eTrust® Access Control for Windows

관리자 안내서

r8 SP1

본 문서 ("문서") 및 관련 컴퓨터 소프트웨어 프로그램 ("소프트웨어")(이하 제품이라고 총칭함)은 최종 사용자에게 정보를 제공하기 위한 것이며 CA 는 언제든지 이를 변경하거나 회수할 수 있습니다.

CA 의 사전 서면 동의 없이 이 제품의 전체 또는 일부를 복사, 전송, 재생산, 공개, 수정 또는 복제할 수 없습니다. 이 제품에 들어 있는 정보는 CA 소유이며 미국 저작권법 및 국제 협약에 의해 보호받습니다.

상기 조항에도 불구하고, 모든 CA 저작권 공지 사항과 범례가 재생산된 각 복사본에 첨부된다는 전제 하에 사용권을 가지고 있는 사용자는 내부적으로 사용하기 위해 문서의 복사본을 합당한 수의 범위 내에서 인쇄할 수 있으며, 백업 및 재난 복구 목적으로 정당하게 필요한 경우에 한해 제품을 복사할 수 있습니다. 인가된 직원, 컨설턴트 또는 소프트웨어 사용권 기밀 조항의 구속력 하에 있는 사용자 대리인만 해당 복사본에 액세스할 수 있습니다.

문서의 복사본을 인쇄할 권리 및 소프트웨어를 복사할 있는 권리는 해당 제품의 사용권이 완전한 효력을 가지는 기간으로 제한됩니다. 어떤 이유로든 사용권이 종료된 경우 사용자는 제품의 전체 및 일부 사본이 CA 로 반납 또는 파기되었음을 서면으로 CA 에 입증할 책임이 있습니다.

해당 법규에서 허용하는 한도 내에서 CA 는 상품성, 특정 목적에 대한 적합성 또는 비침해에 대한 묵시적 보증을 포함하여, 이에 한정되지 않고, 어떠한 종류의 보증도 없이 이 제품을 "있는 그대로" 제공합니다. CA 는 이익 손실, 사업 중단, 신용 또는 데이터의 손실을 포함하여, 이에 한정되지 않고, 이 제품의 사용으로 인한 직간접 손해 또는 손실과 관련하여 그러한 손해 또는 손실에 대해 명백히 알고 있는 경우를 포함하여 그 어떠한 경우에도 최종 사용자 또는 기타 제 3 자에 대해 책임을 지지 않습니다.

이 제품 및 문서에 언급된 모든 제품에 대한 사용 조건은 해당 최종 사용자 사용권 계약서의 내용을 따릅니다.

본 문서는 CA.에서 작성하였습니다.

이 제품은 "권리 제한"과 함께 제공됩니다. 미국 정부에 의한 사용, 복제 또는 공개는 FAR 12.212, 52.227-14 항 및 52.227-19(c)(1) - (2) 항 및 DFARS 252.227-7013(c)(1)(ii) 항 또는 해당하는 경우 후속 조항에 명시된 "제한"을 따릅니다.

여기에 언급된 모든 상표, 상호, 서비스표 및 로고는 각 해당 회사의 소유입니다.

Copyright © 2006 CA. All rights reserved.

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: 소개

이 장은 아래의 주제를 포함하고 있습니다:

서문

본 가이드에서는 개방형 시스템을 위한 토탈 보안 솔루션을 제공하는 Windows 용 eTrust AC 에서 사용하는 개념에 대해 설명하며, 특히 Windows 용 eTrust AC 관리에 사용되는 사용자 인터페이스 및 정책 관리자에 대해 설명합니다.

가이드 사용자

이 가이드는 eTrust AC 보호 환경을 구현하고 유지 관리하는 보안 및 시스템 관리자용으로 작성되었습니다.

명령 표기 규칙

eTrust AC 설명서는 명령 구문 및 사용자 입력을 설명할 때 몇 가지 특별한 규칙을 사용합니다.

서식	의미
고정 폭 글꼴	코드 또는 프로그램 출력
기울임꼴	제공해야 하는 정보의 자리 표시자
굵게	표시된 대로 동일하게 입력해야 하는 요소
대괄호([]) 사이	선택적인 항목
중괄호({}) 사이, 파이프(|)로 구분된 선택 항목	반드시 하나를 선택해야 하는 필수 선택 항목 집합
줄 끝의 공백과 백슬래시(\)	명령이 다음 줄에서 계속됩니다.

참고:

- 굵게 표시된 텍스트는 단순한 강조를 위해 사용되기도 합니다. 예:

  암호를 기록하여 모니터에 붙여두지 **마십시오**.

- 이 가이드에서 명령이 한 줄에 모두 표시되지 않는 경우가 있습니다. 이런 경우에는 줄 끝에 공백과 백슬래시(\)를 표시하여 명령이 다음 줄에서 계속됨을 나타냅니다.

  참고: 실제 명령 구문에는 필요하지 않으므로 백슬래시 문자를 복사하지 마십시오.

- 파이프(|)는 서로 독립적인 항목을 분리합니다. 여러 항목이 있는 중괄호({})는 실제로 입력하지 **않으며** 그 안의 항목 중 하나만 입력합니다. 예를 들어, 다음은 사용자 이름 **또는** 그룹 이름 **중** 하나라는 의미입니다.

  {*username*|*groupname*}

예: 명령 표기 규칙

다음 코드는 이 가이드에서 명령 규칙이 사용되는 방식을 보여 줍니다.

ruler *className* [**props**({**all**|{*propertyName1*[,*propertyName2*]})]

이 예제에서는 다음과 같습니다.

- 표시되는 그대로 입력해야 하는 명령 이름(ruler)은 굵게 표시됩니다.
- *className* 옵션은 클래스 이름(예: USER)의 자리 표시자이므로 기울임꼴로 표시됩니다.
- 대괄호로 묶인 두 번째 부분은 선택 사항이므로 해당 부분 없이 명령을 실행할 수 있습니다.
- 선택적 매개 변수(props) 사용 시 키워드로 *all* 을 선택하거나 하나 이상의 속성 이름을 쉼표로 구분하여 지정할 수 있습니다.

제 2 장: 기본 개념

이 장은 아래의 주제를 포함하고 있습니다:

eTrust AC

eTrust AC는 개방형 시스템을 위한 탁월한 기능의 포괄적인 보안 소프트웨어 솔루션 제품으로 운영 체제에 동적으로 연결됩니다. 사용자가 파일 열기, 사용자 ID 대체, 네트워크 서비스 획득 등과 같이 보안상 중요한 작업을 요청할 때마다 eTrust AC는 실시간으로 이벤트를 인터셉트하고 그 유효성을 평가한 후에 표준 운영 체제(OS) 기능에 대한 제어권을 넘겨줍니다.

Access Control의 정의

eTrust AC는 사용자 기본 플랫폼의 보안을 관리하는 강력한 도구를 제공하여 기업의 보안 요구 사항에 맞춰 전체적으로 사용자 정의할 수 있도록 지원합니다. eTrust AC를 사용하면 기본 운영 체제에서 사용자, 그룹 및 리소스용으로 제공되는 보안 이상의 보안이 제공되어 중앙에서 조직 전체의 Windows 보안을 관리하고 서로 다른 환경의 Windows 및 UNIX 보안 정책을 통합할 수 있습니다.

보호 대상

eTrust AC 에서는 다음과 같은 엔터티를 보호합니다.

- **파일**

  사용자가 특정 파일에 대한 액세스 권한을 부여받았습니까?

  eTrust AC 는 파일에 액세스할 수 있는 사용자의 능력을 제한합니다. 사용자에게 READ, WRITE, EXECUTE, DELETE 및 RENAME 과 같은 하나 이상의 액세스 유형을 지정할 수 있습니다. 개별 파일에 대한 액세스를 지정하거나, 이름이 유사한 파일의 집합에 대한 액세스를 지정할 수 있습니다.

- **터미널**

  사용자에게 특정 터미널을 사용할 권한이 있습니까?

  이 검사는 로그인 프로세스 중에 수행됩니다. 개별 터미널 및 터미널 그룹은 eTrust AC 데이터베이스에서 정의할 수 있으며 터미널이나 터미널 그룹을 사용할 수 있는 사용자 또는 사용자 그룹을 설명하는 액세스 규칙도 함께 정의할 수 있습니다. 터미널 보호를 사용하면 권한 없는 터미널이나 스테이션을 통해 강력한 권한을 가진 사용자 계정에 로그인할 수 없습니다.

- **로그온 시간**

  사용자가 특정 요일의 특정 시간에 로그온할 수 있는 권한을 부여받았습니까?

  대부분의 사용자는 스테이션을 주중과 근무 시간에만 사용합니다. 휴일 제한뿐만 아니라--시간 및--요일 로그인 제한은 해커와 권한 없는 다른 액세서로부터 보호합니다.

- **TCP/IP**

  다른 스테이션이 로컬 컴퓨터에서 TCP/IP 서비스를 받을 수 있는 권한을 부여받았습니까? 다른 스테이션이 로컬 컴퓨터에 TCP/IP 서비스를 제공할 권한이 있습니까? 다른 스테이션이 로컬 스테이션의 모든 사용자로부터 서비스를 수신할 수 있습니까?

  컴퓨터와 네트워크가 모두 개방되어 있는 개방형 시스템의 장점은 단점이 되기도 합니다. 컴퓨터를 외부에 연결하면 누가 시스템에 들어오고 외부 사용자가 고의적으로 또는 실수로 어떠한 피해를 입힐 수 있는지 확신할 수 없습니다. eTrust AC 에는 로컬 스테이션과 서버가 알 수 없는 스테이션에 서비스를 제공하는 것을 방지하는 "방화벽"이 있습니다.

- **다중 로그인 권한**

  사용자가 두 번째 터미널에서 로그인할 수 있습니까?

  *동시 로그인*이라는 용어는 두 개 이상의 터미널에서 시스템에 로그인할 수 있는 사용자의 능력을 의미합니다. eTrust AC 에서는 사용자가 두 번 이상 로그인하지 못하게 할 수 있습니다. 이러한 기능을 통해 침입자는 이미 로그인되어 있는 사용자 계정에 로그인할 수 없습니다.로그인

- **사용자-정의된 항목**

  일반 항목(예: TCP/IP 서비스 및 터미널)과 *추상* 개체라고도 하는 기능 항목(예: 트랜잭션 수행 및 데이터베이스의 레코드 액세스)을 모두 정의하고 보호할 수 있습니다. 추상 개체를 정의하고 보호하기 위해 사용되는 API(Application Programmer's Interface)에 대해서는 *SDK 개발자 가이드*를 참조하십시오.

- **관리자 권한 측면**

  eTrust AC 에서는 관리자 권한을 운영자에게 위임하고 루트 자체를 제한하는 방법을 제공합니다.

  eTrust AC 에서는 관리자 권한을 운영자에게 위임하고 관리자 자체를 제한하는 방법을 제공합니다.

- **레지스트리 키**

  사용자가 특정 레지스트리 키에 액세스할 수 있는 권한이 있습니까?

  eTrust AC 는 레지스트리 키를 액세스할 수 있는 사용자 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.

- **프로그램**

  특정 프로그램을 트러스트할 수 있습니까? 사용자가 이 프로그램을 호출할 권한이 있습니까? 사용자가 프로그램을 사용하여 특정 리소스를 액세스할 수 있습니까?

  보안 관리자는 프로그램을 테스트하여 프로그램에 대한 무단 액세스를 얻는데 사용될 수 있는 보안상 허점이 없는지 확인할 수 있습니다. 테스트를 통과하여 안전한 것으로 간주되는 프로그램은 트러스트된 프로그램으로 정의됩니다. **watchdog** 라고도 하는 eTrust AC 자체 보호 모듈은 특정 시간에 제어되는 프로그램을 인식하고 해당 프로그램이 트러스트된 것으로 분류된 후 수정 또는 이동되었는지 여부를 확인합니다. 트러스트된 프로그램을 수정 또는 이동한 경우에는 더 이상 트러스트된 것으로 간주하지 않고 eTrust AC 에서 해당 프로그램의 실행을 허용하지 않습니다.

또한 eTrust AC 는 의도하거나 의도하지 않은 다음과 같은 위협으로부터 보호합니다.

- **중지 시도**

  eTrust AC 를 사용하면 중지 시도로부터 중요한 서버와 서비스 또는 데몬을 보호할 수 있습니다.

- **암호 공격**

  eTrust AC 는 여러 유형의 암호 공격으로부터 보호하고 사용자 사이트의 암호 정의 정책을-강화하며 침입 시도를-탐지합니다.

- **암호를 이용한 범죄**

  eTrust AC 는 사용자가 최적의 암호를 만들어 사용하도록 하는 규칙을 설정합니다. 사용자가 적합한 암호를 만들어 사용할 수 있도록 eTrust AC 는 암호의 최대 및 최소 수명을 설정하고, 특정 단어를 사용하지 못하게 하며, 문자를 반복해서 사용할 수 없도록 하고, 기타 제한 사항을 적용할 수 있습니다. 암호는 너무 오랫동안 사용할 수 없습니다.

- **계정 관리**

  eTrust AC 정책을 통해 유휴 계정이 적절히 처리되도록 합니다.

보호 방법

운영 체제에서 eTrust AC 서비스 초기화가 완료되면 해당 서비스가 바로 시작됩니다. eTrust AC는 보호가 필요한 시스템 서비스에 후크를 배치합니다. 이런 식으로 서비스가 수행되기 전에 eTrust AC로 제어권이 넘어갑니다. eTrust AC는 해당 사용자에게 서비스를 허용할지 여부를 결정합니다.

예를 들어, 한 사용자가 eTrust AC로 보호되는 리소스에 액세스하려고 시도한다고 가정합니다. 이러한 액세스를 요청하면 리소스를 열기 위해 커널에 대한 시스템 호출이 생성됩니다. eTrust AC는 해당 시스템 호출을 인터셉트하고 액세스 권한을 부여할지 여부를 결정합니다. 사용 권한이 부여되면, eTrust AC는 일반 시스템 서비스로 제어를 전달합니다. 반면 eTrust AC가 사용 권한을 거부하는 경우 시스템 호출을 활성화한 프로그램에 표준 사용 권한 거부 오류 코드를 반환하고 시스템 호출은 종료됩니다.

데이터베이스에 정의된 액세스 규칙 및 정책을 기준으로 결정이 이루어집니다. 보안 관리자는 데이터베이스에 포함된 대부분의 레코드를 정의합니다.

데이터베이스는 두 가지 유형의 개체인 액세서 및 리소스에 대해 설명합니다. *액세서*는 사용자 및 그룹이며, *리소스*는 파일 및 서비스와 같이 보호되는 개체입니다. 데이터베이스의 각 레코드는 액세서 또는 리소스에 대해 설명합니다.

각 개체는 동일한 유형의 개체 모음인 클래스에 속합니다. 예를 들어, TERMINAL은 eTrust AC에서 보호하는 터미널(워크스테이션) 개체를 포함하는 클래스입니다.

클래스 활성화

CLASS 상태에 대한 정보(클래스가 활성인지 비활성인지 여부)는 데이터베이스에 저장됩니다. 리소스를 액세스하려는 모든 시도는 eTrust AC에 의해 인터셉트되고 데이터베이스에서 상태를 확인합니다. 클래스가 비활성일 경우, 더 이상 권한 부여를 확인하지 않고 액세스가 허용됩니다.

eTrust AC는 엔진이 시작되고 사용자가 CLASS 활성 상태를 변경할 때 활성 클래스 목록을 작성합니다. 클래스가 비활성 상태이면 리소스에 대한 액세스가 인터셉트되지 않아 오버헤드가 감소됩니다.

액세서 요소

각 사용자는 데이터베이스의 사용자 레코드가 내부 메모리에 반영된 *액세서 요소*(ACEE)로 나타납니다. eTrust AC 는 로그인 프로세스 중에 액세서 요소를 작성합니다. 액세서 요소는 사용자 프로세스와 연결되어 있습니다. 프로세스가 eTrust AC 에서 보호되는 시스템 서비스나 암시적으로 리소스 액세스를 요청하는 시스템 서비스를 요청할 때마다 eTrust AC 에서 해당 리소스 레코드를 액세스합니다. 그런 다음 사용자의 보안 수준, 모드 및 그룹과 같이 이미 작성된 액세서 요소의 정보로 사용자가 리소스에 액세스할 수 있는지 여부를 결정합니다.

구성요소

eTrust AC 에는 데이터베이스(seosdb), 두 개의 드라이버(seosdrv, drveng), 여러 서비스(Watchdog, 에이전트, 엔진(seosd), 정책 모델 및 작업 위임 포함) 및 그래픽 사용자 인터페이스가 포함됩니다.

데이터베이스

데이터베이스에는 다음과 같은 요소에 대한 정의가 있습니다.

- 조직의 사용자 및 그룹
- 보호가 필요한 시스템 리소스
- 시스템 리소스에 대한 사용자 및 그룹 액세스를 제어하는 규칙

드라이버

드라이버는 다음 작업을 수행하여 모든 eTrust AC 파일과 레지스트리 키를 보호합니다.

- 파일 또는 레지스트리 키 열기, 프로세스 종료 및 네트워크 활동 수행의 모든 요청 인터셉트
- 이러한 요청을 eTrust AC 엔진에 전달하고 해당 요청을 허용 또는 거부할지 여부에 대한 엔진의 결정 수신
- 결정을 운영 체제의 기존 시스템 호출로 전달하고, 드라이버로부터 수신한 답변에 따라 처리 작업을 계속 수행

서비스

Watchdog

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

에이전트

또한 에이전트는 다음과 같은 작업을 수행합니다.

- TCP/IP 의 소유 응용 프로그램 프로토콜을 통해 eTrust AC 클라이언트와 통신
- eTrust AC 사용자에 대한 보안 관리

엔진

엔진은 다음 작업을 담당합니다.

- 모든 데이터베이스 업데이트 제어를 포함한 데이터베이스 관리
- 드라이버와 에이전트로부터 받은 액세스 요청의 허가 여부 결정
- Watchdog 서비스가 실행 중인지 확인하고, Watchdog 의 실행이 중단된 것으로 인식되면 Watchdog 재시작

엔진은 데이터베이스 액세스 요청을 **처리하고** 액세스를 결정하여 효율적인 서비스를 작성합니다.

정책 모델

수십 또는 수백 개의 데이터베이스를 개별적으로 관리하는 것은 실용적이지 않습니다. 따라서, eTrust AC 는 한 대의 컴퓨터에서 여러 대의 컴퓨터를 관리할 수 있도록 해주는 구성 요소인 정책 모델 서비스를 제공합니다. 정책 모델 서비스를 사용하는 것은 선택사항이지만 큰 사이트에서 이 서비스를 사용하면 관리 작업이 상당히 간단해집니다.

정책 모델 서비스와 함께 정책 모델 데이터베이스(PMDB)를 사용합니다. 다른 eTrust AC 데이터베이스와 달리 PMDB 에는 사용자, 그룹, 보호된 리소스, 리소스에 대한 액세스를 제어하는 규칙 등이 포함됩니다. 또한 PMDB 에는 구독자 스테이션 목록도 포함됩니다. 구독자 스테이션은 PMDB 에 대한 모든 변경 내용이 구독자 데이터베이스로 자동으로 보내질 수 있도록 PMDB 에 연결된 스테이션입니다.

조직에 대한 기본 보안 정책을 만들고 필요한 모든 규칙을 하나의 정책 모델 데이터베이스에 구현할 수 있습니다. 구독자는 Windows 및 UNIX 스테이션 등을 포함하여 최소한의 관리 노력으로 통일된 규칙을 유지할 수 있습니다.

시스템 또는 보안 관리자가 PMDB 를 업데이트합니다. 그러면 PMDB 는 PMDB 의 모든 업데이트를 해당구독자에게 배치 모드로 전파하여 관리자가 다른 작업을 수행할 수 있도록 합니다.

PMDB 에는 두 가지 유형의 구독자 (다른 PMDB 와 로컬 데이터베이스)가 있을 수 있습니다. 이 PMDB 에는 데이터베이스 업데이트를 전파할 구독자 목록도 포함됩니다. 이 기능을 사용하면 PMDB 계층을 작성할 수 있습니다. 로컬 데이터베이스는 스테이션에 정의된 사용자, 그룹 및 리소스를 보호하는 데 사용할 수 있습니다.

그래픽 사용자 인터페이스

정책 관리자 (페이지 37) 모든 eTrust AC 기능을 수행하는 GUI(그래픽 사용자 인터페이스)입니다.

특징

eTrust AC 를 사용하면 중앙의 한 위치에서 기본 Windows 를 관리할 수 있으며 기본 Windows 보안이 상당히 향상됩니다. eTrust AC 는 또한 자체 보안도 제공합니다. 다음 절에서 이 기능을 설명합니다.

Windows 관리

eTrust AC 를 조직의 Windows 스테이션에 설치했으면, 속해 있는 도메인에 상관없이 하나의 중앙 스테이션에서 모든 스테이션을 관리할 수 있습니다. 정책 관리자 인터페이스나 selang 이라는 명령줄 언어를 사용하여 이 작업을 수행할 수 있습니다.

자체 방어 제공

실제로 해커나 사용자가 eTrust AC 서비스를 고의적으로 또는 실수로 중단시킬 수 없으며, eTrust AC 가 실행 중이면 권한 없는 사용자가 eTrust AC 파일과 데이터를 변경하거나 지우는 것도 실제로 불가능합니다.

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

Active Directory

Active Directory는 Windows 2000부터 Windows 운영 체제에서 사용되는 디렉터리 서비스로, 네트워크에 있는 사용자, 컴퓨터 및 서비스와 같은 개체 정보를 저장할 수 있는 계층식 저장소를 제공합니다.

Active Directory가 Windows 운영 체제에 설치되어 있으면, 기본 Windows 환경에서 사용자와 그룹을 관리할 수 있는 것처럼 eTrust AC를 사용하여 사용자 및 그룹과 확장된 사용자 및 그룹의 속성을 추가하고 수정할 수 있습니다.

Active Directory가 Windows 서버에 설치되어 있으면, OU 클래스를 사용하여 지정된 조직 단위 내에서 사용자, 그룹 및 컴퓨터를 작성할 수 있습니다.

파일 보호

Windows에서는 서로 다른 유형의 여러 파일 시스템을 사용할 수 있습니다. 가장 많이 사용되는 파일 시스템은 FAT과 NTFS입니다. NTFS 파일 시스템을 사용하는 경우, Windows는 각 파일의 ACL을 작성하고 업데이트하여 시스템에 있는 파일을 보호합니다. eTrust AC는 파일 ACL을 지원합니다.

암호 보호

기본 Windows 보안은 여러 가지 방법으로 암호를 보호하고 암호 등급을 제한할 수 있습니다. Windows는 다음과 같은 기능을 제공합니다.

- 암호의 최대 사용 기간 제한
- 암호의 최소 길이 제한
- 최대 24개의 사용자 암호 생성
- 반복되는 로그인 실패 시 계정 잠금
- 암호를 변경하기 전에 Windows에 사용자를 강제로 로그온

eTrust AC도 동일한 규칙을 적용하지만 자체의 고유 메커니즘을 사용합니다. 또한 eTrust AC는 메인프레임 컴퓨터와-양방향으로 암호를 동기화합니다.

기본 Windows 보안 확장

다음과 같은 eTrust AC 기능은 기본 Windows 보안을 확장합니다.

관리자 계정 제한

Windows 를 관리하는 사용자는 일반적으로 시스템 설치 중 자동으로 작성되는 미리 정의된 그룹의 구성원입니다. 미리 정의된 그룹은 일련의 특정 시스템 기능을 실행하기 위해 존재합니다. 그룹 구성원인 사용자는 그룹의 모든 함수를 실행할 수 있는 권한을 가집니다

Windows 에서 가장 강력한 그룹은 Administrators 그룹이며, 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 사용자 권한을 제한할 수 있습니다. 이 기능을 통해 Windows 시스템의 취약성을 보완할 수 있습니다.

일반 사용자에게 관리자 권한 부여

eTrust AC 는 일반 사용자(관리자가 아닌 사용자)에게 필요한 권한을 부여하여 해당 사용자가 관리자 그룹의 구성원이 아니더라도 관리 작업을 수행할 수 있습니다. *작업 위임*이라고 불리는 이 기능은 정확한 방식으로 관리자 권한을 위임하는 작업으로 eTrust AC 의 가장 중요한 장점 중 하나입니다.

- SUDO 클래스의 레코드에는 사용자가 빌린 권한으로 스크립트를 실행할 수 있는 명령 스크립트가 저장되어 있습니다.
- 데이터 속성 값이 명령 스크립트입니다. 값에 선택적인 스크립트 매개 변수 값을 추가함으로써 값을 수정할 수 있습니다.
- SUDO 클래스의 각 레코드는 다른 사용자로부터 사용 권한을 빌려 올 수 있는 명령을 식별합니다.
- SUDO 클래스 레코드의 키는 SUDO 레코드 이름입니다. 이 이름은 사용자가 SUDO 레코드에서 명령을 실행할 때 명령 이름 대신 사용됩니다.

SUDO 레코드 정의

SUDO 클래스의 레코드에는 사용자가 빌린 권한으로 스크립트를 실행할 수 있는 명령 스크립트가 저장되어 있습니다. 권한을 빌려올 수 있는 자격은 스크립트를 실행하는 sesudo 명령과 SUDO 레코드가 엄격하게 제어합니다.

참고: 터미널 서비스를 설치한 컴퓨터에서 SYSTEM 계정이 아닌 다른 사용자 계정으로 SeOS Task Delegation 서비스가 실행되는 경우에는 sesudo 명령에서 대화형 프로세스를 실행할 수 없습니다.

SUDO 레코드에서 comment 속성은 특수 목적으로 사용되며 이 속성은 종종 다른 이름인 data 속성으로 알려집니다.

comment 속성 값은 명령 스크립트이며 금지하거나 허용할 스크립트 매개 변수 값을 하나 이상 이 속성 값에 선택적으로 추가할 수 있습니다. 트로이 목마 바이러스가 침입하는 것을 방지하려면 전체 comment 속성 값을 작은따옴표로 묶어야 하고 실행 파일을 전체 경로 이름으로 참조해야 합니다.

comment 속성의 형식은 다음과 같습니다.

```
comment('cmd[;[prohibited-values][;permitted-values]]')
```

금지된 값과 허용된 값의 목록은 선택 사항이므로 간단한 comment 속성 값은 다음과 같을 수 있습니다.

```
newres SUDO NET comment('net use')
```

이 간단한 명령은 sesudo NET 명령에서 'net use' 명령을 실행한다는 것을 나타냅니다. 금지되는 특정 스크립트 매개 변수 값은 없으며, 모두 허용됩니다.

와일드카드와 적합한 변수를 사용하면 금지된 매개변수와 허용된 매개변수를 다양하게 지정할 수 있습니다. 사용할 수 있는 와일드카드는 표준 Windows 와일드카드입니다. 금지된 매개 변수와 허용된 매개 변수는 다음 변수를 포함할 수 있습니다.

변수	설명
$A	영문자 값
$G	기존 eTrust AC 그룹 이름
$H	사용자의 홈 디렉터리로 시작되는 매개 변수.
$N	숫자 값
$O	sesudo 를 실행하는 사용자의 eTrust AC 이름
$U	기존 eTrust AC 사용자 이름

변수	설명
$e	비어 있는 항목. 규칙에 대한 매개 변수가 없는 SUDO 명령을 지정할 때 사용합니다
$f	기존 파일 이름
$g	기존 Windows 그룹 이름
$h	기존 호스트 이름
$r	Windows 읽기 권한이 있는 기존 파일
$u	기존 Windows 사용자 이름
$w	Windows 쓰기 권한이 있는 기존 파일
$x	Windows 실행 권한이 있는 기존 파일

prohibited 매개 변수 값 목록을 스크립트에 추가할 경우에는 다음을 수행합니다.

- 금지된 매개변수 값과 스크립트를 세미콜론으로 구분하지만, 앞뒤에 작은 따옴표를 입력해야 합니다. 예를 들어, 사용자가 -start 매개 변수를 제외한 다른 모든 매개 변수를 사용할 수 있도록 지정하려면 다음 명령을 입력하십시오.

  ```
  newres SUDO scriptname comment('cmd;-start')
  ```

  여기서 *cmd* 는 스크립트를 나타냅니다.

  또한 매개 변수 값을 허용하지 않으면서 모든 매개 변수를 기본값으로 사용하려면 다음과 같이 SUDO 레코드를 정의하십시오.

  ```
  newres SUDO scriptname comment('cmd;*')
  ```

- script 매개 변수에 둘 이상의 금지된 값이 있는 경우, 공백을 구분자로 사용하십시오. 예를 들어, 사용자가 -start 및 -stop 매개 변수를 제외한 다른 모든 매개 변수를 사용할 수 있도록 지정하려면 다음 명령을 입력하십시오.

  ```
  newres SUDO scriptname comment('cmd;-start -stop')
  ```

- 둘 이상의 script 매개 변수에 금지된 값이 있는 경우, 파이프 문자(|)를 금지된 값 집합 사이의 구분자로 사용하십시오. 예를 들어, 사용자가 스크립트의 첫 번째 매개 변수로 -start 및 -stop 을 사용하지 못하도록 하고 두 번째 매개 변수로 기존 Windows 사용자 이름을 사용하지 못하도록 하려면(앞의 변수 목록 참조) 다음 명령을 입력합니다.

  ```
  newres SUDO scriptname comment('cmd;-start -stop | $u')
  ```

  스크립트에 나열한 매개 변수보다 많은 수의 매개 변수가 있는 경우 금지된 매개 변수의 마지막 집합은 나머지 모든 매개 변수에 적용됩니다.

permitted 매개 변수 값 목록을 스크립트에 추가할 경우에는 다음을 수행합니다.

- sesudo 유틸리티에서는 두 가지 검사를 실행합니다.
  - 해당하는 *금지된* 값과 일치해서는 *안* 되며
  - 해당하는 하나 이상의 *허용된* 값과 일치해야 합니다.

  따라서 매개 변수 값이 금지된 목록에 있으면 허용된 목록에 지정되어 있더라도 허용되지 않습니다.

- *허용된* 값의 목록과 *금지된* 값의 목록을 세미콜론으로 구분하지만, 전체를 작은 따옴표로 묶어야 합니다. 금지된 값의 목록이 없는 경우에도 세미콜론은 필요합니다. 세미콜론이 없으면 허용하려고 했던 값이 금지될 수 있습니다. 예를 들어, 스크립트에 대한 매개 변수 값으로 NAME 값만 허용하려면 다음 명령을 입력하십시오.

  ```
  newres SUDO scriptname comment('cmd;;NAME')
  ```

- 다른 목록에서도 다음 작업을 수행합니다.
  - script 매개 변수에 둘 이상의 허용된 값이 있는 경우, 공백을 구분자로 사용하십시오.
  - 둘 이상의 script 매개 변수에 허용된 값이 있는 경우, 파이프 문자(|)를 허용된 값 집합 사이의 구분자로 사용하십시오.

예를 들어, 두 개의 매개 변수가 있을 때 첫 번째 매개 변수는 숫자여야 하지만 Windows 사용자 이름을 사용할 수 없으며 두 번째 매개 변수는 영문자여야 하지만 Windows 그룹 이름을 사용할 수 없는, 다음 명령을 입력합니다.

```
newres SUDO scriptname comment('cmd;$u | $g ;$N | $A')
```

스크립트에 나열한 매개 변수보다 많은 수의 매개 변수가 있는 경우 허용된 매개 변수의 마지막 집합은 나머지 모든 매개 변수에 적용됩니다.

따라서 comment 속성의 전체적인 형식은 먼저 스크립트가 나오고 금지된 값, 매개 변수별 매개 변수, 그리고 허용된 값, 매개 변수별 매개 변수입니다.

```
comment('cmd; \
param1_prohib1 param1_prohib2 ... param1_ prohibN | \
param2_prohib1 param2_prohib2 ... param2_ prohibN | \
 ...
paramN_prohib1 paramN_prohib2 ... paramN_prohibN ; \
param1_permit1 param1_permit2 ... param1_ permitN | \
param2_permit1 param2_permit2 ... param2_ permitN |
 ...
paramN_permit1 paramN_permit2 ... paramN_permitN')
```

Sesudo 유틸리티는 사용자가 입력한 각 매개 변수를 다음과 같은 방식으로 검사합니다.

1. 매개 변수 N 이 허용된 매개 변수 N 과 일치하는지 테스트합니다. (허용된 매개 변수 N 이 없으면 마지막으로 허용된 매개 변수가 사용됩니다.)
2. 매개 변수 N 이 금지된 매개 변수 N 과 일치하는지 테스트합니다. (금지된 매개 변수 N 이 없으면 마지막으로 금지된 매개 변수가 사용됩니다.)

모든 매개 변수가 허용된 매개 변수와 일치하며 금지된 매개 변수와 일치하는 매개 변수가 없을 경우에만 sesudo 는 명령을 실행합니다.

작업 위임 예제

예제 1

1. [액세스 제어] 프로그램 표시줄에서 [리소스] 아이콘  을 선택합니다.

   [리소스] 창이 표시됩니다.

2. 작업 위임 리소스 트리를 확장하고 [작업]을 마우스 오른쪽 단추로 클릭한 다음 [새로 만들기]를 선택합니다.

   새로운 정책을 작성할 수 있는 [새 SUDO 리소스 작성 - 일반] 대화 상자가 표시됩니다.

3. [이름] 필드에 SUDO 레코드의 이름 *NET*을 입력합니다.

   [데이터] 필드에 다음 값을 입력합니다.

   ```
   net;start;send
   ```

   데이터 속성의 형식은 다음과 같습니다.

   ```
   command; prohibited-values; permitted-values
   ```

   예를 들어, *net send* 실행을 허용하고 사용자 *any_user*에 대해 *net start* 실행을 금지하려면 [데이터] 필드에 다음 명령을 입력하고 any_user에게 이 SUDO 레코드에 대한 권한을 부여합니다.

   ```
   net;start;send computer_name message
   ```

4. [소유자] 필드에서 [찾아보기]를 클릭하고 [사용자] 탭에서 *nobody*를 선택한 다음 [확인]을 클릭합니다.

5. [기본 액세스 설정]을 클릭하고 [없음]을 선택한 후 [확인]을 클릭합니다.

6. 대화 상자의 왼쪽 패널에서 [권한 부여] 아이콘을 선택합니다.

   대화 상자의 [권한 부여] 페이지가 나타납니다.

7. [삽입]  을 클릭하여 액세서를 추가한 다음 [이름] 필드 옆의 [찾아보기]를 클릭합니다.

8. 사용자 또는 그룹을 선택하여 사용 권한을 위임하고 [확인]을 클릭합니다.

   [eTrust 액세서 추가/편집] 대화 상자가 나타납니다.

9. [확인]을 클릭합니다.

10. [사용 권한 실행]을 선택하고 [확인]을 클릭합니다.

    새 SUDO 리소스가 작성됩니다.

11. SUDO 레코드를 테스트합니다.
    a. SUDO 레코드가 적용된 사용자로 로그인합니다.
    b. 명령 프롬프트를 열고 다음 명령을 실행합니다.

       ```
       sesudo -do NET start
       ```

       다음과 같은 메시지가 나타납니다.

       ```
       sesudo: 'start'을(를) 매개 변수 번호 1(으)로 사용할 수 없습니다.
       ```

       참고: *net start* 는 금지된 값으로 정의되었기 때문에 실행되지 않습니다.
    c. 다음 값을 실행합니다.

       ```
       sesudo -do NET send
       ```

       명령이 실행됩니다.

