eTrust® Access Control for Windows

시작하기

r8 SP1

CA 제품 참조

이 문서는 다음 CA 제품을 참조합니다 :

- eTrust® Access Control(eTrust AC)
- eTrust® Single Sign-On(eTrust SSO)
- eTrust® Web Access Control(eTrust Web AC)
- eTrust® CA-Top Secret®
- eTrust® CA-ACF2®
- eTrust® Audit
- Unicenter® TNG
- Unicenter® Network and Systems Management(Unicenter NSM)
- Unicenter® Software Delivery

기술 지원 정보

온라인 기술 지원 및 위치, 서비스 시간 , 전화 번호에 대한 자세한 정보는 http://www.ca.com/camap.htm 에서 기술 지원부에 문의하시기 바랍니다.

목차

제 1 장: e-비즈니스를 위한 전방위 보안 소개

이 장은 아래의 주제를 포함하고 있습니다:

이 가이드의 목적

이 안내서는 eTrust AC 에 대해 소개합니다. 본 가이드를 읽고 나면 다양한 제품에 대한 개요를 파악하고 제품의 유용성을 잘 알 수 있습니다. eTrust AC 를 사용하기 전에 먼저 익숙해지는 것이 좋습니다.

CA 기술 서비스: 기업 IT 환경 관리의 비전을 실행

CA Technology Services™는 기업의 IT 관리 솔루션을 제공하여 고객으로 하여금 더 효율적인 작업을 수행하고 IT 인프라 관리를 개선하도록 도움으로써 좀 더 유효한 비즈니스 가치와 경제적인 결과를 내도록 합니다. CA Technology Services 는 글로벌 전문 지식을 비롯하여 기업 시스템 관리 분야, 비즈니스 서비스 최적화, 보안 관리 및 저장 관리 분야의 공인된 전문가군을 최대로 활용하여 고객의 IT 투자 효과를 최대화합니다.

27 년 이상 축적된 관리 소프트웨어 분야에서의 경험, 1,000 여 명의 기술 서비스 전문가(대부분 CISSP, ITIL 및 SNIA 공인 전문가임) 및 업계 유수의 서비스 파트너사와의 상호 보완적인 서비스 제공 능력 등을-십분 발휘하여 고객에게 최고의 전략과 세월의 검증을 거친 방법을 제공합니다.

교육 및 훈련: CA 기술의 비즈니스 가치 최대화

CA Technology Services 의 교육과 훈련은 간결해진 구현 방법, 가치 대비 투자 시간 절감, 생산성 개선 덕분에 CA 기술의 비즈니스 가치 최대화를 고객이 실감하는 데 초점을 맞추고 있습니다. 기업 IT 관리(EIM)를 위한-CA 의 총체적, 통합 개방 솔루션을 주제로 강사 지도 하에 스스로 스케줄을 조정할 수 있는 확장된 학습 솔루션을 제공합니다. 또한, 선도적인 부가 가치 교육 제공업체와 파트너 관계를 맺어 수업 과정을 기업 시스템 관리, 보안 관리, 저장 관리 및 비즈니스 서비스 최적화 분야로도 확대하고 있습니다. 숙련된 공인 전문가 팀이 CA 소프트웨어 제품 최적화 및 입증된 IT 프로세스 모델을 활용하는 데 있어 최신 전문 지식을 전달함으로써 고객의 IT 환경에서의 최고의 전략을 실질적으로 응용하는 방법에 대해 교육합니다.

교육 및 훈련 과정에 대한 전체 목록은 http://ca.com/education 을 참조하십시오.

eTrust 솔루션

eTrust 솔루션은 조직의 환경을 쉽게 보호할 수 있도록 하는 혁신적인 기술을 제공하므로 e-비즈니스를 활성화할 수 있습니다. 이 포괄적인 보안 제품군은 위험 평가, 공격 탐지, 손실 방지 등을 포함한 솔루션으로 모든 e-비즈니스에 대한 더 많은 기회를 제공합니다. 조직은 eTrust 를 사용하여 보안 솔루션을 독립 실행형 제품이나 보안 제품군 또는 Unicenter NSM 과 완전히 통합된 제품으로 자유롭게 배치할 수 있는-유연성을 확보합니다. eTrust 솔루션을 Unicenter TNG 와 함께 사용하면 광범위한 엔터프라이즈 관리 작업의 일부로 보안의 생성, 배치 및 관리에 일관되게 접근할 수 있습니다.

CA: e-비즈니스를 관리하는 소프트웨어

차세대 e-비즈니스는 기존 비즈니스 인프라를 활용하고 새로운 기술을 채택함으로써 제한되지 않은 여러 기회를 보장합니다. 동시에 조직 영역 전체에 걸쳐 컴퓨팅 장치 관리에서 응용 프로그램, 데이터 및 비즈니스 프로세스의 통합 및 관리에 이르기까지 매우 복잡해지는 관리가 문제입니다. CA 에서 그 해답을 찾으십시오. e-비즈니스가 이러한 중요한 문제를 해결할 수 있도록 지원하는 솔루션을 CA 가 보유하고 있습니다. 업계 최고의-eBusiness Process Management, eBusiness Information Management 및 eBusiness Infrastructure Management 제품을 통해 CA 는 오늘날 확장된 글로벌 경제 환경에서 모든 이해 관계자를 만족시키는 종합적인 첨단 솔루션만을 제공합니다.

추가 정보

이 사용 설명서를 읽고 난 후에는 다양한 형태로 제공되는 리소스에서 추가 정보를 참조할 수 있습니다. 제품 CD 에는 소프트웨어를 소개하고, 제품의 포괄적이고도 기능이 풍부한 구성 요소에 대한 상세한 설명을 제공하는 사용 설명서가 들어 있습니다.

도움이 필요하면 기술 지원 부서(http://ca.com/support)에 문의하십시오.

귀하의 개방형 분산 네트워크 환경은 정말로 안전합니까?

대부분의 기업은 금융 거래, 고객 정보 및 인사 기밀 기록 등과 같은 중요한 정보를 분산 서버에 보관하고 있습니다. 이에 따라 중요한 데이터를 보호하고 액세스를 제어하는 것이 주요 비즈니스 요구사항이 되었습니다. 안타깝게도 개방형 시스템 서버는 적절한 데이터 보안 기능을 제공하지 못합니다. 실제로 분산 서버는 기본 운영 체제가 가지는 허점으로 인해 인가되지 않은 접근에 취약한 것이 사실입니다. Windows 및 UNIX 운영 체제는 응용 프로그램, 데이터 및 감사 로그에 대한 모든 권한을 가진 단일 사용자 계정을 통해 보안 문제가 발생하는 *수퍼유저* 관리자 개념을 기반으로 작성되었습니다.

참고: 별도로 지정되지 않은 경우 "Windows"는 eTrust AC에서 지원하는 모든 Microsoft Windows 운영 체제를 나타냅니다.

Windows 및 UNIX Superuser 권한

이와 같은 시스템의 가장 심각한 문제 중 하나는 시스템의 수퍼유저 또는 관리자를 통한 위험 경로의 단일화입니다. 관리자는 모든 작업을 실행하고 시스템에 있는 전체 파일을 보거나 수정할 수 있는 특수 권한을 가진 사용자입니다. 이 계정은 시스템 서비스를 종료하고 중요한 파일을 삭제할 수 있을 뿐만 아니라 기밀 정보에 접근하고 자체 감사 추적을 제거할 수 있기 때문에 계정의 단일화는 이러한 운영 체제에서 가장 큰 위험 요소 중 하나로 간주됩니다. 동시에 수퍼유저 계정은 데이터 백업, 계정 작성 및 삭제 또는 암호 재설정을 위해 다른 시스템 관리자에게 빈번하게 부여됩니다. 일단 계정이 노출되면 해커들은 실제 원하는 모든 작업을 수행할 수 있기 때문에 수퍼유저 계정은 해커들의 최우선 공략 대상이 되는 사용자 계정입니다.

사용자 환경 보안

eTrust AC 를 사용하면 기업에서 사용자 액세스 권한을 중앙 집중식으로 관리하고 미리 구성된 기본 보안 정책을 신속하게 배포할 수 있습니다. eTrust AC 는 올바른 사용자가 올바른 정보에 액세스하도록 합니다. 조직 전체의 Windows 시스템 서버에 위치한 데이터와 응용프로그램에 대한 액세스에 보안이 적용됩니다.

eTrust AC 는 DSX(Dynamic Security Extension) 기술을 통해 신뢰할 수 있고 침입이 불가한 보호 기능을 제공합니다. DSX 는 운영 체제 커널을 영구적으로 변경하지 않고도 보안 관련 실시간 요청을 동적으로 인터셉트합니다. 서버 처리 작업을 방해하지 않으면서 상당히 높은 수준의 보안이 제공됩니다. eTrust AC 의 일반 파일 보호와 같은 고급 기능은 Windows 운영 체제의 보안을 현저히 향상시킵니다. 조직에서는 일반 파일 보호 기능으로 관련 파일 또는 프로그램 그룹을 보호하기 위해 와일드카드 옵션을 사용할 수 있습니다. 이 기능을 통해 강력한 일반 액세스 정책을 쉽게 개발할 수 있습니다.

호스트 기반 침입 방지

eTrust AC 는 외부 웜 공격이나 멀웨어 피해 등의 보안 위험을 줄여 주는 HIPS(Host-based Intrusion Prevention System)의 여러 가지 기능을 제공합니다. eTrust AC 의 스택 오버플로 보호(STOP) 기능, 트로이 목마 방지 기능, 미리 정의된 응용 프로그램 보안 템플릿 샘플, 응용 프로그램 동작 프로필 프로그램 등을 통해 관리자는 더 강력하게 중요 서버를 보호할 수 있고 시스템 취약성 해결과 보안 패치 배포 등을 수행할 시간을 더 확보할 수 있습니다.

데이터 및 응용프로그램 보호

조직의 성공은 조직이 소유한 데이터와 응용 프로그램의 무결성 및 프라이버시에 달려 있습니다. eTrust AC 에서 사용자와 프로그램은 필요한 정보에 올바르게 액세스할 수 있으므로 권한 없는 모든 정보 요청은 금지되고 로그 파일에 기록됩니다.

eTrust AC 는 향상된 응용 프로그램 보안을 위해 사용자 지정 보안 정책을 제공합니다. CA 는 eTrust AC 에서 특정 응용 프로그램에 대한 액세스를 제어할 수 있도록 업계 선두의 소프트웨어 공급업체들과도 파트너 관계를 맺고 있습니다. 이러한 "강력한" 솔루션은 업무상 중요한 응용 프로그램에 대한 완벽한 보호를 제공합니다.

사용자 계정 및 암호 관리

기업들이 e-비즈니스 시장에서 그 규모가 커지면서 서로 다른 지역적 위치 또는 시스템 도메인 및 다양한 부서의 사용자를 관리하는 것이 시스템 관리자의 중요한 업무가 되었습니다. 각각 시스템이나 플랫폼에서 사용자 계정 암호 및 보안 정책을 동기화하면 오류가 쉽게 발생하고, 프로세스가 복잡하게 되고, 반응 시간 및 비용이 늘어날 수 있는 등 여러 가지 문제가 발생할 수 있습니다.

다수의 서버 보안

네트워크상의 여러 서버 보안에 대한 문제를 해결하기 위해 eTrust AC 는 정책 모델 데이터베이스(PMDB) 인프라를 제공합니다. PMDB 를 사용하면 계정, 암호 및 보안 정책 동기화 작업을 구독된 계층 노드에서 안전하고 정확하게 실행할 수 있습니다. eTrust AC 의 중요한 한 가지 설계 목표는 네트워크 연결이 제대로 작동하지 않는 경우에도 해당 서버에 대한 보안을 강제로 적용하는 것입니다. 결과적으로 규칙이 분산되어 각 서버는 자체 보안을 유지할 수 있습니다.

일관된 교차 플랫폼 보안 수준 올리기

eTrust AC 는 전반적인 비즈니스 요구 사항을 충족하기 위해 각 시스템의 보안 수준을 올립니다. 하나의 eTrust AC 보안 정책을 중앙에서 작성하고 다양한 Windows 및 UNIX 운영 체제에 자동으로 배포 및 적용할 수 있습니다. 결과적으로 최소한의 시간과 노력으로 강력하면서 일관된 수준의 서버 보안이 구축됩니다.

eTrust AC 를 사용하지 않을 경우 관리자는 컴퓨팅 시스템에 대해 별도의 보안 정책을 생성하고 유지 관리해야 하므로 엄청난 시간과 노력이 요구됩니다. 또한 회사 전체의 보안 표준은 종종 가장 낮은 보안 수준의 시스템을 기반으로 하므로 조직 대부분의 보안 요구 사항을 충족하기가 어렵습니다.

정책은 기업 전체를 기반으로 생성, 관리 및 배포하거나 특정 응용 프로그램의 보안 요구 사항을 만족시키도록 사용자 지정할 수 있습니다. 이러한 완벽한 솔루션은 회계나 연구 개발부와 같은 부서 단위에서 대기업에 이르는 모든 조직에 배포할 수 있습니다. 강화된 운영 체제 보안, 완벽한 감사 기능 및 플랫폼 간 액세스 제어 기능으로 프로그램이 배포된 시스템의 중요 프로세스 및 정보를 보호합니다.

개방형의 확장성 있는 이 강력한 솔루션은 모든 업계 표준 플랫폼, 데이터베이스 및 응용 프로그램을 지원하며 모든 리소스를 보호할 수 있도록 출시된 인터페이스를 포함하고 있습니다. eTrust AC 는 Unicenter TNG 와 통신함으로써 기업 관리의 더 큰 작업의 일부인 보안 구축, 배포 및 관리를 수행할 포괄적이면서 강력한 솔루션을 제공할 수 있습니다.

특별한 기능

eTrust AC 에서는 기업 보안을 관리하기 위해 여러 기능을 제공합니다.

중앙 집중식 관리

eTrust AC 는 중앙 집중식 관리를 통해 관리자 워크스테이션과 단일 지점에서 eTrust AC 가 설치된 다른 모든 워크스테이션을 관리할 수 있습니다.

자체-보호

자체-방어 메커니즘으로 인해 해커나 다른 사용자는 eTrust AC 서비스를 중단할 수 없습니다. 이 메커니즘은 eTrust AC 파일과 감사 데이터도 보호합니다.

프로필 그룹

eTrust AC 에서는 그룹 멤버쉽을 기반으로 보안 역할을 설정할 수 있습니다. 예를 들어, 관리자 그룹과 이 그룹의 구성원인 사용자에게 부여되는 권한을 제한할 수 있습니다.

레지스트리 보호

eTrust AC 는 권한 없는 사용자가 시스템 매개 변수를 변경하지 않도록 레지스트리를 보호합니다. 권한 있는 사용자가 필요에 따라 레지스트리 설정을 업데이트할 수 있습니다.

프로세스 보호

eTrust AC 에서는 프로세스가 종료되지 않도록 지정된 프로세스를 보호합니다. 또한 eTrust AC 프로세스 보호는 Windows 서비스 및 기타 비대화식 Windows 응용 프로그램을 보호하는 데도 유용합니다.

네트워크 보호

eTrust AC 는 들어오고 나가는 네트워크 연결을 규정하여 네트워크 서비스 및 포트에 대한 액세스를 제어합니다.

SPECIALPGM 보호

eTrust AC 에서는 논리 사용자만 액세스할 수 있도록 SYSTEM 계정으로 보통 실행되어야 하는 지정된 프로그램(예: 시스템 서비스)을 보호합니다.

로그온 보호

eTrust AC 는 계정 만료일부터 요일 및 시간 제한에 이르는 여러 방법으로 사용자 로그온을 제한할 수 있습니다.

프로그램 및 파일 서명

eTrust AC 에서는 서명을 부여하여 프로그램 및 파일을 보호합니다. 서명이 변경된 경우, 프로그램 또는 파일은 트러스트되지 않게 되어 액세스할 수 없습니다.

작업 위임

eTrust AC 는 일반 사용자가 관리 작업을 수행할 수 있도록 필요한 권리 및 권한을 부여할 수 있습니다. 이것을 작업 위임이라고 부릅니다. 이런 방식으로 작업을 위임할 수 있는 권한(관리자 권한 부여)은 eTrust AC 의 중요한 장점 중 하나입니다.

향상된 파일 보호

eTrust AC 는 현재 Windows 에서 사용되는 모든 파일 시스템 즉, NTFS(Windows 파일 시스템) 및 FAT(파일 할당 테이블)를 보호합니다. eTrust AC 는 CDFS 및 HPFS 도 지원합니다.

STOP(스택 오버플로 보호)

STOP 을 사용하면 해커가 시스템에 침입하기 위해 임의의 명령을 실행할 수 있는 스택 오버플로우가 사용되지 않습니다.

교차-플랫폼 지원

관리자는 비슷하거나 동일한 Windows 및 UNIX 컴퓨터의 보안 정책을 만들고 구현하며 유지 관리할 수 있습니다.

Active Directory 지원

많은 조직들이 사용자 데이터 저장소를 Active Directory 또는 LDAP 기반 리포지토리로 중앙 집중화하는 추세입니다. eTrust AC 는 eTrust Identity and Access Management 을 통해 외부 사용자(외부 리포지토리에서 정의된 사용자)를 지원합니다. 즉 이것이 외부 디렉터리에 있는 사용자들을 정의할 수 있고 eTrust Identity and Access Management 은 이 사용자들을 eTrust AC 데이터베이스에 연결합니다. eTrust AC 는 또한 Active Directory 또는 SAM(Security Account Manager), Windows NT 사용자 계정 데이터베이스 에 있는 기본 사용자를 생성하거나 수정 또는 삭제할 수 있습니다.

정책 모델 관리

eTrust AC는 관리자가 정책 설정-버전 관리로 부서 보안 정책을 쉽게 관리할 수 있는 독립 실행형 정책 관리자 시스템을 제공하여 모든 구독 서버가 최신 보안 정책을 얻었는지 확인하고 용이하게 버전을 제어할 수 있습니다.

eTrust AC 를 사용하면 다음 두 가지 방식으로 단일 중앙 컴퓨터에서 여러 데이터베이스를 관리할 수 있습니다.

- 자동 규칙 기반 정책 업데이트

  PMDB 에서 정의한 일반 규칙은 자동으로 구성된 계층의 데이터베이스에 전파됩니다.

- 고급 정책 기반 관리 및 보고

  중앙 위치에서 저장한 정책(규칙 그룹)이 배포되어 구성된 계층의 모든 데이터베이스에 전파될 수 있습니다. 또한 배포된 정책 버전을 제거하고(배포 취소) 배포 상태, 배포 편차 및 배포 계층에 대해 보고할 수 있습니다. 이 기능을 사용하려면 추가 구성 요소를 설치하고 구성해야 합니다.

응용 프로그램 정책 생성기

자동화 정책 생성기 프로그램을 사용하여 응용 프로그램 동작을 프로필하고 그에 따른 보안 정책을 생성합니다. 응용 프로그램에 Security Envelope 를 작성하고 규칙을 구성하는 데 필요한 배포 작업을 상당히 줄여줍니다.

제 2 장: 운영 체제 보안 강화

이 장은 아래의 주제를 포함하고 있습니다:

구성요소, 기능 및 설치 고려사항

새로운 개방형 및 분산 컴퓨팅 패러다임은 컴퓨터 보안에 대한 요구를 계속해서 증대시키고 있으며 다른 플랫폼 간의 통합 작업이 더욱 더 복잡해지고 있습니다. 일관된 보안 적용 범위에서 개별 시스템을 처리할 수 있는 보안 솔루션을 사용하려는 요구가 보안 목록에서 중요한 항목으로 대두되고 있습니다. 대기업의 인수 및 합병 사례가 그 어느 때보다 빈번해짐에 따라 폭발적인 확장 기능, 분산 용량, 능률적인 중앙 집중식 관리 및 교차 플랫폼 지원 등을 비롯한 새로운 수준의 보안 요구사항이 추가되고 있습니다.

eTrust AC에 기본 제공된 정책은 각 조직에게 즉각적인 결과를 바로 사용할 수 있도록 제공합니다. 개방형의 확장성 있는 이 강력한 솔루션은 모든 업계 표준 플랫폼, 데이터베이스 및 응용 프로그램을 지원하며 모든 리소스를 보호할 수 있도록 출시된 인터페이스를 포함하고 있습니다.

중앙 집중화된 사용자 및 액세스 관리의 편리한 사용을 통해 조직은 오늘날의 e-비즈니스 기회를 십분 이용할 수 있습니다. eTrust 보안 솔루션의 일부인 eTrust AC는 Unicenter NSM과 상호 운용됨으로써 기업을 관리하는 더 큰 작업의 일부로 보안을 구축, 배포 및 관리하기 위한 포괄적이면서 강력한 솔루션을 제공할 수 있습니다.

eTrust AC 의 구성 요소

eTrust AC 에는 데이터베이스(seosdb), 드라이버 두 개(seosdrv 및 drveng), 많은 서비스(Watchdog, Agent, 엔진, 정책 모델 및 작업 위임 포함) 및 GUI 가 있습니다.

데이터베이스

데이터베이스에는 조직에 있는 사용자 및 그룹의 정의, 보호해야 하는 시스템 리소스와 시스템 리소스에 대한 사용자 및 그룹의 액세스를 제어하는 규칙이 있습니다.

드라이버

드라이버는 파일 열기, 레지스트리 키 열기, 프로세스 종료 또는 네트워크 활동 수행의 모든 요청을 인터셉트합니다. 드라이버는 이러한 요청을 엔진에 전달하고 요청이 허용될지 거부될지에 대한 엔진의 결정을 수신하며 해당 결정을 운영 체제의 기존 시스템 호출로 전달한 후 드라이버로부터 수신하는 응답에 따라 계속 처리합니다.

