings` 파일은 사용자의 최소 레이블, 클리어런스 및 기본 레이블 보기를 정의합니다. 파일에 대한 자세한 내용은 `label_encodings(4)` 매뉴얼 페이지를 참조하십시오. 사이

트의 label_encodings 파일은 초기 설정 팀에서 설치했습니다. 이러한 결정 사항은 “레이블 전략 고안” [19] 및 “Trusted Extensions Label Administration ”의 예를 기준으로 합니다.

보안 관리자가 개별 사용자에 대해 명시적으로 설정하는 레이블 값은 label_encodings 파일의 값을 대체합니다.

Trusted Extensions의 policy.conf 파일 기본값

/etc/security/policy.conf 파일에는 시스템에 대한 기본 보안 값이 들어 있습니다. Trusted Extensions는 이 파일에 두 개의 키워드를 추가합니다. 시스템 전체적으로 값을 변경하려면 이러한 *keyword=value* 쌍을 파일에 추가합니다. 다음 표는 이러한 키워드에 대한 기본값 및 가능한 값을 나타냅니다.

표 10-1 policy.conf 파일의 Trusted Extensions 보안 기본값

키워드	기본값	가능한 값	주
IDLECMD	LOCK	LOCK | LOGOUT	로그인 사용자에게 적용됩니다.
IDLETIME	15	0 - 120분	로그인 사용자에게 적용됩니다.

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

“Trusted Extensions의 사용자 보안 계획” [24]에는 모든 policy.conf 키워드의 표가 포함되어 있습니다. policy.conf(4) 매뉴얼 페이지도 참조하십시오.

Trusted Extensions에서 구성 가능한 사용자 속성

둘 이상의 레이블에 로그인할 수 있는 사용자에 대해 각 사용자의 최소 레이블 홈 디렉토리에서 .copy_files 및 .link_files의 두 도우미 파일을 설정할 수도 있습니다. 자세한 내용은 “.copy_files 및 .link_files 파일” [126]을 참조하십시오.

사용자에게 지정해야 하는 보안 속성

보안 관리자는 새 사용자에 대한 보안 속성을 수정할 수 있습니다. 기본값이 포함된 파일에 대한 자세한 내용은 “Trusted Extensions의 기본 사용자 보안 속성” [123]을 참조하십시오. 다음 표에는 사용자에게 지정할 수 있는 보안 속성과 각 지정의 효과가 나와 있습니다.

표 10-2 사용자를 만든 후 지정되는 보안 속성

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

Trusted Extensions에서 사용자에게 보안 속성 지정

사용자 계정이 만들어진 후 보안 관리자는 사용자에게 보안 속성을 지정합니다. 올바른 기본값을 설정한 경우 다음 단계는 기본값에 대한 예외가 필요한 사용자에 대해서만 보안 속성을 지정하는 것입니다.

사용자에게 보안 속성을 지정할 때 다음 정보를 고려하십시오.

암호 지정

시스템 관리자는 계정을 만들 때 사용자 계정에 암호를 지정할 수 있습니다. 이 초기 지정 이후 보안 관리자 또는 사용자는 암호를 변경할 수 있습니다.

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

참고 - 역할을 맡을 수 있는 사용자에 대한 암호는 암호 만료일 제약 조건의 적용을 받지 않습니다.

역할 지정

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

권한 부여 지정

Oracle Solaris OS와 마찬가지로 사용자에게 권한 부여를 지정하면 해당 권한 부여가 기존 권한 부여에 추가됩니다. 확장성을 위해서는 권한 프로파일에 권한 부여를 추가한 다음 사용자에게 프로파일을 지정합니다.

권한 프로파일 지정

Oracle Solaris OS와 마찬가지로 권한 프로파일의 순서가 중요합니다. 권한 부여를 제외하고 프로파일 방식에서는 지정된 보안 속성의 첫번째 인스턴스 값을 사용합니다. 자세한 내용은 "Oracle Solaris 11.2의 사용자 및 프로세스 보안 "의 "지정된 권한 검색 순서"를 참조하십시오.

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

참고 - 관리 명령이 포함된 권한 프로파일을 일반 사용자에게 지정하지 마십시오. 일반 사용자는 전역 영역에 들어갈 수 없으므로 권한 프로파일이 작동하지 않습니다.

권한 기본값 변경

기본 권한은 많은 사이트에서 너무 광범위할 수 있습니다. 시스템의 일반 사용자에 대한 권한 세트를 제한하려면 `policy.conf` 파일 설정을 변경합니다. 개별 사용자에 대한 권한을 변경하려면 사용자의 권한 세트를 제한하는 방법 [137]을 참조하십시오.

레이블 기본값 변경

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

감사 기본값 변경

Oracle Solaris OS와 마찬가지로 감사 클래스를 사용자에게 지정하면 사용자의 사전 선택 마스크가 수정됩니다. 감사에 대한 자세한 내용은 "Oracle Solaris 11.2의 감사 관리 " 및 22장. Trusted Extensions와 감사를 참조하십시오.

`.copy_files` 및 `.link_files` 파일

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

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

`.copy_files` 파일은 사용자가 다른 레이블에서 약간 다른 시작 파일을 원할 때 유용합니다. 예를 들어, 사용자가 다른 레이블에서 다른 메일 별칭을 사용할 경우 복사가 권장됩니다. `.link-files` 파일은 시작 파일이 호출된 모든 레이블에서 같아야 할 때 유용합니다. 예를 들어, 모든 레이블이 있는 인쇄 작업에 하나의 프린터가 사용되는 경우 링크가 권장됩니다. 예

제 파일은 Trusted Extensions에서 사용자의 시작 파일을 구성하는 방법 [132]을 참조하십시오.

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

```
.acrorc                 .cshrc                  .mime_types
.aliases                .emacs                  .newsrc
.bashrc                 .login                  .signature
.bashrc.user            .mailrc                 .soffice
```

♦ ♦ ♦ 11 장

11 Trusted Extensions에서 사용자, 권한 및 역할 관리

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

보안을 위한 사용자 환경 사용자 정의

다음 작업 맵에서는 모든 사용자에 대해 시스템을 사용자 정의하거나 개발 사용자의 계정을 사용자 정의할 때 수행할 수 있는 일반적인 작업을 설명합니다. 이러한 작업 중 상당수는 일반 사용자가 로그인하기 전에 수행됩니다.

표 11-1 보안을 위한 사용자 환경 사용자 정의 작업 맵

작업	설명	수행 방법
레이블 속성을 변경합니다.	사용자 계정에 대한 최소 레이블 및 기본 레이블 보기와 같은 레이블 속성을 수정합니다.	기본 사용자 레이블 속성을 수정하는 방법 [130]
시스템의 모든 사용자에 대한 Trusted Extensions 정책을 변경합니다.	`policy.conf` 파일을 변경합니다.	`policy.conf` 기본값을 수정하는 방법 [130]
	시스템이 유휴 상태인 일정 시간 경과 후 화면 보호기를 실행하거나 사용자를 로그아웃시킵니다.	예 11-1. "시스템의 유휴 설정 변경"
	시스템의 모든 일반 사용자에게서 불필요한 권한을 제거합니다.	예 11-2. "모든 사용자의 기본 권한 세트 수정"
	공용 키오스크에서 인쇄된 출력에 레이블이 나타나지 않도록 합니다.	예 11-3. "시스템의 모든 사용자에게 인쇄 관련 권한 부여 지정"
사용자에 대한 초기화 파일을 구성합니다.	모든 사용자의 시작 파일(`.bashrc`, `.cshrc`, `.copy_files`, `.soffice` 등)을 구성합니다.	Trusted Extensions에서 사용자의 시작 파일을 구성하는 방법 [132]
비상 안전 세션에 로그인합니다.	잘못된 사용자 초기화 파일을 수정합니다.	Trusted Extensions에서 비상 안전 세션에 로그인하는 방법 [134]

▼ 기본 사용자 레이블 속성을 수정하는 방법

첫번째 시스템 구성 중에 기본 사용자 레이블 속성을 수정할 수 있습니다. 추가 Trusted Extensions 시스템을 설치할 때 수정된 인코딩 파일을 사용합니다.

주의 - 일반 사용자가 시스템에 액세스하기 전에 이 작업을 완료해야 합니다.

시작하기 전에 전역 영역에서 보안 관리자 역할을 가진 사용자여야 합니다. 자세한 내용은 Trusted Extensions에서 전역 영역으로 들어가는 방법 [114]을 참조하십시오.

1. **`/etc/security/tsol/label_encodings` 파일에서 기본 사용자 속성 설정을 검토합니다.**

   기본값은 "Trusted Extensions의 사용자 보안 계획" [24]의 표 1-2. "사용자 계정에 대한 Trusted Extensions 보안 기본값"를 참조하십시오.

2. **활성 인코딩 파일의 복사본을 편집합니다.**

   a. **활성 파일을 찾습니다.**

   ```
   # labeladm encodings
   Label encodings file: /var/tsol/encodings/label_encodings.fSaG.L
   ```

   b. **활성 파일의 복사본을 편집합니다.**

   ```
   # cp /var/tsol/encodings/label_encodings.fSaG.L /tmp/tmp-encodings
   # pfedit /tmp/tmp-encodings
   ```

3. **시스템의 레이블 인코딩 파일을 바꾸고 시스템을 재부트합니다.**

   ```
   # labeladm encodings /tmp/tmp-encodings
   # /usr/sbin/reboot
   ```

4. **모든 Trusted Extensions 시스템에서 이 절차를 반복합니다.**

주의 - 활성 레이블 인코딩 파일의 컨텐츠는 모든 시스템에서 동일해야 합니다.

▼ `policy.conf` 기본값을 수정하는 방법

Trusted Extensions에서 `policy.conf` 기본값을 변경하는 것은 Oracle Solaris에서 보안 관련 시스템 파일을 변경하는 것과 유사합니다. 이 절차를 사용하여 시스템의 모든 사용자에 대한 기본값을 변경합니다.

시작하기 전에 전역 영역에서 root 역할을 가진 사용자여야 합니다. 자세한 내용은 Trusted Extensions에서 전역 영역으로 들어가는 방법 [114]을 참조하십시오.

1. **/etc/security/policy.conf 파일에서 기본 설정을 검토합니다.**

   Trusted Extensions 키워드는 표 10-1, "policy.conf 파일의 Trusted Extensions 보안 기본값"을 참조하십시오.

2. **설정을 수정합니다.**

   ```
   # pfedit /etc/security/policy.conf
   ```

예 11-1 시스템의 유휴 설정 변경

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

```
IDLECMD=LOGOUT
```

또한 관리자는 시스템이 유휴 상태 이후 로그아웃되는 시간을 줄이려고 합니다. 따라서 root 역할은 IDLETIME *keyword=value* 쌍을 policy.conf 파일에 다음과 같이 추가합니다.

```
IDLETIME=10
```

이제 시스템은 10분 동안의 유휴 상태 이후 사용자를 로그아웃합니다.

로그인 사용자가 역할을 맡을 경우 해당 사용자의 IDLECMD 및 IDLETIME 값이 해당 역할에 적용됩니다.

예 11-2 모든 사용자의 기본 권한 세트 수정

이 예에서 대규모 Sun Ray 설치의 보안 관리자는 일반 사용자가 다른 Sun Ray 사용자의 프로세스를 보지 못하게 하려고 합니다. 따라서 Trusted Extensions로 구성된 모든 시스템에서 root 역할은 기본 권한 세트에서 proc_info를 제거합니다. /etc/policy.conf 파일의 PRIV_DEFAULT 설정은 다음과 같이 주석 처리 해제 및 수정됩니다.

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

예 11-3 시스템의 모든 사용자에게 인쇄 관련 권한 부여 지정

이 예에서 사이트 보안은 공용 키오스크 컴퓨터에서 레이블 없이 인쇄할 수 있도록 허용합니다. 공용 키오스크에서 root 역할이 /etc/security/policy.conf 파일에서 AUTHS_GRANTED 값을 수정합니다. 다음 부팅부터 이 키오스크에서 모든 사용자의 인쇄 작업은 페이지 레이블 없이 인쇄됩니다.

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

그런 다음 관리자는 용지 절약을 위해 배너 및 트레일러 페이지를 제거하기로 결정합니다. 관리자가 `policy.conf` 항목을 더 수정합니다.

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

공용 키오스크를 재부트한 후에 모든 인쇄 작업은 레이블이 없으며 배너나 트레일러 페이지도 없습니다.

▼ Trusted Extensions에서 사용자의 시작 파일을 구성하는 방법

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

시작하기 전에 전역 영역에서 시스템 관리자 역할을 가진 사용자여야 합니다. 자세한 내용은 Trusted Extensions에서 전역 영역으로 들어가는 방법 [114]을 참조하십시오.

1. **두 Trusted Extensions 시작 파일을 만듭니다.**

   `.copy_files` 및 `.link_files`를 시작 파일 목록에 추가할 것입니다.

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

2. **`.copy_files` 파일을 사용자 정의합니다.**

   a. **편집기에서 `.copy_files` 파일의 전체 경로 이름을 입력합니다.**

      ```
      # pfedit /etc/skel/.copy_files
      ```

   b. **모든 레이블에서 사용자의 홈 디렉토리에 복사할 파일을 한 행에 하나씩 `.copy_files`에 입력합니다.**

      “`.copy_files` 및 `.link_files` 파일” [126]을 참조하십시오. 샘플 파일은 예 11-4. “사용자의 시작 파일 사용자 정의”를 참조하십시오.

3. **`.link_files` 파일을 사용자 정의합니다.**

   a. **편집기에서 `.link_files`의 전체 경로 이름을 입력합니다.**

      ```
      # pfedit /etc/skel/.link_files
      ```

   b. **모든 레이블에서 사용자의 홈 디렉토리에 링크할 파일을 한 행에 하나씩 `.link_files`에 입력합니다.**

4. **사용자에 대한 기타 시작 파일을 사용자 정의합니다.**

   - 시작 파일에 포함할 파일에 대한 설명은 "Oracle Solaris 11.2의 사용자 계정 및 사용자 환경 관리 "의 "사용자 작업 환경 정보"를 참조하십시오.
   - 자세한 내용은 "Oracle Solaris 11.2의 사용자 계정 및 사용자 환경 관리 "의 "사용자 초기화 파일을 사용자가 정의하는 방법"을 참조하십시오.

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

   P는 프로파일 셸을 나타냅니다.

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

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

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

예 11-4 사용자의 시작 파일 사용자 정의

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

시스템 관리자는 다음 내용으로 `.copy_files` 및 `.link_files` 파일을 만듭니다.

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

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

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

셸 초기화 파일에서 관리자가 사용자 정의를 추가합니다.

```
## .cshrc file
setenv EDITOR emacs
```

```
setenv ETOOLS /net/tools/etools

## .ksh file
export EDITOR emacs
export ETOOLS /net/tools/etools
```

사용자 정의된 파일은 적절한 골격 디렉토리에 복사됩니다.

```
# cp .copy_files .link_files .bashrc .bashrc.user .cshrc \
.login .profile .mailrc /etc/skelC
# cp .copy_files .link_files .ksh .profile .mailrc \
/etc/skelK
```

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

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

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

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

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

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

▼ Trusted Extensions에서 비상 안전 세션에 로그인하는 방법

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

시작하기 전에 root 암호를 알고 있어야 합니다.

1. **로그인 화면에서 사용자 이름을 입력합니다.**
2. **화면 하단의 데스크탑 메뉴에서 Solaris Trusted Extensions Failsafe Session(비상 안전 세션)을 선택합니다.**
3. **메시지가 표시되면 암호를 입력합니다.**
4. **추가 암호를 입력하라는 프롬프트가 표시되면 root 암호를 입력합니다.**

이제 사용자의 초기화 파일을 디버깅할 수 있습니다.

사용자 및 권한 관리

Trusted Extensions에서 사용자, 권한 부여, 권한 및 역할을 관리하려면 보안 관리자 역할을 맡습니다. 다음 작업 맵에서는 레이블이 있는 환경에서 작업하는 사용자에 대해 수행하는 일반적인 작업을 설명합니다.

표 11-2 사용자 및 권한 관리 작업 맵

작업	설명	수행 방법
사용자의 레이블 범위를 수정합니다.	사용자가 작업할 수 있는 레이블을 수정합니다. 수정으로 `label_encodings` 파일에서 허용하는 범위를 제한하거나 확장할 수 있습니다.	사용자의 레이블 범위를 수정하는 방법 [135]
편리한 권한 부여를 위해 권한 프로파일을 만듭니다.	일반 사용자에게 유용한 여러 권한이 있습니다. 이러한 권한 부여 자격을 갖춘 사용자에 대한 프로파일을 만듭니다.	편리한 권한 부여를 위해 권한 프로파일을 만드는 방법 [136]
사용자의 기본 권한 세트를 수정합니다.	사용자의 기본 권한 세트에서 권한을 제거합니다.	사용자의 권한 세트를 제한하는 방법 [137]
특정 사용자에 대한 계정 잠금을 방지합니다.	역할을 맡을 수 있는 사용자에 대해 계정 잠금을 해제해야 합니다.	사용자에 대한 계정 잠금을 방지하는 방법 [137]
사용자가 데이터 레이블을 재지정할 수 있도록 합니다.	사용자가 정보를 다운그레이드하거나 업그레이드할 수 있게 권한 부여합니다.	사용자가 데이터의 보안 레벨을 변경할 수 있게 하는 방법 [138]
시스템에서 사용자를 제거합니다.	사용자 및 사용자의 프로세스를 완전히 제거합니다.	Trusted Extensions 시스템에서 사용자 계정을 삭제하는 방법 [139]

▼ 사용자의 레이블 범위를 수정하는 방법

사용자에게 관리 응용 프로그램에 대한 읽기 액세스 권한을 부여하기 위해 사용자의 레이블 범위를 확장할 수 있습니다. 예를 들어, 전역 영역에 로그인할 수 있는 사용자는 특정 레이블에서 실행되는 시스템의 목록을 볼 수 있습니다. 사용자는 내용을 볼 수 있지만 변경할 수는 없습니다.

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

시작하기 전에 전역 영역에서 보안 관리자 역할을 가진 사용자여야 합니다.

- **다음 중 하나를 수행합니다.**

  - **사용자의 레이블 범위를 확장하려면 더 상위의 클리어런스를 지정합니다.**

```
# usermod -K min_label=INTERNAL -K clearance=ADMIN_HIGH jdoe
```

최소 레이블을 낮추어 사용자의 레이블 범위를 확장할 수도 있습니다.

```
# usermod -K min_label=PUBLIC -K clearance=INTERNAL jdoe
```

자세한 내용은 usermod(1M) 및 user_attr(4) 매뉴얼 페이지를 참조하십시오.

- **레이블 범위를 하나의 레이블로 제한하려면 클리어런스가 최소 레이블과 같아지도록 합니다.**

```
# usermod -K min_label=INTERNAL -K clearance=INTERNAL jdoe
```

▼ 편리한 권한 부여를 위해 권한 프로파일을 만드는 방법

사이트 보안 정책에서 허용하는 경우 권한 부여가 필요한 작업을 수행할 수 있는 사용자에 대해 권한 부여가 포함된 권한 프로파일을 만들 수 있습니다. 특정 시스템의 모든 사용자가 권한 부여를 받도록 하려면 policy.conf 기본값을 수정하는 방법 [130]을 참조하십시오.

시작하기 전에 전역 영역에서 보안 관리자 역할을 가진 사용자여야 합니다.

1. **다음 권한 부여 중 하나 이상이 포함된 권한 프로파일을 만듭니다.**
   단계별 절차는 "Oracle Solaris 11.2의 사용자 및 프로세스 보안 "의 "권한 프로파일을 만드는 방법"을 참조하십시오.
   사용자에게 편리할 수 있는 권한 부여:
   - solaris.device.allocate - 사용자가 마이크나 CD-ROM과 같은 주변 장치를 할당할 수 있게 권한 부여합니다.
     기본적으로 Oracle Solaris 사용자는 CD-ROM을 읽고 쓸 수 있습니다. 그러나 Trusted Extensions에서는 장치를 할당할 수 있는 사용자만 CD-ROM 드라이브에 액세스할 수 있습니다. 사용할 드라이브를 할당하려면 권한 부여가 필요합니다. 따라서 Trusted Extensions에서 CD-ROM을 읽고 쓰려면 사용자에게 Allocate Device(장치 할당) 권한 부여가 필요합니다.
   - solaris.label.file.downgrade - 사용자가 파일의 보안 레벨을 낮출 수 있게 권한 부여합니다.
   - solaris.label.file.upgrade - 사용자가 파일의 보안 레벨을 높일 수 있게 권한 부여합니다.
   - solaris.label.win.downgrade - 사용자가 상위 레벨 파일에서 정보를 선택하고 하위 레벨 파일에 해당 정보를 넣을 수 있게 권한 부여합니다.
   - solaris.label.win.noview - 사용자가 이동되는 정보를 보지 않고 정보를 이동할 수 있게 권한 부여합니다.
   - solaris.label.win.upgrade - 사용자가 하위 레벨 파일에서 정보를 선택하고 상위 레벨 파일에 해당 정보를 넣을 수 있게 권한 부여합니다.

- `solaris.login.remote` - 사용자가 원격으로 로그인할 수 있게 권한 부여합니다.
- `solaris.print.nobanner` - 사용자에게 배너 페이지 없이 복사본을 인쇄할 수 있는 권한을 부여합니다.
- `solaris.print.unlabeled` - 사용자에게 레이블을 표시하지 않는 복사본을 인쇄할 수 있는 권한을 부여합니다.
- `solaris.system.shutdown` - 사용자가 시스템과 영역을 종료할 수 있게 권한 부여합니다.

2. **사용자 또는 역할에 권한 프로파일을 지정합니다.**

   단계별 지침은 "Oracle Solaris 11.2의 사용자 및 프로세스 보안 "의 "사용자에게 권한 지정"을 참조하십시오.

▼ 사용자의 권한 세트를 제한하는 방법

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

시작하기 전에 전역 영역에서 보안 관리자 역할을 가진 사용자여야 합니다.

- **`basic` 세트에서 하나 이상의 권한을 제거합니다.**

주의 - `proc_fork` 또는 `proc_exec` 권한은 제거하지 마십시오. 이러한 권한이 없으면 사용자는 시스템을 사용할 수 없습니다.

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

`proc_info` 권한을 제거하면 사용자가 자신이 실행하지 않는 프로세스를 검사할 수 없게 됩니다. `proc_session` 권한을 제거하면 사용자가 현재 세션 외부에 있는 프로세스를 볼 수 없게 됩니다. `file_link_any` 권한을 제거하면 사용자가 소유하고 있지 않은 파일에 대한 하드 링크를 만들 수 없게 됩니다.

참조 권한 프로파일에서 권한 제한 사항을 수집하는 예는 "Oracle Solaris 11.2의 사용자 및 프로세스 보안 "의 "권한 프로파일을 만드는 방법"의 예제를 참조하십시오.

시스템에서 모든 사용자의 권한을 제한하려면 예 11-2. "모든 사용자의 기본 권한 세트 수정"를 참조하십시오.

▼ 사용자에 대한 계정 잠금을 방지하는 방법

역할을 맡을 수 있는 모든 사용자에 대해 이 절차를 수행합니다.

시작하기 전에 전역 영역에서 보안 관리자 역할을 가진 사용자여야 합니다.

- **로컬 사용자에 대한 계정 잠금을 해제합니다.**

```
# usermod -K lock_after_retries=no jdoe
```

LDAP 사용자에 대한 계정 잠금을 해제하려면 LDAP 저장소를 지정합니다.

```
# usermod -S ldap -K lock_after_retries=no jdoe
```

▼ 사용자가 데이터의 보안 레벨을 변경할 수 있게 하는 방법

파일 및 디렉토리나 선택한 텍스트의 보안 레벨 또는 레이블을 변경할 수 있게 일반 사용자나 역할을 권한 부여할 수 있습니다. 또한 두 개 이상의 레이블에서 작업할 수 있도록 사용자나 역할을 구성해야 합니다. 그리고 레이블 재지정을 허용하도록 레이블이 있는 영역을 구성해야 합니다. 절차는 레이블이 있는 영역에서 파일의 레이블을 재지정할 수 있게 설정하는 방법 [162]을 참조하십시오.

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

시작하기 전에 전역 영역에서 보안 관리자 역할을 가진 사용자여야 합니다.

- **적절한 사용자 및 역할에 Object Label Management 권한 프로파일을 지정합니다.**

  단계별 절차는 “Oracle Solaris 11.2의 사용자 및 프로세스 보안 ”의 “사용자에게 권한 지정”을 참조하십시오.

예 11-5 사용자가 파일의 레이블을 업그레이드할 수 있지만 다운그레이드할 수는 없도록 설정

Object Label Management 권한 프로파일을 사용하여 레이블을 업그레이드 및 다운그레이드할 수 있습니다. 이 예에서 관리자는 신뢰할 수 있는 사용자가 데이터를 업그레이드하는 것은 허용하지만 다운그레이드하는 것은 허용하지 않습니다.

관리자는 Object Label Management 프로파일을 기반으로 권한 프로파일을 만들고 새 프로파일에서 Downgrade File Label(파일 레이블 다운그레이드) 및 Downgrade DragNDrop or CutPaste Info(DragNDrop 또는 CutPaste 정보 다운그레이드) 권한 부여를 제거합니다.

```
# profiles -p "Object Label Management"
profiles:Object Label Management> set name="Object Upgrade"
profiles:Object Upgrade> info auths
...
profiles:Object Upgrade> remove auths="solaris.label.file.downgrade,
solaris.label.win.downgrade"
profiles:Object Upgrade> commit
```

```
profiles:Object Upgrade> end
```

그런 다음 관리자는 신뢰할 수 있는 사용자에게 프로파일을 지정합니다.

```
# usermod -P +"Object Upgrade" jdoe
```

▼ Trusted Extensions 시스템에서 사용자 계정을 삭제하는 방법

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

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

시작하기 전에 전역 영역에서 시스템 관리자 역할을 가진 사용자여야 합니다.

1. **모든 레이블에서 사용자의 홈 디렉토리를 아카이브합니다.**
2. **모든 레이블에서 사용자의 메일 파일을 아카이브합니다.**
3. **사용자 계정을 삭제합니다.**

   ```
   # userdel -r jdoe
   ```

4. **모든 레이블이 있는 영역에서 사용자의 디렉토리 및 메일 파일을 수동으로 삭제합니다.**

참고 - `/tmp` 디렉토리의 파일을 비롯하여 모든 레이블에서 사용자의 임시 파일을 찾아 삭제해야 합니다.

추가 고려 사항은 "사용자 삭제 방법" [109]을 참조하십시오.

♦ ♦ ♦ 12 장

12 Trusted Extensions에서 원격 관리

이 장에서는 원격 관리를 위해 Trusted Extensions 시스템을 설정하고 로그인 및 관리하는 방법을 설명합니다.

참고 - 헤드리스 시스템과 기타 원격 시스템에 필요한 구성 방법은 평가된 구성의 조건을 만족시키지 않습니다. 자세한 내용은 “사이트 보안 정책의 이해” [18]를 참조하십시오.

Trusted Extensions에서 원격 관리

원격 관리는 높은 보안 위험을 노출하게 되며, 특히 신뢰할 수 없는 시스템의 사용자의 경우 더욱 그러합니다. 기본적으로 Trusted Extensions는 어느 시스템에서나 원격 관리를 허용하지 않습니다.

네트워크가 구성될 때까지 모든 원격 호스트에는 `admin_low` 보안 템플리트가 지정되어 레이블이 없는 호스트로 인식됩니다. 레이블이 있는 영역이 구성될 때까지는 전역 영역만 사용할 수 있습니다. Trusted Extensions에서 전역 영역은 관리 영역입니다. 역할만 여기에 액세스할 수 있습니다. 구체적으로 전역 영역에 접근하려면 계정에 `ADMIN_LOW ~ ADMIN_HIGH` 범위의 레이블이 있어야 합니다.

이 초기 상태에서 Trusted Extensions 시스템은 다양한 방식을 통해 원격 공격으로부터 보호됩니다. 방식에는 `netservices` 값, 기본 `ssh` 정책, 기본 로그인 정책 및 기본 PAM 정책이 포함됩니다.

- 설치 시 보안 셸을 제외한 원격 서비스는 네트워크에서 수신이 사용으로 설정되지 않습니다.

  하지만 `ssh` 서비스는 `ssh`, 로그인 및 PAM 정책으로 인해 `root`나 다른 역할에서 원격 로그인을 위해 사용할 수 없습니다.
- `root`는 역할이므로 원격 로그인을 위해 `root` 계정을 사용할 수 없습니다. 역할은 PAM으로 인해 로그인할 수 없습니다.

root가 사용자 계정으로 변경되더라도 기본 로그인 및 ssh 정책에서 root 사용자의 원격 로그인을 막습니다.

- 두 기본 PAM 값이 원격 로그인을 막습니다.

  pam_roles 모듈은 role 유형 계정에서의 로컬 및 원격 로그인을 거부합니다.

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

따라서 Oracle Solaris 시스템과 마찬가지로 원격 관리를 구성해야 합니다. Trusted Extensions에는 전역 영역에 접근하는 데 필요한 레이블 범위 및 pam_tsol_account 모듈의 두 가지 구성 요구 사항이 추가됩니다.

Trusted Extensions에서 원격 시스템을 관리하는 방법

Trusted Extensions에서는 호스트 기반 인증과 함께 Secure Shell 프로토콜을 사용하여 원격 시스템에 연결하고 관리해야 합니다. 호스트 기반 인증을 통해 동일하게 이름이 지정된 사용자 계정이 원격 Trusted Extensions에서 역할을 맡을 수 있습니다.

호스트 기반 인증을 사용할 때 Secure Shell 클라이언트는 원래 사용자 이름과 역할 이름을 모두 원격 시스템인 서버에 보냅니다. 이 정보와 함께 서버는 충분한 컨텐츠를 pam_roles 모듈에 전달하여 사용자 계정이 서버에 로그인하지 않고도 역할을 맡을 수 있도록 합니다.

Trusted Extensions에서는 다음과 같은 방법으로 원격 관리를 수행할 수 있습니다.

- **Trusted Extensions 시스템에서 관리** - 대부분의 보안 원격 관리에서는 두 시스템이 해당 피어를 CIPSO 보안 템플리트에 지정합니다. 예 12-1. “원격 관리를 위한 CIPSO 호스트 유형 지정”을 참조하십시오.
- **레이블이 없는 시스템에서 관리** - Trusted Extensions 시스템에서 관리가 불가능한 경우 PAM 스택에서 pam_tsol_account 모듈에 대해 allow_unlabeled 옵션을 지정하여 네트워크 프로토콜 정책을 완화할 수 있습니다.

  이 정책을 완화할 경우 임의의 시스템에서 전역 영역에 접근할 수 없도록 기본 보안 템플리트를 변경해야 합니다. admin_low 템플리트는 가끔씩 사용해야 하며 와일드카드 주소 0.0.0.0은 기본값이 ADMIN_LOW 레이블이 되면 안됩니다. 자세한 내용은 신뢰할 수 있는 네트워크에서 연결할 수 있는 호스트를 제한하는 방법 [212]을 참조하십시오.

관리 시나리오에서 원격 로그인을 위해 root 역할을 사용하려면 pam_roles 모듈에 대해 allow_remote 옵션을 지정하여 PAM 정책을 완화해야 합니다.

일반적으로 관리자는 ssh 명령을 사용하여 명령줄에서 원격 시스템을 관리합니다. -X 옵션을 통해 Trusted Extensions 관리 GUI를 사용할 수 있습니다.

또한 Xvnc 서버를 사용하여 원격 Trusted Extensions를 구성할 수도 있습니다. 그런 다음 가상 네트워크 컴퓨팅(VNC) 연결을 사용하여 원격 다중 레벨 데스크탑을 표시하고 시스템을 관리할 수 있습니다. 원격 액세스를 위해 Xvnc를 사용하여 Trusted Extensions 시스템을 구성하는 방법 [145]을 참조하십시오.

Trusted Extensions에서 원격 시스템 구성 및 관리

원격 시스템을 Trusted Extensions로 재부트하기 전에 원격 관리를 사용으로 설정한 후 가상 네트워크 컴퓨팅(VNC) 또는 ssh 프로토콜을 사용하여 시스템을 구성할 수 있습니다.

표 12-1 Trusted Extensions에서 원격 시스템 구성 및 관리 작업 맵

작업	설명	수행 방법
Trusted Extensions 시스템의 원격 관리를 사용으로 설정합니다.	지정된 ssh 클라이언트에서 Trusted Extensions 시스템의 관리를 사용으로 설정합니다.	원격 Trusted Extensions 시스템의 원격 관리 사용 [143]
가상 네트워크 컴퓨팅(VNC)을 사용으로 설정합니다.	클라이언트에서 원격 Trusted Extensions 시스템의 Xvnc 서버를 사용하여 클라이언트로 다시 연결되는 서버의 다중 레벨 세션을 표시합니다.	원격 액세스를 위해 Xvnc를 사용하여 Trusted Extensions 시스템을 구성하는 방법 [145]
Trusted Extensions 시스템에 원격으로 로그인합니다.	원격 시스템을 관리할 수 있는 역할을 맡습니다.	원격 Trusted Extensions 시스템에 로그인하고 관리하는 방법 [148]

참고 - 보안 정책을 검토하여 사이트에서 허용되는 원격 관리 방법을 결정합니다.

▼ 원격 Trusted Extensions 시스템의 원격 관리 사용

이 절차에서는 Trusted Extensions 기능을 추가하기 전에 Oracle Solaris 원격 시스템에서 호스트 기반 인증을 사용으로 설정합니다. 원격 시스템은 Secure Shell 서버입니다.

시작하기 전에 원격 시스템에는 Oracle Solaris가 설치되어 있고 해당 시스템에 액세스할 수 있습니다. root 역할을 가진 사용자여야 합니다.

1. **두 시스템에서 호스트 기반 인증을 사용으로 설정합니다.**

   절차는 "Oracle Solaris 11.2의 보안 셸 액세스 관리 "의 "보안 셸에 대한 호스트 기반 인증 설정 방법"을 참조하십시오.

   참고 - cat 명령을 사용하지 마십시오. Secure Shell 연결을 통해 공개 키를 복사하여 붙여 넣습니다. Secure Shell 클라이언트가 Oracle Solaris 시스템이 아닌 경우 Secure Shell 클라이언트를 호스트 기반 인증으로 구성하기 위한 해당 플랫폼의 지침을 따르십시오.

   이 단계를 완료하면 두 시스템에서 root 역할을 맡을 수 있는 사용자 계정을 가지게 됩니다. 계정에는 동일한 UID, GID 및 역할이 지정됩니다. 또한 공개/개인 키 쌍을 생성하고 공개 키를 공유했습니다.

2. **Secure Shell 서버에서 ssh 정책을 완화하여 root가 원격으로 로그인하도록 사용으로 설정합니다.**

```
# pfedit /etc/ssh/sshd_config
## Permit remote login by root
PermitRootLogin yes
```

이후의 단계는 root 로그인을 특정 시스템 및 사용자로 제한합니다.

참고 - 관리자가 root 역할을 맡게 되므로 원격 root 로그인을 막는 로그인 정책을 완화할 필요가 없습니다.

3. **Secure Shell 서버에서 ssh 서비스를 다시 시작합니다.**

```
# svcadm restart ssh
```

4. **Secure Shell 서버의 root 홈 디렉토리에서 호스트 기반 인증을 위한 호스트 및 사용자를 지정합니다.**

```
# cd
# pfedit .shosts
client-host username
```

.shosts 파일은 공용/개인 키가 공유되면 *client-host* 시스템의 *username*이 서버에서 root 역할을 맡을 수 있도록 설정합니다.

5. **Secure Shell 서버에서 두 가지 PAM 정책을 완화합니다.**

   a. **/etc/pam.d/other를 /etc/pam.d/other.orig에 복사합니다.**

```
# cp /etc/pam.d/other /etc/pam.d/other.orig
```

   b. **pam_roles 항목을 수정하여 역할의 원격 로그인을 허용합니다.**

```
# pfedit /etc/pam.d/other
...
# Default definition for Account management
# Used when service name is not explicitly mentioned for account management
# ...
#account requisite    pam_roles.so.1
# Enable remote role assumption
account requisite    pam_roles.so.1   allow_remote
...
```

이 정책은 *client-host* 시스템의 *username*이 서버에서 역할을 맡을 수 있도록 설정합니다.

   c. **pam_tsol_account 항목을 수정하여 레이블이 없는 호스트가 Trusted Extensions 원격 시스템에 연결할 수 있도록 합니다.**

```
# pfedit /etc/pam.d/other
# Default definition for Account management
```

```
# Used when service name is not explicitly mentioned for account management
# ...
#account requisite    pam_roles.so.1
# Enable remote role assumption
account requisite    pam_roles.so.1   allow_remote
#
account required     pam_unix_account.so.1
#account required     pam_tsol_account.so.1
# Enable unlabeled access to TX system
account required     pam_tsol_account.so.1  allow_unlabeled
```

6. **구성을 테스트합니다.**

   a. **원격 시스템에서 새 터미널을 엽니다.**

   b. ***client-host*에서 *username*이 소유한 창에서 원격 시스템의 `root` 역할을 맡습니다.**

      ```
      % ssh -l root remote-system
      ```

7. **구성 작동을 확인한 후 원격 시스템에서 Trusted Extensions를 사용으로 설정하고 재부트합니다.**

   ```
   # svcadm enable -s labeld
   # /usr/sbin/reboot
   ```

예 12-1 원격 관리를 위한 CIPSO 호스트 유형 지정

이 예에서 관리자는 Trusted Extensions 시스템을 사용하여 원격 Trusted Extensions 호스트를 구성합니다. 이를 위해 관리자는 각 시스템에서 `tncfg` 명령을 사용하여 피어 시스템의 호스트 유형을 정의합니다.

remote-system `# tncfg -t cipso add host=192.168.1.12` *Client-host*

client-host `# tncfg -t cipso add host=192.168.1.22` *Remote system*

관리자가 레이블이 없는 시스템에서 원격 Trusted Extensions 호스트를 구성할 수 있도록 하려면 관리자는 `pam.d/other` 파일에서 `allow_unlabeled` 옵션을 그대로 둡니다.

▼ 원격 액세스를 위해 Xvnc를 사용하여 Trusted Extensions 시스템을 구성하는 방법

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

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

시작하기 전에 Xvnc 서버로 사용될 이 시스템에서 Trusted Extensions를 설치하고 구성했습니다. 이 시스템의 전역 영역은 고정 IP 주소를 가지므로 자동 네트워크 구성 프로파일을 사용하지 않습니다. netcfg(1M) 매뉴얼 페이지를 참조하십시오.

이 시스템은 호스트 이름 또는 IP 주소로 VNC 클라이언트를 인식합니다. 구체적으로 admin_low 보안 템플리트는 명시적으로 또는 와일드카드를 사용하여 이 서버의 VNC 클라이언트가 될 수 있는 시스템을 식별합니다. 보안 연결 구성에 대한 자세한 내용은 신뢰할 수 있는 네트워크에서 연결할 수 있는 호스트를 제한하는 방법 [212]을 참조하십시오.

미래 Trusted Extensions Xvnc 서버 콘솔의 GNOME 세션에서 현재 실행 중인 경우 데스크탑 공유가 사용으로 설정되지 않습니다.

미래 Trusted Extensions Xvnc 서버의 전역 영역에서 root 역할을 가집니다.

1. **Xvnc 소프트웨어를 로드하거나 업데이트합니다.**

```
# pkg search vnc
... set    VNC client based on the TigerVNC open source release that
           displays a session over RFB protocol from a VNC server
           pkg:/desktop/remote-desktop/tigervnc@version
... set    X Window System server based on X.Org Foundation open source
           release and TigerVNC open source release that displays over
           RFB protocol to a VNC client
           pkg:/x11/server/xvnc@version
...
```

한 가지 옵션은 TigerVNC X11/VNC 서버 소프트웨어입니다.

```
# pkg install server/xvnc
# pkg install remote-desktop/tigervnc
```

참고 - GUI를 열 수 없는 경우 X 서버 액세스 제어 목록에 로컬 root 계정을 추가합니다. X 서버에 로그인한 사용자로 이 명령을 실행합니다.

```
% xhost +si:localuser:root
```

자세한 내용은 xhost(1) 및 Xsecurity(5) 매뉴얼 페이지를 참조하십시오.

---

2. **X 디스플레이 관리자 제어 프로토콜을 사용으로 설정합니다.**

   GNOME 디스플레이 관리자(gdm) 사용자 정의 구성 파일을 수정합니다. /etc/gdm/custom.conf 파일에서 [xdmcp] 머리글 아래에 Enable=true를 입력합니다.

```
[xdmcp]
Enable=true
```

3. **/etc/gdm/Xsession 파일의 27행 주위에 다음 행을 삽입합니다.**

작은 정보 - 변경하기 전에 원래 `Xsession` 파일의 복사본을 저장합니다.

```
DISPLAY=unix:$(echo $DISPLAY|sed -e s/::ffff://|cut -d: -f2)
```

2단계 및 3단계의 파일은 패키지 속성 `preserve=true`로 표시됩니다. 패키지 업그레이드 및 패키지 수정 동안 이 속성이 수정된 파일에 미치는 영향에 대한 자세한 내용은 `pkg`(5) 매뉴얼 페이지를 참조하십시오.

4. **Xvnc 서버 서비스를 사용으로 설정합니다.**

```
# svcadm enable xvnc-inetd
```

5. **이 서버에서 모든 활성 GNOME 세션을 로그아웃합니다.**

```
# svcadm restart gdm
```

데스크탑 관리자가 다시 시작될 때까지 1분 정도 기다립니다. 그러면 VNC 클라이언트가 연결할 수 있습니다.

6. **Xvnc 소프트웨어가 사용으로 설정되었는지 확인합니다.**

```
% svcs | grep vnc
```

7. **이 Xvnc 서버의 모든 VNC 클라이언트에 VNC 클라이언트 소프트웨어를 설치합니다.**

클라이언트 시스템의 경우 소프트웨어를 선택할 수 있습니다. Oracle Solaris 저장소에서 VNC 소프트웨어를 사용할 수 있습니다.

8. **(옵션) VNC 연결을 감사합니다.**

시스템 및 사용자별로 감사 이벤트를 사전 선택하는 방법에 대한 자세한 내용은 "Oracle Solaris 11.2의 감사 관리 "의 "감사 서비스 구성"을 참조하십시오.

9. **VNC 클라이언트에 Xvnc 서버 작업 공간을 표시하려면 다음 단계를 수행합니다.**

   a. **클라이언트의 터미널 창에서 서버에 연결합니다.**

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

   명령 옵션은 `vncviewer`(1) 매뉴얼 페이지를 참조하십시오.

   b. **표시되는 창에서 사용자 이름과 암호를 입력합니다.**

   로그인 절차를 계속합니다. 나머지 단계에 대한 자세한 설명은 "Trusted Extensions 사용자 설명서 "의 "Trusted Extensions에 로그인"을 참조하십시오.

예 12-2 Vino를 사용하여 테스트 환경에서 데스크탑 공유

이 예에서는 두 개발자가 GNOME Vino 서비스를 사용하여 Launch(시작) -> System(시스템) -> Preferences(기본 설정) -> Desktop Sharing(데스크탑 공유) 메뉴에서 화면을 공유합니다. 앞의 단계와 더불어 이들 개발자는 XTEST 확장자를 사용으로 설정하여 Trusted Extensions 정책을 완화합니다.

```
# pfedit /usr/X11/lib/X11/xserver/TrustedExtensionsPolicy
## /usr/X11/lib/X11/xserver/TrustedExtensionsPolicy file
...
#extension XTEST
extension XTEST
...
```

▼ 원격 Trusted Extensions 시스템에 로그인하고 관리하는 방법

이 절차에서는 명령줄 및 `txzonemgr` GUI를 사용하여 원격 Trusted Extensions 시스템을 관리할 수 있습니다.

시작하기 전에 원격 Trusted Extensions 시스템의 원격 관리 사용 [143]에 설명된 대로 사용자, 역할 및 역할 지정은 로컬 및 원격 시스템에서 동일하게 정의됩니다.

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

   desktop `#` **`xhost +`** *remote-sys*

2. **두 시스템에 모두 동일하게 이름이 지정된 사용자인지 확인합니다.**

3. **터미널 창에서 원격 시스템에 로그인합니다.**
   `ssh` 명령을 사용하여 로그인합니다.

   ```
   desktop % ssh -X -l identical-username remote-sys
   Password: xxxxxxxx
   remote-sys %
   ```

   -X 옵션은 GUI가 표시되도록 합니다.

4. **동일한 터미널 창에서 두 시스템에 모두 동일하게 정의된 역할을 맡습니다.**
   예를 들어 `root` 역할을 수락합니다.

   ```
   remote-sys % su - root
   Password: xxxxxxxx
   ```

   이제 사용자가 전역 영역에 있습니다. 이 터미널을 사용하여 명령줄에서 원격 시스템을 관리할 수 있습니다. GUI가 화면에 표시됩니다. 예제는 예 12-3. "원격 시스템에서 레이블이 있는 영역 구성"를 참조하십시오.

예 12-3 원격 시스템에서 레이블이 있는 영역 구성

이 예에서는 관리자가 txzonemgr GUI를 사용하여 레이블이 있는 데스크탑 시스템에서 레이블이 있는 원격 시스템에 레이블이 있는 영역을 구성합니다. Oracle Solaris에서와 마찬가지로 관리자는 ssh 명령에 -X 옵션을 사용하여 X 서버에서 데스크탑 시스템에 액세스 할 수 있게 합니다. 사용자 jandoe는 두 시스템에 모두 동일하게 정의되어 있으며 remoterole 역할을 수락할 수 있습니다.

```
TXdesk1 # xhost + TXnohead4

TXdesk1 % ssh -X -l jandoe TXnohead4
Password: xxxxxxxx
TXnohead4 %
```

전역 영역에 접근하기 위해 관리자는 jandoe 계정을 사용하여 remoterole 역할을 맡습니다. 이 역할은 두 시스템에 모두 동일하게 정의되어 있습니다.

```
TXnohead4 % su - remoterole
Password: xxxxxxxx
```

동일한 터미널에서 remoterole 역할을 맡은 관리자가 txzonemgr GUI를 시작합니다.

```
TXnohead4 # /usr/sbin/txzonemgr &
```

Labeled Zone Manager(레이블이 있는 영역 관리자)가 원격 시스템에서 실행되고 로컬 시스템에 표시됩니다.

예 12-4 원격 레이블이 있는 영역에 로그인

관리자는 PUBLIC 레이블에서 원격 시스템의 구성 파일을 변경하려고 합니다.

관리자에게는 두 가지 옵션이 있습니다.

- 전역 영역에 원격으로 로그인하고 원격 전역 영역 작업 공간을 표시한 다음 작업 공간을 PUBLIC 레이블로 변경하고 터미널 창을 열어 파일을 편집합니다.
- PUBLIC 터미널 창에서 ssh 명령을 사용하여 PUBLIC 영역에 원격으로 로그인한 다음 파일을 편집합니다.

원격 시스템이 모든 영역에 대해 하나의 이름 지정 서비스 데몬(nscd)을 실행 중이고 원격 시스템이 파일 이름 지정 서비스를 사용 중인 경우 원격 PUBLIC 영역에 대한 암호는 영역이 마지막으로 부트되었을 때 유효한 암호입니다. 원격 PUBLIC 영역에 대한 암호가 변경되었지만 변경 이후 영역이 부트되지 않은 경우 원래 암호가 액세스를 허용합니다.

일반 오류 -X 옵션이 작동하지 않을 경우 패키지를 설치해야 할 수 있습니다. xauth 이진이 설치되지 않으면 X11 전달이 사용 안함으로 설정됩니다. **pkg install pkg:/x11/session/xauth** 명령은 이진을 로드합니다.

♦ ♦ ♦ 13 장

13 Trusted Extensions에서 영역 관리

이 장에서는 비전역 또는 레이블이 있는 영역이 Trusted Extensions 시스템에서 어떻게 작동하는지 설명합니다. 레이블이 있는 영역에 고유한 절차도 포함되어 있습니다.

Trusted Extensions의 영역

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

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

Trusted Extensions 시스템에서 모든 영역은 레이블 있음 브랜드를 가지며 레이블이 있는 영역의 모든 쓰기 가능한 파일 및 디렉토리는 영역의 레이블에 있습니다. 기본적으로 사용자는 현재 레이블보다 하위 레이블에 있는 영역의 파일을 볼 수 있습니다. 이 구성을 통해 현재 작업 공간의 레이블보다 하위 레이블에 있는 홈 디렉토리를 볼 수 있습니다. 사용자는 하위 레이블에서 파일을 볼 수 있지만 수정할 수는 없습니다. 사용자는 파일과 동일한 레이블을 가진 프로세스에서만 파일을 수정할 수 있습니다.

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

레이블이 있는 영역에서 디렉토리를 공유하는 방법과 레이블이 있는 영역에서 원격으로 디렉토리를 마운트하는 방법은 14장. Trusted Extensions에서 파일 관리 및 마운트 및 “mlslabel 등록 정보 및 단일 레벨 파일 시스템 마운트” [170]를 참조하십시오.

Trusted Extensions의 영역은 Oracle Solaris 영역 제품을 기반으로 구축됩니다. 참조 정보는 “Oracle Solaris 영역 소개 ”를 참조하십시오.

Trusted Extensions의 영역 및 IP 주소

초기 설치 팀이 전역 영역과 레이블이 있는 영역에 IP 주소를 지정했습니다. “레이블이 있는 영역에 액세스” [22]에 설명된 대로 세 가지 유형의 구성을 고려했으며 다음과 같이 요약됩니다.

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

  이 기본 구성은 DHCP 소프트웨어를 사용하여 해당 IP 주소를 얻는 시스템에 유용합니다.
- 시스템에 전역 영역에 대한 IP 주소와 전역 영역을 포함한 모든 영역에서 공유되는 IP 주소가 하나씩 있습니다. 모든 영역에서 고유 주소와 공유 주소를 조합하여 사용할 수 있습니다.

  이 구성은 일반 사용자가 로그인하는 네트워크로 연결된 시스템에 유용합니다. 프린터나 NFS 서버에도 이 구성을 사용할 수 있습니다. 이 구성은 IP 주소를 절약합니다.
- 시스템에 전역 영역에 대한 IP 주소가 하나 있고 레이블이 있는 영역마다 고유 IP 주소가 있습니다.

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

비전역 영역에 대한 네번째 유형의 구성은 배타적 IP 인스턴스로 Oracle Solaris에서 사용할 수 있습니다. 이 구성에서 비전역 영역은 자신의 IP 인스턴스에 지정되고 자신의 물리적 인터페이스를 관리합니다. 각 영역은 고유 시스템처럼 작동합니다. 자세한 내용은 “Oracle Solaris 영역 소개 ”의 “영역 네트워크 인터페이스”를 참조하십시오.

Trusted Extensions에서 배타적 IP 인스턴스를 구성할 경우 각 레이블이 있는 영역은 고유의 단일 레벨 시스템인 것처럼 작동합니다. Trusted Extensions의 다중 레벨 네트워킹 기능은 공유 IP 스택의 기능을 사용합니다. 이 설명서에서는 네트워킹을 전적으로 전역 영역에서 제어하는 것으로 간주합니다. 따라서 초기 설치 팀에서 배타적 IP 인스턴스로 레이블이 있는 영역을 설치한 경우 사이트별 설명서를 제공하거나 알려줘야 합니다.

영역 및 다중 레벨 포트

기본적으로 영역 간에는 패킷을 보내고 받을 수 없습니다. 포트의 특정 서비스에서 MLP(다중 레벨 포트)를 사용하여 레이블 범위나 레이블 세트에서 요청을 받을 수 있습니다. 이 권한 있는 서비스에서는 요청 레이블에 응답할 수 있습니다. 예를 들어, 모든 레이블을 수신할 수

있지만 레이블에 의해 응답이 제한되는 권한 있는 웹 브라우저 포트를 만들 수 있습니다. 기본적으로 레이블이 있는 영역에는 MLP가 없습니다.

MLP가 받을 수 있는 패킷을 제한하는 레이블 범위나 레이블 세트는 영역의 IP 주소를 기반으로 합니다. IP 주소는 Trusted Extensions 시스템과 통신하여 보안 템플리트에 지정됩니다. 보안 템플리트의 레이블 범위나 레이블 세트는 MLP가 받을 수 있는 패킷을 제한합니다.

다른 IP 주소 구성에 대한 MLP 제약 조건은 다음과 같습니다.

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

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

예는 영역에 대한 다중 레벨 포트를 만드는 방법 [218]을 참조하십시오.