예제 2

사용자는 다음 예제와 같이 스냅인 MSC 모듈을 사용하여 높은 수준의 권한이 필요한 작업을 수행할 수 있습니다.

1. [리소스] 창에서 작업 위임 리소스 트리를 확장하고 [작업]을 마우스 오른쪽 단추로 클릭한 다음 [새로 만들기]를 선택합니다.

   새로운 정책을 작성할 수 있는 [새 SUDO 리소스 작성 - 일반] 대화 상자가 표시됩니다.
2. [이름] 필드에 *services* 를 입력합니다.
3. [데이터] 필드에 *c:\winnt\system32\mmc.exe* 를 입력합니다.
4. [소유자] 필드에서 *없음*을 선택합니다.
5. *대화형* 확인란을 선택합니다.

   대화형 기능은 서비스가 시작되었을 때 로그인한 사용자가 사용할 수 있는 데스크톱 사용자 인터페이스를 제공합니다. 이 기능은 서비스가 LocalSystem 계정으로 실행 중인 경우에만 사용할 수 있습니다.
6. [기본 액세스 설정]을 클릭하고 [없음]을 선택한 후 [확인]을 클릭합니다.
7. 대화 상자의 왼쪽 패널에서 [권한 부여] 아이콘을 선택합니다.

   대화 상자의 [권한 부여] 페이지가 나타납니다.
8. [삽입]  을 클릭하여 액세서를 추가한 다음 [이름] 필드 옆의 [찾아보기]를 클릭합니다.
9. 사용자 또는 그룹을 선택하여 사용 권한을 위임하고 [확인]을 클릭합니다.
10. [사용 권한 실행]을 선택하고 [확인]을 클릭합니다.

    새 SUDO 리소스가 작성됩니다.
11. SUDO 리소스를 테스트합니다.
    a. SUDO 리소스가 적용된 사용자로 로그인합니다.

b. 명령 프롬프트를 열고 다음 명령을 실행합니다.

```
sesudo -do services
```

c. mmc.exe 가 시작됩니다.

12. SUDO 리소스 실행을 거부하려면, SUDO 권한 부여 속성을 편집하고 거부 열의 확인란을 선택합니다.

13. 명령 프롬프트를 열고 다음 명령을 입력합니다.

```
sesudo -do services
```

다음과 같은 메시지가 나타납니다.

```
sesudo: services 명령을 사용할 수 있는 권한이 없습니다.
```

참고: *services* 는 이 예제를 위해 만든 SUDO 리소스의 이름입니다. SUDO 리소스는 services 스크립트의 실행을 금지해야 합니다.

향상된 파일 보호

eTrust AC 는 논리적 파일 이름 형식과 절대 파일 이름 형식을 모두 지원합니다. 예를 들어, foo.txt 파일이 논리적 드라이브 D 의 \tmp 디렉터리에 있고 논리적 이름 "D:" "가 물리적 디스크 1, 파티션 0 에 할당되어 있는 경우, 논리적 파일 이름이나 절대 파일 이름을 사용하여 파일을 eTrust AC 데이터베이스에 정의할 수 있습니다.

```
nr file D:\tmp\foo.txt
```

또는

```
nr file \Device\HardDisk1\Partition1\tmp\foo.txt
```

참고: 두 번째 형식을 사용할 경우 파일은 디스크의 논리적 이름이 변경되더라도 계속 보호됩니다. 절대 파일 이름 형식은 eTrust AC 일반 파일 보호에서도 지원됩니다.

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

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

일반 파일 보호

eTrust AC는 논리적 파일 이름 형식과 절대 파일 이름 형식을 모두 지원합니다. 절대 파일 이름 형식은 eTrust AC 일반 파일 보호에서도 지원됩니다.

일반 파일 보호 기능을 통해 지정된 와일드카드 패턴(정규 표현식)과 일치하는 모든 파일을 보호할 수 있습니다. 지정한 와일드카드 패턴과 일치하는 이름을 가진 모든 리소스는 지정한 일반 액세스 규칙에 의해 보호됩니다. eTrust AC를 사용하면 파일을 전체적으로 보호할 수 있습니다.

리소스가 둘 이상의 일반 액세스 규칙과 일치할 경우, eTrust AC는 파일과 가장 근접하게 일치하는 규칙을 선택합니다.

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

향상된 암호 보호

기본 Windows 보안은 사용자 암호에 대해 상당한 보호 기능을 제공합니다. (페이지 18). 그러나 eTrust AC는 암호 보호 기능을 현저히 확장하여 해커가 암호를 알아내는 데 성공할 확률을 크게 줄여줍니다.

eTrust AC를 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.

프로그램 경로 지정(Program Pathing)

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

B1 보안 수준 인증

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

- 데이터베이스의 액세서와 리소스에 *보안 수준*을 할당할 수 있습니다. 보안 수준은 1과 255 사이의 정수입니다. 접근자는 리소스에 할당된 보안 수준보다 크거나 같은 보안 수준을 가질 경우에만 리소스에 접근할 수 있습니다.
- 데이터베이스의 액세서와 리소스는 하나 이상의 *보안 범주*에 속할 수 있습니다. 액세서는 리소스에 할당된 모든 보안 범주에 속해 있을 경우에만 리소스를 액세스할 수 있습니다.

- *보안 레이블*은 특정 보안 수준을 0 개 이상의 보안 범주 집합에 연결하는 이름입니다. 사용자에게 보안 레이블을 할당하면 보안 수준과 보안 레이블에 관련된 보안 범주가 사용자에게 모두 부여됩니다.

참고: B1 Orange Book 기능에 대한 자세한 내용은 *구현 가이드*를 참조하십시오.

eTrust AC 실행

eTrust AC 는 정책 관리자 인터페이스나 selang 이라는 명령줄 언어를 사용하여 관리할 수 있습니다. 이러한 도구를 사용하여 로컬 워크스테이션과 eTrust AC 가 설치되어 있는 다른 모든 Windows 워크스테이션을 관리할 수 있습니다.

정책 관리자

정책 관리자는 eTrust AC 의 관리 도구입니다.

selang

명령줄 언어인 selang 은 eTrust AC 의 모든 함수를 실행합니다. selang 명령을 사용하려면, 명령 프롬프트 창을 열고 selang 을 시작하십시오. selang 은 스크립트에서도 사용할 수 있습니다.

selang 및 해당 명령에 대한 자세한 내용은 *참조 가이드*의 "selang 명령 언어" 장을 참조하십시오.

Windows 및 UNIX 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 모두 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 워크스테이션으로 변경 내용을 전파하는 기능을 사용하면 관리 오버헤드를 상당히 줄일 수 있습니다.

공통 보안 정책에서 특히 중요한 몇 가지 요소를 다음 절에서 설명합니다.

하나의 사용자 집합 유지관리

사이트에 eTrust AC를 설치했으면 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. UNIX, Windows 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 작업 부하가 줄어들 수 있습니다.

eTrust AC를 사용하면 UNIX 및 Windows 환경에서 모두 사용할 수 있는 하나의 그룹 집합을 만들고 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. PMDB를 통해 보안 데이터베이스와 그에 대한 모든 변경 내용을 모든 해당 구독자에게 전파할 수 있습니다. Windows 및 UNIX 워크스테이션은 동일한 PMDB에 가입할 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. 이 디자인은 네트워크 트래픽을 최소화하며 구독자의 무결성을 보장합니다.

관리자 설정

eTrust AC 를 설치할 때 하나 이상의 eTrust AC 관리자 이름을 지정하라는 요청을 받았습니다. eTrust AC 관리자는 규칙 데이터베이스를 일부 수정하거나 전부 수정할 수 있는 권한을 가지고 있습니다. 모든 권한을 가진 관리자가 적어도 한 명 있어야 합니다. 관리자는 원하는 대로 액세스 규칙을 수정하거나 작성할 수 있으며, 다른 수준의 관리자를 지정할 수 있습니다.

시스템 사용자를 정의했으면, 다른 사용자에게 ADMIN 속성을 할당함으로써 관리 권한을 할당할 수 있습니다.

참고: ADMIN 속성을 가진 사용자는 강력한 권한을 보유합니다. 따라서 ADMIN 사용자의 수는 엄격히 제한되어야 합니다. eTrust AC 보안 관리자를 한 명 이상 설정한 후 관리자로부터 ADMIN 속성을 제거하여 Windows 관리자와 ADMIN 의 역할을 구분하는 것도 바람직합니다.

데이터베이스를 관리할 수 있는 권한을 가진 사용자가 항상 한 명 이상 필요하므로, eTrust AC 에서 ADMIN 속성을 가진 마지막 사용자는 삭제할 수 없습니다. 관리자에서 ADMIN 속성을 제거하려면, 먼저 다른 사용자에게 ADMIN 속성을 부여해야 합니다.

eTrust AC 관리자 중 한 명 이상이 워크스테이션에서 다른 호스트를 관리할 것으로 예상할 경우, 해당 호스트의 데이터베이스에 있는 규칙이 워크스테이션에서 READ 및 WRITE 액세스를 해당 관리자에게 부여하는지 확인하십시오.

일거양득: 하위 관리자 작성

eTrust AC 에는 관리자가 일반 사용자에게 특정 클래스를 관리할 수 있는 권한을 부여하는 하위 관리 기능이 있습니다. 이러한 사용자를 하위 관리자라고 합니다.

예를 들어, 특정 사용자에게 사용자와 그룹만 관리하도록 허용할 수 있습니다.

또한 특정 클래스에 대한 액세스를 허용하면서 해당 클래스에 속한 특정 *개체*에 대한 액세스도 허용함으로써 더 높은 수준의 하위 관리를 지정할 수 있습니다.

감사 절차 설정

eTrust AC는 데이터베이스에 정의된 감사 규칙에 따라 액세스 거부 및 허용 이벤트에 대한 감사 레코드를 유지합니다. 특정 이벤트의 기록 여부는 다음 규칙에 따라 결정됩니다.

- 모든 액세서와 리소스에는 액세스 성공, 실패 또는 모두 로그 파일에 기록해야 하는지 여부를 나타내도록 설정할 수 있는 AUDIT 속성이 있습니다. 또한 액세서의 AUDIT 속성은 로그인 성공, 실패 또는 모두 로그 파일에 기록해야 하는지 여부를 나타낼 수 있습니다.
- 리소스 또는 액세서에 AUDIT(ALL) 속성이 있는 경우 eTrust AC에서 보호되는 리소스에 대한 모든 이벤트가 액세스 성공 여부에 상관 없이 로그 파일에 기록됩니다.
- eTrust AC에서 보호되는 리소스에 대한 액세스가 성공하고 사용자 또는 리소스에 AUDIT(SUCCESS)가 있는 경우 이벤트가 로그 파일에 기록됩니다.
- eTrust AC에서 보호되는 리소스에 대한 액세스가 실패하고 사용자 또는 리소스에 AUDIT(FAIL)가 있는 경우 이벤트가 로그 파일에 기록됩니다.

AUDITOR 속성이 할당된 사용자인 시스템 감사자만 사용자 및 리소스에 할당된 감사 속성의 변경과 같은 감사 작업을 수행할 수 있습니다.

특정 리소스가 경고 모드로 설정된 경우, 해당 리소스에 대한 액세스 규칙을 위반하면 경고 모드가 설정되므로 위반이 허용되었음을 알리는 감사 레코드가 결과적으로 작성됩니다.

감사 레코드는 *감사 로그*(seos.audit)라는 파일을 구성합니다. 감사 로그의 위치는 오류 로그의 위치와 마찬가지로 레지스트리에서 지정됩니다.

감사 로그(및 오류 로그)는 다음 레지스트리 키에서 지정됩니다.

```
HKEY_LOCAL_MACHINE\Software\ComputerAssociates\eTrustAccessControl\logmgr
```

감사 로그는 바이너리 파일로, 편집하거나 변경할 수 없습니다. 그러나 정책 관리자를 사용하여 기록된 이벤트를 보고, 시간 제한 또는 이벤트 유형 등을 기준으로 이벤트를 필터링할 수 있습니다. (seaudit 유틸리티를 사용하여 동일한 작업을 수행할 수도 있습니다.)

이벤트를 나중에 검사할 수 있도록 오래된 감사 로그와 오류 로그를 보관(백업)하는 방법을 고려하십시오.

Unicenter TNG 로 감사 이벤트 전송

Unicenter TNG 와의 통합은 설치할 때 설정됩니다.

감사 데이터를 Unicenter TNG 로 전송하거나, Unicenter TNG 에서 eTrust AC 를 시작할 수 있게 하거나, 또는 두 가지를 모두 선택할 수 있습니다. 두 가지 옵션은 상호 연관성이 없습니다.

첫번째 옵션을 선택하면 하위 키 아래에서 레지스트리 값이 다음과 같이 설정됩니다.

```
HKEY_LOCAL_MACHINE\Software\ComputerAssociates\eTrustAccessControl\UCTNG
```

통합 값은 1(예)로 설정되고 EvtManagerServer 값은 Unicenter TNG 호스트 이름을 문자열 값으로 받아들입니다.

Unicenter TNG 에 전달된 감사 이벤트는 Unicenter Enterprise Management\Enterprise Managers\Windows NT\Event 창에 있는 콘솔 로그에 표시됩니다.

감사 이벤트	표시 색상	심각도
성공	파란색	S
거부됨	주황색	F
Fail	주황색	F
경고	파란색	W
eTrust AC 가 중지됨(감사 종료)	파란색	I
eTrust AC 가 시작됨(감사 시작)	파란색	I

두 번째 옵션을 사용하면 Managed Objects 창에 있는 TCP/IP 네트워크를 나타내는 아이콘를 가리키고 마우스 오른쪽 버튼을 클릭하면 나타나는 메뉴에서 eTrust AC 를 선택하여 Unicenter WorldView 메뉴에서 eTrust AC 를 시작할 수 있습니다.

eTrust AC 에서는 이벤트에 대한 다음 정보도 보냅니다.

- 제품 이름(eTrust Access Control + 버전 번호)
- 사용자 이름
- 터미널 이름
- 클래스 이름
- 리소스 이름
- 프로세스 이름
- 이벤트 시간
- eTrust AC 감사 형식의 전체 감사 메시지

이벤트 유형에 따라서는 사용자 이름, 터미널 이름, 클래스 이름, 리소스 이름 및 프로세스 이름 필드를 보내지 않을 수도 있습니다.

정책 모델 데이터베이스 사용

많은 컴퓨터와 워크스테이션이 있는 대규모 사이트에서 수십 또는 수백 개의 eTrust AC 데이터베이스를 개별적으로 관리하는 것은 실용적이지 않습니다. 보안 규칙이 기업 내 대부분의 컴퓨터에 대해 동일한 경우, 관리자는 보안 규칙을 한 번 적용하고 동일한 규칙이 적합하게 전파되는 방법을 필요로 합니다. eTrust AC 에서는 *정책 모델 데이터베이스*(PMDB)가 이런 기능을 제공합니다.

PMDB 에는 로컬 데이터베이스(eTrust AC 또는 기본 운영 체제)에 있는 정보와 동일한 종류의 정보뿐 아니라 로컬 데이터베이스나 다른 호스트에 있는 다른 PMDB 일 수 있는 구독 데이터베이스 목록이 포함되어 있습니다. PMDB 는 본질적으로 마스터 규칙 데이터베이스 또는 템플릿입니다. PMDB 에서 정의되는 규칙 및 규칙 변경사항은 구독 데이터베이스에 적용됩니다.

PMDB 기능은 여러 시스템에 액세스 규칙을 배포하고 호스트 그룹에 대해 동일한 액세스 규칙을 작성하기 위한 간단한 계층 모델을 제공합니다. PMDB 를 계층으로 구성하면 최상위 템플릿(기업 내의 모든 호스트에 적용되는 액세스 규칙)에서-호스트의 하위 그룹에 적용할 수 있는 특정 규칙을 정의하는 하위 템플릿에 이르는 여러 수준의 정책을 지원할 수 있습니다.

PMDB 에는 여러 구독자가 있을 수 있지만, PMDB 또는 로컬 데이터베이스는 전파된 규칙 변경사항을 수신하기 위해서만 하나의 상위 PMDB 에 구독할 수 있습니다. 또한 각 PMDB 는 암호 변경사항을 전파하기 위해 동일한 상위 PMDB 를 가지거나 암호 PMDB 라는 다른 PMDB 를 가질 수 있습니다. 암호 변경 사항은 규칙 변경 사항과 달리 양방향으로 모두 전파됩니다. 다시 말하면, 암호 변경 사항은 변경 사항이 처음 적용된 호스트의 로컬 데이터베이스에서 암호 정책 모델의 맨 위로 전파된 후 계층의 모든 구독자로 다시 전파됩니다.

암호화 설정

네트워크에 eTrust AC 를 실행하는 서버가 두 대 이상이면, 서로 다른 서버에 있는 eTrust AC 서비스 간의 통신은 암호화됩니다. 기본적으로 eTrust AC 는 암호화를 위해 빠르고 효율적인 스크램블링 알고리즘을 사용합니다.

eTrust AC 는 설치 중에 선택할 수 있는 AES, DES 및 3DES 암호화 옵션도 제공합니다.

표준 암호화

eTrust AC 암호화 양식은 동적 링크 라이브러리(DLL)에서 구현됩니다. DLL 은 모든 데이터 암호화 및 해독을 구현하여 클라이언트 프로그램(selang.exe 또는 SeAM.exe)과 에이전트 서비스 간에 데이터를 안전한 형태로 전송할 수 있게 해줍니다. 명령 프롬프트에서 sechkey 유틸리티를 사용하거나 Windows 에서 ChEncKey.exe 유틸리티를 사용하여 기본 암호화 키를 변경할 수 있습니다.

eTrust AC 를 설치할 때 defenc.dll(기본 암호화용), aes128enc.dll(128 비트 AES 암호화용), aes192enc.dll(192 비트 AES 암호화용), aes256enc.dll(256 비트 AES 암호화용), desenc.dll((DES 암호화용) 및 tripledesenc.dll(3DES 암호화용) 파일이 다음 디렉터리에 설치됩니다.

eTrustACDir\bin

여기서 *eTrustACDir* 은 eTrust AC 가 설치된 디렉터리입니다.

defenc.dll, aesenc.dll, desenc.dll 또는 tripledesenc.dll 의 전체 경로는 레지스트리 하위 키에서 레지스트리 값 Encryption Package 로 저장됩니다.

HKEY_LOCAL_MACHINE\Software\ComputerAssociates\eTrustAccessControl

사용자 지정 암호화

사용자 자신의 암호화 방식을 사용하려면, 새 DLL 을 작성해야 합니다. 새 암호화 DLL 은 다음 디렉터리에 저장할 필요가 없지만 레지스트리 값 Encryption Package 를 새 DLL 의 전체 경로 디렉터리 이름으로 변경해야 합니다.

eTrustACDir\bin

여기서 *eTrustACDir* 은 eTrust AC 가 설치된 디렉터리입니다.

암호화 DLL 에는 다음과 같은 세 개의 내보낸 함수가 있어야 합니다.

1. DWORD Init(PCHAR pKey, DWORD dwLength)

   이 함수는 암호화 키를 초기화합니다.

2. DWORD Scramble(void *param, char *buffWithPlainText, int sizeofbuffWithPlainText, char *buffWithEncryptText, int *sizeofbuffWithEncryptText)

   이 함수는 두번째 매개 변수에서 받은 데이터를 암호화하고 암호화된 버퍼를 네번째 매개 변수에 저장합니다.

3. DWORD Unscramble(void *param, char *buffWithEncryptText, int sizeofbuffWithEncryptText, char *buffWithPlainText, int *sizeofbuffWithPlainText)

   이 함수는 두번째 매개 변수에서 받은 데이터를 해독하고 버퍼를 네번째 매개 변수에 일반 텍스트로 저장합니다.

중요: 암호화 키나 암호화 DLL 을 변경할 경우, 동일한 변경 사항을 서로 통신하는 모든 호스트에 적용해야 합니다. 그렇지 않으면, 암호화가 동일하지 않게 되어 호스트가 성공적으로 통신할 수 없는 상황이 발생합니다.

제 3 장: 관리자 인터페이스 사용

이 장은 아래의 주제를 포함하고 있습니다:

정책 관리자

정책 관리자는 Windows 와 UNIX 에서 eTrust AC 로컬 데이터베이스와 PMDB 를 관리하고 감사하기 위한 인터페이스입니다. 이 장의 절에서는 정책 관리자와 eTrust AC 를 통해 보안 정책을 구현하고 유지 관리하는 방법을 설명합니다. 정책 관리자는 기본 Windows 및 기본 UNIX 환경도 관리할 수 있습니다. Windows 사용자 관리자 또는 UNIX 명령줄을 통해 수행할 수 있는 대부분의 작업은 정책 관리자를 사용하여 수행할 수 있습니다.

인터페이스

모든 데이터 관리는 정책 관리자의 주 창에서 시작합니다. 성공적으로 로그온하면 다음과 같은 창이 나타납니다.

참고: 정책 관리자를 실행하려면, 설치 중에 스테이션을 관리 콘솔로 정의해야 합니다. 자세한 내용은 *구현 가이드*를 참조하십시오.

메뉴 모음

메뉴 모음에는 정책 관리자에서 사용할 수 있는 명령을 나열한 풀다운 메뉴가 있습니다. 메뉴 표시줄은 동적인 구조를 갖고 있어 실행하는 동작에 적합한 명령을 표시합니다. 예를 들어, [활성] 창에 트리 구조가 있을 때에만 [트리] 메뉴가 나타납니다.

도구 모음

도구모음을 통해 자주 사용되는 명령에 쉽게 액세스할 수 있습니다. 대부분의 명령은 메뉴 표시행에서도 이용할 수 있습니다. 메뉴 표시행과 같이 도구모음도 동적인 구조를 갖고 있어 실행하는 동작에 적합한 명령을 표시합니다. 다음 절에서는 일반적인 도구에 대해 설명합니다. 특정 창에 한정되는 도구는 해당 기능에 대한 단원에서 설명합니다.

프로그램 표시줄

프로그램 표시행을 통해 보호하거나 보호될 구체적인 항목을 선택할 수 있습니다. [프로그램 표시줄]에 패널을 표시하려면 [Access Control], [Windows NT] 및 [도구] 버튼을 클릭하십시오.

작업공간

작업 영역에 파일 메뉴 또는 프로그램 표시줄에서 열린 창이 표시됩니다. 이러한 창은 응용 프로그램 창입니다.

결과 표시행

출력 표시줄은 eTrust AC 에서 selang 명령을 작성하는 파일(명령 로그)을 표시합니다. 출력 표시줄에는 작성된 명령, 명령을 작성할 때 사용한 호스트, 명령이 작성된 환경, 명령이 실행된 날짜와 시간 등이 표시됩니다.

새 정책 관리자 세션을 시작할 때마다 eTrust AC 는 새 명령 로그를 작성합니다. 따라서 세션에서 명령을 저장하려면 로그를 저장하거나 인쇄해야 합니다.

참고: 참고: [정책 관리자] 창의 출력 표시줄에 있는 각 줄은 명령 로그에 두 개 이상의 selang 명령을 표시할 수도 있습니다.

참고: 정책 관리자 및 그 사용법에 대한 자세한 내용은 *정책 관리자 온라인 도움말*을 참조하십시오.

액세서 관리

계정이라고도 하는 *액세서*는 시스템 리소스에 액세스할 수 있는 항목입니다. 가장 일반적인 유형의 액세서는 유형은 일반적으로 로그온하고 액세스 권한이 할당 및 확인되는 *사용자*입니다. *그룹*, *프로그램* 및 *터미널*도 액세서입니다.

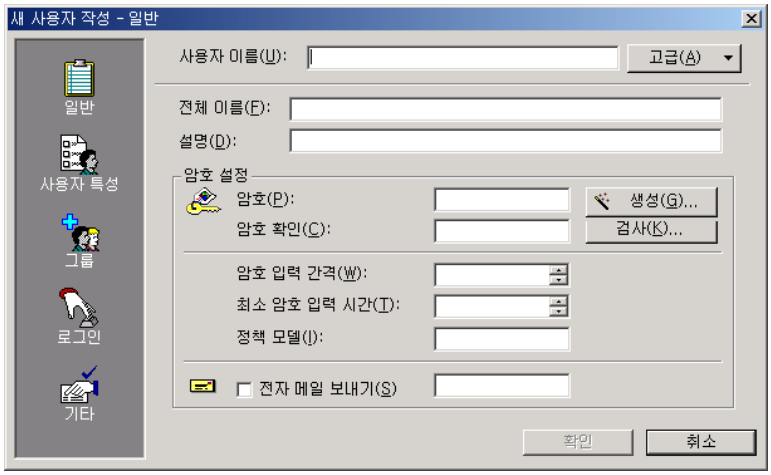
eTrust AC는 eTrust AC 데이터베이스에서 사용자 레코드를 작성할 때 사용하는 항목에 따라 계정 이름만으로 사용자를 확인하거나, Windows 도메인 이름 또는 (사용자 계정이 Windows 도메인에 속해 있지 않는 경우) 서버 이름이 앞에 붙은 계정 이름을 기준으로 사용자를 확인할 수 있습니다.

기본 Windows 운영 체제와 eTrust AC 데이터베이스(eTrust 환경)에서 정의한 모든 사용자 및 그룹을 관리할 수 있습니다. 다음 작업을 수행할 수 있습니다.

- 사용자 또는 그룹을 두 개의 환경(Windows 및 eTrust) 중 하나 또는 모든 환경에 추가
- 두 개의 환경 중 하나 또는 모든 환경에서 사용자 또는 그룹 업데이트
- 두 개의 환경 중 하나 또는 모든 환경에서 사용자 또는 그룹 삭제
- 사용자 이름 변경(Windows 환경에서만)
- 그룹에서 사용자 추가 또는 제거
- 그룹에서 그룹 추가 또는 제거
- 사용자 또는 그룹의 보호된 리소스 보기

이러한 기능을 수행하려면  사용자 또는  프로그램 표시줄의 [Access Control] 패널에서 그룹을 클릭한 후 도구 모음에서 [새로 만들기], [삭제], 또는 [속성]을 클릭합니다.

사용자 추가> 대화 상자는 다음과 같습니다([사용자]와 [새로 만들기]를 클릭합니다).



왼쪽 아이콘을 클릭하여 여러 패널을 표시하십시오. 예를 들어, 표시된 [일반] 패널에서는 사용자 이름과 설명을 입력하고, eTrust AC 환경 또는 Windows 환경을 지정하고([고급] 버튼), 암호 정보를 설정할 수 있습니다.

참고: eTrust AC 는 액세서 관리에 필요한 일부 작업을 수행하기 위한 마법사도 제공합니다. 마법사에 액세스하려면 [Access Control] 패널에서 [사용자] 또는 [그룹]을 클릭한 후 [도구] 메뉴에서 선택하거나 마법사 도구모음 버튼을 클릭합니다.

중요: Windows NT 백업 도메인 컨트롤러(BDC)를 사용하여 사용자를 정의하지 않는 것이 좋습니다. 기본 Windows 에서 사용자 관리자와 도메인 사용자 관리자를 통해 수행할 수 있는 대부분의 기능은 프로그램 표시행의[Access Control]및[Windows] 패널에서 수행할 수 있습니다.

설치 도중이나 설치 후 NT 가져오기 마법사를 사용하여 사용자와 그룹을 Windows 시스템에서 eTrust AC 데이터베이스로 가져올 수 있습니다.

참고: 자세한 내용과 절차는 *정책 관리자의 온라인 도움말*을 참조하십시오.

액세서에게 Windows 권한 할당

Windows 의 사용자 및 그룹에게 기본 또는 고급 권한을 할당할 수 있습니다. 최고급 권한은 Windows Workstation 또는 Windows Server 를 실행하는 컴퓨터 응용 프로그램을 작성하는 프로그래머들에게만 유용하므로, 고급 권한은 일반적으로 그룹이나 일반 사용자에게 부여되지 않습니다.

참고: 고급 권한에 대한 내용은 Windows Server 프로그래밍 문서를 참조하십시오.

사용자 로그인 제한

사용자 로그인 권한을 다음과 같은 방법으로 제한할 수 있습니다.

- 만료일을 지정합니다.
- 계정이 eTrust AC 데이터베이스에 존재하지만 사용자가 로그온할 수 없도록 계정을 일시 중지합니다.
- 유예 로그인 횟수를 지정합니다.
- 사용자가 로그온할 수 있는 터미널의 최대 수를 지정합니다.
- 계정이 비활성화되기 전에 경과해야 하는 일수를 지정합니다.
- 특정 날짜 및 시간으로 로그온 권한을 제한합니다.

기본적으로, 계정은 만료되거나 비활성화되지 않고 일시 중지되지도 않으므로, 사용자는 제한 없이 터미널에 로그온할 수 있습니다.

[로그인] 패널을 사용하여 로그인 권한을 제한합니다.

감사할 사용자 활동 선택

eTrust AC 데이터베이스에서 정의한 사용자에 대해 eTrust AC가 감사해야 하는 사용자 활동을 지정할 수 있습니다.

참고: 데이터베이스에서 AUDITOR 속성을 통해 정의한 사용자만 감사 속성을 지정할 수 있습니다. 기본 환경에서만 정의된 사용자인 경우에는 이 옵션이 흐리게 나타납니다.

다음과 같은 감사 모드는 eTrust AC 감사 로그에 어떤 사용자 활동을 포함할지 지정합니다. 이러한 옵션은 [사용자 작성 및 편집] 대화 상자의 [기타] 패널에서 사용할 수 있습니다.

성공

eTrust AC에서 정의한 리소스에 대한 성공적인 액세스가 로그 파일에 기록됩니다.

로그온 성공

성공적인 로그온이 로그 파일에 기록됩니다.

로그온 실패

실패한 로그인 시도가 로그 파일에 기록됩니다.

실패

데이터베이스에서 정의한 리소스에 대한 실패한 액세스 시도가 로그 파일에 기록됩니다.

모두

성공 여부와 관계 없이 모든 사용자 활동이 로그 파일에 기록됩니다.

None

사용자 활동이 로그 파일에 기록되지 않습니다.

개인 정보 입력

사용자 작성 및 편집> 대화상자의 [기타] 패널에서 사용자의 개인 정보를 입력할 수 있습니다. 다음과 같은 속성은 선택사항입니다.

위치

Main Office 또는 East Coast Sales 와 같이 사용자의 위치를 구체적으로 명시하는 최대 128 자의 영숫자 문자열입니다.

국가

사용자가 거주하는 국가를 표시하는 최대 19 자의 영숫자 문자열입니다.

조직

사용자가 할당된 조직을 나타내는 최대 256 자의 영숫자 문자열입니다.

조직 구성 단위

사용자가 할당된 조직 단위를 나타내는 최대 256 자의 영숫자 문자열입니다.

전화 번호

사용자의 전화 번호를 나타내는 최대 19 자의 영숫자 문자열

전자 메일

사용자의 전자 메일 주소를 나타내는 최대 256 자의 영숫자 문자열입니다.

계정 정보 설정

사용자 작성 및 편집> 대화 상자의 [기타] 패널에서 사용자의 계정 정보를 설정할 수 있습니다. 다음과 같은 속성은 선택사항입니다.

홈 디렉터리

사용자 홈 디렉터리 사용자가 자신의 홈 디렉터리로 자동 로그인합니다.

스크립트

사용자가 로그인할 때 자동으로 실행되는 파일 이름입니다. 로그인 스크립트는 작업 환경을 구성합니다.

프로필 경로

사용자 프로필이 들어 있는 파일의 전체 경로입니다. 사용자가 워크스테이션에 로그인할 때마다 동일한 환경이 화면에 표시됩니다.

사용자 권한 할당

사용자 작성 및 편집> 대화 상자의 [기타] 패널에서 사용자 권한을 할당할 수 있습니다. 사용자 권한에는 다음과 같은 항목이 포함됩니다.

- 시스템 시간 변경
- 장치 드라이버 로드 및 언로드
- 로컬로 로그인
- 파일 및 디렉터리 복원
- 파일 및 디렉터리 백업

B1 보안 기능 사용

B1 "Orange Book" 보안 기능을 사용하여 보안을 추가할 수 있습니다. 사용자 작성 및 편집 대화 상자의 [기타] 패널에 있는 [B1 기능] 버튼을 클릭하여 [B1 기능] 대화 상자에서 보안 레이블, 범주 및 수준을 선택합니다.

- 사용자에게 1 과 255 사이의 보안 수준을 할당할 수 있습니다. 리소스에 할당된 보안 수준 이상의 보안 수준을 가진 경우에만 리소스에 액세스할 수 있습니다.
- 사용자는 하나 이상의 보안 범주에 속할 수 있습니다. 사용자는 리소스에 할당된 모든 보안 범주에 속한 경우에만 리소스에 액세스할 수 있습니다.
- 보안 레이블은 특정 보안 수준을 일련의 보안 범주와 연결합니다. 사용자에게 보안 레이블을 할당하면 보안 수준과 보안 레이블에 관련된 보안 범주가 사용자에게 모두 부여됩니다.

세션 그룹 할당

사용자 작성 및 편집을 위한 [기타] 패널에서 [세션 그룹] 버튼을 사용하여 eTrust SSO 세션 그룹을 사용자에게 할당할 수 있습니다.

그룹에 사용자 추가

그룹에 사용자를 추가하면 관리 작업을 훨씬 쉽게 수행할 수 있습니다. 사용자 작성 및 편집 대화 상자의 [그룹] 패널을 사용하십시오.

중첩 그룹 추가

그룹 작성 및 편집> 대화 상자의 [기타] 영역에서 중첩 그룹을 추가하거나 수정할 수 있습니다. 프로그램 모음에서 [그룹]을 누른 다음 도구 모음에서 [새로 만들기]나 [속성]을 누릅니다.)

중첩 그룹> 대화 상자를 통해 기존 그룹에서 수퍼 그룹(상위그룹)과 구성원 그룹(하위그룹)을 추가 및 삭제할 수 있습니다. 수퍼 그룹의 속성은 해당 구성원 그룹으로 전달됩니다.

Active Directory 속성 설정

Active Directory 가 설치된 Windows 2000 컴퓨터에 연결되어 있으면 사용자 또는 그룹 대화 상자의 [Directory Services] 패널을 사용하여 Active Directory 사용자 또는 그룹 속성을 설정할 수 있습니다. 이러한 속성은 Active Directory 가 없는 Windows NT, Windows 2000 또는 eTrust AC 기본 환경 데이터베이스에서 지원되지 않습니다.

패널을 활성화하는 아이콘은 Active Directory 가 있는 Windows 2000 컴퓨터에 연결되어 있어야 나타납니다.

참고: Active Directory 를 사용하여 사용자를 다른 폴더에 구성할 수 있습니다. 정책 관리자는 모든 Active Directory 사용자를 하나의 사용자 패널에 표시합니다.

기본 운영 체제와 데이터 동기화

selang 명령을 사용할 때에는 기본 운영 체제에서 데이터를 변경하지 않고도 데이터베이스에서 액세서에 대한 데이터를 변경할 수 있습니다. 마찬가지로, Windows 에서 사용자 관리자를 사용할 때 eTrust AC 에서 데이터를 변경하지 않고 Windows 에서 액세서 데이터를 변경할 수 있습니다.이와 같은 방법으로 데이터를 변경하면 액세서는 각 데이터베이스에서 서로 다르게 정의됩니다.

eTrust AC 는 eTrust AC 와 기본 운영 체제의 정의를 모두 모니터링하고 Windows 와 eTrust AC 의 정의가 일치하지 않을 때 [동기화] 패널을 제공합니다. 정의가 일치하면 [동기화] 아이콘은 보이지 않습니다.

eTrust AC 리소스 관리

*리소스*란 사용자와 그룹이 액세스할 수 있는 항목입니다. 가장 일반적인 유형의 리소스는 파일입니다. 파일에 있는 정보를 읽거나 파일에 정보를 쓸 때 파일을 액세스합니다.