Watchdog

Watchdog 은 다른 eTrust AC 서비스가 실행 중인지 계속 확인합니다. 드물지만 Watchdog 이 중지된 다른 서비스를 발견한 경우 서비스가 즉시 다시 시작됩니다.

에이전트

에이전트는 TCP/IP 를 통해 고유 응용 프로그램 프로토콜에서 eTrust AC 클라이언트와 통신하고 eTrust AC 사용자의 보안을 관리합니다.

엔진

엔진은 모든 데이터베이스 업데이트 제어, 드라이버 및 에이전트로부터 수신된 액세스 요청 허용 여부 결정, Watchdog 서비스의 실행 여부 확인 및 Watchdog 실행이 중지된 경우 Watchdog 다시 시작을 포함하는 데이터베이스 관리 작업을 수행합니다.

엔진은 데이터베이스 액세스 요청 및 의사 결정 기능을 처리하여 프로세스 간 통신을 최소로 줄이면서 최대의 효과를 얻습니다.

정책 모델

수많은 데이터베이스를 개별적으로 관리하는 것은 사실상 어려우므로 eTrust AC 는 한 컴퓨터에서 많은 컴퓨터를 관리할 수 있는 구성 요소인 정책 모델 서비스를 제공합니다. 정책 모델 서비스를 사용하는 것은 선택사항이지만 큰 사이트에서 이 서비스를 사용하면 관리 작업이 상당히 간단해집니다.

작업 위임

eTrust AC 는 일반 사용자가 관리 작업을 수행할 수 있도록 필요한 권리 및 권한을 부여할 수 있습니다. 이것을 작업 위임이라고 부릅니다.

그래픽 사용자 인터페이스

정책 관리자는 모든 eTrust AC 기능이 수행되는 그래픽 사용자 인터페이스(GUI)입니다.

참고: 정책 관리자에 대한 자세한 내용은 *관리자 가이드*를 참조하십시오.

eTrust AC 의 기능

eTrust AC 를 사용하면 중앙 위치에서 기본 Windows 를 관리할 수 있으며 기본 Windows 보안이 상당히 향상됩니다. eTrust AC 에는 자체 보호 기능도 있습니다. 다음 절에서 이 기능을 설명합니다.

Windows 관리

eTrust AC 를 조직의 Windows 스테이션에 설치했으면 속해 있는 도메인에 상관 없이 하나의 중앙 스테이션에서 모든 스테이션을 관리할 수 있습니다. 이 작업을 수행하려면 정책 관리자를 사용하거나 selang 명령줄 언어를 사용하십시오.

정책 관리자

정책 관리자는 eTrust AC 의 그래픽 사용자 인터페이스(GUI)입니다. 정책 관리자를 사용하여 eTrust AC 의 모든 기능을 수행할 수 있습니다.

참고: 정책 관리자에 대한 자세한 내용은 *관리자 가이드*를 참조하십시오.

selang

Selang 은 eTrust AC 의 명령줄 언어입니다. selang 을 사용하여 스크립트를 작성할 수도 있습니다. 정책 관리자의 명령 및 스크립트 도구 또는 명령 프롬프트 창에서 selang 을 호출하여 selang 명령을 실행할 수 있습니다.

참고: selang 및 해당 명령에 대한 자세한 내용은 *참조 가이드*를 참조하십시오.

eTrust AC 자체 방어

해커나 사용자가 고의적으로 또는 실수로 eTrust AC 서비스를 다운시키는 것은 불가능합니다. eTrust AC 는 특수 파일 서명을 사용하므로 eTrust AC 가 실행 중일 때 권한 없는 사용자가 eTrust AC 파일과 데이터를 변경하거나 지우는 것은 불가능합니다.

관리자 계정 제한

Windows 를 관리하는 사용자는 일반적으로 시스템 설치 중 자동으로 작성되는 미리 정의된 그룹의 구성원입니다. 각각의 미리 정의된 그룹은 특정 시스템 기능을 실행하기 위해 존재합니다. 그룹의 구성원인 사용자는 해당 그룹의 모든 기능을 실행할 수 있습니다.

Windows 에서 가장 강력한 그룹은 Administrators 그룹이며, Administrators 그룹에서 관리자라는 하나의 계정을 작성합니다. Administrators 그룹의 모든 구성원은 사용자 작성, 삭제 및 수정에서 서버 잠금, 재구성 및 종료에 이르는 광범위한 작업을 수행할 수 있습니다.

Windows 에서 가장 큰 보안 위험 중 하나는 권한 없는 사용자가 Administrators 그룹에 속한 사용자 계정을 제어할 수 있다는 점입니다. 이런 경우, 권한 없는 사용자로 인해 시스템에 엄청난 손상이 발생할 수 있습니다.

eTrust AC 를 통해 관리자 계정에 부여되는 권한을 제한하고 관리자 그룹의 구성원인 사용자의 권한을 제한할 수 있습니다. 이 기능을 통해 Windows 시스템의 취약성을 보완할 수 있습니다.

기본 Windows 보안 관리

다음과 같은 Windows 보안 요소는 eTrust AC 를 통해 관리할 수 있습니다.

레지스트리 보호

Windows 레지스트리는 장치 드라이버, 구성 상세 정보, 하드웨어, 환경 및 보안 설정을 제어하는 매개 변수를 포함한 대부분의 운영 체제 매개 변수가 있는 중앙 집중식 데이터베이스입니다.

eTrust AC 는 권한 없는 사용자가 시스템 매개 변수를 변경하지 않도록 레지스트리를 보호합니다. 권한 있는 사용자가 필요에 따라 레지스트리 설정을 업데이트할 수 있습니다.

파일 보호

Windows 에서는 서로 다른 여러 유형의 파일 시스템을 사용하는 데, 가장 많이 사용되는 파일 시스템은 FAT 과 NTFS 입니다. NTFS 파일 시스템을 사용하는 경우, Windows 는 각 파일의 Access Control 목록(ACL)을 작성하고 업데이트하여 시스템에 있는 파일을 보호합니다. eTrust AC 는 파일 ACL 을 지원합니다.

암호 보호

eTrust AC 에서는 암호를 보호할 수 있으며 기본 Windows 보안에서와 같이 암호 품질을 제한할 수 있습니다. 이 경우 자체 보유 메카니즘을 통해서 수행합니다. eTrust AC 는 다음 작업을 수행할 수 있습니다.

- 암호의 최대 사용 기간 제한
- 암호의 최소 길이 제한
- 최대 20 개의 사용자 암호 생성
- 반복되는 로그인 실패 시 계정 잠금
- 암호를 변경하기 전에 Windows 에 사용자를 강제로 로그인

Server Manager 기능

eTrust AC 에서는 Windows NT 프로그램 표시줄에 있는 서버 관리자를 통해 다른 기본 Windows 리소스를 관리할 수 있습니다. 보호되는 Windows 리소스는 다음과 같습니다.

COM

COM 클래스 레코드는 Ports 의 Control Panel 목록에 있는 직렬 포트(COM) 또는 병렬 포트(LPT)로 장치를 정의합니다.

장치

DEVICE 클래스 레코드는 Windows 하드웨어 장치를 정의합니다(Devices 의 Control Panel 목록에 있음).

디스크

DISK 클래스 레코드는 시스템 볼륨을 정의합니다.

도메인 관리

DOMAIN 클래스 레코드는 공통 데이터베이스 및 보안 정책(도메인)을 공유하는 컴퓨터의 컬렉션을 정의합니다.

프린터

PRINTER 클래스 레코드는 매체의 시각 이미지를 복제할 수 있는 Windows 컴퓨터 시스템에 연결된 장치를 정의합니다(PRINTERS 폴더 목록에 있음).

프로세스

PROCESS 클래스 레코드는 실행 프로그램, 가상 메모리 주소 집합 및 스레드로 구성된 개체를 정의합니다(Windows 작업 관리자 목록에 있음).

서비스

SERVICE 클래스 레코드는 Windows 서비스를 정의합니다(Services 의 Control Panel 목록에 있음).

공유

SHARE 클래스 레코드는 디렉터리, 파일, 프린터 및 명명된 파이프와 같은 네트워크 사용자가 이용하는 장치, 데이터 또는 프로그램을 포함하는 공유된 리소스를 정의합니다.

Windows 세션

SESSION 클래스 레코드는 로컬 호스트에 있는 사용자 세션을 정의합니다. 레코드에는 사용자 이름, 컴퓨터 이름, 연결 경과 시간 및 사용 중인 리소스가 있습니다.

기본 Windows 보안 확장

다음과 같은 eTrust AC 기능은 기본 Windows 보안을 확장합니다.

일반 사용자를 위한 관리자 권한

eTrust AC 에서는 일반 사용자에게 필요한 권한을 부여하여 해당 사용자가 관리자 그룹의 구성원이 아니더라도 관리 작업을 수행할 수 있습니다. 이것을 작업 위임이라고 부릅니다. 이런 방식으로 작업을 위임할 수 있는 권한(관리자 권한 부여)은 eTrust AC 의 중요한 장점 중 하나입니다.

향상된 파일 보호

eTrust AC 는 현재 Windows 와 함께 사용되는 모든 파일 시스템을 보호합니다. 가장 많이 사용되는 두 가지 파일 시스템은 Windows 파일 시스템(NTFS)과 파일 할당 테이블(FAT)입니다. eTrust AC 는 CD 전용 파일 시스템인 CDFS 와 OS/2 파일 시스템인 HPFS 도 지원합니다.

eTrust AC 는 파일 할당 테이블(FAT)에 대한 완전한 보안 솔루션을 제공하고, NTFS 및 CDFS 를 포함한 다른 파일 시스템에 대한 보안 계층을 추가로 제공합니다.

일반 파일 보호

일반 파일 보호는 지정된 와일드카드 패턴(정규 표현식)과 일치하는 모든 파일을 보호할 수 있는 기능입니다. 지정 와일드카드 패턴과 일치하는 이름을 가진 모든 리소스는 지정한 일반 액세스 규칙에 의해 보호됩니다. eTrust AC 에서는 파일을 전체적으로 보호할 수 있습니다.

리소스가 둘 이상의 일반 액세스 규칙과 일치할 경우, eTrust AC 는 파일과 가장 많이 일치하는 규칙을 선택합니다.

일반 파일 보호의 경우, 보호가 필요한 여러 개의 파일을 보호하기 위해 5 개 이하의 보안 규칙을 정의해야 합니다.

향상된 암호 보호

기본 Windows 보안은 사용자 암호를 상당한 보호 기능을 제공합니다 (페이지 21). 그러나 eTrust AC는 암호 보호 기능을 현저히 확장하여 해커가 암호를 알아내는 데 성공할 확률을 크게 줄여줍니다.

eTrust AC 를 사용할 때 사용자가 보다 안전하고 보안성이 높은 암호를 선택하도록 하는 규칙을 추가로 작성할 수 있습니다. 예를 들어, 사용자에게 일정한 수 이상의 알파벳, 숫자, 특수 문자, 소문자 또는 대문자를 선택하도록 요구할 수 있습니다. 또한 사용자가 선택한 새 암호에 기존 암호가 들어 가지 않으며 기존 암호에 의해 새 암호가 포함되지 않도록 지정할 수 있습니다.

프로세스 보호

eTrust AC 에서는 프로세스가 종료되지 않도록 지정된 프로세스를 보호합니다. 또한 eTrust AC 프로세스 보호는 Windows 서비스 및 기타 비대화형 Windows 응용 프로그램을 보호하는 데 유용합니다.

SPECIALPGM 보호

eTrust AC 에서는 논리 사용자만 액세스할 수 있도록 SYSTEM 계정으로 보통 실행되어야 하는 지정된 프로그램(예: 시스템 서비스)을 보호합니다.

프로그램 및 보안 파일 보호

eTrust AC 에서는 서명을 부여하여 프로그램 및 파일을 보호합니다. 서명이 변경된 경우, 프로그램 또는 파일은 트러스트되지 않게 되어 액세스할 수 없습니다.

STOP(스택 오버플로 보호)

STOP 을 사용하면 해커가 시스템에 침입하기 위해 임의의 명령을 실행할 수 있는 스택 오버플로우가 사용되지 않습니다.

프로그램 경로 지정(Program Pathing)

프로그램 경로 지정은 특정 프로그램을 통해서만 특정 파일을 액세스하도록 요구할 수 있는 기능입니다. 프로그램 경로 지정을 통해 중요한 파일의 보안이 상당히 향상됩니다. eTrust AC 에서는 프로그램 경로 지정을 사용하여 시스템의 파일에 대한 보호를 추가로 제공할 수 있습니다.

B1 보안 수준 인증

eTrust AC 에는 다음과 같은 B1 "Orange Book" 기능이 있습니다. 보안 수준, 보안 범주 및 보안 레이블이 있습니다.

Active Directory 관리

다음과 같은 eTrust AC 기능은 Windows Active Directory 서비스를 확장합니다.

사용자 및 그룹 속성

최신 버전의 Windows 에서는 사용자(예: Full Name 및 Logon Name)를 고유하게 식별하는 여러 속성을 사용하지만 이전 버전의 Windows 에서 사용자 속성을 관리한 Microsoft Net API 는 이러한 속성을 지원하지 않습니다.

eTrust AC 에서는 이러한 속성을 지원하여 사용자 및 그룹의 Active Directory 레코드에서 사용자 정의된 속성 값을 관리할 수 있습니다. 또한 이 속성에 대한 지원을 통해 조직 단위 관리도 향상됩니다.

컨테이너 관리

eTrust AC에서는 Active Directory 조직 구성 단위(OU)의 작성 및 편집을 지원합니다. OU는 사용자, 그룹, 컴퓨터 및 기타 개체 유형이 위치한 논리적 컨테이너입니다. eTrust AC는 세 가지 유형의 일반 개체인 **사용자, 그룹** 및 **컴퓨터**를 지원하고, 개체 유형 OU도 지원하여 OU 중첩을 지원합니다. 다음과 같은 기능을 제공합니다.

- OU 에서 또는 기본 컨테이너 USERS 가 아닌 컨테이너에서 새 사용자 및 그룹 작성
- Active Directory 에서 컨테이너나 OU 작성 또는 삭제
- 하나의 컨테이너나 OU 에서 다른 컨테이너로 사용자 또는 그룹 이동
- eTrust AC 에서 계층 Active Directory 구조(부모 자식 관계)를 참조하십시오.

OU 클래스의 개체는 주 도메인 컨트롤러에서 작성할 수 있습니다.

참고: OU 클래스는 Active Directory가 설치된 Windows 2000 Advanced Server 스테이션에서만 사용 가능합니다. 다른 구성이 설치된 컴퓨터에서 eTrust AC를 실행할 경우 이 클래스는 적용되지 않습니다.

Windows 및 UNIX 용 보안 관리

대규모 조직은 Windows 와 UNIX 시스템을 모두 보유하고 있는 경우가 많으며, 이런 경우 올바른 보안 상태를 유지하는 작업이 복잡해집니다. 모든 유형의 시스템에 구현할 수 있는 하나의 보안 정책을 개발하는 것이 가장 좋습니다.

eTrust AC 를 사용하여 다음 작업을 수행할 수 있습니다.

- UNIX 및 Windows 용으로 하나의 공용 보안 정책 개발
- eTrust AC 를 사용하여 정책 구현
- 한 대의 Windows 워크스테이션을 사용하여 Windows 및 UNIX 환경의 보안 관리

변경 작업을 수행하고 eTrust AC 에서 서로 다른 환경의 여러 워크스테이션에 변경 내용을 전파할 수 있는 기능을 사용하면 관리 오버헤드가 상당히 줄어듭니다.

공용 보안 정책에서 특히 중요한 일부 요소는 다음 절에서 설명합니다.

하나의 사용자 집합 유지관리

사이트에 eTrust AC가 설치되었으면 모든 사용자가 포함된 하나의 eTrust AC 데이터베이스를 유지 관리할 수 있습니다. 이것은 사용자 유지 관리를 한 번만 수행하면 된다는 의미입니다. eTrust AC는 업데이트를 받아야 할 모든 워크스테이션(UNIX 및 Windows)에 추가, 변경 및 삭제 내용을 전파할 수 있습니다.

하나의 그룹 집합 유지관리

특정 프로젝트를 수행하거나 조직의 특정 부서에서 일하는 사용자를 함께 그룹화하는 것이 편리할 경우가 많습니다. Windows , UNIX 및 eTrust AC 모두에서 사용자 그룹을 정의할 수 있습니다. 사용자에게 권한을 할당하는 것과 똑같이 그룹에 권한을 할당할 수 있습니다. 그룹을 사용하면 같은 권한을 개별 사용자에게 반복적으로 할당하지 않고 그룹에 한 번만 할당하므로 작업량이 줄어들 수 있습니다. 각 사용자는 그룹에 할당된 권한을 받습니다.

eTrust AC를 사용하면 UNIX 및 Windows 환경에서 모두 사용할 수 있는 하나의 그룹 집합을 만들어 유지 관리할 수 있습니다.

하나의 액세스 규칙 집합 유지관리

정책 모델 서비스를 사용하면 Windows 및 UNIX에 대한 하나의 액세스 규칙 집합을 개발하고 유지관리할 수 있습니다. PMDB(Policy Model database – 정책 모델 데이터베이스)를 통해 보안 데이터베이스 및 모든 해당 변경 내용을 모든 구독자에게 전파할 수 있습니다. Windows 및 UNIX 워크스테이션은 모두 동일한 PMDB에 구독할 수 있습니다.

PMDB 및 PMDB 구독자 간의 통신은 보통 한 방향으로 이루어집니다. 다시 말하면, PMDB는 변경사항을 PMDB 데이터베이스에서 PMDB 구독자에게 전송합니다. 구독자는 온라인 상태임을 PMDB에게 알리고 중단된 동안 PMDB에서 전송된 모든 변경사항을 요청할 때만 PMDB와 통신합니다. 이러한 설계는 네트워크 트래픽을 최소화하고 구독자의 무결성을 보장합니다.

암호 동기화

우수한 보안 정책의 주요 구성요소 중 하나는 사용자가 좋은 암호를 선택하도록 하는 것입니다. 사용자는 시스템에서 사용할 수 있는 암호를 하나만 기억해야 하는 것이 더 쉽습니다. eTrust AC를 구현함으로써 하나의 암호 규칙 집합을 적용하고 두 개의 시스템 간에 암호를 동기화할 수 있습니다.

PMDB는 적합한 암호를 정의하는 규칙을 전파할 수 있습니다. 또한 PMDB는 새 암호와 변경된 암호를 메인 프레임 컴퓨터를 비롯한 모든 구독자 스테이션에 전파할 수 있습니다.

참고: 자세한 내용은 *구현 가이드*를 참조하십시오.

eTrust AC 서비스 관리

기본적으로 모든 eTrust AC 서비스는 자동으로 시작됩니다. eTrust AC 서비스의 시작 방식을 자동에서 수동으로 변경하거나 서비스를 비활성화할 수 있습니다. 서비스를 액세스하려면:

1. eTrust AC 를 닫습니다.
2. Windows 제어판에서 서비스를 엽니다.
3. 변경하거나 비활성화할 서비스에서 마우스 오른쪽 버튼을 클릭합니다.
4. 시작 유형으로 자동, 수동 또는 사용 안 함을 선택하여 서비스 시작 방법을 표시한 후 [확인]을 클릭합니다.

eTrust AC 설명서

eTrust AC 설명서는 PDF 파일로 제공됩니다. Adobe Reader 를 설치하지 않은 경우 PDF 파일을 보려면 Adobe 웹사이트에서 Adobe Reader 를 다운로드하여 컴퓨터에 설치해야 합니다.

업데이트된 안내서는 http://ca.com/support 에서 구할 수 있습니다.

참고: 적절한 버전의 Adobe Reader도 제품 CD에 있습니다.

eTrust AC 설명서의 전체 목록은 추가 정보 파일에서 확인할 수 있습니다.

다음 내용

이제 eTrust AC 기능을 더욱 잘 이해하게 되었으므로 기업의 시스템 무결성과 데이터 기밀을 보호하는 방법을 익힙니다. 다음 장에서는 사용자와 그룹의 프로그램과 파일을 보호하는 과정을 안내합니다.

제 3 장: 관리자 인터페이스 실행

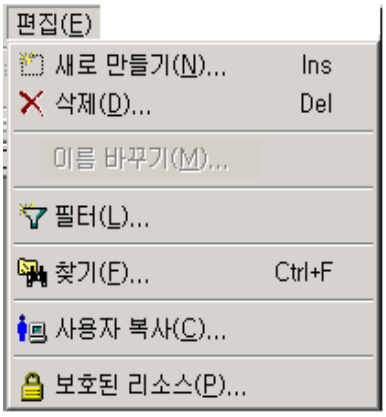
이 장은 아래의 주제를 포함하고 있습니다:

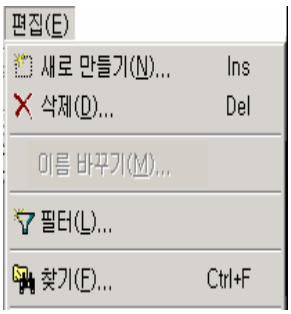
보안 정책 구현 및 유지관리

이 장에서는 정책 관리자의 일부인 eTrust AC 그래픽 사용자 인터페이스를 살펴봅니다. 그래픽 사용자 인터페이스에서 Windows 및 UNIX 플랫폼상의 데이터베이스를 관리할 수 있습니다.