Trusted Extensions의 영역 및 ICMP

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

전역 영역 프로세스 및 레이블이 있는 영역

Trusted Extensions에서는 전역 영역의 프로세스를 포함한 모든 프로세스에 MAC 정책이 적용됩니다. 전역 영역의 프로세스는 ADMIN_HIGH 레이블에서 실행됩니다. 전역 영역에서 공유되는 파일은 ADMIN_LOW 레이블에서 공유됩니다. MAC에서는 상위 레이블이 있는 프로세

스에서 하위 레이블 객체를 수정하지 못하므로 일반적으로 전역 영역에서 NFS 마운트된 시스템에 쓸 수 없습니다.

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

전역 영역 프로세스는 다음 조건에서 읽기/쓰기 권한으로 원격 파일 시스템을 마운트할 수 있습니다.

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

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

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

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

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

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

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

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

예를 들어, 공용 영역에서 장치를 할당하면 ADMIN_HIGH 레이블에서 실행되는 전역 영역 프로세스에서 영역 경로의 dev 디렉토리(/zone/public/dev)를 수정합니다. 마찬가지로 사용자가 데스크탑 구성을 저장하면 /zone/public/home/*username*의 전역 영역 프로세스에서 데스크탑 구성 파일을 수정합니다. 레이블이 있는 파일 시스템을 공유하려면 레이블이 있는 영역에서 파일 시스템을 공유하는 방법 [176]을 참조하십시오.

기본 및 보조 레이블이 있는 영역

특정 레이블에서 만드는 첫번째 영역은 기본 레이블이 있는 영역입니다. 이 영역의 레이블은 고유합니다. 해당 레이블에 다른 기본 영역을 만들 수 없습니다.

보조 영역은 기본 영역의 레이블에 있는 영역입니다. 보조 영역을 사용하여 서비스를 동일한 레이블에서 별도의 영역에 격리할 수 있습니다. 이러한 서비스는 이름 서버, 프린터 및 데이터베이스와 같은 네트워크 리소스를 권한 사용 없이 공유할 수 있습니다. 동일한 레이블에 여러 보조 영역이 있을 수 있습니다.

특히 보조 영역은 다음과 같은 면에서 기본 영역과 다릅니다.

- 보조 영역의 레이블 지정은 고유하지 않아도 됩니다.
- 보조 영역은 배타적 IP 네트워킹을 사용해야 합니다.

  이 제한에 따라 레이블이 있는 패킷은 올바른 영역에 연결해야 합니다.
- 보조 영역에는 GNOME 패키지가 설치되지 않습니다.

  보조 영역은 GNOME 신뢰할 수 있는 데스크탑에 표시되지 않습니다.
- 보조 영역은 `setlabel` 명령의 대상 영역이 될 수 없습니다.

  여러 영역이 동일한 레이블에 있는 경우 이 명령으로 대상 영역을 확인할 수 없습니다.

레이블에는 하나의 기본 레이블이 있는 영역과 임의 수의 보조 레이블이 있는 영역이 있을 수 있습니다. 전역 영역은 계속 예외입니다. 이 영역만 `ADMIN_LOW` 레이블을 지정할 수 있으므로 보조 영역을 포함할 수 없습니다. 보조 영역을 만들려면 보조 레이블이 있는 영역을 만드는 방법 [65] 및 `zenity`(1) 매뉴얼 페이지를 참조하십시오.

Trusted Extensions의 영역 관리 유틸리티

영역 관리 작업은 명령줄에서 수행할 수 있습니다. 하지만 영역을 관리하는 가장 간단한 방법은 Trusted Extensions에서 제공하는 셸 스크립트 `/usr/sbin/txzonemgr`를 사용하는 것입니다. 이 스크립트는 영역을 만들고 설치, 초기화 및 부트하기 위한 메뉴 기반 마법사를 제공합니다. 자세한 내용은 `txzonemgr`(1M) 및 `zenity`(1) 매뉴얼 페이지를 참조하십시오.

영역 관리

다음 작업 맵에서는 Trusted Extensions에 특정한 영역 관리 작업을 설명합니다. 또한 이 맵은 Oracle Solaris 시스템과 Trusted Extensions에서 수행되는 공통 절차에 대한 링크를 제공합니다.

표 13-1 영역 관리 작업 맵

작업	설명	수행 방법
모든 영역을 봅니다.	모든 레이블에서 현재 영역의 지배를 받는 영역을 봅니다.	준비 또는 실행 중인 영역을 표시하는 방법 [156]
마운트된 디렉토리를 봅니다.	모든 레이블에서 현재 레이블의 지배를 받는 디렉토리를 봅니다.	마운트된 파일의 레이블을 표시하는 방법 [157]
일반 사용자가 `/etc` 파일을 볼 수 있게 합니다.	루프백에서는 레이블이 있는 영역에 기본적으로 표시되지 않는 디렉토리 또는 파일을 전역 영역에서 마운트합니다.	레이블이 있는 영역에 일반적으로 표시되지 않는 파일을 루프백 마운트하는 방법 [158]
일반 사용자가 상위 레이블에서 하위 레벨 홈 디렉토리를 보지 못하게 합니다.	기본적으로 하위 레벨 디렉토리는 상위 레벨 영역에서 표시됩니다. 한 하위 레벨 영역의 마운트를 사용 안함으로 설정하면 하위 레벨 영역의 모든 마운트가 사용 안함으로 설정됩니다.	하위 레벨 파일의 마운트를 사용 안함으로 설정하는 방법 [159]
파일의 레이블 변경을 위한 다중 레벨 데이터 세트를 만듭니다.	권한 없이 하나의 ZFS 데이터 세트에서 파일의 레이블을 다시 지정을 사용으로 설정합니다.	다중 레벨 데이터 세트를 만들고 공유하는 방법 [66]
파일에서 레이블을 변경할 수 있도록 영역을 구성합니다.	기본적으로 레이블이 있는 영역에는 권한 부여된 사용자가 파일 레이블을 변경하게 할 수 있는 권한이 없습니다. 영역 구성을 수정하여 권한을 추가합니다.	레이블이 있는 영역에서 파일의 레이블을 재지정할 수 있게 설정하는 방법 [162]
ZFS 데이터 세트를 레이블이 있는 영역에 연결하고 공유합니다.	레이블이 있는 영역에서 읽기/쓰기 권한으로 ZFS 데이터 세트를 마운트하고 상위 영역과 읽기 전용으로 공유합니다.	레이블이 있는 영역에서 ZFS 데이터 세트를 공유하는 방법 [160]
새 기본 영역을 구성합니다.	이 시스템에서 영역의 레이블을 지정하는 데 현재 사용되고 있지 않은 레이블에서 영역을 만듭니다.	레이블이 있는 영역을 대화식으로 만드는 방법 [44]을 참조하십시오.
보조 영역을 구성합니다.	데스크탑이 필요하지 않은 서비스를 격리하기 위한 영역을 만듭니다.	보조 레이블이 있는 영역을 만드는 방법 [65].
응용 프로그램에 대한 다중 레벨 포트를 만듭니다.	다중 레벨 포트는 레이블이 있는 영역에 대한 다중 레벨 피드를 필요로 하는 프로그램에 유용합니다.	영역에 대한 다중 레벨 포트를 만드는 방법 [218] 예 16-22. “`udp`를 통해 NFSv3에 대한 개인 다중 레벨 포트 구성”
NFS 마운트 및 액세스 문제를 해결합니다.	마운트 및 영역에 대한 일반 액세스 문제를 디버깅합니다.	Trusted Extensions에서 마운트 실패 문제를 해결하는 방법 [179]
레이블이 있는 영역을 제거합니다.	레이블이 있는 영역을 시스템에서 완전히 제거합니다.	“Oracle Solaris 영역 만들기 및 사용 ”의 “비전역 영역 제거 방법”

▼ 준비 또는 실행 중인 영역을 표시하는 방법

시작하기 전에 전역 영역에서 시스템 관리자 역할을 가진 사용자여야 합니다.

1. **윈도우화 시스템에서 `txzonemgr &` 명령을 실행합니다.**
   영역 이름, 해당 상태 및 해당 레이블은 GUI에 표시됩니다.

2. **또한 `zoneadm list -v` 명령을 사용할 수도 있습니다.**

```
# zoneadm list -v
ID NAME       STATUS     PATH              BRAND       IP
0 global     running    /                 ipkg        shared
5 internal   running    /zone/internal    labeled     shared
6 public     running    /zone/public      labeled     shared
```

출력은 영역의 레이블을 나열하지 않습니다.

▼ 마운트된 파일의 레이블을 표시하는 방법

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

시작하기 전에 전역 영역에서 시스템 관리자 역할을 가진 사용자여야 합니다.

1. **편집기에서 `getmounts` 스크립트를 만듭니다.**

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

2. **다음 컨텐츠를 추가하고 파일을 저장합니다.**

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

3. **전역 영역에서 스크립트를 테스트합니다.**

```
# /usr/local/scripts/getmounts
/:      ADMIN_HIGH
/dev:   ADMIN_HIGH
/system/contract:        ADMIN_HIGH
/proc:                   ADMIN_HIGH
/system/volatile:        ADMIN_HIGH
/system/object:          ADMIN_HIGH
/lib/libc.so.1:          ADMIN_HIGH
/dev/fd:        ADMIN_HIGH
/tmp:           ADMIN_HIGH
/etc/mnttab:    ADMIN_HIGH
/export:        ADMIN_HIGH
/export/home:   ADMIN_HIGH
/export/home/jdoe:   ADMIN_HIGH
/zone/public:        ADMIN_HIGH
/rpool:              ADMIN_HIGH
/zone:               ADMIN_HIGH
/home/jdoe:          ADMIN_HIGH
/zone/public:        ADMIN_HIGH
```

```
/zone/snapshot:      ADMIN_HIGH
/zone/internal:      ADMIN_HIGH
...
```

예 13-1 restricted 영역의 파일 시스템 레이블 표시

일반 사용자가 레이블이 있는 영역에서 getmounts 스크립트를 실행하면 해당 영역에 마운트된 모든 파일 시스템의 레이블이 표시됩니다. 시스템에서 기본 label_encodings 파일의 모든 레이블에 대해 영역을 만든 경우 restricted 영역의 샘플 출력은 다음과 같습니다.

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

▼ 레이블이 있는 영역에 일반적으로 표시되지 않는 파일을 루프백 마운트하는 방법

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

시작하기 전에 전역 영역에서 시스템 관리자 역할을 가진 사용자여야 합니다.

1. **구성을 변경할 영역을 중지합니다.**

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

2. **파일이나 디렉토리를 루프백 마운트합니다.**
   예를 들어, 일반 사용자가 /etc 디렉토리에서 파일을 볼 수 있도록 허용합니다.

   ```
   # zonecfg -z zone-name
   ```

```
add filesystem
set special=/etc/filename
set directory=/etc/filename
set type=lofs
add options [ro,nodevices,nosetuid]
end
exit
```

3. **영역을 시작합니다.**

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

예 13-2 /etc/passwd 파일 루프백 마운트

이 예에서 보안 관리자는 테스터와 프로그래머가 로컬 암호가 설정되었는지 확인할 수 있도록 합니다. sandbox 영역이 중지된 후 passwd 파일을 루프백 마운트하도록 구성됩니다. 영역이 다시 시작된 후 일반 사용자는 passwd 파일의 항목을 볼 수 있습니다.

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

▼ 하위 레벨 파일의 마운트를 사용 안함으로 설정하는 방법

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

시작하기 전에 전역 영역에서 시스템 관리자 역할을 가진 사용자여야 합니다.

1. **구성을 변경할 영역을 중지합니다.**

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

2. **하위 레벨 파일을 보지 못하도록 영역을 구성합니다.**

영역에서 net_mac_aware 권한을 제거합니다.

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

3. **영역을 다시 시작합니다.**

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

예 13-3 사용자가 하위 레벨 파일을 보지 못하도록 금지

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

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

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

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

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

▼ 레이블이 있는 영역에서 ZFS 데이터 세트를 공유하는 방법

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

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

시작하기 전에 데이터 세트로 영역을 구성하려면 먼저 영역을 중지해야 합니다. 전역 영역에서 root 역할을 가진 사용자여야 합니다.

1. **ZFS 데이터 세트를 만듭니다.**

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

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

2. **전역 영역에서 레이블이 있는 영역을 중지합니다.**

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

3. **데이터 세트의 마운트 지점을 설정합니다.**

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

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

4. **데이터 세트가 공유되도록 설정합니다.**

```
# zfs set sharenfs=on datasetdir/subdir
```

5. **데이터 세트를 영역에 파일 시스템으로 추가합니다.**

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

데이터 세트를 파일 시스템으로 추가하면 데이터 세트가 영역의 /data에 마운트됩니다. 이 단계를 수행하면 영역이 부팅되기 전에 데이터 세트가 마운트되지 않습니다.

6. **레이블이 있는 영역을 부트합니다.**

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

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

예 13-4 레이블이 있는 영역에서 ZFS 데이터 세트 공유 및 마운트

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

먼저 관리자가 영역을 중지합니다.

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

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

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

그런 다음 관리자는 데이터 세트를 공유합니다.

```
# zfs set sharenfs=on zone/data
```

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

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

그런 다음 관리자는 needtoknow 영역을 부트합니다.

```
# zoneadm -z needtoknow boot
```

이제 데이터 세트를 액세스할 수 있습니다.

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

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

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

▼ 레이블이 있는 영역에서 파일의 레이블을 재지정할 수 있게 설정하는 방법

이 절차를 수행해야 사용자가 파일의 레이블을 바꿀 수 있습니다.

시작하기 전에 구성하려는 영역은 정지되어야 합니다. 전역 영역에서 보안 관리자 역할을 가진 사용자여야 합니다.

1. **Labeled Zone Manager(레이블이 있는 영역 관리자)를 엽니다.**

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

2. **레이블을 바꿀 수 있게 영역을 구성합니다.**

a. **영역을 두 번 누릅니다.**

b. **목록에서 Permit Relabeling(레이블 재지정 허용)을 선택합니다.**

3. **Boot(부트)를 선택하여 영역을 다시 시작합니다.**

4. **영역 목록으로 돌아가려면 Cancel(취소)을 누릅니다.**

   레이블 바꾸기를 허용하는 사용자 및 프로세스 요구 사항은 `setflabel`(3TSOL) 매뉴얼 페이지를 참조하십시오. 파일 레이블을 바꿀 수 있게 사용자를 권한 부여하려면 사용자가 데이터의 보안 레벨을 변경할 수 있게 하는 방법 [138]을 참조하십시오.

예 13-5 `internal` 영역에서 다운그레이드만 허용

이 예에서 보안 관리자는 `zonecfg` 명령을 사용하여 `CNF: INTERNAL USE ONLY` 영역에서 정보 다운그레이드는 사용으로 설정하지만 정보 업그레이드는 사용 안함으로 설정합니다.

```
# zonecfg -z internal set limitpriv=default,file_downgrade_sl
```

예 13-6 `internal` 영역에서 다운그레이드 방지

이 예에서 보안 관리자는 이전에 파일을 다운그레이드하는 데 사용된 시스템에서 `CNF: INTERNAL USE ONLY` 파일의 다운그레이드를 방지합니다.

관리자는 Labeled Zone Manager(레이블이 있는 영역 관리자)를 사용하여 `internal` 영역을 정지한 다음 `internal` 영역 메뉴에서 Deny Relabeling(레이블 재지정 거부)을 선택합니다.

♦ ♦ ♦ 14 장

14 Trusted Extensions에서 파일 관리 및 마운트

이 장에서는 파일 공유 및 마운트와 관련된 Trusted Extensions 정책 및 이 정책이 다중 레벨 데이터 세트의 ZFS 마운트와 단일 레벨 ZFS 데이터 세트의 LOFS 및 NFS 마운트에 미치는 영향에 대해 설명합니다. 이 장에서는 파일을 백업하고 복원하는 방법도 다룹니다.

Trusted Extensions에서 마운트 가능성

Trusted Extensions는 두 가지 종류의 ZFS 데이터 세트를 마운트할 수 있습니다.

- 단일 레벨 레이블 지정 데이터 세트는 데이터가 있거나 마운트된 영역과 레이블이 같습니다. 단일 레벨 데이터 세트의 모든 파일과 디렉토리는 동일한 레이블에 있습니다. 이러한 데이터 세트는 Trusted Extensions에서 일반적인 데이터 세트입니다.
- 다중 레벨 데이터 세트는 파일과 디렉토리를 여러 레이블에 포함할 수 있습니다. 이러한 데이터 세트는 여러 다른 레이블의 NFS 클라이언트를 지원하는 데 효율적이며 파일의 레이블을 다시 지정하는 프로세스를 간소화할 수 있습니다.

Trusted Extensions에서는 다음 마운트가 가능합니다.

- **ZFS 마운트** - 관리자가 만드는 다중 레벨 데이터 세트는 전역 영역에 ZFS 마운트될 수 있습니다. ZFS 마운트된 다중 레벨 데이터 세트는 동일한 시스템의 레이블이 있는 영역으로 LOFS 마운트될 수 있습니다.

  레이블이 있는 영역의 관리자가 단일 레벨 데이터 세트를 만들고 ZFS 마운트할 수도 있습니다.
- **LOFS 마운트** - 앞 단락에서 설명한 대로 전역 영역에서는 단일 레벨 데이터 세트를 레이블이 있는 영역으로 LOFS 마운트할 수 있습니다. 마운트의 레이블은 `ADMIN_LOW`이므로 마운트된 모든 파일은 레이블이 있는 영역에서 읽기 전용입니다.

전역 영역에서는 다중 레벨 데이터 세트도 레이블이 있는 영역으로 LOFS 마운트할 수 있습니다. 영역과 레이블이 동일한 마운트된 파일은 수정할 수 있습니다. 적절한 권한이 있으면 파일의 레이블을 다시 지정할 수 있습니다. 영역의 레이블보다 낮은 레벨에 있는 마운트된 파일을 볼 수 있습니다.

- **NFS 마운트** - 레이블이 있는 영역에서는 단일 레벨 데이터 세트를 영역의 레이블로 마운트할 수 있습니다. 이러한 파일은 다른 레이블이 있는 영역이나 레이블이 있는 영역과 동일한 레이블이 지정된 신뢰할 수 없는 시스템에서 온 것일 수 있습니다.

  전역 영역에서는 다른 Trusted Extensions 시스템에 있는 다중 레벨 데이터 세트를 NFS 마운트할 수 있습니다. 마운트된 파일을 보고 수정할 수는 있지만 레이블을 다시 지정할 수는 없습니다. 또한 마운트 영역의 레이블에 있는 파일 및 디렉토리만 올바른 레이블을 반환합니다.

  레이블이 있는 영역에서는 다른 Trusted Extensions 시스템에 있는 다중 레벨 데이터 세트를 NFS 마운트할 수 있습니다. NFS 마운트된 파일은 레이블을 다시 지정할 수 없고 `getlabel` 명령으로 파일의 레이블을 확인할 수 없습니다. 그러나 MAC 정책은 올바로 작동합니다. 영역과 레이블이 동일한 마운트된 파일은 보고 수정할 수 있습니다. 하위 레벨 파일을 볼 수 있습니다.

마운트된 파일 시스템에 대한 Trusted Extensions 정책

Trusted Extensions에서는 Oracle Solaris와 동일한 파일 시스템 및 파일 시스템 관리 명령을 지원하지만 Trusted Extensions의 마운트된 파일 시스템에서는 레이블 지정된 데이터를 보고 수정하기 위해 MAC(필수 액세스 제어) 정책을 준수해야 합니다. 마운트 정책과 읽기 및 쓰기 정책에서는 레이블 지정에 MAC 정책을 적용합니다.

단일 레벨 데이터 세트에 대한 Trusted Extensions 정책

단일 레벨 데이터 세트에 대해 마운트 정책에서는 MAC에 위반되는 NFS 또는 LOFS 마운트를 방지합니다. 예를 들어, 영역의 레이블은 마운트된 파일 시스템 레이블을 모두 지배해야 하고, 동일한 레이블의 파일 시스템만 읽기-쓰기 권한으로 마운트될 수 있습니다. 다른 영역이나 NFS 서버에 속한 공유 파일 시스템은 소유자 레이블에 마운트됩니다.

다음은 NFS 마운트된 단일 레벨 데이터 세트의 동작을 요약한 것입니다.

- 전역 영역에서 마운트된 파일은 모두 볼 수 있지만 `ADMIN_HIGH` 레이블이 지정된 파일만 수정할 수 있습니다.
- 레이블이 있는 영역에서는 영역의 레이블보다 낮거나 동일한 레이블에 마운트된 파일을 모두 볼 수 있지만 영역의 레이블에 있는 파일만 수정할 수 있습니다.
- 신뢰할 수 없는 시스템에서는 레이블이 신뢰할 수 없는 시스템에 지정된 레이블과 동일한 레이블이 있는 영역의 파일 시스템만 보고 수정할 수 있습니다.

LOFS 마운트된 단일 레벨 데이터 세트의 경우 마운트된 파일을 볼 수 있습니다. 이들 파일은 `ADMIN_LOW` 레이블에 있으므로 수정할 수 없습니다.

다중 레벨 데이터 세트에 대한 Trusted Extensions 정책

다중 레벨 데이터 세트의 경우 MAC 일기 및 쓰기 정책이 파일 시스템 단위가 아니라 파일 및 디렉토리 단위에서 적용됩니다.

다중 레벨 데이터 세트는 전역 영역에만 마운트될 수 있습니다. 레이블이 있는 영역에서는 LOFS `zonecfg` 명령으로 지정하는 LOFS 마운트 지점을 사용하여 다중 레벨 데이터 세트에 액세스할 수 있습니다. 절차는 다중 레벨 데이터 세트를 만들고 공유하는 방법 [66]을 참조하십시오. 전역 영역 또는 레이블이 있는 영역에서 적절히 권한이 부여된 프로세스를 통해 파일 및 디렉토리의 레이블을 다시 지정할 수 있습니다. 레이블 다시 지정 예는 “Trusted Extensions 사용자 설명서 ”를 참조하십시오.

- 전역 영역에서는 다중 레벨 데이터 세트의 모든 파일을 볼 수 있습니다. 레이블이 `ADMIN_HIGH`인 마운트된 파일은 수정할 수 있습니다.
- 레이블이 있는 영역에서는 다중 레벨 데이터 세트가 LOFS를 통해 마운트됩니다. 영역과 동일한 레이블이나 영역보다 낮은 레벨에 마운트된 파일을 볼 수 있습니다. 영역과 동일한 레이블에 마운트된 파일을 수정할 수 있습니다.
- 다중 레벨 데이터 세트는 전역 영역에서 NFS를 통해 공유될 수도 있습니다. 원격 클라이언트는 해당 네트워크 레이블에서 지배되는 파일을 볼 수 있고 동일한 레이블의 파일을 수정할 수 있습니다. 그러나 NFS 마운트된 다중 레벨 데이터 세트에 대한 레이블 다시 지정은 가능하지 않습니다. NFS 마운트에 대한 자세한 내용은 “다른 시스템에서 다중 레벨 데이터 세트 마운트” [171]를 참조하십시오.

자세한 내용은 “파일의 레이블 다시 지정을 위한 다중 레벨 데이터 세트” [170]를 참조하십시오.

MAC 읽기/쓰기 정책에 대한 권한 대체 없음

파일 읽기 및 쓰기에 대한 MAC 정책에는 권한 대체가 없습니다. 단일 레벨 데이터 세트는 영역의 레이블이 데이터 세트의 레이블과 동일한 경우에만 읽기/쓰기로 마운트될 수 있습니다. 읽기 전용 마운트의 경우 영역 레이블이 데이터 세트 레이블을 지배해야 합니다. 다중 레벨 데이터 세트의 경우 모든 파일 및 디렉토리는 `mlslabel` 등록 정보에 의해 지배되어야 합니다. 이 등록 정보는 기본적으로 `ADMIN_HIGH`로 설정됩니다. 다중 레벨 데이터 세트의 경우 MAC 정책이 파일 및 디렉토리 레벨에서 적용됩니다. MAC 정책 적용은 일부 사용자에게 표시되지 않습니다. 객체에 대한 MAC 액세스 권한이 없는 사용자는 객체를 볼 수 없습니다.

다음은 단일 레벨 데이터 세트에 대한 Trusted Extensions의 공유 및 마운트 정책을 요약한 것입니다.

- Trusted Extensions 시스템에서 다른 Trusted Extensions 시스템의 파일 시스템을 마운트하려면 서버와 클라이언트에 `cipso` 유형의 호환 가능한 원격 호스트 템플리트가 있어야 합니다.
- Trusted Extensions 시스템에서 신뢰할 수 없는 시스템의 파일 시스템을 마운트하려면 Trusted Extensions 시스템에서 신뢰할 수 없는 시스템에 지정한 단일 레이블이 전역 영역의 레이블과 일치해야 합니다.

마찬가지로 레이블이 있는 영역에서 신뢰할 수 없는 시스템의 파일 시스템을 마운트하려면 Trusted Extensions 시스템에서 신뢰할 수 없는 시스템에 지정한 단일 레이블이 있는 영역의 레이블과 일치해야 합니다.

- 레이블이 마운트 영역과 다르고 LOFS로 마운트된 파일은 볼 수 있지만 수정할 수는 없습니다. NFS 마운트에 대한 자세한 내용은 "Trusted Extensions에서 NFS 서버 및 클라이언트 구성" [172]을 참조하십시오.

다음은 다중 레벨 데이터 세트에 대한 Trusted Extensions의 공유 및 마운트 정책을 요약한 것입니다.

- Trusted Extensions 시스템에서 다른 시스템과 다중 레벨 데이터 세트를 공유하려면 NFS 서버를 다중 레벨 서비스로 구성해야 합니다.
- Trusted Extensions 시스템에서 자체 시스템의 레이블이 있는 영역과 다중 레벨 데이터 세트를 공유하려면 전역 영역에서 데이터 세트를 영역으로 LOFS 마운트해야 합니다.

  레이블이 있는 영역에서는 영역의 레이블과 레이블이 일치하는 LOFS 마운트된 파일 및 디렉토리에 대해서는 쓰기 권한이 있고 해당 영역에서 지배하는 파일 및 디렉토리에 대해서는 읽기 권한이 있습니다. MAC 정책은 개별 파일 및 디렉토리 레벨에서 적용됩니다.

Trusted Extensions에서 파일 시스템 공유 및 마운트의 결과

Trusted Extensions에서 공유 파일은 관리를 간소화하고 효율성을 제공하며 시간을 단축합니다. MAC는 항상 적용됩니다.

- NFS를 통해 레이블이 있는 영역에서 단일 레벨 데이터 세트 공유 - Oracle Solaris에서와 같이 공유 디렉토리는 관리를 간소화합니다. 예를 들어 Oracle Solaris에 대한 매뉴얼 페이지를 한 시스템에 설치하고 매뉴얼 페이지 디렉토리를 다른 시스템과 공유할 수 있습니다.
- LOFS를 통해 전역 영역에서 다중 레벨 데이터 세트 공유 - LOFS 마운트된 데이터 세트는 레이블 간에 파일을 이동할 때 효율성과 속도를 향상합니다. 파일이 데이터 세트 내에서 이동되므로 I/O 작업이 사용되지 않습니다.
- NFS를 통해 전역 영역에서 다중 레벨 데이터 세트 공유 - NFS 서버는 여러 레이블의 파일을 포함하는 다중 레벨 데이터 세트를 여러 클라이언트와 공유할 수 있습니다. 이러한 구성은 관리를 간소화하고 파일 배포를 위한 단일 위치를 제공합니다. 특정 레이블에서 서버 없이도 클라이언트를 지원할 수 있습니다.

전역 영역에서 파일 공유 및 마운트

전역 영역에서 파일을 마운트하는 것은 Oracle Solaris에서 파일을 마운트하는 것과 동일하며 MAC 정책의 적용을 받습니다. 전역 영역에서 공유되는 파일은 파일의 레이블에서 공유됩니다. 그러므로 전역 영역의 파일 시스템을 다른 Trusted Extensions 시스템의 전역 영역

과 공유하는 것은 유용하지 않습니다. 모든 파일이 ADMIN_LOW 레이블에서 공유되기 때문입니다. 전역 영역에서 다른 시스템과 공유하면 유용한 파일은 다중 레벨 데이터 세트입니다.

전역 영역에서 LOFS를 통해 공유되는 단일 레벨 데이터 세트의 파일 및 디렉토리는 ADMIN_LOW에서 공유됩니다. 예를 들어, 전역 영역의 /etc/passwd 및 /etc/shadow 파일은 시스템의 레이블이 있는 영역으로 LOFS 마운트될 수 있습니다. 이 파일은 ADMIN_LOW이므로 레이블이 있는 영역에서 표시되고 읽기 전용입니다. 다중 레벨 데이터 세트의 파일 및 디렉토리는 객체의 레이블에서 공유됩니다.

전역 영역에서는 NFS를 통해 다중 레벨 데이터 세트도 공유할 수 있습니다. 클라이언트는 NFS 서비스가 다중 레벨 포트를 사용하도록 구성된 경우 데이터 세트를 마운트하도록 요청할 수 있습니다. 클라이언트 레이블이 클라이언트의 NFS 마운트 요청을 처리하는 네트워크 인터페이스의 cipso 템플리트에 지정된 레이블 범위 내에 있는 경우 요청이 성공합니다.

특히 전역 영역 및 마운트된 파일의 동작의 다음과 같습니다.

- Trusted Extensions 클라이언트의 전역 영역에서 공유의 모든 항목은 읽을 수 있고 클라이언트는 로컬 전역 영역 프로세스와 마찬가지로 ADMIN_HIGH에서 쓸 수 있습니다.
- 클라이언트가 레이블이 있는 영역인 경우 영역의 레이블이 공유 파일의 레이블과 일치하면 마운트된 파일은 읽기/쓰기가 가능합니다.
- 클라이언트가 레이블 없는 시스템인 경우 클라이언트의 지정된 레이블이 공유 파일의 레이블과 일치하면 마운트된 파일은 읽기/쓰기가 가능합니다.
- ADMIN_LOW 레이블의 클라이언트는 데이터 세트를 마운트할 수 없습니다.
- 다중 레벨 데이터 세트를 동일한 시스템의 레이블 있는 영역과 공유하려면 전역 영역에서 LOFS를 사용할 수 있습니다.

NFS 마운트의 파일을 보고 레이블을 다시 지정하는 방법에 대한 자세한 내용은 “다른 시스템에서 다중 레벨 데이터 세트 마운트” [171]를 참조하십시오.

레이블이 있는 영역에서 파일 공유 및 마운트

레이블이 있는 영역에서는 영역의 레이블에 있는 다른 시스템과 파일을 공유할 수 있습니다. 따라서 레이블이 있는 영역의 파일 시스템은 다른 Trusted Extensions 시스템에서 동일한 레이블에 있는 영역 및 영역과 동일한 레이블이 지정된 신뢰할 수 없는 시스템과 공유할 수 있습니다. 이러한 마운트를 중개하는 ZFS 등록 정보에 대한 자세한 내용은 “mlslabel 등록 정보 및 단일 레벨 파일 시스템 마운트” [170]를 참조하십시오.

레이블이 있는 영역의 전역 영역에서 LOFS 마운트는 단일 레벨 데이터 세트의 경우 읽기 전용입니다. 다중 레벨 데이터 세트의 경우 “MAC 읽기/쓰기 정책에 대한 권한 대체 없음” [167]에서 설명한 대로 MAC 정책이 파일 및 디렉토리 레이블별로 적용됩니다.

mlslabel 등록 정보 및 단일 레벨 파일 시스템 마운트

ZFS는 데이터 세트의 데이터 레이블을 포함하는 보안 레이블 등록 정보 mlslabel을 제공합니다. mlslabel 등록 정보는 상속 가능합니다. ZFS 데이터 세트에 명시적인 레이블이 있을 경우 Trusted Extensions로 구성되지 않은 Oracle Solaris 시스템에 데이터 세트를 마운트할 수 없습니다.

mlslabel 등록 정보가 정의되지 않은 경우 기본값은 레이블 없음을 나타내는 문자열 none입니다.

레이블이 있는 영역에서 ZFS 데이터 세트를 마운트할 경우 다음이 발생합니다.

- 데이터 세트에 레이블이 없는 경우, 즉, mlslabel 등록 정보가 정의되지 않은 경우 mlslabel 등록 정보의 값은 마운트 영역의 레이블로 바뀝니다.

  전역 영역의 경우 mlslabel 등록 정보가 자동으로 설정되지 않습니다. 데이터 세트 admin_low에 명시적으로 레이블을 지정할 경우 데이터 세트를 읽기 전용으로 마운트해야 합니다.
- 데이터 세트에 레이블이 있을 경우 커널은 데이터 세트 레이블이 마운트 영역의 레이블과 일치하는지 확인합니다. 레이블이 일치하지 않을 경우 영역에서 하위 읽기 마운트를 허용하지 않는다면 마운트가 실패합니다. 영역에서 하위 읽기 마운트를 허용하는 경우 하위 레벨 파일 시스템이 읽기 전용으로 마운트됩니다.

명령줄에서 mlslabel 등록 정보를 설정하려면 다음과 비슷한 구문을 사용합니다.

```
# zfs set mlslabel=public export/publicinfo
```

초기 레이블을 설정하거나 기본값 이외의 레이블을 상위 레벨 레이블로 변경하려면 file_upgrade_sl 권한이 필요합니다. 레이블을 제거하려면(즉, 레이블을 none으로 설정하려면) file_downgrade_sl 권한이 필요합니다. 기본값 이외의 레이블을 하위 레벨의 레이블로 변경하려는 경우에도 이 권한이 필요합니다.

파일의 레이블 다시 지정을 위한 다중 레벨 데이터 세트

다중 레벨 ZFS 데이터 세트는 여러 레이블에서 파일과 디렉토리를 포함할 수 있습니다. 각 파일과 디렉토리의 레이블을 개별적으로 지정하며 파일을 이동 또는 복사하지 않고도 레이블을 변경할 수 있습니다. 데이터 세트의 레이블 범위 내에서 파일의 레이블을 다시 지정할 수 있습니다. 다중 데이터 세트를 만들고 공유하려면 다중 레벨 데이터 세트를 만들고 공유하는 방법 [66]을 참조하십시오.

일반적으로 데이터 세트의 모든 파일 및 디렉토리는 데이터 세트가 마운트되는 영역과 동일한 레이블을 갖습니다. 이 레이블은 데이터 세트가 처음 영역으로 마운트될 때 mlslabel이라는 ZFS 등록 정보에 자동으로 기록됩니다. 이러한 데이터 세트는 단일 레벨 레이블 지정 데이터 시트입니다. 데이터 세트가 마운트된 동안에는 mlslabel 등록 정보를 변경할 수 없습니다. 즉, 마운트 영역에서는 mlslabel 등록 정보를 변경할 수 없습니다.

mlslabel 등록 정보를 설정한 후에는 영역의 레이블이 데이터 세트의 mlslabel 등록 정보와 일치하지 않으면 데이터 세트를 영역에 읽기/쓰기로 마운트할 수 없습니다. 또한 데이터 세트가 현재 전역 영역을 비롯한 다른 영역에 ZFS로 마운트된 경우 데이터 세트를 어떠한 영역에도 ZFS로 마운트할 수 없습니다. 단일 레벨 레이블 지정 데이터 세트의 파일 레이블은 고정되어 있으므로 setlabel 명령으로 파일의 레이블을 다시 지정하면 실제로 파일이 대상 레이블에 해당하는 기본 영역의 동일한 경로 이름으로 이동됩니다. 이러한 영역 간 이동은 비효율적이고 혼동될 수 있습니다. 다중 레벨 데이터 세트는 데이터의 레이블을 다시 지정하기 위한 효율적인 컨테이너를 제공합니다.

전역 영역에 마운트된 다중 레벨 데이터 세트의 경우 mlslabel 등록 정보의 기본값은 ADMIN_HIGH입니다. 이 값은 데이터 세트 레이블 범위의 상한을 지정합니다. 하위 레이블을 지정하는 경우 mlslabel 등록 정보에 의해 레이블이 지배되는 영역에서만 데이터 세트에 쓸 수 있습니다.

Object Label Management 권한 프로파일이 있는 사용자 또는 역할은 DAC 액세스 권한이 있는 파일이나 디렉토리를 업그레이드 또는 다운그레이드할 수 있는 적합한 권한이 있습니다. 절차는 사용자가 데이터의 보안 레벨을 변경할 수 있게 하는 방법 [138]을 참조하십시오.

사용자 프로세스에는 추가 정책 제약 조건이 적용됩니다.

- 기본적으로 레이블이 있는 영역의 프로세스에서는 파일이나 디렉토리의 레이블을 다시 지정할 수 없습니다. 다시 레이블 지정을 사용으로 설정하려면 레이블이 있는 영역에서 파일의 레이블을 재지정할 수 있게 설정하는 방법 [162]을 참조하십시오. 파일의 다운그레이드는 허용하지만 업그레이드는 허용하지 않는 등의 더 세분화된 제어를 지정하려면 예 13-5. “internal 영역에서 다운그레이드만 허용”를 참조하십시오.
- 디렉토리는 비어 있지 않은 경우 레이블을 다시 지정할 수 없습니다.
- 파일 및 디렉토리를 이들이 포함된 디렉토리의 레이블 아래로 다운그레이드할 수 없습니다.

  레이블을 다시 지정하려면 먼저 파일을 하위 레벨 디렉토리로 이동한 다음 레이블을 다시 지정합니다.
- 데이터 세트를 마운트하는 영역에서는 파일이나 디렉토리를 영역 레이블 위로 업그레이드할 수 없습니다.
- 영역의 프로세스에서 파일이 현재 열려 있는 경우 파일의 레이블을 다시 지정할 수 없습니다.
- 파일과 디렉토리를 데이터 세트의 mlslabel 값 위로 업그레이드할 수 없습니다.

다른 시스템에서 다중 레벨 데이터 세트 마운트

전역 영역에서는 Trusted Extensions 시스템 및 레이블 없는 시스템과 NFS를 통해 다중 레벨 데이터 세트를 공유할 수 있습니다. 데이터 세트는 전역 영역과 레이블 있는 영역 및 레이블 없는 영역의 지정된 레이블에 마운트될 수 있습니다. ADMIN_LOW 레이블 없는 시스템은 예외입니다. 이 시스템은 다중 레벨 데이터 세트를 마운트할 수 없습니다.

다중 레벨 데이터 세트가 ADMIN_HIGH보다 낮은 레이블에서 생성된 경우, 데이터 세트를 다른 Trusted Extensions 시스템의 전역 영역에 마운트할 수 있습니다. 하지만 파일은 전역 영역

에서만 볼 수 있으며, 수정할 수 없습니다. 레이블이 있는 영역에서 다른 시스템 전역 영역의 다중 레벨 데이터 세트를 NFS 마운트하는 경우 몇 가지 제한 사항이 적용됩니다.

- NFS 마운트된 다중 레벨 데이터 세트에는 몇 가지 제한 사항이 적용됩니다.
- Trusted Extensions NFS 클라이언트는 쓰기 가능한 파일에 대해서만 올바른 레이블을 볼 수 있습니다. `getlabel` 명령은 하위 레벨 파일의 레이블을 클라이언트의 레이블인 것으로 잘못 보고합니다. MAC 정책이 적용되므로 파일이 읽기 전용으로 유지되고 상위 레벨 파일이 표시되지 않습니다.
- NFS 서버는 클라이언트에 있을 수 있는 모든 권한을 무시합니다.

이러한 제한 사항 때문에 자체의 전역 영역에서 제공되는 레이블 있는 영역 클라이언트에는 LOFS를 사용하는 것이 좋습니다. NFS는 이러한 클라이언트에 대해 작동하기는 하지만 위의 제한 사항이 적용됩니다. LOFS 마운트 절차는 다중 레벨 데이터 세트를 만들고 공유하는 방법 [66]을 참조하십시오.

Trusted Extensions에서 NFS 서버 및 클라이언트 구성

하위 레벨 디렉토리는 상위 레벨 영역의 사용자에게 표시될 수 있습니다. 하위 레벨 디렉토리에 대한 NFS 서버는 Trusted Extensions 시스템 또는 신뢰할 수 없는 시스템일 수 있습니다.

신뢰할 수 있는 시스템에는 서버 구성이 필요하고 신뢰할 수 없는 시스템에는 클라이언트 구성이 필요합니다.

- **신뢰할 수 있는 시스템에서 NFS 서버 구성** - 신뢰할 수 있는 시스템의 하위 레벨 디렉토리를 레이블 있는 영역에서 표시하려면 서버를 구성해야 합니다.
  - NFS 서버의 전역 영역에서 NFS 서비스를 다중 레벨 서비스로 구성해야 합니다.
  - 전역 영역에서 사용자는 레이블이 있는 영역의 `limitpriv` 권한 세트에 `net_bindmlp` 권한을 추가해야 합니다.
  - 레이블 있는 영역에서 해당하는 공유 등록 정보를 설정하여 ZFS 파일을 내보냅니다. 레이블이 있는 영역의 상태가 `running`이면 파일 시스템이 영역의 레이블에서 공유됩니다. 절차는 레이블이 있는 영역에서 파일 시스템을 공유하는 방법 [176]을 참조하십시오.
- **신뢰할 수 없는 NFS 서버에 대한 NFS 클라이언트 구성** - 서버를 신뢰할 수 없으므로 NFS 클라이언트를 신뢰할 수 있어야 합니다. `net_mac_aware` 권한이 초기 영역 구성 중 사용된 영역 구성 파일에 지정되어야 합니다. 따라서 모든 하위 레벨 홈 디렉토리를 볼 수 있는 사용자에게는 최하위 영역을 제외한 모든 영역에서 `net_mac_aware` 권한이 있어야 합니다. 예는 레이블이 있는 영역에서 파일을 NFS 마운트하는 방법 [178]을 참조하십시오.

Trusted Extensions에서 홈 디렉토리 만들기

홈 디렉토리는 Trusted Extensions에서 특수한 경우입니다.

- 사용자가 사용할 수 있는 모든 영역에서 홈 디렉토리가 만들어졌는지 확인해야 합니다.
- 또한 홈 디렉토리 마운트 지점이 사용자 시스템의 영역에서 만들어져야 합니다.
- NFS 마운트된 홈 디렉토리가 제대로 작동하려면 디렉토리에 대한 기본 위치인 `/export/home`이 사용되어야 합니다.

참고 - `txzonemgr` 스크립트에서는 홈 디렉토리가 `/export/home`으로 마운트되었다고 간주합니다.

- Trusted Extensions에서는 모든 영역 즉, 모든 레이블의 홈 디렉토리를 처리할 수 있도록 자동 마운트가 수정되었습니다. 자세한 내용은 "Trusted Extensions의 자동 마운트 변경 사항" [173]을 참조하십시오.

사용자가 만들어질 때 홈 디렉토리가 만들어집니다. 하지만 홈 디렉토리는 홈 디렉토리 서버의 전역 영역에 만들어집니다. 해당 서버에서 디렉토리는 LOFS로 마운트됩니다. 홈 디렉토리는 LOFS 마운트로 지정된 경우 자동 마운트에서 자동으로 만들어집니다.

참고 - 사용자를 삭제할 경우 전역 영역에 있는 사용자의 홈 디렉토리만 삭제됩니다. 레이블이 있는 영역에 있는 사용자의 홈 디렉토리는 삭제되지 않습니다. 레이블이 있는 영역의 홈 디렉토리 아카이브 및 삭제는 사용자가 결정해야 합니다. 절차는 Trusted Extensions 시스템에서 사용자 계정을 삭제하는 방법 [139]을 참조하십시오.

그러나 자동 마운트는 원격 NFS 서버에 홈 디렉토리를 자동으로 만들 수 없습니다. 사용자가 먼저 NFS 서버에 로그인해야 하거나 관리자 작업이 필요합니다. 사용자에 대한 홈 디렉토리를 만들려면 사용자가 각 NFS 서버에 로그인하여 모든 레이블에서 원격 홈 디렉토리에 액세스할 수 있도록 설정하는 방법 [61]을 참조하십시오.

Trusted Extensions의 자동 마운트 변경 사항

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

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

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

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

```
+auto_home_public
```

```
*    public-zone-IP-address:/export/home/&
```

txzonemgr 스크립트가 전역 영역의 auto_master 파일에서 이 PUBLIC 항목을 설정합니다.

```
+auto_master
/net  -hosts  -nosuid,nobrowse
/home  auto_home -nobrowse
/zone/public/home      auto_home_public      -nobrowse
```

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

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

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

Trusted Extensions 소프트웨어 및 NFS 프로토콜 버전

Trusted Extensions 소프트웨어는 NFSv3(NFS 버전 3) 및 NFSv4의 레이블을 인식합니다. 다음 마운트 옵션 세트 중 하나를 사용할 수 있습니다.

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

Trusted Extensions에는 tcp 프로토콜을 통한 마운트 제한 사항이 없습니다. NFSv3 및 NFSv4에서는 동일 레이블(same-label) 마운트와 하위 읽기(read-down) 마운트에 tcp 프로토콜을 사용할 수 있습니다.

NFSv3의 경우, Trusted Extensions는 Oracle Solaris와 같이 동작합니다. udp 프로토콜은 NFSv3의 기본값이지만, udp는 초기 마운트 작업에만 사용됩니다. 이후 NFS 작업에는 시스템에서 tcp를 사용합니다. 따라서 하위 읽기 마운트는 기본 구성의 NFSv3에 대해 작동합니다.

드물지만 초기 및 이후 NFS 작업에 udp 프로토콜을 사용하도록 NFSv3 마운트를 제한한 경우 udp 프로토콜을 사용하는 NFS 작업에 대해 MLP를 만들어야 합니다. 절차는 예 16-22. “udp를 통해 NFSv3에 대한 개인 다중 레벨 포트 구성”를 참조하십시오.

Trusted Extensions 시스템은 단일 레벨 데이터 세트를 레이블 없는 호스트와 공유할 수도 있습니다. 레이블이 없는 호스트로 내보낸 파일 시스템은 해당 레이블이 내보내는 시스템에서 원격 호스트에 지정한 레이블과 같을 경우 쓰기 가능합니다. 레이블이 없는 호스트로 내보낸 파일 시스템은 해당 레이블이 원격 시스템에 지정된 레이블의 지배를 받는 경우에만 읽기 가능합니다.

전역 영역에서 NFSv4 서비스를 실행 중인 클라이언트와 공유하는 다중 레벨 데이터 세트의 경우 MAC정책은 전체 데이터 세트의 레이블에서가 아니라 개별 파일 및 디렉토리 단위로 적용됩니다.

Trusted Solaris 소프트웨어 릴리스를 실행 중인 시스템과의 통신은 단일 레이블에서만 가능합니다. Trusted Solaris 시스템에 지정된 레이블에 따라 단일 레벨 및 다중 레벨 데이터 세트에 대한 액세스 권한이 결정됩니다.

사용되는 NFS 프로토콜은 로컬 파일 시스템의 유형에 독립적입니다. 오히려 프로토콜은 공유 컴퓨터의 운영 체제 유형에 따라 달라집니다. 원격 파일 시스템에 대해 `mount` 명령에 지정되는 파일 시스템 유형은 항상 NFS입니다.

레이블이 있는 파일 백업, 공유 및 마운트

다음 작업 맵에서는 레이블이 있는 파일 시스템에서 데이터를 백업 및 복원하고, 레이블이 있는 파일 시스템을 공유 및 마운트하는 데 사용되는 일반적인 작업을 설명합니다.

표 14-1 레이블이 있는 파일 백업, 공유 및 마운트 작업 맵

작업	설명	수행 방법
파일을 백업합니다.	레이블을 유지한 상태로 데이터를 아카이브합니다.	Trusted Extensions에서 파일을 백업하는 방법 [175]
데이터를 복원합니다.	백업에서 레이블 지정 데이터를 복원합니다.	Trusted Extensions에서 파일을 복원하는 방법 [176]
레이블이 있는 파일 시스템을 공유합니다.	레이블이 있는 파일 시스템을 다른 시스템의 사용자가 액세스할 수 있도록 허용합니다.	레이블이 있는 영역에서 파일 시스템을 공유하는 방법 [176]
레이블이 있는 영역에서 공유된 파일 시스템을 마운트합니다.	파일 시스템의 컨텐츠가 레이블이 있는 영역의 동일한 레이블에서 읽기-쓰기로 마운트되도록 허용합니다. 상위 레벨 영역에서 공유 디렉토리를 마운트하는 경우 디렉토리는 읽기 전용으로 마운트됩니다.	레이블이 있는 영역에서 파일을 NFS 마운트하는 방법 [178]
홈 디렉토리 마운트 지점을 만듭니다.	모든 레이블의 모든 사용자를 위한 마운트 지점을 만듭니다. 이 작업을 통해 사용자는 NFS 홈 디렉토리 서버가 아닌 시스템의 모든 레이블에서 홈 디렉토리에 액세스할 수 있습니다.	사용자가 각 NFS 서버에 로그인하여 모든 레이블에서 원격 홈 디렉토리에 액세스할 수 있도록 설정하는 방법 [61]
상위 레이블에서 작업하는 사용자에게서 하위 레벨 정보를 숨깁니다.	상위 레벨에서 하위 레벨 정보를 볼 수 없도록 합니다.	하위 레벨 파일의 마운트를 사용 안함으로 설정하는 방법 [159]
파일 시스템 마운트 문제를 해결합니다.	파일 시스템 마운트 문제를 해결합니다.	Trusted Extensions에서 마운트 실패 문제를 해결하는 방법 [179]

▼ Trusted Extensions에서 파일을 백업하는 방법

시작하기 전에 Media Backup 권한 프로파일이 지정되어야 합니다. 사용자가 전역 영역에 있습니다.

- **다음 명령 중 하나를 사용해서 레이블을 보존하는 백업을 수행합니다.**
  - 주 백업의 경우 `zfs send -r | -R` *filesystem*`@snap`

    백업을 원격 서버로 전송하는 것을 비롯해 사용 가능한 방법은 "Oracle Solaris 11.2의 ZFS 파일 시스템 관리 "의 "ZFS 데이터 전송 및 수신"을 참조하십시오.
  - 소규모 백업의 경우 `/usr/sbin/tar cT`

    `tar` 명령의 `T` 옵션에 대한 자세한 내용은 `tar`(1) 매뉴얼 페이지를 참조하십시오.
  - `zfs` 또는 `tar` 백업 명령을 호출하는 스크립트

▼ Trusted Extensions에서 파일을 복원하는 방법

시작하기 전에 전역 영역에서 `root` 역할을 가진 사용자입니다.

- **다음 명령 중 하나를 사용해서 레이블이 있는 백업을 복원합니다.**
  - 주 복원의 경우 `zfs receive -vF` *filesystem*`@snap`

    원격 서버에서 백업을 복원하는 것을 비롯해 사용 가능한 방법은 "Oracle Solaris 11.2의 ZFS 파일 시스템 관리 "의 "ZFS 데이터 전송 및 수신"을 참조하십시오.
  - 소규모 복원의 경우 `/usr/sbin/tar xT`

    `tar` 명령의 `T` 옵션에 대한 자세한 내용은 `tar`(1) 매뉴얼 페이지를 참조하십시오.
  - `zfs` 또는 `tar` 복원 명령을 호출하는 스크립트

▼ 레이블이 있는 영역에서 파일 시스템을 공유하는 방법

레이블이 있는 영역의 디렉토리를 마운트하거나 공유하려면 파일 시스템에서 적합한 ZFS 공유 등록 정보를 설정합니다. 그런 후 영역을 다시 시작해서 레이블이 있는 디렉토리를 공유합니다.

주의 - 공유 파일 시스템에 대해 독점적 이름을 사용하지 마십시오. 공유 파일 시스템의 이름은 모든 사용자에게 표시됩니다.

시작하기 전에 ZFS File System Management 권한 프로파일이 지정되어 있어야 합니다.

1. **공유할 파일 시스템의 레이블에서 작업 공간을 만듭니다.**

   자세한 내용은 "Trusted Extensions 사용자 설명서 "의 "최소 레이블에서 작업 공간 추가 방법"을 참조하십시오.

2. **영역에서 파일 시스템을 만듭니다.**

```
# zfs create rpool/wdocs1
```

3. **ZFS 공유 등록 정보를 설정하여 파일 시스템을 공유합니다.**

   예를 들어, 다음 명령 세트는 쓰기 사용자를 위해 문서 파일 시스템을 공유합니다. 파일 시스템이 읽기-쓰기로 공유되어 쓰기 사용자가 이 서버에서 문서를 수정할 수 있습니다. `setuid` 프로그램은 허용되지 않습니다.

   ```
   # zfs set share=name=wdocs1,path=/wdocs1,prot=nfs,setuid=off,
   exec=off,devices=off rpool/wdocs1
   # zfs set sharenfs=on rpool/wdocs1
   ```

   명령줄은 표시 목적으로 줄바꿈되었습니다.

