CA Access Control Premium Edition

구현 안내서

12.6.01

타사 고지 사항

CONTAINS IBM(R) 32-bit Runtime Environment for AIX(TM), Java(TM) 2 Technology Edition, Version 1.4 Modules

샘플 스크립트와 샘플 SDK 코드

CA Access Control 제품에 포함된 샘플 스크립트와 샘플 SDK 코드는 정보 제공 목적으로만 "있는 그대로" 제공됩니다. 이 항목은 특정 환경에 맞게 수정이 필요할 수 있으며, 프로덕션 환경에 사용하려면 프로덕션 시스템에 배포하기 전에 반드시 테스트 및 검사를 수행해야 합니다.

CA Technologies 는 이러한 샘플에 대한 지원을 제공하지 않으며 이 스크립트로 인한 어떠한 오류에도 책임을 지지 않습니다.

CA Technologies 제품 참조

이 문서는 다음 CA Technologies 제품을 참조합니다 :

- CA Access Control Premium Edition
- CA Access Control
- CA Single Sign-On(eTrust SSO)
- CA Top Secret®
- CA ACF2™
- CA Audit
- CA NSM(CA Network and Systems Management, 이전의 Unicenter NSM 및 Unicenter TNG)
- CA Software Delivery(이전의 Unicenter Software Delivery)
- Unicenter Service Desk(이전 이름: Unicenter Service Desk)
- CA User Activity Reporting Module (이전 명칭: CA Enterprise Log Manager)
- CA Identity Manager

설명서 규칙

CA Access Control 설명서는 다음과 같은 규칙을 따릅니다.

형식	의미
고정 폭 글꼴	코드 또는 프로그램 출력
기울임꼴	강조 또는 새 용어
굵게	표시된 대로 동일하게 입력해야 하는 텍스트
슬래시(/)	UNIX 및 Windows 경로를 기술하는 데 사용되는 플랫폼 독립적인 디렉터리 구분 기호

이 설명서는 또한 명령 구문과 사용자 입력(고정 폭 글꼴로 표시됨)을 설명할 때 다음과 같은 특별한 규칙을 사용합니다.

형식	의미
기울임꼴	반드시 입력해야 하는 정보
대괄호([ ]) 사이	선택적 피연산자
중괄호({ }) 사이	필수 피연산자 집합
파이프(|)로 구분된 선택 사항	대체 피연산자(하나 선택)를 구분합니다. 예를 들어, 다음은 사용자 이름 *또는* 그룹 이름 중 *하나*라는 의미입니다. {*username*|*groupname*}
...	앞의 항목 또는 항목 그룹이 반복될 수 있음을 나타냅니다.
밑줄	기본값
줄 마지막에 공백 다음의 백슬래시(\)	때때로 이 안내서에서 명령이 한 줄에 모두 표시되지 않는 경우가 있습니다. 이런 경우에는 줄 끝에 공백과 백슬래시(\)를 표시하여 명령이 다음 줄에서 계속됨을 나타냅니다. **참고:** 실제 명령을 입력할 때는 이러한 백슬래시를 포함하지 말고 줄바꿈 없이 명령을 한 줄에 입력하십시오. 백슬래시 및 줄바꿈은 실제 명령 구문에 포함되지 않습니다.

예제: 명령 표기 규칙

다음 코드는 이 안내서에서 명령 규칙이 사용되는 방식을 보여 줍니다.

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

설명:

- 표시되는 그대로 입력해야 하는 명령 이름(ruler)은 일반 고정 폭 글꼴로 표시됩니다.
- *className* 옵션은 클래스 이름(예: USER)이 들어갈 자리이므로 기울임꼴로 표시됩니다.

- 대괄호로 묶인 두 번째 부분은 선택적 피연산자를 의미하므로 이 부분 없이 명령을 실행할 수도 있습니다.
- 옵션 매개 변수(props)를 사용할 때 키워드 *all* 을 선택하거나 하나 이상의 속성 이름을 쉼표로 구분하여 지정할 수 있습니다.

파일 위치 규칙

CA Access Control 설명서는 다음과 같은 파일 위치 규칙을 따릅니다.

- *ACInstallDir* - 기본 CA Access Control 설치 디렉터리입니다.
  - Windows - C:\Program Files\CA\AccessControl\
  - UNIX - /opt/CA/AccessControl/
- *ACSharedDir* - UNIX 에서 CA Access Control 에 의해 사용되는 기본 디렉터리입니다.
  - UNIX - /opt/CA/AccessControlShared
- *ACServerInstallDir* - 기본 CA Access Control 엔터프라이즈 관리 설치 디렉터리입니다.
  - /opt/CA/AccessControlServer
- *DistServerInstallDir* - 기본 배포 서버 설치 디렉터리입니다.
  - /opt/CA/DistributionServer
- *JBoss_HOME* - 기본 JBoss 설치 디렉터리입니다.
  - /opt/jboss-4.2.3.GA

CA 에 문의

기술 지원팀에 문의

온라인 기술 지원 및 지사 목록, 기본 서비스 시간, 전화 번호에 대해서는 http://www.ca.com/worldwide에서 기술 지원팀에 문의하십시오.

설명서 변경 사항

이 설명서가 마지막으로 릴리스된 이후에 다음과 같이 업데이트되었습니다.

- Microsoft 클러스터에 CA Access Control 고가용성 구현 - Microsoft 2008 클러스터에서 고가용성을 위한 CA Access Control 을 구현하는 방법을 설명하는 시나리오가 추가되었습니다.
- VMware vCenter 에 CA Access Control 고가용성 구현 - VMWare vCenter 에서 고가용성을 위한 CA Access Control 을 구현하는 방법을 설명하는 시나리오가 추가되었습니다.
- 엔터프라이즈 관리 서버 설치 - 업데이트된 장에서 부하 분산 엔터프라이즈 관리 서버를 설치하는 지침이 추가되었습니다.
- 통신 암호화 방법 변경 - "엔터프라이즈 관리 서버 설치" 장의 다음 항목이 추가되어 업데이트되었습니다.
  - 메시지 큐 서버 SSL 포트 번호
  - 동일한 암호화 키를 사용하도록 서버 구성
  - CA Access Control 웹 서비스 URL 변경
  - Microsoft SQL Server 데이터베이스 연결 설정 수정
  - 보고서 포털을 위한 Windows 인증 구성
  - Windows 인증에서 작업하기 위해 보고서 포털을 구성하는 방법
  - Windows 인증을 위한 보고서 포털 구성
  - 시스템 DSN 연결 구성 예제
  - Windows 인증에서 작업하는 보고서 포털에 보고서 패키지 배포

목차

제 1 장: 안내서 정보

이 안내서는 다양한 CA Access Control Premium Edition 구성 요소를 계획, 설치 및 사용자 지정하는 방법에 대한 정보를 제공합니다. 이러한 구성 요소에는 Windows 및 UNIX 용 CA Access Control 서버와 끝점 그리고 CA Access Control 끝점 관리 구성 요소가 포함됩니다. 엔터프라이즈 관리 및 보고 설치 관련 장은 CA Access Control Premium Edition 에만 해당됩니다.

용어를 간단히 나타내기 위해 이 안내서에서는 제품을 CA Access Control 이라고 합니다.

제 2 장: 회사 구현 계획

이 섹션은 다음 항목을 포함하고 있습니다.

보안 시스템 계획

보안 시스템의 주요 목표는 조직의 정보 자산을 보호하는 것입니다. 사이트에서 보안 기능을 효과적으로 구현하려면 사이트에 존재하는 위협에 대해 인지한 다음, 이와 같은 위협에서 사이트를 가장 잘 보호할 수 있는 방법을 결정해야 합니다.

권한 없는 사용으로부터 컴퓨터 리소스를 보호하는 기본적인 두 가지 방법은 다음과 같습니다.

- 권한 없는 사용자의 시스템 액세스를 차단합니다.
- 권한을 가진 사용자라도 액세스 권한이 없는 항목에 액세스하는 경우 차단합니다.

CA Access Control 은 두 가지 방법 모두로 시스템을 보호할 수 있는 도구를 제공합니다. 또한, CA Access Control 은 사용자의 활동을 추적하여 컴퓨터 시스템을 오용하려는 시도가 있었는지 확인할 수 있는 감사 도구를 제공합니다.

보안 프로젝트의 목표를 결정하고 나면 보안 정책을 작성하고 구현 팀을 구성할 수 있습니다. 구현 팀은 보안 대상이 되는 데이터, 응용 프로그램 및 사용자를 결정하는 데 유용한 우선 순위를 설정해야 합니다.

구현 계획 준비

구현 계획을 정의하는 동안 계획의 목표가 보안 정책에 따른 것인지 반복적으로 확인합니다. 새 보안 제어는 단계적으로 실행되어 사용자에게 조정 기간을 제공해야 합니다.

- 보안 계획을 기준으로 특정 목표를 정의합니다.

  보안 계획을 구현하는 데 도움을 주는 목표를 정의합니다.

- CA Access Control 구현을 위한 프로토타입으로 파일럿 사용자 그룹을 정의합니다.

  파일럿 그룹의 모든 CA Access Control 기능을 테스트한 다음 파일럿 그룹 외부의 엔터티를 보호합니다. 파일럿 그룹의 테스트는 나머지 조직의 보호 방법을 익히는 데 유용합니다.

- 보호 대상을 결정합니다.

  CA Access Control 은 파일럿 그룹의 비즈니스 데이터, 작업 및 사용자를 보호합니다.

- 보안 통제를 전개하는 방법을 정의합니다.

  현재 업무 패턴의 중단을 최소화한 상태에서 새 보안 통제를 단계적으로 도입하는 방법을 고려합니다. 다양한 리소스와 클래스에 대해 액세스를 제한하지 않은 채 감사만을 위한 액세스 기간을 고려해야 합니다. 결과로 생성되는 감사 레코드는 리소스에 대한 액세스가 필요한 사용자를 보여줍니다.

참고: 경고 모드(감사 전용 모드)에 대한 자세한 내용은 *UNIX 용 끝점 관리 안내서* 및 *Windows 용 끝점 관리 안내서*를 참조하십시오.

관리진의 참여 보장

CA Access Control 을 설치하기로 한 관리진의 결정만으로는 사이트에 대한 적절한 보안을 보장할 수 없습니다. 보안 프로젝트가 성공하려면 관리진의 능동적인 참여가 필수적입니다. 관리진은 보안 기능에 할당해야 하는 보안 정책, 절차 및 리소스를 결정하고 컴퓨터 시스템 사용자의 책임을 정해야 합니다. 이러한 관리진의 지원 없이는 보안 절차는 오용되어 실용적인 보호 체계라기보다는 관리적인 잡무가 되고 맙니다. 실제 이러한 상황은 심각한 보안 노출로 이어질 수 있는 잘못된 보안 의식을 키울 수 있습니다.

보안 관리자는 관리진과 협조하여 명확하고 포괄적인 보안 정책 규정을 준비해야 합니다. 이 문서에는 다음 내용이 포함되어야 합니다.

- 상근 직원, 파트 타임 직원, 계약직 및 고문직에 대한 회사 정책
- 외부 시스템 사용자에 대한 회사 정책
- 모든 시스템 사용자에게서 예상되는 행동
- 물리적인 보호 고려 사항
- 사용자 부분의 보안 요구 사항
- 감사 요구 사항

이에 따라 작성된 보안 정책은 설치 보안 정책과 상충되지 않는 현실적인 CA Access Control 구현 계획을 보장하도록 지원합니다.

보호 방법 결정

CA Access Control 을 설치하기 전에 어떤 소프트웨어 기능을 사용할지 결정합니다.

CA Access Control 은 다음과 같은 보호 방법을 제공합니다.

- 네이티브 보안 - CA Access Control 끝점 관리를 사용하여 이미 친숙한 보안 기능을 구현합니다.
- 고급 네이티브 보안 - 보다 정교한 공격에 대한 보호 CA Access Control 에서는 다음 작업을 수행합니다.
  - 권한 있는 계정의 권한을 제한
  - 특정 사용자의 사용자 암호 변경 기능과 같은 특수 권한을 일반 사용자에게 할당
  - NTFS, FAT, CDFS 를 비롯한 여러 파일 시스템 지원
  - Windows 및 UNIX 시스템을 포함한 서로 다른 환경에서 보안 정책 및 감사 중앙 집중화
- 고급 정책 관리 - 회사를 위해 작성하는 다중 규칙 정책(스크립트 파일)을 배포 이러한 정책 기반 방법을 사용하여 버전 제어 정책을 작성하고 엔터프라이즈 내 호스트 그룹에 정책을 할당 및 할당 취소하고 정책을 직접 배포하거나 배포된 정책을 제거하고(배포 취소) 배포 상태와 배포 위반을 확인할 수 있습니다.

- PMDB(정책 모델 데이터베이스) - 보안 데이터베이스에 여러 구독자에 대한 액세스, 그룹, 사용자 규칙을 전파할 수 있게 해 줍니다. PMDB 는 수신한 모든 업데이트 내용을 정기적으로 구독자에게 전파합니다. 이 메커니즘은 시스템 관리자의 관리 부담을 줄여 줍니다.
- 권한 있는 사용자 암호 관리(PUPM)를 사용하면 중앙 위치에서 대상 끝점의 권한 있는 계정에 대한 역할 기반 액세스 관리를 수행할 수 있습니다. PUPM 은 또한 권한 있는 계정 및 응용 프로그램 ID 암호를 안전하게 저장하고 정책에 기반하여 권한 있는 계정 및 암호에 대한 액세스를 제어합니다.
- UNIX 인증 브로커(UNAB)를 사용하면 Active Directory 를 통해 로컬 UNIX 사용자 및 그룹의 자격 증명의 유효성을 검사할 수 있습니다. 모든 사용자에 대해 단일 리포지토리를 사용하므로 사용자들이 동일한 사용자 이름과 암호로 모든 플랫폼에 로그인할 수 있게 됩니다.

직원 교육 및 훈련

보안 관리자의 업무 중 하나는 CA Access Control 이 설치될 때 작업이 중단되지 않도록 시스템 사용자가 알아야 할 정보를 알려주는 일입니다.

각 사용자가 CA Access Control 에 대해 알고 있어야 하는 세부 정보의 양은 각 사용자에게 부여한 기능에 따라 다릅니다. 다양한 유형의 시스템 사용자가 필요로 하는 정보의 예는 다음과 같습니다.

- PUPM 사용자

  권한 있는 계정 암호를 체크 아웃 및 체크 인하는 방법을 알아야 하고, 권한 있는 계정에 대한 액세스를 요청할 때 및 Break Glass 를 수행할 때에 대해 이해해야 합니다.

- CA Access Control 끝점 데이터베이스에 정의된 모든 사용자
  - 자신의 사용자 이름과 암호로 시스템에 액세스하고 암호를 변경하는 방법을 알아야 합니다. 또한 시스템 보안에 있어 암호의 중요성도 알고 있어야 합니다.
  - 암호 정책 검사를 구현하는 경우 암호 관리자에 알고 있어야 합니다.
  - 동시 로그인을 활성화하거나 비활성화하는 *secons -d-* 및 *secons -d+* 명령에 대해 알고 있어야 합니다. *동시 로그인*은 동시에 둘 이상의 터미널에서 동일한 사용자가 한 시스템에 대해 시작하는 다중 세션입니다.
  - 암호 검사를 실행하거나 실행하지 않고서 미리 정의된 액세스 규칙에 따라 사용자를 대체할 수 있는 sesudo 명령에 대해 알아야 합니다.

- 기술 지원 인력

  마이그레이션 고려 사항과 CA Access Control 설치 또는 제거에 필요한 단계에 대해 알아야 합니다. 데이터베이스를 유지 관리하는 사용자는 데이터베이스 유틸리티에 대해 잘 알고 있어야 합니다.

- 감사자

  AUDITOR 특성을 가진 사용자는 감사 도구인 CA Access Control 끝점 관리 및 seaudit 유틸리티에 대해 잘 알고 있어야 합니다.

  참고: seaudit 유틸리티에 대한 자세한 내용은 *참조 안내서*를 참조하십시오.

- 권한 없는 응용 프로그램을 작성하는 프로그래머

  프로그래머는 응용프로그램에서 CA Access Control* 함수 라이브러리를 사용하여 보호되는 리소스에 대한 제어 액세스(SEOSROUTE_RequestAuth 함수 사용)를 비롯한 보안 관련 서비스를 요청할 수 있습니다. 설치 시 설치가 정의된 리소스 클래스를 작성할 수 있습니다. 설치 과정에서 해당 클래스에 레코드가 작성된 경우, 응용 프로그램은 SEOSROUTE_RequestAuth 명령을 작성하여 사용자가 이 작업을 완료할 수 있는 권한이 있는지 확인합니다. 특정 사용자 작업에 필요한 권한 수준은 응용 프로그램이 SEOSROUTE_RequestAuth 함수를 실행하는 방법에 따라 결정됩니다.

  참고: CA Access Control API 에 대한 자세한 내용은 *SDK 안내서*를 참조하십시오.

- 권한 있는 응용 프로그램을 작성하는 프로그래머

  권한 있는 응용프로그램(SERVER 특성으로 실행되는 프로그램)을 작성하는 프로그래머는 CA Access Control* 함수 라이브러리를 사용하여 다음과 같은 보안 관련 서비스를 요청할 수 있습니다.

  - 사용자 식별 및 검증
  - 사용자 로그아웃 서비스
  - 사용자 권한 부여 요청

구현 크기 조정

CA Access Control 의 구현을 시작하기 전에 구현의 규모를 산정하고 이에 맞는 리소스를 할당해야 합니다. 다음 정보는 구현의 크기를 산정하는 데 도움이 됩니다.

3000 개의 CA Access Control 끝점마다 하나의 배포 서버를 설치할 것을 권장합니다.

다음 표는 엔터프라이즈 서버와 보고서 포털 컴퓨터에 있는 여러 구성 요소에 대해 할당해야 하는 데이터베이스 크기를 설명합니다.

구성 요소	기준	척도	할당
엔터프라이즈 관리 서버	사용자 저장소로서 Active Directory	매 1000 개의 Active Directory 계정에 대해	20MB

구성 요소	기준	척도	할당
CA Access Control	보고서 스냅숏	매 1000 개 CA Access Control 끝점마다	매 스냅숏에 대해 5 GB
PUPM	끝점 유형 정의	매 1000 개 PUPM 끝점마다	2MB
PUPM	권한 있는 계정	매 1000 개 권한 있는 계정마다	75MB
PUPM	권한 있는 계정 암호 작업	매 1000 개 PUPM 권한 있는 계정 암호 작업마다	250MB
CA Business Intelligence	CMS 및 감사 데이터베이스	기본 설치에 대해	300MB

참고: 시스템 요구 사항에 대한 자세한 내용은 *릴리스 정보*를 참조하십시오.

CA Access Control 데이터베이스 크기 제한

CA Access Control 데이터베이스는 1 백만(1,000,000) 개체로 제한됩니다. 이 크기 제한은 대규모 환경에서 고급 정책 관리를 사용하는 경우에만 배포에 영향을 줄 가능성이 있습니다.

회사의 CA Access Control 데이터베이스에 포함되는 개체가 1,000,000 개를 초과할 것으로 예상되는 경우 더 이상 사용되지 않는 오래된 DEPLOYMENT 개체를 제거해야 합니다.

예: CA Access Control 데이터베이스에서 개체 수 계산

다음 예는 DMS(중앙 CA Access Control 관리 데이터베이스)에 포함될 것으로 예상하는 개체의 수를 계산하는 방법을 설명합니다.

이 예에서는 5000 개의 끝점에 엔터프라이즈용 CA Access Control 가 배포되어 있으며, 각각은 50 개의 할당된 정책이 있습니다. 따라서 DMS 는 다음과 같이 최소 250,000 개의 개체를 포함하고 있습니다.

5,000 끝점 X 50 정책 = 250,000 DEPLOYMENT 개체

나중에 각 정책에 대해 네 가지 버전을 만들어 5000 개 끝점 각각에 할당하면 DMS 의 개체 수는 다음과 같이 개체 제한 값인 1,000,000 개에 도달하게 됩니다.

5,000 끝점 X 50 정책 X 4 버전 = 1,000,000 DEPLOYMENT 개체

CA Access Control 엔터프라이즈 관리 구현 방법

회사에서 CA Access Control 엔터프라이즈 관리을 구현하기 전에 어떤 구성 요소를 어떤 순서로 어디에 설치할지 이해해야 합니다. CA Access Control 엔터프라이즈 관리의 엔터프라이즈 배포를 구현할 때 다음 지침을 검토하십시오.

- 구현 프로세스에 '위에서 아래' 접근 방식을 사용하십시오. 엔터프라이즈 관리 서버의 설치부터 시작해서 추가 배포 서버를 설치하고, 엔터프라이즈 보고를 구현한 다음 CA Access Control 끝점을 설치하십시오.
- 구현을 시작하기 전에 사용하는 컴퓨터가 필요한 사양을 충족하고 모든 필수 소프트웨어가 설치되어 있는지 확인하십시오.

  참고: 요구되는 하드웨어 및 소프트웨어 사양에 대한 자세한 내용은 CA Support의 CA Access Control 제품 페이지에 있는 "CA Access Control Compatibility Matrix"(CA Access Control 호환성 표)를 참조하십시오.

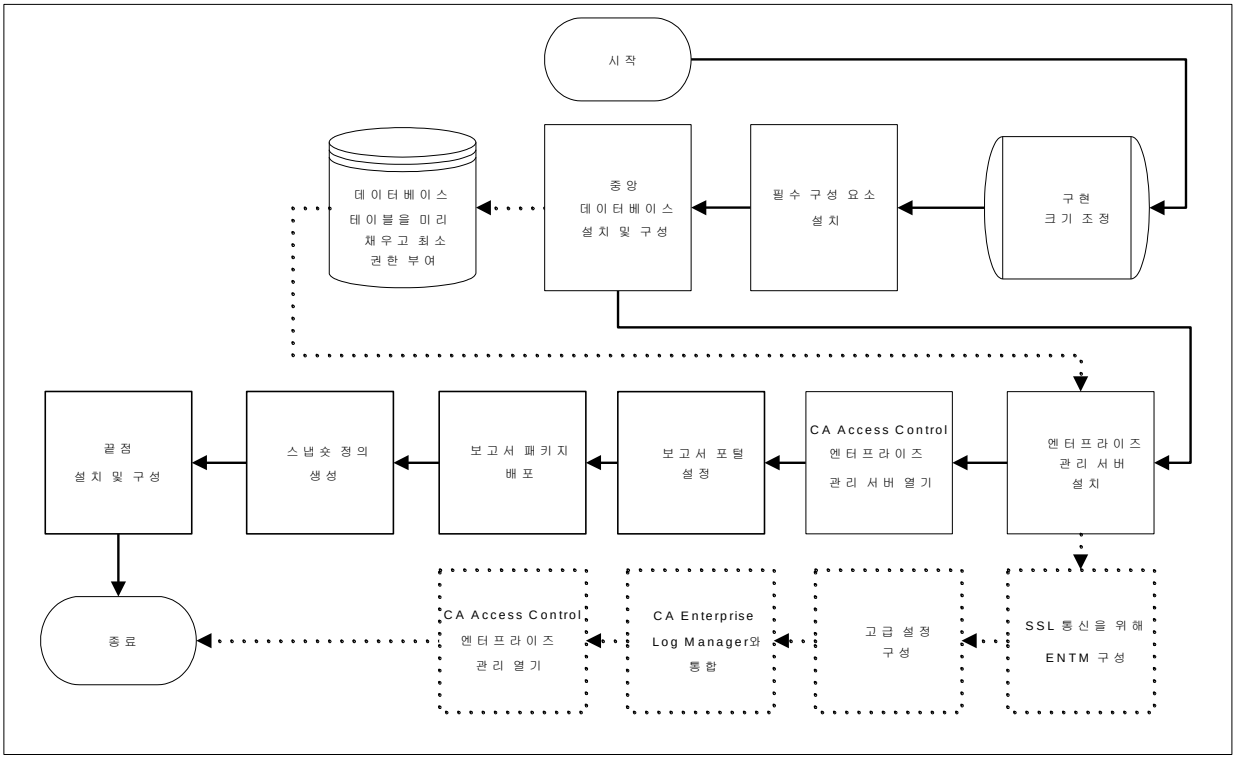
다음 프로세스를 사용하여 CA Access Control 엔터프라이즈 관리를 구현하십시오.

1. 사용할 배포 아키텍처를 결정합니다.
2. 중앙 데이터베이스로서 지원되는 RDBMS 를 설치합니다.
3. (선택 사항) 지원되는 사용자 저장소를 설치합니다.
4. 엔터프라이즈 관리 서버를 설치합니다.
5. 엔터프라이즈 보고 기능을 구현합니다.
6. (선택 사항) CA User Activity Reporting Module 과 통합합니다.
7. 끝점을 설치합니다.

다음 다이어그램은 CA Access Control 엔터프라이즈 관리의 구현 프로세스를 설명합니다.

엔터프라이즈 관리 서버 구현

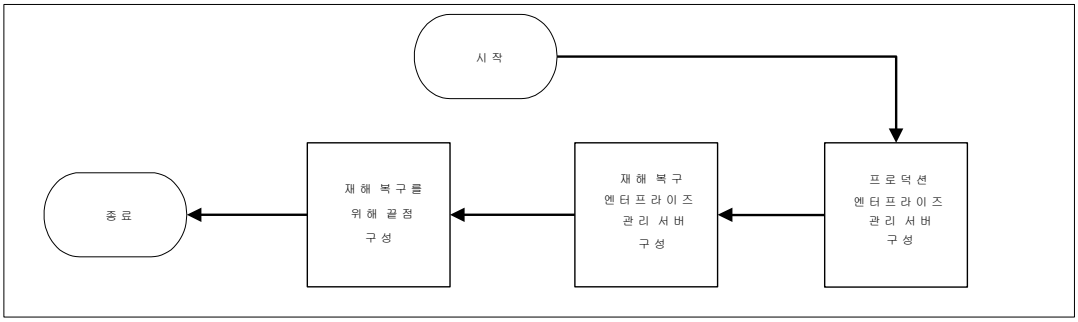
엔터프라이즈 관리 서버를 구현할 때 이 다이어그램이 도움이 됩니다.



참고: 점선은 선택적 단계를 나타냅니다.

재해 복구를 위한 CA Access Control 구현

재해 복구를 위해 CA Access Control 을 구현할 때 이 다이어그램이 도움이 됩니다.



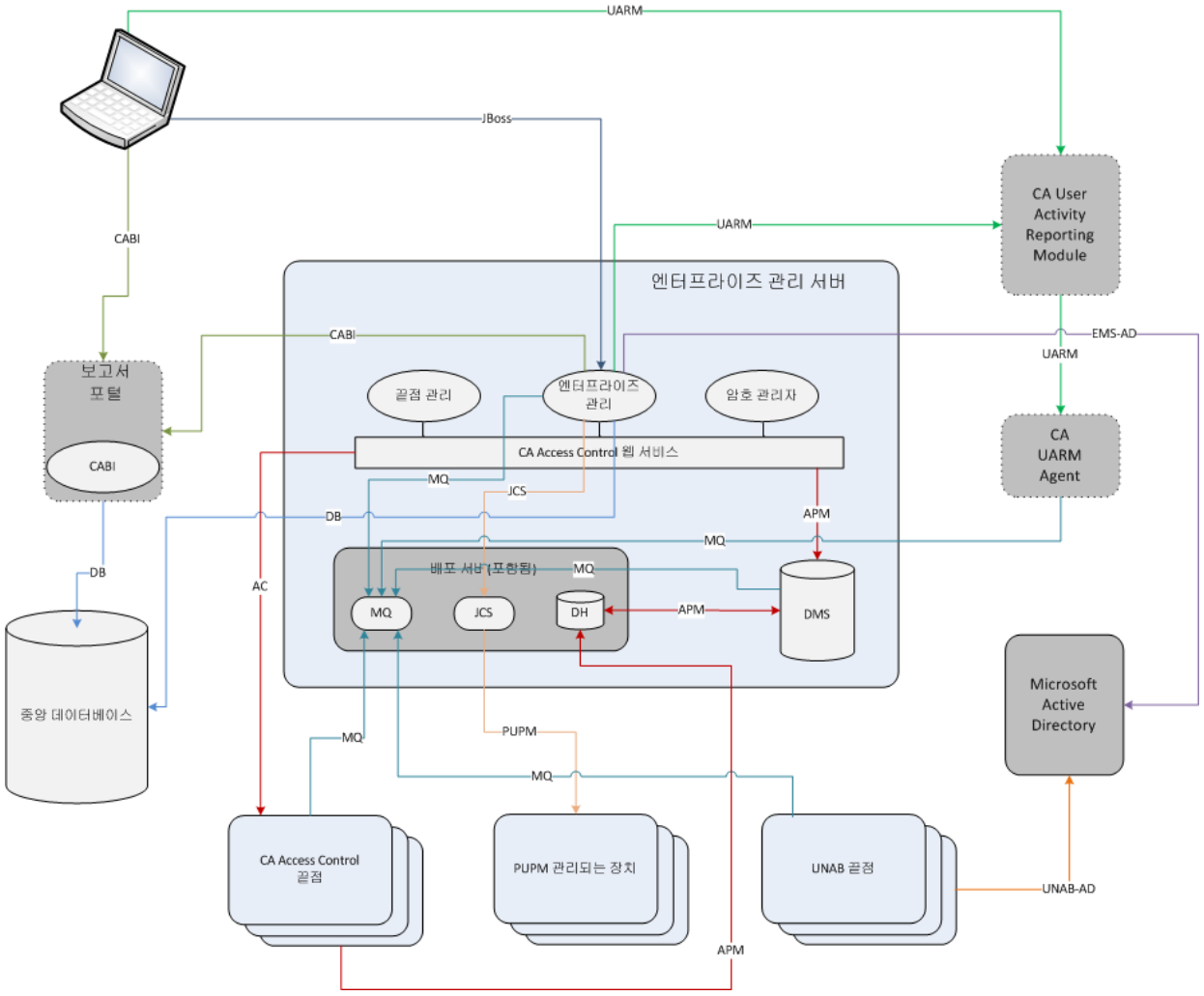
CA Access Control 엔터프라이즈 관리 배포 아키텍처

CA Access Control 엔터프라이즈 관리 구현을 시작하기 전에 다음 중 어떤 구현 아키텍처 중 사용할지 결정해야 합니다.

- 기본 - 기본 배포에서 CA Access Control 엔터프라이즈 관리의 모든 구성 요소를 하나의 서버에 설치합니다. 기본 아키텍처를 구현하는 것이 CA Access Control 엔터프라이즈 관리를 구현하는 가장 빠른 길입니다. 기본 구현 아키텍처는 고가용성 및 재해 복구 기능을 지원하지 않습니다.
- 부하 분산 - 부하 분산 배포 아키텍처는 공용 사용자 및 데이터 저장소를 사용하여 엔터프라이즈 관리 서버 사이에서 작업 부하를 분산시킬 수 있게 해 줍니다. 부하 분산 배포에서는 하나 또는 여러 개의 부하 분산 엔터프라이즈 관리 서버를 배포합니다.
- 고가용성 - 고가용성 배포 아키텍처를 사용하면 장애 조치 및 중복성을 위해 CA Access Control 엔터프라이즈 관리를 구현할 수 있습니다. 고가용성 구현에서는 서버 장애 시 끝점의 데이터에 계속 액세스할 수 있도록 여러 서버에 CA Access Control 엔터프라이즈 관리를 구현합니다.
- 재해 복구 - 재해 복구를 위해 CA Access Control 엔터프라이즈 관리를 구현할 수 있게 해 주는 재해 복구 구현 아키텍처입니다. 재해 복구 배포에서는 재해 복구 기능을 위해 여러 서버에 CA Access Control 엔터프라이즈 관리를 배포합니다.

기본 엔터프라이즈 배포 아키텍처

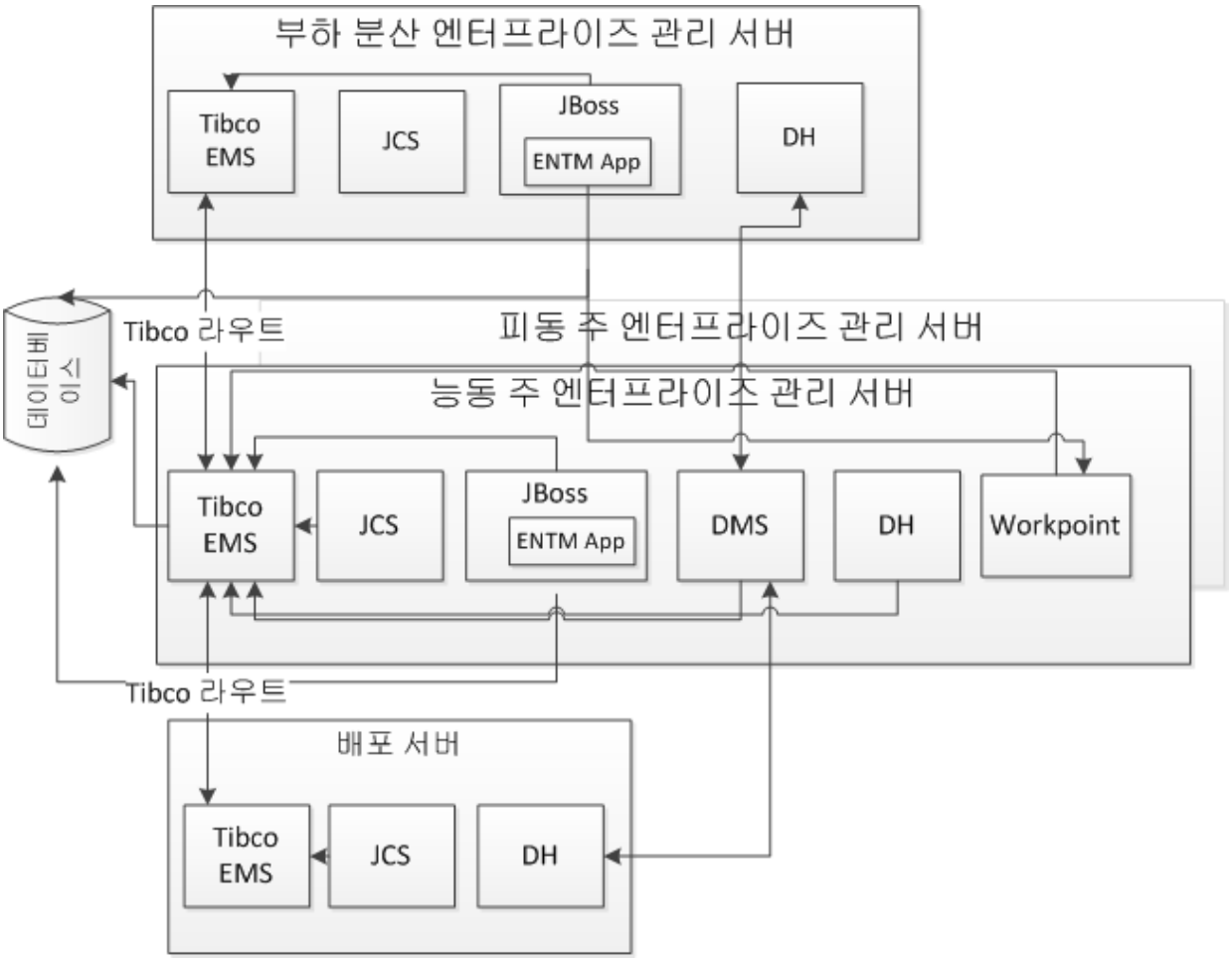
다음 다이어그램에서는 엔터프라이즈에 CA Access Control 을 배포하는 방법을 설명합니다.



참고: 점선은 옵션 구성 요소를 나타냅니다.

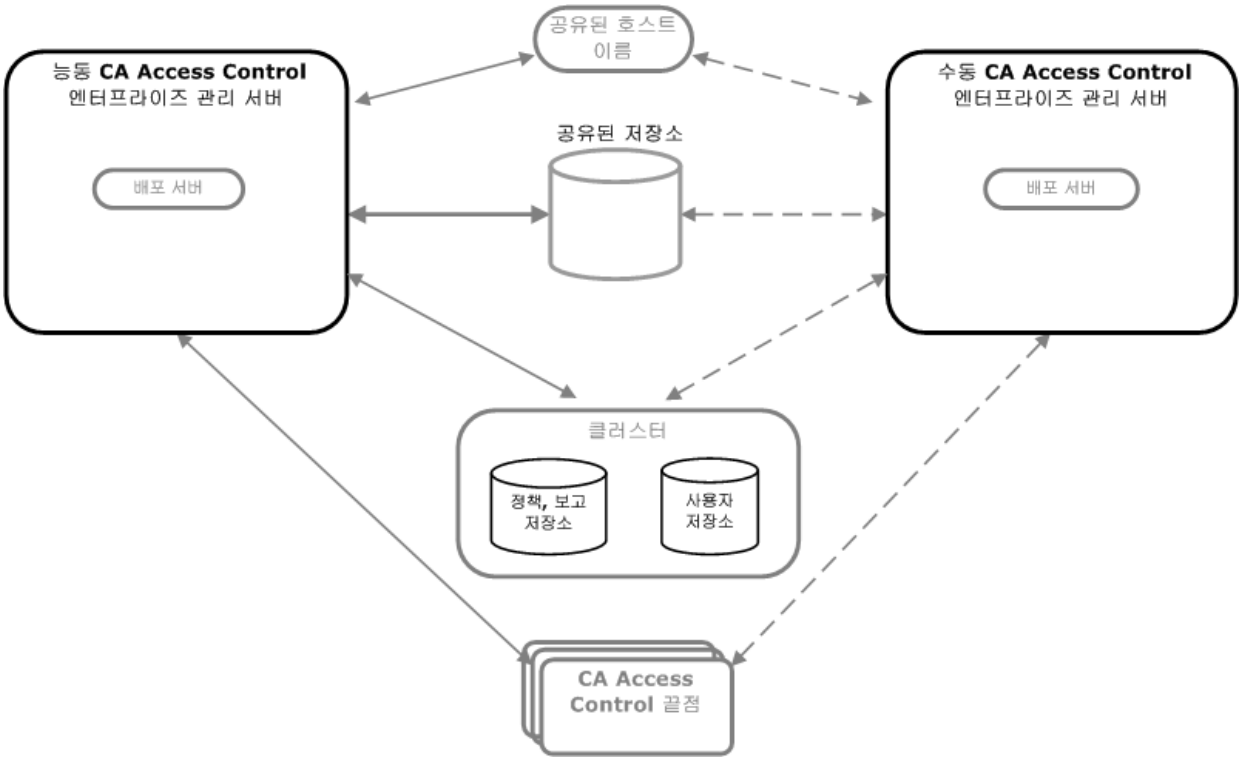
부하 분산 배포 아키텍처

다음 다이어그램은 환경에서 부하 분산 엔터프라이즈 관리 서버를 배포하는 방법을 보여 줍니다.



고가용성 배포 아키텍처

다음 다이어그램은 고가용성 환경의 CA Access Control 엔터프라이즈 관리를 보여줍니다.

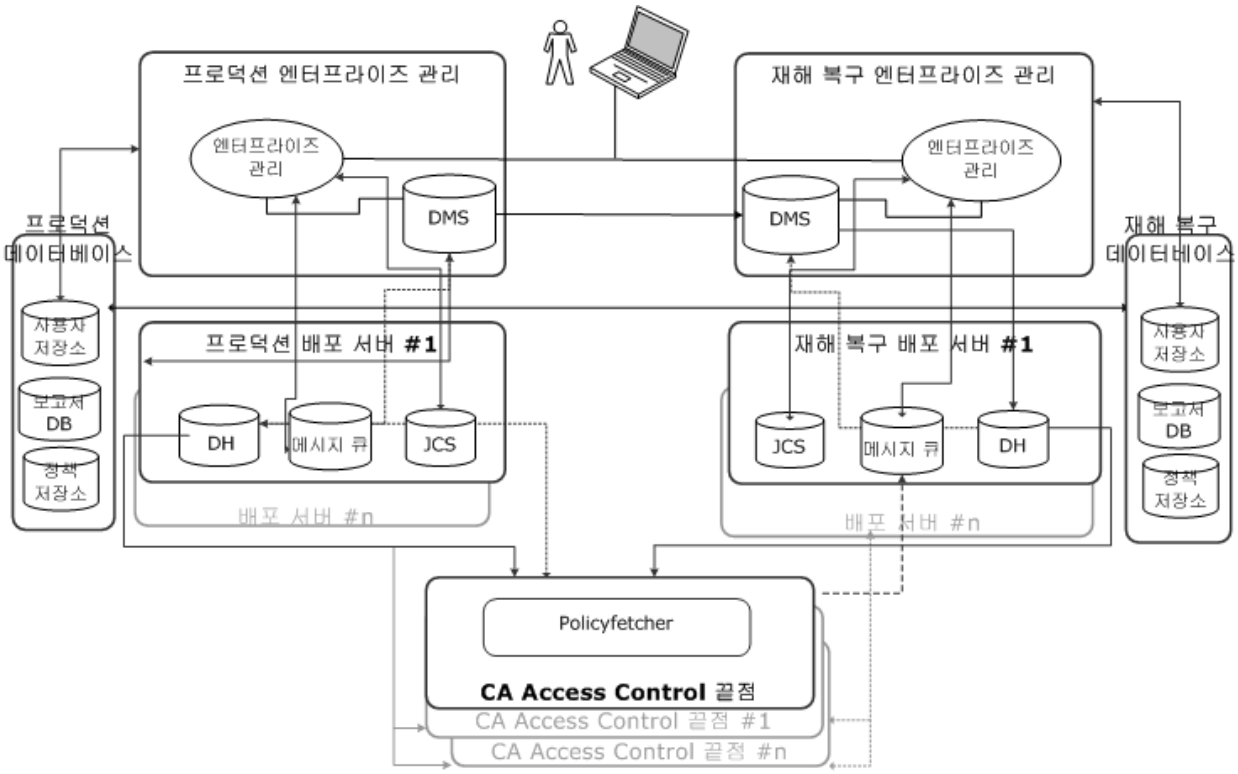


이전 다이어그램에 표시된 것처럼 고가용성 배포는 다음 구성 요소를 포함합니다.

- 기본 엔터프라이즈 관리 서버 및 하나 이상의 보조 엔터프라이즈 관리 서버
- 정책, 보고 저장소, 사용자 저장소의 클러스터된 설치
- 주 및 보조 CA Access Control 엔터프라이즈 관리 서버 모두가 액세스할 수 있는 공유 저장소
- 공유된 호스트 이름
- 기본 및 보조 엔터프라이즈 관리 서버 모두와 동작할 수 있는 CA Access Control 끝점

재해 복구 아키텍처

다음 다이어그램에서는 재해 복구 구성에 CA Access Control 을 배포하는 방법을 설명합니다.



CA Access Control 엔터프라이즈 관리의 구성 요소

CA Access Control 엔터프라이즈 관리는 다음 구성 요소로 구성되거나 이러한 구성 요소를 이용합니다.

엔터프라이즈 관리 서버

엔터프라이즈 서버는 중앙 관리 서버로서, 끝점에 정책을 배포하고, 권한 있는 계정을 관리하고, 리소스/접근자/액세스 수준을 정의할 수 있는 도구 및 구성 요소를 포함하고 있습니다. 엔터프라이즈 관리 서버는 또한 엔터프라이즈 관리 서버, 끝점, 기타 구성 요소 사이의 통신을 관리하는 구성 요소를 포함하고 있습니다.

CA Access Control 은 엔터프라이즈 관리 서버를 설치할 때 자동으로 설치됩니다. CA Access Control 은 엔터프라이즈 관리 서버를 보호하고 엔터프라이즈 서버의 응용 프로그램을 지원하는 핵심 기능을 제공합니다.

배포 서버

배포 서버는 응용 프로그램 서버와 끝점 사이의 통신을 처리합니다. 배포 서버는 다음과 같은 구성 요소를 포함하고 있습니다.

- DH(배포 호스트)
- 메시지 큐(MQ)
- ava Connector Server(Java Connector Server)

참고: 장애 조치 용도로 회사에 여러 개의 배포 서버를 설치하거나 다른 컴퓨터에 배포 서버 구성 요소를 설치할 수 있습니다. 기본적으로 배포 서버는 엔터프라이즈 관리 서버에 설치됩니다.

DH(배포 호스트)

DH 는 DMS 에서 만들어진 정책 배포를 끝점으로 분산하고 끝점에서 DMS 로 보낼 배포 상태를 수신합니다. 이 작업을 수행하기 위해 DH 는 두 가지 정책 모델 데이터베이스를 사용합니다.

- **DH 작성기** - 끝점에서 수신한 데이터를 DMS 로 작성하는 책임을 집니다.

  이 PMDB 의 이름은 *DHName*WRITER 이며 여기서 *DHName* 은 DH 의 이름(기본값은 **DH__**)입니다.

- **DH 판독기** - 끝점에서 검색할 수 있도록 DMS 의 데이터를 판독하는 책임을 집니다.

  이 PMDB 의 이름은 *DHName* 이며 여기서 *DHName* 은 DH 의 이름(기본값은 **DH__**)입니다.

기본적으로 DH 는 배포 서버와 같은 컴퓨터에 설치됩니다. 그러나 부하 분산을 위해 각 노드에서 엔터프라이즈의 섹션을 관리하도록 여러 개의 DH 노드를 설치할 수도 있습니다.

메시지 큐

메시지 큐는 엔터프라이즈 서버와 기타 구성 요소 사이의 인바운 및 아웃바운드 메시지를 관리합니다. 메시지 큐에는 엔터프라이즈 관리 서버와 통신하는 다음과 같은 각 클라이언트 구성 요소에 대한 전용 큐가 있습니다.

- 보고서 큐 - 끝점 데이터베이스의 예약된 스냅숏을 받습니다.

  보고 서비스는 CA Access Control 보고서를 생성하기 위해 스냅숏을 사용합니다.

- 감사 큐 - 끝점에서 발생하는 감사 이벤트를 받습니다.

  CA Enterprise Log Manager 를 구성하여 감사 이벤트를 수집하고 보고할 수 있습니다.

- 서버에서 끝점 큐 - 끝점에 의해 수집된 DMS 에서 데이터를 받습니다.

  예를 들어, UNAB 구성 정책을 배포하면 DMS 는 구성 정책을 이 큐로 보냅니다. 그러면 UNAB 에이전트가 큐에서 정책을 수집하여 UNAB 끝점에 이 정책을 배포합니다.

- 끝점에서 서버 큐 - DMS 에서 수집된 끝점에서 정보를 받습니다.

  예를 들어, UNAB 끝점은 이 큐로 하트비트 알림을 보냅니다. 그러면 DMS 가 큐에서 하트비트 알림을 수집하여 데이터베이스에서 끝점 상태를 업데이트합니다.

ava Connector Server(Java Connector Server)

JCS(Java Connector Server)는 Windows 운영 체제와 SQL 서버와 같은 Java 를 지원하는 관리되는 장치와 통신하고 PUPM 끝점에 있는 권한 있는 계정을 관리합니다.

웹 기반 응용 프로그램

웹 기반 응용 프로그램을 사용하여 CA Access Control 의 엔터프라이즈 설치를 관리합니다. 웹 기반 응용 프로그램은 응용 프로그램 서버에 설치됩니다. 기본적으로 응용 프로그램 서버는 엔터프라이즈 관리 서버에 설치됩니다.

응용 프로그램 서버는 다음과 같은 웹 기반 응용 프로그램을 포함하고 있습니다.

- CA Access Control 엔터프라이즈 관리 - 회사 전체에서 정책을 관리하고 끝점을 구성할 수 있게 해 줍니다. CA Access Control 엔터프라이즈 관리는 또한 회사 전체에서 권한 있는 계정을 관리할 수 있게 해 주고 권한 있는 계정을 위한 암호 저장소의 역할을 하는 권한 있는 사용자 암호 관리(PUPM)를 포함하고 있습니다.
- CA Access Control 끝점 관리 - 중앙 관리 서버를 통해 각각의 CA Access Control 끝점을 관리 및 구성할 수 있게 해줍니다.
- CA Access Control 암호 관리자 - CA Access Control 사용자 암호를 관리할 수 있게 해줍니다. CA Access Control 사용자의 암호를 수정하거나 사용자가 다음에 로그인할 때 자신의 암호를 변경하도록 강제할 수 있습니다.

CA Access Control 엔터프라이즈 관리

CA Access Control 엔터프라이즈 관리는 회사를 관리하는 사용하는 사용자 인터페이스입니다. CA Access Control 엔터프라이즈 관리와 CA Access Control 끝점의 최초 설치가 완료된 이후에 사용자 인터페이스에 대해 스스로 친숙해지도록 하는 것이 좋습니다.

CA Access Control 엔터프라이즈 관리를 쉽게 탐색할 수 있도록 각 탭 아래에 주제별로 작업이 그룹화되어 있습니다. 이러한 작업을 사용하여 다음을 수행할 수 있습니다.

- 회사 전체에서 CA Access Control 의 구현을 봅니다.
- 호스트 및 호스트 그룹을 구성하고 정책을 CA Access Control 및 UNAB 끝점에 할당합니다.
- 권한 있는 계정 암호를 체크 아웃 및 체크 인합니다.
- 권한 있는 계정, 끝점, 암호 정책, 암호 소비자를 구성합니다.
- 보고서를 표시하고, 스냅숏 정의를 관리하고, 스냅숏 데이터를 캡처합니다.
- 사용자, 그룹, 역할, 작업을 관리합니다.
- 시스템 전반의 연결 설정을 관리합니다.
- 감사 레코드를 봅니다.

참고: CA Access Control 엔터프라이즈 관리에서 작업을 완료하는 방법에 대한 자세한 내용은 *온라인 도움말*을 참조하십시오.

DMS(Deployment Map Server)

DMS 는 고급 정책 관리의 핵심이 되는 시스템이며 정책과 각 컴퓨터에서의 정책 배포 상태에 관한 최신 정보 유지를 목표로 합니다. DMS 는 나중에 필요에 따라 할당, 할당 취소, 배포 및 배포 취소할 수 있는 여러 정책 버전을 저장합니다.

DMS 는 정책 모델 노드로서, 데이터 리포지토리로 PMDB 를 사용합니다. DMS 는 구성된 각 끝점의 알림에서 수신한 데이터를 수집하고 각 끝점에 대한 배포 정보를 저장합니다.

보고서 포털

보고서 포털에서는 CA Access Control 보고서를 볼 수 있습니다.

CA Access Control 보고서는 각 끝점에 있는 CA Access Control 데이터베이스의 데이터에 대한 정보(끝점에 배포하는 규칙 및 정책과 규칙 및 정책에 대한 위반)를 제공합니다. CA Access Control 보고서는 CA Business Intelligence 또는 CA Access Control 엔터프라이즈 관리에서 봅니다.

중앙 RDBMS 는 CA Access Control 보고서에서 사용되는 끝점 데이터를 저장합니다.

중앙 RDBMS

중앙 RDBMS 는 다음 항목을 저장합니다.

- CA Access Control 보고서에서 사용되는 끝점 데이터
- 권한 있는 계정 암호
- 웹 기반 응용 프로그램의 세션 데이터
- 웹 기반 응용 프로그램의 사용자 데이터(사용자 저장소로 Active Directory 또는 Sun ONE 을 사용하지 않는 경우)

참고: 웹 기반 응용 프로그램은 CA Access Control 엔터프라이즈 관리, CA Access Control 끝점 관리, CA Access Control 암호 관리자입니다.

끝점

CA Access Control 의 엔터프라이즈 배포에는 세 가지 유형의 끝점이 있습니다.

- CA Access Control 끝점 - CA Access Control 이 설치된 끝점입니다.

  CA Access Control 끝점은 또한 선택적으로 PUPM 끝점의 역할을 할 수도 있습니다.
- UNAB 끝점 - UNIX 인증 브로커(UNAB)가 설치된 UNIX 끝점입니다.
- PUPM 끝점 - 권한 있는 사용자 암호 관리(PUPM)로 관리하는 끝점입니다.

CA User Activity Reporting Module 구성 요소

각 끝점 및 엔터프라이즈 관리 서버로부터 CA User Activity Reporting Module 로 수집 및 보고를 위해 CA Access Control 감사 이벤트를 보낼 수 있습니다. 다음 구성 요소는 CA User Activity Reporting Module 와 CA Access Control 의 통합을 지원합니다.

- CA User Activity Reporting Module 에이전트 - 배포 서버의 감사 큐에서 감사 이벤트를 수집하여 감사 이벤트를 CA User Activity Reporting Module 서버로 보내 처리합니다.
- CA User Activity Reporting Module 서버 - 감사 이벤트를 받고 이벤트가 저장되기 전에 비표시(suppression) 또는 요약화 규칙을 적용할 수 있습니다.

참고: CA User Activity Reporting Module 구성 요소에 대한 자세한 내용은 CA User Activity Reporting Module 설명서를 참조하십시오.

사용자 저장소

Active Directory 또는 Sun One 에 정의된 그룹 및 사용자를 사용하도록 CA Access Control 및 CA Access Control 웹 기반 응용 프로그램을 구성할 수 있습니다. 즉, 이렇게 하면 모든 사용자에 대해 하나의 데이터 저장소를 사용할 수 있게 됩니다.

참고: 웹 기반 응용 프로그램은 CA Access Control 엔터프라이즈 관리, CA Access Control 끝점 관리, CA Access Control 암호 관리자입니다.

제 3 장: 엔터프라이즈 관리 서버 설치

이 섹션은 다음 항목을 포함하고 있습니다.

환경 아키텍처

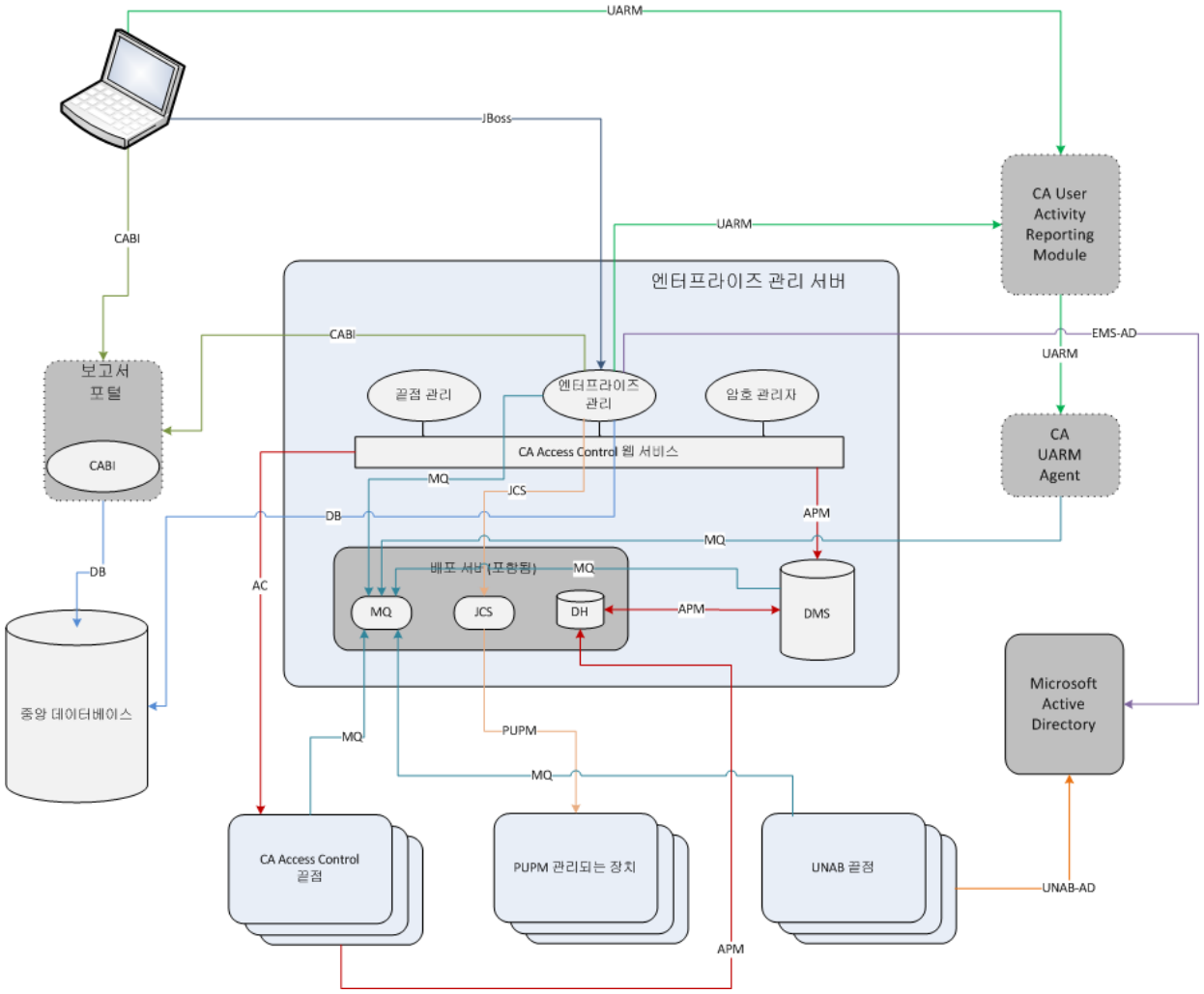
CA Access Control 의 엔터프라이즈 설치를 사용하면 정책, 권한 있는 계정, CA Access Control 끝점을 중앙에서 관리하고, 각 끝점에 배포된 정책에 대한 정보를 보고, 끝점의 보안 상태에 대해 보고할 수 있습니다. 이러한 기능은 웹 기반 인터페이스 또는 유틸리티를 통해 관리할 수 있습니다.

CA Access Control 의 엔터프라이즈 설치를 관리하려면 중앙 컴퓨터에서 엔터프라이즈 관리 서버를 설치하고 사용자의 회사에 맞게 구성해야 합니다.

CA Access Control 은 엔터프라이즈 관리 서버를 설치할 때 자동으로 설치됩니다. CA Access Control 은 엔터프라이즈 관리 서버를 보호하고 엔터프라이즈 서버의 응용 프로그램을 지원하는 핵심 기능을 제공합니다.

엔터프라이즈 관리 서버를 설치한 다음 CA Access Control 및 UNAB 끝점을 설치하고 구성합니다. 기존 CA Access Control 끝점이 있는 경우 각 끝점에서 고급 정책 관리 및 보고 기능을 구성합니다.

다음 다이어그램은 엔터프라이즈 관리 서버 아키텍처를 나타냅니다.



앞의 다이어그램은 다음을 보여줍니다.

- 엔터프라이즈 관리 서버는 다음 포트를 사용합니다.
  - 대칭 암호화를 위한 포트 8891, CA Access Control 끝점과의 SSL 통신을 위한 포트 5249
  - RDBMS 와의 통신을 위한 포트 1433(MS SQL) 또는 1521(Oracle)
  - Active Directory 와의 암호화된 통신을 위한 포트 389 또는 686
  - JCS(Java Connector Server)와의 암호화된 통신을 위한 포트 20411
  - 메시지 큐와의 암호화된 통신을 위한 포트 7243

- PUPM 은 끝점 유형(Windows Agentless, SSH 장치 등)에 따라 끝점과 통신합니다.
- 엔터프라이즈 관리 서버는 포트 8080 을 사용하여 CA Business Intelligence 와 통신합니다.
- 엔터프라이즈 관리 서버는 암호화된 통신을 위한 포트 5250 을 사용하여 CA User Activity Reporting Module 과 통신합니다.
- UNAB 는 다음 포트를 사용하여 Active Directory 와 통신합니다: 53, 88, 123, 289, 445, 464, 3268

엔터프라이즈 관리 서버를 준비하는 방법

엔터프라이즈 관리 서버를 설치하기 전에 이 서버 준비하십시오. r12.5 이상을 업그레이드하는 경우 이미 엔터프라이즈 관리 서버를 준비했으며 이 단계를 다시 수행할 필요가 없습니다.

참고: 엔터프라이즈 관리 서버를 설치할 때, CA Access Control 끝점 관리가 아직 설치되어 있지 않으면 설치 프로그램에 의해 자동으로 설치됩니다. CA Access Control 끝점 관리를 설치한 경우 이 단계를 반복하지 마십시오.

엔터프라이즈 관리 서버를 준비하려면 다음 단계를 수행하십시오.

1. 엔터프라이즈 관리를 위해 중앙 데이터베이스를 준비합니다.

   RDBMS 네이티브 관리 도구를 사용하여 중앙 데이터베이스를 직접 만들고 구성하는 방법으로 데이터베이스를 준비할 수도 있습니다.

2. 다음 방법 중 *하나*를 사용하여 필수 소프트웨어를 설치합니다.

   - (Windows) 필수 설치 유틸리티를 실행합니다 (페이지 53).

     CA Access Control 은 JDK(Java Development Kit)와 JBoss Application Server 를 설치하는 유틸리티를 제공합니다. 이 소프트웨어가 이미 설치되어 있으면 이 단계를 건너뛰어도 됩니다.

   - 다음과 같이 기존 소프트웨어를 사용하거나 직접 필수 소프트웨어를 설치합니다.

     참고: 필수 타사 소프트웨어는 CA Access Control Premium Edition 타사 구성 요소 DVD 에서 찾을 수 있습니다. 지원되는 버전에 대한 자세한 내용은 *릴리스 정보*를 참조하십시오.

     a. 지원되는 JDK(Java Development Kit) 버전을 설치합니다.

b. (Linux) 시스템 PATH 의 JDK/bin 디렉터리를 정의하고 그 값을 설치 경로로 설정합니다.

   예를 들어, bash 셸을 사용하여 Linux 에서 경로를 설정하려면 다음 명령을 입력하십시오.

   ```
   export PATH=/usr/jdk/j2sdk.1.6.0_19/bin:$PATH
   ```

   참고: 경로를 영구적으로 설정하려면 셸 시작 파일에 경로를 설정하십시오.

c. 지원되는 JBoss 버전을 설치합니다.

   JBoss 를 서비스로서 설치할 것을 권장합니다. (UNIX 의 데몬).

   참고: 이미 JBoss 가 설치되어 있는 경우 사용 중인 포트 문제를 피하기 위해 CA Access Control 엔터프라이즈 관리 설치 전에 JBoss 를 한 번 실행하는 것이 좋습니다. CA Access Control 엔터프라이즈 관리 설치 프로그램은 기본 JBoss 포트를 사용하지 않습니다. 예를 들어, 설치 프로그램은 HTTP 연결에 대해 포트 번호 8080 대신 포트 번호 18080 을 사용합니다. 엔터프라이즈 관리 서버 설치 중에 JBoss 가 사용하는 포트를 지정하십시오.

d. (Linux) 사용하는 Linux 배포의 rpmbuild 패키지가 설치되었는지 확인하십시오.

   엔터프라이즈 관리 서버는 서버에 고급 정책 관리 옵션을 설치하려면 rpmbuild 패키지가 필요합니다.

이제 엔터프라이즈 관리 서버에 CA Access Control 엔터프라이즈 관리를 설치할 수 있습니다.

엔터프라이즈 관리의 중앙 데이터베이스를 준비합니다.

CA Access Control 엔터프라이즈 관리에는 RDBMS(relational database management system)가 필요합니다. CA Access Control 엔터프라이즈 관리를 설치하기 전에 이를 먼저 설치하십시오.

CA Access Control 엔터프라이즈 관리와 동작하도록 데이터베이스를 설정하는 두 가지 옵션이 있습니다.

- CA Access Control 이 제공하는 배포 스크립트를 사용하여 중앙 데이터베이스를 미리 채웁니다.

  이 옵션을 사용하면 데이터베이스 준비와 CA Access Control 엔터프라이즈 관리 설치가 분리됩니다. 데이터베이스 관리자는 CA Access Control 이 데이터베이스에 대해 수행하는 변경 내용을 검토하고 제어할 수 있습니다.

- CA Access Control 엔터프라이즈 관리가 설치 중 중앙 데이터베이스를 준비하도록 합니다.

  이 옵션을 사용하면 CA Access Control 엔터프라이즈 관리 설치가 설치 프로세스의 일부로 데이터베이스를 채웁니다.

다음 단계를 수행하십시오.

1. 이미 설치되지 않은 경우 지원되는 RDBMS 를 중앙 데이터베이스로 설치합니다.

   참고: 지원되는 RDBMS 소프트웨어 목록을 보려면 *릴리스 정보*를 참조하십시오.

2. CA Access Control 엔터프라이즈 관리를 위한 RDBMS 구성:

   로컬에서와 원격 클라이언트에서 데이터베이스에 액세스할 수 있어야 합니다.

   - Oracle 의 경우 다음 단계를 수행하십시오.

   a. 중앙 데이터베이스에 대한 사용자를 생성합니다. 이 사용자는 다음과 같은 권한과 설정이 있어야 합니다.

      - 역할: CONNECT, RESOURCE
      - 시스템 권한: ALTER SESSION, CREATE CLUSTER, CREATE DATABASE LINK, CREATE SEQUENCE, CREATE SESSION, CREATE SYNONYM, CREATE TABLE, CREATE VIEW, CREATE INDEXTYPE, CREATE OPERATOR, CREATE PROCEDURE, CREATE TRIGGER, CREATE TYPE, SELECT ANY DICTIONARY, UNLIMITED TABLESPACE

   b. 다음 명령을 입력하여 데이터베이스 연결 수를 늘립니다.

      ALTER SYSTEM SET transactions=275 SCOPE=SPFILE

      ALTER SYSTEM SET sessions=250 SCOPE=SPFILE

      ALTER SYSTEM SET processes=200 SCOPE=SPFILE

   - SQL Server 의 경우:
      - 대소문자를 구분하지 *않는* 새 데이터베이스를 만듭니다.

        데이터베이스에는 정렬 순서 SQL_Latin1_General_CP1_CI_AS 가 있어야 합니다.
      - 사용자를 만들고, 새 데이터베이스를 사용자의 기본 데이터베이스로 만들고, 다음 권한을 할당합니다: DBCREATOR, SYSADMIN

3. (선택 사항) CA Access Control 이 제공하는 배포 스크립트를 사용하여 중앙 데이터베이스를 미리 채웁니다.

   a. 배포 스크립트를 배포하기 전에 배포 스크립트를 사용자 지정합니다 (페이지 50).

      배포 스크립트는 CA Access Control 엔터프라이즈 관리가 사용하는 4 개의 기본 사용자 계정(superadmin, selfreguser, neteautoadmin, [default user])을 정의합니다. 이러한 기본 계정과 암호를 변경할 수 있습니다.

      중요! 기본 제공되는 사용자 저장소를 사용하려는 경우에만 이 스크립트를 사용자 지정하십시오. Active Directory 를 사용하는 경우 CA Access Control 엔터프라이즈 관리는 계정 정보를 중앙 데이터베이스에 저장하지 않습니다.

   b. 배포 스크립트를 배포합니다 (페이지 51).

   c. CA Access Control 엔터프라이즈 관리 설치에 사용할 데이터베이스 사용자를 구성합니다.

      - Oracle 의 경우 생성한 사용자에 대한 CONNECT 및 RESOURCE 역할을 유지합니다.
      - SQL Server 의 경우 사용자를 만들고, 앞에서 기본 데이터베이스로 만든 데이터베이스를 선택하고, 사용자를 이 데이터베이스로 매핑하고, 다음 권한을 설정합니다: CONNECT.SELECT, INSERT, DELETE, UPDATE, EXECUTE

중앙 데이터베이스 배포 스크립트 사용자 지정

배포 스크립트는 CA Access Control 엔터프라이즈 관리가 사용하는 4 개의 기본 사용자 계정(superadmin, selfreguser, neteautoadmin, [default user])을 정의합니다. 이러한 기본 계정과 암호를 변경할 수 있습니다.

중요! 기본 제공되는 사용자 저장소를 사용하려는 경우에만 이 스크립트를 사용자 지정하십시오. Active Directory 를 사용하는 경우 CA Access Control 엔터프라이즈 관리는 계정 정보를 중앙 데이터베이스에 저장하지 않습니다.

중앙 데이터베이스 배포 스크립트를 사용자 지정하려면

1. 광학 디스크 드라이브에 사용하는 운영 체제용의 적절한 CA Access Control Premium Edition 서버 구성 요소 DVD 를 넣습니다.
2. RDBMS 에 대한 배포 스크립트를 임시 로컬 폴더로 복사합니다.

   기본적으로 데이터베이스 배포 스크립트는 광학 미디어에서 다음 위치에 있습니다.

   - Oracle: /Scheme/ORACLE/AC125_oracle_script.sql
   - SQL Server: /Scheme/MSSQL/AC125_mssql_script.txt
3. 다음과 같이 스크립트를 편집하십시오.
   a. *Table : TBLUSERS* 섹션을 찾습니다.
   b. 필요한 경우 계정 이름과 암호를 변경하려면 사용자를 정의하는 각 줄을 (INSERT INTO tblusers ...)로 변경하십시오.
4. 스크립트를 저장한 후 닫습니다.

   이제 사용자 지정된 스크립트를 배포할 수 있습니다.

예: CA Access Control RDBMS 배포 스크립트 사용자 지정

이 예는 Microsoft SQL Server 및 Oracle 데이터베이스 배포 스크립트에 일반적인 코드 조각을 사용합니다. 이 예에서 기본 사용자 계정 superadmin 과 암호를 변경하기 위해 스크립트를 사용자 지정합니다.

RDBMS 를 사용자 저장소로 사용하는 경우 다음 조각은 기본 CA Access Control 엔터프라이즈 관리 슈퍼 사용자를 설정합니다.

```
INSERT INTO tblUsers (ID,loginid, lastname, firstname, password) VALUES (1,'superadmin', 'Admin','Super', 'test')
```

이 SQL 명령은 암호 *test* 를 사용하여 *superadmin*(이름이 *Super*, 성이 *Admin*)이란 사용자 계정을 만듭니다.

편집하는 조각에서 사용자 계정을 sysadmin 으로 수정하고 암호 *C0mp!ex* 를 할당합니다.

```
INSERT INTO tblUsers (ID,loginid, lastname, firstname, password) VALUES (1,'sysadmin', 'Admin','System', 'C0mp!ex')
```

중앙 데이터베이스 스크립트 배포 예제

배포 스크립트의 사용자 지정을 완료한 다음에는 데이터베이스에 배포할 수 있습니다. 스크립트를 배포하면 중앙 데이터베이스를 채우고 CA Access Control 엔터프라이즈 관리 설치를 위해 데이터베이스를 준비합니다. 네이티브 데이터베이스 도구를 사용하여 스크립트를 배포합니다.

예: Oracle Database 10g 에서 CA Access Control Oracle 배포 스크립트 배포

이 예는 CA Access Control Oracle 배포를 Oracle Database 10g 에 배포하는 방법을 설명합니다.

1. "시작", "모든 프로그램", "Oracle - *ORACLE_HOME*", "Application Development", "SQL Plus"를 선택합니다.

   Oracle SQL*PLUS 창이 열립니다.
2. 앞에서 만든 사용자를 사용하여 Oracle 데이터베이스에 연결합니다.
3. @ 기호 다음에 스크립트 파일에 대한 전체 경로 이름을 입력합니다. 예:

   ```
   @C:\\temp_directory\AC126_oracle_script.sql
   ```

   Oracle 이 이 스크립트를 데이터베이스에 배포합니다.

예: SQL Server 2005 에서 CA Access Control Microsoft SQL Server 배포 스크립트 배포

이 예는 CA Access Control Microsoft SQL Server 배포를 SQL Server 2005 에 배포하는 방법을 설명합니다.

1. "시작", "모든 프로그램", "Microsoft SQL Server 2005", "SQL Server Management Studio"를 클릭합니다.

   로그인 창이 나타납니다.

2. 시스템 관리자로 로그인합니다.

   Microsoft SQL Server Management Studio 가 열립니다.

3. "파일", "열기", "파일"을 클릭합니다.

   "파일 열기" 대화 상자가 나타납니다.

4. CA Access Control Microsoft SQL Server 배포 스크립트를 찾아 선택한 다음 "열기"를 클릭합니다.

5. "사용 가능한 데이터베이스" 드롭다운 목록에서 앞에서 스크립트를 배포하기 위해 만든 데이터베이스를 선택합니다.

6. "실행"을 클릭하여 스크립트를 배포합니다.

   Microsoft SQL Server 가 스크립트를 데이터베이스에 배포합니다.

필수 소프트웨어 설치 유틸리티 실행

Windows 에 해당

CA Access Control 엔터프라이즈 관리를 실행하려면 JDK(Java Development Kit) 및 JBoss Application Server 가 필요합니다. CA Access Control Premium Edition "Third-Party Component"(타사 구성 요소) DVD 에는 이 필수 타사 소프트웨어의 올바른 버전이 포함되어 있습니다. 또한 이 DVD 에는 다음과 같이 필수 소프트웨어를 설치하는 유틸리티가 포함되어 있습니다.

- CA Access Control 엔터프라이즈 관리에 적절한 설정을 사용하여 설치하도록 JDK 및 JBoss 를 설정합니다.
- JBoss 를 서비스로서 설치합니다.
- 미리 구성된 필수 소프트웨어 설정을 사용하여 CA Access Control 엔터프라이즈 관리가 시작되도록 합니다.

이 소프트웨어가 이미 설치되어 있으면 이 단계를 건너뛰어도 됩니다. 이 소프트웨어가 설치되어 있지 않은 경우 제공된 유틸리티를 사용하여 이 절차에 설명된 방법대로 설치할 것을 권장합니다.

이미 JBoss 가 설치되어 있는 경우 사용 중인 포트 문제를 피하기 위해 CA Access Control 엔터프라이즈 관리 설치 전에 JBoss 를 한 번 실행하는 것이 좋습니다.

다음 단계를 수행하십시오.

1. Windows 용 CA Access Control Premium Edition "Third-Party Components"(타사 구성 요소) DVD 를 광 디스크 드라이브에 넣습니다.
2. 광학 디스크 드라이브에 있는 PrereqInstaller 디렉터리로 이동하여 **install_PRK.exe** 를 실행하십시오.

   InstallAnywhere 마법사가 열립니다.
3. 필요에 따라 마법사를 완료합니다.

   참고: JBoss 포트 번호를 추가로 구성하려면 "JBoss 포트 설정" 페이지에서 "고급 구성"을 선택하십시오. 지정한 JBoss 포트가 현재 사용 중이면 설치 관리자가 다른 포트 번호를 지정하도록 요구합니다.

4. 요약 보고서의 내용을 검토한 후 "설치"를 클릭합니다.

   필수 소프트웨어가 설치됩니다. 이 작업은 시간이 걸릴 수 있습니다.

5. 다음 작업 중 *하나*를 수행합니다.

   - 필수 소프트웨어 설치 이후에 CA Access Control 엔터프라이즈 관리 설치 프로세스를 시작하려면 요청될 때 사용하는 운영 체제용의 CA Access Control Premium Edition 서버 구성 요소 DVD 를 광학 디스크 드라이브에 넣은 다음 "완료"를 선택하십시오. 제품 탐색기 창이 표시되면 이 창을 닫습니다.
   - 고가용성 또는 재해 복구를 위해 추가 엔터프라이즈 관리 서버를 설치하려면 CA Access Control 엔터프라이즈 관리 설치에 사용할 사용자 지정 FIPS 키를 지정하십시오. 요구하는 경우 "완료" 및 "마침"을 클릭하여 표시된 대화 상자를 닫으십시오.
   - 필수 소프트웨어 설치 이후에 CA Access Control 엔터프라이즈 관리 설치를 시작하지 않으려면 요청될 때 "완료"와 "마침"을 각각 클릭하여 표시되는 대화 상자를 닫으십시오.

     필수 소프트웨어 설치 프로세스가 완료되었습니다.

엔터프라이즈 관리 서버 구성 요소를 설치하는 방법

엔터프라이즈 관리 서버 구성 요소를 사용하여 CA Access Control 의 엔터프라이즈 배포를 중앙에서 관리할 수 있습니다. 엔터프라이즈 관리 서버 구성 요소를 설치한 다음 보고 서비스를 설치하고 CA Access Control 과 UNAB 끝점을 설치합니다.

구현을 시작하기 전에 사용하는 컴퓨터가 요구되는 하드웨어 및 소프트웨어 사양을 충족하는지 확인하십시오.

참고: 요구되는 하드웨어 및 소프트웨어 사양에 대한 자세한 내용은 CA Support의 CA Access Control 제품 페이지에 있는 "CA Access Control Compatibility Matrix"(CA Access Control 호환성 표)를 참조하십시오.

엔터프라이즈 관리 서버 구성 요소를 설치하려면 다음을 수행하십시오.

1. 엔터프라이즈 관리 서버를 준비합니다.

   엔터프라이즈 관리 서버를 설치하기 전에 필수 구성 요소를 설치 및 구성하여 컴퓨터를 준비하십시오.

   참고: 엔터프라이즈 관리 서버를 설치하기 전에 시스템에 최신 소프트웨어 업데이트와 패치를 설치하는 것이 좋습니다.

2. 마스터 CA Access Control 엔터프라이즈 관리를 설치합니다.

   여기까지 모든 웹 기반 응용 프로그램, 배포 서버, DMS, CA Access Control 이 설치되었습니다.

3. (선택 사항) 부하 분산 엔터프라이즈 관리 서버를 설치합니다.

4. (선택 사항) Sun ONE 디렉터리 또는 CA Directory 사용자 저장소를 사용하도록 엔터프라이즈 관리 서버를 구성합니다.

   Active Directory 또는 관계형 데이터베이스 사용자 저장소 대신 Sun ONE 또는 CA Directory 사용자 저장소를 사용하도록 CA Access Control 엔터프라이즈 관리를 정의할 수 있습니다.

5. (선택 사항) 다음과 같이 SSL 통신을 위해 엔터프라이즈 관리 서버를 구성합니다.

   a. SSL 통신을 사용하도록 JBoss 를 구성합니다.

   b. (Active Directory) SSL 통신을 위해 엔터프라이즈 관리 서버를 구성합니다.

6. (선택 사항) 고급 구성을 설정합니다.

   CA Identity Manager 관리 콘솔을 사용하여 고급 구성 작업을 수행할 수 있습니다. 예를 들어, 중앙 데이터베이스의 속성을 수정하여 사용자 지정 보고서를 만들거나 CA Access Control 엔터프라이즈 관리를 구성하여 특정 이벤트가 발생할 때 전자 메일 알림을 보낼 수 있습니다.

7. (선택 사항) 엔터프라이즈 보고 기능을 구현합니다.

   엔터프라이즈 관리 서버는 CA Business Intelligence 공용 보고 서버(CA Access Control 보고서 포털)을 통해 보고 기능을 제공합니다.

8. (선택 사항) CA User Activity Reporting Module 와 통합합니다.

   엔터프라이즈 관리 서버를 설치했습니다. 이제 끝점을 설치하여 구성할 수 있습니다.

추가 정보:

보고 서비스 서버 구성 요소 설정 방법 (페이지 99)

Windows 에 CA Access Control 엔터프라이즈 관리 설치

CA Access Control 엔터프라이즈 관리를 설치하면 모든 엔터프라이즈 관리 서버 구성 요소가 설치됩니다. CA Access Control 엔터프라이즈 관리를 설치하기 전에 엔터프라이즈 관리 서버를 준비해야 합니다.

필수 구성 요소 설치 관리자를 사용하여 CA Access Control 엔터프라이즈 관리 설치를 시작하는 것이 좋습니다. 이 설치 관리자는 필수 타사 소프트웨어를 설치한 다음 CA Access Control 엔터프라이즈 관리 설치를 시작합니다.

참고: CA Access Control 엔터프라이즈 관리는 네트워크 설치를 통해 설치할 수 없습니다. CA Access Control Premium Edition 서버 구성 요소 DVD 의 Disk 1 디렉터리에 있는 전체 콘텐츠를 설치 디렉터리에 복사하거나 드라이브를 DVD 에 매핑하십시오.

다음 단계를 수행하십시오.

1. JBoss 응용 프로그램 서버가 실행 중이면 중지합니다.
2. CA Access Control 이 이미 설치된 컴퓨터에 CA Access Control 엔터프라이즈 관리를 설치하는 경우 CA Access Control 서비스를 중지합니다.
3. Windows 용 CA Access Control Premium Edition 서버 구성 요소 DVD 를 광 디스크 드라이브에 넣습니다.
4. 제품 탐색기에서 "구성 요소" 폴더를 확장한 다음 CA Access Control 엔터프라이즈 관리를 선택하고 "설치"를 클릭합니다.
   a. (선택 사항) 설치 중 사용할 사용자 지정 FIPS 키의 전체 경로 이름을 지정합니다.

      예를 들어, C:\tmp\FIPS.key 에 있는 사용자 지정 FIPS 키를 사용하여 설치하려면:

      ```
      E:\EnterpriseMgmt\Disk1\InstData\NoVM\install_EntM_r125.exe -DFIPS_KEY=C:\tmp\FIPSkey.dat
      ```

      중요! 고가용성을 위해 CA Access Control 엔터프라이즈 관리를 설치한 경우 주 및 보조 엔터프라이즈 관리 서버에 동일한 FIPS 키를 지정하십시오. FIPS 지원을 포함하여 고가용성을 위해 CA Access Control 엔터프라이즈 관리를 설치하는 경우 사용자 지정 FIPS 를 지정하십시오.

5. 필요에 따라 마법사를 완료합니다. 다음 설치 입력 항목은 자동으로 채워지지 않습니다.

설치 모드 선택

엔터프라이즈 관리 서버 설치 모드를 정의합니다.

- 주 엔터프라이즈 관리 서버 - 주 엔터프라이즈 관리 서버를 설치하도록 선택합니다.
- 부하 분산 엔터프라이즈 관리 서버 - 부하 분산 엔터프라이즈 관리 서버를 설치하도록 선택합니다.

중요! 설치 모드는 새 설치에만 적용됩니다.

설치 폴더 선택

설치 폴더의 전체 경로를 정의합니다.

기본값: \ProgramFiles\CA\AccessControlServer\

참고: 64 비트 운영 체제에서 기본 설치 폴더는 다음과 같습니다.

\Program Files(x86)\CA\AccessControlServer\

JDK(Java Development Kit)

기존 JDK 의 위치를 정의합니다.

참고: CA Access Control Premium Edition 타사 구성 요소 DVD 를 사용하여 필수 소프트웨어를 설치한 직후에 CA Access Control 엔터프라이즈 관리 설치를 실행하면 이 마법사 페이지가 나타나지 않습니다. 설치 유틸리티는 필수 소프트웨어 설치 프로세스 중에 제공한 값을 기반으로 이 페이지의 설치 설정을 구성합니다.

JBoss 응용 프로그램 서버 정보

응용 프로그램을 설치할 JBoss 인스턴스를 정의합니다.

이렇게 하려면 다음을 정의하십시오.

- JBoss 폴더: JBoss 가 설치된 최상위 디렉터리입니다.

  예를 들어 Windows 에서는 C:\jboss-4.2.3.GA, Solaris 에서는 /opt/jboss-4.2.3.GA 입니다.

- URL: 설치할 대상 컴퓨터의 IP 주소 또는 호스트 이름
- 포트: JBoss 가 사용하는 포트
- 포트: JBoss 가 보안 통신(HTTPS)을 위해 사용하는 포트
- 포트 번호

참고: CA Access Control Premium Edition 타사 구성 요소 DVD 를 사용하여 필수 소프트웨어를 설치한 직후에 CA Access Control 엔터프라이즈 관리 설치를 실행하면 이 마법사 페이지가 나타나지 않습니다. 설치 유틸리티는 필수 소프트웨어 설치 프로세스 중에 제공한 값을 기반으로 이 페이지의 설치 설정을 구성합니다.

통신 암호

(주 엔터프라이즈 관리 서버만 해당) CA Access Control 엔터프라이즈 관리 서버 내부 구성 요소 통신에 사용되는 암호를 정의합니다.

참고: CA Access Control 엔터프라이즈 관리는 통신 암호를 사용하여 메시지 큐 키 저장소와 관리자 계정을 관리하고, CA Access Control 엔터프라이즈 관리와 끝점 사이의 통신을 처리하고, Java Connection Server 를 관리합니다.

주 엔터프라이즈 관리 서버 정보

(부하 분산 엔터프라이즈 관리 서버 호스트 이름 또는 IP 주소 및 FIPS 키에 대한 전체 경로 이름을 정의합니다.

참고: 기본적으로 FIPS 키는 다음 경로에 있습니다. 여기서 *JBoss_HOME* 은 JBoss 를 설치한 디렉터리입니다.

JBoss_HOME/server/default/deploy/IdentityMinder.ear/config/com/netegrity/config/keys

데이터베이스 정보

RDBMS 에 대한 연결 세부 사항을 정의합니다.

- **데이터베이스 유형** - 지원되는 RDBMS 를 지정합니다.
- **호스트 이름** - RDBMS 를 설치한 호스트의 이름을 정의합니다.

- **포트 번호** - 지정한 RDBMS 에서 사용하는 포트를 정의합니다. 설치 프로그램에서는 RDBMS 의 기본 포트를 제공합니다.
- **서비스 이름** - (Oracle) 시스템에서 RDBMS 를 식별하는 이름을 정의합니다. 예를 들어, Oracle Database 10g 의 경우 이 이름은 기본적으로 *orcl* 입니다.
- **데이터베이스 이름** - (MS SQL) 만든 데이터베이스의 이름을 정의합니다.
- **사용자 이름** - 데이터베이스를 준비할 때 만든 사용자의 이름을 정의합니다.

  참고: 이 데이터베이스를 준비할 때 이 사용자에게 적절한 데이터베이스 권한을 부여했습니다.
- **암호** - 데이터베이스를 준비할 때 만든 사용자의 RDBMS 암호를 정의합니다.

설치 프로그램은 계속하기 전에 데이터베이스와의 연결을 확인합니다.

Active Directory 설정

Active Directory 사용자 저장소 설정을 정의합니다.

- **호스트** - Active Directory 의 도메인 컨트롤러 호스트 이름을 정의합니다.
- **포트** - Active Directory 에 대한 LDAP 쿼리에 기본적으로 사용되는 포트를 정의합니다. 예: 389
- **검색 루트** - 검색 루트(예: ou=DomainName, DC=com)를 정의합니다.

  참고: 사용자 DN 및 시스템 사용자에 대해 지정된 사용자의 고유 이름(DN)보다 디렉터리에서 최소한 한 노드 위에 검색 루트를 설정하십시오. 그렇지 않으면 엔터프라이즈 관리가 표시되는 탭 없이 시작될 수 있습니다.

- **사용자 DN** - CA Access Control 엔터프라이즈 관리를 관리하는 데 사용되는 Active Directory 사용자 계정 이름을 정의합니다. 예: CN=Administrator, cn=Users, DC=DomainName, DC=Com.

  참고: 이 사용자는 Active Directory 에 대해 LDAP 쿼리를 실행합니다. 이 매개 변수에 대해 읽기 전용 권한을 가진 사용자를 정의할 수 있습니다. 하지만 읽기 전용 권한 가진 사용자를 정의하면 CA Access Control 엔터프라이즈 관리의 사용자에게 관리자 역할이나 권한 있는 액세스 역할을 할당할 수 없습니다. 대신, Active Directory 그룹을 가리키도록 각 역할에 대한 구성원 정책을 수정합니다.

- **암호** - CA Access Control 엔터프라이즈 관리를 관리하는 데 사용되는 Active Directory 사용자 계정의 암호를 정의합니다.

설치 프로그램은 계속하기 전에 Active Directory 에 대한 연결을 검사합니다.

참고: DSQUERY 디렉터리 쿼리 유틸리티를 사용하여 사용자 DN(User Distinguished Name)을 검색할 수 있습니다. 이 쿼리는 반드시 Active Directory 서버에서 실행해야 합니다. 예:

dsquery user -*name* administrator
"CN=Administrator,CN=Users,DC=lab.DC=demo"

시스템 사용자

(Active Directory 에만 해당) CA Access Control 엔터프라이즈 관리에서 시스템 관리자 관리 역할이 할당된 Active Directory 사용자의 DN 을 정의합니다.

예: CN=SystemUser, ou=OrganizationalUnit, DC=DomainName, DC=Com

참고: 기본적으로 시스템 관리자 관리 역할이 있는 사용자는 CA Access Control 엔터프라이즈 관리에서 모든 작업을 수행하고, 만들고, 관리할 수 있습니다. 시스템 관리자 관리 역할에 대한 자세한 내용은 *엔터프라이즈 관리 안내서*를 참조하십시오.

관리자 암호

(포함된 사용자 저장소만 해당) CA Access Control 엔터프라이즈 관리 관리자인 *superadmin* 의 암호를 정의합니다. 설치가 완료되었을 때 CA Access Control 엔터프라이즈 관리에 로그인할 수 있도록 암호를 메모해 두십시오.

참고: 이 단계에서 포함된 사용자 저장소에 superadmin 사용자를 만듭니다. superadmin 사용자는 CA Access Control 엔터프라이즈 관리에서 시스템 관리자 관리 역할이 할당됩니다. CA Access Control 엔터프라이즈 관리에 처음 로그인할 때 superadmin 으로 로그인합니다. 시스템 관리자 관리 역할에 대한 자세한 내용은 *엔터프라이즈 관리 안내서*를 참조하십시오.

엔터프라이즈 관리 서버는 마법사를 완료한 후에 설치됩니다. 설치를 완료하려면 컴퓨터를 다시 시작하십시오.

6. "예, 컴퓨터를 다시 시작합니다"를 선택하고 "완료"를 클릭합니다.

   컴퓨터가 다시 시작됩니다. 이제 회사에 대한 CA Access Control 엔터프라이즈 관리를 구성할 수 있습니다.

Linux 에 CA Access Control 엔터프라이즈 관리 설치

CA Access Control 엔터프라이즈 관리를 설치하면 모든 엔터프라이즈 관리 서버 구성 요소가 설치됩니다. CA Access Control 엔터프라이즈 관리를 설치하기 전에 엔터프라이즈 관리 서버를 준비하십시오.

Linux 컴퓨터에 CA Access Control 엔터프라이즈 관리를 설치하려면 콘솔 설치를 사용하십시오.

다음 단계를 수행하십시오.

1. JBoss Application Server 가 실행 중이면 종료합니다.
2. CA Access Control 이 이미 설치된 컴퓨터에 CA Access Control 엔터프라이즈 관리를 설치하는 경우 CA Access Control 서비스를 중지합니다. 다음 단계를 수행하십시오.
   a. 다음 명령을 입력하여 CA Access Control 서비스를 중단합니다.

      /opt/CA/AccessControl/bin/secons -sk

      CA Access Control 이 중단됩니다.
   b. 다음 명령을 입력하여 CA Access Control 을 언로드합니다.

      /opt/CA/AccessControl/bin/SEOS_load -u

   CA Access Control 이 중단되고 컴퓨터에 설치할 준비가 됩니다.
3. 다음 단계를 완료합니다.
   a. 광학 디스크 드라이브에 사용하는 운영 체제용의 적절한 CA Access Control Premium Edition 서버 구성 요소 DVD 를 넣습니다.
   b. 광 디스크 드라이브를 마운트합니다. noexec 옵션을 지정하지 *마십시오*. noexec 옵션을 지정하면 설치가 실패합니다.

      참고: Linux 의 일부 릴리스에서는 운영 체제가 noexec 옵션을 사용하여 광학 디스크 드라이브를 자동 마운트합니다.
   c. 터미널 창을 열고 작업 디렉터리로서 쓰기 가능한 임시 디렉터리를 설정합니다.

      참고: 설치 관리자는 이 작업 디렉터리에서 설치 파일의 압축을 풉니다. 광학 미디어에 작업 디렉터리를 지정하면 설치 관리자가 파일의 압축을 풀지 못해 설치가 실패합니다.

d. 명령에 설치 관리자의 전체 경로를 지정하여 설치 관리자를 실행합니다. 예를 들어, /media 디렉터리에 광학 디스크 드라이브를 마운트하는 경우 다음 명령을 입력하십시오.

```
/media/EnterpriseMgmt/Disk1/InstData/NoVM/install_EntM_r125.bin -i console
```

설치 중 사용자 지정 FIPS 키를 사용하려면 -DFIPS_KEY=*경로* 형식을 사용하여 명령에 FIPS 키의 전체 경로 이름을 지정하십시오.예를 들어, /tmp/FIPSkey.dat 에 있는 사용자 지정 FIPS 키를 사용하여 설치하려면:

```
/media/EnterpriseMgmt/Disk1/InstData/NoVM/install_EntM_r125.bin -i console
-DFIPS_KEY=/tmp/FIPSkey.dat
```

중요! 고가용성을 위해 CA Access Control 엔터프라이즈 관리를 설치한 경우 주 및 보조 엔터프라이즈 관리 서버에 동일한 FIPS 키를 지정하십시오. FIPS 지원을 포함하여 고가용성을 위해 CA Access Control 엔터프라이즈 관리를 설치하는 경우 사용자 지정 FIPS 를 지정하십시오.

잠시 후 InstallAnywhere 콘솔이 나타납니다.

4. 필요에 따라 프롬프트를 완성합니다. 다음 설치 입력 항목은 자동으로 채워지지 않습니다.

JDK(Java Development Kit)

기존 JDK 의 위치를 정의합니다.

JBoss 응용 프로그램 서버 정보

응용 프로그램을 설치할 JBoss 인스턴스를 정의합니다.

다음 작업을 수행해야 합니다.

- JBoss 폴더를 정의하십시오. 이 폴더는 JBoss 를 설치한 최상위 디렉터리입니다.

  예: /opt/jboss-4.2.3.GA

- JBoss 에서 사용하는 포트를 정의하십시오.
- 보안 통신(HTTPS)을 위해 JBoss 가 사용하는 포트를 정의하십시오.
- 명명 포트 번호를 정의합니다.

참고: CA Access Control 엔터프라이즈 관리 설치 프로그램은 기본 JBoss 포트를 사용하지 않고 대신 기본 JBoss 포트 번호에 10000 을 추가합니다. 예를 들어, 설치 프로그램은 HTTP 연결에 대해 포트 번호 8080 대신 포트 번호 18080 을 사용합니다. JBoss 가 사용하는 포트를 지정하는지 확인하십시오.

통신 암호

(주 엔터프라이즈 관리 서버만 해당) CA Access Control 엔터프라이즈 관리 서버 내부 구성 요소 통신에 사용되는 암호를 정의합니다.

참고: CA Access Control 엔터프라이즈 관리는 통신 암호를 사용하여 메시지 큐 키 저장소와 관리자 계정을 관리하고, CA Access Control 엔터프라이즈 관리와 끝점 사이의 통신을 처리하고, Java Connection Server 를 관리합니다.

주 엔터프라이즈 관리 서버 정보

(부하 분산 엔터프라이즈 관리 서버 호스트 이름 또는 IP 주소 및 FIPS 키에 대한 전체 경로 이름을 정의합니다.

참고: 기본적으로 FIPS 키는 다음 경로에 있습니다. 여기서 *JBoss_HOME* 은 JBoss 를 설치한 디렉터리입니다.

JBoss_HOME/server/default/deploy/IdentityMinder.ear/config/com/netegrity/config/keys

데이터베이스 정보

RDBMS 에 대한 연결 세부 사항을 정의합니다.