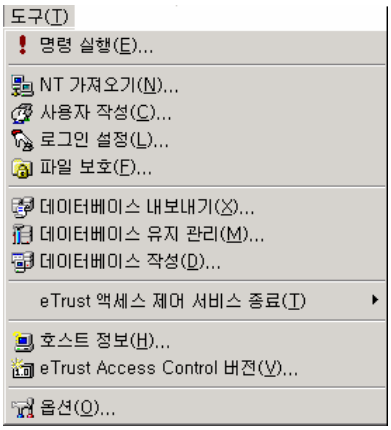
메뉴 모음 및 도구 모음

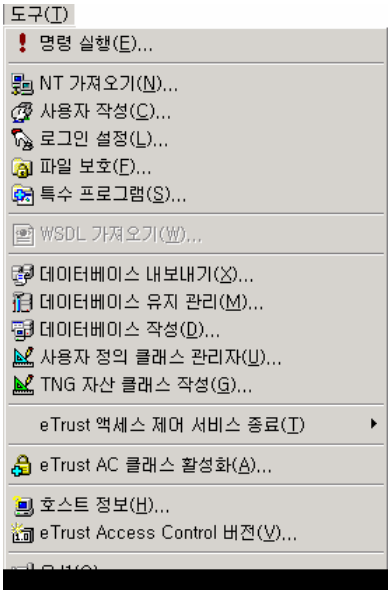
메뉴는 어떤 창이 열려 있는 지에 따라 관련 정보를 표시합니다. [사용자] 창 및 [리소스] 창의 경우[편집] 메뉴를 비교하십시오. 예는 다음과 같습니다.





다른 예로 [도구] 메뉴를 보십시오. [사용자] 창과 [리소스] 창의 경우 [도구] 메뉴는 다음과 같이 표시됩니다.



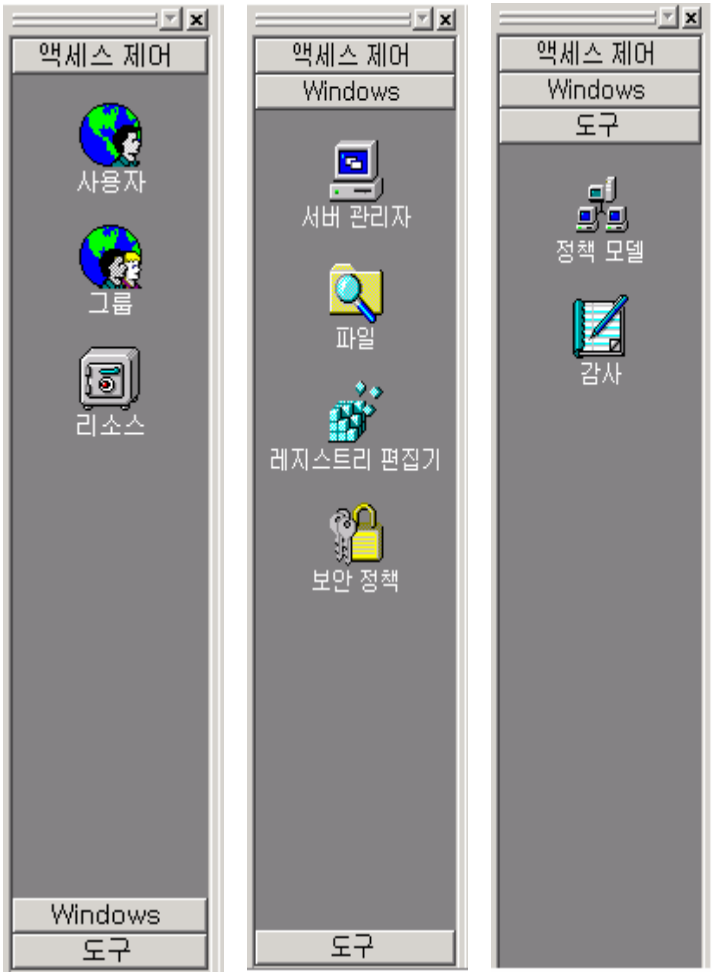


[보기] 메뉴는 도구모음과 창 표시에 대한 제어 권한을 부여합니다.

프로그램 표시줄

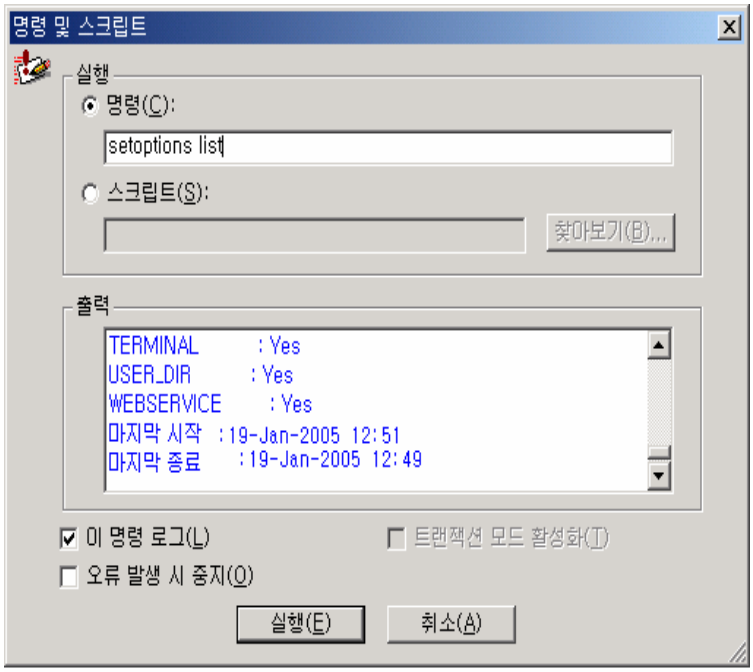
기능은 eTrust 액세서 및 리소스, NT 리소스 그리고 도구의 세 가지 프로그램 표시줄로 나누어 집니다. [파일], [열기]를 사용할 때도 동일한 기능이 실행됩니다.

참고: eTrust Web AC가 설치된 경우, eTrust Web AC 기능을 관리할 수 있는 네 번째 표시줄이 나타납니다. 이 내용은 eTrust Web AC문서에 나와 있습니다.



selang 명령

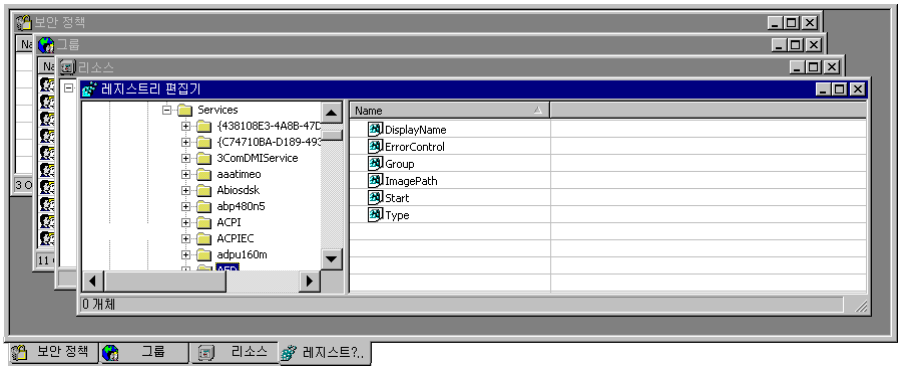
[도구] 메뉴에서 [명령 실행]을 선택하여 정책 관리자에서 selang 명령을 실행할 수 있습니다. 그런 다음 [명령 및 스크립트] 대화 상자에서 [명령 실행] 필드에 명령을 입력합니다.



Admin 기본값 설정

GUI 기본값을 설정하려면 [도구] 메뉴에서 [옵션]을 선택하십시오.

옵션을 변경할 수 있습니다. *표시* 및 *형식*은 인터페이스를 사용자 지정합니다. 편안하게 생각하십시오. 예를 들어, 워크북 모드는 탭을 창에 놓습니다. 창을 여러 개 열어 놓고 작업하는 경우에 편리합니다.



*시작*은 시작 기본값을 설정하고 사용자 지정 스플래시 화면을 활성화합니다. *작성*은 새 사용자 및 그룹을 생성하기 위한 기본 환경을 정의합니다. 둘러보기를 통해 eTrust에서만 기본값을 변경할 수도 있습니다. (정리 작업이 최소화됩니다.)

참고: [확인]을 클릭하면 즉시 설정이 적용됩니다.

마법사

eTrust AC 는 일반적인 절차를 통해 사용할 수 있는 여러 마법사를 제공합니다.

로그인 보호 설정 마법사 사용

eTrust AC 보안은 권한 없는 터미널로부터 사용자가 로그인하는 것을 금지합니다. 특히 모든 터미널은 TERMINAL 클래스 레코드에서 정의되어야 하고 모든 사용자는 사용하는 각 터미널의 ACL(Access Control List-액세스 제어 목록)에서 정의된 액세스 권한을 가져야 합니다. [로그인 보호 설정 마법사]는 이 작업 외에도 다른 많은 작업을 수행합니다.

1. 마법사 관리자 도구 모음 버튼을 클릭하여 로그인 보호 설정 마법사를 시작합니다. [로그인 보호] 를 선택합니다.
2. [보호된 사용자 및 그룹]을 선택합니다.

   참고: 보호된 사용자 및 그룹 페이지에서 여러 사용자와 그룹을 정의할 수 있습니다.
3. 로그인 터미널 페이지에서 사용자와 그룹이 로그인할 수 있거나 로그인할 수 없는 터미널을 지정합니다.
4. 사용자 계정 제한 페이지에서 지정된 사용자와 그룹이 로그인할 수 있는 날짜 및 시간을 지정할 수 있습니다.

   참고: [평일] 버튼을 사용하여 [토요일]과 [일요일]을 클릭하여 선택 취소하십시오.
5. 다음 페이지에서 휴일에 대한 로그인 권한을 지정하고 [마침]을 클릭합니다.

참고: 특정 휴일에 로그온을 허용하거나 금지하려면 이 대화 상자를 사용하기 전에 달력에서 휴일을 먼저 정의해야 합니다.

사용자 작성 마법사 사용

[사용자 작성 마법사]를 사용하여 사용자를 확인합니다. 마법사를 실행하여 사용자 속성(예: 운영자 또는 관리자), 암호 및 그룹 구성원 정보를 지정하십시오.

파일 보호 마법사 사용

[파일 보호 마법사]를 사용하여 지정된 파일 및 디렉터리를 보호합니다. 마법사를 실행하여 보호할 파일, 파일에 액세스할 수 있는 사용자 및 그룹, 해당 접근 수준을 선택하십시오.

NT 가져오기 마법사 사용

설치 중에 Windows 사용자와 그룹을 가져오지 않은 경우, [NT 가져오기 마법사]를 사용하여 다음 작업을 수행하십시오.

- Windows 데이터베이스에서 로컬 호스트 데이터베이스 또는 PMDB 로 사용자 가져오기
- Windows 데이터베이스에서 로컬 호스트 데이터베이스 또는 PMDB 로 그룹 가져오기

원격 호스트로 가져올 수 없습니다. Windows 데이터베이스를 직접 가져오거나 스크립트 파일(.lng)로 저장할 수 있습니다.

특별 프로그램 마법사 사용

[특별 프로그램 마법사]를 사용하여 특정 프로그램을 보호합니다.

보통 SYSTEM 계정으로 실행되어야 하는 시스템 서비스와 같은 프로그램인 경우 권한 보호를 설정할 수 있습니다. 논리적 사용자 또는 바이패스를 사용하여 지정된 프로그램에 대한 액세스를 제한할 수 있습니다.

마법사는 SPECIALPGM 리소스를 작성하고 [정책 관리자] 창의 출력 표시줄에 결과를 표시합니다.

사용자 복사 마법사 사용

[사용자 복사 마법사]를 사용하여 다음 작업을 수행합니다.

- 한 호스트에서 다른 호스트 또는 같은 호스트에 있는 PMDB 로 사용자 레코드 복사
- 사용자를 복사할 때 그룹에 사용자 추가
- 한 호스트에서 다른 호스트 또는 같은 호스트에 있는 PMDB 로 여러 사용자 레코드 복사
- 하나의 사용자 레코드를 템플릿으로 사용하여 같은 호스트에서 다른 레코드 작성
- 사용자 레코드를 복사하기 위해 스크립트 작성

참고: 사용자 복사 마법사에 액세스하려면 Access Control 프로그램 표시줄에서 [사용자]를 클릭한 후 [편집] 메뉴에서 [사용자 복사]를 선택하십시오.

그룹 복사 마법사 사용

[그룹 복사 마법사]를 사용하여 다음 작업을 수행합니다.

- 한 호스트에서 다른 호스트 또는 같은 호스트에 있는 PMDB 로 그룹 레코드 복사
- 한 호스트에서 다른 호스트 또는 같은 호스트에 있는 PMDB 로 구성원 사용자 레코드 복사
- 한 호스트에서 다른 호스트 또는 같은 호스트에 있는 PMDB 로 여러 그룹 레코드 복사
- 하나의 그룹 레코드를 템플릿으로 사용하여 같은 호스트에서 다른 레코드 작성
- 그룹 레코드를 복사하기 위해 스크립트 작성

참고: 그룹 복사 마법사에 액세스하려면 Access Control 프로그램 표시줄에서 [그룹] 아이콘을 클릭한 후 [편집] 메뉴에서 [그룹 복사]를 선택하십시오.

다음 내용

이제 정책 관리자를 더욱 잘 이해하게 되었으므로, 다음 장에서는 액세스 및 계정 제한을 설정 등에 관한 소프트웨어 사용 방법에 대해 설명합니다.

제 4 장: 보호 기능 탐색

이 장은 아래의 주제를 포함하고 있습니다:

프로그램 보호에서 시스템 파일 모니터까지

이 장에서는 eTrust AC 사용에 필요한 다음 단계인 새 사용자 및 그룹 등록, 파일 및 디렉터리 보호, 권한 없는 사용자로부터 파일 보호, 프로그램 경로 지정 및 파일 이름 패턴으로 파일을 보호하는 방법에 대해 설명합니다.

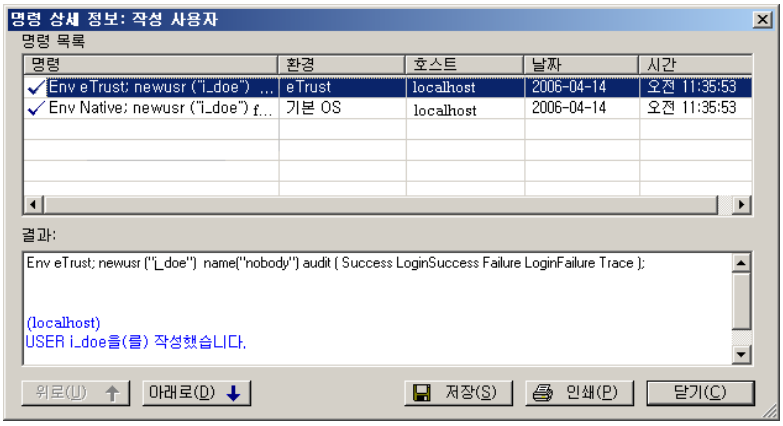
사용자 및 그룹 작성

사용자를 작성하려면:

1. GUI 왼쪽에 있는 [프로그램 표시줄]에서 [사용자] 아이콘을 클릭합니다.
2. 도구모음에서 [새로 만들기] 아이콘을 클릭합니다. [사용자 이름} 입력란에 "j_doe"를 입력합니다. 지금은 암호 옵션을 건너뜁니다.
3. [사용자 특성]을 클릭합니다. [소유자] 필드에 **nobody**를 입력합니다. j_doe는 일반 사용자이므로 [사용자 유형] 상자를 선택하지 마십시오.
4. [기타] 아이콘을 클릭하고 [감사 정보]를 선택합니다.

   참고: 제목은 어떤 패널에서 작업 중인지 알려줍니다.
5. [모두]를 클릭한 후 각 창에 있는 [확인]을 클릭하여 닫습니다.

인터페이스의 하단에 있는 결과 표시줄에는 새 사용자를 성공적으로 작성했다고 나타납니다. [상세 정보] 창을 보려면 입력행을 두 번 클릭합니다.



창의 상단 부분에는 정책 관리자에서 생성된 selang 명령이 표시되고 하단 부분에는 결과가 표시됩니다. 각 명령을 선택하여 명령 결과를 확인합니다.

보시다시피 이 예는 상당히 간단합니다. eTrust AC 데이터베이스의 사용자 레코드에 보다 많은 매개 변수를 매우 간단하게 추가할 수 있습니다.

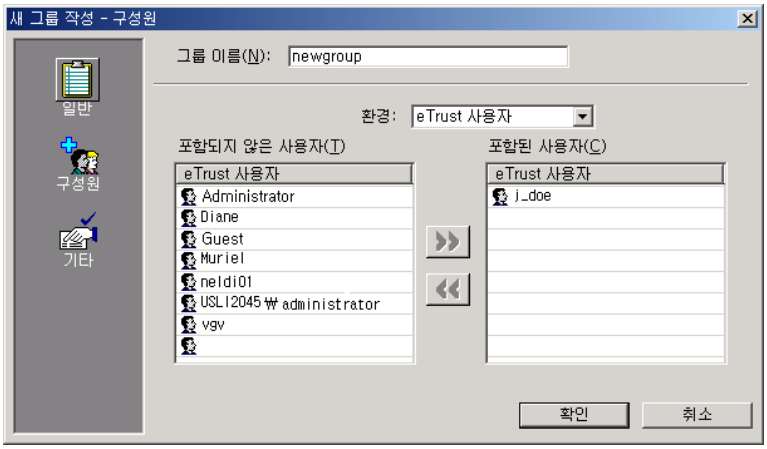
또 다른 예제가 있습니다. 이번에는 그룹을 작성합니다.

1. 프로그램 표시줄에서 [그룹] 아이콘을 클릭한 후 도구모음에서 [새로 만들기] 아이콘을 클릭합니다. [새 그룹 작성] 창은 [새 사용자] 창과 거의 동일합니다.

   참고: 또한 [그룹] 창의 아무 곳에나 마우스를 가져가 마우스 오른쪽 버튼을 클릭할 수 있습니다. 새 그룹은 마우스 오른쪽 버튼을 클릭할 때 나타나는 바로 가기 메뉴에 있는 옵션 중 하나입니다.

2. 그룹에 이름을 지정하고 소유자를 **nobody**로 할당합니다. 또한 수퍼 그룹도 할당할 수 있습니다. 그러면 새 그룹은 하위 그룹이 되므로, 그룹을 작성할 때 변경하거나 추가한 그룹 속성을 제외하고 수퍼 그룹의 모든 속성을 상속합니다.

3. [구성원] 아이콘을 클릭하여 구성원을 새 그룹에 추가합니다.

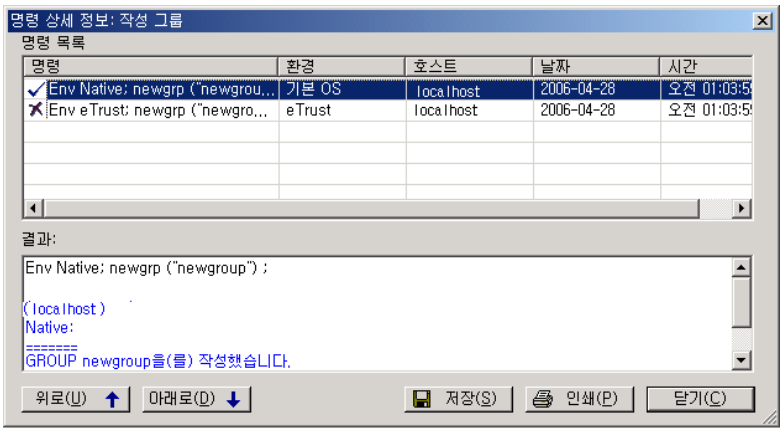


   이 예제에서는 한 명의 사용자만 추가했으며, 더 많이 추가할 수도 있습니다. 그룹을 선택하여 여러 명의 사용자를 한 번에 추가하려면 Shift 또는 Ctrl 키를 누른 상태에서 사용자를 선택합니다.

4. 그룹에 사용자를 추가했으면 [기타] 아이콘을 클릭합니다. 요일 및 시간 제한을 추가한 후 [확인]을 클릭하여 새 그룹을 작성합니다.

   참고: 사용자에게 할당된 제한 사항은 그룹에 할당된 제한 사항에 우선합니다.

5. 이제 [명령 상세 정보]를 보고 결과를 확인합니다.



파일 및 디렉터리 보호

모든 컴퓨터 시스템에는 두 가지 종류의 파일이 있습니다. 시스템 파일은 운영 체제의 정상적인 작동을 위해 필요하고, 응용프로그램 파일은 응용프로그램과 사이트의 사용자가 작성하고 사용합니다.

각 파일 종류에 대해 어떤 유형의 보호 기능을 제공할지 결정한 후 보호 기능을 구현해야 합니다. eTrust AC 의 주요 장점 중 하나는 파일과 디렉터리를 원하지 않는 액세스(시스템 관리자의 액세스도 해당)로부터 보호할 수 있다는 점이고, 보호 기능은 비 NTFS 파일 시스템으로 확장될 수 있습니다.

연습에 사용할 더미 파일을 만드십시오.

1. 프로그램 표시줄에서 [리소스] 아이콘을 클릭하여 [리소스] 창을 표시합니다. [시스템 리소스]에서 [파일]을 클릭합니다.
2. 도구 모음에서 [새로 만들기] 아이콘을 클릭한 후 [찾아보기] 버튼을 사용하여 파일을 찾아 소유자를 **nobody**로 정의합니다.
3. 일부 사용자나 그룹에게 파일을 액세스할 수 있는 권한을 부여합니다. 이 작업을 수행하려면 [권한 부여]를 클릭하고 [액세서 추가] 목록 상자 옆에 있는 [추가] 버튼을 클릭합니다. [사용자] 또는 [그룹]을 선택하고 [확인]을 클릭합니다. 추가한 이름이 [액세서 추가 목록] 상자에 나타납니다.

4. 각 사용자 또는 그룹을 차례로 선택하여 해당 권한을 선택합니다.

   관리자 adm1 의 경우, Delete only 를 선택했습니다. 이것은 관리자의 액세스 권한을 제한하는 극단적인 예제입니다.