리소스는 *클래스*로 그룹화되며, 클래스는 리소스 유형을 가리키는 이름입니다. 예를 들어, TERMINAL 클래스는 tty1, tty2 등과 같이 터미널인 모든 개체를 포함하고, SHARE 클래스는 공유되는 모든 개체를 포함하며, FILE 클래스는 파일 및 디렉터리의 정의를 포함합니다.

참고: eTrust AC 클래스에 대한 자세한 내용은 *참조 가이드*를 참조하십시오.

보호되는 리소스의 속성은 리소스의 *레코드*에 저장됩니다. 레코드란 리소스 이름과 속성으로 구성된 데이터의 집합입니다. 특정 클래스의 모든 레코드에는 동일한 속성(클래스가 설명하는 개체의 유형에 해당하는 속성) 집합에 대한 값이 있습니다.

속성은 리소스를 정의한 사람, 리소스가 정의된 날짜 등을 나타냅니다. 일반적으로, 리소스 레코드에 포함되는 가장 중요한 정보는 리소스를 액세스할 수 있는 권한이 있는 액세서 목록입니다. 이 목록을 ACL(access control list)이라 합니다. 많은 리소스에는 액세스가 거부되는 또 다른 액세서 목록이 있습니다. 이 목록을 NACL(Negative ACL)이라고 합니다.

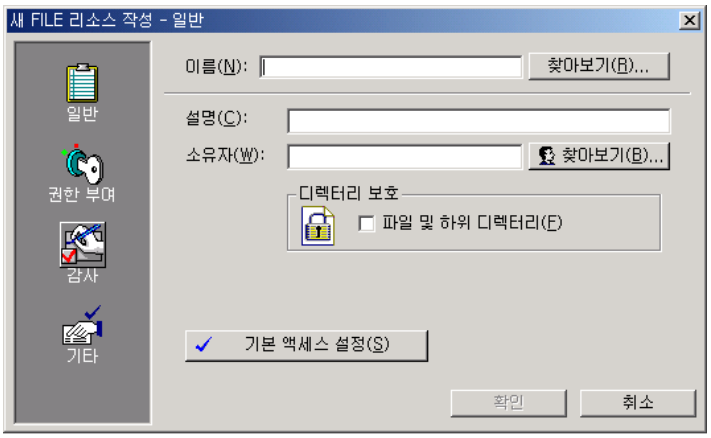
참고: 사용자 또는 그룹 이름을 마우스 오른쪽 버튼으로 눌렀을 때 표시되는 메뉴에서 [보호된 리소스]를 선택하여 특정 사용자 또는 그룹에 대한 ACL 이나 NACL 을 볼 수 있습니다.

다음 작업을 수행하여 eTrust AC 데이터베이스에 있는 모든 리소스를 관리할 수 있습니다.

- eTrust AC 데이터베이스의 클래스에 리소스 추가
- eTrust AC 데이터베이스의 클래스에 리소스 업데이트
- eTrust AC 데이터베이스의 클래스에서 리소스 삭제
- 사용자가 로그인할 수 있는 터미널과 터미널 그룹 정의
- 사용자가 로그인을 위해 추가 권한이 필요한 휴일 정의
- 작업 위임 및 작업 그룹 정의

이러한 기능을 수행하려면 클릭하십시오.  프로그램 표시줄의 [Access Control] 패널에서 리소스를 클릭하고 작업 영역에서 리소스를 선택한 후 도구 모음에서 [새로 만들기], [삭제] 또는 [속성]을 클릭합니다.

다음은 FILE 클래스에서 리소스를 작성하기 위한 대화 상자입니다.([리소스]와 [새로 만들기]를 클릭합니다.)



왼쪽 아이콘을 클릭하여 여러 패널을 표시하십시오. 예를 들어, 위의 [일반] 패널을 통해 리소스의 이름과 설명을 입력하고, 소유자를 지정하는 등의 작업을 수행할 수 있습니다.

달력을 사용하여 eTrust AC 리소스 관리

eTrust AC 는 Unicenter TNG 달력에 따라 사용자, 그룹 및 리소스 액세스 적용을 지원합니다. 달력에는 ON 또는 OFF 로 설정할 수 있는 15 분의 시간 간격이 있습니다. 달력 시간 간격이 OFF 로 설정되면 리소스에 액세스할 수 없으며, 달력 시간 간격이 ON 으로 설정되면 리소스에 액세스할 수 있습니다. eTrust AC 는 지정된 시간 간격으로 Unicenter TNG 활성 달력을 검색합니다.

리소스 보기를 사용하여 달력 리소스를 추가하거나 편집 또는 제거할 수 있습니다. 로그인 보호를 선택합니다. 달력 트리 항목을 클릭한 후 마우스 오른쪽 버튼을 클릭하여옵션을 선택합니다.

Windows 리소스 관리

리소스 작성 및 편집> 대화 상자를 사용하여 기본 Windows 데이터베이스에 있는 리소스를 관리할 수 있습니다. 다음 작업을 수행할 수 있습니다.

- Windows 데이터베이스의 REGISTRY 및 SHARE 클래스에 리소스 추가
- Active Directory 데이터베이스를 포함한 Windows 데이터베이스의 클래스에서 리소스 업데이트
- Windows 데이터베이스의 클래스에서 리소스 삭제

참고: Windows 리소스에 대한 자세한 내용은 *참조 가이드*의 Windows 환경 클래스 및 속성 장을 참조하십시오.

Windows 도메인 관리

정책 관리자를 사용하여 다음 작업을 수행할 수 있습니다.

- Windows 도메인에 대한 정보 표시
- Windows 도메인에 새 컴퓨터 추가
- Windows 도메인에서 컴퓨터 삭제
- Windows 도메인 간에 트러스트된 관계 생성 및 삭제

리소스 트리에서 NT 관련을 선택합니다. 도메인 트리 항목을 누르고 마우스 오른쪽 버튼을 눌러 옵션을 선택합니다.

eTrust AC는 정책 관리자 또는 selang과 같은 eTrust AC 클라이언트가 이러한 동작을 수행할 경우 해당 동작의 유효성을 확인합니다. 동작의 유효성을 확인할 때, eTrust AC는 도메인 컨트롤러의 eTrust AC 데이터베이스에 존재하는 권한 부여 규칙을 사용합니다.

eTrust AC 클래스 DOMAIN의 각 레코드는 Windows 도메인을 정의합니다. DOMAIN 클래스에서 사용 가능한 세 개의 레코드 액세스 유형은 다음과 같습니다.

READ

사용자는 도메인의 속성을 표시할 수 있습니다.

CHMOD(트러스트 변경)

사용자는 도메인 간의 트러스트 관계를 만들거나 삭제할 수 있습니다.

EXEC(실행)

사용자는 도메인에서 구성원을 추가하거나 삭제할 수 있습니다.

프로세스 보호

PROCESS 클래스의 개체는 eTrust AC 보호가 필요한 프로세스 응용 프로그램을 정의합니다.

eTrust AC 로 프로세스를 보호하려면, 다음 단계를 수행합니다.

1. eTrust AC 정책 관리자 시작
2. [프로그램] 표시행에서 [리소스]를 선택합니다.
3. eTrust AC 리소스 트리를 확장하여 [시스템 리소스]를 표시하고 [프로세스]를 선택합니다.
4. 보호할 새 프로세스를 추가하려면, [이름] 열에서 마우스 오른쪽 버튼을 클릭하여[새로 만들기]를 선택하거나 키보드에서 [삽입]을 클릭합니다.
5. Windows 작업 관리자(taskmgr.exe)를 시작합니다. 다음 단계를 수행하려면 작업 관리자를 실행해야 합니다.
6. [이름] 필드 옆에 있는 [찾아보기]를 클릭합니다. 보호할 프로세스(taskmgr.exe)를 선택합니다. [확인]을 클릭합니다.
7. [소유자]필드 옆에 있는 [찾아보기]를 클릭합니다.
8. nobody 를 선택합니다. [확인]을 클릭합니다.
9. 기본 액세스 설정 버튼을 클릭합니다.

   기본 액세스 설정> 대화 상자가 나타납니다.
10. 없음을 선택했는지 확인합니다. [확인]을 클릭합니다.
11. 규칙을 테스트하려면, 작업 관리자(taskmgr.exe)를 열고 프로세스 탭을 선택한 후 taskmgr.exe 를 선택하고 프로세스 끝내기를 클릭합니다.
12. 작업 관리자 경고> 대화 상자가 나타납니다. 예를 클릭합니다.

    규칙이 성공적으로 실행된 경우, Unable to Terminate Process 제목의 대화 상자가 나타납니다.
13. 선택한 프로세스를 종료할 수 있는 권한이 있는 사용자를 추가하려면, eTrust AC 리소스 트리를 확장하여 [시스템 리소스]를 표시한 후 [프로세스]를 선택합니다.
14. 프로세스에서 마우스 오른쪽 버튼을 클릭하고[속성]을 선택합니다.
15. [권한 부여] 클릭합니다.
16. [삽입]을 클릭합니다.
17. [이름] 필드 옆에 있는 [찾아보기]를 클릭합니다.
18. 사용자 또는그룹 탭을 선택하고 [확인]을클릭합니다.
19. [읽기] 권한을 선택하고 [확인]을 클릭합니다.
20. 새 규칙을 테스트하려면, 프로세스를 종료할 수 있는 권한이 있는 사용자로 로그인합니다.

21. 작업 관리자(taskmgr.exe)를 열고 프로세스 탭을 선택한 후 taskmgr.exe 를 선택하고 프로세스 끝내기를 클릭합니다.

    프로세스가 끝납니다.

참고: 이 서비스의 대부분은 GUI 또는 대화형 응용 프로그램이 아닌 백그라운드에서 실행되므로, Windows 서비스는 eTrust AC 프로세스를 보호하기 위한 우수한 서비스입니다.

SPECIALPGM 으로 리소스 보호

SPECIALPGM 클래스에 있는 개체는 특수 eTrust AC 권한 부여 보호가 필요한 응용 프로그램을 정의합니다. 이 클래스는 일반적으로 System 계정으로 실행되어야 하는 시스템 서비스와 같은 프로그램을 보호하는 데 특히 유용합니다. 이런 프로그램을 보호하려면, 해당 프로그램을 SPECIALPGM 클래스의 레코드로 정의하고 (eTrust AC 데이터베이스에서 USER 레코드로 정의된) 논리적 사용자 이름을 프로그램 실행에 필요한 Windows 사용자 이름과 연결하여 해당되는 논리적 사용자만 프로그램을 실행할 수 있도록 권한을 부여하십시오

Windows 에서는 특별 프로그램 마법사를 사용하여 이와 같은 보호 기능을 설정할 수 있습니다. GUI 에서 마법사를 실행하려면 프로그램 표시줄에서 [리소스] 버튼을 클릭하십시오. 그런 다음 [도구] 메뉴에서 특별 프로그램 마법사를 선택하십시오.

정책 모델 관리

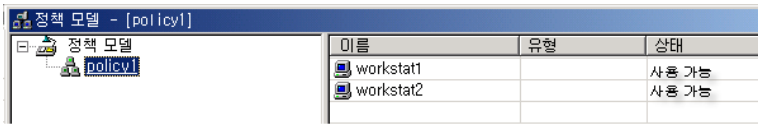
정책 관리자를 사용하여 여러 PMDB 기능을 관리할 수 있습니다. 이러한 기능에는 PMDB 를 지정하고, 가입자를 관리하며, 오류 로그를 관리하고, 정책 모델 데몬을 (UNIX 에서) 시작 및 종료하며, 사용 불가능한 가입자를 재활성화하고, 속성을 표시하는 기능이 있습니다.

PMDB 지정

eTrust AC 는 단일 호스트에서 복수의 정책 모델을 지원합니다. 정책 관리자 또는 selang 을 사용하여 PMDB 를 지정할 수 있습니다.

정책 모델 창 표시

프로그램 표시행의 [도구] 패널에서 활성화하는 [정책 모델] 창에는 사용자(해당될 경우 구독자도 포함)가 연결되어 있는 스테이션에서 정의한 모든 PMDB 가 나열되어 있습니다.



정책 모델] 창에는 다음과 같은 열이 있습니다.

이름

선택한 PMDB 의 구독자를 나열합니다.

유형

구독자의 유형인 eTrust 데이터베이스, PMDB 또는 MF(메인프레임)를 표시합니다.

상태

구독자가사용 가능한지 사용 불가능한지표시합니다. 실행 대기 중인 명령이 없을 때 구독자는사용 가능합니다. 상위 PMDB 가 아직 실행되지 않은 하나 이상의 명령을 전송한 경우 구독자는 불가능합니다. 명령은 updates.dat 파일에 저장되며, 이 파일의 기본 위치는 *eTrustACDir*\data\pmdb(*eTrustACDir* 은 eTrust AC 를 설치한 디렉터리임)입니다.

다음 명령

실행 대기 중인 명령을 표시합니다.

구독자가 사용 가능 상태이면 이 열은 비어 있습니다.

오류

선택된 가입자에 대한 오류의 수를 표시합니다. 오류는 가입자를 업데이트할 수 없는 명령입니다. 연결 실패는 포함되지 않습니다.

실행된 명령

실행된 명령을 백분율로 표시합니다. 구독자가 사용 가능 상태이면 이 열은 100% 값을 표시합니다.

정책 모델 계층 관리

PMDB 구독자가 될 수 있는 경우는 다음과 같습니다.

- 동일한 호스트나 원격 호스트에 있는 다른 PMDB
- 동일한 호스트나 원격 호스트에 있는 eTrust 데이터베이스
- 메인프레임 데이터베이스

정책 관리자를 사용하여 다음 작업을 수행할 수 있습니다.

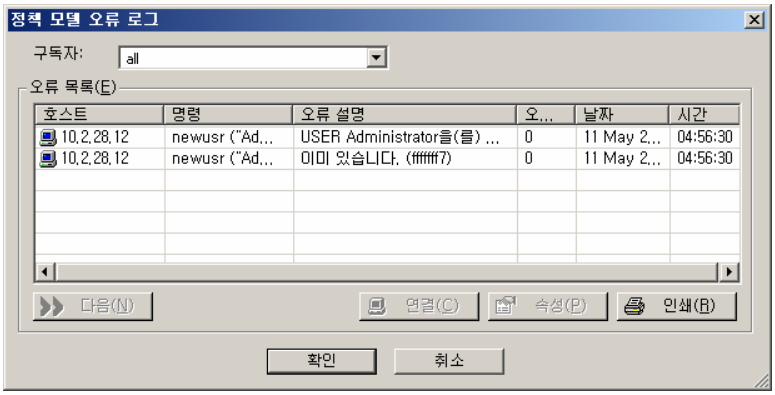
- PMDB 에 구독자 추가
- PMDB 에서 구독자 제거
- 구독자에게 전송되었지만 업데이트에 실패한 명령(오류 로그에 나타나는 오류) 표시
- 오류 로그의 내용 삭제

구독자를 추가할 때 상위 PMDB 와 여기에 구독하려는 모든 스테이션이 동일한 네트워크의 일부이고 서로 이름을 사용하여 통신할 수 있는지 확인해야 합니다. 이렇게 하면 eTrust AC 가 구독자의 레지스트리에 있는 parent_pmd 키를 업데이트할 수 있습니다.

오류 로그 관련 작업

WatchdogÀº 정책 모델 오류 로그에는 구독자 스테이션이 적용을 거부한 트랜잭션의 목록이 있습니다.

정책 관리자를 사용하여 PMDB 와 모든 구독자의 오류를 표시하거나 한 명의 구독자에 대한 오류만 표시할 수 있습니다. 또한 오류 로그의 내용을 삭제할 수도 있습니다.



정책 모델오류 로그> 대화 상자에는 다음 열이 있습니다.

호스트

명령이 실패한 PMDB 의 전체 이름입니다.

명령

실패한 전체 eTrust AC 명령입니다.

오류 설명

명령이 실패한 이유입니다.

오프셋

updates.dat 파일에 있는 명령의 위치입니다.

날짜

명령이 실패한 날짜입니다.

시간

명령이 실패한 시간입니다.

참고: [다음] 버튼을 클릭하면, eTrust AC 는 다음 레코드 집합을 불러옵니다. query_size 레지스트리 키는 집합 내 레코드의 수를 정의합니다. (기본값은 100 입니다.) 다음 집합에 있는 레코드가 디스플레이에 추가됩니다. 이것은 다음을 한 번 클릭한 경우(그리고 키의 값이 여전히 100 인 경우), 200 개의 레코드가 표시된다는 의미입니다.

속성 표시

[보기] 메뉴 또는 마우스 오른쪽 버튼을 클릭하면 나타나는 메뉴에서 [속성]을 선택하여 PMDB 또는 구독자의 속성을 표시합니다.

상위 PMDB 에 대해 표시되는 속성에 대한 설명은 다음과 같습니다.

정책 모델 이름

PMDB 의 이름입니다.

상위 정책 모델

PMDB 가 상위 DB 인지 나타냅니다.

암호 파일

전체 이름, ID, 사용자가 속해 있는 그룹의 ID, 홈 디렉터리 및 암호화된 암호와 같이 로컬에서 정의한 사용자에 대한 정보가 들어 있는 파일의 이름입니다(UNIX 만 해당).

그룹 파일

그룹 ID 와 그룹의 사용자 목록과 같이 로컬에서 정의한 그룹에 대한 정보가 들어 있는 파일의 이름입니다(UNIX 만 해당).

eTrust AC는 구독자의 속성을 보여주기 위해 (페이지 49) [정책 모델] 창을 표시합니다.

Windows 용 eTrust AC 를 사용하여 UNIX 관리

정책 관리자를 사용하여 eTrust AC 가 설치된 UNIX 시스템을 관리할 수 있습니다. UNIX 및 eTrust AC 환경에 정의된 사용자, 그룹, 리소스 및 PMDB 계층을 관리할 수 있습니다.

관리자 리소스

ADMIN 클래스

정책 관리자의 클래스별 액세스 기능을 사용하여 ADMIN 클래스에 개체를 추가할 수 있습니다.

- ADMIN 클래스에는 비 ADMIN 사용자에게 특정 클래스의 관리를 허용하는 정의가 포함됩니다.
- ADMIN 레코드는 위임된 사용자에 의해 관리되는 각 eTrust AC 클래스를 나타냅니다.
- 레코드는 각 레코드에 대한 액세스 권한이 있는 액세서의 목록을 포함합니다.
- ADMIN 클래스 레코드의 키는 보호될 클래스의 이름입니다.

예:

ADMIN 클래스 함수를 수행하는 비 ADMIN 사용자를 정의하려면, 다음 예제를 참조하십시오.

참고: 다음 예를 수행하려면 두 개의 워크스테이션이 필요합니다. 로컬 터미널을 **computer1**, 원격 터미널을 **computer2** 라 부릅니다. 실제 환경에서는 컴퓨터 이름이 다를 수도 있습니다.

1. 로컬 터미널(computer1)에서 sub_admin 사용자를 작성합니다.
   a. eTrust AC 시작
   b. [프로그램] 메뉴에서 [사용자]를 클릭하고 새 사용자를 작성합니다.
   c. [사용자 이름] 필드에 sub_admin 을 입력합니다.
   d. [전체 이름] 필드에 sub_admin 을 입력합니다.
   e. [설명] 필드에 sub_admin 을 입력합니다.
   f. [암호] 필드에 기억할 암호를 입력합니다.
   g. [고급 드롭다운] 메뉴를 클릭합니다. 다음 두 항목을 모두 선택해야 합니다.
      – Create in Native OS environment
      – Create in eTrust AC environment
   h. [확인]을 누릅니다.

2. 원격 터미널(computer2)에서 sub_admin 사용자를 작성합니다.
   a. eTrust AC 시작
   b. [프로그램] 메뉴에서 [사용자]를 클릭하고 새 사용자를 작성합니다.

      참고: 원격 액세스 사용자 이름은 다음 형식으로 입력해야 합니다.

      `computer_name\user_name.`
   c. [사용자 이름] 필드에 computer1\sub_admin 을 입력합니다.
   d. [전체 이름] 필드에 computer1\sub_admin 을 입력합니다.
   e. [설명] 필드에 computer1\sub_admin 을 입력합니다.
   f. [고급 드롭다운] 메뉴를 클릭하니다. create in eTrust AC Environment 만 선택합니다. [확인]을 클릭합니다.
3. 원격 터미널(computer2)에서 로컬 터미널(computer1) 액세스를 허용합니다.
   a. 원격 터미널(computer2)에서 eTrust AC [프로그램] 메뉴를 클릭한 후 [리소스]를 클릭합니다.
   b. login protection 트리를 펼쳐 이름열의 열려 있는 필드에서 마우스 오른쪽 버튼을 클릭하고 [새로 만들기]를 선택합니다.
   c. 로컬 터미널(computer1) 정보를 입력합니다.
   d. [이름] 필드에 로컬 터미널(Computer1) 이름을 입력합니다.
   e. [설명] 필드에 터미널(Computer1)을 입력합니다.
   f. [소유자] 필드에 *nobody* 를 입력합니다.
   g. [기본 액세스 설정]을 클릭하고 *None* 이 선택되어 있는지 확인합니다.
   h. [확인]을 클릭합니다.
   i. [권한 부여] 클릭합니다.
   j. [삽입]을 클릭합니다.
   k. [이름] 필드 옆에 있는 [찾아보기] 버튼을 클릭합니다.
   l. 앞에서 작성한 computer1\sub_admin 사용자를 선택하고 [확인]을 클릭하여 <eTrust 액세서 추가/편집> 대화 상자로 돌아갑니다.
   m. <eTrust 액세서 추가/편집> 대화 상자가 나타납니다. [확인]을 클릭합니다.
   n. 추가한 사용자를 선택한 후 읽기 권한을 선택하고 [확인]을 클릭합니다.

4. 원격 터미널(computer2)에서 관리 트리를 펼쳐 [클래스별 액세스]를 선택한 후 USER 클래스를 선택합니다.

   a. USER 클래스에서 마우스 오른쪽 단추를 클릭하여 [속성]를 선택하고 [권한 부여]를 클릭합니다.

   b. [삽입]을 클릭합니다.

   c. [이름] 필드 옆에 있는 [찾아보기]를 클릭합니다.

   d. 앞에서 작성한 computer1\sub_admin 사용자를 선택하고 [확인]을클릭하여 <eTrust 액세서 추가/편집> 대화 상자로 돌아갑니다.

   e. <eTrust 액세서 추가/편집> 대화 상자가 나타납니다. [확인]을 클릭합니다.

   f. 추가한 사용자를 선택한 후 읽기 권한을 선택하고 [확인]을 클릭합니다.

5. 두 대의 컴퓨터는 모두 동일한 네트워크에서 eTrust AC를 실행 중이어야 합니다.

6. 로컬 컴퓨터(computer1)에서 sub_admin 사용자로 Windows에 로그인합니다.

7. 로컬 컴퓨터(computer1)에서 eTrust AC를 시작합니다. 왼쪽 상단에 위치한 [connect] 아이콘을 클릭합니다.

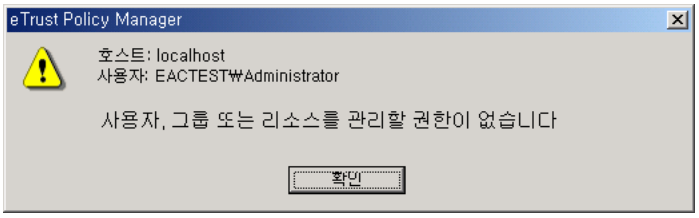
8. 원격 터미널 호스트(computer2)의 이름을 입력하고 [확인]을 클릭합니다.

9. <연결 정보> 대화 상자가 나타납니다. [확인]을 클릭합니다.

   [확인]을 클릭하면 정책 관리자가 열립니다. 원격 터미널(computer2)에 연결됩니다.

10. 정책 관리자에서  사용자를 클릭합니다.

11. 다음 오류 메시지가 나타납니다.



12. 클래스별 액세스는 하위 관리에도 사용됩니다.

    관리자가 지정한 클래스와 리소스를 하위 관리자가 관리하도록 하려면, 원격 터미널(computer2)에서만 다음 단계를 수행합니다.

    a. [도구] 메뉴, [옵션], [시작] 탭을 선택합니다.

    b. [사용자 및 그룹 하위 관리]를 선택하고 [확인]을클릭합니다.

13. USERS]를 다시 클릭합니다.

    사용자 목록과사용자 속성이 나타납니다. 사용자 속성을 변경하려는 경우, "작업을 수행할 수 없습니다."라는 오류 메시지가 나타납니다. 그 이유는 사용자가 ADMIN/USER 클래스에 읽기 액세스만 가지고 있기 때문입니다.

    ADMIN 클래스나 GROUP 클래스에 대한 권한이 있는 사용자가 아니므로, "작업을 수행할 수 없습니다."라는오류 메시지는[그룹]을 클릭한 경우에도 나타납니다.

14. Groups Properties> 대화 상자에서 [그룹] 및 [파일]을 검색하려면, Set [Admin Properties] 대화 상자에서 Object Group 에 읽기 권한을 추가해야 합니다.

    a. 원격 터미널에서 Administration Resource 트리를 펼쳐 클래스별 액세스를 선택한 후 그룹 클래스에서 마우스 오른쪽 버튼을 클릭하고 속성를 선택합니다.

    b. 권한 부여]를 클릭한 후 삽입을 클릭하고 작성한 터미널을 선택한 후 User Permissions 를 설정합니다.

    c. 로컬 터미널에서 원격 터미널로 연결한 후 [그룹]을 클릭합니다.

    d. 그룹 클래스가 나타납니다.

컨테이너 클래스

컨테이너컨테이너 클래스의 각 레코드는 다른 리소스 클래스의 개체, 파일 및 사용자 그룹을 정의합니다. 이것은 규칙이 여러 클래스의 개체에 적용될 때 액세스 규칙의 정의를 단순화합니다. Container 클래스 레코드의 구성원은 eTrust AC 클래스 중 하나의 개체, 파일 및 사용자일 수 있습니다

예:

이 예제에서 컨테이너 클래스에 My 컨테이너 개체를 작성합니다. 이 개체에 대해 두 명의 구성원을 수집하는 데, 하나는 FILE 클래스(c:\winnt\notepad.exe)에서 다른 하나는 TERMINAL 클래스(MyComp.ca.com)에서 수집합니다. 그런 다음, John 의 읽기 및 실행 권한을 My 컨테이너로 부여하거나 허용합니다.

1. 시스템 리소스 트리를 펼치고 File 에서 마우스 오른쪽 버튼을 클릭한 후 New 를 클릭하고 다음 정보를 입력합니다.

    a. [이름] 필드에 c:\winnt\notepad.exe 를 입력합니다.

    b. [설명] 필드에 컨테이너 Test Rule 을 입력합니다.

    c. [소유자] 필드에 Nobody 를 지정합니다

    d. [기본 액세스]를 없음으로 설정합니다.

2. Administration Resource 트리를 펼치고 컨테이너에서 마우스 오른쪽 버튼을 클릭한 후 New 를 선택하고 다음 정보를 입력합니다.

   a. [이름] 필드에 MyContainer 를 입력합니다.

   b. [설명] 필드에 MyContainer 테스트를 입력합니다.

   c. [소유자] 필드에 nobody 를 지정합니다.

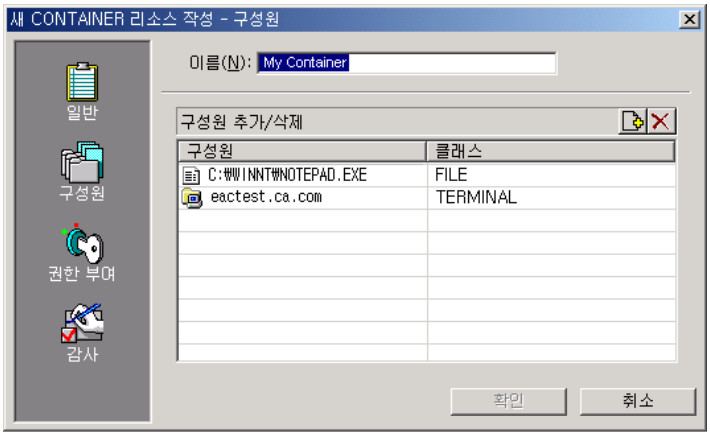
3. [구성원]을 클릭하고 MEMBERS 열의 열려 있는 필드에서 마우스 오른쪽 버튼을 클릭한 후 [추가]를 클릭합니다.

4. File 클래스를 선택한 후 작성한 File 규칙(c:\winnt\notepad.exe)을 선택하고[확인]을 클릭합니다.

5. 구성원 열의 열려 있는 필드에서 마우스 오른쪽 버튼을 클릭한 후 Add 를 클릭합니다.

6. 터미널클래스를 선택한 후 추가할 터미널 이름을 선택하고[확인]을 클릭합니다.

   Container Resource> 대화 상자는 다음과 같습니다.

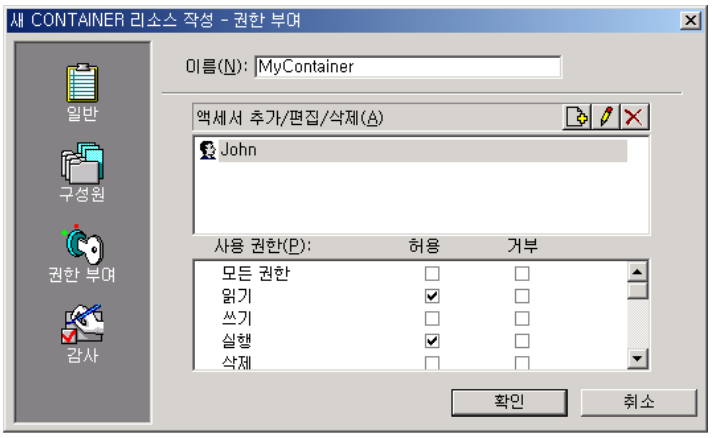


7. [권한 부여], [삽입]을차례로 클릭하고[이름] 필드 옆의 [찾아보기]를 클릭한 후 [사용자]를 선택합니다. 그리고 [확인]을 클릭합니다.

   <eTrust 액세서 추가/편집> 대화 상자가 나타납니다.

8. [확인]을 클릭합니다.

9. 선택한 사용자에게 읽기 및 실행 권한을 부여합니다.



10. 앞에서 지정한 사용자로 로그인합니다. MyContainer 에서 이 사용자에 대한 읽기 액세스를 허용했기 때문에 로그인에 성공해야 합니다.

11. c:\winnt\notepad.exe 를 실행하고 실행을 허용합니다.

12. c:\winnt\notepad.exe 삭제를 시도합니다. 이 작업은 금지되어야 합니다.

13. eTrust AC 클라이언트, 정책 관리자, 또는 selang 에 대해 세션 열기를 시도합니다. John 은 My 컨테이너에서 쓰기 액세스가 허용되지 않았으므로 이 작업이 금지되어야 합니다.

14. 사용자 권한을 변경하고 모든 항목을 거부합니다.

    지정된 사용자는 로그인이 거부됩니다. c:\winnt\notepad.exe 의 실행도 거부됩니다.

하위 관리자 작성

정책 관리자에서 사용자 및 그룹을 관리할 하위 관리자를 설정하려면, 다음 단계를 수행하십시오.

1. 정책 관리자를 실행합니다.

   참고: 시스템에 eTrust AC 서버가 설치된 경우에는 정책 관리자에 로그인한 후 eTrust AC 서비스를 종료합니다.

2. 정책 관리자 [도구 모음]에서 [도구], [옵션]을 선택합니다.

   [옵션] 대화 상자가 나타납니다.

3. [시작] 탭을 선택한 후 Enable Sub Administration 을 선택합니다.

4. [확인]을 클릭합니다.

하위 관리자가 특정 터미널에서 정책 관리자를 액세스하려면 다음 단계를 수행하십시오.

1. eTrust AC 프로그램 표시줄에서 [리소스] 아이콘을 선택하여 [리소스] 창을 표시합니다.

2. 로그인 보호 폴더를 펼칩니다.

3. 터미널을 선택하여 사용 가능한 터미널 목록을 표시합니다.

4. 원하는 터미널을 두 번 클릭합니다. View or Set Terminal Properties - General> 대화 상자가 표시됩니다.

5. [권한 부여] 아이콘을 선택하여 [View or Set Terminal Properties - Authorize(터미널 속성 보기 및 설정 - 권한 부여)] 대화 상자를 표시합니다.

6. 권한을 부여할 하위 관리자를 선택한 후 읽기 및 쓰기 권한을 선택합니다.

7. [확인]을 클릭합니다.

사용자를 관리하는 권한을 가진 하위 관리자를 정의하려면, 다음 작업을 수행하십시오.

1. eTrust AC 프로그램 표시줄에서 [리소스] 아이콘을 선택하여 [리소스] 창을 표시합니다.

2. 관리 폴더를 펼칩니다.

3. 클래스별 액세스를 선택하여 사용 가능한 클래스 목록을 표시합니다.

4. USER 클래스를 두 번 클릭한 후 속성을 선택합니다. View or Set ADMIN Properties - General> 대화 상자가 표시됩니다.

   참고: 하위 관리자가 다른 클래스를 관리할 수 있도록 하려면 USER 클래스를 원하는 클래스(GROUP, USER_DIR 등)로 바꿉니다.

5. 권한 부여] 아이콘을 선택하여 [View or Set ADMIN Properties - Authorize] 대화 상자를 표시합니다.

6. [추가]를 클릭하여 eTrust AC 액세서 추가 대화 상자를 표시합니다.

7. 하위 관리자 이름을 [이름] 필드에 입력하거나 [찾아보기]를 클릭하여 이름을 찾습니다.
8. 하위 관리자에게 액세스를 지정할 권한을 선택합니다.
9. [ADMIN 속성 보기 또는 설정 - 권한 부여] 대화 상자로 돌아가려면 [확인]을 클릭합니다.
10. [확인]을 클릭하여 종료합니다.

제 4 장: 사용자 암호 관리

이 장은 아래의 주제를 포함하고 있습니다:

암호 관리 유틸리티

다음 소프트웨어를 사용하여 사용자 암호를 관리할 수 있습니다.

암호 관리자

암호 관리자를 사용하여 사용자 암호를 설정하고 변경할 수 있습니다.

암호 관리자는 정책 관리자를 실행하지 않는 컴퓨터에 설치할 수 있는 독립된 암호 관리 유틸리티입니다. 이 유틸리티를 사용하면 관리자가 아닌 사용자에게 암호 관리 작업을 보다 쉽게 할당할 수 있습니다.

정책 관리자

Windows 에서 사용자를 새로 만들거나 정의된 사용자를 업데이트할 때마다 사용자 암호를 설정하거나 변경할 수 있습니다.

암호 정책을 설정하는 데 정책 관리자 (페이지 37) 를 사용할 수도 있습니다.

selang 명령

selang 명령인 newusr, editusr, chusr 은 사용자의 암호를 설정합니다.

참고: 이 명령에 대한 자세한 내용은 *참조 가이드*를 참조하십시오.

Windows 유틸리티

명령 프롬프트 창에서 Windows 사용자 관리자 또는 Windows 명령을 사용하여 사용자 암호를 관리할 수 있습니다.

Note: 자세한 내용은 관련 Windows 문서를 참조하십시오.