4. **각 영역에 대해 영역을 시작하여 디렉토리를 공유합니다.**

   전역 영역에서 각 영역에 대해 다음 명령 중 하나를 실행합니다. 각 영역은 이러한 방식으로 파일 시스템을 공유할 수 있습니다. 실제 공유는 각 영역이 `ready` 또는 `running` 상태가 될 때 이루어집니다.

   - **영역이 running 상태가 아니고 사용자가 영역의 레이블에서 서버에 로그인하지 못하게 하려는 경우 영역 상태를 `ready`로 설정합니다.**

     ```
     # zoneadm -z zone-name ready
     ```

   - **영역이 running 상태가 아니고 사용자가 영역의 레이블에서 서버에 로그인할 수 있는 경우 영역을 부팅합니다.**

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

   - **영역이 이미 실행 중인 경우 영역을 재부팅합니다.**

     ```
     # zoneadm -z zone-name reboot
     ```

5. **시스템에서 공유된 파일 시스템을 표시합니다.**

   전역 영역에서 `root` 역할로 다음 명령을 실행합니다.

   ```
   # zfs get all rpool
   ```

   자세한 내용은 "Oracle Solaris 11.2의 ZFS 파일 시스템 관리 "의 "ZFS 파일 시스템 정보 질의"를 참조하십시오.

6. **클라이언트가 공유된 파일 시스템을 마운트할 수 있도록 하려면 레이블이 있는 영역에서 파일을 NFS 마운트하는 방법 [178]을 참조하십시오.**

예 14-1 `PUBLIC` 레이블에서 `/export/share` 파일 시스템 공유

`PUBLIC` 레이블에서 실행되는 응용 프로그램의 경우 시스템 관리자는 사용자가 `public` 영역의 `/export/reference` 파일 시스템에 있는 문서를 읽도록 할 수 있습니다.

먼저, 관리자는 작업 공간 레이블을 public 작업 공간으로 변경하고 터미널 창을 엽니다. 창에서 관리자는 /reference 파일 시스템에서 선택한 share 등록 정보를 설정합니다. 다음 명령은 표시 목적으로 줄바꿈되었습니다.

```
# zfs set share=name=reference,path=/reference,prot=nfs,
setuid=off,exec=off,devices=off,rdonly=on rpool/wdocs1
```

그런 다음 관리자는 파일 시스템을 공유합니다.

```
# zfs set sharenfs=on rpool/reference
```

관리자는 public 작업 공간에서 나와 Trusted Path(신뢰할 수 있는 경로) 작업 공간으로 돌아갑니다. 사용자는 이 파일 서버에 로그인할 수 없으므로 관리자가 영역을 ready 상태로 설정하여 파일 시스템을 공유합니다.

```
# zoneadm -z public ready
```

사용자의 시스템에 마운트되면 사용자가 공유된 파일 시스템에 액세스할 수 있습니다.

▼ 레이블이 있는 영역에서 파일을 NFS 마운트하는 방법

Trusted Extensions에서 레이블이 있는 영역은 해당 영역의 파일 마운트를 관리합니다. 레이블이 없는 호스트 및 레이블이 있는 호스트의 파일 시스템은 Trusted Extensions 레이블이 있는 시스템에 마운트할 수 있습니다. 시스템에는 마운트 영역의 레이블에서 파일 서버에 대한 경로가 있어야 합니다.

- 단일 레이블 호스트에서 파일을 읽기-쓰기로 마운트하려면 원격 호스트의 지정된 레이블이 마운트 영역의 레이블과 일치해야 합니다. 두 가지 원격 호스트 구성이 가능합니다.
  - 신뢰할 수 없는 원격 호스트가 마운트 영역과 동일한 레이블로 지정됩니다.
  - 신뢰할 수 있는 원격 호스트가 마운트 영역의 레이블을 포함하는 다중 레벨 서버입니다.
- 상위 레벨 영역에서 마운트된 파일 시스템은 읽기 전용입니다.
- Trusted Extensions에서 auto_home 구성 파일은 영역별로 사용자 정의됩니다. 파일은 영역 이름을 따라 지정됩니다. 예를 들어, 전역 영역과 공용 영역이 있는 시스템에는 두 개의 auto_home 파일인 auto_home_global과 auto_home_public이 있습니다.

Trusted Extensions에서는 Oracle Solaris와 동일한 마운트 인터페이스를 사용합니다.

- 기본적으로 파일 시스템은 부트 시 마운트됩니다.
- 동적으로 파일 시스템을 마운트하려면 레이블이 있는 영역의 mount 명령을 사용합니다.
- 홈 디렉토리를 자동 마운트하려면 auto_home_*zone-name* 파일을 사용합니다.
- 다른 디렉토리를 자동 마운트하려면 표준 자동 마운트 맵을 사용합니다.

시작하기 전에 마운트하려는 파일의 레이블 영역에서 클라이언트 시스템에 있어야 합니다. 마운트하려는 파일 시스템이 공유되었는지 확인합니다. 자동 마운트를 사용하지 않는 경우 File System

Management 권한 프로파일이 지정되어 있어야 합니다. 하위 레벨 서버에서 마운트하려면 이 클라이언트의 영역이 `net_mac_aware` 권한으로 구성되어야 합니다.

- **레이블이 있는 영역에서 파일을 NFS 마운트하려면 다음 절차를 따릅니다.**

  대부분의 절차에는 특정 레이블에서 작업 공간 만들기가 포함됩니다. 작업 공간을 만들려면 "Trusted Extensions 사용자 설명서 "의 "최소 레이블에서 작업 공간 추가 방법"을 참조하십시오.

  - **파일을 동적으로 마운트합니다.**

    레이블이 있는 영역에서 `mount` 명령을 사용합니다.

  - **영역이 부트될 때 파일을 마운트합니다.**

  - **파일로 관리되는 시스템에 대한 홈 디렉토리를 마운트합니다.**

    a. **`/export/home/auto_home_`*lowest-labeled-zone-name* 파일을 만들고 채웁니다.**

    b. **새로 채워진 파일을 가리키도록 `/etc/auto_home_`*lowest-labeled-zone-name* 파일을 편집합니다.**

    c. **단계 a**에서 만든 파일을 가리키도록 모든 상위 영역의 **`/etc/auto_home_`**lowest-labeled-zone-name1.3.a단계 **파일을 수정합니다.**

▼ Trusted Extensions에서 마운트 실패 문제를 해결하는 방법

시작하기 전에 마운트하려는 파일 시스템의 레이블 영역에 있어야 합니다. `root` 역할을 가진 사용자여야 합니다.

1. **NFS 서버의 파일 시스템이 공유되었는지 확인합니다.**

2. **NFS 서버의 보안 속성을 확인합니다.**

   a. **`tninfo` 또는 `tncfg` 명령을 사용하여 서버의 IP 주소 또는 NFS 서버가 포함된 IP 주소의 범위를 찾습니다.**

   주소는 직접 지정되거나 와일드카드 방식을 통해 간접적으로 지정될 수 있습니다. 주소는 레이블이 있는 템플리트 또는 레이블이 없는 템플리트에 있을 수 있습니다.

   b. **템플리트가 NFS 서버에 지정하는 레이블을 확인합니다.**

   레이블은 파일을 마운트하려는 레이블과 일관성이 있어야 합니다.

3. **현재 영역의 레이블을 확인합니다.**

   레이블이 마운트된 파일 시스템의 레이블보다 상위인 경우 원격 파일 시스템을 읽기/쓰기 권한으로 내보내더라도 마운트에 쓸 수 없습니다. 마운트의 레이블에서 마운트된 파일 시스템에만 쓸 수 있습니다.

4. **이전 버전의 Trusted Solaris 소프트웨어를 실행하는 NFS 서버에서 파일 시스템을 마운트하려면 다음을 수행합니다.**

   - **Trusted Solaris 1 NFS 서버의 경우 `mount` 명령에 `vers=2` 및 `proto=udp` 옵션을 사용합니다.**
   - **Trusted Solaris 2.5.1 NFS 서버의 경우 `mount` 명령에 `vers=2` 및 `proto=udp` 옵션을 사용합니다.**
   - **Trusted Solaris 8 NFS 서버의 경우 `mount` 명령에 `vers=3` 및 `proto=udp` 옵션을 사용합니다.**

   이러한 서버에서 파일 시스템을 마운트하려면 레이블이 없는 템플리트에 서버가 지정되어야 합니다.

♦ ♦ ♦ 15 장

15 신뢰할 수 있는 네트워킹

이 장에서는 Trusted Extensions의 신뢰할 수 있는 네트워크 개념과 방식에 대해 설명합니다.

신뢰할 수 있는 네트워크 정보

Trusted Extensions는 영역, 호스트 및 네트워크에 보안 속성을 지정합니다. 이러한 속성은 네트워크에 다음과 같은 보안 기능이 적용되도록 합니다.

- 네트워크 통신에서 데이터의 레이블이 적절히 지정됩니다.
- 로컬 네트워크를 통해 데이터를 보내거나 받을 때 그리고 파일 시스템을 마운트할 때 MAC(필수 액세스 제어) 규칙이 적용됩니다.
- 원거리 네트워크로 데이터를 경로 지정할 때 MAC 규칙이 적용됩니다.
- 영역으로 데이터를 경로 지정할 때 MAC 규칙이 적용됩니다.

Trusted Extensions에서 네트워크 패킷은 MAC로 보호됩니다. 레이블은 MAC 결정에 사용됩니다. 민감도 레이블에 따라 데이터의 레이블이 명시적 또는 암시적으로 지정됩니다. 레이블에는 ID 필드, 분류 또는 "레벨" 필드 및 구획 또는 "범주" 필드가 있습니다. 데이터는 승인 검사를 통과해야 합니다. 이 검사에서는 레이블이 올바른 형식이고 받는 호스트의 승인 범위 내에 있는지 확인합니다. 받는 호스트의 승인 범위 내에 있는 올바른 형식의 패킷은 액세스가 승인됩니다.

신뢰할 수 있는 시스템 간에 교환되는 IP 패킷에는 레이블을 지정할 수 있습니다. 패킷의 레이블은 IP 패킷을 분류, 분리 및 경로 지정하는 데 사용됩니다. 경로 지정 결정에서는 데이터의 민감도 레이블을 대상 레이블과 비교합니다.

Trusted Extensions에서는 IPv4 및 IPv6 패킷의 레이블을 지원합니다.

- IPv4 패킷의 경우 Trusted Extensions는 CIPSO(Commercial IP Security Option) 레이블을 지원합니다.
- IPv6 패킷의 경우 Trusted Extensions는 CALIPSO(Common Architecture Label IPv6 Security Option) 레이블을 지원합니다.

  IPv6 CIPSO 네트워크의 시스템과 상호 운영해야 하는 경우 Trusted Extensions에서 IPv6 CIPSO 네트워크를 구성하는 방법 [42]을 참조하십시오.

일반적으로 신뢰할 수 있는 네트워크에서 레이블은 전송 호스트에 의해 생성되고 받는 호스트에 의해 처리됩니다. 또한 신뢰할 수 있는 라우터는 신뢰할 수 있는 네트워크에서 패킷을 전달하는 동안 레이블을 추가하거나 제거할 수 있습니다. 민감도 레이블은 전송하기 전에 CALIPSO 또는 CIPSO 레이블에 매핑됩니다. 이 레이블은 IP 패킷에 포함되므로 IP 패킷은 레이블이 있는 패킷이 됩니다. 일반적으로 패킷을 보낸 사람과 받는 사람은 동일한 레이블에서 작업합니다.

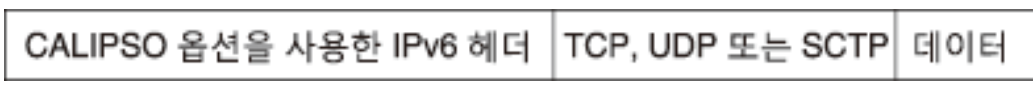
신뢰할 수 있는 네트워킹 소프트웨어는 주체(프로세스)와 객체(데이터)가 서로 다른 호스트에 있는 경우 Trusted Extensions 보안 정책이 적용되도록 합니다. Trusted Extensions 네트워킹은 분산된 응용 프로그램 전체에서 MAC를 유지합니다.

Trusted Extensions 데이터 패킷

Trusted Extensions 데이터 패킷에는 레이블 옵션이 포함됩니다. CIPSO 데이터 패킷은 IPv4 네트워크를 통해 전송됩니다. CALIPSO 패킷은 IPv6 네트워크를 통해 전송됩니다.

표준 IPv4 형식에서는 IPv4 헤더와 옵션, TCP, UDP 또는 SCTP 헤더, 실제 데이터의 순서로 표시됩니다. Trusted Extensions 버전의 IPv4 패킷에서는 보안 속성에 대한 IP 헤더에 CIPSO 옵션을 사용합니다.

표준 IPv6 형식에서는 옵션이 포함된 IPv6 헤더 다음에 TCP, UDP 또는 SCTP 헤더와 실제 데이터가 순서대로 표시됩니다. Trusted Extensions 버전의 IPv6 패킷에서는 보안 속성에 대한 IP 헤더에 CALIPSO 옵션을 사용합니다.



Trusted Extensions 멀티캐스트 패킷

Trusted Extensions는 LAN 내의 멀티캐스트 패킷에 레이블을 추가할 수 있습니다. 이 기능을 사용하면 동일한 레이블 또는 멀티캐스트 패킷의 레이블 범위 내에서 작동되는 CIPSO 또는 CALIPSO 시스템에 레이블이 있는 멀티캐스트 패킷을 전송할 수 있습니다. 이기종 LAN 즉, 레이블이 있는 호스트와 레이블이 없는 호스트가 모두 있는 LAN에서 멀티캐스트는 멀티캐스트 그룹의 구성원을 확인할 수 없습니다.

주의 - 이기종 LAN에서 레이블이 있는 멀티캐스트 패킷을 전송하지 마십시오. 레이블이 있는 정보가 누출될 수 있습니다.

신뢰할 수 있는 네트워크 통신

Trusted Extensions는 신뢰할 수 있는 네트워크에서 레이블이 있는 호스트와 레이블이 없는 호스트를 지원합니다. `txzonemgr` GUI 및 `tncfg` 명령이 네트워크를 구성하는 데 사용됩니다.

Trusted Extensions 소프트웨어를 실행하는 시스템은 Trusted Extensions 시스템과 다음 유형의 호스트 간 네트워크 통신을 지원합니다.

- Trusted Extensions를 실행 중인 다른 호스트
- 보안 속성을 인식하지 않지만 TCP/IP를 지원하는 운영 체제를 실행 중인 호스트(예: Oracle Solaris 시스템), 기타 UNIX 시스템, Microsoft Windows 및 Macintosh OS 시스템
- IPv4 패킷의 CIPSO 레이블 및 IPv6 패킷의 CALIPSO 레이블을 인식하는 다른 신뢰할 수 있는 운영 체제를 실행 중인 호스트

Oracle Solaris OS에서와 마찬가지로 이름 지정 서비스를 통해 Trusted Extensions 네트워크 통신과 서비스를 관리할 수 있습니다. Trusted Extensions는 Oracle Solaris 네트워크 인터페이스에 다음과 같은 인터페이스를 추가합니다.

- Trusted Extensions는 신뢰할 수 있는 네트워크 관리를 위한 명령을 추가하고 GUI를 제공합니다. 또한 Trusted Extensions는 Oracle Solaris 네트워크 명령에 대한 옵션을 추가합니다. 이러한 명령에 대한 자세한 내용은 “Trusted Extensions의 네트워크 명령” [184]을 참조하십시오.

  인터페이스는 `tnzonecfg`, `tnrhdb` 및 `tnrhtp`의 세 Trusted Extensions 네트워크 구성 데이터베이스를 관리합니다. 자세한 내용은 “Trusted Extensions의 네트워크 구성 데이터베이스” [185]를 참조하십시오.
- Trusted Extensions는 `tnrhtp` 및 `tnrhdb` 데이터베이스를 이름 지정 서비스 스위치 SMF 서비스의 등록 정보 `svc:/system/name-service/switch`에 추가합니다.
- Trusted Extensions의 초기 구성 [15]에서는 네트워크를 구성할 때 영역 및 호스트를 정의하는 방법을 설명합니다. 추가 절차는 16장. Trusted Extensions에서 네트워크 관리를 참조하십시오.

- Trusted Extensions는 IKE 구성 파일 /etc/inet/ike/config를 확장합니다. 자세한 내용은 "레이블이 있는 IPsec 관리" [195] 및 ike.config(4) 매뉴얼 페이지를 참조하십시오.

Trusted Extensions의 네트워크 명령

Trusted Extensions는 신뢰할 수 있는 네트워킹을 관리하는 다음 명령을 추가합니다.

- tncfg - 이 명령은 Trusted Extensions 네트워크의 구성을 만들고 수정하며 표시합니다. tncfg -t 명령은 지정된 보안 템플리트를 보거나 만들거나 수정하는 데 사용됩니다. tncfg -z 명령은 지정된 영역의 네트워크 등록 정보를 보거나 수정하는 데 사용됩니다. 자세한 내용은 tncfg(1M) 매뉴얼 페이지를 참조하십시오.
- tnchkdb - 이 명령은 신뢰할 수 있는 네트워크 데이터베이스의 정확성을 확인하는 데 사용됩니다. tnchkdb 명령은 txzonemgr 또는 tncfg 명령을 사용하여 보안 템플리트(tnrhtp), 보안 템플리트 지정(tnrhdb) 또는 영역 구성(tnzonecfg)을 변경할 때마다 호출됩니다. 자세한 내용은 tnchkdb(1M) 매뉴얼 페이지를 참조하십시오.
- tnctl - 이 명령을 사용하여 커널에서 신뢰할 수 있는 네트워크 정보를 업데이트할 수 있습니다. tnctl은 시스템 서비스이기도 합니다. svcadm restart /network/tnctl 명령으로 다시 시작하면 로컬 시스템의 신뢰할 수 있는 네트워크 데이터베이스에서 커널 캐시를 새로 고쳐집니다. 자세한 내용은 tnctl(1M) 매뉴얼 페이지를 참조하십시오.
- tnd - 이 데몬은 LDAP 디렉토리 및 로컬 파일에서 tnrhdb 및 tnrhtp 정보를 끌어옵니다. 검색 순서는 name-service/switch SMF 서비스가 결정합니다. 부팅하는 동안 svc:/network/tnd 서비스에 의해 tnd 데몬이 시작됩니다. 이 서비스는 svc:/network/ldap/client에 종속됩니다.

  LDAP 네트워크에서 tnd 명령은 폴링 간격을 변경하거나 디버깅하는 데도 사용될 수 있습니다. 자세한 내용은 tnd(1M) 매뉴얼 페이지를 참조하십시오.
- tninfo - 이 명령은 신뢰할 수 있는 네트워크 커널 캐시의 현재 상태에 대한 세부 정보를 표시합니다. 호스트 이름, 영역 또는 보안 템플리트별로 출력을 필터링할 수 있습니다. 자세한 내용은 tninfo(1M) 매뉴얼 페이지를 참조하십시오.

Trusted Extensions는 다음 Oracle Solaris 네트워크 명령에 옵션을 추가합니다.

- ipadm - all-zones 주소 등록 정보는 지정된 인터페이스를 시스템의 모든 영역에서 사용할 수 있도록 합니다. 데이터에 연결된 레이블에 따라 데이터를 전달할 적절한 영역이 결정됩니다. 자세한 내용은 ipadm(1M) 매뉴얼 페이지를 참조하십시오.
- netstat - -R 옵션은 Oracle Solaris netstat 사용을 확장하여 경로 지정 테이블 항목 및 다중 레벨 소켓에 대한 보안 속성 등의 Trusted Extensions 관련 정보를 표시합니다. 확장된 보안 속성에는 소켓이 한 영역에 특정한지 아니면 여러 영역에서 사용 가능한지와 피어의 레이블이 포함됩니다. 자세한 내용은 netstat(1M) 매뉴얼 페이지를 참조하십시오.
- route - -secattr 옵션은 Oracle Solaris route 사용을 확장하여 경로의 보안 속성을 표시합니다. 옵션 값의 형식은 다음과 같습니다.

`min_sl=`*label*`,max_sl=`*label*`,doi=`*integer*`,cipso`

`cipso` 키워드는 선택 사항이며 기본적으로 설정됩니다. 자세한 내용은 `route`(1M) 매뉴얼 페이지를 참조하십시오.

- `snoop` - Oracle Solaris에서와 마찬가지로 이 명령에 대한 -v 옵션을 사용하여 IP 헤더를 자세히 표시할 수 있습니다. Trusted Extensions에서는 헤더에 레이블 정보가 포함됩니다.
- `ipseckey` - Trusted Extensions에서 IPsec로 보호된 패킷에 레이블을 지정하는 데 `label` *label*, `outer-label` *label* 및 `implicit-label` *label* 확장을 사용할 수 있습니다. 자세한 내용은 `ipseckey`(1M) 매뉴얼 페이지를 참조하십시오.

Trusted Extensions의 네트워크 구성 데이터베이스

Trusted Extensions는 네트워크 구성 데이터베이스를 커널로 로드합니다. 이러한 데이터베이스는 호스트 간에 데이터를 전송할 때 승인 검사에 사용됩니다.

- `tnzonecfg` - 이 로컬 데이터베이스는 보안과 관련된 영역 속성을 저장합니다. `tncfg` 명령은 이 데이터베이스에 액세스하고 수정하기 위한 인터페이스입니다.

  각 영역에 대한 속성은 영역 레이블과 단일 레벨 및 다중 레벨 호스트에 대한 영역의 액세스 권한을 지정합니다. 다른 속성은 `ping`과 같은 제어 메시지에 대한 응답을 처리합니다. 영역에 대한 레이블은 `label_encodings` 파일에 정의되어 있습니다. 자세한 내용은 `label_encodings`(4) 매뉴얼 페이지를 참조하십시오. 다중 레벨 포트에 대한 자세한 내용은 "영역 및 다중 레벨 포트" [152]를 참조하십시오.
- `tnrhtp` - 이 데이터베이스는 호스트 및 게이트웨이의 보안 속성을 설명하는 템플리트를 저장합니다. `tncfg` 명령은 이 데이터베이스에 액세스하고 수정하기 위한 인터페이스입니다.

  호스트와 게이트웨이는 트래픽을 전송할 때 대상 호스트와 다음 홉 게이트웨이의 속성을 사용하여 MAC를 적용합니다. 트래픽을 받을 때는 보낸 사람의 속성을 사용합니다. 그러나 적응형 호스트가 발신자인 경우 수신 네트워크 인터페이스는 수신 패킷에 기본 레이블을 지정합니다. 보안 속성에 대한 자세한 내용은 "Trusted Extensions의 네트워크 보안 속성" [186]을 참조하십시오.
- `tnrhdb` - 이 데이터베이스는 이 시스템과 통신할 수 있는 모든 호스트에 해당하는 IP 주소 및 IP 주소 범위를 포함합니다. `tncfg` 명령은 이 데이터베이스에 액세스하고 수정하기 위한 인터페이스입니다.

  각 호스트 또는 IP 주소에는 `tnrhtp` 데이터베이스의 보안 템플리트가 지정됩니다. 템플리트의 속성은 지정된 호스트의 속성을 정의합니다.

신뢰할 수 있는 네트워크 보안 속성

Trusted Extensions에서 네트워크 관리는 보안 템플리트를 기반으로 합니다. 보안 템플리트는 동일한 프로토콜과 보안 속성을 가지는 호스트 세트를 설명합니다.

보안 속성은 템플리트를 통해 원격 시스템인 호스트 및 라우터 모두에 관리용으로 지정됩니다. 보안 관리자는 템플리트를 관리하고 원격 시스템에 지정합니다. 원격 시스템에 템플리트가 지정되지 않으면 해당 시스템과 통신이 허용되지 않습니다.

템플리트마다 이름이 있으며 다음을 포함합니다.

- 네 가지 호스트 유형(`unlabeled`, `cipso`, `adaptive` 또는 `netif`) 중 하나. 네트워크 통신에 사용되는 프로토콜은 템플리트의 호스트 유형에 의해 결정됩니다. 자세한 내용은 "보안 템플리트의 호스트 유형 및 템플리트 이름" [187]을 참조하십시오.
- 각 호스트 유형에 적용되는 보안 속성 세트.

자세한 내용은 "Trusted Extensions의 네트워크 보안 속성" [186]을 참조하십시오.

Trusted Extensions의 네트워크 보안 속성

Trusted Extensions 시스템에는 원격 호스트의 레이블 등록 정보를 정의하는 데 사용되는 기본 보안 템플리트 세트가 설치됩니다. Trusted Extensions에서는 보안 템플리트를 통해 네트워크의 레이블이 없는 호스트와 레이블이 있는 호스트 모두에 보안 속성이 지정됩니다. 보안 템플리트가 지정되지 않은 호스트는 Trusted Extensions로 구성된 호스트와 통신할 수 없습니다. 템플리트는 로컬에 저장됩니다.

호스트는 IP 주소나 IP 주소 범위로 보안 템플리트에 추가할 수 있습니다. 자세한 내용은 "신뢰할 수 있는 네트워크 폴백 방식" [189]을 참조하십시오.

호스트 유형마다 추가 필수 및 선택적 보안 속성이 있습니다. 보안 템플리트에서 지정되는 보안 속성은 다음과 같습니다.

- **호스트 유형** - CALIPSO 또는 CIPSO 보안 레이블을 사용하여 패킷의 레이블을 지정할지 레이블을 아예 지정하지 않을지를 정의합니다.
- **기본 레이블** - 레이블이 없는 호스트의 신뢰 레벨을 정의합니다. 레이블이 없는 호스트에서 보내는 패킷은 받는 Trusted Extensions 시스템 또는 게이트웨이가 이 레이블에서 읽습니다.

  기본 레이블 속성은 호스트 유형 `unlabeled`에만 한정됩니다. 자세한 내용은 "보안 템플리트의 기본 레이블" [188]을 참조하십시오.
- **DOI** - DOI를 식별하는 0이 아닌 양의 정수입니다. DOI는 네트워크 통신 또는 네트워크 엔티티에 적용되는 레이블 인코딩 세트를 나타내는 데 사용됩니다. 다른 항목이 동일하더라도 DOI가 다른 레이블은 서로 분리됩니다. `unlabeled` 호스트의 경우 DOI가 기본 레이블에 적용됩니다. Trusted Extensions에서 기본값은 `1`입니다.
- **최소 레이블** - 레이블 승인 범위의 하한을 정의합니다. 호스트 및 다음 홉 게이트웨이가 템플리트에 지정된 최소 레이블보다 낮은 패킷을 받지 않습니다.
- **최대 레이블** - 레이블 승인 범위의 상한을 정의합니다. 호스트 및 다음 홉 게이트웨이가 템플리트에 지정된 최대 레이블보다 높은 패킷을 받지 않습니다.
- **보조 레이블 세트** - 선택 사항입니다. 보안 템플리트에 대해 별개의 보안 레이블 세트를 지정합니다. 최대 레이블과 최소 레이블에 의해 결정되는 승인 범위 이외에 보조 레이블 세트와 함께 템플리트에 추가되는 호스트는 레이블 세트의 레이블 중 하나와 일치하는 패킷을 보내고 받을 수 있습니다. 지정할 수 있는 최대 보조 레이블 수는 4개입니다.

보안 템플리트의 호스트 유형 및 템플리트 이름

Trusted Extensions는 신뢰할 수 있는 네트워크 데이터베이스에서 네 가지 호스트 유형을 지원하고 네 개의 기본 템플리트를 제공합니다.

- `cipso` **호스트 유형** - 레이블이 있는 신뢰할 수 있는 운영 체제를 실행하는 호스트용입니다. 이 호스트 유형은 CALIPSO 및 CIPSO 레이블을 지원합니다.

  IPv6의 경우 CALIPSO 프로토콜을 사용하여 IP 옵션 필드로 전달되는 보안 레이블을 지정합니다. IPv4의 경우 CIPSO 프로토콜을 사용합니다. CALIPSO 및 CIPSO 헤더의 레이블은 데이터의 레이블에서 자동으로 파생됩니다. 그런 다음 파생된 레이블은 IP 레벨에서 보안 검사를 수행하고 네트워크 패킷의 레이블을 지정하는 데 사용됩니다.
- `unlabeled` **호스트 유형** - 표준 네트워킹 프로토콜을 사용하지만 레이블이 있는 옵션을 지원하지 않는 호스트용입니다. Trusted Extensions는 이 호스트 유형에 대해 `admin_low` 템플리트를 제공합니다.

  이 호스트 유형은 Oracle Solaris OS 또는 레이블이 없는 다른 운영 체제를 실행하는 호스트에 지정됩니다. 이 호스트 유형은 레이블이 없는 호스트와의 통신에 적용할 기본 레이블을 제공합니다. 또한 패킷을 레이블이 없는 게이트웨이로 보내서 전달할 수 있도록 레이블 범위나 개별 레이블 세트를 지정할 수 있습니다.
- `adaptive` **호스트 유형** - 레이블은 없지만 레이블이 있는 시스템의 특정 네트워크 인터페이스에 패킷을 전송하는 호스트의 서브넷용입니다. 레이블이 있는 시스템에서는 네트워크 인터페이스 기본 레이블을 수신 패킷에 적용됩니다.

  이 호스트 유형은 Oracle Solaris OS 또는 다른 레이블이 없는 운영 체제를 실행하고 레이블이 있는 시스템에 데이터를 전송해야 하는 호스트에 지정됩니다. 이 호스트 유형은 기본 레이블을 제공하지 않습니다. 통신 레이블은 수신 시스템의 레이블이 있는 네트워크 인터페이스에서 파생됩니다. 이 호스트 유형은 게이트웨이가 아니라 끝 노드 시스템에 지정됩니다.

  `adaptive` 호스트 유형은 신뢰할 수 있는 네트워크 계획 및 크기 조정을 위한 융통성을 제공합니다. 관리자는 새 시스템의 기본 레이블을 미리 알지 않고도 새 레이블이 없는 시스템으로 네트워크를 확장할 수 있습니다. `adaptive` 호스트가 `netif` 호스트에서 레이블이 있는 네트워크 인터페이스로 패킷을 전송하도록 구성된 경우 해당 `netif` 호스트에서 인터페이스의 기본 레이블은 수신 패킷에 적절한 레이블을 지정합니다.
- `netif` **호스트 유형** - `adaptive` 호스트에서 특정 네트워크 인터페이스의 패킷을 수신하는 인터페이스를 호스트 이름용입니다. 이 호스트 유형은 Trusted Extensions 시스템의 인터페이스에 지정됩니다. `netif` 인터페이스의 기본 레이블은 도착하는 패킷에 적용됩니다.

주의 - `admin_low` 템플리트는 사이트별 레이블로 레이블이 없는 템플리트를 구성하는 예를 제공합니다. `admin_low` 템플리트는 Trusted Extensions를 설치하는 데 필요하지만 보안 속성은 일반 시스템 작업에 너무 광범위할 수 있습니다. 시스템 유지 보수 및 지원을 위해 제공된 템플리트를 수정하지 않고 그대로 유지하십시오.

보안 템플리트의 기본 레이블

`unlabeled` 및 `netif` 호스트 유형에 대한 템플리트는 기본 레이블을 지정합니다. 이 레이블은 운영 체제에서 레이블을 인식하지 못하는 호스트(예: Oracle Solaris 시스템)와의 통신을 제어하는 데 사용됩니다. 지정되는 기본 레이블은 호스트와 해당 사용자에 적합한 신뢰 레벨을 반영합니다.

레이블이 없는 호스트와의 통신은 기본 레이블로 제한되기 때문에 이러한 호스트를 단일 레이블 호스트라고도 합니다. 이러한 호스트를 "단일 레이블"이라고 하는 기술적인 이유는 이러한 호스트에 `admin_high` 및 `admin_low` 레이블이 없기 때문입니다.

보안 템플리트의 DOI

동일한 DOI(Domain of Interpretation)를 사용하는 조직 간에는 레이블 정보와 기타 보안 속성을 동일한 방법으로 해석한다는 동의가 있습니다. Trusted Extensions에서 레이블 비교를 수행할 때 DOI가 같은지 여부를 검사합니다.

Trusted Extensions 시스템에서는 하나의 DOI 값에 레이블 정책을 적용합니다. Trusted Extensions 시스템의 모든 영역이 동일한 DOI에서 작동해야 합니다. Trusted Extensions 시스템은 다른 DOI를 사용하는 시스템에서 받은 패킷에 대한 예외 처리를 제공하지 않습니다.

사이트에서 기본값과 다른 DOI 값을 사용하는 경우 DOI(Domain of Interpretation)를 구성하는 방법 [42]에 설명된 대로 모든 보안 템플리트에서 이 값을 사용해야 합니다.

보안 템플리트의 레이블 범위

최소 레이블 및 최대 레이블 속성은 레이블이 있는 호스트와 레이블이 없는 호스트에 대한 레이블 범위를 설정하는 데 사용됩니다. 이러한 속성을 사용하여 다음을 수행할 수 있습니다.

- 호스트가 원격 레이블이 있는 호스트와 통신할 때 사용할 수 있는 레이블 범위 설정

  패킷을 대상 호스트로 보내려면 패킷의 레이블이 대상 호스트의 보안 템플리트에 지정된 레이블 범위에 속해야 합니다.
- 레이블이 있는 게이트웨이 또는 레이블이 없는 게이트웨이를 통해 전달되는 패킷에 대한 레이블 범위 설정

  레이블이 없는 호스트 유형에 대한 템플리트에 레이블 범위를 지정할 수 있습니다. 레이블 범위를 사용하면 호스트에서 호스트 레이블에 없어도 되지만 지정된 레이블 범위 내에 있는 패킷을 전달할 수 있습니다.

보안 템플리트의 보조 레이블

보조 레이블 세트는 원격 호스트에서 패킷을 수락, 전달 또는 전송할 수 있는 4개 이하의 개별 레이블을 정의합니다. 이 속성은 선택 사항입니다. 기본적으로 보조 레이블 세트는 정의되어 있지 않습니다.

신뢰할 수 있는 네트워크 폴백 방식

호스트 IP 주소는 보안 템플리트에 직접 또는 간접적으로 추가할 수 있습니다. 직접 지정은 호스트의 IP 주소를 추가합니다. 간접 지정은 호스트가 포함된 IP 주소 범위를 추가합니다. 특정 호스트와 일치시키기 위해 신뢰할 수 있는 네트워크 소프트웨어는 먼저 특정 IP 주소를 찾습니다. 검색에서 호스트에 대한 특정 항목을 찾을 수 없는 경우 "일치하는 비트의 가장 긴 접두어"를 찾습니다. 호스트의 IP 주소가 고정 접두어 길이를 가진 IP 주소의 "일치하는 비트의 가장 긴 접두어" 내에 속하면 호스트를 보안 템플리트에 간접적으로 지정할 수 있습니다.

IPv4에서는 서브넷에서 간접 지정을 수행할 수 있습니다. 4, 3, 2 또는 1 후행 제로(0) 옥테트를 사용하여 간접 지정을 수행하면 소프트웨어에서 접두어 길이를 각각 0, 8, 16 또는 24로 계산합니다. 예는 표 15-1. “Trusted Extensions 호스트 주소 및 폴백 방식 항목”을 참조하십시오.

슬래시(/)와 고정 비트 수를 추가하여 고정 접두어 길이를 설정할 수도 있습니다. IPv4 네트워크 주소의 가능한 접두어 길이는 1 - 32입니다. IPv6 네트워크 주소의 가능한 접두어 길이는 1 - 128입니다.

다음 표에는 폴백 주소와 호스트 주소의 예가 나와 있습니다. 폴백 주소 세트 내의 한 주소가 간접적으로 지정되는 경우 해당 주소에 폴백 방식이 사용되지 않습니다.

표 15-1 Trusted Extensions 호스트 주소 및 폴백 방식 항목

IP 버전	host_type=cipso에 대한 호스트 항목	포함되는 IP 주소
IPv4	192.168.118.57 192.168.118.57/32	192.168.118.57 /32는 접두어 길이를 32 고정 비트로 설정합니다.
	192.168.118.128/26	192.168.118.0 - 192.168.118.63
	192.168.118.0 192.168.118.0/24	192.168.118. 서브넷의 모든 주소.
	192.168.0.0/24	192.168.0. 서브넷의 모든 주소.
	192.168.0.0 192.168.0.0/16	192.168. 서브넷의 모든 주소.
	192.0.0.0 192.0.0.0/8	192. 서브넷의 모든 주소.
	192.168.118.0/32	호스트 주소 192.168.118.0. 주소 범위가 아닙니다.

IP 버전	host_type=cipso에 대한 호스트 항목	포함되는 IP 주소
	192.168.0.0/32	호스트 주소 192.168.0.0. 주소 범위가 아닙니다.
	192.0.0.0/32	호스트 주소 192.0.0.0. 주소 범위가 아닙니다.
	0.0.0.0/32	호스트 주소 0.0.0.0. 주소 범위가 아닙니다.
	0.0.0.0	모든 네트워크의 모든 주소
IPv6	2001\:DB8\:22\:5000\:\:21f7	2001:DB8:22:5000::21f7
	2001\:DB8\:22\:5000\:\:0/52	2001:DB8:22:5000::0 ~ 2001:DB8:22:5fff:ffff:ffff:ffff:ffff
	0\:\:0/0	모든 네트워크의 모든 주소

0.0.0.0/32 주소는 특정 주소 0.0.0.0과 일치합니다. 0.0.0.0/32 항목을 시스템의 레이블이 없는 보안 템플리트에 추가하면 특정 주소 0.0.0.0의 호스트가 시스템에 연결할 수 있게 됩니다. 예를 들어, DHCP 클라이언트는 서버가 클라이언트에 IP 주소를 제공하기 전에 DHCP 서버에 0.0.0.0으로 연결합니다.

DHCP 클라이언트를 서비스하는 Sun Ray 서버에 tnrhdb 항목을 만들려면 예 16-19. “레이블이 있는 Sun Ray 서버에 대한 유효한 초기 주소 구성”를 참조하십시오. DHCP 클라이언트를 서비스하는 응용 프로그램에 대한 tnrhdb 항목을 만들려면 예 16-18. “호스트 주소 0.0.0.0/32를 유효한 초기 주소로 만들기”를 참조하십시오. 0.0.0.0:admin_low 네트워크는 admin_low 레이블이 없는 호스트 템플리트의 기본 항목입니다. 이 기본값을 변경해야 할 수 있는 보안 문제는 신뢰할 수 있는 네트워크에서 연결할 수 있는 호스트를 제한하는 방법 [212]을 검토하십시오.

IPv4 및 IPv6 주소에서 접두어 길이에 대한 자세한 내용은 “Oracle Solaris 11.2의 네트워크 배치 계획 ”의 “네트워크에 대한 IP 주소 지정 형식 결정”을 참조하십시오.

Trusted Extensions의 경로 지정 정보

Trusted Extensions에서는 서로 다른 네트워크에 있는 호스트 간의 경로 지정 시 각 전송 단계에서 보안이 유지되어야 합니다. Trusted Extensions는 Oracle Solaris OS의 경로 지정 프로토콜에 확장된 보안 속성을 추가합니다. Oracle Solaris와 달리 Trusted Extensions는 동적 경로 지정을 지원하지 않습니다. 정적 경로 지정에 대한 자세한 내용은 route(1M) 매뉴얼 페이지의 -p 옵션을 참조하십시오.

게이트웨이와 라우터는 패킷을 경로 지정합니다. 이 항목에서는 용어 "게이트웨이"와 "라우터"가 같은 의미로 사용됩니다.

동일한 서브넷에 있는 호스트 간 통신에서는 라우터가 사용되지 않으므로 끝점에서만 승인 검사가 수행됩니다. 레이블 범위 검사는 소스에서 수행됩니다. 받는 호스트에서 Trusted Extensions 소프트웨어를 실행 중인 경우 대상에서도 레이블 범위 검사가 수행됩니다.

소스 호스트와 대상 호스트가 서로 다른 서브넷에 있는 경우 패킷은 소스 호스트에서 게이트웨이로 전송됩니다. 대상과 첫번째 홉 게이트웨이의 레이블 범위는 경로 선택 시 소스에서 검

사됩니다. 게이트웨이는 대상 호스트가 연결되는 네트워크에 패킷을 전달합니다. 패킷은 대상에 도달하기 전에 여러 게이트웨이를 통과할 수 있습니다.

참고 - `adaptive` 호스트에서 패킷을 전달해야 하는 레이블이 있는 게이트웨이는 `netif` 호스트 유형 템플리트를 사용하여 인바운드 인터페이스를 구성해야 합니다. `adaptive` 및 `netif` 호스트 유형에 대한 정의는 "보안 템플리트의 호스트 유형 및 템플리트 이름" [187]을 참조하십시오.

경로 지정 배경

Trusted Extensions 게이트웨이에서는 특정한 경우에만 레이블 범위 검사가 수행됩니다. 레이블이 없는 두 호스트 사이에서 패킷을 경로 지정하는 Trusted Extensions 시스템은 소스 호스트의 기본 레이블을 대상 호스트의 기본 레이블과 비교합니다. 레이블이 없는 호스트가 기본 레이블을 공유하는 경우 패킷이 경로 지정됩니다.

각 게이트웨이는 모든 대상에 대한 경로 목록을 유지합니다. 표준 Oracle Solaris 경로 지정은 경로를 최적화하는 선택 사항을 만듭니다. Trusted Extensions는 경로 선택 사항에 적용되는 보안 요구 사항을 검사하는 추가 소프트웨어를 제공합니다. 보안 요구 사항을 충족하지 않는 Oracle Solaris 선택 사항은 건너뜁니다.

Trusted Extensions의 경로 지정 테이블 항목

Trusted Extensions의 경로 지정 테이블 항목은 보안 속성을 통합할 수 있습니다. 보안 속성은 `cipso` 키워드를 포함할 수 있으며 보안 속성은 최대 레이블, 최소 레이블 및 DOI를 포함해야 합니다.

항목에서 보안 속성을 제공하지 않는 경우 게이트웨이의 보안 템플리트에 있는 속성이 사용됩니다.

Trusted Extensions 승인 검사

Trusted Extensions 소프트웨어에서는 보안을 위해 경로의 적합성을 결정합니다. 이 소프트웨어는 소스 호스트, 대상 호스트 및 중간 게이트웨이에서 승인 검사라는 일련의 테스트를 실행합니다.

참고 - 다음 설명에서 레이블 범위에 대한 승인 검사는 보조 레이블 세트에 대한 검사를 의미하기도 합니다.

승인 검사에서는 레이블 범위와 CALIPSO 또는 CIPSO 레이블 정보를 확인합니다. 경로에 대한 보안 속성은 경로 지정 테이블 항목에서 가져오며, 항목에 보안 속성이 없는 경우 게이트웨이의 보안 템플리트에서 가져오기도 합니다.

받는 통신의 경우 Trusted Extensions 소프트웨어에서는 가능하면 패킷 자체에서 레이블을 가져옵니다. 레이블을 지원하는 호스트에서 메시지를 보내는 경우에만 패킷에서 레이블을 가져올 수 있습니다. 패킷에서 레이블을 사용할 수 없는 경우 보안 템플리트의 메시지에 기본 레이블이 지정됩니다. 그러면 승인 검사 중에 이러한 레이블이 사용됩니다. Trusted Extensions는 나가는 메시지, 전달된 메시지 및 받는 메시지에 대해 여러 가지 검사를 수행합니다.

소스 승인 검사

보내는 프로세스 또는 보내는 영역에서 다음과 같은 승인 검사가 수행됩니다.

- 모든 대상에 대해 나가는 패킷의 DOI가 대상 호스트의 DOI와 일치해야 합니다. 또한 DOI가 첫번째 홉 게이트웨이를 포함하여 경로를 따라 모든 홉의 DOI와 일치해야 합니다.
- 모든 대상에 대해 나가는 패킷의 레이블이 경로의 다음 홉 즉, 첫번째 홉의 레이블 범위 내에 있어야 합니다. 또한 레이블이 첫번째 홉 게이트웨이의 보안 속성에 포함되어야 합니다.
- 대상 호스트가 레이블이 없는 호스트인 경우 다음 조건 중 하나를 충족해야 합니다.
  - 보내는 호스트의 레이블이 대상 호스트의 기본 레이블과 일치해야 합니다.
  - 보내는 호스트가 교차 레이블 통신을 수행할 권한이 있고 보낸 사람의 레이블이 대상의 기본 레이블을 지배합니다.
  - 보내는 호스트에 레이블 간 통신을 수행할 권한이 있고 보낸 사람의 레이블이 `ADMIN_LOW`입니다. 즉, 보낸 사람이 전역 영역에서 보내고 있습니다.

참고 - 게이트웨이를 통해 한 네트워크의 호스트에서 다른 네트워크의 호스트로 메시지를 보낼 때 첫번째 홉 검사가 수행됩니다.

게이트웨이 승인 검사

Trusted Extensions 게이트웨이 시스템에서 다음 홉 게이트웨이에 대해 다음과 같은 승인 검사가 수행됩니다.

- 받는 패킷에 레이블이 없는 경우 해당 패킷은 보안 템플리트에서 소스 호스트의 기본 레이블을 상속합니다. 그렇지 않으면 CALIPSO 또는 CIPSO 옵션에 지정된 레이블을 수신합니다.
- 패킷 전달 검사는 다음과 같이 소스 승인과 비슷하게 진행됩니다.
  - 모든 대상에 대해 나가는 패킷의 DOI가 대상 호스트의 DOI와 일치해야 합니다. 또한 DOI가 다음 홉 호스트의 DOI와 일치해야 합니다.

- 모든 대상에 대해 나가는 패킷의 레이블이 다음 홉의 레이블 범위 내에 있어야 합니다. 또한 레이블이 다음 홉 호스트의 보안 속성에 포함되어야 합니다.
- 레이블이 없는 패킷의 레이블이 대상 호스트의 기본 레이블과 일치해야 합니다.
- 레이블이 있는 패킷의 레이블이 대상 호스트의 레이블 범위 내에 있어야 합니다.
- `adaptive` 호스트에서 패킷을 전달해야 하는 레이블이 있는 게이트웨이는 `netif` 호스트 유형 템플리트를 사용하여 인바운드 인터페이스를 구성해야 합니다. `adaptive` 및 `netif` 호스트 유형에 대한 정의는 "보안 템플리트의 호스트 유형 및 템플리트 이름" [187]을 참조하십시오.

대상 승인 검사

Trusted Extensions 시스템에서 데이터를 받으면 소프트웨어에서 다음과 같은 검사를 수행합니다.

- 받는 패킷에 레이블이 없는 경우 해당 패킷은 보안 템플리트에서 소스 호스트의 기본 레이블을 상속합니다. 그렇지 않으면 레이블이 있는 옵션에 지정된 레이블을 수신합니다.
- 패킷의 레이블과 DOI가 대상 영역 또는 대상 프로세스의 레이블 및 DOI와 일치해야 합니다. 프로세스가 다중 레벨 포트에서 수신 대기하는 경우는 예외입니다. 수신 프로세스에 레이블 간 통신을 수행할 권한이 있고, 프로세스가 전역 영역 내에 있거나 프로세스에 패킷의 레이블을 지배하는 레이블이 있는 경우 프로세스에서 패킷을 받을 수 있습니다.

Trusted Extensions에서 경로 지정 관리

Trusted Extensions는 네트워크 간의 통신을 경로 지정하는 다양한 방법을 지원합니다. 해당 사이트의 보안 정책에서 요구하는 보안 정도를 적용하는 경로를 설정할 수 있습니다.

예를 들어, 사이트에서 로컬 네트워크 외부 통신을 단일 레이블로 제한할 수 있습니다. 이 레이블은 공개적으로 사용 가능한 정보에 적용됩니다. `UNCLASSIFIED` 또는 `PUBLIC`과 같은 레이블은 공용 정보를 나타낼 수 있습니다. 제한 사항을 적용하기 위해 이러한 사이트에서는 외부 네트워크에 연결된 게이트웨이의 네트워크 인터페이스를 단일 레이블 템플리트에 추가합니다. TCP/IP 및 경로 지정에 대한 자세한 내용은 다음을 참조하십시오.

- "Oracle Solaris 11.2 네트워크 구성 요소의 구성 및 관리 "의 "Oracle Solaris 네트워크 관리에 대한 추가 정보 위치"
- `netcfg`(1M) 매뉴얼 페이지

Trusted Extensions에서 라우터 선택

Trusted Extensions 호스트는 가장 높은 수준의 신뢰를 라우터로 제공합니다. 다른 유형의 라우터는 Trusted Extensions 보안 속성을 인식할 수 없습니다. 관리 작업 없이 MAC 보안 보호를 제공하지 않는 라우터를 통해 패킷을 경로 지정할 수 있습니다.

- 레이블이 있는 라우터는 IP 옵션 구역에서 올바른 유형의 정보를 찾을 수 없는 패킷을 삭제합니다. 예를 들어 레이블이 있는 라우터는 옵션이 필수 항목일 때 IP 옵션에서 레이블이 있는 옵션을 찾을 수 없거나 IP 옵션의 DOI가 대상의 승인과 일치하지 않는 경우 패킷을 삭제합니다.
- Trusted Extensions 소프트웨어를 실행하지 않는 다른 유형의 라우터는 패킷을 전달하거나 레이블이 있는 옵션을 포함하는 패킷을 삭제하도록 구성할 수 있습니다. Trusted Extensions에서 제공하는 레이블 인식 게이트웨이에서만 CALIPSO 또는 CIPSO IP 옵션의 내용을 사용하여 MAC를 적용할 수 있습니다.

신뢰할 수 있는 경로 지정을 지원하기 위해 Trusted Extensions 보안 속성을 포함하도록 경로 지정 테이블이 확장되었습니다. 속성에 대한 자세한 내용은 "Trusted Extensions의 경로 지정 테이블 항목" [191]을 참조하십시오. Trusted Extensions는 관리자가 경로 지정 테이블 항목을 수동으로 만드는 정적 경로 지정을 지원합니다. 자세한 내용은 `route`(1M) 매뉴얼 페이지의 `-p` 옵션을 참조하십시오.

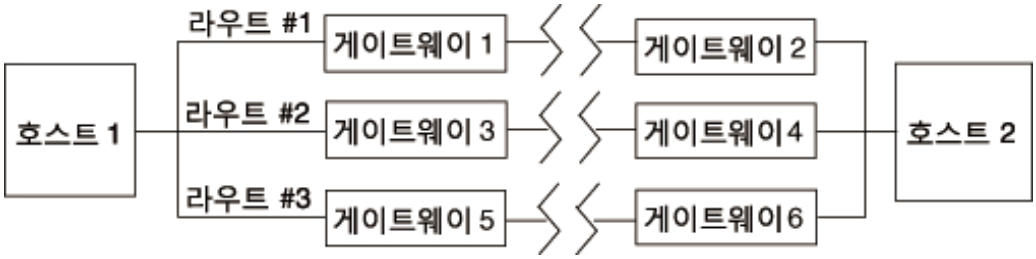
경로 지정 소프트웨어는 경로 지정 테이블에서 대상 호스트로 가는 경로를 찾으려고 합니다. 호스트 이름이 명시적으로 지정되지 않은 경우 경로 지정 소프트웨어는 호스트가 있는 서브넷에 대한 항목을 찾습니다. 호스트와 서브넷이 모두 정의되지 않은 경우 호스트는 기본 게이트웨이(정의된 경우)로 패킷을 보냅니다. 여러 기본 게이트웨이를 정의할 수 있으며 각 기본 게이트웨이는 동일하게 처리됩니다.

이 Trusted Extensions 릴리스에서 보안 관리자는 경로를 수동으로 설정한 다음 조건이 변경될 경우 경로 지정 테이블을 수동으로 변경합니다. 예를 들어, 많은 사이트에서 단일 게이트웨이를 사용하여 외부 세계와 통신합니다. 이 경우 단일 게이트웨이를 네트워크의 각 호스트에 대한 기본값으로 정적으로 정의할 수 있습니다.

Trusted Extensions의 게이트웨이

다음은 Trusted Extensions의 경로 지정 예입니다. 다이어그램과 표는 Host 1과 Host 2 사이의 세 가지 잠재적 경로를 보여줍니다.

그림 15-1 일반적인 Trusted Extensions 경로 및 경로 지정 테이블 항목



경로	첫번째 홉 게이트웨이	최소 레이블	최대 레이블	DOI
#1	게이트웨이 1	CONFIDENTIAL	SECRET	1
#2	게이트웨이 3	ADMIN_LOW	ADMIN_HIGH	1
#3	게이트웨이 5			

- 경로 #1은 CONFIDENTIAL ~ SECRET 레이블 범위 내의 패킷을 전송할 수 있습니다.
- 경로 #2는 ADMIN_LOW ~ ADMIN_HIGH의 패킷을 전송할 수 있습니다.
- 경로 #3은 경로 지정 정보를 지정하지 않습니다. 따라서 해당 보안 속성은 게이트웨이 5의 보안 템플리트에서 파생됩니다.