   사용자 p_jones 에게 전체 권한을 부여했습니다. (p_jones 의 권한은 앞의 그림에 나와 있습니다.) 그러나 Jones 도 읽기 전용 권한을 가진 새 그룹의 구성원입니다. 규칙에 따르면 권한이 추가될 수 있으므로, Jones 는 새 그룹에 있는 구성원 정보로 제한되지 않습니다.

   우리는 그룹을 위해 프로그램(Word)을 선택했습니다. 이것은 프로그램 경로 지정으로 알려져 있으며, 사용자는 특정 프로그램을 사용하는 파일에만 액세스할 수 있음을 의미합니다. 프로그램 경로 지정을 통해 중요한 파일의 보안이 상당히 향상됩니다. 이런 경우, 예를 들어 그룹의 누구도 메타데이터를 읽는 응용프로그램에서 이 파일을 열 수 없습니다.

5. 파일 리소스를 작성하기 위해 감사 모드를 지정하고 [확인]을 클릭하여 완료합니다.

6. [명령 상세 정보]를 확인하여 어떤 selang 명령이 작성되었는지 확인합니다.

참고: 이러한 파일 보호에 대한 자세한 내용은 *참조 가이드*의 FILE 클래스를 참조하십시오.

파일 그룹

일단 데이터베이스에서 파일을 정의하면, 정의한 파일을 그룹화하고 그룹에 권한을 할당할 수 있습니다. 예를 들어, Finance 라는 그룹에 재무 부서의 파일을 모두 넣고 최고 관리진과 재무 부서 직원들에게만 액세스를 허용할 수 있습니다.

그룹에서 각 파일 또는 패턴은 파일에 액세스하기 위해 부서 내에 있는 개인 또는 그룹의 필요에 따라 다른 액세서 권한 집합을 가집니다. 또한 파일 권한 계층의 세부 제어를 위해 파일 그룹 내에서 파일 그룹을 중첩할 수 있습니다.

프로그램 보호

eTrust AC는 TCB(*Trusted* Computing Base)의 일부로 간주되는 프로그램을 정의합니다. Watchdog은 프로그램을 수정하지 않았는지 모니터링하므로 이 클래스의 프로그램은 보안을 위반하지 않도록 트러스트됩니다. 트러스트된 프로그램이 수정된 경우, eTrust AC는 자동으로 프로그램을 트러스트되지 않음으로 표시하여 해당 프로그램은 실행되지 않습니다.

참고: PROCESS 클래스에서 프로그램을 정의할 때 해당 FILE 클래스 레코드도 작성해야 합니다. 레코드를 작성한 순서는 중요하지 않습니다.

프로그램을 보호하려면, [리소스] 창의 [시스템 리소스] 부분을 확인하십시오.

1. [프로그램]을 클릭합니다.

   데이터베이스에는 이미 Microsoft Word에 대한 레코드가 있습니다. eTrust AC는 앞의 연습에서 NewGroup에 대한 프로그램 경로 지정을 구현했을 때 이 레코드를 자동으로 작성했습니다.

2. Microsoft Word에서 마우스 오른쪽 버튼을 클릭한 후 [속성]을 선택합니다.

   액세서에게 실행 권한만 할당할 수 있습니다. 권한을 거부하면 프로그램에 대한 액세스가 차단됩니다.

3. [감사] 아이콘을 클릭합니다.

   [일반] 패널에는 Trust라는 확인란이 있습니다. eTrust AC는 Program 레코드를 작성할 때 이 속성을 설정합니다. 프로그램이 수정될 경우 eTrust AC는 이 속성을 "트러스트되지 않음"으로 재설정하고 프로그램 실행을 금지합니다. 문제가 해결되면, 이 창에서 트러스트 속성을 재설정할 수 있습니다.

파일 모니터

eTrust AC는 중요한 시스템 파일을 모니터할 수 있습니다. SECFILE 클래스(보호된 파일을 나타내는 개체가 있는 클래스)에서 레코드를 작성함으로써 자주 수정되지 않는 중요한 시스템 파일을 권한 없는 사용자가 수정하지 않는 것을 확인할 수 있습니다. watchdog은 이 파일을 검사하고 파일 정보가 변경되지 않았는지 확인합니다.

포함할 파일 유형의 몇 가지 예는 다음과 같습니다.

- \Winnt\system32\drivers\etc\hosts
- *\etc\services
- *\etc\protocol
- *\etc\networks

프로세스 중지 방지

자체 주소 공간에서 실행되는 실행 파일은 종료 또는 중지되지 않도록 보호해야 할 수도 있습니다. 이러한 프로세스는 서비스 거부 공격의 주요 대상이 되므로 주요 유틸리티 및 데이터베이스 서버는 eTrust AC 프로세스 보호 기능을 사용할 수 있는 좋은 예가 될 수 있습니다. 또한 eTrust AC 프로세스 보호는 Windows 서비스 및 기타 비대화식 Windows 응용 프로그램을 보호하는 데도 유용합니다.

eTrust AC는 세 개의 중지 신호로부터 보호할 수 있습니다. 일반 terminate 신호(TERM)와 응용프로그램에서 마스크할 수 없는 두 개의 신호(Terminate Process 및 STOP)로부터 보호합니다.

다음 예제에서는 작업 관리자(Taskmgr.exe)를 보호합니다.

1. [프로세스]를 선택한 후 [새로 만들기]를 클릭합니다.
2. Taskmgr.exe(\system32 하위 디렉터리에 위치)용 새 레코드를 작성합니다.

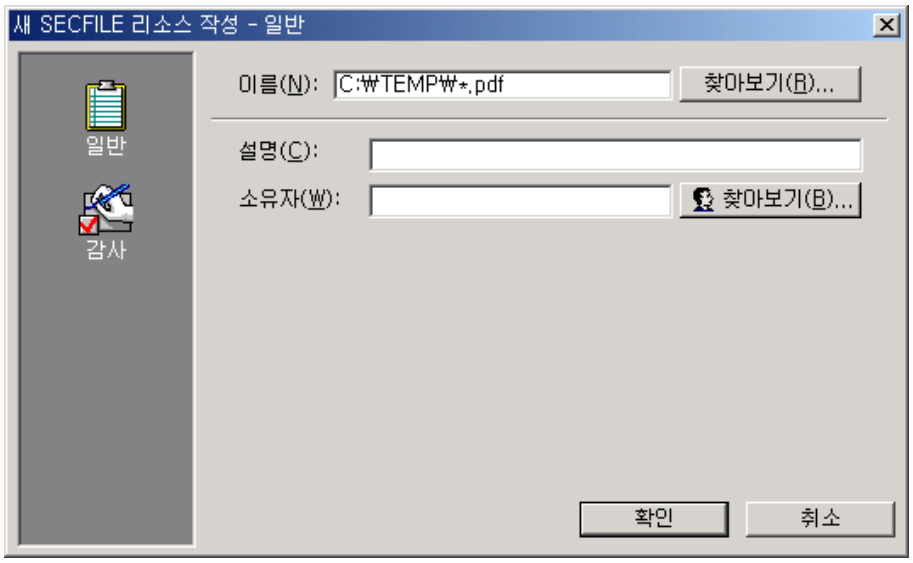
   참고: [찾아보기] 버튼으로 선택할 수 있는 항목으로 나타나려면 Taskmgr.exe를 활성화해야 합니다(Windows 작업 표시줄에 나타남).
3. 사용자에게 프로세스 종료 권한을 부여합니다. 읽기 권한은 사용자가 프로세스를 종료할 수 있다는 의미이고 거부는 사용자가 프로세스를 종료할 수 없다는 의미입니다.

프로그램 패턴

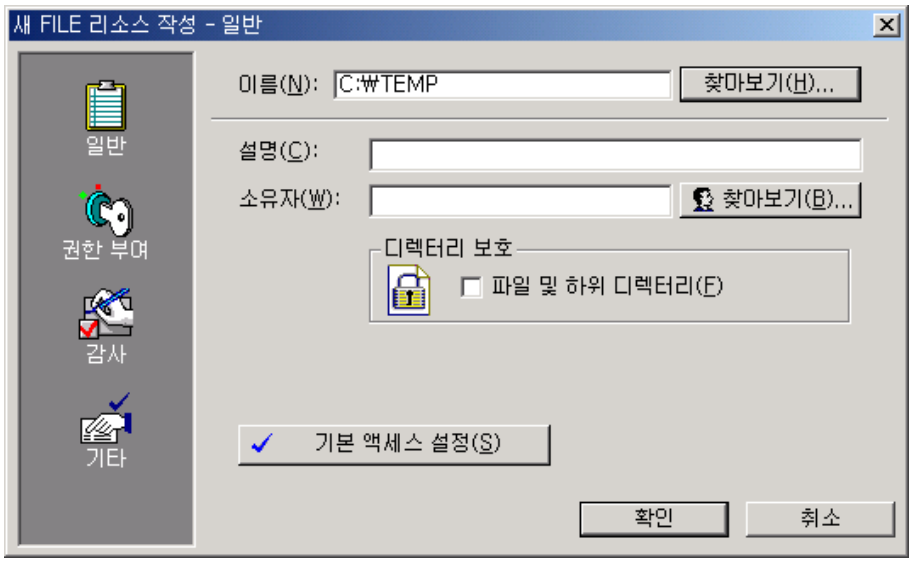
시스템에서 각 파일에 대한 파일 리소스를 정의하는 작업에 시간이 오래 걸릴 수 있습니다. eTrust AC는 해당 프로세스의 수행 속도를 높일 수 있는 도구를 제공합니다.

다음 예제에서는 파일 그룹을 보호하는 신속한 방법을 보여줍니다. 특정 이름이 아닌 패턴을 지정함으로써 패턴에 따라 모든 파일에 동일한 액세스 제한을 실행할 수 있습니다.

[리소스] 창에서 [모니터된 파일]을 선택하고 [새로 만들기]를 클릭합니다.



또한 디렉터리를 보호할 수 있습니다.



파일 및 하위 디렉터리를 보호할 수 있는 확인란을 보십시오. [확인란]을 선택하거나 선택하지 않고 파일 리소스를 작성해 보십시오. 리소스 목록에서 다른 점을 볼 수 있습니다. 작성된 기타 명령을 보려면 [명령 상세 정보]를 확인하십시오.

기타 리소스 보호

eTrust AC가 보호할 수 있는 다른 유형의 리소스가 있습니다. eTrust AC가 네트워크 및 Windows 레지스트리와 같은 필수 시스템 구성 요소를 모니터할 수 있는지 확인하려면 [리소스] 창의 트리를 확장하십시오.

미리 정의된 그룹으로 액세스 제한

eTrust AC에는 파일에 대한 액세스를 제한하기 위해 사용할 수 있는 4개의 미리 정의된 그룹이 있습니다.

- _abspath
- _interactive
- _network
- _restricted

_restricted 그룹 사용

_restricted 그룹에 사용자를 추가하면 별도로 액세스가 주어지지 않은 파일에 대한 액세스는 차단됩니다. 이런 파일에는 데이터베이스에 나열되지 않은 파일이 포함되고, FILE 클래스의 기본 액세스 값으로 제어됩니다. 설치 중에 기본값은 none 으로 자동 설정됩니다.

참고: _restricted 그룹에 사용자를 추가하고 데이터베이스에 FILE 액세스 규칙이 거의 없는 경우 _restricted 사용자는 원하는 작업을 수행할 수 없습니다. FILE 클래스에 대한 기본 액세스로 NONE을 사용하여 _restricted 그룹에 사용자를 추가하려면 경고 모드를 사용하십시오. 그러면 감사 이벤트에서 _restricted 사용자가 작업하는 데 필요한 파일을 보여줍니다. 잠시 후 적합한 권한을 부여하고 경고 모드를 해제할 수 있습니다.

여러분은 이미 사용자를 그룹에 추가하는 방법을 알고 있습니다. _restricted 그룹에 사용자를 추가하는 것도 동일합니다.

보안 수준을 올리려면 FILE 클래스의 감사 모드를 재설정하십시오.

1. [리소스] 창에서 Administration 폴더를 열고 [클래스별 액세스]를 클릭합니다. [파일]을 두 번 클릭합니다.

   참고: [기본 액세스 설정] 버튼 위에 커서를 놓으면 도구 설명이 현재 액세스 기본값을 표시합니다.

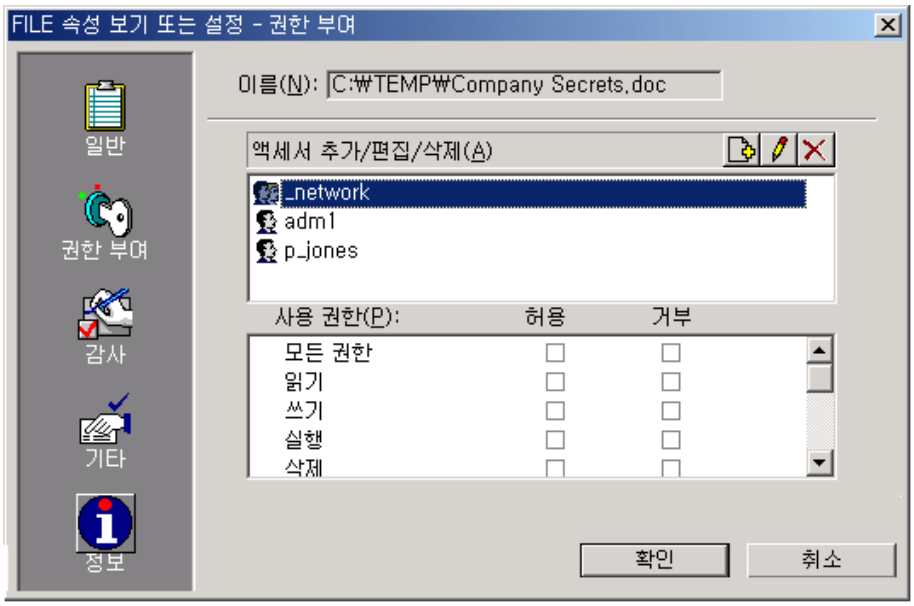
2. [감사] 패널을 엽니다. [실패]를 선택 취소하고 [경고 모드]를 선택합니다.
3. 사용자를 _restricted 에 추가한 결과를 테스트할 수 있습니다.

참고: eTrust AC에서는 시작할 때만 _restricted 사용자 목록을 읽습니다. 사용자가 _restricted 그룹에 조인하거나 그룹을 떠난 경우 변경 사항은 eTrust AC를 재시작한 후에만 적용됩니다.

_network 및 _interactive 그룹 사용

_network 그룹은 특정 리소스에 대한 네트워크의 액세스를 정의합니다. _interactive 그룹은 리소스가 위치한 컴퓨터에서 특정 리소스에 허용된 액세스를 정의합니다. 이러한 그룹은 파일뿐만 아니라 모든 리소스에 적용됩니다. 또한 그룹은 모든 사용자에게도 적용되므로, 그룹에 명시적으로 사용자를 추가해야 할 필요가 없습니다.

다음 예를 살펴봅시다.



이 예에서는 파일 Company Secrets.doc 의 Access Control 목록(ACL)에 대한 권한이 없이 _network 를 추가했습니다. 이것은 파일을 네트워크에서 액세스할 수 없음을 의미합니다. _interactive 는 로컬 호스트에서 동일한 방법으로 작동합니다. 이 그룹에는 사용자를 추가하지 않습니다.

참고: eTrust AC에서 _network 그룹과 _interactive 그룹은 서로 연관성이 없습니다. 두 개의 그룹을 같은 리소스에 추가할 수 있습니다.

다음 내용

이제 사용자 및 그룹 작성, 파일, 디렉터리 및 프로그램 보호에 대해 더욱 잘 알게 되었습니다. 다음 장에서는 관리자 인터페이스에 대해 설명합니다.

제 5 장: 향상된 사용자 계정 제어

이 장은 아래의 주제를 포함하고 있습니다:

사용자 액세스 및 권한 제한

이 장에서는 eTrust AC 작업에 필요한 다음 단계인 관리자 권한 설정, 터미널로부터의 액세스 제한, 시간 및 요일 규칙 설정, 조건부 액세스 설정 등에 대해 설명합니다.

관리자 사용 제한

컴퓨터 네트워크에서 가장 큰 보안 위험 중 하나는 권한 없는 사용자가 Administrators 그룹에 속한 사용자 계정을 제어할 수 있다는 점입니다. 이런 경우, 권한 없는 사용자로 인해 시스템에 엄청난 손상이 발생할 수 있습니다.

eTrust AC를 통해 관리자 계정에 부여되는 권한을 제한하고 관리자 그룹의 구성원인 사용자 권한을 제한할 수 있습니다. 그런 다음 관리자 유형의 권한을 일반 사용자에게 배포할 수 있으므로 이 권한을 사용하여 해당 사용자는 Administrators 그룹의 구성원이 아니더라도 관리 작업을 수행할 수 있습니다. *작업 위임*이라는 이 기능은 eTrust AC의 가장 중요한 장점 중 하나입니다.

사용자 유형

eTrust AC 에서는 부분적으로 관리자 권한을 가지는 여러 사용자 유형을 제공합니다. 일반적으로 사용자에게 이러한 속성을 할당하는 것이 관리자 권한을 배포하는 첫번째 단계입니다.

eTrust AC 에서 사용자 유형은 다음과 같습니다.

그룹 관리자

하나의 특정 그룹 내에서 대부분의 관리 기능을 수행할 수 있는 사용자입니다.

하위 관리자

관리자가 지정한 클래스 및 리소스를 관리할 수 있는 사용자입니다.

암호 관리자

다른 사용자의 암호 설정을 수정할 수 있는 권한을 가진 사용자입니다.

그룹 암호 관리자

하나의 특정 그룹 내 다른 사용자의 암호 설정을 수정할 수 있는 권한을 가진 사용자입니다.

감사자

감사 로그를 읽을 수 있는 권한을 가진 사용자입니다. 또한 각 로그인과 각 리소스 액세스 시도에 대해 수행되는 감사 종류를 결정합니다.

그룹 감사자

특정 그룹에 대한 감사 로그를 읽을 수 있는 사용자입니다. 또한 해당 그룹 내에서 수행되는 감사 종류를 결정할 수 있는 권한도 가집니다.

연산자

데이터베이스에서 모든 정보를 표시(읽기)할 수 있는 사용자입니다.

그룹 운영자

사용자가 정의되어 있는 그룹의 데이터베이스에 모든 정보를 표시할 수 있는 사용자입니다.

참고: 관리자 그룹(기본 Windows의 *일부임*)과 그룹 관리자(기본 Windows의 일부가 아님)를 혼동하지 마십시오.

기본 환경과 eTrust 환경에서 이러한 특정 사용자 유형을 정의할 수 있습니다. 그러나 이러한 특정 권한은 Windows 의 일부가 아니라 eTrust 의 한 부분입니다.

새 사용자를 작성하거나 기존 사용자 레코드를 수정할 때 사용자 특성을 할당할 수 있습니다. 정책 관리자는 eTrust 데이터베이스에 특성 할당을 지원합니다.

기존 사용자에게 사용자 속성을 할당하려면 [사용자] 아이콘을 클릭하십시오. 나타나는 목록에서 사용자 이름을 선택하고 [사용자 특성]을 클릭하십시오.

그룹 내에서만 적용되는 특성을 사용자에게 할당하려면 [그룹] 아이콘을 클릭하십시오. "소속 그룹" 열에서 [그룹 이름]을 선택하고 [그룹 특성]을 클릭하십시오.

이 속성은 사용자 j_doe 에게 감사 액세서에 대한 권한과 그룹 관리자가 소유한 리소스 권한을 부여합니다.

참고: 그룹을 액세서나 리소스의 소유자로 지정하면, 그룹에 있는 관리자, 감사자 및 다른 구성원은 각각 해당 액세서나 그룹의 관리 권한을 가집니다.

터미널의 액세스 제한

eTrust AC 에서는 사용자 액세스를 제한하는 여러 방법을 제공합니다. 계정 만료일 설정, 유예 로그인 설정, 특정 요일 및 시간에 로그인 제한 및 사용자가 로그인하는 터미널 제어가 있습니다. 여기서는 터미널을 살펴보고 다음 절에서 시간 제한에 대해 살펴봅니다.

마법사로 새 사용자를 작성할 때 [로그인 설정 마법사]를 사용하여 사용자의 터미널을 정의했습니다. 터미널과 사용자가 일치하지 않으면 해당 사용자는 로그인하거나 보호된 리소스에 액세스할 수 없습니다. 터미널 리소스에 대해 자세히 살펴봅시다.

먼저 기본 환경에서 정의된 한 쌍의 사용자가 필요합니다. 정의하지 않았으면 지금 정의하십시오. 시간을 절약하려면 기존 eTrust 사용자를 기본 환경에 추가하십시오.

1. [사용자]를 선택하고 도구 모음의 [속성] 아이콘을 클릭한 후 [고급] 버튼을 사용하여 기본 환경을 추가합니다.

   참고: 또한 사용자를 마우스 오른쪽 버튼을 클릭한 후 바로 가기 메뉴에서 [속성]을 선택할 수 있습니다.

2. 터미널 권한을 사용자에게 할당합니다.

   a. [프로그램 표시줄]에서 [리소스] 아이콘을 클릭한 후 [로그인 보호] 옆에 있는 [더하기 기호]를 클릭하여 [트리]를 엽니다.

   b. [터미널]을 선택한 후 [로컬 호스트]를 두 번 클릭합니다.

   c. [권한 부여] 패널을 열고 [액세서 추가]에 대해 [삽입] 아이콘을 클릭합니다.

   d. [찾아보기] 버튼을 사용하여 사용자를 추가한 후 [확인]을 클릭합니다.

   e. 읽기 및 쓰기 권한에 대해 [거부] 상자를 선택합니다.