암호 관리자, 정책 관리자 또는 selang 을 사용하여 사용자 암호를 설정하거나 변경하면 eTrust AC 는 데이터베이스에 암호를 추가하기 전에 암호 규칙을 검사하지 않습니다. eTrust AC 는 이러한 기능으로 입력한 모든 암호를 허용합니다. 따라서 새 암호는 eTrust AC 암호 규칙에 유효하지 않을 수 있습니다. Windows 사용자 관리자를 사용하거나 eTrust AC 가 아닌 다른 소프트웨어를 사용하여 암호를 변경하면 eTrust AC 는 새 암호의 유효성을 검사합니다.

암호 관리 및 잠금 정책

암호는 인증에 가장 많이 사용되는 장치이지만 암호 보호 방법에는 다음과 같이 잘 알려진 문제점이 있습니다. 흔한 암호는 쉽게 추측할 수 있고 수 년간 사용한 암호나 주기적인 암호는 결국 해킹되며 네트워크를 통해 일반 텍스트 형태로 전송된 암호는 수신기에 의해 트랩될 수 있습니다.

Windows 에는 이와 같은 일반적인 위험을 방지하기 위해 사용자가 암호를 사용하는 경우 지켜야 하는 일련의 암호 규칙과 정책이 있습니다. eTrust AC 에는 추가 규칙을 통해 사용자가 더욱 안전한 암호를 선택할 수 있도록 합니다.

eTrust AC 에서 지정할 수 있는 규칙은 다음과 같습니다.

- 새 암호는 이전 암호와 동일할 수 없습니다. eTrust AC 가 저장하는 기존 암호의 개수는 암호 정책에서 지정됩니다.
- 새 암호에는 사용자 이름이 들어갈 수 없습니다.
- 새 암호는 변경 중인 암호를 포함할 수 없습니다.
- 새 암호는 바꾸려는 현재 암호와 같을 수 없습니다. eTrust AC 는 대소문자 구분을 무시합니다.
- 새 암호에는 암호 정책에서 지정된 최소 영숫자, 특수 문자, 숫자, 소문자 및 대문자를 사용해야 합니다.
- 새 암호에는 암호 정책에서 지정된 수보다 많은 반복 문자가 나올 수 없습니다.
- 새 암호는 eTrust AC 에 포함된 사전에 제한된 단어 중 하나가 될 수 없습니다. 사전은 레지스트리 하위 키의 사전값에 지정되어 있습니다.

  `HKEY_LOCAL_MACHINE\Software\ComputerAssociates\eTrustAccessControl\passwd`

각 암호에는 최대 수명이 있어야 합니다. 즉, 사용자가 특정 간격 이후 새 암호를 선택하도록 암호가 만료되어야 합니다.

- 각 암호에는 최소 수명이 있어야 합니다. 최소 수명을 지정하여 사용자가 자주 반복적으로 암호를 변경하는 것을 금지할 수 있습니다. 자주 변경되는 암호의 경우 암호 기록 스택을 오버플로하여 기존 암호를 다시 사용할 수 있습니다.

암호 관리자 사용

암호 관리자가 스테이션에 설치된 경우, 이 프로그램을 사용하여 새 암호를 설정하거나 기존 암호를 변경할 수 있습니다.

암호를 설정하거나 변경할 때 다음 작업을 수행할 수 있습니다.

- 사용자가 다음 번에 로그온할 때 암호를 변경하라고 요구합니다.
- 사용자가 더 이상 잠금되지 않도록 잠금된 사용자 계정을 재설정합니다.
- 원격 호스트의 사용자, 로컬 호스트 PMDB 의 사용자 또는 원격 호스트 PMDB 의 사용자에 대해 암호를 설정할 수 있도록 대상 호스트를 변경합니다. 기본적으로 eTrust AC 는 사용자가 로컬 호스트에 있는 것으로 가정합니다.
- 조직의 암호 정책에 맞는 사용자 암호를 생성하도록 eTrust AC 를 구성합니다.
- 암호를 변경한 사용자에게 전자 메일을 전송하여 새 암호를 통지하도록 eTrust AC 를 구성합니다.

암호 생성

암호 관리자에서 기존 사용자를 위해 암호를 생성할 수 있습니다. eTrust AC 가 생성한 암호는 사이트에 대해 설정한 기준에 항상 일치합니다. 암호를 생성하려면 시스템 옵션으로 [암호 생성 사용 가능]을 선택해야 합니다. 기본적으로 암호 생성 옵션이 선택됩니다.

대상 호스트 변경

로컬 호스트 PMDB 의 사용자, 원격 호스트의 사용자 또는 원격 호스트 PMDB 의 사용자에 대해 암호를 설정할 수 있도록 대상 호스트를 변경할 수 있습니다.

사용자 암호 변경 설정

정책 관리자에서는 사용자에게 암호 변경 시기를 알리도록 기능을 설정할 수 있습니다. 사용자가 정책 관리자에 로그인하면 암호 변경 시기를 알려주는 대화 상자가 나타납니다. [예]를 클릭하면 [암호 변경] 대화 상자가 나타납니다.

이 기능을 설정하려면, 다음 단계를 완료하십시오.

1. [Access Control] 프로그램 표시줄에서 [리소스] 아이콘을 클릭합니다.
2. [도구] 메뉴에서 [eTrust 클래스 활성화]를 선택합니다. [암호] 상자와 [고유 암호 변경] 상자를 선택합니다.
3. [확인]을 클릭합니다.

오류 메시지 확인

Windows NT 시스템에서 사용자 암호를 설정하는 경우, 다음 메시지가 나타날 수 있습니다.

암호가 요구된 것보다 짧습니다.

이 오류는 암호가 정책 요구사항에 맞지 않는다는 의미입니다. 오류 발생 원인은 다음 중 하나입니다.

- 암호가 필요한 길이보다 짧거나 깁니다.
- 최근에 사용된 적이 있으며 Windows NT 변경 내역 필드에 존재하는 암호입니다.
- 암호의 고유 문자가 부족합니다.
- 암호가 다른 암호 정책 요구 사항(예: eTrust AC 암호 정책에 따라 설정된 요구 사항)에 일치하지 않습니다.

이 오류를 방지하려면, 적용되는 모든 요구사항에 적합한 암호를 설정해야 합니다.

제 5 장: 계정 보호

이 장은 아래의 주제를 포함하고 있습니다:

사용자 가장 요청 보호

계정이 로그인한 후 시스템 리소스에 대한 권한이 있는 기능만 수행하는지 모니터해야 합니다. 운영 체제는 액세서의 사용자 SID 를 기반으로 파일에 대한 어느 정도의 보호를 제공합니다. 그러한 보호 기능을 통과하려면 사용자는 먼저 다른 사용자의 SID 로 가장해야 합니다. 운영 체제는 요청 사용자에게 대상 사용자의 암호를 지정하도록 요청함으로써 권한 없는 가장으로부터 보호합니다.

이러한 구성에는 오류가 많습니다. 자신을 사용자 SID 로 가장하려는 사용자는 대상 사용자의 암호를 기억하여 기록하거나 대상 사용자에게 일반적인 암호를 사용할 것을 요청해야 합니다. 이것은 여러 암호 정책에 위반되며 책임 소재도 확인할 수 없습니다. 특정 사용자의 ID 를 변경한 사용자가 누구인지 알 수 없기 때문입니다. 또한 수퍼유저 암호가 사용자에게 알려지면 모든 보안이 무시되어 이 사용자가 어떠한 제한도 받지 않고 시스템에 액세스할 수 있습니다.

eTrust AC 는 가장으로부터 보호하기 위해 보다 향상된 방법을 사용합니다. 사용자는 지정된 규칙에서 변경을 허용할 경우에만 사용자 SID 를 다른 사용자의 SID 로 변경할 수 있습니다.

예를 들어, 사용자 X 가 사용자 Y 로서 일부 작업을 수행하는 프로그램을 실행한다고 가정할 때 사용자 X 는 사용자 Y 의 암호를 가지고 있지만 사용자 Y 로 대체할 수 있는 권한이 없으므로, 프로그램 요청은 거부됩니다.

이 방법을 사용하면 침입자는 관리자의 암호만 가지고 침입할 수 없으며, 침입자가 관리자가 될 수 있도록 허용하는 데이터베이스의 규칙이 있어야 합니다.

각 사용자 SID 및 그룹 SID 의 경우 데이터베이스에 액세스 규칙을 포함할 수 있습니다. eTrust AC 는 이 보호 유형에 SURROGATE 클래스를 할당합니다. 초기 단계에 모든 가장 요청에 대한 액세스를 허용하려면, 다음 명령을 사용하십시오.

```
eTrust> editres SURROGATE _default defaccess(READ)
```

이 명령은 eTrust AC 에게 다른 사용자로 자신을 가장할 것을 요청하고 데이터베이스의 레코드가 명시적으로 사용자 대체를 보호하지 않는 경우 액세스를 허용하라고 알려줍니다.

SID 를 수퍼유저의 SID 로 대체하는 것을 방지하려면 다음 명령을 사용하십시오.

```
eTrust> newres SURROGATE USER.Administrator defaccess(NONE)
```

이 명령은 eTrust AC 에게 관리자 사용자 이름이 보호되고 이 이름을 사용하도록 명시적으로 허용되지 않은 사용자는 관리자로 가장할 수 없음을 나타냅니다. 보안 관리자가 관리자를 사용할 수 있도록 하려면 다음 명령을 사용하여 명시적으로 지정해야 합니다.

```
eTrust> authorize SURROGATE USER. Administrator gid("Security Admins")
```

참고:

- 사용자의 SURROGATE 레코드가 특정 사용자의 대체 작업 수행을 허용하지 않는 경우, 사용자는 해당 레코드에 대한 기본 액세스 권한만 가집니다. 이전 예제에서 기본값은 NONE 이고 사용자가 권한 없이 관리자로 가장할 수 없음을 의미합니다.
- USER._default 레코드는 자신의 레코드가 없는 모든 사용자를 나타냅니다. 이와 유사하게 GROUP._default 레코드도 자신의 레코드가 없는 모든 그룹을 나타냅니다. 특정 액세서에 대한 SURROGATE 레코드가 존재하지 않는 경우, 해당 액세서로 대체하기 위한 요청은 SURROGATE USER._default 레코드에서 지정한 기본값이나 SURROGATE GROUP._default 레코드 또는 (사용자와 그룹 모두일 경우) _default 레코드로 종료됩니다.
- _default 레코드에 대한 기본값은 READ 로, 정의되지 않은 SURROGATE 레코드가 해당 사용자로 가장할 수 있는 권한을 의미합니다. 이 기본값은 구현 시 "eTrust AC 에 정의되지 않은 것은 eTrust AC 에서 보호하지 않는다."라는 기본 규칙을 준수하며, 이는 "eTrust AC 에서 허용되지 않는 것은 eTrust AC 에 의해 자동으로 금지된다"는 반대 규칙을 구현한 후에 수정할 수 있습니다.
- 대부분의 Windows 유틸리티와 서비스(예: [다음 계정으로 실행])는 이를 실행하는 원래 사용자가 아니라 "NT AUTHORITY\SYSTEM"으로 식별합니다. 이러한 유틸리티와 서비스를 사용하는 사용자가 다른 사용자를 가장하도록 하려면 eTrust AC 데이터베이스에 이 SYSTEM 사용자를 작성하고 대상 사용자를 가장하도록 권한을 부여해야 합니다. 예:

  ```
  auth SURROGATE USER.Administrator uid("NT AUTHORITY\SYSTEM") acc(R)
  ```

Surrogate DO 기능 설정

작업자, 생산 직원 및 최종 사용자가 수퍼유저만 수행할 수 있는 작업을 수행해야 하는 경우가 있습니다.

기존의 접근 방식은 이러한 모든 사용자에게 수퍼유저 암호를 제공하는 것이었지만 이 경우 사이트의 보안이 위협을 받게 됩니다. 암호의 보안을 유지하는 대체 보안 방법을 사용하면 사용자의 일상적인 작업 수행 관련 요청으로 인해 시스템 관리자의 업무량이 늘어납니다.

Surrogate DO(sesudo) 유틸리티로 이 문제를 해결할 수 있습니다. 이 유틸리티로 사용자는 작업(SUDO) 클래스에 정의된 동작을 수행할 수 있습니다. 작업(SUDO) 클래스의 각 레코드에는 스크립트가 포함되고 스크립트를 실행할 수 있는 사용자와 그룹이 지정되며 목적에 따라 필요한 권한이 부여됩니다.

예를 들어, 사용자가 System 역할을 수행하여 "Print Spooler" 서비스를 시작하는 SUDO 리소스를 정의하려면 다음 명령을 입력하십시오.

```
eTrust> newres SUDO StartSpooler data("net start spooler")
```

newres 명령은 StartSpooler 를 일부 사용자가 해당 System 권한을 가질 수 있는 보호된 작업으로 정의합니다.

중요! 데이터 속성에서 전체 절대 경로 이름을 사용하십시오. 상대 경로 이름을 사용하면 보호되지 않은 디렉터리에 있는 트로이 목마 프로그램이 실수로 실행될 수 있습니다.

또한 사용자는 authorize 명령을 사용하여 StartSpooler 작업을 수행할 수 있는 권한을 가질 수 있습니다. 예를 들어, *operator1* 사용자가 "Print Spooler" 서비스를 시작할 수 있게 하려면 다음 명령을 입력하십시오.

```
eTrust> authorize SUDO StartSpooler uid(operator1)
```

또한 authorize 명령을 사용하여 사용자가 보호된 작업을 수행할 수 없도록 할 수 있습니다. 예를 들어, *operator2* 사용자가 "Print Spooler" 서비스를 시작하는 것을 방지하려면 다음 명령을 입력하십시오.

```
eTrust> authorize SUDO StartSpooler uid(operator2) access(None)
```

sesudo 유틸리티를 실행하면 보호된 작업이 수행됩니다. 예를 들어, *operator1* 사용자는 다음 명령을 사용하여 "Print Spooler" 서비스를 시작합니다.

```
cmd> sesudo -do StartSpooler
```

sesudo 유틸리티는 처음에는 사용자가 SUDO 작업을 수행할 수 있는 권한이 있는지 여부를 확인한 다음 사용자가 리소스에 대한 권한이 있는 경우 리소스에 정의되어 있는 명령 스크립트를 실행합니다. 위의 예제에서 sesudo 는 operator1 이 StartSpooler 작업을 수행할 수 있는 권한이 있는지 확인한 후 System 자격 증명으로 "net start spooler" 명령을 호출합니다.

참고: sesudo 유틸리티에 대한 자세한 내용은 *유틸리티 가이드*를 참조하십시오. SUDO 레코드의 데이터 속성 형식 지정에 대한 자세한 내용은 *참조 가이드*의 chres, editres 및 newres 명령을 참조하십시오.

사용자 비활성 확인

비활성 기능을 사용하면 조직에 더 이상 소속되지 않은 소유자의 계정으로 시스템에 무단 액세스하는 것을 금지할 수 있습니다. [비활성 일]은 사용자가 로그인하지 않은 날입니다. 사용자 계정이 일시 중단되거나 로그인할 수 없게 되기 전에 경과해야 하는 비활성 날짜 수를 지정할 수 있습니다. 계정이 일시 중단되면 수동으로 다시 활성화해야 합니다.

참고: 비밀번호 변경은 비활성 검사에 의해 활동으로 간주됩니다. 사용자의 암호가 변경되면 해당 사용자는 비활성이 되기 때문에 일시 중단할 수 없습니다.

USER 클래스 레코드 또는 GROUP 클래스 레코드의 비활성 속성으로 비활성 기간의 일 수를 설정할 수 있습니다. GROUP 클래스 레코드는 그룹을 프로파일 그룹으로 가지는 사용자에게만 영향을 미칩니다. SEOS 클래스의 INACT 속성으로 전체 시스템에서 모든 사용자에 대한 비활성을 설정할 수도 있습니다.

selang 및 보안 관리자는 모두 비활성을 설정할 수 있는 방법을 제공합니다. selang 에서 다음 명령을 사용하여 비활성을 전체적으로 지정하십시오.

```
setoptions inactive ( numdays)
```

그룹에 대한 전체 시스템의 비활성 설정을 재지정하는 그룹에 대한 총 일 수를 설정하려면 다음 명령을 사용하십시오.

```
{chgrp | editgrp | newgrp} groupName inactive ( numdays)
```

사용자에 대한 그룹 및 전체 시스템 설정을 재지정하는 사용자에 대한 총 일 수를 설정하려면 다음 명령을 사용하십시오.

```
{chusr | editusr | newusr} userName inactive ( numdays)
```

일시 중지된 사용자 계정을 다시 활성화하려면 다음 명령을 사용하십시오.

```
{chusr | editusr} userName resume
```

일시 중지된 프로파일 그룹을 다시 활성화하려면 다음 명령을 사용하십시오.

```
{chgrp | editgrp} userName resume
```

전체 시스템 수준에서 비활성 로그인 검사를 비활성화하려면 다음 명령을 사용하십시오.

```
setoptions inactive-
```

그룹에 대한 비활성 로그인 검사를 비활성화하려면 다음 명령을 사용하십시오.

```
{chgrp | editgrp} groupName inactive-
```

사용자에 대한 비활성 로그인 검사를 비활성화하려면 다음 명령을 사용하십시오.

```
{chusr | editusr} userName inactive-
```

제 6 장: 중앙에서 정책 관리

이 장은 아래의 주제를 포함하고 있습니다:

정책 모델 데이터베이스

수십 또는 수백 개의 데이터베이스를 개별적으로 관리하는 것은 실용적이지 않습니다. eTrust AC 는 하나의 중앙 데이터베이스에서 여러 데이터베이스를 관리할 수 있는 구성 요소인 정책 모델 서비스를 제공합니다. 정책 모델(PMD) 서비스를 사용하는 것은 선택 사항이지만 큰 사이트에서 이 서비스를 사용하면 관리 작업이 상당히 간단합니다.

참고: Windows 작업 관리자에서 정책 모델 서비스는 sepmdd.exe 로 나타납니다.

정책 모델 서비스에서는 정책 모델 데이터베이스(PMDB)를 사용합니다. 다른 eTrust AC 데이터베이스와 달리 PMDB 에는 사용자, 그룹, 보호된 리소스, 리소스에 대한 액세스를 제어하는 규칙 등이 포함됩니다. 또한 PMDB 에는 *구독자* 데이터베이스 목록이 포함합니다. 각 구독자는 별도의 컴퓨터에 있는 eTrust AC 데이터베이스나 동일한 컴퓨터 또는 다른 컴퓨터에 있는 다른 PMDB 입니다. 구독자를 업데이트하는 PMDB 를 구독자의 *상위*라고 합니다.

PMDB 는 권한 제한 및 액세스 규칙이 유사한 여러 데이터베이스를 관리하는 데 유용한 도구입니다.

참고: sepmd 유틸리티를 사용하여 PMDB 를 관리하는 방법과 PMDB 를 원격으로 관리하는 방법에 대한 자세한 내용은 *참조 가이드*를 참조하십시오.

디스크에서 PMDB 의 위치

컴퓨터에 있는 모든 PMDB 는 공용 디렉터리에 위치합니다. Windows 레지스트리의 다음 하위 키에서 _pmd_directory_ 값은 디렉터리의 이름을 지정합니다.

```
HKEY_LOCAL_MACHINE\Software\ComputerAssociates\eTrustAccessControl\Pmd
```

NTFS 루트 디렉터리에서 _pmd_directory_의 기본값은 *eTrustACDir*\data 입니다. 여기서 *eTrustACDir* 는 eTrust AC 의 설치 디렉터리이며, 기본적으로 C:\Program Files\CA\eTrustAccessControl 입니다.

각 PMDB 는 공용 디렉터리의 하위 디렉터리를 사용합니다. 하위 디렉터리의 파일에는 정책 모델을 정의하는 데 필요한 데이터가 모두 들어 있습니다. 정책 모델 구성 설정은 eTrust AC 레지스트리 설정의 Pmd 하위 키에 저장됩니다. 하위 키의 이름은 정책 모델 이름입니다.

로컬 PMDB 관리

eTrust AC 에서는 PMDB 를 관리하기 위한 다음과 같은 유틸리티를 제공합니다.

sepmd

다음을 수행할 수 있는 PMDB 관리 유틸리티입니다.

- 가입자 관리
- 업데이트 파일 잘라내기
- 관리자 이중 제어
- 정책 모델 로그 파일 관리
- 기타 관리 작업 수행

참고: sepmd 에 대한 자세한 내용은 *참조 가이드*를 참조하십시오.

원격 PMDB 관리

eTrust AC 는 또한 pmd 환경에서 사용할 수 있는 여러 selang 명령을 제공합니다. 다음 명령을 사용하여 PMDB 를 원격으로 관리할 수 있습니다.

createpmd

PMDB 를 작성합니다.

deletepmd

PMDB 를 삭제합니다.

findpmd

컴퓨터에 있는 모든 PMDB 이름을 표시합니다.

listpmd

PMDB 에 대한 다음 정보를 나열합니다.

- 구독자 및 구독자 상태
- PMDB 에 대한 설명 및 PMDB 상태
- 업데이트 파일의 명령과 해당 오프셋
- 오류 로그의 내용

pmd

다음을 수행할 수 있는 PMDB 관리 명령입니다.

- 사용할 수 없는 구독자 목록에서 구독자 제거
- 정책 모델 오류 로그 지우기
- 정책 모델 서비스 시작 및 중지
- 업데이트 파일 잘라내기
- 레지스트리 설정 다시 로드

subs

다음을 수행할 수 있는 PMDB 구독 명령입니다.

- 상위 PMDB 에 구독자 추가
- 데이터베이스(eTrust AC 또는 다른 PMDB)에 상위 PMDB 할당

subspmd

로컬 데이터베이스에 상위 PMDB 를 할당합니다.

unsubs

PMDB 에서 구독자를 제거합니다.

참고: pmd 환경에서 사용할 수 있는 selang 명령에 대한 자세한 내용은 *참조 가이드*를 참조하십시오.

아키텍처 종속성

eTrust AC 를 배포할 때는 사용자 환경의 계층 구조를 고려해야 합니다. 많은 사이트에서 네트워크는 다양한 아키텍처를 포함합니다. 트러스트된 프로그램 목록과 같은 일부 정책 규칙은 아키텍처에 따라 다릅니다. 반면 대부분의 규칙은 시스템 아키텍처와 관련이 없습니다.

계층을 사용하여 두 종류 규칙 모두를 포함할 수 있습니다. 아키텍처와 관련되지 않은 규칙에 대해 전역 데이터베이스를 정의하고 이 데이터베이스에 아키텍처에 따라 달라지는 규칙을 정의하는 구독자 PMDB 를 지정할 수 있습니다.

참고: 루트 PMBD 와 모든 구독자는 사용자 환경의 실제 필요에 따라 같은 컴퓨터나 개별 컴퓨터에 있을 수 있습니다.

예: 두 개 계층으로 이루어진 배포 계층 구조

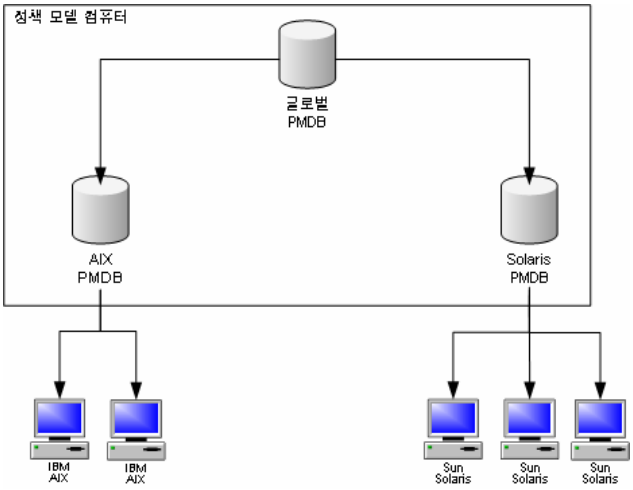
다음 UNIX 예제는 약간만 수정하면 Windows 아키텍처에도 적용됩니다.

이 예에서 사이트는 IBM AIX 및 Sun Solaris 시스템으로 구성됩니다. IBM AIX 의 트러스트된 프로그램 목록이 Sun Solaris 의 트러스트된 프로그램 목록과 다르기 때문에 PMDB 는 아키텍처 종속성을 고려해야 합니다.

다중 아키텍처 PMDB 를 설정하려면 PMDB 를 다음과 같이 설정하십시오.

1. 이름이 whole_world 인 PMDB 를 정의하여 사용자, 그룹 및 기타 아키텍처 독립적인 모든 정책을 포함합니다.
2. 이름이 pm_aix 인 PMDB 를 정의하여 IBM AIX 고유의 모든 규칙을 포함합니다.
3. 이름이 pm_sol 인 PMDB 를 Sun Solaris 고유의 모든 규칙을 포함하도록 정의합니다.

   pm_aix 및 pm_solaris PMDB 는 whole_world PMDB 의 구독자입니다. 사이트의 모든 IBM AIX 컴퓨터는 pm_aix 의 구독자입니다. 사이트의 모든 Sun Solaris 컴퓨터는 pm_sol 의 구독자입니다. 이 개념은 다음 차트에 설명되어 있습니다.



4. 사용자 추가 또는 SURROGATE 규칙 설정과 같은 플랫폼에 독립적인 명령을 whole_world 에 입력하면 사이트의 모든 데이터베이스가 자동으로 업데이트됩니다.
5. pm_aix 에 트러스트된 프로그램을 추가하면 IBM AIX 컴퓨터만 업데이트되고 Sun Solaris 시스템에는 영향을 주지 않습니다.

중앙에서 정책을 관리하기 위한 방법

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

- 자동 규칙 기반 정책 업데이트

  PMDB 에서 정의한 일반 규칙은 자동으로 구성된 계층의 데이터베이스에 전파됩니다.

  참고: 이중 제어는 이 방법에만 사용할 수 있으며 UNIX 에서만 사용할 수 있습니다.

- 고급 정책 관리 및 보고

  사용자가 배포하는 정책 즉, 규칙 그룹은 구성된 계층 구조 내의 모든 데이터베이스에 전파됩니다. 또한 정책을 배포 취소(제거)하거나 배포 상태, 배포 편차 및 배포 계층에 대한 보고서를 작성할 수도 있습니다. 이 기능을 사용하려면 추가 구성 요소를 설치하고 구성해야 합니다.

참고: 고급 정책 관리 및 보고에서는 자동 규칙 기반 정책 업데이트와 함께 사용할 수 없는 추가 기능을 제공합니다. 그러나 고급 정책 관리를 사용하려면 먼저 자동 규칙 기반 정책 업데이트에 맞게 환경을 구성해야 합니다.

자동 규칙 기반 정책 업데이트

중앙 데이터베이스에서 만든 단일 규칙 정책 업데이트(일반 selang 규칙)은 자동으로 구독자 데이터베이스에 전파됩니다. 동일한 데이터베이스에 여러 컴퓨터를 구독하고 데이터베이스를 서로 구독하여 계층을 작성할 수 있습니다. 설치 후 자동 규칙 기반 정책 업데이트에 맞게 환경을 구성해야 합니다.

참고: 이러한 정책 관리 방법에서는 계층 간에 단일 규칙 정책 업데이트만 만들 수 있습니다. 고급 정책 관리 및 보고 (페이지 87)를 구현해야만 다른 기능을 사용할 수 있습니다.

자동 규칙 기반 정책 업데이트의 작동 방법

자동 규칙 정책 업데이트에 맞게 환경을 구성하면 중앙 데이터베이스에서 정의하는 각 규칙이 다음과 같은 방법으로 모든 구독자에게 자동으로 전파됩니다.

1. 하나 이상의 구독자가 있는 모든 PMDB 에 대해 규칙이 정의됩니다.
2. PMDB 에서 모든 구독자 데이터베이스에 명령을 보냅니다.
3. 구독자 데이터베이스에서 전파된 명령을 적용합니다.
   a. 구독자 데이터베이스가 응답하지 않는 경우 PMDB 는 구독자 데이터베이스가 업데이트될 때까지 일정한 간격(기본값: 30 분마다)으로 명령을 보냅니다.
   b. 구독자 데이터베이스가 응답하지만 명령 적용을 거부하는 경우 PMDB는 해당 명령을 정책 모델 오류 로그 (페이지 84)에 기록합니다.
4. 구독자 데이터베이스가 다른 구독자의 상위인 경우 해당 구독자에 명령을 보냅니다.

예: 계층에 있는 모든 컴퓨터에서 사용자 제거

rmusr 명령을 사용하여 PMDB 에서 사용자를 삭제하면 동일한 rmusr 명령이 모든 구독자 데이터베이스에 보내집니다. 이런 방법으로 하나의 rmusr 명령을 통해 여러 컴퓨터의 많은 데이터베이스에서 사용자를 제거할 수 있습니다.

계층을 설정하는 방법

eTrust AC 에서는 정책 모델 서비스를 사용하여 규칙 기반 정책 업데이트를 구성된 계층 간에 전파합니다. 동일한 PMDB 에 여러 eTrust AC 컴퓨터를 구독하고 PMDB 를 서로 구독하여 계층을 작성할 수 있습니다.

PMDB 계층을 설정하는 가장 간단한 방법은 eTrust AC 를 설치하면서 설정하는 것이므로, 설치를 시작하기 전에 계층을 어떻게 구성할지 미리 생각해 두는 것이 좋습니다. 상위 PMDB 와 해당 구독자는 서로 통신할 수 있어야 하므로 PMDB 계층의 모든 호스트가 동일한 네트워크에 속해 있는지 확인하십시오. 즉, 상위 PMDB 는 이름을 통해 구독자와 연결할 수 있어야 하며, 모든 구독자는 이름을 통해 상위 PMDB 와 연결할 수 있어야 합니다.

참고: eTrust AC 설치에 대한 자세한 내용은 *구현 가이드*를 참조하십시오.

설치 중에 작성한 구성을 변경하거나 설치 중에 PMDB 구조를 작성하지 않은 경우, 언제든지 PMDB 구성을 변경하거나 작성할 수 있습니다. 다음 방법 중 하나를 사용하여 이 작업을 수행할 수 있습니다.

- 정책 관리자 사용
- sepmd 유틸리티 사용

설치 후 PMDB 계층을 작성하고 자동 규칙 기반 정책 업데이트를 활성화하려면 다음 작업을 수행합니다.

1. 마스터 PMDB 를 작성하고 구성합니다.
2. (선택 사항)구독자 PMDB 를 작성하고 구성합니다.
3. *끝점*이라고 하는 구독 컴퓨터의 상위 PMDB 를 정의합니다.

구독자 업데이트

구독자를 업데이트할 때 정책 모델에서는 다음 작업을 수행합니다.

1. 정책 모델은 구독자 이름이 정책 모델에서 추가되거나 삭제될 때 구독자 이름을 정규화하려고 시도합니다.
2. PMDB 서비스 sepmdd 에서 구독자 데이터베이스를 업데이트하려고 시도합니다.
3. 최대 시간이 경과했는데도 서비스에서 구독자를 업데이트하지 못한 경우에는 해당 구독자를 건너뛰고 목록의 나머지 구독자를 업데이트합니다.
4. 구독자 목록의 최초 검사를 완료하면 sepmdd 는 두번째 검사를 수행합니다. 여기서는 첫번째 검사에서 업데이트에 실패한 구독자를 업데이트하려고 시도합니다.

참고: PMDB에서 구독자에게 업데이트를 전파하는 동안 오류가 발생하면 sepmdd 서비스는 정책 모델 오류 로그 파일 (페이지 84)에 항목을 작성합니다. 이 ERROR_LOG 파일은 PMDB 디렉터리 (페이지 74)에 있습니다.

정책 모델 데이터베이스 업데이트

PMDB 가 있는 컴퓨터에서 작업할 때 PMDB 가 자동으로 업데이트되지는 않습니다. PMDB 를 업데이트하려면 해당 PMDB 를 대상 데이터베이스로 지정해야 합니다.

정책 관리자 또는 selang 을 사용하여 PMDB 를 지정할 수 있습니다. selang 을 사용하여 대상 데이터베이스를 지정하려면 selang 명령 셸에서 hosts 명령을 사용합니다.

```
eTrustAC> hosts <pmd_name>@<pmd_host>
```

이제 모든 selang 명령으로 지정한 정책 모델 데이터베이스가 업데이트됩니다. 그런 다음 명령이 이 컴퓨터와 모든 구독자 컴퓨터의 활성 데이터베이스에 자동으로 전파됩니다.

참고: 정책 관리자에 대한 자세한 내용은 *정책 관리자 온라인 도움말*을 참조하십시오.

예: 대상 PMDB 지정

myPMD_host 에서 대상 데이터베이스를 policy1 로 설정하려면 다음 명령을 사용합니다.

```
eTrustAC> hosts policy1@myPMD_host
```

이제 newusr 명령을 입력하면 새 사용자가 이 컴퓨터와 모든 구독자 컴퓨터의 활성 데이터베이스뿐 아니라 policy1 데이터베이스에도 추가됩니다.

업데이트 파일 정리

sepmd 유틸리티는 <pmd.ini> 파일에 받은 각 업데이트를 자동으로 씁니다. 이 파일이 지나치게 커지지 않게 하려면 파일에서 처리된 업데이트를 정기적으로 삭제하는 것이 좋습니다.

업데이트 파일을 정리하려면 다음 명령을 사용합니다.

```
<eTrustAC_InstallDir>/bin sepmd -t pmdbName auto
```

sepmd 는 전파되지 않은 첫 번째 업데이트 항목의 오프셋을 계산하여 그 이전의 모든 업데이트 항목을 삭제합니다.

암호 전파 및 동기화

PMDB 계층을 설정한 후에는 이 계층을 사용하여 Windows 사용자 관리자를 사용하거나 eTrust AC 이외의 소프트웨어를 사용하여 사용자 암호가 변경될 때 사용자 암호가 시스템 전체에서 동기화되도록 할 수 있습니다.

참고: eTrust AC에서는 메인프레임 암호 동기화 (페이지 145)도 지원합니다.

암호를 전파하고 동기화하려면

1. PMDB 계층을 작성합니다.
2. 사용자 또는 관리자가 암호를 변경할 수 있는 모든 스테이션의 레지스트리에서 passwd_pmd 항목 값으로 해당되는 상위 PMDB 의 이름을 입력합니다.

   HKEY_LOCAL_MACHINE\Software\ComputerAssociates\eTrustAccessControl\ eTrustAccessControl\passwd_pmd

   그러면 PMDB 가 모든 PMDB 의 구독자에게 암호 변경사항을 전파합니다. passwd_pmd 값이 비어 있을 경우, eTrust AC 는 secondary_pmd 값을 확인하고 이 값이 비어 있지 않으면 이 값에 나열된 PMDB 로 새 암호화 업데이트된 암호를 전송합니다.

참고: PMDB 가 사용자를 정의하지 않은 구독자에게 사용자 암호를 전송할 경우, 설정은 변경되지 않으며 구독자에 대해 사용자를 정의하지 않은 상태가 유지됩니다.

구독자 제거

특정 구독자에 더 이상 업데이트를 전파하지 않으려면 해당 구독자를 제거해야 합니다.

구독자를 제거하려면

1. 구독자 목록에서 컴퓨터를 제거합니다.

   `sepmd -u <PMDB_name> <computer_name>`

   컴퓨터가 정책 모델 구독 목록에서 제거됩니다.

2. 구독 목록에서 제거한 컴퓨터에서 seosd 를 종료합니다.

   `secons -s`

   seosd 서비스가 종료됩니다.

3. 구독 목록에서 제거한 컴퓨터의 다음 레지스트리 키에 있는 parent_pmd 레지스트리 값을 삭제합니다.

   `HKEY_LOCAL_MACHINE\Software\ComputerAssociates\eTrustAccessControl\ eTrustAccessControl`

   컴퓨터에서 더 이상 상위 PMDB 의 업데이트를 받지 않습니다.