Trusted Extensions의 경로 지정 명령

소켓에 대한 레이블 및 확장 보안 속성을 표시하기 위해 Trusted Extensions는 다음 Oracle Solaris 네트워크 명령을 수정합니다.

- `netstat -rR` 명령은 경로 지정 테이블 항목의 보안 속성을 표시합니다.
- `netstat -aR` 명령은 소켓에 대한 보안 속성을 표시합니다.
- `add` 또는 `delete` 옵션이 있는 `route -p` 명령은 경로 지정 테이블 항목을 변경합니다.

자세한 내용은 `netstat`(1M) 및 `route`(1M) 매뉴얼 페이지를 참조하십시오.

경로 지정 테이블 항목을 변경할 수 있도록 Trusted Extensions는 다음 인터페이스를 제공합니다.

- `txzonemgr` GUI를 사용하여 인터페이스에 대한 기본 경로를 지정할 수 있습니다.
- `route -p` 명령과 함께 `add` 또는 `delete` 옵션을 사용하여 경로 지정 테이블 항목을 변경할 수 있습니다.

예는 기본 경로를 추가하는 방법 [217]을 참조하십시오.

레이블이 있는 IPsec 관리

Trusted Extensions 시스템은 IPsec로 레이블이 있는 네트워크 패킷을 보호할 수 있습니다. IPsec 패킷은 명시적이나 암시적인 Trusted Extensions 레이블과 함께 사용할 수 있습니다. 레이블은 CALIPSO 또는 CIPSO IP 옵션을 사용하여 명시적으로 전송됩니다. 레이블은 레이블 있는 IPsec SA(보안 연관)를 사용하여 암시적으로 전송됩니다. 또한 서로 다른 암시적 레이블과 함께 IPsec 암호화된 패킷은 레이블이 없는 네트워크를 통해 터널링할 수 있습니다.

일반 IPsec 개념과 구성 절차는 “Oracle Solaris 11.2의 네트워크 보안 ”을 참조하십시오. IPsec 절차에 대해 Trusted Extensions에서 수정된 사항은 “레이블이 있는 IPsec 구성” [220]을 참조하십시오.

IPsec로 보호된 교환에 대한 레이블

IPsec로 보호된 통신을 포함하여 Trusted Extensions 시스템에서의 모든 통신은 보안 레이블 승인 검사를 충족해야 합니다. 검사는 “Trusted Extensions 승인 검사” [191]에 설명되어 있습니다.

이러한 검사를 통과해야 하는 레이블이 있는 영역의 응용 프로그램에서 IPsec 패킷의 레이블은 내부 레이블, 전송 중 레이블 및 키 관리 레이블입니다.

- **응용 프로그램 보안 레이블** - 응용 프로그램이 상주하는 영역의 레이블입니다.
- **내부 레이블** - IPsec AH 또는 ESP 헤더가 적용되기 전에 암호화되지 않은 메시지 데이터의 레이블입니다. 이 레이블은 `SO_MAC_EXEMPT` 소켓 옵션(MAC-exempt) 또는 multilevel port(MLP, 다중 레벨 포트) 기능을 사용 중인 경우 응용 프로그램 보안 레이블과 다를 수 있습니다. 레이블로 제한되는 보안 연결(SA) 및 IKE 규칙을 선택할 경우 IPsec 및 IKE에서 이 내부 레이블을 사용합니다.

  기본적으로 내부 레이블은 응용 프로그램 보안 레이블과 동일합니다. 일반적으로 양 끝의 응용 프로그램은 동일한 레이블을 가집니다. 하지만 MAC-exempt 또는 MLP 통신의 경우 이 조건은 true가 아닐 수 있습니다. IPsec 구성 설정은 내부 레이블이 네트워크에서 전달되는 방식, 즉 전송 중 레이블을 정의할 수 있습니다. IPsec 구성 설정은 내부 레이블의 값을 정의할 수 없습니다.
- **전송 중 레이블** - IPsec AH 또는 ESP 헤더가 적용된 후에 암호화된 메시지 데이터의 레이블입니다. IKE 및 IPsec 구성 파일에 따라 전송 중 레이블은 내부 레이블과 다를 수 있습니다.
- **키 관리 레이블** - 두 노드 간의 모든 IKE 협상은 협상을 트리거하는 응용 프로그램 메시지의 레이블에 상관 없이 단일 레이블에서 제어됩니다. IKE 협상의 레이블은 IKE별 규칙을 기준으로 `/etc/inet/ike/config` 파일에서 정의됩니다.

IPsec 보안 연결에 대한 레이블 확장

IPsec 레이블 확장은 Trusted Extensions 시스템에서 레이블을 보안 연결(SA) 내부에서 전달되는 트래픽과 연결하는 데 사용됩니다. 기본적으로 IPsec 데이터는 레이블 확장을 사용하지 않으므로 레이블을 무시합니다. 두 시스템 간의 모든 트래픽은 Trusted Extensions 레이블에 상관 없이 단일 SA를 통해 이동합니다.

레이블 확장을 통해 다음 작업을 수행할 수 있습니다.

- 각 Trusted Extensions 레이블에서 사용할 여러 IPsec SA를 구성합니다. 이 구성은 두 다중 레벨 시스템 간에 이동하는 트래픽의 레이블을 전달하기 위한 추가 방식을 효과적으로 제공합니다.
- 암호화되지 않은 형식의 텍스트와 다른 IPsec로 암호화된 메시지 텍스트에 대한 전송 중 레이블을 지정합니다. 이 구성은 보안이 약한 네트워크를 통해 암호화된 기밀 데이터의 전송을 지원합니다.

- IP 패킷에서 CALIPSO 또는 CIPSO IP 옵션 사용을 숨깁니다. 이 구성을 사용하면 레이블이 있는 트래픽이 레이블을 인식할 수 없는 네트워크나 레이블 유해 네트워크를 순회할 수 있습니다.

"IKE에 대한 레이블 확장" [197]에 설명된 대로 IKE를 통해 자동으로 또는 `ipseckey` 명령을 통해 수동으로 레이블 확장을 사용하도록 지정할 수 있습니다. 레이블 확장 기능에 대한 자세한 내용은 `ipseckey`(1M) 매뉴얼 페이지를 참조하십시오.

레이블 확장을 사용할 때 아웃바운드 트래픽에 대한 SA 선택 항목에는 일치 항목의 일부로 내부 민감도 레이블이 포함됩니다. 인바운드 트래픽의 보안 수준은 수신된 패킷 SA의 보안 레이블로 정의됩니다.

IKE에 대한 레이블 확장

Trusted Extensions 시스템의 IKE는 레이블을 인식하는 피어와의 SA에 대한 레이블 협상을 지원합니다. `/etc/inet/ike/config` 파일의 다음 키워드를 사용하여 이 방식을 제어할 수 있습니다.

- **label_aware** - `in.iked` 데몬의 Trusted Extensions 레이블 인터페이스 사용 및 피어와의 레이블 협상을 사용으로 설정합니다.
- **single_label** - 피어가 SA에 대한 레이블 협상을 지원하지 않음을 나타냅니다.
- **multi_label** - 피어가 SA에 대한 레이블 협상을 지원함을 나타냅니다. IKE는 IKE가 두 노드 간의 트래픽에서 발견하는 각 추가 레이블에 대해 새로운 SA를 만듭니다.
- **wire_label inner** - `in.iked` 데몬에서 전송 중 레이블이 내부 레이블과 동일한 레이블이 있는 SA를 만들도록 합니다. 데몬이 `cipso` 피어와 협상 중인 경우 키 관리 레이블은 `ADMIN_LOW`입니다. 데몬이 레이블이 없는 피어와 협상 중인 경우 키 관리 레이블은 피어의 기본 레이블입니다. 전송되는 패킷에 레이블이 있는 IP 옵션이 포함된 경우 일반적인 Trusted Extensions 규칙을 따릅니다.
- **wire_label** *label* - `in.iked` 데몬에서 내부 레이블의 값에 상관 없이 전송 중 레이블이 *label*로 설정된 레이블이 있는 SA를 만들도록 합니다. `in.iked` 데몬은 지정된 레벨에서 키 관리 협상을 수행합니다. 전송되는 패킷에 레이블이 있는 IP 옵션이 포함된 경우 일반적인 Trusted Extensions 규칙을 따릅니다.
- **wire_label none** *label* - `wire_label` *label*과 유사한 동작을 유발하지만, 레이블이 있는 IP 옵션이 SA에 따라 전송되는 IKE 패킷 및 데이터 패킷에서 숨겨집니다.

자세한 내용은 `ike.config`(4) 매뉴얼 페이지를 참조하십시오.

터널 모드 IPsec의 레이블 및 승인

응용 프로그램 데이터 패킷이 터널 모드에서 IPsec로 보호되는 경우 패킷에는 여러 IP 헤더가 포함됩니다.

IKE 프로토콜의 IP 헤더에는 응용 프로그램 데이터 패킷의 외부 IP 헤더와 동일한 소스 및 대상 주소 쌍이 포함됩니다.

Trusted Extensions는 내부 레이블 승인 검사를 위해 내부 IP 헤더 주소를 사용합니다. Trusted Extensions는 외부 IP 헤더 주소를 사용하여 전송 중 및 키 관리 레이블 검사를 수행합니다. 승인 검사에 대한 자세한 내용은 “Trusted Extensions 승인 검사” [191]를 참조하십시오.

레이블 확장으로 기밀성 및 무결성 보호

다음 표에서는 레이블 확장의 다양한 구성으로 IPsec 기밀성 및 무결성 보호가 보안 레이블에 어떻게 적용되는지 설명합니다.

보안 연관	기밀성	무결성
레이블 확장 없음	레이블이 레이블이 있는 IP 옵션에 표시됩니다.	레이블이 있는 IP 옵션의 메시지 레이블이 ESP가 아닌 AH로 보호됩니다. 주를 참조하십시오.
레이블 확장 있음	레이블이 있는 IP 옵션이 표시되지만, 내부 메시지 레이블과 다를 수 있는 전송 중 레이블을 나타냅니다.	레이블 무결성이 레이블별 SA의 존재로 암시적으로 보호됩니다. 전송 중 레이블이 있는 IP 옵션이 AH로 보호됩니다. 주를 참조하십시오.
레이블 확장이 있고 레이블이 있는 IP 옵션이 숨겨짐	메시지 레이블이 표시되지 않습니다.	레이블 무결성이 레이블별 SA의 존재로 암시적으로 보호됩니다.

참고 - 메시지가 네트워크를 통해 이동할 때 레이블 인식 라우터가 레이블이 있는 IP 옵션을 제거하거나 추가할 수 있는 경우 IPsec AH 무결성 보호를 사용하여 레이블이 있는 IP 옵션을 보호할 수 없습니다. 레이블이 있는 IP 옵션을 수정하면 메시지가 무효화되고 AH로 보호된 패킷이 대상에서 삭제됩니다.

♦ ♦ ♦ 16 장

16 Trusted Extensions에서 네트워크 관리

이 장에서는 Trusted Extensions 네트워크 보안을 위한 구현 세부 정보와 절차를 제공합니다.

호스트 및 네트워크 레이블 지정

Trusted Extensions 시스템은 다른 호스트의 보안 속성을 정의한 후에만 해당 호스트에 연결할 수 있습니다. 원격 호스트는 유사한 보안 속성을 가질 수 있으므로 Trusted Extensions는 호스트를 추가할 수 있는 보안 템플리트를 제공합니다.

사이트별 보안 템플리트가 필요한지 여부 확인

통신하는 호스트에 대해 다음 작업을 원하는 경우 사이트별 보안 템플리트를 만들 수 있습니다.

- 호스트 또는 호스트 그룹의 레이블 범위를 제한합니다.
- `ADMIN_LOW` 이외의 레이블에서 단일 레이블 호스트를 만듭니다.
- 레이블이 없는 호스트에 대해 `AD MIN_LOW` 이외의 기본 레이블이 필요합니다.
- 제한된 레이블 세트를 인식하는 호스트를 만듭니다.
- `1` 이외의 DOI를 사용합니다.
- 올바른 레이블을 지정하도록 구성된 신뢰할 수 있는 네트워크 인터페이스에 대해 지정된 레이블이 없는 호스트의 정보를 레이블이 없는 호스트의 패킷에 보냅니다.

기존 보안 템플리트 보기

원격 호스트 및 네트워크에 레이블을 지정하기 전에 제공된 보안 템플리트를 검토하고 원격 호스트 및 네트워크에 연결할 수 있는지 확인합니다. 지침은 다음을 참조하십시오.

- 보안 템플리트를 확인합니다. 보안 템플리트를 보는 방법 [200]을 참조하십시오.
- 사이트에 사용자 정의된 보안 템플리트가 필요한지 여부를 확인합니다. "사이트별 보안 템플리트가 필요한지 여부 확인" [199]을 참조하십시오.
- 신뢰할 수 있는 네트워크에 시스템과 네트워크를 추가합니다. 시스템의 알려진 네트워크에 호스트를 추가하는 방법 [201]을 참조하십시오.

▼ 보안 템플리트를 보는 방법

보안 템플리트의 목록 및 각 템플리트의 컨텐츠를 볼 수 있습니다. 이 절차에 표시된 예제에는 기본 보안 템플리트가 사용됩니다.

1. **사용 가능한 보안 템플리트를 나열합니다.**

```
# tncfg list
cipso
admin_low
adapt
netif
```

2. **나열된 템플리트의 컨텐츠를 봅니다.**

```
# tncfg -t cipso info
name=cipso
host_type=cipso
doi=1
min_label=ADMIN_LOW
max_label=ADMIN_HIGH
host=127.0.0.1/32
```

위의 `cipso` 보안 템플리트에 있는 `127.0.0.1/32` 항목은 이 시스템을 레이블이 있는 시스템으로 식별합니다. 피어가 `cipso`의 `host_type`을 사용하여 이 시스템을 피어의 원격 호스트 템플리트에 지정하면 두 시스템은 레이블이 있는 패킷을 교환할 수 있습니다.

```
# tncfg -t admin_low info
name=admin_low
host_type=unlabeled
doi=1
def_label=ADMIN_LOW
min_label=ADMIN_LOW
max_label=ADMIN_HIGH
host=0.0.0.0/0
```

위의 admin_low 보안 템플리트에 있는 0.0.0.0/0 항목은 보안 템플리트에 명시적으로 지정되지 않은 모든 호스트가 이 시스템에 연결할 수 있도록 합니다. 이러한 호스트는 레이블이 없는 호스트로 인식됩니다.

- 0.0.0.0/0 항목의 장점은 이 시스템이 부트 시 필요한 모든 호스트(서버 및 게이트웨이 등)를 찾을 수 있다는 점입니다.
- 0.0.0.0/0 항목의 단점은 이 시스템의 네트워크에 있는 모든 호스트가 이 시스템에 연결할 수 있다는 점입니다. 이 시스템에 연결할 수 있는 호스트를 제한하려면 신뢰할 수 있는 네트워크에서 연결할 수 있는 호스트를 제한하는 방법 [212]을 참조하십시오.

```
# tncfg -t adapt info
name=adapt
host_type=adapt
doi=1
min_label=ADMIN_LOW
max_label=ADMIN_HIGH
host=0.0.0.0/0
```

adapt 템플리트는 adaptive 호스트 즉, 기본 레이블을 가질 수 없는 신뢰할 수 없는 시스템을 식별합니다. 대신 이 시스템의 레이블은 수신하는 신뢰할 수 있는 시스템에서 지정합니다. 이 레이블은 레이블이 있는 시스템의 netif 템플리트에 지정된 패킷을 수신하는 IP 인터페이스의 기본 레이블에서 파생됩니다.

```
# tncfg -t netif info
name=netif
host_type=netif
doi=1
def_label=ADMIN_LOW
min_label=ADMIN_LOW
max_label=ADMIN_HIGH
host=127.0.0.1/32
```

netif 템플리트는 원격 호스트가 아니라 신뢰할 수 있는 로컬 네트워크 인터페이스를 지정합니다. netif 템플리트의 기본 레이블은 IP 주소가 해당 템플리트의 호스트 주소와 일치하는 전용 네트워크 인터페이스가 있는 모든 영역의 레이블과 동일해야 합니다. 또한 일치하는 영역 인터페이스에 해당하는 하위 링크는 동일한 레이블을 공유하는 다른 영역에만 지정할 수 있습니다.

▼ 시스템의 알려진 네트워크에 호스트를 추가하는 방법

호스트 및 호스트 그룹을 시스템의 /etc/hosts 파일에 추가하면 호스트가 시스템에 알려집니다. 알려진 호스트만 보안 템플리트에 추가할 수 있습니다.

시작하기 전에 전역 영역에서 root 역할을 가진 사용자입니다.

1. **개별 호스트를 /etc/hosts 파일에 추가합니다.**

```
# pfedit /etc/hosts
```

```
...
192.168.111.121   ahost
```

2. **호스트 그룹을 `/etc/hosts` 파일에 추가합니다.**

```
# pfedit /etc/hosts

...
192.168.111.0   111-network
```

보안 템플리트 만들기

이 절에는 다음 네트워크 구성에 대한 보안 템플리트를 만드는 것과 관련된 예 또는 포인터가 포함되어 있습니다.

- DOI 값이 1이 아닙니다. DOI(Domain of Interpretation)를 구성하는 방법 [42]을 참조하십시오.
- 신뢰할 수 있는 원격 호스트에 특정 레이블이 지정되었습니다. 예 16-1. “패킷을 하나의 레이블로 처리하는 게이트웨이에 대한 보안 템플리트 만들기”을 참조하십시오.
- 신뢰할 수 없는 원격 호스트에 특정 레이블이 지정되었습니다. 예 16-2. “PUBLIC 레이블에서 레이블이 없는 보안 템플리트 만들기”를 참조하십시오.

특정 요구 사항을 해결하는 보안 템플리트의 다른 예는 “보안 템플리트에 호스트 추가” [204]를 참조하십시오.

▼ 보안 템플리트를 만드는 방법

시작하기 전에 전역 영역에서 네트워크 보안을 수정할 수 있는 역할을 가진 사용자여야 합니다. 예를 들어, Information Security 또는 Network Security 권한 프로파일이 지정된 역할은 보안 값을 수정할 수 있습니다. 보안 관리자 역할에는 이러한 권한 프로파일이 포함됩니다.

참고 - 지원을 위해 기본 보안 템플리트를 변경하거나 삭제하지 마십시오.

- 이러한 템플리트를 복사하여 수정할 수는 있습니다.
- 그리고 이러한 템플리트에 지정된 호스트를 추가하고 제거할 수 있습니다. 예는 신뢰할 수 있는 네트워크에서 연결할 수 있는 호스트를 제한하는 방법 [212]을 참조하십시오.

---

1. **(옵션) `ADMIN_HIGH` 및 `ADMIN_LOW` 이외의 레이블에 대한 16진수 버전을 결정합니다.**

   `CONFIDENTIAL`과 같은 레이블의 경우 레이블 문자열 또는 16진수 값을 레이블 값으로 사용할 수 있습니다. `tncfg` 명령에서는 두 가지 형식을 허용합니다.

```
# atohexlabel "confidential : internal use only"
```

```
0x0004-08-48
```

자세한 내용은 레이블에 해당하는 16진수를 얻는 방법 [117]을 참조하십시오.

2. **보안 템플리트를 만듭니다.**

   `tncfg -t` 명령은 새 템플리트를 만들 수 있는 3가지 방법을 제공합니다.

   - **처음부터 보안 템플리트를 만듭니다.**

     대화식 모드로 `tncfg` 명령을 사용합니다. `info` 하위 명령은 기본적으로 제공되는 값을 표시합니다. Tab 키를 눌러서 부분 등록 정보 및 값을 완성합니다. `exit`를 입력하여 템플리트를 완성합니다.

```
# tncfg -t newunlabeled
tncfg:newunlabeled> info
name=newunlabeled
host_type=unlabeled
doi=1
def_label=ADMIN_LOW
min_label=ADMIN_LOW
max_label=ADMIN_HIGH
tncfg:newunlabeled> set mTab
set max_label=" set min_label="      Auto-complete shows two possible completions
tncfg:newunlabeled> set maTab        User types the letter a
tncfg:newunlabeled> set max_label=ADMIN_LOW
...
tncfg:newunlabeled> commit
tncfg:newunlabeled> exit
```

     명령줄에서 보안 템플리트에 대한 전체 속성 목록을 제공할 수도 있습니다. 세미콜론은 `set` 하위 명령을 구분합니다. 생략된 속성에는 기본값이 사용됩니다. 네트워크 보안 속성에 대한 자세한 내용은 “Trusted Extensions의 네트워크 보안 속성” [186]을 참조하십시오.

```
# tncfg -t newunlabeled set host_type=unlabeled;set doi=1; \
set min_label=ADMIN_LOW;set max_label=ADMIN_LOW
```

   - **기존 보안 템플리트를 복사하여 수정합니다.**

```
# tncfg -t cipso
tncfg:cipso> set name=newcipso
tncfg:newcipso> info
name=newcipso
host_type=cipso
doi=1
min_label=ADMIN_LOW
max_label=ADMIN_HIGH
```

     기존 보안 템플리트에 지정된 호스트는 새 템플리트에 복사되지 않습니다.

   - **`export` 하위 명령이 만드는 템플리트 파일을 사용합니다.**

```
# tncfg -f unlab_1 -f template-file
tncfg: unlab_1> set host_type=unlabeled
...
# tncfg -f template-file
```

가져올 소스 템플리트를 만드는 예는 tncfg(1M) 매뉴얼 페이지를 참조하십시오.

예 16-1 패킷을 하나의 레이블로 처리하는 게이트웨이에 대한 보안 템플리트 만들기

이 예에서 보안 관리자는 PUBLIC 레이블에서만 패킷을 전달할 수 있는 게이트웨이를 정의합니다.

```
# tncfg -t cipso_public
tncfg:cipso_public> set host_type=cipso
tncfg:cipso_public> set doi=1
tncfg:cipso_public> set min_label="public"
tncfg:cipso_public> set max_label="public"
tncfg:cipso_public> commit
tncfg:cipso_public> exit
```

그런 다음 보안 관리자는 게이트웨이 호스트를 보안 템플리트에 추가합니다. 추가는 예 16-4. “패킷을 하나의 레이블로 처리하는 게이트웨이 만들기”를 참조하십시오.

예 16-2 PUBLIC 레이블에서 레이블이 없는 보안 템플리트 만들기

이 예에서는 보안 관리자가 PUBLIC 레이블에서만 패킷을 전송 및 수신할 수 있는 신뢰할 수 없는 호스트에 대한 레이블이 없는 템플리트를 만듭니다. 이 템플리트는 Trusted Extensions 시스템에서 파일 시스템을 PUBLIC 레이블에 마운트해야 하는 호스트에 지정할 수 있습니다.

```
# tncfg -t public
tncfg:public> set host_type=unlabeled
tncfg:public> set doi=1
tncfg:public> set def_label="public"
tncfg:public> set min_sl="public"
tncfg:public> set max_sl="public"
tncfg:public> exit
```

그런 다음 보안 관리자는 호스트를 보안 템플리트에 추가합니다. 추가는 예 16-15. “PUBLIC 레이블에서 레이블이 없는 하위 네트워크 만들기”를 참조하십시오.

보안 템플리트에 호스트 추가

이 절에는 보안 템플리트에 호스트를 추가하는 것에 대한 예 또는 포인터가 포함되어 있습니다. 불연속 IP 주소의 경우 호스트를 보안 템플리트에 추가하는 방법 [205]을 참조하십시

오. 호스트 범위의 경우 호스트 범위를 보안 템플리트에 추가하는 방법 [210]을 참조하십시오.

이 절의 예에서는 다음과 같은 원격 호스트 레이블 지정을 보여 줍니다.

- 신뢰할 수 있는 원격 게이트웨이가 PUBLIC 트래픽을 처리합니다. 예 16-4. “패킷을 하나의 레이블로 처리하는 게이트웨이 만들기”를 참조하십시오.
- 단일 레이블 라우터로 작동하는 신뢰할 수 없는 원격 호스트 - 예 16-5. “레이블이 있는 패킷을 경로 지정하는 레이블이 없는 라우터 만들기”
- 신뢰할 수 있는 원격 호스트가 트래픽을 좁은 레이블 범위 내로 제한합니다. 예 16-6. “제한된 레이블 범위를 사용하여 게이트웨이 만들기”을 참조하십시오.
- 신뢰할 수 있는 원격 호스트에 제한된 레이블 세트가 지정되었습니다. 예 16-7. “고유의 레이블에서 호스트 만들기”을 참조하십시오.
- 신뢰할 수 있는 원격 호스트에 나머지 네트워크와 분리된 레이블이 지정되었습니다. 예 16-8. “개발자에 대한 레이블이 있는 호스트 만들기”을 참조하십시오.
- 신뢰할 수 있는 netif 호스트가 adaptive 시스템의 패킷에 레이블을 지정합니다. 예 16-9. “netif 호스트에 대한 보안 템플리트 만들기”를 참조하십시오.
- 신뢰할 수 없는 adaptive 호스트가 패킷을 netif 호스트로 전송합니다. 예 16-10. “적응형 호스트에 대한 보안 템플리트 만들기”을 참조하십시오.
- 신뢰할 수 있는 동종 네트워크가 특정 레이블에서 멀티캐스트 주소를 추가합니다. 예 16-11. “레이블이 있는 멀티캐스트 메시지 보내기”을 참조하십시오.
- 호스트가 보안 템프리트에서 제거되었습니다. 예 16-12. “보안 템플리트에서 여러 호스트 제거”를 참조하십시오.
- 신뢰할 수 없는 원격 호스트 및 네트워크에 레이블이 지정되었습니다. 예 16-15. “PUBLIC 레이블에서 레이블이 없는 하위 네트워크 만들기”를 참조하십시오.

▼ 호스트를 보안 템플리트에 추가하는 방법

시작하기 전에 다음이 필요합니다.

- IP 주소가 /etc/hosts 파일에 있거나 DNS에서 확인할 수 있어야 합니다.

  hosts 파일은 시스템의 알려진 네트워크에 호스트를 추가하는 방법 [201]을 참조하십시오.

  DNS의 경우 “Oracle Solaris 11.2의 이름 지정 및 디렉토리 서비스 작업: DNS 및 NIS”의 3 장, “DNS(Domain Name System) 관리”를 참조하십시오.
- 레이블 끝점이 일치해야 합니다. 규칙은 “Trusted Extensions의 경로 지정 정보” [190]를 참조하십시오.
- 전역 영역에서 보안 관리자 역할을 가진 사용자여야 합니다.

1. **(옵션) 추가할 호스트 이름 또는 IP 주소에 연결할 수 있는지 확인합니다.**

   이 예에서는 192.168.1.2에 연결할 수 있는지 확인합니다.

```
# arp 192.168.1.2
gateway-2.example.com (192.168.1.2) at 0:0:0:1:ad:cd
```

arp 명령은 호스트가 시스템의 /etc/hosts 파일에 정의되어 있거나 DNS에서 확인할 수 있는지 확인합니다.

2. **호스트 이름 또는 IP 주소를 보안 템플리트에 추가합니다.**
   이 예제에서는 192.168.1.2 IP 주소를 추가합니다.

```
# tncfg -t cipso
tncfg:cipso> add host=192.168.1.2
```

   이전에 다른 템플리트에 추가한 호스트를 추가하는 경우 보안 템플리트 지정을 바꾼다는 메시지가 나타납니다. 정보 메시지는 예 16-3. “호스트의 보안 템플리트 지정 바꾸기”을 참조하십시오.

3. **변경된 보안 템플리트를 봅니다.**
   다음 예제는 192.168.1.2 주소가 cipso 템플리트에 추가되었음을 보여줍니다.

```
tncfg:cipso> info
...
host=192.168.1.2/32
```

   /32의 접두어 길이는 주소가 정확함을 나타냅니다.

4. **변경 작업을 계속하고 보안 템플리트를 종료합니다.**

```
tncfg:cipso> commit
tncfg:cipso> exit
```

   호스트 항목을 제거하려면 예 16-12. “보안 템플리트에서 여러 호스트 제거”를 참조하십시오.

예 16-3 호스트의 보안 템플리트 지정 바꾸기

이 예제는 이미 템플리트 지정이 포함된 호스트에 보안 템플리트를 지정할 때 표시되는 정보 메시지를 보여줍니다.

```
# tncfg -t cipso
tncfg:cipso> add host=192.168.1.2
192.168.1.2 previously matched the admin_low template
tncfg:cipso> info
...
host=192.168.1.2/32
tncfg:cipso> exit
```

예 16-4 패킷을 하나의 레이블로 처리하는 게이트웨이 만들기

예 16-1. “패킷을 하나의 레이블로 처리하는 게이트웨이에 대한 보안 템플리트 만들기”에서 보안 관리자는 PUBLIC 레이블에서만 패킷을 전달할 수 있는 게이트웨이를 정의하는 보안 템플리트를 만듭니다. 이 예에서 보안 관리자는 게이트웨이 호스트의 IP 주소를 확인할 수 있는지 확인합니다.

```
# arp 192.168.131.75
gateway-1.example.com (192.168.131.75) at 0:0:0:1:ab:cd
```

arp 명령은 호스트가 시스템의 /etc/hosts 파일에 정의되어 있거나 DNS에서 확인할 수 있는지 확인합니다.

그런 다음 관리자는 gateway-1 호스트를 보안 템플리트에 추가합니다.

```
# tncfg -t cipso_public
tncfg:cipso_public> add host=192.168.131.75
tncfg:cipso_public> exit
```

시스템은 즉시 gateway-1을 통해 public 패킷을 송수신할 수 있습니다.

예 16-5 레이블이 있는 패킷을 경로 지정하는 레이블이 없는 라우터 만들기

라우터에서 명시적으로 레이블을 지원하지 않더라도 모든 IP 라우터는 CALIPSO 또는 CIPSO 레이블로 메시지를 전달할 수 있습니다. 이러한 레이블이 없는 라우터에는 대개 라우터 관리를 위한 라우터 연결을 처리해야 하는 레벨을 정의하기 위한 기본 레이블이 필요합니다. 이 예에서 보안 관리자는 어느 레이블에서나 트래픽을 전달할 수 있는 라우터를 만들지만, 라우터와의 모든 직접 통신은 기본 레이블인 PUBLIC에서 처리됩니다.

먼저 보안 관리자가 처음부터 템플리트를 만듭니다.

```
# tncfg -t unl_public_router
tncfg:unl_public_router> set host_type=unlabeled
tncfg:unl_public_router> set doi=1
tncfg:unl_public_router> set def_label="PUBLIC"
tncfg:unl_public_router> set min_label=ADMIN_LOW
tncfg:unl_public_router> set max_label=ADMIN_HIGH
tncfg:unl_public_router> exit
```

그런 다음 관리자는 라우터를 보안 템플리트에 추가합니다.

```
# tncfg -t unl_public_router
tncfg:unl_public_router> add host=192.168.131.82
tncfg:unl_public_router> exit
```

시스템이 192.168.131.82 주소의 호스트 이름 router-1을 통해 즉시 모든 레이블에서 패킷을 보내고 받을 수 있습니다.

예 16-6 제한된 레이블 범위를 사용하여 게이트웨이 만들기

이 예에서 보안 관리자는 패킷을 좁은 레이블 범위로 제한하는 템플리트를 만들고 게이트웨이를 이 템플리트에 추가합니다.

```
# arp 192.168.131.78
gateway-ir.example.com (192.168.131.78) at 0:0:0:3:ab:cd

# tncfg -t cipso_iuo_rstrct
tncfg:cipso_iuo_rstrct> set host_type=cipso
tncfg:cipso_iuo_rstrct> set doi=1
```

```
tncfg:cipso_iuo_rstrct> set min_label=0x0004-08-48
tncfg:cipso_iuo_rstrct> set max_label=0x0004-08-78
tncfg:cipso_iuo_rstrct> add host=192.168.131.78
tncfg:cipso_iuo_rstrct> exit
```

시스템은 즉시 gateway-ir을 통해 internal 및 restricted 레이블이 지정된 패킷을 송수신할 수 있습니다.

예 16-7 고유의 레이블에서 호스트 만들기

이 예에서 보안 관리자는 confidential : internal use only 및 confidential : restricted의 두 가지 레이블만 인식하는 보안 템플리트를 만듭니다. 기타 모든 트래픽은 거부됩니다.

먼저 보안 관리자는 각 호스트의 IP 주소를 확인할 수 있는지 확인합니다.

```
# arp 192.168.132.21
host-auxset1.example.com (192.168.132.21) at 0:0:0:4:ab:cd
# arp 192.168.132.22
host-auxset2.example.com (192.168.132.22) at 0:0:0:5:ab:cd
# arp 192.168.132.23
host-auxset3.example.com (192.168.132.23) at 0:0:0:6:ab:cd
# arp 192.168.132.24
host-auxset4.example.com (192.168.132.24) at 0:0:0:7:ab:cd
```

그런 다음 관리자는 레이블을 정확하게 입력해야 합니다. 소프트웨어는 대소문자의 레이블 및 짧은 이름의 레이블을 인식하지만 공백이 부정확한 레이블은 인식하지 못합니다. 예를 들어 cnf :restricted 레이블은 유효한 레이블이 아닙니다.

```
# tncfg -t cipso_int_and_rst
tncfg:cipso_int_and_rst> set host_type=cipso
tncfg:cipso_int_and_rst> set doi=1
tncfg:cipso_int_and_rst> set min_label="cnf : internal use only"
tncfg:cipso_int_and_rst> set max_label="cnf : internal use only"
tncfg:cipso_int_and_rst> set aux_label="cnf : restricted"
tncfg:cipso_int_and_rst> exit
```

그런 다음 관리자는 접두어 길이를 사용하여 IP 주소 범위를 보안 템플리트에 지정합니다.

```
# tncfg -t cipso_int_rstrct
tncfg:cipso_int_rstrct> set host=192.168.132.0/24
```

예 16-8 개발자에 대한 레이블이 있는 호스트 만들기

이 예에서 보안 관리자는 cipso_sandbox 보안 템플리트를 만듭니다. 이 템플리트는 신뢰할 수 있는 소프트웨어의 개발자가 사용하는 시스템에 지정됩니다. SANDBOX 레이블은 네트워크의 다른 레이블과 떨어져 있으므로 개발자 테스트는 다른 레이블이 있는 호스트에 영향을 주지 않습니다.

```
# tncfg -t cipso_sandbox
tncfg:cipso_sandbox> set host_type=cipso
```

```
tncfg:cipso_sandbox> set doi=1
tncfg:cipso_sandbox> set min_sl="SBX"
tncfg:cipso_sandbox> set max_sl="SBX"
tncfg:cipso_sandbox> add host=196.168.129.102
tncfg:cipso_sandbox> add host=196.168.129.129
tncfg:cipso_sandbox> exit
```

196.168.129.102 및 196.168.129.129 시스템을 사용하는 개발자는 SANDBOX 레이블에서 서로 통신할 수 있습니다.

예 16-9 netif 호스트에 대한 보안 템플리트 만들기

이 예에서 보안 관리자는 netif 보안 템플리트를 만듭니다. 이 템플리트는 IP 주소 10.121.10.3을 호스트하는 레이블이 있는 네트워크 인터페이스에 지정됩니다. 이 지정으로 Trusted Extensions IP 모듈은 adaptive 호스트에서 도달하는 모든 수신 패킷에 기본 레이블 PUBLIC을 추가합니다.

```
# tncfg -t netif_public
tncfg:netif_public> set host_type=netif
tncfg:netif_public> set doi=1
tncfg:netif_public> set def_label="PUBLIC"
tncfg:netif_public> add host=10.121.10.3
tncfg:netif_public> commit
tncfg:netif_public> exit
```

예 16-10 적응형 호스트에 대한 보안 템플리트 만들기

이 예에서 보안 관리자는 미리 계획합니다. 관리자는 공개 정보를 보유하는 네트워크와 내부 정보를 보유하는 네트워크에 대해 서로 다른 서브넷을 만듭니다. 그런 다음 관리자는 두 개의 adaptive 호스트를 정의합니다. 공용 서브넷의 시스템에는 PUBLIC 레이블이 지정됩니다. 내부 네트워크의 시스템에는 IUO 레이블이 지정됩니다. 이 네트워크는 미리 계획되므로 각 네트워크는 특정 레이블의 정보를 보유하고 전송합니다. 또 다른 장점은 패킷이 예상된 인터페이스에서 배달되지 않는 경우 네트워크를 쉽게 디버그할 수 있다는 것입니다.

```
# tncfg -t adpub_192_168_10
tncfg:adapt_public> set host_type=adapt
tncfg:adapt_public> set doi=1
tncfg:adapt_public> set min_label="public"
tncfg:adapt_public> set max_label="public"
tncfg:adapt_public> add host=192.168.10.0
tncfg:adapt_public> commit
tncfg:adapt_public> exit

# tncfg -t adiuo_192_168_20
tncfg:adapt_public> set host_type=adapt
tncfg:adapt_public> set doi=1
tncfg:adapt_public> set min_label="iuo"
tncfg:adapt_public> set max_label="iuo"
tncfg:adapt_public> add host=192.168.20.0
tncfg:adapt_public> commit
tncfg:adapt_public> exit
```

예 16-11 레이블이 있는 멀티캐스트 메시지 보내기

이 예제의 레이블이 있는 동종 LAN에서 관리자는 PUBLIC 레이블의 패킷을 보내는 데 사용할 수 있는 멀티캐스트 주소를 선택합니다.

```
# tncfg -t cipso_public
tncfg:cipso_public> add host=224.4.4.4
tncfg:cipso_public> exit
```

예 16-12 보안 템플리트에서 여러 호스트 제거

이 예에서 보안 관리자는 cipso 보안 템플리트에서 여러 호스트를 제거합니다. 관리자는 info 하위 명령을 사용하여 호스트를 표시한 다음 remove를 입력하고 4개의 host= 항목을 복사하여 붙여 넣습니다.

```
# tncfg -t cipso info
name=cipso
host_type=cipso
doi=1
min_label=ADMIN_LOW
max_label=ADMIN_HIGH
host=127.0.0.1/32
host=192.168.1.2/32
host=192.168.113.0/24
host=192.168.113.100/25
host=2001:a08:3903:200::0/56

# tncfg -t cipso
tncfg:cipso> remove host=192.168.1.2/32
tncfg:cipso> remove host=192.168.113.0/24
tncfg:cipso> remove host=192.168.113.100/25
tncfg:cipso> remove host=2001:a08:3903:200::0/56
tncfg:cipso> info
...
max_label=ADMIN_HIGH
host=127.0.0.1/32
host=192.168.75.0/24
```

호스트를 제거한 후 관리자는 변경 사항을 커밋하고 보안 템플리트를 종료합니다.

```
tncfg:cipso> commit
tncfg:cipso> exit
#
```

▼ 호스트 범위를 보안 템플리트에 추가하는 방법

시작하기 전에 요구 사항은 호스트를 보안 템플리트에 추가하는 방법 [205]을 참조하십시오.

1. **보안 템플리트를 서브넷에 지정하려면 서브넷 주소를 템플리트에 추가합니다.**
   이 예제에서는 두 IPv4 서브넷을 cipso 템플리트에 추가한 다음 보안 템플리트를 표시합니다.

```
# tncfg -t cipso
tncfg:cipso> add host=192.168.75.0
tncfg:cipso> add host=192.168.113.0
tncfg:cipso> info
...
host=192.168.75.0/24
host=192.168.113.0/24
tncfg:cipso> exit
```

/24의 접두어 길이는 .0으로 끝나는 주소가 서브넷임을 나타냅니다.

```
# tncfg -t cipso
tncfg:cipso> add host=192.168.113.100/25
192.168.113.100/25 previously matched the admin_low template
```

2. **보안 템플리트를 주소 범위에 지정하려면 IP 주소 및 접두어 길이를 지정합니다.**
   다음 예에서 /25 접두어 길이에는 192.168.113.0에서 192.168.113.127 사이의 연속 IPv4 주소가 포함됩니다. 주소에는 192.168.113.100이 포함됩니다.

```
# tncfg -t cipso
tncfg:cipso> add host=192.168.113.100/25
tncfg:cipso> exit
```

다음 예에서 /56 접두어 길이에는 2001:a08:3903:200::0에서 2001:a08:3903:2ff:ffff:ffff:ffff:ffff 사이의 연속 IPv6 주소가 포함됩니다. 주소에는 2001:a08:3903:201:20e:cff:fe08:58c가 포함됩니다.

```
# tncfg -t cipso
tncfg:cipso> add host=2001:a08:3903:200::0/56
tncfg:cipso> info
...
host=2001:a08:3903:200::0/56
tncfg:cipso> exit
```

이전에 다른 템플리트에 추가한 호스트를 추가하는 경우 보안 템플리트 지정을 바꾼다는 메시지가 나타납니다. 정보 메시지는 예 16-13. “호스트 범위에 대한 보안 템플리트 바꾸기”을 참조하십시오.

잘못 입력된 항목도 예 16-14. “보안 템플리트에서 잘못 입력된 IP 주소 처리”에 표시된 것처럼 정보 메시지를 표시합니다.

예 16-13 호스트 범위에 대한 보안 템플리트 바꾸기

이 예제는 이미 템플리트 지정이 포함된 호스트 범위에 보안 템플리트를 지정할 때 표시되는 정보 메시지를 보여줍니다.

```
# tncfg -t cipso
tncfg:cipso> add host=192.168.113.100/32
192.168.113.100/32 previously matched the admin_low template
tncfg:cipso> info
...
```

```
host=192.168.113.100/32
tncfg:cipso> exit
```

"신뢰할 수 있는 네트워크 폴백 방식" [189]에 설명된 대로 Trusted Extensions 폴백 방식은 이 명시적 지정이 이전 지정을 대체하도록 합니다.

예 16-14 보안 템플리트에서 잘못 입력된 IP 주소 처리

잘못 입력된 항목은 정보 메시지를 표시합니다. 다음 호스트 추가에는 주소에서 `:200`이 누락되어 있습니다.

```
# tncfg -t cipso
tncfg:cipso> add host=2001:a08:3903::0/56
Invalid host: 2001:a08:3903::0/56
```

예 16-15 `PUBLIC` 레이블에서 레이블이 없는 하위 네트워크 만들기

예 16-2. "`PUBLIC` 레이블에서 레이블이 없는 보안 템플리트 만들기"에서 보안 관리자는 신뢰할 수 없는 호스트에 `PUBLIC` 레이블을 지정하는 보안 템플리트를 만듭니다. 이 예에서 보안 관리자는 서브넷을 `PUBLIC` 레이블에 지정합니다. 지정하는 시스템의 사용자는 이 서브넷의 호스트에서 `PUBLIC` 영역으로 파일 시스템을 마운트할 수 있습니다.

```
# tncfg -t public
tncfg:public> add host=10.10.0.0/16
tncfg:public> exit
```

서브넷은 즉시 `PUBLIC` 레이블에서 연결할 수 있습니다.

신뢰할 수 있는 네트워크에 연결할 수 있는 호스트 제한

이 절에서는 네트워크에 연결할 수 있는 호스트를 제한하여 네트워크를 보호합니다.

- 신뢰할 수 있는 네트워크에서 연결할 수 있는 호스트를 제한하는 방법 [212].
- 부트 시 연결할 시스템을 지정하여 보안을 향상시킵니다. 예 16-16. "`0.0.0.0/0` IP 주소의 레이블 변경"을 참조하십시오.
- 원격 클라이언트의 초기 연결을 수락하도록 애플리케이션 서버를 구성합니다. 예 16-18. "호스트 주소 `0.0.0.0/32`를 유효한 초기 주소로 만들기"을 참조하십시오.
- 원격 클라이언트의 초기 연결을 수락하도록 레이블이 있는 Sun Ray를 구성합니다. 예 16-19. "레이블이 있는 Sun Ray 서버에 대한 유효한 초기 주소 구성"를 참조하십시오.

▼ 신뢰할 수 있는 네트워크에서 연결할 수 있는 호스트를 제한하는 방법

다음은 임의의 레이블이 없는 호스트가 레이블이 있는 호스트에 연결하지 못하게 하는 절차입니다. Trusted Extensions가 설치되면 `admin_low` 기본 보안 템플리트가 네트워크의 모든 호스트를 정의합니다. 이 절차를 사용하여 레이블이 없는 특정 호스트를 열거합니다.

각 시스템의 로컬 신뢰할 수 있는 네트워크 값은 부트 시 네트워크에 연결하는 데 사용됩니다. 기본적으로 `cipso` 템플리트가 제공되지 않은 모든 호스트는 `admin_low` 템플리트로 정의됩니다. 이 템플리트는 다르게 정의되지 않은 모든 원격 호스트(`0.0.0.0/0`)을 기본 레이블 `admin_low`의 레이블이 없는 시스템이 되도록 지정합니다.

주의 - 기본 `admin_low` 템플리트는 Trusted Extensions 네트워크에서 보안상 위험할 수 있습니다. 사이트 보안에 강력한 보호가 요구되는 경우 보안 관리자는 시스템이 설치된 후 `0.0.0.0/0` 와일드카드 항목을 제거할 수 있습니다. 항목은 시스템이 부트 시 연결하는 모든 호스트에 대한 항목으로 바뀌어야 합니다.

예를 들어, `0.0.0.0/0` 와일드카드 항목이 제거된 후 DNS 서버, 홈 디렉토리 서버, 감사 서버, 브로드캐스트/멀티캐스트 주소 및 라우터가 템플리트에 명시적으로 추가되어야 합니다.

응용 프로그램이 처음에 호스트 주소 `0.0.0.0/32`의 클라이언트를 인식하는 경우 `admin_low` 템플리트에 `0.0.0.0/32` 호스트 항목을 추가해야 합니다. 예를 들어 잠재적 Sun Ray 클라이언트에서 초기 연결 요청을 받으려면 Sun Ray 서버에 다음 항목을 포함해야 합니다. 그러면 서버에서 클라이언트를 인식할 때 클라이언트에 IP 주소가 제공되고 레이블이 있는 클라이언트로 연결됩니다.

시작하기 전에 전역 영역에서 보안 관리자 역할을 가진 사용자여야 합니다.

부트 시 연결해야 하는 모든 호스트는 `/etc/hosts` 파일에 있어야 합니다.

1. **부트 시 연결해야 하는 모든 레이블이 없는 호스트에 `admin_low` 템플리트를 추가합니다.**

   - 부트 시 연결해야 하는 각 레이블이 없는 호스트를 포함합니다.
   - Trusted Extensions를 실행하지 않는 모든 온-링크 라우터를 포함합니다. 이 라우터를 통해 이 시스템이 통신해야 합니다.
   - `0.0.0.0/0` 지정을 제거합니다.

2. **호스트를 `cipso` 템플리트에 추가합니다.**

   부팅 시 연결해야 하는 각 레이블이 있는 호스트를 추가합니다.

   - Trusted Extensions를 실행하는 모든 온-링크 라우터를 포함합니다. 이 라우터를 통해 이 시스템이 통신해야 합니다.
   - 모든 네트워크 인터페이스가 템플리트에 지정되었는지 확인합니다.
   - 브로드캐스트 주소를 포함합니다.
   - 부트 시 연결해야 하는 레이블이 있는 호스트의 범위를 포함합니다.

   샘플 데이터베이스는 예 16-17. “부트 시 Trusted Extensions 시스템에서 연결할 시스템 열거”를 참조하십시오.

3. **호스트 지정에서 시스템 부팅을 허용하는지 확인합니다.**

예 16-16 `0.0.0.0/0` IP 주소의 레이블 변경

이 예에서 관리자는 공용 게이트웨이 시스템을 만듭니다. 관리자는 `0.0.0.0/0` 호스트 항목을 `admin_low` 템플리트에서 제거하고 `0.0.0.0/0` 호스트 항목을 레이블이 없는 `public` 템플리트에 추가합니다. 그러면 시스템은 다른 보안 템플리트에 명시적으로 지정되지 않은 모든 시스템을 `public` 보안 템플리트의 보안 속성을 가진 레이블이 없는 시스템으로 인식합니다.

```
# tncfg -t admin_low info
tncfg:admin_low> remove host=0.0.0.0      Wildcard address
tncfg:admin_low> exit

# tncfg -t public
tncfg:public> set host_type=unlabeled
tncfg:public> set doi=1
tncfg:public> set def_label="public"
tncfg:public> set min_sl="public"
tncfg:public> set max_sl="public"
tncfg:public> add host=0.0.0.0      Wildcard address
tncfg:public> exit
```

예 16-17 부트 시 Trusted Extensions 시스템에서 연결할 시스템 열거

다음 예에서 관리자는 두 네트워크 인터페이스를 사용하여 Trusted Extensions 시스템의 신뢰할 수 있는 네트워크를 구성합니다. 시스템은 다른 네트워크 및 라우터와 통신합니다. 원격 호스트는 `cipso`, `admin_low` 또는 `public`의 세 템플리트 중 하나에 지정됩니다. 다음 명령은 주석 처리됩니다.

```
# tncfg -t cipso
tncfg:admin_low> add host=127.0.0.1      Loopback address
tncfg:admin_low> add host=192.168.112.111      Interface 1 of this host
tncfg:admin_low> add host=192.168.113.111      Interface 2 of this host
tncfg:admin_low> add host=192.168.113.6      File server
tncfg:admin_low> add host=192.168.112.255      Subnet broadcast address
tncfg:admin_low> add host=192.168.113.255      Subnet broadcast address
tncfg:admin_low> add host=192.168.113.1      Router
tncfg:admin_low> add host=192.168.117.0/24      Another Trusted Extensions network
tncfg:admin_low> exit

# tncfg -t public
tncfg:public> add host=192.168.112.12      Specific network router
tncfg:public> add host=192.168.113.12      Specific network router
tncfg:public> add host=224.0.0.2      Multicast address
tncfg:admin_low> exit

# tncfg -t admin_low
tncfg:admin_low> add host=255.255.255.255      Broadcast address
tncfg:admin_low> exit
```

부트 시 연결할 호스트를 지정한 후 관리자는 `0.0.0.0/0` 항목을 `admin_low` 템플리트에서 제거합니다.

```
# tncfg -t admin_low
```

```
tncfg:admin_low> remove host=0.0.0.0
tncfg:admin_low> exit
```

예 16-18 호스트 주소 0.0.0.0/32를 유효한 초기 주소로 만들기

이 예제에서 보안 관리자는 잠재적인 클라이언트의 초기 연결 요청을 수락하도록 애플리케이션 서버를 구성합니다.

관리자는 서버의 신뢰할 수 있는 네트워크를 구성합니다. 서버 및 클라이언트 항목은 주석 처리됩니다.

```
# tncfg -t cipso info
name=cipso
host_type=cipso
doi=1
min_label=ADMIN_LOW
max_label=ADMIN_HIGH
host=127.0.0.1/32
host=192.168.128.1/32       Application server address
host=192.168.128.0/24       Application's client network
     Other addresses to be contacted at boot time

# tncfg -t admin_low info
name=cipso
host_type=cipso
doi=1
def_label=ADMIN_LOW
min_label=ADMIN_LOW
max_label=ADMIN_HIGH
host=192.168.128.0/24       Application's client network
host=0.0.0.0/0       Wildcard address
     Other addresses to be contacted at boot time
```

이 테스트 단계가 성공한 후 관리자는 기본 와일드카드 주소 0.0.0.0/0을 제거하고 변경 사항을 커밋한 다음 특정 주소를 추가하여 구성을 잠급니다.

```
# tncfg -t admin_low info
tncfg:admin_low> remove host=0.0.0.0
tncfg:admin_low> commit
tncfg:admin_low> add host=0.0.0.0/32      For initial client contact
tncfg:admin_low> exit
```

최종 admin_low 구성은 다음과 유사하게 나타납니다.

```
# tncfg -t admin_low
name=cipso
host_type=cipso
doi=1
def_label=ADMIN_LOW
min_label=ADMIN_LOW
max_label=ADMIN_HIGH
192.168.128.0/24       Application's client network
```

```
host=0.0.0.0/32       For initial client contact
    Other addresses to be contacted at boot time
```

`0.0.0.0/32` 항목은 응용 프로그램의 클라이언트만 응용 프로그램 서버에 연결할 수 있도록 허용합니다.