   사용자 j_doe 는 지금 workstation1 이름의 터미널 사용이 차단되었습니다.

3. 이제 또 다른 사용자에게 권한을 계속 부여하고 읽기 권한을 할당합니다.

   참고: 사용자가 터미널을 관리할 수 있게 하려면 읽기 및 쓰기 권한을 할당하십시오.

4. 컴퓨터를 로그오프하고 각 사용자로 로그인합니다. 사용자 j_doe 는 로그인 오류 메시지를 수신하지만 사용자 b_raines 는 터미널을 액세스할 수 있습니다.

중요! 이 연습을 정리할 때 컴퓨터의 터미널 리소스를 삭제하지 **마십시오**. (원격 컴퓨터의 터미널 리소스를 삭제할 수 있습니다.) 컴퓨터 자체의 읽기 및 쓰기 권한을 삭제하거나 변경하지 **마십시오**. 이런 권한을 삭제하면 eTrust AC를 관리할 수 없게 됩니다. 소프트웨어를 재설치하지 않는 한 권한을 복원할 수 없습니다.

터미널 그룹

유사한 제한을 여러 대의 컴퓨터에 할당하려는 경우 이러한 제한을 터미널 그룹에 넣고 한 번에 모두 권한을 부여할 수 있습니다.

1. [리소스] 창에서 [터미널 그룹]을 선택하고 도구 모음에서 [새로 만들기] 아이콘을 클릭합니다.
2. 그룹 이름 및 소유자를 지정합니다.
3. [구성원] 패널을 엽니다. [구성원 추가/삭제]에서 [새로 만들기] 아이콘을 클릭하고 [터미널]을 선택합니다.

   참고: Ctrl 키 또는 Shift 키를 누른 상태에서 선택하면 여러 터미널을 선택할 수 있습니다.
4. 이전 경우와 같이 권한 부여 및 감사를 완료합니다.
5. [명령 상세 정보]를 확인하여 어떤 selang 명령이 생성되었는지 확인합니다.

가장 요청 제한

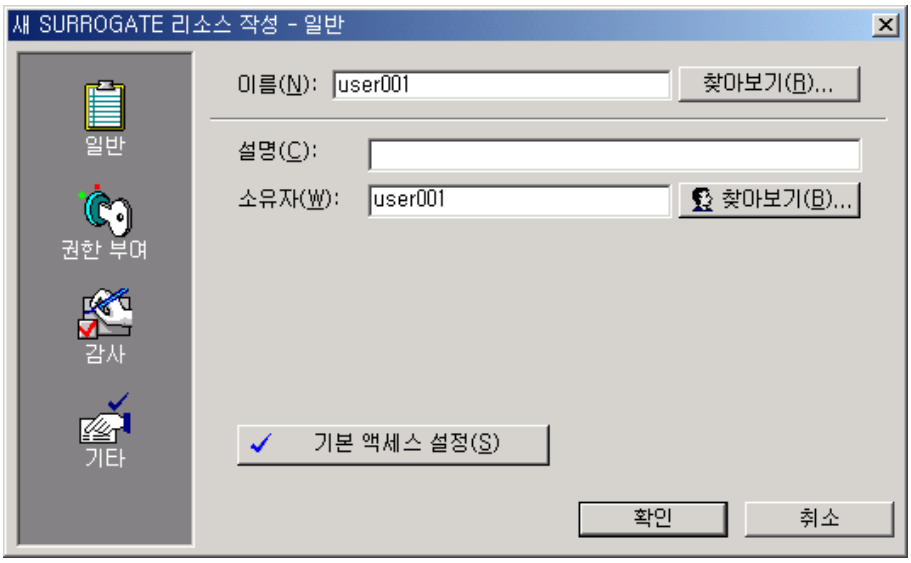
*가장 요청*은 사용자가 사용자 이름을 다른 사용자 이름으로 전환하려고 할 때 생성됩니다. 가장 요청은 RunAs 명령에서 직접 시작되거나 적합한 Win32 API를 사용하는 프로그램에서 시작될 수 있습니다.

eTrust AC는 가장 요청에 대한 제한을 실행하여 관리자 및 기타 사용자를 보호합니다. 직접 확인하려면 다음 단계를 수행하십시오.

1. 암호를 알고 있는 [사용자 이름]을 선택합니다. 다음 명령에서 *user001*은 선택한 사용자 이름을 나타냅니다.

   [리소스] 창에서 [사용자 ID 제어]], [사용자 ID 대체]를 선택하고 도구 모음에서 [새로 만들기]를 클릭합니다.

2. [정책 관리자]에서 다음 규칙을 정의합니다.



이 규칙은 eTrust AC에게 사용자 *user001*에 대한 가장 요청으로부터 보호하고 명시적인 권한이 없는 경우 누구도 user001을 가장할 수 없게 하도록 지시합니다.

다음과 같이 surrogate 규칙을 테스트할 수 있습니다.

- Windows shell 에서 다음 명령을 입력합니다.

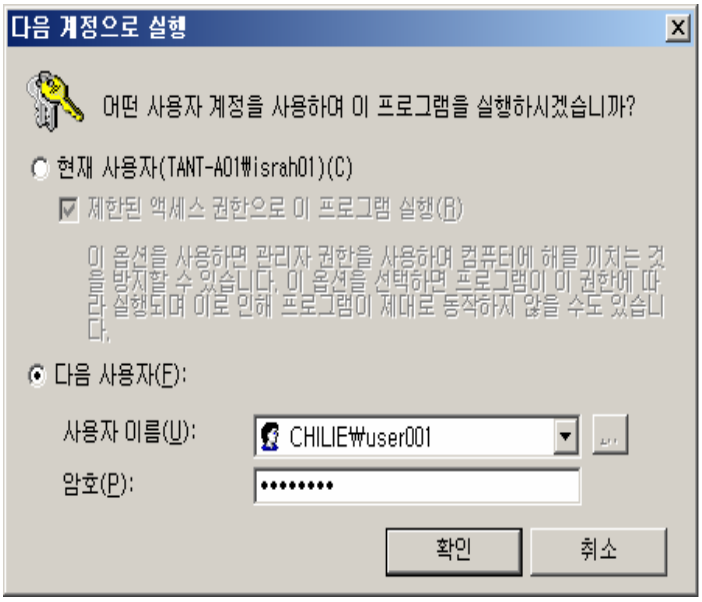
```
cmd> RunAs /profile /USER:CHILE\user001 cmd.exe
```

  - CHILE\user001 의 암호를 입력합니다.

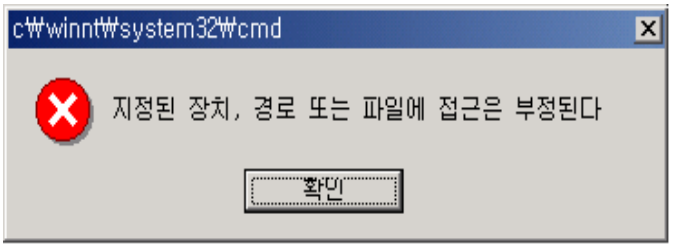
    시스템은 다음 메시지를 반환합니다.

```
Attempting to start "cmd.exe" as user "CHILE\user001"...
RUNAS ERROR: Unable to run - cmd.exe
5: Access is denied.
```

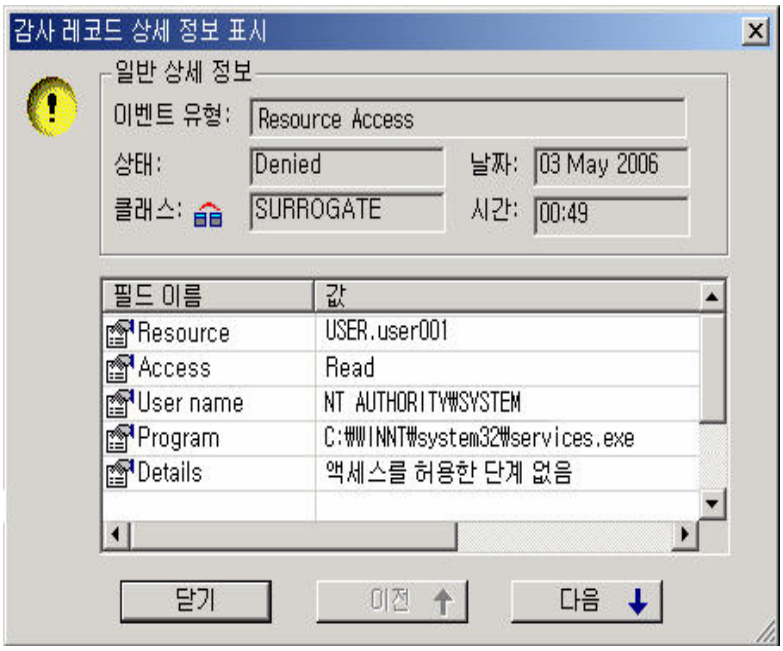
- Windows Run As Another User> 대화 상자에서 다음 명령을 입력합니다.



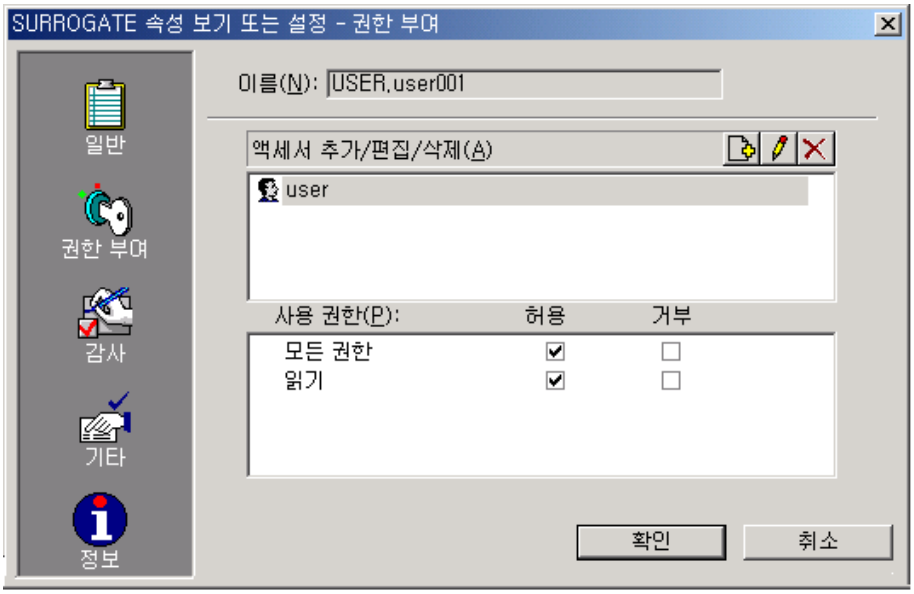
시스템은 다음 메시지를 반환합니다.



감사] 창에서 사용자에게 액세스를 허용하는 규칙이 없으므로 가장 이벤트가 거부된 것을 알 수 있습니다.



eTrust AC 에서 user001 로 가장할 수 있으려면 [정책 관리자] 창에서 다음 규칙을 지정합니다. user001 로 가장할 수 있는 유일한 사용자가 되려는 경우 자신의 사용자 이름을 지정할 수 있습니다. 정의된 모든 eTrust AC 사용자에게 user001 로 가장할 수 있도록 허용하려는 경우, 별표(*)를 사용자로 사용할 수 있습니다.



참고: authorize 명령을 사용하여 이러한 가장 요청에 명시적으로 권한을 부여하지 않은 경우 수퍼유저라도 *user001*로 가장할 수 없습니다.

하루중 시간 및 요일 규칙 설정

시스템이 가장 취약한 시간은 감사자나 다른 직원이 거의 없는 늦은 밤과 주말입니다. eTrust AC 에서는 사용자 로그인을 하루 중 특정 시간 및 주중 특정 요일로 제한하여 더 높은 보안 수준을 확보할 수 있습니다.

사용자에 시간 제한을 추가하여 시작하십시오.

1. [사용자]를 선택하고 [사용자 속성] 창을 엽니다. [기타] 패널에 있는 [날짜/시간 제한]버튼을 클릭하여 시간 제한을 설정합니다.

   기본값은 하루 24시간, 일주일 7일입니다. 원하는 요일의 선택을 취소할 수 있습니다. 시간은 선택한 모든 요일에 적용되지만, 각 요일마다 다른 시간을 설정할 수 없습니다.

   또한 달력 기능을 사용하기 위해 [Unicenter TNG 달력]을 선택할 수 있습니다.

2. 제한을 설정했으면 [확인]을 클릭합니다.
3. 인증된 시간 및 인증되지 않은 시간 동안 사용자로 로그인하여 결과를 확인합니다.

계정 잠금

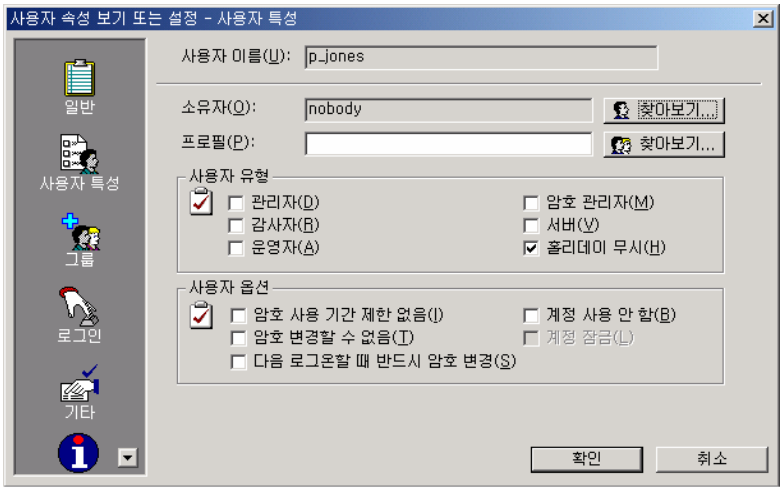
앞의 예제에서 Peter Jones 에게 기본적인 업무 시간의 추가 로그인 액세스를 부여했습니다. 이 시간은 로그인에만 관련됩니다. 일단 로그인하면 원하는 시간 동안 네트워크에 머물 수 있습니다. Peter가 오후 6시에 네트워크에 없도록 하려면, 다음과 같이 설정해야 합니다.

[정책] 메뉴에서 [계정]을 선택합니다. [계정 잠금] 탭에는 로그오프할 수 있도록 맨 아래에 확인란이 있습니다.

휴일 정보 설정

사용자가 시스템에 대한 액세스를 가진 경우 시간을 제한하는 다른 방법은 휴일을 정의하는 것입니다. 휴일은 특정 권한이 없는 모든 사용자의 시스템에 대한 액세스를 차단합니다.

참고: 사사용자 자신이 시스템에 액세스하지 못하게 잠기지 않도록 하는 최상의 방법은 이 연습을 시작하기 전에 사용자 특성을 변경하여 휴일 무시를 포함하는 것입니다. 이렇게 하면 모든 휴일 중에 로그인할 수 있는 권한이 부여됩니다. 다음 그림을 참조하십시오.



[휴일]을 설정하려면:

1. [리소스] 창을 다시 엽니다.
2. [로그인 보호]에서 [휴일]을 선택합니다.
3. [도구 모음]에서 [새로 만들기] 아이콘을 클릭하여 새 휴일 리소스를 작성합니다.

   [휴일] 아이콘을 선택하면 날짜가 추가됩니다. 단일 휴일 리소스에 원하는 만큼의 휴일 수를 입력할 수 있고, 권한에 대해 더 많은 제어를 원하는 경우 별개의 휴일을 정의할 수 있습니다.
4. 시작 및 종료 날짜를 입력하거나 날짜 필드 옆에 있는 화살표를 클릭하여 달력을 드롭다운해서 마우스로 선택할 수 있습니다. 기본값은 매년 휴일에 대해 하루 종일로 설정하지만 해당 확인란을 선택 취소하여 휴일을 변경할 수 있습니다.
5. 다음으로, 인증 권한을 할당합니다. 읽기 권한이 부여된 각 사용자 또는 그룹은 지정된 휴일 동안 로그인할 수 있습니다.
6. 오늘의 휴일 리소스를 작성합니다. 일부 사용자에게 Read 권한을 부여하고, 다른 사용자에게는 None 권한을 부여하며 나머지 사용자는 목록에서 완전히 삭제합니다.
7. 이제 각 사용자로 로그인합니다.

리소스

리소스의 경우 리소스에 적용되는 시간 제한도 있습니다. 터미널, 파일 네트워크 보호 개체, 컨테이너 개체, 레지스트리 개체(사실상 모든 리소스)에 대해 특정 요일 및 시간으로 액세스를 제한할 수 있습니다.

절차는 사용자에 대해 시간을 제한하는 것과 동일합니다. [리소스]를 선택하고 [속성] 창을 연 후 [기타] 패널에서 제한사항을 입력합니다.

다음 내용

이제 네트워크 보안 제어에 유용한 사용자 액세스 및 권한 제한 방법에 대해 더욱 잘 이해하게 되었습니다. 다음 장에서는 네트워크 보호, 발송 연결 제어 등에 대해 설명합니다.

제 6 장: 네트워크 활동 보호

이 장은 아래의 주제를 포함하고 있습니다:

네트워크 수준 Access Control

이 장에서는 사용자에 맞게 eTrust AC 를 사용하는 다음 단계로, 네트워크의 TCP/IP 연결을 보호하는 방법에 대해 설명합니다.

네트워크(TCP/IP) 보호

TCP/IP 네트워크의 개방은 가장 유용한 기능이지만 보안 면에서는 가장 큰 결함입니다. 네트워크 보호 프로그램인 eTrust AC 는 별도의 전용 컴퓨터가 없어도 방화벽 기능을 제공합니다. eTrust AC 를 사용하면 특정 클라이언트가 특정 TCP/IP 서비스를 특정 호스트로 전송하는 것을 허용하고 특정 호스트만 특정 TCP/IP 서비스를 로컬 호스트로 전송하는 것을 허용할 수 있습니다.

인바운드 연결 제어

eTrust AC 가 네트워크의 무단 액세스로부터 컴퓨터를 보호하는 방법을 보려면 다음 단계를 수행합니다.

1. HOST 클래스가 활성화되어 있는지 확인합니다.
   a. [도구] 메뉴에서 [Activates eTrust AC Classes(eAC 클래스 활성화)]를 선택합니다.

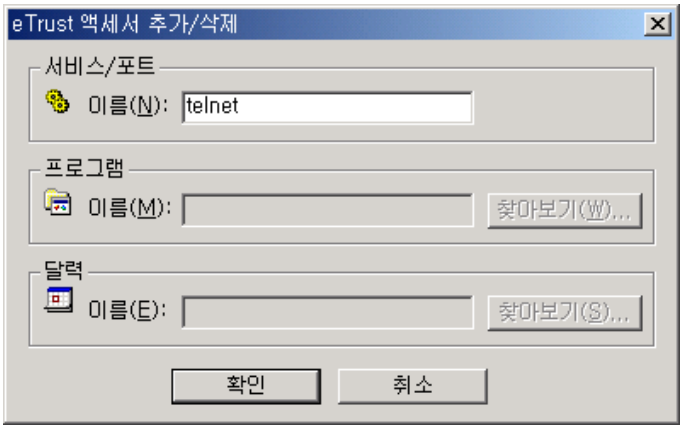
      [eTrust 클래스 활성화] 대화 상자가 나타납니다.

   b. HOST 를 찾을 때까지 스크롤합니다. [HOST] 상자를 선택하지 않은 경우, 상자를 선택하고 [확인]을 클릭합니다.
2. eTrust AC를 실행 중인 컴퓨터에 연결된 다른 컴퓨터를 선택하여 호스트로 정의합니다. 다음 예제에서 *workstation2*는 사용자가 선택한 컴퓨터를 표시합니다.

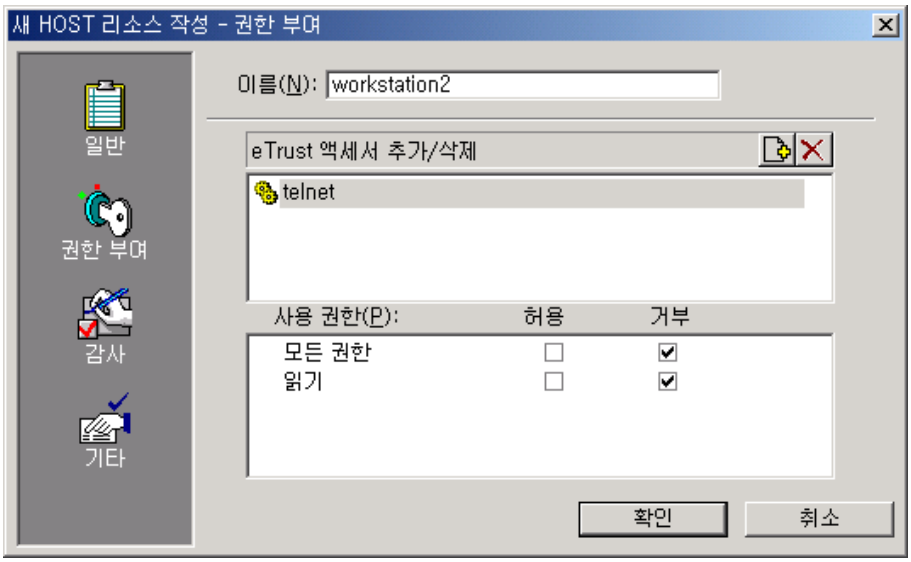
3. workstation2 를 호스트로 정의합니다.

   [Access Control 프로그램 표시줄]에서 [리소스] 아이콘을 클릭하고 [네트워크 보호]를 펼친 후 [호스트]를 선택합니다. 그런 다음 [도구 모음]에서 [새로 만들기] 아이콘을 클릭하십시오. [새 HOST 리소스 작성-일반] 대화 상자가 나타납니다.