- **데이터베이스 유형** - 지원되는 RDBMS 를 지정합니다.
- **호스트 이름** - RDBMS 를 설치한 호스트의 이름을 정의합니다.
- **포트 번호** - 지정한 RDBMS 에서 사용하는 포트를 정의합니다. 설치 프로그램에서는 RDBMS 의 기본 포트를 제공합니다.
- **서비스 이름** - (Oracle) 시스템에서 RDBMS 를 식별하는 이름을 정의합니다. 예를 들어, Oracle Database 10g 의 경우 이 이름은 기본적으로 *orcl* 입니다.
- **데이터베이스 이름** - (MS SQL) 만든 데이터베이스의 이름을 정의합니다.
- **사용자 이름** - 데이터베이스를 준비할 때 만든 사용자의 이름을 정의합니다.

  참고: 이 데이터베이스를 준비할 때 이 사용자에게 적절한 데이터베이스 권한을 부여했습니다.
- **암호** - 데이터베이스를 준비할 때 만든 사용자의 RDBMS 암호를 정의합니다.

설치 프로그램은 계속하기 전에 데이터베이스와의 연결을 확인합니다.

사용자 저장소 유형

CA Access Control 엔터프라이즈 관리가 사용하는 사용자 저장소 유형을 정의합니다. 다음 중 *하나*를 선택하십시오.

- **포함된 사용자 저장소** - CA Access Control 엔터프라이즈 관리는 RDBMS 에 사용자 정보를 저장합니다.
- **Active Directory -** 다음 화면에서 연결 세부 정보를 지정합니다.
- **다른 사용자 저장소** - CA Access Control 엔터프라이즈 관리 설치가 완료된 후 사용자 저장소 구성 정보를 지정합니다.

참고: 로그인 권한 부여 정책을 UNAB 로 배포하려면 "Active Directory" 또는 "다른 사용자 저장소"를 사용자 저장소로 선택해야 합니다. 사용자 저장소로 "Active Directory" 또는 "다른 사용자 저장소"를 선택하는 경우 CA Access Control 엔터프라이즈 관리에서 사용자 및 그룹을 만들거나 삭제할 수 없습니다. UNAB 및 Active Directory 제한 사항에 대한 자세한 내용은 *엔터프라이즈 관리 안내서*를 참조하십시오.

Active Directory 설정

Active Directory 사용자 저장소 설정을 정의합니다.

- **호스트** - Active Directory 의 도메인 컨트롤러 호스트 이름을 정의합니다.
- **포트** - Active Directory 에 대한 LDAP 쿼리에 기본적으로 사용되는 포트를 정의합니다. 예: 389
- **검색 루트** - 검색 루트(예: ou=DomainName, DC=com)를 정의합니다.

  참고: 사용자 DN 및 시스템 사용자에 대해 지정된 사용자의 고유 이름(DN)보다 디렉터리에서 최소한 한 노드 위에 검색 루트를 설정하십시오. 그렇지 않으면 엔터프라이즈 관리가 표시되는 탭 없이 시작될 수 있습니다.

- **사용자 DN** - CA Access Control 엔터프라이즈 관리를 관리하는 데 사용되는 Active Directory 사용자 계정 이름을 정의합니다. 예: CN=Administrator, cn=Users, DC=DomainName, DC=Com.

  참고: 이 사용자는 Active Directory 에 대해 LDAP 쿼리를 실행합니다. 이 매개 변수에 대해 읽기 전용 권한을 가진 사용자를 정의할 수 있습니다. 하지만 읽기 전용 권한 가진 사용자를 정의하면 CA Access Control 엔터프라이즈 관리의 사용자에게 관리자 역할이나 권한 있는 액세스 역할을 할당할 수 없습니다. 대신, Active Directory 그룹을 가리키도록 각 역할에 대한 구성원 정책을 수정합니다.

- **암호** - CA Access Control 엔터프라이즈 관리를 관리하는 데 사용되는 Active Directory 사용자 계정의 암호를 정의합니다.

설치 프로그램은 계속하기 전에 Active Directory 에 대한 연결을 검사합니다.

참고: DSQUERY 디렉터리 쿼리 유틸리티를 사용하여 사용자 DN(User Distinguished Name)을 검색할 수 있습니다. 이 쿼리는 반드시 Active Directory 서버에서 실행해야 합니다. 예:

dsquery user -*name* administrator
"CN=Administrator,CN=Users,DC=lab.DC=demo"

시스템 사용자

(Active Directory 에만 해당) CA Access Control 엔터프라이즈 관리에서 시스템 관리자 관리 역할이 할당된 Active Directory 사용자의 DN 을 정의합니다.

예: CN=SystemUser, ou=OrganizationalUnit, DC=DomainName, DC=Com

참고: 기본적으로 시스템 관리자 관리 역할이 있는 사용자는 CA Access Control 엔터프라이즈 관리에서 모든 작업을 수행하고, 만들고, 관리할 수 있습니다. 시스템 관리자 관리 역할에 대한 자세한 내용은 *엔터프라이즈 관리 안내서*를 참조하십시오.

관리자 암호

(포함된 사용자 저장소만 해당) CA Access Control 엔터프라이즈 관리 관리자인 *superadmin* 의 암호를 정의합니다. 설치가 완료되었을 때 CA Access Control 엔터프라이즈 관리에 로그인할 수 있도록 암호를 메모해 두십시오.

참고: 이 단계에서 포함된 사용자 저장소에 superadmin 사용자를 만듭니다. superadmin 사용자는 CA Access Control 엔터프라이즈 관리에서 시스템 관리자 관리 역할이 할당됩니다. CA Access Control 엔터프라이즈 관리에 처음 로그인할 때 superadmin 으로 로그인합니다. 시스템 관리자 관리 역할에 대한 자세한 내용은 *엔터프라이즈 관리 안내서*를 참조하십시오.

5. 설치 전 요약 정보를 검토합니다. 정보가 정확하면 Enter 키를 누릅니다.

   CA Access Control 엔터프라이즈 관리가 설치되었습니다.

6. Enter 키를 누릅니다.

   설치 관리자가 닫힙니다.

7. 필요하면 컴퓨터를 다시 시작합니다.

   환경에 대한 CA Access Control 엔터프라이즈 관리 구성을 계속하십시오.

부하 분산 엔터프라이즈 관리 서버 및 배포 서버 설치 후 구독자 만들기

여러 엔터프라이즈 관리 서버를 설치하는 경우 CA Access Control 엔터프라이즈 관리를 시작하기 전에 구독자를 만들어야 합니다. 주 엔터프라이즈 관리 서버에서 다음 절차를 완료하십시오.

중요! 부하 분산 엔터프라이즈 관리 서버 및 배포 서버를 설치하는 경우 이 단계를 완료하십시오.

다음 단계를 수행하십시오.

1. 명령 프롬프트 창을 엽니다.
2. 다음 명령을 입력하여 구독자를 만듭니다.

   sepmd -n DMS__DH__@<LB_entm>

참고: sepmd 유틸리티에 대한 자세한 내용은 *참조 안내서*를 참조하십시오.

제 4 장: SUN ONE 및 CA Directory 에 대한 엔터프라이즈 관리 서버 구성

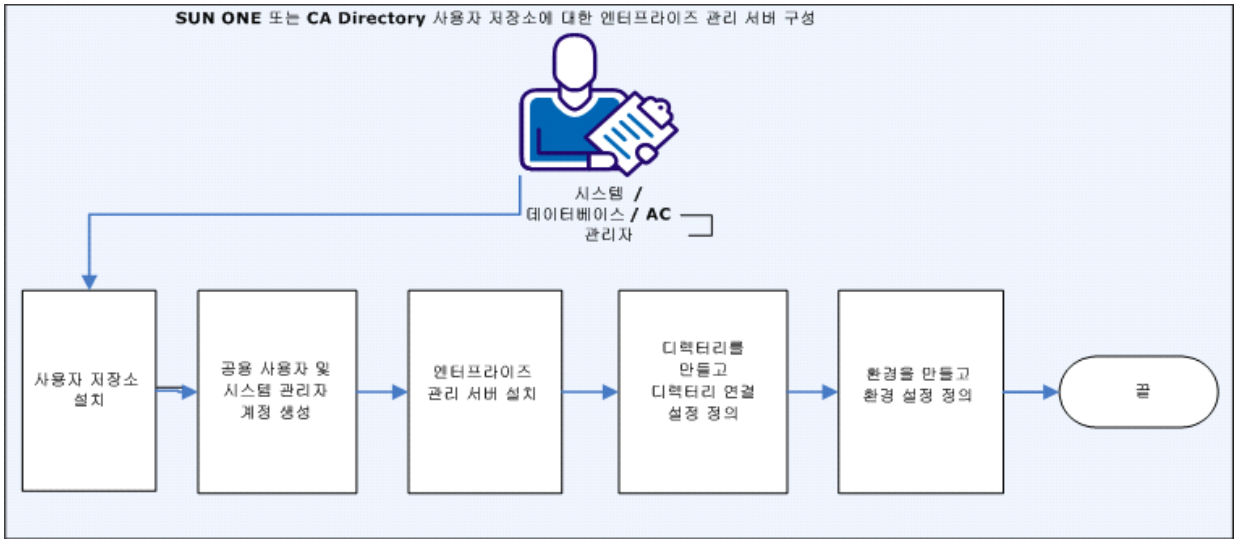
이 시나리오는 SUN ONE 또는 CA Directory 에 대한 엔터프라이즈 관리 서버를 구성하는 방법을 설명합니다. 사용자 저장소로 SUN ONE 또는 CA Directory 를 사용하는 경우 CA Access Control 엔터프라이즈 관리를 설치한 후에 사용자 저장소 설정을 구성합니다. 디렉터리 및 환경 설정을 구성하려면 CA Identity Manager 관리 콘솔을 사용합니다.

중요! 사용자 저장소로 SUN ONE 디렉터리 또는 CA Directory 를 사용하려면 CA Access Control 엔터프라이즈 관리 설치 마법사의 "사용자 저장소 선택" 화면에서 "다른 사용자 저장소" 옵션을 선택하십시오.

이 시나리오의 대상 독자:

- 시스템 관리자
- 데이터베이스 관리자
- CA Access Control 관리자

다음 다이어그램은 SUN ONE 또는 CA Directory 사용자 저장소에 대한 엔터프라이즈 관리 서버를 구성하기 위해 완료하는 단계를 설명합니다.



다음 단계를 수행하십시오.

1. 사용자 저장소 디렉터리를 설치합니다.

   참고: SUN ONE 의 경우 SUN ONE Directory Suite 와 Administration Services 를 설치하는지 확인하십시오. CA Directory 에 대한 자세한 내용은 *CA Directory Installation Guide*(CA Directory 설치 안내서)를 참조하십시오.

2. 공용 사용자 및 시스템 관리자 계정을 만듭니다.

   환경을 만들 때 사용자 자격 증명을 지정합니다.

3. 엔터프라이즈 관리 서버를 설치합니다.

   참고: 설치 중에 사용자 저장소를 지정하지 마십시오. 엔터프라이즈 관리 서버 설치에 대한 자세한 내용은 *구현 안내서를 참조하십시오.*

4. 디렉터리를 만들고 연결 설정을 정의합니다.

   - SUN ONE (페이지 70)
   - CA Directory (페이지 75)

5. 환경을 만들고 환경 설정을 정의합니다.

   - SUN ONE (페이지 71)
   - CA Directory (페이지 76)

   참고: 디렉터리 및 환경에 대한 설정은 CA Identity Manager 관리 콘솔을 사용하여 구성 및 정의합니다.

SUN ONE 사용자 저장소에 대한 디렉터리 만들기

디렉터리는 엔터프라이즈 관리 서버가 관리하는 사용자 디렉터리에 대한 정보를 제공합니다. 엔터프라이즈 관리 서버를 설치한 이후에 SUN ONE 디렉터리 설정을 구성합니다.

다음 단계를 수행하십시오.

1. 다음 디렉터리로 이동합니다. 여기서 *JBOSS_HOME* 은 JBoss 를 설치한 디렉터리를 나타냅니다.

   JBOSS_HOME/server/default/deploy/IdentityMinder.ear/user_console.war/META-INF/

2. SAM_iPlanet_directory.xml 파일을 찾아 임시 디렉터리에 복사합니다.

3. 다음과 같이 CA Identity Manager 관리 콘솔을 엽니다.

   http://*enterprise_host*:*port*/idmmanage

4. "디렉터리", "새로 만들기"를 선택합니다.

   새 디렉터리 창이 열립니다.

5. "찾아보기"를 선택하고 SAM_iPlanet_directory.xml 파일을 찾습니다. "다음"을 클릭합니다.

6. 다음 정보를 입력합니다.
   - **이름** - 디렉터리 논리적 이름을 정의합니다.
   - **설명** - (선택 사항) 디렉터리에 대한 설명을 지정합니다.
   - **개체 연결 이름** - 사용자 저장소의 이름을 지정합니다.
   - **호스트** - 디렉터리 호스트 이름 또는 IP 주소를 정의합니다.
   - **포트** - 디렉터리 포트 번호를 정의합니다.

     예: 389
   - **검색 루트** - 조직 검색 루트를 정의합니다. 디렉터리 검색은 루트 수준에서 시작됩니다.
   - **사용자 DN** - 디렉터리에 로그인할 수 있는 권한으로 사용자 계정을 정의합니다.

     예: cn=Usename, ou=Administration, ou=Corporate, o=Democorp, c=AU
   - **암호** - 사용자 계정 암호를 정의합니다.
   - **암호 확인** - 암호를 확인하기 위해 사용자 계정 암호를 입력합니다.
   - **보안 연결** - 디렉터리에 대한 연결의 보안이 유지됨을 나타냅니다.

7. "다음"과 "마침"을 클릭합니다.

   새 디렉터리가 만들어졌습니다. 이제 환경을 만들어야 합니다.

SUN ONE 사용자 저장소에 대한 환경 만들기

Windows 에 해당

SUN ONE 디렉터리에 대한 디렉터리 설정을 만들어 구성한 다음에는 환경을 만듭니다. 환경은 사용자 저장소의 한 뷰입니다. 환경에서는 사용자, 그룹, 조직, 작업, 역할을 관리합니다.

참고: JBoss Application Server 서비스는 Windows 가 시작될 때 자동으로 시작되고, 환경이 없는 경우 환경이 생성됩니다. 자동 서비스 시작은 비활성화하는 것이 좋습니다. 환경이 있으면 SUN ONE 사용자 저장소에 대한 환경을 만들기 전에 이 환경을 삭제하십시오.

환경을 만들기 전에 Sun ONE 사용자 디렉터리에 시스템 관리자 계정을 정의해야 합니다.

중요! 시스템 관리자 계정은 검색 루트 조직 단위(OU) 바로 아래에 정의하지 말고, 대신 검색 루트 아래에 있는 조직 단위에서 정의하십시오. 예를 들어, 정의한 검색 루트가 dc=company, dc-com 인 경우, 다음과 같이 시스템 관리자 계정을 사용자 OU 아래에 만드십시오:
uid=Sysmanager,ou=Users,dc=company,dc=com

다음 단계를 수행하십시오.

1. 다음 디렉터리로 이동합니다. 여기서 *JBOSS_HOME* 은 JBoss 를 설치한 디렉터리를 나타냅니다.

   JBOSS_HOME/server/default/deploy/IdentityMinder.ear/user_console.war/META-INF/

   a. 다음 파일을 찾아 임시 디렉터리로 복사합니다.

      ac-RoleDefinitions_Iplanet_EN.xml

      ac-environmentSettings.xml

   b. ac-environment.properties 파일이 있으면 삭제합니다.

2. CA Identity Manager 관리 콘솔을 열고 "환경"을 선택한 다음 "새로 만들기"를 선택합니다.

   새 환경 화면이 나타납니다.

3. 환경의 이름으로 **ac-env** 를 입력하고 설명을 입력한 다음 공용 URL 별칭으로 **ac** 를 입력한 후 "다음"을 클릭합니다.

   사용 가능한 디렉터리의 목록을 표시하는 화면이 나타납니다.

4. 이 환경에 연결할 정의된 SUN ONE 디렉터리를 선택하고 "다음"을 클릭합니다.

   a. (선택 사항) 이 환경에 대해 프로비저닝 디렉터리로 사용할 디렉터리를 선택합니다.

   b. (선택 사항) 익명 연결을 인증하기 위해 사용할 사용자 계정을 지정한 다음 "유효성 검사"를 선택합니다.

      CA Identity Manager 관리 콘솔이 사용자 계정의 유효성을 검사합니다.

5. 계속하려면 "다음"을 누르십시오.

6. "파일에서 역할 가져오기"를 선택하고 ac-RoleDefinitions_iPlanet_EN.xml 파일을 찾은 후 "다음"을 클릭합니다.
7. 사용자 관리자 계정을 지정하고 "추가"를 선택한 후 "다음"을 선택합니다.

   요약 화면이 열립니다.

   중요! 사용자 관리자 계정이 디렉터리에 있는지 확인하십시오.
8. 요약 정보를 검토한 다음 "마침"을 클릭합니다.

   CA Identity Manager 관리자 콘솔이 환경을 만듭니다.
9. "환경", "ac-env", "고급 설정"을 선택한 다음 "가져오기"를 클릭합니다.

   "설정 가져오기" 창이 열립니다.

   a. ac-environmentSettings.xml 파일을 저장한 디렉터리로 이동하여 이 파일을 선택한 다음 "마침"을 클릭합니다.

      CA Identity Manager 관리자 콘솔이 환경을 만듭니다.
10. "계속"을 선택한 다음 "시작"을 선택합니다.

    환경이 시작됩니다.
11. "환경", "ac-env", "고급 설정", "워크플로"를 선택합니다.

    워크플로 속성 창이 열립니다.

    a. "사용" 속성 옆의 확인란을 선택하여 워크플로를 활성화한 다음 "저장"을 클릭합니다.

       CA Identity Manager 관리 콘솔이 변경 내용을 환경에 적용합니다.
12. "환경", "ac-env", "시스템 관리자"를 선택합니다.

    "시스템 관리자" 창이 열립니다.

    a. 시스템 관리자 사용자 계정을 지정한 다음 "유효성 검사"를 선택합니다.

       CA Identity Manager 관리 콘솔이 시스템 관리자 계정 속성을 표시합니다.

    b. "다음", "마침"을 선택합니다.

       CA Identity Manager 관리 콘솔이 시스템 관리자 구성 출력을 표시하고 오류가 발견된 경우 오류를 표시합니다.

    c. "계속"을 선택합니다.

13. "상태" 필드에서 "다시 시작"을 선택합니다.

    CA Identity Manager 관리자 콘솔이 환경을 다시 시작합니다.

14. JBoss Application Server 를 다시 시작합니다.

    SUN ONE 디렉터리를 CA Access Control 엔터프라이즈 관리에 대한 사용자 저장소를 정의했습니다. 이제 CA Access Control 엔터프라이즈 관리에 로그인할 수 있습니다.

CA Directory 에 대한 디렉터리 만들기

한 디렉터리가 CA Access Control 엔터프라이즈 관리가 관리하는 사용자 디렉터리에 대한 정보를 제공합니다. CA Access Control 엔터프라이즈 관리를 설치한 이후에 CA Directory 설정을 구성합니다.

중요! 디렉터리의 UID 특성에 값이 없으면 디렉터리를 만들기 전에 SAM_CA_Directory.xml 파일을 편집해야 합니다. 예:

<ImsManagedObjectAttr physicalname="uid" displayname="User ID" description="User ID" valuetype="String" required="true" multivalued="false" wellknown="%USER_ID%" maxlength="0" permission="WRITEONCE"/>

참고: UID 특성에는 고유한 사용자 정의된 데이터가 있어야 합니다. 각 CA Directory 특성은 CA Directory XML 파일의 CA Access Control 엔터프라이즈 관리 특성에 한 번 매핑됩니다.

다음 단계를 수행하십시오.

1. 다음 디렉터리로 이동합니다. 여기서 JBoss_HOME 은 JBoss 를 설치한 디렉터리를 나타냅니다.

   JBoss_HOME/server/default.deploy/IdentityMinder.ear/user_console.war/META-INF/

2. 다음 파일을 임시 디렉터리에 복사합니다.
   a. SAM_CA_Directory.xml
   b. ac-RoleDefinitions_CADir_EN.xml
   c. ac-environmentSettings.xml
3. ac-environment.properties 파일이 있으면 삭제합니다.
4. JBoss Application Server 를 시작합니다.
5. 다음과 같이 CA Identity Manager 관리 콘솔을 엽니다.

   http://enterprise_host:port/idmmanage

   CA Identity Manager 관리 콘솔이 열립니다.
6. "디렉터리", "새로 만들기"를 선택합니다.

   새 디렉터리 창이 열립니다.
7. "찾아보기"를 선택하고 SAM_CA_Directory.xml 파일을 찾습니다. "다음"을 클릭합니다.
8. 다음 세부 정보를 입력합니다.
   - **이름** - 디렉터리 논리적 이름을 정의합니다.
   - **설명** - (선택 사항) 디렉터리에 대한 설명을 지정합니다.

- **개체 연결 이름** - 사용자 저장소의 이름을 지정합니다.
- **호스트** - 디렉터리 호스트 이름 또는 IP 주소를 정의합니다.
- **포트** - 디렉터리 포트 번호를 정의합니다.

  예: 389
- **검색 루트** - 조직 검색 루트를 정의합니다. 디렉터리 검색은 루트 수준에서 시작됩니다.

  참고: 여러 도메인을 사용하여 작업하는 경우 이 필드는 비워 두십시오.
- **사용자 DN** - 디렉터리에 로그인할 수 있는 권한으로 사용자 계정을 정의합니다.

  예: cn=Usename, ou=Administration, ou=Corporate, o=Democorp, c=AU
- **암호** - 사용자 계정 암호를 정의합니다.
- **암호 확인** - 암호를 확인하기 위해 사용자 계정 암호를 입력합니다.
- **보안 연결** - 디렉터리에 대한 연결의 보안이 유지됨을 나타냅니다.

9. "다음"과 "마침"을 클릭합니다.

   새 디렉터리가 만들어졌습니다. 이제 환경을 만들어야 합니다.

CA Directory 의 환경 만들기

Windows 에 해당

CA Directory 에 대한 디렉터리 설정을 만들어 구성한 다음에는 환경을 만듭니다. 환경은 사용자 저장소의 한 뷰입니다. 환경에서는 사용자, 그룹, 조직, 작업, 역할을 관리합니다.

참고: JBoss Application Server 서비스는 Windows 가 시작될 때 자동으로 시작되고, 환경이 없는 경우 환경이 생성됩니다. 자동 서비스 시작은 비활성화하는 것이 좋습니다. 환경이 있으면 CA Directory 에 대한 환경을 만들기 전에 이 환경을 삭제하십시오.

환경을 만들기 전에 CA Directory 에서 시스템 관리자 계정을 정의해야 합니다.

중요! 시스템 관리자 계정은 검색 루트 조직 단위(OU) 바로 아래에 정의하지 말고, 대신 검색 루트 아래에 있는 조직 단위에서 정의하십시오. 예를 들어, 정의한 검색 루트가 dc=company, dc-com 인 경우, 다음과 같이 시스템 관리자 계정을 사용자 OU 아래에 만드십시오:
uid=Sysmanager,ou=Users,dc=company,dc=com

참고: 여러 도메인을 지원하려면 사용자 전체 DN 을 정의하십시오.

다음 단계를 수행하십시오.

1. CA Identity Manager 관리 콘솔을 열고 "환경"을 선택한 다음 "새로 만들기"를 선택합니다.

   새 환경 화면이 나타납니다.

2. 환경의 이름으로 **ac-env** 를 입력하고 설명을 입력한 다음 공용 URL 별칭으로 **ac** 를 입력한 후 "다음"을 클릭합니다.

   사용 가능한 디렉터리의 목록을 표시하는 화면이 나타납니다.

3. 이 환경과 연계할 CA Directory 를 선택한 다음 "다음"을 클릭합니다.

   a. (선택 사항) 이 환경에 대해 프로비저닝 디렉터리로 사용할 디렉터리를 선택합니다.

   b. (선택 사항) 익명 연결을 인증하기 위해 사용할 사용자 계정을 지정한 다음 "유효성 검사"를 선택합니다.

      CA Identity Manager 관리 콘솔이 사용자 계정의 유효성을 검사합니다.

4. 계속하려면 "다음"을 누르십시오.

5. "파일에서 역할 가져오기"를 선택하고 ac-RoleDefinitions_CADir_EN.xml 파일을 찾은 후 "다음"을 클릭합니다.

6. 사용자 관리자 계정을 지정하고 "추가"를 선택한 후 "다음"을 선택합니다.

   참고: 여러 도메인을 지원하려면 사용자 전체 DN 을 지정하십시오.

   요약 화면이 열립니다.

   중요! 사용자 관리자 계정이 디렉터리에 있는지 확인하십시오.

7. 요약 정보를 검토한 다음 "마침"을 클릭합니다.

   CA Identity Manager 관리자 콘솔이 환경을 만듭니다.

8. "환경", "ac-env", "고급 설정"을 선택한 다음 "가져오기"를 클릭합니다.

   "설정 가져오기" 창이 열립니다.

   a. ac-environmentSettings.xml 파일을 저장한 디렉터리로 이동하여 이 파일을 선택한 다음 "마침"을 클릭합니다.

      CA Identity Manager 관리자 콘솔이 환경을 만듭니다.

9. "계속"을 선택한 다음 "시작"을 선택합니다.

   환경이 시작됩니다.

10. "환경", "ac-env", "고급 설정", "워크플로"를 선택합니다.

    워크플로 속성 창이 열립니다.

    a. "사용" 속성 옆의 확인란을 선택하여 워크플로를 활성화한 다음 "저장"을 클릭합니다.

       CA Identity Manager 관리 콘솔이 변경 내용을 환경에 적용합니다.

11. "환경", "ac-env", "시스템 관리자"를 선택합니다.

    "시스템 관리자" 창이 열립니다.

    a. 시스템 관리자 사용자 계정을 지정한 다음 "유효성 검사"를 선택합니다.

       CA Identity Manager 관리 콘솔이 시스템 관리자 계정 속성을 표시합니다.

    b. "다음", "마침"을 선택합니다.

       CA Identity Manager 관리 콘솔이 시스템 관리자 구성 출력을 표시하고 오류가 발견된 경우 오류를 표시합니다.

    c. "계속"을 선택합니다.

12. "상태" 필드에서 "다시 시작"을 선택합니다.

    CA Identity Manager 관리자 콘솔이 환경을 다시 시작합니다.

13. JBoss Application Server 를 다시 시작합니다.

14. "명령 프롬프트" 창을 열고 bin 디렉터리로 이동합니다.
15. 다음 명령을 실행하여 CredentialSender 를 실행합니다.

    CredentialsSender cn=root,dc=etasa dc=im,dc=etasa <communication_password> CA Portal <yes|no>

    예:CredentialSecder cn=root,dc=etasa,dc=im,dc=esata *password* 20411 yes

CA Directory 를 사용하도록 CA Access Control 엔터프라이즈 관리를 정의했습니다. 이제 CA Access Control 엔터프라이즈 관리에 로그인할 수 있습니다.

CA Access Control 엔터프라이즈 관리 시작

CA Access Control 엔터프라이즈 관리를 설치한 후에는 CA Access Control 및 웹 응용 프로그램 서버를 시작해야 합니다.

다음 단계를 수행하십시오.

1. CA Access Control 서비스가 시작되었는지 확인합니다.

   CA Access Control 엔터프라이즈 관리를 시작하려면 CA Access Control 이 실행되고 있어야 합니다.

2. JBoss Application Server 서비스가 시작되었는지 확인합니다. JBoss Application Server 서비스가 시작되지 않은 경우 다음 중 하나를 수행하십시오.

   - (Windows) "시작", "프로그램", "CA", "Access Control", "작업 엔진 시작"을 클릭합니다.

     참고: 처음 시작하는 경우 작업 엔진이 로드될 때까지 시간이 걸릴 수 있습니다.

   - "서비스" 패널에서 "JBoss Application Server" 서비스를 시작합니다.
   - (Linux) ./JBOSS_DIR/bin/run.sh -b 0.0.0.0 을 입력합니다.

   JBoss Application Server 의 로드가 완료되면 CA Access Control 엔터프라이즈 관리 웹 기반 인터페이스에 로그인할 수 있습니다.

CA Access Control 엔터프라이즈 관리 열기

CA Access Control 엔터프라이즈 관리를 설치해서 시작했으면 CA Access Control 엔터프라이즈 관리에 대한 URL 을 사용하여 원격 컴퓨터에서 웹 기반 인터페이스를 시작할 수 있습니다.

CA Access Control 엔터프라이즈 관리를 열려면

1. 웹 브라우저를 열고 호스트에 대해 다음 URL 중 *하나*를 입력합니다.
   - SSL 이 아닌 연결을 사용하려면 다음 URL 을 입력하십시오.

     http://*enterprise_host*:*port*/iam/ac
   - SSL 연결을 사용하려면 다음 URL 을 입력하십시오.

     https://*enterprise_host*:*HTTPSport*/iam/ac
2. 사용자의 자격 증명을 사용하여 로그인합니다.

   CA Access Control 엔터프라이즈 관리 홈 페이지가 나타납니다.

참고: "시작", "프로그램", "CA", "Access Control", "엔터프라이즈 관리"를 클릭하여 CA Access Control 엔터프라이즈 관리를 설치한 Windows 컴퓨터에서 CA Access Control 엔터프라이즈 관리를 열 수도 있습니다.

예: CA Access Control 엔터프라이즈 관리 열기

네트워크에 있는 임의의 컴퓨터에서 CA Access Control 엔터프라이즈 관리를 열려면 웹 브라우저에 다음 URL 을 입력하십시오.

http://appserver123:18080/iam/ac

이 URL 은 CA Access Control 엔터프라이즈 관리가 appserver123 이라는 이름의 호스트에 설치되었으며 기본 CA Access Control 엔터프라이즈 관리 포트 18080 을 사용함을 나타냅니다.

예: SSL 을 사용하여 CA Access Control 엔터프라이즈 관리 열기

네트워크에 있는 임의의 컴퓨터에서 SSL 을 사용하여 CA Access Control 엔터프라이즈 관리를 열려면 웹 브라우저에 다음 URL 을 입력하십시오.

https://appserver123:18443/iam/ac

이 URL 은 CA Access Control 엔터프라이즈 관리가 appserver123 이라는 이름의 호스트에 설치되었으며 기본 CA Access Control 엔터프라이즈 관리 SSL 포트 18443 을 사용함을 나타냅니다.

엔터프라이즈 관리 서버 SSL 통신

기본적으로 엔터프라이즈 관리 서버 구성 요소는 통신에 SSL 을 사용하지 않습니다. SSL 을 사용하여 통신하기 위해 다음 구성 요소를 설정할 수 있습니다.

- JBoss Application Server

  기본적으로 JBoss 는 SSL 지원 없이 설치됩니다.

- 메시지 큐

  잘 알려진 포트에 대한 무단 액세스를 방지하기 위해 메시지 큐 기본 SSL 포트를 수정할 수 있습니다.

- CA Access Control 엔터프라이즈 관리

- (선택 사항) Java Connector Server

  기본 인증서를 사용한 경우에만 CA Access Control r12.5 SP3 으로 업그레이드한 이후에 새 SSL 인증서를 가져오십시오.

JBoss 를 위한 SSL 통신

기본적으로 JBoss 는 SSL 지원 없이 설치됩니다. 즉, CA Access Control 엔터프라이즈 관리와 JBoss 사이의 모든 통신은 암호화되지 않습니다. 통신 보안을 유지하기 위해 JBoss 에서 SSL 을 사용하도록 구성할 수 있습니다.

참고: JBoss 에서 SSL 을 구성하는 방법에 대한 자세한 내용은 JBoss 제품 설명서를 참조하십시오.

예: Windows 에서 SSL 통신을 사용하도록 JBoss 구성

이 예는 보안 통신을 위해 SSL 을 사용하도록 JBoss Application Server 를 구성하는 방법을 설명합니다.

중요! 이 절차는 JBoss 버전 4.2.3 및 JDK 버전 1.5.0 을 사용하여 JBoss 에서 통신 보안을 위해 SSL 을 사용하도록 구성하는 방법에 대해 설명합니다.

다음 단계를 수행하십시오.

1. JBoss 가 실행 중인 경우 중지합니다.
2. 명령 프롬프트 창을 열고 다음 디렉터리로 이동합니다.

   JBoss_HOME\server\default\deploy\IdentityMinder.ear\custom\ppm\truststore

3. 다음 명령을 입력하여 기본 SSL 키 저장소 암호를 변경합니다.

   keytool -storepasswd -new *password* -keystore ssl.keystore -storepass secret

   -storepasswd

   키 저장소 암호를 변경하도록 지정합니다. 암호의 길이는 6 자 이상이어야 합니다.

   -keystore

   인증서를 추가할 키 저장소 이름을 지정합니다.

   -keystore

   키 저장소 이름을 지정합니다.

   -storepass

   키 저장소를 보호하는 데 사용되는 암호를 정의합니다.

4. 다음 명령을 입력하여 엔터프라이즈 관리 서버를 위한 키를 만듭니다.

   keytool -genkey -alias entm -keystore ssl.keystore -keyalg RSA

   -genkey

   명령이 키 쌍(공개 키 및 개인 키)을 생성하도록 지정합니다.

   -alias

   키 저장소에 항목을 추가하기 위해 사용할 별칭을 정의합니다.

   -keyalg

   키 쌍을 생성하기 위해 사용할 알고리즘을 지정합니다.

   keytool 유틸리티가 시작됩니다.

5. 암호 *secret* 를 입력합니다.
6. 지시에 따라 프롬프트를 완성하고 Enter 키를 눌러 입력한 매개 변수를 확인합니다.

   인증서가 키 저장소에 추가됩니다.

   참고: 키 저장소 및 키 별칭은 동일한 암호를 사용해야 합니다.

7. 다음 명령을 입력하여 키 저장소 암호를 파일로 암호화합니다.

   java -cp JBoss_HOME/server/default/lib/jbossx.jar org.jboss.security.plugins.FilePassword welcometojboss 13 *passowrd* <*kestore_password*> keystore.password

   참고: Salt 및 IterationCount 는 암호화된 암호의 강도를 정의하는 변수입니다. 이 예에서 "welcometojboss"가 salt 이고, 13 이 반복 횟수입니다.

8. 다음 디렉터리에서 server.xml 이란 이름의 파일을 찾아 편집을 위해 엽니다.

   JBossInstallDir\server\default\deploy\jboss-web.deployer

9. 다음 섹션에서 <Connector Port> 태그를 찾습니다.

```
<!-- Define a SSL HTTP/1.1 Connector on port 8443
     This connector uses the JSSE configuration, when using APR, the
     connector should be using the OpenSSL style configuration
     described in the APR documentation -->
  <!--
  <Connector port="18443" protocol="HTTP/1.1" SSLEnabled="true"
       maxThreads="150" scheme="https" secure="true"
       clientAuth="false" sslProtocol="TLS" />
```

   참고: 커넥터 포트 번호는 필수 소프트웨어 또는 CA Access Control 엔터프라이즈 관리 설치 프로세스 중에 지정한 JBoss HTTPS 포트 번호와 일치합니다.

10. <Connector port> 태그 위에서 "<!--"의 주석을 제거합니다.

    이제 이 태그를 편집할 수 있습니다.

11. <Connector port> 태그에 다음 속성을 추가합니다.

```
securityDomain="java:/jaas/encrypt-keystore-password" SSLImplementation="org.jboss.net.ssl.JBossImplementation"
```

12. server.xml 파일을 저장한 후 닫습니다.

13. 다음 디렉터리로 이동하여 jboss-service.xml 파일을 찾습니다.

    JBOss_HOME/server/default/deploy/jboss-web.deployer/META-INF

14. <server>과 </server> 태그 사이에 다음 mbean 을 추가합니다.

```
<mbean code="org.jboss.security.plugins.JaasSecurityDomain" name="jboss.security:service=PBESecurityDomain">
    <constructor>
      <arg type="java.lang.String" value="encrypt-keystore-password"></arg>
    </constructor>
    <attribute
name="KeyStoreURL">${jboss.server.home.dir}/deploy/IdentityMinder.ear/custom/ppm/truststore/ssl.keystore</attribute>
    <attribute
name="KeyStorePass">{CLASS}org.jboss.security.plugins.FilePassword:${jboss.server.home.dir}/deploy/IdentityMinder.ear/custom/ppm/truststore/keystore.password</attribute>
<attribute name="Salt">welcometojboss</attribute>
<attribute name="IterationCount">13</attribute>
 </mbean>
```

   참고: 위의 예에서 welcometojboss 가 salt 이고, 13 이 반복 횟수입니다.

15. jboss-service.xml 파일을 저장하고 닫습니다.
16. CA Access Control 엔터프라이즈 관리를 시작하고 엽니다.

    참고: 이 절차를 완료한 다음에는 SSL 사용 또는 비사용 모드로 JBoss 및 CA Access Control 엔터프라이즈 관리에 연결하도록 선택할 수 있습니다.

SSL 통신을 사용하도록 CA Access Control 엔터프라이즈 관리를 구성하는 방법

기본적으로 CA Access Control 엔터프라이즈 관리는 SSL 지원 없이 설치됩니다. 즉, CA Access Control 엔터프라이즈 관리와 사용자 디렉터리 사이의 통신은 암호화되지 않습니다. Active Directory 또는 CA Directory 를 사용하여 작업할 때 SSL 을 사용하도록 CA Access Control 엔터프라이즈 관리를 구성할 수 있습니다. SSL 을 사용하도록 CA Access Control 엔터프라이즈 관리를 구성하려면 다음을 수행하십시오.

1. DER, CRT, CERT 형식으로 사용자 디렉터리 인증서를 획득합니다.
2. 인증서를 키 저장소에 추가합니다.
3. SSL 통신을 사용하도록 CA Access Control 엔터프라이즈 관리 구성합니다.

추가 정보:

사용자 디렉터리 인증서를 키 저장소에 추가 (페이지 84)
SSL 통신을 사용하도록 CA Access Control 엔터프라이즈 관리 구성 (페이지 86)

사용자 디렉터리 인증서를 키 저장소에 추가

SSL 통신을 사용하도록 CA Access Control 엔터프라이즈 관리를 구성하기 전에 사용자 디렉터리 인증서를 키 저장소에 추가하십시오.

참고: Active Directory 또는 CA Directory 에서 SSL 을 구성하는 방법에 대한 자세한 내용은 Active Directory 및 CA Directory 설명서를 참조하십시오.

예: Active Directory 인증서를 키 저장소에 추가

중요! 이 예는 JBoss 버전 4.2.3 및 JDK 버전 1.5.0 을 사용하는 Active Directory 와의 보안 통신을 위해 SSL 을 사용하도록 CA Access Control 엔터프라이즈 관리를 구성하는 방법에 대해 설명합니다. 이 절차를 시작하기 전에 DER, CER, CERT 암호화된 바이너리 형식의 Active Directory 인증서를 획득해야 합니다.

1. JBoss 가 실행 중인 경우 중지합니다. 다음 작업 중 *하나*를 수행합니다.
   - JBoss 작업 창에서 프로세스를 인터럽트(Ctrl+C)합니다.
   - "서비스" 패널에서 "JBoss Application Server" 서비스를 중지합니다.
2. 엔터프라이즈 관리 서버에서 명령 프롬프트 창을 열고 다음 디렉터리로 이동합니다.

   jbossInstallDir/server/default/deploy/IdentityMinder.ear/custom/ppm/truststore
3. 다음 명령을 입력합니다.

   keytool -import -keystore ssl.keystore -*alias ad* -file <*activedirecoty.cert*>

   암호 프롬프트가 나타납니다.

   -import

   유틸리티가 인증서를 읽어 키 저장소에 저장하도록 지정합니다.

   -alias

   키 저장소에 항목을 추가하기 위해 사용할 별칭을 지정합니다.

   -file

   Active Directory 인증서 파일의 전체 경로 이름을 지정합니다.
4. 암호 *secret* 를 입력합니다.
5. JBoss bin 디렉터리로 이동합니다. 기본적으로 이 디렉터리는 다음 위치에 있습니다.

   JbossInstallDir/bin
6. run.bat 파일을 열고 트러스트된 사용자 저장소 데이터로 java_ops 매개 변수를 설정합니다. 예:

   set JAVA_OPTS=%JAVA_OPTS% -Xms128m -Xmx512m
   -Djavax.net.ssl.trustStore=C:\jboss-4.2.3.GA\server\default\deploy\IdentityMinder.ear\custom\ppm\truststore\ssl.keystor
   e
7. 파일을 저장하고 JBoss 를 시작합니다.

추가 정보:

SSL 통신을 사용하도록 CA Access Control 엔터프라이즈 관리 구성 (페이지 86)

SSL 통신을 사용하도록 CA Access Control 엔터프라이즈 관리 구성

사용자 디렉터리 인증서를 키 저장소에 추가한 다음에 SSL 통신을 사용하도록 CA Access Control 엔터프라이즈 관리를 구성할 수 있습니다.

참고: SSL 연결을 사용하도록 CA Access Control 엔터프라이즈 관리를 구성하려면 CA Identity Manager 관리 콘솔을 활성화해야 합니다. CA Identity Manager 관리 콘솔에 대한 자세한 내용은 *CA Identity Manager 관리 콘솔 온라인 도움말*을 참조하십시오.

SSL 통신을 사용하도록 CA Access Control 엔터프라이즈 관리를 구성하려면

1. CA Identity Manager 관리 콘솔에서 "디렉터리"를 클릭합니다.
2. ac-dir 디렉터리를 클릭합니다.

   "디렉터리 속성" 창이 나타납니다.
3. 속성 창의 맨 아래에서 "내보내기"를 클릭합니다.
4. 요청을 받으면 XML 파일을 저장합니다.
5. 편집을 위해 XML 파일을 엽니다.
6. <Provider userdirectory="ac-dir" type="LDAP"> 태그를 찾습니다.
7. 'secure' 매개 변수를 true 로 변경합니다. 예:

   <LDAP searchroot="DC=abc,DC=company,DC=com" secure="true">
8. <Connection host="COMPUTER.abc.company.com" port=" "> 태그를 찾은 다음 포트 번호를 636 으로 변경합니다. 예:

   <Connection host="COMPUTER.abc.company.com" port="636">
9. <Container objectclass="top,organizationalUnit" attribute="ou"/> 태그를 모두 찾아 각 줄 끝에 *value* 매개 변수를 입력합니다. 예:

   <Container objectclass="top,organizationalUnit" attribute="ou" value=""/>
10. 파일을 저장합니다.
11. CA Identity Manager 관리 콘솔에 있는 디렉터리 속성 페이지에서 "업데이트"를 클릭합니다.

    "디렉터리 업데이트" 창이 나타납니다.

12. Identity Manager 디렉터리를 업데이트하기 위한 XML 파일의 경로와 파일 이름을 입력하거나 파일을 탐색한 다음 "마침"을 클릭합니다.

    상태 정보는 "디렉터리 구성 출력"에 표시됩니다.

13. "계속"을 클릭하고 환경을 다시 시작합니다.

    CA Access Control 엔터프라이즈 관리가 이제 SSL 을 사용하여 사용자 디렉터리와 통신합니다.

추가 정보:

CA Identity Manager 관리 콘솔 활성화 (페이지 88)
CA Identity Manager 관리 콘솔 열기 (페이지 88)
사용자 디렉터리 인증서를 키 저장소에 추가 (페이지 84)

고급 구성

CA Identity Manager 관리 콘솔을 사용하여 보고 데이터베이스의 속성을 수정하여 사용자 지정 보고서를 만들거나 CA Access Control 엔터프라이즈 관리를 구성하여 특정 이벤트가 발생할 때 전자 메일 알림을 보내는 것과 같은 고급 구성 작업을 수행할 수 있습니다.

CA Identity Manager 관리 콘솔을 사용하면 디렉터리의 시각적 표시 및 관리를 제어하는 환경을 만들어 관리할 수 있습니다.

참고: 자세한 내용은 제품에 포함된 *CA Identity Manager 관리 콘솔 온라인 도움말*을 참조하십시오.

추가 정보:

CA Identity Manager 관리 콘솔 활성화 (페이지 88)
CA Identity Manager 관리 콘솔 열기 (페이지 88)
전자 메일 알림 설정 구성 (페이지 89)

CA Identity Manager 관리 콘솔 활성화

엔터프라이즈 관리 서버를 처음 설치하면 CA Identity Manager 관리 콘솔 옵션이 비활성화되어 있습니다. CA Identity Manager 관리 콘솔을 활성화하려면 기본 설정을 변경하십시오.

중요!: 설치 중에 Active Directory 또는 포함된 사용자 저장소를 사용하도록 선택한 경우에만 아래 절차를 수행하십시오.

CA Identity Manager 관리 콘솔을 활성화하려면

1. JBoss 가 실행 중인 경우 중지합니다. 다음 작업 중 *하나*를 수행합니다.
   - JBoss 작업 창에서 프로세스를 인터럽트(Ctrl+C)합니다.
   - "서비스" 패널에서 "JBoss Application Server" 서비스를 중지합니다.
2. 다음 디렉터리로 이동합니다. 여기서 *JBoss_HOME* 은 JBoss 를 설치한 디렉터리를 나타냅니다.

   JBoss_HOME/server/default/deploy/
   IdentityMinder.ear/management_console.war/WEB-INF
3. 편집 가능한 형식으로 *web.xml* 파일을 엽니다.
4. 다음 섹션을 찾습니다.

   AccessFilter
5. <param-value> 필드에서 값을 'True'로 변경합니다.
6. 파일을 저장한 후 닫습니다.
7. JBoss 를 시작합니다.

   CA Identity Manager 관리 콘솔이 활성화됩니다.

CA Identity Manager 관리 콘솔 열기

CA Identity Manager 관리 콘솔은 웹 기반 인터페이스를 사용합니다. CA Identity Manager 관리 콘솔을 활성화하고 CA Access Control 엔터프라이즈 관리를 시작하면 네트워크에 있는 모든 컴퓨터에서 CA Identity Manager 관리 콘솔을 열 수 있습니다.

CA Identity Manager 관리 콘솔을 열려면 웹 브라우저를 열고 호스트에 대해 다음 URL 을 입력하십시오.

http://*enterprise_host*:*port*/idmmanage

CA Identity Manager 관리 콘솔이 열립니다.

예: CA Identity Manager 관리 콘솔 열기

다음 URL 을 웹 브라우저에 입력하면 네트워크에 있는 모든 컴퓨터에서 CA Identity Manager 관리 콘솔을 열 수 있습니다.

http://appserver123:18080/idmmanage

이 예에서 CA Identity Manager 관리 콘솔은 appserver123 이란 이름의 호스트에 설치되어 있으며 기본 CA Access Control 엔터프라이즈 관리 포트 18080 을 사용합니다.

전자 메일 알림 설정 구성

CA Identity Manager 관리 콘솔을 열 때는 *환경*에서 작업하게 됩니다. 디렉터리의 시각적 표시 및 관리는 환경에 의해 제어됩니다. 예를 들어, 환경에서 보고 데이터베이스 설정을 정의하고 전자 메일 알림 옵션을 설정할 수 있습니다. PUPM 이벤트에 대해 전자 메일 알림만 활성화하는 것이 좋습니다.

참고: 환경에 대한 자세한 내용은 콘솔에서 제공되는 *CA Identity Manager 관리 콘솔 온라인 도움말*을 참조하십시오.

중요! 환경에 대한 변경 내용은 CA Access Control 엔터프라이즈 관리의 안정성에 영향을 줄 수 있습니다. 도움이 필요한 경우 기술 지원부(http://ca.com/support)에 문의하십시오.

전자 메일 알림 설정을 구성하려면

1. JBoss 가 실행 중인 경우 중지합니다. 다음 작업 중 *하나*를 수행합니다.
   - JBoss 가 서비스로서 설치되지 않은 경우 JBoss 응용 프로그램 서버 창을 인터럽트(Ctrl+C)합니다.
   - JBoss 가 서비스로서 설치된 경우 "서비스" 창에서 JBoss 서비스를 중지합니다.
2. mail-service.xml 파일을 엽니다. 기본적으로 파일은 다음 디렉터리에 있습니다.

   JBoss_HOME/server/default/deploy
3. 파일에서 다음 항목을 찾습니다.

   <property name="mail.smtp.host" value="smtp.nosuchhost.nosuchdomain.com"/>

4. smtp.nosuchhost.nosuchdomain.com 값을 나가는 전자 메일 서버 호스트(SMTP 서버)의 전체 DNS 도메인 이름으로 변경합니다. 예:

   myMailServer.myDomain.com

   참고: 엔터프라이즈 관리 서버의 호스트 파일은 SMTP 서버의 IP 주소를 이 속성에 대해 지정하는 전체 DNS 도메인 이름으로 확인해야 합니다.

5. 전자 메일 알림을 구성할 각 이벤트에 대해 다음을 수행합니다.

   a. 해당 전자 메일 템플릿을 엽니다. 예를 들어, 받는 사람에게 권한 있는 계정 암호 요청이 승인되었음을 알리는 전자 메일 알림을 구성하려면 다음 디렉터리에서 CreatePrivilegedAccountExceptionEvent.tmpl 파일을 여십시오.

      JBoss_HOME/server/default/deploy/IdentityMinder.ear/custom/emailTemplates/default/approved

      참고: 전자 메일 템플릿에 대한 자세한 내용은 *엔터프라이즈 관리 안내서*를 참조하십시오.

   b. 템플릿 호스트 이름과 포트를 "localhost:8080"에서 엔터프라이즈 관리 서버 호스트 이름 및 포트(예: *computer.com:18080*)로 수정합니다.

   c. 파일을 저장한 후 닫습니다.

6. email.properties 파일을 엽니다. 이 파일은 다음 디렉터리에 있습니다.

   JBoss_HOME/server/default/deploy/IdentityMinder.ear/config/com/netegrity/config/

7. 보내는 사람 전자 메일 주소를 지정한 다음 파일을 닫습니다. 예:

   admin.email.address=admin@company.com

8. JBoss 를 시작합니다.

9. CA Identity Manager 관리 콘솔에서 구성할 "환경"을 클릭한 다음 "고급 설정", "전자 메일"을 클릭합니다.

   "전자 메일 속성" 창이 나타납니다.

10. 다음과 같이 엔터프라이즈에 사용 가능한 옵션을 구성합니다.

이벤트 전자 메일 활성화됨

PUPM 이벤트를 포함하여 CA Access Control 엔터프라이즈 관리 이벤트에 대한 전자 메일 알림을 활성화합니다.

작업 전자 메일 활성화됨

CA Access Control 엔터프라이즈 관리 작업에 대한 전자 메일 알림을 활성화합니다.

참고: CA Access Control 엔터프라이즈 관리는 작업에 대한 전자 메일 템플릿을 제공하지 않습니다. 작업에 대해 전자 메일 알림을 활성화하지 않는 것이 좋습니다.

템플릿 디렉터리

CA Access Control 엔터프라이즈 관리가 전자 메일 메시지를 작성하는 데 사용하는 전자 메일 템플릿의 위치를 지정합니다.

참고: 전자 메일 템플릿은 다음 디렉터리에 있습니다.

jboss_dir/server/default/deploy/IdentityMinder.ear/custom/emailTemplates/default

11. 전자 메일 알림을 전달할 이벤트를 지정합니다.

전자 메일 템플릿이 제공되는 PUPM 이벤트만 지정하는 것이 좋습니다. 다음 작업을 수행하십시오.

a. 다음 PUPM 이벤트를 *제외*하고 모든 이벤트 옆의 확인란을 선택합니다.

- BreakGlassCheckOutAccountEvent
- CheckOutAccountPasswordEvent
- CreatePrivilegedAccountExceptionEvent

b. "삭제"를 클릭합니다.

세 개의 PUPM 이벤트를 제외하고 모든 이벤트가 삭제됩니다. 이러한 세 개의 PUPM 이벤트에 대해 전자 메일 알림을 보내도록 CA Access Control 엔터프라이즈 관리를 구성했습니다.

12. "저장"을 클릭합니다.

    전자 메일 알림 속성이 저장됩니다.

13. "다시 시작"을 클릭합니다.

    CA Identity Manager 관리 콘솔이 환경을 다시 시작하고 변경 내용을 적용합니다.

참고: 전자 메일 알림에 대한 자세한 내용은 *엔터프라이즈 관리 안내서*를 참조하십시오.

Windows 에서 CA Access Control 엔터프라이즈 관리 제거

Windows 에 해당

Windows 에서 CA Access Control 엔터프라이즈 관리를 제거하려면 Windows 관리 권한이 있는 사용자(즉, Windows administrator 또는 Windows Administrators 그룹의 구성원)로 Windows 시스템에 로그인되어 있어야 합니다.

참고: 이 절차는 필수 소프트웨어를 제거하지 않습니다. 필수 소프트웨어를 제거하려면 JDK 를 제거하기 전에 먼저 JBoss 를 제거해야 합니다. 필수 소프트웨어 제거에 대한 자세한 내용은 제품 설명서를 참조하십시오.

Windows 에서 CA Access Control 엔터프라이즈 관리를 제거하려면

1. JBoss 가 실행 중인 경우 중지합니다.
2. "시작", "제어판", "프로그램 추가/제거"를 차례로 클릭합니다.

   "프로그램 추가/제거" 대화 상자가 나타납니다.

3. 프로그램 목록을 스크롤하여 CA Access Control 엔터프라이즈 관리를 선택합니다.
4. "변경/제거"를 클릭합니다.

   CA Access Control 엔터프라이즈 관리 제거 마법사가 나타납니다.

5. 마법사의 지침을 따라 CA Access Control 엔터프라이즈 관리를 제거합니다.

   제거가 완료되고 컴퓨터에서 CA Access Control 엔터프라이즈 관리가 제거됩니다.

6. "마침"을 클릭하여 마법사를 닫습니다.

Linux 에서 CA Access Control 엔터프라이즈 관리 제거

컴퓨터에서 CA Access Control 엔터프라이즈 관리를 제거하려면 CA Access Control 엔터프라이즈 관리에서 제공하는 제거 프로그램을 사용해야 합니다.

다음 단계를 수행하십시오.

1. 다음 중 *하나*를 수행하여 JBoss 를 중지합니다.
   - JBoss 작업 창에서 프로세스를 인터럽트(Ctrl+C)합니다.
   - 다른 창에서 다음을 입력합니다.

     ./*JBoss_path*/bin/shutdown -S
2. 다음 명령을 입력합니다.

   "/*ACPMInstallDir*/Uninstall_EnterpriseManagement/Uninstall_CA_Access_Control_Enterprise_Management"

   ACPMInstallDir

   CA Access Control 엔터프라이즈 관리의 설치 디렉터리를 정의합니다. 기본적으로 이 경로는 다음과 같습니다.

   /opt/CA/AccessControlServer/

   InstallAnywhere 가 제거 마법사와 콘솔을 로드합니다.
3. 화면에 표시되는 메시지에 따라 CA Access Control 엔터프라이즈 관리를 제거합니다.

   제거가 완료되고 컴퓨터에서 CA Access Control 엔터프라이즈 관리가 제거됩니다.

엔터프라이즈 관리 서버에서 추가 구성 요소 제거

CA Access Control 엔터프라이즈 관리를 완전히 제거하려면 제거 프로그램을 실행한 다음에 컴퓨터에서 추가 구성 요소를 제거하십시오.

비즈니스 데이터의 손실을 방지하기 위해 제거 프로그램은 다음 리소스를 제거하지 않습니다.

- *JBoss_Dir*/server/default/conf/accesscontrol 에 있는 CA Access Control 끝점 관리 필터
- *ACServerDir*/MessageQueue/tibco/ems/data 에 있는 메시지 큐 데이터 파일

엔터프라이즈 관리 서버에서 추가 구성 요소를 제거하려면

1. 다음 디렉터리를 삭제합니다.
   - *JBoss_Dir*/server/default/deploy/IdentityMinder.ear
   - *JBoss_Dir*/server/default/deploy/SiteMinderAgent.ear
2. CA Access Control 을 제거합니다.
3. (Windows) 다음 레지스트리 키를 제거합니다.

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\uninstall\CA Access Control Advanced Policy Management Server
4. 다음과 같이 JCS 를 삭제합니다.
   a. (Windows) "프로그램 추가/제거" 대화 상자를 사용하여 "CA Identity Manager – Connector Server"를 제거합니다.
   b. jcs.exe 프로세스를 중지합니다.
   c. "CA Identity Manager – Connector Server (Java)" 서비스를 삭제합니다.
5. 엔터프라이즈 관리 서버를 설치한 디렉터리를 삭제합니다.

   예를 들어 C:\Program Files\CA\AccessControlServer 를 삭제합니다.

   이제 모든 CA Access Control 엔터프라이즈 관리 구성 요소가 컴퓨터에서 제거됩니다.

추가 정보:

제거 방법 (페이지 177)

배포 서버 구현

배포 서버는 응용 프로그램 서버와 끝점 사이의 통신을 처리합니다. 기본적으로 배포 서버는 엔터프라이즈 관리 서버에 설치됩니다. 장애 조치 및 고가용성 용도로 회사에 여러 개의 배포 서버를 설치할 수 있습니다.

배포 서버 설치

CA Access Control 배포의 크기를 조정하려거나 별도의 끝점에 있는 끝점에 서비스를 제공하려면 별도 컴퓨터에 배포 서버를 설치하고 배포 서버가 이들 사이에서 파일을 전파하도록 구성하십시오.

다음 단계를 수행하십시오.

1. 광학 디스크 드라이브에 사용하는 운영 체제용의 적절한 CA Access Control Premium Edition 서버 구성 요소 DVD 를 넣습니다.
2. 다음 단계를 완료합니다.
   - Windows 의 경우:

     자동 실행이 활성화된 경우 제품 탐색기가 자동으로 표시됩니다. 다음 단계를 수행하십시오.

     a. 제품 탐색기가 열리지 않으면 광학 디스크 드라이브 디렉터리로 이동한 다음 ProductExplorerx86.EXE 파일을 두 번 클릭합니다.

     b. 제품 탐색기에서 "구성 요소" 폴더를 확장한 다음 CA Access Control 배포 서버를 선택하고 "설치"를 클릭합니다.
   - Linux 의 경우:

     a. 광 디스크 드라이브를 마운트합니다.

     b. 터미널 창을 열고 광 디스크 드라이브에서 다음 디렉터리로 이동합니다.

     /DistServer/Disk1/InstData/NoVM

     c. 다음 명령을 실행합니다.

     ./install_DistServer_r125.bin -i console

3. 필요에 따라 마법사를 완료합니다. 다음 설치 입력 항목은 자동으로 채워지지 않습니다.

   메시지 큐 설정

   메시지 큐 서버 관리자 암호(통신 암호)를 정의합니다.

   제한: 최소 6 자

   Java Connector Server - 프로비저닝 디렉터리 정보

   Java Connector Server 의 암호를 정의합니다.

   참고: Java Connector Server 는 CA Access Control 엔터프라이즈 관리에 권한 있는 계정 관리 기능을 제공합니다.

   CA Access Control 배포 서버 설치가 완료됩니다.

   중요! 엔터프라이즈 관리 서버를 설치하는 동안 정의한 동일한 통신 암호를 지정하십시오. CA Access Control 엔터프라이즈 관리는 이 통신 암호를 사용하여 CA Access Control 엔터프라이즈 관리와 끝점 사이의 통신을 관리하고, 메시지 큐 키 저장소와 관리자 계정을 관리하고, Java Connection Server 를 관리합니다.

   참고: 배포 서버를 재해 복구 구현의 일부로 설치한 경우 추가 단계를 완료하십시오.

추가 정보:

프로덕션 배포 서버 설정 (페이지 382)
재해 복구 배포 서버 설정 (페이지 384)

제 5 장: 엔터프라이즈 보고 기능 구현

이 섹션은 다음 항목을 포함하고 있습니다.

엔터프라이즈 보고 기능

CA Access Control 엔터프라이즈 관리는 CA Business Intelligence 공용 보고 서버(CA Access Control 보고서 포털)을 통해 보고 기능을 제공합니다. 엔터프라이즈 보고 기능을 사용하면 한 위치에서 각 끝점(사용자, 그룹 및 리소스)의 보안 상태를 볼 수 있습니다. CA Access Control 보고서는 각 끝점에서 누가 무엇을 할 수 있으며 정책 위반이 있는지 여부를 결정하는 규칙 및 정책을 기술합니다.

구성된 이후에 CA Access Control 엔터프라이즈 보고 기능은 독립적으로 실행되어 수동 개입 없이 지속적으로 각 끝점에서 데이터를 수집하여 이 정보를 중앙 서버에 저장합니다. 예약을 통해 또는 요청 시에 각 끝점에서 데이터를 수집할 수 있습니다. 어떤 사용자가 어떤 리소스에 액세스할 수 있는 권한이 있는지 확인하기 위해 각 끝점에 일일이 연결할 필요가 없습니다. 수집 서버가 실행 중인지 여부에 관계없이 각 끝점은 자신의 상태를 보고합니다.

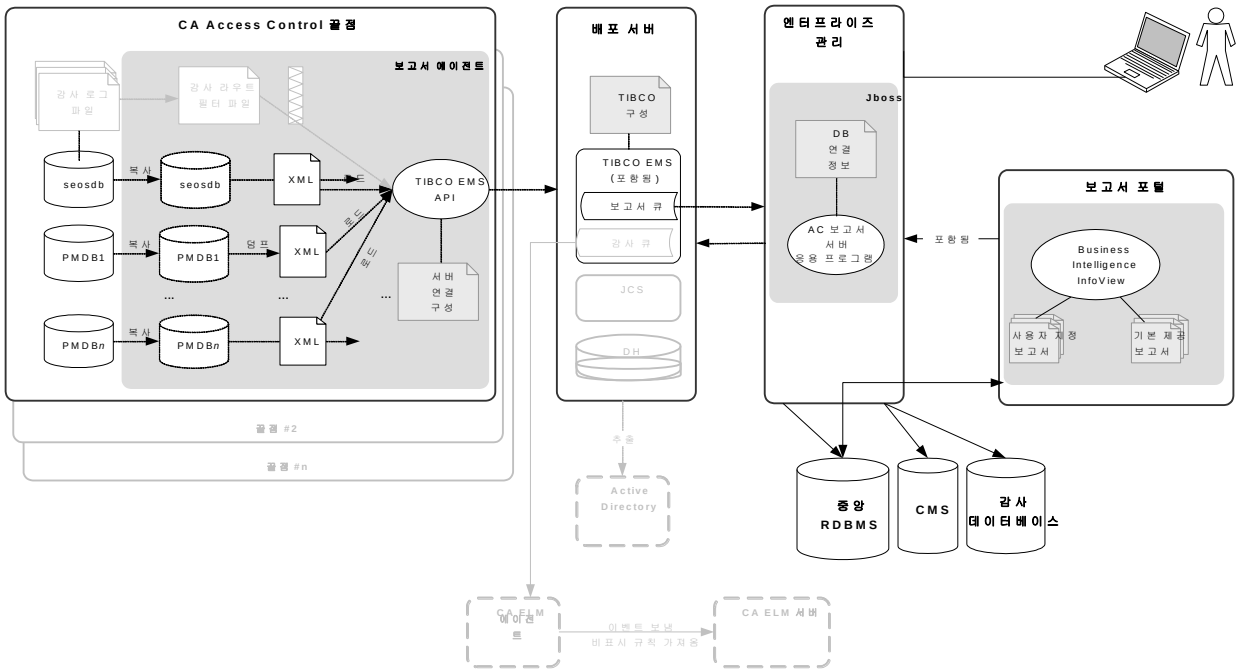
보고 서비스 아키텍처

CA Access Control 보고 서비스는 CA Access Control 엔터프라이즈 보고를 위한 서버 기반 플랫폼을 제공합니다. 이 플랫폼을 사용하여 모든 CA Access Control 끝점의 데이터가 들어 있는 보고서를 작성할 수 있습니다. 작성한 보고서는 웹에서 사용할 수 있는 응용 프로그램을 통해 보고 관리할 수 있습니다.

보고 서비스를 사용하면 기존 CA Access Control 인프라 위에 보고 환경을 구축할 수 있습니다.

참고: 엔터프라이즈 보고에 대한 자세한 내용은 *엔터프라이즈 관리 안내서*를 참조하십시오.

다음 다이어그램에서는 보고 서비스 구성 요소의 아키텍처를 보여줍니다. 또한 다음 다이어그램에서는 구성 요소 간의 데이터 흐름을 보여줍니다.



앞의 다이어그램은 다음을 보여줍니다.

- 하나의 CA Access Control 데이터베이스(seosdb)와 임의의 수의 정책 모델(PMDB)이 들어 있는 각 끝점에 보고서 에이전트 구성 요소가 설치되어 있습니다.
- 보고서 에이전트가 끝점에서 데이터를 수집하여 이를 처리하도록 배포 서버로 전송합니다.
- 간단한 엔터프라이즈 모델에서는 하나의 배포 서버를 사용하여 모든 끝점 데이터를 처리하고 중앙 데이터베이스로 보내 저장합니다. 또한 대규모 엔터프라이즈 환경에서 내결함성을 확보하고 처리 성능을 높이기 위해 배포 서버 구성 요소를 복제할 수도 있습니다.
- 중앙 데이터베이스(RDBMS)는 끝점 데이터를 저장합니다.
- 보고서 포털을 사용하면 중앙 데이터베이스의 데이터에 액세스하여 기본 제공 보고서를 만들거나 데이터를 조사하여 사용자 지정 보고서를 만들 수 있습니다.

보고 서비스 서버 구성 요소 설정 방법

엔터프라이즈 보고를 사용하려면 CA Access Control 보고 서비스 서버 구성 요소를 설치 및 구성하십시오. 이 서버 구성 요소를 설치 및 구성한 이후에 각 끝점에서 보고서 에이전트를 구성하십시오.

참고: 보고서 에이전트 설치 및 구성은 CA Access Control 및 UNAB 끝점 설치의 일부이며 이 절차에서는 다루지 않습니다.

보고 서비스 서버 구성 요소를 설치하려면 다음 절차를 따르십시오.

1. 이미 수행하지 않은 경우 엔터프라이즈 관리 서버를 설치 및 구성합니다.
2. 보고서 포털 컴퓨터(CA Business Intelligence)를 설정합니다.

   CA Business Intelligence 설치 파일은 CA Support 웹 사이트에서 찾을 수 있습니다.
3. 보고서 포털에 CA Access Control 보고서 패키지를 배포합니다.
4. CA Business Intelligence 에 대한 연결을 구성합니다.
5. 스냅숏 정의를 만듭니다.

   CA Business Intelligence 및 CA Access Control 엔터프라이즈 관리에서 이제 보고서를 생성하고 볼 수 있습니다.

참고: 보고서 생성 및 보기에 대해 자세한 내용은 *엔터프라이즈 관리 안내서*를 참조하십시오.

추가 정보:

보고를 위해 Windows 끝점 구성 (페이지 175)
보고를 위해 UNIX 끝점 구성 (페이지 240)
보고를 위한 UNAB 구성 (페이지 321)

보고서 포털 컴퓨터를 설정하는 방법

보고서 포털을 사용하면 기본 제공 보고서를 만들거나 데이터를 검색하여 사용자 지정 보고서를 만들기 위해 CA Access Control 엔터프라이즈 관리가 중앙 데이터베이스에 저장하는 끝점 데이터에 액세스할 수 있습니다. 보고서 포털은 CA Business Intelligence 를 사용합니다.

참고: 이전 버전의 보고서 포털이나 독립 실행형으로 설치된 CA Business Intelligence 또는 BusinessObjects Enterprise XI 가 이미 있는 경우 업그레이드할 필요 없이 기존 설치된 제품을 대신 사용할 수 있습니다.

보고서 포털을 설정하려면 다음을 수행하십시오.

1. Oracle 데이터베이스를 사용하는 경우 보고서 포털 컴퓨터에 전체 Oracle 클라이언트를 설치하십시오.
2. Microsoft SQL Server 를 사용하는 경우 보고서 포털 컴퓨터에 Microsoft SQL Server Native Client 를 설치하십시오.
3. 중앙 데이터베이스와 배포 서버를 아직 설정하지 않았으면 지금 설정합니다.

   참고: 엔터프라이즈 관리 서버를 설치할 때 중앙 데이터베이스와 배포 서버를 설정합니다.
4. (UNIX) 보고서 포털 컴퓨터가 Solaris 또는 Linux 컴퓨터인 경우 CA Business Intelligence 설치를 위해 UNIX 컴퓨터를 준비합니다.
5. 보고서 포털과 엔터프라이즈 관리 서버의 시스템 시간을 동기화합니다.

   시스템 시간을 동기화하지 않으면 CA Access Control 엔터프라이즈 관리가 생성하는 보고서가 보류 또는 되풀이 상태로 유지됩니다.
6. 사용하는 운영 체제용 CA Business Intelligence 를 설치합니다.

   CA Business Intelligence 설치 파일은 CA Support 웹 사이트에서 찾을 수 있습니다.

   참고: Windows 용 보고서 포털은 기본적으로 Microsoft SQL Server 인증을 사용하여 연결을 인증합니다. 인증을 위해 도메인 사용자 계정 설정을 사용하려면 Windows 인증에서 작업 (페이지 419)하도록 보고서 포털을 구성할 수 있습니다.

   보고서 포털이 설정되고 이제 CA Access Control 보고서 패키지를 배포할 수 있습니다.

참고: CA Business Intelligence 에 대한 자세한 내용은 CA Technologies Support에 있는 *CA Business Intelligence 설치 안내서*를 참조하십시오.

예: Windows 에서 CA Business Intelligence 설치

다음 절차는 Windows 에서 CA Business Intelligence 를 설치하는 절차를 설명합니다.

참고: 설치는 완료될 때까지 약 한 시간 정도 걸릴 수 있습니다.

1. 광 디스크 드라이브에 Windows 용 CA Business Intelligence DVD 를 넣습니다.
2. \Disk1\InstData\VM 폴더로 이동하여 install.exe 를 두 번 클릭합니다.

   CA Business Intelligence 설치 마법사가 시작됩니다.
3. 다음 표를 사용하여 설치 마법사를 완료합니다.

정보	동작
설치 언어	사용할 지원되는 설치 언어를 선택한 다음 "확인"을 클릭하십시오. **참고:** 영어 이외의 지원되는 언어로 설치하려면 현지화(로컬라이제이션)된 운영 체제가 필요합니다.
사용권 계약	"동의함"을 선택한 하고 "다음"을 클릭하십시오.
설치 유형	유형을 선택하고 "다음"을 클릭하십시오.
비 root 자격 증명	비 root 사용자 이름과 암호를 입력하십시오.
BusinessObjects XI 관리자 암호	P@ssw0rd 를 암호 및 암호 확인에 입력한 후 "다음"을 클릭하십시오. **참고:** 암호 규칙에 대한 자세한 내용은 CA Access Control Premium Edition 북셸프에 있는 *CA Business Intelligence 설치 안내서*를 참조하십시오.
웹 서버 구성	"다음"을 클릭하여 기본값을 사용하십시오.

정보	동작
CMS 데이터베이스 설정	다음 정보를 입력한 다음 "다음"을 클릭하십시오. ■ **MySQL 루트 암호:** P@ssw0rd ■ **사용자 이름:** cadbusr ■ **암호:** C0nf1dent1al ■ **데이터베이스 이름:** MySQL1 **참고:** CA Business Intelligence 중앙 관리 서버(CMS)는 내부 관리 용도로만 사용됩니다.
감사 사용	"다음"을 클릭하여 기본값을 사용하십시오.
감사 데이터베이스 설정	다음 정보를 입력한 다음 "다음"을 클릭하십시오. ■ **사용자 이름:** cadbusr ■ **암호:** C0nf1dent1al ■ **데이터베이스 이름:** MySQL1
설정 검토	설정을 검토한 다음 "설치"를 클릭하여 설치를 완료하십시오.

설치가 시작되고 완료될 때까지 약 한 시간 정도 걸릴 수 있습니다.

중요! CA Business Intelligence 중앙 관리 서버(CMS)는 내부 관리 용도로만 사용되며 보고서를 생성 및 표시하는 데 사용되는 보고서 데이터를 포함하지 않습니다. CA Access Control 엔터프라이즈 관리를 설치할 때 정의한 보고 데이터베이스는 보고서 에이전트가 배포 서버로 업로드하는 데이터를 포함하고 있습니다. CMS 에 대한 자세한 내용은 *CA Business Intelligence 설치 안내서*를 참조하십시오.

CA Business Intelligence 설치를 위해 Linux 준비

Linux 에 CA Business Intelligence 를 설치하려면 우선 설치를 위해 컴퓨터를 준비하십시오. CA Business Intelligence 설치를 위한 비 root 사용자를 만들고, Oracle RDBMS 가 CA Business Intelligence 의 설치를 위해 노출되어 있는지 확인하고, 환경 변수를 설정하십시오.

다음 단계를 수행하십시오.

1. root 사용자로 로그인합니다.
2. 비 root 사용자를 만듭니다. CA Business Intelligence 설치에는 비 root 사용자가 필요합니다.

   예를 들어, 그룹 'other'에 속한 사용자 'bouser'를 만들려면 다음 명령을 입력하십시오.

   ```
   groupadd other
   useradd -d /home/bouser -g other -m -s /bin/bash -c bouser bouser
   passwd bouser
   ```

   메시지가 나타나면 정의한 사용자에 대해 암호를 입력 및 확인합니다.
3. LANG 환경 변수가 다음과 같이 구성되었는지 확인합니다.

   ```
   LANG=en US.utf8
   ```
4. 작성한 비루트 사용자로 로그인합니다.
5. ORACLE_HOME 및 TNS_ADMIN 환경 변수가 올바르게 설정되었는지 확인하기 위해 다음 명령을 입력합니다.

   ```
   echo $ORACLE_HOME
   echo $TNS_ADMIN
   ```

   출력이 비어 있지 않으면 이러한 환경 변수가 유효한 것입니다. 예:

   ```
   /opt/oracle/app/oracle/product/10.2.0/client_1
   /opt/oracle/app/oracle/product/10.2.0/client_1/admin/network
   ```

   명령에 대한 출력이 비어 있으면 만든 비 root 사용자에 대해 변수가 설정되어 있는지 확인하십시오. 예를 들면, /home/bouser/.profile 을 다음과 같이 편집합니다.

   ```
   ORACLE_HOME=/opt/oracle/app/oracle/product/10.2.0/client_1
   export ORACLE_HOME
   TNS_ADMIN=$ORACLE_HOME/network/admin
   export TNS_ADMIN
   ```

6. 비루트 사용자에 대한 LD_LIBRARY_PATH 에 다음 경로가 포함되어 있는지 확인합니다.

   $ORACLE_HOME/lib:$ORACLE_HOME/lib32

   예를 들면, 다음 명령을 입력하고 이러한 경로의 출력을 검색합니다.

   echo $LD_LIBRARY_PATH

   이러한 경로가 누락되었으면 이 경로를 LD_LIBRARY_PATH 에 추가합니다. 예를 들면, /home/bouser/.profile 을 다음과 같이 편집합니다.

   LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$ORACLE_HOME/lib:$ORACLE_HOME/lib32
   export LD_LIBRARY_PATH

7. LD_LIBRARY_PATH 및 TNS_ADMIN 의 폴더가 액세스 가능한 폴더인지 다음과 같이 확인합니다.

   ls -l $ORACLE_HOME
   ls -l $TNS_ADMIN/tnsnames.ora

   이러한 명령 실행 결과 **사용 권한이 거부되었습니다** 오류가 반환되지 않아야 합니다. 이 오류가 반환될 경우 적절한 권한을 허용해야 합니다. 예를 들어 root/oracle 사용자는 다음 명령을 실행해야 합니다.

   chmod -R +xr $ORACLE_HOME

8. TNS Ping 유틸리티를 사용하여 Oracle 연결이 유효한지 다음과 같이 확인합니다.

   $ORACLE_HOME/bin/tnsping *service_name*

   TNS Ping 의 출력은 다음 예와 유사합니다.

   TNS Ping Utility for Solaris: Version 10.2.0.1.0 - Production on 07-MAY-2008 09:17:02
   Copyright (c) 1997, 2005, Oracle. All rights reserved.
   Used parameter files:
   /opt/oracle/app/oracle/oracle/product/10.2.0/client_1/network/admin/sqlnet.ora
   Used TNSNAMES adapter to resolve the alias
   Attempting to contact (DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP)(HOST = 172.16.234.75)(PORT = 1521))) (CONNECT_DATA = (SERVICE_NAME = *service_name*)))
   OK (30 msec)

   이제 Linux 에 CA Business Intelligence 를 설치할 수 있습니다.

보고서 패키지 배포

보고서 패키지는 CA Access Control 표준 보고서를 배포하는 .BIAR 파일입니다. 여기에는 보고서 포털에서의 배포에 대한 아티팩트 및 설명자 모음이 수록되어 있습니다. 이러한 표준 보고서를 사용하려면 보고서 패키지 파일을 BusinessObjects InfoView 로 가져와야 합니다.

참고: 패키지는 보고서 포털의 이전 버전과 호환됩니다. 최신 보고서 패키지를 사용하기 위해 보고서 포털을 업그레이드할 필요는 없습니다. 또한, 별도의 .biar 파일로 제공되는 현지화(로컬라이제이션)된 보고서 패키지를 함께 배포할 수도 있습니다.

보고서 포털에 보고서 패키지 배포

표준 CA Access Control 보고서를 사용하려면 보고서 패키지 파일을 BusinessObjects InfoView 로 가져와야 합니다.

참고: 이 절차는 동일한 패키지의 이전 버전이 이미 배포되지 않은 경우 보고서 포털에서 보고서 패키지를 배포하는 방법을 설명합니다.

다음 단계를 수행하십시오.

1. 중앙 데이터베이스, 배포 서버, 보고서 포털이 설정되었는지 확인합니다.

   참고: 보고서 포털 컴퓨터에서 JAVA_HOME 변수가 설정되었는지 확인합니다.

2. Windows 용 CA Business Intelligence DVD 를 광 디스크 드라이브에 넣고 \Disk1\cabi\biconfig 폴더로 이동합니다.
3. biconfig 디렉터리의 내용을 임시 디렉터리로 복사합니다.
4. 광학 디스크 드라이브에 사용하는 운영 체제용의 적절한 CA Access Control Premium Edition 서버 구성 요소 DVD 를 넣은 다음 \ReportPackages 폴더로 이동합니다.
5. 광학 디스크에서 동일한 임시 디렉터리로 다음 파일을 복사합니다.
   - \ReportPackages*RDBMS**import_biar_config*.xml
   - \ReportPackages*RDBMS**AC_BIAR_File*.biar

   RDBMS

   CA Access Control 보고에 사용되는 RDBMS 의 유형을 정의합니다.

   값: Oracle, MSSQL2005

***import_biar_config*.xml**

사용하는 RDBMS 에 대한 가져오기 구성 파일(.xml)의 이름을 정의합니다.

값: import_biar_config_oracle10g.xml, import_biar_config_oracle11g.xml, import_biar_config_mssql_2005.xml

참고: 중앙 데이터베이스로 MS SQL Server 2008 을 사용하는 경우 import_biar_config_mssql_2005.xml 파일을 구성하십시오.

***AC_BIAR_File*.biar**

해당 언어 및 RDBMS 의 CA Access Control 보고서 파일(.biar) 이름을 정의합니다.

참고: 사용하는 RDBMS 에 대한 가져오기 구성 파일의 <biar-file name> 속성은 이 파일을 가리킵니다. 이 속성은 기본적으로 사용하는 RDBMS 의 영어 버전 이름으로 설정되어 있습니다.

6. *import_biar_config*.xml 파일의 사본을 편집합니다. 다음 XML 속성을 정의합니다.

<biar-file name>

CA Access Control 보고서 파일(.biar)에 대한 전체 경로 이름을 정의합니다. 이전 단계에서 이 파일을 복사했습니다.

<networklayer>

사용하는 RDBMS 에서 지원하는 네트워크 계층을 정의합니다.

값(Windows):

- OLE DB - MS SQL Server 인증 모드에 사용
- Oracle OCI
- ODBC - Windows 인증 모드에 사용

<rdms>

CA Access Control 보고에 사용되는 RDBMS 의 유형을 정의합니다.

값(Oracle OCI): Oracle 10 또는 Oracle 11

값(ODBC): 일반 ODBC datasource

값(OLE DB): MS SQL Server 2005, 또는 Oracle 10 또는 Oracle 11 을 *제외*한 임의의 값

참고: MS SQL Server 2008 을 사용하는 경우 이 속성에 대해 MS SQL Server 2005 를 지정하십시오. 이 속성에 대해 지정할 수 있는 값에 대한 자세한 내용은 CA Business Intelligence 설명서를 참조하십시오.

<username>

엔터프라이즈 관리를 위한 중앙 데이터베이스를 준비할 때 만든 RDBMS 관리 사용자의 사용자 이름을 정의합니다.

<password>

엔터프라이즈 관리를 위한 중앙 데이터베이스를 준비할 때 만든 RDBMS 관리 사용자의 암호를 정의합니다.

<datasource>

다음 중 *하나*를 정의합니다.

- (Oracle) 데이터베이스의 이름입니다.
- (SQL Server 2005 또는 2008) 만든 데이터베이스입니다.
- (ODBC) 만든 DSN 입니다.

중요! CA Business Intelligence CMS 가 아니라 보고를 위해 CA Access Control 이 사용하는 데이터베이스의 이름을 지정하십시오.

<server>

SQL Server 2005 또는 2008 컴퓨터의 이름을 정의합니다. Oracle Database 10g, 11g 및 ODBC 에 대해 이 값을 비워두십시오.

7. 다음을 수행합니다.

- 명령 프롬프트를 열고 다음 명령을 입력합니다.

System_Drive:\BO\biconfig.bat -h *host_name* -u *user_name* -p *password* -f *ac_biar_config*.xml

host_name

보고서 포털 호스트 이름을 정의합니다.

user_name

보고서 포털을 설치할 때 구성한 보고서 포털 관리자를 정의합니다.

password

보고서 포털 관리자의 암호를 정의합니다.

예:

biconfig.bat -h reportportal.comp.com -u Administrator -p P@ssw0rd -f C:\BO\import_biar_config_oracle11g.xml

- (UNIX) 스크립트 파일 biconfig.sh 의 실행 권한을 설정하고 다음과 같이 실행합니다.

  temp_dir/biconfig.sh -h *host_name* -u *user_name* -p *password* -f *ac_biar_config*.xml

  예:

  biconfig.sh -h reportportal.comp.com -u Administrator -p P@ssw0rd -f /tmp/rp/import_biar_config_orcl.xml

배치 파일은 CA Access Control 보고서를 InfoView 로 가져옵니다. 가져오기 작업은 완료될 때까지 몇 분 정도 걸릴 수 있습니다. 배치 파일과 동일한 폴더에 작성된 로그 파일(biconfig.log)은 가져오기의 성공 여부를 나타냅니다.

예: 예제 Oracle Database 11g 가져오기 구성 파일

다음 코드 조각은 Oracle Database 11g 에 대한 편집된 가져오기 구성 파일(import_biar_config_oracle11g.xml)의 예제입니다.

```
<?xml version="1.0"?>
<biconfig version="1.0">
__<step priority="1">
____<add>
______<biar-file name="c:\temp\AccessControl_R12.5_EN_ORCL_22_JUN_2009.biar">
________<networklayer>Oracle OCI</networklayer>
________<rdms>Oracle 11</rdms>
________<username>root</username>
________<password>P@ssw0rd</password>
________<datasource>orcl</datasource>
________<server></server>
______</biar-file>
____</add>
__</step>
</biconfig>
```

예: 예제 Microsoft SQL Server 2005 가져오기 구성 파일

다음 코드 조각은 MS SQL Server 2005 에 대한 편집된 가져오기 구성 파일(import_biar_config_mssql2005.xml)의 예제입니다.

```
<?xml version="1.0"?>
<biconfig version="1.0">
__<step priority="1">
____<add>
______<biar-file name="c:\temp\AccessControl_R12.5_EN_SQL_11_JUN_2009.biar">
________<networklayer>OLE DB</networklayer>
________<rdms>MS SQL Server 2005</rdms>
________<username>dbAdmin</username>
________<password>P@ssw0rd</password>
________<datasource>r125db</datasource>
________<server>rdbms.org</server>
______</biar-file>
____</add>
__</step>
</biconfig>
```

추가 정보:

보고를 위해 UNIX 끝점 구성 (페이지 240)
보고를 위해 Windows 끝점 구성 (페이지 175)

대규모 배포를 위한 BusinessObjects 구성

대규모 배포에서 CA Access Control 보고서를 실행하려면 BusinessObjects 기본 구성을 변경해야 합니다. BusinessObjects 페이지 서버에서 허용되는 최대 동시 연결 수(기본값: 20,000)를 변경할 수 있습니다. 또한 입력 매개 변수 선택 목록에 표시된 값의 최대 수를 변경합니다.

대규모 배포를 위해 BusinessObjects 를 구성하려면

1. BusinessObjects 페이지 서버가 연결할 수 있는 동시 연결 수를 변경합니다.
   a. 보고서 포털 컴퓨터에서 "시작", "프로그램", "Crystal Enterprise", "Crystal Configuration Manager"를 클릭합니다.

      BusinessObjects 구성 매니저가 열립니다.

   b. Crystal 페이지 서버를 마우스 오른쪽 버튼으로 클릭한 다음 "중지"를 선택합니다.

c. Crystal 페이지 서버를 마우스 오른쪽 버튼으로 클릭한 다음 "속성"을 선택합니다.

d. "실행 파일" 경로 필드의 *-restart* 뒤에 다음 텍스트가 표시되는지 확인합니다.

-maxDBResultRecords 0

e. BusinessObjects 페이지 서버를 다시 시작합니다.

2. 보고서의 입력 매개 변수 선택 목록에 표시된 값의 최대 수를 변경합니다.

a. Windows 레지스트리 편집기를 엽니다.

b. 다음 레지스트리 키를 탐색합니다.

HKEY_CURRENT_USER/Software/Business Objects/Suite 11.5/Crystal Reports/Database

c. "편집", "새로 만들기", "DWORD 값"을 클릭합니다.

REG_DWORD 유형의 새 레지스트리 항목이 나타납니다.

d. 항목의 이름을 *QPMaxLOVSize* 로 지정합니다.

e. 항목을 두 번 클릭하고 그 값의 데이터를 1000 으로 편집합니다.

새 레지스트리 항목이 설정됩니다.

f. BusinessObjects CMC(Central Management Console-중앙 관리 콘솔)를 엽니다.

g. 서버 관리 영역으로 이동합니다.

h. 설정을 변경할 웹 인텔리전스 보고서 서버를 클릭합니다.

"웹 인텔리전스 보고서 서버" 페이지가 "속성" 탭에 열립니다.

i. 다음 값을 1000 이상 또는 요구된 값으로 수정합니다.

- 값 배치 크기 목록
- 사용자 지정 정렬 값의 최대 목록 크기

변경 내용을 제출하려면 "적용"을 클릭하고 변경 내용의 효력이 즉시 발생할 수 있도록 서버를 다시 시작합니다.

CA Business Intelligence 에 대한 연결 구성

CA Access Control 엔터프라이즈 관리는 CA Business Intelligence 공용 보고 서버(CA Access Control 보고서 포털)을 통해 보고 기능을 제공합니다. 보고서 포털을 설치하고 보고서를 배포한 다음에는 CA Access Control 엔터프라이즈 관리에서 CA Business Intelligence 로의 연결을 구성해야 합니다. 이 연결을 구성하려면 CA Identity Manager 관리 콘솔을 사용합니다.

CA Business Intelligence 에 대한 연결을 구성하려면

1. CA Identity Manager 관리 콘솔을 활성화합니다 (페이지 88).
2. CA Identity Manager 관리 콘솔을 엽니다 (페이지 88).
3. "환경", "AC 환경", "고급 설정", "보고서"를 차례로 클릭합니다.

   "보고서 속성" 창이 나타납니다.
4. 데이터베이스 및 Business Objects 속성을 입력합니다.

   중요! CA Business Intelligence 중앙 관리 서버(CMS)는 내부 관리 용도로만 사용되며 보고서를 생성 및 표시하는 데 사용되는 보고서 데이터를 포함하지 않습니다. CMS 에 대한 자세한 내용은 *CA Business Intelligence 설치 안내서*를 참조하십시오.

   참고: 자세한 내용은 제품에 포함된 *CA Identity Manager 관리 콘솔 온라인 도움말*을 참조하십시오.

   중요! "Business Objects 포트" 필드에서 보고서 포털이 사용하는 포트 번호를 입력하십시오. 기본 포트는 8080 입니다. "Business Objects 보고서 폴더" 필드에 "CA Access Control r12"를 입력합니다.
5. "저장"을 클릭합니다.

   CA Business Intelligence 설정이 저장됩니다.

참고: CA Business Intelligence 에 대한 자세한 내용은 CA Technologies Support에 있는 *CA Business Intelligence 설치 안내서*를 참조하십시오.

스냅숏 정의 만들기

보고서는 CA Access Control 및 UNAB 끝점에서 수집하여 중앙 데이터베이스에 저장된 데이터 스냅숏, CA Access Control 엔터프라이즈 관리의 PUPM 데이터, 사용자 저장소의 데이터에 기반합니다.

CA Access Control 보고서를 실행하고 보려면 먼저 스냅숏 정의를 만들고 스냅숏 데이터를 캡처합니다. 스냅숏 정의는 CA Access Control 이 수집하는 보고서 데이터와 데이터 수집을 위한 일정을 지정합니다.

스냅숏 매개 변수 XML 파일은 CA Access Control 이 수집하는 보고서 데이터를 지정합니다. 기본적으로 이 파일은 모든 CA Access Control 및 UNAB 끝점, PUPM 데이터, 보고서 스냅숏의 사용자 저장소에 있는 데이터를 포함하도록 지정합니다. 보고서 스냅숏의 범위를 제한하도록 스냅숏 매개 변수 XML 파일을 사용자 지정할 수 있습니다.

보고서에 가장 최신 데이터가 수록되도록 끝점 스냅숏보다 더 자주 스냅숏이 실행되도록 예약하지 마십시오. 예를 들어, 끝점이 매주 스냅숏을 보내도록 구성하고 CA Access Control 엔터프라이즈 관리가 매일 스냅숏을 캡처하도록 구성하면 보고서 데이터가 끝점에서는 매주 수집되지만 PUPM 및 사용자 저장소에서는 매일 수집되어 보고서에 오래된 끝점 데이터가 표시됩니다.

중요! 여러 스냅숏 정의를 활성화하지 마십시오. 여러 스냅숏 정의가 활성화된 경우 CA Access Control 엔터프라이즈 관리는 모든 보고서를 성공적으로 실행할 수 없습니다.

참고: 기본적으로 스냅숏 정의를 만들려면 시스템 관리자 역할이 있어야 합니다.

스냅숏 정의를 만들려면

1. CA Access Control 엔터프라이즈 관리에서 다음을 수행합니다.
   a. "보고서"를 클릭합니다.
   b. "작업" 하위 탭을 클릭합니다.
   c. 작업 메뉴에서 왼쪽에 있는 "스냅숏 정의 관리" 트리를 확장합니다.

      사용할 수 있는 작업 목록에 "스냅숏 정의 만들기" 작업이 나타납니다.
2. "스냅샷 정의 만들기"를 클릭합니다.

   "스냅숏 정의 만들기: 스냅숏 정의 선택" 페이지가 나타납니다.

3. "확인"을 클릭합니다.

   "스냅숏 정의 만들기" 페이지가 나타납니다.

4. "프로필" 탭에서 다음 필드를 완성합니다.

   스냅숏 정의 이름

   스냅숏 정의의 이름을 정의합니다.

   스냅숏 정의 설명

   스냅숏 정의를 설명하는 추가 정보를 지정합니다.

   사용

   CA Access Control 엔터프라이즈 관리가 스냅숏 정의를 활성화하도록 지정합니다.

   참고: 이 확인란을 선택하지 않으면 CA Access Control 엔터프라이즈 관리가 스냅숏을 캡처하지 않으며 보고서가 표시되지 않습니다. 스냅숏은 한 번에 하나씩만 활성화할 수 있습니다.

   식별자

   보고서 스냅숏의 범위를 정의하는 스냅숏 매개 변수 XML 파일을 지정합니다.

   기본값: PPM_ALL.xml

   마지막 유지

   중앙 데이터베이스에 저장된 성공한 스냅숏의 수를 지정합니다. CA Access Control 은 데이터베이스에 있는 스냅숏의 수가 지정된 수에 도달하면 오래된 스냅숏을 삭제합니다.

   참고: 스냅숏 수는 0 보다 커야 합니다. 이 필드의 값을 지정하지 않으면 CA Access Control 은 스냅숏을 무제한 저장합니다. 최대 3 개의 성공한 스냅숏을 저장하는 것이 좋습니다.

5. "되풀이" 탭을 클릭하고 "일정"을 선택합니다.

   일정 옵션이 나타납니다.

6. 스냅숏 실행 시간 및 되풀이 패턴을 지정하고 "제출"을 클릭합니다.

   참고: CA Access Control 및 UNAB 끝점의 스냅숏보다 덜 자주 스냅숏이 실행되도록 예약하는 것이 좋습니다.

   CA Access Control 은 예정된 시간 및 빈도로 스냅숏을 캡처하도록 구성되었습니다.

참고: 스냅숏 정의를 만든 이후에 필요할 때 스냅숏을 캡처하거나 예약된 시간 및 빈도로 스냅숏을 캡처하도록 선택할 수 있습니다. 스냅숏 데이터 캡처에 대한 자세한 내용은 *엔터프라이즈 관리 안내서*를 참조하십시오.

보고서 스냅숏의 범위 제한

CA Access Control 엔터프라이즈 관리가 보고서 스냅숏을 캡처할 때는 CA Access Control 및 UNAB 끝점의 스냅숏에서 데이터를 수집하고, CA Access Control 엔터프라이즈 관리에서 PUPM 데이터를 수집하고, 사용자 저장소에서 데이터를 수집합니다. CA Access Control 엔터프라이즈 관리가 보고서 데이터를 수집한 다음에는 이 데이터를 중앙 데이터베이스에 저장합니다.

스냅숏 매개 변수 XML 파일은 CA Access Control 엔터프라이즈 관리이 수집하는 보고서 데이터를 지정합니다. 스냅숏 매개 변수 XML 파일을 사용자 지정하여 보고서 스냅숏의 범위를 제한할 수 있습니다.

예를 들어, 사용자 저장소로 Active Directory 를 사용하는 경우, CA Access Control 엔터프라이즈 관리는 보고서 스냅숏을 캡처할 때 모든 Active Directory 사용자에 대한 데이터를 수집합니다. 이 작업은 완료하는 데 시간이 오래 걸릴 수 있습니다. 스냅숏을 캡처하는 데 걸리는 시간을 줄이려면 스냅숏 매개 변수 XML 파일을 사용자 지정하여 Active Directory 스냅숏의 범위를 제한할 수 있습니다.

보고서 스냅숏의 범위를 제한하려면

1. 다음 디렉터리로 이동합니다. 여기서 *JBOSS_HOME* 은 JBoss 를 설치한 디렉터리를 나타냅니다.