예 16-19 레이블이 있는 Sun Ray 서버에 대한 유효한 초기 주소 구성

이 예제에서 보안 관리자는 잠재적인 클라이언트의 초기 연결 요청을 수락하도록 Sun Ray 서버를 구성합니다. 서버는 개인 토폴로지와 Sun Ray 서버 기본값을 사용합니다.

```
# utadm -a net0
```

그런 다음 관리자는 서버의 신뢰할 수 있는 네트워크를 구성합니다. 서버 및 클라이언트 항목은 주석 처리됩니다.

```
# tncfg -t cipso info
name=cipso
host_type=cipso
doi=1
min_label=ADMIN_LOW
max_label=ADMIN_HIGH
host=127.0.0.1/32
host=192.168.128.1/32       Sun Ray server address
host=192.168.128.0/24       Sun Ray client network
    Other addresses to be contacted at boot time

# tncfg -t admin_low info
name=cipso
host_type=cipso
doi=1
def_label=ADMIN_LOW
min_label=ADMIN_LOW
max_label=ADMIN_HIGH
host=192.168.128.0/24       Sun Ray client network
host=0.0.0.0/0      Wildcard address
    Other addresses to be contacted at boot time
```

이 테스트 단계가 성공한 후 관리자는 기본 와일드카드 주소 `0.0.0.0/0`을 제거하고 변경 사항을 커밋한 다음 특정 주소를 추가하여 구성을 잠급니다.

```
# tncfg -t admin_low info
tncfg:admin_low> remove host=0.0.0.0
tncfg:admin_low> commit
tncfg:admin_low> add host=0.0.0.0/32      For initial client contact
tncfg:admin_low> exit
```

최종 `admin_low` 구성은 다음과 유사하게 나타납니다.

```
# tncfg -t admin_low
name=cipso
host_type=cipso
doi=1
```

```
def_label=ADMIN_LOW
min_label=ADMIN_LOW
max_label=ADMIN_HIGH
192.168.128.0/24        Sun Ray client network
host=0.0.0.0/32         For initial client contact
      Other addresses to be contacted at boot time
```

`0.0.0.0/32` 항목은 Sun Ray 클라이언트만 서버에 연결할 수 있게 합니다.

경로 및 다중 레벨 포트 구성

정적 경로는 레이블이 있는 패킷이 레이블이 있는 게이트웨이와 레이블이 없는 게이트웨이를 통해 대상에 도달할 수 있도록 합니다. MLP는 응용 프로그램에서 하나의 진입점을 사용하여 모든 영역에 도달할 수 있도록 합니다.

▼ 기본 경로를 추가하는 방법

이 절차는 GUI를 사용해서 기본 경로를 추가합니다. 이 예제는 명령줄을 사용해서 기본 경로를 추가하는 방법을 보여줍니다.

시작하기 전에 전역 영역에서 보안 관리자 역할을 가진 사용자여야 합니다.

각 대상 호스트, 네트워크 및 게이트웨이를 보안 템플리트에 추가했습니다. 자세한 내용은 호스트를 보안 템플리트에 추가하는 방법 [205] 및 호스트 범위를 보안 템플리트에 추가하는 방법 [210]을 참조하십시오.

1. **`txzonemgr` GUI를 사용하여 기본 경로를 만듭니다.**

   ```
   # txzonemgr &
   ```

2. **기본 경로를 설정할 영역을 두 번 누른 다음 IP 주소 항목을 두 번 누릅니다.**
   영역에 둘 이상의 IP 주소가 있을 경우 원하는 인터페이스가 있는 항목을 선택합니다.

3. **프롬프트에서 라우터의 IP 주소를 입력하고 OK(확인)를 누릅니다.**

참고 - 기본 라우터를 제거하거나 수정하려면 항목을 제거하고 IP 항목을 다시 만든 다음 라우터를 추가합니다. 영역에 하나의 IP 주소만 있는 경우 IP 인스턴스를 제거하여 항목을 제거해야 합니다.

예 16-20 **`route`** 명령을 사용하여 전역 영역에 대한 기본 경로 설정

이 예에서 관리자는 `route` 명령을 사용하여 전역 영역에 대한 기본 경로를 만듭니다.

```
# route add default 192.168.113.1 -static
```

▼ 영역에 대한 다중 레벨 포트를 만드는 방법

개인 및 공유 MLP를 레이블이 있는 영역 및 전역 영역에 추가할 수 있습니다.

이 절차는 레이블이 있는 영역에서 실행되는 응용 프로그램이 영역과 통신하기 위해 다중 레벨 포트(MLP)가 필요한 경우 사용됩니다. 이 절차에서 웹 프록시는 영역과 통신합니다.

시작하기 전에 전역 영역에서 `root` 역할을 가진 사용자여야 합니다. 시스템에는 둘 이상의 IP 주소가 있어야 하고 레이블이 있는 영역은 정지됩니다.

1. **프록시 호스트 및 웹 서비스 호스트를 `/etc/hosts` 파일에 추가합니다.**

```
## /etc/hosts file
...
proxy-host-name  IP-address
web-service-host-name IP-address
```

2. **영역을 구성합니다.**

   예를 들어, 명시적으로 `PUBLIC` 레이블이 지정된 패킷을 인식하도록 `public` 영역을 구성합니다. 이 구성의 경우 보안 템플리트의 이름은 `webprox`입니다.

```
# tncfg -t webprox
tncfg:public> set name=webprox
tncfg:public> set host_type=cipso
tncfg:public> set min_label=public
tncfg:public> set max_label=public
tncfg:public> add host=mywebproxy.oracle.com      host name associated with public zone
tncfg:public> add host=10.1.2.3/16      IP address of public zone
tncfg:public> exit
```

3. **MLP를 구성합니다.**

   예를 들어, 웹 프록시 서비스는 `8080/tcp` 인터페이스를 통해 `PUBLIC` 영역과 통신할 수 있습니다.

```
# tncfg -z public add mlp_shared=8080/tcp
# tncfg -z public add mlp_private=8080/tcp
```

4. **MLP를 커널에 추가하려면 영역을 부트합니다.**

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

5. **전역 영역에서 새 주소에 대한 경로를 추가합니다.**

   경로를 추가하려면 기본 경로를 추가하는 방법 [217]을 수행합니다.

예 16-21 txzonemgr GUI를 사용하여 MLP 구성

관리자는 Labeled Zone Manager(레이블이 있는 영역 관리자)를 열어 웹 프록시 서비스를 구성합니다.

```
# txzonemgr &
```

관리자는 PUBLIC 영역을 두 번 누른 다음 Configure Multilevel Ports(다중 레벨 포트 구성)를 두 번 누릅니다. 그런 다음 관리자는 Private interfaces(개인 인터페이스) 행을 선택하고 두 번 누릅니다. 선택이 다음과 유사한 입력 필드로 바뀝니다.

```
Private interfaces:111/tcp;111/udp
```

관리자는 세미콜론 구분자를 사용하여 웹 프록시 입력을 시작합니다.

```
Private interfaces:111/tcp;111/udp;8080/tcp
```

개인 입력을 완료한 후 관리자는 웹 프록시를 Shared interfaces(공유 인터페이스) 필드에 입력합니다.

```
Shared interfaces:111/tcp;111/udp;8080/tcp
```

public 영역에 대한 다중 레벨 포트가 영역의 다음 부트 시 활성화된다는 팝업 메시지가 나타납니다.

예 16-22 udp를 통해 NFSv3에 대한 개인 다중 레벨 포트 구성

이 예에서 관리자는 udp를 통해 NFSv3 하위 읽기 마운트를 사용으로 설정합니다. 관리자는 tncfg 명령을 사용할 수도 있습니다.

```
# tncfg -z global add mlp_private=2049/udp
```

txzonemgr GUI는 MLP를 정의할 수 있는 또 하나의 방법을 제공합니다.

Labeled Zone Manager(레이블이 있는 영역 관리자)에서 관리자는 global 영역을 두 번 누른 다음 Configure Multilevel Ports(다중 레벨 포트 구성)를 두 번 누릅니다. MLP 메뉴에서 관리자는 Private interfaces(개인 인터페이스) 행을 선택하고 두 번 누른 다음 포트/프로토콜을 추가합니다.

```
Private interfaces:111/tcp;111/udp;8080/tcp
```

global 영역에 대한 다중 레벨 포트가 다음 부트 시 활성화된다는 팝업 메시지가 나타납니다.

예 16-23 시스템의 다중 레벨 포트 표시

이 예에서 시스템은 레이블이 있는 여러 영역으로 구성되어 있습니다. 모든 영역은 동일한 IP 주소를 공유합니다. 또한 일부 영역은 영역별 주소로 구성되어 있습니다. 이 구성에서 웹 브라우징을 위한 TCP 포트인 8080 포트는 공용 영역의 공유 인터페이스에서 MLP입니다. 또한 관리자는 telnet용 TCP 포트 23이 공용 영역에서 MLP가 되도록 설정했습니다. 이러한 두

MLP는 공유 인터페이스에 있으므로 전역 영역을 비롯한 다른 영역에서는 공유 인터페이스의 8080 및 23 포트에서 패킷을 받을 수 없습니다.

또한 ssh에 대한 TCP 포트인 22 포트는 공용 영역에서 영역별 MLP입니다. 공용 영역의 ssh 서비스는 주소의 레이블 범위 내에 있는 영역별 주소에서 패킷을 수신할 수 있습니다.

다음 명령은 공용 영역에 대한 MLP를 보여줍니다.

```
# tninfo -m public
private: 22/tcp
shared:  23/tcp;8080/tcp
```

다음 명령은 전역 영역에 대한 MLP를 보여줍니다. 전역 영역은 공용 영역과 동일한 주소를 공유하므로 23 및 8080 포트는 전역 영역에서 MLP가 될 수 없습니다.

```
# tninfo -m global
private: 111/tcp;111/udp;514/tcp;515/tcp;631/tcp;2049/tcp;
6000-6003/tcp;38672/tcp;60770/tcp;
shared:  6000-6003/tcp
```

레이블이 있는 IPsec 구성

다음 작업 맵에서는 레이블을 IPsec 보호에 추가하는 데 사용되는 작업을 설명합니다.

표 16-1 레이블이 있는 IPsec 구성 작업 맵

작업	설명	수행 방법
Trusted Extensions와 함께 IPsec를 사용합니다.	레이블을 IPsec 보호에 추가합니다.	다중 레벨 Trusted Extensions 네트워크에서 IPsec 보호를 적용하는 방법 [220]
신뢰할 수 없는 네트워크에서 Trusted Extensions와 함께 IPsec를 사용합니다.	레이블이 없는 네트워크에서 레이블이 있는 IPsec 패킷을 터널링합니다.	신뢰할 수 없는 네트워크에서 터널을 구성하는 방법 [222]

▼ 다중 레벨 Trusted Extensions 네트워크에서 IPsec 보호를 적용하는 방법

이 절차에서는 다음 조건을 처리하기 위해 두 Trusted Extensions 시스템에서 IPsec를 구성합니다.

- enigma 및 partym의 두 시스템이 다중 레벨 네트워크에서 작동하는 다중 레벨 Trusted Extensions 시스템입니다.
- 응용 프로그램 데이터가 암호화되고 네트워크 내에서 무단 변경을 막도록 보호되어 있습니다.

- 데이터의 보안 레이블은 enigma 및 partym 시스템 사이의 경로에 있는 다중 레벨 라우터 및 보안 장치에서 사용하도록 CALIPSO 또는 CIPSO IP 옵션의 형태로 표시됩니다.
- enigma 및 partym이 교환하는 보안 레이블은 무단 변경을 막도록 보호됩니다.

시작하기 전에 전역 영역에서 root 역할을 가진 사용자입니다.

1. **enigma 및 partym 호스트를 cipso 보안 템플리트에 추가합니다.**
   "호스트 및 네트워크 레이블 지정" [199]의 절차를 따릅니다. cipso 호스트 유형의 템플리트를 사용합니다.

2. **enigma 및 partym 시스템에 대해 IPsec를 구성합니다.**
   절차는 "Oracle Solaris 11.2의 네트워크 보안 "의 "IPsec을 사용하여 두 서버 간의 네트워크 트래픽을 보호하는 방법"을 참조하십시오. 다음 단계에 설명된 대로 키 관리를 위해 IKE를 사용합니다.

3. **레이블을 IKE 협상에 추가합니다.**
   "Oracle Solaris 11.2의 네트워크 보안 "의 "미리 공유한 키로 IKEv2를 구성하는 방법"에 나온 절차를 따른 다음 ike/config 파일을 다음과 같이 수정합니다.

   a. **label_aware, multi_label 및 wire_label inner 키워드를 enigma 시스템의 /etc/inet/ike/config 파일에 추가합니다.**
      결과 파일은 다음과 유사하게 나타납니다. 레이블 추가는 강조 표시되어 있습니다.

```
 ### ike/config file on enigma, 192.168.116.16
## Global parameters
#
## Use IKE to exchange security labels.
label_aware
#
## Defaults that individual rules can override.
p1_xform
{ auth_method preshared oakley_group 5 auth_alg sha encr_alg 3des }
p2_pfs 2
#
## The rule to communicate with partym
# Label must be unique
{ label "enigma-partym"
local_addr 192.168.116.16
remote_addr 192.168.13.213
multi_label
wire_label inner
p1_xform
{ auth_method preshared oakley_group 5 auth_alg sha1 encr_alg aes }
p2_pfs 5
}
```

   b. **동일한 키워드를 partym 시스템의 ike/config 파일에 추가합니다.**

```
 ### ike/config file on partym, 192.168.13.213
```

```
## Global Parameters
#
## Use IKE to exchange security labels.
label_aware
#
p1_xform
{ auth_method preshared oakley_group 5 auth_alg sha encr_alg 3des }
p2_pfs 2
## The rule to communicate with enigma
# Label must be unique
{ label "partym-enigma"
local_addr 192.168.13.213
remote_addr 192.168.116.16
multi_label
wire_label inner
p1_xform
{ auth_method preshared oakley_group 5 auth_alg sha1 encr_alg aes }
p2_pfs 5
}
```

4. **CALIPSO 또는 CIPSO IP 옵션의 AH 보호를 네트워크에서 사용할 수 없는 경우 ESP 인증을 사용합니다.**

   `/etc/inet/ipsecinit.conf` 파일의 `auth_algs` 대신 `encr_auth_algs`를 사용하여 인증을 처리하십시오. ESP 인증은 IP 헤더 및 IP 옵션을 포함하지 않지만, ESP 헤더 이후의 모든 정보를 인증합니다.

   ```
   {laddr enigma raddr partym} ipsec {encr_algs any encr_auth_algs any sa shared}
   ```

참고 - 인증서로 보호되는 시스템에 레이블을 추가할 수도 있습니다. 공개 키 인증서는 Trusted Extensions 시스템의 전역 영역에서 관리됩니다. "Oracle Solaris 11.2의 네트워크 보안 "의 "공개 키 인증서로 IKEv2 구성"에 나온 절차를 완료할 때 `ike/config` 파일을 유사하게 수정합니다.

▼ 신뢰할 수 없는 네트워크에서 터널을 구성하는 방법

이 절차에서는 두 Trusted Extensions VPN 게이트웨이 시스템 사이의 공용 네트워크에서 IPsec 터널을 구성합니다. 이 절차에서 사용된 예는 "Oracle Solaris 11.2의 네트워크 보안 "의 "VPN을 보호하기 위한 IPsec 작업에 대한 네트워크 토폴로지 설명"에 나온 구성을 기준으로 합니다.

이 구성에서 다음과 같은 수정 사항이 있습니다.

- `10` 서브넷은 다중 레벨 신뢰할 수 있는 네트워크입니다. CALIPSO 또는 CIPSO IP 옵션 보안 레이블을 이러한 LAN에서 볼 수 있습니다.
- `192.168` 서브넷은 `PUBLIC` 레이블에서 작동하는 단일 레이블 신뢰할 수 없는 네트워크입니다. 이러한 네트워크는 CALIPSO 또는 CIPSO IP 옵션을 지원하지 않습니다.
- `euro-vpn` 및 `calif-vpn` 간의 레이블이 있는 트래픽은 무단 변경으로부터 보호됩니다.

시작하기 전에 전역 영역에서 root 역할을 가진 사용자입니다.

1. **"호스트 및 네트워크 레이블 지정" [199]의 절차에 따라 다음을 정의합니다.**

   a. **10.0.0.0/8 IP 주소를 레이블이 있는 보안 템플리트에 추가합니다.**

      cipso 호스트 유형의 템플리트를 사용합니다. ADMIN_LOW ~ ADMIN_HIGH의 기본 레이블 범위를 유지합니다.

   b. **192.168.0.0/16 IP 주소를 PUBLIC 레이블에서 레이블이 없는 보안 템플리트에 추가합니다.**

      레이블이 없는 호스트 유형의 템플리트를 사용합니다. 기본 레이블을 PUBLIC으로 설정합니다. ADMIN_LOW ~ ADMIN_HIGH의 기본 레이블 범위를 유지합니다.

   c. **Calif-vpn 및 Euro-vpn 인터넷 연결 주소인 192.168.13.213 및 192.168.116.16을 cipso 템플리트에 추가합니다.**

      기본 레이블 범위를 유지합니다.

2. **IPsec 터널을 만듭니다.**

   "Oracle Solaris 11.2의 네트워크 보안 "의 "터널 모드에서 IPsec을 사용하여 두 LAN 사이의 연결을 보호하는 방법"의 절차를 따릅니다. 다음 단계에 설명된 대로 키 관리를 위해 IKE를 사용합니다.

3. **레이블을 IKE 협상에 추가합니다.**

   "Oracle Solaris 11.2의 네트워크 보안 "의 "미리 공유한 키로 IKEv2를 구성하는 방법"에 나온 절차를 따른 다음 ike/config 파일을 다음과 같이 수정합니다.

   a. **label_aware, multi_label 및 wire_label none PUBLIC 키워드를 euro-vpn 시스템의 /etc/inet/ike/config 파일에 추가합니다.**

      결과 파일은 다음과 유사하게 나타납니다. 레이블 추가는 강조 표시되어 있습니다.

```
        ### ike/config file on euro-vpn, 192.168.116.16
## Global parameters
#
## Use IKE to exchange security labels.
label_aware
#
## Defaults that individual rules can override.
p1_xform
{ auth_method preshared oakley_group 5 auth_alg sha encr_alg 3des }
p2_pfs 2
#
## The rule to communicate with calif-vpn
# Label must be unique
{ label "eurovpn-califvpn"
local_addr 192.168.116.16
remote_addr 192.168.13.213
```

```
multi_label
wire_label none PUBLIC
p1_xform
{ auth_method preshared oakley_group 5 auth_alg sha1 encr_alg aes }
p2_pfs 5
}
```

b. **동일한 키워드를 `calif-vpn` 시스템의 `ike/config` 파일에 추가합니다.**

```
 ### ike/config file on calif-vpn, 192.168.13.213
## Global Parameters
#
## Use IKE to exchange security labels.
label_aware
#
p1_xform
{ auth_method preshared oakley_group 5 auth_alg sha encr_alg 3des }
p2_pfs 2
## The rule to communicate with euro-vpn
# Label must be unique
{ label "califvpn-eurovpn"
local_addr 192.168.13.213
remote_addr 192.168.116.16
multi_label
wire_label none PUBLIC
p1_xform
{ auth_method preshared oakley_group 5 auth_alg sha1 encr_alg aes }
p2_pfs 5
}
```

참고 - 인증서로 보호되는 시스템에 레이블을 추가할 수도 있습니다. “Oracle Solaris 11.2의 네트워크 보안 ”의 “공개 키 인증서로 IKEv2 구성”에 나온 절차를 완료할 때 `ike/config` 파일을 유사하게 수정합니다.

신뢰할 수 있는 네트워크 문제 해결

다음 작업 맵에서는 Trusted Extensions 네트워크를 디버깅하는 데 도움이 되는 작업을 설명합니다.

표 16-2 신뢰할 수 있는 네트워크 문제 해결 작업 맵

작업	설명	수행 방법
시스템과 원격 호스트가 통신할 수 없는 이유를 확인합니다.	단일 시스템의 인터페이스가 작동 중인지 확인합니다.	시스템의 인터페이스가 작동 중인지 확인하는 방법 [225]
	시스템과 원격 호스트가 서로 통신할 수 없을 때 디버깅 도구를 사용합니다.	Trusted Extensions 네트워크를 디버깅하는 방법 [226]

작업	설명	수행 방법
LDAP 클라이언트가 LDAP 서버에 연결할 수 없는 이유를 확인합니다.	LDAP 서버와 클라이언트 간의 연결 끊김 문제를 해결합니다.	LDAP 서버에 대한 클라이언트 연결을 디버깅하는 방법 [229]

▼ 시스템의 인터페이스가 작동 중인지 확인하는 방법

시스템이 다른 호스트와 예상한 대로 통신하지 않을 경우 이 절차를 사용합니다.

시작하기 전에 전역 영역에서 네트워크 속성 값을 확인할 수 있는 역할을 가진 사용자여야 합니다. 보안 관리자 역할 및 시스템 관리자 역할이 이러한 값을 확인할 수 있습니다.

1. **시스템의 네트워크 인터페이스가 작동 중인지 확인합니다.**
   Labeled Zone Manager(레이블이 있는 영역 관리자) GUI 또는 `ipadm` 명령을 사용하여 시스템의 인터페이스를 표시할 수 있습니다.

   - **Labeled Zone Manager(레이블이 있는 영역 관리자)를 연 다음 관심 영역을 두 번 누릅니다.**

     ```
     # txzonemgr &
     ```

     Configure Network Interfaces(네트워크 인터페이스 구성)를 선택하고 영역에 대한 `Status` 열의 값이 `Up`인지 확인합니다.

   - **또는 `ipadm show-addr` 명령을 사용합니다.**

     ```
     # ipadm show-addr
     ...
     ADDROBJ           TYPE      STATE        ADDR
     lo0/v4            static    ok           127.0.0.1/8
     net0/_a           dhcp      down         10.131.132.133/23
     net0:0/_a         dhcp      down         10.131.132.175/23
     ```

     `net0` 인터페이스의 값이 `ok`이어야 합니다. `ipadm` 명령에 대한 자세한 내용은 `ipadm`(1M) 매뉴얼 페이지를 참조하십시오.

2. **인터페이스가 작동 중이 아닌 경우 작동시킵니다.**

   a. **Labeled Zone Manager(레이블이 있는 영역 관리자) GUI에서 인터페이스 작동이 중지된 영역을 두 번 누릅니다.**

   b. **Configure Network Interfaces(네트워크 인터페이스 구성)를 선택합니다.**

   c. **상태가 Down(작동 중지)인 인터페이스를 두 번 누릅니다.**

   d. **Bring Up(작동 시작)을 선택한 다음 OK(확인)를 선택합니다.**

e. **Cancel(취소) 또는 OK(확인)를 누릅니다.**

▼ Trusted Extensions 네트워크를 디버깅하는 방법

통신 중이 아닌 두 호스트를 디버깅하려면 Trusted Extensions 및 Oracle Solaris 디버깅 도구를 사용합니다. 예를 들어, `snoop` 및 `netstat`와 같은 Oracle Solaris 네트워크 디버깅 명령을 사용할 수 있습니다. 자세한 내용은 `snoop`(1M) 및 `netstat`(1M) 매뉴얼 페이지를 참조하십시오. Trusted Extensions에 대한 특정 명령은 부록 D. Trusted Extensions 매뉴얼 페이지 목록을 참조하십시오.

- 레이블이 있는 영역에 대한 연결 문제는 “영역 관리” [155]를 참조하십시오.
- NFS 마운트 디버깅은 Trusted Extensions에서 마운트 실패 문제를 해결하는 방법 [179]을 참조하십시오.

시작하기 전에 전역 영역에서 네트워크 속성 값을 확인할 수 있는 역할을 가진 사용자여야 합니다. 보안 관리자 역할 또는 시스템 관리자 역할이 이러한 값을 확인할 수 있습니다. `root` 역할만 파일을 편집할 수 있습니다.

1. **통신할 수 없는 호스트가 동일한 이름 지정 서비스를 사용 중인지 확인합니다.**

   a. **각 시스템에서 `name-service/switch` SMF 서비스의 Trusted Extensions 데이터베이스에 대한 값을 확인합니다.**

   ```
   # svccfg -s name-service/switch listprop config
   config/value_authorization  astring  solaris.smf.value.name-service.switch
   config/default              astring  ldap
   ...
   config/tnrhtp               astring  "files ldap"
   config/tnrhdb               astring  "files ldap"
   ```

   b. **값이 여러 호스트에서 서로 다른 경우 해당 호스트의 값을 수정합니다.**

   ```
   # svccfg -s name-service/switch setprop config/tnrhtp="files ldap"
   # svccfg -s name-service/switch setprop config/tnrhdb="files ldap"
   ```

   c. **그런 다음 해당 호스트에서 이름 지정 서비스 데몬을 다시 시작합니다.**

   ```
   # svcadm restart name-service/switch
   ```

2. **전송 중 소스, 대상 및 게이트웨이 호스트에 대한 보안 속성을 표시하여 각 호스트가 올바르게 정의되었는지 확인합니다.**

   명령줄을 사용하여 네트워크 정보가 올바른지 확인합니다. 각 호스트에 대한 지정 사항이 네트워크의 다른 호스트에 대한 지정 사항과 일치하는지 확인합니다. 원하는 보기에 따라 `tncfg` 명령, `tninfo` 명령 또는 `txzonemgr` GUI를 사용합니다.

- **템플리트 정의를 표시합니다.**

  `tninfo -t` 명령은 레이블을 문자열 및 16진수 형식으로 표시합니다.

```
# tninfo -t template-name
template: template-name
host_type: one of cipso or UNLABELED
doi: 1
min_sl: minimum-label
hex: minimum-hex-label
max_sl: maximum-label
hex: maximum-hex-label
```

- **템플리트 및 여기에 지정된 호스트를 표시합니다.**

  `tncfg -t` 명령은 레이블을 문자열 형식으로 표시하고 지정된 호스트를 나열합니다.

```
# tncfg -t template info
name=<template-name>
host_type=<one of cipso or unlabeled>
doi=1
min_label=<minimum-label>
max_label=<maximum-label>
host=127.0.0.1/32            /** Localhost **/
host=192.168.1.2/32          /** LDAP server **/
host=192.168.1.22/32         /** Gateway to LDAP server **/
host=192.168.113.0/24        /** Additional network **/
host=192.168.113.100/25            /** Additional network **/
host=2001:a08:3903:200::0/56     /** Additional network **/
```

- **특정 호스트에 대한 IP 주소 및 지정된 보안 템플리트를 표시합니다.**

  `tninfo -h` 명령은 지정된 호스트의 IP 주소 및 지정된 보안 템플리트의 이름을 표시합니다.

```
# tninfo -h hostname
IP Address: IP-address
Template: template-name
```

  `tncfg get host=` 명령은 지정된 호스트를 정의하는 보안 템플리트의 이름을 표시합니다.

```
# tncfg get host=hostname|IP-address[/prefix]
template-name
```

- **영역에 대한 다중 레벨 포트(MLP)를 표시합니다.**

  `tncfg -z` 명령은 행당 하나의 MLP를 나열합니다.

```
# tncfg -z zone-name info [mlp_private | mlp_shared]
mlp_private=<port/protocol-that-is-specific-to-this-zone-only>
mlp_shared=<port/protocol-that-the-zone-shares-with-other-zones>
```

`tninfo -m` 명령은 첫번째 행에 개인 MLP를 나열하고, 두번째 행에 공유 MLP를 나열합니다. MLP는 세미콜론으로 구분됩니다.

```
# tninfo -m zone-name
private: ports-that-are-specific-to-this-zone-only
shared: ports-that-the-zone-shares-with-other-zones
```

MLP의 GUI 표시는 `txzonemgr` 명령을 사용합니다. 영역을 두 번 누른 다음 Configure Multilevel Ports(다중 레벨 포트 구성)를 선택합니다.

3. **잘못된 정보를 수정합니다.**

   a. **네트워크 보안 정보를 변경하거나 확인하려면 신뢰할 수 있는 네트워크 관리 명령인 `tncfg` 및 `txzonemgr`을 사용합니다. 데이터베이스의 구문을 확인하려면 `tnchkdb` 명령을 사용합니다.**

   예를 들어, 다음 출력은 템플리트 이름 `internal_cipso`가 정의되지 않았음을 나타냅니다.

```
# tnchkdb
checking /etc/security/tsol/tnrhtp ...
checking /etc/security/tsol/tnrhdb ...
tnchkdb: unknown template name: internal_cipso at line 49
tnchkdb: unknown template name: internal_cipso at line 50
tnchkdb: unknown template name: internal_cipso at line 51
checking /etc/security/tsol/tnzonecfg ...
```

   오류는 `internal_cipso` 보안 템플리트를 만들고 지정하는 데 `tncfg` 및 `txzonemgr` 명령이 사용되지 않았음을 나타냅니다.

   복구하려면 `tnrhdb` 파일을 원본 파일로 바꾼 다음 `tncfg` 명령을 사용하여 보안 템플리트를 만들고 지정합니다.

   b. **커널 캐시를 지우려면 재부트합니다.**

   부팅 시 캐시는 데이터베이스 정보로 채워집니다. SMF 서비스 `name-service/switch`는 커널을 채우는 데 로컬 또는 LDAP 데이터베이스가 사용되는지 결정합니다.

4. **전송 정보를 수집하면 디버깅에 도움이 됩니다.**

   a. **경로 지정 구성을 확인합니다.**

```
# route get [ip] -secattr sl=label,doi=integer
```

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

   b. **패킷의 레이블 정보를 봅니다.**

```
# snoop -v
```

-v 옵션은 레이블 정보를 포함한 패킷 헤더의 세부 사항을 표시합니다. 이 명령은 많은 세부 사항을 제공하므로 명령이 검사하는 패킷을 제한하는 것이 좋습니다. 자세한 내용은 snoop(1M) 매뉴얼 페이지를 참조하십시오.

c. **경로 지정 테이블 항목 및 소켓의 보안 속성을 봅니다.**

```
# netstat -aR
```

-aR 옵션은 소켓에 대한 확장 보안 속성을 표시합니다.

```
# netstat -rR
```

-rR 옵션은 경로 지정 테이블 항목을 표시합니다. 자세한 내용은 netstat(1M) 매뉴얼 페이지를 참조하십시오.

▼ LDAP 서버에 대한 클라이언트 연결을 디버깅하는 방법

LDAP 서버에서 클라이언트 항목을 잘못 구성하면 클라이언트가 서버와 통신하지 못할 수 있습니다. 마찬가지로 클라이언트에서 파일을 잘못 구성해도 통신에 방해가 될 수 있습니다. 클라이언트와 서버 간 통신 문제를 디버깅할 때 다음 항목과 파일을 확인하십시오.

시작하기 전에 LDAP 클라이언트의 전역 영역에서 보안 관리자 역할을 가진 사용자여야 합니다.

1. **LDAP 서버에 대한 원격 호스트 템플리트 및 LDAP 서버의 게이트웨이에 대한 원격 호스트 템플리트가 올바른지 확인합니다.**

   a. **tncfg 또는 tninfo 명령을 사용하여 정보를 봅니다.**

   ```
   # tncfg get host=LDAP-server
   # tncfg get host=gateway-to-LDAP-server

   # tninfo -h LDAP-server
   # tninfo -h gateway-to-LDAP-server
   ```

   b. **서버에 대한 경로를 확인합니다.**

   ```
   # route get LDAP-server
   ```

   템플리트 지정이 올바르지 않은 경우 호스트를 올바른 템플리트에 추가합니다.

2. **/etc/hosts 파일을 확인하고 필요한 경우 수정합니다.**

   시스템, 시스템의 레이블이 있는 영역에 대한 인터페이스, LDAP 서버에 대한 게이트웨이 및 LDAP 서버가 파일에 나열되어야 합니다. 추가 항목이 있을 수도 있습니다.

중복된 항목을 찾습니다. 다른 시스템의 레이블이 있는 영역인 항목을 제거합니다. 예를 들어, Lserver가 LDAP 서버의 이름이고 LServer-zones가 레이블이 있는 영역에 대한 공유 인터페이스인 경우 /etc/hosts 파일에서 LServer-zones를 제거합니다.

3. **DNS를 사용하는 경우 svc:/network/dns/client 서비스의 구성을 확인합니다.**

```
# svccfg -s dns/client listprop config
config                      application
config/value_authorization  astring       solaris.smf.value.name-service.dns.switch
config/nameserver           astring       192.168.8.25 192.168.122.7
```

4. **값을 변경하려면 svccfg 명령을 사용합니다.**

```
# svccfg -s dns/client setprop config/search = astring: example1.domain.com
# svccfg -s dns/client setprop config/nameserver = net_address: 192.168.8.35
# svccfg -s dns/client:default refresh
# svccfg -s dns/client:default validate
# svcadm enable dns/client
# svcadm refresh name-service/switch
# nslookup some-system
Server:         192.168.135.35
Address:        192.168.135.35#53

Name:   some-system.example1.domain.com
Address: 10.138.8.22
Name:   some-system.example1.domain.com
Address: 10.138.8.23
```

5. **name-service/switch 서비스의 tnrhdb 및 tnrhtp 항목이 정확한지 확인합니다.**

   다음 출력에서 tnrhdb 및 tnrhtp 항목은 나열되지 않았습니다. 따라서 이러한 데이터베이스는 기본값인 files ldap 이름 지정 서비스를 순서대로 사용하는 것입니다.

```
# svccfg -s name-service/switch listprop config
config                      application
config/value_authorization  astring       solaris.smf.value.name-service.switch
config/default              astring       "files ldap"
config/host                 astring       "files dns"
config/netgroup             astring       ldap
```

6. **클라이언트가 서버에서 올바르게 구성되었는지 확인합니다.**

```
# ldaplist -l tnrhdb client-IP-address
```

7. **레이블이 있는 영역에 대한 인터페이스가 LDAP 서버에서 올바르게 구성되었는지 확인합니다.**

```
# ldaplist -l tnrhdb client-zone-IP-address
```

8. **현재 실행 중인 모든 영역에서 LDAP 서버에 연결할 수 있는지 확인합니다.**

```
# ldapclient list
```

```
...
NS_LDAP_SERVERS= LDAP-server-address
# zlogin zone-name1 ping LDAP-server-address
LDAP-server-address is alive
# zlogin zone-name2 ping LDAP-server-address
LDAP-server-address is alive
...
```

9. **LDAP를 구성하고 재부팅합니다.**

   a. **절차는 Trusted Extensions에서 전역 영역을 LDAP 클라이언트로 만들기 [83]를 참조하십시오.**

   b. **모든 레이블이 있는 영역에서 LDAP 서버의 클라이언트로 영역을 재설정합니다.**

```
# zlogin zone-name1
# ldapclient init \
-a profileName=profileName \
-a domainName=domain \
-a proxyDN=proxyDN \
-a proxyPassword=password LDAP-Server-IP-Address
# exit
# zlogin zone-name2 ...
```

   c. **모든 영역을 정지하고 재부트합니다.**

```
# zoneadm list
zone1
zone2
,
,
,
# zoneadm -z zone1 halt
# zoneadm -z zone2 halt
.
.
.
# reboot
```

   대신 `txzonemgr` GUI를 사용하여 레이블이 있는 영역을 정지할 수도 있습니다.

♦ ♦ ♦ 17 장

17 Trusted Extensions 및 LDAP 정보

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

Trusted Extensions에서 LDAP 이름 지정 서비스 사용

여러 Trusted Extensions 시스템이 있는 보안 도메인에서 사용자, 호스트 및 네트워크 속성의 동일성을 확보하기 위해 대부분의 구성 정보 배포 시 이름 지정 서비스가 사용됩니다. `svc:/system/name-service/switch` 서비스는 사용되는 이름 지정 서비스를 결정합니다. Trusted Extensions에는 LDAP를 이름 지정 서비스로 사용하는 것이 좋습니다.

LDAP 서버는 Trusted Extensions 및 Oracle Solaris 클라이언트에 대한 LDAP 이름 지정 서비스를 제공할 수 있습니다. 서버에 Trusted Extensions 네트워크 데이터베이스가 포함되어야 하며, Trusted Extensions 클라이언트가 다중 레벨 포트를 통해 해당 서버에 연결되어야 합니다. 보안 관리자는 시스템 구성 중 다중 레벨 포트를 지정합니다.

일반적으로 이 다중 레벨 포트는 전역 영역에서 전역 영역에 대해 구성됩니다. 따라서 레이블이 있는 영역에는 LDAP 디렉토리에 대한 쓰기 권한이 없습니다. 대신 레이블이 있는 영역은 자체 시스템 또는 네트워크의 다른 신뢰할 수 있는 시스템에서 실행 중인 다중 레벨 프록시 서비스를 통해 읽기 요청을 보냅니다. Trusted Extensions에서는 레이블당 하나의 디렉토리 서버로 이루어진 LDAP 구성도 지원합니다. 사용자의 자격 증명이 레이블별로 다른 경우 이러한 구성이 필요합니다.

Trusted Extensions는 LDAP 서버에 두 개의 신뢰할 수 있는 네트워크 데이터베이스, 즉 `tnrhdb`와 `tnrhtp`를 추가합니다.

- Oracle Solaris에서 LDAP 이름 지정 서비스 사용에 대한 자세한 내용은 "Oracle Solaris 11.2의 이름 지정 및 디렉토리 서비스 작업: LDAP "를 참조하십시오.
- Trusted Extensions에 대한 LDAP 서버 설정은 5장. Trusted Extensions에 대한 LDAP 구성에 설명되어 있습니다. Trusted Extensions로 구성된 프록시를 사용하여 Trusted Extensions 시스템이 Oracle Solaris LDAP 서버의 클라이언트가 될 수 있습니다.

- Trusted Extensions LDAP 서버의 클라이언트 설정은 “Trusted Extensions LDAP 클라이언트 만들기” [83]에 설명되어 있습니다.

로컬로 관리되는 Trusted Extensions 시스템

사이트에서 분산 이름 지정 서비스가 사용되지 않는 경우 관리자는 모든 시스템에서 사용자, 시스템 및 네트워크에 대한 구성 정보가 동일한지 확인해야 합니다. 한 시스템에서 정보를 변경하면 모든 시스템에서도 변경되어야 합니다.

로컬로 관리되는 Trusted Extensions 시스템에서 구성 정보는 `/etc`, `/etc/security` 및 `/etc/security/tsol` 디렉토리의 파일과 `name-service/switch` SMF 서비스의 구성 등록 정보로 유지 관리됩니다.

Trusted Extensions LDAP 데이터베이스

Trusted Extensions는 LDAP Server의 스키마를 확장하여 `tnrhdb` 및 `tnrhtp` 데이터베이스를 수용합니다. Trusted Extensions는 `ipTnetNumber` 및 `ipTnetTemplateName`이라는 두 개의 새로운 속성과 `ipTnetTemplate` 및 `ipTnetHost`라는 두 개의 새로운 객체 클래스를 정의합니다.

속성 정의는 다음과 같습니다.

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

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

객체 클래스 정의는 다음과 같습니다.

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

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

```
MUST ( ipTnetNumber $ ipTnetTemplateName ) )
```

LDAP의 `cipso` 템플리트 정의는 다음과 유사합니다.

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

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

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

Trusted Extensions의 이름 지정 서비스에 대한 빠른 참조

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

- LDAP 구성 문제를 해결하기 위한 전략은 “Oracle Solaris 11.2의 이름 지정 및 디렉토리 서비스 작업: LDAP ”의 6 장, “LDAP 문제 해결”을 참조하십시오.
- 레이블로 인한 클라이언트-서버 LDAP 연결 문제를 해결하려면 LDAP 서버에 대한 클라이언트 연결을 디버깅하는 방법 [229]을 참조하십시오.
- 다른 클라이언트-서버 LDAP 연결 문제를 해결하기 위해서는 “Oracle Solaris 11.2의 이름 지정 및 디렉토리 서비스 작업: LDAP ”의 6 장, “LDAP 문제 해결”을 참조하십시오.
- LDAP 클라이언트에서 LDAP 항목을 표시하려면 다음을 입력합니다.

  ```
  # ldaplist -l
  # ldap_cachemgr -g
  ```

- LDAP 서버에서 LDAP 항목을 표시하려면 다음을 입력하십시오.

  ```
  # ldap_cachemgr -g
  # idsconfig -v
  ```

- LDAP가 관리하는 호스트를 나열하려면 다음을 입력하십시오.

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

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

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

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

- 클라이언트의 LDAP 서비스 상태를 표시하려면 다음을 입력하십시오.

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

- LDAP 클라이언트를 시작하고 중지하려면 다음을 입력합니다.

```
# svcadm enable network/ldap/client

# svcadm disable network/ldap/client
```

- Oracle Directory Server Enterprise Edition 소프트웨어의 버전 6 또는 7에서 LDAP 서버를 시작하고 중지하려면 다음을 입력합니다.

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

- Oracle Directory Server Enterprise Edition 소프트웨어의 버전 6 또는 7에서 프록시 LDAP 서버를 시작하고 중지하려면 다음을 입력합니다.

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

♦ ♦ ♦ 18 장

18 Trusted Extensions의 다중 레벨 메일 정보

이 장에서는 Trusted Extensions를 사용하여 구성된 시스템의 보안 및 다중 레벨 메일러에 대해 설명합니다.

다중 레벨 메일 서비스

Trusted Extensions는 모든 메일 응용 프로그램에 대해 다중 레벨 메일을 제공합니다. 일반 사용자가 해당 메일러를 시작하면 사용자의 현재 레이블에서 응용 프로그램이 열립니다. 사용자가 다중 레벨 시스템에서 작업 중인 경우 해당 메일러 초기화 파일을 연결하거나 복사해야 할 수 있습니다. 자세한 내용은 Trusted Extensions에서 사용자의 시작 파일을 구성하는 방법 [132]을 참조하십시오.

Trusted Extensions 메일 기능

Trusted Extensions에서 시스템 관리자 역할은 “Oracle Solaris 11.2에서의 sendmail 서비스 관리 ”의 2 장, “메일 서비스 관리”의 지침에 따라 메일 서버를 설정 및 관리합니다. 또한 보안 관리자는 Trusted Extensions 메일 기능 구성 방법을 결정합니다.

메일 관리에 대한 다음 내용은 Trusted Extensions에만 해당됩니다.

- 사용자의 로컬 구성 파일(예: `.mailrc`)은 사용자의 최소 레이블에 있습니다.

  따라서 여러 레이블에서 작업하는 사용자는 최소 레이블 디렉토리에서 각 상위 디렉토리로 `.mailrc` 파일을 복사하거나 연결하지 않는 한 상위 레이블에 `.mailrc` 파일이 없습니다.

  보안 관리자 역할이나 개별 사용자는 `.mailrc` 파일을 `.copy_files` 또는 `.link_files` 중 하나에 추가할 수 있습니다. 이러한 파일에 대한 설명은 `updatehome`(1) 매뉴얼 페이지를 참조하십시오. 구성 제안은 “`.copy_files` 및 `.link_files` 파일” [126]을 참조하십시오.

- 메일 판독기는 시스템의 모든 레이블에서 실행할 수 있습니다. 메일 클라이언트를 서버에 연결하려면 일부 구성이 필요합니다.

  예를 들어 다중 레벨 메일에 Thunderbird 메일을 사용하려면 각 레이블에서 Thunderbird 메일 클라이언트를 구성하여 메일 서버를 지정해야 합니다. 각 레이블에 대해 메일 서버가 동일하거나 다를 수 있지만 서버는 반드시 지정해야 합니다.
- Trusted Extensions 소프트웨어는 메일을 보내거나 전달하기 전에 호스트 및 사용자 레이블을 확인합니다.
  - 이 소프트웨어는 해당 메일이 호스트의 승인 범위 내에 있는지 확인합니다. 확인 사항은 이 목록 및 "Trusted Extensions 승인 검사" [191]에 설명되어 있습니다.
  - 이 소프트웨어는 해당 메일이 계정의 클리어런스 및 최소 레이블 사이에 있는지 확인합니다.
  - 사용자는 인정 범위 내에서 수신된 전자 메일을 읽을 수 있습니다. 세션 중에 사용자는 현재 레이블에서만 메일을 읽을 수 있습니다.

    전자 메일을 사용하여 일반 사용자와 연락하려면 사용자가 읽을 수 있는 레이블에 있는 작업 공간에서 관리 역할이 메일을 보내야 합니다. 일반적으로 사용자의 기본 레이블을 선택하는 것이 좋습니다.

♦ ♦ ♦ 19 장

19 레이블이 있는 인쇄 관리

이 장에서는 Trusted Extensions를 사용하여 레이블이 있는 인쇄를 구성하는 방법을 설명합니다. 레이블 지정 옵션 없이 Trusted Extensions 인쇄 작업을 구성하는 방법도 설명합니다.

레이블, 프린터 및 인쇄

Trusted Extensions는 레이블을 사용하여 프린터 액세스를 제어합니다. 프린터 및 대기열의 인쇄 작업 정보에 대한 액세스를 제어하는 데 레이블이 사용됩니다. 또한 이 소프트웨어는 인쇄 출력에 레이블을 지정합니다. 본문 페이지에 레이블이 지정되고 필수 배너와 트레일러 페이지에 레이블이 지정됩니다. 배너와 트레일러 페이지에는 처리 지침도 포함될 수 있습니다.

시스템 관리자는 기본적인 프린터 관리 작업을 수행합니다. 보안 관리자 역할은 프린터 보안을 관리하며 여기에는 레이블 및 레이블이 있는 출력의 처리 방법이 포함됩니다. 관리자는 기본 Oracle Solaris 프린터 관리 절차를 따릅니다. 레이블을 적용하고, 인쇄 작업의 레이블 범위를 제한하고, 인쇄할 레이블이 있는 영역을 구성하고, 인쇄 제한 사항을 완화하려면 구성이 필요합니다.

Trusted Extensions는 단일 레벨과 다중 레벨 인쇄를 모두 지원합니다. 기본적으로 Trusted Extensions 시스템의 전역 영역에서 구성된 인쇄 서버는 전체 레이블을 인쇄할 수 있습니다. 즉, 이 인쇄 서버는 다중 레벨입니다. 레이블이 있는 영역이나 시스템에서 해당 인쇄 서버에 연결할 수 있으면 연결된 프린터로 인쇄할 수 있습니다. 레이블이 있는 영역은 단일 레벨 인쇄를 지원할 수 있습니다. 이 영역은 전역 영역을 통해 프린터에 연결할 수 있거나 영역을 프린터 서버로 구성할 수 있습니다. 레이블이 있는 영역에 연결할 수 있는 해당 레이블의 모든 영역과 해당하는 인쇄 서버는 연결된 프린터로 인쇄할 수 있습니다. 임의 레이블이 지정된 레이블이 없는 시스템의 인쇄 서버를 사용해서도 단일 레벨 인쇄가 가능합니다. 이러한 인쇄 작업은 레이블 없이 인쇄합니다.

Oracle Solaris 10 및 Oracle Solaris 11 간 Trusted Extensions 인쇄의 차이점

Oracle Solaris 10의 기본 인쇄 프로토콜은 LP 인쇄 서비스입니다. Oracle Solaris 11의 기본값은 CUPS(Common UNIX Printing System)입니다. Oracle Solaris의 CUPS에 대한 포괄적인 안내는 "Oracle Solaris 11.2의 인쇄 구성 및 관리 "를 참조하십시오. 다음 표에서는 CUPS와 LP 인쇄 프로토콜 사이의 두드러진 차이점을 나열합니다.

표 19-1 CUPS - LP 차이점

차이점 영역	CUPS	LP
IANA 포트 번호	631	515
인쇄 면	단면	양면
인쇄 중첩	인쇄 서버에서 프린터를 공유해야 함	프린터에 대한 경로를 구성해야 함
네트워크 프린터 액세스	프린터 및 인쇄 서버의 IP 주소를 성공적으로 `ping`할 수 있어야 함	프린터에 대한 경로를 구성해야 함
원격 인쇄 작업	레이블 없이 인쇄할 수 없음	레이블 없이 인쇄할 수 있음
클라이언트에 원격 프린터 추가	`lpadmin -p` *printer-name* `-E \ -v ipp://`*print-server-IP-address*`/printers/`*printer-name-on-server*	`lpadmin -p` *printer-name* `\ -s` *server-name*
인쇄 서버를 사용으로 설정 및 승인	`lpadmin -E` 옵션	`accept` 및 `enable` 명령
포스트스크립트 보호	기본적으로 제공	권한 부여 필요
배너 페이지를 사용으로 설정	`-o job-sheets=labeled` 옵션	기본적으로 제공
배너 및 트레일러 페이지를 사용 안함으로 설정	`-o job-sheets=none` 옵션	`-o nobanner` 옵션
`lp -d` *printer* `file1 file2`	인쇄 작업당 하나의 배너 페이지와 하나의 트레일러 페이지	인쇄 작업의 각 파일에 대한 배너와 트레일러 페이지
작업 페이지의 레이블 방향	항상 세로	항상 작업의 방향

인쇄 서비스	`svc:/application/cups/scheduler`
	`.../in-lpd:default`
		`svc:/application/print/service-selector`
		`.../server`
		`.../rfc1179`
		`.../ipp-listener`
		`svc:/network/device-discovery/printers:snmp`

Trusted Extensions에서 프린터 및 인쇄 작업 정보에 대한 액세스 제한

Trusted Extensions를 사용하여 구성된 시스템의 사용자 및 역할은 해당 세션의 레이블에서 인쇄 작업을 만듭니다. 인쇄 작업은 해당 레이블을 인식하는 인쇄 서버에서만 허용됩니다. 레이블은 인쇄 서버의 레이블 범위에 있어야 합니다.

사용자와 역할은 세션의 레이블과 동일한 레이블을 가진 인쇄 작업을 볼 수 있습니다. 전역 영역의 경우 역할은 영역의 레이블에 의해 지배되는 레이블을 가진 작업을 볼 수 있습니다.

레이블이 있는 프린터 출력

Trusted Extensions는 본문 페이지와 배너 및 트레일러 페이지에 보안 정보를 인쇄합니다. 이 정보는 `/etc/security/tsol/label_encodings` 파일 및 `/usr/lib/cups/filter/tsol_separator.ps` 파일에서 제공됩니다. 80자가 넘는 레이블은 모든 페이지의 맨 위와 아래에 잘려서 인쇄됩니다. 잘림은 화살표(->)로 표시됩니다. 머리글과 바닥글 레이블은 본문 페이지가 가로로 인쇄되더라도 세로 방향으로 인쇄됩니다. 예제를 보려면 그림 19-4. “본문 페이지가 가로 모드로 인쇄될 때 작업의 레이블이 세로 모드로 인쇄”를 참조하십시오.

인쇄 작업에서 표시되는 텍스트, 레이블 및 경고를 구성할 수 있습니다. 지역화를 위해 텍스트를 다른 언어의 텍스트로 바꿀 수도 있습니다. 보안 관리자는 다음을 구성할 수 있습니다.

- 배너와 트레일러 페이지의 텍스트 지역화 또는 사용자 정의
- 배너와 트레일러 페이지의 여러 필드 또는 본문 페이지에 인쇄할 대체 레이블 지정
- 원하는 텍스트나 레이블 변경 또는 생략

레이블이 없는 프린터로 지정된 사용자는 레이블 없이 출력을 인쇄할 수 있습니다. 자체 인쇄 서버가 있는 레이블이 있는 영역의 사용자는 `solaris.print.unlabeled` 권한 부여가 지정된 경우 레이블 없이 출력을 인쇄할 수 있습니다. Trusted Extensions 인쇄 서버에 의해 제어되는 로컬 프린터로 레이블 없이 출력을 인쇄하도록 역할을 구성할 수 있습니다. 지원 정보는 “Trusted Extensions에서 인쇄 제한 사항 감소” [254]를 참조하십시오.

레이블이 있는 배너 및 트레일러 페이지

다음 그림에서는 기본 배너 페이지 및 이 페이지와 기본 트레일러 페이지의 차이점을 보여줍니다. 콜아웃은 다양한 섹션을 식별합니다. 이러한 섹션의 텍스트 소스에 대한 설명은 “Trusted Extensions Label Administration ”의 4 장, “Labeling Printer Output”을 참조하십시오. 트레일러 페이지에서는 윤곽선을 사용합니다.