4. seosd 를 다시 시작합니다.

   구독 목록에서 제거한 컴퓨터의 활성 데이터베이스는 더 이상 지정한 PMDB 의 구독자가 아닙니다.

참고: 데이터베이스가 PMDB 에서 구독 해제된 경우 PMDB 는 더 이상 명령을 보내지 않습니다.

업데이트 필터링

PMDB 를 통해 다른 구독자 데이터베이스에 있는 다른 데이터 하위 집합을 업데이트하려면 구독자 데이터베이스로 보낼 레코드를 정의해야 합니다.

업데이트를 필터링하려면

1. PMDB 가 subscriber 서브세트의 부모 역할을 하도록 구성합니다.
2. 상위 PMDB 의 레지스트리 키에 있는 *Filter* 레지스트리 항목을 수정하여 같은 컴퓨터에서 설정한 필터 파일을 가리키도록 만듭니다.

   그러면 구독자 데이터베이스에 대한 업데이트가 해당 필터를 통과하는 레코드로 제한됩니다.

정책 모델 필터 파일

필터 파일은 각각 6 개의 필드가 있는 줄로 구성됩니다. 이 필드에는 다음에 대한 정보가 포함되어 있습니다.

- 허용되거나 거부된 액세스 형식.

  예: EDIT 또는 MODIFY

- 영향 받는 환경. 예:

  eTrust, UNIX 또는 Native

- 레코드 클래스.

  예: USER 또는 TERMINAL

- 규칙이 적용되는 클래스 내 개체.

  예를 들어 User1, AuditGroup, 또는 COM2 입니다.

- 레코드가 허용하거나 취소한 속성.

  예를 들어 필터 줄의 OWNER 와 FULL_NAME 은 이러한 속성을 갖는 명령이 필터링된다는 것을 나타냅니다. 각 속성은 *참조 가이드*에 나온 대로 정확히 입력해야 합니다.

- 레코드를 구독자 데이터베이스로 전달해야 하는지 여부.

  PASS 또는 NOPASS

필터 파일의 각 줄에 다음 규칙이 적용됩니다.

- 필드에 별표(*)를 사용하여 가능한 모든 값을 표시할 수 있습니다.
- 두 개 이상의 줄이 동일한 레코드를 포함할 경우, 적용 가능한 *첫 번째* 줄이 사용됩니다.
- 필드는 공백으로 구분합니다.
- 필드에 여러 개의 값이 있는 경우 세미콜론으로 값을 구분합니다.
- #으로 시작하는 줄은 주석 줄로 간주됩니다.
- 빈 줄은 허용되지 않습니다.

예: 필터 파일

다음 예에서는 필터 파일의 행을 설명합니다.

CREATE	eTrust	USER	*	FULL_NAME;OBJ_TYPE	NOPASS
↑	↑	↑	↑	↑	↑
액세스 형식	환경	클래스	레코드 이름 (* =all)	속성	처리

예를 들어, 이 줄이 있는 파일의 이름이 Printer1_Filter.flt 이고 PMDB PM-1 의 레지스트리를 . filter=C:\Program Files\CA\eTrustAccessControl\Printer1_Filter.flt 가 되도록 편집하는 경우 PMDB PM-1 은 FULL_NAME 및 OBJ_TYPE 속성을 사용하여 새 사용자를 작성하는 레코드를 구독자에게 전파하지 않습니다.

정책 모델 오류 로그 파일

정책 모델 오류 로그는 시간순으로 구성되며 다음과 비슷합니다.

오류 텍스트	오류 범주
20 Nov 03 11:56:07 (pmdb1): fargo nu u5 0 Retry 오류: Login procedure failed (10068) 오류: 상위가 아닌 PMDB(pmdb1@name.company.com)에서 받은 업데이트는-수락할 수 없습니다(10104).	구성 오류
20 Nov 03 19:53:17 (pmdb1): fargo nu u5 0 Retry 오류: Connection failed (10071) 호스트에 연결할 수 없습니다.(12296)	연결 오류
20 Nov 03 11:57:06 (pmdb1): fargo nu u5 560 Cont 오류: Failed to create USER u5 (10028) 이미 있습니다(-9) 20 Nov 03 11:57:06 (pmdb1): fargo nu u5 1120 Cont 오류: Failed to create USER u5 (10028) 이미 있습니다(-9)	데이터베이스 업데이트 오류

정책 모델 오류 로그는 이진 형식이기 때문에 다음 명령을 입력해야만 볼 수 있습니다.

<eTrustAC_InstallDir>/bin sepmd -e *pmdname*

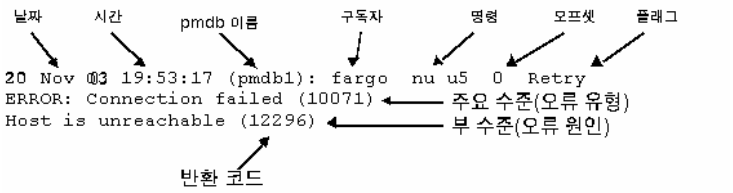
참고: rm 등과 같은 UNIX 명령을 사용하여 오류 로그를 수동으로 삭제하지 마십시오. 로그를 삭제하려면 다음 명령만 사용해야 합니다.

<eTrustAC_InstallDir>/bin sepmd -c *pmdname*

중요! eTrust AC r5.1 보다 최신 버전의 오류 로그는 이전 버전의 형식과 호환되지 않는 형식을 갖습니다. 따라서 sepmd 는 이전 버전의 오류 로그를 처리하지 못합니다. 이 형식의 버전으로 업그레이드하는 경우 이전의 오류 로그는 ERROR_LOG.bak 으로 복사되고 sepmdd 를 시작할 때 새 로그 파일이 생성됩니다.

예: PMDB 업데이트 오류 메시지

다음은 일반적인 오류 메시지의 예입니다.



- 맨 위 행은 항상 날짜, 시간 및 구독자로 구성됩니다. 그런 다음 오류를 생성한 명령과 오프셋(10 진수 형식)을 차례로 표시하여 업데이트 파일 내에서 실패한 업데이트의 위치를 나타냅니다. 마지막으로 PMDB 에서 업데이트를 자동으로 다시 시도할지 여부를 나타내는 플래그가 표시됩니다.
- 두 번째 행에는 기본 수준 메시지(발생 오류 유형) 및 해당 반환 코드의 예가 표시됩니다.
- 세 번째 행에는 보조 수준 메시지(오류가 발생한 이유)와 반환 코드의 예가 표시됩니다.

예: 오류 메시지

명령은 두 개 이상의 오류를 생성하고 표시할 수도 있습니다. 또한 하나의 오류가 기본 수준 메시지 및/또는 보조 수준 메시지로 구성될 수도 있습니다.

다음 오류는 하나의 메시지 수준만 가집니다.

```
Fri Dec 29 10:30:43 2003 CIMV_PROD:릴리스하지 못했습니다. 반환 코드 = 9241
```

이 메시지는 sepmdpull 이 이미 사용 가능한 구독자를 릴리스하려고 할 때 표시됩니다.

기본 정책 모델 저장소

모든 기본 환경 사용자 및 그룹 개체 유형을 PMDB에 저장할 수 있습니다. 이 정보를 PMDB에 저장하면, show user 또는 show group과 같은 show 명령을 사용하여 개체에 대한 정보를 수신할 수 있습니다. 반환된 개체는 Windows 또는 UNIX 구독자에서 정의한 실제 개체의 이미지입니다.

정책 모델에 연결한 후 사용자는 다음 환경을 선택할 수 있습니다.

- eTrust
- 기본
- NT
- UNIX

참고: Native는 Windows 운영 체제에서 작업할 때 Windows와 동일하게 작동하고, UNIX 운영 체제에서 작업할 때는 UNIX와 동일하게 작동합니다.

기본 환경 저장소를 사용하려면, 다음 명령을 사용하십시오.

- selang 프롬프트에 다음 명령을 입력합니다.

  ```
  env NT; find
  ```

  결과 목록에는 모든 기본 환경 개체 유형이 나열됩니다.

  참고: 이러한 개체 유형에 대한 설명은 *참조 가이드*의 Windows 환경 클래스 및 속성을 참조하십시오.

- NT 및 Active Directory USER 속성 목록을 수신하려면 다음 명령을 입력합니다.

  ```
  env NT; ruler user
  ```

- NT 및 Active Directory GROUP 속성 목록을 수신하려면 다음 명령을 입력합니다.

  ```
  env NT; ruler group
  ```

정책 모델이 다른 (상위) 정책 모델의 구독자일 경우, 정책 모델은 전파 과정을 통해 상위 정책 모델로부터 데이터를 수신하고 데이터베이스에 모든 사용자 및 그룹 속성을 저장하여 사용자는 이러한 정보를 확인하고 변경할 수 있습니다.

참고: 자세한 내용은 *참조 가이드*의 sepmd 유틸리티를 참조하십시오.

고급 정책 관리 및 보고

사용자가 작성한 여러 규칙 정책(스크립트 파일)을 저장한 다음 구성된 계층 구조에 배포할 수 있습니다. 이 정책 기반 방법을 사용하여 정책 버전을 저장한 다음 이를 배포하거나 배포 취소할 수 있습니다. 또한 배포 상태, 배포 편차 및 배포 계층 구조에 대한 보고서를 작성할 수도 있습니다.

참고: 이중 제어는 이 방법에 사용할 수 *없으며* UNIX 에서만 사용할 수 있습니다.

환경 아키텍처

고급 정책 관리 및 보고를 사용하려면 다음 추가 구성 요소를 설치 및 구성해야 합니다.

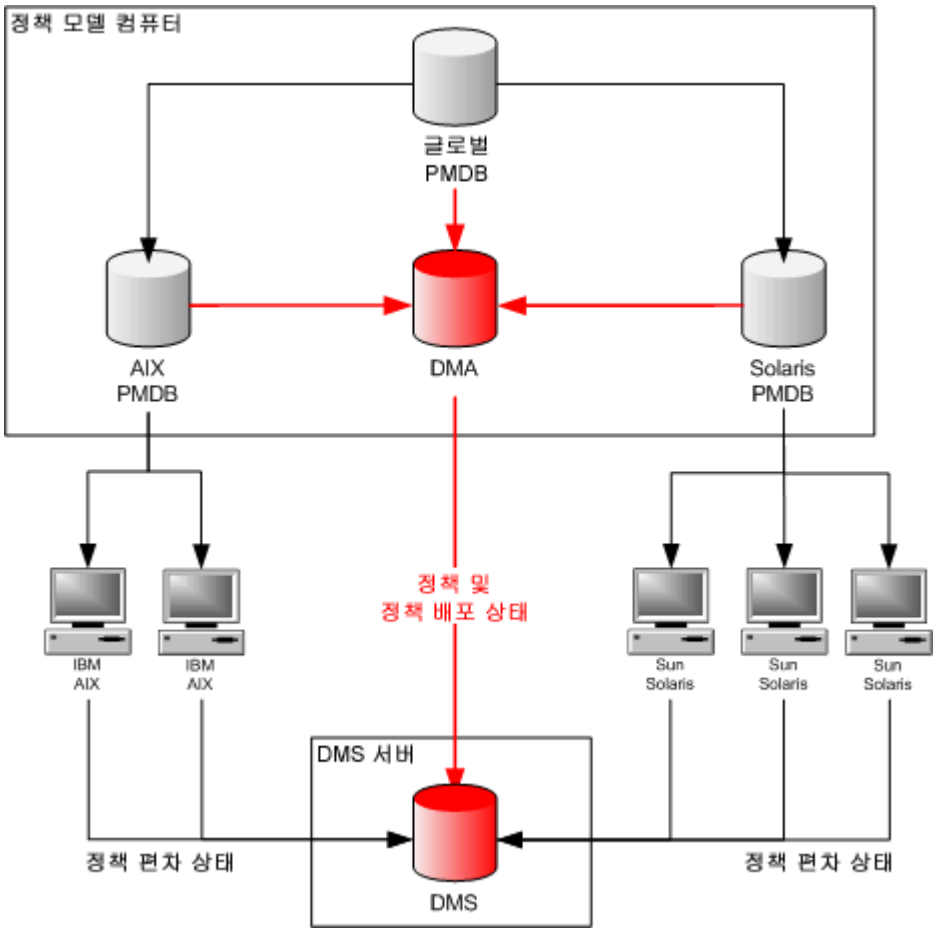
- 중앙 컴퓨터에서 이러한 용도에 사용할 DMS(Deployment Map Server) (페이지 89)
- 각 컴퓨터에서 하나 이상의 PMDB가 있는 DMA(Deployment Map Agent) (페이지 89)

참고: 고급 정책 관리 및 보고를 사용하려면 먼저 자동 규칙 기반 정책 업데이트에 맞게 환경을 설정해야 합니다. 적절한 컴퓨터에 DMS 및 DMA를 설치한 후 상위 및 구독자 데이터베이스를 구성 (페이지 79)합니다.

예: 중앙에 DMS가 있는 두 개 계층으로 이루어진 배포 계층 구조

참고: 다음 UNIX 예제는 약간만 수정하면 Windows 아키텍처에도 적용됩니다.

이 예제에서 사이트는 IBM AIX 및 Sun Solaris 시스템으로 구성됩니다. IBM AIX의 트러스트된 프로그램 목록이 Sun Solaris의 트러스트된 프로그램 목록과 다르기 때문에 PMDB는 아키텍처 종속성을 고려해야 합니다. 관리 및 보고를 위해 DMS 및 DMA를 설정하여 다중 PMDB 환경 (페이지 76)을 구성할 때 작성한 환경을 지원합니다. DMS는 모든 정책 배포 및 편차 정보를 저장하며 eTrust AC에서 이 정보를 사용하여 보고서를 작성할 수 있습니다.



DMS(Deployment Map Server)

DMS 는 고급 정책 관리 및 보고의 핵심이 되는 시스템이며 DMS 의 용도는 eTrust AC 배포 계층 구조와 각 컴퓨터에 배포된 정책 상태의 최신 맵을 유지하는 데 있습니다. 계층 구조 방식의 각 데이터베이스에 연결하는 대신 이 데이터를 중앙 위치에 저장하면 보고서를 생성하는 데 필요한 시간을 줄일 수 있습니다. 또한 DMS 는 나중에 배포하고 필요한 경우 배포 취소할 수 있는 여러 정책 버전을 저장합니다.

DMS 는 PMD 노드이며, 데이터 리포지토리로 PMDB 를 사용합니다. DMS 는 DMS 에 대해 구성되어 있는 각 PMD 노드에서 전송된 알림 데이터를 수집합니다.

DMA(Deployment Map Agent)

DMA 는 DMS 와의 PMD 통신을 담당하는 에이전트입니다. 하나 이상의 PMDB 에서 각 PMD 노드에 DMA 를 설치해야 합니다. 상위 PMDB 의 DMA 는 정책 배포 상태와 계층 변경 사항을 DMS 에 알려 줍니다. 끝점에서는 정책 편차 상태만 DMS 에 직접 보냅니다.

참고: 끝점 컴퓨터에는 DMA 를 설치하지 마십시오.

DMA 에서는 표준 eTrust AC 통신 및 암호화 메커니즘을 사용하여 DMS 와 통신합니다.

참고: DMA\DMS 통신을 활성화하기 위해 DMA 를 DMS 의 상위로 정의할 필요는 없습니다.

고급 정책 관리 클래스

eTrust AC 배포 계층 구조와 각 컴퓨터에 배포된 정책 상태의 최신 맵을 유지하기 위해 DMS 는 특정 eTrust AC 클래스를 사용합니다.

HNODE

각 HNODE 개체는 계층 구조의 노드를 나타냅니다. 이 개체에는 각각 나타내는 특정 노드, 구독자 및 부모 PMDB 에 대한 정보가 저장됩니다. 또한 각 HNODE 개체에는 각 개체가 나타내는 노드에 배포해야 하는 정책 및 각 정책의 상태(배포됨, 배포되었지만 오류 발생 등)에 대한 정보가 저장됩니다.

HNODE 개체의 이름은 다음과 같이 개체가 나타내는 노드의 유형에 따라 달라집니다.

- 끝점의 실제 호스트 이름

  예: myhost.mydomain.com

- PMDB 의 정책 모델 이름

  예: mypmd@hostB.domain.com

POLICY

각 POLICY 개체는 HNODE 계층 구조의 원하는 위치에 배포할 수 있는 정책 버전을 나타냅니다. 이 개체에는 관련된 정책 스크립트가 저장되어 있는 위치(RULESET 개체) 및 정책을 배포해야 하는 노드에 대한 정보가 포함되어 있습니다.

이 개체의 이름은 정책 이름 다음에 접미사로 버전 번호가 지정된 형식(*policy_name#xx*)입니다.

RULESET

각 RULESET 개체에는 정책 버전과 관련된 배포 스크립트와 배포 취소(제거) 스크립트가 모두 저장됩니다.

이 개체의 이름은 각 POLICY 개체 이름에 따라 다릅니다.

참고: 이러한 클래스에 대한 자세한 내용은 *참조 가이드*를 참조하십시오.

고급 정책 기반 관리 및 보고에 대한 계층 구조를 설정하는 방법

eTrust AC 에서는 DMS 를 사용하여 eTrust AC 배포 계층과 각 컴퓨터에 배포된 정책 상태의 최신 맵을 유지합니다. 계층 구조의 각 컴퓨터에 적절한 구성 요소를 설치 및 구성하여 정책 기반 관리 및 보고 기능을 활성화할 수 있습니다.

정책 기반 관리 및 보고를 사용하려면 다음 작업을 수행합니다.

1. 중앙 컴퓨터에 DMS 를 설치합니다.

   DMS 는 eTrust AC 설치 시 설치하거나 dmsmgr 유틸리티를 사용하여 설치할 수 있습니다.

2. 각 PMD 노드에 DMA 를 설치합니다.

   DMA 는 eTrust AC 설치 시 설치하거나 dmsmgr 유틸리티를 사용하여 설치할 수 있습니다.

3. 각 eTrust AC 컴퓨터에 고급 정책 관리 및 보고 기능을 설치합니다.

   이를 통해 정책 편차 상태를 DMS 에 보내는 편차 계산을 구성할 수 있습니다.

4. 계층 구조를 설정 (페이지 79)합니다.

   계층 구조를 설정할 때 계층 구조의 각 노드를 나타내는 HNODE 개체가 DMS 에 추가됩니다.

   중요! 컴퓨터에서 eTrust AC를 제거하거나 PMDB를 삭제해도 HNODE 개체는 그대로 남습니다. 사용되지 않는 개체 노드를 제거 (페이지 93)해야 합니다. 계층 구조에서 데이터베이스의 구독을 취소하면 HNODE 개체는 그대로 유지되지만 이 개체를 상위 노드에 연결하는 링크는 제거됩니다. 이 개체를 제거할 필요는 없지만 이 개체에서는 해당 노드에 이전에 배포된 정책 개체와의 링크를 유지 관리합니다.

참고: DMS 및 DMA 설치와 고급 정책 관리 및 보고 기능 구성에 대한 자세한 내용은 *구현 가이드*를 참조하십시오.

DMS 알림

고급 정책 관리 및 보고를 위한 환경을 구성할 때 계층 구조의 구성 요소에서는 다음 세 가지 영역의 상태 변경 사항을 DMS 에 알려 줍니다.

- 계층 구조 변경.

  구독자(PMD 노드 또는 끝점)가 추가되거나 삭제되는 경우 알림을 보냅니다.

- 정책 배포 및 배포 취소.

  구독자(PMD 노드 또는 끝점)에서 정책이 배포되거나 배포 취소될 때 알림을 보냅니다. 그런 다음 작업 결과(성공, 실패 등)에 따라 정책 상세 정보와 배포 상태가 업데이트됩니다.

- 편차 상태.

  eTrust AC 끝점에서 정책 편차를 계산하고 결과(편차가 있거나 없음)를 보낼 때 알림을 보냅니다.

참고: 계층 구조 변경과 정책 배포 및 배포 취소 알림은 PMD 노드에서만 DMA 가 보내고 편차 상태 알림은 eTrust AC 끝점에서만 편차 계산기가 보냅니다.

계층 구조 및 정책 상태 알림의 작동 방법

DMA 는 DMS 에 계층 구조 변경 및 정책 상태 알림을 보냅니다. DMA 알림은 다음과 같은 방법으로 처리됩니다.

1. DMA 에서는 업데이트 파일에 알림 메시지를 저장합니다.

   이러한 메시지는 계층 구조 변경과 정책 배포 및 배포 취소 알림입니다.

2. DMA 에서 DMS 에 연결합니다.

   - DMS 를 사용할 수 없는 경우 DMA 는 모든 메시지를 성공적으로 보낼 때까지 정기적으로 DMS 와 통신하려고 시도합니다.
   - DMS 를 사용할 수 있는 경우 DMA 는 저장된 알림을 보냅니다.

   참고: 각 DMA 에서는 DMS 와 직접 통신하여 계층 구조를 바이패스하고 종속성을 줄입니다.

3. DMS 는 각 DMA 에서 받은 정보를 나중에 사용하기 위해 저장합니다.

   보고서를 작성할 때마다 eTrust AC 에서는 DMS 의 정보를 검색합니다.

편차 알림 작동 방법

편차 계산기는 eTrust AC에 설치되며 편차를 계산할 끝점에서 로컬로 실행됩니다. 편차 계산기에서는 다음 작업을 수행하고 이와 관련된 알림은 DMS에 보냅니다.

1. 끝점에 selang 명령(start devcalc)을 보내 계산 프로세스가 시작됩니다.

   사용자 지정 스크립트를 사용하여 이 작업을 예약된 시간에 실행하는 것이 좋습니다.

2. 계산이 완료되면 편차 계산기에서 결과를 데이터 파일에 저장합니다.

   이 파일은 *<eTrustAC_Dir>*\data\devcalc\deviation.dat 입니다.

   참고: 보고 유틸리티에서 -dev 옵션을 사용하여 편차 세부 정보를 검색할 수 있습니다. 또는 끝점에서 *get devcalc* 명령을 사용하여 데이터 파일의 내용을 검색할 수도 있습니다.

3. 그런 다음 편차 계산기에서 편차 상태(편차가 있는지 여부)를 DMS에 보냅니다.

   편차(데이터 파일의 내용)는 상태 알림과 함께 보내지 않습니다.

계층 구조에서 사용하지 않는 노드 제거

DMS에서는 계층 구조에 대한 정보를 저장합니다. 컴퓨터에서 eTrust AC를 제거할 때 계층 구조에서 해당 컴퓨터를 제거해도 DMS에는 해당 노드에 대한 참조가 계속 포함되어 있습니다. 정기적인 유지 관리 절차에 따라 DMS에서 이러한 사용되지 않는 노드를 정리하는 것이 좋습니다.

계층 구조에서 사용되지 않는 노드를 제거하려면 DMS 컴퓨터에서 dmsmgr 유틸리티를 실행하여 정기적인 정리 작업을 수행합니다.

```
dmsmgr -dms -cleanup <number_of_days>
```

여기서 *<number_of_days>*는 eTrust AC 노드가 사용할 수 없는 상태로 있을 수 있는 최소 일수입니다.

참고: 또한 DMS 컴퓨터에서 다음 selang 명령을 실행하여 특정 노드를 수동으로 삭제할 수도 있습니다.

```
rr HNODE <HNODE_name>
```

고급 정책 기반 관리의 작동 방법

고급 정책 기반 관리를 통해 정책 버전을 저장, 배포 및 배포 취소하고 나중에 배포 상태, 배포 편차 및 배포 계층 구조에 대한 보고서를 작성할 수도 있습니다. 각 정책은 사용자가 작성한 selang 스크립트 파일 쌍으로 구성됩니다. 첫 번째 스크립트 파일은 *배포 스크립트*라고 하며 정책을 구성하는 selang 명령 세트가 포함되어 있습니다. 두 번째 스크립트 파일은 *배포 취소 스크립트*라고 하며 끝점 데이터베이스에서 정책의 배포를 취소(제거)하는 데 필요한 명령이 포함되어 있습니다.

각 정책은 사용자가 지정한 대상 데이터베이스에 다음 2 단계로 적용됩니다.

1. DMS 에 정책 상세 정보를 저장합니다.

   정책 상세 정보에는 배포 및 배포 취소 스크립트와 동일한 정책의 변형을 감지하는 데 사용되는 자동으로 생성된 정책 서명이 포함됩니다.

   DMS 에 정책 상세 정보를 저장할 수 없는 경우에는 다음 사항을 확인하십시오.

   - DMS 에 대한 터미널 권한이 있는 컴퓨터에서 정책을 저장해야 합니다.
   - DMS 의 POLICY 및 RULESET 클래스에 대한 하위 관리 권한이 있어야 합니다.
   - 구문 오류가 있는 배포 또는 배포 취소 스크립트가 있어서는 안 됩니다.

2. 유틸리티는 자동 버전 제어를 사용하여 정책을 저장합니다.

   DMS 에 이미 정책이 있는지 여부에 따라 유틸리티는 다음 중 *하나*를 수행합니다.

   - DMS 에 정책 이름이 없으면 첫 번째 정책 버전*(policy_name*#01)을 작성합니다.
   - DMS 에 이미 정책 이름이 있는 경우에는 발견된 가장 높은 정책 버전에 한 버전을 높여 새로운 정책 버전을 작성합니다.

3. 저장된 정책 버전을 대상 데이터베이스에 배포합니다.

   저장된 정책을 대상 계층 구조에 배포할 수 없는 경우에는 다음 사항을 확인하십시오.

   - 대상 정책 모델 루트에 대한 터미널 권한이 있는 컴퓨터에서 배포해야 합니다.
   - DMS 및 정책을 배포하려는 계층 구조의 각 데이터베이스의 POLICY, RULESET 및 HNODE 클래스에 대한 하위 관리 권한이 있어야 합니다.
   - 대상 정책 모델 루트 컴퓨터에 하위 관리 권한이 있어야 합니다.
   - 배포 계층 구조의 일부인 호스트에 이미 배포된 것과 동일한 정책 버전이 있어서는 안 됩니다.

4. 각 규칙(배포 스크립트에 지정된 selang 명령)은 대상 데이터베이스에서 실행됩니다.

   특정 데이터베이스에 규칙을 배포할 수 없는 경우 정책이 배포되었지만 오류가 발생한 것(상태: *실패*)으로 간주됩니다.

   이러한 현상은 배포 스크립트에 다음 사항이 포함되어 있는 정책을 호스트에 배포하려는 경우 발생합니다.

   - 실제로 없는 개체에 대한 참조. 예를 들면 다음과 같습니다.

     ```
     cr FILE /does_not_exist comment(123)
     ```

     이러한 이유로 인해 정책 배포 스크립트는 자체 완결적이어야 합니다. 즉, 배포 스크립트는 직접 사용하는 모든 리소스를 작성하도록 구성되어 있어야 합니다.

   - 오류가 발생하는 명령.
   - 사용자가 실행할 수 있는 하위 관리 권한이 없는 명령입니다.

5. 정책 상태가 기록됩니다.

   정책 상태는 배포됨, 배포 취소, 전송됨, 실패(배포되었지만 오류 발생), 대기열에 추가됨, 전송 실패, 서명 실패, 배포 취소 실패(배포 취소되었지만 오류 발생) 또는 알 수 없음 중 하나가 될 수 있습니다.

   참고: 정책을 배포했지만 오류가 발생한 경우에는 정책이 오류와 함께 배포된 컴퓨터에서 로그 파일을 확인해야 합니다.

DMS 에 정책 상세 정보를 저장한 다음 대상 데이터베이스에 배포한 경우 대상 데이터베이스가 PMDB 이면 규칙 기반 정책 자동 업데이트 메커니즘을 사용하여 정책이 계층 구조 전체로 전파됩니다.

계층 구조에 새 가입자를 추가하면 모든 정책이 계층 구조 전체에 전파되고 계층 구조에 노드가 추가되었다는 알림이 DMS 에 전송됩니다.

관리 요구 사항

eTrust AC 가 설치되어 있는 컴퓨터에서 정책 배포 유틸리티(policydeploy)를 실행할 수 있습니다. DMS 에 정책을 저장하거나 계층 구조의 데이터베이스에 정책을 배포하고 배포 취소하려면 사용자와 사용자가 작업하는 컴퓨터에 적절한 사용 권한이 있어야 합니다.

DMS 에 정책을 저장하는 방법

- policydeploy 유틸리티를 실행하는 *컴퓨터*에 DMS 에 대해 터미널 권한(TERMINAL 클래스)이 있어야 합니다.
- *사용자*는 DMS 의 POLICY 및 RULESET 클래스에 대해 하위 관리 권한이 있어야 합니다.

계층 구조 전체에 정책을 배포하고 배포 취소하는 방법

- policydeploy 유틸리티를 실행하는 *컴퓨터*에 대상 정책 모델 루트인 컴퓨터에 대해 터미널 권한(TERMINAL 클래스)이 있어야 합니다.
- *사용자*는 다음 권한이 있어야 합니다.
  - DMS 의 POLICY 및 RULESET 클래스에 대한 읽기 권한과 HNODE 클래스에 대한 하위 관리 권한
  - 정책을 배포하는 계층 구조의 각 데이터베이스에 POLICY, HNODE 및 RULESET 클래스에 대한 하위 관리 권한
  - 정책을 배포하는 계층 구조의 각 데이터베이스에 적절한 하위 관리 권한

    이러한 권한은 해당 각 컴퓨터에 정책을 구성하는 selang 명령을 배포하는 데 필요한 권한입니다.

    예를 들어, 다음과 같이 새 파일 리소스를 작성하는 경우에는 FILE 클래스에 대한 하위 관리 권한이 필요합니다.

    ```
    nr FILE /inetpub/* defaccess(none)
    ```

승인된 정책 버전의 배포 방법

고급 정책 기반 관리를 사용하여 정책의 초안 버전을 저장하고 필요에 따라 검토 및 수정한 다음 승인된 버전을 배포할 수 있습니다.

승인된 정책 버전을 배포하려면 다음 작업을 수행합니다.

1. 정책 버전을 DMS 에 저장합니다.

   정책 버전을 저장한 다음 정책을 검토하고 배포할 수 있습니다.

2. 정책을 검토합니다 (페이지 100).

   POLICY 및 RULESET 개체에 대해 읽기 권한이 있는 사용자는 정책 및 이와 관련된 규칙을 볼 수 있습니다.

3. 필요한 경우 승인된 변경 내용으로 새로운 정책 버전을 저장합니다.

   정책을 업데이트할 때마다 필요한 수정된 정책 배포 및 배포 취소 규칙을 포함하는 새로운 정책 버전을 저장해야 합니다.

4. 승인된 정책 버전을 계층 구조에 배포합니다 (페이지 101).

정책 버전 저장

DMS 에 저장하는 모든 정책에는 자동으로 버전 번호가 지정됩니다. 처음 정책을 저장하면 버전 번호 "01"이 지정됩니다. 예를 들어, 정책 *myPolicy* 를 처음 저장하면 policydeploy 유틸리티는 *myPolicy#01* 이라는 POLICY 개체를 작성합니다. DMS 에 이미 있는 정책을 저장할 때마다 정책의 최신 저장 버전이 한 버전씩 증가하면서 새로운 정책 버전이 작성됩니다. 예를 들어, *myPolicy* 버전을 28 번째 저장하면 policydeploy 유틸리티는 *myPolicy#28* 이라는 POLICY 개체를 작성합니다.

그러면 저장된 정책을 보고 필요한 경우 계층 구조에 배포할 수 있습니다.

정책 버전을 저장하는 방법

1. selang 배포 명령을 사용하여 새 스크립트 파일을 작성합니다.

   이러한 명령은 계층 구조의 각 컴퓨터에 배포할 정책을 구성하는 데 필요한 명령입니다.

   중요! 정책 배포는 사용자 암호를 설정하는 명령을 지원하지 않으므로 배포 스크립트 파일에 이러한 명령을 포함시키지 마십시오. Windows(기본) selang 명령은 지원되지만 편차 보고서에는 표시되지 않습니다.

2. selang 배포 취소 명령을 사용하여 새 스크립트 파일을 작성합니다.

   이러한 명령은 계층 구조의 컴퓨터에서 정책을 배포 취소(제거)하는 데 필요한 명령입니다.

   참고: 정책을 배포 취소할 때 새로운 정책 배포 취소 스크립트를 제공하지 않는 경우 대상 계층 구조에서 정책을 배포 취소할 때 기본적으로 이러한 명령이 사용됩니다.

3. 다음과 같이 -store 옵션을 사용하여 policydeploy 유틸리티를 실행합니다.

   ```
   policydeploy -store name -ds file1 -uds file2 [-dms list]
   ```

   여기서 *name* 은 저장할 정책의 이름을 나타내고, *file1* 은 배포 스크립트 파일의 전체 경로와 이름을 나타내며, *file2* 는 배포 취소 스크립트 파일의 전체 경로와 이름을 나타내며, *list* 는 쉼표로 구분된 DMS 노드 목록(선택적)을 나타냅니다.

   policydeploy 유틸리티가 DMS 에 새로운 버전의 정책을 작성할지 여부를 묻는 메시지를 표시합니다.

   참고: 정책 *이름*에는 정책 버전 번호를 나타내기 위해 예약되고 자동으로 추가되는 #(해시) 문자를 사용할 수 없습니다.

4. y 를 입력하여 이 작업을 확인합니다.

   policydeploy 유틸리티가 DMS 에 새로운 버전의 정책을 작성합니다.

예: IIS 5 보호 정책 저장

다음 예에서는 IIS(Internet Information Services) 5 웹 서버의 보안을 위한 정책을 저장하는 방법을 설명합니다. 이 과정은 이 정책을 DMS 에 처음 저장하는 경우에 해당합니다.

여기에서는 iis5@host.company.com 이 루트 PMDB 인 정책 모델 계층 구조에 정책 IIS5 를 배포합니다.

1. 다음 IIS 스크립트를 사용하여 IIS5.selang 이라는 파일을 저장합니다.

   ```
   nu inet_pers owner(nobody)
   nr FILE c:\InetPub\wwwroot\* defaccess(none) owner(nobody)
   authorize FILE c:\InetPub\wwwroot\* uid(inet_pers) access(all)
   nr FILE c:\InetPub\wwwroot\scripts defaccess(none) owner(nobody)
   nr FILE *.asp defaccess(none) owner(nobody)
   authorize FILE *.asp uid(inet_pers) via(pgm(inetinfo.exe)) access(read, execute)
   ```

   이러한 명령은 IIS 5 보호 정책을 배포하는 데 필요한 명령입니다.

2. 다음 스크립트를 사용하여 IIS5_rm.selang 이라는 파일을 저장합니다.

   ```
   ru inet_pers
   rr FILE c:\InetPub\wwwroot\*
   rr FILE c:\InetPub\wwwroot\scripts
   rr FILE *.asp
   ```

   이러한 명령은 1 단계에서 작성한 IIS 5 보호 정책의 배포를 취소하는 데 필요한 명령입니다.

3. 다음과 같이 policydeploy 유틸리티를 실행합니다.

   ```
   policydeploy -store IIS5 -ds IIS5.selang -uds IIS5_rm.selang
   ```

   그러면 IIS5.selang 및 IIS5_rm.selang 에 정의된 IIS5 정책의 첫 번째 버전(IIS5#01)이 DMS 에 저장됩니다.

정책과 관련된 규칙 보기

DMS 에 정책을 저장하면 POLICY 및 RULESET 개체에 대한 읽기 권한이 있는 모든 사용자가 정책 및 이와 관련된 규칙을 볼 수 있습니다. 저장된 정책의 최신 버전을 모르는 경우에는 먼저 이를 찾아볼 수 있습니다.