   JBOSS_HOME/server/default/deploy/IdentityMinder.ear/config/com/netegrity/config/imrexport/sample

2. PPM_ALL.xml 파일을 복사하고, 새 파일의 이름을 변경하고, 파일을 동일한 디렉터리에 저장합니다.

   새 스냅숏 매개 변수 XML 파일을 만들었습니다.

3. 편집 가능한 형식으로 새 스냅숏 매개 변수 XML 파일을 엽니다.

4. <!--IM COLLECTORS--> 섹션의 항목을 편집하여 CA Access Control 엔터프라이즈 관리가 사용자 저장소에서 수집하는 데이터의 범위를 지정합니다.

5. 보고서 스냅숏에 포함하고 싶지 않은 CA Access Control 엔터프라이즈 관리 구성 요소에 해당하는 <!--PUPM COLLECTORS--> 섹션의 항목을 주석 처리(!-- 및 --)합니다.

6. (선택 사항) Active Directory 스냅숏의 범위를 제한합니다.

   a. LDAP 쿼리가 보고서 스냅숏을 제한하는 방법 (페이지 122)과 LDAP 구문 고려 사항 (페이지 123) 항목을 검토합니다.

      이 항목의 정보는 다음 단계를 통해 올바른 LDAP 쿼리를 정의하는 데 도움을 줍니다.

   b. <!--PUPM COLLECTORS--> 섹션에서 다음 요소를 찾습니다.

      ```
      <export object="com.ca.ppm.export.ADUsersCollector">
      </export>
      ```

      이 요소는 스냅숏에 포함된 Active Directory 사용자 데이터를 지정합니다.

   c. 다음과 같이 보이도록 이 요소를 편집합니다. 여기서 *ldap_query* 는 데이터가 수집된 대상 사용자를 정의하는 LDAP 쿼리를 지정합니다.

      ```
      <export object="com.ca.ppm.export.ADUsersCollector">
              <where attr="%USER" satisfy="ANY">
                      <value op="EQUALS">(ldap_query)</value>
              </where>
      </export>
      ```

   d. <!--PUPM COLLECTORS--> 섹션에서 다음 요소를 찾습니다.

      ```
      <export object="com.ca.ppm.export.ADGroupsCollector">
      </export>
      ```

e. 다음과 같이 보이도록 이 요소를 편집합니다. 여기서 *ldap_query* 는 데이터가 수집된 대상 그룹을 정의하는 LDAP 쿼리를 지정합니다.

```
<export object="com.ca.ppm.export.ADGroupsCollector">
        <where attr="%USER" satisfy="ANY">
                <value op="EQUALS">(ldap_query)</value>
        </where>
</export>
```

Active Directory 스냅숏의 범위를 제한했습니다.

7. 새 스냅숏 매개 변수 XML 파일을 저장하고 닫습니다.
8. 새 스냅숏 매개 변수 XML 파일을 사용하도록 CA Access Control 엔터프라이즈 관리에서 스냅숏 정의를 수정합니다.

캡처 스냅숏 작업이 실행되면 이 작업은 스냅숏 매개 변수 XML 파일에 지정한 데이터만 수집합니다.

예: 보고서 스냅숏의 범위를 CA Access Control 끝점으로 제한

PUPM 과 UNAB 를 사용하지 않는 경우 CA Access Control 끝점에서만 데이터를 수집하도록 보고서 스냅숏의 범위를 제한할 수 있습니다. 데이터 수집의 범위를 CA Access Control 끝점으로 제한하려면 <-- PUPM COLLECTORS --> 섹션 아래에서 ReportIdMarkerCollector 항목을 *제외*한 모든 항목을 주석 처리(!-- 및 --)하십시오.

다음은 ReportIdMarkerCollector 항목을 제외하고 <-- PUPM COLLECTORS --> 섹션 아래의 모든 항목을 주석 처리하도록 수정된 이후의 PPM_ALL.xml 파일의 코드 조각입니다.

```
<!-- PUPM COLLECTORS -->
        <!-- export object="com.ca.ppm.export.AccountPasswordCollector">
        </export -->

        <!-- export object="com.ca.ppm.export.PPMRolesCollector">
                <exportattr attr="|rolemembers|" />
        </export -->

        <!-- export object="com.ca.ppm.export.
                PrivilegedAccountExceptionCollector">
        </export -->

        <!-- export object="com.ca.ppm.export.PPMPasswordPolicyCollector">
        </export -->

        <!-- export object="com.ca.ppm.export.ADUsersCollector">
        </export -->

        <export object="com.ca.ppm.export.PPMAccountUserAccessCollector">
        </export --!>

        <!-- export object="com.ca.ppm.export.ADGroupsCollector">
                <exportattr attr="|groupmembers|" />
        </export -->

        <export object="com.ca.ppm.export.ReportIdMarkerCollector">
        </export>
```

스냅숏 매개 변수 XML 파일 구문 - 보고서 스냅숏 제한

스냅숏 매개 변수 XML 파일은 CA Access Control 엔터프라이즈 관리가 수집하는 보고서 데이터를 지정합니다. 스냅숏 매개 변수 XML 파일을 편집하여 보고서 스냅숏의 범위를 제한할 수 있습니다.

CA Access Control 엔터프라이즈 관리는 스냅숏 매개 변수 XML 파일에 정의하는 조건을 충족하는 개체에 대해서만 보고서 데이터를 수집합니다. 파일의 각 수집기는 CA Access Control 엔터프라이즈 관리가 수집하는 여러 개체를 정의합니다.

각 수집기는 다음과 같은 구조를 갖습니다.

```
<export object=" ">
        <where attr=" " satisfy=" ">
                <value> </value>
        </where>
        <exportattr attr=" " />
</export>
```

참고: <where>, <value>, <exportattr> 요소는 선택 사항입니다.

각 수집기는 다음 요소를 포함하고 있습니다.

<export>

CA Access Control 엔터프라이즈 관리가 수집하는 개체 데이터를 나타냅니다. 예를 들어, <export> 요소는 CA Access Control 엔터프라이즈 관리가 사용자 데이터를 수집하도록 지정할 수 있습니다.

<export> 요소는 하나 이상의 <exportattr> 및 <where> 요소를 포함할 수 있으며, 이 요소를 사용하여 특정 조건을 충족하는 데이터만 수집할 수 있습니다. <exportattr> 또는 <where> 요소를 지정하지 않으면 CA Access Control 엔터프라이즈 관리는 개체에 대한 모든 데이터를 수집합니다.

<export> 요소는 개체 매개 변수만 가집니다.

<where>

<value> 요소에 의해 정의된 조건을 기준으로 수집된 데이터를 필터링합니다. <where> 요소는 하나 이상의 <value> 요소를 포함해야 합니다. 또한 필터를 구체화하기 위해 여러 개의 <where> 요소(OR 요소로 작동)를 지정할 수 있습니다.

다음 표에서는 <where> 요소에 대한 매개 변수를 설명합니다.

매개 변수	설명
attr	필터에서 사용할 특성을 나타냅니다.
satisfy	개체 또는 특성을 수집하기 위해 일부 또는 모든 값 평가를 충족해야 하는지 나타냅니다. ■ ALL - 특성 또는 개체가 모든 값 평가를 충족해야 합니다. ■ ANY - 특성 또는 개체가 하나 이상의 값 평가를 충족해야 합니다.

<value>

<where> 요소에서 특성 또는 개체를 수집하기 위해 충족해야 하는 조건을 정의합니다. <value> 요소에는 연산자(op) 매개 변수가 필요합니다. 연산자는 EQUALS 또는 CONTAINS 일 수 있습니다.

참고: 스냅숏 매개 변수 XML 파일의 <!--PUPM COLLECTORS--> 섹션에서 <value> 요소에 LDAP 구문을 사용할 수 있습니다. LDAP 구문은 Active Directory 에서 CA Access Control 엔터프라이즈 관리가 수집하는 사용자 및 그룹 데이터를 지정할 수 있게 해 줍니다.

<exportattr>

수집할 특정 특성을 나타냅니다. 수집하는 개체에 대한 하위 특성을 수집하려면 <exportattr> 요소를 사용하십시오. 예를 들어, <exportattr> 요소를 사용하여 사용자의 ID 만 수집할 수 있습니다.

<exportattr> 요소는 attr 매개 변수를 갖습니다.

다음 표에서는 <where> 요소 또는 <exportattr> 요소에서 개체가 사용할 수 있는 특성을 표시합니다.

개체	<where> 요소에서 사용할 수 있는 특성	<exportattr> 요소에서 사용할 수 있는 특성
role	이름 특성으로 필터링할 수 있습니다. name - 필터를 충족하는 이름의 역할	다음 특성을 수집할 수 있습니다. ■ |tasks| - 역할과 관련된 모든 태스크 ■ |rules| - 역할에 적용되는 모든 구성원, 관리자, 소유자 및 범위 규칙 ■ |users| - 역할의 모든 구성원, 관리자 및 소유자 ■ |rolemembers| - 모든 역할 구성원 ■ |roleadmins| - 모든 역할 관리자 ■ |roleowners| - 모든 역할 소유자
사용자	잘 알려진 특성 또는 물리적 특성 및 다음 특성: ■ |groups| - 그룹의 구성원 ■ |roles| - 역할의 구성원 ■ |orgs| - 필터를 충족하는 조직에 프로필이 있는 사용자	다음 특성을 수집할 수 있습니다. ■ |all_attributes| - 사용 가능한 모든 사용자 특성 ■ |groups| - 사용자가 구성원 또는 관리자로 있는 모든 그룹 ■ |roles| - 사용자가 구성원, 관리자 또는 소유자로 있는 모든 역할

개체	<where> 요소에서 사용할 수 있는 특성	<exportattr> 요소에서 사용할 수 있는 특성
그룹	잘 알려진 특성 또는 물리적 특성 또는 다음 특성: |groups| - 필터를 충족하는 그룹 내 중첩된 그룹 목록	잘 알려진 특성 또는 물리적 특성 또는 다음 특성을 수집할 수 있습니다. ■ |all_attributes| - 디렉터리 구성 파일(directory.xml)에 그룹 개체에 대해 정의된 모든 특성 ■ |groups| - 그룹 내 중첩된 모든 그룹 ■ |users| - 그룹의 모든 구성원 ■ |groupadmins| - 지정된 그룹의 관리자인 모든 사용자 ■ |groupmembers| - 지정된 그룹의 구성원인 모든 사용자 ■ |users| - 모든 그룹 관리자 및 구성원
organization	잘 알려진 특성 또는 물리적 특성	잘 알려진 특성 또는 물리적 특성 또는 다음 특성을 수집할 수 있습니다. ■ |all_attributes| - 디렉터리 구성 파일(directory.xml)에 조직 개체에 대해 정의된 모든 특성 ■ |orgs| - 조직 내 중첩된 모든 조직 ■ |groups| - 조직의 모든 그룹 ■ |users| - 조직의 모든 사용자

LDAP 쿼리가 보고서 스냅숏에서 사용자 및 그룹 데이터를 제한하는 방법

사용자 저장소로 Active Directory 를 사용하는 경우 보고서 스냅숏에 캡처된 사용자 및 그룹 데이터를 지정할 수 있습니다.

사용자 및 그룹으로 Active Directory 데이터를 필터링하는 LDAP 쿼리를 스냅숏 매개 변수 XML 파일에서 사용할 수 있습니다. 하지만 역할 구성원 자격으로 Active Directory 데이터를 필터링하는 LDAP 쿼리를 사용할 수는 없습니다. LDAP 쿼리는 스냅숏 매개 변수 XML 파일의 <!--PUPM COLLECTORS--> 섹션에서만 사용할 수 있습니다.

다음 프로세스는 스냅숏 매개 변수 XML 파일의 LDAP 쿼리가 CA Access Control 엔터프라이즈 관리가 수집하는 Active Directory 데이터를 제한하는 방법을 설명합니다. 이 정보는 보고서 스냅숏을 제한하기 위해 올바른 LDAP 쿼리를 작성하는 데 도움을 줍니다.

CA Access Control 엔터프라이즈 관리가 Active Directory 보고서 스냅숏을 캡처할 때는 다음을 수행합니다.

1. 다음 요소 내에서 LDAP 쿼리에 지정된 Active Directory 사용자에 대해서만 데이터를 수집합니다.

   <export object="com.ca.ppm.export.ADUsersCollector">

   요소에 LDAP 쿼리가 없으면 CA Access Control 엔터프라이즈 관리는 스냅숏에 모든 Active Directory 사용자에 대한 데이터를 포함합니다.

2. 다음 요소 내에서 LDAP 쿼리에 지정된 Active Directory 그룹에 대해서만 데이터를 수집합니다.

   <export object="com.ca.ppm.export.ADGroupsCollector">

   요소에 LDAP 쿼리가 없으면 CA Access Control 엔터프라이즈 관리는 스냅숏에 모든 Active Directory 그룹에 대한 데이터를 포함합니다.

   참고: CA Access Control 엔터프라이즈 관리는 1 단계에서 쿼리에 의해 반환되지 않은 모든 사용자에 대해 데이터를 수집하지 않습니다. 사용자가 2 단계에서 쿼리에 의해 반환된 그룹의 구성원이지만 사용자가 1 단계에서 쿼리에 의해 반환되지 않았으면 CA Access Control 엔터프라이즈 관리는 Active Directory 스냅숏에 사용자에 대한 어떠한 데이터도 포함하지 않습니다.

LDAP 구문 고려 사항

Active Directory 스냅숏의 범위를 제한하기 위해 LDAP 쿼리를 작성할 때는 다음 사항을 고려하십시오.

- LDAP 쿼리에 다음과 같은 논리 연산자를 사용할 수 있습니다.
  - EQUAL TO (=)
  - OR (|)
  - AND (&)

    참고: 앰퍼샌드(&) 문자의 사용에는 일부 제한이 적용됩니다.
  - NOT (!)
  - 와일드카드(*)
- 앰퍼샌드(&) 문자 및 왼쪽 꺾쇠 괄호 문자(<)는 다음 구문에서만 사용할 수 있습니다.
  - 태그 구분 기호로 사용
  - 주석 내에서 사용
  - 프로세싱 지침 내에서 사용
  - CDATA 섹션 내에서 사용

다른 구문에서 앰퍼샌드 문자를 나타내려면 문자열 **&** 또는 유니코드 문자 참조를 사용하십시오. 다른 구문에서 왼쪽 꺾쇠 괄호 문자를 나타내려면 문자열 **<** 또는 유니코드 문자 참조를 사용하십시오.

- 오른쪽 꺾쇠 괄호 문자(>)는 CDATA 섹션( ]]>)의 끝을 표시하는 문자열 뒤에만 사용할 수 있습니다.

  다른 구문에서 오른쪽 꺾쇠 괄호 문자를 나타내려면 문자열 **>** 또는 유니코드 문자 참조를 사용하십시오.

예: 앰퍼샌드 문자

스냅숏 매개 변수 XML 파일의 다음 코드 조각은 보고서 스냅숏에 모든 Active Directory 사용자 데이터를 포함하도록 지정합니다. 스냅숏의 LDAP 쿼리는 & 문자열을 사용하여 앰퍼샌드를 나타냅니다.

```
<export object ="com.ca.ppm.export.ADUsersCollector">
        <where attr="%USER%" satisfy="ANY">
                <value op="EQUALS">(&amp;(objectClass=user))</value>
        </where>
</export>
```

CA Access Control r12.0 에서 설치된 보고서 포털에 보고서 패키지 배포

Windows 에 해당

이러한 표준 CA Access Control 보고서를 사용하려면 보고서 패키지 파일을 BusinessObjects InfoView 로 가져와야 합니다.

이 절차는 CA Access Control r12.0 을 설치할 때 함께 설치된 기존 CA Business Intelligence 에서 보고서 패키지를 배포하는 방법을 설명합니다.

다음 단계를 수행하십시오.

1. 광학 디스크 드라이브에 사용하는 운영 체제용의 적절한 CA Access Control Premium Edition 서버 구성 요소 DVD 를 넣은 다음 /ReportPackages 디렉터리로 이동합니다.
2. 설치 파일용 임시 폴더를 만듭니다.
   - Windows 에서는 루트 C:\ 드라이브 아래에 폴더 'BO'를 만듭니다.

     참고: 이 폴더에는 약 2 GB 의 메모리가 필요합니다.
   - Linux 에서는 /work/bo 디렉터리를 작성합니다.

3. 광학 디스크 드라이브에서 동일한 임시 디렉터리로 다음 파일을 복사합니다.
   - /ReportPackages/*RDBMS/import_biar_config*.xml
   - /ReportPackages/*RDBMS/AC_BIAR_File*.biar

   RDBMS

   사용하는 RDBMS 의 유형을 정의합니다.

   값: Oracle, MSSQL2005

   ***import_biar_config*.xml**

   사용하는 RDBMS 에 대한 가져오기 구성 파일(.xml)의 이름을 정의합니다.

   값: import_biar_config_oracle10g.xml, import_biar_config_oracle11g.xml, import_biar_config_mssql_2005.xml

   참고: 중앙 데이터베이스로 MS SQL Server 2008 을 사용하는 경우 import_biar_config_mssql_2005.xml 파일을 구성하십시오.

   ***AC_BIAR_File*.biar**

   해당 언어 및 RDBMS 의 CA Access Control 보고서 파일(.biar) 이름을 정의합니다.

   참고: 사용하는 RDBMS 에 대한 가져오기 구성 파일의 <biar-file name> 속성은 이 파일을 가리킵니다. 이 속성은 기본적으로 사용하는 RDBMS 의 영어 버전 이름으로 설정되어 있습니다.

4. 해당 플랫폼의 CA Access Control Premium Edition r12.0 서버 구성 요소 DVD 를 광 디스크 드라이브에 넣고 /ReportPortal 디렉터리로 이동합니다.

   참고: 이 DVD 는 r12.0 과 함께 제공된 미디어에 포함되어 있습니다.

5. 다음 단계 중 하나를 완료합니다.
   - Windows 에서는 DVD 의 \ReportPortal\BO 디렉터리에 있는 내용을 만든 C:\BO 폴더로 복사합니다.
   - Linux 에서는 /ReportPortal/bo_install.tar.gz 를 만든 /work/bo 폴더로 압축 해제합니다.

6. DVD 의 \ReportPortal\BO 디렉터리에 있는 내용을 만든 C:\BO 폴더로 복사합니다.

7. 대상 디렉터리를 열고 *BO_files*/biek-sdk 로 이동합니다.
8. biekInstall.properties 파일의 사본을 다음과 같이 편집합니다.

BIEK_CONNECT_LAYER=*networklayer*
BIEK_CONNECT_DB=*rdms*
BIEK_CONNECT_USER=*rdbms_adminUserName*
BIEK_CONNECT_PASSWORD=rdbms_*adminUserPass*
BIEK_CONNECT_SOURCE=*rdbms_Datasource*
BIEK_CONNECT_SERVER=*rdbms_hostName*
BIEK_BO_USER=*InfoView_adminUserName*
BIEK_BO_PASSWORD=*InfoView_adminUserPass*
BIEK_BIAR_FILE=*AC_BIAR_File*.biar

networklayer

사용하는 RDBMS 에서 지원하는 네트워크 계층을 정의합니다.

제한: 대소문자 구분

rdms

사용하는 RDBMS 의 유형을 정의합니다.

제한: 대소문자 구분

rdbms_adminUserName

만든 RDBMS 관리 사용자의 사용자 이름을 정의합니다.

rdbms_adminUserPass

만든 RDBMS 관리 사용자의 암호를 정의합니다.

rdbms_Datasource

Oracle 데이터베이스의 TNS(Transparent Network Substrate) 이름을 정의합니다.

rdbms_hostName

RDBMS 서버의 호스트 이름을 정의합니다.

InfoView_adminUserName

InfoView 관리 사용자의 사용자 이름을 정의합니다. 기본적으로 이 사용자는 *관리자*입니다.

InfoView_adminUserPass

InfoView 관리 사용자의 암호를 정의합니다. 이 사용자는 기본적으로 암호가 없습니다(비워 둠).

***AC_BIAR_File*.biar**

CA Access Control 보고서 파일(.biar)에 대한 전체 경로 이름을 정의합니다. 이 파일은 앞에서 복사한 파일입니다.

9. *BO_Files*/biek-sdk/importBiarFile.bat 배치 파일을 시작합니다.

   이 파일은 CA Access Control 보고서를 InfoView 로 가져옵니다. 가져오기 작업은 완료될 때까지 몇 분 정도 걸릴 수 있습니다.

제 6 장: 끝점 구현 준비

이 섹션은 다음 항목을 포함하고 있습니다.

보호할 정책 개체 결정

다음 절에서는 엔터프라이즈 응용 프로그램과 데이터에 대한 액세스 권한을 부여하기 위해 보안 정책에서 사용할 수 있는 몇 가지 주요 개체에 대해 설명합니다.

사용자

CA Access Control 에는 여러 유형의 사용자가 있으며, 각 유형의 사용자는 일정 수준의 권한과 제한을 가지고 있습니다. 조직의 보안 정책을 개발하는 과정 중에 어떤 특수 권한을 누구에게 부여할지 결정합니다.

CA Access Control 에는 사용자 로그인 허용 횟수, 사용자에게 수행할 감사 유형 등과 같은 사용자 관련 정보가 저장됩니다. 사용자 관련 정보는 데이터베이스 레코드의 속성에 저장됩니다.

참고: 사용자에 대한 자세한 내용은 *끝점 관리 안내서*를 참조하십시오.

사용자 유형

CA Access Control 은 CA Access Control 데이터베이스에서 리소스를 관리하는 데 사용되는 다음과 같은 사용자 유형을 지원합니다.

일반 사용자

조직의 업무를 수행하는 사람들, 즉 조직의 내부 최종 사용자입니다. 네이티브 OS 및 CA Access Control 에서 시스템에 대한 일반 사용자의 액세스를 제한할 수 있습니다.

특수 권한이 있는 사용자(하위 관리자)

하나 이상의 특수 관리 작업을 수행할 수 있는 권한이 부여된 일반 사용자입니다. 특수 관리 기능을 수행할 수 있는 권한이 일반 사용자에게 부여되면 관리자의 업무 부하가 줄어듭니다. CA Access Control 에서는 이를 작업 위임이라고 합니다.

관리자

네이티브 OS 와 CA Access Control 에서 가장 많은 권한을 갖는 사용자입니다. 관리자는 사용자를 추가, 삭제 및 업데이트할 수 있으며 대부분의 관리 작업을 수행할 수 있습니다. CA Access Control 에서는 네이티브 슈퍼 사용자의 권한을 제한할 수 있습니다. 관리 작업을 계정이 자동으로 알려지지 않은 특정 사용자에게 할당할 수 있습니다. 이렇게 하면 침입자가 어떤 사용자가 관리 작업을 수행하는지 쉽게 알 수 없습니다.

그룹 관리자

하나의 특정 그룹 내에서 사용자 추가, 삭제 및 업데이트와 같은 대부분의 관리 기능을 수행할 수 있는 사용자입니다. 네이티브 Windows 에는 권한이 제한되는 이런 유형의 사용자가 없습니다.

암호 관리자

다른 사용자의 암호를 변경할 수 있는 권한을 가진 사용자입니다. 암호 관리자는 다른 사용자 특성을 변경할 수 없습니다. 네이티브 OS 에는 이런 유형의 사용자가 없습니다.

그룹 암호 관리자

하나의 특정 그룹 내 다른 사용자의 암호를 변경할 수 있는 권한을 가진 사용자입니다. 그룹 암호 관리자는 그룹 내 사용자의 다른 사용자 특성을 변경할 수 없습니다. 네이티브 OS 에는 이런 유형의 사용자가 없습니다.

감사자

감사 로그를 읽을 수 있는 권한을 가진 사용자입니다. 또한 각 로그인과 각 리소스 액세스 시도에 대해 수행되는 감사 종류를 결정합니다. 네이티브 OS 에는 이런 유형의 사용자가 없습니다.

그룹 감사자

그룹에 관련된 감사 로그를 읽을 수 있는 사용자로, 특정 그룹 내에서 수행되는 감사 종류를 결정할 수 있는 권한도 가집니다. 네이티브 OS 에는 이런 유형의 사용자가 없습니다.

운영자

데이터베이스의 모든 정보를 표시(읽기)하고, CA Access Control 을 종료하고, secons 유틸리티를 사용하여 CA Access Control 추적을 관리하고 런타임 통계를 표시하는 등의 작업을 수행할 수 있는 사용자입니다. 네이티브 OS 에는 이런 유형의 사용자가 없습니다.

참고: secons 유틸리티에 대한 자세한 내용은 *참조 안내서*를 참조하십시오.

그룹 운영자

사용자가 정의된 그룹의 데이터베이스에 있는 모든 정보를 표시할 수 있는 사용자입니다. 네이티브 OS 에는 이런 유형의 사용자가 없습니다.

서버

다른 사용자에 대한 권한 부여를 요청할 수 있는 특별한 유형의 사용자로, 실제로는 프로세스입니다.

보안 정책 및 사용자

구현을 준비할 때 다음 사항을 결정해야 합니다.

- 정의된 사용자에게 부여할 특수 권한
- 정의된 사용자에게 부여할 전역 권한 부여 및 그룹 권한 부여 특성

  예를 들어, 시스템 관리자, 암호 관리자, 그룹 암호 관리자, 감사자, 운영자로 정의할 사람을 결정해야 합니다.

그룹

그룹은 동일한 액세스 권한을 일반적으로 공유하는 사용자 집합입니다. 관리자는 그룹에 사용자를 추가하고 그룹에서 사용자를 제거하며 그룹별 시스템 리소스에 대한 액세스를 할당하거나 거부할 수 있습니다. 이런 유형의 그룹은 네이티브 OS 및 CA Access Control 에 모두 존재합니다.

그룹 레코드에는 그룹에 대한 정보가 포함됩니다. 그룹에 저장된 가장 중요한 정보는 그룹 구성원인 사용자 목록입니다.

중요! 그룹 레코드에 대한 권한 부여 규칙은 그룹 계층의 각 사용자에게 반복적으로 적용됩니다.

예를 들어, 그룹 A 에 사용자 X 및 그룹 B 의 두 구성원이 있습니다. 사용자 Y 는 그룹 B 의 구성원입니다. 그룹 A 의 권한 부여 규칙을 변경하면 CA Access Control 은 변경된 권한 부여 규칙을 그룹 A 계층에 있는 모든 사용자와 그룹(즉, 사용자 X, 그룹 B, 사용자 Y)에 적용합니다.

그룹 레코드의 정보는 *속성*에 저장되고,

CA Access Control 에서 그룹 관리자는 자신이 그룹 관리자로 정의된 특정 그룹에 대해 그룹 기능을 관리할 수 있습니다. 그룹 암호 관리자는 그룹 구성원의 암호를 변경할 수 있습니다.

보안 정책 및 그룹

사용자 조직에 대한 보안 정책을 개발할 때에는 다음 사항을 결정해야 합니다.

- 보안 관리 용도로 만들 그룹
- 각 그룹에 조인할 사용자
- 그룹 관리자 및 그룹 암호 관리자 정의 여부, 관리자 역할을 부여할 사용자(정의할 경우)

미리 정의된 사용자 그룹

CA Access Control 에는 사용자가 조인할 수 있는 미리 정의된 그룹이 있습니다. 이러한 그룹은 _restricted 그룹입니다. _restricted 그룹의 사용자인 경우, 모든 파일과 레지스트리 키가 CA Access Control 로 보호됩니다. 파일이나 레지스트리 키에 명백하게 정의된 액세스 규칙이 없는 경우, 액세스 권한은 해당 클래스(FILE 또는 REGKEY)의 _default 레코드에 의해 처리됩니다.

_restricted 그룹 사용 시에는 주의해야 합니다. _restricted 그룹의 사용자가 작업을 수행할 충분한 권한을 가지고 있지 않을 수도 있습니다. _restricted 그룹에 사용자를 추가하려면 초기에 경고 모드를 사용해 보십시오. 경고 모드에서는 사용자가 작업하는 데 필요한 파일과 레지스트리 키가 감사 로그에 표시됩니다. 감사 로그를 검사한 다음, 적절한 권한을 부여하고 경고 모드를 해제할 수 있습니다.

리소스 액세스에 대해 미리 정의된 그룹

CA Access Control 에서 다른 유형의 미리 정의된 그룹은 특정 리소스에 대해 허용되거나 금지된 액세스 유형을 정의합니다. 이러한 그룹으로는 다음과 같은 그룹이 있습니다.

- _network

  (Windows 에만 해당) _network 그룹은 특정 리소스에 대한 네트워크의 액세스를 정의합니다. 모든 사용자는 그룹의 구성원인 것처럼 처리되며, 그룹에 사용자를 명시적으로 추가해야 할 필요가 없습니다.

  예를 들어 특정 리소스는 네트워크에서 읽기만 가능하도록 지정할 수 있습니다. selang 을 사용하여 다음과 같이 새 리소스를 정의합니다.

  ```
  newres FILE c:\temp\readonly defaccess(none)
  ```

  그런 다음 네트워크를 통해 허용된 액세스를 지정합니다.

  ```
  authorize FILE c:\temp\readonly gid(_network) access(read)
  ```

  CA Access Control 끝점 관리를 사용하여 이 작업을 수행할 수도 있습니다.

  이제 네트워크에서 c:\temp\readonly 를 액세스할 때 사용자들은 네트워크에서 파일을 읽을 수만 있습니다.

- _interactive

  _interactive 그룹은 리소스가 위치한 컴퓨터에서 특정 리소스에 허용된 액세스를 정의합니다. 예를 들어 네트워크에서 리소스에 대한 액세스가 허용되지 않더라도 파일이 정의된 컴퓨터에는 파일에 대한 READ 액세스 권한을 부여할 수 있습니다.

다음 항목은 매우 중요합니다.

- CA Access Control 에서 _network 와 _interactive 그룹은 서로 연관성이 없습니다. 다시 말하면, _network 그룹에는 네트워크의 특정 리소스에 대한 액세스를 정의하는 규칙이 있을 수 있다는 의미입니다. _interactive 그룹의 다른 규칙은 동일한 리소스에 대한 액세스를 정의할 수 있습니다.
- _network 그룹 및 _interactive 그룹에 사용자를 추가할 필요가 없습니다.
- 이러한 그룹은 데이터베이스에 정의된 모든 Windows 리소스를 보호할 수 있습니다.

권한 부여 특성

권한 부여 특성은 데이터베이스의 사용자 레코드에 설정되어 사용자는 일반 사용자에게 수행이 허용되지 않는 작업을 수행할 수 있습니다. 권한 부여 특성에는 *전역* 및 *그룹*이라는 두 가지 종류가 있습니다. 각 전역 권한 부여 특성은 사용자가 데이터베이스에 있는 임의의 레코드에서 특정 유형의 기능을 수행할 수 있도록 허용합니다. 그룹 권한 특성은 사용자가 지정된 그룹 내에서 특정 유형의 기능을 수행할 수 있도록 허용합니다. 각 전역 권한 부여 특성과 그룹 권한 부여 특성의 기능과 제한은 다음 절에서 설명합니다.

전역 권한 부여 특성

자신의 사용자 레코드에 전역 권한 부여 특성이 설정된 사용자는 데이터베이스에 있는 관련 레코드에서 특수 기능을 수행할 수 있습니다. 전역 권한 부여 특성은 다음과 같습니다.

- ADMIN
- AUDITOR
- OPERATOR
- PWMANAGER
- SERVER
- IGN_HOL

참고: 전역 권한 부여 특성에 대한 자세한 내용은 *끝점 관리 안내서*를 참조하십시오.

그룹 권한 부여 특성

자신의 사용자 레코드에 *그룹 권한 부여 특성*을 가진 사용자는 지정된 그룹 내에서 특수 기능을 수행할 수 있습니다. 그룹 권한 부여 특성은 다음과 같습니다.

- GROUP-ADMIN
- GROUP-AUDITOR
- GROUP-OPERATOR
- GROUP-PWMANAGER

참고: 그룹 권한 부여 특성에 대한 자세한 내용은 *끝점 관리 안내서*를 참조하십시오.

경고 기간 사용

보호할 대상을 결정하는 작업 외에 구현 팀은 새 보안 제어를 단계적으로 실시할 수 있는 방법을 고려해야 합니다. 현재 작업 패턴에 최대한 지장을 주지 않으려면, 초기 단계에는 액세스 제한을 실행하기 보다는 리소스에 대한 액세스만 모니터링하는 것을 고려하는 것이 좋습니다.

리소스를 경고 모드에 두면 액세스를 모니터링할 수 있습니다. 리소스나 클래스에 대해 경고 모드가 활성화된 상태에서 사용자 액세스가 액세스 제한을 위반하면 CA Access Control 은 감사 로그에 경고 메시지를 기록하고 사용자에게 리소스에 대한 액세스를 제공합니다.

참고: 경고 모드 사용 시에는 감사 로그의 최대 크기를 늘리는 것을 고려해 보십시오. 경고 모드에 대한 자세한 내용은 *끝점 관리 안내서*를 참조하십시오.

CA Access Control 백도어

CA Access Control 을 처음 설치할 때(예를 들어, 평가 배포에서) CA Access Control 데이터베이스에서 부정확하게 규칙을 정의하는 경우가 있습니다. 잘못 정의된 규칙으로 인해 사용자가 로그인하지 못하거나 명령을 실행하지 못할 수 있습니다. 예를 들어, 시스템 디렉터리나 Windows 레지스트리의 중요 부분에 대한 액세스를 정의하는 규칙을 잘못 정의할 수 있습니다.

CA Access Control 을 중지하고 이러한 실수를 수정하기 어렵기 때문에 CA Access Control 에는 이러한 유형의 문제를 해결할 수 있도록 백도어가 있습니다. 백도어는 악의적인 용도로 악용될 수 있으므로 시스템이 설정되어 안정화된 이후에는 CA Access Control 에 있는 이러한 백도어를 비활성화할 수 있습니다.

이러한 백도어에 액세스하려면 컴퓨터를 시작할 때 부팅 메뉴에서 "안전 모드" 또는 "안정 모드(네트워킹 지원)"를 선택하십시오. 이 옵션 중 하나를 선택하면 CA Access Control 서비스가 자동으로 시작되지 않고 시스템이 시작됩니다.

백도어를 비활성화하려면 레지스트리 키 HKEY_LOCAL_MACHINE\Software\ComputerAssociates\ AccessControl\AccessControl\에서 reg_dword 데이터 유형의 레지스트리 'LockEE'를 정의하고 그 값을 1 로 설정하십시오.

참고: 이 레지스트리 값은 기본적으로 비어 있습니다.

이제 LockEE 가 1 로 설정된 시스템을 다음 모드에서 시작합니다.

- 안전 모드: CA Access Control 엔진 및 CA Access Control Watchdog 만 로드됩니다.

  네트워크 서비스에 의존하는 CA Access Control 에이전트(및 모든 정책 모델)는 로드되지 않습니다.
- 안전 모드(네트워킹 사용): CA Access Control 이 정상적으로 시작됩니다.

구현 추가 정보

이 절에서는 CA Access Control 을 설치한 후 고려해야 하는 기타 구현 정보를 설명합니다.

보안 유형

다음 방식 중 하나에 따라 사이트에서 보안을 처리할 수 있습니다.

- 명시적으로 허용되지 않은 작업은 모두 금지됩니다. 이상적인 방식이지만 구현 중에는 사용할 수 없습니다. 시스템에 대한 작업 수행을 허용하는 규칙이 없으므로 시스템은 액세스 규칙을 정의하려는 모든 시도를 차단합니다. 이것은 열쇠를 시동 장치에 꽂아 둔 상태로 차 문을 닫고 밖으로 나온 것과 같습니다.
- 구체적으로 금지되지 않은 작업은 모두 허용됩니다. 이러한 접근 방법은 보안이 다소 약할 수 있지만 보안 시스템을 구현하기 위한 실용적인 방법입니다.

CA Access Control 에서는 두 번째 방식으로 시작할 수 있으며, 액세스 규칙을 정의한 후에는 첫 번째 방식으로 전환할 수 있습니다. 기본 액세스(defaccess)와 범용 액세스(_default) 규칙을 통해 언제든지 방식을 정의하고 보호 정책을 전환할 수 있습니다.

중요! 보호 정책을 전환할 때 모든 사용자를 _restricted 그룹에 추가해야 할 수 있습니다. 보호 정책 사이에서 전환할 때 성능이 크게 저하될 수 있습니다.

접근자

*접근자*는 리소스를 액세스할 수 있는 엔터티입니다. 가장 일반적인 유형의 접근자는 사용자나 그룹인데, 이러한 사용자나 그룹에는 액세스 권한이 할당 및 확인되어야 합니다. 프로그램에서 리소스에 액세스할 경우, 프로그램의 소유자(사용자나 그룹)가 접근자가 됩니다. 접근자는 다음과 같은 세 범주로 나뉩니다.

- 특정 사용자 ID 와 연관된 개인
- 액세스 권한을 가진 그룹의 구성원인 개인
- 특정 사용자 ID 와 연관된 프로덕션 프로세스

가장 일반적인 유형의 접근자는 로그인을 수행할 수 있고 액세스 권한이 할당 및 확인되는 사람인 사용자입니다. CA Access Control 의 가장 중요한 특징 중 하나는 책임입니다. 요청을 담당하는 사용자를 대신하여 각 동작이나 액세스가 시도됩니다.

CA Access Control 을 사용하면 사용자 그룹을 정의할 수 있습니다. 일반적으로 사용자는 프로젝트, 부서 또는 부문별로 그룹을 이룹니다. 사용자를 그룹으로 묶으면 보안을 관리하기 위해 필요한 작업량을 크게 줄일 수 있습니다.

CA Access Control 끝점 관리 또는 selang 명령을 통해 새 사용자와 그룹을 정의하고 기존 사용자와 그룹을 수정할 수 있습니다.

리소스

보안 정책에서 필수적인 항목은 보호해야 할 시스템 리소스를 결정하고 리소스에 대한 보호 유형을 정의하는 것입니다.

리소스 클래스 및 액세스 규칙

설치가 완료되면, CA Access Control 은 즉시 시스템 이벤트를 차단한 후 리소스에 액세스하는 사용자 권한을 확인합니다. CA Access Control 에서 시스템 리소스에 대한 액세스를 제한하는 방법 및 제한할 리소스를 지정하기 전까지는 권한 확인 때마다 항상 액세스가 허용됩니다.

보호된 리소스의 속성은 리소스 레코드에 저장되며 리소스 레코드는 클래스로 그룹화됩니다. 리소스 레코드에 들어 있는 가장 중요한 정보는 액세스 규칙입니다. *액세스 규칙*은 하나 이상의 리소스 관련 작업을 수행하기 위한 하나 이상의 접근자 권한을 제어합니다. 액세스 규칙을 정의하는 몇 가지 방법은 다음과 같습니다.

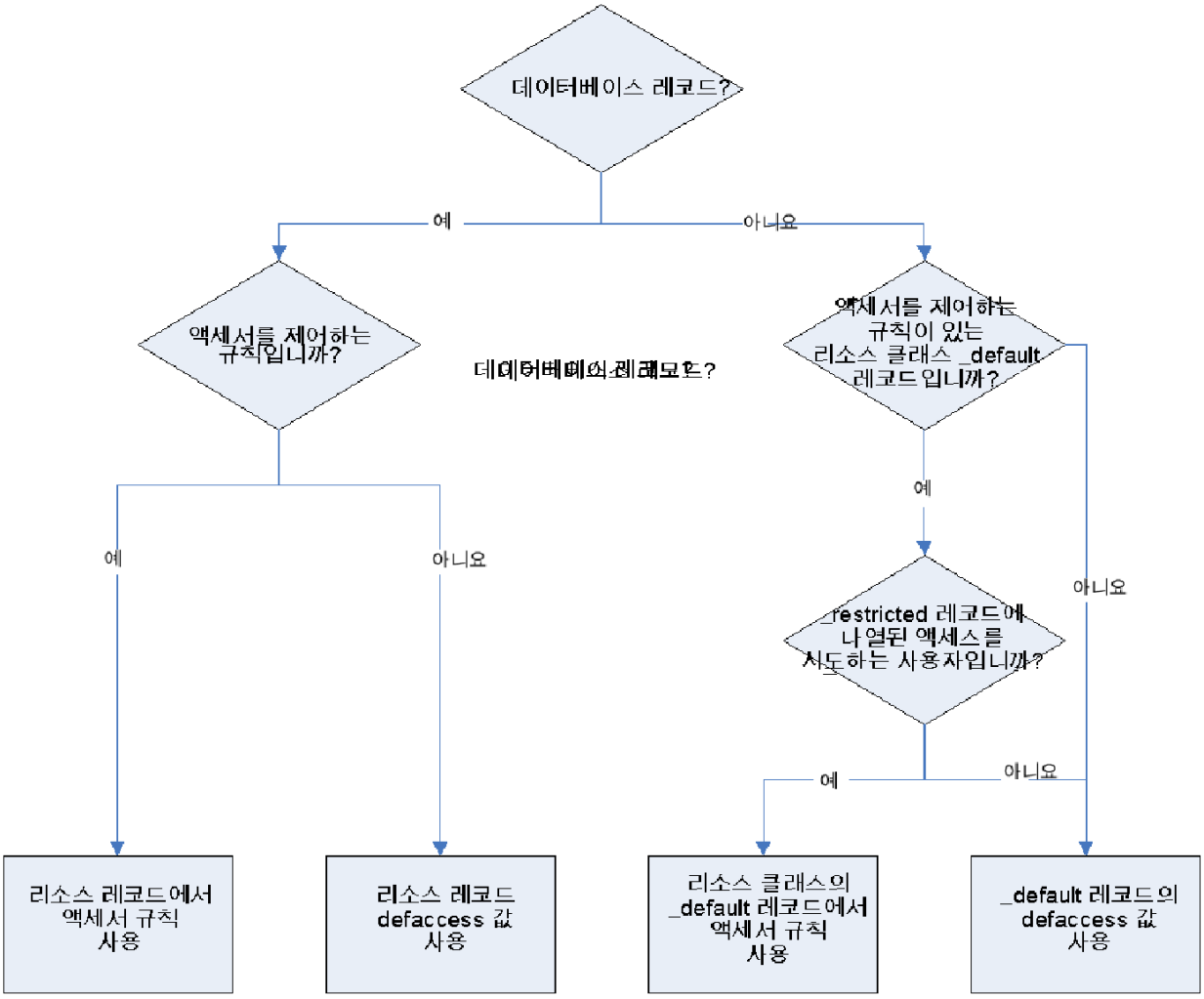
- ACL 이라고 하는 액세스 제어 목록(리소스에 액세스할 수 있는 권한이 있는 접근자 및 접근자가 보유한 올바른 액세스의 구체적인 목록)
- NACL 이라고 하는 네거티브 액세스 제어 목록(액세스를 거부해야 하는 접근자의 구체적인 목록)
- 리소스에 대한 기본 액세스 - ACL 에 구체적으로 나열되지 않은 접근자의 액세스 규칙을 지정합니다.
- 범용 액세스(클래스에 대한 _default 레코드) - 클래스에 특정 리소스 레코드가 아직 없는 리소스의 액세스를 지정합니다.
- 프로그램 ACL - 특정 프로그램을 통해 특정 접근자에 대한 액세스를 정의합니다.

- 조건 ACL - 일부 조건에 따라 액세스합니다. 예를 들어 TCP 레코드에서 특정 접근자를 통해 특정 원격 호스트에 대한 액세스를 정의할 수 있습니다.
- Inet ACL - 특정 포트를 통해 인바운드 네트워크 활동에 대한 액세스를 정의합니다.

defaccess 및 _default 사용

리소스에 대한 액세스가 요청되면 데이터베이스를 다음 순서로 검색하여 요청을 어떻게 처리할지 결정합니다. 그러면 CA Access Control 은 발견된 첫 번째 액세스 규칙을 사용합니다. *기본 액세스*(defaccess)와 _default 의 차이점에 유의하십시오.

1. 리소스가 데이터베이스에 레코드를 가지고 있으며 레코드에 접근자 제어 규칙이 있는 경우, CA Access Control 은 이 규칙을 사용합니다.
2. 레코드가 존재하지만 접근자를 제어하는 규칙이 없는 경우 *레코드*의 기본 액세스 규칙(*defaccess 값*)이 접근자에 적용됩니다.
3. 레코드가 존재하지 *않지만* 리소스 클래스의 _default 레코드에 접근자 제어 규칙이 있는 경우 CA Access Control 은 이 규칙을 사용합니다.
4. 레코드가 존재하지 않고 리소스 클래스의 _default 레코드에 접근자 제어 규칙이 없는 경우 _default 레코드의 기본 액세스 규칙(defaccess 값)이 접근자에 적용됩니다. 파일과 레지스트리 키인 경우에는 이러한 규칙이 _restricted 사용자 (페이지 133)에만 적용됩니다.



참고: 리소스 클래스 및 액세스 규칙에 대한 자세한 내용은 *selang 참조 안내서*를 참조하십시오.

제 7 장: Windows 끝점 설치 및 사용자 지정

이 섹션은 다음 항목을 포함하고 있습니다.

시작하기 전에

CA Access Control 을 설치하기 전에 사전 요구 사항이 충족되었는지 그리고 필요한 모든 정보가 준비되었는지 확인해야 합니다.

설치 방법

다음 방법으로 CA Access Control Windows 용 끝점 구성 요소 DVD 에서 Windows 용 CA Access Control 을 설치할 수 있습니다.

- **제품 탐색기** - CA Access Control 을 설치하는 가장 쉬운 방법은 제품 탐색기를 사용하는 것입니다. 제품 탐색기는 CA Access Control 의 여러 아키텍처 설치 중 하나를 선택하고 런타임 SDK 를 설치할 수 있는 그래픽 인터페이스의 설치 프로그램입니다. 제품 탐색기는 설치 프로세스의 각 단계를 안내하고 각 단계에서 제공해야 하는 정보를 묻습니다.
- **명령줄** - 설치 프로그램의 명령줄 인터페이스를 사용하면 다음을 수행할 수 있습니다.
  - 그래픽 설치 프로그램 실행을 위한 사용자 지정 기본값 설정

    명령줄에서 그래픽 설치 프로그램으로 기본값을 전달할 수 있습니다. 사용하고자 하는 사전 설정 기본값으로 설치 프로그램을 열지만 사용자가 각 설치의 옵션을 사용자 지정할 수 있는 배치 파일을 작성할 때 이 방법을 사용하십시오.
  - 자동 설치 수행

    명령줄을 사용하면 단순히 그래픽 설치 프로그램으로 기본값을 전달하는 것이 아니라 CA Access Control 을 자동으로 설치할 수 있습니다. 원격 컴퓨터에 설치하는 경우 이 방법을 사용하십시오.
- **Unicenter Software Delivery** - Unicenter Software Delivery 를 사용하여 CA Access Control 을 배포하기 위한 패키지를 작성할 수 있습니다.

방화벽 설정

CA Access Control 을 Windows Server 2003 또는 Windows Server 2008 에 설치할 때 CA Access Control 은 비 SSL TCP 연결을 위한 8891 포트와 SSL TCP 연결을 위한 5249 포트를 엽니다. 이 포트는 CA Access Control 에이전트-클라이언트 연결을 위한 기본 포트로 사용됩니다.

참고: CA Access Control 이 Windows 에서 사용하는 포트에 대한 자세한 내용은 *참조 안내서*를 참조하십시오.

새 설치

새로운 CA Access Control 인스턴스를 설치할 경우 다음을 주의하십시오.

- *릴리스 정보*를 읽으십시오.

  릴리스 정보에는 지원되는 플랫폼에 대한 정보, 알려진 문제, 고려 사항, CA Access Control 설치 전에 반드시 읽어야 하는 기타 중요 정보 등이 들어 있습니다.

- CA Access Control 은 Windows 관리자나 Administrators 그룹의 구성원이 설치해야 합니다.

- CA Access Control 는 다른 제품이 설치되지 않은 디렉터리에 설치하십시오.

- Microsoft Internet Explorer 6.x 또는 7.x 가 설치되어 있어야 합니다.

- CA Access Control 이 제품 설치를 완료하려면 Microsoft Visual C++ 2005 Redistributable Package 가 있어야 합니다.

  이 패키지가 없는 경우 설치 프로그램에서 이 패키지를 먼저 설치합니다.

- CA Technologies 라이선스 사용

  모든 CA Technologies 엔터프라이즈 제품 및 옵션은 네트워크에서 CA 소프트웨어를 실행하는 모든 컴퓨터에 대해 라이선스 파일 CA.OLF 를 요구합니다. CA Access Control 을 구입하면 제품을 설치하고 라이선스를 등록하는 데 필요한 정보가 들어 있는 라이선스 인증서를 받습니다.

  엔터프라이즈 라이선스 파일을 설치하려면 CA Access Control 행을 추가한 CA.OLF 파일을 CA_license 디렉터리(예: C:\Program Files\CA\SharedComponents\CA_LIC)에 복사합니다.

업그레이드 및 재설치

CA Access Control 을 업그레이드할 경우 다음을 주의하십시오.

- *릴리스 정보*를 읽으십시오.

  이 문서에는 지원되는 플랫폼에 대한 정보, 업그레이드할 수 있는 CA Access Control 버전, 알려진 문제, 고려 사항, CA Access Control 설치 전에 반드시 읽어야 하는 기타 중요 정보 등이 들어 있습니다.

- 제품 환경을 업그레이드하기 전에 새로운 릴리스에 대해 규모가 축소된 내부 테스트를 실시하는 것이 좋습니다.

- CA Access Control 을 업그레이드하는 경우 설치를 완료하려면 컴퓨터의 재부팅이 필요할 수 있습니다. 추후 패치에는 재부팅이 필요하지 않을 수도 있습니다.

  참고: 업그레이드할 때 재부팅이 필요한 CA Access Control 릴리스에 대한 자세한 내용은 *릴리스 정보*를 참조하십시오.

- 환경이 PMDB 계층으로 설정되었거나 설정하고자 하는 경우 다음 사항을 권장합니다.

  - 계층상의 하위부터 상위 순서로(구독자 먼저) 각 컴퓨터를 설치하거나 업그레이드하십시오.

    이전 버전의 구독자가 있는 PMDB 를 업그레이드하면 오류가 있는 명령이 전송될 수 있습니다. 이러한 문제는 이전 버전 PMDB 에 존재하지 않았던 클래스와 속성이 새 PMDB 에 있는 경우 발생할 수 있습니다.

    참고: 단일 컴퓨터에서 실행 중인 PMDB 계층은 동시에 업그레이드할 수 있습니다.

  - PMDB 또는 정책 업데이트 동안 업그레이드를 실시하지 *마십시오*.

  - 구독자와 PMDB 정책을 백업하십시오.

  참고: 이전 버전의 PMDB 는 최신 버전의 구독자를 포함할 수 있지만 최신 버전의 PMDB 는 이전 버전의 구독자를 포함할 수 없습니다. 이전 버전의 명령이 이후 버전에서 지원되므로 이전 PMDB 를 현재 CA Access Control 구독자에게 전파할 수 있습니다.

- 업그레이드 전에 사용했던 암호화 키를 그대로 사용해야 합니다.

- 설치 프로그램에서 이전 설치의 레지스트리 설정을 자동으로 저장하고 업그레이드합니다. 이전 버전의 레지스트리 키가 재배치되면 업그레이드 프로세스에서 이전 설정을 새 위치로 복사합니다.

  CA Access Control 레지스트리 설정은 다음 위치에 저장되어 있습니다.

  HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl

- CA Access Control 를 업데이트하면 기본적으로 전체 감사가 활성화됩니다.

  중요! 데이터베이스에서 사용하는 규칙에 따라 차이가 있지만 이 기능으로 인해 CA Access Control 가 로그 파일에 기록하는 감사 이벤트의 숫자가 크게 증가할 수 있습니다. 따라서 감사 로그 파일의 크기 및 백업 설정을 검토하는 것이 좋습니다.

  참고: 전체 감사에 대한 정보 및 감사 로그 백업을 위해 레지스트리 설정을 구성하고 사용하는 방법에 대한 자세한 내용은 *Windows 용 끝점 관리 안내서*를 참조하십시오.

다른 제품과의 공존

CA Access Control 을 설치할 때는 컴퓨터에 있는 다른 프로그램과 CA Access Control 의 공존 문제를 고려합니다.

CA Access Control 은 다른 프로그램(예: CA Antivirus)과 함께 환경에서 실행됩니다. 이로 인해 CA Access Control 과 로컬 컴퓨터에서 실행되는 프로그램 간에 충돌이 발생할 수 있습니다. 이러한 문제를 방지하기 위해 CA Access Control 설치 중에 공존 유틸리티(eACoexist.exe)가 실행되어 로컬 컴퓨터에서 충돌을 발생시킬 수 있는 프로그램을 검색합니다. 이 유틸리티는 CA Access Control 이 지원하는 각 공존 프로그램에 대해 하나의 플러그인(바이너리 모듈)을 사용합니다. CA Access Control 에서 검색한 프로그램이 트러스트되는 경우 CA Access Control 은 SPECIALPGM 규칙을 만들어 해당 프로그램을 등록합니다. 이 SPECIALPGM 규칙에 따라 이 프로그램에 대한 액세스가 결정되고 액세스가 허용되는 경우 CA Access Control 에서 해당 프로그램을 바이패스합니다.

참고: eACoexist 유틸리티 및 지원되는 플러그인에 대한 자세한 내용은 *참조 안내서*를 참조하십시오.

예: Dr Watson 에 대한 트러스트되는 프로그램 규칙

이 예에서는 공존 유틸리티가 CA Access Control 과 동일한 컴퓨터에서 Dr Watson 응용 프로그램을 발견할 경우 이 응용 프로그램에 대해 만들 수 있는 트러스트된 프로그램 규칙을 보여 줍니다. 기본 Windows 2000 Server 설치 컴퓨터에서 이러한 규칙은 다음과 같습니다.

```
editres SPECIALPGM ('C:\WINNT\system32\DRWTSN32.EXE') pgmtype(DCM)
editres PROGRAM ('C:\WINNT\system32\DRWTSN32.EXE') owner(nobody) defacc(x) trust
```

제품 탐색기 설치

CA Access Control 제품 탐색기를 사용하여 CA Access Control 의 여러 아키텍처 설치 중에서 원하는 설치를 선택하고 런타임 SDK 를 설치할 수 있습니다. 또한 설치 구성 요소에 대한 시스템 요구 사항도 볼 수 있습니다.

참고: 자동 실행이 활성화된 경우 광 디스크 드라이브에 Windows DVD 용 CA Access Control 끝점 구성 요소를 넣을 때 제품 탐색기가 자동으로 표시됩니다.

제품 탐색기를 사용한 설치

CA Access Control 제품 탐색기를 사용하여 CA Access Control 의 여러 아키텍처 설치 중에서 원하는 설치를 선택하고 런타임 SDK 를 설치할 수 있습니다. 제품 탐색기에서는 그래픽 인터페이스로 CA Access Control 을 설치하고 인터랙티브 방식의 정보를 얻을 수 있습니다.

제품 탐색기를 사용하여 설치하려면

1. Windows 관리자 권한을 가진 사용자(Windows administrator 또는 Windows Administrators 그룹의 구성원)로 Windows 시스템에 로그인합니다.
2. Windows 시스템에서 실행 중인 모든 응용 프로그램을 종료합니다.
3. 광 디스크 드라이브에 Windows DVD 용 CA Access Control 끝점 구성 요소를 넣습니다.

   자동 실행이 활성화된 경우 제품 탐색기가 자동으로 표시됩니다. 그렇지 않은 경우 광 디스크 드라이브 디렉터리로 이동하여 PRODUCTEXPLORERX86.EXE 파일을 두 번 클릭합니다.
4. "제품 탐색기" 기본 메뉴에서 "구성 요소" 폴더를 확장하고 "Windows 용 CA Access Control(*my_architecture*)"를 선택한 다음 "설치"를 클릭합니다.

   설치를 진행 중인 컴퓨터의 아키텍처와 일치하는 설치 옵션을 선택해야 합니다(32 비트, 64 비트 x64 또는 64 비트 Itanium).

   "설치 언어 선택" 창이 나타납니다.

5. CA Access Control 설치에 사용할 언어를 선택하고 "확인"을 클릭합니다.

   CA Access Control 설치 프로그램이 로드되기 시작하고 잠시 후 "소개" 화면이 나타납니다.

   참고: 설치 프로그램에서 기존 CA Access Control 설치를 탐지하면 CA Access Control 을 업그레이드할지 선택하라는 메시지가 표시됩니다.

6. 설치 화면의 지침을 수행합니다.

   설치를 하는 동안 설치 프로그램에서 정보를 입력하라는 메시지가 표시됩니다. CA Access Control 설치 시 필요한 정보에 대한 자세한 내용은 설치 워크시트 (페이지 149)를 참조하십시오.

   설치 프로그램이 CA Access Control 을 설치합니다. 설치가 완료되면 Windows 를 지금 재시작할지 또는 나중에 재시작할지 선택할 수 있습니다.

7. "예, 지금 시스템을 다시 시작합니다."를 선택한 다음 "확인"을 클릭합니다.

   시스템을 재부팅한 후 CA Access Control 이 제대로 설치되었는지 (페이지 173) 확인할 수 있습니다.

   참고: 컴퓨터를 나중에 다시 시작할 것을 선택할 경우 컴퓨터가 재부팅될 때까지 설치가 완료되지 않는다는 추가 경고 메시지가 나타납니다. 로그온 차단과 같은 일부 CA Access Control 기능은 컴퓨터를 다시 시작할 때까지 작동하지 않습니다.

설치 워크시트

설치 프로그램에서 초기 CA Access Control 설정에 필요한 정보를 묻는 메시지가 표시됩니다. 다음 절에서는 이 때 입력해야 할 정보에 대해 설명하고 권장 사항을 제시합니다.

기능 선택

설치 프로그램의 "기능 선택" 화면에서는 CA Access Control 을 설치할 위치와 이 컴퓨터에 설치할 기능을 정의할 수 있습니다. 사용 가능한 기능은 다음과 같습니다.

기능	설명	권장 사항
작업 위임	일반 사용자에게 관리 작업을 수행하는 데 필요한 권한을 부여할 수 있습니다. **참고:** 기본적으로 선택됩니다.	사용자에게 하위 관리 권한을 제공하려는 경우 이 기능을 선택하십시오. 이 사후 설치를 구성할 수도 있습니다.
SDK	SDK 라는 하위 디렉터리를 작성합니다. CA Access Control SDK 사용에 필요한 라이브러리와 파일 그리고 API 샘플이 들어 있습니다.	내부 CA Access Control 보안 응용 프로그램을 개발하고자 하는 경우 이 기능을 선택하십시오.
STOP(스택 오버플로 보호)	CA Access Control 스택 오버플로 보호 기능을 활성화합니다.	프로그램이 악용되는 것을 방지하려면 이 기능을 선택하십시오.
메인프레임 암호 동기화	사용자 암호를 메인프레임 컴퓨터와 동기화할 수 있게 해줍니다.	동기화하고자 하는 메인프레임 컴퓨터가 있는 경우 이 기능을 선택하십시오.
Unicenter 통합	Unicenter NSM 과 CA Access Control 을 통합하여 Unicenter NSM 데이터를 마이그레이션할 수 있습니다. CA Access Control 은 감사 데이터를 Unicenter NSM 의 구성 매개 변수에 의해 지정된 호스트 또는 사용자가 선택한 호스트로 전송합니다. **참고:** 이 컴퓨터에 Unicenter NSM 이 설치된 경우에만 이 기능을 사용할 수 있습니다.	

기능	설명	권장 사항
고급 정책 관리 클라이언트	고급 정책 관리를 위해 로컬 컴퓨터를 구성합니다.	(고급 정책 관리를 사용하여) 정책을 배포할 수 있도록 하려는 모든 끝점에 대해 이 기능을 선택하십시오. **참고:** 고급 정책 관리에 대한 자세한 내용은 *엔터프라이즈 관리 안내서*를 참조하십시오.
정책 모델 구독자	PMDB 부모로부터 업데이트를 받을 로컬 컴퓨터를 구성합니다.	PMDB 부모로부터 업데이트를 받을 수 있도록 하려는 모든 끝점에 대해 이 기능을 선택하십시오. **참고:** 정책 모델 서비스에 대한 자세한 내용은 *Windows 용 끝점 관리 안내서*를 참조하십시오.
PUPM 통합	PUPM 통합은 컴퓨터에서 권한 있는 계정과 응용 프로그램 검색할 수 있도록 로컬 컴퓨터에서 권한 있는 사용자 암호 관리(PUPM)를 구성합니다.	PUPM 을 사용하여 관리할 권한 있는 계정이 있는 모든 끝점에 대해 이 기능을 선택하십시오. **참고:** PUPM 에 대한 자세한 내용은 *엔터프라이즈 관리 안내서*를 참조하십시오.
보고서 에이전트	데이터베이스의 예약된 스냅숏을 배포 서버로 보내도록 컴퓨터를 구성할 수 있습니다. 그런 다음 감사 레코드도 배포 서버로 보내도록 선택할 수 있습니다.	엔터프라이즈 보고서에 이 끝점을 포함하려면 보고서 에이전트 기능을 선택합니다. CA Enterprise Log Manager 를 사용하여 엔터프라이즈 감사 로그를 관리하려면 감사 라우팅 하위 기능을 선택하십시오.

관리자 및 호스트 정보

다음 테이블에서는 입력해야 하는 정보에 대해 설명하고 권장 사항을 제시합니다.

정보	설명	권장 사항
관리자	CA Access Control 데이터베이스에 대한 관리자 액세스를 가진 사용자를 정의할 수 있습니다.	
관리 터미널	관리자가 CA Access Control 데이터베이스를 관리할 수 있는 컴퓨터를 정의할 수 있습니다.	관리자가 CA Access Control 끝점 관리를 사용하여 CA Access Control 을 관리하는 경우 CA Access Control 끝점 관리가 설치된 컴퓨터만 정의하면 됩니다. 관리자가 브라우저를 여는 컴퓨터를 정의할 필요는 없습니다.
DNS 도메인 이름	호스트 이름에 추가할 CA Access Control 의 네트워크 도메인 이름을 입력할 수 있습니다.	CA Access Control 이 호스트 이름에 추가한 도메인 이름을 최소한 하나는 입력해야 합니다.

사용자 및 그룹

다음 테이블에서는 입력해야 하는 정보에 대해 설명하고 권장 사항을 제시합니다.

정보	설명	권장 사항
기본 저장소에 있는 사용자 및 그룹을 지원합니다.	기존 엔터프라이즈 사용자 저장소(주 저장소)를 사용할 수 있어 사용자를 CA Access Control 데이터베이스에 복제할 필요가 없습니다.	CA Access Control 이 주 저장소(즉, 엔터프라이즈 사용자 저장소)를 지원하도록 설정하는 것을 좋습니다. 엔터프라이즈 저장소를 지원하지 *않도록* 선택하면 보호하려는 접근자를 CA Access Control 데이터베이스에서 복제해야 합니다.

정보	설명	권장 사항
Windows 사용자 및 그룹 데이터 가져오기	보호할 접근자를 작성하도록 선택하는 경우 데이터베이스에 기존 Windows 사용자와 그룹을 자동으로 작성할 수 있습니다.	Windows 사용자 및 그룹을 가져오기로 선택한 경우 다음 옵션 중 하나 이상을 선택하십시오. ■ **사용자 가져오기** - Windows 사용자를 데이터베이스로 가져옵니다. ■ **그룹 가져오기** - Windows 그룹을 데이터베이스로 가져옵니다. ■ **기본 그룹에 사용자 연결** - 가져온 사용자를 데이터베이스의 적절한 가져온 그룹에 자동으로 추가합니다. ■ **가져온 데이터의 소유자 변경** - 가져온 데이터의 소유자로 자신이 아닌 다른 사용자를 정의합니다. 기본적으로 이러한 레코드의 소유자는 설치를 실행하는 관리자(사용자)로 설정됩니다. ■ **도메인에서 가져오기** - 지정한 도메인에서 접근자 데이터를 가져옵니다.

Unicenter 통합

다음 테이블에서는 입력해야 하는 정보에 대해 설명하고 권장 사항을 제시합니다.

정보	설명	권장 사항
Unicenter TNG 와 CA Access Control 통합	CA Access Control 에서 감사 데이터를 Unicenter TNG 의 구성 매개 변수에 의해 지정된 호스트 또는 사용자가 선택한 호스트로 전송하도록 설정할 수 있습니다.	통합하려면, 감사 데이터가 Unicenter NSM 으로 전송되도록 지정한 후 CA Access Control 이 감사 데이터를 전송할 대상 호스트를 선택합니다.
Unicenter 달력과 CA Access Control 통합	Unicenter NSM 달력과 사용자 및 액세스 권한 통합을 지원하도록 설정할 수 있습니다.	Unicenter NSM 달력 호스트 서버에서 10 분(기본값)보다 자주 업데이트를 검색하도록 CA Access Control 을 구성합니다.

정보	설명	권장 사항
Unicenter Security 데이터 마이그레이션	Unicenter Security 데이터를 CA Access Control 로 마이그레이션할 수 있습니다.	이 옵션을 선택하지 않을 경우, Unicenter Security 에서 NSM 로의 마이그레이션이 수행되지 않으며 NSM 의 사용자 이름이 정규화된 이름으로 나타납니다(DOMAINNAME\USERNAME). 마이그레이션하면 사용자 이름이 정규화되지 않습니다(USERNAME).

내부 구성 요소 통신 암호화

다음 테이블에서는 입력해야 하는 정보에 대해 설명하고 권장 사항을 제시합니다.

화면	설명	권장 사항
SSL 통신	내부 구성 요소 통신에 SSL(Secure Socket Layer)을 사용할지 여부를 지정할 수 있습니다. SSL 및 대칭 키 암호화를 모두 사용할 수 있습니다.	SSL(공용 키 사용)과 대칭 키 암호화를 모두 사용하도록 권장합니다.
인증서 설정	SSL 을 사용하기로 선택한 경우 사용할 인증서를 선택할 수 있습니다.	잘 알려진 CA(인증 기관)의 인증서를 사용하는 것이 좋습니다.
인증서 생성	루트 인증서로 사용할 키 쌍과 자체 서명된 인증서를 작성할 수 있습니다.	권장되는 방법은 아니지만 자체 서명된 인증서를 사용할 수 있습니다. 자체 서명된 인증서를 사용하는 경우 모든 호스트에서 사용될 수 있도록 허용해야 합니다.
인증서 설정 변경	인증서 설정을 변경할 수 있습니다.	기본 인증서 및 키 쌍의 설정을 기본값이 아닌 값으로 변경하는 것이 좋습니다. 서버 인증서에 대한 개인 키를 보호하기 위해 암호를 지정할 수도 있습니다.
기존 인증서	설치한 인증서에 대한 정보를 입력할 수 있습니다.	

화면	설명	권장 사항
암호화 설정	암호화 방법과 대칭 암호화를 위한 키를 설정할 수 있습니다.	암호화 키의 설정을 기본 설정이 아닌 값으로 변경하는 것이 좋습니다.

추가 정보:

대칭 암호화 (페이지 399)
SSL, 인증 및 인증서 (페이지 403)

정책 모델 구독자 설정

다음 테이블에서는 입력해야 하는 정보에 대해 설명하고 권장 사항을 제시합니다.

정보	설명	권장 사항
부모 정책 모델 데이터베이스 지정	이 데이터베이스가 구독하는 하나 이상의 부모 PMDB 를 정의할 수 있습니다. 로컬 데이터베이스는 이 목록에서 지정하지 않는 PMDB 에서 업데이트를 받지 않습니다. 부모 PMDB 를 *pmdb@hostname.com* 형식으로 정의하십시오.	설치가 끝난 후 부모 PMDB 에서 이 데이터베이스를 구독자로 정의해야 합니다. **참고:** _NO_MASTER_를 부모 PMDB 로 지정하여 로컬 데이터베이스가 PMDB 로부터 업데이트를 수신함을 나타냅니다.
암호 정책 모델	암호 변경 내용을 전파하는 부모 암호 정책 모델을 정의할 수 있습니다. 암호 PMDB 를 *pmdb@hostname.com* 형식으로 정의하십시오.	설치가 끝난 후 암호 PMDB 에서 이 데이터베이스를 구독자로 정의해야 합니다.

고급 정책 관리 클라이언트

다음 테이블에서는 입력해야 하는 정보에 대해 설명하고 권장 사항을 제시합니다.

정보	설명	권장 사항
고급 정책 관리 서버 호스트 이름 지정	고급 정책 관리 서버 구성 요소가 설치된 서버의 이름을 정의하도록 해줍니다.	*dhName@hostName* 형식으로 호스트 이름을 정의합니다. **참고:** 고급 정책 관리 및 보고에 대한 자세한 내용은 *엔터프라이즈 관리 안내서*를 참조하십시오.

보고서 에이전트 구성

다음 테이블에서는 입력해야 하는 정보에 대해 설명하고 권장 사항을 제시합니다.

정보	설명	권장 사항
보고 일정 선택	보고서 에이전트가 데이터베이스의 스냅숏을 배포 서버로 보내는 시기를 지정할 수 있습니다.	시스템 리소스의 누수가 큰 시간대에는 보고서 에이전트가 스냅숏을 보내도록 예약하지 않는 것이 좋습니다.
감사 라우팅 구성	타임스탬프가 지정된 감사 로그 파일의 백업을 만들도록 지정할 수 있습니다. **참고:** 이 옵션은 "기능 선택" 페이지에서 감사 라우팅을 설치하도록 선택한 경우에만 표시됩니다.	타임스탬프가 지정된 감사 로그 파일 백업을 유지하도록 선택해야 합니다. 이것은 기본 설정이며, 보고서 에이전트가 모든 감사 레코드를 읽을 수 있도록 하는 데 필요합니다. CA Access Control 은 백업 감사 로그 파일이 50 개에 도달하면 파일을 덮어씁니다. 이 값이 적절하지 않은 경우 logmgr 레지스트리 하위 키의 audit_max_files 토큰을 기업에 적절한 값으로 편집해야 합니다.

배포 서버 구성

다음 표는 사용자가 제공하는 정보와 권장 사항에 대해 설명합니다.

정보	설명	권장 사항
서버 이름	배포 서버가 설치된 호스트의 이름을 정의할 수 있습니다.	배포 서버가 설치된 호스트의 정규화된 호스트 이름을 지정해야 합니다.
보안 통신 사용	배포 서버와 보고서 에이전트, 배포 서버와 PUPM 에이전트 사이의 통신에 SSL 을 사용할지 여부를 지정할 수 있습니다.	SSL 을 사용하는 것이 권장됩니다. SSL 을 사용하지 않는 경우 배포 서버는 TCP 를 사용하여 보고서 에이전트 및 PUPM 에이전트와 통신합니다.
서버 포트	배포 서버와 보고서 에이전트, 배포 서버와 PUPM 에이전트 사이의 통신에 사용하는 포트 번호를 정의할 수 있습니다.	SSL 통신을 사용하는 경우 기본 서버 포트는 7243 입니다. SSL 통신을 사용하지 않는 경우 기본 서버 포트는 7222 입니다.
통신 키	배포 서버와 보고서 에이전트, 배포 서버와 PUPM 에이전트 사이의 통신을 인증하기 위한 새 키를 정의할 수 있습니다.	배포 서버를 설치할 때 사용한 것과 동일한 키를 사용해야 합니다. **참고:** SSL 통신을 사용하는 경우 통신 키를 지정해야 합니다. SSL 통신을 사용하지 않는 경우 통신 키를 지정하지 않을 수 있습니다.

명령줄 설치

명령줄을 사용하여 다음 작업을 수행할 수 있습니다.

- 그래픽 설치 프로그램에 기본값을 전달
- 자동으로 CA Access Control 을 설치

설치 프로그램의 사용자 지정 기본값 설정

회사에 대해 사용하려는 기본값을 사용하여 CA Access Control 설치 프로그램을 설정하기 위해 명령줄을 사용할 수 있습니다. 그래픽 설치 프로그램은 명령줄에서 입력 사항을 수락하여 사전 선택할 옵션을 결정합니다.

설치 프로그램의 사용자 지정 기본값을 설정하려면

1. Windows 관리자 권한을 가진 사용자(Windows administrator 또는 Windows Administrators 그룹의 구성원)로 Windows 시스템에 로그인합니다.
2. Windows 시스템에서 실행 중인 모든 응용 프로그램을 종료합니다.
3. 광 디스크 드라이브에 Windows DVD 용 CA Access Control 끝점 구성 요소를 넣습니다.

   자동 실행을 활성화한 경우 CA Access Control 제품 탐색기가 나타납니다.
4. 표시된 제품 탐색기를 닫습니다.
5. 명령줄을 열고 광 디스크 드라이브에서 다음 디렉터리로 이동합니다.

   architecture

   architecture

   운영 체제의 아키텍처 약어를 정의합니다.

   X86, **X64** 및 **IA64** 중 하나를 사용할 수 있습니다.
6. 다음 명령을 입력합니다.

   setup [/s] /v"<*insert_params_here*>"

   <insert_params_here> 변수는 설치 프로그램에 전달하려는 설치 설정을 지정합니다.

   설치 프로그램이 나타납니다. 설치 프로그램 화면에 전달하도록 사용자가 선택한 기본 옵션이 표시되고 이를 수정하여 CA Access Control 을 설치할 수 있습니다.

자동 설치

대화식 피드백 없이 CA Access Control 을 설치하려면 명령줄을 사용하여 자동으로 CA Access Control 을 설치할 수 있습니다.

자동으로 CA Access Control 을 설치하려면

1. Windows 관리자 권한을 가진 사용자(Windows administrator 또는 Windows Administrators 그룹의 구성원)로 Windows 시스템에 로그인합니다.
2. Windows 시스템에서 실행 중인 모든 응용 프로그램을 종료합니다.
3. 광 디스크 드라이브에 Windows DVD 용 CA Access Control 끝점 구성 요소를 넣습니다.

   자동 실행을 활성화한 경우 CA Access Control 제품 탐색기가 나타납니다.
4. 표시된 제품 탐색기를 닫습니다.
5. 명령줄을 열고 광 디스크 드라이브에서 다음 디렉터리로 이동합니다.

   \architecture

   architecture

   운영 체제의 아키텍처 약어를 정의합니다.

   X86, **X64** 및 **IA64** 중 하나를 사용할 수 있습니다.
6. 다음 명령을 입력합니다.

   setup /s /v"/qn COMMAND=*keyword* <*insert_params_here*>"

   <insert_params_here> 변수는 설치 프로그램에 전달하려는 설치 설정을 지정합니다.

   참고: 자동 설치를 실행하려면 사용권 계약에 동의해야 합니다. 사용권 계약서 동의와 CA Access Control 자동 설치에 필요한 *키워드*는 설치 프로그램 실행 시 표시되는 사용권 계약의 맨 아래에 있습니다.

setup 명령 - Windows 용 CA Access Control 설치

setup 명령을 사용하여 미리 설정된 사용자 지정 기본값 (페이지 158)으로 또는 자동 설치 (페이지 159)를 수행할 때 Windows 용 CA Access Control 을 설치합니다.

참고: 명령줄 구문에 대한 자세한 내용은 MSDN(Microsoft Developer Network) 라이브러리에 있는 Windows Installer SDK 설명서를 참조하십시오.

이 명령의 형식은 다음과 같습니다.

setup [/s] [/L] [/v"*<insert_params_here>*"]

/s

설정 초기화 대화 상자를 숨깁니다.

/L

CA Access Control 설치 언어를 정의합니다.

참고: 이 릴리스에서 지원되는 CA Access Control 설치 언어에 대한 자세한 내용은 *릴리스 정보*를 참조하십시오.

/v "*<insert_params_here>*"

설치 프로그램으로 전달할 매개 변수를 정의합니다.

참고: 모든 매개 변수는 큰따옴표("")로 묶어야 합니다.

다음 매개 변수는 /v 매개 변수를 통해 설치 프로그램으로 전달됩니다.

/l[*mask*] *log_file*

설치 로그 파일의 전체 경로와 이름을 정의합니다. 사용 가능한 모든 정보를 기록하려면 마스크 *v 를 사용하십시오.

/forcerestart

설치가 완료된 후 강제로 컴퓨터를 다시 시작하도록 지정합니다.

/norestart

설치가 완료된 후 컴퓨터를 다시 시작하지 않도록 지정합니다.

/qn

/s 옵션을 사용하여 자동 설치를 지정합니다.

중요! 자동 설치를 실행하려면 *COMMAND* 매개 변수를 사용하십시오.

AC_API={1 | 0}

SDK 라이브러리와 샘플을 설치(1)할지 여부를 지정합니다.

기본값: 0(설치하지 않음)

ADMIN_USERS_LIST=\"*users*\"

CA Access Control 데이터베이스에 대한 관리자 액세스 권한을 가진 각 사용자를 공백으로 구분하여 나열한 목록을 정의합니다.

기본값: 설치를 수행하는 사용자

중요! 목록에 있는 NT Authority\System 사용자를 정의하지 마십시오. 로컬 관리 사용자 계정을 정의하십시오.

ADV_POLICY_MNGT_CLIENT={1 | 0}

고급 정책 관리를 위해 로컬 컴퓨터를 구성합니다. (1)

기본값: 1

이 옵션이 1 로 설정되면 다음과 같이 지정하십시오.

- **APMS_HOST_NAME=\"*name*\"**

  고급 정책 관리 구성 요소가 설치된 서버의 이름을 정의합니다.

COMMAND=*keyword*

사용권 계약 동의 및 CA Access Control 자동 설치에 필요한 명령을 정의합니다. 실제 *키워드*는 그래픽 설치 프로그램 실행 시 표시되는 사용권 계약의 맨 아래에 있습니다.

기본값: *none*

DIST_SERVER_NAME=\"*name*\"

PUPM 에이전트 및 보고서 에이전트가 통신하는 배포 서버 호스트의 정규화된 이름(예: test.company.com)을 정의합니다.

기본값: *none*

DIST_SERVER_PORT=\"*port*\"

PUPM 에이전트 및 보고서 에이전트가 배포 서버와 통신하기 위해 사용하는 포트 번호를 정의합니다.

기본값: 7243

DOMAIN_LIST=\"*domains*\"

CA Access Control 이 호스트 이름에 추가할 네트워크 DNS 도메인 이름의 공백으로 구분하여 나열된 목록을 정의합니다.

기본값: *none*

ENABLE_STOP={1 | 0}

STOP(스택 오버플로 보호) 기능을 활성화(1)할지 여부를 지정합니다.

기본값: 0(비활성화)

참고: STOP 지원은 x86 및 x64 설치에만 가능합니다.

HOSTS_LIST=\"*hosts*\"

관리자가 CA Access Control 데이터베이스(CA Access Control 터미널)를 관리할 수 있는 컴퓨터를 공백으로 구분하여 나열한 목록을 정의합니다.

기본값: 현재 컴퓨터

IMPORT_NT={Y | N}

주 (엔터프라이즈) 사용자 저장소를 지원할지 여부를 지정합니다.. 'N'으로 지정하면 주 사용자 저장소가 지원됩니다. 'Y'로 지정하면 주 사용자 저장소가 지원되지 않으며 다음 옵션 중 하나 이상을 지정하여 Windows 사용자 및 그룹을 CA Access Control 데이터베이스로 가져올 수 있습니다.

- **IMPORT_USERS={1 | 0}**

  Windows 사용자를 데이터베이스로 가져올지 여부를 지정합니다.

- **IMPORT_GROUPS={1 | 0}**

  Windows 그룹을 데이터베이스로 가져올지 여부를 지정합니다.

- **IMPORT_CONNECT_USERS={1 | 0}**

  가져온 사용자를 데이터베이스의 적절한 가져온 그룹에 추가할지 여부를 지정합니다.

- **IMPORT_CHANGE_OWNER={1 | 0} NEW_OWNER_NAME=***name*

  가져온 데이터의 소유자로 자신이 아닌 다른 사용자를 지정합니다.

- **IMPORT_FROM_DOMAIN={1 | 0} IMPORT_DOMAIN_NAME=***name*

  정의된 도메인에서 접근자 데이터를 가져올지 여부를 지정합니다.

참고: 기본적으로 이러한 모든 옵션은 지정되어 있지 않습니다(0 값과 동일).

INSTALLDIR=\"*location*\"

CA Access Control 을 설치할 위치를 정의합니다.

기본값: C:\Program Files\CA\AccessControl\

MAINFRAME_PWD_SYNC={1 | 0}

메인프레임 암호 동기화 기능을 설치(1)할지 여부를 지정합니다.

기본값: 0(설치하지 않음)

NEW_KEY=\"*name*\"

배포 서버와 PUPM 에이전트 및 배포 서버 사이의 통신을 인증하는 SSL 키를 정의합니다.

PMDB_CLIENT={1 | 0}

로컬 CA Access Control 데이터베이스를 부모 정책 모델 데이터베이스로 구독되는 여부를 지정합니다.

기본값: 0(아니오)

이 옵션을 지정하고 1 로 설정하는 경우 다음과 같이 지정하십시오.

- **PMDB_PARENTS_STR=\"***parents***\"**

  로컬 CA Access Control 데이터베이스가 구독된 부모 정책 모델 데이터베이스의 쉼표로 구분된 목록을 정의합니다. 로컬 데이터베이스가 PMDB 로부터 업데이트를 받도록 _NO_MASTER_를 부모 PMDB 로 지정합니다.

  기본값: *none*

- **PWD_POLICY_NAME=\"***name***\"**

  암호 정책 모델의 이름을 정의합니다.

  기본값: *none*

PMDB_PARENT={1 | 0}

정책 모델 부모 데이터베이스가 작성되는지 여부를 지정합니다. 이 옵션을 지정하고 1 로 설정하는 경우 다음과 같이 지정하십시오.

- **PMDB_NAME=\"***name***\"**

  작성할 PMDB 의 이름을 정의합니다.

  기본값: pmdb

- **PMDB_SUBSCRIBERS_STR=\"***subs***\"**

  PMDB_NAME 옵션으로 지정된 PMDB 가 변경 사항을 전파할 구독자 데이터베이스를 쉼표로 구분하여 나열한 목록으로 정의합니다. 기본적으로 이 데이터베이스가 설치된 PMDB 부모의 구독자 데이터베이스가 됩니다.

PUPM_AGENT={1 | 0}

PUPM 에이전트가 설치되는지 여부를 지정합니다. (1)

기본값: 0(설치하지 않음)

이 옵션을 지정하고 1 로 설정하는 경우 DIST_SERVER_NAME, DIST_SERVER_PORT, USE_SECURE_COMM 을 지정하십시오.

REPORT_AGENT={1 | 0}

보고서 에이전트를 설치(1)할지 여부를 지정합니다.

기본값: 0(설치하지 않음)

이 옵션을 지정하고 1 로 설정하는 경우 DIST_SERVER_NAME, DIST_SERVER_PORT, USE_SECURE_COMM 및 다음 매개 변수를 지정하십시오.

- **AUDIT_ROUTING={1 | 0}**

  감사 라우팅 기능이 설치되는지 여부를 지정합니다. (1)

  기본값: 0(설치하지 않음)

- **REPORT_DAYS_SCHEDULE=***days*

  보고서 에이전트를 실행할 요일을 쉼표로 구분하여 나열한 목록으로 정의합니다.

  값: Sun, Mon, Tue, Wed, Thu, Fri, Sat

  기본값: *none*

- **REPORT_TIME_SCHEDULE={***hh*:*mm***}**

  지정된 요일에 보고서 에이전트를 실행할 시간을 정의합니다(예: 14:30).

  제한: *hh* 는 0-23 까지의 숫자이며 *mm* 은 0-59 까지의 숫자입니다.

  기본값: *none*

TASK_DELEGATION={1 | 0}

작업 위임 기능이 사용되는지 여부를 지정합니다.

기본값: 1(사용됨)

UNICENTER_INTEGRATION={1 | 0}

Unicenter 통합 기능이 사용되는지 여부를 지정합니다. (1) 이 기능은 컴퓨터에 Unicenter NSM 이 설치된 경우에만 사용할 수 있습니다.

기본값: 0(사용되지 않음)

이 옵션을 지정하고 1 로 설정하는 경우 다음과 같이 지정하십시오.

- **SEND_DATA_TO_TNG={1 | 0}**

  감사 데이터가 Unicenter NSM 로 전달되는지 여부를 지정합니다. (1)

  기본값: 1(데이터가 전달됨)

- **OTHER_TNG_HOST_NAME=\"*name*\"**

  감사 데이터가 전달되는 호스트를 정의합니다.

  기본값: Unicenter NSM 에 지정된 호스트 이름

- **SUPPORT_TNG_CALENDAR= {1 | 0}**

  Unicenter NSM 달력이 지원되는지 여부를 지정합니다. (1)

  기본값: 1(지원됨)

- **TNG_REFRESH_INTERVAL=\"*mm*\"**

  새로 고침 간격(분)을 정의합니다.
  SUPPORT_TNG_CALENDAR=1 도 설정했는지 확인합니다.

  기본값: 10

- **UNICENTER_MIGRATION={1 | 0}**

  Unicenter 보안 데이터가 CA Access Control 로 마이그레이션되는지 여부를 지정합니다. (1)

  기본값: 1(마이그레이션됨)

USE_SECURE_COMM={1 | 0}

PUPM 에이전트 및 보고서 에이전트가 보안 통신을 사용하는지 여부를 지정합니다. (1)

기본값: 0(아니오)

이 옵션을 지정하고 1 로 설정하는 경우 NEW_KEY 의 SSL 키 값도 지정하십시오.

USE_SSL={1 | 0}

통신 암호화의 SSL 을 설정할지 여부를 지정합니다.

기본값: 0(아니오)

이 옵션을 지정하고 1 로 설정하는 경우 다음과 같이 지정하십시오.

- **CERT_OPTION={1 | 2}**

  사용할 인증서 옵션을 지정합니다.

  값: 1 - CA Access Control 인증서 생성; **2** - 설치된 기존 인증서 사용.

  기본값: 1

- **GENERATE_OPTION={1 | 2}**

  CA Access Control 인증서 생성 방법을 지정합니다. CERT_OPTION=1 로 설정했는지 확인하십시오.

  값: 1 - 기본 루트 인증서 사용; **2** - 루트 인증서 지정.

- **SERVER_PRIV_KEY_PWD=\"*password*\"**

  생성된 CA Access Control 인증서에 대한 개인 키의 암호를 정의합니다. CERT_OPTION=1 로 설정했는지 확인하십시오.

- **GEN_ROOT_CERT=\"*file*\"**

  루트 인증서 파일(.pem)의 정규화된 파일 이름을 정의합니다. CERT_OPTION=1 및 GENERATE_OPTION=2 로 설정했는지 확인하십시오.

- **GEN_ROOT_PRIVATE=\"*file*\"**

  루트 개인 키 파일(.key)의 정규화된 파일 이름을 정의합니다. CERT_OPTION=1 및 GENERATE_OPTION=2 로 설정했는지 확인하십시오.

- **ROOT_PRIV_KEY_PWD=\"*password*\"**

  루트 개인 키에 대한 암호를 정의합니다. CERT_OPTION=1 및 GENERATE_OPTION=2 로 설정했는지 확인하십시오.

- **EXIST_ROOT_CERT=\"*file*\"**

  루트 인증서 파일(.pem)의 정규화된 파일 이름을 정의합니다. CERT_OPTION=2 로 설정했는지 확인하십시오.

- **EXIST_SERVER_CERT=\"*file*\"**

  서버 인증서 파일(.pem)의 정규화된 파일 이름을 정의합니다. CERT_OPTION=2 로 설정했는지 확인하십시오.

- **EXIST_PRIVATE_KEY=\"*file*\"**

  서버 개인 키 파일(.key)의 정규화된 파일 이름을 정의합니다. CERT_OPTION=2 로 설정했는지 확인하십시오.

- **EXIST_PRIV_KEY_PWD=\"*password*\"**

  서버 개인 키에 대한 암호를 정의합니다. CERT_OPTION=2 로 설정했는지 확인하십시오.

USE_SYMT_KEY={1 | 0}

통신에 대칭 키 암호화를 설정할지 여부를 지정합니다. USE_SSL=0 인 경우 이 매개 변수는 1 로 설정됩니다.

기본값: 1

이 옵션을 지정하고 1 로 설정하는 경우 또한 다음과 같이 지정하십시오.

- **ENCRYPTION_METHOD={Default | DES | 3DES | 256AES | 192AES | 128AES}**

  통신에 사용할 암호화 방법을 지정합니다.

  기본값: 256AES

- **CHANGE_ENC_KEY={1 | 0}**

  기본 암호화 키를 변경하도록 지정합니다. (1)

  기본값: 1(예)

- **NEW_ENCRYPT_KEY=\"*key*\"**

  기본 암호화 키를 변경하도록 선택하는 경우 암호화 키를 정의합니다. 또한 CHANGE_ENC_KEY=1 로 설정합니다.

예제: setup 명령을 사용하여 설치 기본값 설정

다음 예제에서는 설치 디렉터리를 설정하고 CA Access Control 설치를 위한 설치 로그 파일 기본값을 정의한 다음 그래픽 설치 프로그램을 엽니다.

```
setup.exe /s /v"INSTALLDIR="C:\Program Files\CA\AccessControl\" /L*v %SystemRoot%\eACInstall.log"
```

예: setup 명령 사용하여 암호화 설정 지정

다음 예는 여러 암호화 설정을 사용하여 자동 모드에서 CA Access Control 을 설치합니다. 각 예에서 각 명령은 또한 CA Access Control 을 설치하고, 기본 보고서 에이전트 및 작업 위임 기능을 설치하고, SSL 을 활성화하고, 설치 로그 파일의 경로 및 이름을 정의합니다.

- 이 예는 기본 CA Access Control 루트 인증서에서 서버 인증서를 생성하고 서버 개인 키에 대한 암호를 정의합니다.

  setup.exe /s /v"qn COMMAND=proceed USE_SSL=1 CERT_OPTION=1 GENERATE_OPTION=1 SERVER_PRIV_KEY_PWD=\"P@ssw0rd\" /l*v C:\AC_silent.log"

- 이 예는 타사 루트 인증서에서 서버 인증서를 생성합니다. 루트 개인 키는 암호로 보호됩니다.

  setup.exe /s /v"qn COMMAND=proceed USE_SSL=2 CERT_OPTION=1 GENERATE_OPTION=1 GEN_ROOT_CERT=\"C:\Crypto\example.pem\" GEN_ROOT_PRIVATE=\"C:\Crypto\example.key\" ROOT_PRIV_KEY_PWD=\"P@ssw0rd\" /l*v C:\AC_silent.log"

- 이 예는 CA Access Control 이 타사 루트 및 서버 인증서를 사용하도록 지정합니다. 서버 개인 키는 암호로 보호됩니다.

  setup.exe /s /v"qn COMMAND=proceed USE_SSL=1 CERT_OPTION=2 EXIST_ROOT_CERT=\"C:\Crypto\example.pem\" EXIST_SERVER_CERT=\"C:\Crypto\server.pem\" EXIST_PRIVATE_KEY=\"C:\Crypto\server.key\" EXIST_PRIV_KEY_PWD=\"P@ssw0rd\" /l*v C:\AC_silent.log"

추가 정보:

통신 암호화 (페이지 399)

Windows 끝점 업그레이드

끝점을 업그레이드하면 CA Access Control 설치 프로그램이 핵심 CA Access Control 기능 및 끝점에 이미 설치된 모든 기능을 업그레이드합니다. 핵심 CA Access Control 기능을 업그레이드한 이후에 새 기능을 설치할 수도 있습니다.

참고: 업그레이드를 완료하기 위해 컴퓨터를 다시 시작해야 할 수도 있습니다. 업그레이드할 때 재부팅이 필요한 CA Access Control 릴리스에 대한 자세한 내용은 *릴리스 정보*를 참조하십시오.

끝점을 업그레이드하려면

1. Windows 관리자 권한을 가진 사용자(Windows administrator 또는 Windows Administrators 그룹의 구성원)로 Windows 시스템에 로그인합니다.
2. Windows 시스템에서 실행 중인 모든 응용 프로그램을 종료합니다.
3. 광학 디스크 드라이브에 Windows 용 CA Access Control 끝점 구성 요소 DVD 를 넣습니다.

   자동 실행이 활성화된 경우 제품 탐색기가 자동으로 표시됩니다. 그렇지 않은 경우 광 디스크 드라이브 디렉터리로 이동하여 PRODUCTEXPLORERX86.EXE 파일을 두 번 클릭합니다.
4. "제품 탐색기" 기본 메뉴에서 "구성 요소" 폴더를 확장하고 "Windows 용 CA Access Control"(*my_architecture*)을 선택한 다음 "설치"를 클릭합니다.

   참고: 컴퓨터의 아키텍처와 일치하는 설치 옵션이 강조 표시되어 컴퓨터에 기존 CA Access Control 버전이 설치되어 있음을 나타냅니다.

   CA Access Control 의 업그레이드를 수행할지 묻는 대화 상자가 표시됩니다.
5. "예"를 클릭합니다.

   CA Access Control 설치 프로그램이 로드되기 시작하고 잠시 후 "소개" 화면이 나타납니다.
6. 설치 화면의 지침을 수행합니다.

   설치 프로그램이 CA Access Control 을 업그레이드합니다. 업그레이드가 완료되면 Windows 를 지금 다시 시작할지 또는 나중에 다시 시작할지 선택할 수 있습니다.
7. (선택 사항) "예"를 선택하여 컴퓨터를 지금 다시 시작합니다.

   컴퓨터가 다시 부팅되고 업그레이드가 완료됩니다.

8. (선택 사항) 다음과 같이 추가 CA Access Control 기능을 설치합니다.
   a. "시작", "제어판", "프로그램 추가/제거"를 차례로 클릭합니다.
   b. 프로그램 목록을 스크롤하여 CA Access Control 을 선택한 다음 "변경"을 클릭합니다.

      CA Access Control 설치 프로그램이 로드되기 시작하고 잠시 후 "프로그램 유지 관리" 화면이 나타납니다.
   c. "수정"을 선택한 다음 설치 화면의 지시를 따라 기능을 설치합니다.

      설치를 하는 동안 설치 프로그램에서 정보를 입력하라는 메시지가 표시됩니다. 기능을 설치할 때 필요한 정보는 설치 워크시트 (페이지 149)를 참조하십시오. 설치를 완료하기 위해 컴퓨터를 다시 시작해야 할 수 있습니다.

CA Access Control 시작 및 중지

기본적으로 CA Access Control 서비스는 Windows 가 시작될 때마다 자동으로 시작됩니다.

CA Access Control 중지

로컬 및 원격 컴퓨터에서 CA Access Control 을 중지하려면 secons 유틸리티를 사용합니다. CA Access Control 을 중지하기 위해 특정 Windows 권한이 필요한 것은 아니지만 CA Access Control 에서 ADMIN 또는 OPERATOR 특성이 있어야 합니다.

참고: Windows 서비스 관리자에서 CA Access Control 이 실행 중일 때는 CA Access Control 을 중지할 수 없습니다. Windows 서비스 관리자에서 CA Access Control 서비스를 수정하기 전에 먼저 secons 유틸리티를 사용하여 CA Access Control 을 중지해야 합니다.