그림 19-1 레이블이 있는 인쇄 작업의 일반적인 배너 페이지

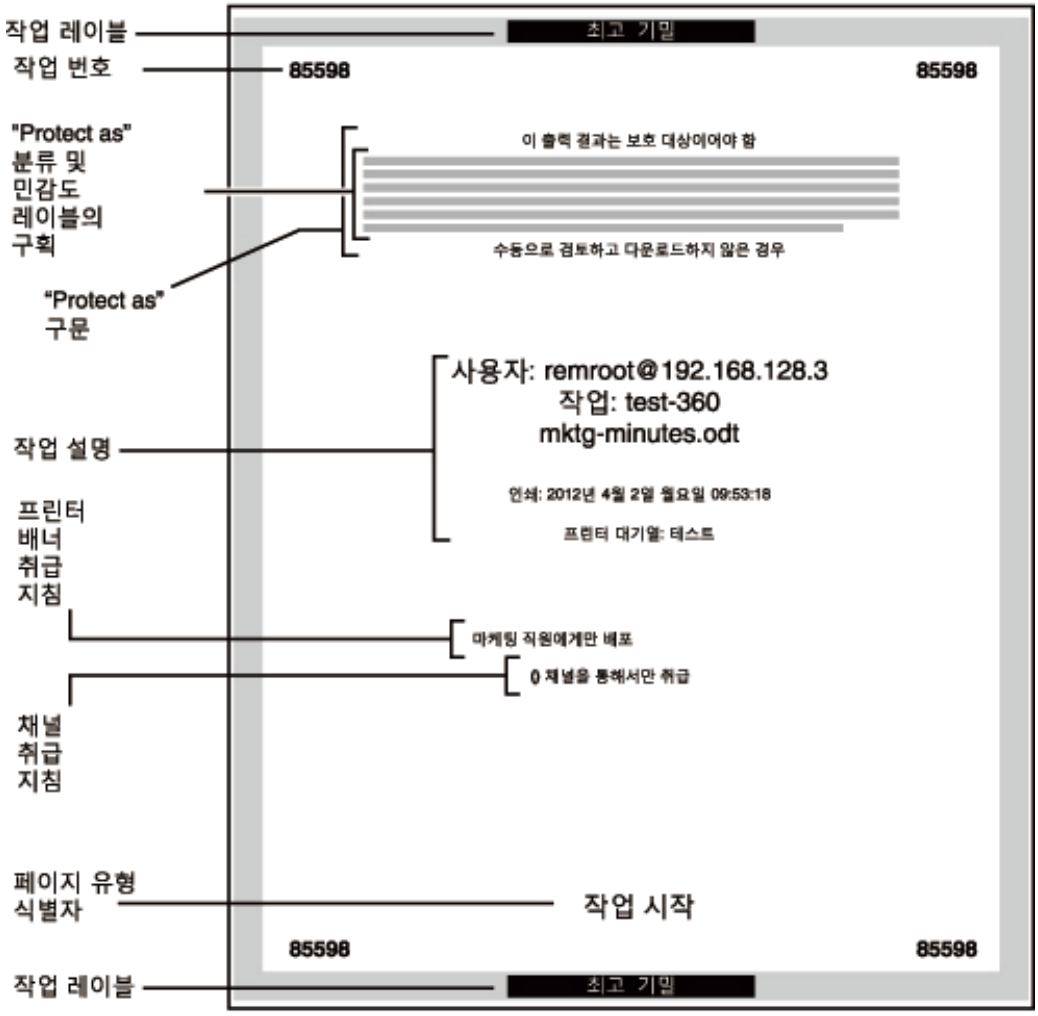
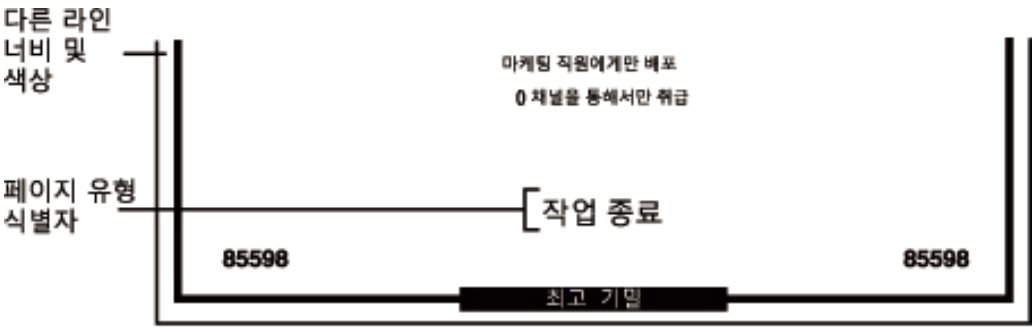


그림 19-2 트레일러 페이지의 차이점

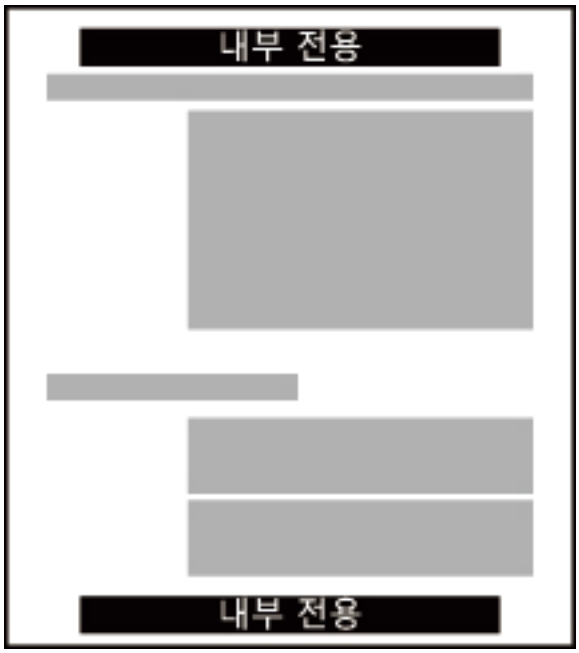


레이블이 있는 본문 페이지

기본적으로 모든 본문 페이지의 맨 위와 아래에는 “Protect as” 분류가 인쇄됩니다. “Protect as” 분류는 작업 레이블의 분류가 `minimum protect as` 분류와 비교될 때 지배 분류입니다. `minimum protect as` 분류는 `label_encodings` 파일에서 정의됩니다.

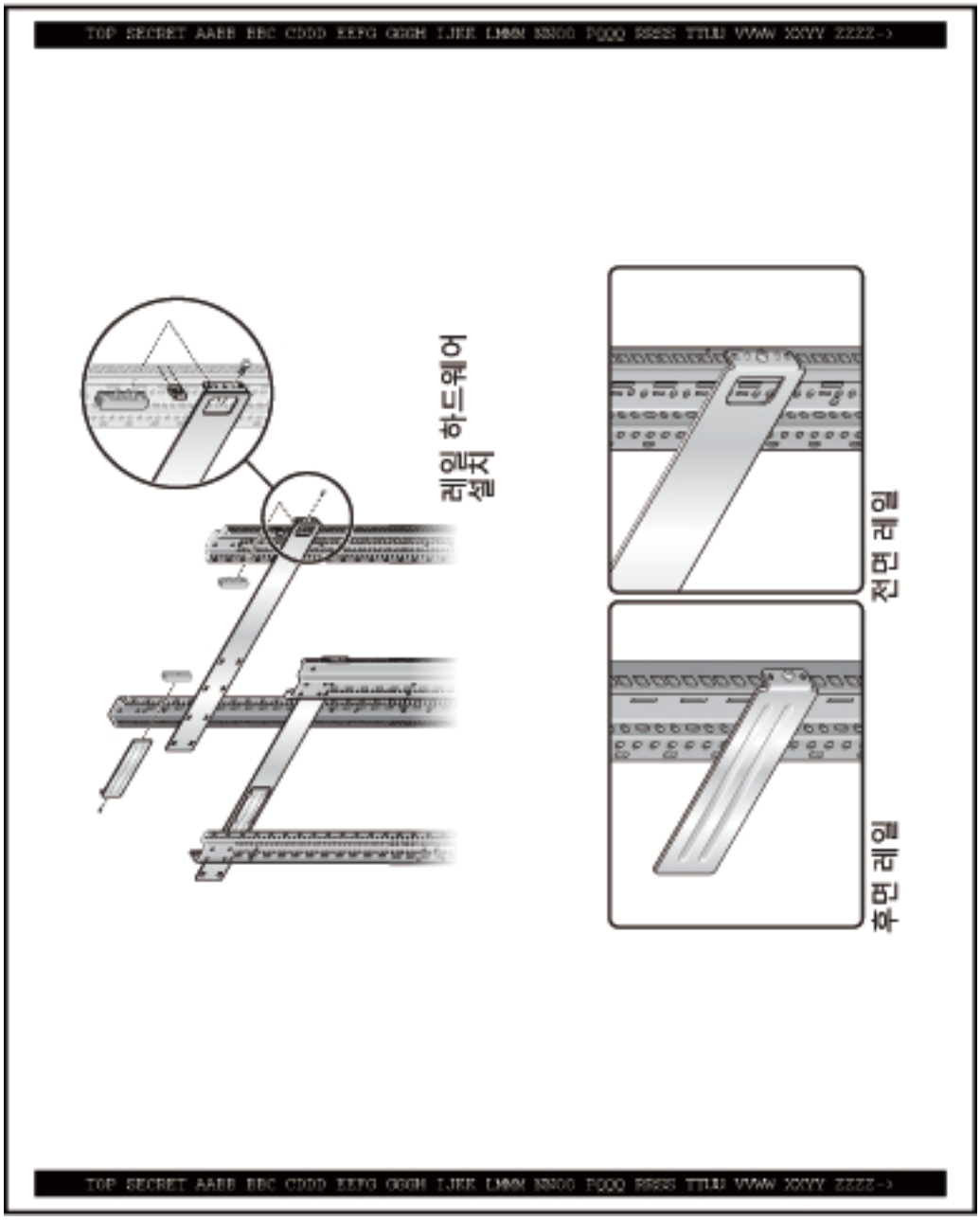
예를 들어 사용자가 `Internal Use Only` 세션에 로그인하면 사용자의 인쇄 작업은 해당 레이블에 있습니다. `label_encodings` 파일의 `minimum protect as` 분류가 `Public`인 경우 `Internal Use Only` 레이블이 본문 페이지에 인쇄됩니다.

그림 19-3 본문 페이지 맨 위와 아래에 인쇄된 작업의 레이블



본문 페이지가 가로 모드로 인쇄될 때 레이블은 세로 모드로 인쇄됩니다. 다음 그림에서는 본문 페이지가 가로 모드로 인쇄되고 Protect As 레이블이 페이지 경계를 넘어 확장됩니다. 레이블은 80자로 잘립니다.

그림 19-4 본문 페이지가 가로 모드로 인쇄될 때 작업의 레이블이 세로 모드로 인쇄



tsol_separator.ps 구성 파일

다음 표에서는 보안 관리자가 /usr/lib/cups/filter/tsol_separator.ps 파일을 수정하여 변경할 수 있는, 신뢰할 수 있는 인쇄의 특성을 보여줍니다.

표 19-2 tsol_separator.ps 파일의 구성 가능한 값

출력	기본값	정의되는 방식	변경 방법
PRINTER BANNERS	/Caveats Job_Caveats	/Caveats Job_Caveats	"Trusted Extensions Label Administration "의 "Specifying Printer Banners"을 참조하십시오.
CHANNELS	/Channels Job_Channels	/Channels Job_Channels	"Trusted Extensions Label Administration "의 "Specifying Channels"을 참조하십시오.
배너 및 트레일러 페이지 맨 위의 레이블	/HeadLabel Job_Protect def	/PageLabel 설명을 참조하십시오.	/PageLabel을 변경하는 것과 동일합니다. "Trusted Extensions Label Administration "의 "Specifying the "Protect As" Classification"을 참조하십시오.
본문 페이지 맨 위와 아래의 레이블	/PageLabel Job_Protect def	작업 레이블을 label_encodings 파일의 minimum protect as classification과 비교합니다. 더 지배적인 분류를 인쇄합니다. 인쇄 작업의 레이블에 구획이 있는 경우 구획을 포함합니다.	/PageLabel 정의를 변경하여 다른 값을 지정합니다. 또는 선택한 문자열을 입력합니다. 또는 아무것도 인쇄하지 않습니다.
"Protect as" 분류 문의 텍스트 및 레이블	/Protect Job_Protect def /Protect_Text1 () def /Protect_Text2 () def	/PageLabel 설명을 참조하십시오. 레이블 위에 표시할 텍스트입니다. 레이블 아래에 표시할 텍스트입니다.	/PageLabel을 변경하는 것과 동일합니다. Protect_Text1 및 Protect_Text2의 ()를 텍스트 문자열로 대체합니다.

보안 정보의 포스트스크립트 인쇄

Trusted Extensions의 레이블이 있는 인쇄는 Oracle Solaris 인쇄 기능에 의존합니다. Oracle Solaris OS에서와 마찬가지로 job-sheets 옵션으로 배너 페이지 생성을 처리합니다. 레이블 지정을 구현하려면 필터를 통해 인쇄 작업을 PostScript 파일로 변환합니다. 그런 다음 포스트스크립트 파일을 조작하여 본문 페이지에 레이블을 삽입하고 배너와 트레일러 페이지를 만듭니다.

참고 - CUPS에서는 PostScript 파일을 변경하지 못합니다. 따라서 지식을 가진 PostScript 프로그래머가 인쇄 출력의 레이블을 수정하는 PostScript 파일을 만들 수 없습니다.

Trusted Extensions 인쇄 인터페이스(참조)

Trusted Extensions에서는 다음 인쇄 권한 부여를 추가하여 Trusted Extensions 보안 정책을 구현합니다. 인쇄 서버에서 이러한 권한 부여를 확인합니다. 따라서 레이블이 있는 영역의 사용자와 같은 원격 사용자는 권한 부여 확인을 통과할 수 없습니다.

- `solaris.print.admin` - 인쇄를 관리하는 역할을 사용으로 설정합니다.
- `solaris.print.list` - 역할에 속하지 않은 인쇄 작업을 보는 역할을 사용으로 설정합니다.
- `solaris.print.nobanner` - 전역 영역에서 배너 및 트레일러 페이지 없이 작업을 인쇄하는 역할을 사용으로 설정합니다.
- `solaris.print.unlabeled` - 전역 영역에서 페이지 레이블 없이 작업을 인쇄하는 역할을 사용으로 설정합니다.

다음과 같은 사용자 명령이 Trusted Extensions 보안 정책에 맞게 확장되었습니다.

- `cancel` - 호출자가 인쇄 작업의 레이블과 동일해야만 작업을 취소할 수 있습니다. 일반 사용자는 자신의 작업만 취소할 수 있습니다.
- `lp` - 레이블 없이 본문 페이지를 인쇄하는 `-o nolabel` 옵션을 사용하려면 `solaris.print.unlabeled` 권한 부여가 필요합니다. 배너나 트레일러 페이지 없이 작업을 인쇄하는 `-o job-sheets=none` 옵션을 사용하려면 `solaris.print.nobanner` 권한 부여가 필요합니다.
- `cancel` - 호출자가 인쇄 작업의 레이블과 동일해야만 작업의 상태를 가져올 수 있습니다. 일반 사용자는 자신의 인쇄 작업만 볼 수 있습니다.

다음과 같은 관리 명령이 Trusted Extensions 보안 정책에 맞게 확장되었습니다. Oracle Solaris OS에서와 마찬가지로 이러한 명령은 Printer Management 권한 프로파일을 포함하는 역할만 실행할 수 있습니다.

- `cancel` - 호출자가 인쇄 작업의 레이블과 동일해야만 작업을 이동할 수 있습니다. 기본적으로 일반 사용자는 자신의 인쇄 작업만 이동할 수 있습니다.
- `lpadmin` - 전역 영역에서 이 명령은 모든 작업에 사용할 수 있습니다. 레이블이 있는 영역에서는 호출자가 인쇄 작업의 레이블을 지배해야만 작업을 볼 수 있고 레이블과 동일해야만 작업을 변경할 수 있습니다.
- `lpsched` - 전역 영역에서 이 명령은 항상 올바로 실행됩니다. Oracle Solaris OS에서와 마찬가지로 `svcadm` 명령을 사용하여 인쇄 서비스를 사용/사용 안함으로 설정하거나, 시작하거나, 다시 시작할 수 있습니다. 레이블이 있는 영역에서는 호출자가 인쇄 서비스의 레이블과 동일해야만 인쇄 서비스를 변경할 수 있습니다. 서비스 관리 기능에 대한 자세한 내용은 `smf`(5), `svcadm`(1M) 및 `svcs`(1) 매뉴얼 페이지를 참조하십시오.

Trusted Extensions에서 인쇄 관리

Oracle Solaris 프린터 설정을 완료한 후 인쇄를 구성하는 Trusted Extensions 절차를 수행합니다. 일부 기본 설정이 이러한 절차에 포함되어 있습니다. 자세한 내용은 "Oracle Solaris

11.2의 인쇄 구성 및 관리 "의 2 장, "CUPS를 사용하여 프린터 설정(작업)"을 참조하십시오. 다음 링크는 레이블이 있는 인쇄를 관리하는 주요 작업을 가리킵니다.

- "레이블이 있는 인쇄 구성" [248]
- "Trusted Extensions에서 인쇄 제한 사항 감소" [254]

레이블이 있는 인쇄 구성

다음 작업 맵은 레이블이 있는 인쇄와 관련된 일반적인 구성 절차를 설명합니다.

표 19-3 레이블이 있는 인쇄 구성 작업 맵

작업	설명	수행 방법
전역 영역에서 인쇄를 구성합니다.	전역 영역에서 다중 레벨 인쇄 서버를 만듭니다.	다중 레벨 인쇄 서버 및 해당 프린터를 구성하는 방법 [248]
네트워크 프린터를 구성합니다.	프린터를 공유합니다.	네트워크 프린터를 구성하는 방법 [250]
레이블이 있는 영역의 인쇄를 구성합니다.	레이블이 있는 영역에 대해 단일 레이블 인쇄 서버를 만듭니다.	영역을 단일 레벨 인쇄 서버로 구성하는 방법 [251]
다중 레벨 인쇄 클라이언트를 구성합니다.	Trusted Extensions 호스트를 프린터에 연결합니다.	Trusted Extensions 클라이언트가 프린터에 액세스할 수 있도록 설정하는 방법 [252]

▼ 다중 레벨 인쇄 서버 및 해당 프린터를 구성하는 방법

Trusted Extensions 인쇄 서버에 연결된 프린터는 본문 페이지, 배너 페이지 및 트레일러 페이지에 레이블을 인쇄합니다. 이러한 프린터는 인쇄 서버의 레이블 범위 내에서 작업을 인쇄할 수 있습니다. 프린터가 공유되는 경우 인쇄 서버에 연결할 수 있는 모든 Trusted Extensions 호스트가 공유 프린터를 사용할 수 있습니다.

시작하기 전에 전역 영역에서 이 인쇄 서버의 시스템 관리자 역할을 가진 사용자여야 합니다.

1. **프린터 제조회사 및 모델명을 확인합니다.**

   ```
   # lpinfo -m | grep printer-manufacturer
   ```

   예를 들어 다음 구문은 모든 Xerox 프린터를 찾습니다.

   ```
   # lpinfo -m | grep Xerox
   gutenprint.5.2://xerox-able_1406/expert Xerox Able 1406 - CUPS+Gutenprint v5.2.4
   gutenprint.5.2://xerox-able_1406/simple Xerox Able 1406 - CUPS+Gutenprint v5.2.4 ...
   gutenprint.5.2://xerox-dc_400/expert Xerox Document Centre 400 - ...
   gutenprint.5.2://xerox-dc_400/simple Xerox Document Centre 400 - ...
   gutenprint.5.2://xerox-dp_4508/expert Xerox DocuPrint 4508 - ...
   ```

```
gutenprint.5.2://xerox-dp_4508/simple Xerox DocuPrint 4508 - ...
...
```

2. **연결된 모든 프린터의 특성을 정의합니다.**

```
# lpadmin -p printer-name -E -v socket://printer-IP-address -m printer-make-and-model
-
```

-E 옵션을 사용하여 이름이 지정된 프린터가 인쇄 요청의 대기열을 수락하도록 할 수 있습니다. 또한 프린터를 활성화하거나 사용으로 설정합니다.

3. **네트워크 프린터를 만들려면 프린터를 공유합니다.**

```
# lpadmin -p printer-name -o printer-is-shared=true
```

다른 시스템에서 프린터를 사용하지 못하게 하려면 이 단계를 건너뜁니다.

4. **프린터 기본값을 표시합니다.**

```
# lpoptions -p printer-name
```

5. **기본값을 조정합니다.**

예를 들어 양면 및 2단을 인쇄할 수 있습니다.

작은 정보 - CUPS 웹 사이트(http://localhost:631)를 사용해서 프린터를 구성할 수 있습니다.

---

6. **레이블이 있는 배너 및 트레일러 페이지로 인쇄 서버에 연결된 각 프린터를 구성합니다.**

```
# lpadmin -p printer-name -o job-sheets=labeled
```

ADMIN_LOW에서 ADMIN_HIGH의 기본 프린터 레이블 범위가 모든 프린터에 대해 허용되면 레이블 구성이 완료됩니다.

7. **인쇄가 허용되는 레이블이 있는 모든 영역에서 프린터를 구성합니다.**

전역 영역에 대해 all-zones IP 주소를 인쇄 서버로 사용합니다.

a. **레이블이 있는 영역의 영역 콘솔에 root로 로그인합니다.**

```
# zlogin -C labeled-zone
```

b. **프린터를 추가합니다.**

```
# lpadmin -p zone-printer-name -E \
-v ipp://global-zone-IP-address/printers/printer-name-in-global-zone
```

c. **(옵션) 이 프린터를 기본 프린터로 설정합니다.**

```
# lpadmin -d zone-printer-name
```

8. **레이블이 있는 모든 영역에서 프린터를 테스트합니다.**

   root 및 일반 사용자로 다음 단계를 수행합니다.

   a. **명령줄에서 텍스트 및 PostScript 파일을 인쇄합니다.**

   ```
   # lp /etc/motd ~/PostScriptTest.ps
   % lp $HOME/file1.txt $HOME/PublicTest.ps
   ```

   b. **메일, Oracle OpenOffice, Adobe Reader 및 브라우저와 같은 응용 프로그램에서 파일을 인쇄합니다.**

   c. **배너 페이지, 트레일러 페이지 및 본문 페이지 레이블이 올바로 인쇄되는지 확인합니다.**

참조
- **레이블이 있는 출력 방지** - "Trusted Extensions에서 인쇄 제한 사항 감소" [254]
- **이 영역을 인쇄 서버로 사용** - Trusted Extensions 클라이언트가 프린터에 액세스할 수 있도록 설정하는 방법 [252]

▼ 네트워크 프린터를 구성하는 방법

프린터가 공유되는 경우 인쇄 서버에 연결할 수 있는 모든 Trusted Extensions 호스트가 공유 프린터를 사용할 수 있습니다.

시작하기 전에 전역 영역에서 이 인쇄 서버의 시스템 관리자 역할을 가진 사용자여야 합니다.

1. **네트워크 프린터의 특성을 정의합니다.**

   1단계의 6단계에서 다중 레벨 인쇄 서버 및 해당 프린터를 구성하는 방법 [248]까지 수행하여 네트워크 프린터를 구성합니다.

   3단계에서 프린터를 공유하면 이 인쇄 서버에 연결할 수 있는 네트워크의 모든 시스템이 이 프린터로 인쇄할 수 있습니다.

2. **네트워크 프린터를 테스트합니다.**

   root 및 일반 사용자로 이 인쇄 서버를 사용하는 시스템에서 다음 단계를 수행합니다.

   a. **명령줄에서 텍스트 및 PostScript 파일을 인쇄합니다.**

   ```
   # lp /etc/motd ~/PostScriptTest.ps
   % lp $HOME/file1.txt $HOME/PublicTest.ps
   ```

   b. **메일, Oracle OpenOffice, Adobe Reader 및 브라우저와 같은 응용 프로그램에서 파일을 인쇄합니다.**

   c. **배너 페이지, 트레일러 페이지 및 본문 페이지 레이블이 올바로 인쇄되는지 확인합니다.**

참조 레이블이 있는 출력을 방지하려면 “Trusted Extensions에서 인쇄 제한 사항 감소” [254]를 참조하십시오.

▼ 영역을 단일 레벨 인쇄 서버로 구성하는 방법

시작하기 전에 영역에서 전역 영역과 IP 주소를 공유하지 않아야 합니다. 전역 영역에서 시스템 관리자 역할을 가진 사용자여야 합니다.

1. **작업 공간을 추가합니다.**
   자세한 내용은 “Trusted Extensions 사용자 설명서 ”의 “최소 레이블에서 작업 공간 추가 방법”을 참조하십시오.

2. **새 작업 공간의 레이블을 해당 레이블의 인쇄 서버가 될 영역의 레이블로 변경합니다.**
   자세한 내용은 “Trusted Extensions 사용자 설명서 ”의 “작업 공간 레이블을 변경하는 방법”을 참조하십시오.

3. **연결된 모든 프린터의 특성을 정의합니다.**
   1단계의 6단계에서 다중 레벨 인쇄 서버 및 해당 프린터를 구성하는 방법 [248]까지 수행하여 영역 프린터를 구성합니다.
   연결된 프린터는 영역의 레이블에서만 작업을 인쇄할 수 있습니다.

4. **프린터를 테스트합니다.**

   참고 - 보안상의 이유로 관리 레이블 `ADMIN_HIGH` 또는 `ADMIN_LOW`가 있는 파일은 인쇄 출력의 본문에 `ADMIN_HIGH`를 인쇄합니다. 배너 및 트레일러 페이지에 `label_encodings` 파일에 있는 최상위 레이블과 구획을 사용하여 레이블이 지정됩니다.

   `root` 및 일반 사용자로 다음 단계를 수행합니다.

   a. **명령줄에서 텍스트 및 PostScript 파일을 인쇄합니다.**

   ```
   # lp /etc/motd ~/PostScriptTest.ps
   % lp $HOME/file1.txt $HOME/PublicTest.ps
   ```

   b. **메일, Oracle OpenOffice, Adobe Reader 및 브라우저와 같은 응용 프로그램에서 파일을 인쇄합니다.**

   c. **배너 페이지, 트레일러 페이지 및 본문 페이지 레이블이 올바로 인쇄되는지 확인합니다.**

참조
- **레이블이 있는 출력 방지** - “Trusted Extensions에서 인쇄 제한 사항 감소” [254]
- **이 영역을 인쇄 서버로 사용** - Trusted Extensions 클라이언트가 프린터에 액세스할 수 있도록 설정하는 방법 [252]

▼ Trusted Extensions 클라이언트가 프린터에 액세스할 수 있도록 설정하는 방법

처음에는 인쇄 서버가 구성된 영역만 해당 인쇄 서버의 프린터에 인쇄할 수 있습니다. 다른 영역 및 시스템에 대해서는 시스템 관리자가 명시적으로 이러한 프린터에 대한 액세스를 추가해야 합니다. 가능한 설정은 다음과 같습니다.

- 전역 영역의 경우 다른 시스템의 전역 영역에 연결되어 있는 공유 프린터에 대한 액세스를 추가합니다.
- 레이블이 있는 영역의 경우 해당 시스템의 전역 영역에 연결되어 있는 공유 프린터에 대한 액세스를 추가합니다.
- 레이블이 있는 영역의 경우 동일한 레이블에 있는 원격 영역에 구성되어 있는 공유 프린터에 대한 액세스를 추가합니다.
- 레이블이 있는 영역의 경우 다른 시스템의 전역 영역에 연결되어 있는 공유 프린터에 대한 액세스를 추가합니다.

시작하기 전에 인쇄 서버를 레이블 범위 또는 단일 레이블로 구성했습니다. 또한 인쇄 서버에 연결된 프린터를 구성하고 공유했습니다. 자세한 내용은 다음을 참조하십시오.

- 다중 레벨 인쇄 서버 및 해당 프린터를 구성하는 방법 [248]
- 영역을 단일 레벨 인쇄 서버로 구성하는 방법 [251]
- 레이블이 없는 인쇄 서버에 레이블을 지정하는 방법 [255]

전역 영역에서 시스템 관리자 역할을 가진 사용자여야 합니다.

1. **프린터를 ping할 수 있는지 확인합니다.**

   ```
   # ping printer-IP-address
   ```

   이 명령이 실패하면 네트워크 연결에 문제가 있는 것입니다. 연결 문제를 해결한 다음 이 절차로 돌아오십시오. 지원 정보는 "신뢰할 수 있는 네트워크 문제 해결" [224]을 참조하십시오.

2. **시스템에서 프린터에 액세스를 사용으로 설정하는 하나 이상의 절차를 완료합니다.**

   - **인쇄 서버가 아닌 시스템에서 전역 영역을 구성하여 프린터 액세스에 다른 시스템의 전역 영역을 사용하도록 합니다.**

     a. **프린터 액세스 권한이 없는 시스템에서 시스템 관리자 역할을 맡습니다.**

     b. **원격 Trusted Extensions 인쇄 서버에 연결된 프린터에 대한 액세스를 추가합니다.**

     ```
     # lpadmin -p printer-name -E \
     -v ipp://print-server-IP-address/printers/printer-name-on-server
     ```

- **레이블이 있는 영역을 구성하여 프린터 액세스에 해당 전역 영역을 사용하도록 합니다.**

  a. **역할 작업 공간의 레이블을 레이블이 있는 영역의 레이블로 변경합니다.**

  자세한 내용은 "Trusted Extensions 사용자 설명서 "의 "작업 공간 레이블을 변경하는 방법"을 참조하십시오.

  b. **프린터에 대한 액세스를 추가합니다.**

```
# lpadmin -p printer-name -E \
-v ipp://print-server-IP-address/printers/printer-name-on-print-server
```

- **레이블이 있는 영역을 구성하여 프린터 액세스에 다른 시스템의 레이블이 있는 영역을 사용하도록 합니다.**

  영역의 레이블이 동일해야 합니다.

  a. **프린터 액세스 권한이 없는 시스템에서 시스템 관리자 역할을 맡습니다.**

  b. **역할 작업 공간의 레이블을 레이블이 있는 영역의 레이블로 변경합니다.**

  c. **레이블이 있는 원격 영역의 인쇄 서버에 연결된 프린터에 대한 액세스를 추가합니다.**

```
# lpadmin -p printer-name -E \
-v ipp://zone-print-server-IP-address/printers/printer-name-on-zone-print-server
```

- **레이블이 없는 인쇄 서버를 사용하여 보안 정보 없이 출력을 인쇄하도록 레이블이 있는 영역을 구성합니다.**

  자세한 내용은 레이블이 없는 인쇄 서버에 레이블을 지정하는 방법 [255]을 참조하십시오.

3. **프린터를 테스트합니다.**

참고 - 보안상 이유로 `ADMIN_HIGH` 또는 `ADMIN_LOW` 관리 레이블이 있는 파일은 인쇄 출력의 본문 페이지에 `ADMIN_HIGH`를 인쇄합니다. 배너 및 트레일러 페이지에 `label_encodings` 파일에 있는 최상위 레이블과 구획을 사용하여 레이블이 지정됩니다.

모든 클라이언트에서 전역 영역에 액세스할 수 있는 모든 계정 및 레이블이 있는 영역에 액세스할 수 있는 모든 계정에 대해 인쇄가 작동하는지 테스트합니다.

a. **명령줄에서 텍스트 및 PostScript 파일을 인쇄합니다.**

```
# lp /etc/motd ~/PostScriptTest.ps
% lp $HOME/file1.txt $HOME/PublicTest.ps
```

b. **메일, Oracle OpenOffice, Adobe Reader 및 브라우저와 같은 응용 프로그램에서 파일을 인쇄합니다.**

c. **배너 페이지, 트레일러 페이지 및 본문 페이지 레이블이 올바로 인쇄되는지 확인합니다.**

Trusted Extensions에서 인쇄 제한 사항 감소

다음 작업은 선택 사항입니다. 이러한 작업은 Trusted Extensions가 제공하는 인쇄 보안 위험을 줄여줍니다.

표 19-4 Trusted Extensions에서 인쇄 제한 축소 작업 맵

작업	설명	수행 방법
레이블을 출력하지 않도록 프린터를 구성합니다.	전역 영역의 인쇄 출력에서 보안 정보가 인쇄되지 않게 합니다.	배너 및 트레일러 페이지를 제거하는 방법 [254]
레이블이 있는 출력 없이 단일 레이블에서 프린터를 구성합니다.	사용자가 특정 레이블에서 인쇄할 수 있도록 설정합니다. 인쇄 작업이 레이블을 사용하여 표시되지 않습니다.	레이블이 없는 인쇄 서버에 레이블을 지정하는 방법 [255]
본문 페이지에 표시되는 레이블을 제거합니다.	레이블이 없는 인쇄 서버로 인쇄합니다. 레이블 지정을 억제하는 인쇄 권한 부여를 지정합니다.	레이블이 없는 인쇄 서버에 레이블을 지정하는 방법 [255] 특정 사용자 및 역할이 레이블 지정 인쇄된 출력을 우회할 수 있도록 설정하는 방법 [256]
배너 및 트레일러 페이지를 억제합니다.	배너 및 트레일러 페이지를 제거하여 이러한 페이지의 추가 보안 정보를 제거합니다.	배너 및 트레일러 페이지를 제거하는 방법 [254]
인쇄 권한 부여를 지정합니다.	특정 사용자 및 역할에 레이블 없이 작업을 인쇄하는 권한을 부여합니다.	특정 사용자 및 역할이 레이블 지정 인쇄된 출력을 우회할 수 있도록 설정하는 방법 [256]

▼ 배너 및 트레일러 페이지를 제거하는 방법

`job-sheets` 옵션을 `none`으로 설정한 프린터는 배너 또는 트레일러 페이지를 인쇄하지 않습니다.

시작하기 전에 전역 영역에서 보안 관리자 역할을 가진 사용자여야 합니다.

- **적절한 레이블에서 배너 또는 트레일러 페이지 없이 프린터를 구성합니다.**

```
# lpadmin -p print-server-IP-address -o job-sheets=none,none
```

또는 `none`을 한 번 지정할 수 있습니다.

```
# lpadmin -p print-server-IP-address -o job-sheets=none
```

본문 페이지에는 여전히 레이블이 있습니다. 본문 페이지에서 레이블을 제거하려면 특정 사용자 및 역할이 레이블 지정 인쇄된 출력을 우회할 수 있도록 설정하는 방법 [256]을 참조하십시오.

▼ 레이블이 없는 인쇄 서버에 레이블을 지정하는 방법

Oracle Solaris 인쇄 서버에 레이블을 지정하면 Trusted Extensions 시스템이 해당 레이블에서 프린터에 액세스할 수 있습니다. 지정된 레이블에서 작업이 레이블 없이 인쇄됩니다. 작업이 배너 페이지와 함께 인쇄되는 경우 해당 페이지에는 보안 정보가 포함되지 않습니다.

레이블이 없는 인쇄 서버에서 관리되는 프린터에 작업을 보내도록 Trusted Extensions 시스템을 구성할 수 있습니다. 사용자는 지정된 레이블에서 레이블이 없는 프린터에 작업을 인쇄할 수 있습니다.

시작하기 전에 전역 영역에서 보안 관리자 역할을 가진 사용자여야 합니다.

1. **레이블이 없는 템플리트를 인쇄 서버에 지정합니다.**

   자세한 내용은 호스트를 보안 템플리트에 추가하는 방법 [205]을 참조하십시오.

   레이블이 없는 템플리트에서 인쇄 서버에 지정한 레이블에서 작업하는 사용자는 해당 레이블에서 Oracle Solaris 프린터에 인쇄 작업을 보낼 수 있습니다.

2. **프린터 액세스 권한이 없는 시스템에서 시스템 관리자 역할을 맡습니다.**

3. **역할 작업 공간의 레이블을 레이블이 있는 영역의 레이블로 변경합니다.**

   자세한 내용은 "Trusted Extensions 사용자 설명서 "의 "작업 공간 레이블을 변경하는 방법"을 참조하십시오.

4. **임의의 레이블이 있는 인쇄 서버에 연결된 프린터에 대한 액세스를 추가합니다.**

   ```
   # lpadmin -p printer-name -E \
   -v ipp://print-server-IP-address/printers/printer-name-on-print-server
   ```

예 19-1 레이블이 없는 프린터에 공용 인쇄 작업 보내기

일반 대중이 사용할 수 있는 파일은 레이블이 없는 프린터에서 인쇄하기에 적합합니다. 이 예에서는 마케팅 담당자가 페이지의 맨 위와 맨 아래에 레이블을 인쇄하지 않는 문서를 생성하려고 합니다.

보안 관리자가 레이블이 없는 호스트 유형 템플리트를 Oracle Solaris 인쇄 서버에 지정합니다. 템플리트는 신뢰할 수 없는 네트워크에서 터널을 구성하는 방법 [222]에 설명되어 있습니다. 이 템플리트의 임의의 레이블은 PUBLIC입니다. 프린터 pr-nolabel1이 이 인쇄 서버에

연결되어 있습니다. PUBLIC 영역 사용자의 인쇄 작업이 pr-nolabel1 프린터에서 레이블 없이 인쇄됩니다. 프린터 설정에 따라 작업에 배너 페이지가 포함되거나 포함되지 않을 수 있습니다. 배너 페이지에는 보안 정보가 포함되지 않습니다.

▼ 특정 사용자 및 역할이 레이블 지정 인쇄된 출력을 우회할 수 있도록 설정하는 방법

사용자 및 역할이 레이블 없이 작업을 인쇄할 수 있도록 하려면 보안 관리자의 권한 부여와 인쇄 작업을 제출할 때 권한이 부여된 사용자나 역할 측에서의 작업이 필요합니다.

시작하기 전에 전역 영역에서 보안 관리자 역할을 가진 사용자여야 합니다.

1. **사용자 또는 역할에 인쇄 권한 부여를 지정합니다.**

   - **사용자 또는 역할이 배너와 트레일러 페이지에서 레이블을 제거할 수 있도록 설정하려면 `solaris.print.nobanner` 권한 부여를 지정합니다.**

     ```
     # usermod -A +solaris.print.nobanner username
     ```

     ```
     # rolemod -A +solaris.print.nobanner rolename
     ```

   - **사용자 또는 역할이 본문 페이지에서 레이블을 제거할 수 있도록 설정하려면 `solaris.print.unlabeled` 권한 부여를 지정합니다.**

     ```
     # usermod -A +solaris.print.unlabeled username
     ```

     ```
     # rolemod -A +solaris.print.unlabeled rolename
     ```

   - **사용자 또는 역할이 인쇄 출력에서 모든 레이블을 제거할 수 있도록 설정하려면 두 권한 부여를 모두 지정합니다.**

     ```
     # usermod -A +solaris.print.unlabeled,+solaris.print.nobanner username
     ```

     ```
     # rolemod -A +solaris.print.unlabeled,+solaris.print.nobanner rolename
     ```

2. **레이블이 없는 출력 인쇄를 준비합니다.**

   프린터가 로컬인지 확인합니다.

   사용자에게 이는 해당 영역의 인쇄 서버가 있는 레이블이 있는 영역에서 인쇄해야 함을 의미합니다. 역할은 전역 영역 또는 레이블이 있는 영역에서 인쇄할 수 있습니다.

3. **레이블이 없는 출력을 인쇄하려면 명령줄에서 레이블을 제거하는 옵션을 지정합니다.**

   레이블이 없는 출력을 인쇄할 권한이 있어야 합니다.

   - **배너 없이 인쇄하려면 `job-sheets=none` 옵션을 사용합니다.**

```
# lp -o job-sheets=none file
```

- **본문 페이지에 레이블 없이 인쇄하려면 `nolabel` 옵션을 사용합니다.**

  ```
  # lp -o nolabels file
  ```

- **출력에 레이블 없이 인쇄하려면 두 옵션을 모두 사용합니다.**

  ```
  # lp -o job-sheets=none -o nolabels file
  ```

♦ ♦ ♦ 20 장

20 Trusted Extensions의 장치 정보

이 장에서는 Trusted Extensions 시스템의 주변 장치 보호에 대해 설명합니다.

Trusted Extensions 소프트웨어로 장치 보호

Oracle Solaris 시스템에서는 할당과 권한 부여로 장치를 보호할 수 있습니다. 기본적으로 일반 사용자가 권한 부여 없이 장치를 사용할 수 있습니다. Trusted Extensions 기능으로 구성된 시스템에서는 Oracle Solaris OS의 장치 보호 방식을 사용합니다.

그러나 기본적으로 Trusted Extensions에서는 사용할 장치를 할당해야 하며 사용자는 장치를 사용할 수 있게 권한 부여되어야 합니다. 또한 장치는 레이블로 보호됩니다. Trusted Extensions에서는 관리자가 장치를 관리하는 데 사용할 수 있는 그래픽 사용자 인터페이스(GUI)를 제공합니다. 사용자가 장치를 할당하는 데도 동일할 인터페이스가 사용됩니다.

참고 - Trusted Extensions에서는 사용자가 `allocate` 및 `deallocate` 명령을 사용할 수 없습니다. 사용자는 Device Manager(장치 할당 관리자)를 사용해야 합니다.

Oracle Solaris의 장치 보호에 대한 자세한 내용은 “Oracle Solaris 11.2에서 시스템 및 연결된 장치의 보안 ”의 4 장, “장치에 대한 액세스 제어”를 참조하십시오.

Trusted Extensions로 구성된 시스템에서는 두 역할이 장치를 보호합니다.

- 시스템 관리자 역할은 주변 기기에 대한 액세스를 제어합니다.

  시스템 관리자는 장치를 할당 가능으로 설정합니다. 시스템 관리자가 할당 불가능으로 설정하는 장치는 누구도 사용할 수 없습니다. 할당 가능한 장치는 권한 부여된 사용자만이 할당할 수 있습니다.
- 보안 관리자 역할은 장치에 액세스할 수 있는 레이블을 제한하고 장치 정책을 설정합니다. 보안 관리자는 장치를 할당할 수 있게 권한 부여된 사용자를 결정합니다.

다음은 Trusted Extensions 소프트웨어를 사용한 주요 장치 제어 기능입니다.

- 기본적으로 Trusted Extensions 시스템에서 권한이 부여되지 않은 사용자는 테이프 드라이브, CD-ROM 드라이브 또는 디스켓 드라이브 등의 장치를 할당할 수 없습니다.

  Allocate Device(장치 할당) 권한이 있는 일반 사용자는 장치를 할당하는 레이블의 정보를 가져오거나 내보낼 수 있습니다.
- 사용자가 직접 로그인한 경우 Device Allocation Manager(장치 할당 관리자)를 사용하여 장치를 할당합니다. 사용자가 원격으로 장치를 할당하려면 전역 영역에 액세스할 수 있어야 합니다. 일반적으로 역할만 전역 영역에 액세스할 수 있습니다.
- 각 장치의 레이블 범위는 보안 관리자가 제한할 수 있습니다. 일반 사용자는 레이블 범위에 해당 사용자가 작업할 수 있는 레이블이 포함된 장치에만 액세스할 수 있습니다. 장치의 기본 레이블 범위는 `ADMIN_LOW ~ ADMIN_HIGH`입니다.
- 할당 가능한 장치와 할당 불가능한 장치 모두에 대해 레이블 범위를 제한할 수 있습니다. 할당 불가능한 장치는 프레임 버퍼와 포인터 등의 장치입니다.

장치 레이블 범위

사용자가 민감한 정보를 복사하지 못하도록 할당 가능한 장치마다 레이블 범위가 있습니다. 할당 가능한 장치를 사용하려면 사용자가 해당 장치의 레이블 범위 내에 있는 레이블에서 작업 중이어야 합니다. 그렇지 않으면 할당이 거부됩니다. 장치가 사용자에게 할당된 동안 가져오거나 내보내는 데이터에는 사용자의 현재 레이블이 적용됩니다. 장치 할당이 해제될 때 내보낸 데이터의 레이블이 표시됩니다. 사용자가 내보낸 데이터가 들어 있는 매체에 물리적인 표시를 해야 합니다.

장치의 레이블 범위 효과

콘솔을 통해 직접 로그인 액세스를 제한하려면 보안 관리자가 프레임 버퍼에 제한된 레이블 범위를 설정합니다.

예를 들어, 제한된 레이블 범위를 지정하여 공용으로 액세스 가능한 시스템으로 액세스를 제한할 수 있습니다. 레이블 범위는 사용자가 프레임 버퍼의 레이블 범위 내에 있는 레이블의 시스템에만 액세스할 수 있게 합니다.

호스트에 로컬 프린터가 있는 경우 프린터의 제한된 레이블 범위에 의해 해당 프린터에서 인쇄할 수 있는 작업이 제한됩니다.

장치 액세스 정책

Trusted Extensions는 Oracle Solaris와 동일한 장치 정책을 따릅니다. 보안 관리자가 기본 정책을 변경하고 새 정책을 정의할 수 있습니다. `getdevpolicy` 명령은 장치 정책에 대

한 정보를 검색하고 update_drv 명령은 장치 정책을 변경합니다. 자세한 내용은 “Oracle Solaris 11.2에서 시스템 및 연결된 장치의 보안 ”의 “장치 정책 구성”을 참조하십시오. getdevpolicy(1M) 및 update_drv(1M) 매뉴얼 페이지도 참조하십시오.

Device-Clean 스크립트

device-clean 스크립트는 장치가 할당되거나 할당 해제될 때 실행됩니다. Oracle Solaris에서는 테이프 드라이브 및 CD-ROM 드라이브에 대한 스크립트를 제공합니다. 사이트에서 시스템에 할당 가능한 장치 유형을 추가할 경우 추가된 장치에 스크립트가 필요할 수 있습니다. 기존 스크립트를 보려면 /etc/security/lib 디렉토리로 이동합니다. 자세한 내용은 “Oracle Solaris 11.2에서 시스템 및 연결된 장치의 보안 ”의 “Device-Clean 스크립트”를 참조하십시오.

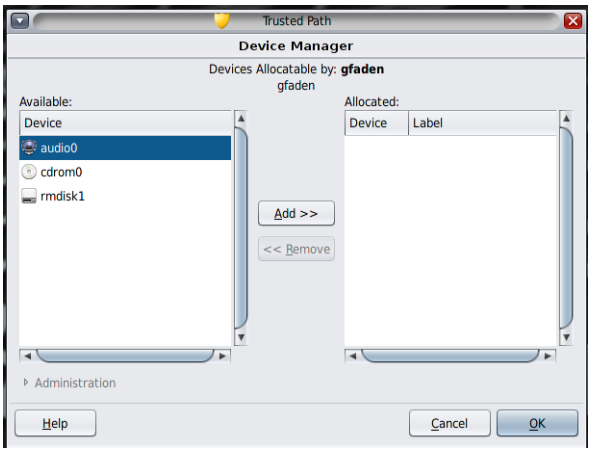
Trusted Extensions 소프트웨어의 경우에는 device-clean 스크립트가 특정 요구 사항을 충족해야 합니다. 이러한 요구 사항은 device_clean(5) 매뉴얼 페이지에 설명되어 있습니다.

장치 관리자 GUI

Device Manager(장치 할당 관리자)는 관리자가 할당 가능한 장치와 할당 불가능한 장치를 관리하는 데 사용됩니다. 일반 사용자가 장치를 할당하고 할당 해제하는 데도 Device Manager(장치 할당 관리자)가 사용됩니다. 사용자에게 장치 할당 권한이 있어야 합니다.

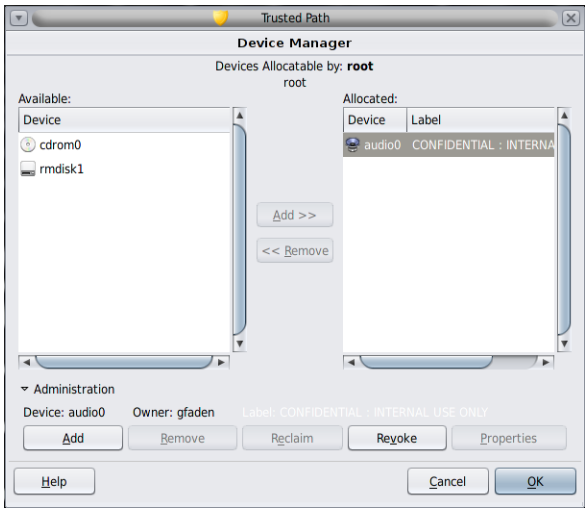
GUI를 Device Manager(장치 할당 관리자)라고 합니다. Trusted Path(신뢰할 수 있는 경로) 메뉴에서 Allocate Device(장치 할당)를 선택하여 이 GUI를 시작합니다. 다음 그림은 audio 장치를 할당할 수 있는 사용자가 열어 놓은 Device Manager(장치 할당 관리자)를 보여줍니다.

그림 20-1 사용자가 열어 놓은 Device Manager(장치 할당 관리자)



장치를 할당할 수 있게 권한 부여되지 않은 사용자의 경우 빈 목록이 표시됩니다. 할당 가능한 장치가 현재 다른 사용자에 의해 할당되거나 오류 상태일 때도 빈 목록이 표시됩니다. Available Devices(사용 가능한 장치) 목록에 장치가 표시되지 않는 경우 담당 관리자에게 문의해야 합니다.

Device Administration(장치 관리) 기능은 장치 관리에 필요한 권한 부여가 하나 이상 있는 역할만 사용할 수 있습니다. 관리 권한 부여는 Configure Device Attributes(장치 속성 구성)와 Revoke or Reclaim Device(장치 해지 또는 재생 이용)입니다. 다음 그림은 Device Allocation Administration(장치 할당 관리) 대화 상자를 보여줍니다.



Trusted Extensions에서 장치 보안 적용

보안 관리자가 장치를 할당할 수 있는 사용자를 결정하고, 장치를 사용할 수 있게 권한 부여된 사용자가 교육을 받았는지 확인합니다. 이러한 사용자는 다음을 수행할 수 있는 것으로 간주됩니다.

- 민감한 정보를 내보낸 경우 다른 사용자가 무단으로 보지 못하도록 해당 정보가 들어 있는 매체에 적절히 라벨을 붙이고 매체를 처리할 수 있습니다.

  예를 들어, `NEED TO KNOW ENGINEERING` 레이블의 정보가 CD에 저장된 경우 이 정보를 내보내는 사용자는 디스크에 직접 `NEED TO KNOW ENGINEERING` 레이블로 표시해야 합니다. CD는 해당 엔지니어링 그룹의 구성원만 액세스할 수 있는 곳에 보관해야 합니다.
- 이러한 장치의 매체에서 가져오거나 읽는 모든 정보에 대해 레이블을 적절히 유지 관리해야 합니다.

  권한 부여된 사용자는 가져오는 정보의 레이블과 일치하는 레이블의 장치를 할당해야 합니다. 예를 들어, 사용자가 `PUBLIC`의 CD-ROM 드라이브를 할당하는 경우 사용자는 `PUBLIC`이라는 레이블의 정보만 가져와야 합니다.

보안 관리자는 이러한 보안 요구 사항을 준수하게 하는 역할도 담당합니다.

Trusted Extensions의 장치(참조)

Trusted Extensions 장치 보호에서는 Oracle Solaris 인터페이스와 Trusted Extensions 인터페이스를 사용합니다.

Oracle Solaris 명령줄 인터페이스에 대해서는 “Oracle Solaris 11.2에서 시스템 및 연결된 장치의 보안 ”의 “장치 보호 참조”를 참조하십시오.

Device Allocation Manager(장치 할당 관리자)에 액세스할 수 없는 관리자는 명령줄을 사용하여 할당 가능한 장치를 관리할 수 있습니다. `allocate` 및 `deallocate` 명령에는 관리 옵션이 있습니다. 예제는 “Oracle Solaris 11.2에서 시스템 및 연결된 장치의 보안 ”의 “장치를 강제로 할당하는 방법” 및 “Oracle Solaris 11.2에서 시스템 및 연결된 장치의 보안 ”의 “장치를 강제로 할당 해제하는 방법”을 참조하십시오.

Trusted Extensions 명령줄 인터페이스는 `add_allocatable`(1M) 및 `remove_allocatable`(1M) 매뉴얼 페이지를 참조하십시오.

♦ ♦ ♦ 21 장

21 Trusted Extensions에 대한 장치 관리

이 장에서는 Trusted Extensions로 구성된 시스템에서 장치를 관리하고 사용하는 방법을 설명합니다.

Trusted Extensions에서 장치 취급

다음 작업 맵에서는 관리자 및 사용자가 주변 기기를 취급하기 위한 작업 맵에 대한 링크를 제공합니다.

표 21-1 Trusted Extensions에서 장치 취급 작업 맵

작업	설명	수행 방법
장치를 사용합니다.	역할이나 일반 사용자로 장치를 사용합니다.	"Trusted Extensions에서 장치 사용 작업 맵" [265]
장치를 관리합니다.	일반 사용자에 대해 장치를 구성합니다.	"Trusted Extensions에서 장치 관리" [266]
장치 권한 부여를 사용자 정의합니다.	보안 관리자 역할은 새 장치 권한 부여를 만들어 장치에 추가한 후 권한 프로파일에 넣고 이 프로파일을 사용자에게 지정합니다.	"Trusted Extensions에서 장치 권한 부여 사용자 정의" [273]

Trusted Extensions에서 장치 사용 작업 맵

Trusted Extensions의 모든 역할은 장치를 할당할 수 있게 권한 부여됩니다. 사용자와 같이 역할도 Device Manager(장치 할당 관리자)를 사용해야 합니다. Oracle Solaris

`allocate` 명령은 Trusted Extensions에서 작동하지 않습니다. 다음 작업 맵에서는 Trusted Extensions에서 장치 사용을 위한 사용자 절차에 대한 링크를 제공합니다.