정책과 관련된 규칙을 보는 방법

1. 다음과 같이 selang 을 통해 DMS 에 연결합니다.

   ```
   hosts dms_name@hostname
   ```

   이제 selang 을 통해 DMS 를 조회할 수 있습니다.

2. 정책의 최신 버전을 확인하려면 다음 selang 명령을 실행하여 정책의 모든 버전을 찾습니다.

   ```
   find POLICY policy_name#*
   ```

   selang 창에 *policy_name* 정책의 모든 버전이 나열됩니다.

3. 다음 selang 명령을 실행하여 정책 배포 및 배포 취소 스크립트를 확인합니다.

   ```
   sr RULESET policy_name#xx
   ```

   여기서 *xx* 는 규칙을 보려는 정책의 번호입니다.

   selang 창에는 *policy_name* 정책의 *xx* 버전과 관련된 배포 및 배포 취소 규칙을 비롯하여 *policy_name#xx* RULESET 개체가 표시됩니다.

저장된 정책 버전 배포

나중에 정책의 배포를 취소할 수 있는 방식으로 계층 구조에 여러 규칙 정책의 저장된 버전을 배포하고 배포 상태, 배포 편차 및 배포 계층 구조에 대한 보고서를 작성할 수 있습니다.

저장된 정책 버전을 배포하는 방법

다음 중 *하나*를 수행합니다.

- 저장된 정책의 *최신* 버전을 배포하려면 다음과 같이 정책 이름과 대상 계층 구조를 지정하여 policydeploy 유틸리티를 실행합니다.

  ```
  policydeploy -deploy name -root db1[,db2] [-dms list]
  ```

  유틸리티는 사용자가 제공한 이름을 사용하여 DMS 에서 정책의 최신 버전을 찾은 다음 대상 데이터베이스에 배포합니다. 그런 다음 정책 명령이 구독 데이터베이스(있는 경우)로 전파됩니다.

- 저장된 정책의 *특정* 버전을 배포하려면 다음과 같이 정책 이름, 정책 버전 및 대상 계층 구조를 지정하여 policydeploy 유틸리티를 실행합니다.

  ```
  policydeploy -deploy name -root db1[,db2] [-dms list]
  ```

  유틸리티는 대상 데이터베이스에 지정된 버전의 정책을 배포합니다. 그런 다음 정책 명령이 구독 데이터베이스(있는 경우)로 전파됩니다.

참고: policydeploy 유틸리티에 대한 자세한 내용은 *유틸리티 가이드*(Unix) 또는 *참조 가이드*(Windows)를 참조하십시오.

중요! 배포 계층 구조의 호스트에 동일한 버전의 정책이 이미 배포되어 있는 경우에는 해당 정책을 배포할 수 없습니다.

예: IIS 5 보호 정책 배포

다음 예에서는 IIS(Internet Information Services) 5 웹 서버의 보안을 위한 정책을 배포하는 방법을 설명합니다. 여기에서는 정책 IIS5 의 네 번째 버전을 검토한 다음 iis5@host1.company.com 이 루트 PMDB 인 정책 모델 계층 구조에 배포합니다. 정책 IIS5 는 crDMS@cr_host.company.com DMS 노드에 저장되어 있습니다.

1. 다음과 같이 selang 을 통해 DMS 에 연결합니다.

   ```
   hosts crDMS@cr_host.company.com
   ```

   이제 selang 을 통해 DMS 를 조회할 수 있습니다.

2. 정책의 최신 버전을 모르는 경우 다음 selang 명령을 실행하여 정책의 모든 버전을 찾습니다.

   ```
   find POLICY IIS5#*
   ```

   selang 창에 IIS5 정책의 모든 버전이 나열됩니다.

3. 다음 selang 명령을 실행하여 정책 배포 및 배포 취소 스크립트를 확인합니다.

   ```
   sr RULESET IIS5#04
   ```

selang 창에는 IIS5 정책의 네 번째 버전과 관련된 배포 및 배포 취소 규칙을 비롯하여 IIS5#04 RULESET 개체가 표시됩니다.

4. 명령줄 창에서 다음과 같이 policydeploy 유틸리티를 실행합니다:

   ```
   policydeploy -deploy IIS5#04 -root iis5@host1.company.com
   ```

   그러면 iis5@host.company.com 아래 PMD 계층 구조에 IIS5 정책의 네 번째 버전이 배포됩니다.

정책 배포 취소

해당 컴퓨터에 더 이상 정책을 배포하지 않으려면 대상 계층 구조에서 여러 규칙 정책의 배포를 취소할 수 있습니다. 정책을 수정하여 업데이트된 버전을 작성하려는 경우에도 정책의 배포를 취소해야 합니다.

정책 배포를 취소하는 방법

1. (선택적) selang 배포 취소 명령을 사용하여 새 스크립트 파일을 작성합니다.

   이러한 명령은 계층 구조의 컴퓨터에서 정책의 배포를 취소(제거)하는 데 필요한 명령입니다.

   새로운 배포 취소 스크립트를 작성하여 지정하지 않은 경우 배포 취소 명령은 해당 정책을 배포할 때 지정된 스크립트를 사용합니다.

   중요! 정책 배포 취소 스크립트를 지정한 경우에도 DMS 는 정책의 배포를 취소하는 데 사용되는 새로운 스크립트가 아니라 정책을 저장할 때 제공된 원래 규칙을 등록합니다.

2. 다음 *중 하나*를 수행합니다.

   - 정책의 *최신* 버전의 배포를 취소하려면 다음과 같이 정책 이름과 대상 계층 구조를 지정하여 policydeploy 유틸리티를 실행합니다.

     ```
     policydeploy -undeploy name -root db1[,db2] [-dms list] [-uds file2]
     ```

     유틸리티는 사용자가 제공한 이름을 사용하여 DMS 에서 정책의 최신 버전을 찾은 다음 대상 데이터베이스에서 이 정책의 배포를 취소합니다. 그런 다음 정책 배포 취소 명령이 구독 데이터베이스(있는 경우)로 전파됩니다.

     중요! 계층 구조의 끝점에 있는 정책 버전에 DMS 에 있는 최신 버전 이외의 다른 버전이 포함된 경우에는 이러한 각 특정 버전을 명시적으로 배포 취소해야 합니다.

   - 정책의 *특정* 버전의 배포를 취소하려면 다음과 같이 정책 이름, 정책 버전 및 대상 계층 구조를 지정하여 policydeploy 유틸리티를 실행합니다.

     ```
     policydeploy -undeploy name#xx -root db1[,db2] [-dms list] [-uds file2]
     ```

     유틸리티는 대상 데이터베이스에서 정책의 지정된 버전(*xx*)을 배포 취소합니다. 그런 다음 정책 배포 취소 명령이 구독 데이터베이스(있는 경우)로 전파됩니다.

   참고: policydeploy 유틸리티에 대한 자세한 내용은 *유틸리티 가이드*(UNIX) 또는 *참조 가이드*(Windows)를 참조하십시오.

참고: 정책의 배포를 취소하면 DMS 에 정책의 상태가 *배포 취소*로 기록됩니다. POLICY 및 RULESET 개체는 DMS 를 포함하여 정책 버전이 배포된 모든 호스트에 그대로 유지되므로 나중에 다시 배포하거나 조회할 수 있습니다.

배포된 정책 수정

배포된 정책을 수정하려면 먼저 배포된 정책 버전의 배포를 취소하고, 수정된 배포 및 배포 취소 스크립트를 사용하여 새로운 버전의 정책을 저장한 다음, 새 버전을 사용하여 정책을 다시 배포합니다.

배포된 정책을 수정하는 방법

1. 새 정책 버전을 저장합니다.

   정책의 새 버전이 DMS 에 저장됩니다.

2. 정책의 배포를 취소합니다 (페이지 103).

   대상 계층 구조에서 정책의 배포가 취소됩니다.

3. 새로운 버전의 정책을 배포합니다 (페이지 101).

   수정된 정책이 대상 계층 구조에 재배포됩니다.

고급 정책 보고의 작동 방법

고급 정책 보고를 사용하면 고급 정책 기반 관리 방법을 통해 작성된 정책과 구성된 계층 구조와 관련된 배포 상태, 배포 편차 및 배포 계층 구조에 대한 보고서를 작성할 수 있습니다. 보고서 생성 유틸리티(policyreport)는 DMS 컨텐츠에 기반하여 지정 시간(정적) HTML 보고서를 생성합니다.

policyreport 유틸리티는 다음 작업을 수행하여 계층 구조와 정책 보고서를 작성합니다.

1. 유틸리티는 DMS 에서 요청된 정보를 조회합니다.

   검색되는 정보는 생성된 보고서 유형에 따라 다릅니다.

2. 편차 계산이 요청된 경우 유틸리티는 끝점에서 정책 편차 결과를 조회합니다.

   편차 상태는 DMS 에 있지만 실제 편차는 각 끝점에서 검색해야 합니다.

3. 유틸리티는 일련의 XML 문서를 생성합니다.

   이는 XML 보고서입니다.

4. 유틸리티는 XML 보고서의 형식을 HTML 로 지정합니다.

   이제 브라우저에서 보고서를 볼 수 있습니다.

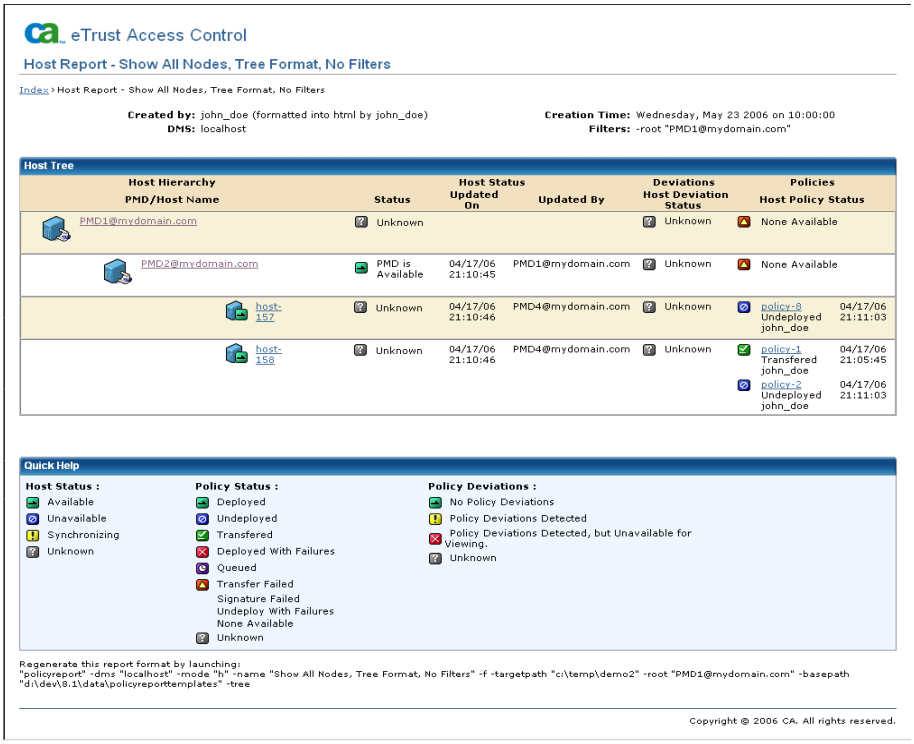
참고: policyreport 유틸리티는 -targetpath 옵션을 사용하여 지정한 디렉토리 아래에서 -name 옵션을 사용하여 지정한 하위 디렉토리에 보고서를 저장합니다.

보고서 유형

보고서 생성 유틸리티를 사용하면 계층 구조 전체에 배포된 정책을 다음 두 가지 모드로 볼 수 있습니다.

- 호스트별

  호스트 보고서는 컴퓨터 중심적인 정보를 제공합니다. 호스트로 환경을 볼 경우에는 이 모드를 사용하십시오. 이 모드에서 컴퓨터 구성 방법과, 계층에서의 각 컴퓨터 상태를 알 수 있으며 어느 컴퓨터가 어느 정책을 가지고 있고 상태는 어떤지 그리고 배포된 실제 규칙이 각 컴퓨터에서 배포되어야 할 규칙에서 어떻게 다른지 알려줍니다.


eTrust Access Control

Host Report - Show All Nodes, Tree Format, No Filters

Index > Host Report - Show All Nodes, Tree Format, No Filters

Created by: john_doe (formatted into html by john_doe)
DMS: localhost
Creation Time: Wednesday, May 23 2006 on 10:00:00
Filters: -root "PMD1@mydomain.com"

Host Tree

Host Hierarchy PMD/Host Name	Status	Host Status Updated On	Updated By	Deviations Host Deviation Status	Policies Host Policy Status
PMD1@mydomain.com	Unknown			Unknown	None Available
PMD2@mydomain.com	PMD is Available	04/17/06 21:10:45	PMD1@mydomain.com	Unknown	None Available
host-157	Unknown	04/17/06 21:10:46	PMD4@mydomain.com	Unknown	policy-8 Undeployed john_doe 04/17/06 21:11:03
host-158	Unknown	04/17/06 21:10:46	PMD4@mydomain.com	Unknown	policy-1 Transfered john_doe 04/17/06 21:05:45 policy-2 Undeployed john_doe 04/17/06 21:11:03

Quick Help

Host Status :
- Available
- Unavailable
- Synchronizing
- Unknown

Policy Status :
- Deployed
- Undeployed
- Transfered
- Deployed With Failures
- Queued
- Transfer Failed
- Signature Failed
- Undeploy With Failures
- None Available
- Unknown

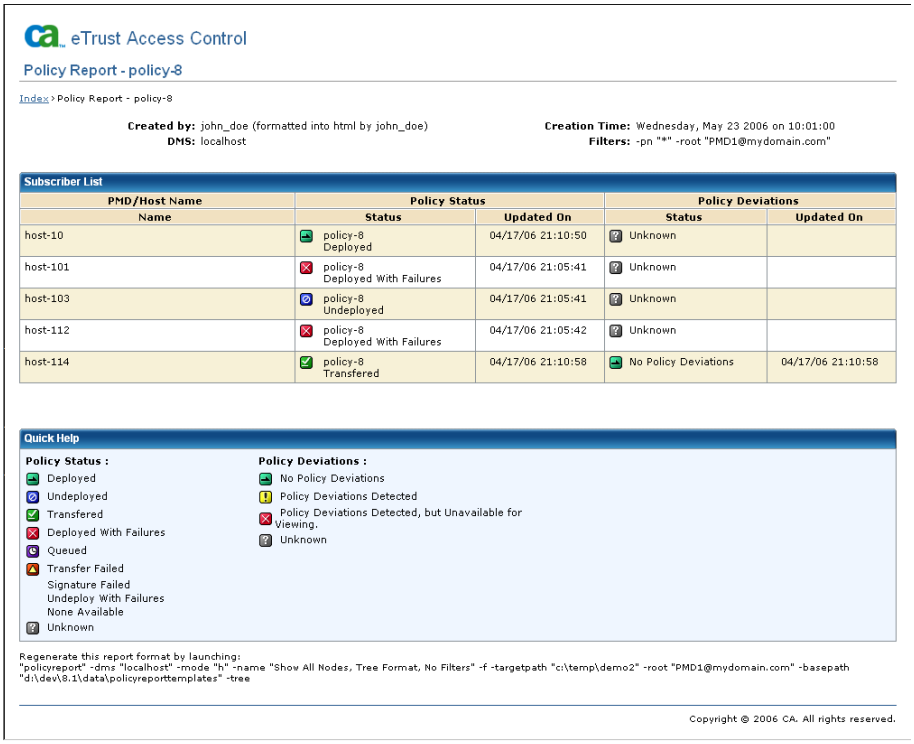
Policy Deviations :
- No Policy Deviations
- Policy Deviations Detected
- Policy Deviations Detected, but Unavailable for Viewing.
- Unknown

Regenerate this report format by launching:
"policyreport" -dms "localhost" -mode "h" -name "Show All Nodes, Tree Format, No Filters" -f -targetpath "c:\temp\demo2" -root "PMD1@mydomain.com" -basepath "d:\dev\8.1\data\policyreporttemplates" -tree

Copyright © 2006 CA. All rights reserved.

- 정책별

  정책 보고서는 정책 중심적인 정보를 제공합니다. 해당 환경에서 하나 이상의 정책의 상태를 보려면 이 모드를 사용하십시오.



eTrust Access Control

Policy Report - policy-8

Index › Policy Report - policy-8

Created by: john_doe (formatted into html by john_doe)
DMS: localhost

Creation Time: Wednesday, May 23 2006 on 10:01:00
Filters: -pn "*" -root "PMD1@mydomain.com"

Subscriber List

PMD/Host Name	Policy Status		Policy Deviations	
Name	Status	Updated On	Status	Updated On
host-10	policy-8 Deployed	04/17/06 21:10:50	Unknown	
host-101	policy-8 Deployed With Failures	04/17/06 21:05:41	Unknown	
host-103	policy-8 Undeployed	04/17/06 21:05:41	Unknown	
host-112	policy-8 Deployed With Failures	04/17/06 21:05:42	Unknown	
host-114	policy-8 Transfered	04/17/06 21:10:58	No Policy Deviations	04/17/06 21:10:58

Quick Help

Policy Status :
Deployed
Undeployed
Transfered
Deployed With Failures
Queued
Transfer Failed
Signature Failed
Undeploy With Failures
None Available
Unknown

Policy Deviations :
No Policy Deviations
Policy Deviations Detected
Policy Deviations Detected, but Unavailable for Viewing.
Unknown

Regenerate this report format by launching:
"policyreport" -dms "localhost" -mode "h" -name "Show All Nodes, Tree Format, No Filters" -f -targetpath "c:\temp\demo2" -root "PMD1@mydomain.com" -basepath "d:\dev\8.1\data\policyreporttemplates" -tree

Copyright © 2006 CA. All rights reserved.

보고서 유형 외에 다음을 통해서도 출력에 영향을 줄 수 있습니다.

- 계층 구조에서 보고서를 생성할 부분 선택
- 단일 컴퓨터에 대한 보고서 생성
- 호스트 이름, 상태 또는 상태 업데이트 시간을 기준으로 필터링 또는 정책 이름 또는 상태를 기준으로 필터링(와일드카드 지원)
- 편차 계산 결과 포함 또는 제외
- 트리와 유사한 형식 선택
- 보고서 열 숨기기

호스트 보고서 작성

호스트 보고서를 통해 계층 구조에서 컴퓨터가 구성되어 있는 방식, 계층 구조에 있는 각 컴퓨터의 상태 또는 각 컴퓨터에 있는 정책과 정책의 상태를 확인할 수 있습니다.

호스트 보고서를 작성하려면 다음과 같이 *h* 모드로 policyreport 유틸리티를 실행합니다.

```
policyreport -name <name> -mode h -dms <dms_name> -root <pmd1>[,<pmd2>] -tree \
-targetpath <path>
```

참고: 추가 선택적 플래그를 사용하여 보고서를 미세 조정할 수도 있습니다. policyutility 유틸리티에 대한 자세한 내용은 *참조 가이드*를 참조하십시오.

예: 지정된 마스크와 호스트 이름이 일치하는 컴퓨터에 대한 보고서를 작성합니다.

다음 예에서는 policyreport 유틸리티를 사용하여 다음 작업을 수행하는 방법을 설명합니다.

- 다음 디렉토리에 호스트 보고서를 생성합니다.

  C:\eac_data\reports\production_March2006

- 다음 DMS 에서 정보를 검색합니다.

  mainhost.domain.com 컴퓨터의 **mainDMS**

- 계층 구조에서 다음 PMDB 아래에 있는 컴퓨터만 포함합니다.

  rootPMD@root.domain.com

- 호스트 이름이 다음 문자로 시작하는 컴퓨터만 포함합니다.

  prod

```
policyreport -name production_March2006 -mode h \
-dms mainDMS@mainhost.domain.com -root rootPMD@root.domain.com -hn prod* \
-targetpath C:\eac_data\reports
```

policyreport 유틸리티는 -targetpath 옵션을 사용하여 지정한 디렉토리(C:\eac_data\reports) 아래에서 -name 옵션을 사용하여 지정한 하위 디렉토리(production_March2006)에 보고서를 저장합니다. 출력 디렉토리에 이미 보고서가 있는 경우에도 보고서를 작성하는 -f 옵션을 추가하여 나중에 이 보고서를 업데이트할 수 있습니다.

참고: -tree 플래그를 지정하면 보고서에 계층 구조의 그래픽 표현이 나타납니다. 부모의 호스트 이름이 지정된 마스크와 일치하지 않는 경우에도 여기에는 보고서에 있는 모든 컴퓨터의 부모가 포함됩니다.

예: 마지막으로 상태가 변경된 날짜가 특정 날짜 범위 내에 있는 컴퓨터에 대한 보고서를 작성합니다.

다음 예에서는 policyreport 유틸리티를 사용하여 다음 작업을 수행하는 방법을 설명합니다.

- 다음 디렉토리에 호스트 보고서를 생성합니다.

  C:\eac_data\reports\Feb06-Mar06

- 다음 DMS 에서 정보를 검색합니다.

  mainhost.domain.com 컴퓨터의 **mainDMS**

- 계층 구조에서 다음 PMDB 아래에 있는 컴퓨터만 포함합니다.

  rootPMD@root.domain.com

- 호스트 상태가 2006 년 2 월에 마지막으로 업데이트된 컴퓨터만 포함합니다.

```
policyreport -name Feb06-Mar06 -mode h \
-dms mainDMS@mainhost.domain.com -root rootPMD@root.domain.com \
-sd 01-02-2006 -ed 28-02-2006 -targetpath C:\eac_data\reports
```

예: 정책 편차 결과를 다시 계산한 다음 현재 작업 디렉토리에 저장하는 보고서를 작성합니다.

다음 예에서는 policyreport 유틸리티를 사용하여 다음 작업을 수행하는 방법을 설명합니다.

- 다음 디렉토리에 호스트 보고서를 생성합니다.

  *<working_directory>***/hierarchy_20March06**

- 다음 DMS 에서 정보를 검색합니다.

  mainhost.domain.com 컴퓨터의 **mainDMS**

- 계층 구조에서 다음 PMDB 아래에 있는 컴퓨터만 포함합니다.

  rootPMD@root.domain.com

- 편차 계산 결과를 포함합니다.
- 들여쓰기를 사용하여 계층 구조를 그래픽으로 표시합니다.

```
policyreport -name hierarchy_20March06 -mode h -dms mainDMS@mainhost.domain.com \
-root rootPMD@root.domain.com -targetpath -dev -tree
```

정책 보고서 작성

정책 보고서를 사용하여 각 컴퓨터에 배포되어 있는 정책을 확인할 수 있습니다.

정책 보고서를 작성하려면 다음과 같이 *p* 모드로 policyreport 유틸리티를 실행합니다.

```
policyreport -name <name> -mode p -dms <dms_name> -root <pmd1>[,<pmd2>] \
-targetpath <path>
```

참고: 추가 선택적 플래그를 사용하여 보고서를 미세 조정할 수도 있습니다. policyutility 유틸리티에 대한 자세한 내용은 *참조 가이드*를 참조하십시오.

예: 지정된 정책의 모든 버전에 대한 보고서를 작성합니다.

다음 예에서는 policyreport 유틸리티를 사용하여 다음 작업을 수행하는 방법을 설명합니다.

- 다음 디렉토리에 정책 보고서를 생성합니다.

  C:\eac_data\reports\iis5Policies_March2006

- 다음 DMS 에서 정보를 검색합니다.

  mainhost.domain.com 컴퓨터의 **mainDMS**

- 계층 구조에서 다음 PMDB 아래에 있는 컴퓨터(구독자)만 포함합니다.

  rootPMD@root.domain.com

- 다음 정책의 버전만 포함합니다.

  iis5

```
policyreport -name prodPolicies_March2006 -mode p \
-dms mainDMS@mainhost.domain.com -root rootPMD@root.domain.com -pn iis5#* \
-targetpath C:\eac_data\reports
```

policyreport 유틸리티는 -targetpath 옵션을 사용하여 지정한 디렉토리(C:\eac_data\reports) 아래에서 -name 옵션을 사용하여 지정한 하위 디렉토리(iis5Policies_March2006)에 보고서를 저장합니다. 출력 디렉토리에 이미 보고서가 있는 경우에도 보고서를 작성하는 -f 옵션을 추가하여 나중에 이 보고서를 업데이트할 수 있습니다.

예: 배포되었지만 오류가 있는 정책에 대한 보고서를 작성합니다

다음 예에서는 policyreport 유틸리티를 사용하여 다음 작업을 수행하는 방법을 설명합니다.

- 다음 디렉토리에 정책 보고서를 생성합니다.

  C:\eac_data\reports\policyErrors

- 다음 DMS 에서 정보를 검색합니다.

  mainhost.domain.com 컴퓨터의 **mainDMS**

- 계층 구조에서 다음 PMDB 아래에 있는 컴퓨터(구독자)만 포함합니다.

  rootPMD@root.domain.com

- 배포되었지만 오류가 있는(실패) 정책만 포함합니다

```
policyreport -name policiesErrors -mode p \
-dms mainDMS@mainhost.domain.com -root rootPMD@root.domain.com \
-pstat "Failed" -targetpath C:\eac_data\reports
```

정책 또는 호스트 보고서 보기

보고서를 생성한 후에는 보고서가 저장된 폴더로 이동하여 보고서를 브라우저에서 열어서 보아야 합니다.

정책 또는 호스트 보고서를 보려면

1. 보고서가 저장된 폴더로 이동합니다.

   이 폴더는 *<target_path>*/*<report_name>*/html 입니다.

   여기서 *<target_path>*는 -targetpath 플래그를 사용하여 지정한 디렉터리이고 *<report_name>*은 보고서를 생성할 때 -name 플래그를 사용하여 지정한 보고서의 이름입니다.

2. **index.html** 파일을 열어 브라우저에서 봅니다.

   브라우저에 보고서의 기본 페이지가 표시됩니다.

정책 편차 계산의 작동 방법

고급 정책 관리 및 보고를 사용하면 끝점에 배포하고자 하는 정책 규칙과 끝점에 적용된 실제 정책 규칙 간의 차이를 알 수 있습니다. 이 정보를 사용하면 정책 배포와 관련된 문제를 처리할 수 있습니다.

각 끝점에서 정책 편차 계산기를 실행하고 다음 작업을 수행합니다.

1. 끝점에 배포해야 하는 규칙 목록을 로컬 호스트에서 검색합니다.

   이러한 규칙은 로컬 RULESET 개체에 지정된 대로 배포된 각 정책에 대해 지정되는 규칙이며, RULESET 개체는 배포된 각 정책의 POLICY 개체와 연결되어 있습니다.

2. 이러한 각 규칙이 끝점에 적용되는지 확인합니다.

   중요! 편차 계산에서는 Windows(기본) 규칙이 적용되는지 여부를 확인하지 않습니다. 또한 데이터베이스에서 개체(사용자 또는 개체 속성, 사용자 또는 리소스 권한, 실제 사용자 또는 리소스)를 제거하는 규칙을 무시합니다. 예를 들어, 편차 계산에서는 다음 규칙이 적용되는지 여부를 확인할 수 없습니다.
   rr FILE C:\tmp\tmp.txt

3. (선택 사항). 로컬 HNODE 개체에 연결된 정책과 사용 가능한 첫 번째 DMS 에 있는 정책을 비교합니다.

   일반적으로 편차 계산기는 로컬 호스트에서만 편차를 확인합니다. *-strict* 옵션을 지정하면 편차 계산기는 또한 로컬 정책과 목록에서 사용 가능한 첫 번째 DMS 에 있는 정책도 비교합니다. 이 경우 다음을 비교합니다.

   a. 로컬 호스트를 나타내는 HNODE 개체에 연결된 정책 목록

   b. HNODE 개체에 연결된 각 POLICY 개체의 정책 상태

   c. HNODE 개체에 연결된 각 POLICY 개체의 정책 서명

4. 다음 두 개의 파일이 출력됩니다.

   - <*eTrustACDir*>\data\devcalc\deviation.log

     마지막 편차 계산 시 수집된 로그 및 오류 메시지입니다.

   - <*eTrustACDir*>\data\devcalc\deviation.dat

     정책 및 해당 편차의 목록입니다.

   참고: eTrust AC 에서는 또한 **seaudit -a** 를 사용하여 볼 수 있는 감사 이벤트도 보냅니다. seaudit 유틸리티에 대한 자세한 내용은 *참조 가이드*를 참조하십시오.

5. 하나 이상의 DMS 에 발견된 모든 편차를 알립니다.

   알릴 DMS 는 *-dms* 옵션을 사용하여 수동으로 지정할 수 있습니다. 또는 DMS 를 지정하지 않으면 편차 계산기에서 로컬 eTrust AC 데이터베이스에 대해 지정된 DMS 목록을 사용합니다.

정책 편차 계산에 대한 끝점 구성

사용자 지정 설치를 사용하여 eTrust AC 를 설치하거나 업그레이드할 때 고급 정책 관리 옵션을 선택하는 경우 설치 과정 중에 정책 편차 계산기가 구성됩니다. 또한 편차를 계산하고 지정한 DMS 데이터베이스 사후 설치에 편차 상태 알림을 보내도록 데이터베이스를 구성할 수도 있습니다.

정책 편차 계산에 대한 끝점을 구성하려면

참고: 이 eTrust AC 컴퓨터를 설치하거나 업그레이드할 때 고급 정책 관리 옵션을 선택하지 않은 경우에만 이 작업을 수행해야 합니다. eTrust AC 설치에 대한 자세한 내용은 *구현 가이드*를 참조하십시오.

1. selang 명령 창을 엽니다.

   selang 명령창이 열리면 selang 명령을 입력할 수 있습니다.

2. 다음 명령을 입력합니다.

   ```
   nu ("+devcalc") admin auditor
   ```

   이 명령은 ADMIN 특성이 있는 *+devcalc* 라는 사용자를 새로 만듭니다. 이 사용자는 eTrust AC 에서 편차 계산기를 실행할 때 사용됩니다.

3. 다음 명령을 입력합니다.

   ```
   nr SPECIALPGM ("<devcalc.exe_path>") seosuid("+devcalc") nativeuid("SYSTEM")
   ```

   여기서 *<devcalc.exe_path>*는 eTrust AC 설치 디렉터리의 bin 디렉터리에 있는 devcalc.exe 응용 프로그램의 전체 경로입니다.

   이 명령은 편차 계산기의 특수 프로그램 리소스를 새로 만들고 이 특수 프로그램을 실행할 권한이 있는 논리적 사용자와 기본 Windows 사용자를 지정합니다.

4. 다음 명령을 입력합니다.

   ```
   so dms+(<DMS1>[,<DMS2>)
   ```

   여기서 *<DMSx>*는 편차 계산에서 정책 편차 상태 알림을 보낼 DMS 의 이름입니다. 각 DMS 는 다음 형식으로 지정해야 합니다. DMS_name@hostname.

예: 정책 편차 상태를 중앙 DMS 로 보내는 끝점 구성

다음 예제에서는 다음 작업을 수행하기 위해 표준 설치 및 기본 설치 디렉터리를 사용하여 설치한 끝점에서 실행해야 하는 명령을 보여 줍니다.

- 편차 계산을 수행할 수 있는 끝점을 구성합니다.
- 정책 편차 상태를 DMS 로 전송합니다.

  centralhost.com 컴퓨터에서 **prodDMS** 를 실행합니다.

```
nu ("+devcalc") admin auditor
nr SPECIALPGM ("C:\Program Files\eTrustAccessControl\bin\devcalc.exe") \
seosuid("+devcalc") nativeuid("SYSTEM")
```

```
so dms+(prodDMS@centralhost.com)
```

정책 편차 로그 및 오류 파일

정책 편차를 계산하면 각 편차 계산 중에 새 로그가 작성됩니다. 이 로그에는 오류 메시지가 포함되어 있으며 *<eTrustACDir>*\data\devcalc\deviation.log 에 저장됩니다.

DMS 에서 가져온 보고서에 표시되는 편차가 마지막으로 실행된 편차 계산에서 수집되지 않은 경우 이 로그를 사용합니다. 이 로그는 편차 계산 결과가 DMS 로 전송되지 않은 이유를 진단하는 데 도움이 됩니다.

중요! 편차 로그에 오류 "오류: DB 라이브러리를 초기화하지 못했습니다. 데이터베이스가 열려 있습니다"가 포함되어 있으면 데이터베이스의 색인 파일을 다시 작성해야 합니다. 이 작업을 수행하려면 selang을 종료하고 *<eTrustACDir>*\data\devcalc\init_ac_db 디렉토리에서 다음 명령을 실행한 다음 편차 계산을 다시 실행합니다 (페이지 114):

```
selang -l -d .
```

예: 편차 로그 및 오류 파일

다음은 예제 편차 로그와 오류 파일입니다.

```
시작 시간: Mon Jan 23 13:04:48 2006
경고,\"DMS 호스트 이름을 검색하지 못했습니다. 편차가 로컬에 저장됩니다.\"
'iis8#02' 정책에 대한 편차를 찾았습니다.
종료 시간: Mon Jan 23 13:05:04 2006
```

정책 편차 데이터 파일

정책 편차를 계산하면 정책 및 정책 편차 목록이 포함된 데이터 파일이 작성됩니다. 이 데이터 파일은 *<eTrustACDir>*\data\devcalc\deviation.dat 에 저장됩니다.

참고: 데이터 파일에 포함되는 정책 목록은 편차를 계산하는 정책에 따라 다릅니다. 기본적으로 끝점의 모든 정책과 모든 정책 버전이 포함됩니다.

중요! 편차 계산은 Windows(기본) 규칙이 적용되는지 여부를 확인하지 않습니다. 또한 데이터베이스에서 개체(사용자 또는 개체 속성, 사용자 또는 리소스 권한, 실제 사용자 또는 리소스)를 제거하는 규칙을 무시합니다. 예를 들어, 편차 계산에서는 다음 규칙이 적용되는지 여부를 확인할 수 없습니다.
rr FILE C:\tmp\tmp.txt

편차가 있는지 여부에 관계없이 편차 상태는 DMS 로 전송되지만 실제 편차는 로컬에 저장됩니다. 보고서를 작성하면 이 파일에서 실제 편차 결과를 가져와서 보고서에 추가할 수 있습니다.

정책 편차 데이터 파일에 나타날 수 있는 줄은 다음과 같습니다.

날짜

편차 계산 날짜입니다.

형식: DATE, *DDD MMM DD hh:mm:ss YYYY*

Strict

-strict 옵션을 사용하여 편차 계산이 실행되었음을 지정합니다.

형식: STRICT, *DMS@hostname*, *policy_name#xx*, {1|0}

여기서 {1|0}은 로컬 HNODE 개체와 관련된 정책과 *DMS@hostname*(사용 가능한 첫 번째 DMS)의 HNODE 개체와 관련된 정책 사이에 편차가 있는지(1) 또는 없는지(0) 여부를 나타냅니다.

Policy Start

이 정책에 대한 편차를 정의한 정책 블록을 시작합니다.

형식: POLICYSTART, *policy_name#xx*

차이

정책에 대해 발견된 편차를 설명합니다. 편차가 적용되는 정책의 이름은 이 줄 위의 가장 가까운 **정책 줄**입니다..

다음 표에서는 네 가지 유형의 편차를 설명합니다.

편차 유형	형식
클래스를 찾을 수 없습니다.	DIFF, (<*class_name*>), (*), (*), (*)
개체를 찾을 수 없습니다.	DIFF, (<*class_name*>), (<*object_name*>), (*), (*)
속성을 찾을 수 없습니다.	DIFF, (<*class_name*>), (<*object_name*>), (<*property_name*>), (*)

편차 유형	형식
속성 값이 일치하지 않습니다.	DIFF, (<*class_name*>), (<*object_name*>), (<*property_name*>), *(<expected_value>)*

Policy End

이 정책에 대한 편차를 정의하는 정책 블록을 종료합니다.