CA Access Control 을 중지하려면

1. 명령 프롬프트 창을 열고 CA Access Control 바이너리가 있는 디렉터리로 이동합니다.

   기본적으로 CA Access Control 바이너리는 C:\Program Files\CA\AccessControl\\bin 에 있습니다.

2. 다음 명령을 입력합니다.

   secons -s [*hosts* | *ghosts*]

   -s [*hosts* | *ghosts*]

   공백으로 구분하여 정의된 원격 호스트에서 CA Access Control 서비스를 종료합니다. 호스트를 지정하지 않으면 CA Access Control 이 로컬 호스트에서 종료됩니다.

   ghost 레코드의 이름을 입력하여 호스트 그룹을 정의할 수 있습니다. 원격 터미널에서 이 옵션을 사용하면 유틸리티가 암호 확인을 요청합니다. 원격 컴퓨터와 로컬 컴퓨터에서 모두 관리자 권한이 필요할 뿐만 아니라 원격 호스트 데이터베이스에 로컬 컴퓨터에 대한 쓰기 권한이 있어야 합니다.

   로컬 컴퓨터에서 CA Access Control 을 중지하면 아래와 같은 메시지가 나타납니다.

   현재 CA Access Control 이(가) 다운되었습니다.

   CA Access Control 이 원격 호스트가 중지되면 CA Access Control 은 원격 호스트 종료가 성공했는지 여부를 보고합니다. 앞에서 원격 호스트가 성공적으로 종료되지 않았더라도 목록에 있는 각 호스트를 종료하려는 시도가 수행됩니다.

수동으로 CA Access Control 시작

일반적으로 Windows 를 시작하면 CA Access Control 이 시작됩니다.

CA Access Control 을 중지한 경우 명령 프롬프트에서 명령을 실행하여 수동으로 다시 시작할 수도 있습니다.

CA Access Control 을 수동으로 시작하려면

1. Windows 관리자 권한을 가진 사용자(Windows 관리자 또는 Windows Administrators 그룹의 구성원)로 Windows 시스템에 로그인합니다.
2. 명령 프롬프트 창에서 CA Access Control 바이너리를 포함한 디렉터리로 변경합니다(기본값은 시스템 디렉터리의 C:\Program Files\CA\AccessControl\\bin 임).
3. 다음 명령을 입력하여 CA Access Control 을 시작합니다.

   seosd -start

설치 확인

CA Access Control 을 성공적으로 설치한 경우 다음 변경 사항이 나타납니다.

- 새 키가 Windows 레지스트리에 추가됩니다.

  HKEY_LOCAL_MACHINE\Software\ComputerAssociates\AccessControl

  CA Access Control 이 실행되는 동안 CA Access Control 키 및 하위 키가 보호되며, 키를 수정하려면 CA Access Control 끝점 관리 또는 selang 명령을 사용해야 합니다. 하지만 키와 값을 읽기 위해 CA Access Control 끝점 관리 또는 selang 명령을 사용할 필요는 없습니다.
- 컴퓨터를 다시 시작할 때 새로운 몇몇 CA Access Control 서비스가 자동으로 시작됩니다. 이러한 서비스에는 Watchdog, 엔진, 에이전트 등이 포함되며 이들 서비스는 항상 설치됩니다. 작업 위임과 같은 기타 서비스는 설치 중 선택한 옵션에 따라 존재 여부가 결정됩니다. 모든 CA Access Control 서비스의 표시 이름은 "CA Access Control"로 시작됩니다. Windows 서비스 관리자를 사용하여 어떠한 서비스가 설치되었고 이러한 서비스가 실행 중인지 여부를 확인할 수 있습니다.

로그인 보호 화면 표시

기본적으로 CA Access Control 을 설치한 후 사용자가 대화식으로 로그인하고(GINA) CA Access Control 서비스가 실행 중이면 컴퓨터가 CA Access Control 에 의해 보호됨을 사용자에게 알리는 보호 화면이 나타납니다.

시작 화면은 4 초 동안 표시되고 자동으로 닫힙니다.

보호 메시지를 비활성화하려면 HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Access Control\SplashEnable 레지스트리 키 값을 1 에서 0 으로 변경하십시오.

고급 정책 관리를 위한 끝점 구성

고급 정책 관리 서버 구성 요소를 설치했으면, 고급 정책 관리를 위해 엔터프라이즈의 각 끝점을 구성해야 합니다. 이때 서버 구성 요소와 정보를 주고받을 수 있도록 끝점을 구성해야 합니다.

참고: 이 절차에서는 고급 정책 관리를 위해 기존 CA Access Control 설치를 구성하는 방법을 보여줍니다. 끝점에 CA Access Control 을 설치할 때 이 정보를 지정한 경우 끝점을 다시 구성할 필요가 없습니다.

고급 정책 관리를 위한 끝점을 구성하려면 명령 창을 열고 다음 명령을 입력합니다.

dmsmgr -config -dhname *dhName*

dhName

끝점과 함께 작동할 DH(배포 호스트) 이름 목록을 쉼표로 구분하여 정의합니다.

예: DH__@centralhost.org.com

이 명령은 고급 정책 관리를 위해 끝점을 구성하고 정의된 DH 와 작업하도록 끝점을 설정합니다.

참고: 자세한 내용은 *참조 안내서*의 dmsmgr -config 명령을 참조하십시오.

보고를 위해 Windows 끝점 구성

CA Access Control 끝점 관리 및 보고서 포털이 설치되어 구성되면 보고서 에이전트를 활성화하고 구성하여 처리를 위해 배포 서버에 데이터를 보내도록 끝점을 구성할 수 있습니다.

참고: CA Access Control 을 설치할 때 보고를 위해 끝점을 구성할 수 있습니다. 이 절차에서는 설치 시 이 옵션을 구성하지 않은 경우 보고서 전송을 위해 기존 끝점을 구성하는 방법에 대해 설명합니다.

보고를 위해 Windows 끝점을 구성하려면

1. "시작", "제어판", "프로그램 추가/제거"를 차례로 클릭합니다.

   "프로그램 추가/제거" 대화 상자가 나타납니다.

2. 프로그램 목록을 스크롤하여 CA Access Control 를 선택합니다.
3. "변경"을 클릭합니다.

   CA Access Control 설치 마법사가 나타납니다.

4. 마법사 프롬프트에 따라 보고서 에이전트 기능이 활성화되도록 CA Access Control 설치를 수정합니다.

참고: 보고서 에이전트를 활성화한 후 CA Access Control 구성 설정을 수정하여 성능 관련 설정을 변경할 수 있습니다. 보고서 에이전트 구성 설정에 대한 자세한 내용은 *참조 안내서*를 참조하십시오.

클러스터 환경에 대한 CA Access Control 사용자 지정

클러스터 환경에서 CA Access Control 을 사용하려면, 클러스터의 각 노드에 CA Access Control 을 설치해야 합니다. 또한 각 노드의 일반 리소스에 동일한 일련의 규칙(쿼럼 디스크 또는 네트워크 차단 사용 시 네트워크)을 정의합니다.

CA Access Control 은 클러스터 환경에서 실행 중인지 감지할 수 있습니다. CA Access Control 이 클러스터에 클러스터 내부 통신 전용으로 사용되는 별도의 네트워크 어댑터가 설치된 자체 네트워크가 있음을 감지할 경우, 해당 네트워크 어댑터에 대해 네트워크 차단이 비활성화됩니다. 클러스터를 나머지 엔터프라이즈에 연결하는 네트워크 인터페이스의 경우, 네트워크 차단이 정상적으로 작동합니다.

참고: 클러스터가 클러스터 내부 통신 *및* 나머지 네트워크에 대한 통신에 동일한 네트워크 인터페이스를 사용할 경우 이 기능을 사용할 수 없습니다.

예제

다음과 같은 두 개의 노드가 있다고 가정합니다.

- NODE1 은 다음과 같은 두 개의 IP 주소를 가집니다.
  - 10.0.0.1 는 내부 클러스터 네트워크 IP 주소입니다.
  - 192.168.0.1 는 외부 네트워크 연결입니다.
- NODE2 도 다음과 같은 두 개의 IP 주소를 가집니다.
  - 10.0.0.2 는 내부 클러스터 네트워크 IP 주소입니다.
  - 192.168.0.2 는 외부 네트워크 연결입니다.

  클러스터 자체에는 192.168.0.3 이라는 추가 IP 주소가 있습니다.

내부 클러스터 네트워크 IP 주소를 사용하여 서로 통신하는 경우 네트워크 차단을 통해 NODE1 은 NODE2 에 연결할 수 없으며 반대의 경우도 마찬가지입니다.

NODE1 또는 NODE2 가 외부 네트워크 IP 주소를 사용하여 접속된 경우 네트워크 차단은 CA Access Control 규칙에서 정의된 대로 작동합니다.

또한 클러스터가 192.168.0.3 IP 주소로 접속된 경우 네트워크 차단은 CA Access Control 규칙에서 정의된 대로 작동합니다.

제거 방법

다음 방법을 사용하여 Windows 끝점에서 CA Access Control 을 제거할 수 있습니다.

- 일반 제거 - 이 방법은 그래픽 인터페이스를 사용하여 CA Access Control 을 제거하고 대화형 피드백을 제공합니다.
- 자동 제거 - 이 방법은 명령줄을 사용하여 대화형 피드백 없이 CA Access Control 을 제거합니다.

CA Access Control 제거

Windows 관리자 권한을 가진 사용자(Windows 관리자 또는 Windows Administrators 그룹의 구성원)로 Windows 시스템에 로그인합니다.

CA Access Control 을 제거하려면

1. (선택 사항) CA Access Control 을 종료합니다 (페이지 172).

   참고: 수동으로 종료하지 않으면 설치 프로그램이 자동으로 CA Access Control 을 종료합니다.

2. "시작", "설정", "제어판"을 차례로 선택합니다.

   Windows 제어판이 나타납니다.

3. "프로그램 추가/제거"를 두 번 누릅니다.

   "추가/제거" 대화 상자가 나타납니다.

4. 설치된 프로그램 목록에서 CA Access Control 을 선택한 후 "추가/제거"를 클릭합니다.

5. CA Access Control 제거를 확인하는 메시지 상자에서 "예"를 클릭합니다.

6. 제거가 완료되면 "확인"을 클릭합니다.

7. 모든 CA Access Control 구성 요소를 제거하려면 컴퓨터를 재부팅합니다.

자동 CA Access Control 제거

대화식 피드백 없이 CA Access Control 을 제거하려면 명령줄을 사용하여 자동으로 CA Access Control 을 제거할 수 있습니다. Windows 관리자 권한을 가진 사용자(Windows 관리자 또는 Windows Administrators 그룹의 구성원)로 Windows 시스템에 로그인합니다.

자동으로 CA Access Control r12.5 를 제거하려면 다음 명령을 입력하십시오.

Msiexec.exe /x{822BFADC-E040-4F5C-A00A-B8E558A2D616} /qn *insert_params_here*

<insert_params_here> 변수는 설치 프로그램에 전달하려는 설치 설정을 지정합니다. 예를 들어 이 명령은 CA Access Control 을 제거하고 c:\ac_uninst.log 에 제거 로그를 작성합니다.

Msiexec.exe /x{822BFADC-E040-4F5C-A00A-B8E558A2D616} /qn /l*v c:\ac_uninst.log

참고: 수동으로 종료하지 않으면 설치 프로그램이 자동으로 CA Access Control 을 종료합니다.

제 8 장: UNIX 끝점 설치 및 사용자 지정

이 장에서는 CA Access Control UNIX 끝점 설치 프로세스를 안내합니다. 이 장에 설명된 지침에 따라 CA Access Control 설치를 마치면 시스템에는 CA Access Control 끝점 소프트웨어 복사본과 기본 CA Access Control 데이터베이스가 설치됩니다. 설치가 끝난 후에는 CA Access Control 을 시작하는 방법과 명령 사용 방법을 설명합니다. 나중에 데이터베이스를 편집하여 시스템을 보호하는 액세스 규칙을 정의할 수 있습니다.

이 섹션은 다음 항목을 포함하고 있습니다.

시작하기 전에

CA Access Control 을 설치하기 전에 사전 요구 사항이 충족되었는지 그리고 필요한 모든 정보가 준비되었는지 확인해야 합니다.

운영 체제 지원 및 요구 사항

지원되는 UNIX 운영 체제 중 하나에 CA Access Control 을 설치할 수 있습니다.

참고: 자세한 내용은 *릴리스 정보*를 확인하십시오.

관리 터미널

CA Access Control 끝점 관리 및 CA Access Control 엔터프라이즈 관리를 사용하여 중앙에서 CA Access Control 정책을 관리하거나, 명령줄(selang)을 통해 컴퓨터에 연결하거나 컴퓨터에서 직접 액세스 규칙을 업데이트하는 방법으로 CA Access Control 정책을 관리할 수 있습니다.

컴퓨터의 액세스 규칙을 직접 업데이트하려면 관리 중인 터미널에 대한 쓰기 액세스 권한 및 CA Access Control 데이터베이스의 컴퓨터 정책에 대한 *admin* 특성이 필요합니다.

CA Access Control 을 설치하면 기본적으로 터미널 권한을 로컬 컴퓨터 터미널에만 부여하도록 설정됩니다. 이 설정은 로컬 터미널에서 이 옵션을 비활성화하거나 원격으로 관리할 수 있는 터미널을 추가하는 방법으로 변경할 수 있습니다.

사용자 *my_user* 를 사용하여 터미널 *my_terminal* 에 대한 관리 옵션을 컴퓨터 *my_machine* 에 추가하려면 selang 규칙을 다음과 같이 작성합니다.

er terminal *my_terminal* owner(nobody) defaccess(r)
auth terminal *my_terminal* xuid(*my_user*) access(all)

이 규칙을 사용하면 모든 사용자가 이 터미널에 로그인(CA Access Control 관리가 아닌 일반 로그인)할 수 있고, 엔터프라이즈 사용자 *my_uid* 가 컴퓨터에 로그인하여 CA Access Control 관리 도구(selang, CA Access Control 끝점 관리 등)를 사용할 수 있습니다.

참고: 관리자가 CA Access Control 끝점 관리를 사용하여 CA Access Control 을 관리하는 경우 CA Access Control 끝점 관리가 설치된 컴퓨터만 정의하면 됩니다. 관리자가 브라우저를 여는 컴퓨터를 정의할 필요는 없습니다.

설치 정보

CA Access Control 을 설치할 때(처음 설치 또는 업그레이드 설치) 다음 사항에 유의하십시오.

- *릴리스 정보*를 읽으십시오.

  이 설명서는 지원되는 플랫폼, 알려진 문제점, 고려 사항 및 기타 중요 정보에 대한 정보를 수록하고 있습니다. CA Access Control 을 설치하기 전에 *릴리스 정보*를 읽으십시오.

- 환경이 PMDB 계층으로 설정되었거나 설정하고자 하는 경우 다음 사항을 권장합니다.

  - 먼저 DMS(Deployment Map Server) 컴퓨터를 설치 또는 업그레이드하십시오.

    이 과정은 고급 정책 기반 관리를 사용하고자 하는 경우에만 필요하며, DMS 에서 각 정책 모델 노드와 그 구독자를 등록하도록 해줍니다.

  - 계층상의 하위부터 상위 순서로(구독자 먼저) 각 컴퓨터를 설치하거나 업그레이드하십시오.

    이전 버전의 구독자가 있는 PMDB 를 업그레이드하면 오류가 있는 명령이 전송될 수 있습니다. 이러한 문제는 이전 버전 PMDB 에 존재하지 않았던 클래스와 속성이 새 PMDB 에 있는 경우 발생할 수 있습니다.

    참고: 단일 컴퓨터에서 실행 중인 PMDB 계층은 동시에 업그레이드할 수 있습니다.

  - PMDB 또는 정책 업데이트 동안 업그레이드를 실시하지 *마십시오*.

  - 구독자와 PMDB 정책을 백업하십시오.

  참고: 이전 버전의 PMDB 는 이후 버전의 구독자를 포함할 수 있었습니다. 이전 버전의 명령이 이후 버전에서 지원되므로 이전 PMDB 를 CA Access Control r12 구독자에게 전파할 수 있습니다.

- r12.0 보다 오래된 버전에서 업그레이드하는 경우:
  - STOP 으로 바이패스해야 하는 프로그램은 이제 데이터베이스 규칙인 *stop* 유형의 SPECIALPGM 레코드로 정의됩니다.
  - SURROGATE 에 의해 바이패스되어야 하는 프로그램은 이제 데이터베이스 규칙인 *surrogate* 유형의 SPECIALPGM 레코드로 정의됩니다.

  참고: 업그레이드 프로세스를 거치면 파일에 보관된 이전 정의가 새 데이터베이스 규칙으로 변환됩니다. 이러한 새 규칙을 기존의 selang 스크립트에 추가합니다.
- 기존 seos.ini 및 pmd.ini 파일을 업그레이드하거나 새로 만들 수 있습니다.

  두 가지 방법 모두 설치 스크립트는 이전 seos.ini 파일 복사본을 seos_ini.back 으로, 각 pmd.ini 파일의 복사본을 pmd_ini.back 으로 각 정책 모델 디렉터리에 저장합니다.
- CA Access Control 은 업그레이드 중에 serevu.cfg, audit.cfg, trcfilter.init 및 sereport.cfg 와 같은 기존 파일을 백업합니다.

  이러한 파일의 변경 사항을 유지하려면 백업된 파일을 사용하십시오.
- 기존 데이터베이스를 업그레이드하는 경우 다음 사항을 권장합니다.
  - 데이터베이스를 먼저 백업합니다.

    dbmgr -b 를 사용하여 데이터베이스를 백업합니다.
  - *동기화* 모드에 구독자가 없는지 확인합니다.

    sepmd -L 을 사용하여 구독자의 상태를 확인합니다.
- Unicenter 보안 통합 및 마이그레이션은 AIX, HP-UX PA-RISC, Solaris SPARC 및 Linux x86 플랫폼에서만 가능합니다.

- UNIX 용 Unicenter TNG 및 CA Access Control

  Unicenter NSM 3.0 이전의 Unicenter TNG 버전이 설치되어 있는 경우 CA Access Control 에서 프로세스 정보를 받을 수 있도록 다음과 같은 Unicenter TNG 픽스를 설치해야 합니다.

  - Unicenter TNG 2.4 를 사용하는 HP-UX 사용자는 픽스 QO01182 를 설치하십시오.
  - Unicenter TNG 2.4 를 사용하는 Linux 사용자는 픽스 PTF LO91335 를 설치하십시오.
  - Unicenter TNG 2.4 를 사용하는 Sun 사용자는 픽스 QO00890 을 설치하십시오.

  참고: Unicenter NSM 3.0 을 실행하는 AIX 5.x 사용자는 CA Technologies Unicenter 지원부에 문의하여 호환 패치를 받으시기 바랍니다. CA Access Control 을 호스트에 설치하기 전에 이 호환 패치를 설치하십시오.

- Linux s390 에 Unicenter 관련 옵션(install_base 옵션: -uni 또는 -mfsd)을 설치하려면 CA Access Control 를 설치하기 전에 korn 쉘(ksh)이 설치되어 있어야 합니다.

  CCISA(CCI Standalone)의 설치 스크립트는 Linux 에 기본적으로 설치되지 않는 ksh 를 사용합니다.

- CA Access Control 32 비트 바이너리를 Linux x86 64 비트에 설치하려면 _LINUX_*xxx*.tar.Z 또는 CAeAC-*xxxx*-*y*.*y*.*iiii*.i386.rpm 설치 패키지를 사용하는 것이 좋습니다. 이러한 설치 패키지는 Linux x86 64 비트 시스템에 32 비트 CA Access Control 바이너리를 설치합니다. 업그레이드하는 경우 이러한 패키지는 이전에 설치된 32 비트 CA Access Control 버전과의 호환성을 유지합니다. CA Access Control 을 설치하기 전에 다음과 같은 운영 체제 32 비트 라이브러리가 설치되어 있는지 확인하십시오.

  ld-linux.so.2, libICE.so.6, libSM.so.6, libX11.so.6, libXext.so.6, libXp.so.6, libXt.so.6, libc.so.6, libcrypt.so.1, libdl.so.2, libgcc_s.so.1, libm.so.6, libncurses.so.5, libnsl.so.1, libpam.so.0, libpthread.so.0, libresolv.so.2, libstdc++.so.5, libaudit.so.0(RHEL5 및 OEL 5 이상 전용).

  다음은 필요한 관련 RPM 패키지의 목록입니다.

  - SLES 10: compat-libstdc++, glibc-32bit, libgcc, ncurses-32bit, pam-32bit, xorg-x11-libs-32bit
  - SLES 9: glibc-32bit, libgcc, libstdc++, ncurses-32bit, pam-32bit, XFree86-libs-32bit

- RHEL 5 and OEL 5: audit-libs, compat-libstdc++, glibc, libgcc, libICE, libSM, libXext, libXp, libXt, ncurses, pam
- RHEL 4 and OEL 4: compat-libstdc++, glibc, libgcc, ncurses, pam, xorg-x11-deprecated-libs, xorg-x11-libs
- RHEL 3: glibc, libgcc, libstdc++, ncurses, pam, XFree86-libs

- CA Access Control 64 비트 바이너리를 Linux x86 64 비트에 설치하려면 _LINUX_X64_*xxx*.tar.Z 또는 CAeAC-*xxxx*-*y*.*y*.*iiii*.x86_64.rpm 설치 패키지를 사용하십시오. 이러한 설치 패키지를 사용하면 다른 RPM 패키지를 추가로 설치할 필요가 없습니다.

  Linux x86 64 비트에서 CA Access Control 64 비트 바이너리를 설치 또는 업그레이드하는 경우 다음 사항에 주의하십시오.

  - 64 비트 설치 패키지는 selock 및 selogo 와 같은 CA Access Control GUI 유틸리티를 지원하지 않습니다.
  - install_base 스크립트가 32 비트 및 64 비트 tar 파일에 모두 액세스할 수 있는 경우, 기본적으로 install_base 스크립트는 32 비트 tar 파일을 사용합니다. 이러한 속성을 변경하려면 install_base 명령을 실행할 때 원하는 tar 파일을 지정하십시오. 64 비트 RPM 패키지를 설치하는 경우 64 비트 바이너리 및 라이브러리만 설치됩니다. 예:

    ./install_base_LINUX_X64_125.tar.Z
  - 빌드되어 API 에 연결된 모든 응용 프로그램은 64 비트 버전을 지원하도록 다시 빌드해야 합니다. 64 비트 API 샘플을 빌드하려면 LINUX64 target 을 사용하십시오. 이 target 은 D64BIT 및 -D64BITALL(-m32 는 제거됨)을 사용합니다. 라이브러리를 빌드하려면 -m elf_x86_64 가 필요합니다.
  - install_base 스크립트를 사용하여 32 비트 CA Access Control 버전에서 64 비트로 업그레이드하는 경우 설치 전에 -force_install 플래그를 설정하십시오. 이 플래그를 설정하지 않으면 설치가 실패합니다.
  - CA Access Control 제거 후에 cawin 을 완전히 제거하려면 rpm -e --allmatches 를 사용하여 제거 프로세스 중에 cawin 의 32 비트 및 64 비트 버전이 모두 제거되도록 하십시오.

- Linux s390x 64 비트에 CA Access Control 을 설치하려면 다음과 같은 운영 체제 32 비트 라이브러리가 설치되어 있어야 합니다.

  ld.so.1, libcrypt.so.1, libc.so.6, libdl.so.2, libICE.so.6, liblaus.so.1(SLES 8, RHEL 3), libaudit.so.0(RHEL 4, RHEL 5), libm.so.6, libnsl.so.1, libpam.so.0, libresolv.so.2, libSM.so.6, libX11.so.6, libXext.so.6, libXp.so.6, libXt.so.6

  다음 RPM 패키지가 필요합니다.

  - SLES 10: glibc-32bit, pam-32bit, xorg-x11-libs-32bit
  - SLES 9: XFree86-libs-32bit, glibc-32bit, pam-32bit
  - RHEL 5: audit-libs, libXp, glibc, libICE, libSM, libX11, libXext, libXt, pam
  - RHEL 4: audit-libs, glibc, pam, xorg-x11-deprecated-libs, xorg-x11-libs
  - RHEL 3: glibc, laus-libs, pam
- -all 옵션을 사용하여 Linux 및 Linux-IA64 플랫폼에 CA Access Control 을 설치하면 mfsd 가 설치되지 않습니다.
- Solaris 에 CA Access Control 을 설치하려면 SUNWlibc(Sun Workshop 컴파일러 번들 libC) 패키지를 설치하십시오.
- CA Access Control 32 비트 바이너리를 32 비트 또는 64 비트 Linux 컴퓨터에 설치하기 전에 libstdc++.so.5 32 비트 라이브러리가 설치되어 있는지 확인하십시오. 이 라이브러리를 설치하지 않으면 CA Access Control 설치 후 ReportAgent 데몬이 시작되지 않습니다.
- Linux 에 CA Access Control 을 설치하려면 먼저 환경의 홈 디렉터리를 지정하십시오.
- Solaris 8 에 CA Access Control 을 설치하기 전에 libCstd 라이브러리 수준이 1.2 이상인지 확인하십시오.
- 엔터프라이즈 관리 서버를 설치하기 전에 CA Access Control 끝점 커널이 언로드되고 시스템에 존재하지 않는지 확인하십시오.

Linux s390 끝점에 대한 설치 고려 사항

메시지 큐 기능을 사용하려는 경우 CA Access Control Linux s390 에서 UNAB 를 원격으로 관리하고 Linux IA64 에서 보고 기능을 사용하려면 끝점에 J2SE 버전 5.0 이상을 설치하십시오.

메시지 큐 기능을 사용하면 CA Access Control 끝점에서 보고서 포털 및 CA Enterprise Log Manager 로 각각 보고서와 감사 데이터를 보낼 수 있습니다. 원격 관리는 CA Access Control 엔터프라이즈 관리를 사용하여 UNAB 끝점을 관리할 수 있게 해줍니다.

끝점에 CA Access Control 또는 UNAB 를 설치하기 전 또는 이후에 J2SE 를 설치할 수 있습니다. CA Access Control 또는 UNAB 를 설치한 이후에 J2SE 를 설치하는 경우 또한 끝점에서 Java 위치를 구성해야 합니다.

설치가 Java 와 상호 작용하는 방법

Linux s390, Linux s390x, Linux IA64 에 해당

메시지 큐 기능을 사용하려면 경우 UNAB Linux s390 끝점을 원격으로 관리하고 Linux IA64 및 Linux s390 에서 보고 기능을 사용하려면 끝점에 지원되는 Java 버전을 설치하십시오.

Linux s390 또는 Linux IA64 끝점에 CA Access Control 또는 UNAB 를 설치할 때 설치는 다음을 수행합니다.

1. 올바른 Java 환경의 경로에 대해 다음 위치를 검사합니다.
   a. 설치 입력의 JAVA_HOME 매개 변수

      설치 입력은 UNAB 설치 매개 변수 파일, UNIX CA Access Control 설치 매개 변수 파일, 네이티브 설치를 위해 사용자 지정된 패키지, 대화형 CA Access Control 설치의 사용자 입력을 포함합니다.

   b. JAVA_HOME 환경 변수

   c. (Linux s390 및 Linux s390x) 기본 설치 경로: /opt/ibm/java2-s390-50/jre

2. accommon.ini 파일의 전역 설정에서 java_home 구성 설정의 값을 다음 값 중 하나로 설정합니다.
   - 설치가 올바른 환경에 대한 경로를 찾으면 구성 설정의 값을 이 경로로 설정합니다.
   - 설치가 올바른 환경에 대한 경로를 찾지 못하면 구성 설정의 값을 *ACSharedDir*/JavaStubs 로 설정합니다.

     기본적으로 *ACSharedDir* 는 /opt/CA/AccessControlShared 입니다.

Linux s390 및 Linux s390x 끝점에서 Java 위치 구성

Linux s390 및 Linux s390x 에 해당

메시지 큐 기능을 사용하고 원격으로 UNAB Linux s390 끝점을 관리하려면 끝점에 J2SE 버전 5.0 이상을 설치해야 합니다. CA Access Control 또는 UNAB 설치 후 J2SE 를 설치하는 경우 추가 구성 단계를 수행해야 합니다.

Linux s390 및 Linux s390x 끝점에서 Java 위치를 구성하려면

1. CA Access Control 과 UNAB 가 실행 중인 경우 중지합니다.
2. accommon.ini 파일의 전역 섹션에서 java_home 구성 설정의 값을 Java 설치 경로로 변경합니다.

   예: java_home=/opt/ibm/java2-s390-50/jre
3. CA Access Control 및 UNAB 를 시작합니다.

   Java 위치가 구성됩니다.

기본 설치

CA Access Control 은 지원되는 운영 체제에서 CA Access Control 을 기본 방식으로 설치 및 관리하기 위한 기본 패키지 형식을 제공합니다. 기본 패키지의 기본 패키지 관리 도구를 사용하면 CA Access Control 설치를 관리할 수 있습니다.

기본 패키지

CA Access Control 에는 지원되는 각 기본 설치 형식에 대한 기본 패키지가 포함되어 있습니다. 기본 패키지를 사용하면 기본 패키지 기능을 사용하여 CA Access Control 구성 요소를 설치, 업데이트 및 제거할 수 있습니다. 기본 패키지는 UNIX 용 CA Access Control 끝점 구성 요소 DVD 의 NativePackages 디렉터리에 있습니다.

다음은 패키지 및 관련 설명입니다.

ca-lic

(Linux 의 경우에만) 기타 모든 패키지의 사전 요구 사항인 CA Technologies 라이선스 프로그램을 설치합니다.

참고: Linux 용 RPM 형식으로만 사용할 수 있습니다.

CAeAC

핵심 CA Access Control 구성 요소를 설치합니다. 이것은 기본 CA Access Control 설치 패키지이며 이전에 별도 패키지로 제공된 서버, 클라이언트, 설명서, TNG 통합, API 및 mfsd 패키지를 모두 포함하고 있습니다.

참고: UNAB 패키지는 또한 CAWIN 공유 구성 요소를 설치합니다.

일부 기본 명령(예: RPM 을 사용하여 패키지 제거)을 수행하려면 패키지 이름을 알아야 합니다. 패키지 파일을 사용하여 패키지 이름을 확인하려면, 적절한 기본 패키지 명령을 입력하십시오. 예를 들어 RPM 패키지의 경우 다음을 입력합니다.

rpm -q -p *RPMPackage_filename*

기본 설치 관련 추가 고려 사항

기본 패키지를 사용하여 CA Access Control 을 설치하는 경우, 다음과 같은 추가 고려 사항에 유의하십시오.

- CA Access Control RPM 패키지를 설치하려면 라이선스 프로그램 패키지 ca-lic-01.0080 이상이 있어야 합니다.
- 사용자 지정 CA Access Control RPM 네이티브 설치 패키지(customize_eac_rpm)를 빌드하려면 컴퓨터에 rpmbuild 유틸리티가 있어야 합니다.

- 사용자 지정 CA Access Control AIX 기본 설치 패키지(customize_eac_bff)를 빌드하려면 컴퓨터에 bos.adt.insttools 를 설치해야 합니다.

  AIX 5.2 의 경우 bos.adt.insttools 의 버전은 5.2.0.75 이상이어야 합니다.

- AIX 네이티브 패키지는 bos.rte.install 5.2.0.75 를 사용하여 빌드되었습니다. 따라서 기본 패키지의 오류를 방지하기 위해 bos.rte.install 5.2.0.75 이상 버전을 사용하는 것이 좋습니다.

- HP-UX 네이티브 패키지는 설치 중 Perl 을 사용합니다.

- Solaris 기본 패키지는 /var/spool/pkg 와 같이 그룹 및 전체에 대한 읽기 액세스가 있는 공용 위치에 있어야 합니다.

- Solaris 기본 패키지 명령 pkgadd -R 은 CA Access Control 패키지에서 지원되지 않습니다.

  설치 디렉터리를 수정하려면 CA Access Control 패키지 사용자 지정 스크립트를 사용하십시오(customize_eac_pkg -i *install_loc*).

- HP-UX 네이티브 패키지의 현지화(로컬라이제이션)된 버전을 설치하려면 사용자 지정된 패키지에 사용하는 매개 변수 파일에 있는 LANG 설정에 대한 값을 *반드시* 설정해야 합니다.

  참고: 매개 변수 파일은 이미 LANG 설정을 포함하고 있습니다. 이 값을 설정하려면 앞의 주석 문자(#)와 공백을 제거한 다음 값을 입력하십시오. OS 에서 지원하는 인코딩 값은 locale -a 명령을 사용하여 찾을 수 있습니다.

CA Access Control 이 암호로 보호되는 루트 인증서를 사용하도록 지정하는 방법

CA Access Control 을 설치할 때 타사 암호로 보호된 루트 인증서를 사용하도록 구성할 수 있습니다.

CA Access Control 을 설치한 후 루트 인증서를 사용하여 CA Access Control 서버 인증서를 만들 수 있습니다. 서버 인증서는 CA Access Control 구성 요소 사이의 통신을 암호화하고 인증합니다.

타사 암호로 보호된 루트 인증서를 사용하도록 CA Access Control 을 구성하려면 네이티브 패키지를 사용하여 CA Access Control 을 설치할 때 다음과 같이 일부 추가 단계를 수행해야 합니다.

1. 네이티브 패키지 설치의 일부로서 매개 변수 파일을 사용자 지정할 때 파일에 다음과 같은 매개 변수를 지정합니다.
   - ENCRYPTION_METHOD_SET=2
   - ROOT_CERT_PATH=*root_cert_path*
   - ROOT_CERT_KEY=*root_key_path*
2. CA Access Control 설치 후 다음을 수행합니다.
   a. 다음과 같이 루트 인증서에서 CA Access Control 서버 인증서를 만듭니다. 여기서 *ACInstallDir* 는 CA Access Control 을 설치한 디렉터리입니다.

      ACInstallDir/bin/sechkey -e -sub -in /opt/CA/AccessControl/crypto/sub_cert_info -priv *root_key_path* -capwd *password* [-subpwd *password*]

      -priv *root_key_path*

      루트 인증서에 대한 개인 키를 포함하는 파일을 지정합니다.

      -ca *password*

      루트 인증서의 개인 키에 대한 암호를 지정합니다.

      -subpwd *password*

      서버 인증서의 개인 키에 대한 암호를 지정합니다.

   b. 서버 키에 대한 암호를 지정한 경우 CA Access Control 이 저장된 암호를 사용하여 키를 열 수 있는지 확인합니다.

      ACInstallDir/bin/sechkey -g -verify

c. crypto 섹션에 있는 communication_mode 구성 설정을 다음 중 하나로 변경하십시오.

all_modes

대칭 및 SSL 암호화를 모두 사용하려면 이 값을 지정하십시오. 이 값은 컴퓨터가 모든 CA Access Control 구성 요소와 통신하도록 만듭니다.

use_ssl

SSL 암호화만 사용하려면 이 값을 지정하십시오. 이 값은 컴퓨터가 SSL 암호화를 사용하는 CA Access Control 구성 요소와만 통신하도록 합니다.

d. CA Access Control 을 시작하고

CA Access Control 이 시작되고 CA Access Control 서버 인증서를 사용하여 통신을 암호화하고 인증합니다.

참고: sechkey 유틸리티에 대한 자세한 내용은 *참조 안내서*를 참조하십시오.

CA Access Control 이 타사 암호로 보호된 서버 인증서를 사용하도록 지정하는 방법

CA Access Control 구성 요소 사이의 통신을 암호화하고 인증하기 위해 타사 암호로 보호된 서버 인증서를 사용할 수 있습니다.

타사 암호로 보호된 서버 인증서를 사용하도록 CA Access Control 을 구성하려면 네이티브 패키지를 사용하여 CA Access Control 을 설치할 때 다음과 같이 일부 추가 단계를 수행해야 합니다.

1. 네이티브 패키지 설치의 일부로서 매개 변수 파일을 사용자 지정할 때 파일에 다음과 같은 매개 변수를 지정합니다.
   - ENCRYPTION_METHOD_SET=2
   - ROOT_CERT_PATH=*root_cert_path*
   - ROOT_CERT_KEY=*root_key_path*
   - PROVIDE_OR_GEN_CERT=2
   - SUBJECT_CERT_PATH=*server_cert_path*
   - SUBJECT_KEY_PATH=*subject_key_path*

2. CA Access Control 설치 후 다음을 수행합니다.

   a. 다음과 같이 컴퓨터의 개인 키에 대한 암호를 저장합니다. 여기서 *ACInstallDir* 는 CA Access Control 을 설치한 디렉터리입니다.

      ACInstallDir/bin/sechkey -g -subpwd *password*

      -subpwd *password*

      서버 인증서의 개인 키에 대한 암호를 지정합니다.

   b. CA Access Control 이 저장된 암호를 사용하여 키를 열 수 있는지 확인합니다.

      ACInstallDir/bin/sechkey -g -verify

   c. crypto 섹션에 있는 communication_mode 구성 설정을 다음 중 하나로 변경하십시오.

      all_modes

      대칭 및 SSL 암호화를 모두 사용하려면 이 값을 지정하십시오. 이 값은 컴퓨터가 모든 CA Access Control 구성 요소와 통신하도록 만듭니다.

      use_ssl

      SSL 암호화만 사용하려면 이 값을 지정하십시오. 이 값은 컴퓨터가 SSL 암호화를 사용하는 CA Access Control 구성 요소와만 통신하도록 합니다.

   d. CA Access Control 을 시작하고

      CA Access Control 이 시작되고 타사 암호로 보호된 서버 인증서를 사용하여 통신을 암호화하고 인증합니다.

참고: sechkey 유틸리티에 대한 자세한 내용은 *참조 안내서*를 참조하십시오.

RPM 패키지 관리자 설치

RPM 패키지 관리자(RPM)는 개별 소프트웨어 패키지를 빌드, 설치, 쿼리, 확인, 업데이트 및 삭제할 수 있는 명령줄 유틸리티입니다. RPM 은 UNIX 플랫폼에서 사용할 수 있습니다.

참고: 자세한 내용은 RPM 패키지 관리자 웹 사이트(http://www.rpm.org) 와 RPM 용 UNIX man 페이지를 참조하십시오.

일반 설치 대신 CA Access Control 에서 제공하는 RPM 패키지를 사용할 수 있습니다. 이 패키지를 사용하면 CA Access Control 설치와 함께 RPM 을 사용하여 수행된 다른 모든 소프트웨어 설치를 관리할 수 있습니다.

RPM 데이터베이스에서 기존 RPM 패키지 제거

직접 작성한 CA Access Control RPM 패키지를 이미 설치한 경우, RPM 데이터베이스에서 이 패키지를 제거해야 설치한 패키지가 데이터베이스에 반영됩니다. 기존 패키지를 제거하지 않고 새 패키지를 설치하면 RPM 데이터베이스에는 이전 패키지와 새 패키지가 모두 설치된 것으로 표시되지만 파일 시스템에서는 새 패키지의 파일이 기존 파일을 덮어씁니다. RPM 에서 패키지를 업그레이드하려면 패키지의 이름이 현재 설치된 패키지와 같아야 합니다.

참고: 패키지를 제거한다고 해서 CA Access Control 파일이 제거되지는 않으며, 기본 패키지 설치가 업그레이드를 실행합니다.

RPM 데이터베이스에서 패키지를 제거하려면 다음 명령을 사용합니다.

rpm -e --justdb *your_ACPackageName*

CA Access Control RPM 패키지 사용자 지정

네이티브 패키지를 사용하여 CA Access Control 을 설치하기 전에 사용권 계약에 동의하도록 지정하기 위해 CA Access Control 패키지를 사용자 지정해야 합니다. 또한 패키지를 사용자 지정할 때는 사용자 지정 설치 설정도 지정해야 합니다.

패키지에서 설치 매개 변수 파일을 추출하여 필요한 대로 수정한 다음 패키지로 다시 로드하는 방법으로 패키지를 사용자 지정합니다. 일부 명령은 사용자 지정된 스크립트에서 사용할 수 있으므로 매개 변수 파일을 수정할 필요는 없습니다.

참고: 사용자가 수동으로 패키지를 수정하는 것은 *권장되지 않습니다*. 대신 다음 절차에 설명된 스크립트를 사용하여 CA Access Control 패키지를 사용자 지정하십시오.

지원되는 각 Linux 운영 체제용 RPM 패키지는 UNIX 용 CA Access Control 끝점 구성 요소 DVD 의 NativePackages/RPMPackages 디렉터리에서 찾을 수 있습니다.

CA Access Control RPM 패키지를 사용자 지정하려면

1. 사용자 지정할 패키지를 파일 시스템의 임시 위치로 복사합니다.

   OS 는 사용하는 운영 체제의 해당 하위 디렉터리 이름입니다.

   파일 시스템의 읽기/쓰기가 가능한 위치에서 패키지를 필요한 대로 사용자 지정할 수 있습니다.

2. 파일 시스템의 임시 위치로 customize_eac_rpm 스크립트 파일과 pre.tar 파일을 복사합니다.

   pre.tar 파일은 설치 메시지와 CA Access Control 사용권 계약이 수록된 압축 tar 파일입니다.

   참고: customize_eac_rpm 스크립트 파일과 pre.tar 파일은 네이티브 패키지가 있는 위치에 있습니다.

3. 사용권 계약을 표시합니다.

   customize_eac_rpm -a [-d *pkg_location*] *pkg_filename*

4. 사용권 계약의 끝에서 대괄호 안에 표시된 키워드를 적어 둡니다.

   다음 단계에서 이 키워드를 지정합니다.

5. 사용권 계약에 동의하도록 지정하기 위해 CA Access Control 패키지를 사용자 지정합니다.

   customize_eac_rpm -w *keyword* [-d *pkg_location*] *pkg_filename*

6. (선택 사항) 설치 매개 변수 파일의 언어를 설정합니다.

   customize_eac_rpm -r -l *lang* [-d *pkg_location*] *pkg_filename*

7. (선택 사항) eTrust Access Control r8 SP1 패키지에서 업그레이드합니다.

   customize_eac_rpm -u *install_prefix* [-d *pkg_location*] *pkg_filename*

8. (선택 사항) 기본 암호화 파일을 변경합니다.

   customize_eac_rpm -s -c *certfile* -k *keyfile* [-d *pkg_location*] *pkg_filename*

9. (선택 사항) 설치 매개 변수 파일을 가져옵니다.

   customize_eac_rpm -g -f *tmp_params* [-d *pkg_location*] *pkg_filename*

10. (선택 사항) 설치 요구 사항에 맞게 설치 매개 변수 파일을 편집합니다.

    이 파일에서 패키지에 대한 설치 기본 설정을 지정할 수 있습니다. 예를 들어 POSTEXIT 설정을 활성화하고(앞의 # 기호를 제거) 실행할 설치 후 스크립트 파일을 지정합니다.

11. (선택 사항) 사용자 지정된 패키지에 설치 매개 변수를 설정합니다.

    customize_eac_rpm -s -f *tmp_params* [-d *pkg_location*] *pkg_filename*

    이제 이 패키지를 사용하여 사용자 지정된 기본 설정으로 CA Access Control 을 설치할 수 있습니다.

예: 사용권 계약에 동의하도록 지정

네이티브 패키지를 설치할 때 사용권 계약에 동의하려면 패키지를 사용자 정의해야 합니다. 다음 예는 UNIX 용 CA Access Control 끝점 구성 요소 DVD(/mnt/AC_DVD 에 마운트)에 있는 x86 CA Access Control RPM 패키지를 사용자 지정하여 사용권 계약에 동의하도록 지정하는 방법을 설명합니다.

cp /mnt/AC_DVD/NativePackages/RPMPackages/LINUX/CAeAC*i386.rpm /tmp
cp /mnt/AC_DVD/NativePackages/RPMPackages/pre.tar /tmp
chmod 777 /tmp/CAeAC*i386.rpm
/mnt/AC_DVD/NativePackages/RPMPackages/customize_eac_rpm -w *keyword* -d /tmp CAeAC*i386.rpm

이제 /tmp 디렉터리에 있는 사용자 지정된 패키지를 사용하여 CA Access Control 을 설치할 수 있습니다.

추가 정보:

customize_eac_rpm 명령 - RPM 패키지 사용자 지정 (페이지 198)

CA Access Control RPM 패키지 설치

다른 모든 소프트웨어 설치와 함께 CA Access Control 설치를 관리하려면 사용자 지정된 CA Access Control RPM 패키지를 설치하십시오.

중요! 사용권 계약에 동의함을 나타내기 위해 사용권 계약 내에서 찾을 수 있는 키워드를 사용하여 패키지를 사용자 지정해야 합니다.

참고: 사용하는 실제 명령은 업그레이드 설치 또는 최초 설치 여부, 기본 디렉터리에 설치 여부 등의 여러 변수에 따라 차이가 있습니다. 이 단원에서 일부 명령 예제가 제공됩니다.

CA Access Control RPM 패키지를 설치하려면

1. rpm 명령을 사용하여 ca-lic 패키지를 설치합니다.

   라이선스 프로그램이 설치됩니다.

2. CAeAC 패키지를 사용자 지정 (페이지 194)합니다.

   사용권 계약에 동의함을 나타내기 위해 사용권 계약 내에서 찾을 수 있는 키워드를 사용하여 패키지를 사용자 지정해야 합니다. 사용자 지정 설치 설정을 지정하기 위해 패키지를 사용자 지정할 수도 있습니다.

   참고: CA Access Control 을 업그레이드하는 경우 사용권 계약에 동의하도록 지정하기 위해 패키지를 사용자 지정할 필요가 없습니다.

3. rpm 명령을 사용하여 CAeAC 패키지를 설치합니다.

   CA Access Control 이 설치됩니다.

   참고: UNAB 패키지는 또한 CAWIN 공유 구성 요소를 설치합니다.

   중요! 기존 CA Access Control 패키지를 업그레이드하는 경우 새 패키지의 설치를 시도하기 전에 SEOS syscall 을 언로드하십시오. 그렇지 않으면 설치가 실패합니다.

예제: Red Hat Linux 에서 CA Access Control 설치 또는 업그레이드

다음 예제에서는 UNIX 용 CA Access Control 끝점 구성 요소 DVD(/mnt/AC_DVD 에 마운트)에서 찾을 수 있는 CA Access Control 패키지를 Red Hat Linux x86 ES 4.0 컴퓨터에 설치하는 방법을 보여 줍니다. 이 설치는 CA Access Control 을 처음 설치하거나 기존에 설치된 패키지를 먼저 제거하지 않고 CA Access Control RPM 패키지를 업그레이드하는 경우입니다. 이렇게 하려면 라이선스 프로그램 패키지를 설치한 다음 CA Access Control 패키지를 사용자 지정하여 라이선스 계약에 동의하고 다음과 같이 설치하십시오.

```
cd /mnt/AC_DVD/NativePackages/RPMPackages/LINUX
rpm -U ca-lic*i386.rpm ca-cs-cawin*i386.rpm
cp CAeAC*i386.rpm /tmp
cp ../pre.tar /tmp
chmod 777 /tmp/CAeAC*i386.rpm
../customize_eac_rpm -w keyword -d /tmp CAeAC*i386.rpm
rpm -U /tmp/CAeAC*i386.rpm
```

예: eTrust Access Control r8 SP1 패키지 설치에서 업그레이드

다음 예는 Linux s390 SLES 9 컴퓨터에서 /opt/CA/eTrustAccessControl 에 설치된 eTrust Access Control r8 SP1 패키지를 UNIX 용 CA Access Control 끝점 구성 요소 DVD(/mnt/AC_DVD 에 마운트)에 있는 CA Access Control 패키지로 업그레이드하는 방법을 보여 줍니다. 이렇게 하려면 다음과 같이 라이선스 프로그램 패키지, CAWIN 패키지, 사용자 지정 CA Access Control 패키지를 순서대로 설치하십시오.

```
cd /mnt/AC_DVD/NativePackages/RPMPackages/LINUX390
rpm -U ca-lic*rpm ca-cs-cawin*rpm
cp -R CAeAC*s390.rpm /tmp
cp ../pre.tar /tmp
chmod 777 /tmp/CAeAC*s390.rpm
../customize_eac_rpm -u /opt/CA  -d /tmp CAeAC*s390.rpm
../customize_eac_rpm -w keyword -d /tmp CAeAC*s390.rpm
rpm -U /tmp/CAeAC*s390.rpm
```

예제: 사용자 지정 디렉터리에 CA Access Control 및 사전 요구 사항 설치

다음 예제에서는 UNIX 용 CA Access Control 끝점 구성 요소 DVD(/mnt/AC_DVD 에 마운트)에서 찾을 수 있는 기본 CA Access Control 및 필수 패키지를 Red Hat Linux Itanium IA64 ES 4.0 의 사용자 지정 디렉터리에 설치하는 방법을 보여 줍니다. 이렇게 하려면 다음 명령을 사용하십시오.

```
cd /mnt/AC_DVD/NativePackages/RPMPackages/LINUX_IA64
rpm -U --prefix /usr/CA/shared ca-lic*ia64.rpm
cp -R CAeAC*ia64.rpm /tmp
cp ../pre.tar /tmp
chmod 777 /tmp/CAeAC*ia64.rpm
../customize_eac_rpm -u /usr/CA  -d /tmp CAeAC*ia64.rpm
../customize_eac_rpm -w keyword -d /tmp CAeAC*ia64.rpm
rpm -U --prefix /usr/CA /tmp/CAeAC*ia64.rpm
```

CA Access Control 은 제공한 사용자 지정 디렉터리와 제품 이름(Access Control)이 결합된 사용자 지정 디렉터리 /usr/CA/AccessControl 에 설치됩니다.

참고: 환경에 $CASHCOMP 변수가 정의(/etc/profile.CA 에 정의 가능)되지 않은 경우에만 라이선스 프로그램이 지정된 디렉터리에 설치됩니다. 그렇지 않으면 라이선스 프로그램은 $CASHCOMP 에 설치됩니다. $CASHCOMP 가 정의되지 않았고 -lic_dir 을 지정하지 않은 경우 라이선스 프로그램은 /opt/CA/SharedComponents 디렉터리에 설치됩니다.

추가 정보:

기본 설치 관련 추가 고려 사항 (페이지 188)
CA Access Control RPM 패키지 사용자 지정 (페이지 194)
customize_eac_rpm 명령 - RPM 패키지 사용자 지정 (페이지 198)

customize_eac_rpm 명령 - RPM 패키지 사용자 지정

customize_eac_rpm 명령은 CA Access Control RPM 패키지 사용자 지정 스크립트를 실행합니다.

이 명령을 사용할 때는 다음 사항을 고려해야 합니다.

- 스크립트는 CA Access Control RPM 패키지에서만 작동합니다.

  참고: 이 스크립트는 라이선스 프로그램 패키지에서 사용되도록 의도되지 않았습니다.
- 패키지를 사용자 지정하려면 패키지가 파일 시스템의 읽기/쓰기 가능한 디렉터리에 있어야 합니다.

이 명령의 형식은 다음과 같습니다.

customize_eac_rpm -h [-l]
customize_eac_rpm -a [-d *pkg_location*] *pkg_filename*
customize_eac_rpm -w *keyword* [-d *pkg_location*] *pkg_filename*
customize_eac_rpm -r [-d *pkg_location*] [-l *lang*] *pkg_filename*
customize_eac_rpm -s [-f *tmp_params*] | -c *certfile* | -k *keyfile*} [-d *pkg_location*] *pkg_filename*
customize_eac_rpm -g [-f *tmp_params*] [-d *pkg_location*] *pkg_filename*
customize_eac_rpm -u *install_prefix* [-d *pkg_location*] *pkg_filename*
customize_eac_rpm -t *tmp_dir* [-d *pkg_location*] *pkg_filename*

pkg_filename

사용자 지정할 CA Access Control 패키지의 파일 이름을 정의합니다.

참고: -d 옵션을 지정하지 않으면 패키지 파일의 전체 경로 이름을 정의해야 합니다.

-a

사용권 계약을 표시합니다.

-c *certfile*

루트 인증서 파일의 전체 경로 이름을 정의합니다.

참고: 이 옵션은 CAeAC 패키지에만 적용됩니다.

-d *pkg_location*

(선택 사항) 패키지가 들어 있는 파일 시스템의 디렉터리를 지정합니다. 패키지가 있는 디렉터리를 지정하지 않으면 스크립트는 패키지 파일의 전체 경로 이름을 *pkg_filename* 으로 가정합니다.

-f *tmp_params*

정보를 가져오거나 작성하려는 설치 매개 변수 파일의 전체 경로 및 이름을 지정합니다.

참고: -g 옵션을 사용할 때 파일을 지정하지 않으면 설치 매개 변수는 표준 출력(stdout)으로 전달됩니다.

-g

설치 매개 변수 파일을 가져와 -f 옵션에서 지정된 파일에 출력합니다.

-h

명령 사용법을 표시합니다. -l 옵션과 함께 사용하면 지원되는 언어의 언어 코드를 표시합니다.

-k *keyfile*

루트 개인 키 파일의 전체 경로 이름을 정의합니다.

참고: 이 옵션은 CAeAC 패키지에만 적용됩니다.

-l *lang*

설치 매개 변수 파일의 언어를 *lang* 으로 설정합니다. 언어를 설정할 때는 -r 옵션을 함께 사용해야 합니다.

참고: 지정할 수 있는 지원되는 언어 코드에 대한 목록을 보려면 -h 옵션을 사용하여 -l 을 실행하십시오. 기본적으로 설치 매개 변수 파일은 영어로 되어 있습니다.

-r

원래 패키지에 사용된 기본값을 사용하도록 패키지를 다시 설정합니다.

-s

지정된 패키지가 -f 옵션으로 지정한 사용자 지정된 설치 매개 변수 파일에서 가져온 입력을 사용하도록 설정합니다.

-t *tmp_dir*

설치 작업을 위한 임시 디렉터리를 설정합니다.

참고: 기본 임시 디렉터리는 /tmp 입니다.

-u *install_prefix*

eTrust Access Control r8 SP1 패키지가 설치되어 있는 위치의 접두사를 정의합니다. 실제 설치 위치는 이 접두사와 제품 이름을 연결한 곳입니다. r8 SP1 패키지는 제품 이름에 eTrust 가 포함되어 있었고 따라서 eTrustAccessControl 하위 디렉터리에 설치되었습니다. 최신 버전은 AccessControl 하위 디렉터리에 설치됩니다.

예를 들어, r8 SP1 이 /opt/CA/eTrustAccessControl 에 설치되어 있고 r12.0 SP1 로 업그레이드하려는 경우 rpm 명령을 사용하여 패키지를 설치하기 전에 다음을 입력하십시오.

```
./customize_eac_rpm -u /opt/CA  -d . CAeAC-1200-0.1106.i386.rpm
```

-w keyword

사용자가 사용권 계약을 수락함을 지정하는 키워드를 정의합니다. 이 키워드는 사용권 계약 끝부분에서 대괄호 안에 표시됩니다. 사용권 계약서 파일을 찾으려면 -a 옵션을 사용하십시오.

RPM 패키지 제거

CA Access Control RPM 패키지를 제거하려면 설치 순서와 반대로 CA Access Control 패키지를 제거해야 합니다.

RPM 패키지를 제거하려면 다음 명령을 실행하십시오.

rpm -e *CAeACPackage_name*

Solaris 네이티브 패키지 설치

Solaris 네이티브 패키지는 개별 소프트웨어 패키지를 만들고, 설치하고, 제거하고, 보고할 수 있는 명령줄 유틸리티로서 제공됩니다.

참고: Solaris 네이티브 패키지에 대한 자세한 내용은 Sun Microsystems 웹 사이트와 pkgadd, pkgrm, pkginfo 및 pkgchk 용 man 페이지를 참조하십시오.

일반 설치 대신 CA Access Control 에서 제공하는 Solaris 네이티브 패키지를 사용할 수 있습니다. 이 패키지를 사용하면 CA Access Control 설치와 함께 Solaris 네이티브 패키지를 사용하여 수행된 다른 모든 소프트웨어 설치를 관리할 수 있습니다.

중요! 패키지 설치 후 CA Access Control 을 제거하려면 *pkgrm* 명령을 사용해야 합니다. uninstall_AC 스크립트를 사용하지 마십시오.

Solaris 네이티브 패키지 사용자 지정

네이티브 패키지를 사용하여 CA Access Control 을 설치하기 전에 사용권 계약에 동의하도록 지정하기 위해 CA Access Control 패키지를 사용자 지정해야 합니다. 또한 패키지를 사용자 지정할 때는 사용자 지정 설치 설정도 지정해야 합니다.

패키지에서 설치 매개 변수 파일을 추출하여 필요한 대로 수정한 다음 패키지로 다시 로드하는 방법으로 패키지를 사용자 지정합니다. 일부 명령은 사용자 지정된 스크립트에서 사용할 수 있으므로 매개 변수 파일을 수정할 필요는 없습니다.

참고: 수동으로 패키지를 수정하는 것은 권장되지 않습니다. 대신 다음 절차에 설명된 스크립트를 사용하여 CA Access Control 패키지를 사용자 지정하십시오.

지원되는 각 Solaris 운영 체제용 Solaris 네이티브 패키지는 CA Access Control UNIX 용 끝점 구성 요소 DVD 의 NativePackages 디렉터리에서 찾을 수 있습니다.

Solaris 네이티브 패키지를 사용자 지정하려면

1. 사용자 지정할 패키지를 파일 시스템의 임시 위치로 추출합니다.

   파일 시스템의 읽기/쓰기가 가능한 위치에서 패키지를 필요한 대로 사용자 지정할 수 있습니다.

   중요! 패키지를 추출할 때는 패키지의 전체 디렉터리 구조에 대한 파일 특성이 그대로 보존되어야 합니다. 그렇지 않으면 Solaris 네이티브 패키지 도구에서 패키지가 손상된 것으로 간주합니다.

2. (선택 사항) 파일 시스템의 임시 위치로 customize_eac_pkg 스크립트 파일과 pre.tar 파일을 복사하십시오.

   pre.tar 파일은 설치 메시지와 CA Access Control 사용권 계약이 수록된 압축 tar 파일입니다.

   참고: customize_eac_pkg 스크립트 파일과 pre.tar 파일은 네이티브 패키지가 들어 있는 위치에 있습니다.

3. 사용권 계약을 표시합니다.

   customize_eac_pkg -a [-d *pkg_location*] *pkg_name*

4. 사용권 계약의 끝에서 대괄호 안에 표시된 키워드를 적어 둡니다.

   다음 단계에서 이 키워드를 지정합니다.

5. 사용권 계약에 동의하도록 지정하기 위해 CA Access Control 패키지를 사용자 지정합니다.

   customize_eac_pkg -w *keyword* [-d *pkg_location*] [*pkg_name*]

6. (선택 사항) 설치 매개 변수 파일의 언어를 설정합니다.

   customize_eac_pkg -r -l *lang* [-d *pkg_location*] [*pkg_name*]

7. (선택 사항) 설치 디렉터리를 변경합니다.

   customize_eac_pkg -i *install_loc* [-d *pkg_location*] [*pkg_name*]

8. (선택 사항) 기본 암호화 파일을 변경합니다.

   customize_eac_pkg -s -c *certfile* -k *keyfile* [-d *pkg_location*] [*pkg_name*]

9. (선택 사항) 설치 매개 변수 파일을 가져옵니다.

   customize_eac_pkg -g -f *tmp_params* [-d *pkg_location*] [*pkg_name*]

10. (선택 사항) 설치 요구 사항에 맞게 설치 매개 변수 파일을 편집합니다.

    이 파일에서 패키지에 대한 설치 기본 설정을 지정할 수 있습니다. 예를 들어 POSTEXIT 설정을 활성화하고(앞의 # 기호를 제거) 실행할 설치 후 스크립트 파일을 지정합니다.

11. (선택 사항) 사용자 지정된 패키지에 설치 매개 변수를 설정합니다.

    customize_eac_pkg -s -f *tmp_params* [-d *pkg_location*] [*pkg_name*]

    이제 이 패키지를 사용하여 사용자 지정된 기본 설정으로 CA Access Control 을 설치할 수 있습니다.

예: 사용권 계약에 동의하도록 지정

네이티브 패키지를 설치할 때 사용권 계약에 동의하려면 패키지를 사용자 정의해야 합니다. 다음 예는 UNIX 용 CA Access Control 끝점 구성 요소 DVD(/mnt/AC_DVD 에 마운트)에 있는 x86 CA Access Control Solaris 패키지를 사용자 지정하여 사용권 계약에 동의하도록 지정하는 방법을 설명합니다.

```
cp /mnt/AC_DVD/NativePackages/_SOLARIS_X86_PKG*.tar.Z /tmp
cp /mnt/AC_DVD/NativePackages/pre.tar /tmp
cd /tmp
zcat _SOLARIS_X86_PKG*.tar.Z | tar -xvf -
/mnt/AC_DVD/NativePackages/customize_eac_pkg -w keyword -d /tmp CAeAC
```

이제 /tmp 디렉터리에 있는 사용자 지정된 패키지를 사용하여 CA Access Control 을 설치할 수 있습니다.

추가 정보:

customize_eac_pkg 명령—Solaris 기본 패키지 사용자 지정 (페이지 208)

Solaris 네이티브 패키지 설치

다른 모든 소프트웨어 설치와 함께 CA Access Control 설치를 관리하려면 CA Access Control Solaris 네이티브 패키지를 설치하십시오. CA Access Control Solaris 네이티브 패키지를 사용하면 간편하게 Solaris 에 CA Access Control 을 설치할 수 있습니다.

중요! 사용권 계약에 동의함을 나타내기 위해 사용권 계약 내에서 찾을 수 있는 키워드를 사용하여 패키지를 사용자 지정해야 합니다.

CA Access Control Solaris 네이티브 패키지를 설치하려면

1. (선택 사항) Solaris 기본 설치 기본값을 구성합니다.
   a. 현재 위치로 설치 관리 파일 복사본을 가져옵니다.

      convert_eac_pkg -p

      설치 관리 파일이 현재 위치에 *myadmin* 이라는 이름으로 복사됩니다.

      설치 관리 파일을 편집하여 pkgadd 설치 기본값을 변경할 수 있습니다. 그런 다음 pkgadd -a 옵션을 사용하여 CA Access Control 과 같은 특정 설치에 대해 수정된 파일을 사용할 수 있습니다. 단, 이 파일이 CA Access Control 에 한정되는 것은 아닙니다.

      중요! 이전 CA Access Control 릴리스에서 기존 Solaris 패키지 설치를 업그레이드하려면 이 단계를 실행해야 합니다.

   b. 설치 관리 파일(myadmin)을 원하는 대로 편집한 다음 파일을 저장합니다.

      이제 다른 설치에 영향을 주지 않고 CA Access Control 네이티브 설치에 대한 수정된 구성 설정을 사용할 수 있습니다.

   참고: Solaris 기본 패키지에는 기본적으로 사용자 상호 작용이 필요할 수 있습니다. 설치 관리 파일과 그 사용 방법에 대한 자세한 내용은 pkgadd(1M) 및 admin(4)용 Solaris man 페이지를 참조하십시오.

2. CAeAC 패키지를 사용자 지정 (페이지 202)합니다.

   사용권 계약에 동의함을 나타내기 위해 사용권 계약 내에서 찾을 수 있는 키워드를 사용하여 패키지를 사용자 지정해야 합니다. 사용자 지정 설치 설정을 지정하기 위해 패키지를 사용자 지정할 수도 있습니다.

3. 패키지를 설치합니다.

   pkgadd [-a *dir*/myadmin] -d *pkg_location* CAeAC

-a *dir*/myadmin

1 단계에서 작성한 myadmin 설치 관리 파일의 위치를 정의합니다.

이 옵션을 지정하지 않으면, pkgadd 가 기본 설치 관리 파일을 사용합니다.

pkg_location

CA Access Control 패키지(CAeAC)가 있는 디렉터리를 정의합니다.

중요! 이 패키지는 공용 위치(즉, 그룹 및 전체에 대한 읽기 액세스)에 있어야 합니다. 예를 들어 /var/spool/pkg 와 같은 위치에 있어야 합니다.

참고: Solaris 네이티브 패키지는 UNIX 용 CA Access Control 끝점 구성 요소 DVD 의 NativePackages 디렉터리에 있습니다.

이제 CA Access Control 이 완전히 설치되었지만 아직 시작되지 않았습니다.

추가 정보:

기본 설치 관련 추가 고려 사항 (페이지 188)
선택한 영역에 Solaris 네이티브 패키지 설치 (페이지 206)
Solaris 네이티브 패키지 사용자 지정 (페이지 202)
customize_eac_pkg 명령—Solaris 기본 패키지 사용자 지정 (페이지 208)
convert_eac_pkg - Solaris 네이티브 설치 구성 (페이지 210)

선택한 영역에 Solaris 네이티브 패키지 설치

Solaris 네이티브 패키지를 사용하여 선택한 영역에 CA Access Control 을 설치할 수 있습니다. 하지만 글로벌 영역에도 CA Access Control 를 설치해야 합니다.

참고: Solaris 네이티브 패키지를 사용하여 *모든* 영역에 CA Access Control 를 설치하는 것이 좋습니다.

선택한 영역에 CA Access Control 을 설치하려면

중요! 모든 영역에서 동일한 CA Access Control 버전을 사용해야 합니다.

1. 글로벌 영역에서 아래 명령을 실행하여 CA Access Control 를 설치합니다.

   pkgadd -G -d *pkg_location* CAeAC

   pkg_location

   사용자 지정된 CA Access Control 패키지(CAeAC)가 있는 디렉터리를 정의합니다.

   중요! 이 패키지는 공용 위치(즉, 그룹 및 전체에 대한 읽기 액세스)에 있어야 합니다. 예를 들어 /var/spool/pkg 와 같은 위치에 있어야 합니다.

   이 명령은 글로벌 영역에만 CA Access Control 를 설치합니다.

2. 글로벌 영역에서 SEOS_load 명령을 입력하여 CA Access Control 커널 모듈을 로드합니다.

   참고: CA Access Control 커널이 로드되어도 CA Access Control 가 글로벌 영역의 이벤트를 차단하지는 않습니다.

3. CA Access Control 을 설치하려는 전역 영역 이외의 각 영역에서

   a. CAeAC 패키지를 전역 영역 이외의 영역 내 임시 위치에 복사합니다.

   b. 전역 영역 이외의 영역에서 다음 명령을 실행합니다.

      pkgadd -G -d *pkg_location* CAeAC

      이 명령을 실행하면 이전 단계에서 복사한 패키지를 사용하여 작업 중인 전역 영역 이외의 영역에 CA Access Control 을 설치합니다.

   이제 내부 영역에서 CA Access Control 를 시작할 수 있습니다.

참고: CA Access Control 를 제거할 때는 글로벌 이외 영역에서 먼저 제거한 후 글로벌 영역에서 제거해야 합니다.

customize_eac_pkg 명령—Solaris 기본 패키지 사용자 지정

customize_eac_pkg 명령은 CA Access Control Solaris 기본 패키지 사용자 지정 스크립트를 실행합니다.

이 명령을 사용할 때는 다음 사항을 고려해야 합니다.

- 이 스크립트는 모든 CA Access Control Solaris 기본 패키지에 대해 사용할 수 있습니다.
- 패키지를 사용자 지정하려면 패키지가 파일 시스템의 읽기/쓰기 가능한 디렉터리에 있어야 합니다.
- 번역된 스크립트 메시지를 표시하려면 pre.tar 파일을 스크립트 파일과 동일한 디렉터리에 넣어야 합니다.

이 명령의 형식은 다음과 같습니다.

customize_eac_pkg -h [-l]
customize_eac_pkg -a [-d *pkg_location*] [*pkg_name*]
customize_eac_pkg -w *keyword* [-d *pkg_location*] [*pkg_name*]
customize_eac_pkg -r [-d *pkg_location*] [-l lang] [*pkg_name*]
customize_eac_pkg -i *install_loc* [-d *pkg_location*] [*pkg_name*]
customize_eac_pkg -s {-f *tmp_params* | -c *certfile* | -k *keyfile*} [-d *pkg_location*] *[pkg_name]*
customize_eac_pkg -g [-f *tmp_params*] [-d *pkg_location*] [*pkg_name*]
customize_eac_pkg -t *tmp_dir* [-d *pkg_location*] [*pkg_name*]

pkg_name

(선택 사항) 사용자 지정할 CA Access Control 패키지의 이름입니다. 패키지를 지정하지 않으면 스크립트는 기본적으로 기본 CA Access Control 패키지(CAeAC)를 선택합니다.

-a

사용권 계약을 표시합니다.

-c *certfile*

루트 인증서 파일의 전체 경로 이름을 정의합니다.

참고: 이 옵션은 CAeAC 패키지에만 적용됩니다.

-d *pkg_location*

(선택 사항) 패키지가 들어 있는 파일 시스템의 디렉터리를 지정합니다. 패키지가 있는 위치를 지정하지 않으면 스크립트는 기본적으로 /var/spool/pkg 를 선택합니다.

-f *tmp_params*

정보를 가져오거나 작성하려는 설치 매개 변수 파일의 전체 경로 및 이름을 지정합니다.

참고: -g 옵션을 사용할 때 파일을 지정하지 않으면 설치 매개 변수는 표준 출력(stdout)으로 전달됩니다.

-g

설치 매개 변수 파일을 가져와 -f 옵션에서 지정된 파일에 출력합니다.

-h

명령 사용법을 표시합니다. -l 옵션과 함께 사용하면 지원되는 언어의 언어 코드를 표시합니다.

-i *install_loc*

패키지의 설치 디렉터리를 *install_loc*/AccessControl 로 설정합니다.

-k *keyfile*

루트 개인 키 파일의 전체 경로 이름을 정의합니다.

참고: 이 옵션은 CAeAC 패키지에만 적용됩니다.

-l *lang*

설치 매개 변수 파일의 언어를 *lang* 으로 설정합니다. 언어를 설정할 때는 -r 옵션을 함께 사용해야 합니다.

참고: 지정할 수 있는 지원되는 언어 코드에 대한 목록을 보려면 -h 옵션을 사용하여 -l 을 실행하십시오. 기본적으로 설치 매개 변수 파일은 영어로 되어 있습니다.

-r

원래 패키지에 사용된 기본값을 사용하도록 패키지를 다시 설정합니다.

-s

지정된 패키지가 -f 옵션으로 지정한 사용자 지정된 설치 매개 변수 파일에서 가져온 입력을 사용하도록 설정합니다.

-t *tmp_dir*

설치 작업을 위한 임시 디렉터리를 설정합니다.

참고: 기본 임시 디렉터리는 /tmp 입니다.

-w keyword

사용자가 사용권 계약을 수락함을 지정하는 키워드를 정의합니다. 이 키워드는 사용권 계약 끝부분에서 대괄호 안에 표시됩니다. 사용권 계약서 파일을 찾으려면 -a 옵션을 사용하십시오.

convert_eac_pkg - Solaris 네이티브 설치 구성

기본 Solaris pkgadd 동작은 설치 관리 파일에 의해 결정됩니다. 기본 설정을 덮어쓰려면 설치 관리 파일(기본값은 /var/sadm/install/admin/default)을 변경해야 합니다. 예를 들어 CA Access Control 패키지는 setuid 실행 파일을 설치하며, 선택적으로 사용자가 설치 후 스크립트(루트로 실행)를 실행할 수 있게 해 줍니다. 기본 Solaris pkgadd 동작에서는 사용자에게 이러한 작업을 확인하는 메시지를 표시합니다.

참고: 설치 관리 파일을 편집하여 pkgadd 설치 기본값을 변경할 수 있습니다. 그런 다음 pkgadd -a 옵션을 사용하여 CA Access Control 과 같은 특정 설치에 대해 수정된 파일을 사용할 수 있습니다. 단, 이 파일이 CA Access Control 에 한정되는 것은 아닙니다.

이 명령의 형식은 다음과 같습니다.

convert_eac_pkg -c [-d *pkg_location*] [*pkg_name*]

convert_eac_pkg -p [-f *file*]

-c

이전 형식 패키지를 새로운 형식으로 변환합니다.

참고: CA Access Control r8 SP1 에는 이전 형식 패키지가 사용되었습니다. 업그레이드하기 전에 이를 변환해야 합니다.

설치된 CA Access Control 패키지나 스풀된 패키지에 대한 정보를 변환할 수 있습니다. 스풀된 패키지의 경우 -d 옵션을 사용하여 패키지 위치를 나타냅니다.

-d *pkg_location*

패키지가 들어 있는 파일 시스템의 디렉터리를 정의합니다.

pkg_name

패키지의 이름(기본값은 CAeAC)을 정의합니다.

-p

명명된 사용자 지정 패키지 구성 파일을 준비합니다.

-f *file*

CA Access Control 설치 관리 파일을 작성하고자 하는 위치를 정의합니다.

지정하지 않는 경우 이 명령은 현재 디렉터리에 *myadmin* 이라는 이름의 파일을 작성합니다.

예제: 자동 설치를 위한 Solaris 네이티브 설치 구성

다음 절차에서는 setuid 실행 파일 설치나 설치 후 스크립트 실행을 확인하는 메시지가 표시되지 않도록 Solaris 네이티브 설치를 구성하는 방법에 대해 보여 줍니다.

1. 현재 위치로 설치 관리 파일 복사본을 가져옵니다.

   convert_eac_pkg -p

   이렇게 하면 다른 설치에 영향을 주지 않고 CA Access Control 네이티브 설치에 대한 구성 설정을 수정할 수 있습니다.

2. 패키지 구성 파일(myadmin)에서 아래와 같이 설정을 편집합니다.

   setuid=nocheck
   action=nocheck

   파일을 저장합니다.

3. 패키지를 사용자 지정합니다.

   최소한 사용권 계약에 동의하도록 지정해야 합니다.

4. 다음 명령을 실행하여 사용자 지정된 CA Access Control 패키지를 자동으로 설치합니다.

   pkgadd -n -a *config_path*\myadmin -d *pkg_path* CAeAC

예제: 이전 형식을 사용하는 Solaris 네이티브 설치 업그레이드

다음 절차에서는 새 릴리스로 업그레이드하기 전에 CA Access Control 네이티브 패키지의 기존 설치를 변환하는 방법을 보여 줍니다. 이렇게 하려면 다음 명령을 실행하십시오.

convert_eac_pkg -c CAeAC

HP-UX 기본 패키지 설치

HP-UX 기본 패키지는 개별 소프트웨어 패키지를 만들고, 설치하고, 제거하고, 보고할 수 있는 일련의 GUI 및 명령줄 유틸리티로서 제공됩니다. HP-UX 기본 패키지를 사용하면 원격 컴퓨터에도 소프트웨어 패키지를 설치할 수 있습니다.

참고: HP-UX 기본 패키지인 SD-UX(Distributor-UX)에 대한 자세한 내용은 HP 웹 사이트 http://www.hp.com을 참조하십시오. swreg, swinstall, swpackage 및 swverify 에 대한 자세한 내용은 man 페이지를 참조하십시오.

일반 설치 대신 CA Access Control 에서 제공하는 SD-UX 기본 패키지를 사용할 수 있습니다. 이 패키지를 사용하면 CA Access Control 설치와 함께 SD-UX 를 사용하여 수행된 다른 모든 소프트웨어 설치를 관리할 수 있습니다.

중요! 패키지 설치 후 CA Access Control 을 제거하려면 *swremove* 명령을 사용해야 합니다. uninstall_AC 스크립트를 사용하지 마십시오.

SD-UX 형식 패키지 사용자 지정

네이티브 패키지를 사용하여 CA Access Control 을 설치하기 전에 사용권 계약에 동의하도록 지정하기 위해 CA Access Control 패키지를 사용자 지정해야 합니다. 또한 패키지를 사용자 지정할 때는 사용자 지정 설치 설정도 지정해야 합니다.

패키지에서 설치 매개 변수 파일을 추출하여 필요한 대로 수정한 다음 패키지로 다시 로드하는 방법으로 패키지를 사용자 지정합니다. 일부 명령은 사용자 지정된 스크립트에서 사용할 수 있으므로 매개 변수 파일을 수정할 필요는 없습니다.

참고: 수동으로 패키지를 수정하는 것은 권장되지 않습니다. 대신 다음 절차에 설명된 스크립트를 사용하여 CA Access Control 패키지를 사용자 지정하십시오.

지원되는 각 HP-UX 운영 체제에 대한 SD-UX(Software Distributor-UX) 형식 패키지는 CA Access Control UNIX 용 끝점 구성 요소 DVD 의 NativePackages 디렉터리에 있습니다.

SD-UX 형식 패키지를 사용자 지정하려면

1. 사용자 지정할 패키지를 파일 시스템의 임시 위치로 추출합니다.

   파일 시스템의 읽기/쓰기가 가능한 위치에서 패키지를 필요한 대로 사용자 지정할 수 있습니다.

   중요! 패키지를 추출할 때는 패키지의 전체 디렉터리 구조에 대한 파일 특성이 그대로 보존되어야 합니다. 그렇지 않으면 HP-UX 네이티브 패키지 도구에서 패키지가 손상된 것으로 간주합니다.

2. 파일 시스템의 임시 위치로 customize_eac_depot 스크립트 파일과 pre.tar 파일을 복사합니다.

   pre.tar 파일은 설치 메시지와 CA Access Control 사용권 계약이 수록된 압축 tar 파일입니다.

   참고: customize_eac_depot 스크립트 파일과 pre.tar 파일은 네이티브 패키지가 들어 있는 위치에 있습니다.

3. 사용권 계약을 표시합니다.

   customize_eac_depot -a [-d *pkg_location*] *pkg_name*

4. 사용권 계약의 끝에서 대괄호 안에 표시된 키워드를 적어 둡니다.

   다음 단계에서 이 키워드를 지정합니다.

5. 사용권 계약에 동의하도록 지정하기 위해 CA Access Control 패키지를 사용자 지정합니다.

   customize_eac_depot -w *keyword* [-d *pkg_location*] [*pkg_name*]

6. (선택 사항) 설치 매개 변수 파일의 언어를 설정합니다.

   customize_eac_depot -r -l *lang* [-d *pkg_location*] [*pkg_name*]

7. (선택 사항) 설치 디렉터리를 변경합니다.

   customize_eac_depot -i *install_loc* [-d *pkg_location*] [*pkg_name*]

8. (선택 사항) 기본 암호화 파일을 변경합니다.

   customize_eac_depot -s -c *certfile* -k *keyfile* [-d *pkg_location*] [*pkg_name*]

9. (선택 사항) 설치 매개 변수 파일을 가져옵니다.

   customize_eac_depot -g -f *tmp_params* [-d *pkg_location*] [*pkg_name*]

10. (선택 사항) 설치 요구 사항에 맞게 설치 매개 변수 파일을 편집합니다.

    이 파일에서 패키지에 대한 설치 기본 설정을 지정할 수 있습니다. 예를 들어 POSTEXIT 설정을 활성화하고(앞의 # 기호를 제거) 실행할 설치 후 스크립트 파일을 지정합니다.

11. (선택 사항) 사용자 지정된 패키지에 설치 매개 변수를 설정합니다.

    customize_eac_depot -s -f *tmp_params* [-d *pkg_location*] [*pkg_name*]

    이제 이 패키지를 사용하여 사용자 지정된 기본 설정으로 CA Access Control 을 설치할 수 있습니다.

예: 사용권 계약에 동의하도록 지정

네이티브 패키지를 설치할 때 사용권 계약에 동의하려면 패키지를 사용자 정의해야 합니다. 다음 예는 UNIX 용 CA Access Control 끝점 구성 요소 DVD(/mnt/AC_DVD 에 마운트)에 있는 x86 CA Access Control SD-UX 패키지를 사용자 지정하여 사용권 계약에 동의하도록 지정하는 방법을 설명합니다.

```
cp /mnt/AC_DVD/NativePackages/_HPUX11_PKG_*.tar.Z /tmp
cp /mnt/AC_DVD/NativePackages/pre.tar /tmp
cd /tmp
zcat _HPUX11_PKG_*.tar.Z | tar -xvf -
/mnt/AC_DVD/NativePackages/customize_eac_depot -w keyword -d /tmp CAeAC
```

이제 /tmp 디렉터리에 있는 사용자 지정된 패키지를 사용하여 CA Access Control 을 설치할 수 있습니다.

추가 정보:

customize_eac_depot 명령—SD-UX 형식 패키지 사용자 지정 (페이지 217)

HP-UX 기본 패키지 설치

설치된 다른 모든 소프트웨어와 함께 설치된 CA Access Control 을 관리하려면 사용자 지정된 CA Access Control SD-UX 형식 패키지를 설치하십시오. CA Access Control SD-UX 형식 패키지를 사용하면 간편하게 HP-UX 에 CA Access Control 을 설치할 수 있습니다.

중요! 사용권 계약에 동의함을 나타내기 위해 사용권 계약 내에서 찾을 수 있는 키워드를 사용하여 패키지를 사용자 지정해야 합니다.

CA Access Control HP-UX 네이티브 패키지를 설치하려면

1. 루트로 로그인합니다.

   HP-UX 네이티브 패키지를 등록 및 설치하려면 루트 계정 권한이 필요합니다.

2. CAeAC 패키지를 사용자 지정 (페이지 213)합니다.

   사용권 계약에 동의함을 나타내기 위해 사용권 계약 내에서 찾을 수 있는 키워드를 사용하여 패키지를 사용자 지정해야 합니다. 사용자 지정 설치 설정을 지정하기 위해 패키지를 사용자 지정할 수도 있습니다.

3. 다음 명령을 사용하여 SD-UX 와 함께 사용자 지정된 패키지를 등록합니다.

   swreg -l depot *pkg_location*

   pkg_location

   CA Access Control 패키지(CAeAC)가 있는 디렉터리를 정의합니다.

4. 다음 명령을 사용하여 CA Access Control 패키지를 설치합니다.

   swinstall -s *pkg_location* CAeAC

   SD-UX 는 *pkg_location* 디렉터리에서 CAeAC 패키지의 설치를 시작합니다.

   이제 CA Access Control 이 완전히 설치되었지만 아직 시작되지 않았습니다.

추가 정보:

기본 설치 관련 추가 고려 사항 (페이지 188)
SD-UX 형식 패키지 사용자 지정 (페이지 213)

customize_eac_depot 명령—SD-UX 형식 패키지 사용자 지정

customize_eac_depot 명령은 SD-UX 형식 패키지에 대한 CA Access Control 기본 패키지 사용자 지정 스크립트를 실행합니다.

이 명령을 사용할 때는 다음 사항을 고려해야 합니다.

- 이 스크립트는 모든 CA Access Control Solaris 기본 패키지에 대해 사용할 수 있습니다.
- 패키지를 사용자 지정하려면 패키지가 파일 시스템의 읽기/쓰기 가능한 디렉터리에 있어야 합니다.
- 번역된 스크립트 메시지를 표시하려면 pre.tar 파일을 스크립트 파일과 동일한 디렉터리에 넣어야 합니다.

이 명령의 형식은 다음과 같습니다.

customize_eac_depot -h [-l]
customize_eac_depot -a [-d *pkg_location*] [*pkg_name*]
customize_eac_depot -w *keyword* [-d *pkg_location*] [*pkg_name*]
customize_eac_depot -r [-l *lang*] [-d *pkg_location*] [*pkg_name*]
customize_eac_depot -i *install_loc* [-d *pkg_location*] [*pkg_name*]
customize_eac_depot -s {-f *tmp_params* | -c *certfile* | -k *keyfile*} [-d *pkg_location*] *[pkg_name*]
customize_eac_depot -g [-f *tmp_params*] [-d *pkg_location*] [*pkg_name*]

pkg_name

(선택 사항) 사용자 지정할 CA Access Control 패키지의 이름입니다. 패키지를 지정하지 않으면 스크립트는 기본적으로 기본 CA Access Control 패키지(CAeAC)를 선택합니다.

-a

사용권 계약을 표시합니다.

-c *certfile*

루트 인증서 파일의 전체 경로 이름을 정의합니다.

참고: 이 옵션은 CAeAC 패키지에만 적용됩니다.

-d *pkg_location*

(선택 사항) 패키지가 들어 있는 파일 시스템의 디렉터리를 지정합니다. 패키지가 있는 위치를 지정하지 않으면 스크립트는 기본적으로 /var/spool/pkg 를 선택합니다.

-f *tmp_params*

정보를 가져오거나 작성하려는 설치 매개 변수 파일의 전체 경로 및 이름을 지정합니다.

참고: -g 옵션을 사용할 때 파일을 지정하지 않으면 설치 매개 변수는 표준 출력(stdout)으로 전달됩니다.

-g

설치 매개 변수 파일을 가져와 -f 옵션에서 지정된 파일에 출력합니다.

-h

명령 사용법을 표시합니다. -l 옵션과 함께 사용하면 지원되는 언어의 언어 코드를 표시합니다.

-i *install_loc*

패키지의 설치 디렉터리를 *install_loc*/AccessControl 로 설정합니다.

-k *keyfile*

루트 개인 키 파일의 전체 경로 이름을 정의합니다.

참고: 이 옵션은 CAeAC 패키지에만 적용됩니다.

-l *lang*

설치 매개 변수 파일의 언어를 *lang* 으로 설정합니다. 언어를 설정할 때는 -r 옵션을 함께 사용해야 합니다.

참고: 지정할 수 있는 지원되는 언어 코드에 대한 목록을 보려면 -h 옵션을 사용하여 -l 을 실행하십시오. 기본적으로 설치 매개 변수 파일은 영어로 되어 있습니다.

-r

원래 패키지에 사용된 기본값을 사용하도록 패키지를 다시 설정합니다.

-s

지정된 패키지가 -f 옵션으로 지정한 사용자 지정된 설치 매개 변수 파일에서 가져온 입력을 사용하도록 설정합니다.

-w keyword

사용자가 사용권 계약을 수락함을 지정하는 키워드를 정의합니다. 이 키워드는 사용권 계약 끝부분에서 대괄호 안에 표시됩니다. 사용권 계약서 파일을 찾으려면 -a 옵션을 사용하십시오.

HP-UX 패키지 제거

CA Access Control HP-UX 패키지를 제거하려면 설치 순서와 반대로 CA Access Control 패키지를 제거해야 합니다.

CA Access Control 패키지를 제거하려면 기본 CA Access Control 패키지를 제거하십시오.

```
swremove CAeAC
```

AIX 기본 패키지 설치

AIX 기본 패키지는 개별 소프트웨어 패키지를 관리하는 데 사용할 수 있는 일련의 GUI 및 명령줄 유틸리티로서 제공됩니다.

일반 설치 대신 CA Access Control 에서 제공하는 AIX 기본 패키지를 사용할 수 있습니다. 이 패키지를 사용하면 CA Access Control 설치와 함께 AIX installp 를 사용하여 수행된 다른 모든 소프트웨어 설치를 관리할 수 있습니다.

참고: 일부 AIX 버전은 여러 패키지 형식(installp, SysV, RPM)을 지원하지만 CA Access Control 은 AIX 기본 패키지 형식(installp)만 제공합니다.

중요! 패키지 설치 후 CA Access Control 을 제거하려면 *installp* 명령을 사용해야 합니다. uninstall_AC 스크립트를 사용하지 마십시오.

bff 네이티브 패키지 파일 사용자 지정

네이티브 패키지를 사용하여 CA Access Control 을 설치하기 전에 사용권 계약에 동의하도록 지정하기 위해 CA Access Control 패키지를 사용자 지정해야 합니다. 또한 패키지를 사용자 지정할 때는 사용자 지정 설치 설정도 지정해야 합니다.

패키지에서 설치 매개 변수 파일을 추출하여 필요한 대로 수정한 다음 패키지로 다시 로드하는 방법으로 패키지를 사용자 지정합니다. 일부 명령은 사용자 지정된 스크립트에서 사용할 수 있으므로 매개 변수 파일을 수정할 필요는 없습니다.

참고: 수동으로 패키지를 수정하는 것은 권장되지 않습니다. 대신 다음 절차에 설명된 스크립트를 사용하여 CA Access Control 패키지를 사용자 지정하십시오.

지원되는 각 AIX 운영 체제용 installp 형식 네이티브 패키지(bff 파일)는 CA Access Control UNIX 용 끝점 구성 요소 DVD 의 NativePackages 디렉터리에서 찾을 수 있습니다.

bff 네이티브 패키지 파일 사용자 지정

1. 사용자 지정할 패키지를 파일 시스템의 임시 위치로 추출합니다.

   파일 시스템의 읽기/쓰기가 가능한 위치에서 패키지(bff 파일)를 필요한 대로 사용자 지정할 수 있습니다.

   중요! 이 위치에는 다시 패키징하는 임시 파일을 수용할 수 있도록 패키지 크기의 두 배 이상 되는 빈 디스크 공간이 필요합니다.

2. 파일 시스템의 임시 위치로 customize_eac_bff 스크립트 파일과 pre.tar 파일을 복사합니다.

   pre.tar 파일은 설치 메시지와 CA Access Control 사용권 계약이 수록된 압축 tar 파일입니다.

   참고: customize_eac_bff 스크립트 파일과 pre.tar 파일은 네이티브 패키지가 들어 있는 위치에 있습니다.

3. 사용권 계약을 표시합니다.

   customize_eac_bff -a [-d *pkg_location*] *pkg_name*

4. 사용권 계약의 끝에서 대괄호 안에 표시된 키워드를 적어 둡니다.

   다음 단계에서 이 키워드를 지정합니다.

5. 사용권 계약에 동의하도록 지정하기 위해 CA Access Control 패키지를 사용자 지정합니다.

   customize_eac_bff -w *keyword* [-d *pkg_location*] *pkg_name*

6. (선택 사항) 설치 매개 변수 파일의 언어를 설정합니다.

   customize_eac_bff -r -l *lang* [-d *pkg_location*] *pkg_name*

7. (선택 사항) 설치 디렉터리를 변경합니다.

   customize_eac_bff -i *install_loc* [-d *pkg_location*] *pkg_name*

8. (선택 사항) 기본 암호화 파일을 변경합니다.

   customize_eac_bff -s -c *certfile* -k *keyfile* [-d *pkg_location*] *pkg_name*

9. 설치 매개 변수 파일을 가져옵니다.

   customize_eac_bff -g -f *tmp_params* [-d *pkg_location*] *pkg_name*

10. (선택 사항) 설치 요구 사항에 맞게 설치 매개 변수 파일을 편집합니다.

    이 파일에서 패키지에 대한 설치 기본 설정을 지정할 수 있습니다. 예를 들어 POSTEXIT 설정을 활성화하고(앞의 # 기호를 제거) 실행할 설치 후 스크립트 파일을 지정합니다.

11. (선택 사항) 사용자 지정된 패키지에 설치 매개 변수를 설정합니다.

    customize_eac_bff -s -f *tmp_params* [-d *pkg_location*] *pkg_name*

    이제 이 패키지를 사용하여 사용자 지정된 기본 설정으로 CA Access Control 을 설치할 수 있습니다.

추가 정보:

customize_eac_bff 명령 - bff 기본 패키지 파일 사용자 지정 (페이지 223)

AIX 기본 패키지 설치

설치된 다른 모든 소프트웨어와 함께 설치된 CA Access Control 을 관리하려면 사용자 지정된 CA Access Control AIX 네이티브 패키지를 설치하십시오. CA Access Control AIX 네이티브 패키지(bff 파일)를 사용하면 간편하게 AIX 에 CA Access Control 을 설치할 수 있습니다.

중요! 사용권 계약에 동의함을 나타내기 위해 사용권 계약 내에서 찾을 수 있는 키워드를 사용하여 패키지를 사용자 지정해야 합니다.

CA Access Control AIX 네이티브 패키지를 설치하려면

1. 루트로 로그인합니다.

   AIX 네이티브 패키지를 등록 및 설치하려면 루트 계정 권한이 필요합니다.

2. CAeAC 패키지를 사용자 지정 (페이지 220)합니다.

   사용권 계약에 동의함을 나타내기 위해 사용권 계약 내에서 찾을 수 있는 키워드를 사용하여 패키지를 사용자 지정해야 합니다. 사용자 지정 설치 설정을 지정하기 위해 패키지를 사용자 지정할 수도 있습니다.

3. (선택 사항) 다음과 같이 설치할 패키지의 수준(버전)을 기록합니다.

   installp -l -d *pkg_location*

   pkg_location

   CA Access Control 패키지(CAeAC)가 있는 디렉터리를 정의합니다.

   pkg_location 의 각 패키지에 대해 AIX 에서 패키지 수준이 나열됩니다.

   참고: AIX 네이티브 패키지 설치 옵션에 대한 자세한 내용은 installp 에 대한 man 페이지를 참조하십시오.

4. 다음 명령을 사용하여 CA Access Control 패키지를 설치합니다.

   installp -ac -d *pkg_location* CAeAC [*pkg_level*]

   pkg_level

   이전에 기록한 패키지의 수준 번호를 정의합니다.

   AIX 는 *pkg_location* 디렉터리에서 CAeAC 패키지의 설치를 시작합니다.

   이제 CA Access Control 이 완전히 설치되었지만 아직 시작되지 않았습니다.

추가 정보:

bff 네이티브 패키지 파일 사용자 지정 (페이지 220)
기본 설치 관련 추가 고려 사항 (페이지 188)

customize_eac_bff 명령 - bff 기본 패키지 파일 사용자 지정

customize_eac_bff 명령은 bff 기본 패키지 파일에 대한 CA Access Control 기본 패키지 사용자 지정 스크립트를 실행합니다.

이 스크립트는 AIX 용의 모든 CA Access Control 기본 패키지에 대해 사용할 수 있습니다. 패키지를 사용자 지정하려면 패키지가 파일 시스템의 읽기/쓰기 가능한 디렉터리에 있어야 합니다.

중요! 패키지를 추출할 위치는 임시로 만들어지는 패키지를 수록할 수 있도록 패키지 크기의 두 배 이상되는 여유 공간이 있어야 합니다.

참고: 번역된 스크립트 메시지를 표시하려면 pre.tar 파일을 스크립트 파일과 동일한 디렉터리에 넣어야 합니다.

이 명령의 형식은 다음과 같습니다.

customize_eac_bff -h [-l]
customize_eac_bff -a [-d *pkg_location*] *pkg_name*
customize_eac_bff -w *keyword* [-d *pkg_location*] *pkg_name*
customize_eac_bff -r [-d *pkg_location*] [-l *lang*] *pkg_name*
customize_eac_bff -i *install_loc* [-d *pkg_location*] *pkg_name*
customize_eac_bff -s {-f *tmp_params* | -c *certfile* | -k *keyfile*} [-d *pkg_location*] *pkg_name*
customize_eac_bff -g [-f *tmp_params*] [-d *pkg_location*] *pkg_name*

pkg_name

사용자 지정할 CA Access Control 패키지(bff 파일)의 이름입니다.

-a

사용권 계약을 표시합니다.

-c *certfile*

루트 인증서 파일의 전체 경로 이름을 정의합니다.

참고: 이 옵션은 CAeAC 패키지에만 적용됩니다.

-d *pkg_location*

(선택 사항) 패키지가 들어 있는 파일 시스템의 디렉터리를 지정합니다. 패키지가 있는 위치를 지정하지 않으면 스크립트는 기본적으로 /var/spool/pkg 를 선택합니다.