표 21-2 Trusted Extensions에서 장치 사용 작업 맵

작업	수행 방법
장치를 할당하고 할당 해제합니다.	"Trusted Extensions 사용자 설명서 "의 "Trusted Extensions에서 장치를 할당하는 방법"
휴대용 매체를 사용하여 파일을 전송합니다.	Trusted Extensions에서 이동식 매체의 파일을 복사하는 방법 [69] Trusted Extensions에서 이동식 매체에 파일을 복사하는 방법 [68]

Trusted Extensions에서 장치 관리

다음 작업 맵에서는 사이트에서 장치를 보호하는 절차를 설명합니다.

표 21-3 Trusted Extensions에서 장치 관리 작업 맵

작업	설명	수행 방법
장치 정책을 설정하거나 수정합니다.	장치에 액세스하는 데 필요한 권한을 변경합니다.	"Oracle Solaris 11.2에서 시스템 및 연결된 장치의 보안 "의 "장치 정책 구성"
장치를 할당할 수 있는 권한 부여를 사용자에게 부여합니다.	보안 관리자 역할은 Allocate Device(장치 할당) 권한이 있는 권한 프로파일을 사용자에게 지정합니다.	"Oracle Solaris 11.2에서 시스템 및 연결된 장치의 보안 "의 "장치를 할당할 수 있도록 사용자에게 권한을 부여하는 방법"
	보안 관리자 역할은 사이트별 권한이 있는 프로파일을 사용자에게 지정합니다.	"Trusted Extensions에서 장치 권한 부여 사용자 정의" [273]
장치를 구성합니다.	장치를 보호하기 위한 보안 기능을 선택합니다.	Trusted Extensions에서 장치 관리자를 사용하여 장치를 구성하는 방법 [267]
장치를 해지하거나 재생 이용합니다.	Device Manager(장치 할당 관리자)로 장치를 사용할 수 있게 만듭니다.	Trusted Extensions에서 장치를 해지하거나 재생 이용하는 방법 [270]
	Oracle Solaris 명령으로 장치를 사용할 수 있게 만들거나 사용할 수 없게 만듭니다.	"Oracle Solaris 11.2에서 시스템 및 연결된 장치의 보안 "의 "장치를 강제로 할당하는 방법" "Oracle Solaris 11.2에서 시스템 및 연결된 장치의 보안 "의 "장치를 강제로 할당 해제하는 방법"
할당 가능한 장치에 대한 액세스를 금지합니다.	장치에 대한 세분화된 액세스 제어를 제공합니다.	예 21-2. "세분화된 장치 권한 부여 만들기"
	할당 가능한 장치에 대한 모든 사용자의 액세스를 거부합니다.	예 21-1. "오디오 장치의 원격 할당 금지"
프린터와 프레임 버퍼를 보호합니다.	할당 불가능한 장치를 할당할 수 없게 합니다.	Trusted Extensions에서 할당 불가능한 장치를 보호하는 방법 [271]
새 device-clean 스크립트를 사용합니다.	적당한 위치에 새 스크립트를 넣습니다.	Trusted Extensions에서 Device_Clean 스크립트를 추가하는 방법 [272]

▼ Trusted Extensions에서 장치 관리자를 사용하여 장치를 구성하는 방법

기본적으로 할당 가능한 장치는 ADMIN_LOW ~ ADMIN_HIGH의 레이블 범위를 가지며 사용하도록 할당되어야 합니다. 또한 장치를 할당할 수 있는 권한 부여가 사용자에게 있어야 합니다. 이러한 기본값은 윈도우화 시스템에서 변경할 수 있습니다. 데스크탑이 없는 시스템에서는 전역 영역의 역할만 할당 가능한 장치를 구성 및 사용할 수 있습니다.

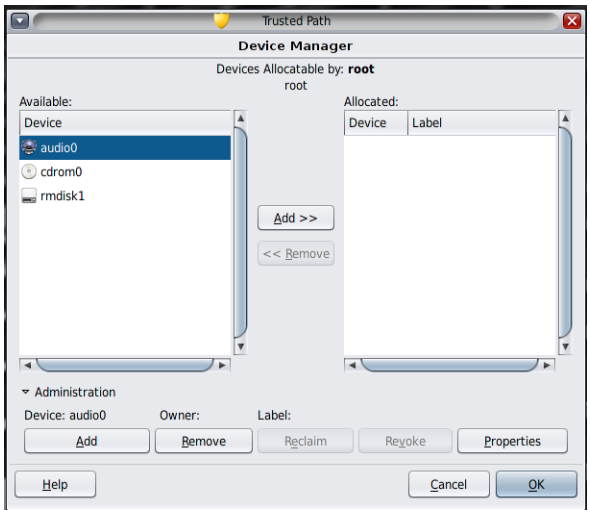
윈도우화 시스템에서는 다음과 같은 장치를 사용하도록 할당할 수 있습니다.

- audio*n* - 마이크로폰 및 스피커를 나타냅니다.
- cdrom*n* - CD-ROM 드라이브를 나타냅니다.
- mag_tape*n* - 테이프 드라이브(스트리밍)를 나타냅니다.
- rmdisk*n* - 이동식 디스크(예: JAZ 또는 ZIP 드라이브) 또는 USB 핫플러그 가능 매체를 나타냅니다.

시작하기 전에 전역 영역에서 보안 관리자 역할을 가진 사용자여야 합니다.

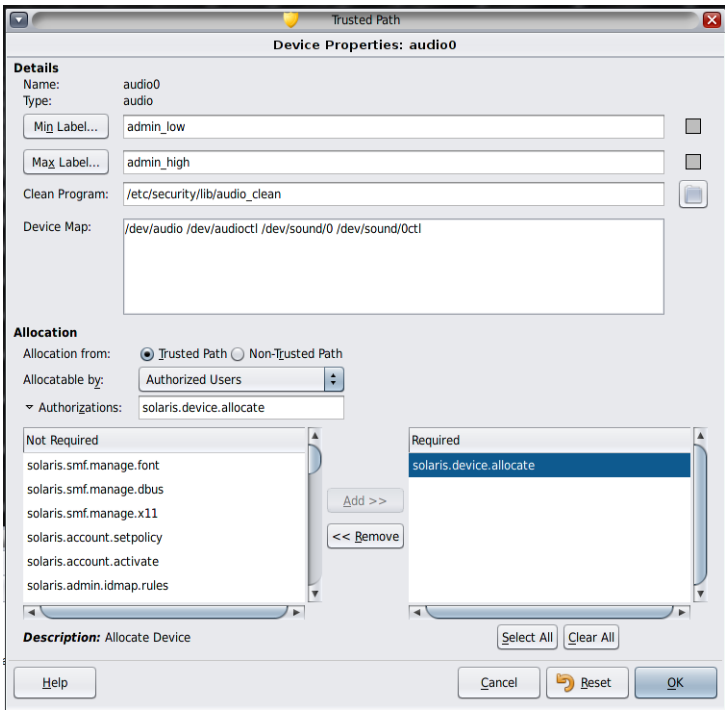
1. **Trusted Path(신뢰할 수 있는 경로) 메뉴에서 Allocate Device(장치 할당)를 선택합니다.**

   Device Manager(장치 할당 관리자)가 나타납니다.



2. **기본 보안 설정을 확인합니다.**

   Administration(장치 관리)을 누르고 장치를 강조 표시합니다. 다음 그림은 root 역할이 보고 있는 오디오 장치를 보여줍니다.



3. **(옵션) 장치의 레이블 범위를 제한합니다.**

   a. **최소 레이블을 설정합니다.**

      Min Label(최소 레이블) 버튼을 누릅니다. 레이블 구축기에서 최소 레이블을 선택합니다. 레이블 구축기에 대한 자세한 내용은 "Trusted Extensions의 레이블 구축기" [101]를 참조하십시오.

   b. **최대 레이블을 설정합니다.**

      Max Label(최대 레이블)... 버튼을 누릅니다. 레이블 구축기에서 최대 레이블을 선택합니다.

4. **장치를 로컬로 할당할 수 있는지 여부를 지정합니다.**

   Device Configuration(장치 할당 구성) 대화 상자의 For Allocations From Trusted Path(신뢰할 수 있는 경로에서 할당)에 있는 Allocatable By(가능한 할당자) 목록에서 옵션을 선택합니다. 기본적으로 Authorized Users(권한 부여된 사용자) 옵션이 선택되어 있습니다. 따라서 장치는 할당 가능하며 사용자가 권한 부여되어야 합니다.

   ■ **장치를 할당할 수 없게 하려면 No Users(사용자 없음)를 누릅니다.**

할당할 수 없어야 하는 프레임 버퍼 또는 기타 장치를 구성할 때 No Users(사용자 없음)를 선택합니다.

참고 - 프린터는 할당하도록 구성할 수 없습니다.

- **권한 부여 없이도 장치를 할당할 수 있게 하려면 All Users(모든 사용자)를 누릅니다.**

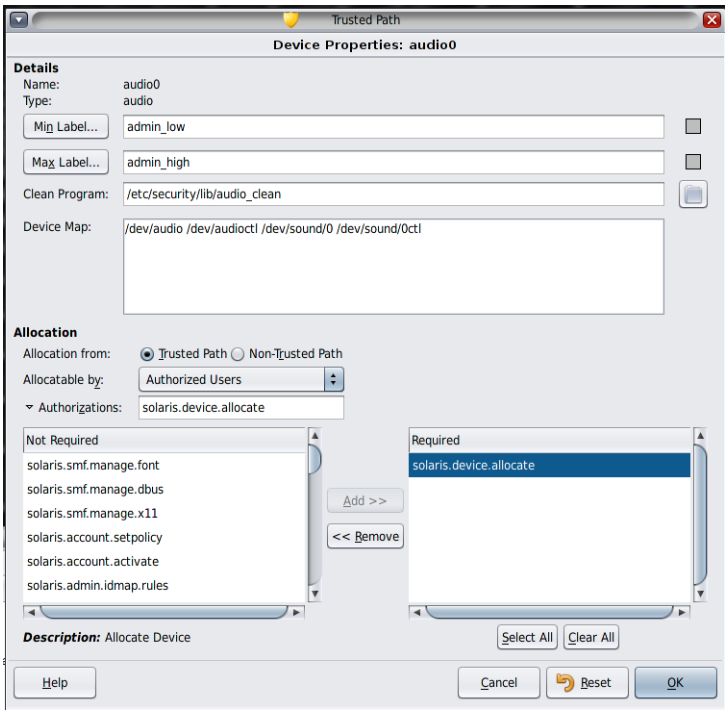
5. **장치를 원격으로 할당할 수 있는지 여부를 지정합니다.**

   For Allocations From Non-Trusted Path(신뢰할 수 없는 경로에서 할당) 구역에 있는 Allocatable By(가능한 할당자) 목록에서 옵션을 선택합니다. 기본적으로 Same As Trusted Path(신뢰할 수 있는 경로와 같음) 옵션이 선택되어 있습니다.

   - **사용자 권한 부여가 필요하도록 하려면 Allocatable by Authorized Users(권한 부여된 사용자가 할당 가능)를 선택합니다.**
   - **원격 사용자가 장치를 할당할 수 없게 하려면 No Users(사용자 없음)를 선택합니다.**
   - **누구나 장치를 할당할 수 있게 하려면 All Users(모든 사용자)를 선택합니다.**

6. **장치를 할당할 수** 있고 **사이트에서 새 장치 권한 부여를 만든 경우 적당한 권한 부여를 선택합니다.**

   다음 대화 상자는 `cdrom0` 장치를 할당하려면 `solaris.device.allocate` 권한 부여가 필요함을 나타냅니다.



사이트별 장치 권한 부여를 만들고 사용하려면 "Trusted Extensions에서 장치 권한 부여 사용자 정의" [273]를 참조하십시오.

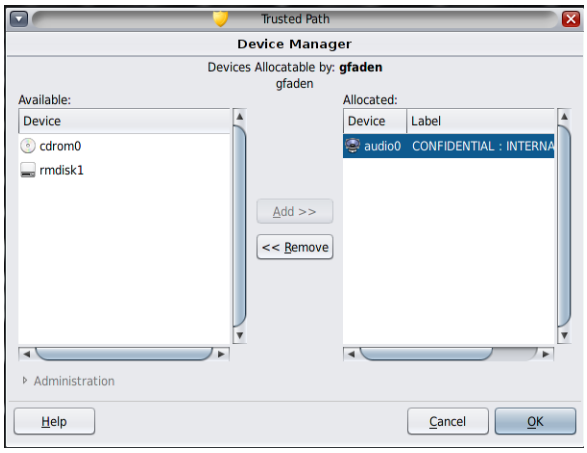
7. **변경 사항을 저장하려면 OK(확인)를 누릅니다.**

▼ Trusted Extensions에서 장치를 해지하거나 재생 이용하는 방법

장치가 Device Manager(장치 할당 관리자)에 나열되지 않을 경우 이미 할당되었거나 할당 오류 상태일 수 있습니다. 시스템 관리자는 사용할 장치를 복구할 수 있습니다.

시작하기 전에 전역 영역에서 시스템 관리자 역할을 가진 사용자여야 합니다. 이 역할에는 `solaris.device.revoke` 권한 부여가 포함됩니다.

1. **Trusted Path(신뢰할 수 있는 경로) 메뉴에서 Allocate Device(장치 할당)를 선택합니다.**
   다음 그림에서는 오디오 장치가 이미 사용자에게 할당되었습니다.



2. **Administration(장치 관리) 버튼을 누릅니다.**

3. **장치의 상태를 확인합니다.**
   장치 이름을 선택하고 State(상태) 필드를 확인합니다.

   - **State(상태) 필드가 Allocate Error State(할당 오류 상태)인 경우 Reclaim(재생 이용) 버튼을 누릅니다.**
   - **State(상태) 필드가 Allocated(할당됨)인 경우 다음 중 하나를 수행합니다.**
     - **Owner(소유자) 필드의 사용자에게 장치를 할당 해제하도록 요청합니다.**
     - **Revoke(해지) 버튼을 눌러 장치를 강제로 할당 해제합니다.**

4. **Device Manager(장치 할당 관리자)를 닫습니다.**

▼ Trusted Extensions에서 할당 불가능한 장치를 보호하는 방법

Device Configuration(장치 구성) 대화 상자의 Allocatable By(가능한 할당자) 구역에 있는 No Users(사용자 없음) 옵션은 사용을 위해 할당할 필요가 없는 프레임 버퍼와 프린터에 가장 자주 사용됩니다.

시작하기 전에 전역 영역에서 보안 관리자 역할을 가진 사용자여야 합니다.

1. **Trusted Path(신뢰할 수 있는 경로) 메뉴에서 Allocate Device(장치 할당)를 선택합니다.**
2. **Device Manager(장치 할당 관리자)에서 Administration(장치 관리) 버튼을 누릅니다.**
3. **새 프린터나 프레임 버퍼를 선택합니다.**

   a. **장치를 할당할 수 없게 하려면 No Users(사용자 없음)를 누릅니다.**

   b. **(옵션) 장치의 레이블 범위를 제한합니다.**

      i. **최소 레이블을 설정합니다.**
      Min Label(최소 레이블)... 버튼을 누릅니다. 레이블 구축기에서 최소 레이블을 선택합니다. 레이블 구축기에 대한 자세한 내용은 "Trusted Extensions의 레이블 구축기" [101]를 참조하십시오.

      ii. **최대 레이블을 설정합니다.**
      Max Label(최대 레이블)... 버튼을 누릅니다. 레이블 구축기에서 최대 레이블을 선택합니다.

예 21-1 오디오 장치의 원격 할당 금지

Allocatable By(가능한 할당자) 섹션의 No Users(사용자 없음) 옵션은 원격 사용자가 원격 시스템 주변의 대화를 들을 수 없도록 합니다.

보안 관리자는 Device Manager(장치 할당 관리자)에서 오디오 장치를 다음과 같이 구성합니다.

```
Device Name: audio
For Allocations From: Trusted Path
Allocatable By: Authorized Users
Authorizations: solaris.device.allocate

Device Name: audio
For Allocations From: Non-Trusted Pathh
Allocatable By: No Users
```

▼ Trusted Extensions에서 Device_Clean 스크립트를 추가하는 방법

장치가 만들어질 때 `device_clean` 스크립트를 지정하지 않을 경우 기본 스크립트인 `/bin/true`가 사용됩니다.

시작하기 전에 물리적 장치에서 사용 가능한 데이터를 모두 비우고 성공 시 `0`을 반환하는 스크립트를 준비합니다. 휴대용 매체가 있는 장치의 경우 사용자가 매체를 꺼내지 않으면 스크립트에서 매체

꺼내기를 시도합니다. 매체가 꺼내지지 않을 경우 스크립트는 장치를 할당 오류 상태로 설정합니다. 요구 사항에 대한 자세한 내용은 device_clean(5) 매뉴얼 페이지를 참조하십시오.

전역 영역에서 root 역할을 가진 사용자여야 합니다.

1. **스크립트를 /etc/security/lib 디렉토리에 복사합니다.**
2. **Device Properties(장치 등록 정보) 대화 상자에서 스크립트의 전체 경로를 지정합니다.**
   a. **Device Manager(장치 할당 관리자)를 엽니다.**
   b. **Administration(장치 관리) 버튼을 누릅니다.**
   c. **장치의 이름을 선택하고 Configure(구성) 버튼을 누릅니다.**
   d. **Clean Program(정리 프로그램) 필드에 스크립트의 전체 경로를 지정합니다.**
3. **변경 사항을 저장합니다.**

Trusted Extensions에서 장치 권한 부여 사용자 정의

다음 작업 맵에서는 사이트에서 장치 권한 부여를 변경하는 절차를 설명합니다.

표 21-4 Trusted Extensions에서 장치 권한 부여 사용자 정의 작업 맵

작업	설명	수행 방법
새 장치 권한 부여를 만듭니다.	사이트별 권한 부여를 만듭니다.	새 장치 권한 부여를 만드는 방법 [273]
장치에 권한 부여를 추가합니다.	선택한 장치에 사이트별 권한 부여를 추가합니다.	Trusted Extensions에서 장치에 사이트별 권한 부여를 추가하는 방법 [277]
사용자와 역할에 장치 권한 부여를 지정합니다.	사용자와 역할이 새 권한 부여를 사용할 수 있도록 합니다.	장치 권한 부여를 지정하는 방법 [277]

▼ 새 장치 권한 부여를 만드는 방법

장치에 권한 부여가 필요하지 않은 경우 기본적으로 모든 사용자가 장치를 사용할 수 있습니다. 권한 부여가 필요한 경우에는 기본적으로 권한이 부여된 사용자만 장치를 사용할 수 있습니다.

할당 가능한 장치에 대한 모든 액세스를 거부하려면 예 21-1. “오디오 장치의 원격 할당 금지”을 참조하십시오. 새 권한 부여를 만들고 사용하려면 예 21-3. “신뢰할 수 있는 경로 및 신뢰할 수 없는 경로 장치 권한 부여 만들기 및 지정”을 참조하십시오.

시작하기 전에 전역 영역에서 보안 관리자 역할을 가진 사용자여야 합니다.

1. **(옵션) 각 새 장치 권한 부여에 대한 도움말 파일을 만듭니다.**

   도움말 파일은 HTML 형식입니다. 이름 지정 규약은 *AuthName*`.html`(예: `DeviceAllocateCD.html`)입니다.

2. **장치 권한 부여를 만듭니다.**

   ```
   # auths add -t "Authorization description" -h /full/path/to/helpfile.html authorization-name
   ```

3. **적절한 권한 프로파일에 새 권한 부여를 추가합니다.**

   ```
   # profiles rights-profile
   profiles:rights-profile > add auths="authorization-name"...
   ```

4. **프로파일을 사용자와 역할에 지정합니다.**

   ```
   # usermod -P "rights-profile" username
   # rolemod -P "rights-profile" rolename
   ```

5. **권한 부여를 사용하여 선택한 장치에 대한 액세스를 제한합니다.**

   Device Manager(장치 할당 관리자)에서 필수 권한 부여 목록에 새 권한 부여를 추가합니다. 절차는 Trusted Extensions에서 장치에 사이트별 권한 부여를 추가하는 방법 [277]을 참조하십시오.

예 21-2 세분화된 장치 권한 부여 만들기

이 예에서는 NewCo의 보안 관리자가 회사를 위한 세분화된 장치 권한 부여를 만들어야 합니다.

먼저 관리자는 다음 도움말 파일을 만듭니다.

```
Newco.html
NewcoDevAllocateCDVD.html
NewcoDevAllocateUSB.html
```

그런 다음 관리자는 템플리트 도움말 파일을 만듭니다. 이 파일을 복사하고 수정하여 다른 도움말 파일을 만들 수 있습니다.

```
<HTML>
-- Copyright 2012 Newco.  All rights reserved.
-- NewcoDevAllocateCDVD.html
-->
```

```
<HEAD>
<TITLE>Newco Allocate CD or DVD Authorization</TITLE>
</HEAD>
<BODY>
The com.newco.dev.allocate.cdvd authorization enables you to allocate the
CD drive on your system for your exclusive use.
<p>
The use of this authorization by a user other than the authorized account
is a security violation.
<p>
</BODY>
</HTML>
```

도움말 파일을 만든 후 관리자는 `auths` 명령을 사용하여 각 장치 권한 부여를 만듭니다. 권한 부여는 회사 전체에서 사용되므로 관리자는 권한 부여를 LDAP 저장소에 둡니다. 이 명령에는 도움말 파일의 경로 이름이 포함됩니다.

관리자는 두 개의 장치 권한 부여와 Newco 권한 부여 헤더를 만듭니다.

- 한 권한 부여는 사용자에게 CD-ROM 또는 DVD 드라이브를 할당할 수 있는 권한을 부여합니다.

  ```
  # auths add -S ldap -t "Allocate CD or DVD" \
    -h /docs/helps/NewcoDevAllocateCDVD.html com.newco.dev.allocate.cdvd
  ```

- 다른 권한 부여는 사용자에게 USB 장치를 할당할 수 있는 권한을 부여합니다.

  ```
  # auths add -S ldap -t "Allocate USB" \
    -h /docs/helps/NewcoDevAllocateUSB.html com.newco.dev.allocate.usb
  ```

- Newco 권한 부여 헤더는 모든 Newco 권한 부여를 식별합니다.

  ```
  # auths add -S ldap -t "Newco Auth Header" \
    -h /docs/helps/Newco.html com.newco
  ```

예 21-3 신뢰할 수 있는 경로 및 신뢰할 수 없는 경로 장치 권한 부여 만들기 및 지정

기본적으로 Allocate Devices(장치 할당) 권한 부여를 통해 신뢰할 수 있는 경로와 그 외부에서 할당을 사용으로 설정합니다.

다음 예의 사이트 보안 정책에서는 원격 CD-ROM 및 DVD 할당 제한을 요구합니다. 보안 관리자는 `com.newco.dev.allocate.cdvd.local` 권한 부여를 만듭니다. 이 권한 부여는 신뢰할 수 있는 경로를 사용하여 할당되는 CD-ROM 및 DVD 드라이브용입니다. `com.newco.dev.allocate.cdvd.remote` 권한 부여는 신뢰할 수 있는 경로 외부에서 CD-ROM 또는 DVD 드라이브를 할당할 수 있는 일부 사용자용입니다.

보안 관리자는 도움말 파일을 만든 후 장치 권한 부여를 `auth_attr` 데이터베이스에 추가하고 권한 부여를 장치에 추가한 다음 권한 부여를 권한 프로파일에 넣습니다. `root` 역할은 장치를 할당할 수 있는 사용자에게 프로파일을 지정합니다.

- 다음 명령은 장치 권한 부여를 `auth_attr` 데이터베이스에 추가합니다.

```
# auths add -S ldap -t "Allocate Local DVD or CD" \
  -h /docs/helps/NewcoDevAllocateCDVDLocal.html \
  com.newco.dev.allocate.cdvd.local
# auths add -S ldap -t "Allocate Remote DVD or CD" \
  -h /docs/helps/NewcoDevAllocateCDVDRemote.html \
  com.newco.dev.allocate.cdvd.remote
```

- 다음은 Device Manager(장치 관리자) 지정을 보여줍니다.

  CD-ROM 드라이브의 로컬 할당은 신뢰할 수 있는 경로로 보호됩니다.

  ```
  Device Name: cdrom_0
  For Allocations From: Trusted Path
  Allocatable By: Authorized Users
  Authorizations: com.newco.dev.allocate.cdvd.local
  ```

  원격 할당은 신뢰할 수 있는 경로로 보호되지 않으므로 원격 사용자는 신뢰할 수 있어야 합니다. 마지막 단계로 관리자는 원격 할당 권한을 두 역할에만 부여합니다.

  ```
  Device Name: cdrom_0
  For Allocations From: Non-Trusted Path
  Allocatable By: Authorized Users
  Authorizations: com.newco.dev.allocate.cdvd.remote
  ```

- 다음 명령은 이러한 권한 부여에 대한 Newco 권한 프로파일을 만들고 권한 부여를 프로파일에 추가합니다.

  ```
  # profiles -S ldap "Remote Allocator"
  profiles:Remote Allocator > set desc="Allocate Remote CDs and DVDs"
  profiles:Remote Allocator > set help="/docs/helps/NewcoDevRemoteCDVD.html"
  profiles:Remote Allocator > add auths="com.newco.dev.allocate.cdvd.remote"
  profiles:Remote Allocator > end
  profiles:Remote Allocator > exit

  # profiles -S ldap "Local Only Allocator"
  profiles:Local Only Allocator > set desc="Allocate Local CDs and DVDs"
  profiles:Local Only Allocator > set help="/docs/helps/NewcoDevLocalCDVD.html"
  profiles:Local Only Allocator > add auths="com.newco.dev.allocate.cdvd.local"
  profiles:Local Only Allocator > end
  profiles:Local Only Allocator > exit
  ```

- 다음 명령은 권한이 부여된 사용자에게 권한 프로파일을 지정합니다. `root` 역할은 프로파일을 지정합니다. 이 사이트에서 역할에만 주변 장치를 원격으로 할당할 수 있는 권한이 부여됩니다.

  ```
  # usermod -P "Local Only Allocator" jdoe
  # usermod -P "Local Only Allocator" kdoe

  # rolemod -P "Remote Allocator" secadmin
  # rolemod -P "Remote Allocator" sysadmin
  ```

▼ Trusted Extensions에서 장치에 사이트별 권한 부여를 추가하는 방법

시작하기 전에 보안 관리자 역할이나 장치 속성 구성 권한 부여를 포함하는 역할을 가진 사용자여야 합니다. 새 장치 권한 부여를 만드는 방법 [273]에 설명된 대로 사이트별 권한 부여를 만들어 놓아야 합니다.

1. **Trusted Extensions에서 장치 관리자를 사용하여 장치를 구성하는 방법 [267] 절차를 따릅니다.**
   a. **새 권한 부여로 보호해야 하는 장치를 선택합니다.**
   b. **Administration(장치 관리) 버튼을 누릅니다.**
   c. **Authorizations(권한 부여) 버튼을 누릅니다.**
      새 권한 부여가 Not Required(필수 아님) 목록에 표시됩니다.
   d. **새 권한 부여를 Required(필수) 권한 부여 목록에 추가합니다.**
2. **변경 사항을 저장하려면 OK(확인)를 누릅니다.**

▼ 장치 권한 부여를 지정하는 방법

Allocate Device(장치 할당) 권한 부여를 통해 사용자는 장치를 할당할 수 있습니다. Allocate Device(장치 할당) 권한 부여와 Revoke or Reclaim Device(장치 해지 또는 재생 이용) 권한 부여는 관리 역할에 적합합니다.

시작하기 전에 전역 영역에서 보안 관리자 역할을 가진 사용자여야 합니다.

기존 프로파일이 적당하지 않은 경우 보안 관리자는 새 프로파일을 만들 수 있습니다. 예는 편리한 권한 부여를 위해 권한 프로파일을 만드는 방법 [136]을 참조하십시오.

- **Allocate Device(장치 할당) 권한 부여가 포함된 권한 프로파일을 사용자에게 할당합니다.**
  단계별 절차는 “Oracle Solaris 11.2의 사용자 및 프로세스 보안 ”의 “사용자에게 권한 지정”을 참조하십시오.
  다음 권한 프로파일을 통해 역할이 장치를 할당하도록 설정할 수 있습니다.
  - 모든 권한 부여
  - 장치 관리
  - 매체 백업
  - 객체 레이블 관리

- 소프트웨어 설치

다음 권한 프로파일을 통해 역할이 장치를 해지하거나 재생을 사용할 수 있습니다.

- 모든 권한 부여
- 장치 관리

다음 권한 프로파일을 통해 역할이 장치를 만들거나 구성할 수 있습니다.

- 모든 권한 부여
- 장치 보안

예 21-2. “세분화된 장치 권한 부여 만들기”에서는 권한 부여를 지정하는 방법을 보여줍니다.

♦ ♦ ♦ 22 장

22 Trusted Extensions와 감사

이 장에서는 Trusted Extensions에서 제공하는 감사에 추가된 기능에 대해 설명합니다.

Trusted Extensions의 감사

Trusted Extensions 소프트웨어로 구성된 시스템의 감사는 Oracle Solaris 시스템의 감사와 유사하게 구성되고 관리됩니다. 그러나 다음과 같은 몇 가지 차이점이 있습니다.

- Trusted Extensions 소프트웨어는 시스템에 감사 클래스, 감사 이벤트, 감사 토큰 및 감사 정책 옵션을 추가합니다.
- 사전 영역 감사는 레이블이 있는 영역에서 `root` 계정이 필요하므로 권장되지 않습니다.
- Trusted Extensions에서는 시스템 관리자와 보안 관리자라는 두 가지 역할로 감사를 구성하고 관리합니다.

  보안 관리자는 감사 대상 및 사이트별 이벤트와 클래스 간 매핑을 계획합니다. 시스템 관리자는 감사 파일에 대한 디스크 공간 요구 사항을 계획하고, 감사 관리 서버를 만들며, 감사 로그를 검토합니다.

Trusted Extensions에서 역할로 감사 관리

Trusted Extensions의 감사에는 Oracle Solaris OS의 감사와 동일한 계획이 필요합니다. 계획에 대한 자세한 내용은 “Oracle Solaris 11.2의 감사 관리 ”의 2 장, “감사 계획”을 참조하십시오.

감사 관리를 위한 역할 책임

Trusted Extensions에서는 여러 역할이 감사를 담당합니다.

- `root` 역할은 사용자 및 권한 프로파일에 감사 플래그를 지정하고, `audit_warn` 스크립트와 같은 시스템 파일을 편집합니다.
- 시스템 관리자 역할은 감사 저장소의 디스크와 네트워크를 설정하며, 감사 레코드도 검토할 수 있습니다.
- 보안 관리자 역할은 감사 대상을 결정하고 감사를 구성합니다. 초기 설정 팀은 Trusted Extensions에서 보안 관리자 역할을 만드는 방법 [55]을 완료하여 이 역할을 만들었습니다.

참고 - 시스템은 보안 관리자가 미리 선택한 감사 클래스의 이벤트만 기록합니다. 따라서 후속 감사 검토에서는 기록된 이벤트만 고려할 수 있습니다. 이를 잘못 구성하면 시스템 보안을 침해하려는 시도가 감지되지 않거나 이를 시도한 사용자를 관리자가 찾아낼 수 없습니다. 관리자는 정기적으로 감사 증적을 분석하여 보안 침해가 있는지 확인해야 합니다.

Trusted Extensions의 감사 작업

Trusted Extensions의 감사를 구성하고 관리하는 절차는 Oracle Solaris 절차와 약간 다릅니다. Trusted Extensions에서 감사 구성은 전역 영역에서 수행됩니다. 사전 영역 감사가 구성되지 않으므로 사용자 작업은 전역 영역과 레이블이 있는 영역에서 동일하게 감사됩니다. 모든 감사된 이벤트의 레이블은 감사 레코드에 포함됩니다.

- 보안 관리자는 Trusted Extensions, `windata_down` 및 `windata_up`에 해당하는 감사 정책을 선택할 수 있습니다.
- 감사 레코드를 검토할 때 시스템 관리자는 레이블로 감사 레코드를 선택할 수 있습니다. 자세한 내용은 `auditreduce`(1M) 매뉴얼 페이지를 참조하십시오.

Trusted Extensions 감사 참조

Trusted Extensions 소프트웨어는 Oracle Solaris에 감사 클래스, 감사 이벤트, 감사 토큰 및 감사 정책 옵션을 추가합니다. 몇 가지 감사 명령이 레이블을 처리하도록 확장되었습니다. 다음 그림은 일반적인 Trusted Extensions 커널 감사 레코드 및 사용자 레벨 감사 레코드를 보여줍니다.

그림 22-1 레이블이 있는 시스템의 일반적인 감사 레코드 구조

Trusted Extensions 감사 클래스

Trusted Extensions는 X 창 감사 클래스를 Oracle Solaris에 추가합니다. 클래스는 `/etc/security/audit_class` 파일에 나열되어 있습니다. 감사 클래스에 대한 자세한 내용은 `audit_class`(4) 매뉴얼 페이지를 참조하십시오.

다음 조건에 따라 X 서버 감사 이벤트가 이들 클래스에 매핑됩니다.

- **xa** - 이 클래스는 X 서버에 대한 액세스(즉, X 클라이언트 연결 및 X 클라이언트 연결 해제)를 감사합니다.
- **xc** - 이 클래스는 서버 객체 만들기나 삭제에 대해 감사합니다. 예를 들어, 이 클래스는 `CreateWindow()`를 감사합니다.
- **xp** - 이 클래스는 권한 사용에 대해 감사합니다. 권한 사용은 성공 또는 실패일 수 있습니다. 예를 들어, 클라이언트가 다른 클라이언트 창의 속성을 변경하려고 하면 `ChangeWindowAttributes()`가 감사됩니다. 이 클래스에는 `SetAccessControl()` 등의 관리 루틴도 포함됩니다.
- **xs** - 이 클래스는 보안 속성으로 인한 오류 발생 시 클라이언트에게 이에 대한 X 오류 메시지를 반환하지 않는 루틴을 감사합니다. 예를 들어, `GetImage()`는 권한이 부족하여 창에서 읽을 수 없는 경우 `BadWindow` 오류를 반환하지 않습니다.

  이러한 이벤트는 성공 시에만 감사하도록 선택해야 합니다. 실패에 대해 `xs` 이벤트를 감사하도록 선택하면 감사 증적이 관계없는 레코드로 채워집니다.
- **xx** - 이 클래스에는 모든 X 감사 클래스가 포함됩니다.

Trusted Extensions 감사 이벤트

Trusted Extensions 소프트웨어에서 시스템에 감사 이벤트를 추가합니다. 새로운 감사 이벤트와 해당 이벤트가 속한 감사 클래스는 `/etc/security/audit_event` 파일에 나열되어 있습니다. Trusted Extensions에 대한 감사 이벤트 번호는 9000에서 10000 사이입니다. 감사 이벤트에 대한 자세한 내용은 `audit_event`(4) 매뉴얼 페이지를 참조하십시오.

Trusted Extensions 감사 토큰

다음 표에는 Trusted Extensions 소프트웨어에서 Oracle Solaris에 추가하는 감사 토큰이 사전순으로 나열되어 있습니다. 토큰 정의는 `audit.log`(4) 매뉴얼 페이지에 나열되어 있습니다.

표 22-1 Trusted Extensions 감사 토큰

토큰 이름	설명
"`label` 토큰" [282]	민감도 레이블
"`xatom` 토큰" [282]	X 창 기본 단위 식별
"`xcolormap` 토큰" [283]	X 창 색상 정보
"`xcursor` 토큰" [283]	X 창 커서 정보
"`xfont` 토큰" [283]	X 창 글꼴 정보
"`xgc` 토큰" [283]	X 창 그래픽 문맥 정보
"`xpixmap` 토큰" [284]	X 창 픽셀 매핑 정보
"`xproperty` 토큰" [284]	X 창 등록 정보 정보
"`xselect` 토큰" [284]	X 창 데이터 정보
"`xwindow` 토큰" [284]	X 창의 창 정보

`label` 토큰

`label` 토큰에는 민감도 레이블이 있습니다.

`label` 토큰은 다음과 같이 `praudit -x` 명령으로 표시됩니다.

```
<sensitivity_label>ADMIN_LOW</sensitivity_label>
```

`xatom` 토큰

`xatom` 토큰은 X 기본 단위를 식별합니다.

xatom 토큰은 다음과 같이 praudit로 표시됩니다.

```
X atom,_DT_SAVE_MODE
```

xcolormap 토큰

xcolormap 토큰에는 X 서버 식별자 및 작성자의 사용자 ID를 포함하여 컬러 맵의 사용에 대한 정보가 포함됩니다.

xcolormap 토큰은 다음과 같이 praudit로 표시됩니다.

```
<X_colormap xid="0x08c00005" xcreator-uid="srv"/>
```

xcursor 토큰

xcursor 토큰에는 X 서버 식별자 및 작성자의 사용자 ID를 포함하여 커서 사용에 대한 정보가 포함됩니다.

xcursor 토큰은 다음과 같이 praudit로 표시됩니다.

```
X cursor,0x0f400006,srv
```

xfont 토큰

xfont 토큰에는 X 서버 식별자 및 작성자의 사용자 ID를 포함하여 글꼴 사용에 대한 정보가 포함됩니다.

xfont 토큰은 다음과 같이 praudit로 표시됩니다.

```
<X_font xid="0x08c00001" xcreator-uid="srv"/>
```

xgc 토큰

xgc 토큰에는 X 창의 그래픽 컨텍스트에 대한 정보가 포함됩니다.

xgc 토큰은 다음과 같이 praudit로 표시됩니다.

```
Xgraphic context,0x002f2ca0,srv

<X_graphic_context xid="0x30002804" xcreator-uid="srv"/>
```

xpixmap 토큰

xpixmap 토큰에는 X 서버 식별자 및 작성자의 사용자 ID를 포함하여 픽셀 매핑의 사용에 대한 정보가 포함됩니다.

xpixmap 토큰은 다음과 같이 praudit -x로 표시됩니다.

```
<X_pixmap xid="0x2f002004" xcreator-uid="srv"/>
```

xproperty 토큰

xproperty 토큰에는 X 서버 식별자, 작성자의 사용자 ID 및 기본 단위 식별자와 같은 창의 다양한 등록 정보에 대한 정보가 포함됩니다.

xproperty 토큰은 다음과 같이 praudit로 표시됩니다.

```
X_property,0x000075d5,root,_MOTIF_DEFAULT_BINDINGS
```

xselect 토큰

xselect 토큰에는 창 간에 이동되는 데이터가 포함됩니다. 이 데이터는 간주할 내부 구조와 등록 정보 문자열이 없는 바이트 스트림입니다.

xselect 토큰은 다음과 같이 praudit로 표시됩니다.

```
X selection,entryfield,halogen
```

xwindow 토큰

xwindow 토큰은 X 서버 및 작성자의 사용자 ID를 식별합니다.

xwindow 토큰은 다음과 같이 praudit로 표시됩니다.

```
<X_window xid="0x07400001" xcreator-uid="srv"/>
```

Trusted Extensions 감사 정책 옵션

Trusted Extensions는 기존 감사 정책 옵션에 두 가지 창 감사 정책 옵션을 추가합니다.

```
# auditconfig -lspolicy
```

```
...
windata_down Include downgraded window information in audit records
windata_up   Include upgraded window information in audit records
...
```

Trusted Extensions의 감사 명령에 대한 확장

Trusted Extensions 정보를 처리하도록 `auditconfig`, `auditreduce` 및 `auditrecord` 명령이 확장되었습니다.

- `auditconfig` 명령에 Trusted Extensions 감사 정책이 포함됩니다. 자세한 내용은 `auditconfig`(1M) 매뉴얼 페이지를 참조하십시오.
- `auditreduce` 명령이 레이블로 레코드 필터링을 위한 `-l` 옵션을 추가합니다. 자세한 내용은 `auditreduce`(1M) 매뉴얼 페이지를 참조하십시오.
- `auditrecord` 명령에 Trusted Extensions 감사 이벤트가 포함됩니다.

♦ ♦ ♦ 23 장

23 Trusted Extensions에서 소프트웨어 관리

이 장에서는 Trusted Extensions 시스템에서 타사 소프트웨어를 신뢰할 수 있는 방법으로 실행하는 방법을 설명합니다.

Trusted Extensions에 소프트웨어 추가

Oracle Solaris 시스템에 추가할 수 있는 모든 소프트웨어는 Trusted Extensions를 사용하여 구성된 시스템에 추가할 수 있습니다. 또한 Trusted Extensions API를 사용하는 프로그램도 추가할 수 있습니다. Trusted Extensions 시스템에 소프트웨어를 추가하는 방법은 비전역 영역을 실행 중인 Oracle Solaris 시스템에 소프트웨어를 추가하는 방법과 비슷합니다.

Trusted Extensions에서 프로그램은 일반적으로 레이블이 있는 영역에서 일반 사용자가 사용하도록 전역 영역에 설치됩니다. 그러나 영역에서 `pkg` 명령을 실행하여 레이블이 있는 영역에 패키지를 설치할 수 있습니다. 이렇게 하는 경우 영역에서 관리 계정 및 암호 프롬프트를 설치할 수 있는지 확인해야 합니다. 자세한 내용은 “레이블이 있는 영역으로 제한된 응용 프로그램” [23]을 참조하십시오. 패키지 및 영역에 대한 자세한 내용은 “Oracle Solaris 영역 만들기 및 사용 ”의 9 장, “영역이 설치된 Oracle Solaris 11.2 시스템의 자동 설치 및 패키지 정보”를 참조하십시오.

Trusted Extensions 사이트에서 시스템 관리자와 보안 관리자가 함께 작업하여 소프트웨어를 설치합니다. 보안 관리자는 소프트웨어 추가가 보안 정책을 준수하는지 평가합니다. 소프트웨어 사용에 권한 또는 권한 부여가 필요한 경우 보안 관리자 역할은 해당 소프트웨어 사용자에게 적절한 권한 프로파일을 지정합니다.

이동식 매체에서 소프트웨어를 가져오려면 권한 부여가 필요합니다. Allocate Device(장치 할당) 권한이 있는 계정은 이동식 매체에서 데이터를 가져오거나 내보낼 수 있습니다. 데이터는 실행 코드를 포함할 수 있습니다. 일반 사용자는 사용자의 클리어런스 내에 있는 레이블에서만 데이터를 가져올 수 있습니다.

시스템 관리자 역할은 보안 관리자가 승인한 프로그램을 추가할 책임이 있습니다.

Oracle Solaris 소프트웨어에 대한 보안 방식

Trusted Extensions는 Oracle Solaris와 동일한 보안 방식을 사용합니다. 방식에는 다음이 포함됩니다.

- **권한 부여** - 프로그램 사용자에게 특정 권한 부여가 요구될 수 있습니다. 권한 부여에 대한 자세한 내용은 "Oracle Solaris 11.2의 사용자 및 프로세스 보안 "의 "사용자 및 프로세스 권한의 기본 사항"을 참조하십시오. 또한 `auth_attr`(4) 매뉴얼 페이지를 참조하십시오.
- **권한** - 프로그램 및 프로세스에 권한이 지정될 수 있습니다. 권한에 대한 자세한 내용은 "Oracle Solaris 11.2의 사용자 및 프로세스 보안 "의 1 장, "권한을 사용하여 사용자 및 프로세스 제어 정보"를 참조하십시오. 또한 `privileges`(5) 매뉴얼 페이지를 참조하십시오.

  `ppriv` 명령은 디버깅 유틸리티를 제공합니다. 자세한 내용은 `ppriv`(1) 매뉴얼 페이지를 참조하십시오. 비전역 영역에서 작동하는 프로그램에 이 유틸리티를 사용하는 방법에 대한 자세한 내용은 "Oracle Solaris 영역 만들기 및 사용 "의 "ppriv 유틸리티 사용"을 참조하십시오.
- **권한 프로파일** - 권한 프로파일은 한 곳에서 사용자 또는 역할에 지정할 보안 속성을 수집합니다. 권한 프로파일에 대한 자세한 내용은 "Oracle Solaris 11.2의 사용자 및 프로세스 보안 "의 "권한 프로파일에 대한 추가 정보"를 참조하십시오.
- **신뢰할 수 있는 라이브러리** - `setuid`, `setgid` 및 권한 있는 프로그램에서 사용하는 동적 공유 라이브러리는 신뢰할 수 있는 디렉토리에서만 로드할 수 있습니다. Oracle Solaris에서와 마찬가지로 `crle` 명령은 신뢰할 수 있는 디렉토리 목록에 권한 있는 프로그램의 공유 라이브러리 디렉토리를 추가하는 데 사용됩니다. 자세한 내용은 `crle`(1) 매뉴얼 페이지를 참조하십시오.

소프트웨어의 보안 평가

소프트웨어에 권한이 지정되거나 소프트웨어를 대체 사용자 ID 또는 그룹 ID로 실행하면 신뢰할 수 있는 소프트웨어가 됩니다. 신뢰할 수 있는 소프트웨어는 Trusted Extensions 보안 정책을 무시할 수 있습니다. 소프트웨어를 신뢰할 만하지 않은 경우에도 신뢰할 수 있는 소프트웨어로 지정할 수 있습니다. 보안 관리자는 세부 조사를 통해 소프트웨어에서 신뢰할 수 있는 방법으로 권한을 사용한다는 사실이 확인될 때까지 기다렸다가 소프트웨어에 권한을 부여해야 합니다.

프로그램은 신뢰할 수 있는 시스템에서 세 가지 범주로 분류됩니다.

- **보안 속성이 필요하지 않은 프로그램** - 일부 프로그램은 단일 레벨에서 실행되므로 권한이 필요하지 않습니다. 이러한 프로그램은 공용 디렉토리(예: `/usr/local`)에 설치할 수 있습니다. 액세스하려면 사용자 및 역할의 권한 프로파일에 있는 명령으로 프로그램을 지정합니다.

- **root로 실행되는 프로그램** - 일부 프로그램은 `setuid 0`으로 실행됩니다. 이러한 프로그램에는 권한 프로파일에서 유효 UID `0`이 지정될 수 있습니다. 그러면 보안 관리자는 프로파일을 관리 역할에 지정합니다.

작은 정보 - 응용 프로그램에서 권한을 신뢰할 수 있는 방법으로 사용할 수 있는 경우 응용 프로그램에 필요한 권한을 지정하고 프로그램을 `root`로 실행하지 마십시오.

- **권한이 필요한 프로그램** - 일부 프로그램은 분명하지 않은 이유로 인해 권한이 필요할 수 있습니다. 프로그램에서 시스템 보안 정책을 위반할 것 같은 기능을 수행하고 있지 않더라도, 해당 프로그램이 보안을 위반하는 기능을 내부적으로 수행할 수 있습니다. 예를 들어, 프로그램에서 공유 로그 파일을 사용하거나 프로그램이 `/dev/kmem`에서 읽을 수 있습니다. 보안 문제에 대한 자세한 내용은 `mem`(7D) 매뉴얼 페이지를 참조하십시오.

  내부 정책을 대체해도 응용 프로그램의 올바른 작동에 특별히 영향을 미치지 않는 경우도 있습니다. 오히려 내부 정책을 대체하면 사용자가 기능을 보다 편리하게 수행할 수 있습니다.

  조직에서 소스 코드에 액세스할 수 있는 경우 응용 프로그램의 성능에 영향을 주지 않고 정책을 대체해야 하는 작업을 제거할 수 있는지 여부를 확인합니다.

신뢰할 수 있는 프로그램을 만들 때의 개발자 책임

프로그램 개발자가 소스 코드에서 권한 세트를 조작할 수 있더라도 보안 관리자가 프로그램에 필요한 권한을 지정하지 않은 경우에는 프로그램이 실패합니다. 따라서 신뢰할 수 있는 프로그램을 만들 때는 개발자와 보안 관리자가 상호 협력해야 합니다.

신뢰할 수 있는 프로그램을 작성하는 개발자는 다음을 수행해야 합니다.

1. 프로그램에서 작업을 수행하는 데 권한이 필요한 경우를 파악합니다.
2. 프로그램에서 권한을 안전하게 사용할 수 있도록 권한 분류 등과 같은 기술을 확인하여 따라야 합니다.
3. 프로그램에 권한을 지정할 때 보안에 미치는 영향에 유의합니다. 프로그램이 보안 정책을 위반하지 않아야 합니다.
4. 신뢰할 수 있는 디렉토리에서 프로그램에 연결되는 공유 라이브러리를 사용하여 프로그램을 컴파일합니다.

   자세한 내용은 “Developer’s Guide to Oracle Solaris 11 Security ”를 참조하십시오. Trusted Extensions에 대한 코드 예제는 “Trusted Extensions Developer’s Guide ”를 참조하십시오.

신뢰할 수 있는 프로그램에 대한 보안 관리자 책임

보안 관리자는 새 소프트웨어를 테스트하고 평가해야 할 책임이 있습니다. 신뢰할 수 있는 소프트웨어인지 확인한 후 보안 관리자는 프로그램에 대한 권한 프로파일과 기타 보안 관련 속성을 구성합니다.

보안 관리자의 책임은 다음과 같습니다.

1. 프로그래머와 프로그램 배포 프로세스가 신뢰할 수 있는지 확인합니다.
2. 다음 중 한 가지 방법으로 프로그램에 필요한 권한을 확인합니다.
   - 프로그래머에게 질문합니다.
   - 소스 코드에서 프로그램에 사용할 권한을 검색합니다.
   - 소스 코드에서 프로그램에서 사용자에게 요구하는 권한 부여를 검색합니다.
   - `ppriv` 명령에 대한 디버깅 옵션을 사용하여 권한 사용을 검색합니다. 예제는 `ppriv`(1) 매뉴얼 페이지를 참조하십시오. 또한 `dtrace`를 사용해서 권한 및 권한 부여 사용을 평가할 수 있습니다.
3. 소스 코드를 조사하여 프로그램을 작동하는 데 필요한 권한과 관련하여 코드가 신뢰할 수 있는 방법으로 작동하는지 확인합니다.

   프로그램에서 신뢰할 수 있는 방법으로 권한을 사용하지 못하는 경우 프로그램의 소스 코드를 수정할 수 있으면 코드를 수정합니다. 보안에 대해 잘 알고 있는 보안 컨설턴트 또는 개발자는 코드를 수정할 수 있습니다. 권한 분류, 권한 부여 확인 등을 수정할 수 있습니다.

   권한은 수동으로 지정해야 합니다. 권한이 부족하여 실패하는 프로그램에 권한을 지정할 수 있습니다. 또는 보안 관리자가 권한이 필요하지 않도록 유효한 UID 또는 GID를 지정할 수 있습니다.
4. 새 프로그램에 대한 권한 프로파일을 만들고 지정합니다.

♦ ♦ ♦ 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 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 "Trusted Extensions 사용자 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 지정되는 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 레벨을 넘지 않도록 지정합니다.
- 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 지정합니다. 한 사람에게는 보안과 관련한 의사 결정을 위한 보안 관리자 권한을 지정합니다. 다른 사람에게는 시스템 관리 작업을 위한 시스템 관리 권한을 지정합니다.

- 정기 백업 루틴을 설정합니다.
- 권한은 해당 권한이 필요하고 적절하게 사용할 것으로 신뢰할 수 있는 사람에게만 지정합니다.
- 프로그램에서 해당 작업을 수행하는 데 권한이 필요하고 프로그램의 권한 사용에 대한 신뢰성을 검토하여 입증된 경우에만 프로그램에 권한을 지정합니다. 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. 프로그램을 실행하고 오용을 방지하기 위해 권한 부여, 권한 및 역할을 사용합니다.
- 관리자는 정기적으로 일반 사용자에게 유효한 로그인 셸이 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 작업을 할 수 있는 영역을 설정합니다.
- 컴퓨터 시설의 구조 도면 및 다이어그램을 보호합니다.
- 건물 다이어그램, 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. 다른 보안 발행물도 UNIX 보안 문제 및 해결 방법을 완전히 이해하는 데 유용합니다.

또한 웹을 통해서도 리소스가 제공됩니다. 특히 CERT (http://www.cert.org) 웹 사이트에서는 기업과 사용자에게 소프트웨어의 보안상 취약성을 경고합니다. SANS 협회 (http://www.sans.org/)에서는 교육, 광범위한 용어집 및 인터넷의 주요 위협 요인에 대한 업데이트 목록을 제공합니다.

미국 정부 발행물

미국 정부는 웹을 통해 여러 발행물을 제공합니다. 미국 국토안보부 (http://www.us-cert.gov/security-publications)는 보안 정보를 게시합니다. 또한 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.
- Scarfone, Karen,Wayne Jansen 및 Miles Tracy. *Guide to General Server Security* SP 800-123, July 2008.
- Souppaya, Murugiah, John Wack 및 Karen Kent. *Security Configuration Checklists Program for IT Products*. SP 800-70, May 2005.

UNIX 발행물

Sun Microsystems 보안 엔지니어. *Solaris 10 Security Essentials*. Prentice Hall, 2009.