   왼쪽 아이콘을 사용하여 새 HOST 레코드에 대한 정보를 입력합니다. [권한 부여] 아이콘을 사용하여 서비스(예: TCP/IP) 또는 포트를 포함하여 권한 정보를 입력합니다.



4. 텔넷을 제외한 workstation2 에서 모든 TCP/IP 서비스를 수신하기 위해 로컬 호스트 권한을 부여합니다. 이 작업을 수행하려면 텔넷 권한을 거부합니다.



5. workstation2 에서 텔넷으로 연결을 시도합니다. 연결 시도가 거부됩니다.

6. workstation2 에서 FTP 로 연결을 시도합니다. FTP 는 텔넷이 아닌 TCP 서비스이므로 FTP 요청이 허용됩니다.

참고: TCP/IP 액세스 규칙을 호스트 그룹 수준, 네트워크 수준, 이름 패턴 수준에서 지정할 수도 있습니다.

호스트 그룹 수준 보호

호스트 그룹을 정의하려면 GHOST 클래스에 데이터베이스 레코드를 만드십시오. 호스트 그룹은 단일 호스트에서와 동일한 방법으로 권한을 수신합니다.

참고: 개별 사용자의 경우와 같이 개별 호스트에 대한 특정 규칙이 그룹 규칙보다 우선합니다.

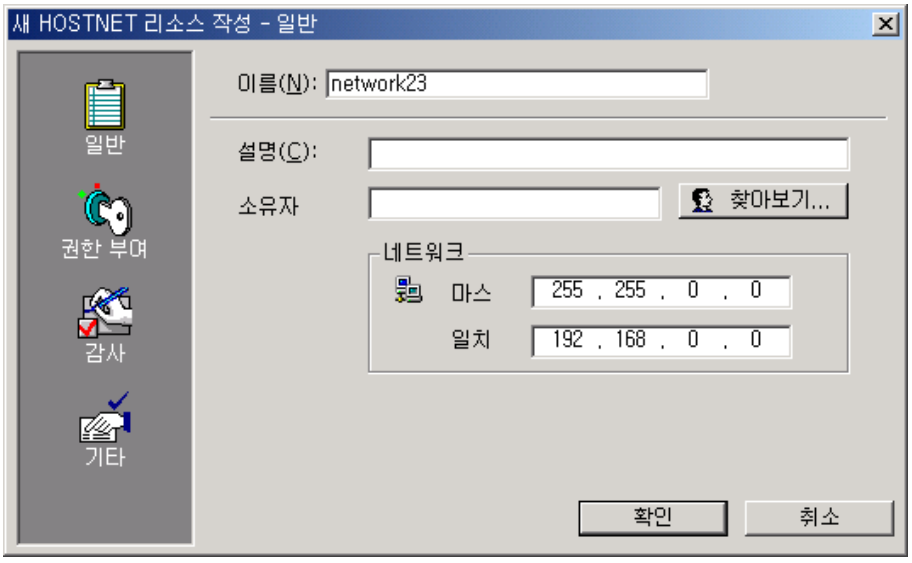
[리소스]에서 TCP/IP 액세스 규칙을 설정하려면 [Access Control 프로그램 표시줄]에 있는 [리소스] 아이콘을 클릭하고 [네트워크 보호]를 펼친 후 [호스트 그룹]을 선택하십시오. 그런 다음 [도구 모음]에서 [새로 만들기] 아이콘을 클릭하십시오.

네트워크 수준 보호

eTrust AC 액세스 규칙을 네트워크 수준에서 지정할 수도 있습니다. 네트워크를 정의하려면 HOSTNET 클래스에 데이터베이스 레코드를 만드십시오. 그러면 네트워크는 단일 HOST 레코드에서와 같은 방법으로 권한을 수신합니다.

참고: 호스트 그룹 수준의 모든 규칙은 네트워크 수준의 규칙보다 우선합니다.

[Access Control 프로그램 표시줄]의 [리소스]에서 TCP/IP 액세스 규칙을 설정하려면 [리소스] 아이콘을 클릭하고 [네트워크 보호]를 펼친 후 [호스트 네트워크]를 선택하십시오. 그런 다음 [도구 모음]에서 [새로 만들기] 아이콘을 클릭하십시오.



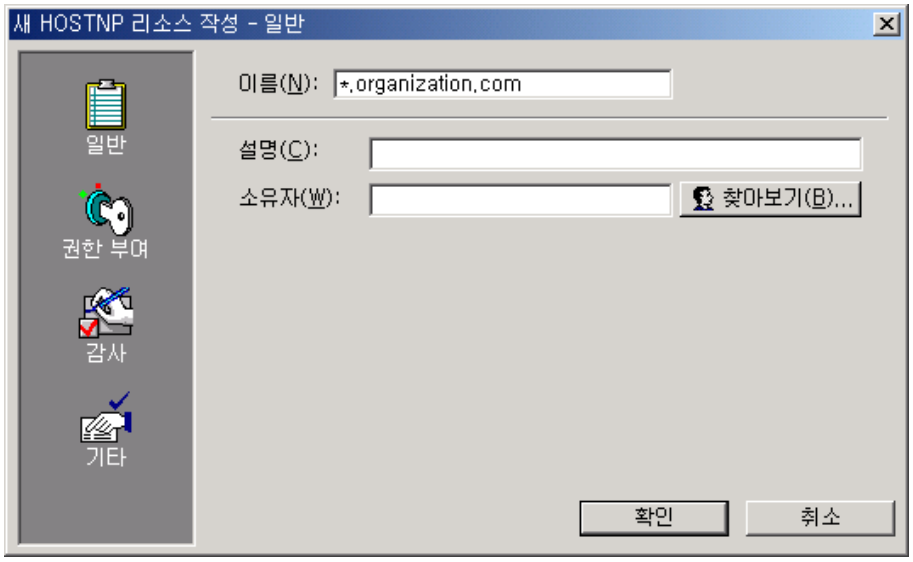
이름 패턴으로 보호

TCP/IP 액세스 규칙을 정의하는 다른 방법은 HOSTNP(호스트 이름 패턴) 클래스를 사용하여 이름 패턴 서비스를 이용하는 것입니다. 네트워크는 단일 HOST 레코드에서와 같은 방법으로 권한을 받습니다.

참고: 네트워크 수준의 모든 규칙은 이름 패턴 수준의 규칙보다 우선합니다.

[리소스]에서 TCP/IP 액세스 규칙을 설정하려면 [Access Control 프로그램 표시줄]에 있는 [리소스] 아이콘을 클릭하고 [네트워크 보호]를 펼친 후 [이름 패턴별 호스트 보호]를 선택하십시오. 그런 다음 [도구 모음]에서 [새로 만들기] 아이콘을 클릭하십시오.

[Create New HOSTNP Resource] 대화 상자가 나타납니다.



발송 연결 제어

각 컴퓨터의 발송 연결을 다른 유형의 리소스로 관리할 수 있습니다.

네트워크 내의 발송 연결을 제한하면 방화벽을 통과한 침입자가 미치는 손상을 최소화할 수 있습니다. 선의의 인터넷 방문자도 네트워크의 특정 서비스 및 시스템 집합으로 제한할 수 있습니다. 예를 들어, 전자 메일 및 필요한 특정 데이터베이스 액세스 형식만 허용합니다.

eTrust AC 에서 발송 연결을 제한하는 방법을 보려면 다음 단계를 수행합니다.

1. CONNECT 클래스가 활성화되었는지 확인합니다.
   a. [도구] 메뉴에서 [Activates eTrust AC Classes(eAC 클래스 활성화)]를 선택합니다.

      [eTrust 클래스 활성화] 대화 상자가 나타납니다.

   b. [CONNECT]를 찾을 때까지 스크롤합니다. [CONNECT] 상자를 선택하지 않은 경우, 상자를 선택하고 [확인]을 클릭합니다.
2. eTrust AC를 실행 중인 컴퓨터에 연결된 다른 컴퓨터를 선택하여 연결 리소스로 정의합니다. 다음 예제에서 *workstation2*는 사용자가 선택한 컴퓨터를 표시합니다.
3. workstation2 를 연결 리소스로 정의합니다. 이 작업을 수행하려면 [Access Control 프로그램 표시줄]에서 [리소스] 아이콘을 클릭하고 [공통] 및 [네트워크 보호] 폴더를 펼친 후 [호스트에 의해 나가는 연결]을 선택합니다. 그런 다음 [새로 만들기] 버튼을 클릭합니다.
4. 사용자의 시스템에서 텔넷으로 또는 FTP 에서 workstaion2 로 연결을 시도합니다. 연결 시도가 거부됩니다.
5. 사용자 j_doe 에게 연결 권한을 할당합니다.
   a. [프로그램 표시줄]에 있는 [리소스]아이콘을 클릭한 후 [네트워크 보호] 옆에 있는 [더하기] 기호를 클릭하여 [트리]를 엽니다.
   b. [호스트에 의해 나가는 연결]을 선택한 후 [workstation2]를 두 번 클릭합니다.
   c. [권한 부여] 아이콘을 클릭하여 [권한 부여] 페이지를 열고 [액세서 추가]에 대해 [십입] 아이콘을 클릭합니다.
   d. [찾아보기] 버튼을 사용하여 사용자 j_doe 를 추가한 후 [확인]을 클릭합니다.
   e. [읽기] 권한의 [허용] 상자를 선택합니다.

   모든 사용자에 대한 거부 규칙에도 불구하고 사용자 j_doe 는 workstation2 에 대해 텔넷 또는 FTP 를 할 수 있는 권한이 이제 부여되었습니다.

서비스 지향 TCP/IP 규칙

eTrust AC 에서는 또한 이 장 앞에서 설명한 규칙과 같은 호스트 지향 및 서비스 지향 TCP/IP 액세스 규칙을 제공합니다.

이러한 종류의 액세스 규칙은 특정 TCP 서비스(포트)로부터 인바운드 및 아웃바운드 연결을 제어할 수 있습니다. 이러한 규칙을 정의하기 위해 TCP 클래스를 사용합니다.

eTrust AC 에서 서비스 지향 TCP/IP 규칙을 사용하여 컴퓨터를 보호하는 방법을 보려면 다음 단계를 수행합니다.

1. HOST 및 CONNECT 클래스를 비활성화합니다.
   a. [도구] 메뉴에서 [Activates eTrust AC Classes(eAC 클래스 활성화)]를 선택합니다.

      [eTrust 클래스 활성화] 대화 상자가 나타납니다.

   b. HOST 를 찾을 때까지 스크롤합니다. [Host] 상자를 선택하지 않아야 합니다.

   c. [CONNECT]를 찾을 때까지 스크롤합니다. [CONNECT] 상자를 선택하지 않아야 합니다.

   d. [확인]을 클릭합니다.
2. 텔넷을 TCP 서비스로 정의합니다.

   [리소스] 창에서 [네트워크 보호], [TCP 보호]를 선택한 후 도구 모음에서 [새로 만들기]를 클릭합니다.

   workstation2 로부터 텔넷 통신을 수신하는 것을 제외하고 모든 컴퓨터와 함께 텔넷 활동 권한을 로컬 호스트에게 부여합니다. 이 작업을 수행하려면 [Create New TCP Resource(새 TCP 리소스 작성)-일반] 대화 상자에서 [기본 액세스 설정] 버튼을 클릭한 후 [모두]를 선택합니다. [확인]을 클릭합니다.
3. [권한 부여] 아이콘을 클릭하여 권한 정보를 입력합니다. [Create New TCP Resource (새 TCP 리소스 작성)-권한 부여] 대화 상자에서 [삽입] 아이콘을 클릭한 후 [eTrust 액세서 추가/편집] 대화 상자에서 [찾아보기] 버튼을 클릭합니다. 그런 다음 [호스트]를 선택한 후 [workstation2]를 선택합니다.

   workstation2 에 대한 읽기 및 쓰기 권한을 선택하지 않아야 합니다.
4. workstation2 에서 텔넷으로 연결을 시도합니다. 연결 시도가 거부됩니다.
5. 텔넷 통신을 workstation2 로 전송하는 사용자 p_jones 를 제외한 로컬 호스트와 함께 텔넷 활동 권한을 모든 컴퓨터에게 부여합니다.

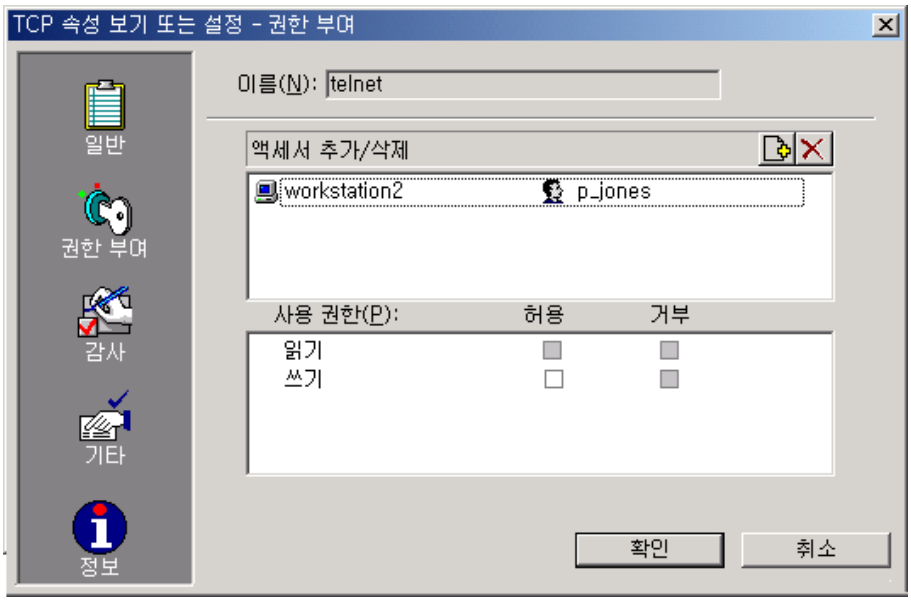
   참고: 텔넷 리소스의 기본 액세스를 [모두]로 이미 설정했습니다.

   a. [View or Set TCP Resource] 대화 상자에서 [권한 부여] 아이콘을 클릭합니다.

   b. [삽입] 아이콘을 클릭하고 [eTrust 액세서 추가/편집] 대화 상자에서 [찾아보기] 버튼을 클릭한 후 [Host]를 선택한 후 [workstation2]를 선택합니다.

   c. [나가는 연결] 상자를 선택 표시한 후 [이름] 필드에 p_jones 를 입력합니다.

d. [확인]을 클릭합니다. 대화 상자는 다음과 같이 나타납니다.



6. 사용자 p_jones 로 로그인하고 workstation2 로 텔넷을 시도합니다. 사용자의 시도가 거부됩니다.

다음 내용

이제 네트워크 보호에 대해 더 잘 알게 되었습니다. 다음 장에서는 암호 정책 설정에 대해 설명합니다.

제 7 장: 암호 및 감사 정책 설정

이 장은 아래의 주제를 포함하고 있습니다:

암호, 로그인 및 감사 규칙

이 장에서는 암호 정책을 정의하고, 암호를 변경하며, 정책 검사 및 감사 정책 등을 활성화합니다. 정책 관리자를 사용하면 기본 보안 정책을 쉽게 설정할 수 있습니다.

보안 정책은 암호 규칙, 로그인 규칙 및 감사 규칙으로 구성됩니다. 사용자에 대해 하나의 일반 정책을 설정하고, 그룹에 대해 서로 다른 정책(그룹 대 그룹 기반)을 설정할 수 있습니다. 일부 설정은 전체적으로 적용되지만 최소 및 최대 사용 기간, 유예와 같은 일부 설정은 개별 사용자 설정에서 재설정될 수 있습니다.

암호 정책 설정

암호 정책을 정의하기 전에 암호 정책 검사가 활성화되었는지 확인합니다. (새로 설치할 경우 이것이 기본 설정입니다.)

1. [도구] 메뉴에서 [Activates eTrust AC Classes(eAC 클래스 활성화)]를 선택합니다.

   [eTrust 클래스 활성화] 대화 상자가 나타납니다.

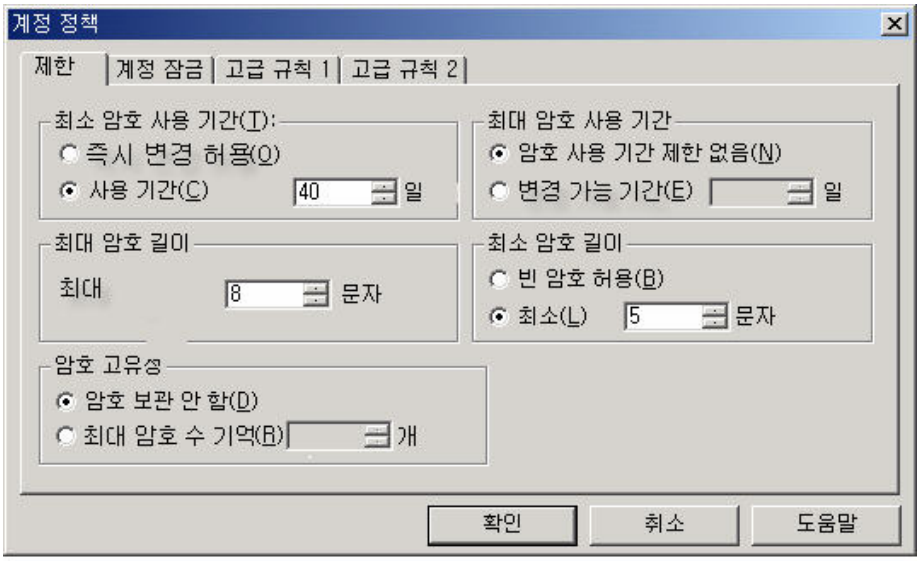
2. [PASSWORD]가 나올 때까지 스크롤합니다. [PASSWORD] 상자를 선택하지 않은 경우, 상자를 선택하고 [확인]을 클릭합니다.

   변경하기 전에 먼저 암호 규칙 기본값을 확인합니다. 이 절의 연습이 끝나면 해당 설정을 복원할 수 있도록 설정을 적어 두십시오.

3. eTrust AC의 현재 값을 검사한 후 사이트의 요구에 맞추어 값을 변경할 수 있습니다. 자세한 내용은 *관리자 가이드*를 참조하십시오.

4. [일반 사용자 계정 정책]을 설정하려면 [사용자] 창을 활성화합니다. [프로그램 표시줄]에서 [사용자] 아이콘을 선택하고, [메뉴 표시줄]에서 [정책]을 선택합니다. 이 메뉴에서 [계정] 또는 [감사] 정책을 설정할 수 있습니다.

   [계정 정책] 창에는 탭이 네 개 있습니다. 처음 두 개의 탭을 사용하여 기본 운영 체제와 eTrust 데이터베이스에 모두 적용되는 규칙을 설정합니다. [고급 규칙] 탭에서는 [eTrust 정책]만 설정합니다.



5. 일부 매개 변수를 변경합니다. 시스템에서 제한을 테스트하여 결과를 확인할 수 있습니다.

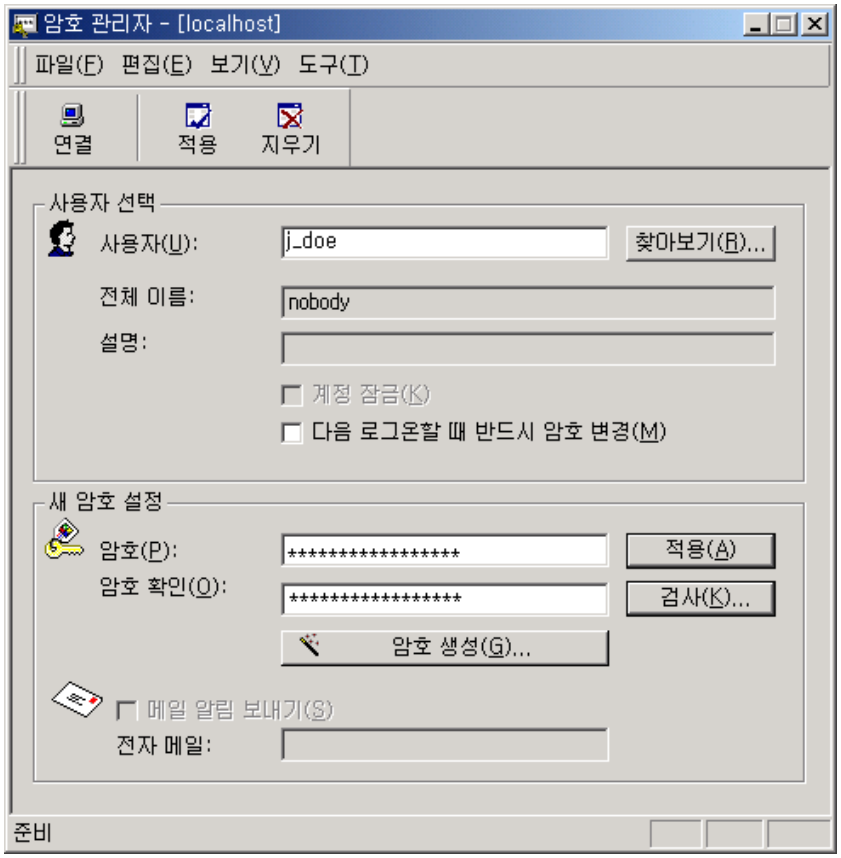
   [고급 규칙]에서는 [eTrust 암호 정책]을 설정합니다. [로그온 수] 필드는 유예 로그인 매개 변수를 나타냅니다.

   참고: 유예 로그인에 대한 자세한 내용은 *관리자 가이드*를 참조하십시오.

암호 변경

사용자 암호를 변경하는 데 정책 관리자는 필요하지 않습니다. 데이터베이스에서 암호 관리자로 지정된 사용자는 [작업 표시줄]의 [시작] 버튼에서 액세스할 수 있는 워크스테이션에 설치된 암호 유틸리티(SetPwd.exe)를 가질 수 있습니다.