-f *tmp_params*

정보를 가져오거나 작성하려는 설치 매개 변수 파일의 전체 경로 및 이름을 지정합니다.

참고: -g 옵션을 사용할 때 파일을 지정하지 않으면 설치 매개 변수는 표준 출력(stdout)으로 전달됩니다.

-g

설치 매개 변수 파일을 가져와 -f 옵션에서 지정된 파일에 출력합니다.

-h

명령 사용법을 표시합니다. -l 옵션과 함께 사용하면 지원되는 언어의 언어 코드를 표시합니다.

-i *install_loc*

패키지의 설치 디렉터리를 *install_loc*/AccessControl 로 설정합니다.

-k *keyfile*

루트 개인 키 파일의 전체 경로 이름을 정의합니다.

참고: 이 옵션은 CAeAC 패키지에만 적용됩니다.

-l *lang*

설치 매개 변수 파일의 언어를 *lang* 으로 설정합니다. 언어를 설정할 때는 -r 옵션을 함께 사용해야 합니다.

참고: 지정할 수 있는 지원되는 언어 코드에 대한 목록을 보려면 -h 옵션을 사용하여 -l 을 실행하십시오. 기본적으로 설치 매개 변수 파일은 영어로 되어 있습니다.

-r

원래 패키지에 사용된 기본값을 사용하도록 패키지를 다시 설정합니다.

-s

지정된 패키지가 -f 옵션으로 지정한 사용자 지정된 설치 매개 변수 파일에서 가져온 입력을 사용하도록 설정합니다.

-w keyword

사용자가 사용권 계약을 수락함을 지정하는 키워드를 정의합니다. 이 키워드는 사용권 계약 끝부분에서 대괄호 안에 표시됩니다. 사용권 계약서 파일을 찾으려면 -a 옵션을 사용하십시오.

AIX 패키지 제거

CA Access Control AIX 패키지를 제거하려면 설치 순서와 반대로 CA Access Control 패키지를 제거해야 합니다.

CA Access Control 패키지를 제거하려면 기본 CA Access Control 패키지를 제거하십시오.

```
installp -u CAeAC
```

일반 스크립트 설치

CA Access Control 은 UNIX 에 CA Access Control 을 대화식으로 또는 자동으로 설치할 수 있도록 install_base 스크립트를 제공합니다.

기본 설치가 아니라 일반 스크립트 설치를 사용하는 경우 CA Access Control 설치 미디어의 파일 3 개가 필요합니다.

- **install_base** - tar 파일에서 CA Access Control 을 설치하는 스크립트입니다.
- ***_opSystemVersion_ACVersion*.tar.Z** - 모든 CA Access Control 파일을 포함하는 압축 tar 파일입니다. 예를 들어, IBM AIX 버전 5 에 CA Access Control r12.0 을 설치하는 경우 tar 파일은 _AIX5_120.tar.Z 입니다.
- **pre.tar** - 설치 메시지와 사용권 계약을 포함하는 압축 tar 파일입니다.

  사용권 계약 내용을 읽은 후 파일 끝에 있는 명령을 입력하여 설치를 계속할 수 있습니다.

  - install_base -autocfg 를 사용하여 자동 설치를 실행하는 경우 사용권 계약 파일 아래에 있는 명령을 실행하여 -command 옵션을 사용할 수 있습니다.
  - 응답 파일인 -autocfg file_name 을 사용하는 경우 -command 옵션을 사용할 필요가 없습니다.

  라이선스 파일의 이름 및 위치를 가져오려면 install_base -h 를 실행해야 합니다. 잘못된 명령을 입력해도 파일 이름 및 위치를 가져옵니다.

이러한 파일은 UNIX 용 CA Access Control 끝점 구성 요소 DVD 의 /Unix/Access-Control 디렉터리에 있습니다.

install_base 스크립트를 사용한 설치

install_base 스크립트를 사용하여 지원되는 어느 OS 에나 CA Access Control 을 설치할 수 있습니다. 이 스크립트는 대화식 스크립트이지만 자동으로도 실행할 수 있습니다.

참고: install_base 스크립트를 실행하기 전에 설치할 기능을 결정하고 install_base 명령 (페이지 228)을 검토하여 그러한 기능의 설치를 시작하는 방법을 알아두십시오. install_base 스크립트의 작동 방식 (페이지 234)을 먼저 알아두는 것도 좋습니다.

CA Access Control 을 설치하려면

1. CA Access Control 이 이미 설치되어 실행 중이라면 관리자로 로그인한 후 다음 명령을 입력하여 종료합니다.

   ACInstallDir/bin/secons -sk
   ACInstallDir/bin/SEOS_load -u

2. 루트로 로그인합니다.

   CA Access Control 을 설치하려면 루트 권한이 필요합니다.

3. UNIX 용 CA Access Control 끝점 구성 요소 DVD 에 광 디스크 드라이브를 마운트합니다.

   중요! 광 디스크 드라이브로 HP 에 설치하는 경우 DVD 의 파일 이름을 제대로 읽고 있는지 확인해야 합니다. 파일 이름을 짧게 줄이고 모두 대문자를 사용해야 하는 경우를 피하려면 *pfs_mountd &* 및 *pfsd &* 명령을 입력하고 다음의 4 개 데몬이 호출되었는지 확인하십시오: pfs_mountd, pfsd.rpc, pfs_mountd.rpc, pfsd 자세한 내용은 특정 pfs* 데몬 및 명령의 man 페이지를 참조하십시오.

4. 사용권 계약을 읽습니다.

   install_base 스크립트를 실행하려면 최종 사용자 사용권 계약을 수락해야 합니다. 사용권 계약 내용을 읽은 후 파일 끝에 있는 명령을 입력하여 설치를 계속할 수 있습니다. -autocfg 를 사용하여 자동 설치를 실행하는 경우 사용권 계약 파일의 끝에 있는 명령을 실행하여 -command 플래그를 사용할 수 있습니다. 라이선스 파일의 이름 및 위치를 가져오려면 install_base -h 를 실행해야 합니다.

5. install_base 스크립트를 실행합니다.

   install_base 스크립트가 시작되고 선택한 사항에 따라 해당되는 설치 관련 질문이 표시됩니다.

   참고: 설치 스크립트에서 해당 압축 tar 파일을 찾아 주므로 플랫폼의 tar 파일 이름 입력은 생략할 수 있습니다.

   이제 CA Access Control 설치가 완료되었지만 아직 실행 중은 아닙니다.

예제: 기본 기능이 포함된 클라이언트 및 서버 패키지 설치

다음 명령은 CA Access Control 의 모든 기본 기능이 포함된 클라이언트 및 서버 패키지를 설치하도록 install_base 대화식 스크립트를 시작하는 방법을 보여 줍니다. 설치하는 동안 CA Access Control 의 클라이언트 및 서버 패키지 설치와 관련된 질문에 답해야 합니다.

```
/dvdrom/Unix/Access-Control/install_base
```

참고: 설치할 패키지를 지정하지 않았으므로 install_base 명령은 클라이언트와 서버 패키지를 모두 설치합니다.

예제: STOP 이 활성화된 상태로 사용자 지정 디렉터리에 클라이언트 패키지 설치

다음 명령은 install_base 대화식 스크립트를 시작하여 /opt/CA/AC 디렉터리에 클라이언트 패키지를 설치하고 스택 오버플로 보호 옵션을 활성화하는 방법을 보여 줍니다.

```
/dvdrom/Unix/Access-Control/install_base -client -stop  -d /opt/CA/AC
```

install_base Command - 설치 스크립트 실행

install_base 명령은 설치 스크립트를 실행하고 하나 이상의 CA Access Control 패키지를 하나 이상의 선택한 설치 옵션으로 설치합니다.

이 명령의 형식은 다음과 같습니다.

install_base [*tar_file*] [*packages*] [*options*]

tar_file

(선택 사항) 플랫폼의 CA Access Control 설치 파일이 들어 있는 tar 파일의 이름을 정의합니다. 설치 스크립트에서 해당 압축 tar 파일을 자동으로 찾아 주므로 tar 파일 이름 입력은 생략할 수 있습니다.

packages

(선택 사항) 설치할 CA Access Control 패키지를 정의합니다. 패키지를 지정하지 않으면 CA Access Control 업그레이드를 위해 설치 스크립트에서 이미 설치한 같은 패키지를 설치하는 경우가 아닌 한, 설치 스크립트에서 클라이언트와 서버 패키지를 모두 설치합니다.

참고: 다른 패키지를 설치하기 전에 클라이언트 패키지를 먼저 설치해야 합니다. 단, 다른 패키지와 함께 클라이언트 패키지를 설치하도록 지정할 수는 있습니다.

다음은 설치할 수 있는 CA Access Control 패키지입니다.

-all

모든 CA Access Control 패키지를 설치합니다. 이러한 패키지로는 클라이언트 패키지, 서버 패키지, API 패키지, MFSD 패키지가 있습니다. 이 경우 STOP(-stop 옵션)도 활성화됩니다.

-api

API 라이브러리와 예제 프로그램이 들어 있는 API 패키지를 설치합니다.

-client

독립형 컴퓨터에 필요한 핵심 CA Access Control 기능이 있는 클라이언트 패키지를 설치합니다.

-mfsd

메인프레임 동기화 데몬이 들어 있는 MFSD 패키지를 설치합니다.

참고: MFSD 패키지를 설치하기 전에 서버 패키지를 설치해야 합니다.

-server

추가 바이너리 및 스크립트(selogrcd, sepmd, sepmdd, sepmdadm, secrepsw)가 들어 있는 서버 패키지를 설치합니다. 이러한 서버 패키지는 클라이언트 패키지를 보완합니다. 예를 들어 sepmdd 를 사용하면 정책 모델을 사용하여 컴퓨터를 설정할 수 있습니다.

-uni

Unicenter 의 CAUTIL, Workload Management 및 Event Management 구성 요소와 CA Access Control 의 통합과 Unicenter EMSec API 를 지원하는 Unicenter 보안 통합 및 마이그레이션 패키지를 설치합니다.

옵션

(선택 사항) 설정할 추가 설치 옵션을 정의합니다.

참고: CA Access Control 기능에 영향을 주는 설치 옵션(예: -stop)은 *클라이언트* 패키지 설치 시에만 지정할 수 있습니다. 설치 프로세스에 영향을 미칠 수 있는 설치 옵션(예: -verbose)은 어느 패키지에서나 지정할 수 있습니다.

다음은 지정할 수 있는 옵션입니다.

-autocfg [*response_file*]

대화식 모드가 아니라 자동 모드로 설치를 실행합니다. 응답 파일이 지정된 경우 설치 시 파일에 저장된 기본 설정을 사용하여 자동으로 대화식 설치 프로세스에 응답합니다. 응답 파일이 지정되지 않았거나 응답 파일에 옵션이 없는 경우, 설치 시 미리 설정된 기본값을 사용합니다.

응답 파일을 만들려면

- *-savecfg* 옵션을 사용합니다.
- parameters.tar 안에 있는 설치 매개 변수 파일을 편집합니다.

중요! 응답 파일을 지정하지 않으면 *-autocfg* 옵션을 사용할 때 *-command* 옵션을 사용해야 합니다.

자동 설치를 실행하는 경우 다음을 고려하십시오.

- 암호화 키는 변경할 수 없습니다.
- 기본적으로 클라이언트 및 서버 패키지만 설치됩니다.

  다른 패키지나 기능을 설치하려면 일반 설치에서와 마찬가지로 해당 옵션을 지정해야 합니다.
- install_base 명령은 설치를 실행하는 동안 화면에 설치 세부 정보를 인쇄하지 않습니다.

  설치하는 동안 화면에 설치 메시지를 표시하려면 *-verbose* 옵션을 사용하십시오.
- 보안상의 이유로 보고서 에이전트와 배포 서버 사이의 SSL 통신의 보안을 유지하는 공유 암호를 자동 설치에 사용할 수 없습니다. 공유 암호를 지정하려면 설치 후 보고서 에이전트 사용자(+reportagent)를 구성해야 합니다.

-command *keyword*

사용자가 사용권 계약을 수락함을 지정하는 명령을 정의합니다. 이 명령은 사용권 계약의 끝에서 대괄호 안에 있으며, -autocfg 옵션을 사용할 때는 이 명령을 반드시 사용해야 합니다. 사용권 계약 파일의 위치를 찾으려면 *install_base -h 를 실행하십시오.*

참고: 사용권 계약은 도움말이 표시된 경우에만 볼 수 있습니다. 도움말 읽기를 마치면 사용권 계약은 삭제됩니다.

-d *target_dir*

사용자 지정 설치 디렉터리를 정의합니다. 기본 설치 디렉터리는 /opt/CA/AccessControl/입니다.

중요! CA Access Control 데이터베이스를 마운트된 네트워크 파일 시스템(NFS)에 넣을 수는 없습니다.

-dns | -nodns

DNS 호스트를 사용하거나 사용하지 않고 lookaside 데이터베이스를 생성합니다. -nodns 옵션은 CA Access Control 이 설치하는 동안 DNS 의 모든 호스트에서 nslookup 을 수행하지 않도록 지정합니다.

-fips

FIPS 전용 공개 키(비대칭) 암호화를 활성화하도록 지정합니다.

-force

설치 시 활성화된 신규 구독자 업데이트(*sepmd -n* 및 *subs <pmdb> newsubs(sub_name)*)를 무시하고 설치를 계속합니다. 기본적으로, 설치를 중단하고 먼저 구독자 업데이트를 마칠지 여부를 묻습니다.

참고: 이 옵션을 사용하면 신규 구독자 업데이트는 실패합니다.

-force_encrypt

설치하는 동안 경고를 표시하지 않고 기본값이 아닌 암호화 키를 허용하도록 합니다.

중요! 업그레이드 후에 암호화 키가 기본값으로 설정됩니다.

참고: CA Access Control 은 SSL, AES(128 비트, 192 비트 및 256 비트), DES, 3DES 등의 암호화 옵션도 제공합니다.

-force_install

이미 설치된 버전 위에 새 버전을 설치합니다. 동일한 버전 위에 설치하려는 경우 이 옵션을 사용하십시오.

-force_kernel

설치하는 동안 이전 커널을 언로드할 수 없다는 경고를 표시하지 않고 설치를 계속하도록 합니다.

참고: 설치 완료 후 컴퓨터를 재부팅해야 할 수도 있습니다.

-g *groupname*

CA Access Control 파일의 그룹 소유자 이름을 정의합니다. 기본값은 0 입니다.

-h | -help

이 명령에 대한 도움말을 표시합니다.

-ignore_dep

설치 중에 다른 제품과의 종속성을 검사하지 *않도록* 지정합니다.

-key *encryption_key*

업그레이드 중에 암호화 키를 복원합니다.

참고: 업그레이드 시 업그레이드 전에 사용했던 동일한 암호화 키를 사용해야 합니다.

-lang *lang*

CA Access Control 을 설치할 언어를 정의합니다. 지원되는 언어 및 문자 집합 목록을 보려면 도움말(install_base -h)을 표시할 때 이 옵션에 대한 설명을 확인하십시오.

-lic_dir *license_dir*

아직 라이선스 프로그램이 설치되어 있지 않은 경우 라이선스 프로그램 설치 디렉터리를 정의합니다.

참고: 컴퓨터 환경에 $CASHCOMP 변수가 정의(/etc/profile.CA 에 정의 가능)되지 않은 경우에만 라이선스 프로그램이 지정된 디렉터리에 설치됩니다. 그렇지 않으면 라이선스 프로그램은 $CASHCOMP 에 설치됩니다. $CASHCOMP 가 정의되지 않았고 -lic_dir 을 지정하지 않은 경우 라이선스 프로그램은 /opt/CA/SharedComponents 디렉터리에 설치됩니다. CAWIN 은 라이선스 패키지와 같은 디렉터리에 설치됩니다.

-nolink

CA Access Control 을 기본 경로(/opt/CA/AccessControl/)에 설치하는 경우 /etc 디렉터리에 seos.ini 에 대한 링크를 작성하지 않도록 지정합니다.

CA Access Control 은 기본 디렉터리가 아닌 다른 디렉터리에 CA Access Control 을 설치하는 경우 /etc 디렉터리에 seos.ini 에 대한 링크를 만듭니다. 이를 통해 CA Access Control 은 설치 위치를 "탐지"할 수 있습니다. 기본 경로에 설치하고 보안상의 이유로 /etc 를 업데이트하지 않으려는 경우 이 옵션을 사용하십시오.

-nolog

설치 프로세스에 대한 로그를 보관하지 않도록 지정합니다. 기본적으로 설치 프로세스와 관련된 모든 트랜잭션은 *ACInstallDir*/AccessControl_install.log(여기서 *ACInstallDir* 은 CA Access Control 의 설치 디렉터리)에 저장됩니다.

-no_tng_int

설치하는 동안 Unicenter Event Management 와 selogrd 통합 설정을 시도하지 않도록 지정합니다.

이 옵션을 지정하지 않으면 설치 스크립트에서 Unicenter Event Management 가 설치되어 있는지 확인합니다. 스크립트에서 Unicenter Event Management 가 설치되어 있는 것으로 확인하면 selogrd.cfg 에 다음 행을 추가하여 Unicenter Event Management 와 selogrd 의 통합을 설정합니다.

uni *hostname*

-post *program_name*

설치 완료 후 실행할 프로그램을 지정합니다.

-pre *program_name*

설치를 시작하기 전에 실행할 프로그램을 지정합니다.

-rcert *certificate.pem*

루트 인증서 파일의 전체 경로 이름을 지정합니다.

참고: 이 옵션을 사용하는 경우 스크립트에서 tar 파일을 추출한 다음 제공된 파일과 함께 다시 패키징하여 기본 파일(def_root.pem)을 대체합니다.

-rkey *certificate.key*

루트 키 파일의 전체 경로 이름을 지정합니다.

참고: 이 옵션을 사용하는 경우 스크립트에서 tar 파일을 추출한 다음 제공된 파일과 함께 다시 패키징하여 기본 파일(def_root.key)을 대체합니다.

-rootprop

루트 암호에 대한 sepass 변경이 정책 모델에 전송되도록 지정합니다.

참고: 이 옵션은 설치 완료 후 seos.ini 파일의 AllowRootProp 토큰을 사용하여 설정할 수 있습니다. seos.ini 초기화 파일에 대한 자세한 내용은 *참조 안내서*를 참조하십시오.

-savecfg <*response_file*>

-autocfg 옵션에서 나중에 사용할 수 있게 대화형 설정에 대한 사용자 응답을 저장해 둡니다.

-stop

STOP(스택 오버플로 보호) 기능 사용을 활성화합니다.

-system_resolve

시스템에서 네트워크 캐싱을 위한 바이패스를 정의하는 시스템 기능을 사용하도록 지정합니다.

참고: IBM AIX 플랫폼에서는 이 옵션을 사용할 수 없습니다.

-v

CA Access Control 패키지의 버전을 표시합니다.

-verbose

설치 중 설치 메시지가 화면에 표시되도록 지정합니다. 이 옵션은 대화식 설치에서는 기본값이므로 *-autocfg* 옵션 사용 시 설치 메시지를 표시하려는 경우에만 지정하면 됩니다.

install_base 스크립트의 작동 방식

install_base 스크립트는 다음 단계를 수행합니다.

1. 기본 설치 디렉터리를 변경할지 여부를 사용자에게 확인합니다.
2. 사용자가 제공한 설치 옵션을 표시하고 해당 옵션으로 설치를 계속할지 여부를 확인합니다.
3. tar.Z 파일에서 설치 위치(기본값 또는 *target_dir* 지정 값)로 데이터를 추출합니다.
4. 플랫폼 유형에 따라 동작도 다릅니다.
   - Sun Solaris 의 경우 install_base 스크립트는 CA Access Control *syscall* 스크립트를 /etc/name_to_sysnum 파일에 추가합니다. 원본 파일은 /etc/name_to_sysnum.bak 로 저장됩니다. 그런 다음 부트 시퀀스의 한 부분을 형성하는 /etc/rc2.d/S68SEOS 파일을 작성합니다.
   - IBM AIX 의 경우 이 스크립트는 SEOS_syscall 스크립트를 로드합니다.
5. CA Access Control 데이터베이스를 할당, 초기화 및 포맷하고 seos.ini 파일을 생성합니다. 데이터베이스 파일은 *ACInstallDir*/seosdb 디렉터리에 있습니다. 여기서 *ACInstallDir* 은 설치 디렉터리입니다.

6. 컴퓨터가 NIS+인지 확인합니다.
   - NIS+인 경우 [passwd] 섹션의 nis_env 토큰을 *nisplus 로 설정합니다.*
   - NIS+가 아니라 NIS 인 경우 토큰을 *nis* 로 설정합니다.

     또한 rpc.nisd 가 실행 중이면 스크립트는 [passwd] 섹션의 NisPlus_server 토큰을 yes 로 설정합니다.
7. 지원되는 32 비트 플랫폼의 Sun Solaris, IBM AIX, HP-UX, Linux 에서 이 스크립트는 컴퓨터가 NIS 또는 DNS(캐시 사용) 환경에서 실행되고 있는지 파악합니다. NIS 또는 DNS 에서 컴퓨터가 실행 중인 경우 스트립트는 lookaside 데이터베이스를 자동으로 작성한 다음 seos.ini 파일의 [seosd] 섹션에서 두 개의 토큰 under_NIS_server 및 use_lookaside 를 yes 로 설정합니다.

   참고: 다른 플랫폼에서는 스크립트가 lookaside 데이터베이스를 설치할지 여부를 묻고 대상 설치 디렉터리를 확인합니다.
8. 다음 추가 정보를 묻습니다. 이 설정은 설치 후 언제라도 수정할 수 있습니다.
   - 감사 파일을 읽을 수 있는 감사자 그룹 이름
   - UNIX 사용자, 사용자 그룹 및 호스트를 모두 CA Access Control 데이터베이스에 지금 추가할지 여부
   - 데이터베이스를 PMDB 에 구독시킬지 여부 및 구독하는 경우 대상 PMDB 지정

     응답을 한다고 해서 실제로 사용자 데이터베이스가 PMDB 로 구독되지는 않으며 추후 구독을 작성할 때 지정된 PMDB 에서 이 데이터베이스에 업데이트하도록 합니다.

     이러한 질문에 대한 두 가지 안전한 응답은 다음과 같습니다.

원하는 작업	응답 방법
자신의 데이터베이스가 특정 PMDB 에 구독하도록 허용합니다.	PMDB 이름(형식: *pmd_name@hostname)*
적어도 자신이 직접 지정할 때까지는 자신의 데이터베이스가 어떤 PMDB 에도 구독하지 못하도록 합니다.	Enter 키

세 번째 응답인 _NO_MASTER_는 자신의 데이터베이스가 모든 PMDB 에 구독하도록 허용합니다. 그러나 이 응답은 PMDB 를 선택할 수 없으므로 위험할 수 있습니다.

- 암호 정책 모델 이름
- CA Access Control 의 보안 관리자가 될 사용자
- CA Access Control 이 엔터프라이즈 사용자를 지원하도록 할지 여부. 지원하도록 하는 경우 특정 엔터프라이즈 사용자를 보안 관리자로 정의할지 여부
- FIPS 전용 설치를 선택한 경우 암호화와 관련된 FIPS 전용 옵션을 지정할지 여부
- FIPS 전용 암호화를 선택하지 않은 경우 기본 암호화 방법을 바꿀지 여부

  CA Access Control 은 사용자가 선택할 수 있는 암호화 옵션으로 대칭, 공용 키 및 그 둘의 조합을 제공합니다.
- 공용 키 암호화를 선택하는 경우 CA Access Control 에서는 제목 인증서와 루트 인증서 제공 방식을 지정할 수 있습니다.

  선택한 방식에 따라 CA Access Control 에서 SSL 설정을 도와 줍니다.
- 대칭 암호화를 선택한 경우 새 암호화 키를 설정할지 여부

  참고: 암호화에 대한 자세한 내용은 *참조 안내서*의 sechkey 를 참조하십시오.
- 기본 보안 규칙 설치 여부

  관리자는 기본 보안 규칙을 사용하여 두 개의 규칙 세트를 포함한 패키지를 설치함으로써 시스템, 암호 및 로그 파일을 보다 안전하게 보호할 수 있습니다. 규칙 세트 중 하나는 CA Access Control 파일을 보호하기 위해 모든 플랫폼에 적용됩니다. 다른 규칙 세트는 UNIX 파일을 보호하며 Sun Solaris, HP-UX, IBM AIX 및 Digital DEC UNIX 플랫폼에 한정됩니다. 둘 중 하나만 설치할 수는 없습니다. 기본 보안 규칙은 실제 보호가 아닌 정보를 제공하는 경고 모드로 설치됩니다. 따라서 규칙에 익숙해지는 즉시 경고 모드를 제거하는 것이 좋습니다.
- 원격 호스트에서 CA Access Control 을 시작할 수 있도록 할지 여부
- 보고서 에이전트를 활성화할지 여부 및 활성화할 경우 CA Enterprise Log Manager 를 활성화할지 여부

  보고서 에이전트는 데이터베이스의 예약된 스냅숏을 메시지 큐로 보냅니다. 보고서 에이전트를 활성화할 경우 배포 서버 호스트 이름, 사용할 포트, 큐 이름을 정의해야 합니다. CA Enterprise Log Manager 를 활성화할 경우 감사 로그 파일의 타임스탬프가 지정된 백업이 유지되도록 지정할 수도 있습니다.

- PUPM 에이전트 사용 여부

  PUPM 에이전트는 로컬 컴퓨터에서 권한 있는 계정 암호를 가져올 수 있도록 이 컴퓨터에서 PUPM 을 구성합니다. PUPM 에이전트를 사용할 경우 보고서 서버 호스트 이름, 사용할 포트, 큐 이름을 정의해야 합니다.

- 이 끝점에서 고급 정책 관리를 설정할지 여부. 이 경우 계산 편차 결과를 보낼 배포 호스트(DH)의 이름

  dhName@hostName 형식을 사용하여 DH 호스트 이름을 정의하십시오. 예를 들어 host123.comp.com 이라는 호스트에 배포 서버를 설치한 경우에는 DH__@host123.comp.com 을 사용해야 합니다.

사후 설치 설정 구성

설치가 완료되면 CA Access Control 을 환경에 맞게 구성해야 합니다.

사후 설치 설정을 구성하려면

1. 경로에 *ACInstallDir*/bin 디렉터리를 추가합니다.

   기본적으로 설치 디렉터리는 /opt/CA/AccessControl/입니다.

2. seos.ini (페이지 245) 파일 토큰을 검사하여 설정이 요구 사항에 맞는지 확인합니다.

   필요하면 설정을 수정하십시오.

3. CA Access Control man 페이지에 액세스하려면 *ACInstallDir*/man 디렉터리를 MANPATH 에 추가합니다.

   예를 들어 현재 세션을 위해 csh 를 사용하고 있다면 다음 명령을 입력합니다.

   ```
   setenv MANPATH $MANPATH:/opt/CA/AccessControl//man
   ```

   다음 세션을 위해 .login, .profile 또는 .cshrc 파일에 유사한 행을 추가합니다.

CA Access Control 시작

X Windows 환경에서 작업하는 경우에는 CA Access Control 을 호출하고 이것이 시스템에 올바로 설치되었는지 확인한 후 다음 순서에 따라 중요한 보호 기능을 초기화합니다.

1. 루트(슈퍼 사용자) 권한으로 창을 두 개 엽니다.
2. 둘 중 하나의 창에서 다음 명령을 입력합니다.

   seload

   seload 명령이 세 개의 CA Access Control 데몬 엔진, 에이전트, Watchdog 을 시작할 때까지 기다립니다.
3. 데몬을 시작한 후 다른 창으로 이동하여 다음 명령을 입력합니다.

   secons -t+ -tv

   CA Access Control 은 운영 체제 이벤트를 보고하는 메시지를 하나의 파일에 누적합니다. 또한 secons -tv 명령은 화면에 메시지를 표시합니다.
4. seload 명령을 입력했던 첫 번째 창에서 다음 명령을 입력합니다.

   who

   CA Access Control 이 추적 메시지를 쓰고 있는 두 번째 창에서 CA Access Control 이 who 명령의 실행을 차단하고 그에 대해 보고하는지 확인합니다. who 명령의 차단에 대해 보고하면 CA Access Control 이 시스템에 올바로 설치되어 있는 것입니다.
5. 원할 경우 명령을 더 입력하여 CA Access Control 이 어떻게 반응하는지 봅니다.

   데이터베이스에는 액세스 시도를 차단하기 위한 규칙이 아직 포함되지 않았습니다. 그렇지만 CA Access Control 은 시스템을 모니터하므로 CA Access Control 이 설치되어 실행 중인 이 시스템과 연동하여 작동되는 방식 및 CA Access Control 이 차단하는 이벤트를 확인할 수 있습니다.
6. 다음 명령을 입력하여 seosd 데몬을 종료합니다.

   secons -s

   화면에 다음 메시지가 표시됩니다.

   CA Access Control 이 지금 종료됩니다!

고급 정책 관리를 위한 끝점 구성

고급 정책 관리 서버 구성 요소를 설치했으면, 고급 정책 관리를 위해 엔터프라이즈의 각 끝점을 구성해야 합니다. 이때 서버 구성 요소와 정보를 주고받을 수 있도록 끝점을 구성해야 합니다.

참고: 이 절차에서는 고급 정책 관리를 위해 기존 CA Access Control 설치를 구성하는 방법을 보여줍니다. 끝점에 CA Access Control 을 설치할 때 이 정보를 지정한 경우 끝점을 다시 구성할 필요가 없습니다.

고급 정책 관리를 위한 끝점을 구성하려면 명령 창을 열고 다음 명령을 입력합니다.

dmsmgr -config -dhname *dhName*

dhName

끝점과 함께 작동할 DH(배포 호스트) 이름 목록을 쉼표로 구분하여 정의합니다.

예: DH__@centralhost.org.com

이 명령은 고급 정책 관리를 위해 끝점을 구성하고 정의된 DH 와 작업하도록 끝점을 설정합니다.

참고: 자세한 내용은 *참조 안내서*의 dmsmgr -config 명령을 참조하십시오.

보고를 위해 UNIX 끝점 구성

CA Access Control 끝점 관리 및 보고서 포털이 설치되어 구성되면 보고서 에이전트를 활성화하고 구성하여 처리를 위해 배포 서버에 데이터를 보내도록 끝점을 구성할 수 있습니다.

참고: CA Access Control 을 설치할 때 보고를 위해 끝점을 구성할 수 있습니다. 이 절차에서는 설치 시 이 옵션을 구성하지 않은 경우 보고서 전송을 위해 기존 끝점을 구성하는 방법에 대해 설명합니다.

보고를 위해 UNIX 끝점을 구성하려면

1. *ACSharedDir*/lbin/report_agent.sh 를 실행합니다.

   report_agent config -server *hostname* [-proto {ssl|tcp}] [-port *port_number* [-rqueue *queue_name*]

   구성 옵션을 생략하면 기본 설정이 사용됩니다.

   참고: report_agent.sh 스크립트에 대한 자세한 내용은 *참조 안내서*를 참조하십시오.

2. 데이터베이스에서 *+reportagent* 사용자를 작성합니다.

   사용자는 ADMIN 과 AUDITOR 특성 및 로컬 터미널에 대한 *쓰기* 액세스 권한을 가지고 있어야 합니다. 또한 배포 서버 설치 시 정의한 보고서 에이전트 공유 암호에 대해 epassword 를 설정해야 합니다.

3. 보고서 에이전트 프로세스에 대해 SPECIALPGM 을 작성합니다.

   SPECIALPGM 은 루트 사용자를 +reportagent 사용자로 매핑합니다.

참고: 보고서 에이전트를 활성화한 후 CA Access Control 구성 설정을 수정하여 성능 관련 설정을 변경할 수 있습니다. 보고서 에이전트 구성 설정에 대한 자세한 내용은 *참조 안내서*를 참조하십시오.

예: selang 을 사용하여 보고를 위해 UNIX 끝점 구성

다음 selang 명령은 보고서 에이전트를 활성화 및 구성했다고 가정하여 필요한 보고서 에이전트 사용자를 만들고 보고서 에이전트 프로세스에 대한 특별한 보안 권한을 지정하는 방법을 보여 줍니다.

```
eu +reportagent admin auditor logical epassword(Report_Agent) nonative
auth terminal (terminal101) uid( +reportagent) access(w)
er specialpgm (/opt/CA/AcessControl/bin/ReportAgent) Seosuid(+reportagent) \
Nativeuid(root) pgmtype(none)
```

CA Access Control 사용자 지정

CA Access Control 을 사용하여 완전한 보안을 구현하려면 시행할 보안 정책을 정의해야 합니다. 보안 정책을 정의하는 데 걸리는 시간은 사이트의 크기와 보안 관리를 위해 선택한 방법에 따라 달라집니다.

예를 들어 대학에서는 대부분의 학생을 CA Access Control 에 정의할 수 없을 것으므로 학생들은 _default 설정에 따라서만 리소스에 액세스할 수 있습니다. 그러나 은행에서는 모든 사용자를 CA Access Control 에 정의하고 모든 리소스에 대한 액세스 목록을 설정하여 특정 사용자가 특정 리소스에 액세스하도록 할 수 있습니다. 따라서 사용자 수가 동일하더라도 대학에서 CA Access Control 을 구현하는 것이 은행에서 구현하는 것보다 시간이 덜 걸립니다.

사용자는 보안 관리자로서 프로젝트의 목표를 정의해야 합니다. 사이트 정책과 관련된 결정은 신중해야 합니다. CA Access Control 에는 사이트의 보안 정책을 구현하는 데 도움이 되도록 사용자 지정할 수 있는 파일이 여러 개 있습니다.

트러스트된 프로그램

트러스트된 프로그램은 변경되지 않은 경우에만 실행할 수 있는 프로그램입니다. 보통 setuid/setgid 프로그램입니다. 또한 CA Access Control 에서는 일반 프로그램을 트러스트된 프로그램으로 지정할 수도 있습니다. 프로그램이 변경되지 않은 경우 CA Access Control 이 무결성을 보장할 수 있는 PROGRAM 클래스에 등록합니다.

사용자가 트러스트된 프로그램을 사용해야만 특정 작업을 수행할 수 있도록 트러스트된 프로그램을 *프로그램 경로 지정(Program Pathing)* 기능과 함께 사용할 수도 있습니다.

참고: 프로그램 경로 지정에 대한 자세한 내용은 *UNIX 용 끝점 관리 안내서*를 참조하십시오.

CA Access Control 은 setuid 및 setgid 프로그램 전체를 트러스트된 프로그램으로 등록할 수 있는 스크립트를 제공합니다.

1. setuid 및 setgid 프로그램을 모두 기억하는 수고를 덜려면 다음에 설명하는 seuidpgm 프로그램을 사용합니다. 이 프로그램은 파일 시스템을 검색하고 모든 setuid 및 setgid 프로그램을 찾은 다음 이러한 프로그램을 PROGRAM 클래스에 모두 등록하는 selang 명령 스크립트를 생성합니다.

   이 명령을 실행합니다.

   ```
   seuidpgm -q -l -f / > /opt/CA/AccessControl//seuid.txt
   ```

   표시된 대로 실행하면 seuidpgm 은 다음을 수행합니다.

   - /로 시작하는 전체 파일 시스템을 검색합니다.
   - 메시지를 표시하지 않습니다. -q 옵션은 "cannot chdir" 메시지가 나타나지 않게 합니다.
   - 모든 심볼 링크(-l)를 무시합니다.
   - FILE 및 PROGRAM 클래스(-f) 모두에 프로그램을 등록합니다.
   - 명령을 /opt/CA/AccessControl//seuid.txt 파일에 출력합니다.

   참고: seuidpgm 에 대한 전체 설명은 *참조 안내서*를 참조하십시오.

2. 텍스트 편집기로 seuid.txt 파일을 열어 트러스트된 모든 setgid/setuid 프로그램을 포함하는지 그리고 다른 프로그램이 포함되지는 않았는지 확인합니다. 필요하다면 파일을 편집합니다.

3. selang 을 사용하여 편집한 파일의 명령을 실행합니다. seosd 데몬을 실행하지 않고 있다면 -l 스위치를 포함합니다.

   ```
   selang [-l] -f /opt/CA/AccessControl//seuid.txt
   ```

   selang 을 완료하는 데 몇 분 정도 걸릴 수 있습니다.

4. seosd 데몬을 이미 실행하고 있지 않은 경우 seosd 데몬을 다시 시작합니다. 그런 다음 시스템이 예상대로 작동하는지와 setuid 프로그램을 호출할 수 있는지 확인합니다.
5. PROGRAM 클래스의 기본 액세스를 NONE 으로 변경하여 언트러스트된 새 setuid 또는 setgid 프로그램이 보안 관리자가 모르는 상태에서 추가되어 실행되지 않도록 하는 것이 좋습니다.

   다음 selang 명령을 입력하여 기본 액세스 값을 설정합니다.

   ```
   chres PROGRAM _default defaccess(none)
   ```

참고: CA Access Control 에 능숙한 사용자는 이 연결의 UACC 클래스에 대해 기억할 것입니다. UACC 클래스는 여전히 존재하며 리소스의 기본 액세스를 지정하는 데 사용할 수 있습니다. 그러나 클래스의 기본 액세스를 지정하는 경우에는 사용상 편의를 위해 클래스의 _default 레코드를 사용하는 것이 좋습니다. _default 사양은 동일한 클래스에 대한 UACC 사양보다 우선합니다.

등록한 setuid, setgid 및 일반 프로그램을 나타내는 PROGRAM 클래스의 레코드는 다음과 같은 실행 파일 특성을 저장합니다.

- 장치-번호
- Inode
- 소유자
- 그룹
- 크기
- 만든 날짜
- 만든 시간
- 마지막 수정 날짜
- 마지막 수정 날짜
- MD5 서명
- SHA1 서명
- 체크섬 CRC(Cyclical Redundancy Check)

등록하는 각 프로그램의 가장 중요한 특성은 *트러스트된* 프로그램이라는 것입니다. 따라서 이러한 프로그램은 실행해도 좋습니다. 위에 열거한 특성이 하나라도 변경되어 프로그램이 트러스트된 상태를 잃게 되면 CA Access Control 은 프로그램이 실행되지 않게 할 수 있습니다.

등록되지 않은 프로그램 사용 모니터링

적절한 프로그램을 모두 데이터베이스에 잘 등록했는지 확실히 모르겠으면 다음 명령을 사용하여 등록되지 않은 프로그램을 찾습니다.

```
chres PROGRAM _default warning
```

경고 속성은 PROGRAM 클래스가 경고 모드가 되게 합니다. 따라서 등록되지 않은 setuid 또는 setgid 프로그램이 사용될 때마다 특수 감사 레코드가 경고로 나타나지만 그런 프로그램의 사용을 *막지는 못합니다*.

감사 로그 검토

감사 로그에서 언트러스트된 레코드를 수동으로 검색하거나 특정 프로그램이 언트러스트되었을 때 특정 알림 지침을 통보하도록 설정할 수 있습니다. 특정 알림을 사용하면 특히 사용자가 보안 관리자에게 문의하지 않고도 언트러스트된 프로그램을 대신 사용하기 때문에 관리자가 프로그램이 언트러스트되었다는 알림을 받자마자 파일을 바로 확인할 수 있습니다.

참고: 특정 감사 알림을 설정하려면 *끝점 관리 안내서*를 참조하십시오.

보호

언트러스트된 setuid 및 setgid 명령을 실행하지 못하도록 하려면 다음 명령을 실행합니다.

참고: CA Access Control 은 사용자 "nobody"를 자동으로 데이터베이스에 포함합니다.

```
newres PROGRAM _default defaccess(none) \
owner(nobody) audit(all)
```

CA Access Control 은 새 프로그램이나 변경된 프로그램의 실행을 허용하기 전에 승인을 요구함으로써 백 도어 및 트로이 목마를 방지합니다.

예를 들어 새롭고 유용한 프로그램인 setuid 프로그램을 받았다고 가정합니다. 이 프로그램이 트로이 목마가 아니라고 확신하기 때문에 모든 사용자가 실행하기를 원합니다. 이 프로그램을 트러스트된 프로그램으로 등록하려면 다음 명령을 실행합니다.

```
newres PROGRAM program-pathname \ defaccess(EXEC)
```

언트러스트된 프로그램 다시 트러스트하기

프로그램의 크기, 프로그램 수정 날짜 또는 기타 모니터링되는 프로그램 속성이 변경되어 CA Access Control 에서 언트러스트된 경우 *다시 트러스트*하여 데이터베이스에 새로 승인 등록을 해야만 다시 실행됩니다. 프로그램을 다시 트러스트하는 방법은 다음과 같습니다.

editres PROGRAM *progam_name* trust

참고: seretrust 유틸리티를 사용하여 프로그램을 다시 트러스트할 수도 있습니다. 이 유틸리티와 해당 옵션에 대한 자세한 내용은 *참조 안내서*를 참조하십시오.

초기화 파일

이 절에서는 초기화할 때 CA Access Control 이 읽어 들이는 여러 가지 파일에 대해 설명합니다. 기본적으로 CA Access Control 의 초기화 파일은 CA Access Control 의 설치 디렉터리이며 seos.ini 파일을 포함하는 디렉터리에 있습니다.

seos.ini

seos.ini 파일은 전역 매개 변수를 설정합니다.

참고: 파일 구조 및 지원되는 토큰에 대한 자세한 내용은 *참조 안내서*를 참조하십시오.

CA Access Control 이 실행되는 동안 seos.ini 파일은 READ 기반으로 모든 사용자가 항상 액세스할 수 있지만 설치된 상태로 보호되며 업데이트할 수 없습니다. CA Access Control 을 실행하는 동안 권한이 부여된 사용자가 파일을 업데이트할 수 있도록 하려면 다음 명령을 입력합니다.

newres FILE *ACInstallDir*/seos.ini owner(*authUser*) defacc(read)

ACInstallDir 은 CA Access Control 의 설치 디렉터리이며 기본값은 /opt/CA/AccessControl/입니다.

이 명령은 파일에 대한 기본 액세스를 READ 로 설정하지만 파일의 소유자인 *authUser* 만 파일을 업데이트할 수 있게 합니다.

참고: 많은 유틸리티가 프로세스 과정에서 seos.ini 파일에 액세스하기 때문에 seos.ini 파일에 대한 기본 액세스를 READ 로 하는 것이 중요합니다. 유틸리티가 파일을 읽을 수 없는 경우 실패합니다.

추적 필터 파일

이 옵션 파일은 모든 종류의 CA Access Control 추적 메시지를 필터링하기 위한 필터 마스크를 지정하는 항목을 포함하고 있습니다.

추적 필터 파일은 필터링해야 하는 추적 메시지, 즉 추적 파일에 나타나지 않는 추적 메시지를 지정합니다. 각 행에서 메시지 그룹을 식별하는 마스크를 표시하지 않도록 지정합니다. 예를 들어 다음 파일은 WATCHDOG 또는 INFO 로 시작되는 모든 메시지와 BYPASS 로 끝나는 모든 메시지가 표시되지 않게 합니다.

```
WATCHDOG*
*BYPASS
INFO*
```

기본적으로 CA Access Control 은 trcfilter.init 라는 추적 필터 파일을 사용합니다. seos.ini 파일의 [seosd] 섹션에 있는 trace_filter 토큰의 값을 편집하여 추적 필터 파일의 이름 및 위치를 변경할 수 있습니다.

추적 레코드를 필터링하려면 필요한 대로 파일을 편집하십시오. 파일에 주석(주석 행)을 추가하려면 행의 시작에 세미콜론(;)이 있어야 합니다.

trcfilter.init 파일은 사용자 추적에 의해 생성된 감사 레코드를 필터링하지 않습니다. 이러한 감사 레코드를 필터링하려면 audit.cfg 파일을 편집하십시오.

참고: 자세한 내용은 *참조 안내서*의 esosd 유틸리티를 참조하십시오.

고급 정책 관리

여러 규칙 정책(selang 명령)을 작성하여 저장한 후, 사용자가 정의하는 방식으로 기업에 배포할 수 있습니다. 이 정책 기반 방법을 사용하여 정책 버전을 저장한 다음 이를 호스트나 그룹 호스트에 할당할 수 있습니다. 할당된 정책은 배포를 위해 큐에 추가됩니다. 또는 호스트나 그룹 호스트에 직접 정책 버전을 배포 및 배포 취소할 수 있습니다.

참고: 고급 정책 관리에 대한 자세한 내용은 *엔터프라이즈 관리 안내서*를 참조하십시오.

고급 정책 관리 구성

고급 정책 기반 관리를 사용하도록 엔터프라이즈를 설정하려면 중앙 위치에 DMS 와 DH 를 설치한 다음 고급 정책 관리에 대해 각 끝점을 구성해야 합니다 (페이지 247).

고급 정책 관리 사후 설치를 위해 계층을 구성하려면 dmsmgr 유틸리티를 사용하십시오.

참고: dmsmgr 유틸리티에 대한 자세한 내용은 *참조 안내서*를 참조하십시오.

정책 위반 계산에 대한 끝점 구성

각 끝점은 정책 위반 계산을 허용하도록 구성해야 합니다. 일반적으로는 설치 시 이 작업을 수행합니다. 이 절차는 대신 이러한 사후 설치를 수행하기 위한 것입니다.

정책 위반 계산에 대해 끝점을 구성하려면 다음 selang 명령을 입력하십시오.

so dms+(*DMS@host*)

DMS@host

표시된 형식으로 지정된 DMS 의 이름을 정의합니다.

sesu 및 sepass 유틸리티

운영 체제의 passwd 명령 대신 sepass 를, su 대신 sesu 명령을 사용하는 것이 좋습니다. 이렇게 하려면 원본 시스템 바이너리를 저장하고 이를 sepass 및 sesu 의 심볼 링크로 각각 교체해야 합니다. 이 작업이 끝나면 언제라도 이러한 유틸리티를 사용할 수 있는지 확인해야 합니다.

대부분의 운영 체제에서는 CA Access Control 이 로드되지 않아도 sepass 및 sesu 유틸리티가 실행됩니다. 그러나 일부 운영 체제(예: AIX)의 경우 CA Access Control 이 로드되지 않으면 이러한 유틸리티가 실행되지 않습니다. 이러한 운영 체제의 경우 CA Access Control 이 래퍼 스크립트를 제공합니다.

sesu 및 sepass 래퍼 스크립트

sesu 및 sepass 래퍼 스크립트는 다음 디렉터리에 있습니다.

ACInstallDir/samples/wrappers

이 디렉터리에는 다음 파일이 있습니다.

파일	설명
sesu_wrap.sh	sesu 용 래퍼 스크립트
sepass_wrap.sh	sepass 용 래퍼 스크립트
README	이러한 래퍼에 대한 사용 및 개념 정보가 들어 있는 텍스트 파일

래퍼 스크립트를 사용하여 sesu 실행

래퍼 스크립트를 사용하여 sesu 유틸리티를 실행하면 CA Access Control 이 로드되어 있지 않은 경우 sesu 유틸리티가 작동되지 않는 운영 체제에서도 해당 유틸리티를 실행할 수 있습니다.

참고: CA Access Control 이 로드되어 있지 않아 sesu 유틸리티가 실행되지 않는 경우 이 절차를 따르기만 하면 됩니다.

래퍼 스크립트를 사용하여 sesu 를 실행하려면

1. 텍스트 편집기에서 sesu_wrap.sh 스크립트를 엽니다.

   래퍼 스크립트가 텍스트 편집기에 표시됩니다.

2. 필요한 경우 다음 두 가지 변수를 변경합니다.

   SEOSDIR

   CA Access Control 설치 디렉터리를 정의합니다. 기본적으로 다음 기본 설치 디렉터리로 설정됩니다.

   /opt/CA/AccessControl/

   SYSSU

   교체해야 할 원래 su 시스템 바이너리의 이름을 정의합니다. 기본적으로 다음으로 설정됩니다.

   /usr/bin/su.orig

3. sesu 유틸리티가 아니라 sesu_wrap.sh 래퍼 스크립트를 가리키도록 su 심볼 링크를 교체합니다.

   su 를 실행할 때마다 sesu 래퍼 스크립트가 sesu 유틸리티를 실행합니다.

래퍼 스크립트를 사용하여 sepass 실행

래퍼 스크립트를 사용하여 sepass 유틸리티를 사용하면 CA Access Control 이 로드되어 있지 않은 경우 sepass 유틸리티가 작동되지 않는 운영 체제에서도 해당 유틸리티를 실행할 수 있습니다.

참고: CA Access Control 이 로드되어 있지 않아 sepass 유틸리티가 실행되지 않는 경우 이 절차를 따르기만 하면 됩니다.

래퍼 스크립트를 사용하여 sepass 를 실행하려면

1. 텍스트 편집기에서 sepass_wrap.sh 스크립트를 엽니다.

   래퍼 스크립트가 텍스트 편집기에 표시됩니다.

2. 필요한 경우 다음 두 가지 변수를 변경합니다.

   SEOSDIR

   CA Access Control 설치 디렉터리를 정의합니다. 기본적으로 다음 기본 설치 디렉터리로 설정됩니다.

   /opt/CA/AccessControl/

   SYSPASSWD

   교체해야 할 원래 sepass 시스템 바이너리의 이름을 정의합니다. 기본적으로 다음으로 설정됩니다.

   /usr/bin/passwd.orig

3. sepass 유틸리티가 아니라 sepass_wrap.sh 래퍼 스크립트를 가리키도록 passwd 심볼 링크를 교체합니다.

   passwd 를 실행할 때마다 sepass 래퍼 스크립트가 sepass 유틸리티를 실행합니다.

유지 관리 모드 보호(자동 모드)

CA Access Control 에는 CA Access Control 데몬이 유지 관리를 위해 종료된 경우 보호할 수 있도록 자동 모드라는 유지 관리 모드가 있습니다. 이 모드에서는 이러한 데몬이 종료된 동안 CA Access Control 에서 이벤트를 거부합니다.

CA Access Control 은 실행 중일 때 보안상 중요한 이벤트를 차단하고 이벤트가 허용되었는지 검사합니다. 유지 관리 모드가 활성화되지 않은 상태에서 CA Access Control 서비스가 종료되면 모든 이벤트가 허용됩니다. 유지 관리 모드를 활성화하면 CA Access Control 데몬이 종료된 동안 이벤트를 거부하여 시스템 유지 관리 동안 사용자의 작업을 중단시킵니다.

유지 관리 모드는 기본적으로 비활성화되어 있으며, 필요할 때 활성화할 수 있습니다.

CA Access Control 보안 서비스가 종료되었을 때:

- 유지 관리 모드가 활성화되어 있으면 유지 관리 사용자가 실행한 이벤트와 특별한 경우를 제외하고 보안에 민감한 이벤트가 모두 거부됩니다.
- 유지 관리 모드가 비활성화되어 있으면 CA Access Control 이 아무 작업도 중단하지 않고 실행이 운영 체제로 전달됩니다.

유지 관리 모드가 활성화되고 보안이 종료된 경우 금지된 이벤트가 감사 로그 파일에 기록되지 않습니다.

유지 관리 모드를 활성화하려면 다음 단계를 수행하십시오.

중요! 루트가 유지 관리 사용자가 아닌 경우 다른 방법으로는 로그인할 수 없으므로 유지 관리 사용자를 위한 세션을 열어 두십시오.

1. CA Access Control 데몬이 종료되었는지 확인합니다.
2. seini 유틸리티를 사용하여 silent_deny 토큰 값을 *yes* 로 변경합니다.

   토큰은 SEOS_syscall 섹션 아래에 있습니다.

   ```
   seini -s SEOS_syscall.silent_deny yes
   ```

3. silent_admin 토큰 값을 CA Access Control 데몬이 종료된 동안 컴퓨터에 액세스할 수 있도록 허용할 UNIX UID(숫자)로 변경합니다.

   ```
   seini -s SEOS_syscall.silent_admin <maintenance_UID>
   ```

   참고: *루트*는 기본 유지 관리 모드 사용자(UID 0)입니다.

   중요! 유지 관리 사용자가 *루트*가 아닌 경우 CA Access Control 권한 부여 데몬 setuid 를 루트 사용자로 해야 유지 관리 모드에서 CA Access Control 을 시작할 수 있습니다. 이처럼 변경하려면 다음 명령을 입력합니다.
   chmod 6111 seosd

4. seload 명령으로 CA Access Control 데몬을 시작합니다.

   참고: 유지 관리 모드 사용자가 루트가 아닌 경우 seosd 명령으로 CA Access Control 데몬을 시작하십시오.

Solaris 10 영역 구현

Solaris 10 은 *영역*이라고 하는 다른 Solaris 인스턴스같은 가상화된 OS 서비스를 제공합니다. 모든 Solaris 10 시스템에는 *전역 영역*이라는 마스터 영역이 포함됩니다. 비전역 영역은 이 영역과 함께 실행되며, 전역 영역에서 이러한 비전역 영역을 구성, 모니터링, 제어할 수 있습니다.

CA Access Control 을 사용하여 환경에서 각 영역 또는 선택한 영역을 보호할 수 있습니다. 그렇게 하면 각 영역에 다른 규칙과 정책을 정의할 수 있어 각 영역에 대해 다른 액세스 제한을 정의할 수 있습니다.

Solaris 10 영역에 CA Access Control 을 설치하는 것은 일반 설치와 다를 바가 없으며 다음 방법 중 하나로 설치할 수 있습니다.

- Solaris 네이티브 패키지를 사용하여 CA Access Control 설치

  CA Access Control 은 Solaris 네이티브 패키지 도구(pkgadd 및 pkgrm)를 사용하여 설치 및 제거하도록 설계되었습니다.

  Solaris 네이티브 패키지 설치를 사용하여 설치한 경우 다음 중 하나를 수행할 수 있습니다.

  - 모든 영역에 CA Access Control 설치 (페이지 201).

    Solaris 10 에 CA Access Control 을 설치하는 가장 손쉽고 권장되는 방법은 전역 영역에 설치하거나, *또는* 비활성 영역과 추후 작성된 영역을 포함한 *모든* 영역에 설치하는 것입니다.

  - 선택한 영역에 CA Access Control 설치 (페이지 206).

    이 단계를 권장하지는 않지만 Solaris 네이티브 패키지 도구를 사용하여 선택한 영역에 CA Access Control 을 설치할 수 있습니다. 하지만 CA Access Control 이 모든 비전역 영역에서 동작하도록 하려면 전역 영역에 CA Access Control 을 설치하십시오.

  Solaris 네이티브 패키지를 사용하여 설치한 경우 기본 패키지를 사용하여 모든 영역에서 CA Access Control 을 제거하십시오.

- install_base 스크립트를 사용하여 각 영역에 CA Access Control 설치 (페이지 226).

  install_base 스크립트는 스크립트를 실행 중인 영역에 CA Access Control 을 설치합니다.

  CA Access Control 이 모든 비전역 영역에서 동작하도록 하려면 전역 영역에 CA Access Control 을 설치하십시오.

  install_base 스크립트를 사용하여 CA Access Control 을 설치한 경우 각 비전역 영역에서 CA Access Control 을 제거할 수 있습니다. 단, CA Access Control 커널은 전역 영역에서만 *그리고* CA Access Control 이 모든 영역에서 중단된 후에만 제거할 수 있습니다.

  참고: Solaris 11 의 제한 사항으로 인해 CA Access Control 패키지는 설치 중 비전역 영역으로 전파되지 않습니다. Solaris 네이티브 패키지 도구(pkgadd)를 사용하여 각 영역에 개별적으로 CA Access Control 을 설치할 것을 권장합니다.

중요! 모든 영역에서 CA Access Control 을 제거하기 전에 먼저 install_base 를 사용하여 전역 영역에서 CA Access Control 을 제거하면 사용자가 이 영역에 로그인할 수 없게 될 수도 있습니다. Solaris 네이티브 패키지를 사용하여 Solaris 영역에서 CA Access Control 을 설치하고 제거할 것을 권장합니다.

영역 보호

CA Access Control 은 컴퓨터 보호 시와 마찬가지 방식으로 Solaris 10 영역을 보호합니다. 각 영역이 다른 영역과 격리되어 보호되며 사용자가 CA Access Control 에 정의한 각 규칙이 해당 영역에서 작업 중인 사용자에게만 적용됩니다. 전역 영역에서 적용한 규칙은 전역 영역 이외의 영역에서 볼 수 있는 리소스에 적용되는 규칙이라 해도 전역 영역에서 액세스한 사용자에게만 적용됩니다.

참고: 필요에 따라 전역 영역 이외의 영역과 전역 영역에서 모두 전역 영역 이외의 영역 리소스를 보호하도록 하십시오.

예제: 전역 영역 규칙과 전역 영역 이외의 영역 규칙

다음 예제에서는 전역 영역 이외의 영역(myZone1) 파일을 보호하도록 규칙을 정의합니다. 모든 시스템 파일은 전역 영역에서 항상 볼 수 있습니다.

보호하고자 하는 파일은 /myZone1/root/bin/kill(전역 영역의 경로)입니다. 이 파일을 보호하기 위해 다음 CA Access Control 규칙을 정의합니다.

- 전역 영역에서

  nu admin_pers owner(nobody)
  nr FILE /myZone1/root/bin/kill defaccess(none) owner(nobody)
  authorize FILE /myZone1/root/bin/kill uid(*admin_pers*) access(all)

- myZone1(전역 영역 이외의 영역)에서

  nu admin_pers owner(nobody)
  nr FILE /bin/kill defaccess(none) owner(nobody)
  authorize FILE /bin/kill uid(*admin_pers*) access(all)

전역 영역 및 전역 영역 이외의 영역에서 모두 이러한 규칙을 사용하여 사용자(admin_pers)를 정의하였고, 파일을 보호할 리소스로 정의하였고, 사용자가 파일에 액세스할 수 있도록 권한을 부여했습니다. 두 영역 모두에서 이러한 작업을 하지 않으면 리소스가 계속 노출된 상태로 남게 됩니다.

새로운 영역 설정

Solaris 기본 패키지를 사용하여 모든 영역에 CA Access Control 을 설치하면 원래 설치 이후에 작성된 영역에도 CA Access Control 이 자동으로 설치됩니다. 그러나 사후 설치 CA Access Control 절차 스크립트는 전역 영역 이외의 영역에서 새 영역에 대해 실행되어야 하는 반면 이러한 스크립트는 새 영역 구성이 완료된 후에만 실행 가능합니다. 구체적으로, "zlogin -C *zonename*" 명령(이름 서비스, 루트 암호 등의 구성을 완료함)을 실행해야 합니다.

중요! "zlogin -C *zonename*" 명령을 실행하지 않거나 부팅 후 지나치게 빨리 새 영역에 로그인하면 사후 설치 스크립트가 실행되지 않아 CA Access Control 설치가 완료되지 않습니다.

참고: 새 영역을 제대로 설치하는 방법에 대한 자세한 내용은 Sun 의 *시스템 관리 안내서: Solaris 컨테이너 - 리소스 관리 및 Solaris 영역*(Sun Microsystems Documentation 웹 사이트에서 볼 수 있음) 을 참조하십시오.

Solaris 브랜드된 영역에 설치

Solaris 의 경우 pkgadd 가 Solaris 10 전역 영역에 설치된 응용 프로그램을 브랜드된 영역으로 전파하는 것을 지원하지 않는 제한 사항이 있습니다. 또한 커널 모듈과 통신하기 위해 CA Access Control 는 syscall 대신 ioctl 을 사용해야 합니다.

Solaris 브랜드된 영역에 설치하려면

1. pkgadd 를 사용하여 Solaris 전역 영역에 CA Access Control 를 설치합니다.
2. pkgadd 를 사용하여 Solaris 브랜드된 영역에 CA Access Control 를 설치합니다.

   참고: 설치 매개 변수 파일을 사용하면 전역 영역에 설치할 때 이 작업을 자동으로 수행할 수도 있습니다.
3. 브랜드된 영역에서 seos.ini 항목 SEOS_use_ioctl 이 1 로 설정되었는지 확인하여 필요하면 수정합니다.

   이렇게 하면 CA Access Control 가 ioctl 을 사용하도록 구성됩니다.
4. 전역 영역에서 seos.ini 항목 SEOS_use_ioctl 이 1 로 설정되었는지 확인합니다.

   이렇게 하면 CA Access Control 가 ioctl 을 사용하도록 구성됩니다.

   이제 설치가 완료되었으며 브랜드된 영역에서 CA Access Control 를 시작할 수 있습니다.

   중요! SEOS_use_ioctl 이 0 으로 설정되어 있으면 모든 영역에서 통신에 ioctl 을 사용하도록 CA Access Control 을 수정해야 합니다. 이렇게 변경한 다음 모든 영역을 다시 부팅하면 설치가 완료됩니다.

ioctl 을 사용하여 통신

CA Access Control 를 Solaris 브랜드된 영역에서 설치하려면 syscall 대신 ioctl 을 사용하여 커널 모듈과 통신해야 합니다.

ioctl 을 사용하여 통신하도록 CA Access Control 을 수정하려면

1. 전역 영역과 모든 비전역 영역에서 CA Access Control 를 중단합니다.

   이벤트 차단을 비활성화하고 커널 모듈 언로드를 준비하기 위해 secons -sk 를 사용하여 마지막 영역을 중단합니다.

2. 전역 영역에서 CA Access Control 커널 모듈을 언로드합니다(SEOS_load -u).

   참고: SEOS_load -u 명령을 사용하면 언로드할 때까지 CA Access Control 가 비전역 영역에서 실행되지 않습니다.

3. CA Access Control 가 설치된 각 영역(전역, 비전역, 브랜드된 영역)에서 seos.ini 항목 SEOS_use_ioctl 을 1 로 설정합니다(기본값: 0).

4. 전역 영역에서 커널 모듈을 로드합니다(SEOS_load).

   이렇게 하면 CA Access Control 가 ioctl 을 통해 커널 모듈과 통신할 수 있도록 의사(pseudo) 장치를 설치하고 ioctl 을 사용할 수 있도록 재부팅이 필요한 영역을 확인합니다.

5. 재부팅이 필요한 것으로 확인된 CA Access Control 가 설치된 각 비전역 및 브랜드 영역을 다시 부팅합니다.

영역에서 CA Access Control 시작 및 중지

Solaris 10 영역에서의 CA Access Control 시작과 중지는 Solaris 컴퓨터에서 일반적으로 CA Access Control 을 시작하고 중지하는 것과 동일한 방식으로 이루어집니다.

영역에서 CA Access Control 을 시작할 때에는 다음 예외가 적용됩니다.

- CA Access Control 커널 모듈(SEOS_load)은 전역 영역에서만 로드할 수 있습니다.
- 전역 영역 이외의 영역에서 CA Access Control 을 시작하기 전에 전역 영역에서 CA Access Control 커널을 로드해야 합니다.

  일단 CA Access Control 커널 모듈이 전역 영역에 로드되면 전역 영역 이외의 영역에서 원하는 순서대로 CA Access Control 을 시작하고 중지할 수 있습니다.

영역에서 CA Access Control 을 중지할 때에는 다음 예외가 적용됩니다.

- 하나 이상의 영역에 유지 관리 모드 (페이지 250)가 활성화된 경우에는 CA Access Control 커널 모듈을 언로드할 수 없습니다.
- 각 영역에서 *secons -s* 명령을 실행하면 모든 영역에서 CA Access Control 을 원하는 순서대로 중지할 수 있습니다.
- 모든 영역을 GHOST 레코드에 추가한 다음 전역 영역에서 secons -s *ghost_name* 명령을 실행하면 모든 영역에서 동시에 CA Access Control 을 중지할 수 있습니다.

  이러한 방식은 예를 들어 모든 영역에서 CA Access Control 을 업그레이드하고자 하는 경우 유용합니다.
- *secons -sk* 를 사용하여 마지막 영역을 중단하여 이벤트 차단을 비활성화하고 언로드할 수 있도록 CA Access Control 커널 모듈을 준비해야 합니다.
- CA Access Control 커널 모듈(SEOS_load -u)은 전역 영역에서만 언로드할 수 있습니다.

  참고: SEOS_load -u 명령을 사용하면 언로드할 때까지 CA Access Control 가 비전역 영역에서 실행되지 않습니다.

전역 영역 이외의 영역에서 CA Access Control 시작

평상 시와 마찬가지로 전역 영역 이외의 영역에서 CA Access Control 을 시작할 수 있지만 전역 영역에 먼저 CA Access Control 커널 모듈을 로드해야 합니다.

전역 영역 이외의 영역에서 CA Access Control 을 시작하려면

1. 글로벌 영역에서 SEOS_load 명령을 입력하여 CA Access Control 커널 모듈을 로드합니다.

   CA Access Control 커널이 로드되고 이제 어느 영역에서나 CA Access Control 을 시작할 수 있습니다.

   참고: CA Access Control 커널이 로드되어도 CA Access Control 가 글로벌 영역의 이벤트를 차단하지는 않습니다.

2. 전역 영역 이외의 영역에서 seload 명령을 입력하여 해당 영역에서 CA Access Control 을 시작합니다.

   전역 영역 이외의 영역은 CA Access Control 에 의해 보호됩니다.

   참고: 전역 영역 이외의 영역에서 원격으로 CA Access Control 을 시작할 수도 있습니다. 자세한 내용은 *참조 안내서*의 seload 명령을 참조하십시오.

zlogin 유틸리티 보호

zlogin 유틸리티를 사용하면 관리자가 영역에 들어갈 수 있습니다. 이 유틸리티에서 전역 영역 이외의 영역에 로그인할 수 있는 사용자를 제어하려면 LOGINAPPL 리소스를 추가해야 합니다.

CA Access Control 에는 zlogin 유틸리티를 보호할 수 있도록 미리 정의된 LOGINAPPL 리소스가 함께 제공됩니다.

자동으로 CA Access Control 시작

CA Access Control 을 테스트하고 기능을 실험적으로 사용해 보았다면 CA Access Control 보호를 구현할 준비가 된 것입니다.

리소스를 즉시 보호하기 위해 부팅 시 seosd 데몬을 자동으로 시작하도록 조정하려면 *ACInstallDir*/samples/system.init/*sub-dir* 디렉터리를 사용하십시오. 여기서 *sub-dir* 은 운영 체제의 디렉터리입니다. 각 하위 디렉터리에는 각 운영 체제에서 이 작업을 수행하는 데 필요한 지침과 함께 README 파일이 들어 있습니다.

CA Access Control 을 관리하기 위해 Service Management Facility 사용

Solaris 10 에서 유효

Solaris Service Management Facility(SMF) 유틸리티를 사용하여 CA Access Control 데몬을 관리할 수 있습니다. SMF 유틸리티를 사용하여 권한 부여 데몬(seosd)(이 데몬은 watchdog 데몬(seoswd)을 관리함)과 seagent 데몬을 제어합니다. seload 및 secons 명령 대신 SMF 관련 명령을 사용합니다.

참고: Service Management Facility 유틸리티를 사용하여 Solaris 10 에 CA Access Control 을 설치한 이후에 CA Access Control 을 즉시 관리할 수 있습니다.

참고: seload 및 secons 명령에 대한 자세한 내용은 *참조 안내서*를 참조하십시오.

SMF 명령은 다음 형식을 사용합니다.

#svcadm enable *데몬*

#svcadm disable *데몬*

#svcadm restart *데몬*

#svcadm refresh *데몬*

#svcs *데몬*

#svcs -l *데몬*

#svcadm clear *데몬*

예: seosd 데몬 시작

다음 예는 seosd 데몬을 시작하는 방법을 보여줍니다.

```
#svcadm enable seosd
```

참고: 이 명령은 seload 명령을 사용하는 것과 동일합니다.

예: seosd 데몬 중지

다음 예는 seosd 데몬을 중지하는 방법을 보여줍니다.

```
#svcadm disable seosd
```

참고: 이 명령은 secons -sk 명령을 사용하는 것과 동일합니다.

예: sesod 데몬 다시 시작

다음 예는 seosd 데몬을 다시 시작하는 방법을 보여줍니다.

```
#svcadm restart seosd
```

예: seosd 구성 다시 로드

이 예는 seosd 데몬 구성을 다시 로드하는 방법을 보여줍니다.

```
#svcadm refresh seosd
```

참고: 이 명령은 secons -rl 명령을 사용하는 것과 동일합니다.

예: seosd 데몬의 상태 표시

다음 예는 seosd 데몬의 상태를 나열하는 방법을 보여줍니다.

```
#svcs -l seosd
```

예: seosd 데몬의 유지 관리 상태 삭제

다음 예는 seosd 데몬의 유지 관리 서비스 상태를 삭제하는 방법을 보여줍니다.

```
#svcadm clear seosd
```

제 9 장: UNAB 호스트 설치 및 사용자 지정

이 섹션은 다음 항목을 포함하고 있습니다.

UNAB 호스트

UNIX 인증 브로커(UNAB)는 Active Directory 데이터 저장소를 사용하여 UNIX 컴퓨터에 로그인할 수 있게 해 줍니다. 즉, 모든 사용자에 대해 단일 리포지토리를 사용할 수 있으므로 사용자들이 동일한 사용자 이름과 암호로 모든 플랫폼에 로그인할 수 있게 됩니다.

UNIX 계정을 Active Directory 와 통합하면 엄격한 인증 및 암호 정책을 시행하고, 기본 UNIX 사용자 및 그룹 속성을 Active Directory 로 전송할 수 있습니다. 이렇게 하면 Windows 사용자와 그룹을 관리하는 동일한 위치에서 UNIX 사용자 및 그룹도 관리할 수 있게 됩니다.

참고: UNAB 는 설치될 때 기존의 어떠한 PAM 모듈도 대체하지 않습니다. UNAB PAM 은 기존 PAM 스택에 삽입되어 있습니다.

UNAB 구현 방법

UNAB 구현을 시작하기 전에 회사에서 UNAB 를 사용자 지정하고, 설치하고, 구성하기 위한 다음과 같은 단계를 검토하는 것이 좋습니다.

1. UNIX 컴퓨터 이름이 확인되는지 검사합니다. (페이지 275)
2. 시스템 호환성을 검사 (페이지 272)합니다.

   uxpreinstall 유틸리티는 시스템이 UNAB 요구 사항을 충족하는지 검사합니다.

3. UNAB 설치 패키지를 사용자 지정합니다. (페이지 276)

   참고: UNAB 를 설치하려는 모든 UNIX 호스트에 대해 UNAB 설치 패키지를 사용자 지정할 필요는 없습니다. 설치 패키지를 각 운영 체제에 대해 한 번 사용자 지정한 다음 이 패키지를 사용하여 회사에 UNAB 를 설치하십시오.

4. CA Access Control 엔터프라이즈 관리와 함께 동작하도록 UNAB 를 구성합니다 (페이지 281).

   UNAB 끝점을 관리하려면 CA Access Control 엔터프라이즈 관리 서버 사용자 인터페이스를 사용하십시오.

5. UNIX 호스트에 UNAB 패키지를 설치합니다.

   참고: 시스템 요구 사항 및 운영 체제 지원에 대한 자세한 내용은 *릴리스 정보*를 참조하십시오.

6. Active Directory 에 UNIX 호스트를 등록합니다 (페이지 318).
7. UNAB 를 시작합니다. (페이지 322)

   이 단계는 UNAB 데몬(uxauthd)을 시작합니다.

8. CA Access Control 엔터프라이즈 관리에 로그인 권한 부여 정책을 만들어 UNAB 끝점에 할당합니다.

   로그인 정책이 UNIX 호스트에 대한 액세스를 허용 또는 거부할 엔터프라이즈 사용자 및 그룹을 정의합니다.

   참고: 로그인 정책에 대한 자세한 내용은 *엔터프라이즈 관리 안내서*를 참조하십시오.

9. UNIX 에서 UNAB 를 활성화합니다 (페이지 322).

   UNAB 를 활성화하면 엔터프라이즈 사용자가 UNIX 호스트에 로그인할 수 있게 됩니다.

10. (선택 사항) UNAB 를 완전 통합 모드에서 구현합니다 (페이지 323).

    완전 통합 모드에서 UNAB 는 Active Directory 를 사용하여 사용자를 인증 및 권한 부여합니다.

시작하기 전에

UNAB 를 설치하기 전에 사전 요구 사항을 충족하고 필요한 정보가 있는지 확인하십시오. UNAB 를 구현하고 예비 검사를 수행하기 위해 완료해야 하는 단계를 검토하는 것이 좋습니다.

설치 모드

UNAB 는 다음과 같은 두 가지 설치 모드를 지원합니다.

- **완전 통합** - 완전 통합 모드에서 UNIX 호스트는 사용자의 인증 및 권한 부여를 모두 Active Directory 서버에 의존합니다.
- **부분 통합** - 부분 통합 모드에서 UNIX 호스트는 인증만 Active Directory 서버에 의존하고, 권한 부여는 UNIX 기반 사용자 저장소를 사용합니다. UNIX 사용자 저장소가 있는 경우 부분 통합 모드를 사용하십시오.

Active Directory 사이트 지원

UNAB 를 설치하기 전에 UNAB 가 Active Directory 사이트 지원을 구현하는 방법을 이해해야 합니다. Active Directory 사이트는 네트워크 트래픽을 최적화하고, 연결 속도를 높이고, 응답 시간을 줄이기 위한 노력을 지원합니다.

UNAB 끝점을 Active Directory 에 등록할 때 기본적으로 uxconsole 유틸리티가 다음을 수행합니다.

- 끝점의 실제 위치와 가장 가까운 Active Directory 사이트를 찾습니다.
- Active Directory 사이트의 이름을 uxauth.ini 파일의 ad 섹션에 있는 ad_site 구성 설정에 기록합니다.

등록 후에 UNAB 끝점은 찾은 Active Directory 사이트의 도메인 컨트롤러(DC)하고만 통신합니다. 끝점이 이 사이트의 DC 와 통신할 수 없으면 UNAB 끝점의 상태가 오프라인으로 변경됩니다.

기본 동작을 변경하지 않는 것이 좋습니다. 하지만 UNAB 설치 패키지를 변경할 때 UNAB 끝점이 통신하는 DC 목록과 UNAB 끝점이 무시하는 목록(각각 lookup_dc_list 및 ignore_dc_list 매개 변수)을 지정할 수 있습니다. 이 목록에 지정하는 DC 는 다음 방법으로 Active Directory 사이트 지원과 상호 작용합니다.

- lookup_dc_list - UNAB 끝점은 이 구성 설정에 나열된 DC 와 통신하고 Active Directory 사이트 지원 또는 DNS 쿼리로 찾은 DC 와 통신하지 않습니다.
- ignore_dc_list - UNAB 끝점은 Active Directory 사이트 지원 또는 이 구성 설정에 나열되지 *않은* DNS 쿼리로 찾은 모든 DC 와 통신합니다.

참고: 설치 후에 uxconsole -register 유틸리티를 사용하여 UNAB 끝점이 통신하는 Active Directory 사이트를 직접 설정할 수 있습니다. uxconsole 유틸리티에 대한 자세한 내용은 *참조 안내서*를 참조하십시오.

64 비트 Linux 호스트에 대한 설치 고려 사항

Linux 64 비트 컴퓨터에 UNAB 를 설치하기 전에 다음과 같은 운영 체제 32 비트 라이브러리가 설치되어 있는지 확인해야 합니다.

ld-linux.so.2, libICE.so.6, libcrypt.so.1, libdl.so.2, libgcc_s.so.1, libm.so.6, libnsl.so.1, libpam.so.0, libpthread.so.0, libresolv.so.2, libstdc++.so.5(및 커널 v2.6 에서 libstdc++), libaudit.so.0(RHEL5 및 OEL 5 에만 해당)

다음은 필요한 관련 RPM 패키지의 목록입니다.

- SLES 10: compat-libstdc++, glibc-32bit, libgcc, pam-32bit
- SLES 9: glibc-32bit, libgcc, libstdc++, pam-32bit
- RHEL 5 및 OEL 5: audit-libs, compat-libstdc++, glibc, libgcc, pam
- RHEL 4 및 OEL 4: compat-libstdc++, glibc, libgcc, pam
- RHEL 3: glibc, libgcc, libstdc++, pam

s390x 64 비트 컴퓨터에 UNAB 를 설치하기 전에 다음과 같은 운영 체제 32 비트 라이브러리가 설치되어 있는지 확인해야 합니다.

ld.so.1, libcrypt.so.1, libc.so.6, libdl.so.2, liblaus.so.1(RHEL 3), libaudit.so.0(RHEL 4, RHEL 5), libm.so.6, libnsl.so.1, libpam.so.0, libresolv.so.2

다음은 필요한 관련 RPM 패키지의 목록입니다.

- SLES 10: compat-libstdc++, glibc-32bit, pam-32bit
- SLES 9: glibc-32bit, libstdc++, pam-32bit
- RHEL 5: audit-libs, compat-libstdc++, glibc, pam
- RHEL 4: audit-libs, compat-libstdc++, glibc, pam
- RHEL 3: glibc, laus-libs, libstdc++, pam

Linux s390 끝점에 대한 설치 고려 사항

메시지 큐 기능을 사용하려는 경우 CA Access Control Linux s390 에서 UNAB 를 원격으로 관리하고 Linux IA64 에서 보고 기능을 사용하려면 끝점에 J2SE 버전 5.0 이상을 설치하십시오.

메시지 큐 기능을 사용하면 CA Access Control 끝점에서 보고서 포털 및 CA Enterprise Log Manager 로 각각 보고서와 감사 데이터를 보낼 수 있습니다. 원격 관리는 CA Access Control 엔터프라이즈 관리를 사용하여 UNAB 끝점을 관리할 수 있게 해줍니다.

끝점에 CA Access Control 또는 UNAB 를 설치하기 전 또는 이후에 J2SE 를 설치할 수 있습니다. CA Access Control 또는 UNAB 를 설치한 이후에 J2SE 를 설치하는 경우 또한 끝점에서 Java 위치를 구성해야 합니다.

설치가 Java 와 상호 작용하는 방법

Linux s390, Linux s390x, Linux IA64 에 해당

메시지 큐 기능을 사용하려면 경우 UNAB Linux s390 끝점을 원격으로 관리하고 Linux IA64 및 Linux s390 에서 보고 기능을 사용하려면 끝점에 지원되는 Java 버전을 설치하십시오.

Linux s390 또는 Linux IA64 끝점에 CA Access Control 또는 UNAB 를 설치할 때 설치는 다음을 수행합니다.

1. 올바른 Java 환경의 경로에 대해 다음 위치를 검사합니다.
   a. 설치 입력의 JAVA_HOME 매개 변수

      설치 입력은 UNAB 설치 매개 변수 파일, UNIX CA Access Control 설치 매개 변수 파일, 네이티브 설치를 위해 사용자 지정된 패키지, 대화형 CA Access Control 설치의 사용자 입력을 포함합니다.

   b. JAVA_HOME 환경 변수

   c. (Linux s390 및 Linux s390x) 기본 설치 경로: /opt/ibm/java2-s390-50/jre
2. accommon.ini 파일의 전역 설정에서 java_home 구성 설정의 값을 다음 값 중 하나로 설정합니다.
   - 설치가 올바른 환경에 대한 경로를 찾으면 구성 설정의 값을 이 경로로 설정합니다.
   - 설치가 올바른 환경에 대한 경로를 찾지 못하면 구성 설정의 값을 *ACSharedDir*/JavaStubs 로 설정합니다.

     기본적으로 *ACSharedDir* 는 /opt/CA/AccessControlShared 입니다.

Linux s390 및 Linux s390x 끝점에서 Java 위치 구성

Linux s390 및 Linux s390x 에 해당

메시지 큐 기능을 사용하고 원격으로 UNAB Linux s390 끝점을 관리하려면 끝점에 J2SE 버전 5.0 이상을 설치해야 합니다. CA Access Control 또는 UNAB 설치 후 J2SE 를 설치하는 경우 추가 구성 단계를 수행해야 합니다.

Linux s390 및 Linux s390x 끝점에서 Java 위치를 구성하려면

1. CA Access Control 과 UNAB 가 실행 중인 경우 중지합니다.
2. accommon.ini 파일의 전역 섹션에서 java_home 구성 설정의 값을 Java 설치 경로로 변경합니다.

   예: java_home=/opt/ibm/java2-s390-50/jre
3. CA Access Control 및 UNAB 를 시작합니다.

   Java 위치가 구성됩니다.

Linux IA64 끝점에서 Java 위치 구성

Linux IA64 에 해당

메시지 큐 기능을 사용하고 CA Access Control Linux IA 64 끝점에서 보고 기능을 사용하려면 끝점에 J2SE 버전 6.0 이상을 설치하십시오. CA Access Control 설치 후 J2SE 를 설치하는 경우 추가 구성 단계를 수행해야 합니다.

Linux IA64 끝점에서 Java 위치를 구성하려면

1. CA Access Control 이 실행 중인 경우 중지합니다.
2. accommon.ini 파일의 전역 섹션에서 java_home 구성 설정의 값을 Java 설치 경로로 변경합니다.

   예: java_home=/usr/share/java016.0/jre
3. CA Access Control 을 시작합니다.

   Java 위치가 구성됩니다.

Kerberos 및 SSO 고려 사항

Kerberos SSO(Single Sign On) 서비스를 이용하여 한 번 인증하고 동일한 사용자 자격 증명으로 여러 끝점에 로그인하기 위해 Kerberos 를 사용하는 끝점에 UNAB 를 설치 및 등록할 수 있습니다. 아직 구성되지 않았으면 Kerberos 를 사용하는 네트워크 서비스 및 응용 프로그램을 설치 및 구성하여 끝점에서 SSO 기능을 활성화합니다.

구성은 시스템마다 차이가 있으므로 끝점에서 Kerberos 와 SSO 를 사용하기 전에 다음을 수행할 것을 강력히 권장합니다.

- 시스템 man 페이지와 SSO 에서 사용할 예정인 네이티브 응용 프로그램 서비스 바이너리(특히 아래 항목)의 특정 옵션에 대해 읽으십시오.
  - sshd(1M)
  - telnetd
  - in.telnetd
  - inetd
  - pam.conf
  - inetd.sec

- Kerberos 를 지원하는 네트워크 응용 프로그램 버전의 PATH 변수를 확인하십시오. 예를 들어, 대부분의 Linux 시스템에서 Kerberos 도구는 /usr/Kerberos 디렉터리에 있습니다.
- 다음과 같은 Kerberos 를 지원하는 응용 프로그램이 아래와 같이 구성되었는지 확인하십시오.
  - SSH - 자격 증명 위임 지원, 예를 들어, GSSAPIDelegateCredentials 토큰을 yes 로 설정
  - SSHD - GSSAPIAuthentication 토큰 지원 및 사용
  - Telnet - Solaris 에서, PAM 스택이 구성되고 Kerberos 구성 및 keytab 파일 사용 가능. keytab 파일을 사용할 수 있게 하려면 심볼 링크 또는 환경 변수 KRB5_CONFIG 및 KRB5_KTNAME 을 만드십시오.
  - rlogin - Kerberos 를 지원하는 응용 프로그램의 버전을 설치

참고: 시스템에 고유한 Kerberos 및 SSO 구성에 대한 정보는 시스템 설명서를 참조하십시오.

예: Solaris 에서 Kerberos 구성

다음 예는 Solaris 에서 Kerberos 를 구성하기 위해 필요한 구성을 설명합니다. 이 예에서는 Kerberos 를 활성화하기 위해 Solaris 패키지를 설치 및 구성합니다.

중요! Kerberos 에 사용하는 시스템을 구성하기 위해 추가 패키지를 설치 및 구성해야 할 수 있습니다.

- 강력한 암호화를 사용하기 위해 SUNWcry 패키지를 설치합니다.
- Solaris 10 에서 SSH 는 GSSAPIDelegateCredentials 를 지원하지 않습니다.
- rsh, rlogin, telnet 서비스를 사용하기 위해 svc:/network/shell:kshell, svc:/network/login:klogin, svc:/network/telnet:default 를 활성화합니다.
- Kerberos 인증을 처리하기 위해 /etc/pam.conf 파일을 수정합니다.

다음은 rlogin, rsh, telnet 에 대해 Kerberos 인증을 활성화하는 추가된 섹션을 나타내는 /etc/pam.conf 파일의 코드 조각입니다.

```
# Kerberized rlogin service
#
krlogin      auth required                pam_unix_cred.so.1
krlogin      auth required                pam_krb5.so.1
#
# rsh service (explicit because of pam_rhost_auth,
# and pam_unix_auth for meaningful pam_setcred)
#
rsh          auth sufficient              pam_rhosts_auth.so.1
rsh          auth required                pam_unix_cred.so.1
#
# Kerberized rsh service
#
krsh         auth required                pam_unix_cred.so.1
krsh         auth required                pam_krb5.so.1
#
# Kerberized telnet service
#
ktelnet      auth required                pam_unix_cred.so.1
ktelnet      auth required                pam_krb5.so.1
```

Kerberos 사용 환경에서 UNAB 등록이 작동하는 방식

Active Directory 에 호스트를 등록할 때 UNAB 는 네이티브 Kerberos 와 동일한 위치에 사용자 티켓을 만듭니다. 그런 다음 사용자는 TGT(Ticket Granting Ticket)를 수동으로 획득할 필요 없이 Kerberos 사용 응용 프로그램을 투명하게 사용할 수 있습니다.

Kerberos 사용 호스트에서 UNAB 등록 프로세스는 다음과 같습니다.

1. uxconsole -register 명령을 실행하고 -sso 인수를 사용하여 UNAB 를 Active Directory 에 등록합니다.

   -sso 인수는 uxconsole 이 uxauth.ini 파일이 아닌 호스트 Kerberos 파일을 사용하도록 강제합니다.

2. uxconsole 이 UNAB 가 구성을 위해 호스트 Kerberos 파일을 사용할 수 있음을 확인합니다. 다음 중 *하나*가 발생합니다.

   a. uxconsole 이 이 파일에 UNAB 를 등록하기 위해 필요한 도메인 정보가 있음을 식별합니다.

   b. uxconsole 이 이 파일에 등록하기 위해 필요한 정보가 없음을 식별합니다.

3. 이 파일에 정보가 수록되어 있지 않으면 UNAB 가 원래 파일의 백업을 만들고 kerberos_configuration 토큰을 internal 로 설정합니다.

   참고: uxconsole -deregister 명령을 사용하여 UNAB 를 Active Directory 에서 제거하면 Kerberos 구성 파일이 수정되지 않으며 백업 파일도 제거되지 않습니다.

4. 이 파일에 필요한 정보가 수록되어 있으면 uxconsole 은 kerberos_configuration 토큰을 standard 로 설정합니다.

5. uxconsole 이 등록 프로세스를 계속합니다.

   참고: uxconsole -register 명령 및 seos.ini kerberos_configuration 토큰에 대한 자세한 내용은 *참조 안내서*를 참조하십시오.

중요! 호스트의 Kerberos 파일에 UNAB 를 등록하기 위해 필요한 정보가 없으면 등록이 실패합니다.

SSO 에 대해 UNAB 호스트를 활성화

SSO 에 대해 UNAB 를 구성하여 한 UNAB 호스트에 로그인한 Active Directory 사용자들이 자신의 사용자 이름을 사용하여 다른 UNAB 호스트에 로그인하도록 활성화할 수 있습니다. SSO 활성화된 모드에서 UNAB 는 UNIX 리포지토리에 자신이 생성한 키를 유지합니다. Kerberos 활성화된 응용 프로그램은 이 키를 사용하여 사용자들이 다른 호스트에 로그인할 때 사용자를 인증합니다.

중요! SSO 모드로 UNAB 를 활성화하는 각 호스트가 Kerberos 에 대해 활성화되었는지 확인하십시오. 이 절차를 시작하기 전에 uxpreinstall 유틸리티를 사용하여 시스템 호환성을 검사하십시오.

SSO 에 대해 UNAB 를 활성화하려면

1. root 로 UNIX 호스트에 로그인합니다.
2. SSO 모드에서 Active Directory 에 UNAB 를 등록합니다. 다음 명령을 실행합니다.

   ```
   ./uxconsole -register -d<active_directory_domain> -sso
   ```

   참고: SSO 모드에서 UNAB 를 등록하기 전에 UNAB 를 등록 취소할 필요는 없습니다.
3. 사용자들이 UNIX 호스트에 로그인할 수 있도록 UNAB 를 활성화합니다. 다음 명령을 실행합니다.

   ```
   ./uxconsole -activate
   ```
4. -status -detail 인수를 사용하여 Kerberos 모드가 Standard 로 설정되었는지 확인합니다. 예:

   ```
   ./uxconsole -status -detail | grep Kerberos

       Kerberos configuration - standard
   ```

   SSO 에 대해 UNAB 호스트를 구성했습니다.

시스템 호환성 검사

uxpreinstall 유틸리티는 UNIX 컴퓨터가 UNAB 시스템 요구 사항을 준수하는지 검사합니다. UNAB 를 시작하여 활성화하기 전에 uxpreinstall 을 사용하여 시스템 호환성을 검사하고 식별된 모든 오류 또는 충돌을 해결할 것을 강력히 권장합니다. 이러한 오류를 해결하면 UNAB 운영 문제를 방지하는 데 도움이 됩니다.

중요! uxpreinstall 유틸리티는 실제 또는 잠재적 문제를 알려주지만 이러한 문제를 해결하지는 못합니다. 이 유틸리티를 사용하여 운영 체제 또는 UNAB 를 구성할 수 없습니다.

UNAB 설치 전 또는 후에 uxpreinstall 을 사용할 수 있습니다. uxpreinstall 은 끝점 또는 UNAB 설치를 수정하지 않지만 가능한 문제를 진단하여 문제에 대한 해결 방법을 제안합니다. uxpreinstall 이 식별하는 모든 문제점은 uxpreinstall 의 문제점이 아니라 끝점의 문제점입니다.

참고: UNAB 를 설치하기 전에 uxpreinstall 을 실행하려면 UNAB 가 설치된 다른 끝점에서 이 유틸리티를 복사하십시오. uxpreinstall 유틸리티에 대한 자세한 내용은 *참조 안내서*를 참조하십시오.

시스템 호환성을 확인하려면

1. superuser 로 UNIX 컴퓨터에 로그인합니다.
2. 세부 수준 0 으로 uxpreinstall 을 실행합니다.

   uxpreinstall 이 실행되고 수행하는 검사의 요약 및 식별된 오류 또는 충돌을 표시합니다.
3. uxpreinstall 이 오류 또는 충돌을 식별하면 세부 수준 2 이상으로 uxpreinstall 을 다시 실행합니다.

   uxpreinstall 이 식별한 오류 또는 충돌에 대한 추가 정보를 표시합니다.
4. 오류와 충돌을 해결합니다.
5. uxpreinstall 이 오류 또는 충돌을 더 이상 식별하지 않을 때까지 2-4 단계를 반복합니다.

   uxpreinstall 출력이 오류 또는 충돌을 더 이상 표시하지 않으면 컴퓨터가 UNAB 요구 사항과 호환되는 것입니다. 이제 UNAB 를 시작하고 활성화할 수 있습니다.

예: uxpreinstall 유틸리티 실행

이 예제는 administrator 자격 증명을 사용하여 세부 정보 표시 수준 3 으로 Active Directory 도메인 domain.com 에 대해 uxpreinstall 유틸리티를 실행합니다.

```
./uxpreinstall -a administrator -w admin -d domain.com -v 3
```

Uxconsole 및 Microsoft 유틸리티를 사용하여 Active Directory 문제 해결

구현 프로세스 중 등록 및 활성화 문제와 같은 Active Directory 에 관련된 다양한 문제가 발생할 수 있습니다. uxpreinstall 유틸리티는 관련된 모든 요인을 수집, 식별, 평가하는 데 도움을 줍니다. Active Directory 의 문제 해결 능력을 개선하기 위해 Microsoft 에서 제공하는 dcdiag(도메인 컨트롤러 진단) 및 netdiag(네트워크 진단) 유틸리티를 사용할 수 있습니다.

중요! Windows Server 2003 을 사용하는 경우 지원 도구 소프트웨어 번들에 dcdiag.exe 와 netdiag.exe 유틸리티가 포함되어 있습니다. 자세한 내용은 Microsoft 기술 자료 문서: KB247811, KB265706, KB321708 을 참조하십시오.

다음 절차에 따라 Active Directory 의 문제를 해결하십시오.

1. 세부 수준 0 으로 uxpreinstall 을 실행합니다.

   uxpreinstall 이 실행되고 수행하는 검사의 요약 및 식별된 오류 또는 충돌을 표시합니다.

2. uxpreinstall 이 오류 또는 충돌을 식별하면 세부 수준 2 이상으로 uxpreinstall 을 다시 실행합니다.

   uxpreinstall 이 식별한 오류 또는 충돌에 대한 추가 정보를 표시합니다.

   참고: –l (시스템 로거 확인) 및 –k(Single Sign On 준비 확인) 인수를 사용하면 많은 양의 출력이 발생하므로 주의하십시오.

3. uxpreinstall 출력을 로깅하려면 uxpreinstall -f 를 실행합니다.
4. Microsoft dcdiag 유틸리티 출력을 로깅하려면 dcdiag /f 를 실행합니다.

   참고: netdiag 유틸리티는 자동으로 NetDiag.log 로그 파일을 생성합니다.

5. 로그 파일에서 실패, 오류 메시지, 경고를 검토합니다. 이런 항목이 있는 경우 더 높은 세부 수준으로 uxpreinstall 과 dcdiag 유틸리티를 실행하십시오.
6. 성공적으로 완료되지 않은 작업과 경고 메시지가 있는지 로그 파일을 다시 검토합니다.

   사용자의 기본 설정에 따라 오류가 오류 메시지가 아닌 경고로 로깅될 수 있습니다.

7. dcdiag /test:DNS /v /e 를 실행하여 도메인 컨트롤러 매개 변수의 문제를 해결합니다.
8. 로그 파일의 끝부터 시작하여 출력을 검토합니다.
9. 모든 경고와 오류 메시지를 해결할 때까지 문제 해결 과정을 계속합니다.

예: dsquery 를 사용하여 사용자 및 그룹 쿼리

다음 예는 dsquery 유틸리티를 사용하여 사용자 및 그룹을 쿼리하는 방법을 보여 줍니다.

```
dsquery user -name user1
dsquery group -name grp1
dsquery * "CN=Users,DC=example,DC=com" -scope base -attr *
```

예: dnscmd 유틸리티를 사용하여 DNS 설정 검색

다음 예는 dnscmd 를 사용하여 DNS 설정을 검색하는 방법을 보여 줍니다.

```
dnscmd /enumzones
dnscmd /zoneprint <zonename>
```

예: dsquery 유틸리티를 사용하여 Active Directory 사이트 검색

다음 예는 dsquery 유틸리티를 사용하여 Active Directory 사이트를 검색하는 방법을 보여 줍니다.

```
dsquery subnet –name 192.168.*
dsquery site -o dn
dsquery subnet -o rdn -site <mysite>
nltest /DSGETSITECOV
```

UNIX 컴퓨터 이름이 올바로 확인되는지 검사합니다.

UNAB 가 작동하려면 UNIX 컴퓨터와 Active Directory 컴퓨터가 모두 UNIX 컴퓨터의 IP 주소를 도메인 이름을 포함한 동일한 컴퓨터 이름으로 확인할 수 있어야 합니다.

UNIX 컴퓨터 이름이 올바로 확인되는지 확인하려면 uxpreinstall 유틸리티를 실행하십시오.