형식: POLICYEND, *policy_name#xx*, {1|0}

여기서 {1|0}은 편차가 있는지(1) 또는 없는지(0) 여부를 나타냅니다.

경고

경고를 설명합니다.

형식: 경고, "*warning_text*"

예: 편차 데이터 파일

```
Date, Sun Mar 19 08:30:00 2006
경고, "DMS 호스트 이름을 검색하지 못했습니다. 편차가 로컬에 저장됩니다"
POLICYSTART, iis8#02
DIFF, (USER), (am), (*), (*)
POLICYEND, iis8#02, 1
```

편차 계산 수행

DMS 에 정책 편차 상태에 대한 최신 정보가 포함되도록 편차 계산을 정기적으로 수행해야 합니다. 보고 요구 사항을 지원하는 간격으로 정책 편차 계산이 발생하도록 정책을 예약하는 것이 좋습니다.

끝점에서 편차 계산을 수행하려면 selang 창에서 다음 명령을 입력합니다.

```
start DEVCALC
```

예: 정기적인 편차 계산을 예약합니다.

다음 예에서는 Solaris 에서 다음과 같은 편차 계산 작업을 작성하는 방법을 설명합니다.

- 매일 자정에 실행
- 편차 상태를 다음 DMS 로 전송합니다.

  mainhost.domain.com 컴퓨터의 **mainDMS**

이 작업을 수행하려면 다음 단계를 따릅니다.

1. 다음 줄이 포함된 배치 파일을 만듭니다.

   ```
   selang -c "start DEVCALC params('-dms mainDMS@mainhost.domain.com')"
   ```

2. 다음 선택 항목을 통해 예약된 작업을 추가합니다.
   - 새 배치 파일을 찾아보고 선택합니다.
   - 이 작업을 매일 수행합니다.
   - 시작 시간: 12:00 AM

PMDB 와 Unicenter 통합

PMDB 를 Unicenter TNG 와 통합하면 PMDB 를 사용하여 Unicenter TNG 개체가 여러 Unicenter TNG 구성 요소(이벤트 관리 및 워크로드 관리와 같은 명령 프로세서 등)에 의해 조작되지 않도록 안전하게 보호하는 규칙을 작성할 수 있습니다.

통합을 수동으로 수행해야 합니다.

PMDB 를 Unicenter TNG 와 통합하려면

1. PMDB 를 작성합니다.
2. 다음 명령을 사용하여 Unicenter Security 옵션을 PMDB 로 마이그레이션합니다.

   `MigOpts` *pmdb-이름*

   여기서 *pmdb-name* 은 PMDB 이름입니다.

   참고: 이 단계는 Unicenter Security 를 사용하고 eTrust AC 설치 도중에 Unicenter 통합에서 Security Data Migration 을 선택한 경우에만 필요합니다. Unicenter Security 를 사용하지 않은 경우에는 어떤 보안 옵션도 설정하지 않은 것이므로 PMDB 로 마이그레이션할 내용이 없습니다.
3. 다음 명령을 사용하여 모든 사용자 정의-Unicenter TNG 자산 유형에 대한 클래스를 작성합니다.

   `defclass.bat.` *pmdb-이름*

   여기서 *pmdb-name* 은 PMDB 이름입니다.

   참고: 이 단계는 Unicenter Security 를 사용하고 사용자 정의 자산 유형을 만든 경우에만-필요합니다. eTrust AC 설치 중에 Unicenter 통합을 선택하면 모든 새 PMDB 에 Unicenter TNG 자산 유형이 자동으로 정의됩니다.

제 7 장: 트랜잭션 관리자 사용

이 장은 아래의 주제를 포함하고 있습니다:

트랜잭션 관리자

트랜잭션 관리자는 eTrust AC, UNIX 및 Windows 보안을 관리하기 위한 도구입니다. 트랜잭션 관리자는 로컬 호스트에서 수행할 때와 같이 eTrust AC 트랜잭션을 여러 호스트로 자동 전송합니다. 트랜잭션 모드는 정책 모델의 빠르고 효율적인 대체 수단 또는 보조 프로그램으로 설계되었습니다. 트랜잭션 모드는 모든 구독자의 보안 데이터베이스에 대한 수정 사항을 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 작업을 수행하십시오.

1. 액세스하는 각 원격 호스트와 로컬 호스트에 대해 ADMIN 권한을 가지고 있는지 확인합니다.

   액세스하는 각 호스트의 관리 컴퓨터에 대한 TERMINAL 레코드를 작성합니다.

   이러한 요구사항은 원격 호스트를 관리할 때와 동일합니다.

   트랜잭션 관리자를 활성화합니다. 정책 관리자에서 [도구], [옵션]을 선택하고 [트랜잭션 관리자] 탭을 엽니다. [Enable multi-host transactions(멀티 호스트 트랜잭션 사용)]를 선택합니다. 활성화하려는 트랜잭션 관리자 옵션을 선택할 수도 있습니다.

2. 대상 호스트 파일을 작성합니다.

멀티 호스트 트랜잭션 옵션

트랜잭션 관리자는 보안 정책 및 감사를 제외하고 프로그램 표시줄에서 열 수 있는 모든 창에서 사용할 수 있습니다. 기본적으로 사용자, 그룹 및 리소스가 선택되어 있습니다.

트랜잭션 관리자 옵션을 통해 트랜잭션 모드의 작동 방식을 원하는 대로 사용자 지정할 수 있습니다. 옵션은 다음과 같습니다.

일반 옵션

처음 오류 발생 시 데이터 전송 중지

기본적으로 오류가 발생하더라도 계속 트랜잭션을 전송합니다. 이 항목을 선택하면 최대한 많은 트랜잭션을 전파한 후 나중에 오류를 처리합니다. 그러나 예를 들어 트랜잭션을 여러 호스트로 전송할 때 한 호스트에서 실패하면 나머지 호스트에서도 실패할 것으로 예상될 경우 첫번째 오류 발생 시 전파를 중단함으로써 시간을 절약할 수 있습니다.

종료 시 트랜잭션 관리자 닫기

이 상자를 선택하면 트랜잭션 관리자는 큐에 있는 트랜잭션을 전송했는지 여부에 상관 없이 정책 관리자가 종료될 때 같이 종료됩니다. 이 옵션은 기본적으로 정책 관리자가 종료되더라도 트랜잭션 관리자를 계속 실행합니다.

참고: 트랜잭션 관리자의 메모리는 휘발성이므로 종료 시 트랜잭션 로그가 손실됩니다.

시작 시 트랜잭션 모드 활성화

정책 관리자를 시작하면 트랜잭션 관리자가 항상 시작됩니다. 그러나 기본적으로 도구모음에서 [트랜잭션 모드] 버튼을 클릭할 때까지 트랜잭션 모드로 전환되지 않습니다. 이 상자를 선택하면 정책 관리자를 시작할 때 트랜잭션 모드로 자동 전환됩니다.

대상 호스트 파일

이 옵션을 사용하여 대상 호스트 파일의 디렉터리 경로를 설정할 수 있습니다. 기본적으로 경로는 *eTrustACDir*\data\hosts.txt(여기서 *eTrustACDir* 는 eTrust AC 를 설치한 디렉터리)입니다.

초 단위 새로 고침 간격입니다....

이 옵션은 [TM Status(TM 상태)] 창에서 트랜잭션 관리자를 모니터링하는 주기를 결정합니다. 기본값은 10 초이지만, 트랜잭션이 짧을 경우에는 진행 상황이 표시되지 않을 수도 있습니다.

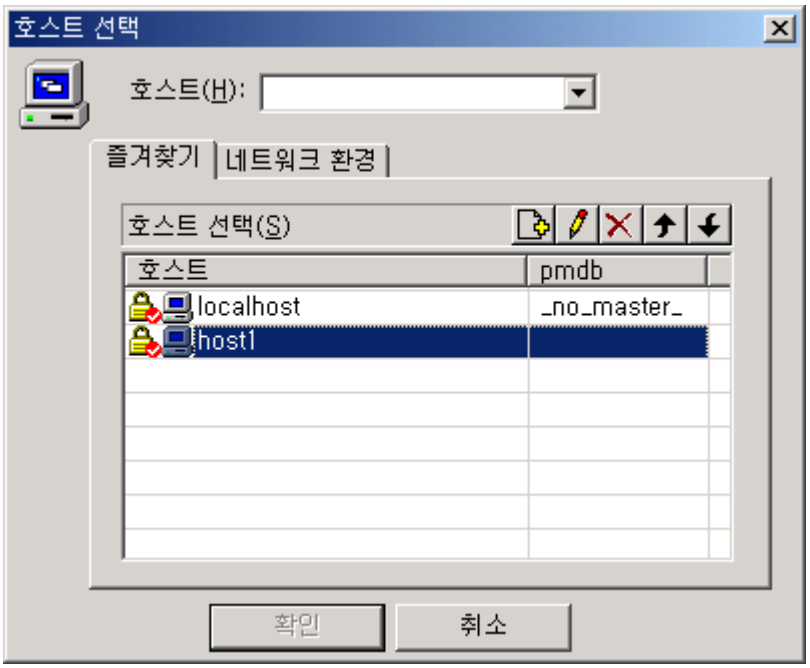
명령 및 스크립트

일반적으로, 트랜잭션 모드는 정책 관리자 트랜잭션과 함께 사용합니다. 또한 트랜잭션 모드를 사용하여 selang 명령이나 스크립트를 여러 호스트로 전송할 수 있습니다. 해당 상자를 선택하면 트랜잭션 모드를 명령 및 스크립트 대화 상자(도구, 명령 실행)와 함께 사용하여 selang 명령을 여러 호스트로 전송할 수 있습니다.

대상 호스트 파일 설정

대상 호스트 파일은 트랜잭션 모드에서 작업할 때 어떤 호스트 또는 호스트 그룹이 트랜잭션을 수신할지 제어합니다.

즐겨찾기즐겨찾기]목록 또는 [네트워크 환경]에서 호스트를 추가합니다.



호스트는 로컬 데이터베이스 또는 PMDB 일 수 있습니다. 선택 시간을 줄이기 위해 호스트 그룹을 만들 수 있습니다. 그룹 이름]을 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 호스트 그룹으로 전송하려면 대상 호스트 파일을 매번 수동으로 재설정해야 합니다.

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

트랜잭션 모드에서 작업

트랜잭션 관리자를 활성화하고 대상 호스트 파일을 작성했으면 도구모음에서 트랜잭션 모드 아이콘을 클릭하시오. 로컬 데이터베이스에서 수행하는 모든 트랜잭션은 선택한 호스트에도 전파됩니다. 예를 들어, 사용자창에서 이름을 선택하고 도구모음에서 [삭제]를 클릭하여 사용자를 삭제하면 트랜잭션은 보통 때와 마찬가지로 로컬 호스트 데이터베이스에서 즉시 실행된 후 대상 호스트 파일의 호스트로 자동 전파됩니다.

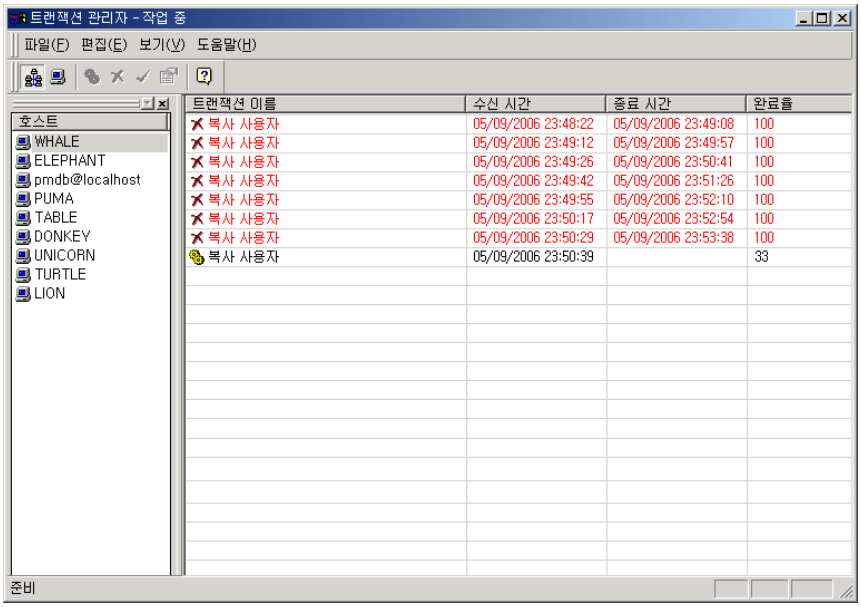
전파의 진행 상황을 [Task Manager Status] 창에서 확인할 수 있습니다. 시간이 오래 걸리는 트랜잭션을 일시 중지하려면 작업 표시줄 트레이의 트랜잭션 관리자 아이콘에서 마우스 오른쪽 버튼을 클릭하고 트랜잭션 관리자 일시 중단을 선택하십시오. 트랜잭션 관리자 다시 시작트랜잭션 관리자 다시 시작을 선택하면 전파가 계속됩니다. 오른쪽 상단 모서리에 있는 닫기 버튼을 클릭하여 트랜잭션 관리자 창을 닫더라도 응용 프로그램은 종료되지 않습니다. 트랜잭션 관리자를 종료하려면, 작업 표시줄 트레이의 아이콘에서 마우스 오른쪽 버튼을 클릭하고 [끝내기]를 선택하십시오. 트랜잭션 관리자를 종료하면 모든 트랜잭션이 로그에서 삭제됩니다.

트랜잭션 관리자 창

Windows 작업 표시줄에서 [트랜잭션 관리자] 아이콘을 두 번 클릭하여 [트랜잭션 관리자] 창을 활성화합니다. 이 창에는 여러 호스트로 전파된 모든 트랜잭션이 기록된 로그가 있습니다. 작업 관리자의 메모리는 휘발성이므로, 현재 세션의 트랜잭션만 표시됩니다. 보기]메뉴에서 호스트 상태 및 호스트 표시줄 보기 중 하나를 선택하거나, 도구모음에서 호스트 아이콘을 클릭하여 보기를 선택할 수 있습니다. 두 개의 아이콘은 동등하므로, 아이콘 중 하나를 클릭하면 보기가 토글됩니다. 도구모음의 버튼은 보기를 선택하거나, 트랜잭션을 다시 실행할 수 있게 허용하거나, 트랜잭션을 삭제 또는 복원하거나, 트랜잭션의 속성을 표시합니다. 큐에 있는 트랜잭션을 삭제하면, 트랜잭션 관리자는 해당 트랜잭션을 건너뛰고 큐에 있는 다음 트랜잭션으로 넘어갑니다. 언제든지 트랜잭션을 복원하여 트랜잭션을 계속 전파할 수 있습니다. 현재 트랜잭션은 삭제할 수 없습니다.

호스트 상태 표시줄 보기

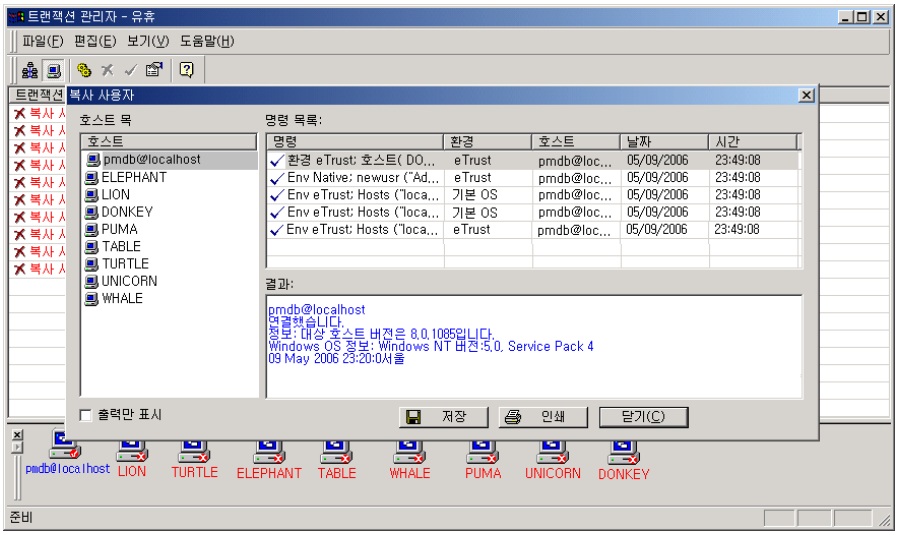
호스트 상태 표시줄 보기에서 각각의 선택된 호스트 아이콘이 창의 왼쪽에 있는 상태 표시줄에 나타납니다. 아이콘을 클릭하면 트랜잭션 목록이 해당 호스트와 관련된 내용으로 바뀝니다. [트랜잭션]을 두 번 클릭하면 [명령 목록] 입력란과 [결과] 입력란이 있는 [업데이트] 대화 상자가 나타납니다. [명령 목록] 입력란에서 명령을 선택하면 명령 결과가[결과] 입력란에 표시됩니다. 결과를 인쇄하거나 파일로 저장할 수 있습니다.



호스트 표시줄 보기

호스트 표시줄 보기에는 트랜잭션 줄이 창 전체에 표시되며, 선택한 호스트의 아이콘은 맨 아래에 표시됩니다. [트랜잭션]을 두 번 클릭하면 호스트 목록 표시줄, [명령 목록] 입력란 및 [결과] 입력란이 있는 [업데이트] 대화 상자가 열립니다. 호스트 아이콘을 선택하면, [명령 목록]는 해당 호스트에 관련된 내용으로 바뀝니다. 명령을 선택하면, [결과]는 해당 명령과 관련된 내용으로 바뀝니다.

또는 트랜잭션을 선택한 후 창의 맨 아래에 있는 호스트 아이콘을 두 번 클릭할 수 있습니다. [업데이트] 대화 상자가 나타납니다.



제 8 장: 모니터 및 감사

이 장은 아래의 주제를 포함하고 있습니다:

보안 감사자

보안 감사자 및 시스템 관리자의 가장 중요한 작업 중 하나는 시스템 활동을 감사하거나 모니터링하여 의심스럽거나 올바르지 않은 활동을 감지하는 것입니다. 보안 감사는 보안 환경에서 중요한 역할을 수행하며, eTrust AC 의 보안 감사 특징은 다음과 같습니다.

- 시스템을 액세스한 사용자, 액세스한 리소스 및 리소스에 액세스한 시기 표시
- 시도가 실패한 경우에도 보안 위반이 시도되었으면 해당 사용자에게 통지 및 경고
- 보안 규칙의 변경사항 및 변경한 사용자 표시
- 적용 전에 액세스 규칙 효과 테스트 방법 제공

eTrust AC 감사는 실제 수행되는 감사를 모델로 합니다. 사용자가 구현사항을 변경할 수 있더라도 보안 감사자는 시스템 및 보안 관리자와 독립적으로 활동하며, 일부 다른 모델이 사용자 환경에 대해 더 적합한 경우에도 보안 감사자의 활동을 제약할 수 없습니다.

보안 감사자는 AUDITOR 속성이 할당되는 사용자입니다. 보안 감사자로 정의된 사용자는 사용자 및 리소스에 할당된 감사 규칙 변경과 같은 감사 작업을 수행할 수 있습니다. 또한 ADMIN 속성 없이 eTrust AC 감사 유틸리티를 사용할 수 있는 권한도 가집니다.

Access Control 활동 모니터

The eTrust AC 추적은 eTrust AC 시스템에서 수행된 모든 작업을 보여주는 실시간 로그입이며, 추적 레코드는 eTrustACDir\log\seosd.trace(여기서 eTrustACDir 는 eTrust AC 을 설치한 디렉터리)에 누적됩니다.

또는 다음과 같이 레지스트리 하위 키에 *trace_file* 값으로 지정한 파일마다 누적됩니다.

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\eTrustAccessControl\SeOSD\
```

추적 파일에서 레코드를 필터링할 수 있지만 추적 메커니즘은 보안 감사가 아닌 시스템 모니터를 위해 설계되었습니다.

기본적으로 eTrust AC 는 eTrust AC 초기화 중에만 추적 메시지를 생성합니다. eTrust AC 가 초기화되면 추적 메커니즘을 중지하여 추적 메시지는 생성되지 않습니다.

추적 레코드 필터링

추적 필터 파일을 사용하여 특정 유형의 활동이 추적 파일에 표시되지 않도록 지정할 수 있습니다. 추적 필터 파일은 다음과 같이 레지스트리 키의 *trace_filter* 값을 사용하여 지정합니다.

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\eTrustAccessControl\SeOSD
```

기본값은 *eTrustACDir*\log\trcfilter.ini(*eTrustACDir* 는 eTrust AC 를 설치한 디렉터리)입니다.

중요: eTrust AC 는 다음 줄을 사용하여 설치 시 추적 필터 파일을 작성합니다. *seosd.trace*. 이 레코드를 절대로 삭제하지 마십시오.

추적 필터 파일의 각 줄은 추적하지 **않아야** 하는 액세스 또는 활동을 나타냅니다. 예를 들어, Microsoft Word 에 대한 사용자 액세스 추적을 제거하려면, 추적 필터 파일에 다음 줄을 추가하십시오.

```
*winword.exe*
```

감사 레코드 필터링

생성될 수 없는 감사 레코드를 정의함으로써 호스트의 감사 레코드를 필터링하려면 audit.cfg 파일(*eTrustACDir*\data 에 있음)을 사용할 수 있습니다. 각 줄은 감사 정보를 필터링하는 규칙을 나타냅니다(예를 들어, 줄에 있는 기준에 일치하는 감사 기록은 감사 파일에 나타나지 않습니다). 이렇게 하면 필요한 레코드만 저장되므로 seos.audit 파일 크기를 제한하는 데 유용합니다. 클래스 이름, 개체 이름, 사용자 이름, 그룹 이름, 프로그램 이름, 액세스 권한 및 인증 결과에 대한 필터링 규칙을 설정할 수 있습니다. eTrust AC 엔진(seosd)은 시작 시에 이 파일을 읽습니다.

구문

```
GHOST;로그인 정보;<user>;<program-path>;<access-mode>;<auth-result>
```

참고: 열에 있는 *는 모든 값을 의미하는 와일드카드입니다.

메시지를 감사 파일에 보낼 때 seosd 는 메시지가 audit.cfg 파일에 있는 다음 항목 중 하나와 일치하는지 여부를 검사합니다.

필드	규칙
클래스	클래스 이름은 대문자로 기록해야 합니다.
개체	리소스 이름은 패턴(*)을 사용하여 기록할 수 있습니다.
사용자	사용자 이름은 패턴(*)을 사용하여 기록할 수 있습니다.
프로그램 경로	사용 중인 프로그램은 패턴(*)을 사용하여 기록할 수 있습니다.
액세스 모드	액세스 권한은 규칙을 준수해야 합니다.
인증 결과	인증 결과는 P(허용) 또는 D(거부)여야 합니다. **참고:** *P* 값은 또한 경고 모드에서 리소스로 생성된 감사 기록을 필터링합니다.

TCP 클래스 구문:

```
GHOST;로그인 정보;<host>;<program-path>;<access-mode>;<auth-result>
```

예: 감사 액세스 필터

다음 예제에서 관리자가 성공적으로 파일을 읽으면 seosd 는 감사 파일로 메시지를 전송하지 않습니다. 관리자가 파일을 읽을 수 없으면 seosd 는 감사 파일로 메시지를 전송합니다.

```
FILE;*;Administrator;*;R;P
```

감사 규칙 설정

보안 감사를 위해 eTrust AC 는 데이터베이스에 정의된 감사 규칙에 따라 액세스 거부 및 허용 이벤트에 대한 감사 레코드를 유지합니다.

모든 액세서와 리소스는 다음 값 중 하나 이상으로 설정될 수 있는 AUDIT 속성을 가집니다.

FAIL

액세서의 리소스 액세스 실패를 로그 파일에 기록합니다.

SUCCESS

액세서의 리소스 액세스 성공을 로그 파일에 기록합니다.

LOGINFAIL

액세서의 모든 로그온 실패를 로그 파일에 기록합니다. (이 값은 리소스에 적용되지 않습니다.)

LOGINSUCCESS

액세서의 모든 성공적인 로그온을 로그 파일에 기록합니다. (이 값은 리소스에 적용되지 않습니다.)

ALL

액세서의 경우 FAIL, SUCCESS, LOGINFAIL 및 LOGINSUCCESS 와 같은 정보를 로그 파일에 기록하고, 리소스의 경우 FAIL 및 SUCCESS 와 같은 정보를 로그 파일에 기록합니다.

없음

액세서 또는 리소스와 관련된 어떤 정보도 로그 파일에 기록하지 않습니다.

데이터베이스에서 액세서 또는 리소스 레코드를 작성하거나 업데이트할 때마다 AUDIT 속성을 지정할 수 있습니다. 또한 기록된 이벤트의 전자 메일 통지를 전송해야 하는지 여부와 전자 메일 통지의 수신인을 지정할 수 있습니다. ("관리자 인터페이스 사용" 장에 설명된 정책 관리자를 사용하거나 또는 *참조 가이드*의 "selang 명령 언어" 장에 설명된 대로 selang 명령을 사용하여 데이터베이스의 레코드를 작성 및 업데이트할 수 있습니다.)

감사 로그의 레코드는 이러한 감사 규칙에 따라 누적됩니다. 이벤트를 어떤 기준에 따라 로그 파일에 기록할지 여부는 다음 사항에 따라 결정됩니다.

- 리소스 또는 액세서에 AUDIT(ALL)가 있는 경우, eTrust AC 에서 보호되는 해당 리소스에 대한 액세서와 모든 이벤트에 대한 모든 로그인 이벤트가 액세스 성공 여부에 상관 없이 기록됩니다.
- eTrust AC 에서 보호되는 리소스에 대한 액세스가 성공하고 사용자 또는 리소스에 AUDIT(SUCCESS)가 있는 경우 이벤트가 로그 파일에 기록됩니다.
- eTrust AC 에서 보호되는 리소스에 대한 액세스가 실패하고 액세서 또는 리소스에 AUDIT(FAIL)가 있는 경우 이벤트가 로그 파일에 기록됩니다.

Windows 에서 감사 정책 설정

액세서 및 리소스에 대한 액세스 규칙 설정 외에도 감사 로그에 기록할 Windows 이벤트를 지정할 수 있습니다. 감사 정책은 전체 조직에 대해 또는 사용자별로 지정할 수 있습니다.

감사 로그

감사 규칙 및 감사 정책에 정의한 이벤트 또는 액세스에서 작성된 감사 레코드는 감사 로그라는 파일을 구성합니다. 다음 Windows 레지스트리 하위 키의 *audit_log* 값은 감사 로그 위치를 지정합니다.

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\eTrustAccessControl\logmgr
```

키의 기본값은 다음과 같습니다.

```
*\Program Files\CA\eTrustAccessControl\log\seos.audit
```

기본적으로 eTrust AC 는 감사 로그 파일의 이름을 변경하고 새 이름을 작성하여 1024KB 에 도달할 때 감사 로그를 자동으로 백업합니다. 하위 키의 *audit_size* 값을 변경하여 백업을 수행하는 감사 로그 크기를 변경할 수 있습니다.

```
HKEY_LOCAL_MACHINE\Software\ComputerAssociates\eTrustAccessControl\logmgr
```

또한 Windows 레지스트리 하위 키에서 *BackUp_Date* 값을 변경하여 감사 로그를 일별, 주별 또는 월별과 같이 주기적으로 해당 감사 로그를 백업하도록 선택할 수 있습니다.

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\eTrustAccessControl\logmgr
```

참고: 레지스트리 하위 키에 대한 자세한 내용은 *참조 가이드*를 참조하십시오.

나중에 이벤트를 검사할 수 있도록 테이프에 기존 감사 로그를 보관하는 것을 고려해야 합니다.

감사 로그 사용

eTrust AC 는 감사 로그 보기, 필터링 및 검색을 위한 다음과 같은 두 개의 기본 도구를 제공합니다.

- 정책 관리자
- seaudit 유틸리티

감사 로그의 모든 레코드를 표시하거나 또는 필터를 사용하여 감사 로그에서 특정 레코드를 선택할 수 있습니다.

이 장의 나머지 부분은 정책 관리자에서 감사 필터를 사용할 때 감사 로그의 레코드를 보는 방법에 대해 설명합니다.

감사 필터

감사 로그의 레코드 수가 엄청나게 많아질 수 있으므로, eTrust AC 에서 표시하는 레코드 수를 줄이려면 필터를 사용하여 표시할 레코드 유형을 선택하십시오. 시간 또는 이벤트 유형을 포함하는 다양한 기준에 따라 이벤트를 필터링할 수 있습니다.

이름을 할당한 후 하나 이상의 스위치를 선택하여 정책 관리자에서 필터를 작성합니다. 추가 스위치와 0 개, 1 개 또는 여러 개의 옵션을 선택할 수 있습니다. 또한 seaudit 유틸리티를 사용하여 레코드를 필터링할 수 있습니다.

정책 관리자는 여러 개의 미리 정의된 필터를 제공하며 자체 필터를 작성할 수 있습니다.

기본적으로 eTrust AC 는 *eTrustACDir*\data\AuditFilters.flt(*eTrustACDir* 는 eTrust AC 를 설치한 디렉터리임)에 모든 감사 필터를 저장합니다.

작성한 필터를 파일에 저장하도록 선택하거나 다른 파일에 필터를 저장할 수 있습니다.

스위치

INet host service

지정된 서비스의 지정된 호스트에서 받은 TCP 요청의 INET 감사 레코드를 나열합니다. Host 와 service 는 모두 검색된 호스트 및 서비스 집합을 나타내는 마스크입니다.

LOGON user terminal

다음 항목을 표시합니다.

- 지정된 터미널의 지정된 사용자에 대한 LOGIN 레코드. *user* 와 *terminal* 은 모두 마스크입니다.
- 잘못된 암호를 여러 번 입력했을 때 권한 부여 엔진에서 작성된 레코드

Resource class resource user

리소스 레코드를 나열합니다. 다음 항목을 지정할 수 있습니다.

- *Class*-액세스된 리소스가 속한 클래스를 나타내는 마스크입니다.
- *Resource*-액세스된 리소스의 이름을 나타내는 마스크입니다.
- *User*-리소스를 액세스한 사용자의 이름을 나타내는 마스크입니다.

시작

eTrust AC 서비스에서 시작 및 종료 메시지를 나열합니다.

Update (cmd, class, object, user)

데이터베이스 업데이트 감사 레코드를 표시합니다. 다음 항목을 지정할 수 있습니다.

- *Cmd*-검색할 selang 명령 집합을 나타내는 마스크입니다.
- *Class*-검색할 클래스를 나타내는 마스크입니다.
- *Object*-검색할 레코드를 나타내는 마스크입니다.
- *User*-명령을 실행한 사용자를 나타내는 마스크입니다.

Watchdog

Watchdog 감사 레코드를 나열합니다.

모두

추적 기능으로 감사 로그에 전송된 레코드를 제외한 모든 레코드를 나열합니다.

옵션

Ending date

종료 날짜를 지정합니다. 지정된 날짜 이후에 기록된 레코드는 나열되지 않습니다.

Ending time

종료 시간을 지정합니다. 지정된 시간 이후에 기록된 레코드는 나열되지 않습니다.

No failure

실패가 나열되지 않도록 지정합니다.

No granted

성공한(허용된) 액세스가 나열되지 않도록 지정합니다.

No logout

로그아웃 레코드가 나열되지 않도록 지정합니다.

Internet address

TCP/IP 레코드에 호스트 이름 대신 인터넷 주소가 나열되도록 지정합니다.

No notify

NOTIFY 감사 레코드가 나열되지 않도록 지정합니다.

No password

암호 시도 레코드가 나열되지 않도록 지정합니다.

원본 *호스트*

지정된 호스트에서 발생하는 레코드만 나열되도록 지정합니다. 이 옵션은 UNIX 워크스테이션에 연결된 경우에만 적용됩니다.

Start date

시작 날짜를 지정합니다. 지정된 날짜 전에 기록된 레코드는 나열되지 않습니다.

Starting time

시작 시간을 지정합니다. 지정된 시간 전에 기록된 레코드는 나열되지 않습니다.

Show port number

서비스 이름 대신 포트 번호가 나열되도록 지정합니다.

경고 없음

경고 레코드가 나열되지 않도록 지정합니다.

미리 정의된 필터

eTrust AC 에는 다음과 같이 미리 정의된 필터가 함께 제공됩니다.

모두

감사 로그의 모든 레코드를 표시합니다. 필터링이 발생하지 않습니다.

오늘

오늘 작성된 모든 레코드를 표시합니다.

지난 2 일 간의 레코드

어제와 오늘 작성된 모든 레코드를 표시합니다.

지난 7 일 간의 레코드

최근 7 일 동안 작성된 레코드를 표시합니다.

Access Control 서비스에 연결

사용자가 정책 관리자 또는 selang 과 같은 eTrust AC 서비스에 연결할 때 나타나는 레코드를 표시합니다.

참고: UNIX 워크스테이션에 연결할 경우, 해당 필터의 이름이 로그인 레코드가 됩니다. 레코드는 사용자 로그인을 나타냅니다.

관리 작업

eTrust AC 또는 운영 체제 데이터베이스를 업데이트하는 모든 레코드를 표시합니다. 데이터베이스 업데이트에는 모든 유형의 레코드에 대한 추가, 삭제 및 변경이 포함됩니다.

사용자 정의 필터

필요한 만큼의 필터를 작성할 수 있습니다. 중요한 필터를 선택한 후 필터에 이름을 지정합니다. eTrust AC 는 정책 관리자를 호출할 때 재사용할 수 있도록 필터를 자동으로 저장합니다.

경고 모드

보안 정책을 단계적으로 실행할 때, 실제로 제한사항을 적용하지 않고 특정 리소스 액세스 제한사항의 동작을 검사하는 것이 유용하다는 것을 알 수 있습니다. 다음과 같은 경우 이 방법이 특히 유용합니다.

- 해당 규칙에 따라 보안 정책을 수정할 수 있도록, 설정하려는 규칙이 너무 엄격하거나 완화된 것인지 판단할 경우
- 제한사항이 시스템 응용 프로그램의 실행에 부정적인 영향을 미칠 수 있다고 의심될 경우

eTrust AC 를 사용하여 제한 사항을 지정하고 제한 사항 적용에 대한 경고 메시지를 대체할 수 있습니다.

경고 모드 구현

경고 모드를 구현하려면:

- 테스트할 규칙이 적용되는 모든 리소스 레코드에서 WARNING 매개 변수를 설정합니다.
- 정책 관리자에서 리소스 작성 또는 수정 시 [감사]를 선택한 후 [경고] 상자를 선택합니다.
- selang 에서 newres, editres 또는 chres 명령과 함께 warning 매개 변수를 사용합니다.

  참고: chres/editres/newres 명령에 대한 자세한 내용은 *참조 가이드*를 참조하십시오.

리소스에 대해 경고 모드를 설정하고 액세서에게 요청된 방법으로 리소스를 액세스할 권한이 부여되지 않은 경우, eTrust AC 는 경고 메시지를 작성하고 액세스(경고 모드가 유효하므로 위반 설명이 허용됨)를 로그 파일에 기록한 후 리소스에 대한 액세스를 허용합니다.

참고:

- eTrust AC 는 경고 모드에서 리소스 그룹에 대한 경고 메시지를 작성하지 않습니다.
- eTrust AC 구현 중에 경고 모드를 사용할 경우, 감사 로그를 저장할 수 있는 디스크 공간이 충분한지 확인하고 감사 로그의 크기 제한이 적합한지 확인합니다.