[시작], [프로그램], [CA], [eTrust Access Control], [암호 관리자]를 차례로 선택합니다. 암호 관리자 유틸리티는 기본 환경에서 정의된 모든 사용자의 암호를 변경할 수 있습니다.



기본 환경에서 감사 정책 설정

[정책] 메뉴에서 [감사]를 선택하여 감사 정책을 설정합니다.

일부 매개 변수를 변경합니다. 명령행 상세 정보를 검사하여 결과를 확인합니다.

[Windows 이벤트 뷰어]를 열어 변경한 결과를 볼 수 있습니다.

정리

암호와 감사 정책을 원래 기본값으로 재설정했는지 확인합니다.

다음 내용

이제 eTrust AC 의 암호와 감사 정책에 대해 더욱 잘 이해하게 되었습니다. 다음 장에서는 여러 호스트 관리에 대해 설명합니다. 정책 모델 데이터베이스를 작성하고 워크스테이션을 PMDB 에 대해 지정하며 정책 모델 관련 작업 등을 수행하게 됩니다.

제 8 장: 중앙 집중식 관리

이 장은 아래의 주제를 포함하고 있습니다:

사용자, 보안 정책 및 기타 항목 작성

이 장에서는 PMDB(Policy Model database – 정책 모델 데이터베이스)를 작성하고 사용자, 권한 및 암호를 등록합니다. 트랜잭션 관리자는 로컬 호스트에서 수행할 때와 같이 eTrust AC 트랜잭션을 여러 호스트로 자동 전송합니다.

PMDB 작성

다음 예제에서는 policy1 이라는 PMDB 를 작성하고 PMDB workstat1 및 workstat2 를 구독자로 등록합니다. 이 예제를 간단하게 만들려면 동일한 호스트에서 구독자를 작성하십시오.

PMDB 에 대한 관리자 권한을 가진 두 명의 사용자인 adm1 과 adm2 를 등록하려면 다음 단계를 수행하십시오.

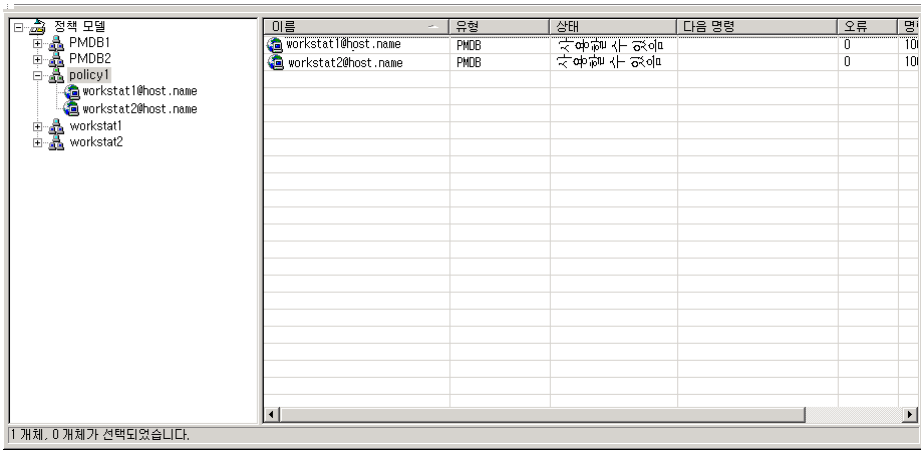
1. bighost 에 연결합니다. 관리자 계정을 작성합니다.
   - PMDB 의 관리자는 PMDB 의 속성을 변경할 권한이 있는 사용자입니다.
   - PMDB 의 감사자는 PMDB 의 감사 로그 파일을 볼 수 있는 권한이 부여된 사용자입니다.
   - PMDB 의 암호 관리자는 PMDB 에서 암호를 변경할 수 있는 권한이 있는 사용자입니다.
2. 세 가지 속성을 모두 가진 사용자를 작성합니다.
3. 관리자에게 워크스테이션에서 관리할 수 있는 터미널 권한을 부여합니다.
4. 로그오프하고 관리자 중 하나로 다시 로그인합니다.
5. [프로그램 표시줄]에서 [도구]를 클릭한 후 [정책 모델]을 선택합니다.
6. [도구 모음]에서 [새로 만들기] 아이콘을 선택하여 새 PMDB 를 작성합니다. PMDB 의 이름을 입력한 후 [관리자] 아이콘을 선택합니다.
7. [새로 만들기]를 선택한 후 이름을 입력하거나 [찾아보기] 버튼을 사용합니다. 두 번째 관리자에 대해 같은 작업을 반복합니다.
8. [터미널]을 선택합니다. [새로 만들기]를 클릭하고 호스트의 이름을 입력하거나 [찾아보기] 버튼을 사용합니다.

9. PMDB 를 작성했으면 구독자를 추가할 수 있습니다. 구독자는 기존 PMDB 또는 eTrust 데이터베이스일 수 있습니다. 이 예제의 경우 구독자 PMDB 를 bighost 에 이미 작성했지만 작성된 PMDB 는 기업의 어느 곳에나 위치할 수 있습니다.

   PMDB policy1 을-마우스 오른쪽 버튼으로 클릭합니다.

10. [구독자 추가]를 선택합니다. 이름을 subscriber@host 형식으로 입력합니다.

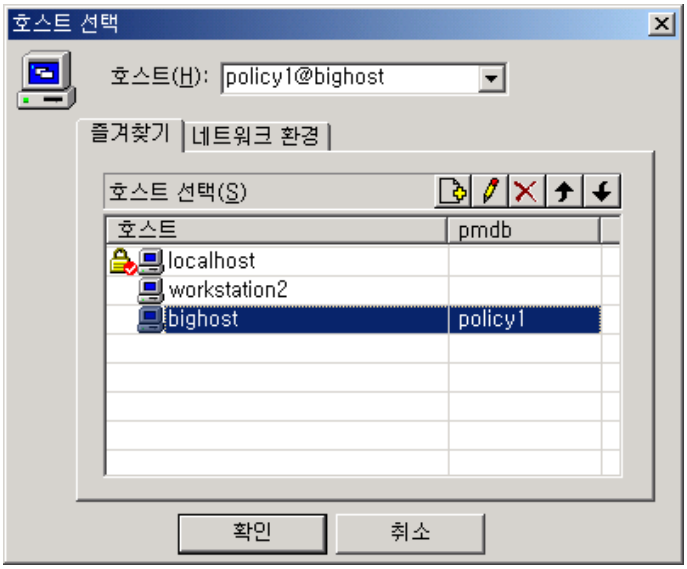
11. 두 번째 구독자에 대해 같은 작업을 반복합니다. [트리]에 정책 모델 계층이 나타납니다.



PMDB 관련 작업

새 사용자를 작성하고 모델을 통해 변경사항이 전파되는지 확인합니다.

1. 먼저 정책 모델에 연결합니다.



2. jsmith(Jennifer Smith)라는 사용자를 생성한 후
3. 구독자 중 한 명에게 연결합니다.

   참고: 호스트가 즐겨찾기 목록에 없는 경우 <연결> 대화상자의 맨 위에 호스트 이름을 입력할 수 있습니다.
4. [사용자] 창을 엽니다.

   새 사용자 jsmith 가 목록에 나타납니다.

트랜잭션 관리자 - 보다 간단한 대안

트랜잭션 관리자는 로컬 호스트에서 수행할 때와 같이 eTrust AC 트랜잭션을 여러 호스트로 자동 전송합니다. 트랜잭션 모드는 정책 모델의 빠르고 효율적인 대체 수단으로 설계되었습니다. 트랜잭션 모드는 모든 구독자의 보안 데이터베이스로 전파할 때 동일한 수준의 전파를 보장하지는 않지만 더 편리하게 사용할 수 있으며 특히 정책 모델 계층의 일부로 정의되지 않은 여러 데이터베이스를 변경할 때 유용합니다.

트랜잭션 관리자 설정

트랜잭션 관리자를 사용하기 전에 다음 항목을 확인하십시오.

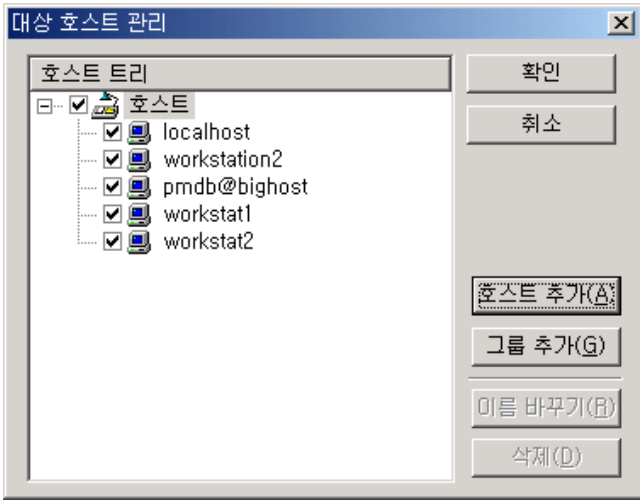
- 로컬 호스트 및 액세스할 각 원격 호스트에 대해 ADMIN 권한을 가지고 있습니다.
- 액세스할 각 호스트에서 컴퓨터를 관리하기 위해 TERMINAL 레코드를 작성했습니다.

이러한 요구사항은 원격 호스트를 관리할 때와 동일합니다. 트랜잭션 관리자를 사용하려면 먼저 활성화해야 합니다.

1. 정책 관리자에서 [도구], [옵션]을 선택하고 [트랜잭션 관리자] 탭을 누릅니다.
2. 목록 위에 있는-[멀티 호스트 트랜잭션 사용] 상자를 선택합니다.

   또한 활성화할 다른 [트랜잭션 관리자] 옵션을 선택할 수 있습니다.
3. [파일], [대상 호스트]를 클릭하여 대상 호스트 파일을 작성합니다.
4. 호스트(workstat1 및 workstat2)를 대상 호스트 목록에 추가합니다.

   명령을 전파할 호스트를 선택합니다.



호스트는 로컬 데이터베이스 또는 PMDB 일 수 있습니다. 선택 시간을 줄이기 위해 호스트 그룹을 만들 수 있습니다. 그룹 이름을 클릭하면 그룹의 모든 구성원이 활성화됩니다. 원하는 개별 호스트를 선택하거나 선택을 해제할 수도 있습니다. 선택한 내용은 [확인]을 클릭하면 즉시 적용되고 변경할 때까지 유지됩니다. 트랜잭션을 다른 그룹의 호스트로 전송할 때마다 대상 호스트 파일을 수동으로 재설정해야 합니다.

참고: [트랜잭션 모드]가 활성화되어 있으면, [호스트 선택] 설정은 [트랜잭션 관리자] 및 [사용자 복사와 그룹 복사 마법사]에 적용됩니다.

5. 계속하기 전에 bighost 에 다시 연결합니다. [도구 모음]에 있는 [트랜잭션 모드] 아이콘을 클릭합니다.

   수행한 모든 트랜잭션이 선택한 호스트로 전파됩니다. [트랜잭션 모드] 아이콘을 다시 클릭하면 명령은 전파되지 않습니다.

이제 작성한 사용자를 삭제합니다.

1. 사용자 jsmith 를 선택하고 [도구 모음]에서 [삭제]를 클릭합니다.

   내부적으로 수행된 작업을 보려면 Windows [작업 표시줄] 트레이의 [트랜잭션 관리자] 아이콘에서 마우스 오른쪽 버튼을 클릭하고 [트랜잭션 관리자 열기]를 선택합니다. 다음 대화상자에는 workstat1 의 결과가 표시됩니다.

2. workstat2 를 선택하여 해당 호스트의 결과를 확인합니다.

   이 예제에서 로그는 빨간색으로 표시되어 명령이 성공적으로 전파되지 않았음을 나타냅니다.

3. 명령 세부사항에 대한 자세한 내용을 보려면 [선택사항]을 두 번 클릭합니다.

참고: 문제를 해결한 후 트랜잭션을 선택하고 [다시 실행] 아이콘을 클릭하여 전파 작업을 다시 실행할 수 있습니다. ([다시 실행] 아이콘은 톱니바퀴처럼 보입니다.)

다음 내용

이제 정책 모델, PMDB 및 트랜잭션 관리자에 대해 더욱 잘 이해하게 되었습니다. 다음 장에서는 eTrust AC 와 Unicenter TNG 로 통합하는 내용에 대해 설명합니다.

제 9 장: Unicenter 와 통합

이 장은 아래의 주제를 포함하고 있습니다:

eTrust AC 를 Unicenter 와 통합

eTrust AC 는 Unicenter TNG 기업 관리 환경에 완전히 통합되었습니다. 이 장에서는 eTrust AC 가 통합을 처리하는 방법을 설명합니다.

참고: 통합을 수행하려면, Unicenter TNG가 eTrust AC와 동일한 시스템에 설치되어야 하고 다음 명령을 사용하여 Unicenter TNG 보안을 활성화해야 합니다.

```
SETOPT CA_ROUTER_CAUSECU 1
SETLOCAL CAIACTSECSV YES
```

Unicenter 통합 도구 설치

Windows 환경에서 Unicenter 통합을 설정하려면 다음 단계를 수행하십시오. eTrust AC 설치 중에 **각** 노드에서 다음 작업을 수행합니다.

1. [설치 마법사]의 [구성 요소 선택] 대화 상자에서 [Unicenter 통합]을 선택한 후 [다음]을 클릭합니다.
2. eTrust AC 는 감사 데이터를 Unicenter TNG 의 구성 매개 변수에 의해 지정된 호스트 또는 사용자가 선택한 호스트로 전송합니다. 통합하려면, 감사 데이터가 Unicenter TNG 로 전송되도록 지정한 후 eTrust AC 가 감사 데이터를 전송할 대상 호스트를 선택합니다.
3. 사용자 및 액세스 권한을 Unicenter TNG 달력과 통합하려면 [Unicenter Calendar 호스트 서버]에서 업데이트를 검색할 주기를 지정한 후 [다음]을 클릭합니다. (기본값은 10 분 간격입니다.)
4. Unicenter 보안 데이터를 마이그레이션하려면 설치 마법사의 [Unicenter 마이그레이션] 대화 상자에서 [eTrust Access Control 에 Unicenter 보안 데이터 마이그레이션]을 선택한 후 [다음]을 클릭합니다.

   참고: Unicenter 보안 데이터를 마이그레이션하지 않으려면 [eTrust Access Control에 Unicenter 보안 데이터 마이그레이션]을 선택하지 **마십시오.**

   이 옵션을 선택하지 않을 경우, Unicenter Security 에서 eTrust AC 로의 마이그레이션이 수행되지 않으며 eTrust AC 의 사용자 이름이 정규화된 이름으로 나타납니다(예: DOMAINNAME\USERNAME). 마이그레이션 중에는 사용자 이름은 완전하지 않습니다(예: USERNAME).
5. 나머지 설치를 계속합니다.
6. 뎅대 대화 상자가 나타날 경우 Windows NT 데이터를 데이터베이스로 가져올지 여부를 나타내려면 [예] 또는 [아니오]를 선택합니다.

   참고: [eTrust Access Control에 Unicenter 보안 데이터 마이그레이션] 옵션을 선택하지 **않은** 경우 [데이터베이스 가져오기] 대화 상자가 나타나지 않습니다.

설치 정보

- Unicenter 통합 및 마이그레이션 설치 프로세스를 실행한 후 Unicenter TNG 로그인 인터셉트를 실행하는 것을 권장하지 않습니다. Unicenter 통합 및 마이그레이션 설치 프로세스를 성공적으로 실행하면 Unicenter TNG 로그인 인터셉트가 비활성화되었는지 확인해야 합니다.
- Unicenter Data Scoping 규칙(-DT 접미사를 가진 Unicenter TNG 자산 유형을 대상으로 하는 규칙)은 eTrust AC 마이그레이션 프로세스에서 지원되지 않습니다. 이런 유형의 규칙은 마이그레이션 프로세스 중에 무시됩니다.
- 다음 Unicenter Security 자산 유형에 대해 구현된 Unicenter Security 규칙은 Unicenter Security 가 더 이상 사용되지 않으므로 필요하지 않습니다: CA-USER, CA-ACCESS, CA-USERGROUP, CA-ASSETGROUP, CA-ASSETTYPE, 및 CA-UPSNODE. 이러한 자산 유형 또는 파생 항목을 대상으로 하는 규칙은 마이그레이션 프로세스 중에 무시됩니다.
- Unicenter 통합 프로세스를 실행한 후 Unicenter TNG를 업그레이드하거나 Unicenter TNG 수정본을 적용할 경우, %CAIGLBL000%\BIN 디렉터리에 있는 CAUSECR.DLL 파일이 바뀌지 않았는지 그리고 *eTrustACDir*\bin 디렉터리의 CAUSECR.DLL.EAC 파일과 동일한지 확인해야 합니다.
- eTrust AC 가 제거된 경우 CA_ROUTER_CAUSECU Unicenter 보안 옵션이 1 로 재설정되고 SETLOCAL CAIACTSECSV Unicenter 보안 옵션이 [예]로 재설정되며 %CAIGLBL000%\BIN 디렉터리의 CAUSECR.DLL 파일이 Unicenter 기본값으로 바뀝니다. 제거 프로세스를 수행한 후 이러한 옵션을 사용자 지정해야 할 경우도 있습니다.

참고: Unicenter 통합 기능과 그 작동 방식에 대한 모든 목록을 보려면 *관리자 가이드*를 참조하십시오.

다음 내용

다음 장에서는 eTrust AC 에 대한 일반적인 질문과 그 대답을 제공합니다. 잠시 시간을 내어 새 소프트웨어에 대한 중요한 정보가 들어 있는 자료를 읽어 보십시오.

제 10 장: 질문과 대답(FAQ)

이 장에서는 몇 가지 일반적인 보안 정책 개념과 eTrust AC 로 UNIX, Linux 및 Windows 보안 관리와 적용 작업을 간편하게 수행하는 방법을 중점적으로 설명합니다. GUI 를 통해 사용자, 그룹 및 시스템 리소스의 관리와 보안 정책의 제어를 중앙 집중식으로 처리할 수 있습니다.

Q: eTrust AC란 무엇입니까?

A: eTrust AC는 UNIX, Linux 및 Windows 서버에 대한 보호와 시스템 관리자에 대한 액세스 관리를 제공하는 소프트웨어 패키지입니다.

기존에 사용되던 일반적인 UNIX 및 Linux 시스템 보호 방법은 위협에 대한 대처, 보안 취약점 평가, root 가 되는 방법 제한에 중점을 두었습니다. 이를 위해 감사 보고서를 자주 실행하고, 셰어웨어 도구를 사용하여 시스템 보안 취약점을 확인하거나 공급업체가 제공하는 CERT 권장 패치를 설치하는 등의-보안 조치를 수행했습니다.

eTrust AC 는 강력한 UNIX 보안을 위해 UNIX 의 시스템 리소스에 대한 액세스 권한을 부여하는 방법을 근본적으로 변경해야 한다는 인식하에 디자인되었습니다. eTrust AC 를 사용하면 간단하고 쉽게 구성할 수 있는 액세스 규칙을 기반으로 서로 다른 운영 OS 리소스에 대한 액세스를 제어할 수 있습니다. 그 결과 보호된 데이터 바로 옆에 보안 층이 추가되었습니다. 이 솔루션은 UNIX 또는 Linux 의 운영 방식이나 관리자의 업무 수행 방법은 변경하지 않습니다.

Q: eTrust AC는 지원되는 각 플랫폼에 대해 동일합니까?

A: 예 eTrust AC의 기능은 지원되는 모든 플랫폼에서 동일합니다. eTrust AC의 모든 인터페이스는-초기 구성 중인 경우를 제외하고 OS 간의 기본적인 차이점에 대해 투명한 교차 플랫폼 관리를 제공합니다. 물론 OS에서 리소스의 이름이 다른 경우 eTrust AC는 기본 운영 체제와 일관성을 유지합니다.

Q: eTrust AC DSX(Dynamic Security Extension) 기술이란 무엇입니까?

A: DSX는 보안 관련 시스템 호출을 동적으로 인터셉트하는 기술입니다. 시스템 호출(또는 시스템 벡터) 테이블은 시스템 호출 커널 코드에 대한 메모리 주소 포인터를 저장합니다. eTrust AC는 이러한 주소 포인터를 저장한 다음, 이들을 해당 eTrust AC 코드에 대한 포인터로 변경합니다.

액세스가 허용되면 원래 syscall 코드에 대한 요청이 계속되고 액세스가 거부되면 요청이 종료됩니다.

Q: eTrust AC는 시스템의 모든 이벤트를 인터셉트합니까?

A: 아니오. eTrust AC는 특정 시스템 호출을 인터셉트합니다. 시스템 호출이 인터셉트되면 eTrust AC 엔진은 데이터베이스에 정의되어 있는 eTrust AC 규칙에 따라 인터셉트된 리소스에 대한 액세스를 허용 또는 거부할지를 결정합니다.

eTrust AC 는 파일 또는 장치에 대한 초기 액세스는 인터셉트하지만 파일에 수행된 후속 I/O 이벤트(예: 읽기와 쓰기)는 인터셉트하지 않습니다.

네트워크 연결에 대해서도 마찬가지입니다. eTrust AC 는 네트워크 소켓 장치(즉, 포트와 IP 주소의 쌍)만-차단하며 이후에 발생하는 데이터 전송은 그대로 진행됩니다.

eTrust AC 는 프로세스에 메모리를 할당하는 루틴을 인터셉트하지 않습니다.

Q: eTrust AC실행 시 발생하는 CPU 오버헤드란 무엇입니까?

A: 이것은 호스트 자체의 기능에 따라 다릅니다. 일반적으로 메일 서버는 데이터베이스 서버를 호스팅하는 시스템보다 성능 문제가 적습니다.