예: uxpreinstall 유틸리티를 사용하여 UNIX 컴퓨터의 이름이 올바로 확인되는지 검사

이 예는 Windows, Active Directory 서버 및 UNIX 컴퓨터 모두에서 이름이 computer.com 인 Linux 컴퓨터에서 세부 수준 3 으로 uxpreinstall 을 실행한 결과를 보여 줍니다.

```
Locating Active Directory services in domain <DOMAIN.COM>
Locating '_ldap._tcp.DOMAIN.COM.' records in DNS ...
computer.com:389 [100:0] (_ldap)
computer.com:389 [100:0] (_ldap)
Found LDAP services:
  computer:389
Performing name resolution on <computer.com>
Running command "host computer.com" ...
  DNS server reply:
    computer.com has address 192.168.1.1
Name <computer.com> was resolved to IP address <1192.168.1.1>
```

예: nslookup 유틸리티를 사용하여 UNIX 컴퓨터의 이름이 올바로 확인되었는지 검사

이 예는 Windows, Active Directory 서버, UNIX 컴퓨터 모두에서 acctdept 란 이름의 컴퓨터에 대한 Linux 에서의 정방향 nslookup 명령의 결과를 보여줍니다.

```
# nslookup acctdept
Server:       172.24.789.0
Address:      172.24.789.0#53

Name:   acctdept.parallel.com
Address: 172.24.123.110
```

UNAB 설치 매개 변수 파일 - UNAB 설치 사용자 지정

UNAB 매개 변수 파일에는 필요에 따라 사용자 지정할 수 있는 설치 매개 변수가 포함되어 있습니다.

이 파일의 형식은 다음과 같습니다.

AUDIT_BK

감사 파일의 타임스탬프가 지정된 백업을 유지할지 여부를 지정합니다.

참고: 감사 데이터를 배포 서버로 전달하려면 이 값을 'yes'로 설정하십시오. 이 값을 'yes'로 지정하면 CA Access Control 은 audit_size 구성 설정에 의해 지정된 크기 제한에 도달할 때 감사 파일을 백업한 후 파일에 타임스탬프를 지정합니다. 이렇게 하면 보고서 에이전트에서 모든 감사 데이터를 사용할 수 있게 됩니다.

제한: yes, no

기본값: no

COMPUTERS_CONTAINER

Active Directory 에서 UNIX 컴퓨터가 등록된 컨테이너 이름을 정의합니다.

기본값: cn=Computers

DIST_SRV_HOST

배포 서버 호스트 이름을 지정합니다.

제한: 임의의 유효한 호스트 이름

기본값: none

DIST_SRV_PORT

배포 서버 포트 번호를 지정합니다.

제한: SSL: 7243, TCP: 7222

기본값: 7243

DIST_SRV_PROTOCOL

배포 서버 통신 프로토콜을 지정합니다.

제한: tcp, ssl

기본값: ssl

ENABLE_ELM

보고서 에이전트가 끝점 감사 데이터를 배포 서버로 보낼지 여부를 지정합니다. 이렇게 하면 CA Enterprise Log Manager 와 통합할 수 있습니다.

참고: 값을 'yes'로 설정하는 경우 감사 백업을 유지하도록 CA Access Control 을 설정(AUDIT_BK=yes)하십시오.

제한: yes, no

기본값: no

GROUP_CONTAINER

UNIX 그룹의 정의가 들어 있는 Active Directory 컨테이너의 이름을 정의합니다.

IGNORE_DC_LIST

LDAP 에 연결할 때 UNAB 가 무시하는 Active Directory 도메인 컨트롤러를 지정합니다.

참고: 현재 및 트러스트된 도메인 모두에서 도메인 컨트롤러를 지정할 수 있습니다.

제한: none - 쉼표로 구분된 목록

기본값: none

IGNORE_DOMAIN_LIST

사용자 및 그룹을 쿼리할 때 UNAB 가 무시할 Active Directory 도메인을 지정합니다.

제한: none - UNAB 가 현재 및 모든 트러스트된 도메인을 쿼리합니다. all - UNAB 가 현재 도메인만 쿼리합니다. 무시할 도메인은 목록에서 각각 쉼표로 구분합니다.

기본값: none

IGNORE_USER_CONTAINER

Active Directory 를 검색할 때 무시할 사용자 컨테이너를 지정합니다.

컨테이너는 세미콜론으로 구분된 고유 이름(DN)으로 정의됩니다. 컨테이너 DN 에 도메인 이름이 없으면 쿼리된 모든 도메인에 적용됩니다.

제한: 세미콜론으로 구분된 컨테이너 DN 의 목록, none

기본값: none

IGNORE_GROUP_CONTAINER

Active Directory 를 검색할 때 무시할 그룹 컨테이너를 지정합니다.

컨테이너는 세미콜론으로 구분된 고유 이름(DN)으로 정의됩니다. 컨테이너 DN 에 도메인 이름이 없으면 쿼리된 모든 도메인에 적용됩니다.

제한: 세미콜론으로 구분된 컨테이너 DN 의 목록, none

기본값: none

INTEGRATION_MODE

UNAB 통합 모드를 지정합니다.

제한: 1 - 부분 통합, 2 - 전체 통합

기본값: 2

JAVA_HOME

(Linux s390) Java 버전과 운영 체제에 따라 설치된 Java 환경에 대한 전체 경로 이름을 지정합니다.

Java 환경이 기본 위치에 설치되지 않은 경우에만 이 매개 변수를 지정하십시오. 기본 위치에 Java 환경이 설치된 경우 설치 프로그램은 이 매개 변수의 값을 설정합니다.

LANG

설치 언어를 지정합니다.

LIC_CMD

라이선스 동의 명령을 지정합니다.

LOCAL_POLICY

로그인 정책 사용 옵션을 지정합니다.

제한: yes - UNAB 정책 및 로컬 로그인 파일 사용, no - UNAB 로그인 정책만 사용

기본값: no

LOOKUP_DC_LIST

LDAP 에 연결할 Active Directory 도메인 컨트롤러(DC)를 지정합니다.

참고: 현재 및 트러스트된 도메인 모두에서 DC 를 지정할 수 있습니다. 사용할 DC 를 지정하는 경우 UNAB 는 Active Directory 에서 DC 의 목록을 가져옵니다. 사용할 DC 를 지정하지 않으면 UNAB 는 끝점의 실제 위치와 가장 가까운 Active Directory 사이트를 찾아 이 사이트의 DC 와 통신합니다.

제한: none - 쉼표로 구분된 목록

기본값: none

NTP_SRV

NTP(Network Time Protocol) 서버의 이름 또는 IP 주소를 정의합니다.

REPORT_SHARED_SECRET

보고서 에이전트가 배포 서버를 인증하기 위해 사용하는 공유 암호를 지정합니다.

제한: 임의의 유효한 문자열

기본값: none

참고: 배포 서버를 설치할 때 정의한 동일한 공유 암호를 지정해야 합니다.

REPORT_SRV_QNAME

스냅숏이 전달되는 큐의 이름을 지정합니다.

제한: 큐 이름을 나타내는 문자열

기본값: queue/snapshots

REPORT_SRV_SCHEDULE

보고서 에이전트가 보고서를 생성하여 배포 서버로 전달하는 시기를 정의합니다.

이 토큰의 형식은 다음과 같습니다: time@day[,day2] [...]

기본값: 00:00@Sun,Mon,Tue,Wed,Thu,Fri,Sat

SSO

UNAB 가 Kerberos 기반 SSO(Single Sign On)를 지원하는지 여부를 지정합니다.

제한: yes, no

기본값: no

TIME_SYNCH

UNAB 가 시스템 시간을 NTP(Network Time Protocol) 서버와 동기화하는지 여부를 지정합니다.

참고: 이 값을 'yes'로 지정하는 경우 NTP_SRV 토큰의 값을 지정해야 합니다. 이 값을 'no'로 설정하는 경우 UNAB 는 /etc/ntp.conf 에 정의된 UNIX 메커니즘을 시스템 시간에 사용합니다.

제한: yes, no

기본값: no

사용자 컨테이너

UNIX 사용자의 정의가 들어 있는 Active Directory 컨테이너 이름을 정의합니다.

UXACT_ADMINISTRATOR

Active Directory 관리자의 사용자 이름을 정의합니다.

UXACT_ADMIN_PASSWORD

Active Directory 관리자의 계정 암호를 정의합니다.

UXACT_DOMAIN

UNIX 컴퓨터가 속한 도메인을 정의합니다.

UXACT_RUN

설치 중 uxconsole -register 명령을 실행할지 여부를 지정합니다.

제한: yes, no

기본값: no

참고: uxconsole -register 명령은 Active Directory 서버의 "컴퓨터" 컨테이너 아래에 UNIX 컴퓨터를 등록합니다.

UXACT_RUN_AGENT

설치 프로세스의 마지막에 UNAB 데몬을 시작할지 여부를 지정합니다.

제한: yes, no

기본값: yes

UXACT_SERVER

Active Directory 서버의 이름을 정의합니다.

UXACT_VERB_LEVEL

세부 정보 수준을 정의합니다.

제한: 0-7

CA Access Control 엔터프라이즈 관리에서 UNAB 관리

CA Access Control 엔터프라이즈 관리를 사용하여 UNAB 끝점을 관리할 수 있습니다. 이 인터페이스를 사용하여 월드 뷰에서 UNAB 끝점을 보고, 로그인 및 구성 정책을 만들어 할당하고, 마이그레이션 프로세스 중 발견된 충돌을 해결할 수 있습니다. CA Access Control 엔터프라이즈 관리가 UNAB 끝점을 관리할 수 있도록 하려면 UNAB 를 CA Access Control 엔터프라이즈 관리에 등록해야 합니다. 패키지 매개 변수를 수정하려면 UNAB 설치 패키지를 사용자 지정하십시오.

참고: UNAB 를 설치하기 전에 이 절차를 완료하십시오.

CA Access Control 엔터프라이즈 관리에서 UNAB 를 관리하려면

1. UNAB 패키지에서 임시 파일로 설치 매개 변수를 추출합니다.
2. 텍스트 편집기에서 임시 파일을 엽니다.

3. 회사에 대해 다음 매개 변수를 수정합니다.

   DISTRIBUTION_SRV_HOST

   배포 서버 호스트 이름을 지정합니다.

   제한: 임의의 유효한 호스트 이름

   기본값: none

   DISTRIBUTION_SRV_PROTOCOL

   배포 서버 통신 프로토콜을 지정합니다.

   제한: tcp, ssl

   기본값: ssl

   DISTRIBUTION_SRV_PORT

   배포 서버 포트 번호를 지정합니다.

   제한: ssl: 7243, tcp: 7222

   기본값: 7243

4. 사용자 지정된 패키지에 설치 매개 변수를 설정합니다.
5. 사용자 지정된 패키지를 사용하여 UNAB 를 설치합니다.

   UNAB 가 사용자 지정된 설정으로 설치되었습니다.

6. acuxchkey 유틸리티를 사용하여 엔터프라이즈 관리 서버 설치 중에 지정한 메시지 큐 암호를 UNAB 호스트로 지정합니다. 예:

   ```
   acuxchkey -t pwd "password"
   ```

   설치가 완료되고 메시지 큐 암호가 UNAB 호스트에서 설정된 이후에 CA Access Control 엔터프라이즈 관리를 사용하여 UNAB 끝점을 관리하십시오.

   참고: acuxcheky 유틸리티에 대한 자세한 내용은 *참조 안내서*를 참조하십시오.

CA Access Control 과의 통합

동일한 끝점에 UNAB 와 CA Access Control 을 설치하려는 경우 UNAB 의 일부 기능을 이용하여 UNAB 관련 정보를 CA Access Control 에 표시할 수 있습니다. 예를 들어, 감사 레코드에 UNIX 계정 이름 대신 엔터프라이즈 사용자 이름을 표시할 수 있습니다. seos.ini 구성 파일에는 UNAB 와 CA Access Control 을 통합하려는 경우 활성화하는 토큰이 수록되어 있습니다.

중요! UNAB 와 CA Access Control 을 통합하기 전에 끝점에 CA Access Control 버전 r12.5 이상이 설치되어 있어야 합니다.

[seosd] 섹션의 다음 토큰은 UNAB 와 CA Access Control 의 통합을 제어합니다.

use_unab_db

seosd 가 UNAB 데이터베이스를 사용하여 사용자 및 그룹 이름을 확인하도록 지정합니다. 이 토큰은 CA Access Control 이 UNAB 에서 변경 사항(예: 새 사용자 로그인)을 감지할 수 있게 해 줍니다.

use_mapped_user_name

seosd 가 감사 레코드에 사용자 엔터프라이즈 이름을 사용할지 여부를 지정합니다. 활성화된 경우 seaudit 유틸리티는 UNIX 계정 이름이 아닌 엔터프라이즈 사용자 이름을 표시합니다.

[OS_User] 섹션의 다음 토큰은 UNAB 와 CA Access Control 의 통합을 제어합니다.

nonunix_unabgroup_enabled

CA Access Control 이 UNAB 데이터베이스의 UNIX 사용자 그룹을 지원하는지 여부를 지정합니다. 활성화되면 CA Access Control 은 비 UNIX 그룹의 사용자를 지원합니다.

osuser_enabled

엔터프라이즈 사용자 및 그룹의 활성화 여부를 지정합니다.

[seos] 섹션의 다음 토큰은 UNAB 와 CA Access Control 의 통합을 제어합니다.

auth_login

로그인 권한 방법을 결정합니다. 이 토큰은 사용자를 인증하기 위한 암호 검사(예: sesudo, sesu, sepass)를 활성화합니다.

pam_enabled

로컬 호스트가 인증 및 암호 변경을 위해 LDAP 데이터베이스에서 PAM 사용을 활성화할지 여부를 지정합니다.

[passwd] 섹션의 다음 토큰은 UNAB 와 CA Access Control 의 통합을 제어합니다.

nis_env

로컬 호스트가 NIS 인지 NIS+ 클라이언트인지를 지정합니다.

change_pam

로컬 호스트가 LDAP 데이터베이스에서 암호 인증 및 변경을 위해 PAM 을 사용할지 여부를 지정합니다. sepass 가 외부 pam 저장소(예: UNAB)와 작업하도록 하려면 이 토큰을 사용하십시오.

[pam_seos] 섹션의 다음 토큰은 UNAB 와 CA Access Control 의 통합을 제어합니다.

PamPassUserInfo

pam_seos 가 사용자 정보를 seosd 로 보낼지 여부를 지정합니다.

pam_login_events_enabled

pam_seos 가 로그인 이벤트를 seosd 로 보낼지 여부를 지정합니다.

pam_surrogate_events_enabled

pam_seos 가 서로게이트 이벤트를 seosd 로 보낼지 여부를 지정합니다.

참고: seos.ini 토큰에 대한 자세한 내용은 *참조 안내서*를 참조하십시오.

RSA SecurID 와 통합

회사에서 RSA SecurID 를 사용하여 사용자를 인증하는 경우 RSA SecurID 의 기능을 사용하여 UNAB 끝점에 로그인하는 사용자를 인증할 수 있습니다. RSA SecurID 클라이언트가 설치된 호스트에 UNAB 를 설치하고 Active Directory 에서 사용자 로그인 정책을 관리할 수 있습니다.

UNAB 가 RSA SecurID 가 설치된 호스트에서 실행 중인 경우 UNAB 는 로그인하는 사용자를 인증하지 않습니다. UNAB 는 타사 프로그램을 통해 사용자 인증이 수행되는지 감지합니다. 그런 후에 UNAB 는 끝점에서 사용자 활동을 관리할 수 있습니다(예: 로컬 및 회사 보안 정책 시행, 감사 메시지 생성 등).

UNAB 가 RSA SecurID 와 통합되는 방법

UNAB 는 PAM 스택 기능을 활용하여 RSA SecurID 와 통합됩니다. PAM 스택 기능은 로그인 프로세스 중 사용자 인증에 어떤 인증 프로그램을 사용할지 설정하고 인증이 수행되는 순서를 설정할 수 있게 해 줍니다.

다음 프로세스는 RSA SecurID 와 UNAB 의 통합을 설명합니다.

1. RSA SecurID 클라이언트가 설치된 끝점에 UNAB 를 설치합니다.
2. 사용자 인증이 수행될 순서로 PAM 스택을 구성합니다. 예를 들어, PAM 스택을 구성하여 사용자 암호 코드와 PIN 을 인증하기 위해 RSA SecurID 를 호출하고, 실패하는 경우 UNAB 를 사용하여 사용자 Active Directory 자격 증명을 인증합니다.
3. 사용자가 UNAB 호스트에 로그인하려고 시도하면 다음이 발생합니다.

   RSA SecurID 인증 및 UNAB 인증 사용:

   a. RSA SecurID 는 사용자에게 암호 코드와 PIN 번호를 요구합니다.

   b. 사용자가 암호 코드와 PIN 번호를 입력합니다.

   c. RSA SecurID 는 이 사용자 암호 코드와 PIN 번호의 인증을 시도합니다. 결과는 다음과 같습니다.

      - RSA SecurID 는 사용자 암호 코드와 PIN 번호를 검사하고 사용자가 로그인할 수 있게 합니다. 인증 프로세스가 여기에서 끝나고 사용자 계정 관리 프로세스가 시작됩니다.
      - RSA SecurId 가 사용자 암호 코드 또는 PIN 번호를 거부합니다.
      - UNAB 가 사용자에게 Active Directory 사용자 계정 또는 로컬 계정 자격 증명을 요구합니다.
      - UNAB 가 사용자 자격 증명의 인증을 시도하고, 인증된 경우 인증 프로세스가 종료되고 사용자 계정 관리 프로세스가 시작됩니다.

예: Red Hat Advanced Server 5.3 에서 RSA SecurID 인증 사용

/etc/pam.d/system-auth 파일에서 가져온 다음 코드 조각은 Red Hat Linux Advanced Server 5.3 에 대한 사용자 인증이 RSA SecurID 로만 수행됨을 나타냅니다.

```
auth required pam_securid.so
```

예: Red Hat Linux Advanced Server 5.3 에서 RSA SecurID, 로컬 UNIX 및 UNAB 인증 사용

/etc/pam.d/system-auth 파일에서 가져온 다음 코드 조각은 Red Hat Linux Advanced Server 5.3 에 대한 사용자 인증이 RSA SecurID, 로컬 UNIX, UNAB 로만 수행됨을 나타냅니다.

```
auth sufficient   pam_securid.so
auth sufficient   pam_unix.so
auth sufficient   pam_uxauth.so
```

이 예에서 /etc/pam.d/system-auth 파일은 사용자 자격 증명의 인증을 시도하기 위해 RSA SecurID(pam_securid.so) 모듈을 호출하도록 구성됩니다. 성공하면, 로컬 UNIX PAM 모듈(pam_unix.so)은 사용자 자격 증명의 인증을 시도합니다. 성공하면, UNAB PAM 스택 모듈(pam_uxauth.so)은 사용자 자격 증명의 인증을 시도합니다. 이 예에서 UNAB PAM 모듈이 사용자 자격 증명의 인증을 시도하면 UNAB 가 사용자에게 암호를 요청하지 않습니다. 로컬 UNIX PAM 모듈은 UNAB PAM 스택 모듈에 암호를 제공합니다.

참고: 인증 프로세스는 이 PAM 스택 모듈 중 하나로 종료될 수 있습니다.

예: Red Hat Advanced Server 5.3 에서 UNAB 인증 및 RSA SecurID 인증 사용

/etc/pam.d/system-auth 파일에서 가져온 다음 코드 조각은 Red Hat Advanced Server 5.3 에 대한 사용자 인증이 UNAB 인증 및 RSA SecurID 인증으로만 수행됨을 나타냅니다.

```
auth optional    pam_unix.so
auth sufficient  pam_uxauth.so
auth sufficient  pam_securid.so
```

이 예에서 /etc/pam.d/system-auth 파일은 RSA SecurID PAM 스택(pam_securid.so)을 사용하여 사용자 암호 코드를 인증하기 전에 사용자 Active Directory 자격 증명의 인증을 시도하기 위해 UNAB PAM 스택(pam_uxauthd.so)을 사용하도록 구성됩니다. 로컬 UNIX PAM 스택 모듈(pam_unix.so)은 선택 사항으로 설정됩니다. 이것은 로컬 UNIX PAM 스택이 사용자를 인증하지 않지만 사용자에게 암호를 요구한 후 이 암호를 PAM 스택에 대한 전달하는 것을 의미합니다.

참고: 이 예에서 인증 프로세스는 로컬 UNIX 인증을 사용하지 않고 RSA SecurID 또는 UNAB 모듈의 성공적 인증을 통해 종료될 수 있습니다.

RPM 패키지 관리자 설치

RPM 패키지 관리자(RPM)는 개별 소프트웨어 패키지를 빌드, 설치, 쿼리, 확인, 업데이트 및 삭제할 수 있는 명령줄 유틸리티입니다. RPM 은 Linux 플랫폼에서 사용할 수 있습니다.

참고: 자세한 내용은 RPM 패키지 관리자 웹 사이트(http://www.rpm.org) 와 RPM 용 UNIX man 페이지를 참조하십시오.

CA Access Control 이 UNAB 에 대해 제공하는 RPM 패키지를 사용하여 RPM 을 사용하여 수행된 기타 모든 소프트웨어 설치와 함께 UNAB 설치를 관리할 수 있습니다.

UNAB RPM 패키지 설치

Active Directory 사용자 계정을 사용하여 UNIX 컴퓨터에 로그인하려면 액세스하려는 각각의 UNIX 컴퓨터에 UNAB 를 설치해야 합니다. UNAB RPM 패키지를 사용하여 Linux 컴퓨터에 UNAB 를 설치합니다.

UNAB RPM 패키지를 설치하려면

1. 루트로 Linux 컴퓨터에 로그인합니다.
2. UNIX 용 CA Access Control 끝점 구성 요소 DVD 의 /UNAB 디렉터리에서 로컬 파일 시스템으로 서버 플랫폼에 적합한 압축된 tar 파일을 복사합니다.

   파일 시스템의 읽기/쓰기가 가능한 위치에서 패키지를 필요한 대로 사용자 지정할 수 있습니다. 압축된 tar 파일에는 UNAB 패키지와 설치 파일이 수록되어 있습니다.
3. 임시 디렉터리 uncompress 로 이동하여 압축된 tar 파일의 압축을 풉니다. 예를 들어, 다음 명령은 _LINUX_Ux_PKG_125.tar.Z 파일의 압축을 풀고 그 콘텐츠를 추출합니다.

   ```
   gunzip _LINUX_Ux_PKG_125.tar.Z
   tar xvf _LINUX_Ux_PKG_125.tar
   ```
4. rpm 명령을 사용하여 ca-lic 패키지를 설치합니다. ca-lic 는 모든 다른 패키지에 필수적인 CA Technologies 라이선스 프로그램입니다. 예:

   ```
   rpm -U ca-lic-0.0080-04.i386.rpm
   ```

   ca-lic 패키지가 설치됩니다.

5. UNAB 패키지를 사용자 지정합니다. (페이지 289)

   사용권 계약에 동의함을 나타내기 위해 사용권 계약 내에서 찾을 수 있는 키워드를 사용하여 패키지를 사용자 지정해야 합니다. 사용자 지정 설치 설정을 지정하기 위해 패키지를 사용자 지정할 수도 있습니다.

6. rpm 명령을 사용하여 UNAB 패키지를 설치합니다. 예:

   ```
   rpm -U uxauth-125-3.0.1517.i386.rpm
   ```

   설치 프로세스가 시작됩니다.

   설치 프로세스가 성공적으로 완료되었음을 알리는 메시지가 표시됩니다.

   참고: UNAB 패키지는 또한 CAWIN 공유 구성 요소를 설치합니다.

7. 설치 로그 파일 uxauth_install.log 에서 설치 프로세스에 대한 정보를 검토합니다.

   이 로그 파일은 기본적으로 아래 위치에 있는 UNAB 설치 디렉터리에 있습니다.

   ```
   /opt/CA/uxauth
   ```

8. 설치가 성공적으로 완료되었는지 확인합니다. (페이지 293)

UNAB RPM 패키지 사용자 지정

UNAB 를 설치하기 전에 사용권 계약에 동의함을 지정하기 위해 RPM 패키지를 사용자 지정해야 합니다. 또한 패키지를 사용자 지정할 때는 사용자 지정 설치 설정도 지정해야 합니다.

수동으로 패키지를 수정하는 것은 권장되지 않습니다. 대신 설명된 대로 customize_uxauth_rpm 스크립트를 사용하십시오. 사용자 지정 UNAB RPM 설치 패키지를 빌드하려면 컴퓨터에 rpmbuild 유틸리티가 있어야 합니다.

UNAB 패키지를 사용자 지정하려면

1. 아직 수행하지 않은 경우 다음을 수행합니다.
   a. UNIX 용 CA Access Control 끝점 구성 요소 DVD 의 /UNAB 디렉터리에서 로컬 파일 시스템으로 서버 플랫폼에 적합한 압축된 tar 파일을 복사합니다.

      파일 시스템의 읽기/쓰기가 가능한 위치에서 패키지를 필요한 대로 사용자 지정할 수 있습니다.

   b. 임시 디렉터리 uncompress 로 이동하여 압축된 tar 파일의 압축을 풉니다.

      압축된 tar 파일에는 UNAB 설치 파일이 수록되어 있습니다.

2. 다음 명령을 입력하여 설치 패키지로부터 uxpreinstall 유틸리티를 추출합니다.

   customize_uxauth_rpm -e uxpreinstall -f tmp_params [-d *pkg_location*] *pkg_filename*

   UNAB 를 설치하기 전에 uxpreinstall 유틸리티를 사용하여 시스템 호환성을 검사하십시오.

3. (선택 사항) 설치 매개 변수 파일의 언어를 설정하려면 다음 명령을 입력하십시오.

   customize_uxauth_rpm -r -l lang [-d pkg_location] *pkg_filename*

4. 다음 명령을 입력하여 사용권 계약을 표시합니다.

   customize_uxauth_rpm -a [-d *pkg_location*] *pkg_filename*

5. 사용권 계약의 끝에서 대괄호 안에 표시된 키워드를 적어 둡니다.

   다음 단계에서 이 키워드를 지정합니다.

6. 다음 명령을 입력합니다.

   customize_uxauth_rpm -w *keyword* [-d *pkg_location*] *pkg_filename*

   이 명령은 사용권 계약에 동의함을 지정합니다.

7. 다음 명령을 입력하여 설치 매개 변수 파일을 가져옵니다.

   customize_uxauth_rpm -g -f *tmp_params* [-d *pkg_location*] *pkg_filename*

8. 설치 요구 사항에 맞게 설치 매개 변수 파일을 편집합니다. (페이지 276)

   이 파일에서 패키지에 대한 설치 기본 설정을 지정할 수 있습니다.

9. 다음 명령을 입력합니다.

   customize_uxauth_rpm -s -f *tmp_params* [-d *pkg_location*] *pkg_filename*

   이 명령은 사용자 지정된 패키지에서 설치 매개 변수를 설정합니다.

   이제 이 패키지를 사용하여 사용자 지정된 기본 설정으로 UNAB 를 설치할 수 있습니다.

예: UNAB RPM 패키지 사용자 지정

다음 예는 /unab_tmp 디렉터리에 있는 uxauth-125-3.0.1517.i386.rpm UNAB RPM 패키지를 사용자 지정하는 방법을 보여 줍니다.

- 이 예는 사용권 계약 및 키워드를 표시합니다.

  ./customize_uxauth_rpm -a /unab_tmp/uxauth-125-3.0.1517.i386.rpm

- 이 예는 사용권 계약에 동의합니다. 이 예의 키워드는 'agreement'입니다.

  ./customize_uxauth_rpm -w agreement /unab_tmp/uxauth-125-3.0.1517.i386.rpm

- 이 예는 설치 매개 변수 파일을 가져와 동일한 디렉터리에 있는 parameters.txt 파일에 넣습니다.

  ./customize_uxauth_rpm -g -f parameters.txt /unab_tmp/uxauth-125-3.0.1517.i386.rpm

- 이 예는 parameters.txt 파일의 매개 변수로부터 설치 매개 변수를 설정합니다.

  ./customize_uxauth_rpm -s -f parameters.txt /unab_tmp/uxauth-125-3.0.1517.i386.rpm

customize_uxauth_rpm Command - Customize the UNAB RPM Package

customize_uxauth_rpm 명령은 UNAB RPM 패키지 사용자 지정 스크립트를 실행합니다.

참고: 패키지를 사용자 지정하려면 패키지가 파일 시스템의 읽기/쓰기 가능한 디렉터리에 있어야 합니다.

이 명령의 형식은 다음과 같습니다.

customize_uxauth_rpm -h [-l]
customize_uxauth_rpm -a [-d *pkg_location*] *pkg_filename*
customize_uxauth_rpm -w *keyword* [-d *pkg_location*] *pkg_filename*
customize_uxauth_rpm -r [-d *pkg_location*] [-l *lang*] *pkg_filename*
customize_uxauth_rpm -s -f *tmp_params* [-d *pkg_location*] *pkg_filename*
customize_uxauth_rpm -g [-f *tmp_params*] [-d *pkg_location*] *pkg_filename*
customize_uxauth_rpm -e uxpreinstall [-d pkgdir] [pgn_name]
customize_uxauth_rpm -t *tmp_dir* [-d *pkg_location*] *pkg_filename*

pkg_filename

사용자 지정할 UNAB 패키지의 파일 이름을 정의합니다.

참고: -d 옵션을 지정하지 않으면 패키지 파일의 전체 경로 이름을 정의해야 합니다.

-a

사용권 계약을 표시합니다.

-e uxpreinstall

설치 패키지에서 uxpreinstall 유틸리티를 추출하도록 지정합니다.

-w keyword

사용자가 사용권 계약을 수락함을 지정하는 키워드를 정의합니다. 이 키워드는 사용권 계약 끝부분에서 대괄호 안에 표시됩니다. 사용권 계약서 파일을 찾으려면 -a 옵션을 사용하십시오.

-d *pkg_location*

(선택 사항) 패키지가 들어 있는 파일 시스템의 디렉터리를 지정합니다. 패키지가 있는 디렉터리를 지정하지 않으면 스크립트는 패키지 파일의 전체 경로 이름이 *pkg_filename* 에 포함되어 있다고 가정합니다.

-f tmp_params

정보를 가져오거나 작성하려는 설치 매개 변수 파일의 전체 경로 및 이름을 지정합니다.

참고: -g 옵션을 사용할 때 파일을 지정하지 않으면 설치 매개 변수는 표준 출력(stdout)으로 전달됩니다.

-g

설치 매개 변수 파일을 가져와 -f 옵션에서 지정된 파일에 출력합니다.

-h

명령 사용법을 표시합니다. -l 옵션과 함께 사용하면 지원되는 언어의 언어 코드를 표시합니다.

-l *lang*

설치 매개 변수 파일의 언어를 *lang* 으로 설정합니다. 언어를 설정할 때는 -r 옵션을 함께 사용해야 합니다.

참고: 지정할 수 있는 지원되는 언어 코드 목록을 보려면 customize_uxauth_rpm -l -h 를 실행하십시오. 기본적으로 설치 매개 변수 파일은 영어로 되어 있습니다.

-r

원래 패키지에 사용된 기본값을 사용하도록 패키지를 다시 설정합니다.

-s

지정된 패키지가 -f 옵션으로 지정한 사용자 지정된 설치 매개 변수 파일에서 가져온 입력을 사용하도록 설정합니다.

-t *tmp_dir*

설치 작업을 위한 임시 디렉터리를 설정합니다.

참고: 기본 임시 디렉터리는 /tmp 입니다.

설치가 성공적으로 완료되었는지 확인

UNAB 의 설치가 끝난 후 설치가 성공적으로 완료되었는지 확인해야 합니다.

설치가 성공적으로 완료되었는지 확인하려면 다음 명령을 입력하십시오.

rpm -q *unab_package_name*

unab_package_name

UNAB 네이티브 패키지의 이름을 정의합니다.

UNAB 가 성공적으로 설치된 경우 패키지가 설치되었음을 알리는 메시지가 표시됩니다.

예: 설치가 성공적으로 완료되었는지 확인

다음 예는 uxauth 란 이름의 UNAB 네이티브 패키지에 대해 설치가 성공적으로 완료되었는지 확인합니다.

rpm -q uxauth

UNAB RPM 패키지 업그레이드

UNAB 의 기존 버전이 설치되어 있을 때 새 버전을 설치하려면 설치된 버전을 제거하지 않고 UNAB 의 기존 버전을 업그레이드할 수 있습니다. UNAB RPM 패키지를 사용하여 Linux 컴퓨터에 UNAB 를 업그레이드합니다.

참고: ca-lic 를 수동으로 업그레이드할 필요는 없습니다.

UNAB RPM 패키지를 업그레이드하려면

1. 루트로 Linux 컴퓨터에 로그인합니다.
2. UNIX 용 CA Access Control 끝점 구성 요소 DVD 의 /UNAB 디렉터리에서 로컬 파일 시스템으로 서버 플랫폼에 적합한 압축된 tar 파일을 복사합니다.

   압축된 tar 파일에는 설치 및 업그레이드 파일이 수록되어 있습니다.
3. 임시 디렉터리 uncompress 로 이동하여 압축된 파일의 압축을 풉니다. 예를 들어, 다음 명령은 _LINUX_Ux_PKG_125.tar.Z 파일의 압축을 풉니다.

   ```
   unzip _LINUX_Ux_PKG_125.tar.Z
   tar xvf _LINUX_Ux_PKG_125.tar
   ```

   압축된 패키지에는 UNAB 설치 및 업그레이드 파일이 수록되어 있습니다.
4. rpm 명령을 사용하여 UNAB 를 업그레이드합니다. 예:

   ```
   rpm -U uxauth-125-3.0.1517.i386.rpm --verbose
   ```

   업그레이드 프로세스가 시작됩니다.

   업그레이드 프로세스가 성공적으로 완료되었음을 알리는 메시지가 표시됩니다.

UNAB RPM 패키지를 제거합니다.

UNAB 를 제거하려면 UNAB 가 설치된 UNIX 컴퓨터에서 RPM 패키지를 제거해야 합니다.

UNAB 를 제거하려면 root 로 로그인하여 다음 명령을 입력합니다.

rpm -e *unab_package_name*

unab_package_name

UNAB 네이티브 패키지의 이름을 정의합니다.

제거 프로세스가 시작됩니다.

프로세스가 성공적으로 완료되었음을 알리는 메시지가 표시됩니다.

Solaris 네이티브 패키지 설치

Solaris 네이티브 패키지는 개별 소프트웨어 패키지를 만들고, 설치하고, 제거하고, 보고할 수 있는 명령줄 유틸리티로서 제공됩니다.

참고: Solaris 네이티브 패키지에 대한 자세한 내용은 Sun Microsystems 웹 사이트와 pkgadd, pkgrm, pkginfo 및 pkgchk 용 man 페이지를 참조하십시오.

중요! 패키지 설치 후 UNAB 를 제거하려면 *pkgrm* 명령을 사용해야 합니다.

UNAB Solaris 네이티브 패키지 사용자 지정

Solaris 네이티브 패키지를 사용하여 UNAB 를 설치하기 전에 설치 패키지를 사용자 지정하여 사용권 계약에 동의하십시오. 또한 패키지를 사용자 지정할 때는 사용자 지정 설치 설정도 지정해야 합니다.

UNAB 패키지를 사용자 지정하려면 다음 절차에 나온 단계를 따르십시오. 수동으로 패키지를 수정하는 것은 권장되지 않습니다. 대신 설명된 대로 customize_uxauth_pkg 스크립트를 사용하십시오.

Solaris 네이티브 패키지를 사용자 지정하려면

1. 사용자 지정할 패키지를 UNIX 용 CA Access Control 끝점 구성 요소 DVD 의 /UNAB 디렉터리에서 파일 시스템의 임시 위치로 추출합니다.

   파일 시스템의 읽기/쓰기가 가능한 위치에서 패키지를 필요한 대로 사용자 지정할 수 있습니다.

   중요! 패키지를 추출할 때는 패키지의 전체 디렉터리 구조에 대한 파일 특성이 그대로 보존되어야 합니다. 그렇지 않으면 Solaris 네이티브 패키지 도구에서 패키지가 손상된 것으로 간주합니다.

2. (선택 사항) 파일 시스템의 임시 위치로 customize_uxauth_pkg 스크립트 파일과 pre.tar 파일을 복사합니다.

   모든 언어로 스크립트 메시지를 받으려면 pre.tar 파일을 스크립트 파일과 동일한 디렉터리에 넣으십시오. pre.tar 파일은 설치 메시지와 UNAB 사용권 계약이 수록된 압축 tar 파일입니다.

   참고: customize_uxauth_pkg 스크립트 파일 및 pre.tar 는 패키지를 추출한 동일한 위치에 있습니다.

3. 다음 명령을 입력하여 설치 패키지로부터 uxpreinstall 유틸리티를 추출합니다.

   customize_uxauth_pkg -e uxpreinstall -f tmp_params [-d *pkg_location*] [*pkg_name]*

   UNAB 를 설치하기 전에 uxpreinstall 을 사용하여 시스템 호환성을 검사하십시오.

4. (선택 사항) 다음 명령을 입력합니다.

   customize_uxauth_pkg -r -l *lang* [-d *pkg_location*] [*pkg_name*]

   설치 매개 변수 파일의 언어가 설정됩니다.

5. 다음 명령을 입력합니다.

   customize_uxauth_pkg -a [-d *pkg_location*] *pkg_name*

   이 명령은 사용권 계약을 표시합니다.

6. 사용권 계약의 끝에서 대괄호 안에 표시된 키워드를 적어 둡니다.

   다음 단계에서 이 키워드를 지정합니다.

7. 다음 명령을 입력합니다.

   customize_uxauth_pkg -w *keyword* [-d *pkg_location*] [*pkg_name*]

   이 명령은 사용권 계약에 동의함을 지정합니다.

8. (선택 사항) 다음 명령을 입력합니다.

   customize_uxauth_pkg -i *install_loc* [-d *pkg_location*] [*pkg_name*]

   이 명령은 설치 디렉터리를 변경합니다.

9. 다음 명령을 입력하여 설치 매개 변수 파일을 가져옵니다.

   customize_uxauth_pkg -g -f *tmp_params* [-d *pkg_location*] [*pkg_name*]

10. 설치 요구 사항에 맞게 설치 매개 변수 파일을 편집합니다. (페이지 276)

    이 파일에서 패키지에 대한 설치 기본 설정을 지정할 수 있습니다.

11. 다음 명령을 입력하여 사용자 지정된 패키지에 설치 매개 변수를 설정합니다.

    customize_uxauth_pkg -s -f *tmp_params* [-d *pkg_location*] [*pkg_name*]

    이제 이 패키지를 사용하여 사용자 지정된 기본 설정으로 UNAB 를 설치할 수 있습니다.

customize_uxauth_pkg 명령 - Solaris 네이티브 패키지 사용자 지정

customize_uxauth_pkg 명령은 UNAB Solaris 네이티브 패키지 사용자 지정 스크립트를 실행합니다.

이 명령을 사용할 때는 다음 사항을 고려해야 합니다.

- 이 스크립트는 모든 UNAB Solaris 네이티브 패키지에 대해 사용할 수 있습니다.
- 패키지를 사용자 지정하려면 패키지가 파일 시스템의 읽기/쓰기 가능한 디렉터리에 있어야 합니다.
- 번역된 스크립트 메시지를 표시하려면 pre.tar 파일을 스크립트 파일과 동일한 디렉터리에 넣어야 합니다.

이 명령의 형식은 다음과 같습니다.

customize_uxauth_pkg -h [-l]
customize_uxauth_pkg -a [-d *pkg_location*] [*pkg_name*]
customize_uxauth_pkg -w *command* [-d *pkg_location*] [*pkg_name*]
customize_uxauth_pkg -r [-d *pkg_location*] [-l lang] [*pkg_name*]
customize_uxauth_pkg -i *install_loc* [-d *pkg_location*] [*pkg_name*]
customize_uxauth_pkg -s -f *tmp_params* [-d *pkg_location*] *[pkg_name*]
customize_uxauth_pkg -g [-f *tmp_params*] [-d *pkg_location*] [*pkg_name*]
customize_uxauth_pkg -e uxpreinstall [-d *pkg_location*] [*pkg_name*]
customize_uxauth_pkg -t *tmp_dir* [-d *pkg_location*] [*pkg_name*]

pkg_name

(선택 사항) 사용자 지정할 UNAB 패키지의 이름입니다. 패키지를 지정하지 않으면 스크립트는 기본적으로 기본 UNAB 패키지(uxauth)를 선택합니다.

-a

사용권 계약을 표시합니다.

-e uxpreinstall

설치 패키지에서 uxpreinstall 유틸리티를 추출하도록 지정합니다.

-w keyword

사용자가 사용권 계약을 수락함을 지정하는 키워드를 정의합니다. 이 키워드는 사용권 계약 끝부분에서 대괄호 안에 표시됩니다. 사용권 계약서 파일을 찾으려면 -a 옵션을 사용하십시오.

-l *lang*

설치 매개 변수 파일의 언어를 *lang* 으로 설정합니다. 언어를 설정할 때는 -r 옵션을 함께 사용해야 합니다.

참고: 지정할 수 있는 지원되는 언어 코드에 대한 목록을 보려면 -h 옵션을 사용하여 -l 을 실행하십시오. 기본적으로 설치 매개 변수 파일은 영어로 되어 있습니다.

-d *pkg_location*

(선택 사항) 패키지가 들어 있는 파일 시스템의 디렉터리를 지정합니다. 패키지가 있는 위치를 지정하지 않으면 스크립트는 기본적으로 /var/spool/pkg 를 선택합니다.

-f tmp_params

정보를 가져오거나 작성하려는 설치 매개 변수 파일의 전체 경로 및 이름을 지정합니다.

참고: -g 옵션을 사용할 때 파일을 지정하지 않으면 설치 매개 변수는 표준 출력(stdout)으로 전달됩니다.

-g

설치 매개 변수 파일을 가져와 -f 옵션에서 지정된 파일에 출력합니다.

-h

명령 사용법을 표시합니다. -l 옵션과 함께 사용하면 지원되는 언어의 언어 코드를 표시합니다.

-i *install_loc*

패키지의 설치 디렉터리를 *install_loc*/uxauth 로 설정합니다.

-r

원래 패키지에 사용된 기본값을 사용하도록 패키지를 다시 설정합니다.

-s

지정된 패키지가 -f 옵션으로 지정한 사용자 지정된 설치 매개 변수 파일에서 가져온 입력을 사용하도록 설정합니다.

-t *tmp_dir*

설치 작업을 위한 임시 디렉터리를 설정합니다.

참고: 기본 임시 디렉터리는 /tmp 입니다.

UNAB Solaris 네이티브 패키지 설치

UNAB Solaris 네이티브 패키지를 사용하면 간편하게 Solaris 에 UNAB 를 설치할 수 있습니다.

참고: 다음 절차는 기본 설정을 사용하여 UNAB 를 설치합니다. 설치 전에 UNAB 패키지를 사용자 지정할 수 있습니다.

UNAB Solaris 네이티브 패키지를 설치하려면

1. (선택 사항) Solaris 기본 설치 기본값을 구성합니다.

   a. 다음 명령을 입력합니다.

      convert_uxauth_pkg -p

      설치 관리 파일이 현재 위치에 *myadmin* 이라는 이름으로 복사됩니다.

      설치 관리 파일을 편집하여 pkgadd 설치 기본값을 변경할 수 있습니다. 그런 다음 pkgadd -a 옵션을 사용하여 UNAB 와 같은 특정 설치에 대해 수정된 파일을 사용할 수 있습니다. 단, 이 파일이 UNAB 에 한정되는 것은 아닙니다.

   b. 설치 관리 파일(myadmin)을 원하는 대로 편집한 다음 파일을 저장합니다.

      이제 다른 설치에 영향을 주지 않고 UNAB 기본 설치에 대한 수정된 구성 설정을 사용할 수 있습니다.

   참고: Solaris 기본 패키지에는 기본적으로 사용자 상호 작용이 필요할 수 있습니다. 설치 관리 파일과 그 사용 방법에 대한 자세한 내용은 pkgadd(1M) 및 admin(4)용 Solaris man 페이지를 참조하십시오.

2. 다음 명령을 입력합니다.

   pkgadd [-a *dir*/myadmin] -d *pkg_location* uxauth

   -a *dir*/myadmin

      1 단계에서 작성한 myadmin 설치 관리 파일의 위치를 정의합니다.

      이 옵션을 지정하지 않으면, pkgadd 가 기본 설치 관리 파일을 사용합니다.

   pkg_location

      UNAB 패키지(uxauth)가 있는 디렉터리를 정의합니다.

      중요! 이 패키지는 공용 위치(즉, 그룹 및 전체에 대한 읽기 액세스)에 있어야 합니다. 예를 들어 /var/spool/pkg 와 같은 위치에 있어야 합니다.

   참고: Solaris 네이티브 패키지는 UNIX 용 CA Access Control 끝점 구성 요소 DVD 의 UNAB 디렉터리에 있습니다.

   이제 UNAB 가 완전히 설치되었지만 아직 시작되지 않았습니다.

선택한 영역에 UNAB Solaris 네이티브 패키지 설치

Solaris 네이티브 패키지를 사용하여 선택한 영역에 UNAB 를 설치할 수 있습니다. 하지만 전역 영역에도 UNAB 를 설치해야 합니다.

참고: Solaris 네이티브 패키지를 사용하여 *모든* 영역에 UNAB 를 설치하는 것이 좋습니다.

선택한 영역에 UNAB 를 설치하려면

중요! 모든 영역에서 동일한 UNAB 버전을 사용해야 합니다.

1. 전역 영역에서 다음 명령을 입력합니다.

   pkgadd -G -d *pkg_location* uxauth

   pkg_location

   UNAB 패키지(uxauth)가 있는 디렉터리를 정의합니다.

   중요! 이 패키지는 공용 위치(즉, 그룹 및 전체에 대한 읽기 액세스)에 있어야 합니다. 예를 들어 /var/spool/pkg 와 같은 위치에 있어야 합니다.

   이 명령은 전역 영역에만 UNAB 를 설치합니다.

2. UNAB 를 설치하려는 전역 영역 이외의 각 영역에서 다음을 수행합니다.

   a. uxauth 패키지를 비 전역 영역에 있는 임시 위치에 복사합니다.

   b. 전역 영역 이외의 영역에서 다음 명령을 입력합니다.

      pkgadd -G -d *pkg_location* uxauth

      이 명령은 (1 단계에서 복사한 패키지를 사용하여) 작업하고 있는 비전역 영역에 UNAB 를 설치합니다.

   이제 내부 영역에서 UNAB 를 시작할 수 있습니다.

참고: UNAB 를 제거할 때는 비전역 영역에서 먼저 제거한 후 전역 영역에서 제거해야 합니다.

Solaris 에서 UNAB 업그레이드

UNAB Solaris 네이티브 패키지는 Solaris 에 있는 기존 UNAB 버전을 UNAB 의 새 버전으로 업그레이드할 수 있게 해줍니다.

Solaris 에서 UNAB 를 업그레이드하려면

1. 모든 UNAB 데몬을 중지합니다.
2. (선택 사항) Solaris 기본 설치 기본값을 구성합니다.
   a. 다음 명령을 입력합니다.

      convert_uxauth_pkg -p

      설치 관리 파일이 현재 위치에 *myadmin* 이라는 이름으로 복사됩니다.

      설치 관리 파일을 편집하여 pkgadd 설치 기본값을 변경할 수 있습니다. 그런 다음 pkgadd -a 옵션을 사용하여 UNAB 와 같은 특정 설치에 대해 수정된 파일을 사용할 수 있습니다. 단, 이 파일이 UNAB 에 한정되는 것은 아닙니다.

   b. 설치 관리 파일(myadmin)을 원하는 대로 편집한 다음 파일을 저장합니다.

      이제 다른 설치에 영향을 주지 않고 UNAB 기본 설치에 대한 수정된 구성 설정을 사용할 수 있습니다.

   참고: Solaris 기본 패키지에는 기본적으로 사용자 상호 작용이 필요할 수 있습니다. 설치 관리 파일과 그 사용 방법에 대한 자세한 내용은 pkgadd(1M) 및 admin(4)용 Solaris man 페이지를 참조하십시오.
3. 다음 명령을 입력합니다.

   pkgadd [-a *dir/myadmin*] –v -d . *UNAB*

   -a *dir*/myadmin

   1 단계에서 작성한 myadmin 설치 관리 파일의 위치를 정의합니다.

   이 옵션을 지정하지 않으면, pkgadd 가 기본 설치 관리 파일을 사용합니다.

   UNAB

   UNAB 네이티브 패키지의 이름을 정의합니다.

   참고: 기본 디렉터리가 아닌 다른 디렉터리에 UNAB 의 이전 버전을 설치한 경우 다음 명령을 실행하여 UNAB 디렉터리에 대한 전체 경로를 지정하십시오.

   ./customize_eac_pkg -i *previous-path* -d ./ CAeAC

-i *Previous-path*

기존 UNAB 디렉터리에 대한 전체 경로를 정의합니다.

참고: 전체 경로 이름의 끝에 슬래시 문자(/)가 포함되지 않도록 하십시오.

UNAB 의 새 버전이 이제 설치되었지만 아직 시작되지 않았습니다.

UNAB Solaris 네이티브 패키지 제거

UNAB Solaris 패키지 설치를 제거하려면 UNAB 패키지를 제거하십시오..

기본 UNAB 패키지를 제거하려면 다음 명령을 입력하십시오.

pkgrm *unab_package_name*

unab_package_name

UNAB 네이티브 패키지의 이름을 정의합니다.

UNAB 가 컴퓨터에서 제거됩니다.

HP-UX 기본 패키지 설치

HP-UX 기본 패키지는 개별 소프트웨어 패키지를 만들고, 설치하고, 제거하고, 보고할 수 있는 일련의 GUI 및 명령줄 유틸리티로서 제공됩니다. HP-UX 기본 패키지를 사용하면 원격 컴퓨터에도 소프트웨어 패키지를 설치할 수 있습니다.

참고: HP-UX 기본 패키지인 SD-UX(Distributor-UX)에 대한 자세한 내용은 HP 웹 사이트 http://www.hp.com을 참조하십시오. swreg, swinstall, swpackage 및 swverify 에 대한 자세한 내용은 man 페이지를 참조하십시오.

중요! 패키지 설치 후 UNAB 를 제거하려면 *swremove* 명령을 사용해야 합니다.

UNAB SD-UX 형식 패키지 사용자 지정

네이티브 패키지를 사용하여 UNAB 를 설치하기 전에 UNAB 패키지를 사용자 지정하여 사용권 계약에 동의해야 합니다. 또한 패키지를 사용자 지정할 때는 사용자 지정 설치 설정도 지정해야 합니다.

수동으로 패키지를 수정하는 것은 권장되지 않습니다. 대신 다음 절차에 설명된 스크립트를 사용하여 UNAB 패키지를 사용자 지정하십시오.

지원되는 각 HP-UX 운영 체제에 대한 SD-UX(Software Distributor-UX) 형식 패키지는 CA Access Control UNIX 용 끝점 구성 요소 DVD 의 UNAB 디렉터리에 있습니다.

SD-UX 형식 패키지를 사용자 지정하려면

1. 사용자 지정할 패키지를 파일 시스템의 임시 위치로 추출합니다.

   파일 시스템의 읽기/쓰기가 가능한 위치에서 패키지를 필요한 대로 사용자 지정할 수 있습니다.

   중요! 패키지를 추출할 때는 패키지의 전체 디렉터리 구조에 대한 파일 특성이 그대로 보존되어야 합니다. 그렇지 않으면 HP-UX 네이티브 패키지 도구에서 패키지가 손상된 것으로 간주합니다.

2. (선택 사항) 파일 시스템의 임시 위치로 customize_uxauth_depot 스크립트 파일과 pre.tar 파일을 복사합니다.

   pre.tar 파일은 설치 메시지와 UNAB 사용권 계약이 수록된 압축 tar 파일입니다.

   참고: customize_uxauth_depot 스크립트 파일과 pre.tar 파일은 다음 디렉터리에 있습니다.

   /uxauth/FILESET/opt/CA/uxauth/lbin

3. 다음 명령을 입력하여 설치 패키지로부터 uxpreinstall 유틸리티를 추출합니다.

   customize_exauth_depot -e uxpreinstall -f tmp_params [-d *pkg_location*] [*pkg_name]*

   UNAB 를 설치하기 전에 uxpreinstall 을 사용하여 시스템 호환성을 검사하십시오.

4. 다음 명령을 입력합니다.

   customize_uxauth_depot -a [-d *pkg_location*] [*pkg_name]*

   이 명령은 사용권 계약을 표시합니다.

5. 사용권 계약의 끝에서 대괄호 안에 표시된 키워드를 적어 둡니다.

   다음 단계에서 이 키워드를 지정합니다.

6. 다음 명령을 입력합니다.

   customize_uxauth_depot -w *keyword* [-d *pkg_location*] [*pkg_name*]

   이 명령은 사용권 계약에 동의함을 지정합니다.

7. (선택 사항) 다음 명령을 입력합니다.

   customize_uxauth_depot -r -l *lang* [-d *pkg_location*] [*pkg_name*]

   이 명령은 설치 매개 변수 파일의 언어를 설정합니다.

8. (선택 사항) 다음 명령을 입력합니다.

   customize_uxauth_depot -i *install_loc* [-d *pkg_location*] [*pkg_name*]

   이 명령은 설치 디렉터리를 변경합니다.

9. (선택 사항) 다음 명령을 입력하여 설치 매개 변수 파일을 가져옵니다.

   customize_uxauth_depot -g -f *tmp_params* [-d *pkg_location*] [*pkg_name*]

10. (선택 사항) 설치 요구 사항에 맞게 설치 매개 변수 파일을 편집합니다. (페이지 276)

    이 파일에서 패키지에 대한 설치 기본 설정을 지정할 수 있습니다.

11. (선택 사항) 다음 명령을 입력합니다.

    customize_uxauth_depot -s -f *tmp_params* [-d *pkg_location*] [*pkg_name*]

    이 명령은 사용자 지정된 패키지에서 설치 매개 변수를 설정합니다.

    이제 이 패키지를 사용하여 사용자 지정된 기본 설정으로 UNAB 를 설치할 수 있습니다.

예: 사용권 계약에 동의하도록 지정

네이티브 패키지를 설치할 때 사용권 계약에 동의하려면 패키지를 사용자 정의해야 합니다. 다음 예는 사용권 계약에 동의하도록 지정하기 위해 패키지 파일을 추출한 디렉터리에 있는 x86 UNAB SD-UX 패키지를 사용자 지정하는 방법을 설명합니다.

```
cp /mnt/AC_DVD/UNAB/_HPUX11_Ux_PKG_1*.tar.Z /tmp
cd /tmp
zcat _HPUX11_Ux_PKG_1*.tar.Z | tar -xvf -
/uxauth/FILESET/opt/CA/uxauth/lbin/customize_eac_depot -w keyword -d /tmp uxauth
```

이제 /tmp 디렉터리에 있는 사용자 지정된 패키지를 사용하여 UNAB 를 설치할 수 있습니다.

추가 정보:

customize_eac_depot 명령—SD-UX 형식 패키지 사용자 지정 (페이지 217)

customize_uxauth_depot 명령 - SD-UX 형식 패키지 사용자 지정

customize_uxauth_depot 명령은 SD-UX 형식 패키지에 대한 UNAB 네이티브 패키지 사용자 지정 스크립트를 실행합니다.

이 명령을 사용할 때는 다음 사항을 고려해야 합니다.

- 이 스크립트는 모든 사용 가능한 UNAB HP-UX 네이티브 패키지에 대해 사용할 수 있습니다.
- 패키지를 사용자 지정하려면 패키지가 파일 시스템의 읽기/쓰기 가능한 디렉터리에 있어야 합니다.
- 번역된 스크립트 메시지를 표시하려면 pre.tar 파일을 스크립트 파일과 동일한 디렉터리에 넣어야 합니다.

이 명령의 형식은 다음과 같습니다.

customize_uxauth_depot -h [-l]
customize_uxauth_depot -a [-d *pkg_location*] [*pkg_name*]
customize_uxauth_depot -w *keyword* [-d *pkg_location*] [*pkg_name*]
customize_uxauth_depot -r [-l *lang*] [-d *pkg_location*] [*pkg_name*]
customize_uxauth_depot -i *install_loc* [-d *pkg_location*] [*pkg_name*]
customize_uxauth_depot -s -f *tmp_params* [-d *pkg_location*] *[pkg_name*]
customize_uxauth_depot -e uxpreinstall [-d pkg_location] [pkg_name]
customize_uxauth_depot -g [-f *tmp_params*] [-d *pkg_location*] [*pkg_name*]

pkg_name

(선택 사항) 사용자 지정할 UNAB 패키지의 이름입니다. 패키지를 지정하지 않으면 스크립트는 기본적으로 기본 UNAB 패키지(uxauth)를 선택합니다.

-a

사용권 계약을 표시합니다.

-e uxpreinstall

설치 패키지에서 uxpreinstall 유틸리티를 추출하도록 지정합니다.

-d *pkg_location*

(선택 사항) 패키지가 들어 있는 파일 시스템의 디렉터리를 지정합니다. 패키지가 있는 위치를 지정하지 않으면 스크립트는 기본적으로 /var/spool/pkg 를 선택합니다.

-f *tmp_params*

정보를 가져오거나 작성하려는 설치 매개 변수 파일의 전체 경로 및 이름을 지정합니다.

참고: -g 옵션을 사용할 때 파일을 지정하지 않으면 설치 매개 변수는 표준 출력(stdout)으로 전달됩니다.

-g

설치 매개 변수 파일을 가져와 -f 옵션에서 지정된 파일에 출력합니다.

-h

명령 사용법을 표시합니다. -l 옵션과 함께 사용하면 지원되는 언어의 언어 코드를 표시합니다.

-i *install_loc*

패키지의 설치 디렉터리를 *install_loc*/uxauth 로 설정합니다.

-l *lang*

설치 매개 변수 파일의 언어를 *lang* 으로 설정합니다. 언어를 설정할 때는 -r 옵션을 함께 사용해야 합니다.

참고: 지정할 수 있는 지원되는 언어 코드에 대한 목록을 보려면 -h 옵션을 사용하여 -l 을 실행하십시오. 기본적으로 설치 매개 변수 파일은 영어로 되어 있습니다.

-r

원래 패키지에 사용된 기본값을 사용하도록 패키지를 다시 설정합니다.

-s

지정된 패키지가 -f 옵션으로 지정한 사용자 지정된 설치 매개 변수 파일에서 가져온 입력을 사용하도록 설정합니다.

-w keyword

사용자가 사용권 계약을 수락함을 지정하는 키워드를 정의합니다. 이 키워드는 사용권 계약 끝부분에서 대괄호 안에 표시됩니다. 사용권 계약서 파일을 찾으려면 -a 옵션을 사용하십시오.

UNAB HP-UX 네이티브 패키지 설치

설치된 다른 모든 소프트웨어와 함께 설치된 UNAB 를 관리하려면 사용자 지정된 UNAB SD-UX 형식 패키지를 설치하십시오. UNAB SD-UX 형식 패키지를 사용하면 간편하게 HP-UX 에 UNAB 를 설치할 수 있습니다.

중요! 사용권 계약에 동의함을 나타내기 위해 사용권 계약 내에서 찾을 수 있는 키워드를 사용하여 패키지를 사용자 지정해야 합니다.

UNAB HP-UX 네이티브 패키지를 설치하려면

1. 루트로 로그인합니다.

   HP-UX 네이티브 패키지를 등록 및 설치하려면 루트 계정 권한이 필요합니다.

2. UNAB 패키지를 사용자 지정합니다. (페이지 304)

   사용권 계약에 동의함을 나타내기 위해 사용권 계약 내에서 찾을 수 있는 키워드를 사용하여 패키지를 사용자 지정해야 합니다. 사용자 지정 설치 설정을 지정하기 위해 패키지를 사용자 지정할 수도 있습니다.

3. 다음 명령을 사용하여 SD-UX 와 함께 사용자 지정된 패키지를 등록합니다.

   swreg -l depot *pkg_location*

   pkg_location

   UNAB 패키지가 있는 디렉터리를 정의합니다.

4. 다음 명령을 사용하여 UNAB 패키지를 설치합니다.

   swinstall -s *pkg_location* uxauth

   SD-UX 는 *pkg_location* 디렉터리에서 패키지의 설치를 시작합니다.

   이제 UNAB 가 완전히 설치되었지만 아직 시작되지 않았습니다.

추가 정보:

기본 설치 관련 추가 고려 사항 (페이지 188)
SD-UX 형식 패키지 사용자 지정 (페이지 213)

HP-UX 패키지 제거

UNAB HP-UX 패키지를 제거하려면 설치 순서와 반대로 UNAB 패키지를 제거해야 합니다.

CA Access Control 패키지를 제거하려면 기본 UNAB 패키지를 제거하십시오.

swremove *unab_package_name*

unab_package_name

UNAB 네이티브 패키지의 이름을 정의합니다.

AIX 기본 패키지 설치

AIX 기본 패키지는 개별 소프트웨어 패키지를 관리하는 데 사용할 수 있는 일련의 GUI 및 명령줄 유틸리티로서 제공됩니다.

참고: 일부 AIX 버전은 여러 패키지 형식(installp, SysV, RPM)을 지원하지만 UNAB 는 AIX 기본 패키지 형식(installp)만 제공합니다.

중요!

- 패키지 설치 후 UNAB 를 제거하려면 *installp* 명령을 사용해야 합니다.
- UNAB 는 사용자를 인증하기 위해 AIX LAM(Loadable Authentication Module)이 아닌 PAM(Pluggable Authentication Mode)을 사용합니다. UNAB 설치 전에 AIX 시스템을 구성하여 PAM 을 활성화하십시오.
- 응용 프로그램 오류를 방지하려면 사용자 ID 와 기본 그룹 ID 를 다른 사용자 저장소에서 가져오지 않았는지 확인하십시오. 예를 들어, 사용자 ID 를 /etc/passwd 에서 오고 기본 그룹을 Active Directory 에서 가져온 경우가 해당됩니다.

AIX 의 PAM(Pluggable Authentication Module)

기본적으로 AIX 는 ID 식별 및 인증 용도로 LAM(Loadable Authentication Module)을 사용합니다. UNAB 가 시스템에 액세스하는 사용자를 인증하도록 하려면 PAM 을 사용하도록 AIX 를 구성해야 합니다. UNAB 를 사용자 지정하고 설치하기 전에 PAM 을 사용하도록 AIX 를 구성하십시오.

참고: AIX 버전 5.3 이상에서 PAM 을 활성화할 수 있습니다.

예: PAM 을 사용하도록 AIX 구성

다음 예는 인증 용도로 UNAB 에서 사용하기 위해, PAM 을 사용하도록 AIX 버전 5.3 이상을 구성하는 방법을 설명합니다.

1. PAM 구성 파일을 만듭니다.

   AIX 는 기본 /etc/pam.conf 파일을 제공하지 않습니다.

2. pam.conf 파일을 열고 기본 모듈 스택을 포함한 다음 파일을 저장합니다. 예:

```
#
# Authentication
#
ftp    auth    required      /usr/lib/security/pam_aix
imap   auth    required      /usr/lib/security/pam_aix
login  auth    required      /usr/lib/security/pam_aix
rexec  auth    required      /usr/lib/security/pam_aix
rlogin auth    required      /usr/lib/security/pam_aix
snapp  auth    required      /usr/lib/security/pam_aix
su     auth    required      /usr/lib/security/pam_aix
telnet auth    required      /usr/lib/security/pam_aix
OTHER  auth    required      /usr/lib/security/pam_aix
#
# Account Management
#
ftp    account required      /usr/lib/security/pam_aix
login  account required      /usr/lib/security/pam_aix
rexec  account required      /usr/lib/security/pam_aix
rlogin account required      /usr/lib/security/pam_aix
rsh    account required      /usr/lib/security/pam_aix
su     account required      /usr/lib/security/pam_aix
telnet account required      /usr/lib/security/pam_aix
OTHER  account required      /usr/lib/security/pam_aix
#
# Password Management
#
login  password required     /usr/lib/security/pam_aix
rlogin password required     /usr/lib/security/pam_aix
su     password required     /usr/lib/security/pam_aix
telnet password required     /usr/lib/security/pam_aix
OTHER  password required     /usr/lib/security/pam_aix
#
# Session Management
#
ftp    session required      /usr/lib/security/pam_aix
imap   session required      /usr/lib/security/pam_aix
login  session required      /usr/lib/security/pam_aix
rexec  session required      /usr/lib/security/pam_aix
```

```
rlogin  session required       /usr/lib/security/pam_aix
rsh     session required       /usr/lib/security/pam_aix
snapp   session required       /usr/lib/security/pam_aix
su      session required       /usr/lib/security/pam_aix
telnet  session required       /usr/lib/security/pam_aix
OTHER   session required       /usr/lib/security/pam_aix
```

3. /lib/security 로 이동하여 편집을 위해 methods.cfg 파일을 엽니다.
4. 다음 줄을 추가한 다음 파일을 저장하여 PAM 인증을 활성화합니다.

```
PAM:
    program = /usr/lib/security/PAM
PAMfiles:
    options = auth=PAM,db=BUILTIN
```

5. /etc/security 로 이동하여 편집을 위해 login.cfg 파일을 엽니다.
6. 인증 유형을 PAM 으로 구성한 다음 파일을 저장합니다: auth_type = PAM_AUTH

   예:

```
chsec -f /etc/security/login.cfg -s usw -a auth_type=PAM_AUTH
```

7. /etc/ssh/로 이동하여 편집을 위해 sshd_config 파일을 엽니다.
8. 다음 매개 변수를 추가한 다음 파일을 저장하여 SSH PAM 인증을 활성화합니다.

```
UsePAM yes
```

   참고: PAM 이 지원되는 OpenSSH 버전(버전 3.9p1 이상)을 사용하는 확인하십시오. 버전을 확인하려면 다음 명령을 사용하십시오.

```
lslpp -i openssh.base.server
```

9. /etc 로 이동하여 편집을 위해 pam.conf 파일을 엽니다.
10. 다음 줄을 추가한 다음 파일을 저장하여 SSH PAM 인증을 추가합니다.

```
sshd    auth        required    /usr/lib/security/pam_aix
OTHER   auth        required    /usr/lib/security/pam_aix
sshd    account     required    /usr/lib/security/pam_aix
OTHER   account     required    /usr/lib/security/pam_aix
sshd    password    required    /usr/lib/security/pam_aix
OTHER   password    required    /usr/lib/security/pam_aix
sshd    session     required    /usr/lib/security/pam_aix
OTHER   session     required    /usr/lib/security/pam_aix
```

11. 컴퓨터를 다시 시작합니다.

    AIX 는 인증을 위해 PAM 을 사용하도록 구성되어 있습니다. 이제 AIX 네이티브 패키지를 사용자 지정하고 UNAB 를 설치할 수 있습니다.

bff 네이티브 패키지 파일 사용자 지정

네이티브 패키지를 사용하여 UNAB 를 설치하기 전에 사용권 계약에 동의하도록 지정하기 위해 UNAB 패키지를 사용자 지정해야 합니다. 또한 패키지를 사용자 지정할 때는 사용자 지정 설치 설정도 지정해야 합니다.

수동으로 패키지를 수정하는 것은 권장되지 않습니다. 대신 다음 절차에 설명된 스크립트를 사용하여 UNAB 패키지를 사용자 지정하십시오.

지원되는 각 AIX 운영 체제용 installp 형식 네이티브 패키지(bff 파일)는 CA Access Control UNIX 용 끝점 구성 요소 DVD 의 UNAB 디렉터리에서 찾을 수 있습니다.

중요! UNAB 를 설치하기 전에 인증을 위해 PAM 을 사용하도록 AIX 를 구성해야 합니다.

bff 네이티브 패키지 파일 사용자 지정

1. 사용자 지정할 패키지를 파일 시스템의 임시 위치로 추출합니다.

   파일 시스템의 읽기/쓰기가 가능한 위치에서 패키지(bff 파일)를 필요한 대로 사용자 지정할 수 있습니다.

   중요! 이 위치에는 다시 패키징하는 임시 파일을 수용할 수 있도록 패키지 크기의 두 배 이상 되는 빈 디스크 공간이 필요합니다.

2. (선택 사항) 파일 시스템의 임시 위치로 customize_uxauth_bff 스크립트 파일과 pre.tar 파일을 복사합니다.

   pre.tar 파일은 설치 메시지와 UNAB 사용권 계약이 수록된 압축 tar 파일입니다.

   참고: customize_uxauth_bff 스크립트 파일과 pre.tar 파일은 네이티브 패키지가 들어 있는 위치에 있습니다.

3. 다음 명령을 입력하여 설치 패키지로부터 uxpreinstall 유틸리티를 추출합니다.

   customize_uxauth_bff -e uxpreinstall -f tmp_params [-d *pkg_location*] *pkg_name*

   UNAB 를 설치하기 전에 uxpreinstall 을 사용하여 시스템 호환성을 검사하십시오.

4. 다음 명령을 입력합니다.

   customize_uxauth_bff -a [-d *pkg_location*] *pkg_name*

   이 명령은 사용권 계약을 표시합니다.

5. 사용권 계약의 끝에서 대괄호 안에 표시된 키워드를 적어 둡니다.

   다음 단계에서 이 키워드를 지정합니다.

6. 다음 명령을 입력합니다.

   customize_uxauth_bff -w *keyword* [-d *pkg_location*] *pkg_name*

   이 명령은 사용권 계약에 동의함을 지정합니다.

7. (선택 사항) 다음 명령을 입력합니다.

   customize_uxauth_bff -r -l *lang* [-d *pkg_location*] *pkg_name*

   이 명령은 설치 매개 변수 파일의 언어를 설정합니다.

8. (선택 사항) 다음 명령을 입력합니다.

   customize_uxauth_bff -i *install_loc* [-d *pkg_location*] *pkg_name*

   이 명령은 설치 디렉터리를 변경합니다.

9. 다음 명령을 입력하여 설치 매개 변수 파일을 가져옵니다.

   customize_uxauth_bff -g -f *tmp_params* [-d *pkg_location*] *pkg_name*

10. (선택 사항) 설치 요구 사항에 맞게 설치 매개 변수 파일을 편집합니다. (페이지 276)

    이 파일에서 패키지에 대한 설치 기본 설정을 지정할 수 있습니다.

11. (선택 사항) 다음 명령을 입력하여 사용자 지정된 패키지에 설치 매개 변수를 설정합니다.

    customize_uxauth_bff -s -f *tmp_params* [-d *pkg_location*] *pkg_name*

    이제 이 패키지를 사용하여 사용자 지정된 기본 설정으로 UNAB 를 설치할 수 있습니다.

customize_uxauth_bff 명령 - bff 네이티브 패키지 파일 사용자 지정(UNAB)

customize_uxauth_bff 명령은 bff 네이티브 패키지 파일에 대한 <uxauth> 네이티브 패키지 사용자 지정 스크립트를 실행합니다.

이 스크립트는 AIX 용의 모든 <uxauth> 네이티브 패키지에 대해 사용할 수 있습니다. 패키지를 사용자 지정하려면 패키지가 파일 시스템의 읽기/쓰기 가능한 디렉터리에 있어야 합니다.

중요! 패키지를 추출할 위치는 임시로 만들어지는 패키지를 수록할 수 있도록 패키지 크기의 두 배 이상되는 여유 공간이 있어야 합니다.

참고: 번역된 스크립트 메시지를 표시하려면 pre.tar 파일을 스크립트 파일과 동일한 디렉터리에 넣어야 합니다.

이 명령의 형식은 다음과 같습니다.

customize_uxauth_bff -h [-l]
customize_uxauth_bff -a [-d *pkg_location*] *pkg_name*
customize_uxauth_bff -w *keyword* [-d *pkg_location*] *pkg_name*
customize_uxauth_bff -r [-d *pkg_location*] [-l *lang*] *pkg_name*
customize_uxauth_bff -i *install_loc* [-d *pkg_location*] *pkg_name*
customize_uxauth_bff -s -f *tmp_params* [-d *pkg_location*] *pkg_name*
customize_uxauth_bff -e uxpreinstall [-d *pkg_location*] *pkg_filename*
customize_uxauth_bff -g [-f *tmp_params*] [-d *pkg_location*] *pkg_name*

pkg_name

사용자 지정할 UNAB 패키지(bff 파일)의 이름입니다.

-a

사용권 계약을 표시합니다.

-e uxpreinstall

설치 패키지에서 uxpreinstall 유틸리티를 추출하도록 지정합니다.

-c *certfile*

루트 인증서 파일의 전체 경로 이름을 정의합니다.

참고: 이 옵션은 CAeAC 패키지에만 적용됩니다.

-d *pkg_location*

(선택 사항) 패키지가 들어 있는 파일 시스템의 디렉터리를 지정합니다. 패키지가 있는 위치를 지정하지 않으면 스크립트는 기본적으로 /var/spool/pkg 를 선택합니다.

-f *tmp_params*

정보를 가져오거나 작성하려는 설치 매개 변수 파일의 전체 경로 및 이름을 지정합니다.

참고: -g 옵션을 사용할 때 파일을 지정하지 않으면 설치 매개 변수는 표준 출력(stdout)으로 전달됩니다.

-g

설치 매개 변수 파일을 가져와 -f 옵션에서 지정된 파일에 출력합니다.

-h

명령 사용법을 표시합니다. -l 옵션과 함께 사용하면 지원되는 언어의 언어 코드를 표시합니다.

-i *install_loc*

패키지의 설치 디렉터리를 *install_loc*/uxauth 로 설정합니다.

-l *lang*

설치 매개 변수 파일의 언어를 *lang* 으로 설정합니다. 언어를 설정할 때는 -r 옵션을 함께 사용해야 합니다.

참고: 지정할 수 있는 지원되는 언어 코드에 대한 목록을 보려면 -h 옵션을 사용하여 -l 을 실행하십시오. 기본적으로 설치 매개 변수 파일은 영어로 되어 있습니다.

-r

원래 패키지에 사용된 기본값을 사용하도록 패키지를 다시 설정합니다.

-s

지정된 패키지가 -f 옵션으로 지정한 사용자 지정된 설치 매개 변수 파일에서 가져온 입력을 사용하도록 설정합니다.

-w keyword

사용자가 사용권 계약을 수락함을 지정하는 키워드를 정의합니다. 이 키워드는 사용권 계약 끝부분에서 대괄호 안에 표시됩니다. 사용권 계약서 파일을 찾으려면 -a 옵션을 사용하십시오.

UNAB AIX 네이티브 패키지 설치

설치된 다른 모든 소프트웨어와 함께 설치된 UNAB 를 관리하려면 사용자 지정된 UNAB AIX 네이티브 패키지를 설치하십시오. UNAB AIX 네이티브 패키지(bff 파일)를 사용하면 간편하게 AIX 에 UNAB 를 설치할 수 있습니다.

중요! 사용권 계약에 동의함을 나타내기 위해 사용권 계약 내에서 찾을 수 있는 키워드를 사용하여 패키지를 사용자 지정해야 합니다. CA Access Control 엔터프라이즈 관리를 통해 UNAB 끝점을 관리하려면 UNAB 를 설치하기 *전에* UNAB 끝점을 CA Access Control 엔터프라이즈 관리에 등록해야 합니다.

UNAB AIX 네이티브 패키지를 설치하려면

1. 루트로 로그인합니다.

   AIX 네이티브 패키지를 등록 및 설치하려면 루트 계정 권한이 필요합니다.

2. UNAB 패키지를 사용자 지정합니다. (페이지 313)

   사용권 계약에 동의함을 나타내기 위해 사용권 계약 내에서 찾을 수 있는 키워드를 사용하여 패키지를 사용자 지정해야 합니다. 사용자 지정 설치 설정을 지정하기 위해 패키지를 사용자 지정할 수도 있습니다.

3. (선택 사항) 다음과 같이 설치할 패키지의 수준(버전)을 기록합니다.

   installp -l -d *pkg_location*

   pkg_location

   UNAB 패키지(uxauth)가 있는 디렉터리를 정의합니다.

   pkg_location 의 각 패키지에 대해 AIX 에서 패키지 수준이 나열됩니다.

   참고: AIX 네이티브 패키지 설치 옵션에 대한 자세한 내용은 installp 에 대한 man 페이지를 참조하십시오.

4. 다음 명령을 사용하여 UNAB 패키지를 설치합니다.

   installp -ac -d *pkg_location* uxauth[*pkg_level*]

   pkg_level

   이전에 기록한 패키지의 수준 번호를 정의합니다.

   AIX 는 *pkg_location* 디렉터리에 있는 UNAB 패키지의 설치를 시작합니다.

   이제 UNAB 가 완전히 설치되었지만 아직 시작되지 않았습니다.

추가 정보:

기본 설치 관련 추가 고려 사항 (페이지 188)

AIX 패키지 제거

UNAB AIX 패키지를 제거하려면 설치 순서와 반대로 UNAB 패키지를 제거해야 합니다.

UNAB 패키지를 제거하려면 기본 UNAB 패키지를 제거하십시오.

installp -u *unab_package_name*

unab_package_name

UNAB 네이티브 패키지의 이름을 정의합니다.

설치 후 작업

다음 항목은 UNAB 끝점을 구성하고 UNAB 끝점을 활성화하기 위해 수행해야 하는 설치 후 작업에 대해 설명합니다.

Active Directory 에 UNIX 호스트 등록

Active Directory 에 정의된 사용자가 UNIX 컴퓨터에 로그인할 수 있게 하려면 UNAB 가 설치된 각 UNIX 컴퓨터를 Active Directory 서버에 등록해야 합니다.

참고: UNAB 설치 매개 변수 파일을 구성하여 설치 프로세스가 UNAB 설치 중 Active Directory 에서 UNIX 끝점을 등록하도록 지정할 수 있습니다.

Active Directory 에 UNIX 호스트를 등록하려면

1. UNIX 호스트와 Active Directory 서버의 시간이 동기화되었는지 확인합니다.
2. superuser 로 UNIX 컴퓨터에 로그인합니다.

   참고: Active Directory 사용자가 UNIX 컴퓨터에 로그온하려면 먼저 UNAB 를 활성화해야 합니다.

3. Microsoft Services for UNIX(SFU)를 사용하는 경우 uxauth.ini 파일의 맵 섹션에 특성 이름을 지정합니다.

   uxauth.ini 파일에서 특성 이름을 지정하지 않으면 SFU 에서만 정의된 사용자가 UNAB 호스트에 로그인할 수 없습니다.

   참고: uxauth.ini 파일에 대한 자세한 내용은 *참조 안내서*를 참조하십시오.

4. UNAB bin 디렉터리로 이동합니다. 기본적으로 이 디렉터리의 위치는 다음과 같습니다.

   /opt/CA/uxauth/bin

5. uxconsole -register 유틸리티를 실행합니다.

   UNAB 가 UNIX 컴퓨터를 Active Directory 에 등록하고 uxauthd 데몬을 시작합니다.

   참고: uxconsole -register 에 대한 자세한 내용은 *참조 안내서*를 참조하십시오.

예: Active Directory 에 UNIX 호스트 등록

이 예는 Active Directory 에 UNIX 컴퓨터를 등록하는 방법을 설명합니다. 사용자 이름(-a administrator)과 암호(-w admin)를 입력하고, Active Directory 호스트 이름을 정의하고(-d Active_Directory_Host), 세부 수준(-v 3)을 설정하고, UNAB 에이전트가 설치 끝에 실행되지 않도록 지정하고(-n), Active Directory 의 컨테이너 이름(-o OU=COMPUTERS)을 정의합니다. 컨테이너는 Active Directory 에 UNIX 컴퓨터를 등록하기 전에 존재해야 합니다.

./uxconsole -register -a administrator -w admin -d *Active_Directory_Host* –v 3 -n -o OU=COMPUTERS

예: Active Directory 사용자에게 UNIX 호스트를 등록하는 권한 위임

uxconsole -register 명령을 실행할 때 관리자 사용자 이름 및 암호를 지정하지 않으려면 UNIX 호스트를 Active Directory 에 등록하기 위한 위임된 권한이 있는 사용자의 사용자 이름과 암호를 지정할 수 있습니다. 다음 예는 Active Directory 에서 UNIX 호스트를 등록하기 위한 권한을 Active Directory 사용자에게 위임하는 방법을 설명합니다.

1. Active Directory 컴퓨터에서 "시작", "프로그램", "관리 도구", "Active Directory 사용자 및 컴퓨터"를 클릭합니다.

   "Active Directory 사용자 및 컴퓨터" 관리 콘솔이 열립니다.

2. "컴퓨터" 폴더를 마우스 오른쪽 단추로 클릭한 다음 "제어 위임"을 선택합니다.

   제어 위임 마법사가 열립니다.

3. "다음"을 클릭합니다.

   마법사가 시작됩니다.

4. 다음 표를 사용하여 설치 마법사를 완료하고 "마침"을 클릭합니다.

정보	동작
사용자 및 그룹	제어를 위임할 사용자를 지정합니다. "추가"를 선택하고 제어를 위임할 사용자를 검색합니다.
위임할 작업	선택한 사용자 또는 그룹에 위임할 작업을 정의합니다. "위임할 사용자 지정 작업 만들기" 선택
Active Directory 개체 유형	위임할 작업의 범위를 정의합니다. 다음 작업을 수행하십시오. ■ "이 폴더, 이 폴더에 있는 기존 개체 및 이 폴더에 새 개체 만들기"를 선택합니다. ■ "목록에서 컴퓨터 개체 만들기 권한"을 선택합니다.

정보	동작
권한	사용자에게 위임할 권한을 정의합니다. "특정 자식 개체 만들기/위임"을 선택합니다.

마법사가 닫히고 Active Directory 에서 컴퓨터 개체를 만드는 권한이 사용자에게 위임되었습니다. 이제 사용자에게 Active Directory 에서 UNIX 호스트를 등록하기 위한 충분한 권한이 있습니다.

UNAB 구성

uxauth.ini 파일은 시작 및 런타임 중에 UNAB 가 수행하는 작업을 지정합니다. uxauth.ini 파일은 필요에 따라 변경할 수 있는 여러 기본 값을 수록하고 있습니다.

UNAB 를 구성하려면

1. UNAB 를 실행하는 UNIX 호스트에 로그인합니다.
2. 기본적으로 다음 디렉터리에 있는 uxauth.ini 파일을 엽니다.

   /opt/CA/uxauth
3. 설정을 검토하고 필요한 대로 수정합니다.

참고: uxauth.ini 구성 설정에 대한 자세한 내용은 *참조 안내서*를 참조하십시오.

참고: CA Access Control 엔터프라이즈 관리를 사용하여 uxauth.ini 파일을 구성할 수 있습니다.

보고를 위한 UNAB 구성

UNAB 가 설치 및 구성되면 보고서 에이전트를 활성화하고 구성하여 처리를 위해 배포 서버로 데이터를 보내도록 UNAB 를 구성할 수 있습니다. UNAB 를 설치할 때 보고서 에이전트를 구성하지 않은 경우 활성화할 때 보고서 에이전트를 구성하십시오.

참고: 이 절차는 보고서 전송을 위해 기존 UNAB 끝점을 구성하는 방법을 설명합니다. 동일한 컴퓨터에 CA Access Control 과 UNAB 를 설치한 경우 보고서 에이전트 설정만 한 번 구성하면 됩니다.

보고를 위해 UNAB 를 구성하려면 *ACSharedDir*/lbin/report_agent.sh 를 실행하십시오.

report_agent config {-server *hostname* [-proto {ssl|tcp}] [-port *port_number*] [-rqueue *queue_name*] -schedule <*time@day*> [,day2][...] > [-audit] | [-silent]]

구성 옵션을 생략하면 이 스크립트는 생략된 옵션에 기본값을 설정합니다.

참고: report_agent.sh 스크립트와 보고서 에이전트 구성 설정에 대한 자세한 내용은 *참조 안내서*를 참조하십시오.

UNAB 시작

Active Directory 의 사용자가 UNIX 컴퓨터에 로그인하려면 UNAB 가 실행 중이어야 합니다.

UNAB 를 시작하려면

1. superuser 로 UNIX 컴퓨터에 로그인합니다.
2. UNAB lbin 디렉터리를 찾습니다.
3. 다음 명령을 입력합니다.

   ./uxauthd.sh start

   UNAB 데몬이 시작됩니다.

UNAB 활성화

Active Directory 에서 UNIX 호스트를 등록한 다음에는 UNAB 를 활성화해야 합니다. 활성화는 UNAB 구현 프로세스의 마지막 단계입니다. UNAB 가 활성화되면 Active Directory 암호를 기반으로 사용자를 인증합니다.

UNAB 를 활성화하려면

1. superuser 로 UNIX 컴퓨터에 로그인합니다.
2. UNAB bin 디렉터리로 이동합니다. 기본적으로 이 디렉터리의 위치는 다음과 같습니다.

   /opt/CA/uxauth/bin

3. 다음 명령을 실행합니다.

   ./uxconsole -activate

   -activate

   Active Directory 사용자에 대한 로그인이 활성화되도록 지정합니다.

   UNAB 가 활성화됩니다.

참고: UNAB 를 활성화하면 Active Directory 계정이 있는 로컬 사용자가 계속 UNIX 호스트에 로그인할 수 있게 됩니다.

참고: uxconsole 유틸리티에 대한 자세한 내용은 *참조 안내서*를 참조하십시오.

예: 활성화 이후 UNAB 에 로그인

다음 예는 UNAB 를 부분 모드로 설치하고 등록한 이후에 Active Directory 계정을 사용하여 UNIX 컴퓨터에 로그인하는 방법을 설명합니다.

1. 터미널 창을 엽니다.
2. UNIX 호스트에 연결합니다.

   telnet computer.com

   UNIX 컴퓨터에 연결되고 UNIX 셸이 열립니다.
3. Active Directory 계정의 사용자 이름과 암호를 입력합니다.

   성공하면 마지막 로그온 정보를 보여주는 메시지가 표시됩니다.

완전 통합 모드를 구현하는 방법

완전 통합 모드에서 UNAB 끝점은 사용자를 인증하고 권한을 부여하기 위해 Active Directory 서버에 의존합니다.

UNAB 를 완전 통합 모드에서 구현하려면

1. UNAB 를 구현합니다.

   이 단계는 UNIX 끝점에서 UNAB 를 설치하고 활성화합니다.

2. Active Directory 의 UNIX 특성을 관리할 수 있게 해주는 도구를 설치합니다.

   Active Directory 사용자 및 컴퓨터는 UNIX 특성을 노출하지 않으므로 이러한 특성을 보고 수정하려면 추가 도구를 설치해야 합니다. 예를 들어, CA Access Control UNIX 특성 플러그 인, Microsoft Identity Management for UNIX, ADSI Edit 또는 단순 LDAP 클라이언트를 사용하여 UNIX 특성을 보고 수정할 수 있습니다.

3. UNAB 끝점의 사용자 및 그룹 특성을 Active Directory 로 마이그레이션합니다. 다음 작업 중 *하나*를 수행합니다.

   - UNAB 마이그레이션 도구를 사용하여 UNAB 끝점 사용자 및 그룹의 속성을 Active Directory 로 복사합니다.
   - 2 단계에서 설치한 도구를 사용하여 Active Directory 에서 UNAB 끝점 사용자 및 그룹의 특성을 구성합니다.

   이 단계에서는 Active Directory 를 사용하여 끝점에 대한 액세스를 제어합니다. UNAB 가 이제 완전 통합 모드에서 구현되었습니다.

4. (선택 사항) UNAB 사용자 및 그룹에 대한 권한을 관리하기 위한 권한을 Active Directory 의 UNIX 관리자에게 위임합니다.

5. 필요한 경우 2 단계에서 설치한 도구를 사용하여 Active Directory 의 UNIX 특성을 업데이트합니다.

   예를 들어, 관리자가 이 도구를 사용하여 사용자의 기본 로그인 셸을 업데이트합니다.

UNAB 와 Active Directory 의 상호 작용

완전 통합 모드에서 다음 UNIX 사용자 및 그룹 특성이 Active Directory 에 저장됩니다.

- UID
- GID
- 홈 디렉터리
- 로그인 셸
- GECOS

UNAB 는 Windows 2003 R2 스키마를 사용하여 이러한 특성을 저장합니다. 일반적으로 UNAB 는 이러한 특성을 읽지만 여기에 기록하지는 않습니다. UNAB 는 uxconsole -migrate 유틸리티를 사용하여 UNIX 사용자 및 그룹을 Active Directory 로 마이그레이션하는 경우에만 Active Directory 특성에 기록합니다.

UNAB 는 Active Directory 스키마를 확장하지 않습니다.

CA Access Control UNIX 특성 플러그 인 설치

CA Access Control UNIX 특성 플러그 인을 사용하면 Active Directory 의 UNAB 사용자에 대한 UNIX 특성을 관리할 수 있습니다. 이 플러그 인은 NIS 서버를 설치하지 않습니다. UNAB 사용자의 UNIX 특성을 관리하기 위해 사용할 수 있는 기타 도구에는 Microsoft Identity Management for UNIX, ADSI Edit, 단순 LDAP 클라이언트 등이 있습니다.

기본적으로 이 플러그 인은 Active Directory 2003 R2 스키마를 사용하여 Active Directory 데이터를 읽고 씁니다. R2 스키마가 없으면 다른 특성을 사용하도록 이 플러그 인을 구성할 수 있습니다.

사용자가 Active Directory 를 관리하기 위해 사용하는 서버에 이 플러그 인을 설치해야 하지만 Active Directory 도메인 컨트롤러(DC)에 이 플러그 인을 설치할 필요는 없습니다.

CA Access Control UNIX 특성 플러그 인을 설치하려면

1. UNIX 용 CA Access Control 끝점 구성 요소 DVD 를 서버의 광학 디스크 드라이브에 넣습니다.
2. 다음 디렉터리로 이동합니다.

   ADTools\UnixADTabExt

3. 사용하는 운영 체제에 맞는 디렉터리를 선택합니다.
4. setup.exe 파일을 두 번 클릭합니다.

   CA Access Control UNIX 특성 플러그 인 설치 마법사가 열립니다.
5. CA Access Control UNIX 특성 플러그 인을 설치하기 위한 지침을 따릅니다.

   CA Access Control UNIX 특성 플러그 인이 Active Directory 호스트에 설치됩니다.
6. (선택 사항) 플러그 인이 사용하는 Active Directory 특성을 구성합니다.

   Active Directory 스키마가 Windows 2003 R2 가 아닌 경우 이 단계를 완료합니다.

플러그 인이 사용하는 특성 구성

CA Access Control UNIX 플러그 인은 Active Directory 2003 R2 스키마를 사용하여 Active Directory 데이터를 읽고 씁니다. Active Directory 서버가 2003 R2 스키마를 사용하지 않는 경우 다른 스키마의 특성을 사용하도록 이 플러그 인을 구성할 수 있습니다.

다른 스키마의 특성을 사용하도록 플러그 인을 구성하는 경우 동일한 특성을 사용하도록 UNAB 끝점도 구성해야 합니다. uxauth.ini 파일의 맵 섹션을 사용하여 UNAB 끝점이 사용하는 특성을 구성합니다.

이 플러그 인이 사용하는 특성을 구성하려면 다음 레지스트리 항목의 값을 변경합니다. 이 항목은 다음 레지스트리 키에 있습니다.

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\uxauth

항목	기본값	플러그 인의 필드 이름
user_uid_attr_name	uidNumber	UID
user_loginshell_attr_name	loginShell	로그인 셸
user_homedir_attr_name	unixHomeDirectory	홈 디렉터리

항목	기본값	플러그 인의 필드 이름
user_gecos_attr_name	gecos	GECOS
user_gid_attr_name	gidNumber	주 그룹 이름/GID
group_gid_attr_name	gidNumber	GID(그룹 ID)

참고: uxauth.ini 파일에 대한 자세한 내용은 *참조 안내서*를 참조하십시오.

CA Access Control UNIX 특성 플러그 인 제거

CA Access Control UNIX 특성 플러그 인을 사용하면 Active Directory 의 사용자 및 그룹에 대한 UNIX 특성을 관리할 수 있습니다.

CA Access Control UNIX 특성 플러그 인을 제거하려면

1. "시작", "제어판", "프로그램 추가/제거"를 차례로 클릭합니다.

   "프로그램 추가/제거" 대화 상자가 나타납니다.

   참고: Windows Server 2008 에서는 "시작", "제어판", "프로그램 및 기능"을 클릭하십시오.

2. 프로그램 목록을 아래로 스크롤하여 "CA Access Control UNIX Attributes Snap-in"을 선택하십시오.
3. 사용하는 운영 체제에 따라 "변경/제거" 또는 "제거"를 클릭합니다.

   제거 프로세스는 시스템에서 CA Access Control UNIX 특성 플러그 인을 제거합니다.

4. 다음 레지스트리 키를 제거합니다.

   HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\uxauth

5. 컴퓨터에서 ACUnixAttributesShellExt.dll 파일을 삭제합니다.

   CA Access Control UNIX 특성 플러그 인이 제거됩니다.

예: ACUnixAttributesShellExt.dll 제거

다음 예는 C:\WINDOWS\system32 디렉터리에서 CA Access Control UNIX 특성 플러그 인을 제거합니다.

```
regsvr32 /u %WINDIR%\system32\ACUnixAttributesShellExt.dll
```

사용자 및 그룹 마이그레이션

UNIX 호스트에서 Active Directory 로 사용자를 마이그레이션하면 관리 작업이 하나의 관리 응용 프로그램으로 통합되므로 사용자 및 그룹의 관리가 단순해집니다. UNIX 호스트에 대한 액세스를 제어하는 Active Directory 로 UNIX 사용자를 마이그레이션하면 각 UNIX 호스트에서 암호 또는 섀도 파일을 관리할 필요가 없어집니다.

UNIX 호스트에서 Active Directory 로 사용자 및 그룹을 마이그레이션하면(완전 통합 모드), Active Directory 가 사용자의 인증과 권한 부여를 수행합니다.

추가 정보:

마이그레이션의 동작 방법 (페이지 329)
UNIX 사용자 및 그룹을 Active Directory 로 마이그레이션 (페이지 330)

마이그레이션의 동작 방법

UNIX 호스트에서 마이그레이션 프로세스를 시작하면 UNAB 는 다음 작업을 수행합니다.

1. 로컬 사용자 및 NIS/NIS+ 사용자의 목록을 검색합니다.

   Active Directory 에서 목록의 각 사용자 이름을 검사하여 각 사용자에 대해 다음 중 하나를 수행합니다.

   - 사용자가 Active Directory 에 있고 사용자 UNIX 특성이 UNIX 호스트에 나타난 특성과 동일한 경우 사용자 계정이 마이그레이션됩니다.
   - 사용자가 Active Directory 에 있고 여러 사용자 UNIX 특성이 없는 경우 UNAB 는 사용자를 마이그레이션하지 않고 누락된 속성을 로깅합니다.
   - 사용자가 Active Directory 에 있고 사용자에게 어떠한 UNIX 특성도 없는 경우 UNAB 는 사용자를 마이그레이션하고 누락된 특성을 추가합니다.
   - 사용자가 Active Directory 에 없으면 UNAB 는 Active Directory 에 해당 사용자 계정을 만들지 않습니다.