Garfinkel, Simson, Gene Spafford 및 Alan Schwartz. *Practical UNIX and Internet Security, 3rd Edition*. O'Reilly & Associates, Inc, Sebastopol, CA, 2006.

Nemeth, Evi, Garth Snyder, Trent R. Hein 및 Ben Whaley. *UNIX and Linux System Administration Handbook(4th Edition)* Pearson Education, Inc. 2010년

일반 컴퓨터 보안 발행물

Brunette, Glenn M. *Toward Systemically Secure IT Architectures*. Archived Oracle Technical Paper, 2006년 6월.

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.

McClure, Stuart, Joel Scambray, George Kurtz. *Hacking Exposed 7: Network Security Secrets & Solutions, Seventh Edition*. McGraw-Hill, 2012.

Stoll, Cliff. *The Cuckoo's Egg*. Doubleday, 1989.

♦ ♦ ♦ 부 록 B

Trusted Extensions 구성 점검 목록

이 점검 목록에서는 Trusted Extensions에 대한 주요 구성 작업의 전체적인 보기를 제공합니다. 세부 작업은 주요 작업에서 개략적으로 설명합니다. 점검 목록은 이 설명서의 다음 단계를 대체하지 않습니다.

Trusted Extensions 구성 점검 목록

다음은 사이트에 Trusted Extensions를 사용으로 설정 및 구성하는 데 필요한 사항을 요약한 목록입니다. 다른 곳에서 다루는 작업은 상호 참조됩니다.

1. 다음 설명을 읽습니다.
   - Trusted Extensions 관리 [87]의 처음 다섯 장을 읽으십시오.
   - 사이트 보안 요구 사항을 이해합니다.
   - "사이트 보안 정책 및 Trusted Extensions" [292]를 참조하십시오.
2. 다음을 준비합니다.
   - 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.
   - Oracle Solaris OS를 설치합니다.
3. Trusted Extensions를 사용으로 설정합니다. "Trusted Extensions 설치 및 사용으로 설정" [35]을 참조하십시오.
   a. 다중 레벨 데스크탑을 실행하는 시스템 또는 그렇지 않은 시스템을 위한 적합한 Trusted Extensions 패키지 세트를 로드합니다.
   b. `labeladm enable` *options* 명령을 실행하여 Trusted Extensions 서비스를 사용으로 설정합니다.
   c. (선택 사항) `labeladm encodings` *encodings-file* 명령을 실행하여 인코딩 파일을 설치합니다.

d. 재부트합니다.

4. (선택 사항) 전역 영역을 사용자 정의합니다. "Trusted Extensions의 전역 영역 설정" [39]을 참조하십시오.

   a. 1이 아닌 DOI를 사용하는 경우 `/etc/system` 파일 및 모든 보안 템플리트에서 DOI를 설정합니다.
   b. 사이트의 `label_encodings` 파일을 확인하고 설치합니다.
   c. 재부트합니다.

5. 레이블이 있는 영역을 추가합니다. "레이블이 있는 영역 만들기" [43]를 참조하십시오.

   a. 두 개의 레이블이 있는 영역을 자동으로 구성합니다.
   b. 본인의 레이블이 있는 영역을 수동으로 구성합니다.
   c. 레이블이 있는 작업 공간을 만듭니다.

6. LDAP 이름 지정 서비스를 구성합니다. 5장. Trusted Extensions에 대한 LDAP 구성을 참조하십시오.

   Trusted Extensions 프록시 서버 또는 Trusted Extensions LDAP 서버를 생성합니다. 파일 이름 지정 서비스는 구성이 필요하지 않습니다.

7. 전역 영역 및 레이블이 있는 영역을 위한 인터페이스 및 경로 지정을 구성합니다. "ProductShort;에서 네트워크 인터페이스 구성" [48]을 참조하십시오.

8. 네트워크를 구성합니다. "호스트 및 네트워크 레이블 지정" [199]을 참조하십시오.

   - 단일 레이블 호스트 및 제한된 범위 호스트를 식별합니다.
   - 레이블이 없는 호스트에서 수신되는 데이터에 적용할 레이블을 결정합니다.
   - 보안 템플리트를 사용자 정의합니다.
   - 개별 호스트를 보안 템플리트에 지정합니다.
   - 서브넷을 보안 템플리트에 지정합니다.

9. 추가 구성을 수행합니다.

   a. LDAP에 대한 네트워크 연결 구성.
      - 모든 보안 템플리트에서 LDAP 서버 또는 프록시 서버를 `cipso` 호스트 유형에 지정합니다.
      - 모든 보안 템플리트에서 LDAP 클라이언트를 `cipso` 호스트 유형에 지정합니다.
      - 로컬 시스템을 LDAP 서버의 클라이언트로 만듭니다.
   b. 로컬 사용자 및 로컬 관리 역할 구성. "Trusted Extensions의 역할 및 사용자 만들기" [54]를 참조하십시오.
      - 보안 관리자 역할을 만듭니다.
      - 보안 관리자 역할을 수락할 수 있는 로컬 사용자를 생성합니다.
      - 다른 역할 및 이러한 역할을 수락할 수 있는 다른 로컬 사용자를 만듭니다.
   c. 사용자가 액세스할 수 있는 모든 레이블에서 홈 디렉토리를 만듭니다. "Trusted Extensions에서 중앙 홈 디렉토리 만들기" [60]를 참조하십시오.
      - NFS 서버에 홈 디렉토리를 만듭니다.
      - 암호화할 수 있는 로컬 ZFS 홈 디렉토리를 만듭니다.

- (선택 사항) 사용자가 하위 레벨의 홈 디렉토리를 읽지 못하도록 합니다.

d. 인쇄를 구성합니다. “레이블이 있는 인쇄 구성” [248]을 참조하십시오.

e. 장치를 구성합니다. “Trusted Extensions에서 장치 취급” [265]을 참조하십시오.

   i. 역할에 Device Management(장치 관리) 프로파일 또는 System ADministrator(시스템 관리자) 프로파일을 지정합니다.

   ii. 장치를 사용 가능하게 하려면 다음 중 하나를 수행합니다.

   - 시스템에 따라 장치를 할당 가능하게 합니다.
   - 선택한 사용자 및 역할에 Allocate Device(장치 할당) 권한을 할당합니다.

f. Oracle Solaris 기능을 구성합니다.

- 감사를 구성합니다.
- 시스템 보안 값을 구성합니다.
- 특정 LDAP 클라이언트가 LDAP를 관리할 수 있도록 합니다.
- LDAP에서 사용자를 구성합니다.
- LDAP에서 네트워크 역할의 구성합니다.

g. 파일 시스템을 마운트 및 공유합니다. 14장. Trusted Extensions에서 파일 관리 및 마운트를 참조하십시오.

♦ ♦ ♦ 부 록 C

Trusted Extensions 관리에 대한 빠른 참조

Trusted Extensions 인터페이스는 Oracle Solaris OS를 확장합니다. 이 부록을 참조하여 차이점을 빠르게 확인할 수 있습니다. 라이브러리 루틴, 시스템 호출을 비롯한 자세한 인터페이스 목록은 부록 D. Trusted Extensions 매뉴얼 페이지 목록을 참조하십시오.

Trusted Extensions의 관리 인터페이스

Trusted Extensions에서는 소프트웨어에 대한 인터페이스를 제공합니다. `labeladm` 명령은 `labeld` 서비스를 사용 및 사용 안함으로 설정하고 Trusted Extensions 시스템에 대해 `label_encodings` 파일을 설정합니다. 다음 인터페이스는 Trusted Extensions 소프트웨어를 실행 중인 경우에만 사용할 수 있습니다.

`txzonemgr` 스크립트
: 레이블이 있는 영역을 만들고 설치, 초기화 및 부팅하는 메뉴 기반의 마법사를 제공합니다. 메뉴 제목은 Labeled Zone Manager(레이블이 있는 영역 관리자)입니다. 이 스크립트는 네트워킹 옵션, 이름 지정 서비스 옵션 및 전역 영역을 기존 LDAP 서버의 클라이언트로 만들기 위한 메뉴 항목도 제공합니다. Oracle Solaris 11 릴리스에서 `txzonemgr -c` 명령은 메뉴를 거치지 않고 처음 두 개의 레이블이 있는 영역을 만듭니다.

장치 관리자
: Trusted Extensions에서 이 GUI는 장치를 관리하는 데 사용됩니다. Device Administration(장치 관리) 대화 상자는 관리자가 장치를 구성하는 데 사용됩니다.

  Device Allocation Manager(장치 할당 관리자)는 역할 및 일반 사용자가 장치를 할당하는 데 사용됩니다. GUI는 Trusted Path(신뢰할 수 있는 경로) 메뉴에서 사용할 수 있습니다.

레이블 구축기
: 이 응용 프로그램은 사용자가 레이블 또는 클리어런스를 선택할 수 있을 때 호출됩니다. 이 응용 프로그램은 역할이 장치, 영역, 사용자 또는 역할에 레이블이나 레이블 범위를 지정할 때도 나타납니다.

  `tgnome-selectlabel` 유틸리티를 사용하여 레이블 구축기를 사용자 정의할 수 있습니다. "Trusted Extensions Developer's Guide "의 "tgnome-selectlabel Utility"를 참조하십시오.

Selection Manager(선택 관리자)	이 응용 프로그램은 권한 부여된 사용자나 역할이 정보를 업그레이드하거나 다운그레이드하려고 할 때 호출됩니다.
신뢰할 수 있는 경로 메뉴	이 메뉴는 TCB(Trusted Computing Base)와의 상호 작용을 처리합니다. 예를 들어, 이 메뉴에는 Change (Login/Workspace) Password((로그인/작업 공간) 암호 변경) 메뉴 항목이 있습니다. Trusted GNOME에서는 신뢰할 수 있는 스트라이프 왼쪽의 신뢰할 수 있는 기호를 눌러서 Trusted Path(신뢰할 수 있는 경로) 메뉴에 액세스합니다.
관리 명령	Trusted Extensions에서는 레이블을 가져오고 기타 작업을 수행하는 명령을 제공합니다. 명령 목록은 "Trusted Extensions의 명령줄 도구" [102]를 참조하십시오.

Trusted Extensions에서 확장된 Oracle Solaris 인터페이스

Trusted Extensions에서 기존 Oracle Solaris 구성 파일, 명령 및 GUI에 다음 사항을 추가합니다.

관리 명령	Trusted Extensions에서 선택된 Oracle Solaris 명령에 옵션을 추가합니다. 모든 Trusted Extensions 인터페이스 목록은 부록 D. Trusted Extensions 매뉴얼 페이지 목록을 참조하십시오.
구성 파일	Trusted Extensions에서 `net_mac_aware`와 `net_mlp`라는 두 가지 권한을 추가합니다. `net_mac_aware` 사용 방법은 "Trusted Extensions에서 NFS 서버 및 클라이언트 구성" [172]을 참조하십시오. Trusted Extensions에서 `auth_attr` 데이터베이스에 권한 부여를 추가합니다. Trusted Extensions에서 `exec_attr` 데이터베이스에 실행 파일을 추가합니다. Trusted Extensions에서 `prof_attr` 데이터베이스의 기존 권한 프로파일을 수정합니다. 또한 데이터베이스에 프로파일을 추가합니다. Trusted Extensions에서 `policy.conf` 데이터베이스에 필드를 추가합니다. 필드는 "Trusted Extensions의 `policy.conf` 파일 기본값" [124]을 참조하십시오. Trusted Extensions에서 감사 토큰, 감사 이벤트, 감사 클래스 및 감사 정책 옵션을 추가합니다. 목록은 "Trusted Extensions 감사 참조" [280]를 참조하십시오.
영역의 공유 디렉토리	Trusted Extensions에서는 레이블이 있는 영역의 디렉토리를 공유할 수 있습니다. 전역 영역에서 `/etc/dfs/dfstab` 파일을 만들어 영역의 레이블에서 디렉토리를 공유합니다.

Trusted Extensions의 강화된 보안 기본값

Trusted Extensions에서는 Oracle Solaris OS보다 보안 기본값이 강화되었습니다.

장치	기본적으로 장치 할당이 사용으로 설정되어 있습니다. 기본적으로 장치 할당에는 권한 부여가 필요합니다. 따라서 기본적으로 일반 사용자는 이동식 매체를 사용할 수 없습니다. 관리자는 권한 부여 요구 사항을 제거할 수 있습니다. 그러나 Trusted Extensions를 설치하는 사이트에는 일반적으로 장치 할당이 필요합니다.
인쇄	일반 사용자는 프린터의 레이블 범위에 사용자의 레이블이 포함되어 있는 프린터로만 인쇄할 수 있습니다. 기본적으로 인쇄된 출력에는 트레일러 페이지와 배너 페이지가 있습니다. 이들 페이지와 본문 페이지에는 인쇄 작업의 레이블이 포함됩니다.
역할	Oracle Solaris OS에서는 역할을 사용할 수 있지만 선택 사항입니다. Trusted Extensions에서는 역할이 적절한 관리를 위한 필수 사항입니다.

Trusted Extensions의 제한된 옵션

Trusted Extensions에서는 Oracle Solaris 구성 옵션 범위를 축소합니다.

이름 지정 서비스	LDAP 이름 지정 서비스가 지원됩니다. 하나의 이름 지정 서비스로 모든 영역을 관리해야 합니다.
영역	전역 영역은 관리 영역입니다. `root` 사용자 또는 역할만 전역 영역에 들어갈 수 있습니다. 따라서 일반 Trusted Extensions 사용자는 일반 Oracle Solaris 사용자가 사용할 수 있는 관리 인터페이스를 사용할 수 없습니다. 비전역 영역은 레이블이 있는 영역입니다. 사용자는 레이블이 있는 영역에서 작업합니다.

♦ ♦ ♦ 부 록 D

Trusted Extensions 매뉴얼 페이지 목록

Trusted Extensions는 Oracle Solaris OS의 구성입니다. 이 부록에서는 Trusted Extensions 정보가 들어 있는 매뉴얼 페이지에 대해 설명합니다.

Trusted Extensions 매뉴얼 페이지(사전순)

다음 매뉴얼 페이지는 Trusted Extensions로 구성된 시스템에만 해당됩니다. 설명에는 Trusted Extensions 문서에서 다루는 해당 기능의 예나 설명에 대한 링크가 포함되어 있습니다.

Trusted Extensions 매뉴얼 페이지	용도 및 추가 정보 링크
`add_allocatable`(1M)	장치 할당 데이터베이스에 장치를 추가하여 할당할 수 있습니다. 기본적으로 분리 가능한 장치를 할당할 수 있습니다. Trusted Extensions에서 장치 관리자를 사용하여 장치를 구성하는 방법 [267]을 참조하십시오.
`atohexlabel`(1M)	사람이 읽을 수 있는 레이블을 해당 내부 텍스트로 변환합니다. 예는 레이블에 해당하는 16진수를 얻는 방법 [117]을 참조하십시오.
`blcompare`(3TSOL)	이진 레이블 비교합니다.
`blminmax`(3TSOL)	두 레이블의 범위를 결정합니다.
`chk_encodings`(1M)	레이블 인코딩 파일 구문을 확인합니다. 예는 "Trusted Extensions Label Administration "의 "How to Debug a

	label_encodings File" 및 예 4-1. "명령줄에서 label_encodings 구문 검사"을 참조하십시오.
fgetlabel(2)	파일의 레이블 가져오기
getlabel(1)	선택된 파일이나 디렉토리의 레이블을 표시합니다. 예는 마운트된 파일의 레이블을 표시하는 방법 [157]을 참조하십시오.
getlabel(2)	파일의 레이블 가져오기
getpathbylabel(3TSOL)	영역 경로 이름 가져오기
getplabel(3TSOL)	프로세스 레이블 가져오기
getuserrange(3TSOL)	사용자의 레이블 범위 가져오기
getzoneidbylabel(3TSOL)	영역 레이블에서 영역 ID 가져오기
getzonelabelbyid(3TSOL)	영역 ID에서 영역 레이블 가져오기
getzonelabelbyname(3TSOL)	영역 이름에서 영역 레이블 가져오기
getzonepath(1)	지정된 레이블에 해당하는 영역의 루트 경로를 표시합니다. "Trusted Extensions Developer's Guide "의 "Acquiring a Sensitivity Label"
getzonerootbyid(3TSOL)	영역 루트 ID에서 영역 루트 경로 이름 가져오기
getzonerootbylabel(3TSOL)	영역 레이블에서 영역 루트 경로 이름 가져오기
getzonerootbyname(3TSOL)	영역 이름에서 영역 루트 경로 이름 가져오기
hextoalabel(1M)	내부 텍스트 레이블을 사람이 읽을 수 있는 해당 레이블로 변환 예는 읽기 가능한 레이블을 해당 16진수 형식에서 얻는 방법 [119]을 참조하십시오.
labeladm(1M)	Trusted Extensions 레이블 지정 서비스를 사용 및 사용 안함으로 설정하고 label_encodings 파일을 설정할 수 있습니다.
labelclipping(3TSOL)	이진 레이블을 변환하고 지정된 폭으로 잘라내기

label_encodings(4)	레이블 인코딩 파일 설명
label_to_str(3TSOL)	레이블을 사람이 읽을 수 있는 문자열로 변환
labels(5)	Trusted Extensions 레이블 속성 설명
libtsnet(3LIB)	Trusted Extensions 네트워크 라이브러리
libtsol(3LIB)	Trusted Extensions 라이브러리
m_label(3TSOL)	새 레이블에 대한 리소스 할당 및 비우기
pam_tsol_account(5)	레이블에 따른 계정 제한 확인 사용 예는 원격 Trusted Extensions 시스템에 로그인하고 관리하는 방법 [148]을 참조하십시오.
plabel(1)	프로세스 레이블 가져오기
remove_allocatable(1M)	장치 할당 데이터베이스에서 해당 항목을 제거하여 장치의 할당을 막습니다. 예제는 Trusted Extensions에서 장치 관리자를 사용하여 장치를 구성하는 방법 [267]을 참조하십시오.
sel_config(4)	복사, 잘라내기, 붙여넣기 및 끌어서 놓기 작업에 대한 선택 규칙 "데이터에 대한 보안 레벨 변경 규칙" [110]을 참조하십시오.
setflabel(3TSOL)	파일을 해당 민감도 레이블의 영역으로 이동
setlabel(1)	선택된 항목의 레이블을 재지정합니다. `solaris.label.file.downgrade` 또는 `solaris.label.file.upgrade` 권한 부여가 필요합니다. 이러한 권한 부여는 Object Label Management 권한 프로파일에 있습니다.
str_to_label(3TSOL)	사람이 읽을 수 있는 문자열을 레이블로 구문 분석
tncfg(1M)	신뢰할 수 있는 네트워크 데이터베이스를 관리합니다. 신뢰할 수 있는 네트워크 관리를 위한 `txzonmgr` GUI의 대체 방법입니다. `list` 하위 명

	령은 네트워크 인터페이스의 보안 특성을 표시합니다. `tncfg`는 `tninfo` 명령보다 많은 정보를 제공합니다. 예는 16장. Trusted Extensions에서 네트워크 관리를 참조하십시오.
`tnctl`(1M)	Trusted Extensions 네트워크 매개변수를 구성합니다. 또한 `tncfg` 명령을 사용할 수 있습니다. 예는 예 12-1. "원격 관리를 위한 CIPSO 호스트 유형 지정"를 참조하십시오.
`tnd`(1M)	LDAP 이름 지정 서비스가 사용으로 설정되었을 때 신뢰할 수 있는 네트워크 데몬을 실행합니다.
`tninfo`(1M)	커널 레벨 Trusted Extensions 네트워크 정보 및 통계를 표시합니다. Trusted Extensions 네트워크를 디버깅하는 방법 [226]. 또한 `tncfg` 명령 및 `txzonemgr` GUI를 사용할 수 있습니다. `tncfg` 명령과 비교는 Trusted Extensions에서 마운트 실패 문제를 해결하는 방법 [179]을 참조하십시오.
`trusted_extensions`(5)	Trusted Extensions 소개
`txzonemgr`(1M)	레이블이 있는 영역 및 네트워크 인터페이스를 관리합니다. 명령줄 옵션을 사용하여 두 영역을 자동으로 만들 수 있습니다. 이 명령은 구성 파일을 입력으로 사용하고 영역을 삭제할 수 있습니다. `txzonemgr`은 `zenity` (1) 스크립트입니다. "레이블이 있는 영역 만들기" [43] 및 "신뢰할 수 있는 네트워크 문제 해결" [224]을 참조하십시오.
`TrustedExtensionsPolicy`(4)	Trusted Extensions X 서버 확장에 대한 구성 파일
`tsol_getrhtype`(3TSOL)	Trusted Extensions 네트워크 정보에서 호스트 유형 가져오기
`tgnome-selectlabel` 유틸리티	레이블 구축기 GUI를 만들 수 있습니다. 자세한 내용은 "Trusted Extensions Developer's Guide "의 "tgnome-selectlabel Utility"를 참조하십시오.

updatehome(1)	현재 레이블에 대한 홈 디렉토리 복사 및 링크 파일 업데이트 Trusted Extensions에서 사용자의 시작 파일을 구성하는 방법 [132]을 참조하십시오.
XTSOLgetClientAttributes(3XTSOL)	X 클라이언트의 레이블 속성 가져오기
XTSOLgetPropAttributes(3XTSOL)	창 등록 정보의 레이블 속성 가져오기
XTSOLgetPropLabel(3XTSOL)	창 등록 정보의 레이블 가져오기
XTSOLgetPropUID(3XTSOL)	창 등록 정보의 UID 가져오기
XTSOLgetResAttributes(3XTSOL)	창 또는 픽스맵의 모든 레이블 속성 가져오기
XTSOLgetResLabel(3XTSOL)	창, 픽스맵 또는 색상맵의 레이블 가져오기
XTSOLgetResUID(3XTSOL)	창 또는 픽스맵의 UID 가져오기
XTSOLgetSSHeight(3XTSOL)	화면 스트라이프의 높이 가져오기
XTSOLgetWorkstationOwner(3XTSOL)	워크스테이션의 소유권 가져오기
XTSOLIsWindowTrusted(3XTSOL)	신뢰할 수 있는 클라이언트가 창을 만들었는지 확인
XTSOLMakeTPWindow(3XTSOL)	이 창을 Trusted Path(신뢰할 수 있는 경로) 창으로 설정
XTSOLsetPolyInstInfo(3XTSOL)	다중 인스턴스화 정보 설정
XTSOLsetPropLabel(3XTSOL)	창 등록 정보의 레이블 설정
XTSOLsetPropUID(3XTSOL)	창 등록 정보의 UID 설정
XTSOLsetResLabel(3XTSOL)	창 또는 픽스맵의 레이블 설정
XTSOLsetResUID(3XTSOL)	창, 픽스맵 또는 색상맵의 UID 설정
XTSOLsetSessionHI(3XTSOL)	세션의 높은 민감도 레이블을 창 서버로 설정
XTSOLsetSessionLO(3XTSOL)	세션의 낮은 민감도 레이블을 창 서버로 설정
XTSOLsetSSHeight(3XTSOL)	화면 스트라이프의 높이 설정
XTSOLsetWorkstationOwner(3XTSOL)	워크스테이션의 소유권 설정

Trusted Extensions에서 수정된 Oracle Solaris 매뉴얼 페이지

Trusted Extensions에서는 다음 Oracle Solaris 매뉴얼 페이지에 정보를 추가합니다.

Oracle Solaris 매뉴얼 페이지	Trusted Extensions 수정 사항 및 추가 정보 링크
allocate(1)	영역에서 장치 할당과 창 환경에서 장치 정리를 지원하는 옵션을 추가합니다. Trusted Extensions에서 일반 사용자는 이 명령을 사용하지 않습니다. 사용자 절차는 "Trusted Extensions 사용자 설명서 "의 "Trusted Extensions에서 장치를 할당하는 방법"을 참조하십시오.
auditconfig(1M)	레이블이 있는 정보에 대한 창 정책, 감사 클래스, 감사 이벤트 및 감사 토큰을 추가합니다.
auditreduce(1M)	레이블로 감사 레코드를 선택하는 -l 옵션을 추가합니다. 예제는 "Oracle Solaris 11.2의 감사 관리 "의 "표시할 감사 이벤트 선택"을 참조하십시오.
auth_attr(4)	레이블 권한 부여 추가
automount(1M)	마운트 기능 즉, 하위 레벨 홈 디렉토리 보기 기능을 추가합니다. 상위 레이블에서 영역 이름 및 영역 표시를 고려하여 auto_home 맵의 이름과 내용을 수정합니다. 자세한 내용은 "Trusted Extensions의 자동 마운트 변경 사항" [173]을 참조하십시오.
deallocate(1)	영역에서 장치 할당 취소, 창 환경에서 장치 정리 및 할당 취소할 장치 유형 지정을 지원하는 옵션을 추가합니다. Trusted Extensions에서 일반 사용자는 이 명령을 사용하지 않습니다. 사용자 절차는 "Trusted Extensions 사용자 설명서 "의 "Trusted Extensions에서 장치를 할당하는 방법"을 참조하십시오.
device_clean(5)	Trusted Extensions에서 기본적으로 호출됨
getpflags(2)	NET_MAC_AWARE 및 NET_MAC_AWARE_INHERIT 프로세스 플래그 인식
getsockopt(3SOCKET)	소켓의 필수 액세스 제어 상태인 SO_MAC_EXEMPT 가져오기
getsockopt(3XNET)	소켓의 필수 액세스 제어 상태인 SO_MAC_EXEMPT 가져오기
ikeadm(1M)	레이블이 있는 IKE 프로세스에 대해 디버그 플래그 0x0400을 추가합니다.

ike.config(4)	label_aware 전역 매개변수와 세 개의 단계 1 변환 키워드인 single_label, multi_label 및 wire_label을 추가합니다.
in.iked(1M)	전역 영역에서 다중 레벨 UDP 포트 500부터 4500까지 레이블이 있는 보안 연결 협상을 지원합니다. 또한 ike.config(4) 매뉴얼 페이지를 참조하십시오.
ipadm(1M)	all-zones 인터페이스를 영구 등록 정보 값으로 추가합니다. 예는 시스템의 인터페이스가 작동 중인지 확인하는 방법 [225]을 참조하십시오.
ipseckey(1M)	label, outer-label 및 implicit-label 확장을 추가합니다. 이러한 확장은 Trusted Extensions 레이블을 보안 연결 내부에서 전달되는 트래픽과 연결합니다.
is_system_labeled(3C)	시스템이 Trusted Extensions로 구성되었는지 여부 확인
ldaplist(1)	Trusted Extensions 네트워크 데이터베이스를 LDAP에 추가합니다.
list_devices(1)	장치에 연결된 속성(예: 레이블)을 추가합니다. 권한 부여 및 레이블과 같은 장치 속성을 표시하는 -a 옵션을 추가합니다. 할당된 장치 유형의 기본 속성을 표시하는 -d 옵션을 추가합니다. 레이블이 있는 영역에 할당할 수 있는 장치를 표시하는 -z 옵션을 추가합니다.
netstat(1M)	소켓 및 경로 지정 테이블 항목에 대한 확장 보안 속성을 표시하는 -R 옵션을 추가합니다. 예는 Trusted Extensions에서 마운트 실패 문제를 해결하는 방법 [179]을 참조하십시오.
pf_key(7P)	레이블을 IPsec 보안 연결(SA)에 추가합니다.
privileges(5)	Trusted Extensions 권한(예: PRIV_FILE_DOWNGRADE_SL) 추가
prof_attr(4)	권한 프로파일(예: Object Label Management) 추가
route(1M)	경로에 확장 보안 속성을 추가하는 -secattr 옵션을 추가합니다. 경로의 보안 속성인 cipso, doi, max_sl 및 min_sl을 표시하는 -secattr 옵션을 추가합니다. 예는 Trusted Extensions에서 마운트 실패 문제를 해결하는 방법 [179]을 참조하십시오.
setpflags(2)	NET_MAC_AWARE 프로세스별 플래그 설정
setsockopt(3SOCKET)	SO_MAC_EXEMPT 옵션 설정

setsockopt(3XNET)	소켓에 필수 액세스 제어인 SO_MAC_EXEMPT 설정
socket.h(3HEAD)	레이블이 없는 피어에 대한 SO_MAC_EXEMPT 옵션 지원
tar(1)	레이블이 있는 파일 및 디렉토리를 아카이브하고 추출하는 -T 옵션을 추가합니다. Trusted Extensions에서 파일을 백업하는 방법 [175] 및 Trusted Extensions에서 파일을 복원하는 방법 [176]을 참조하십시오.
tar.h(3HEAD)	레이블이 있는 tar 파일에 사용되는 속성 유형 추가
ucred_getlabel(3C)	사용자 자격 증명에서 레이블 값 가져오기 기능 추가
user_attr(4)	Trusted Extensions 관련 clearance 및 min_label 사용자 보안 속성을 추가합니다. "Trusted Extensions의 사용자 보안 계획" [24]을 참조하십시오.

용어

.copy_files file(.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 `.firefox` 등의 시작 파일 목록이 포함되어 있습니다. `.copy_files`에 나열된 파일은 해당 디렉토리를 만들 때 상위 레이블의 사용자 홈 디렉토리로 복사됩니다. .link_files file(.link_files 파일)을 참조하십시오.

.link_files file(.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 `.firefox` 등의 시작 파일 목록이 포함되어 있습니다. `.link_files`에 나열된 파일은 해당 디렉토리를 만들 때 상위 레이블의 사용자 홈 디렉토리로 연결됩니다. .copy_files file(.copy_files 파일)을 참조하십시오.

평가된 구성 외부 evaluated configuration(평가된 구성)의 조건을 만족시키는 것으로 입증된 소프트웨어가 보안 조건을 만족시키지 않는 설정으로 구성된 경우 소프트웨어가 *outside the evaluated configuration*에 있다고 합니다.

accreditation range(승인 범위) 사용자 또는 리소스 클래스에 대해 승인된 민감도 레이블의 세트입니다. 유효한 레이블 세트입니다. system accreditation range(시스템 승인 범위) 및 user accreditation range(사용자 승인 범위)를 참조하십시오.

administrative role(관리 역할) 필요한 권한 부여, 권한 있는 명령 및 신뢰할 수 있는 경로의 security attribute(보안 속성)을 제공하여 해당 역할이 관리 작업을 수행할 수 있도록 하는 role(역할)입니다. 역할은 백업 또는 감사와 같은 Oracle Solaris `root` 기능의 일부를 수행합니다.

allocation(할당) device(장치)에 대한 액세스를 제어하는 방식입니다. device allocation(장치 할당)을 참조하십시오.

authorization(권한 부여) 작업을 수행하도록 사용자 또는 역할에게 부여되는 권한으로, 이러한 권한 없이는 보안 정책에 따라 해당 작업을 수행할 수 없습니다. 권한은 권한 프로파일에서 부여됩니다. 특정 명령을 성공적으로 수행하려면 사용자에게 특정 권한 부여가 있어야 합니다.

branded zone(브랜드 영역) Trusted Extensions에서 레이블이 있는 비전역 영역입니다. 더욱 일반적으로는 비원시 운영 환경을 포함하는 비전역 영역입니다. `brands`(5) 매뉴얼 페이지를 참조하십시오.

CIPSO label(CIPSO 레이블) Common IP Security Option(공통 IP 보안 옵션)입니다. CIPSO는 Trusted Extensions에서 구현되는 레이블 표준입니다.

classification(분류) clearance(클리어런스) 또는 label(레이블)의 계층적 구성 요소입니다. 분류는 보안의 계층적 레벨(예: `TOP SECRET` 또는 `UNCLASSIFIED`)을 나타냅니다.

clearance(클리어런스) 사용자가 작업할 수 있는 레이블 세트의 상한입니다. 하한은 minimum label(최소 레이블)가 지정한 security administrator(보안 관리자)입니다. 클리어런스 유형은 세션 클리어런스 또는 user clearance(사용자 클리어런스) 중 하나입니다.

client(클라이언트) 네트워크에 연결된 시스템입니다.

closed network(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. open network(개방형 네트워크)와 반대입니다.

compartment(구획) label(레이블) 구성 요소와 함께 사용되어 classification(분류) 또는 clearance(클리어런스)을 형성하는 label(레이블)의 비계층적 구성 요소입니다. 구획은 엔지니어링 부서 또는 여러 전문 분야의 프로젝트 팀에서 사용하는 것과 같은 정보의 모음을 나타냅니다.

DAC discretionary access control(임의 액세스 제어)를 참조하십시오.

device allocation(장치 할당) 장치를 할당한 사용자 이외의 사용자가 할당 가능 device(장치) 정보에 액세스하는 것을 방지하기 위한 방식입니다. 장치 할당이 해제될 때까지는 장치를 할당한 사용자만 장치 관련 정보에 액세스할 수 있습니다. 사용자가 장치를 할당하려면 security administrator(보안 관리자)가 해당 사용자에게 Device Allocation(장치 할당) 권한을 부여해야 합니다.

device(장치) 장치에는 프린터, 컴퓨터, 테이프 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 device allocation(장치 할당)에 의해 제어됩니다.

discretionary access control(임의 액세스 제어) 파일이나 디렉토리 소유자가 임의로 허용하거나 거부하는 액세스 유형입니다. Trusted Extensions에서는 UNIX permission bits(권한 비트)와 ACL, 두 종류의 임의 액세스 제어(DAC)를 제공합니다.

DOI(Domain of Interpretation) Trusted Extensions로 구성된 Oracle Solaris 시스템에서 DOI는 유사한 레이블이 정의되어 있을 수 있는 다른 `label_encodings` 파일을 구분하는 데 사용됩니다. DOI는 네트워크 패킷에 있는 보안 속성을 로컬 `label_encodings` 파일별 해당 보안 속성 표현으로 변환하는 규칙 세트입니다. 시스템에 동일한 DOI가 있는 경우 시스템은 해당 규칙 세트를 공유하여 레이블이 있는 네트워크 패킷을 변환할 수 있습니다.

domain name(도메인 이름) 시스템 그룹의 ID입니다. 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.

domain(도메인) 인터넷 이름 지정 계층의 일부입니다. 관리 파일을 공유하는 로컬 네트워크의 시스템 그룹을 나타냅니다.

evaluated configuration(평가된 구성) 인증 기관에 의해 특정 기준을 충족하는 것으로 인증된 구성에서 실행 중인 하나 이상의 Trusted Extensions 호스트입니다.

Trusted Extensions 소프트웨어는 Common Criteria v2.3[2005년 8월], ISO 표준, EAL(Evaluation Assurance Level) 4 및 여러 보호 프로파일에 대한 인증을 위해 평가를 받고 있습니다.

file system(파일 시스템) 논리적 계층 구조로 설정할 때 체계적이고 구조화된 정보 세트를 구성하는 파일 및 디렉토리의 모음입니다. 파일 시스템은 로컬 system(시스템) 또는 원격 시스템에서 마운트할 수 있습니다.

GFI Government Furnished Information의 약어입니다. 이 설명서에서는 미국 정부에서 제공하는 label_encodings file(label_encodings 파일)을 가리킵니다. Trusted Extensions 소프트웨어에서 GFI를 사용하려면 GFI의 끝에 Oracle 고유의 `LOCAL DEFINITIONS` 섹션을 추가해야 합니다. 자세한 내용은 "Trusted Extensions Label Administration "의 5 장, "Customizing the LOCAL DEFINITIONS Section"를 참조하십시오.

host name(호스트 이름) 네트워크의 다른 시스템에 알려진 system(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.

initial label(초기 레이블) 사용자나 역할에 지정된 minimum label(최소 레이블) 및 사용자의 초기 작업 공간의 레이블입니다. 초기 레이블은 사용자나 역할이 작업할 수 있는 가장 낮은 레이블입니다.

initial setup team(초기 설정 팀) Trusted Extensions 소프트웨어의 사용과 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.

IP address(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 첫번째 숫자는 224보다 작아야 하고 마지막 숫자는 0이 될 수 없습니다.

IP 주소는 논리적으로 네트워크와 네트워크에 있는 system(시스템)으로 나뉩니다. 네트워크 번호는 지역 번호와 유사합니다. 네트워크에 대해 시스템 번호는 전화 번호와 유사합니다.

label configuration(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.

label range(레이블 범위) 명령, 영역 및 할당 가능 장치에 할당된 민감도 레이블의 세트입니다. 범위는 최대 레이블 및 최소 레이블을 정의하여 지정됩니다. 명령의 경우 최소 및 최대 레이블은 명령이 실행될 수 있는 레이블을 제한합니다. 레이블을 인식하지 않는 원격 호스트에는 단일 sensitivity label(민감도 레이블)이 지정되며 security administrator(보안 관리자)가 단일 레이블로 제

한하고자 하는 다른 호스트도 마찬가지입니다. 레이블 범위는 장치가 할당될 수 있는 레이블을 제한하며 장치 사용 시 정보를 저장하거나 처리할 수 있는 레이블을 제한합니다.

label relationships(레이블 관계) Trusted Extensions로 구성된 Oracle Solaris 시스템에서 한 레이블은 다른 레이블보다 우선하거나, 다른 레이블과 동일하거나, 다른 레이블에서 분리될 수 있습니다. 예를 들어 `Top Secret` 레이블은 `Secret` 레이블보다 우선합니다. 동일한 DOI(Domain of Interpretation)를 포함하는 2개 시스템에서 한 시스템의 `Top Secret` 레이블은 다른 시스템의 `Top Secret` 레이블과 동일합니다.

label set(레이블 세트) security label set(보안 레이블 세트)을 참조하십시오.

label_encodings file(label_encodings 파일) 인정 범위, 레이블 보기, 기본 레이블 가시성, 기본 사용자 클리어런스 및 레이블의 기타 측면과 같은 전체 sensitivity label(민감도 레이블)이 정의되어 있는 파일입니다.

label(레이블) 객체에 지정된 보안 식별자입니다. 레이블은 객체를 보호해야 하는 정보의 레벨을 기반으로 합니다. security administrator(보안 관리자)가 사용자를 구성한 방법에 따라 사용자는 sensitivity label(민감도 레이블)을 볼 수 있거나 전혀 레이블을 볼 수 없습니다. 레이블은 label_encodings file(label_encodings 파일)에서 정의합니다.

labeled host(레이블이 있는 호스트) 레이블이 있는 시스템으로 구성된 신뢰할 수 있는 네트워크의 일부인 labeled system(레이블이 있는 시스템)입니다.

labeled system(레이블이 있는 시스템) 레이블이 있는 시스템은 MLS가 사용으로 설정된 SELinux 또는 Trusted Extensions와 같은 다중 레벨 운영 체제를 실행하는 시스템입니다. 시스템에서는 패킷 헤더에 CIPSO(Common IP Security Option)라는 레이블이 있는 네트워크 패킷을 보내고 받을 수 있습니다.

labeled zone(레이블이 있는 영역) Trusted Extensions로 구성된 Oracle Solaris 시스템에서는 모든 영역에 레이블이 지정됩니다. 일반적으로 레이블이 있는 영역은 전역 영역에 레이블이 있다 하더라도 레이블이 지정된 비전역 영역을 참조합니다. 레이블이 있는 영역에는 레이블로 구성되지 않은 Oracle Solaris 시스템의 비전역 영역과 다른 2가지 특징이 있습니다. 먼저 레이블이 있는 영역은 동일한 사용자 ID 및 그룹 ID 풀을 사용해야 합니다. 다음으로 레이블이 있는 영역은 IP 주소를 공유할 수 있습니다.

MAC mandatory access control(필수 액세스 제어)를 참조하십시오.

mandatory access control(필수 액세스 제어) 파일, 디렉토리 또는 sensitivity label(민감도 레이블)의 device(장치)을 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.

minimum label(최소 레이블) 사용자 민감도 레이블의 하한 및 시스템 민감도 레이블의 하한입니다. 사용자의 보안 속성을 지정할 때 security administrator(보안 관리자)가 설정하는 최소 레이블은 최초 로그인 시

사용자의 첫번째 작업 공간의 민감도 레이블입니다. security administrator(보안 관리자)가 `label_encodings` 파일에서 최소 레이블 필드에 지정하는 민감도 레이블은 시스템의 하한을 설정합니다.

multilevel desktop(다중 레벨 데스크탑) Trusted Extensions로 구성된 Oracle Solaris 시스템에서 사용자는 특정 레이블에서 데스크탑을 실행할 수 있습니다. 사용자에게 2개 이상의 레이블에서 작업할 권한이 있는 경우 사용자는 개별 작업 공간을 만들어 각 레이블에서 작업할 수 있습니다. 이 다중 레벨 데스크탑에서 권한있는 사용자는 다른 레이블의 창 사이에서 잘라내어 붙여넣기할 수 있으며, 다른 레이블에서 메일을 수신하고, 다른 레이블의 작업 공간에서 레이블이 있는 창을 보고 사용할 수 있습니다.

multilevel port(MLP, 다중 레벨 포트) Trusted Extensions로 구성된 Oracle Solaris 시스템에서 MLP는 한 영역에서 다중 레벨 서비스를 제공하는 데 사용됩니다. 기본적으로 X 서버는 전역 영역에 정의된 다중 레벨 서비스입니다. MLP는 포트 번호와 프로토콜로 지정됩니다. 예를 들어 다중 레벨 데스크탑용 X 서버의 MLP는 6000-6003 및 TCP로 지정됩니다.

naming service(이름 지정 서비스) 시스템 간 상호 통신할 수 있도록 네트워크상의 모든 시스템에 대한 핵심 시스템 정보를 포함하는 분산 네트워크 데이터베이스입니다. 이러한 서비스가 없으면 각 system(시스템)이 로컬 `/etc` 파일에 자체 시스템 정보 복사본을 유지해야 합니다.

networked systems(네트워크로 연결된 시스템) 하드웨어 및 소프트웨어를 통해 연결된 시스템 그룹이며 로컬 영역 네트워크(LAN)라고도 합니다. 시스템이 네트워크에 연결되면 일반적으로 하나 이상의 서버가 필요합니다.

non-networked systems(네트워크로 연결되지 않은 시스템) 네트워크에 연결되지 않았거나 다른 호스트에 의존하지 않는 컴퓨터입니다.

open network(개방형 네트워크) 다른 네트워크에 물리적으로 연결되어 있으며 Trusted Extensions 소프트웨어를 사용하여 비 Trusted Extensions 호스트와 통신하는 Trusted Extensions 호스트의 네트워크입니다. closed network(폐쇄형 네트워크)와 반대입니다.

permission bits(권한 비트) 파일 또는 디렉토리를 읽거나 쓰거나 실행할 수 있는 사람을 나타내는 비트 세트를 소유자가 지정하는 discretionary access control(임의 액세스 제어) 유형입니다. 각 파일이나 디렉토리에 세 가지 사용 권한 세트가 지정됩니다. 세트 하나는 소유자에 대한 권한이고, 다른 하나는 소유자의 그룹에 대한 권한, 나머지 하나는 기타 모든 사용자에 대한 권한입니다.

privilege(권한) 명령을 실행 중인 프로세스에 부여되는 권한입니다. 기본 기능부터 관리 기능까지 시스템의 모든 기능을 설명하는 전체 권한 세트입니다. 시스템의 클럭 설정과 같이 security policy(보안 정책)을 우회하는 권한은 사이트의 security administrator(보안 관리자)가 부여할 수 있습니다.

process(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 사용자로부

터 여러 보안 속성을 수신합니다. 프로세스가 수신하는 보안 속성에는 실행 중인 명령에 사용 가능한 권한과 현재 작업 공간의 sensitivity label(민감도 레이블)이 포함됩니다.

profile shell(프로파일 셸) 권한, 권한 부여, 특수 UID 및 GID와 같은 보안 속성을 인식하는 특수 셸입니다. 일반적으로 프로파일 셸은 사용자가 실행할 수 있는 명령 개수를 제한하지만 더 높은 권한으로 이러한 명령을 실행하도록 허용할 수 있습니다. 프로파일 셸은 trusted role(신뢰할 수 있는 역할)의 기본 셸입니다.

remote host(원격 호스트) 로컬 시스템과 다른 시스템입니다. 원격 호스트는 unlabeled host(레이블이 없는 호스트)이거나 labeled host(레이블이 있는 호스트)일 수 있습니다.

rights profile(권한 프로파일) 명령과 이러한 실행 파일에 지정된 보안 속성에 대한 번들 방식입니다. 권한 프로파일을 사용하여 Oracle Solaris 관리자는 각 명령을 실행할 수 있는 사용자를 제어하고 명령 실행 시 명령의 속성을 제어할 수 있습니다. 사용자가 로그인하면 해당 사용자에게 지정된 모든 권한이 적용되며, 사용자는 해당 사용자의 모든 권한 프로파일에 지정된 모든 명령 및 권한 부여에 액세스할 수 있습니다.

role(역할) 역할은 로그인할 수 없는 점을 제외하고 사용자와 비슷합니다. 일반적으로 역할은 관리 기능을 지정하는 데 사용되며 특정 명령 및 권한 부여 세트에 대해서만 사용할 수 있습니다. administrative role(관리 역할)을 참조하십시오.

security administrator(보안 관리자) 민감한 정보를 보호해야 하는 조직에서 사이트의 security policy(보안 정책)을 정의하고 적용하는 사람입니다. 이러한 사용자는 사이트에서 처리되는 모든 정보에 액세스할 수 있습니다. 소프트웨어에서 보안 관리자 administrative role(관리 역할)은 적절한 clearance(클리어런스)를 가진 한 명 이상의 사용자에게 지정됩니다. 이러한 관리자는 소프트웨어가 사이트의 보안 정책을 적용하도록 모든 사용자와 호스트의 보안 속성을 구성합니다. system administrator(시스템 관리자)와 비교해 보십시오.

security attribute(보안 속성) Trusted Extensions security policy(보안 정책)을 적용하는 데 사용되는 속성입니다. process(프로세스), 사용자, 영역, 호스트, 할당 가능 장치 및 기타 객체에 다양한 보안 속성 세트가 지정됩니다.

security label set(보안 레이블 세트) tnrhtp database(tnrhtp 데이터베이스) 항목에 대해 별개의 보안 레이블 세트를 지정합니다. 보안 레이블 세트가 설정된 템플리트에 지정된 호스트는 레이블 세트에서 모든 레이블에 일치하는 패킷을 보내고 받을 수 있습니다.

security policy(보안 정책) Trusted Extensions 호스트에서 정보에 액세스하는 방법을 정의하는 DAC, MAC 및 레이블 지정 규칙 세트입니다. 고객 사이트에서, 사이트에서 처리되는 정보의 민감도를 정의하고 허용되지 않은 액세스로부터 정보를 보호하는 데 사용되는 대책을 정의하는 규칙 세트입니다.

security template(보안 템플리트) `tnrhtp` 데이터베이스에서 Trusted Extensions 네트워크에 액세스할 수 있는 호스트 클래스의 보안 속성을 정의하는 레코드입니다.

sensitivity label(민감도 레이블) 객체 또는 프로세스에 지정된 보안 label(레이블)입니다. 레이블은 포함된 데이터의 보안 레벨에 따라 액세스를 제한하는 데 사용됩니다.

separation of duty(책임 구분) 사용자를 만들고 권한을 부여하기 위해 두 명의 관리자나 역할이 필요한 보안 정책입니다. 한 명의 관리자나 역할은 사용자 및 사용자의 홈 디렉토리를 만들고 기타 기본적인 관리 업무를 담당합니다. 다른 관리자나 역할은 암호 및 레이블 범위 등 사용자의 보안 속성을 담당합니다.

system accreditation range(시스템 승인 범위) security administrator(보안 관리자)가 label_encodings file(label_encodings 파일)에 정의한 규칙에 따라 만들어진 모든 유효한 레이블 세트와 Trusted Extensions로 구성된 모든 시스템에서 사용되는 두 개의 관리 레이블입니다. 관리 레이블은 `ADMIN_LOW`와 `ADMIN_HIGH`입니다.

system administrator(시스템 관리자) Trusted Extensions에서 사용자 계정의 비보안 부분을 설정하는 것처럼 표준 시스템 관리 작업을 담당하는 사용자에게 지정되는 trusted role(신뢰할 수 있는 역할)입니다. security administrator(보안 관리자)와 비교해 보십시오.

system(시스템) 컴퓨터의 일반 이름입니다. 설치 후 네트워크의 시스템을 호스트라고도 합니다.

tnrhdb database(tnrhdb 데이터베이스) 신뢰할 수 있는 네트워크 원격 호스트 데이터베이스입니다. 이 데이터베이스는 원격 호스트에 레이블 특성 세트를 지정합니다. 데이터베이스는 `/etc/security/tsol/tnrhdb`의 파일로 액세스할 수 있습니다.

tnrhtp database(tnrhtp 데이터베이스) 신뢰할 수 있는 네트워크 원격 호스트 템플리트입니다. 이 데이터베이스는 원격 호스트에 지정할 수 있는 레이블 특성 세트를 정의합니다. 데이터베이스는 `/etc/security/tsol/tnrhtp`의 파일로 액세스할 수 있습니다.

Trusted Network databases(신뢰할 수 있는 네트워크 데이터베이스) 신뢰할 수 있는 네트워크 원격 호스트 템플리트 `tnrhtp`와 신뢰할 수 있는 네트워크 원격 호스트 데이터베이스 `tnrhdb`는 Trusted Extensions 시스템이 통신할 수 있는 원격 호스트를 정의합니다.

trusted path(신뢰할 수 있는 경로) Trusted Extensions로 구성된 Oracle Solaris 시스템에서 신뢰할 수 있는 경로는 무단 변경을 방지하고 믿을 수 있는 시스템과의 상호 작용 방법입니다. 신뢰할 수 있는 경로는 관리 기능이 손상되지 않도록 하는 데 사용됩니다. 암호 변경과 같이 보호해야 하는 사용자 기능에서도 신뢰할 수 있는 경로가 사용됩니다. 신뢰할 수 있는 경로가 활성 상태이면 데스크탑에는 무단 변경 방지 표시기가 나타납니다.

trusted role(신뢰할 수 있는 역할) administrative role(관리 역할)을 참조하십시오.

trusted stripe(신뢰할 수 있는 스트라이프) 스푸핑할 수 없는 영역입니다. Trusted GNOME에서 스트라이프는 맨 위에 있습니다. 스트라이프는 윈도우 시스템 상태에 대한 시각적 피드백인 신뢰할 수 있는 경로 표시기 및 윈도우 sensitivity label(민감도 레이블)을 제공합니다. 민감도 레이블이 사용자에게 보이지 않도록 구성된 경우 신뢰할 수 있는 스트라이프는 신뢰할 수 있는 경로 표시기만 보여 주는 아이콘으로 축소됩니다.

txzonemgr script(txzonemgr 스크립트) `/usr/sbin/txzonemgr` 스크립트는 레이블이 있는 영역을 관리하기 위한 간단한 GUI를 제공합니다. 스크립트는 네트워킹 옵션에 대한 메뉴 항목도 제공합니다. `txzonemgr`은 전역 영역에서 루트에 의해 실행됩니다.

unlabeled host(레이블이 없는 호스트) Oracle Solaris OS를 실행하는 시스템과 같이 레이블이 없는 네트워크 패킷을 보내는 네트워크로 연결된 시스템입니다.

unlabeled system(레이블이 없는 시스템) Trusted Extensions로 구성된 Oracle Solaris 시스템에서 레이블이 없는 시스템은 MLS가 사용으로 설정된 SELinux 또는 Trusted Extensions와 같은 다중 레벨 운영 체제를 실행하지 않는 시스템입니다. 레이블이 없는 시스템은 레이블이 있는 패킷을 전송하지 않습니다. 통신 중인 Trusted Extensions 시스템이 레이블이 없는 시스템에 단일 레이블을 지정한 경우 해당 레이블에서 Trusted Extensions 시스템과 레이블이 없는 시스템 간의 네트워크 통신이 발생합니다. 레이블이 없는 시스템은 "단일 레벨 시스템"이라고도 합니다.

user accreditation range(사용자 승인 범위) 일반 사용자가 system(시스템)에서 작업할 수 있는 가능한 모든 레이블의 세트입니다. 사이트의 security administrator(보안 관리자)가 label_encodings file(label_encodings 파일)에서 범위를 지정합니다. system accreditation range(시스템 승인 범위)가 파일의 `ACCREDITATION RANGE` 섹션 값(상한, 하한, 제약 조건 및 기타 제한의 조합)에 의해 추가적으로 제한된다는 것을 정의하는 올바른 형식의 레이블에 대한 규칙입니다.

user clearance(사용자 클리어런스) 사용자가 언제든지 작업할 수 있는 레이블 세트의 상한을 설정하며 clearance(클리어런스)가 지정하는 security administrator(보안 관리자)입니다. 사용자는 기본값을 사용할 수도 있고 특정 로그인 세션 중 해당 클리어런스를 더 제한할 수도 있습니다.

색인