고성능을 요구하는 시스템을 사용한 결과 CPU 에-1-5%의 추가 오버헤드가 발생했습니다.

Q: 액세스 규칙은 어디에 저장됩니까?

A: eTrust AC 액세스 규칙은 로컬 호스트의 보호된 데이터베이스에 저장됩니다.

Q: eTrust AC에는 API가 있습니까?

A: 예 실제로 eTrust AC에는 eTrust AC 개방형 아키텍처와 관련된 수많은 API가 있습니다. API는 Access Control부터 관리 및 경고 알림에 이르는 모든 작업에 사용될 수 있습니다. eTrust AC 설명서에는 각 API의 사용법이 자세히 설명되어 있으며 C에서 설명한 샘플 프로그램이 소프트웨어에 포함되어 있습니다. eTrust AC API에는 다음이 포함됩니다.

- **권한 API**는 임의의 리소스에 대한 사용자 액세스 권한을 확인하기 위해 응용 프로그램에서 사용됩니다. 이 API 호출을 통해 사이트에서 가정용 응용 프로그램에 대해서도 eTrust AC 보안을 중앙 집중식으로 관리할 수 있습니다.
- **관리 API**는 eTrust AC를 통해 제어되는 Windows, UNIX 또는 Linux 보안 측면을 관리하는 응용 프로그램에서 사용됩니다.
- **감사 API**는 eTrust AC 감사 기능을 사용자 지정할 수 있도록 합니다.
- **암호 API**는 제품에 제공된 암호 품질 확인 기능을 사용할 수 있을 뿐만 아니라 암호 품질 확인 기능을 사용자 지정할 수 있도록 합니다.

Q: eTrust AC는 네트워크 프로세스 통신에 대한 암호화를 제공합니까?

A: 예. eTrust AC는 eTrust AC에 관련된 모든 네트워크 통신을 암호화합니다.

Q: eTrust AC는 무엇을 보호합니까?

A: eTrust AC는 보호된 호스트에 있는 운영 체제와 응용 프로그램 리소스를 보호합니다. 시스템 리소스에 대한 액세스를 제어하여 이러한 보호 작업이 수행됩니다. 다음은 eTrust AC를 통해 보호할 수 있는 리소스 유형과 제어되는 액세스 유형에 대한 간단한 목록입니다.

파일(일반 파일 및 개별 파일)

확장된 파일 액세스 제어는 운영 체제 제한 이상으로 파일을 보호합니다. 예를 들어 파일에 대한 액세스 권한이 없는 사용자는 root 액세스 권한을 가지고도 액세스할 수 없습니다. eTrust AC는 또한 사용자가 파일에 액세스하는 *방법*(어느 프로그램이나 응용 프로그램을 사용하여 액세스하는지)을 제어합니다.

네트워크 연결

eTrust AC 는 들어오고 나가는 네트워크 연결을 규정하여 네트워크 서비스 및 포트에 대한 액세스를 제어합니다.

프로세스

eTrust AC 는 권한이 없는 사용자에 의해 프로세스가 강제 중단되지 않도록 보호합니다. Windows 서비스를 보호하는 데 이 기능이 유용합니다.

사용자 ID 및 그룹 ID(su)

UNIX 에만 해당함. eTrust AC 는 사용자 ID 교체와 그룹 ID 교체를 제어할 수 있습니다. 다른 사용자의 암호를 알고 있어도 다른 사용자 ID 로 서로게이트할 수 없습니다.

권한이 있는 프로그램

인증된 권한으로 실행되는 프로그램은 허가 없이 은밀하게 시스템 리소스에 액세스하는 주요 소스가 됩니다. eTrust AC 는 권한 있는 프로그램의 트러스트된 기반이 수정되지 않도록 보호하며 인식되지 않는 권한 있는 새 프로그램이 실행되지 않도록 합니다.

특수 프로그램(SPECIALPGM)

프로그램 또는 시스템 서비스와 같은 일부 응용 프로그램에는 특정 eTrust AC 권한 보호가 필요합니다. 특수 프로그램은 논리적 사용자 이름(eTrust AC 데이터베이스에서 USER 레코드로 정의됨)을 프로그램 실행에 필요한 Windows 사용자 이름과 연결하여 논리적 사용자만 프로그램을 사용할 수 있도록 권한을 부여함으로써 지정된 프로그램을 보호합니다.

STOP(스택 오버플로 보호)

STOP 을 사용하면 해커가 시스템에 침입하기 위해 임의의 명령을 실행할 수 있는 스택 오버플로우가 사용되지 않습니다.

터미널

eTrust AC 는-어떤 사용자가 어떤 조건에서 어떤 터미널에서 로그인할 수 있는지 정의하여 시스템 액세스의 초기 상황을 제어합니다.

사용자-정의된 리소스

eTrust AC 권한 API 및 데이터베이스 도구를 사용하여-eTrust AC 서버에 연결된 응용 프로그램에 연결된 응용 프로그램에서 데이터로의 액세스를 보호하기 위한 사이트 특정 규칙을 정의할 수 있습니다.

사용자 및 그룹 가장

Windows 에만 해당함. eTrust AC 는 사용자 및 그룹의 가장을 제어합니다. 다른 사용자의 암호를 알더라도 해당 사용자를 가장할 수 없습니다.

Windows 레지스트리

Windows 에만 해당함. eTrust AC 는 레지스트리 키를 액세스할 수 있는 사용자의 능력을 제한합니다. 사용자에게 READ, WRITE 및 DELETE 와 같은 하나 이상의 액세스 유형을 지정할 수 있습니다. 개별 레지스트리 키에 대한 액세스를 지정하거나 이름이 유사한 레지스트리 키의 집합에 대한 액세스를 지정할 수 있습니다.

Q: eTrust AC는 root 액세스 권한을 얻은 공격자로부터 리소스를 보호할 수 있습니까?

A: 예 실제로 이 방법은 eTrust AC가 UNIX 및 Linux 보안을 향상시키는 기본적인 방법 중 하나입니다. 원시 UNIX에서 ID가 0 인 사용자는 모든 시스템 리소스에 효율적으로 액세스할 수 있습니다. 사용자 암호와 파일 사용 권한은 root를 성공적으로 공격하는 사용자에 대해 효율적으로 보호하지 못하며 감사 추적 없이 규칙을 수정할 수 있습니다.

Q: eTrust AC는 루트 권한을 어떻게 관리합니까?

A: UNIX 및 Linux에 대한 가장 큰 보안 위협은 강력한 사용자인 수퍼유저 - 루트 --전체 권한 사용자-ID를 사용하여 조직 내 다양한 사용자에게 액세스할 수 있다는 것입니다. eTrust AC:

- root 에 대한 액세스를 감시합니다.
- root 권한 사용자가 수행할 수 있는 작업을 정의하고 제한합니다.
- root 권한 사용자의 무제한적인 권한을 수정합니다.
- 이러한 권한을 책임 있는 사용자에게 부여합니다.
- 공격자의 root 액세스를 통해 발생할 수 있는 손상 범위를 제한합니다.
- 시장에 유통되는 어떠한 보안 솔루션도 이러한 혁신적인 기능을 제공하지 못합니다.

Q: root 권한을-사용 필요성을 기반으로-위임하는 방법은 무엇입니까?

A: 관리자와 운영자는 자신들의 작업을 수행하기 위해 권한이 있는 루트 접근이 필요합니다. eTrust AC를 사용하지 않는 경우 루트 암호를 제공함으로써 루트 액세스가 "완전히 되거나 아니면 아예 되지 않습니다". eTrust AC는 "역할"을 정의하는 데 적용하기 쉬운 규칙을 제공합니다. 이러한 역할은 책임 있는 사용자에게 루트 권한을 위임합니다.

Q: eTrust AC 파일 액세스 제어 기능이 UNIX 또는 Linux의 파일 사용 권한을 대신합니까?

A: 아니오. 파일 접근 제어는 UNIX 파일 권한을 강화합니다. 원시 UNIX는 root 액세스 권한이 있는 공격자에 대한 파일 보안 기능을 제공하지 못하며 파일 그룹에 대해 액세스 권한을 결정하고 관리하기 위한 일반 와일드카드 정의를 통해 파일을 보호할 수 없습니다.

eTrust AC 는 모든 파일 액세스 요청을 인터셉트하고 해당 액세스 제어 목록(ACL)에 따라 요청된 방법으로 파일에 액세스할 수 있는 권한이 부여되었는지 확인하여 완전한 파일 보호를 제공합니다.

eTrust AC 는 전체 디렉터리(예: /etc/* or $DIR/webserver/ht-docs/*)의 내용을 보호할 수 있습니다. eTrust AC 규칙은 $HOME/*/.rhosts 와 같은 파일을 보호하여 모든 사용자의 .rhosts 파일을 보호할 수도 있습니다. /app/config* 패턴의 이름이 있는 파일 세트를 보호하는 규칙을 설정할 수도 있습니다. 예를 들면 /app/config.dat 와 /app/config.tar 등의 파일이 보호됩니다.

디렉터리 또는 공통 표기법에 매핑되지 않은 파일을 보호해야 하는 경우 GFILE 클래스를 사용할 수 있습니다. 이 클래스를 사용하여 특정 파일을 정의하고 공통 Access Control 규칙 집합을 모든 파일에 적용할 수 있습니다.

또한 프로그램 ACL(PACL)을 사용하여 중요한 리소스의 경우 허가된 프로그램을 사용해야만 액세스할 수 있도록 합니다. 예를 들어 직원 데이터베이스 파일은 데이터베이스 응용 프로그램을 사용해야만 기록할 수 있습니다. 기본 UNIX ACL 을 지원하는 운영 체제(Solaris 및 HP-UX)의 경우, eTrust AC 는 eTrust AC ACL 과 운영 체제를 동기화할 수 있습니다.

Q: 규칙이 지나치게 제한적인지 확인하는 방법은 무엇입니까?

A: "접속률"을 살펴보거나 또는 거부된 접근을 가려내기 위해 규칙을 적용하는 것은 실용적이지 못하므로 eTrust AC에서는 모니터-전용 모드(경고 모드)를 포함합니다. 사용자가 접근 권한이 없는 리소스에 접근을 시도한다고 가정합니다. 리소스가 경고 모드에 있으면 액세스 규칙이 적용되지 않지만(즉, 해당 운영 체제가 허용하는 경우 사용자 리소스 액세스 가능) 특수 감사 로그 항목이 생성되어 적용 모드에서는 액세스가 거부된다는 내용을 나타냅니다.

감사 로그 항목에서 경고를 발생시킨 리소스 액세스를 검토함으로써 규칙을 실제로 적용하지 않고도 규칙이 지나치게 제한적인지 여부를 확인할 수 있습니다. 이 방법은 OS 내에서 예상치 못한 작업을 수행하는 응용 프로그램을 중단하지 않으면서 새 규칙을 개발하는 데 매우 유용합니다.

Q: 인터페이스와 일괄 처리를 통해 eTrust AC를 관리할 수 있습니까?

A: 예 selang 명령줄 인터페이스는 정책 관리자(관리 인터페이스) 및 일괄 처리에 함께 사용할 수 있습니다.

Q: 정책 모델이란 무엇입니까?

A: 정책 모델은 여러 시스템에 액세스 규칙을 전파하고, 다양한 호스트를 구독자로 가진 액세스 규칙 집합 모델을 작성하기 위한 간단한 계층형 메커니즘입니다. 각 PMDB는-독립 실행형 eTrust AC 데이터베이스로, 특정 호스트 시스템과 연관된 eTrust AC 데이터베이스와 동일한 유형의 규칙을 포함합니다. 마스터 PMDB에 적용된 규칙은 마스터 PMDB에 대해 정의된 모든 구독된 데이터베이스로 전파됩니다.

Q: eTrust AC는 Windows 및 UNIX 운영 체제를 모두 관리할 수 있도록 합니까?

A: 예 eTrust AC는 관리자가 중앙에서 Windows 및 UNIX의 사용자 계정과 리소스를 관리할 수 있는 강력하고 간편한 GUI를 제공합니다.

Q: 사용자를 두 번에 걸쳐 즉, 한 번은 UNIX나 Linux에, 한 번은 eTrust AC에 추가해야 합니까?

A: 아니오. 하지만 명시적 리소스 접근 제어가 있어야 하는 사용자는 두 환경 모두에서 필요합니다. 따라서 이러한 사용자는 원시 UNIX와 eTrust AC 데이터베이스 모두에 정의되어야 합니다. 정책 관리자 인터페이스를 사용하여 UNIX 사용자와 그룹 및 eTrust AC 사용자와 그룹을 정의하거나 정의를 변경할 수 있습니다.

Q: eTrust AC를 사용하여 UNIX 및 Linux 운영 체제뿐만 아니라 Windows 운영 체제도 관리할 수 있습니까?

A: 예 eTrust AC는 강력하고 간편한 GUI를 제공하여 관리자가 중앙의 한 위치에서 여러 운영 체제의 사용자 계정과 리소스를 관리할 수 있도록 합니다.

Q: eTrust AC는 하드웨어-기반 인증(예: SecureID)을 지원합니까?

A: eTrust AC는 인증 과정을 인터럽트하지 않는 한 모든 인증 소프트웨어와 호환됩니다.

Q: eTrust AC를 방화벽과 비교할 경우 어떤 차이가 있습니까?

A: 방화벽은 네트워크, 호스트, 사용자, 프로토콜, 서비스 및 응용프로그램을 사용하는 외부 소스에 대한 네트워크 액세스와 이러한 외부 소스로부터의 네트워크 액세스를 제한하기 위해 사용됩니다. 비즈니스의 네트워크-기반 연결성 수준이 높아짐에 따라 점점 많은 데이터가 방화벽을 통해 전달됩니다.

방화벽으로 보호되는 서버와 데이터는 공격받기 쉽습니다. eTrust AC 는 방화벽 뒤에 있는 시스템의 리소스와 DMZ 에 있는 리소스를 보호합니다.

Q: 방화벽이 있는 경우 왜 eTrust AC가 필요합니까?

A: 방화벽은 들어오고 나가는 네트워크 트래픽을 필터하기 위해 중요합니다. 적절히-구성할 경우 방화벽은 시스템에 침입할 수 있는 의심스러운 사용자 수를 크게 줄일 수 있으며 인터넷을 통해 정보 자산이 빠져나가지 않도록 보호할 수 있습니다.

그러나 방화벽은 일단 네트워크 내부로 침입한 사용자에 대해서는 어떠한 보안 조치도 취할 수 없습니다. 또한 방화벽은 솜씨 좋은 해커에 의해 쉽게 뚫릴 수 있으며 지금까지 그래왔습니다.

Q: eTrust AC가 사전 대처형 보안을 제공한다는 것은 정확히 무엇을 의미합니까?

A: 대부분의 보안 솔루션은 특성상 요청에 반응하는 수동적인 메소드를 제공하는 것이 일반적입니다. 지금까지 컴퓨터 보안을 보면 수동적인 메소드는 보안 증상을 응용 프로그램 수준에서 처리하기 때문에 임시적인 방어책밖에 되지 못했습니다. eTrust AC는 시스템 및 시스템 호출 수준에서 보안 이벤트를 해결하는 방식으로 설계되었습니다.

모든 리소스 액세스 요청(응용 프로그램 또는 다른 리소스)이 시스템에 의해 처리되며 커널을 통과한다는 사실을 토대로 이러한 방법이 수행됩니다. 보안에 민감한 요청을 수행하는 경우 eTrust AC 는 보안 위협을 받기 전에 요청을 차단하여 비활성화시킬 수 있습니다.

Q: 다른 프리웨어 보안 솔루션과 비교할 때 eTrust AC의 혜택은 무엇입니까?

A: 프리웨어 솔루션은 순간 대처형 기능을 제공합니다. 이 솔루션은 원인이 아닌 증상을 해결하며 루트 또는 시스템 공격으로부터 보호할 수 없는 해결책을 제공합니다.

프리웨어와 비교하여 eTrust AC 가 제공하는 이점은 다음과 같습니다.

- 자체-보호.
- 자체-검사 기능(규칙 데이터베이스, 서비스 및 데몬)은
- 구성 파일 실행 시 구성 파일을 보호합니다.
- 설치 및 유지 관리에 필요한 관리 오버헤드가 낮습니다.
- 공급업체 지원을 받을 수 있습니다.
- 점진적인 구현을 제공합니다. eTrust AC 에는 경고 모드라는 개념이 있습니다. 업무에 영향을 주지 않으면서 규칙을 간단히 적용할 수 있습니다.
- 프리웨어 솔루션을 포함하는 공통된 솔루션을 제공하여 여러 시스템과 플랫폼을 단일 지점에서 관리할 수 있도록 합니다.

보다 잘 알려져 있는 호스트-기반 솔루션에는 SUDO, 감사, Tripwire 및 TCP 래퍼가 있습니다. eTrust AC 는 이러한 솔루션을 모두 단일 패키지로 제공하며, 사전 대처형 보안 기능을 커널에 제공하여 증상이 아닌 핵심 문제를 해결합니다.

"루트 계정이 누군가에 의해 손상될 경우 프리웨어 솔루션으로 이러한 문제를 해결할 수 있을까?"라는 의문을 가질 수 있습니다. 대답은 그렇지 않다는 것입니다. 이러한 도구는 보안에 대해 잘못된 인식을 심어줍니다. 그러나 eTrust AC 를 사용하면 이러한 문제를 해결할 수 있습니다. 이 프로그램은 주요 리소스에 대한 보호 기능을 제공할 수 있습니다.

Q: eTrust AC를 원시 파일 사용 권한과 비교할 경우 어떤 차이가 있습니까?

A: 기본 파일 권한은 단순히 소유자, 단일 그룹 및 전체에 대해 읽기, 쓰기 및 실행 등의 권한을 제공합니다. 기본 파일 액세스 권한은-루트 액세스 권한 사용자나 해당 파일의 소유자에 의해 재정의될 수 있습니다.

eTrust AC 는 업데이트, 삭제 및 생성 등의 다양한 액세스 권한을 사용하여 일반 운영 체제 액세스 모드 이상의 액세스 모드로 확장합니다. eTrust AC 액세스 모드는 해당 파일 소유자 또는 루트 계정에 의해 손상되지 않습니다. UNIX 또는 Linux 에서 액세스 그룹이 하나로 제한되어 있는 경우 eTrust AC 는 여러 개의 그룹에 서로 다른 액세스 권한을 부여할 수 있습니다.

eTrust AC 는 또한 파일 액세스가 허용된 프로그램을 기반으로 파일 액세스 권한을 확장합니다. 원시 UNIX 또는 Linux 에서는 이 기능을 제공하지 않습니다.

Q: eTrust AC는 100% 보안 솔루션을 제공할 수 있습니까?

A: 100% 보안을 제공하는 솔루션이란 존재하지 않습니다. 그러나 eTrust AC는 운영 체제 보안 문제의 원인을 해결하여 이전에는 없었던 포괄적이며 보다 합리적인 소프트웨어 솔루션을 제공할 수 있습니다. 소프트웨어 제어만으로는 보안 문제를 해결할 수 없으며 실제 액세스와 계정 공유 등과 관련된 일반적인 정책을 설정하고 준수함으로써 접근해야 합니다.

Q: "rootkit"과 같은 도구를 사용하여 컴퓨터에 접근하는 해커들이 있다고 들었습니다. eTrust AC는 이러한 해커들로부터 시스템을 보호할 수 있습니까?

A: Rootkit은 컴퓨터에 권한 없이 접근하기 위해 사용되는 여러 가지 도구 중 하나입니다. 이 도구는 해커들이 사용하는 유일한 도구는 아닙니다. eTrust AC가 이러한 문제들을 해결하는 방법을 설명하기 위해 아래에서 해커의 목표와 일반적인 프로파일, 도구, eTrust AC에서의 해결 방법을 알아보겠습니다.

해커의 목표는 루트 계정을 확보하여 시스템을 완전 제어하는 것입니다. eTrust AC 는 루트가 되는 사용자 및 방법을 제한하여 이 문제에 대응할 수 있습니다. 허가되지 않은 root 액세스가 발생할 경우 eTrust AC 는 액세스 가능한 대상을 제어할 수 있습니다.

다음은 해커의 침입에 대해 방어하는 방법을 보여 줍니다.

공격 프로필	해킹 공격	eTrust AC 방어
A) 침입	A1) 잘 알려진 서비스 결함	A1a) 유효한 원격 소스에 대한 액세스를 비활성화하거나 제한합니다.
	A2) 잘못된 암호를 가진 계정	A2a) 반복적으로 공격받는 계정을 비활성화합니다.
		A2b) 중요한 계정으로만 로컬 액세스를 제한합니다.
		A2c) 암호 품질 제어 수행
B) root 획득	B1) 결함 있는 프로그램	B1a) root 액세스를 허용하는 프로그램을 제한합니다.
	B2) root 암호 추측	B2a) root 권한 사용자로만 로컬 액세스를 제한합니다.
		B2b) 암호가 알려진 경우에도 root 권한을 가질 수 있는 사용자를 제한합니다.
C) root 획득	C1) 기존의 권한 있는 프로그램 변경	C1a) 권한 있는 프로그램의 무단 변경을 방지합니다.
	C2) 권한이 있는 새로운 프로그램의 도입	C2a) 시스템에 허가되지 않은 프로그램이 유입되지 않도록 보호합니다.
	C3) 침입을 숨기기 위해 시스템 로그 변경	C3a) 시스템 로그의 무단 변경을 방지합니다.
		C3b) 시스템과는 별개의 로깅을 제공합니다.

또한 eTrust AC 는 스택 오버플로 공격 또는 버퍼 오버플로 공격으로부터 시스템을 보호하기 위해 eTrust AC 의 기능을 강화하는 스택 오버플로 보호(STOP)라는 새 eTrust 기술을 사용합니다.