2. 로컬 그룹 및 NIS/NIS+ 그룹의 목록을 검색합니다.

   Active Directory 에서 그룹 이름을 검사하여 각 그룹에 대해 다음 중 하나를 수행합니다.

   - 그룹이 Active Directory 에 있고 그룹 UNIX 특성이 UNIX 호스트의 특성과 동일하면 그룹이 마이그레이션됩니다.
   - 그룹이 Active Directory 에 있고 그룹 ID 가 UNIX 호스트에 있는 ID 와 다르면 UNAB 는 그룹과 그 구성원을 Active Directory 로 마이그레이션하지 않습니다.
   - 그룹이 Active Directory 에 있고 그룹 ID 가 동일하지만 여러 UNIX 특성이 없는 경우 UNAB 는 그룹을 Active Directory 로 마이그레이션하고 누락된 특성을 완성합니다.
   - 그룹이 Active Directory 에 없으면 UNAB 는 그룹을 만들어 이 그룹을 Active Directory 로 마이그레이션합니다.

참고: Active Directory 에 동일한 이름의 사용자 또는 그룹이 있으면 사용자 또는 그룹을 마이그레이션할 수 없습니다. 예를 들어, 이름이 g1 인 그룹을 마이그레이션하려고 할 때 이름이 g1 인 사용자가 Active Directory 에 있으면 UNAB 가 이 그룹을 마이그레이션할 수 없습니다.

참고: root 사용자를 Active Directory 로 마이그레이션하도록 선택한 경우 root 계정이 로컬 및 Active Directory 에서 로그온 시 인증됩니다. 따라서 인증 프로세스가 길어질 수 있습니다.

UNIX 사용자 및 그룹을 Active Directory 로 마이그레이션

로컬 UNIX 호스트에서 Active Directory 로 사용자를 마이그레이션하면 단일 위치에서 호스트에 대한 액세스를 관리할 수 있습니다.

UNIX 사용자 및 그룹을 Active Directory 로 마이그레이션하려면

1. root 로 UNIX 컴퓨터에 로그인합니다.
2. 기본적으로 다음 위치에 있는 UNAB 설치 bin 디렉터리로 이동합니다.

   /opt/CA/uxauth/bin

3. -uxconsole -migrate 유틸리티를 실행합니다.

   uxconsole 프로그램은 UNIX 사용자 및 그룹을 Active Directory 로 마이그레이션합니다. 작업이 성공적으로 완료되었음을 알리는 메시지가 표시됩니다.

참고: 마이그레이션 충돌 해결에 대한 자세한 내용은 *엔터프라이즈 관리 안내서*를 참조하십시오. uxconsole 유틸리티에 대한 자세한 내용은 *참조 안내서*를 참조하십시오.

UNIX 관리자에게 UNIX 사용자 및 그룹 특성 관리 권한 위임

UNIX 관리자가 Active Directory 에서 UNIX 사용자 및 그룹 특성을 관리할 수 있도록 특정 관리 권한을 UNIX 관리자에게 위임할 수 있습니다. 관리 권한을 위임하면 UNIX 관리자가 Active Directory 로 마이그레이션된 이후에 계속 UNIX 사용자 및 그룹 특성을 관리할 수 있습니다.

관리 권한을 위임하기 전에 Active Directory 사용자의 UNIX 특성을 관리할 수 있게 해주는 도구를 설치했는지 확인하십시오. 관리 권한은 개별 사용자가 아닌 그룹에 위임하는 것이 좋습니다.

예: UNIX 관리자에게 UNIX 사용자 및 그룹 특성 관리 권한 위임

다음 예는 Active Directory 의 UNIX 사용자 및 그룹을 관리하기 위한 권한을 UNIX 관리자의 그룹에 위임하는 방법을 보여줍니다.

1. Active Directory 컴퓨터에서 "시작", "프로그램", "관리 도구", "Active Directory 사용자 및 컴퓨터"를 클릭합니다.

   "Active Directory 사용자 및 컴퓨터" 관리 콘솔이 열립니다.

2. 조직 단위(OU)를 마우스 오른쪽 단추로 클릭하고 "속성"을 선택합니다.

   "조직 단위" 속성 창이 열립니다.

3. "보안" 탭을 선택합니다.

   참고: "보안" 탭이 보이지 않으면 "보기" 탭 아래의 "고급 기능" 옵션이 강조 표시되어 있는지 확인하십시오.

4. "고급"을 클릭한 다음 "추가" 단추를 클릭합니다.

   "사용자, 컴퓨터 또는 그룹 선택" 창이 열립니다.

5. 관리 권한을 위임할 대상 그룹 또는 사용자의 이름을 입력합니다. "확인"을 클릭합니다.

   "권한 항목" 창이 열립니다.

6. "속성" 탭을 클릭합니다.

   이 창에서 그룹 또는 사용자에게 권한을 할당합니다.

7. "적용 대상" 메뉴에서 "그룹 개체"를 선택합니다.

8. "허용" 열에서 "gidNumber 읽기" 및 "gidNumber 쓰기" 옵션을 선택합니다.

9. "확인"을 클릭합니다.

   UNIX 그룹에 대한 관리 특성을 UNIX 관리자 그룹에게 위임했습니다.

10. 1-6 단계를 반복하여 UNIX 사용자에 대한 관리 권한을 위임합니다.

11. "적용 대상" 메뉴에서 "사용자 개체"를 선택합니다.

12. "허용" 열에서 다음 특성을 선택합니다.
    - Gecos 읽기
    - Gecos 쓰기
    - gidNumber 읽기
    - gidNumber 쓰기
    - uid 읽기
    - uid 쓰기
    - uidNumber 읽기
    - uidNumber 쓰기
    - unixHomeDirectory 읽기
    - unixHomeDirectory 쓰기
    - loginShell 읽기
    - LoginShell 쓰기
13. "확인"을 클릭합니다.

    UNIX 사용자에 대한 관리 특성을 UNIX 관리자 그룹에게 위임했습니다.

Active Directory 사용자에 대한 UNIX 특성 구성

이 절차는 CA Access Control UNIX 특성 플러그 인을 사용하여 Active Directory 에서 UNIX 사용자의 특성을 관리하는 방법에 대해 설명합니다. Microsoft Identity Management for UNIX, ADSI Edit, 단순 LDAP 클라이언트와 같은 다른 도구를 사용하여 Active Directory 에서 UNIX 특성을 관리할 수 있습니다.

참고: 사용자 계정 속성을 정의할 때 이 사용자가 로그온할 수 있는 컴퓨터를 지정할 필요는 없습니다. 이 설정은 UNIX 호스트에 적용되지 않습니다.

Active Directory 사용자에 대한 UNIX 특성 구성

1. "시작", "프로그램", "관리 도구", "Active Directory 사용자 및 도구"를 차례로 선택합니다.

   "Active Directory 사용자 및 컴퓨터" 창이 열립니다.
2. 사용자 계정을 두 번 클릭합니다.

   사용자 계정 속성이 표시됩니다.

3. "CA Access Control UNIX 특성" 탭을 클릭합니다.

   "CA Access Control UNIX 특성" 탭이 나타납니다.

4. 다음 필드를 완료하십시오.

   UNIX 특성 활성화

   UNIX 특성이 사용자 계정에서 활성화되었는지 여부를 지정합니다. 해당 사용자에 대한 UNIX 특성을 활성화하려면 이 확인란을 선택해야 합니다.

   UID

   UNIX 컴퓨터에서 사용자 ID 번호를 정의합니다. "생성"을 클릭하여 다음 사용 가능한 UID 를 찾습니다.

   홈 디렉터리

   UNIX 컴퓨터에서 사용자 홈 디렉터리를 정의합니다.

   예: /home/user

   중요! 사용자 홈 디렉터리를 구성하기 전에 홈 디렉터리의 부모 디렉터리가 있는지 확인하십시오.

   로그인 셸

   사용자 계정 로그인 셸을 정의합니다.

   예: /bin/sh

   GECOS

   사용자 GECOS 정보를 지정합니다.

   주 그룹 이름/GID

   사용자가 구성원으로 포함된 주 그룹 이름 또는 GID 를 정의합니다.

   예: UNIXUsers

   중요! 사용자 계정을 정의할 때 올바른 그룹 이름/GID 를 할당해야 합니다.

5. "확인"을 클릭합니다.

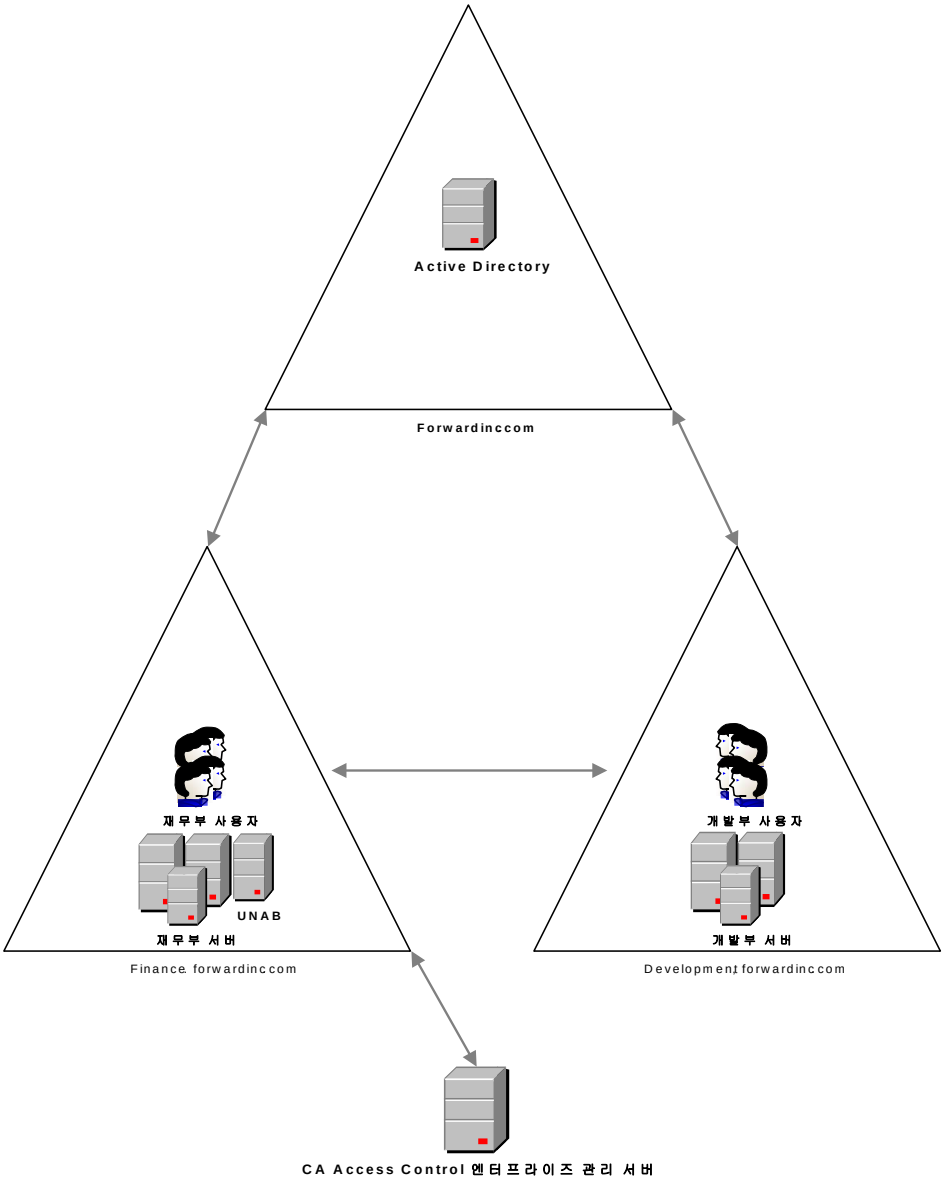
   사용자 UNIX 특성이 구성되었습니다.

트러스트된 도메인 환경에서 UNAB 구현

UNAB 를 설치할 때 UNAB 가 등록할 도메인의 매개 변수를 지정합니다. UNAB 를 설치, 등록, 활성화한 이후에 사용자 및 그룹을 이 도메인으로 마이그레이션합니다.

지정한 도메인에 다른 도메인과의 트러스트 관계가 있는 경우, 이러한 도메인의 사용자들은 잠재적으로 UNAB 가 구성원인 도메인의 컴퓨터에 액세스할 수 있습니다.

이 다이어그램은 트러스트된 도메인 환경에서 UNAB 구현을 표시합니다.



이전 다이어그램에서 UNAB 는 다른 도메인과 트러스트 연결된 도메인에 설치되어 있습니다. 이 환경에서 트러스트된 도메인의 사용자들은 다른 도메인의 구성원이 아님에도 불구하고 해당 도메인에 액세스할 수 있습니다.

트러스트된 도메인 환경에서 UNAB 를 설치하기 전에 다음 사항을 고려하십시오.

- UNAB 로그인 정책은 사용자 이름을 기반으로 도메인에 있는 컴퓨터에 대한 액세스를 제어합니다. 동일한 이름을 사용하는 여러 사용자가 여러 도메인에서 정의된 경우 UNAB 는 사용자의 원래 도메인을 구분할 수 없으며 도메인에 대한 액세스를 부여합니다.
- UNAB 가 구성원으로 속한 도메인에 대해서만 보고서를 생성할 수 있습니다. 트러스트된 도메인에 대해 보고서를 생성할 수 없습니다.
- UNAB 가 구성원으로 속한 도메인에 정의된 사용자를 Active Directory 로 마이그레이션할 수 있습니다.

트러스트된 도메인의 권한 없는 사용자가 액세스할 수 없도록 고유한 사용자 및 그룹 이름을 사용하는 것이 좋습니다.

제 10 장: 끝점 관리 설치

이 섹션은 다음 항목을 포함하고 있습니다.

끝점 관리 서버를 준비하는 방법

CA Access Control 끝점 관리를 설치하기 전에 서버를 준비해야 합니다.

중요! CA Access Control 엔터프라이즈 관리를 동일한 컴퓨터에 설치하려는 경우 다음 단계를 수행할 필요가 없습니다. 설치 프로그램은 CA Access Control 끝점 관리를 CA Access Control 엔터프라이즈 관리 설치의 일부로 설치합니다.

끝점 관리 서버를 준비하려면 다음을 수행하십시오.

1. 지원되는 JDK(Java Development Kit)를 설치합니다.

   참고: 필수 타사 소프트웨어는 CA Access Control Premium Edition 타사 구성 요소 DVD 에서 찾을 수 있습니다. 지원되는 버전에 대한 자세한 내용은 *릴리스 정보*를 참조하십시오.

2. 지원되는 JBoss 버전을 설치합니다.

   JBoss 를 서비스(UNIX 의 데몬)로 설치할 것을 권장합니다.

   참고: 필수 타사 소프트웨어는 CA Access Control Premium Edition 타사 구성 요소 DVD 에서 찾을 수 있습니다. 지원되는 버전에 대한 자세한 내용은 *릴리스 정보*를 참조하십시오.

3. CA Access Control 을 설치합니다.

   참고: CA Access Control 끝점 설치 지침을 따르십시오.

4. (Windows 전용) 컴퓨터를 다시 시작합니다.
5. CA Access Control 서비스(secons -s)를 중지합니다.

   이제 서버에 CA Access Control 끝점 관리를 설치할 준비가 되었습니다.

Windows 에 CA Access Control 끝점 관리 설치

Windows 에 해당

그래픽 인터페이스 설치에서는 마법사를 사용하여 CA Access Control 끝점 관리를 WIndows 컴퓨터에 설치하는 과정을 안내합니다.

Windows 에 CA Access Control 끝점 관리를 설치하려면

1. 서버를 올바르게 준비 (페이지 337)하는지 확인합니다.
2. Windows 용 CA Access Control Premium Edition 서버 구성 요소 DVD 를 광 디스크 드라이브에 넣습니다.
3. CA Access Control 제품 탐색기(ProductExplorerx86.EXE)를 엽니다.

   CA Access Control 제품 탐색기가 나타납니다.
4. "구성 요소" 폴더를 확장하고 CA Access Control 끝점 관리를 선택한 다음, "설치"를 클릭합니다.

   InstallAnywhere 마법사가 로드되기 시작합니다.
5. 필요에 따라 마법사를 완료합니다. 다음 설치 입력 항목은 자동으로 채워지지 않습니다.

   JBoss 폴더

   JBoss 응용 프로그램 서버를 설치할 위치를 정의합니다.

   지원되는 JBoss 버전을 사용하는 경우 이 위치는 JBoss zip 파일의 내용을 추출한 위치입니다.

   웹 서비스 정보

   CA Access Control 웹 서비스를 설치하려는 *위치*와 이 서비스가 사용할 *포트*(기본값: 5248)를 정의합니다.

   전체 컴퓨터 이름

   응용 프로그램 서버(로컬 컴퓨터)의 이름을 정의합니다. 응용 프로그램에 액세스할 때 URL 에서 사용해야 하는 이름입니다.

   이제 설치가 완료되었습니다.

Solaris 또는 Linux 에 CA Access Control 끝점 관리 설치

Solaris 또는 Linux 컴퓨터에 CA Access Control 끝점 관리를 설치하려면 콘솔 설치를 사용해야 합니다.

Solaris 또는 Linux 에 CA Access Control 끝점 관리를 설치하려면

1. 서버를 올바르게 준비 (페이지 337)했는지 확인합니다.
2. Solaris 용 CA Access Control Premium Edition 서버 구성 요소 또는 Linux 용 서버 구성 요소 DVD 를 광 디스크 드라이브에 넣습니다.
3. 광 디스크 드라이브를 마운트합니다.
4. 터미널 창을 열고 광디스크 드라이브에서 EndPointMgmt 디렉터리로 이동합니다.
5. 다음 명령을 입력합니다.

   ```
   install_EM_r125.bin -i console
   ```

   잠시 후 InstallAnywhere 콘솔이 나타납니다.
6. 필요에 따라 프롬프트를 완성합니다. 다음 설치 입력 항목은 자동으로 채워지지 않습니다.

   번호로 로캘 선택

   설치할 때 사용할 로캘을 나타내는 번호를 정의합니다.

   참고: 영어 이외의 지원되는 언어로 설치하려면 현지화(로컬라이제이션)된 운영 체제가 필요합니다.

   JBoss 폴더

   JBoss 응용 프로그램 서버를 설치할 위치를 정의합니다.

   지원되는 JBoss 버전을 사용하는 경우 이 위치는 JBoss zip 파일의 내용을 추출한 위치입니다.

   웹 서비스 정보

   CA Access Control 웹 서비스를 설치하려는 *위치*와 이 서비스가 사용할 *포트*(기본값: 5248)를 정의합니다.

   전체 컴퓨터 이름

   응용 프로그램 서버(로컬 컴퓨터)의 이름을 정의합니다. 응용 프로그램에 액세스할 때 URL 에서 사용해야 하는 이름입니다.

   이제 설치가 완료되었습니다.

Windows 에서 CA Access Control 끝점 관리 제거

Windows 관리자 권한을 가진 사용자(Windows administrator 또는 Windows Administrators 그룹의 구성원)로 Windows 시스템에 로그인합니다.

Windows 에서 CA Access Control 끝점 관리를 제거하려면

1. JBoss 가 실행 중인 경우 중지합니다.
2. "시작", "제어판", "프로그램 추가/제거"를 차례로 클릭합니다.

   "프로그램 추가/제거" 대화 상자가 나타납니다.
3. 프로그램 목록을 스크롤하여 CA Access Control 끝점 관리를 선택합니다.
4. "변경/제거"를 클릭합니다.

   CA Access Control 끝점 관리 제거 마법사가 나타납니다.
5. 마법사의 지시에 따라 CA Access Control 끝점 관리를 제거합니다.

   제거가 완료되고 컴퓨터에서 CA Access Control 끝점 관리가 제거됩니다.
6. "마침"을 클릭하여 마법사를 닫습니다.

Solaris 또는 Linux 에서 CA Access Control 끝점 관리 제거

컴퓨터에서 CA Access Control 끝점 관리를 제거하려면 CA Access Control 끝점 관리에서 제공하는 제거 프로그램을 사용해야 합니다.

Solaris 또는 Linux 에서 CA Access Control 끝점 관리를 제거하려면

1. 다음 중 *하나*를 수행하여 JBoss 를 중지합니다.
   - JBoss 작업 창에서 프로세스를 인터럽트(Ctrl+C)합니다.
   - 다른 창에서 다음을 입력합니다.

     ./JBoss_path/bin/shutdown -S
2. 다음 명령을 입력합니다.

   "*/ACEMInstallDir*/Uninstall_EndpointManagement/Uninstall_CA_Access_Control_Endpoint_Management"

   ACEMInstallDir

   CA Access Control 끝점 관리의 설치 디렉터리를 정의합니다. 기본적으로 이 경로는 다음과 같습니다.

   /opt/CA/AccessControlServer/EndpointManagement/

   InstallAnywhere 가 제거 콘솔을 로드합니다.
3. 화면에 표시되는 메시지에 따라 CA Access Control 끝점 관리를 제거합니다.

   제거가 완료되고 컴퓨터에서 CA Access Control 끝점 관리가 제거됩니다.

CA Access Control 끝점 관리 시작

CA Access Control 끝점 관리를 설치한 후에는 CA Access Control 및 웹 응용 프로그램 서버를 시작해야 합니다.

CA Access Control 끝점 관리를 시작하려면

1. CA Access Control 서비스를 시작합니다.

   CA Access Control 끝점 관리를 시작하려면 CA Access Control 이 실행 중이어야 합니다.

2. (Windows 에만 해당) 다음을 수행합니다.

   a. 다음 추가 서비스를 시작합니다. 이러한 서비스는 seosd -start 명령의 실행으로 로드되지 않습니다.

      - CA Access Control 웹 서비스
      - CA Access Control 메시지 큐(있는 경우)

   b. 다음 중 하나를 수행하여 JBoss 응용 프로그램 서버를 시작합니다.

      - "시작", "프로그램", "CA, Access Control", "작업 엔진 시작"을 클릭합니다.

        참고: 처음 시작하는 경우 작업 엔진이 로드될 때까지 시간이 걸릴 수 있습니다.

      - "서비스" 패널에서 "JBoss Application Server" 서비스를 시작합니다.

      JBoss Application Server 의 로드가 완료되면 CA Access Control 끝점 관리 웹 기반 인터페이스에 로그인할 수 있습니다.

3. (UNIX 에만 해당) ./*JBoss_HOME*/bin/run.sh -b 0.0.0.0 을 입력합니다.

   참고: JBoss Application Server 를 처음 시작하는 경우 로드할 때 시간이 오래 걸릴 수 있습니다.

   JBoss Application Server 의 로드가 완료되면 CA Access Control 끝점 관리 웹 기반 인터페이스에 로그인할 수 있습니다.

CA Access Control 끝점 관리 열기

CA Access Control 끝점 관리를 설치하고 시작하면 CA Access Control 끝점 관리의 URL 을 사용하여 원격 컴퓨터에서 웹 기반 인터페이스를 열 수 있습니다.

CA Access Control 끝점 관리를 열려면

1. 웹 브라우저를 열고 호스트에 대해 다음 URL 을 입력합니다.

   http://*enterprise_host*:*port*/acem

2. 다음 정보를 입력합니다.

   사용자 이름

   CA Access Control 관리 작업을 수행할 권한이 있는 사용자의 이름을 정의합니다.

   참고: 로그인에 사용한 사용자 이름에는 컴퓨터 이름(예: Windows 의 경우 *myComputer\Administrator* 또는 UNIX 의 경우 *root*)이 포함되어야 합니다.

   암호

   CA Access Control 사용자의 암호를 정의합니다.

   호스트 이름

   관리 작업을 수행할 끝점의 이름을 정의합니다. 이 이름은 호스트 또는 PMDB 가 될 수 있으며 *PMDB_name@host_name* 형식으로 지정해야 합니다.

   참고: 사용자는 CA Access Control 끝점 관리가 설치된 컴퓨터에서 끝점을 관리할 권한을 가지고 있어야 합니다(TERMINAL 리소스 사용).

   "로그인"을 클릭합니다.

   CA Access Control 끝점 관리가 "대시보드" 탭에서 열립니다.

참고: CA Access Control 끝점 관리를 설치한 Windows 컴퓨터에서 "시작", "프로그램", "CA, Access Control", "끝점 관리"를 클릭하여 CA Access Control 끝점 관리를 열 수도 있습니다.

예: CA Access Control 끝점 관리 열기

네트워크에 있는 임의의 컴퓨터에서 CA Access Control 끝점 관리를 열려면 웹 브라우저에 다음 URL 을 입력하십시오.

http://appserver123:18080/acem

이 URL 은 CA Access Control 끝점 관리가 appserver123 이라는 이름의 호스트에 설치되었으며 기본 JBoss 포트 18080 을 사용함을 나타냅니다.

제 11 장: 고가용성 배포 설치

이 섹션은 다음 항목을 포함하고 있습니다.

고가용성

CA Access Control 엔터프라이즈 관리는 미러링된 사이트를 사용하여 고가용성 배포를 제공합니다. *미러된* 사이트는 완전한 실시간 정보 미리링을 사용하는 완전히 중복된 설비이며 모든 기술 측면에서 기본 사이트와 동일합니다. 데이터는 처리되어 동시에 기본 및 미러된 사이트에 저장됩니다.

미러된 사이트는 장애 조치를 위한 능동-수동 배포를 사용합니다. *능동-수동* 배포는 두 개 이상의 데이터센터를 포함하며, 그 중 하나는 능동적으로 프로세스 요청을 처리하고 다른 하나는 현재 동작 중인 데이터센터에 장애가 발생할 경우 요청을 처리할 수 있도록 대기합니다. 선택하는 클러스터링 소프트웨어는 능동 및 수동 서버를 제어하고 장애 발생 시 이 둘을 서로 전환할 책임이 있습니다.

능동-활성 배포에서 능동 서버는 기본 서버, 수동 서버는 보조 서버라고 불립니다.

고가용성 배포의 이점 및 제한

고가용성 배포를 사용하면 하나 이상의 구성 요소 또는 서버에 장애가 발생하는 경우 CA Access Control 엔터프라이즈 관리 구성 요소가 계속 요청을 처리할 수 있습니다. 끝점이 기본 환경에 연결할 수 없는 경우 기본 환경이 복구될 때까지 보조 서버에 연결합니다.

고가용성 배포는 다음과 같은 이점이 있습니다.

- 기본 엔터프라이즈 관리 서버에 장애가 발생하는 경우 권한 있는 계정, DMS 데이터 원본 파일, 끝점 정의의 손실을 방지합니다.
- 사용에 중단이 발생하지 않게 합니다.

고가용성 배포를 계획할 때는 다음과 같은 제한 사항을 고려하십시오.

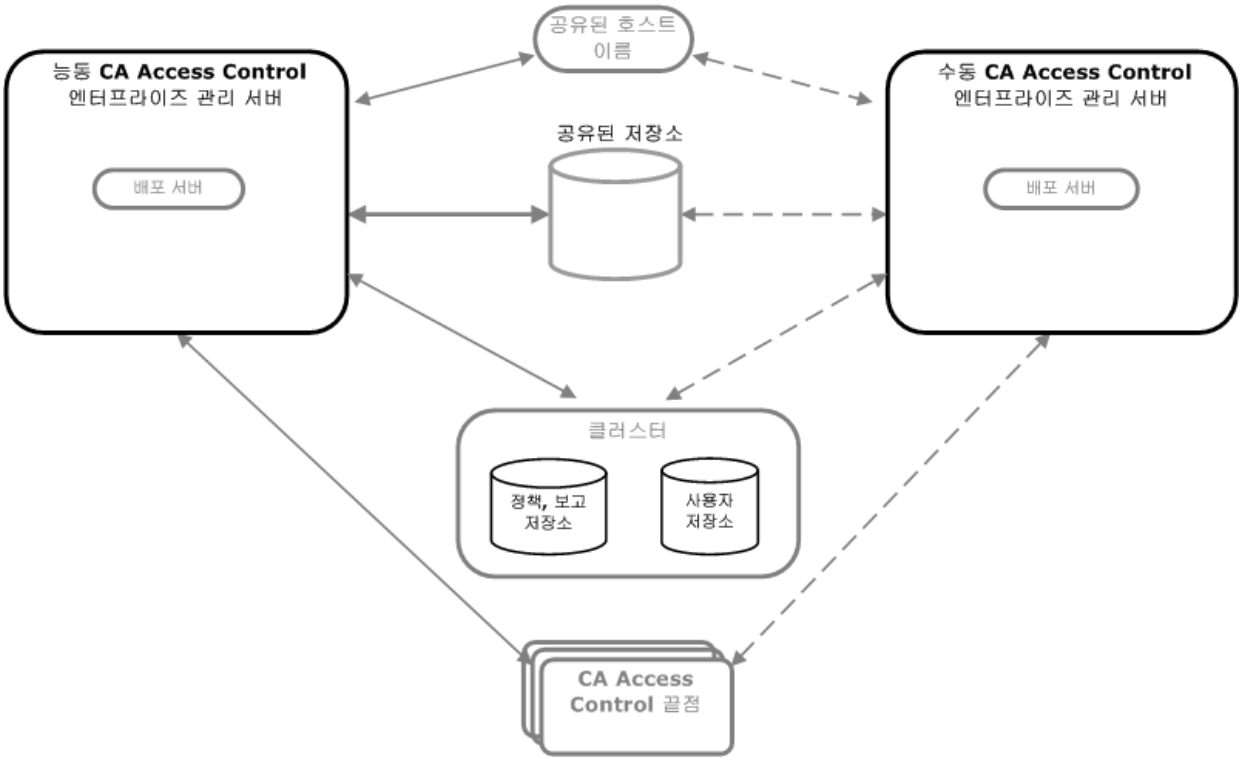
- 엔터프라이즈 관리 서버는 장애 발생 시 세션 연속성을 지원하지 않습니다. 능동 서버가 응답하지 않으면 사용자 세션이 종료됩니다. 로그인한 사용자는 반드시 다시 로그인해야 합니다.
- 하나의 능동 DMS 만 지원됩니다.
- 기본 및 보조 엔터프라이즈 관리 서버를 설치할 때는 동일한 통신 암호가 사용됩니다.
- 기본 및 보조 서버의 Java Connector Sever(JCS)의 이름은 동일해야 합니다.

참고: 장애 발생 시 서버 사이에서 원활히 전환될 수 있도록 클러스터링 소프트웨어 솔루션에서 제어되는 가상 DNS 이름을 사용하는 것이 좋습니다.

예를 들어, 사용자 세션이 열렸을 때 기본 엔터프라이즈 관리 서버에 장애가 발생할 경우 사용자는 보조 엔터프라이즈 관리 서버의 URL 을 입력하거나, 가상 DNS 또는 부하 분산 장치를 사용하여 동일한 URL 을 사용하여 계속 작업할 수 있습니다.

고가용성 배포 아키텍처

다음 다이어그램은 고가용성 환경의 CA Access Control 엔터프라이즈 관리를 보여줍니다.



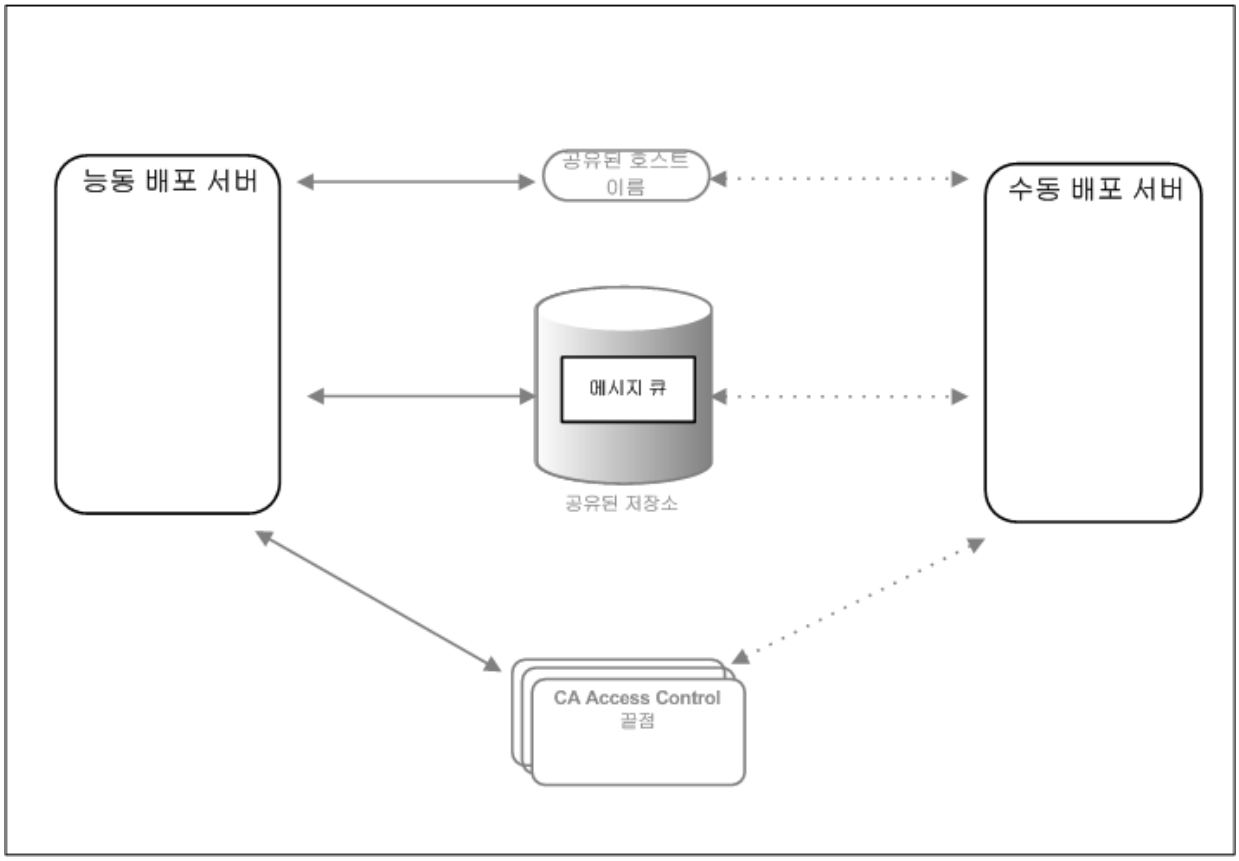
이전 다이어그램에 표시된 것처럼 고가용성 배포는 다음 구성 요소를 포함합니다.

- 기본 엔터프라이즈 관리 서버 및 하나 이상의 보조 엔터프라이즈 관리 서버
- 정책, 보고 저장소, 사용자 저장소의 클러스터된 설치
- 주 및 보조 CA Access Control 엔터프라이즈 관리 서버 모두가 액세스할 수 있는 공유 저장소
- 공유된 호스트 이름
- 기본 및 보조 엔터프라이즈 관리 서버 모두와 동작할 수 있는 CA Access Control 끝점

고가용성 환경 아키텍처의 배포 서버

배포 서버에 장애가 발생할 경우 끝점에서 수집된 감사 이벤트의 손실을 방지하기 위해 고가용성을 위해 추가 배포 서버를 배포할 수 있습니다.

다음 다이어그램은 고가용성 환경에서 기본 및 보조 배포 서버의 구현을 보여줍니다.



이전 다이어그램에 표시된 것처럼 배포 서버의 고가용성 구현은 다음 사항에 기반합니다.

- 기본 배포 서버 및 하나 이상의 보조 배포 서버
- 메시지 큐 데이터 파일을 보유하며 기본 및 보조 배포 서버가 모두 액세스할 수 있는 공유 저장소

  배포 서버에 장애가 발생할 경우 끝점에서 받은 감사 이벤트 메시지가 손실되지 않도록 메시지 큐 데이터 파일을 공유 저장소에 저장합니다.
- 공유 호스트 이름
- 기본 및 보조 배포 서버 모두와 동작할 수 있는 CA Access Control 끝점

고가용성 환경의 구성 요소

고가용성 환경에서 CA Access Control 을 배포하려면 다음 항목이 필요합니다.

- 기본 서버:
  - 엔터프라이즈 관리 서버
- 보조 서버:
  - 엔터프라이즈 관리 서버
- 사용자 리포지토리
- 정책 및 보고 데이터베이스
- 공유 저장소 솔루션:
  - 클러스터 소프트웨어
  - 공유 저장소

공유 저장소

공유 저장소 장치를 사용하여 공유 저장소 솔루션을 구현하는 것이 좋습니다. 공유 저장소는 능동 및 수동 서버 모두가 액세스할 수 있어야 합니다. 사용하는 공유 저장소 솔루션이 다음 조건을 충족하는지 확인하십시오.

- 쓰기 순서 - 공유 저장소 솔루션은 버퍼에 발생한 순서와 동일한 순서로 데이터 블록을 공유 저장소에 써야 합니다.
- 동기 쓰기 보존 - 동기 쓰기 호출에서 반환되었을 때 저장소 솔루션은 모든 데이터가 지속 가능한 보존 저장소에 기록되었음을 보증합니다.

다음은 소프트웨어 기반 공유 저장소 솔루션의 예입니다.

- 이중 포트 SCSI 장치
- SAN(저장소 영역 네트워크)

이중 포트 SCSI 및 SAN 솔루션은 쓰기 순서 및 동기 쓰기 보존 요구 사항을 충족합니다.

클러스터 소프트웨어

클러스터 소프트웨어는 네트워크에 있는 여러 서버가 하나의 컴퓨터 클러스터로 동작하여 응용 프로그램 고가용성을 제공할 수 있게 합니다.

중요! 이 장에서 설명한 단계는 Microsoft 클러스터 소프트웨어와 Active Directory 에만 적용됩니다.

고가용성 배포에서 클러스터 소프트웨어는 다음 작업을 수행합니다.

- 기본 및 보조 엔터프라이즈 관리 서버의 상태를 모니터링합니다.
- 한 번에 하나의 인스턴스(기본 또는 보조 서버)만 활성화되어 있는지 확인합니다.
- 엔터프라이즈 관리 서버에서 CA Access Control 서비스를 관리합니다.
- 끝점을 활성 서버로 가리키는 공유 호스트 이름을 관리합니다.

장애 시 어떤 일이 발생합니까?

고가용성 배포에서 클러스터링 솔루션 소프트웨어는 지정된 주기로 기본 서버의 가용성을 쿼리합니다. 기본 서버가 미리 정의된 기간 내에 응답하지 않으면 클러스터링 소프트웨어와 CA Access Control 이 다음을 수행합니다.

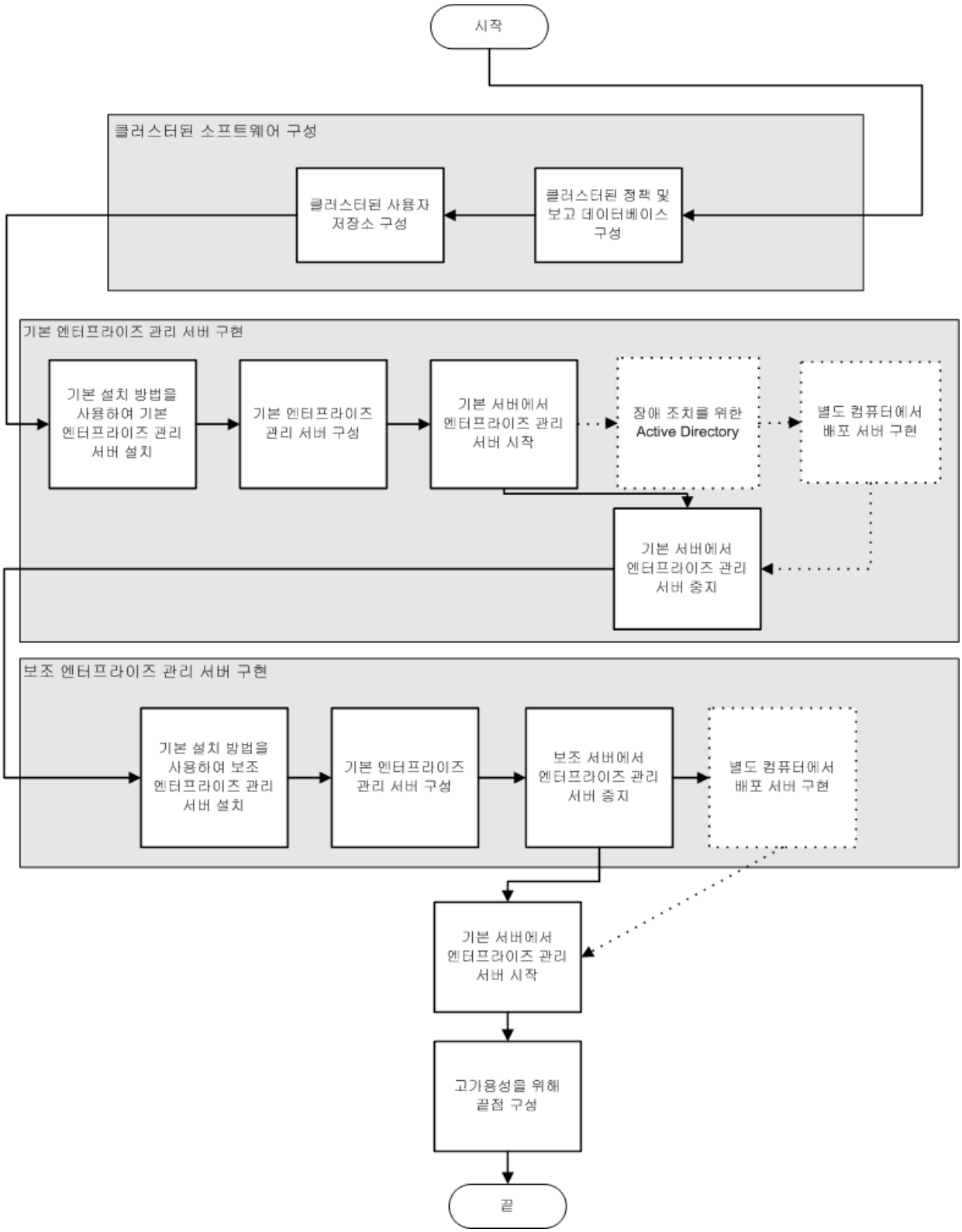
1. 클러스터링 솔루션 소프트웨어는 기본 서버에서 실행 중인 모든 엔터프라이즈 관리 서버 서비스를 중지합니다.
2. 클러스터링 솔루션 소프트웨어는 보조 서버에서 모든 엔터프라이즈 관리 서버 서비스를 시작합니다.
3. CA Access Control 은 보조 서버에 대한 연결을 시도하고 작업을 계속합니다.
4. 클러스터링 소프트웨어 솔루션이 기본 서버에서 엔터프라이즈 관리 서버 서비스를 중지하고 응용 프로그램에 로그인한 모든 사용자가 로그아웃됩니다. 응용 프로그램을 계속 사용하려면 사용자는 CA Access Control 엔터프라이즈 관리에 다시 로그인해야 합니다.

고가용성을 위해 CA Access Control 엔터프라이즈 관리를 구성하는 방법

고가용성 배포를 올바로 구성하려면 올바른 순서로 기본 및 보조 엔터프라이즈 관리 서버를 설정해야 합니다.

다음 다이어그램은 고가용성 환경에서 여러 엔터프라이즈 관리 서버를 구현하기 위해 수행하는 단계를 보여줍니다.

참고: 장애 조치를 위해 Active Directory 를 구성하고 별도 컴퓨터에서 배포 서버를 구성하는 것은 선택적인 단계입니다.


시작
클러스터된 소프트웨어 구성
클러스터된 사용자 저장소 구성
클러스터된 정책 및 보고 데이터베이스 구성
기본 엔터프라이즈 관리 서버 구현
기본 설치 방법을 사용하여 기본 엔터프라이즈 관리 서버 설치
기본 엔터프라이즈 관리 서버 구성
기본 서버에서 엔터프라이즈 관리 서버 시작
장애 조치를 위한 Active Directory
별도 컴퓨터에서 배포 서버 구현
기본 서버에서 엔터프라이즈 관리 서버 중지
보조 엔터프라이즈 관리 서버 구현
기본 설치 방법을 사용하여 보조 엔터프라이즈 관리 서버 설치
기본 엔터프라이즈 관리 서버 구성
보조 서버에서 엔터프라이즈 관리 서버 중지
별도 컴퓨터에서 배포 서버 구현
기본 서버에서 엔터프라이즈 관리 서버 시작
고가용성을 위해 끝점 구성
끝

추가 정보:

엔터프라이즈 관리 서버 구성 요소를 설치하는 방법 (페이지 54)
보고 서비스 서버 구성 요소 설정 방법 (페이지 99)

기본 엔터프라이즈 관리 서버 구성

기본 엔터프라이즈 서버는 중앙 관리 서버로서, 끝점에 정책을 배포하고, 권한 있는 계정을 관리하고, 리소스/접근자/액세스 수준을 정의할 수 있는 도구 및 구성 요소를 포함하고 있습니다.

다음 단계를 수행하십시오.

1. 아직 수행하지 않은 경우 기본 서버에 CA Access Control 엔터프라이즈 관리를 설치합니다.

   여기까지 모든 웹 기반 응용 프로그램, 배포 서버, DMS, CA Access Control 이 설치되었습니다.
2. 모든 CA Access Control 서비스를 중지합니다.
3. 서비스를 수정하여 자동이 아닌 수동으로 시작되도록 합니다.
4. 다음과 같이 DMS 및 DH 를 공유 저장소에 복사합니다.
   a. DMS 디렉터리를 찾아 공유 저장소에 복사합니다. 이 디렉터리는 다음 위치에 있습니다.

      ACServerInstallDir/APMS/AccessControl/data/DMS__

      ACServerInstallDir

      엔터프라이즈 관리 서버가 설치된 디렉터리의 이름을 정의합니다.

   b. DH 디렉터리를 찾아 공유 저장소에 복사합니다. 이 디렉터리는 다음 위치에 있습니다.

      ACServerInstallDir/APMS/AccessControl/Data/DH__

   c. DH__WRITER 디렉터리를 찾아 공유 저장소에 복사합니다. 기본적으로 이 디렉터리는 다음 위치에 있습니다.

      ACServerInstallDir/APMS/AccessControl/Data/DH__WRITER

   d. _pmd directory_ 레지스트리 키 구성 설정을 DMS 및 DH 를 복사한 공유 저장소 디렉터리의 전체 경로 이름으로 설정합니다. 예: Z:\PMD.

   기본 서버는 공유 저장소에 DMS 및 DH 를 사용하도록 구성됩니다.

5. 다음과 같이 공유 저장소를 사용하도록 메시지 큐를 구성합니다.
   a. 메시지 큐 데이터 저장소 폴더를 공유 저장소로 복사합니다. 이러한 파일은 다음 디렉터리에 있습니다.

      ACServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data

   b. 편집을 위해 tibemsd.conf 파일을 엽니다. 이 파일은 기본적으로 다음 디렉터리에 있습니다.

      EACServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data

   c. "store" 토큰의 값을 데이터 저장소 파일을 복사한 공유 저장소의 디렉터리에 대한 지점으로 설정합니다. 예:Z:\PMD\DATASTORE
   d. 파일을 저장한 후 닫습니다.
   e. 편집을 위해 queues.conf 파일을 엽니다.
   f. 쉼표를 추가하고 모든 쿼리 정의 줄의 끝에 "failsafe"란 단어를 추가한 다음 파일을 저장하고 닫습니다.
6. 다음과 같이 기본 엔터프라이즈 관리 서버가 작업을 다시 시작할 때 모든 CA Access Control 서비스를 시작하는 배치 파일을 만듭니다.

   ```
   seosd -start
   net start acrptmq
   net start "CA Access Control Web Service"
   net start im_jcs
   net start JBAS50SVC
   ```

7. 다음과 같이 기본 엔터프라이즈 관리 서버에 오류가 발생할 경우 모든 CA Access Control 서비스를 중지하는 배치 파일을 만듭니다.

   ```
   secons -s

   net stop acrptmq
   net stop "CA Access Control Web Service"
   net stop im_jcs
   net stop JBAS50SVC
   ```

8. 오류 발생 시 스크립트를 실행하는 클러스터 소프트웨어를 구성합니다.
9. 모든 CA Access Control 서비스를 시작합니다.

예: queues.conf 파일 편집

queues.conf 파일의 다음 조각은 공유 저장소를 사용하도록 메시지 큐를 구성하기 위해 파일을 수정하는 방법의 예제입니다.

```
queue/snapshots secure,failsafe
queue/audit secure,failsafe
ac_endpoint_to_server secure,failsafe
ac_server_to_endpoint secure,failsafe
```

보조 엔터프라이즈 관리 서버 구성

보조 엔터프라이즈 관리 서버는 기본 서버에 장애가 발생할 경우 끝점 요청을 처리합니다.

다음 단계를 수행하십시오.

1. 필요하면 기본 엔터프라이즈 관리 서버에서 임시 디렉터리로 FIPS 키를 복사합니다. 이 파일은 다음 디렉터리에 있습니다.

   JBOSS_HOME/server/default/deploy/IdentityMinder.ear/config/com/netegrity/config/keys

   JBOSS_HOME

   JBoss 가 설치된 디렉터리의 이름을 정의합니다.

2. "명령 프롬프트" 창에서 보조 서버에 엔터프라이즈 관리 서버를 설치하고 -DFIPS_KEY=<*full_pathname_to_key*> 옵션을 지정합니다.

   중요! 보조 엔터프라이즈 관리 서버 설치 프로그램을 실행할 때 **--DFIPS_KEY** 옵션을 지정하십시오. 설치 프로세스를 시작하기 전에 기본 엔터프라이즈 서버에서 보조 엔터프라이즈 관리 서버로 FIPS 키를 복사하십시오.

   여기까지 모든 웹 기반 응용 프로그램, 배포 서버, DMS, CA Access Control 이 설치되었습니다.

3. 모든 CA Access Control 서비스를 중지합니다.
4. 서비스를 수정하여 자동이 아닌 수동으로 시작되도록 합니다.
5. *_pmd directory_* 레지스트리 키 구성 설정을 DMS 및 DH 를 복사한 공유 저장소 디렉터리의 전체 경로 이름으로 설정합니다. 예: Z:\PMD.

   보조 서버는 공유 저장소에 DMS 및 DH 를 사용하도록 구성됩니다.

6. 공유 저장소를 사용하도록 메시지 큐를 구성합니다. 다음 작업을 수행하십시오.

   a. 편집을 위해 tibemsd.conf 파일을 엽니다. 이 파일은 기본적으로 다음 디렉터리에 있습니다.

      ACServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data

      ACServerInstallDir

      엔터프라이즈 관리 서버가 설치된 디렉터리의 이름을 정의합니다.

   b. "*store*" 토큰의 값을 데이터 저장소 파일을 복사한 공유 저장소의 디렉터리에 대한 지점으로 설정합니다. 예: Z:\PMD

   c. 파일을 저장한 후 닫습니다.

   d. 편집을 위해 queues.conf 파일을 엽니다.

   e. 쉼표를 추가하고 모든 쿼리 정의 줄의 끝에 "**failsafe**"란 단어를 추가한 다음 파일을 저장하고 닫습니다.

7. CA Access Control 서비스가 실행 중이지 않은지 확인합니다.

8. 다음과 같이 DMS 를 구성하여 보조 엔터프라이즈 관리 서버를 인증하도록 합니다.

   a. 기본 엔터프라이즈 관리 서버에서 JCS, JBoss Application Server, CA Access Control, 메시지 큐 서비스를 시작합니다.

   b. selang 명령 프롬프트 창을 열고 다음 명령을 입력합니다.

      host DMS__@

      로컬 호스트에 연결되었음을 알리는 메시지가 표시됩니다.

   c. 인증된 터미널을 표시하려면 다음 명령을 입력합니다.

      sr TERMINAL *

      CA Access Control 은 인증된 터미널의 세부 정보를 표시합니다.

   d. 인증된 터미널 목록에 보조 엔터프라이즈 관리 서버를 추가하려면 다음 명령을 입력합니다.

      newres TERMINAL <*secondary_enterprise_management_server_full_DN*> audit (f)
      owner(nobody)defacc(r)
      authorize TERMINAL <*ssecondary_enterprise_management_server_full_DN*>
      uid(+reportagent) access(write)
      authorize TERMINAL <*ssecondary_enterprise_management_server_full_DN*>
      uid(DOMAIN\Administrator) access(write,read)
      authorize TERMINAL <*secondary_enterprise_management_server_full_DN*>
      uid(an_entm_pers) access(write,read)

9. 다음과 같이 기본 엔터프라이즈 관리 서버에 오류가 발생할 경우 모든 CA Access Control 서비스를 시작하는 배치 파일을 만듭니다.

```
seosd -start
net start acrptmq
net start "CA Access Control Web Service"
net start im_jcs
net start JBAS50SVC
```

10. 다음과 같이 기본 엔터프라이즈 관리 서버가 작업을 다시 시작할 때 모든 CA Access Control 서비스를 중지하는 배치 파일을 만듭니다.

```
secons -s
net stop acrptmq
net stop "CA Access Control Web Service"
net stop im_jcs
net stop JBAS50SVC
```

11. 오류 발생 시 스크립트를 실행하는 Microsoft 클러스터 소프트웨어를 구성합니다.

    보조 엔터프라이즈 관리 서버가 구성되었습니다.

장애 조치를 위한 Active Directory 구성

사용자 저장소로 Active Directory 를 사용하는 경우 여러 도메인 컨트롤러와 동작하도록 엔터프라이즈 관리 서버를 구성할 수 있습니다. 기본 도메인 컨트롤러에 장애가 발생하면 다른 도메인 컨트롤러가 클라이언트 요청을 승계하여 계속 처리합니다.

다음 단계를 수행하십시오.

1. CA Identity Manager 관리 콘솔을 활성화합니다 (페이지 88).

   환경에서 도메인 컨트롤러의 목록을 구성하려면 CA Identity Manager 관리 콘솔을 사용합니다.

2. CA Identity Manager 관리 콘솔을 엽니다 (페이지 88).
3. "디렉터리"를 클릭한 다음 ac-dir 환경을 클릭합니다.

   "디렉터리 속성" 창이 나타납니다.

4. "내보내기"를 클릭하고 XML 파일을 저장합니다.
5. 편집을 위해 XML 파일을 엽니다. <Connection host= *host_name*> 태그를 찾습니다. 예:

   ```
   <Connection host="primaryDir.com" port="389">
   ```

6. 줄의 끝에 문자열 "**failover**"를 붙이고 공백으로 구분된 목록에 도메인 컨트롤러의 호스트 이름과 포트 번호를 지정한 다음 파일을 저장합니다. 예:

   ```
   <Connection host="ADserver1" port="389" failover="ADserver2:389"/>
   ```

7. 관리 콘솔에서 "업데이트"를 클릭합니다.

   "디렉터리 업데이트" 창이 열립니다.

8. 편집한 XML 파일의 전체 경로 이름을 입력거나 파일을 탐색하여 찾은 다음 "마침"을 클릭합니다.

   상태 정보는 "디렉터리 구성 출력"에 표시됩니다.

9. "계속"을 클릭하고 환경을 다시 시작합니다.

   이제 엔터프라이즈 관리 서버가 기본 및 보조 도메인 컨트롤러와 동작할 수 있습니다.

로컬 DMS 를 사용하여 CA Access Control 엔터프라이즈 관리 구성

정규화된 도메인 이름 대신 "localhost"를 사용하여 DMS 에 연결하도록 엔터프라이즈 관리 서버에서 DMS 를 구성합니다.

로컬 DMS 를 사용하여 CA Access Control 엔터프라이즈 관리를 구성하려면

1. CA Access Control 엔터프라이즈 관리에 로그인한 다음 "시스템", "DMS", "연결 수정"을 선택합니다.

   "연결 수정:연결 검색" 창이 나타납니다.

2. 기본 DMS 연결을 검색하고 "선택"을 클릭합니다.

   "연결 수정:*ConnectionName*" 창이 열립니다.

3. 호스트 이름을 다음과 같이 LocalHost 로 수정합니다.

   DMS__@localhost

4. "제출"을 클릭합니다.

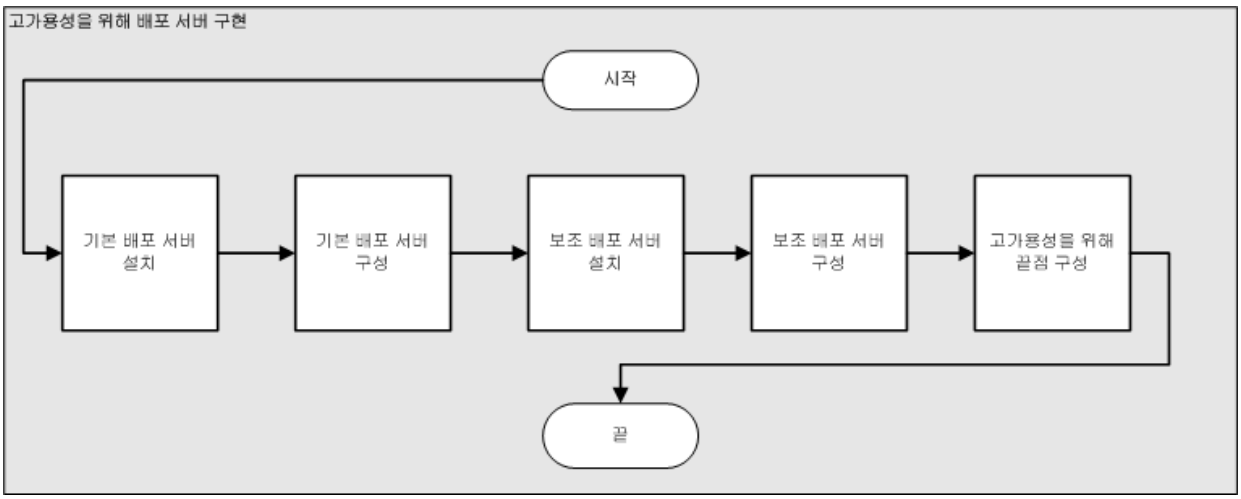
   기본 및 보조 배포 호스트가 이제 DMS 컴퓨터를 공유할 수 있습니다.

고가용성을 위해 배포 서버를 구성하는 방법

고가용성 환경에서 여러 배포 서버를 올바로 구성하려면 올바른 순서로 기본 및 보조 배포 서버를 설정하십시오.

다음 다이어그램은 하나의 엔터프라이즈 관리 서버에 대해 동작하도록 여러 배포 서버를 설정하기 위해 수행하는 단계를 보여줍니다.

중요! CA Access Control 엔터프라이즈 관리와 CA Enterprise Log Manager 를 통합하는 경우에만 다음 단계를 수행하십시오. 장애가 발생한 배포 서버에 수집되어 엔터프라이즈 관리 서버와 CA Enterprise Log Manager 로 전달되지 않은 모든 이벤트의 손실을 방지하려면 고가용성을 위해 배포 서버를 구성하십시오.



추가 정보:

배포 서버 설치 (페이지 381)

기본 배포 서버 구성

배포 서버는 응용 프로그램 서버와 끝점 사이의 통신을 처리합니다.

독립 실행형 배포 서버만 설치하려면 이 절차를 완료해야 합니다.

다음 단계를 수행하십시오.

1. "서비스" 창에서 JCS, CA Access Control, 메시지 큐 서버 서비스를 중지합니다.
2. 서비스를 수정하여 자동이 아닌 수동으로 시작되도록 합니다.
3. 공유 저장소에 PMD 디렉터리를 만듭니다.
4. 다음과 같이 공유 저장소를 사용하도록 배포 호스트를 구성합니다.
   a. 공유 저장소로 DH 디렉터리를 복사합니다. 이 디렉터리는 다음 위치에 있습니다.

      DistServerInstallDir/APMS/AccessControl/Data/DH__

      DistServerInstallDir

      배포 서버를 설치한 디렉터리의 이름을 정의합니다.

   b. 공유 저장소로 DH__WRITER 디렉터리를 복사합니다. 이 디렉터리는 다음 위치에 있습니다.

      DistServerInstallDir/APMS/AccessControl/Data/DH__WRITER

   c. 공유 저장소로 DMS__ 디렉터리를 복사합니다. 이 디렉터리는 다음 위치에 있습니다.

      DistServerInstallDir/APMS/AccessControl/Data/DMS__

   d. *\ComputerAssociates\AccessControl\PMD* 에서 *_pmd_directory_* 레지스트리 키 구성 설정을 DMS 및 DH 를 복사한 공유 저장소 디렉터리의 전체 경로 이름으로 설정합니다. 예: Z:\PMD.

   기본 서버는 공유 저장소에 DMS 및 DH 를 사용하도록 구성됩니다.

5. 다음과 같이 공유 저장소를 사용하도록 메시지 큐를 구성합니다.
   a. 공유 저장소에 디렉터리를 만듭니다. 예: Z\MessageQueue
   b. 메시지 큐 데이터 저장소 파일을 공유 저장소로 복사합니다. 이러한 파일은 다음 디렉터리에 있습니다.

      DistServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data

   c. 편집을 위해 tibemsd.conf 파일을 엽니다. 이 파일은 다음 디렉터리에 있습니다.

      DistServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data

   d. "*store*" 토큰의 값을 데이터 저장소 파일을 복사한 공유 저장소의 디렉터리에 대한 지점으로 설정합니다. 예: F:\MessageQueue.
   e. 파일을 저장한 후 닫습니다.
   f. 편집을 위해 queues.conf 파일을 엽니다.
   g. 쉼표를 추가하고 모든 쿼리 정의 줄의 끝에 "**failsafe**"란 단어를 추가한 다음 파일을 저장합니다.
6. CA Access Control 서비스를 시작합니다.

예: queues.conf 파일 편집

queues.conf 파일의 다음 조각은 공유 저장소를 사용하도록 메시지 큐를 구성하기 위해 파일을 수정하는 방법을 보여줍니다.

```
queue/snapshots secure,failsafe
queue/audit secure,failsafe
ac_endpoint_to_server secure,failsafe
ac_server_to_endpoint secure,failsafe
```

보조 배포 서버 구성

보조 배포 서버는 능동 배포 서버가 미리 정의된 시간 간격 내에 응답하지 않으면 응용 프로그램 서버와 끝점 사이의 통신을 처리합니다.

다음 단계를 수행하십시오.

1. JCS, CA Access Control, 메시지 큐 서버 서비스를 중지합니다.
2. 서비스를 수정하여 자동이 아닌 수동으로 시작되도록 합니다.
3. *\ComputerAssociates\AccessControl\PMD* 에서 *_pmd_directory_* 레지스트리 키 구성 설정을 DMS 및 DH 를 복사한 공유 저장소 디렉터리의 전체 경로 이름으로 설정합니다. 예: Z:\PMD.

   보조 배포 서버는 이제 공유 저장소의 DMS 및 DH 파일에 액세스할 수 있습니다. 공유 저장소를 사용하도록 배포 호스트를 구성했습니다.
4. 다음과 같이 공유 저장소를 사용하도록 메시지 큐를 구성합니다.
   a. 편집을 위해 tibemsd.conf 파일을 엽니다. 이 파일은 다음 디렉터리에 있습니다.

      DistServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data

      DistServerInstallDir

      배포 서버를 설치한 디렉터리의 이름을 정의합니다.

   b. "*store*" 토큰의 값을 데이터 저장소 파일을 복사한 공유 저장소의 디렉터리에 대한 지점으로 설정합니다. 예: Z:\Datastore
   c. 파일을 저장한 후 닫습니다.
   d. 편집을 위해 queues.conf 파일을 엽니다.
   e. 쉼표를 추가하고 모든 쿼리 정의 줄의 끝에 "**failsafe**"란 단어를 추가한 다음 파일을 저장합니다.
5. 보조 서버에서 CA Access Control 서비스가 중지되었는지 확인합니다.

고가용성을 위한 끝점 구성

기본 및 보조 엔터프라이즈 관리 서버를 설치 및 구성한 이후에 고가용성 환경에서 동작하도록 CA Access Control 끝점을 설정합니다.

고가용성을 위한 끝점을 구성하려면

1. 고급 정책 관리 클라이언트 구성 요소가 활성화된 상태에서 끝점 호스트에 CA Access Control 끝점 기능을 설치합니다.

   CA Access Control 끝점이 설치됩니다.

2. 끝점에서 명령 프롬프트 창을 열고 다음 명령을 입력합니다.

   dmsmgr –config -dhname *names*

   이 명령은 끝점이 쉼표로 구분된 배포 호스트 목록을 사용하여 동작하도록 구성합니다.

   참고: dmsmgr 유틸리티에 대한 자세한 내용은 *참조 안내서*를 참조하십시오.

3. *Distribution_Server* 구성 설정이 배포 서버의 목록을 쉼표로 구분하여 나열하도록 설정합니다.

   ssl://ds1.sample.com:7243, ssl://ds2.sample.com:7243

4. 설정을 저장합니다.

   끝점이 통신하는 배포 호스트와 배포 서버의 목록을 구성했습니다. 이제 끝점이 고가용성 환경에서 동작할 수 있습니다.

예: 배포 서버의 목록 구성

다음 예는 고가용성을 위해 배포 서버의 목록을 구성하는 방법을 보여줍니다.

끝점의 설치 중 끝점이 통신하는 배포 서버의 매개 변수를 입력하도록 요청을 받습니다. 기본적으로 여기에는 엔터프라이즈 관리 서버가 사용됩니다. 고가용성을 위해 기본 배포 서버에 장애가 발생할 경우 보조 배포 서버를 사용하도록 끝점을 구성합니다.

1. 기본 및 보조 배포 서버의 이름을 입력합니다.

   dmsmgr -config -dhname DH__@node1.computer.com,DH__@node2.computer.com

   작업을 확인하는 메시지가 표시됩니다.

2. 기본 및 보조 배포 서버 URL 의 목록을 지정합니다.

   - UNIX: accommon.ini 파일의 [communication] 섹션에서 Distribution_Server 매개 변수를 수정합니다.
   - Windows: Distribution_Sever 값 Windows 레지스트리를 수정합니다. 이 매개 변수는 다음 위치에 있습니다.

     HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\common\communication

추가 정보:

Windows 끝점 설치 및 사용자 지정 (페이지 143)
UNIX 끝점 설치 및 사용자 지정 (페이지 179)

고가용성을 위한 Oracle RAC 구성

정책 및 보고 데이터베이스로 Oracle 을 사용하는 경우, Oracle RAC 를 사용하여 고가용성을 위해 Oracle 을 구성할 수 있습니다. Oracle RAC(Real Applications Cluster)는 Oracle 데이터베이스에 대한 고가용성을 제공하는 공유 디스크 아키텍처에 기반한 클러스터 데이터베이스입니다.

예: Oracle RAC 를 사용하여 고가용성을 위해 CA Access Control 엔터프라이즈 관리 구성

다음 예는 고가용성을 위해 Oracle RAC 를 사용하도록 CA Access Control 엔터프라이즈 관리를 구성하는 방법을 설명합니다.

1. 엔터프라이즈 관리를 위해 Oracle 데이터베이스를 준비합니다.

   Oracle RAC 서버에 사용자 계정을 만들고 사용자에게 CA Access Control 엔터프라이즈 관리를 설치하기 위한 권한을 할당합니다.

2. 고가용성을 위해 CA Access Control 엔터프라이즈 관리를 구현합니다.

   기본 및 보조 엔터프라이즈 관리 서버를 설치 및 구성합니다.

   참고: "호스트 이름"에 Oracle RAC 의 논리적 이름을 지정하고 "서비스 이름" 필드에 공유 서비스 이름을 지정합니다.

3. Oracle RAC 호스트 컴퓨터 이름이 올바로 확인되는지 검사합니다.

   Oracle RAC 의 논리적 이름에 대한 호스트 IP 주소를 매핑합니다. 예:

   11.11.111.11 Node1MachineName
   11.11.111.12 Node2MachineName
   11.11.111.11 Node1LogicalMachineName
   11.11.111.12 Node2LogicalMachineName

4. Oracle RAC 를 사용하도록 기본 및 보조 엔터프라이즈 관리 서버 설정을 수정합니다. 다음 작업을 수행하십시오.

   a. JBoss Application Server 를 중지합니다.

   b. 다음 경로로 이동합니다. 여기서 JBoss_HOME 은 JBoss 를 설치한 디렉터리를 나타냅니다.

      JBoss_HOME/server/default/deploy

5. 편집을 위해 다음 파일을 엽니다:

   imauditdb-ds.xml
   imtaskpersistencedb-ds.xml
   imworkflowdb-ds.xml
   objectstore-ds.xml
   reportsnapshot-ds.xml

6. 각 파일에서 <connection-url> 태그를 찾아 다음과 같이 호스트 이름과 서비스 이름을 지정합니다.

   <connection-url>jdbc:oracle:thin:@(DESCRIPTION=(LOAD_BALANCE=off)(FAILOVER=on)(ADDRESS_LIST=(ADDRESS=(protocol=tcp)(host=Node1LogicalMachineName)(port=1521))(ADDRESS=(protocol=tcp)(host=Node2LogicalMachineName)()(port=1521)))(CONNECT_DATA=(SERVER=DEDICATED)(SERVICE_NAME=SharedService)))</connection-url>

7. 각 파일에서 다음 줄을 추가합니다.

```
<check-valid-connection-sql>select 1 from dual</check-valid-connection-sql>
```

8. 파일을 저장한 후 닫습니다.
9. JBoss Application Server 를 시작합니다.

   기본 및 보조 엔터프라이즈 관리 서버를 구성했습니다.

제 12 장: 재해 복구 배포 설치

이 섹션은 다음 항목을 포함하고 있습니다.

재해 복구 개요

하위 시스템 작동 중단 또는 그 밖의 치명적 오류가 발생한 후 재해 복구를 통해 시스템을 복원할 수 있습니다.

재해 복구의 목적은 최대한 많은 데이터를 복원하고 백업 및 복원 단계에서 필요한 리소스를 제한하는 것입니다.

추가 정보:

재해 복구

재해 복구 배포는 치명적 서버 장애 시 엔터프라이즈 관리 서버를 보다 쉽게 복원할 수 있게 해 줍니다. CA Access Control 및 PUPM 끝점이 프로덕션 환경에 연결될 수 없는 경우 프로덕션 환경이 복원될 때까지 재해 복구 환경에 연결됩니다.

재해 복구 배포는 다음과 같은 이점을 제공합니다.

- 재해 복구 DMS 의 데이터베이스는 프로덕션 DMS 데이터베이스의 복제본입니다. 따라서 프로덕션 DMS 데이터베이스가 손상되더라도 해당 정책의 복사본이 마련되어 있습니다.
- 끝점은 프로덕션 또는 재해 복구 환경에 연결할 수 있습니다. 프로덕션 환경이 중단될 경우, 끝점은 재해 복구 환경으로 데이터를 보내므로 치명적인 시스템 오류가 발생하더라도 정책 상태 및 위반에 대한 정보를 잃지 않습니다.
- 재해에서 복구한 이후에 각 끝점을 다시 구독할 필요는 없습니다.

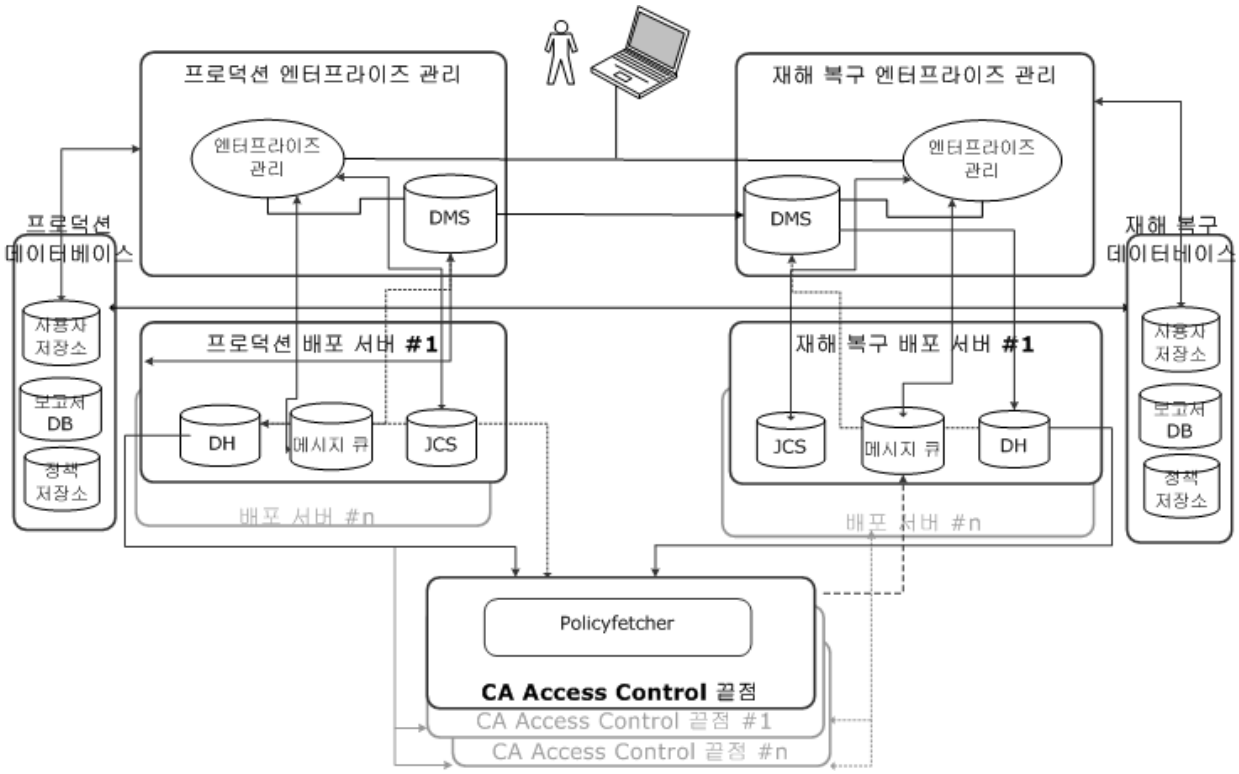
다음 CA Access Control 구성 요소는 재해 복구 프로세스 중에 백업되거나 복원되지 않습니다. 이러한 구성 요소는 별도로 백업하십시오.

- 암호 정책 모델
- PMDB:
- RDBMS
- CA Access Control 끝점 관리
- CA Access Control 엔터프라이즈 관리
- 끝점의 데이터
- CA Access Control 감사 파일
- CA Access Control 끝점
- 보고서
- 메시지 큐
- CA Business Intelligence

참고: DMS 감사 파일은 DMS 백업될 때 저장됩니다.

재해 복구 아키텍처

다음 다이어그램에서는 재해 복구 구성에 CA Access Control 을 배포하는 방법을 설명합니다.



재해 복구 구성 요소

재해 복구 구성에서 CA Access Control 을 배포하려면 다음 구성 요소가 필요합니다.

- 프로덕션 환경:
  - 설치된 하나의 엔터프라이즈 관리 서버
  - 중앙 데이터베이스(RDBMS)
  - 하나 이상의 설치된 배포 서버
- 재해 복구 환경:
  - 설치된 하나의 엔터프라이즈 관리 서버
  - 중앙 데이터베이스(RDBMS)
  - 하나 이상의 설치된 배포 서버

재해 복구 배포를 계획할 때 다음 사항을 고려하십시오.

- 동일한 플랫폼, 운영 체제 및 CA Access Control 버전에 저장된 백업 파일에서만 DMS 를 복원할 수 있습니다. 예를 들어, CA Access Control r12.0 SP1 에서 만든 DMS 백업 파일을 사용하여 CA Access Control r12.5 에서 이 DMS 를 복원할 수 없습니다.
- RDBMS 에 클러스터링 또는 기타 장애 조치 솔루션을 구성할 수 있습니다.
- 프로덕션과 재해 복구 서버 사이에서 RDBMS 에 있는 데이터를 동기화해야 합니다.
- 프로덕션과 재해 복구 서버 사이에서 메시지 큐 데이터 저장소를 동기화해야 합니다.

끝점에서 재해 복구 배포가 작동하는 방법

재해 복구 배포는 프로덕션 배포 서버 데이터베이스의 복제본을 만들고, 끝점에서 보낸 데이터가 시스템 오류로 인해 손실되지 않게 하고, 재해가 발생하는 경우 프로덕션 환경을 보다 쉽게 복원하게 해줍니다.

다음 프로세스는 끝점에서 재해 복구 배포가 어떻게 작동하는지 설명합니다.

1. 프로덕션 및 재해 복구 배포 서버의 목록을 사용하여 작동하도록 끝점을 구성합니다.

2. 지정된 시간에 끝점은 프로덕션 환경에 있는 배포 서버에 연결을 시도합니다.

   a. 끝점이 목록에 있는 첫 번째 프로덕션 배포 서버에 연결하려고 시도합니다. 연결하지 못하는 경우 지정된 횟수만큼 해당 배포 서버에 연결하려고 시도합니다. 다음 중 *한 가지* 결과가 나타납니다.

      - 끝점이 프로덕션 배포 서버에 연결됩니다. 이 단계에서 프로세스가 끝납니다.
      - 끝점이 프로덕션 배포 서버에 연결할 수 없습니다. 프로세스가 b 단계로 이동합니다.

      참고: 끝점이 배포 서버에 연결을 시도할 횟수는 configuration 섹션의 Distribution_Server 설정 및 policyfetcher 섹션의 max_dh_command_retry 구성 설정에 정의되어 있습니다.

   b. 끝점이 목록에서 두 번째, 세 번째 및 나머지 프로덕션 배포 서버에 차례로 (필요한 경우 동일하게 정의된 횟수만큼) 연결을 시도합니다. 다음 중 *한 가지* 결과가 나타납니다.

      - 끝점이 프로덕션 배포 서버에 연결됩니다. 이 단계에서 프로세스가 끝납니다.
      - 끝점이 어떠한 프로덕션 배포 서버에도 연결하지 못하고 주기가 끝납니다. 프로세스가 3 단계로 이동합니다.

3. 끝점은 지정된 주기 횟수만큼 2 단계를 반복합니다. 다음 중 *한 가지* 결과가 나타납니다.

   - 끝점이 프로덕션 배포 서버에 연결됩니다. 이 단계에서 프로세스가 끝납니다.
   - 끝점이 프로덕션 배포 서버에 연결할 수 없습니다. 프로세스가 다음 단계로 진행됩니다.

     참고: 끝점이 배포 서버에 연결을 시도할 횟수는 configuration 섹션의 Distribution_Server 설정 및 policyfetcher 섹션의 max_dh_command_retry 구성 설정에 정의되어 있습니다.

4. 끝점이 목록에 있는 첫 번째 재해 복구 배포 서버에 연결하려고 시도합니다. 끝점이 이 배포 서버에 연결할 수 없는 경우, 끝점이 재배 복구 배포 서버에 연결할 때까지 목록에 있는 두 번째, 세 번째 및 나머지 재해 복구 배포 서버에 차례로 연결을 시도합니다.

   참고: 끝점이 프로덕션 또는 재해 복구 배포 서버에 연결할 수 없는 경우 DMS 에 하트비트를 보내지 않습니다. 끝점이 온라인인지 오프라인인지 확인하려면 마지막 하트비트 알림이 DMS 에 보내진 시간을 점검합니다.

5. 끝점이 재해 복구 배포 서버에 연결한 다음에는 프로덕션 배포 서버에 연결하기 위해 계속 시도합니다. 다음 중 *한 가지* 결과가 나타납니다.
   - 끝점이 프로덕션 배포 서버에 연결되고 프로덕션 환경으로 복귀합니다.
   - 끝점이 프로덕션 배포 서버에 연결할 수 없습니다. 끝점은 재해 복구 환경에 머무르면서 4 단계를 반복합니다.

   참고: policyfetcher 및 communication 섹션에 대한 자세한 내용은 *참조 안내서*를 참조하십시오.

재해 복구 배포 설치 방법

재해 복구 구성 요소가 서로를 올바르게 구독하게 하려면 다음 프로세스에서 지정한 순서대로 프로덕션 및 재해 복구 구성 요소를 설정해야 합니다.

재해 복구 구성은 치명적 서버 장애 시 엔터프라이즈 관리 서버 구성 요소를 보다 쉽게 복원할 수 있게 해 줍니다. 중앙 데이터베이스(RDBMS)와 같은 기타 CA Access Control 구성 요소를 별도로 백업해야 할 수 있습니다.

중요!: 다른 운영 환경 또는 CA Access Control 버전을 사용하는 백업 파일에서 DMS 를 복원할 수 없습니다. 프로덕션 및 재해 복구 환경이 동일한 플랫폼, 운영 체제 및 CA Access Control 버전에 배포되었는지 확인하십시오.

참고: 이 프로세스는 서로 다른 호스트에 DMS 와 DH 를 설치했다고 가정합니다.

다음 프로세스는 재해 복구 배포를 설치하는 방법을 보여 줍니다.

1. 프로덕션 엔터프라이즈 관리 서버 설정 (페이지 375)
2. 재해 복구 엔터프라이즈 관리 서버 설정 (페이지 377)
3. 프로덕션 및 재해 복구 서버 사이에서 데이터베이스 복제 구성
4. DMS 구독 구성 (페이지 379)
5. 메시지 큐 서버 데이터 파일 동기화 (페이지 396)
6. 끝점을 설정합니다 (페이지 380).

참고: 클러스터 또는 사이트 간 데이터 동기화를 허용하는 다른 방법을 사용하여 RDBMS 를 설치하는 것이 좋습니다.

프로덕션 CA Access Control 엔터프라이즈 관리 설정

프로덕션 엔터프라이즈 관리 서버에는 DMS 가 포함되어 있습니다. DMS 는 각 끝점의 정책 버전, 정책 스크립트, 정책 배포 상태에 대한 최신 정보를 저장합니다. 프로덕션 DMS 를 사용하여 엔터프라이즈 정책을 배포하고 관리합니다.

프로덕션 DH 와 재해 복구 DMS 가 프로덕션 DMS 를 구독하므로, 다른 재해 복구 구성 요소를 설정하기 전에 먼저 프로덕션 DMS 를 설정하십시오. 이렇게 하면 설치 프로세스의 이후 단계에서 구독이 올바르게 구성됩니다.

프로덕션 엔터프라이즈 관리 서버를 설정하려면

1. 엔터프라이즈 관리 서버를 구현합니다.

   모든 웹 기반 응용 프로그램, 배포 서버, DMS, CA Access Control 이 설치되었습니다.

2. (선택 사항) 배포 서버를 구현합니다 (페이지 381).

   메시지 큐 및 Java Connector Server 가 설치되었습니다.

3. (선택 사항) 엔터프라이즈 관리 서버에서 로컬 DH 를 제거하고, 관리 및 배포 서버 사이의 구분을 위해 배포 서버에서 DH 를 사용하려면 프로덕션 엔터프라이즈 관리 서버에서 다음 명령을 실행합니다.

   dmsmgr -remove -*dh name*

   -dh *name*

   로컬 호스트에 지정된 *name* 의 DH 를 제거합니다.

   예: *dmsmgr -remove -dh DH*

   위의 예제는 호스트에서 DH 란 이름의 DH 를 제거합니다.

   프로덕션 DMS 가 구독자 없이 작성됩니다.

4. 메시지 큐가 failsafe 모드로 작동하도록 구성합니다. 다음 작업을 수행하십시오.

   a. 다음 디렉터리로 이동합니다. 여기서 *ACServerInstallDir* 는 엔터프라이즈 관리 서버를 설치한 디렉터리를 나타냅니다.

      ACServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data

   b. 편집을 위해 queues.conf 파일을 엽니다.

   c. 모든 쿼리 정의 줄의 끝에 "**failsafe**"란 단어를 추가한 다음 파일을 저장하고 닫습니다.

5. 로컬 DMS 를 사용하여 CA Access Control 엔터프라이즈 관리를 구성합니다 (페이지 359).

   프로덕션 엔터프라이즈 관리 서버를 설치 및 구성했습니다. 이제 재해 복구 엔터프라이즈 관리 서버를 구성할 수 있습니다.

예: queues.conf 파일 편집

queues.conf 파일의 다음 조각은 공유 저장소를 사용하도록 메시지 큐를 구성하기 위해 파일을 수정하는 방법의 예제입니다.

```
queue/snapshots secure,failsafe
queue/audit secure,failsafe
ac_endpoint_to_server secure,failsafe
ac_server_to_endpoint secure,failsafe
```

재해 복구 CA Access Control 엔터프라이즈 관리 설정

심각한 시스템 장애가 발생하면 재해 복구 엔터프라이즈 관리 서버가 엔터프라이즈 정책을 배포 및 관리합니다. 재해 복구 엔터프라이즈 관리 서버는 프로덕션 엔터프라이즈 관리 서버의 구독자이므로, 해당 데이터베이스는 프로덕션 엔터프라이즈 관리 서버와 동일한 정책 버전, 정책 스크립트, 끝점 배포 상태 정보를 포함합니다.

참고: 재해 복구 엔터프라이즈 관리 서버를 설정하기 전에 프로덕션 엔터프라이즈 관리 서버를 구성하십시오.

재해 복구 엔터프라이즈 관리 서버를 설정하려면

1. 프로덕션 엔터프라이즈 관리 서버에서 FIPSKey.dat 파일을 재해 복구 서버로 복사합니다. 이 파일은 다음 디렉터리에 있습니다. 여기서 *JBoss_HOME* 은 JBoss 를 설치한 디렉터리를 나타냅니다.

   JBoss_HOME/server/default/deploy/IdentityMinder.ear/config/com/netegrity/config/keys

2. 재해 복구 서버에서 엔터프라이즈 관리 서버를 구현합니다.

   모든 웹 기반 응용 프로그램, 배포 서버, DMS, CA Access Control 이 설치되었습니다.

   중요! 설치 프로세스를 시작할 때 프로덕션 엔터프라이즈 관리 서버에서 복사한 FIPSKey.dat 파일을 지정합니다. 예:

   E:\EnterpriseMgmt\Disk1\InstData\NoVM\install_EntM_r125.exe -DFIPS_KEY=C:\tmp\FIPSkey.dat

3. (선택 사항) 재해 복구 배포 서버를 구현합니다 (페이지 384).

   메시지 큐 및 Java Connector Server 가 설치되었습니다.

4. (선택 사항) 로컬 DH 를 제거하고, 관리 및 배포 서버 사이의 구분을 위해 배포 서버에서 DH 를 사용하려면 재해 복구 엔터프라이즈 관리 서버에서 다음 명령을 실행합니다.

   dmsmgr -remove -dh *name*

   -dh *name*

   로컬 호스트에 지정된 *name* 의 DH 를 제거합니다.

   예: *dmsmgr -remove -dh DH*

   재해 복구 DMS 가 구독자 없이 작성됩니다.

5. 메시지 큐가 failsafe 모드로 작동하도록 구성합니다. 다음 작업을 수행하십시오.

   a. 다음 디렉터리로 이동합니다. 여기서 *ACServerInstallDir* 는 엔터프라이즈 관리 서버를 설치한 디렉터리를 나타냅니다.

      ACServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data

   b. 편집을 위해 queues.conf 파일을 엽니다.

   c. 모든 쿼리 정의 줄의 끝에 "**failsafe**"란 단어를 추가한 다음 파일을 저장하고 닫습니다.

6. 로컬 DMS 를 사용하여 CA Access Control 엔터프라이즈 관리를 구성합니다 (페이지 359).

재해 복구 엔터프라이즈 관리 서버를 설치 및 구성했습니다.

예: queues.conf 파일 편집

queues.conf 파일의 다음 조각은 공유 저장소를 사용하도록 메시지 큐를 구성하기 위해 파일을 수정하는 방법의 예제입니다.

```
queue/snapshots secure,failsafe
queue/audit secure,failsafe
ac_endpoint_to_server secure,failsafe
ac_server_to_endpoint secure,failsafe
```

DMS 구독 구성

재해 복구 엔터프라이즈 관리 서버는 프로덕션 엔터프라이즈 관리 서버의 구독자입니다. 따라서 그 데이터베이스는 정책 버전, 정책 스크립트, 끝점 배포 상태에 대해 엔터프라이즈 관리 서버와 동일한 정보를 수록하고 있습니다.

재해 복구 엔터프라이즈 관리 서버의 데이터베이스를 프로덕션 엔터프라이즈 관리 서버의 구독자로 구성하여 두 데이터베이스를 동기화합니다.

DMS 구독을 구성하려면

1. 재해 복구 엔터프라이즈 관리 서버로 이동하려면
2. 프로덕션 엔터프라이즈 관리 서버를 재해 복구 엔터프라이즈 관리 서버의 부모로 정의합니다. 다음 명령을 실행합니다.

   env pmd

   subs drpmd_name *parentpmd*(<pr_dms_pmdname>@pr_host)

   drpmd_name

   재해 복구 PMDB 의 이름을 정의합니다.
3. 프로덕션 엔터프라이즈 관리 서버로 이동합니다.
4. 다음 명령을 실행합니다.

   sepmd -n *prDMS_name drDMS_name*

   prDMS_name

   프로덕션 DMS 의 이름을 정의합니다.

   drDMS_name

   재해 복구 DMS 의 이름을 정의합니다. 재해 복구 DMS 는 *drDMS_name@hostname* 형식으로 지정하십시오.

재해 복구 엔터프라이즈 관리 서버가 프로덕션 엔터프라이즈 관리 서버에 구독되고 동기화됩니다.

끝점 설정

프로덕션 및 재해 복구 환경에 엔터프라이즈 관리 서버를 설치한 다음에는 프로덕션 및 재해 복구 서버 구성 요소와 동작하도록 회사에 있는 각 끝점을 구성해야 합니다. 이때 서버 구성 요소와 정보를 주고받을 수 있도록 끝점을 구성해야 합니다.

참고: 설치 프로세스 중에 고급 정책 관리 서버 구성 요소 호스트 이름을 제공하십시오. 프로덕션 DH 의 이름은 *prDH_name@hostname*[, *prDH_name@hostname*..] 형식으로 입력합니다.

끝점을 설정하려면

1. 고급 정책 관리 클라이언트 구성 요소가 활성화된 상태에서 끝점 호스트에 CA Access Control 끝점 기능을 설치합니다.

   CA Access Control 끝점 기능이 호스트에 설치되며, 끝점이 프로덕션 DH 에 구독됩니다.

2. 끝점에서 selang 명령 창을 엽니다.

3. 다음 명령을 입력합니다.

   so dh_dr+(*drDH_name*[, *drDH_name*...])

   drDH_name

   재해 복구 DH 의 이름을 *drDH_name@hostname* 형식으로 정의합니다.

   끝점이 재해 복구 DH 에 구독됩니다.

4. 프로덕션 및 재해 복구 배포 서버 URL 의 목록을 지정합니다.

   - UNIX: accommon.ini 파일의 [communication] 섹션에서 Distribution_Server 매개 변수를 수정합니다.
   - Windows: Distribution_Sever 값 Windows 레지스트리를 수정합니다. 이 매개 변수는 다음 위치에 있습니다.

     HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\common\communication

   참고: Distribution_Server 값에 대한 자세한 내용은 *참조 안내서*를 참조하십시오.

   참고: 위 selang 명령으로 정책을 만들어 끝점에 배포하는 방법으로 끝점을 재해 복구 DH 에 구독할 수도 있습니다. 참고: 정책 작성 및 배포에 대한 자세한 내용은 *엔터프라이즈 관리 안내서*를 참조하십시오.

재해 복구 배포를 설치하기 위한 추가 정보

다음은 재해 복구 배포를 설치하기 수행해야 할 수도 있는 추가 구성 단계를 설명합니다.

배포 서버 설치

재해 복구 또는 고가용성 환경에서 동작하도록 CA Access Control 을 구성할 때 서로 다른 컴퓨터에 배포 서버를 설치하고 이 사이에서 배포 서버가 파일을 전파하도록 구성합니다.

배포 서버를 설치하려면

1. 광학 디스크 드라이브에 사용하는 운영 체제용의 적절한 CA Access Control Premium Edition 서버 구성 요소 DVD 를 넣습니다.
2. 다음 중 하나를 수행합니다.
   - Windows 의 경우:

     자동 실행이 활성화된 경우 제품 탐색기가 자동으로 표시됩니다. 다음 작업을 수행하십시오.

     a. 제품 탐색기가 열리지 않으면 광학 디스크 드라이브 디렉터리로 이동한 다음 ProductExplorerx86.EXE 파일을 두 번 클릭합니다.

     b. 제품 탐색기에서 "구성 요소" 폴더를 확장한 다음 CA Access Control 배포 서버를 선택하고 "설치"를 클릭합니다.

     InstallAnywhere 설치 프로그램이 시작됩니다.
   - UNIX 의 경우:

     a. 광 디스크 드라이브를 마운트합니다.

     b. 터미널 창을 열고 광 디스크 드라이브에서 다음 디렉터리로 이동합니다.

     /DistServer/Disk1/InstData/NoVM

     c. 다음 명령을 실행합니다.

     ```
     ./install_DistServer_r125.bin -i console
     ```

     InstallAnywhere 설치 프로그램이 시작됩니다.

3. 필요에 따라 마법사를 완료합니다. 다음 설치 입력 항목은 자동으로 채워지지 않습니다.

   메시지 큐 설정

   메시지 큐 서버 관리자 암호(통신 암호)를 정의합니다.

   제한: 최소 6 자

   Java Connector Server - 프로비저닝 디렉터리 정보

   Java Connector Server 의 암호를 정의합니다.

   참고: Java Connector Server 는 CA Access Control 엔터프라이즈 관리에 권한 있는 계정 관리 기능을 제공합니다.

   CA Access Control 배포 서버 설치가 완료됩니다.

   참고: 배포 서버를 재해 복구 구현의 일부로 설치한 경우 추가 단계를 완료해야 합니다.

추가 정보:

프로덕션 배포 서버 설정 (페이지 382)
재해 복구 배포 서버 설정 (페이지 384)

프로덕션 배포 서버 설정

프로덕션 배포 서버는 DH 를 포함합니다. DH 는 프로덕션 DMS 에서 작성된 정책 배포를 끝점에 분산하고, 끝점으로부터 배포 상태 업데이트를 받아 프로덕션 DMS 로 보냅니다.

프로덕션 DH 와 재해 복구 DMS 가 프로덕션 DMS 를 구독하므로, 다른 재해 복구 구성 요소를 설정하기 전에 먼저 프로덕션 DMS 를 설정하십시오. 이렇게 하면 설치 프로세스의 이후 단계에서 구독이 올바르게 구성됩니다.

프로덕션 배포 서버를 설정하려면

1. 프로덕션 배포 서버 컴퓨터에 배포 서버를 설치 (페이지 381)합니다.
2. 프로덕션 배포 서버에서 다음 명령을 실행하여 DH 를 구성합니다.

   dmsmgr -remove -auto

   dmsmgr -create -dh *name* -parent *name*\
   [-admin *user*[,*user*...]] [-desktop *host*[,*host*...]]

   -dh *name*

   로컬 호스트에 지정된 *name* 으로 DH 를 작성합니다.