제 9 장: Unicenter 마이그레이션 및 통합

이 장은 아래의 주제를 포함하고 있습니다:

Unicenter 통합 도구 설치

eTrust AC는 Unicenter 엔터프라이즈 관리 환경에 완전 통합되었습니다. 다음 절에서는 eTrust AC가 통합을 처리하는 방법에 대해 설명합니다.

중요: eTrust AC와 Unicenter TNG를 통합하려면 Unicenter TNG가 eTrust AC와 동일한 컴퓨터에 설치되어 있어야 합니다.

참고: Windows 환경에서의 전체 설치 지침은 *구현 가이드*를 참조하십시오.

Unicenter 통합 기능

다음 절에서는 eTrust AC가 Unicenter TNG와 통합되는 방법에 대해 설명합니다.

SSF/EMSec API 지원

Windows 채널의 EMSec API는 단일 DLL을 호출합니다. Unicenter 통합 설치에 대한 EMSec 지원은 교체 CAUSECR.DLL로 이루어집니다. 이 DLL은 EMSec API에 대한 호출을 수신한 후 동일한 eTrust AC API에 이러한 요청을 다시 지정하고 리디렉션합니다. eTrust AC API의 반환 코드는 해당하는 EMSec API 반환 코드로 다시 변환되고 EMSec API 호출자에게 제어가 반환됩니다. 이 방법은 현재 EMSec API를 사용하는 기존 응용 프로그램의 무결성을 보호합니다.

EMSec 지원은 Unicenter 통합 설치 프로시저가 완료된 후 활성화됩니다. Unicenter 통합 설정은 Unicenter 설치 경로(CAIGLBL0000 디렉터리)의 현재 CAUSECR.DLL을 대체합니다. 이 때 수신 EMSec API 요청을 교체 CAUSER.DLL이 인터셉트해서 eTrust AC API에서 요청된 정보를 원활하게 검색합니다.

Unicenter Security 데이터 마이그레이션 기능

다음 절에서는 Unicenter Security 데이터를 eTrust AC 로 마이그레이션하는 방법에 대해 설명합니다.

Unicenter Security 옵션 마이그레이션

eTrust AC 에는 선택된 Unicenter Security 옵션을 추출하고 이들 옵션에 따라 대상 eTrust AC 데이터베이스를 사용자 정의하는 MigOpts.exe 라는 프로그램이 포함되어 있습니다. 이 기능을 활성화하려면 Unicenter Security 데이터 마이그레이션 설치 프로시저에 따라 Unicenter 통합을 실행해야 합니다. 설치 절차에서는 MigOpts.exe 를 자동으로 실행합니다.

참고: 다음 Unicenter Security 옵션은 eTrust AC 환경에 **완전히** 마이그레이션될 수 있습니다.

- AUDIT_LOGIN
- MODIFY_PWDNEVEREXP
- PWDQUEUESIZE
- SEC_AUDIT_DBUPDATE
- SEC_AUDIT_SEND
- SEC_PASSWORD_ALPHA
- SSF_MAXPWDVIO
- SSF_MINPWDLEN
- SSF_SECPWEXCL
- USER_DEFSESID
- USER_PWDCHANGE
- USER_PWDCHGMAXDAYS
- USER_PWDCHGMINDAYS
- USER_PWDMAINT

참고: USER_PWDMAINT 는 기존 Unicenter Security 데이터에 지정된 eTrust AC 환경으로 마이그레이션됩니다. eTrust AC 는 암호 정보를 유지 관리하지만 이 프로세스는 자동으로 수행되지 않습니다. 기존 Unicenter TNG 사용자를 Unicenter Security 로부터 eTrust AC 데이터베이스로 내보낼 때, USER_PWDMAINT 옵션 값이 yes 일 경우 수동 프로세스가 자동으로 수행됩니다. 그러나 마이그레이션 완료 후 관리자가 암호 정보를 추적해야 할 새 사용자를 추가할 경우 관리자는 "__workload__" 응용 프로그램 개체가 존재하는지 추가로 확인해야 합니다. 예:

```
eTrust> na __workload__;
```

그런 다음 관리자는 "__workload__" 응용 프로그램 개체를 포함하도록 사용자의 로그인 정보를 업데이트해야 합니다. 예:

```
eTrust> el (Username) appl('__workload__');
```

또한 ExportTngDb.exe 는 eTrust AC 에 추가하기 전에 사용자의 관리자 속성을 설정하여 **SSF_AUTH** Unicenter Security 옵션의 구성원인 Unicenter TNG 사용자를 eTrust AC 환경으로 마이그레이션합니다.

Unicenter Security 데이터베이스 마이그레이션

eTrust AC 는 Unicenter Security 데이터베이스에서 데이터를 추출하여 eTrust AC 데이터베이스에 채우기 위해 eTrust AC 명령으로 변환하는 ExportTngDb.exe 라는 프로그램 기능을 갖고 있습니다. ExportTngDb.exe 는 다음 항목을 마이그레이션합니다.

- Unicenter Security 사용자
- Unicenter Security 사용자 그룹
- Unicenter Security 규칙

참고:

- Unicenter 통합 및 마이그레이션 설치 프로세스를 실행한 후 Unicenter TNG 로그인 인터셉트를 실행하는 것을 권장하지 않습니다. Unicenter 통합 및 마이그레이션 설치 프로세스가 성공적으로 실행되면 Unicenter TNG 로그인 인터셉트가 비활성화되었는지 확인해야 합니다.
- Unicenter TNG Data Scoping 규칙(-DT 접미사를 가진 Unicenter TNG 자산 유형이 대상인 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, CA-UPSNODE. 이러한 자산 유형 또는 파생 항목을 대상으로 하는 규칙은 마이그레이션 프로세스 중에 무시됩니다.

ExportTngDb.exe 를 활성화하려면 Unicenter Security 데이터 마이그레이션 설치 프로시저에 따라 Unicenter 통합을 실행해야 합니다. 설치 프로시저는 Unicenter Security 데이터 마이그레이션 프로세스를 자동으로 수행합니다.

참고: 모든 Unicenter TNG 개체의 작성 및 수정 통계는 마이그레이션 프로세스 중에 손실됩니다.

Unicenter TNG 와 eTrust AC 제품은 서로 다르기 때문에 다음과 같은 Unicenter Security **사용자** 사용자 특성은 eTrust AC 에 마이그레이션될 수 없습니다.

Statistics

다음 사용자 통계는 eTrust AC 에서 지원하지 않습니다.

- 마지막 로그인 통계 (날짜 및 시간 , 마지막 로그인의 노드)
- 암호 변경 통계(날짜 및 시간, 노드, 마지막으로 암호를 변경한 사용자 및 암호 만료 날짜)
- 암호 위반 통계 (날짜 및 시간 , 마지막으로 실패한 로그인의 노드 및 마지막으로 성공한 로그인 이후 실패한 로그인 수)
- 액세스 위반 통계 (날짜 및 시간 , 마지막 액세스 위반의 노드 및 액세스 위반 수)
- 보류 통계 (보류 날짜 및 시간)

PWDCHANGE VALUE (RANDOM)

임의의 암호 생성

UPSSTATGROUP

UPS 스테이션 그룹

- eTrust AC 에서 지원하지 않습니다.

USERORIGIN

사용자의 원래 위치(NIS 또는 Local)

VIOLMODE

위반 모드(FAIL, MONITOR, WARN, QUIET)

- eTrust AC 는 FAIL 모드만 지원합니다.

VIOLACTION

위반 작업(CANUSER, CANU&LOG, CANU&LOG&SUS)

- eTrust AC 는 CANUSER 작업만 지원합니다.

Unicenter TNG 와 eTrust AC 제품은 서로 다르기 때문에 다음과 같은 Unicenter Security **규칙** 특성은 eTrust AC 에 마이그레이션될 수 없습니다.

EXPIRES

규칙 만료 날짜는 eTrust AC 에서 지원하지 않습니다.

Unicenter User Exit 지원

마이그레이션을 돕기 위해 eTrust AC 는 이제 eTrust AC 환경에서 변경되지 않은 기존의 Unicenter Security user exit 을 실행할 수 있습니다. 모든 user exit 를 마이그레이션의 일부로 다시 작성할 필요가 없습니다.

Unicenter Security 및 eTrust AC 의 기존 user exit 인터페이스만 사용하면 설치된 각 구성 요소가 표준 eTrust AC user exit 으로 등록되어 해당 Unicenter Security exit 을 표시합니다.

이 기능을 시작하려면 Unicenter Security 데이터 마이그레이션 설치 프로시저에 따라 Unicenter 통합을 실행합니다. 설치 프로시저가 완료되면 이 기능이 활성화됩니다.

참고: Unicenter TNG 및 eTrust AC 는 다른 아키텍처를 사용하기 때문에 Unicenter Security 와 eTrust AC 사이의 호환 가능한 exit 지점 및 데이터 항목만 지원됩니다. 다음과 같은 Unicenter Security exit 지점이 지원됩니다.

EmSec_CredExit()

Unicenter Credential Authentication exit 인 EmSec_CredExit()에 대한 입력은 EMSECSIGNON 에 의해 매핑됩니다. eTrust AC 의 경우 이 구조 내의 사용자 및 노드 구성원만 의미있는 데이터를 갖습니다. 사용자 구성원은 인증될 사용자 이름으로 설정되고 노드 구성원은 현재 로컬 노드 이름으로 설정됩니다. EMSECSIGNON 구조의 다른 모든 구성원은 이진수 0 으로 설정됩니다. Unicenter Resource Check Exit 로부터 다시 전달된 메시지, 기타 매개 변수 및 상세 반환 코드가 무시됩니다.

EmSec_PwExitNew()

Unicenter Password Validation exit 인 EmSec_PwExitNew 에 대한 입력은 사용자(암호를 변경 중인 사용자), 암호(새 암호) 및 노드 이름(eTrust AC 를 지원할 경우 항상 로컬 노드 이름임)으로 구성됩니다. 이 프로그램이 실패할 경우 기존 exit 인 EmSec_PwExit 가 사용됩니다. 입력으로 사용자 및 암호만 포함하며 eTrust AC 에서 완전히 지원됩니다.

EmSecSSFResCheck()

Resource Check exit 인 EmSecSSFResCheck()에 대한 입력은 EMSECRESCHECK 에 의해 매핑됩니다. EMSECRESCHECK 의 사용자 구성원은 액세스 사용자의 값으로 설정됩니다. EMSECRESCHECK 의 클래스 구성원은 액세스의 리소스 클래스 값으로 설정됩니다. EMSECRESCHECK 의 항목 구성원은 개체 이름 값으로 설정됩니다. eTrust AC 액세스 정보가 Unicenter 형식의 액세스 권한으로 변환되어 EMSECRESCHECK 의 속성 구성원에 저장됩니다. EMSECRESCHECK 의 다른 모든 구성원은 바이너리 0 으로 설정됩니다. Unicenter Resource Check Exit 로부터 다시 전달된 메시지, 기타 매개 변수 및 상세 반환 코드가 무시됩니다. Unicenter 통합 설치가 완료되면 이 기능이 활성화됩니다.

Unicenter 달력

Unicenter TNG는 사용자, 그룹 및 리소스에 대한 시간 제한을 설정할 수 있는 달력 기능을 제공합니다. 달력에는 ON 또는 OFF로 설정할 수 있는 15분의 시간 간격이 있습니다. 달력 시간 간격이 OFF로 설정되면 리소스에 액세스할 수 없으며, 달력 시간 간격이 ON으로 설정되면 리소스에 액세스할 수 있습니다.

Windows에서 관리자는 보안 시작 전에만 달력 사용을 설정할 수 있습니다.

참고: Unicenter TNG는 로컬 시스템에 설치해야 합니다. eTrust AC는 로컬 Unicenter TNG 서비스를 사용하여 달력 설정을 검색합니다.

1. eTrust AC 보안을 중지합니다. 다음 명령을 입력합니다.

   ```
   secons -s
   ```

2. Windows 레지스트리에서 다음 하위 키로 이동합니다.

   ```
   HKEY_LOCAL_MACHINE\Software\ComputerAssociates\eTrustAccessControl\UCTNG
   ```

   하위 키에서 TNG_calendars 값을 yes로 설정합니다. TNG_refresh_interval 값을 적합한 시간(분) 값으로 설정합니다.

3. eTrust AC 보안을 시작합니다. 다음 명령을 입력합니다.

   ```
   seosd -start
   ```

eTrust AC 리소스를 달력에 링크하려면, 프롬프트에서 다음 데이터베이스 명령을 작성해야 합니다.

```
eTrust> nr CALENDAR calendar_name
eTrust> nr file C:\myfile.txt calendar (calendar_name) defaccess (a)
```

Unicenter TNG 달력 Access Control 목록(ACL)은 추가적인 보안 제약 조건 기능입니다. 일반적인 Unicenter TNG 달력 속성은 해당 Unicenter TNG 달력 상태에 따라 현재 리소스를 제한합니다. Unicenter TNG 달력 ACL 속성은 Unicenter TNG 달력 상태에 따라 현재 리소스에 대한 특정 사용자 및 그룹의 액세스(또는 액세스 부여)를 제한합니다.

ACL Unicenter TNG 달력 속성의 두 가지 유형에는 일반 및 제한이 있습니다.

- 일반적인 달력 ACL 속성은 ACL 액세스에 따라 리소스에 대한 사용자 또는 그룹 액세스를 허용합니다.
- 제한(거부됨) 달력 ACL 속성은 ACL 액세스에 따라 리소스에 대한 사용자 또는 그룹 액세스를 거부합니다.

일반적인 달력 ACL(CALACL)에 사용자 또는 그룹을 추가하려면 다음 명령을 selang에 입력하십시오.

```
eTrust> auth resource_class_name object_name uid_or_gid_name calendar(calendar name)
access(access_value)
```

예:

```
eTrust> auth file file1 uid(george) calendar(basecalendar) access(r w)
```

거부된 달력 ACL 에 사용자 또는 그룹을 추가하려면 다음 명령을 selang 에 입력하십시오.

```
eTrust> auth resource_class_name object_name uid_or_gid_name
calendar(TNG_calendar_name) deniedaccess(access_value)
```

예:

```
eTrust> auth file file2 uid(george) calendar(holidays) access(r w)
```

동일한 리소스(calendar, uid 등)에 대해 일반 및 제한 속성을 사용할 수 있습니다. 다음 명령은 읽기 권한을 가진 George 라는 사용자를 파일 1 에 대한 거부된 일정 ACL 에 추가합니다.속성제한적

```
eTrust> auth file file1 uid(george) calendar(holidays) deniedaccess(r)
```

Unicenter TNG 달력 ACL 속성에서 사용자 또는 그룹을 제거하려면 다음과 같이 auth-를 사용하십시오.

```
eTrust> auth- file file2 uid(george) calendar(holidays)
```

특정 리소스에 할당된 모든 Unicenter TNG 달력 ACL 을 표시하려면 Show Resource(sr) 명령을 사용하십시오.

```
eTrust> sr file file1
```

Unicenter 의 인증

- 다음 기능은 Unicenter TNG 2.2 SP1, Unicenter TNG 2.4 또는 Unicenter NSM 3.0 에서 사용됩니다.
  - "이벤트"보내기
  - 메인프레임 암호 동기화
  - Unicenter TNG 달력 사용

부록 A: 메인프레임과 암호 동기화

이 장은 아래의 주제를 포함하고 있습니다:

암호 동기화 지원

eTrust AC 는 eTrust CA-Top Secret Security, eTrust CA-ACF2 Security 또는 RACF 보안 제품을 실행하는 메인프레임과 eTrust AC 를 실행하는 Windows 또는 UNIX 시스템 간의 암호 동기화를 지원합니다. 동기화는 표준 eTrust AC 암호 정책 모델 메커니즘을 사용하여 수행됩니다.

암호 정책 모델 방법

메인프레임을 사용하여 암호 동기화를 네트워크에 구현하려면 메인프레임에 대한 상위 역할을 수행할 eTrust AC 를 실행하는 Windows 시스템을 선택하고 메인프레임 암호 동기화 옵션이 선택한 Windows 시스템에 설치되었는지 확인해야 합니다. 그런 다음, eTrust AC 에 대한 메인프레임을 정의하고 이 메인프레임을 Windows 컴퓨터에 있는 암호 정책 모델에 구독시킵니다. 이 작업을 완료하면, 메인프레임 사용자의 암호 변경사항은 암호 정책 모델 계층의 모든 시스템에 전파됩니다.

메인프레임 관리자에게 암호를 변경할 수 있는 eTrust AC 권한을 부여한 경우, 관리자가 메인프레임에서 수행하는 사용자 암호 변경, 일시 중지 또는 다시 시작 등의 사용자 작업이 암호 정책 모델 계층을 통해 메인프레임에서 전파됩니다. 마찬가지로 암호 정책 모델 계층의 모든 위치에서 수행된 관리 암호 변경, 일시 중지, 다시 시작 등의 사용자 작업이 메인프레임에 전파됩니다.

암호 동기화 설치 요구사항

메인프레임

Unicenter TNG 2.2 SP1, Unicenter TNG 2.4, Unicenter NSM 3.0 또는 CA Common Services 가 컴퓨터에 설치되어야 합니다. 암호 동기화 유틸리티는 Unicenter TNG 의 기본 CAICCI(Common Communication Interface)에 따라 결정됩니다.

다음 위치에서 암호 동기화에 대한 메인프레임 구성 지침을 찾을 수 있습니다.

- eTrust CA-ACF2 Security 의 경우 eTrust CA-ACF2 Security 관리자 가이드
- eTrust CA-Top Secret Security 의 경우 *eTrust CA-Top Secret Security 사용자 가이드*
- RACF 의 경우 CA Common Services 설치 CD

Windows

암호 동기화를 위한 메인프레임의 상위로 사용할 각 Windows 컴퓨터에서 [Mainframe Password Synchronization(메인프레임 암호 동기화)] 옵션을 사용하여 eTrust AC 를 설치해야 합니다.

참고: eTrust AC 를 이미 설치한 경우에는 설치 프로그램을 다시 실행하여 [Mainframe Password Synchronization(메인프레임 암호 동기화)] 옵션을 선택할 수 있습니다. 재설치를 통해 현재 데이터베이스 또는 설정이 변경되지는 않습니다.

설치를 시작하기 전에 시스템의 정책 모델에 구독할 각 메인프레임에 대한 호스트 이름, SYSID 및 관리자 이름이 필요할 수도 있습니다. 설치 시 이 정보에 대한 액세스 권한이 없으면 해당 설치 부분을 건너뛰고 나중에 메인프레임을 구독할 수 있습니다.

eTrust AC 설치 프로그램을 시작하려면 [사용자 정의 설치]를 선택한 후 [Mainframe Password Synchronization(메인프레임 암호 동기화)]옵션을 선택하십시오. 설치 마법사는 Unicenter CAICCI 패키지를 사용하지만 CAICCI 구성을 업데이트하려면 Unicenter TNG 를 재시작해야 합니다.

이렇게 설치되면 호스트를 정책 모델에 구독할수 있습니다. 메인프레임에 대한 호스트 이름 및 SYSID 를 가지고 있으면 이들 호스트를 지금 구독할 수 있습니다. 그렇지 않으면 이 단계를 건너 뛰고 이러한 호스트를 나중에 구독할 수 있습니다.

설치 확인

eTrust AC 설치를 완료했으면, 필요한 서비스와 프로세스가 성공적으로 설치되었는지 다음과 같이 확인할 수 있습니다.

1. Windows 서비스 애플릿(Windows NT 의 경우 시작, 설정, 제어판, 서비스를 차례로 선택 또는 Windows 2000 의 경우 시작, 설정, 제어판, 관리 도구, 서비스를 차례로 선택)을 사용하여 서비스 목록을 확인합니다.

   다음 서비스가 서비스 목록에 나타납니다.

   - Unicenter (NR-Server)
   - Unicenter (Remote)
   - Unicenter (Transport)

   eTrust AC Main Frame Sync

2. Windows 작업 관리자를 열고 프로세스 탭을 선택합니다.

   다음 프로세스가 목록에 나타납니다.

   - mfscpfd.exe
   - mfsd.exe
   - eacmfs.exe

설치 중에 메인프레임 호스트를정책 모델에 구독한 경우, 다음과 같이 구독자 목록에 표시되는지 확인하십시오.

1. [시작] 메뉴에서 프로그램, [CA], [eTrust Access Control], [정책 관리자]를 선택합니다.
2. 왼쪽 패널의 맨 아래에 있는 [Tools] 버튼을 클릭합니다.
3. 정책 모델] 아이콘을 클릭합니다.
4. 트리 보기에서 설치 도중 메인프레임을 구독한 정책 모델을 선택합니다.
5. 구독한 메인프레임 호스트가 오른쪽 목록에 표시되는지 확인합니다.

정책 모델 구성 완료

메인프레임과 상위 Windows 시스템에 적합한 소프트웨어를 설치했으면 Windows 시스템에서 다음 작업을 수행하여 암호 동기화에 필요한 구성을 완료해야 합니다.

- 정책 모델에 구독할 각 메인프레임 호스트에 대해 PMDB 에 MFTERMINAL 레코드를 작성합니다.

  로컬 데이터베이스 대신 PMDB 에 레코드를 작성하면 이 레코드는 정책 모델계층에 있는 모든 호스트로 전파됩니다.

- 암호 변경을 작성하는 각 메인프레임 관리자에 대하여 PMDB 와 기본 Windows 환경에 USER 레코드를 작성하여 eTrust AC 가 암호를 변경할 수 있는 권한을 인식하도록 사용자에게 관리자 또는 암호 관리자 권한을 부여합니다.
- 다시 PMDB 에서 메인프레임 관리자에게 Windows 컴퓨터의 경우 TERMINAL 레코드에 대한 전체 액세스 권한(읽기 및 쓰기)을 부여하고, 암호 변경을 작성할 수 있는 메인프레임의 경우 MFTERMINAL 레코드에 대한 읽기 액세스를 부여합니다.
- 기본 Windows 환경에서 로컬로 로그온 권한을 메인프레임 관리자에게 부여합니다. 메인프레임에서 수신된 암호 변경 사항은 해당 메인프레임 관리자 사용자 권한이 부여된 상태에서 로컬 컴퓨터의 eTrust AC 에서 실행할 수 있어야 합니다.
- 메인프레임을 정책 모델에 구독킵니다(설치 중에 이 작업을 수행하지 않은 경우).
- 로컬 컴퓨터 및 구독자의 암호 변경사항에 대하여 암호 정책 모델을 지정하는지 확인하려면 Windows 레지스트리에서 passwd_pmd 키를 확인합니다. 필요에 따라 레지스트리 항목을 업데이트합니다.

이러한 항목은 특정 순서로 수행할 필요가 없지만, 관리자의 사용자 레코드 및 메인프레임의 MFTERMINAL 레코드를 작성할 때까지 메인프레임 관리자에게 MFTERMINAL 레코드에 대한 액세스 권한을 부여할 수 없습니다.

다음 절차는 위와 같은 단계를 수행할 수 있는 한 가지 방법입니다.

1. [시작] 메뉴에서 [프로그램], [CA], [eTrust Access Control], [정책 관리자]를 선택합니다.
2. 설치 도중 정책 모델에 메인프레임을 구독하지 않은 경우, 다음 단계를 수행합니다. 그렇지 않은 경우 3 단계로 이동합니다.
   a. 왼쪽 프로그램 표시행에서 [Tools] 버튼을 클릭합니다.
   b. 정책 모델] 아이콘을 클릭합니다.
   c. 적합한 정책 모델을 선택합니다.
   d. [편집] 메뉴에서 [구독자 추가]를 선택합니다.
   e. [구독자 이름]에서 메인프레임의 완전한 호스트 이름을 입력합니다.
   f. Mainframe 구독자> 상자를 선택합니다.
   g. 메인프레임에 대한 호스트 유형(ACF, ACF2, RACF, TNG 또는 TSS)을 선택한 후 메인프레임의 SYSID 와 관리자 이름을 입력합니다.

h. [확인]을 클릭합니다.

i. 추가할 각각의 메인프레임 구독자에 대해 이 단계를 반복합니다.

3. passwd_pmd 키를 다음과 같이 확인합니다.

   a. 왼쪽 프로그램 표시행에서 Windows NT 버튼을 클릭합니다.

   b. [레지스트리 편집기] 아이콘을 클릭합니다.

   c. 트리 보기에서 다음 위치로 이동합니다.

   `HKEY_LOCAL_MACHINE\Software\ComputerAssociates\eTrustAccessControl\eTrustAccessControl`

   d. 오른쪽 목록에서 passwd_pmd 키를 두 번 클릭합니다.

   e. 해당 항목이 아직 올바르게 지정되지 않은 경우 값 영역에서 [문자열] 버튼을 선택한 후 암호 정책 모델 계층에 있는 로컬 컴퓨터의 상위 항목에 대한 정규화된 이름을 입력합니다.

   f. [확인]을 클릭합니다.

4. 메인프레임 관리자에 대한 USER 레코드를 작성하고 eTrust AC 에서 암호를 변경할 수 있는 권한을 부여한 후 다음과 같이 Windows 에서 로컬로 로그온할 수 있는 사용자 권한을 부여합니다.

   a. 파일, 연결를 선택하거나 도구모음에서 [연결] 버튼을 클릭합니다.

   b. [호스트 선택] 대화 상자에서 localhost pmdb 를 선택하거나 [호스트] 입력란에 *pmdbName*@localhost 를 입력합니다. 여기서 *pmdbName* 은 적합한 정책 모델입니다.

   c. [확인]을 클릭합니다.

   d. 왼쪽 프로그램 표시행에서 [Access Control] 버튼을 클릭합니다.

   e. 사용자] 아이콘을 클릭합니다.

   f. 도구모음에서 [새로 만들기] 단추를 클릭합니다.

   g. [Create New User - General(새 사용자 작성-일반)] 대화 상자에서 메인프레임 관리자의 이름을 입력합니다.

   h. 사용자 특성] 아이콘을 클릭합니다.

   i. 사용자 특성> 대화 상자에서 사용자에게 부여할 권한에 따라 관리자 또는 암호 관리자를 선택합니다.

   j. 기타] 아이콘을 클릭합니다.

   k. 기타> 대화 상자에서 [사용자 권한] 버튼을 클릭합니다.

   l. 사용 가능한 사용자 권한 목록에서 [Logon locally(로컬로 로그온)]를 선택한 후 [>>] 단추를 클릭하여 사용자 권한을 [Privileges Granted(허용된 권한)] 목록으로 이동합니다.

   m. [사용자 권한] 대화 상자를 닫으려면 [확인]을 클릭합니다.

   n. 사용자를 추가하려면 OK 를 클릭합니다.

   o. 각 메인프레임 관리자에 대해 e - n 단계를 반복합니다.

p. 리소스] 아이콘을 클릭합니다.

q. 트리 보기에서 Logon Protection, 터미널을 선택합니다.

r. TERMINAL 레코드 목록에서 로컬 컴퓨터에 대한 레코드를 선택합니다.

s. View or set TERMINAL properties> 대화 상자에서 왼쪽의 [권한 부여] 아이콘을 클릭합니다.

t. 액세서 추가 오른쪽에 있는 [새로 만들기] 버튼을 클릭합니다.

u. 액세서 목록을 찾은 후 목록에서 메인프레임 관리자를 선택합니다.

v. [확인]을 클릭합니다.

w. 사용 권한 영역에서 All 버튼을 선택합니다.

x. 각 메인프레임 관리자에 대해 e - i 단계를 반복합니다.

y. [확인]을 클릭합니다.

5. 정책 관리자를 닫고 selang 을 시작합니다.

6. 다음과 같이 정책 모델에 연결합니다.

```
eTrust> host pmd@localhost
```

7. 다음 명령을 사용하여 각 메인프레임에 대한 MFTERMINAL 레코드를 작성합니다.

```
eTrust> newres MFTERMINAL mfSYSID defaccess (none) owner (userName)
```

여기서 *mfSYSID* 는 메인프레임의 SYSID 이고 *userName* 은 MFTERMINAL 레코드를 소유하는 사용자입니다.

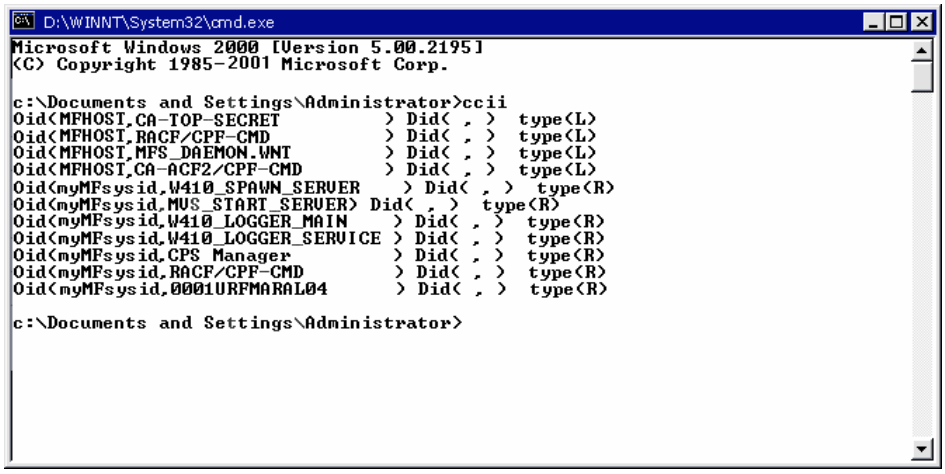
8. 다음 명령을 사용하여 각 메인프레임 관리자에게 적합한 MFTERMINAL 레코드에 대한 액세스 권한을 부여합니다.

```
eTrust> authorize MFTERMINAL mfSYSID uid (mfAdmin) access (read)
```

여기서 *mfSYSID* 는 메인프레임의 SYSID 이고 *mfAdmin* 은 메인프레임 관리자입니다.

메인프레임 동기화 시작

통신이 설정되었는지 확인하려면, 명령 프롬프트에서 ccii 유틸리티를 실행하십시오.



CAICCI 구성 파일

설치 중에 언제든지 메인프레임을 정책 모델, eTrust AC 에 구독할 때는 CAICCI 구성 파일을 자동으로 업데이트합니다.

수동으로 업데이트하려면 다음 절차를 수행하십시오.

1. 메모장에서 CAICCI 구성 파일(*cciDirectory*\tng\caiuser\ccirmtd.rc)을 엽니다.
2. 다음 행을 추가합니다.

   ```
   REMOTE = mfName mfSYSID 1024 startup port 1721
   ```

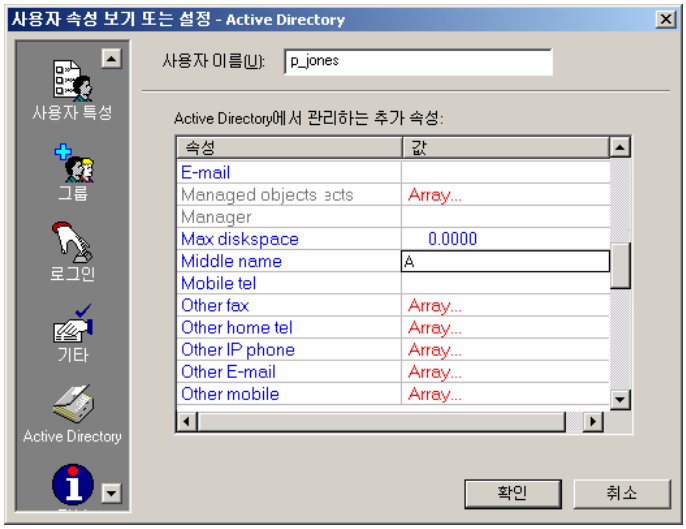
   여기서 *mfName* 은 메인프레임 이름이고 *mfSYSID* 는 메인프레임 SYSID 입니다.
3. 파일을 저장합니다.
4. 원격 CAICCI 서비스를 중지합니다.

   ```
   ccicntrl stop rmt
   ```
5. 원격 CAICCI 서비스를 다시 시작합니다.

   ```
   ccicntrl start rmt
   ```

Active Directory 사용자 또는 그룹 속성 설정

Active Directory 가 설치된 Windows 2000 컴퓨터에 연결되어 있으면 [User or Group Properties] 대화 상자의 [Directory Services] 패널을 사용하여 Active Directory 사용자 또는 그룹 속성을 설정할 수 있습니다. 이러한 속성은 Active Directory 가 없는 Windows NT, Windows 2000 또는 eTrust AC 기본 환경 데이터베이스에서 지원되지 않습니다.



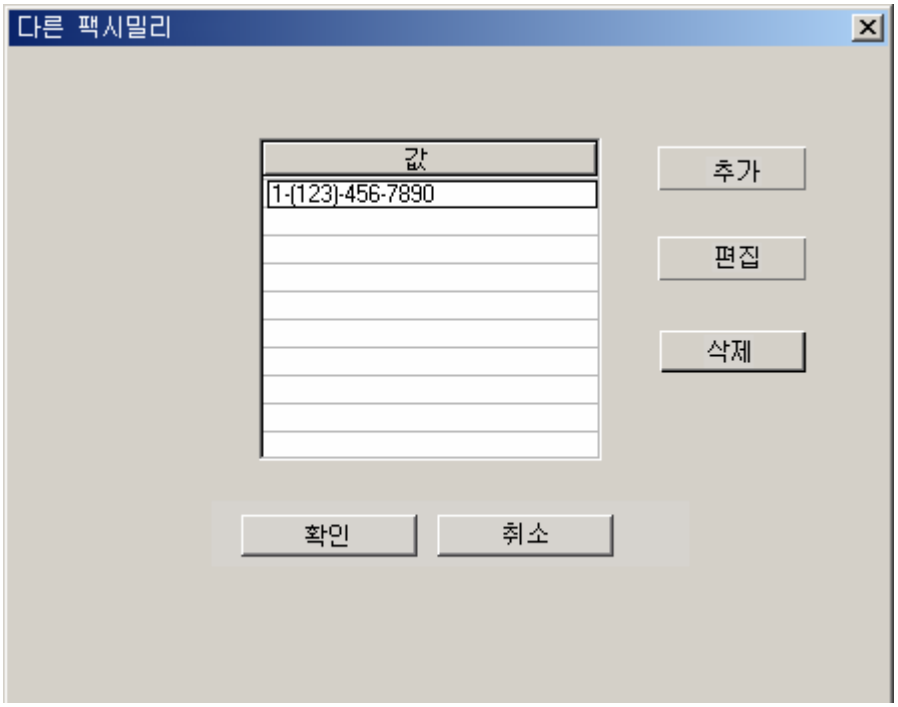
컴퓨터에 Active Directory 가 설치되지 않은 경우, Active Directory 가 설치된 컴퓨터에 연결하십시오. (연결하는 컴퓨터에는 eTrust AC 가 설치되어 있어야 합니다.)

1. 새 사용자를 작성한 후 [Directory Services] 패널을 엽니다.

   참고: 패널을 활성화하는 아이콘은 Active Directory 가 있는 Windows 2000 컴퓨터에 연결되어 있어야 나타납니다.

2. 목록에서 아래로 스크롤합니다. 값을 입력하려면, 표의 Value(오른쪽) 부분을 두 번 클릭합니다. 셀 주위에 입력할 수 있는 상자가 나타납니다.

   참고: Array 라는 단어가 표시된 곳을 두 번 클릭하면, 입력 가능한 표가 있는 대화 상자가 나타납니다.



색인

B

C

D

E

F

G

H

K

L

M

N

O

P

S

T

U

W