   -parent *name*

   DH 에서 끝점 알림을 보낼 프로덕션 DMS 를 정의합니다. 프로덕션 DMS 는 *DMS_name*@hostname 형식으로 지정하십시오.

   -admin *user*[,*user*...]

   (선택 사항) 내부 사용자를 작성된 DH 의 관리자로 정의합니다.

   -desktop *host*[,*host*...]

   (선택 사항) 작성된 DH 가 있는 컴퓨터에 대해 TERMINAL 액세스 권한을 갖는 컴퓨터의 목록을 정의합니다.

   참고: 지정 여부와 상관 없이, 이 유틸리티를 실행하는 터미널에는 항상 작성된 DH 에 대한 관리 권한이 부여됩니다.

   프로덕션 DH 가 작성되고 구성됩니다.

3. 다음 명령을 실행합니다.

   sepmd -n *prDMS_name prDH_name*

   prDMS_name

   프로덕션 DMS 의 이름을 정의합니다.

   prDH_name

   프로덕션 DHs 의 이름을 정의합니다. 이름은 *prDH_name@hostname* 형식으로 지정하십시오.

   예: DH__@prdh.com

   DH 가 프로덕션 DMS 에 구독되고 동기화됩니다.

4. 배포 서버와 프로덕션 DMS 사이에서 라우팅하는 메시지 큐를 설정합니다.
5. 각 프로덕션 배포 서버에 대해 1-4 단계를 반복합니다.

재해 복구 배포 서버 설정

재해 복구 배포 서버는 프로덕션 배포 서버의 구독자이므로, 해당 데이터베이스는 프로덕션 배포 서버와 동일한 정책 버전, 정책 스크립트, 끝점 배포 상태 정보를 포함합니다.

참고: 재해 복구 배포 서버를 설정하기 전에 프로덕션 배포 서버를 설정해야 합니다.

재해 복구 배포 서버를 설정하려면

1. 재해 복구 배포 서버 컴퓨터에 배포 서버를 설치 (페이지 381)합니다.
2. 재해 복구 배포 서버에서 다음 명령을 실행하여 DH 를 구성합니다.

   dmsmgr -remove -auto

   dmsmgr -create -dh *name* -parent *name*\
   [-admin *user*[,*user*...]] [-admin *user*[,*user*...]]

   -dh *name*

   로컬 호스트에 지정된 *name* 으로 DH 를 작성합니다.

   -parent *name*

   DH 에서 끝점 알림을 보낼 재해 복구 DMS 를 정의합니다. 재해 복구 DMS 는 *drDMS_name@hostname* 형식으로 지정하십시오.

   -admin *user* [,*user*...]

   (선택 사항) 내부 사용자를 작성된 DH 의 관리자로 정의합니다.

   -desktop *host*[,*host*...]

   (선택 사항) 작성된 DH 가 있는 컴퓨터에 대해 TERMINAL 액세스 권한을 갖는 컴퓨터의 목록을 정의합니다.

   참고: 지정 여부와 상관 없이, 이 유틸리티를 실행하는 터미널에는 항상 작성된 DH 에 대한 관리 권한이 부여됩니다.

   재해 복구 DH 가 작성되고 구성됩니다.

3. 재해 복구 배포 서버에서 다음 명령을 실행합니다.

   sepmd -n *drDMS_name drDH_name*

   drDMS_name

   재해 복구 DMS 의 이름을 정의합니다.

   drDH_name

   재해 복구 DH 의 이름을 정의합니다. 이름은 *drDH_name@hostname* 형식으로 지정하십시오.

   예: DH__@drdh.com

   DH 가 재해 복구 DMS 에 구독되고 동기화됩니다.

4. 배포 서버와 재해 복구 DMS 사이에서 메시지 큐 라우팅을 설정합니다.
5. 각 재해 복구 배포 서버에 대해 1-4 단계를 반복합니다.

재해 복구 프로세스

재해 복구 프로세스는 백업과 복원의 두 단계로 구성됩니다. 백업 단계에서는 DMS 데이터베이스의 데이터가 다른 디렉터리에 복사됩니다. 복원 단계에서는 dmsgmr 유틸리티가 백업 DMS 파일을 사용하여 기존 DMS 를 복원하거나 새 DMS 를 만듭니다.

참고: 재해 복구 구성은 치명적 시스템 오류가 발생한 경우 고급 정책 관리 구성 요소를 더 쉽게 복원할 수 있게 해줍니다. 다른 CA Access Control 구성 요소를 별도로 백업하는 작업이 필요할 수 있습니다.

추가 정보:

복원 가능한 데이터 (페이지 386)
DMS 를 복원해야 하는 경우 (페이지 386)
DH 를 복원해야 하는 경우 (페이지 387)
DMS 가 복원되는 방법 (페이지 387)
DH 가 복원되는 방법 (페이지 388)

복원 가능한 데이터

DMS 를 복원할 때 dmsmgr 는 다른 DMS 의 백업 파일을 사용하여 새 DMS 를 작성합니다. DH 를 복원할 때 dmsmgr 는 DMS 백업 파일의 데이터를 DH 구독기 디렉터리에 복사합니다. 두 경우 모두 동일한 데이터를 복원합니다.

복원된 데이터는 DMS 데이터베이스에 있는 데이터의 복제본으로서 다음을 포함합니다.

- 엔터프라이즈 정책, 버전 및 할당 정보
- 배포 및 정책 상태, 배포 위반 및 배포 계층 정보
- 호스트 및 호스트 그룹 정의
- 구성 설정
- updates.dat 파일
- 레지스트리 항목
- DMS 감사 파일

참고: DH__Writer 는 임시 데이터베이스가 있으므로 복원할 필요 없습니다.

DMS 를 복원해야 하는 경우

DMS 를 복원할 때 dmsmgr 는 다른 DMS 의 백업 파일을 사용하여 새 DMS 를 작성합니다. 다음 시나리오는 프로덕션 DMS 를 복원해야 하는 경우를 소개합니다.

- 치명적인 프로덕션 시스템 오류가 발생한 경우
- 프로덕션 DMS 데이터베이스가 손상된 경우
- 다른 호스트에 새 프로덕션 DMS 를 설정해야 하는 경우

다음 시나리오는 재해 복구 DMS 를 복원해야 하는 경우를 소개합니다.

- 재해 복구 DMS 가 프로덕션 DMS 와 동기화되지 않은 경우
- 재해 복구 DMS 데이터베이스가 손상된 경우
- 다른 호스트에 새 재해 복구 DMS 를 설정해야 하는 경우

참고: 기존 DMS 위에 또는 DMS 가 없는 새 디렉터리에 DMS 를 복원할 수 있습니다.

DH 를 복원해야 하는 경우

DH 를 복원할 때 dmsmgr 는 DMS 백업 파일의 데이터를 DH 구독기 디렉터리에 복사합니다. 다음 시나리오는 DH 를 복원해야 하는 경우를 소개합니다.

- 치명적인 프로덕션 시스템 오류가 발생한 경우
- DH 데이터베이스가 손상된 경우
- DH 가 DMS 와 동기화되지 않은 경우
- 다른 호스트에 새 DH 를 설정해야 하는 경우

참고: DH 작성기는 임시 데이터베이스가 있으므로 복원할 필요 없습니다. DH 를 복원하기 전에 기존 DH 파일 구조에 DH 작성기가 있는지 확인하십시오.

DMS 가 복원되는 방법

dmsmgr 유틸리티가 DMS 를 복원하는 방법을 이해하면 복원 프로세스 중에 발생할 수 있는 문제를 진단하는 데 도움이 됩니다.

다음 프로세스는 dmsmgr 가 DMS 를 복원하는 방법을 설명합니다.

1. dmsmgr 는 기존 DMS 를 제거합니다.
2. dmsmgr 는 사용자가 지정한 위치의 백업 DMS 파일을 DMS 디렉터리로 복사합니다.
3. dmsmgr 는 DMS 에 대한 모든 구독자를 삭제합니다.
4. 다음 중 *한 가지* 결과가 나타납니다.
   - 프로덕션 DMS 를 복원한 경우 dmsmgr 는 재해 복구 DMS 를 프로덕션 DMS 에 첫 번째 구독자로 추가하며, 이 때 백업 파일에 저장된 마지막 전역 오프셋과 동일한 오프셋 값을 사용합니다.
   - 재해 복구 DMS 를 복원한 경우 dmsmgr 는 재해 복구 DMS 를 프로덕션 DMS 에 다시 구독시키며, 이 때 백업 파일에 저장된 마지막 전역 오프셋과 동일한 오프셋 값을 사용합니다.
5. dmsmgr 는 각 DH 를 DMS 에 구독시킵니다. 각 DH 는 오프셋 값 0 을 가지며 비동기화 상태입니다.

   참고: DH 는 비동기화 상태일 때 DMS 로부터 업데이트를 받을 수 없습니다. DH 를 비동기화 상태로부터 해제하려면 DH 를 복원합니다.

DH 가 복원되는 방법

dmsmgr 유틸리티가 DH 를 복원하는 방법을 이해하면 복원 프로세스 중에 발생할 수 있는 문제를 진단하는 데 도움이 됩니다.

다음 프로세스는 dmsmgr 가 DH 를 복원하는 방법을 설명합니다.

1. dmsmgr 는 기존 DH 를 제거합니다.
2. dmsmgr 는 사용자가 지정한 위치의 백업 DH 파일을 DH 디렉터리로 복사합니다.
3. dmsmgr 는 DH 를 DMS 에 구독시키며, 이 때 백업 파일에 저장된 마지막 전역 오프셋과 동일한 오프셋 값을 사용합니다.
4. dmsmgr 는 DH 에서 비동기화 플래그를 지웁니다.

오프셋 값

updates.dat 파일은 DMS 가 배포하는 각 명령을 저장합니다. 새 구독자를 작성하면 정책 모델은 updates.dat 파일의 명령을 구독자에게 보냅니다. 각 명령은 *오프셋 값*이라고 부르는 수치만큼 증가하면서 인덱싱됩니다.

DMS 에 구독자를 추가할 때 다음과 같이 오프셋을 지정할 수 있습니다.

- **0**—정책 모델은 모든 명령을 구독자에게 보냅니다.
- **마지막 오프셋**—정책 모델은 구독자에게 어떤 명령도 보내지 않습니다.
- **0 와 마지막 오프셋 사이의 정수 X**—정책 모델은 X 와 마지막 오프셋 사이의 모든 명령을 구독자에게 보냅니다.

비동기화 구독자

*비동기화 구독자*는 updates.dat 파일이 마지막으로 잘려진 후 어떤 업데이트도 받지 못한 구독자입니다. 어떤 구독자에 비동기화 플래그를 지정하면 CA Access Control 에서는 그 구독자를 무시하며 어떤 명령도 이 구독자에게 보내지지 않습니다.

비동기화 구독자는 부모 DMS 또는 정책 모델로부터 어떤 업데이트도 받지 않습니다. 비동기화 플래그를 지우고 구독자가 업데이트를 받게 하려면 그 구독자를 부모에게 다시 구독시켜야 합니다.

부모 DMS 또는 정책 모델에 대한 모든 구독자가 비동기화 상태인 경우 그 부모는 사실상 구독자가 없는 것입니다.

재해에서 복구하는 방법

프로덕션 시스템 오류가 발생한 경우 끝점은 재해 복구 환경을 대상으로 작동합니다. 재해에서 복구되면 재해 복구 환경에서 복원된 프로덕션 환경으로 작업을 이동합니다.

다음 프로세스는 재해로부터 복구되는 방법을 보여 줍니다.

1. 프로덕션 엔터프라이즈 관리 서버 및 프로덕션 배포 서버에서 CA Access Control 을 중지합니다.
2. 재해 복구 DMS 에 대한 모든 관리 작업을 중단합니다. 즉 CA Access Control 엔터프라이즈 관리 및 policydeploy 유틸리티를 중단합니다.
3. (선택 사항) updates.dat 파일을 자동으로 자릅니다.
4. 재해 복구 DMS 를 백업합니다. 다음 방법 중 하나로 DMS 를 백업할 수 있습니다.
   - 로컬 백업 (페이지 390)
   - 원격 백업 (페이지 391)
5. 프로덕션 데이터베이스(RDBMS)를 복원합니다.
6. 재해 복구 DMS 백업 파일로부터 프로덕션 DMS 를 복원 (페이지 393)합니다.
7. 프로덕션 DMS 에서 CA Access Control 을 시작합니다.
8. 프로덕션 DMS 를 백업합니다. 다음 방법 중 하나로 DMS 를 백업할 수 있습니다.
   - 로컬 백업 (페이지 390)
   - 원격 백업 (페이지 391)
9. 프로덕션 DMS 백업 파일로부터 각 프로덕션 DH 를 복원 (페이지 392)합니다.
10. 각 프로덕션 배포 서버에서 CA Access Control 을 시작합니다.
11. 모든 관리 작업을 프로덕션 DMS 로 이동합니다. 즉 프로덕션 CA Access Control 엔터프라이즈 관리에서 CA Access Control 엔터프라이즈 관리 및 policydeploy 유틸리티를 시작합니다.

12. (선택 사항) 재해 복구 DMS 가 프로덕션 DMS 와 비동기화 상태인 경우 다음 단계를 완료합니다.
    a. 프로덕션 DMS 백업 파일로부터 재해 복구 DMS 를 복원 (페이지 394)합니다.
    b. 재해 복구 DMS 를 백업합니다. 다음 방법 중 하나로 DMS 를 백업할 수 있습니다.
        - sepmd 유틸리티 (페이지 390)
        - selang 명령 (페이지 391)
    c. 재해 복구 DMS 백업 파일로부터 각 재해 복구 DH 를 복원 (페이지 392)합니다.

sepmd 를 사용하는 DMS 백업

끝점에 배포한 정책 사본을 저장하고 끝점에서 엔터프라이즈 관리 서버가 받은 보고서 스냅숏을 저장하려면 DMS 를 백업하십시오.

DMS 를 백업할 때 DMS 데이터베이스의 데이터를 지정된 디렉터리로 복사합니다.

sepmd 유틸리티는 오로지 로컬 호스트의 DMS 만 백업합니다. 백업된 DMS 파일은 가급적 CA Access Control 액세스 규칙에 의해 보호되는 안전한 곳에 보관해야 합니다. DMS 를 백업하기 전에 updates.dat 파일을 자동으로 자르는 것이 좋습니다.

참고: selang 명령을 사용하여 로컬 또는 원격 호스트의 DMS 를 백업할 수도 있습니다.

sepmd 를 사용하여 DMS 를 백업하려면

1. 다음 명령을 사용하여 DMS 를 잠급니다.

   sepmd -bl *dms_name*

   DMS 가 잠기며, 이제 구독자에게 어떤 명령도 보낼 수 없습니다.

2. 다음 명령을 사용하여 DMS 데이터베이스를 백업합니다.

   sepmd -bd *dms_name* [*destination_directory*]

   dms_name

   로컬 호스트에 백업된 DMS 이름을 정의합니다.

   destination_directory

   DMS 를 백업할 대상 디렉터리를 정의합니다.

   기본값: (UNIX) *ACInstallDir*/data/policies_backup/dmsName

   기본값: (Windows) *ACInstallDir*\data\policies_backup\dmsName

   DMS 데이터베이스가 대상 디렉터리에 백업됩니다.

3. 다음 명령을 사용하여 DMS 를 잠금 해제합니다.

   sepmd -ul *dms_name*

   DMS 가 잠금 해제되며, 이제 구독자에게 명령을 보낼 수 있습니다.

selang 을 사용하는 DMS 백업

DMS 데이터베이스에서 지정된 디렉터리로 데이터를 복사하려면 DMS 를 백업하십시오.

selang 명령을 사용하여 로컬 또는 원격 호스트의 DMS 를 백업할 수 있습니다. 백업된 DMS 파일은 가급적 CA Access Control 액세스 규칙에 의해 보호되는 안전한 곳에 보관해야 합니다. DMS 를 백업하기 전에 updates.dat 파일을 자동으로 자르는 것이 좋습니다.

참고: sepmd 유틸리티를 사용하여 로컬 호스트에서 DMS 를 백업할 수도 있습니다.

selang 을 사용하여 DMS 를 백업하려면

1. (선택 사항) selang 을 사용하여 원격 호스트로부터 DMS 에 연결하려는 경우 다음 명령으로 DMS 호스트에 연결합니다.

   host *dms_host_name*

2. 다음 명령을 사용하여 PMD 환경으로 이동합니다.

   env pmd

3. 다음 명령을 사용하여 DMS 를 잠급니다.

   pmd *dms_name* lock

   DMS 가 잠기며, 이제 구독자에게 어떤 명령도 보낼 수 없습니다.

4. 다음 명령을 사용하여 DMS 데이터베이스를 백업합니다.

   backuppmd *dms_name* [destination(*destination_directory*)]

   dms_name

   로컬 호스트에 백업된 DMS 이름을 정의합니다.

   destination*(destination_directory)*

   DMS 를 백업할 대상 디렉터리를 정의합니다.

   기본값: (UNIX) *ACInstallDir*/data/policies_backup/dmsName

   기본값: (Windows) *ACInstallDir*\data\policies_backup\dmsName

   DMS 데이터베이스가 대상 디렉터리에 백업됩니다.

5. 다음 명령을 사용하여 DMS 를 잠금 해제합니다.

   pmd *dms_name* unlock

   DMS 가 잠금 해제되며, 이제 구독자에게 명령을 보낼 수 있습니다.

DH 복원

dmsmgr 유틸리티를 사용하여 DMS 백업 파일에서 DH_Reader 디렉터리로 데이터를 복사하려면 DH 를 복원하십시오. DH 작성기는 임시 데이터베이스가 있으므로 복원할 필요가 없습니다. DH 를 복원하기 전에 기존 DH 파일 구조에 DH 작성기가 있는지 확인하십시오.

참고: 기존 DH 파일 구조에 DH 작성기가 없거나 새 DH 를 설정하고 싶으면 DH 를 복원하기 전에 dmsmgr -create 기능을 사용하여 새 DH 를 만드십시오.

참고: dmsmgr 유틸리티를 사용하려면 운영 체제에 대해 완전한 관리 액세스 권한이 있어야 합니다.

DH 를 복원하려면 DH 호스트에서 다음 명령을 실행합니다.

dmsmgr -restore -dh *name* -source *path* -parent *name*\
[-admin *user*[,*user*...]] [-xadmin *user*[,*user*...]] [-desktop *host*[, *host*...]]

-admin *user*[,*user*...]

(UNIX) 내부 사용자를 복원된 DMS 또는 DH 의 관리자로 정의합니다.

-desktop *host*[, *host...*]

(선택 사항) 복원된 DH 가 있는 컴퓨터에 대해 TERMINAL 액세스 권한을 갖는 컴퓨터의 목록을 정의합니다.

참고: 지정 여부에 관계없이 이 유틸리티를 실행하는 터미널에는 복원된 DH 에 대한 관리 권한이 항상 부여됩니다.

-dh *name*

로컬 호스트에 복원된 DH 이름을 정의합니다.

-parent *name*

복원된 DH 가 구독할 부모 DMS 의 이름을 정의합니다. 부모 DMS 는 *DMS_name@hostname* 형식으로 지정하십시오.

-source *path*

복원할 백업 파일이 있는 디렉터리를 정의합니다.

-xadmin *user*[,*user...*]

(UNIX) 엔터프라이즈 사용자를 복원된 DMS 또는 DH 의 관리자로 정의합니다.

DH 가 복원되며 DH 가 DMS 를 구독합니다.

프로덕션 DMS 복원

프로덕션 DMS 를 복원할 때 dmsmgr 는 재해 복구 DMS 백업 파일의 데이터를 프로덕션 DMS 디렉터리에 복사합니다.

참고: dmsmgr 유틸리티를 사용하려면 운영 체제에 대해 완전한 관리 액세스 권한이 있어야 합니다.

프로덕션 DMS 를 복원하려면 프로덕션 DMS 호스트에서 다음 명령을 입력합니다.

dmsmgr -restore -dms *name* -source *path* -replica *name*\
[-subscriber *dhname*[,*dhname...*]] [-admin *user*[,*user...*]]\
[-xadmin *user*[,*user...*]]

-admin *user*[,*user...*]

(UNIX) 내부 사용자를 복원된 DMS 또는 DH 의 관리자로 정의합니다.

-dms *name*

로컬 호스트에 복원된 DMS 이름을 정의합니다.

-replica *name*

프로덕션 DMS 에 구독한 재해 복구 DMS 의 이름을 정의합니다. 재해 복구 DMS 는 *DMS_name@hostname* 형식으로 지정하십시오.

-subscriber *dh_name*[, *dh_name*...]

(선택 사항) 복원된 DMS 가 정책 업데이트를 보낼 DH 의 목록을 쉼표로 구분하여 정의합니다. 각 DH 는 *DH_name@hostname* 형식으로 지정하십시오.

-source *path*

복원할 백업 파일이 있는 디렉터리를 정의합니다.

-xadmin *user*[,*user*...]

(UNIX) 엔터프라이즈 사용자를 복원된 DMS 또는 DH 의 관리자로 정의합니다.

프로덕션 DMS 가 복원되었습니다.

참고: 프로덕션 DMS 를 복원한 다음 프로덕션 DMS 를 백업하고 그 백업 파일로부터 프로덕션 DH 를 복원해야 합니다. 그러면 프로덕션 DMS 와 프로덕션 DH 가 동기화됩니다.

재해 복구 DMS 복원

재해 복구 DMS 를 복원할 때 dmsmgr 는 백업 파일의 데이터를 재해 복구 DMS 디렉터리에 복사합니다.

참고: dmsmgr 유틸리티를 사용하려면 운영 체제에 대해 완전한 관리 액세스 권한이 있어야 합니다.

재해 복구 DMS 를 복원하려면 재해 복구 DMS 호스트에서 다음 명령을 입력합니다.

dmsmgr -restore -dms *name* -source *path* -parent *name*\
[-subscriber *dhname*[,*dhname*...]] [-admin *user*[,*user*...]]\
[-xadmin *user*[,*user*...]]

-admin *user*[,*user*...]

(UNIX) 내부 사용자를 복원된 DMS 또는 DH 의 관리자로 정의합니다.

-dms *name*

로컬 호스트에 복원된 DMS 이름을 정의합니다.

-parent *name*

복원된 재해 복구 DMS 가 구독할 프로덕션 DMS 의 이름을 정의합니다. 프로덕션 DMS 는 *DMS_name*@hostname 형식으로 지정하십시오.

-source *path*

복원할 백업 파일이 있는 디렉터리를 정의합니다.

-subscriber *dh_name*[, *dh_name*...]

(선택 사항) 복원된 DMS 가 정책 업데이트를 보낼 DH 의 목록을 쉼표로 구분하여 정의합니다. 각 DH 는 *DH_name@hostname* 형식으로 지정하십시오.

-xadmin *user*[,*user*...]

(UNIX) 엔터프라이즈 사용자를 복원된 DMS 또는 DH 의 관리자로 정의합니다.

재해 복구 DMS 가 복원되며 재해 복구 DMS 가 프로덕션 DMS 를 구독합니다.

참고: 재해 복구 DMS 를 복원한 다음 재해 복구 DMS 를 백업하고 그 백업 파일로부터 재해 복구 DH 를 복원해야 합니다. 그러면 재해 복구 DMS 와 재해 복구 DH 가 동기화됩니다.

메시지 큐 서버 데이터 파일 백업

프로덕션 메시지 큐 서버에서 재해 복구 메시지 큐 서버로 데이터를 복사하기 위해 메시지 큐 서버 데이터 파일을 백업합니다.

메시지 큐 서버 데이터 파일을 백업하려면 프로덕션 배포 서버에서 재해 복구 배포 서버로 메시지 큐 서버 데이터 파일을 복사하십시오. 기본적으로 데이터 파일은 아래 디렉터리에 있습니다. 여기서 *ACServerInstallDir* 는 메시지 큐 서버를 설치한 디렉터리입니다.

ACServerInstallDir/MessageQueue/tibco/ems/bin/datastore

메시지 큐 서버 데이터 파일 복원

재해 복구 메시지 큐 서버에서 프로덕션 메시지 큐 서버로 데이터를 복사하려면 메시지 큐 서버 데이터 파일을 복원하십시오.

메시지 큐 서버 데이터 파일을 복원하려면 재해 복구 배포 서버에서 프로덕션 배포 서버로 메시지 큐 서버 데이터 파일을 복사하십시오. 기본적으로 데이터 파일은 아래 디렉터리에 있습니다. 여기서 *ACServerInstallDir* 는 메시지 큐 서버를 설치한 디렉터리입니다.

ACServerInstallDir/MessageQueue/tibco/ems/bin/datastore

메시지 큐 서버 데이터 파일을 동기화하는 방법

재해 복구 환경에서 작업하는 경우 프로덕션 및 재해 복구 메시지 큐 서버를 동기화하는 것이 매우 중요합니다. 서버를 동기화하면 프로덕션 및 재해 복구 메시지 큐 서버 모두에서 데이터가 업데이트되며, 프로덕션 서버가 작동하지 않는 경우 재해 복구 서버가 중단 없이 계속 데이터를 제공할 수 있습니다.

참고: 동기화 솔루션은 타사 복제 도구에 기반합니다. 스토리지 솔루션이 공유된 스토리지에 데이터 블록을 데이터 버퍼와 동일한 순서로 기록하는지 확인하십시오. 동기적 쓰기 호출에서 돌아올 때 스토리지 솔루션이 모든 데이터가 지속 가능한 스토리지에 기록되었는지 여부를 확인하도록 하십시오.

메시지 큐 서버의 데이터 파일을 동기화하려면 다음을 수행하십시오.

1. 프로덕션 서버에서 메시지 큐 서버와 엔터프라이즈 관리 서버에 설치된 모든 메시지 큐 서버 사이에서 메시지 라우팅 설정을 구성합니다.
2. 재해 복구 배포 서버의 메시지 큐 서버와 재해 복구 엔터프라이즈 관리 서버 사이에서 메시지 라우팅 설정을 구성합니다.

3. 엔터프라이즈 관리 서버의 재해 복구 및 프로덕션 메시지 큐 서버 모두에서 queues.conf 파일을 수정하여 "fail-safe" 줄을 추가합니다.

   예:

   queue/snapshots secure,failsafe
   queue/audit secure, failsafe
   ac_endpoint_to_server secure, failsafe
   ac_server_to_endpoint secure,failsafe

   기본적으로 이 파일은 다음 디렉터리에 있습니다. 여기서 *ACServerInstallDir* 는 엔터프라이즈 관리 서버를 설치한 디렉터리입니다.

   ACServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data

4. 타사 복제 도구를 사용하여 엔터프라이즈 관리 서버에 있는 프로덕션 메시지 큐 서버 EMS 데이터 파일을 재해 복구 엔터프라이즈 관리 서버에 있는 메시지 큐 서버로 복제합니다.

   기본적으로 메시지 큐 서버 EMS 데이터 파일은 아래 디렉터리에 있습니다. 여기서 *ACServerInstallDir* 는 엔터프라이즈 관리 서버를 설치한 디렉터리입니다.

   ACServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data/datastore

   메시지 큐 서버 EMS 데이터 파일 동기화 설정을 구성했습니다.

부록 A: 통신 암호화 방법 변경

이 섹션은 다음 항목을 포함하고 있습니다.

통신 암호화

다음 방법을 사용하여 CA Access Control 구성 요소 사이의 통신을 암호화하고 CA Access Control 클라이언트/서버 통신을 암호화할 수 있습니다.

- 대칭 암호화
- SSL

참고: Windows 에서 암호화 모드(예: FIPS 전용 모드)를 변경할 때 암호 PMDB 로부터 암호를 전파해야 하는 경우에는 CA Access Control 서비스를 다시 시작하십시오.

대칭 암호화

CA Access Control 은 암호화 라이브러리를 사용하여 대칭(표준) 암호화를 구현합니다. 다음 방법을 사용하여 CA Access Control 구성 요소 사이의 통신을 암호화할 수 있습니다.

- 기본 (독자적) 암호화
- AES128
- AES192
- AES256
- DES
- 3DES

참고: '기본'이란 이름의 암호화 방법은 기본 CA Access Control 암호화 방법이 아닙니다. 기본 암호화 방법은 AES256.

CA Access Control 을 설치할 때 설치 관리자는 암호화 라이브러리를 다음 디렉터리에 저장합니다. 여기서 *ACInstallDir* 는 CA Access Control 을 설치한 디렉터리입니다.

- (Windows) *ACInstallDir*\bin
- (UNIX) *ACInstallDir*/lib

Windows 에서 CA Access Control 은 대칭 암호화에 사용하는 암호화 라이브러리의 전체 경로를 다음 구성 설정에 저장합니다.

HKEY_LOCAL_MACHINE\Software\ComputerAssociates\AccessControl\Encryption Package

대칭 암호화 키와 대칭 암호화 방법을 변경하려면 sechkey 유틸리티를 사용합니다.

추가 정보:

대칭 암호화 키 변경 (페이지 401)
대칭 암호화 방법 변경 (페이지 402)

sechkey 가 대칭 암호화를 구성하는 방법

대칭 암호화 키의 길이는 55 자입니다. sechkey 는 키 길이가 이보다 길면 자동으로 자르고 짧으면 자동으로 늘입니다.

sechkey 를 사용하여 암호화 키를 변경하면 sechkey 가 CA Access Control 데이터베이스의 모든 프로그램에서 키를 즉시 변경합니다. sechkey 가 대칭 키 또는 대칭 암호화 방법을 변경할 때는 암호를 해독한 다음 다음을 다시 암호화합니다.

- 컴퓨터 설치된 모든 정책 모델의 암호화된 레코드
- CA Access Control 메시지 큐 암호를 포함하여 CA Access Control 데이터베이스의 모든 암호화된 암호 및 (CA Access Control 이 양방향 암호를 사용하는 경우) USER 암호
- 키가 암호로 보호되지 않는 경우 서버 개인 키
- 키가 암호로 보호되는 경우 서버 개인 키에 대한 암호

또한 CA Access Control API 를 사용하여 CA Access Control 과 통신하는 프로그램을 만들 때마다 새 프로그램의 통신은 동일한 키를 사용하여 암호화됩니다.

대칭 암호화 키 변경

대칭 암호화 키는 CA Access Control 구성 요소 사이의 통신을 보호합니다. 대칭 암호화 키를 변경하려면 sechkey 유틸리티를 사용합니다. sechkey 는 대화형 또는 비대화형 모드로 사용할 수 있습니다.

대칭 암호화 키를 변경하기 전에 다음 제한 사항에 유의하십시오.

- 암호의 길이는 1-55 자여야 합니다.
- 암호는 높은 ASCII 문자를 포함할 수 없습니다.
- 암호는 큰따옴표(")를 포함할 수 없습니다.

sechkey 를 사용하려면 ADMIN 특성이 있어야 합니다.

중요! 통신 문제가 발생하지 않도록 하려면 CA Access Control 구성 요소를 실행하는 모든 컴퓨터에서 동일한 암호화 키를 사용하십시오.

대칭 암호화 키를 변경하려면

1. CA Access Control 을 중지합니다.

   CA Access Control 엔터프라이즈 관리 서버에서 암호화 설정을 변경하는 경우 CA Access Control 웹 서비스도 중지해야 합니다.

2. 대화형 모드에서 sechkey 유틸리티 실행:

   ```
   sechkey
   ```

   이 유틸리티는 기존 키와 새 키를 입력하고 대칭 암호화 키를 변경하도록 요청합니다.

3. CA Access Control 을 시작하고

   CA Access Control 엔터프라이즈 관리 서버에서 암호화 설정을 변경하는 경우 CA Access Control 웹 서비스도 시작해야 합니다.

   CA Access Control 은 새 암호화 키를 사용하여 통신을 시작하고 암호화합니다.

예: 비대화형 모드에서 대칭 암호화 키 변경

다음 예는 값 newkey 를 사용하는 새 키로 기본 CA Access Control 대칭 키를 변경합니다.

```
sechkey -d newkey
```

참고: sechkey 유틸리티에 대한 자세한 내용은 *참조 안내서*를 참조하십시오.

대칭 암호화 방법 변경

대칭 암호화는 CA Access Control 구성 요소 사이의 통신을 보호하며, 암호화 라이브러리에 의해 구현됩니다. 암호화 라이브러리를 변경(따라서 대칭 암호화 방법도 변경)하려면 sechkey 유틸리티를 사용합니다.

sechkey 를 사용하려면 ADMIN 특성이 있어야 합니다.

참고: CA Access Control 이 FIPS 전용 모드에서 실행되는 경우 대칭 암호화 방법을 변경할 수 없습니다. crypto 섹션의 fips_only 구성 토큰의 값이 1 인 경우 CA Access Control 은 FIPS 전용 모드로 동작합니다. 이 제한으로 인해 암호화 방법을 FIPS 와 호환되지 않는 방법으로 변경할 수 없습니다.

중요! 통신 문제가 발생하지 않도록 하려면 CA Access Control 구성 요소를 실행하는 모든 컴퓨터에서 동일한 암호화 방법을 사용하십시오.

대칭 암호화 방법을 변경하려면

1. CA Access Control 을 중지합니다.

   CA Access Control 엔터프라이즈 관리 서버에서 암호화 설정을 변경하는 경우 CA Access Control 웹 서비스도 중지해야 합니다.
2. 대칭 암호화 방법을 변경하려면 sechkey 유틸리티를 사용하십시오.
3. CA Access Control 을 시작합니다.

   CA Access Control 엔터프라이즈 관리 서버에서 암호화 설정을 변경하는 경우 CA Access Control 웹 서비스도 시작해야 합니다.

   CA Access Control 은 새 암호화 방법을 사용하여 통신을 시작하고 암호화합니다.

예: 대칭 암호화 방법을 3DES 로 변경

다음 명령은 대칭 암호화 방법을 3DES 로 변경합니다.

```
sechkey -m -sym tripledes
```

참고: sechkey 유틸리티에 대한 자세한 내용은 *참조 안내서*를 참조하십시오.

엔터프라이즈 배포에서 여러 대칭 암호화 방법

끝점은 다른 암호화 방법을 사용하는 다른 CA Access Control 구성 요소와 통신할 수 있습니다. crypto 섹션의 encryption_methods 구성 설정은 끝점이 허용하는 대칭 암호화를 지정합니다.

기본적으로, 이 구성 설정은 다음 암호화 방법을 순서대로 나열합니다.

- AES256
- AES192
- AES128
- DES
- 3DES

CA Access Control 에이전트가 다른 구성 요소로부터 들어오는 통신을 암호화할 때는 암호화가 성공할 때까지 목록의 각 방법을 사용하려고 시도합니다. 에이전트는 동일한 암호화 방법을 사용하여 해당 구성 요소로 나가는 통신을 암호화합니다.

유사하게, CA Access Control 웹 서비스가 끝점에 연결을 시도할 때는 끝점과 성공적으로 통신할 때까지 목록의 각 방법을 사용하려고 시도합니다.

여러 암호화 방법을 사용하여 엔터프라이즈 CA Access Control 배포를 쉽게 업그레이드할 수 있습니다. 예를 들어, DES 암호화를 사용하는 r12.5 배포가 있다고 가정합니다. r12.5 SP4 로 단계별 업그레이드를 수행하고 업그레이드된 구성 요소에 대해 암호화 방법을 AES256 으로 변경하려고 합니다. 엔터프라이즈 관리 서버를 r12.5 SP4 로 업그레이드합니다. 이 서버는 이제 기본적으로 AES256 암호화를 사용합니다. 하지만 r12.5 SP4 서버가 DES 암호화를 사용하는 CA Access Control 구성 요소와도 통신할 수 있으므로 엔터프라이즈 관리 서버는 계속 r12.5 끝점을 관리할 수 있습니다.

SSL, 인증 및 인증서

TLS 를 비롯한 SSL(Secure Sockets Layer)은 컴퓨터 프로그램 간의 통신을 제공합니다. SSL 은 통신이 다음과 같은 속성을 갖도록 합니다.

- 통신의 참가자는 인증됩니다. 즉, 통신의 참가자는 프로그램 또는 사용자입니다.
- 데이터를 안전하게 암호화하고 참가자만 이를 읽을 수 있습니다.

참가자는 X.509 인증서를 사용하여 서로 인증합니다. X.509 인증서는 인증서의 소유자 주소와 공용 키를 연결하는 전자 문서입니다. 인증서는 위조할 수 없습니다.

SSL 은 클라이언트/서버 모델에서 동작하며 PKI(공개 키 인프라)를 사용합니다. 클라이언트는 서버에서 X.509 인증서를 받으면 유효한 인증서인지 확인합니다. 유효한 인증서인 경우 클라이언트는 서버가 의도된 프로그램이나 사용자임을 알게 되며 따라서 서버가 인증됩니다. 또한, 클라이언트에서 데이터 암호화에 인증서의 공용 키를 사용하는 경우 서버만 해당 데이터를 해독할 수 있으므로 데이터가 안전합니다. 반대로 서버는 클라이언트에서 받은 X.509 인증서를 동일한 방식으로 사용합니다.

인증서의 내용

프로그램은 공개 키에 바인딩되었음 입증하기 위해 X.509 인증서를 보냅니다. 이렇게 하면 다른 프로그램이 메시지를 암호화할 때 인증서의 주체만이 이 메시지를 해독할 수 있음을 알게 됩니다.

X.509 인증서의 내용은 다음과 같습니다.

- **인증서 데이터** - 가장 중요한 인증서 데이터 필드는 다음과 같습니다.
  - 인증서 주체의 공용 식별자(예: 웹 주소)
  - 인증서의 유효 기간(시작 및 종료 날짜)
- **인증서를 인증하는 인증 기관(CA)의 이름** - 인증서의 리더는 서명이 유효한지 여부를 알 수 있습니다. CA 는 공개 키가 주체와 연관되어 있는지 여부를 검증합니다. 즉, 인증서의 리더가 CA 를 트러스트하는 경우 공개 키를 사용하여 암호화된 데이터는 해당 주체만 읽을 수 있음을 확신하게 됩니다.
- 주체의 공개 키 - 인증서 리더는 공개 키를 사용하여 인증서 주체에게 전송할 데이터를 암호화합니다.

- **디지털 서명** - 디지털 서명은 인증서에 있는 모든 다른 데이터의 해시된 캡슐화로, CA 의 개인 키로 암호화됩니다. 전송자가 공개 키로 데이터를 암호화하는 암호화 경우와는 반대로, CA 공개 키에 액세스할 수 있는 사용자는 누구나 서명을 읽고 인증서의 다른 데이터와 이 서명이 일치하는지 검사할 수 있습니다. 인증서의 텍스트가 변경된 경우 서명은 더 이상 인증서 텍스트와 일치하지 않게 됩니다.

주체의 개인 키는 인증서와 연결되어 있으나 별도로 안전하게 보관됩니다. 주체는 프로그램에서 공개 키를 사용하여 암호화한 메시지를 개인 키를 사용하여 해독합니다.

인증서 입증 사항

리더는 CA(인증 기관)의 공개 키를 사용하여 인증서 서명의 유효성을 검사할 수 있습니다. 해독된 서명이 나머지 인증서와 일치하고 리더가 CA 를 트러스트하면 다음이 사실임을 리더가 알고 있음을 의미합니다.

- 리더가 공개 키를 사용하여 데이터를 암호화한 경우 개인 키의 소유자만 해당 데이터를 해독하고 읽을 수 있음.
- 인증서 개인 키의 소유자가 인증서에서 지정된 주체임.

인증서가 유효한 것에 대해 확신을 가지려면 리더가 CA 를 트러스트해야 하며 CA 공개 키에도 액세스해야 합니다. 대부분의 경우 CA 가 잘 알려진 회사이고 프로그램(그리고 많이 사용되는 모든 웹 브라우저)에 CA 의 공개 키 사본이 있으므로 리더가 인터넷을 통해 CA 가 실제로 인증서의 유효성을 검사했는지 확인할 필요가 없습니다.

발급자가 소유자이기도 한 경우 인증서는 자체 서명된 것으로 보므로 발급자를 트러스트하는 데 더 많은 문제가 생깁니다.

인증서를 전송한 프로그램이 인증서 소유자인지를 확인하기 위해서는 리더가 몇 가지 다른 방법을 사용해야 합니다. 일반적으로 리더는 인증서 전송자를 찾기 위해 사용된 주소가 인증서에 있는 주소와 동일한지를 확인합니다.

루트 및 서버 인증서

루트(또는 CA) 인증서는 인증 기관(CA)에 의해 검증된 트러스트된 X.509 인증서입니다. 추가 X.509 인증서 명명된 서버, 주체, 인증서를 만들려면 이 트러스트된 인증서를 사용합니다. 각 서버 인증서는 루트 인증서의 개인 키로 서명됩니다. 리더가 루트 인증서를 트러스트하면 리더는 해당 루트 인증서에서 생성된 모든 서버 인증서를 트러스트할 수 있습니다.

루트 인증서는 서버 인증서를 생성하고 인증합니다. CA Access Control 에서 다음과 같은 유형의 루트 인증서를 사용할 수 있습니다.

- 기본 CA Access Control 루트 인증서
- 암호로 보호된 인증서를 포함한 타사 루트 인증서

서버 인증서는 CA Access Control 클라이언트/서버 통신과 CA Access Control 구성 요소 사이의 통신을 암호화하고 인증합니다. CA Access Control 에서 다음과 같은 유형의 서버 인증서를 사용할 수 있습니다.

- 기본 CA Access Control 서버 인증서
- 암호로 보호된 인증서를 포함한 타사 서버 인증서
- 타사 루트 인증서에서 만든 CA Access Control 서버 인증서

SSL 암호화 활성화

CA Access Control 을 설치할 때 암호화 설정을 구성합니다. 설치 이후에 sechkey 유틸리티를 사용하여 SSL 암호화를 변경할 수 있습니다. 구성 설정의 값도 변경해야 할 수 있습니다.

중요! 통신 문제가 발생하지 않도록 하려면 CA Access Control 구성 요소를 실행하는 모든 컴퓨터에서 동일한 암호화 방법을 사용하십시오.

SSL 암호화를 활성화하려면

1. CA Access Control 을 중지합니다.

   CA Access Control 엔터프라이즈 관리 서버에서 암호화 설정을 변경하는 경우 CA Access Control 웹 서비스도 중지하십시오.

2. crypto 섹션에 있는 communication_mode 구성 설정을 다음 중 *하나*로 변경하십시오.

   all_modes

   대칭 및 SSL 암호화를 모두 사용하려면 이 값을 지정하십시오. 이 값은 컴퓨터가 모든 CA Access Control 구성 요소와 통신하도록 만듭니다.

   참고: 이 값을 지정하는 경우 CA Access Control 은 다른 CA Access Control 구성 요소와 통신을 시도할 때마다 SSL 암호화를 사용합니다. SSL 이 실패하는 경우 대칭 암호화를 사용합니다. 이 값은 CA Access Control 배포를 대칭 암호화 환경에서 SSL 암호화 환경으로 마이그레이션할 수 있게 합니다.

   use_ssl

   SSL 암호화만 사용하려면 이 값을 지정하십시오. 이 값은 컴퓨터가 SSL 암호화를 사용하는 CA Access Control 구성 요소와만 통신하도록 합니다.

   참고: (Windows) CA Access Control SDK 를 사용하는 타사 프로그램으로 작업하는 경우 crypto 섹션은 설치 중 정의하는 CA Access Control SDK 레지스트리 경로에 있습니다.

3. (권장) 다음 중 *하나*를 수행하기 위해 SSL 통신을 구성하십시오.

   - 타사 루트 및 서버 인증서를 사용합니다 (페이지 408).
   - 타사 루트 인증서에서 생성하는 서버 인증서를 사용합니다 (페이지 410).

참고: SSL 암호화를 더 이상 구성하지 않는 경우 기본 CA Access Control X.509 인증서를 사용하여 CA Access Control 구성 요소 사이의 통신을 암호화하고 인증할 수 있습니다. 하지만 기본 인증서를 대신 변경하는 것이 좋습니다.

4. CA Access Control 을 시작합니다.
   - CA Access Control 엔터프라이즈 관리 서버에서 암호화 설정을 변경하는 경우 CA Access Control 웹 서비스도 시작하십시오.
   - CA Access Control SDK 를 사용하는 타사 프로그램을 사용하여 작업하는 경우 CA Access Control SDK 를 사용하는 프로세스를 다시 시작하십시오.

   SSL 암호화가 활성화됩니다.

타사 루트 및 서버 인증서 사용

SSL 암호화를 사용하는 경우 타사 루트 및 서버 인증서를 사용하여 CA Access Control 구성 요소 사이의 통신을 암호화하고 인증할 수 있습니다.

타사 루트 및 서버 인증서를 사용하려면 다음 파일이 필요합니다.

- **root.pem** - 루트 인증서
- **server.pem** - 서버 인증서
- **server.key** - 서버 인증서의 개인 키

  OU 암호로 보호된 서버 인증서를 사용하는 경우 서버 인증서의 개인 키에 대한 암호도 필요합니다.

참고: 서버 인증서가 이미 만들어졌으므로 루트 인증서에 대한 개인 키가 필요 없습니다.

타사 루트 및 서버 인증서를 사용하려면

1. CA Access Control 서비스가 중지되었고 SSL 이 활성화되었는지 확인합니다.
2. 루트 인증서를 대체합니다. 다음 작업 중 *하나*를 수행합니다.
   - 새 루트 인증서를 crypto 섹션에 있는 ca_certificate 구성 설정에 지정된 위치에 복사합니다.
   - crypto 섹션에 있는 ca_certificate 구성 설정의 값을 편집하여 새 루트 인증서에 대한 전체 경로를 지정합니다.

     참고: 새 디렉터리에 루트 인증서를 설치하는 경우 새 디렉터리를 보호하기 위해 CA Access Control FILE 규칙을 작성하십시오.
3. 서버 인증서를 대체합니다. 다음 작업 중 *하나*를 수행합니다.
   - 새 서버 인증서를 crypto 섹션에 있는 subject_certificate 구성 설정에 지정된 위치에 복사합니다.
   - crypto 섹션에 있는 subject_certificate 구성 설정의 값을 편집하여 새 서버 인증서에 대한 전체 경로를 지정합니다.

     참고: 새 디렉터리에 서버 인증서를 설치하는 경우 새 디렉터리를 보호하기 위해 CA Access Control FILE 규칙을 작성하십시오.
4. 서버 키를 대체합니다. 다음 작업 중 *하나*를 수행합니다.
   - 새 서버 키를 crypto 섹션에 있는 private_key 구성 설정에 지정된 위치에 복사합니다.
   - crypto 섹션에 있는 private_key 구성 설정의 값을 편집하여 새 서버 키에 대한 전체 경로를 지정합니다.

     참고: 새 디렉터리에 서버 키를 설치하는 경우 새 디렉터리를 보호하기 위해 CA Access Control FILE 규칙을 작성하십시오.

5. OU 암호로 보호된 인증서를 사용하는 경우 다음을 수행하십시오.

   a. crypto 섹션의 fips_only 구성 설정의 값이 0 인지 확인합니다.

      참고: CA Access Control 이 FIPS 전용 모드에서 실행 중인 경우 암호로 보호된 인증서를 사용할 수 없습니다.

   b. 다음과 같이 서버 인증서 개인 키에 대한 암호를 컴퓨터에 저장하십시오.

      sechkey -g -subpwd *private_key_password*

      참고: sechkey 를 사용하려면 ADMIN 특성이 있어야 합니다.

   c. CA Access Control 이 저장된 암호를 사용하여 개인 키를 열 수 있는지 확인합니다.

      sechkey -g -verify

      CA Access Control 이 키를 열 수 없는 경우 b 단계를 반복하여 올바른 암호를 지정합니다.

   참고: sechkey 유틸리티에 대한 자세한 내용은 *참조 안내서*를 참조하십시오.

6. CA Access Control 을 시작합니다.

   - CA Access Control 엔터프라이즈 관리 서버에서 암호화 설정을 변경하는 경우 CA Access Control 웹 서비스도 시작하십시오.
   - CA Access Control SDK 를 사용하는 타사 프로그램을 사용하여 작업하는 경우 CA Access Control SDK 를 사용하는 프로세스를 다시 시작하십시오.

   SSL 암호화가 활성화됩니다.

타사 루트 인증서에서 생성하는 서버 인증서 사용

SSL 암호화를 사용하는 경우 타사 루트 인증서에서 서버 인증서를 만들 수 있습니다. 이러한 인증서를 사용하여 CA Access Control 구성 요소 사이의 통신을 암호화하고 인증합니다.

암호로 보호된 서버 인증서를 만들 수 있으며, 이 경우 CA Access Control 은 지정된 암호를 사용하여 서버 인증서에 대한 개인 키를 보호합니다.

타사 루트 인증서에서 서버 인증서를 만들려면 다음 파일이 필요합니다.

- **root.pem** - 루트 인증서
- **root.key** - 루트 인증서의 개인 키

타사 루트 인증서에서 생성하는 서버 인증서를 사용하려면

1. CA Access Control 서비스가 중지되었고 SSL 이 활성화되었는지 확인합니다.
2. OU 암호로 보호된 인증서를 사용하는 경우 crypto 섹션의 fips_only 구성 설정의 값이 0 인지 확인하십시오.

   참고: CA Access Control 이 FIPS 전용 모드에서 실행 중인 경우 암호로 보호된 인증서를 사용할 수 없습니다.
3. 다음 디렉터리에서 sub_cert_info 를 *제외한* 모든 파일을 삭제합니다. 여기서 *ACInstallDir* 는 CA Access Control 을 설치한 디렉터리입니다.

   ACInstallDir/data/crypto

   중요! sub_cert_info 파일은 삭제하지 마십시오.

   기본 서버 인증서 및 서버 인증서의 기본 키가 삭제됩니다.
4. 루트 인증서를 대체합니다. 다음 작업 중 *하나*를 수행합니다.
   - 새 루트 인증서를 crypto 섹션에 있는 ca_certificate 구성 설정에 지정된 위치에 복사합니다.
   - crypto 섹션에 있는 ca_certificate 구성 설정의 값을 편집하여 새 루트 인증서에 대한 전체 경로를 지정합니다.

     참고: 새 디렉터리에 루트 인증서를 설치하는 경우 이 디렉터리를 보호하기 위한 CA Access Control FILE 규칙을 작성하십시오.
5. sechkey 유틸리티를 사용하여 서버 인증서를 만듭니다.

   참고: sechkey 유틸리티에 대한 자세한 내용은 *참조 안내서*를 참조하십시오. sechkey 를 사용하려면 ADMIN 특성이 있어야 합니다. CA Access Control SDK 를 사용하는 타사 프로그램을 사용하여 작업하는 경우 sechkey 를 실행할 때 sechkey 명령에 -s 옵션을 사용하십시오.

6. (선택 사항) 루트 인증서에 대한 개인 키를 삭제합니다.

   루트 인증서로부터 다른 서버 인증서를 만들지 않으려면 루트 인증서에 대한 개인 키를 삭제해도 됩니다.

7. CA Access Control 을 시작합니다.

   - CA Access Control 엔터프라이즈 관리 서버에서 암호화 설정을 변경하는 경우 CA Access Control 웹 서비스도 시작하십시오.
   - CA Access Control SDK 를 사용하는 타사 프로그램을 사용하여 작업하는 경우 CA Access Control SDK 를 사용하는 프로세스를 다시 시작하십시오.

   SSL 암호화가 활성화됩니다.

예: sechkey 를 사용하여 서버 인증서 만들기

이 예는 타사 루트 인증서에서 서버 인증서를 만듭니다. 이 예는 기본 CA Access Control 인증서 정보 파일을 사용합니다. 루트 인증서의 개인 키 이름은 custom_root.key 이며 /opt/CA/AccessControl/data/crypto 에 있습니다.

```
sechkey -e -sub -in "/opt/CA/AccessControl/data/crypto/sub_cert_info" -priv
/opt/CA/AccessControl/data/crypto/custom_root.key
```

암호로 보호된 서버 인증서

CA Access Control 이 암호로 보호된 서버 인증서를 사용하도록 구성할 수 있으며, 이 경우 CA Access Control 은 지정된 암호를 사용하여 서버 인증서에 대한 개인 키를 보호합니다. CA Access Control 은 *ACInstallDir*/Data/crypto 디렉터리에 있는 crypto.dat 파일에 암호를 저장합니다. 여기서 *ACInstallDir* 는 CA Access Control 을 설치한 디렉터리입니다. crypto.dat 파일은 읽기 전용의 암호화된 숨김 파일로, CA Access Control 에 의해 보호됩니다. CA Access Control 이 중지되면 superuser 만 이 암호에 액세스할 수 있습니다.

암호로 보호된 서버 인증서를 만드는 경우 sechkey 는 인증서를 암호화하지 않습니다. 암호로 보호되지 않는 서버 인증서를 만드는 경우 sechkey 는 AES256 및 CA Access Control 암호화 키를 사용하여 인증서를 암호화합니다.

메시지 큐 서버 SSL 포트 번호

CA Access Control 엔터프라이즈 관리를 설치할 때 메시지 큐 서버는 기본 SSL 통신 포트 번호를 사용하여 구성됩니다. 잘 알려진 포트를 통한 무단 액세스를 방지하기 위한 목적 등으로 CA Access Control 엔터프라이즈 관리를 설치한 이후에 이 포트 번호를 수정할 수 있습니다.

예: 메시지 큐 서버 SSL 포트 번호 수정

다음 예는 메시지 큐 서버 SSL 포트 번호를 기본 포트 번호에서 다른 번호를 변경하는 방법에 대해 설명합니다.

메시지 큐 서버 SSL 포트 번호를 수정하려면

참고: 메시지 큐 서버 설정을 수정하기 전에 모든 CA Access Control 서비스 및 데몬을 중지하십시오.

1. CA Access Control 엔터프라이즈 관리 서버에서 다음 디렉터리로 이동합니다.

   ACServer_InstallDir/AccessControlServer/MessageQueue/tibco/ems/bin

2. 편집을 위해 routes.conf 파일을 엽니다.
3. [PR_DMS_SERVER] 항목을 찾아 url 필드에서 포트 번호를 수정합니다. 예:

   url = ssl://PR_DMS_SERVER:7777

4. 편집을 위해 tibemsd.conf 파일을 엽니다.
5. 수신 포트 항목을 찾아 포트 번호를 수정합니다. 예:

   listen = ssl://7777

6. 편집을 위해 tibcoems-service.xml 파일을 엽니다.
7. <!-- The JMS provider loader --> 섹션을 찾아 java.naming.provider.url 줄에서 포트 번호를 수정합니다. 예:

   java.naming.provider.url=tibjmsnaming://localhost:7777

8. 편집을 위해 factories.conf 파일을 엽니다.

9. [SSLQueueConnectionFactory], [SSLTopicConnectionFactory], [SSLXAQueueConnectionFactory] 섹션을 찾아 url 필드에서 포트 번호를 수정합니다. 예:

```
[SSLQueueConnectionFactory]
 type              = queue
 url               = ssl://7777
 ssl_verify_host   = disabled

[SSLTopicConnectionFactory]
 type              = topic
 url               = ssl://7777
 ssl_verify_host   = disabled

[SSLXAQueueConnectionFactory]
 type              = xaqueue
 url               = ssl://7777
 ssl_verify_host   = disabled
```

10. org.jboss.naming.NamingAlias 항목을 찾아 포트 번호를 수정합니다. 예:

```
tibjmsnaming://localhost:7777
```

11. CA Access Control 서비스를 시작합니다.

    이제 메시지 큐 서버 SSL 포트 번호가 원하는 대로 수정됩니다.

동일한 암호화 키를 사용하도록 서버 구성

여러 엔터프라이즈 관리 서버를 설치하는 경우 각 서버는 자체 암호화 키를 사용하여 중앙 데이터베이스의 데이터를 암호화/암호 해독합니다. 환경에서 여러 엔터프라이즈 관리 서버를 사용하여 하나의 중앙 데이터베이스에서 데이터를 읽고 쓰는 경우 각 서버는 동일한 암호화 키를 사용해야 합니다.

중요! -DFIPS_KEY 옵션을 사용하여 보조 엔터프라이즈 관리 서버를 설치할 때 기본 엔터프라이즈 관리 서버가 사용하는 FIPS 키를 지정하지 않은 경우에만 다음 단계를 수행하십시오.

동일한 암호화 키를 사용하도록 서버를 구성하려면

1. JBoss 가 실행 중인 경우 중지합니다. 다음 작업 중 *하나*를 수행합니다.
   - JBoss Application Server 창을 인터럽트(Ctrl+C)합니다.
   - "서비스" 패널에서 "JBoss" 서비스를 중지합니다.

2. 동일한 암호화 키를 사용하도록 엔터프라이즈 관리 서버를 구성합니다. 다음과 같이 수행합니다.

   a. 기본 엔터프라이즈 관리 서버의 다음 디렉터리에서 FIPSKey.dat 파일을 복사합니다.

      JBoss_HOME/server/default/deploy/IdentityMinder.ear/config/com/netegrity/config/keys

   b. 이 디렉터리의 FIPSKey.dat 파일을 각 보조 엔터프라이즈 관리 서버에 붙여넣습니다.

      해당 이름을 사용하는 파일이 존재한다는 메시지가 나타납니다.

   c. 기존 파일을 새 파일로 덮어쓰도록 선택합니다.

      새 파일이 해당 디렉터리에 복사됩니다. 이제 각 엔터프라이즈 관리 서버가 동일한 암호화 키를 사용합니다.

3. 새 암호화 키를 사용하여 각 보조 엔터프라이즈 관리 서버에서 AES 암호를 업데이트합니다. 다음과 같이 수행합니다.

   a. 일반 텍스트 암호를 암호화합니다 (페이지 456).

   b. 각 보조 엔터프라이즈 관리 서버에서 다음 파일을 찾습니다.

      JBoss_HOME/server/default/conf/login-config.xml

      JBoss_HOME/server/default/deploy/properties-service.xml

   c. 이 파일에서 각 AES 암호를 암호화된 새 암호로 바꿉니다.

4. JBoss 를 시작합니다.

   이제 기본 및 보조 엔터프라이즈 관리 서버가 동일한 암호화 키를 사용하여 데이터를 암호화/암호 해독합니다.

예: 암호화된 AES 암호

login-config.xml 파일의 다음 조각은 암호화된 AES 암호를 나타냅니다.

```
<application-policy name="imobjectstoredb">
        <authentication>
                <login-module code="com.netegrity.jboss.datasource.PasswordEncryptedLogin"
                flag="required">
                        <module-option name="userName">user1</module-option>
                        <module-option name="password">
                        {AES}:/lxnvWwAEcYhSmOu3YT3ow==</module-option>
                        <module-option name="managedConnectionFactoryName">
                        jboss.jca:name=jdbc/objectstore,service=NoTxCM</module-option>
                </login-module>
        </authentication>
</application-policy>
```

CA Access Control 웹 서비스 URL 변경

CA Access Control 웹 서비스를 사용하여 CA Access Control 엔터프라이즈 관리 및 CA Access Control 끝점 관리에 액세스합니다. CA Access Control 웹 서비스 URL 의 형식은 HTTP:*hostname*:*port* 입니다. 예: http://entmserver:5248. 기본적으로 *hostname* 은 엔터프라이즈 관리 서버의 이름입니다.

CA Access Control 웹 서비스 URL 을 변경할 때는 IP 주소와 웹 서비스가 수신하는 포트를 변경합니다. 보안을 강화하기 위해 호스트 이름을 localhost 로 변경할 수 있습니다. 예: http://127.0.0.1:5248. localhost 를 사용하면 localhost 환경 바로 밖에서 웹 서비스를 감지할 수 없으므로 웹 서비스의 노출을 줄이는 데 도움을 줍니다.

다음 단계를 수행하십시오.

1. JBoss 및 CA Access Control 서비스가 실행 중인 경우 중지합니다.
2. 다음과 같이 URL 에서 호스트 이름을 변경합니다.
   - (Windows) WebService 레지스트리 키에서 machineName 레지스트리 값을 새 호스트 이름으로 변경합니다.
   - (Linux) seos.ini 파일의 WebService 섹션에서 machineName 구성 설정의 값을 새 호스트 이름으로 변경합니다.
3. (선택 사항) 다음과 같이 URL 에서 포트 번호를 변경합니다.
   - (Windows) WebService 레지스트리 키에서 portNumber 레지스트리 값을 새 포트 번호로 변경합니다.
   - (Linux) seos.ini 파일의 WebService 섹션에서 portNumber 구성 설정의 값을 포트 번호로 변경합니다.
4. 다음 파일을 엽니다. 여기서 *JBoss_home* 는 JBoss 를 설치한 디렉터리를 나타냅니다.

   JBoss_home/server/default/conf/webservice.properties

5. webservice.url 속성의 값을 새 호스트 이름과 포트로 변경합니다. 예:

   webservice.url=http://127.0.0.1:5248

6. 파일을 저장한 후 닫습니다.
7. CA Access Control 웹 서비스를 포함하여 CA Access Control 서비스를 다시 시작합니다.
8. JBoss 를 다시 시작합니다.

   CA Access Control 웹 서비스 URL 이 변경됩니다.

Microsoft SQL Server 데이터베이스 연결 설정 수정

Microsoft SQL 서버에 엔터프라이즈 관리 서버를 설치할 때 인증 모드가 "SQL 서버 인증"으로 설정됩니다. 설치가 완료된 이후에 Windows 인증 모드로 동작하도록 데이터베이스 인증 모드를 수정할 수 있습니다.

SQL Sever 가 Windows 인증 모드에서 실행될 때 엔터프라이즈 관리 서버는 SQL Sever 의 중앙 데이터베이스를 관리하기 위해 JBoss 서비스 계정을 사용합니다. 다른 JBoss 서비스 계정을 사용하려면 SQL Sever 데이터베이스 인스턴스의 계정도 변경합니다.

중요! SQL Sever 가 Windows 인증 모드에서 작동하도록 설정하려면 SQL Sever JDBC 2.0 드라이버를 설치해야 합니다.

중요! Microsoft SQL Server 에서 지정하는 사용자에게 dbowner 데이터베이스 역할을 할당해야 합니다.

SQL Sever 데이터베이스 연결 설정을 수정하려면

1. 이미 수행하지 않은 경우 SQL Server JDBC 2.0 드라이버 파일을 다운로드하여 임시 폴더에 압축을 해제합니다.
2. JBoss 가 실행 중인 경우 중지합니다. 다음 작업 중 하나를 수행합니다.
   - JBoss Application Server 창을 인터럽트(Ctrl+C)합니다.
   - "서비스" 패널에서 "JBoss" 서비스를 중지합니다.
3. JBoss lib 디렉터리로 이동합니다. 디렉터리는 다음 위치에 있습니다.

   JBossInstallDir/server/default/lib
4. 임시 디렉터리에서 sqljdbc.jar 파일을 JBoss lib 디렉터리로 복사합니다.

   해당 이름의 파일이 존재한다는 메시지가 나타납니다.
5. 기존 파일을 새 파일로 덮어쓰도록 선택합니다.

   새 파일이 해당 디렉터리에 복사됩니다.
6. JBoss bin 디렉터리로 이동합니다. 기본적으로 이 디렉터리는 다음 위치에 있습니다.

   JBossInstallDir/bin
7. 임시 디렉터리에서 sqljdbc_auth.dll 파일을 JBoss bin 디렉터리로 복사합니다.

   새 파일이 해당 디렉터리에 복사됩니다.

8. JBoss deploy 디렉터리로 이동합니다. 기본적으로 이 디렉터리는 다음 위치에 있습니다.

   JBoss-directory/server/default/deploy

9. 다음 파일을 엽니다.
   - imauditdb-ds.xml
   - imtaskpersistencedb-ds.xml
   - imworkflowdb-ds.xml
   - objectstore-ds.xml
   - reportsnapshot-ds.xml

10. 각 파일에서 <connection-url> 태그를 찾아 DatabaseName= parameter 뒤에 다음을 추가합니다.

    ;integratedSecurity=true

11. 각 파일에서 <security-domain> 태그를 삭제합니다.

12. 파일을 저장하고 JBoss 를 다시 시작합니다.

    CA Access Control 엔터프라이즈 관리는 이제 Windows 인증 모드에서 SQL Server 와 작업할 수 있습니다.

예: Windows 인증 모드를 사용하기 위해 JBoss 구성 파일 수정

이 예는 SQL 인증 모드에서 Windows 인증 모드로 전환하기 위해 JBoss 구성 파일 중 하나를 수정하는 방법을 설명합니다. 이 예에서 관리자가 objectstore-ds.xml 파일을 수정하고 연결 모드를 Windows 인증(;integratedSecurity=true)으로 지정합니다. 그런 다음, 관리자가 파일에서 <security-domain> 태그를 제거합니다. 이 태그는 SQL 인증 모드에서만 사용할 수 있으므로 제거합니다.

다음은 관리자가 연결 설정을 수정한 이후 objectsstore-ds.xml 파일의 모습입니다.

```
<connection-url>jdbc:sqlserver://example.comp.com:1433;
selectMethod=cursor;DatabaseName=ACDB;
integratedSecurity=true</connection-url>
```

보고서 포털을 위한 Windows 인증 구성

Windows 에 해당

보고서 포털(CA Business Intelligence)을 설치하고 CMS 데이터베이스로 Microsoft SQL Server 를 선택하는 경우, 인증 모드는 SQL Server 인증으로 설정됩니다. Microsoft SQL Server 인증은 SQL 사용자 계정을 사용하여 데이터베이스 연결을 인증합니다.

조직에서 Active Directory 를 사용하는 경우 인증 방법을 Windows 인증으로 수정할 수 있습니다. Windows 인증에서 CMS 데이터베이스에 대한 연결은 로컬 사용자 계정이 아닌 도메인 사용자 계정을 사용하여 인증됩니다.

Windows 인증에서 연결을 인증하면 모든 보고서 포털 구성 요소 사이의 통신 보안을 강화합니다. 사용자 자격 증명을 포함하는 데이터베이스에 대한 ODBC 연결을 구성하므로 보고서 포털에 배포하는 보고서 패키지에서 일반 텍스트 암호를 제거할 수 있습니다.

중요! Windows 인증을 사용하려면 Internet Information Server(IIS)와 Microsoft SQL Server 가 필요합니다.

Windows 인증에서 작업하기 위해 보고서 포털을 구성하는 방법

보고서 포털 데이터베이스 연결 인증 모드를 수정하기 위해 수행하는 단계를 이해하면 Windows 인증에서 보고서 포털을 구현할 때 도움이 됩니다.

Windows 인증을 위한 보고서 포털을 구성하려면 다음을 수행하십시오.

1. CMS 데이터베이스로 사용할 Microsoft SQL Server 2005 데이터베이스를 준비합니다.
2. 기본 사용자 및 데이터 정렬(collation)을 사용하여 CA Business Intelligence CMS 데이터베이스를 준비합니다.
3. 시스템 DSN 을 만들고 SQL Server 인증을 사용하도록 지정합니다.

   보고서 포털 CMS 데이터베이스에 연결하기 위해 시스템 DSN 이 사용됩니다.
4. Active Directory 사용자를 로컬 Administrators 그룹에 추가합니다.

   Windows 인증에서 작업하도록 보고서 포털을 구성할 때 이 사용자를 인증하도록 지정합니다.

5. ASP.NET 웹 서비스 확장이 허용되도록 설정합니다.
6. 보고서 포털CA Business Intelligence (페이지 100)을 설치합니다. 설치 중 다음을 수행하십시오.
    a. 사용자 지정 모드로 CA Business Intelligence 를 설치하도록 선택합니다.
    b. Microsoft SQL Server 2005 를 데이터베이스로 지정합니다.
    c. IIS 를 웹 서버로 지정합니다.
7. Windows 인증에 대해 보고서 포털을 구성합니다.

    Windows 인증에서 인증하기 위해 Active Directory 사용자 계정을 사용하도록 CA Business Intelligence 서비스를 구성합니다.
8. Windows 인증을 사용하여 CA Access Control 보고 데이터베이스에 대한 시스템 DSN 을 만듭니다.

    CA Access Control 보고 포털에 연결하기 위해 시스템 DSN 이 사용됩니다.
9. 보고서 포털에 보고서 패키지를 배포합니다.

Windows 인증을 위한 보고서 포털 구성

보고서 포털을 설치한 다음에는 Windows 인증에서 작업하도록 보고서 포털을 구성할 수 있습니다. Active Directory 사용자 계정을 사용하도록 보고서 포털을 구성하고 시스템 DSN 연결 매개 변수를 수정합니다.

Windows 인증을 위한 보고서 포털을 구성하려면

1. 운영 체제 관리자로 보고서 포털 호스트에 로그인합니다.
2. 보고서 포털 CMS 에 대한 시스템 DSN 을 Windows NT 인증으로 수정합니다.
3. "시작", "프로그램", "BusinessObjects XI Release 2", "Business Objects Enterprise", "Central Configuration Manager"를 차례로 선택합니다.

   Central Configuration Manager 가 열리고 CA Business Intelligence 서비스가 표시됩니다.
4. 모든 CA Business Intelligence 서비스를 중지합니다.
5. 서비스 "Log On As" 설정을 Active Directory 사용자 자격 증명으로 수정합니다. 모든 CA Business Intelligence 서비스에 대해 이 작업을 수행하십시오.

   중요! "WinHTTP Web Proxy Auto-Discovery" 및 "World Wide Web Publishing" 서비스의 설정을 변경합니다.
6. 모든 CA Business Intelligence 서비스를 시작합니다.

   보고서 포털이 이제 Windows 인증에서 인증하도록 구성되었습니다.

   참고: Microsoft SQL Server 작업 모니터에서 보고 데이터베이스에 대한 연결이 Active Directory 사용자 계정을 사용함을 확인할 수 있습니다.

예: CA Business Intelligence 서비스 "Log On As" 연결 설정 수정

다음 예는 CA Business Intelligence 연결 서버 서비스 "Log On As" 자격 증명을 시스템 계정에서 Active Directory 계정으로 수정하는 방법을 설명합니다.

1. 목록에서 "Connection Server" 서비스를 마우스 오른쪽 단추로 클릭하고 "Properties"를 선택합니다.

   "Connection Server" 서비스 속성 창이 열립니다.

2. "Log On As" 섹션에서 "System Account" 옵션의 표시를 제거합니다.

   연결 설정 필드가 활성화됩니다.

3. Active Directory 사용자 이름, 암호를 입력하고 암호를 확인합니다.

   예: Domain/username

   "확인"을 클릭합니다. 서비스 연결 설정이 변경되었습니다.

4. Central Configuration Manager 를 종료합니다.

시스템 DSN 연결 구성 예제

시스템 DSN 연결 설정은 데이터베이스에 연결하기 위해 필요한 매개 변수를 정의합니다. 다음 예에서는 보고서 포털이 설치되었을 때 SQL 인증만 지원하므로 SQL Server 서버 인증에서 사용자 연결을 인증하는 시스템 DSN 을 만듭니다. CA Business Intelligence 를 설치하기 전에 CMS 데이터베이스 시스템 DSN 을 구성합니다.

다음 예에서는 보고서 포털 CMS 데이터베이스에 대한 시스템 DSN 을 만듭니다.

1. "시작", "설정", "제어판", "관리 도구", "데이터 원본 (ODBC)"를 차례로 선택합니다.

   ODBC 데이터 원본 관리자가 열립니다.

2. "시스템 DSN" 탭에서 "만들기"를 선택합니다.

   "새 데이터 원본 선택" 창이 열립니다.

3. 아래로 스크롤하여 "SQL Server"를 선택한 다음 "마침"을 클릭합니다.

   "SQL Server 에 새로운 데이터 원본 만들기" 마법사가 열립니다.

4. 연결 이름, 설명, SQL 서버 이름을 입력합니다. "다음"을 클릭합니다.
5. SQL Server 인증을 사용하도록 선택합니다.
6. SQL 서버에 연결하기 위한 administrator 사용자 자격 증명을 입력합니다. "다음"을 클릭합니다.
7. "기본 데이터베이스를 다음으로 변경" 옵션을 선택하고 목록에서 보고서 포털 CMS 데이터베이스를 선택합니다. "다음"을 클릭합니다.
8. "마침"을 클릭합니다. 연결을 테스트하도록 선택하고 "확인"을 클릭합니다.

   시스템 DSN 이 생성되었습니다.

Windows 인증에서 작업하는 보고서 포털에 보고서 패키지 배포

Windows 에 해당

이러한 표준 CA Access Control 보고서를 사용하려면 보고서 패키지 파일을 BusinessObjects InfoView 로 가져와야 합니다.

참고: 이 절차는 동일한 패키지의 이전 버전이 이미 배포되지 않은 경우 보고서 포털에서 보고서 패키지를 배포하는 방법을 설명합니다.

보고서 포털에 보고서 패키지를 배포하려면

1. 중앙 데이터베이스, 배포 서버, 보고서 포털이 설정되었는지 확인합니다.

   참고: 보고서 포털 컴퓨터에서 JAVA_HOME 변수가 설정되었는지 확인합니다.

2. CA Access Control 보고 데이터베이스에 대한 시스템 DSN 을 만들고 Windows NT 인증을 사용하도록 지정합니다.

   만드는 시스템 DSN 은 CA Access Control 보고 데이터베이스에 연결하는 데 사용됩니다. 보고서 패키지를 구성할 때 시스템 DSN 을 지정합니다.

3. Windows 용 CA Business Intelligence DVD 를 광 디스크 드라이브에 넣고 \Disk1\cabi\biconfig 폴더로 이동합니다.

4. biconfig 디렉터리의 내용을 임시 디렉터리로 복사합니다.
5. 광학 디스크 드라이브에 사용하는 운영 체제용의 적절한 CA Access Control Premium Edition 서버 구성 요소 DVD 를 넣은 다음 \ReportPackages 폴더로 이동합니다.
6. 광학 디스크에서 동일한 임시 디렉터리로 다음 파일을 복사합니다.
   - \ReportPackages*RDBMS**import_biar_config*.xml
   - \ReportPackages*RDBMS**AC_BIAR_File*.biar

   RDBMS

   CA Access Control 보고에 사용되는 RDBMS 의 유형을 정의합니다.

   값: MSSQL2005

   ***import_biar_config*.xml**

   사용하는 RDBMS 에 대한 가져오기 구성 파일(.xml)의 이름을 정의합니다.

   값: import_biar_config_mssql_2005.xml

   참고: 중앙 데이터베이스로 MS SQL Server 2008 을 사용하는 경우 import_biar_config_mssql_2005.xml 파일을 구성하십시오.

   ***AC_BIAR_File*.biar**

   해당 언어 및 RDBMS 의 CA Access Control 보고서 파일(.biar) 이름을 정의합니다.

   참고: 사용하는 RDBMS 에 대한 가져오기 구성 파일의 <biar-file name> 속성은 이 파일을 가리킵니다. 이 속성은 기본적으로 사용하는 RDBMS 의 영어 버전 이름으로 설정되어 있습니다.
7. *import_biar_config*.xml 파일의 사본을 편집합니다. 다음 XML 속성을 정의합니다.

   중요! 파일에서 사용자 이름, 암호, 서버 필드를 제거하십시오.

   <biar-file name>

   CA Access Control 보고서 파일(.biar)에 대한 전체 경로 이름을 정의합니다. 이 파일은 이전 단계에서 복사한 파일입니다.

   <networklayer>

   사용하는 RDBMS 에서 지원하는 네트워크 계층을 정의합니다.

   값: ODBC

<rdms>

CA Access Control 보고에 사용되는 RDBMS 의 유형을 정의합니다.

값: 일반 ODBC 데이터 원본

<datasource>

만든 DSN 을 정의합니다.

중요! CA Business Intelligence CMS 가 아니라 보고를 위해 CA Access Control 이 사용하는 데이터베이스의 이름을 지정하십시오.

8. 명령 프롬프트 창을 열고 다음 명령을 입력합니다.

System_Drive:\BO\biconfig.bat -h *host_name* -u *user_name* -p *password* -f *ac_biar_config*.xml

host_name

보고서 포털 호스트 이름을 정의합니다.

user_name

보고서 포털을 설치할 때 구성한 보고서 포털 관리자를 정의합니다.

password

보고서 포털 관리자의 암호를 정의합니다.

예:

biconfig.bat -h reportportal.comp.com -u Administrator -p P@ssw0rd -f C:\BO\import_biar_config_mssql_2005.xml

예: Windows 인증을 사용하도록 구성된 예제 Microsoft SQL Server 2005 가져오기 구성 파일

다음 코드 조각은 Windows 인증에서 작업하는 보고서 포털에 배포하는 MS SQL Server 2005 에 대한 편집된 가져오기 구성 파일(import_biar_config_mssql2005.xml)의 예제입니다.

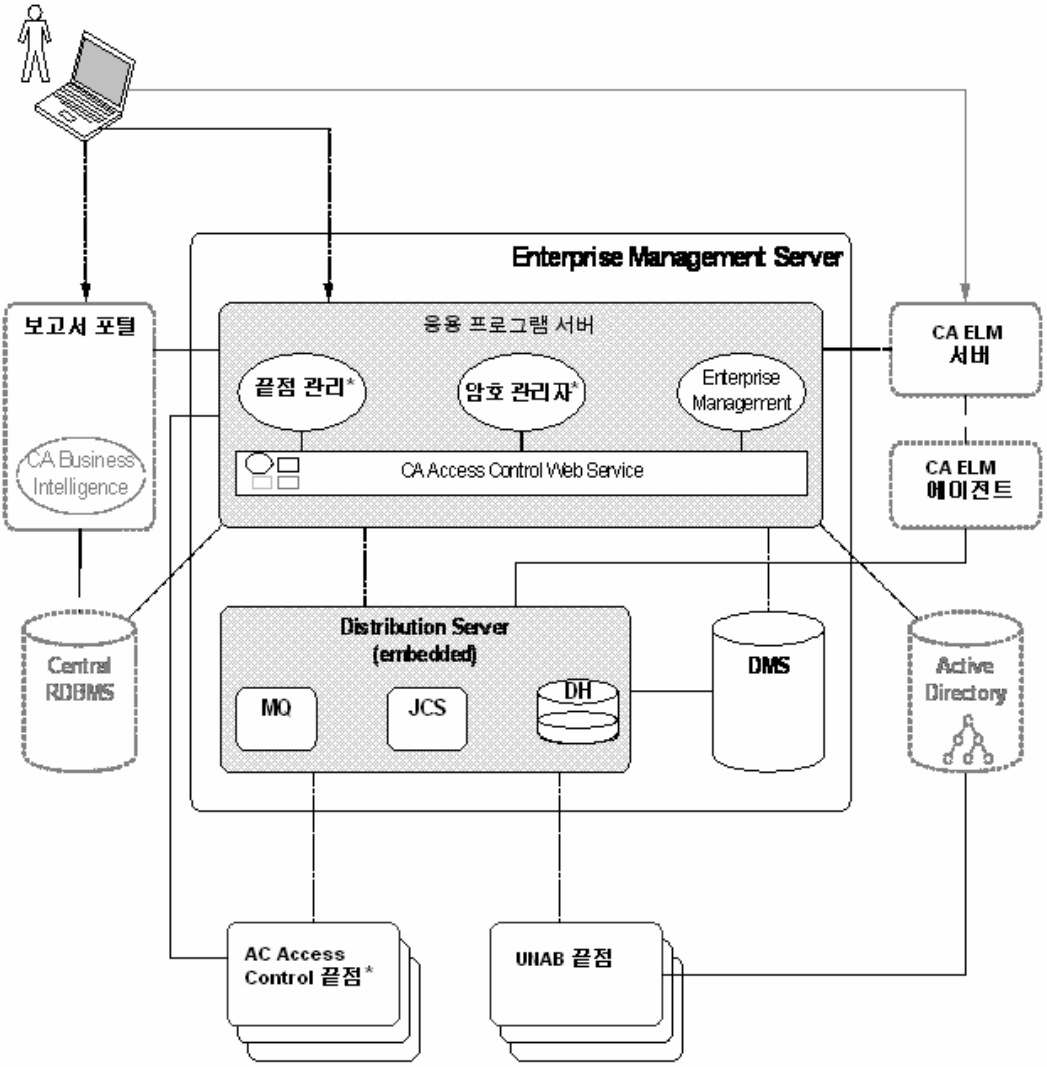
```
<?xml version="1.0"?>
<biconfig version="1.0">
        <step priority="1">
                <add>
                        <biar-file name="c:\temp\biconfig\
                        AccessControl_R12.5_EN_JP_KR_SQL_6_DEC_2009.biar">
                                <networklayer>ODBC</networklayer>
                                <rdms>Generic ODBC datasource</rdms>
                                <datasource>acdb</datasource>
                        </biar-file>
                </add>
        </step>
</biconfig>
```

부록 B: CA Access Control 서비스 계정 설정 변경

이 섹션은 다음 항목을 포함하고 있습니다.

CA Access Control 서비스 계정이 CA Access Control 구성 요소와 상호 작용하는 방법

다음 다이어그램은 서비스 계정이 여러 CA Access Control 구성 요소와 상호 작용하는 방법을 보여줍니다.



다이어그램에 있는 번호는 다음 서비스 계정에 해당합니다.

1. RDBMS_service_user

   이 계정은 엔터프라이즈 관리 서버와 RDMBS 사이의 통신을 인증합니다.

   참고: 이 계정은 RDBMS_service_user 로 명명되지 않습니다. 이 계정의 이름은 CA Access Control 엔터프라이즈 관리에 대한 데이터베이스를 준비하기 위해 사용자를 만들 때 지정합니다.

2. guest

   이 계정은 메시지 큐 서버에서 메시지 큐를 찾는 JNDI 연결 계정입니다.

   참고: 설치 후에 JNDI 연결 계정을 변경할 수 있습니다.

3. reportserver

   이 계정은 DMS 및 CA Access Control 엔터프라이즈 관리가 메시지 큐에 로그인할 수 있게 해 줍니다.

4. +reportagent

   이 계정은 끝점이 메시지 큐에 로그인할 수 있게 해 줍니다.

5. +policyfetcher

   이 계정은 끝점에서 policyfetcher 데몬 또는 서비스를 실행합니다.

6. +devcalc

   이 계정은 끝점에서 정책 위반 계산을 실행합니다.

7. ac_entm_pers

   이 계정은 엔터프라이즈 관리 서버와 DMS 사이의 통신을 인증합니다.

8. ADS_LDAP_bind_user

   이 계정은 CA Access Control 엔터프라이즈 관리가 Active Directory 에서 LDAP 쿼리를 수행할 수 있게 해 줍니다.

   참고: 이 계정은 ADS_LDAP_bind_user 로 명명되지 않습니다. 이 계정의 이름은 CA Access Control 엔터프라이즈 관리를 설치할 때 Active Directory 설정 마법사 페이지에서 지정하는 사용자 DN 입니다.

서비스 계정 암호

대부분의 경우 CA Access Control 엔터프라이즈 관리를 설치할 때 CA Access Control 서비스 계정에 대한 암호를 설정합니다. 하지만 설치 후에 이러한 계정의 암호를 변경해야 할 수 있습니다. 예를 들어, 회사의 보안 또는 암호 정책에 따라 암호를 매년 변경해야 할 수 있습니다.

서비스 계정이 두 개의 CA Access Control 구성 요소와 상호 작용하는 경우 각 구성 요소의 계정에 대한 암호를 변경해야 합니다. 하나의 구성 요소에서만 암호를 변경하는 경우 서비스 계정은 다른 구성 요소에 로그인할 수 없습니다.

RDBMS_service_user 암호 변경

RDBMS_service_user 계정은 엔터프라이즈 관리 서버와 RDBMS 사이의 통신을 인증합니다. 이 계정은 RDBMS_service_user 로 명명되지 않습니다. 이 계정은 CA Access Control 엔터프라이즈 관리에 대한 데이터베이스를 준비할 때 만들며, CA Access Control 엔터프라이즈 관리를 설치할 때 다른 데이터베이스 정보와 함께 계정 이름과 암호를 제공합니다.

조직의 보안 및 암호 정책에 따라 RDBMS_service_user 암호를 정기적으로 변경해야 할 수 있습니다. 암호는 엔터프라이즈 관리 서버 및 RDBMS 에서 모두 변경해야 합니다.

이 계정의 암호를 변경하기 전에 다음 사항에 주의하십시오.

- 이 계정의 기본 암호는 사용자를 만들 때 지정한 암호입니다.
- 이 암호는 다음과 같은 제한이 있습니다.
  - 길이는 1-50 자여야 합니다.
  - 높은 ASCII 문자를 포함할 수 없습니다.
  - 큰따옴표("")를 포함할 수 없습니다.
  - RDBMS 암호 규칙을 따라야 합니다.
- 암호는 다음 XML 파일에 저장됩니다. *JBoss_home* 은 JBoss 를 설치한 디렉터리입니다.

  JBoss_home/server/default/conf/login-config.xml

RDBMS_service_user 암호를 변경하려면

1. 데이터베이스 도구를 사용하여 암호를 변경합니다.

   참고: 암호를 변경하는 방법에 대한 자세한 내용은 MS SQL 또는 Oracle 설명서를 참조하십시오.

2. 엔터프라이즈 관리 서버에서 암호를 변경합니다.

   a. JBoss Application Server 를 중지합니다.

   b. 일반 텍스트 암호를 암호화합니다 (페이지 456).

   c. login-config.xml 파일에서 암호를 변경합니다 (페이지 458).

   d. JBoss Appplication Server 를 다시 시작합니다.

   e. CA Access Control 엔터프라이즈 관리에 로그인할 수 있는지 확인합니다.

      JBoss 가 성공적으로 시작되고 암호가 엔터프라이즈 관리 서버에서 변경됩니다.

   RDBMS_service_user 암호가 모든 위치에서 변경됩니다.

예: login-config.xml 파일에서 암호 변경

login-config.xml 파일의 이 조각은 변경된 RDMBS_service_user 암호의 한 인스턴스를 보여 줍니다. 사용자 이름은 caidb01 입니다.
암호는 }>8:Jt^+%INK&i^v 이며 암호화되었습니다.

```
<application-policy name="imobjectstoredb">
        <authentication>
                <login-module code="com.netegrity.jboss.datasource.PasswordEncryptedLogin"
                flag="required">
                        <module-option name="userName">caidb01</module-option>
                        <module-option name="password">
                        {AES}:}>8:Jt^+%INK&i^v==</module-option>
                        <module-option name="managedConnectionFactoryName">
                        jboss.jca:name=jdbc/objectstore,service=NoTxCM</module-option>
                </login-module>
        </authentication>
</application-policy>
```

reportserver 암호 변경

CA Access Control 엔터프라이즈 관리 및 DMS 는 reportserver 계정을 사용하여 메시지 큐에 연결합니다.

CA Access Control 엔터프라이즈 관리는 reportserver 계정을 사용하여 다음을 수행합니다.

- 보고 데이터를 CA Enterprise Log Manager 에 보냅니다.
- UNAB 원격 마이그레이션 명령을 보냅니다.
- PUPM 끝점의 PUPM 에이전트에 권한 있는 계정 암호를 제공합니다.
- CA Access Control 끝점에서 보고 데이터를 받습니다.

DMS 는 reportserver 계정을 사용하여 다음을 수행합니다.

- UNAB 정책을 UNAB 끝점에 보냅니다.
- UNAB 끝점에서 보낸 정책 배포 상태 정보를 받습니다.

조직의 보안 및 암호 정책에 따라 reportserver 암호를 정기적으로 변경해야 할 수 있습니다. 배포 서버, 엔터프라이즈 관리 서버, DMS 에서 암호를 변경해야 합니다.

reportserver 암호를 변경하기 전에 다음 사항에 주의하십시오.

- 이 계정의 기본 암호는 CA Access Control 엔터프라이즈 관리를 설치할 때 지정하는 통신 암호입니다.
- 이 암호는 다음과 같은 제한이 있습니다.
  - 길이는 1–240 자여야 합니다.
  - 높은 ASCII 문자를 포함할 수 없습니다.
  - 큰따옴표("")를 포함할 수 없습니다.
- 암호는 메시지 큐와 다음 XML 파일에 저장됩니다. *JBoss_home* 은 JBoss 를 설치한 디렉터리입니다.
  - *JBoss_home*/server/default/deploy/properties-service.xml
  - *JBoss_home*/server/default/conf/login-config.xml

중요! 회사에 여러 대의 배포 서버가 있는 경우 엔터프라이즈 관리 서버에 설치된 배포 서버에서 암호를 먼저 변경한 다음 다른 배포 서버에서 암호를 변경하십시오.

reportserver 암호를 변경하려면

1. 배포 서버에서 reportserver 사용자에 대한 메시지 큐 암호를 설정 (페이지 454)합니다.

   배포 서버에서 reportserver 암호를 변경했습니다.

2. 다음과 같이 엔터프라이즈 관리 서버에서 암호를 변경합니다.

   a. JBoss Application Server 를 중지합니다.

   b. 일반 텍스트 암호를 암호화합니다 (페이지 456).

   c. properties-service.xml 파일에서 암호를 변경합니다 (페이지 457).

   d. login-config.xml 파일에서 암호를 변경합니다 (페이지 458).

   e. JBoss Application Server 를 다시 시작합니다.

   f. CA Access Control 엔터프라이즈 관리에 로그인할 수 있는지 확인합니다.

      JBoss 가 성공적으로 시작되고 엔터프라이즈 관리 서버의 암호가 변경됩니다.

3. sechkey 를 사용하여 DMS 에서 reportserver 암호를 변경합니다 (페이지 452).

   reportserver 암호가 모든 위치에서 변경됩니다.

예: reportserver 사용자에 대한 메시지 큐 암호 설정

이 Tibco EMS Administration Tool 명령은 reportserver 사용자에 대한 메시지 큐 암호를 설정합니다. 암호는 "secret"이며, 큰따옴표로 둘러싼 일반 텍스트여야 합니다.

```
ssl://localhost:7243> set password reportserver "secret"
사용자 'reportserver'의 암호가 수정되었습니다.
ssl://localhost:7243>
```

예: properties-service.xml 파일에서 암호 변경

properties-service.xml 파일의 이 조각은 변경된 reportserver 암호를 보여줍니다. 암호는 }>8:Jt^+%INK&i^v 이며 암호화되었습니다.

```
<attribute name="Properties">
        SamMDB.mdb-user=reportserver
        <!-- encoded tibco password -->
        SamMDB.mdb-passwd={AES}:}>8:Jt^+%INK&i^v==
</attribute>
```

예: login-config.xml 파일에서 암호 변경

login-config.xml 파일의 이 조각은 변경된 reportserver 암호를 보여 줍니다. 암호는 }>8:Jt^+%INK&i^v 이며 암호화되었습니다.

```
<application-policy name="JmsXATibcoRealm">
    <authentication>
      <login-module code="com.netegrity.jboss.datasource.PasswordEncryptedLogin" flag="required">
        <module-option name="userName">reportserver</module-option>
              <module-option name="password">{AES}:}>8:Jt^+%INK&i^v==</module-option>
                    <module-option name="managedConnectionFactoryName">
                    jboss.jca:service=TxCM,name=TibcoJmsXA</module-option>
      </login-module>
    </authentication>
  </application-policy>
```

예: sechkey 를 사용하여 DMS 에서 메시지 큐 암호 변경

이 명령은 DMS 에서 메시지 큐 암호를 변경합니다. 암호는 "secret"이며, 큰따옴표로 둘러싼 일반 텍스트여야 합니다.

```
sechkey -t -server -pwd "secret"
```

+reportagent 암호 변경

+reportagent 계정은 끝점이 메시지 큐에 로그인할 수 있게 해 줍니다. 각 끝점에서 UNAB 에이전트, PUPM 에이전트, 보고서 에이전트는 이 계정을 사용하여 메시지 큐와 통신합니다.

조직의 보안 및 암호 정책에 따라 +reportagent 암호를 정기적으로 변경해야 할 수 있습니다. 메시지 큐와 끝점 모두에서 암호를 변경합니다.

+reportagent 암호를 변경하기 전에 다음 사항에 주의하십시오.

- 기본 암호는 CA Access Control 엔터프라이즈 관리를 설치할 때 지정하는 통신 암호입니다.
- 이 암호는 다음과 같은 제한이 있습니다.
  - 길이는 1–240 자여야 합니다.
  - 높은 ASCII 문자를 포함할 수 없습니다.
  - 큰따옴표("")를 포함할 수 없습니다.
- 암호는 끝점(seosdb)의 CA Access Control 데이터베이스 및 메시지 큐에 저장됩니다.

중요! 회사에 여러 대의 배포 서버가 있는 경우 엔터프라이즈 관리 서버에 설치된 배포 서버에서 암호를 먼저 변경한 다음 다른 배포 서버에서 암호를 변경하십시오. 메시지 큐는 배포 서버의 일부입니다.

+reportagent 암호를 변경하려면

1. 배포 서버에서 +reportagent 사용자에 대한 메시지 큐 암호를 설정 (페이지 454)합니다.

   +reportagent 암호가 메시지 큐에서 변경됩니다.

2. ReportAgent 가 끝점의 메시지 큐에 연결하는 데 사용하는 암호를 변경하려면 sechkey 를 사용 (페이지 452)하십시오.

   변경된 +reportagent 암호는 끝점에 전파됩니다.

   참고: selang 을 사용하여 끝점에서 +reportagent 암호를 변경할 수도 있습니다. 하지만 사용자 암호를 설정하기 위해 고급 정책 관리를 사용할 수 없으므로 selang 명령을 전파하기 위해 정책을 사용할 수 없습니다.

예: +reportagent 사용자에 대한 메시지 큐 암호 설정

이 Tibco EMS Administration Tool 명령은 +reportagent 사용자에 대한 메시지 큐 암호를 설정합니다. 암호는 "secret"이며, 큰따옴표로 둘러싼 일반 텍스트여야 합니다.

```
ssl://localhost:7243> set password +reportagent "secret"
사용자 '+reportagent'의 암호가 수정되었습니다.
ssl://localhost:7243>
```

예: sechkey 를 사용하여 끝점에서 메시지 큐 암호 변경

이 명령은 +reportagent 사용자에 대한 메시지 큐 암호를 배포 서버에 구독된 끝점에 전파합니다. 암호는 "secret"이며, 큰따옴표로 둘러싼 일반 텍스트여야 합니다.

```
sechkey -t -pwd "secret"
```

+policyfetcher 암호 변경

+policyfetcher 계정은 DH 에서 배포 작업을 찾는 policyfetcher 데몬 또는 서비스를 실행하고, 정책 업데이트를 로컬 CA Access Control 데이터베이스(seosdb)에 적용하고, 일정 간격으로 DH 에 하트비트를 보냅니다. CA Access Control 은 SPECIALPGM 규칙을 사용하여 +policyfetcher 를 시스템 사용자로 정의합니다. +policyfetcher 는 Windows 에서 NT Authority\System 사용자로 실행됩니다.

조직의 보안 및 암호 정책에 따라 +policyfetcher 암호를 정기적으로 변경해야 할 수 있습니다.

+policyfetcher 암호를 변경하기 전에 다음 사항에 주의하십시오.

- 이 계정에 대한 기본 암호는 없습니다. CA Access Control 은 설치 중 +policyfetcher 에 대한 암호를 설정하지 않습니다.
- 이 암호는 다음과 같은 제한이 있습니다.
  - 길이는 1–240 자여야 합니다.
  - 높은 ASCII 문자를 포함할 수 없습니다.
  - 큰따옴표("")를 포함할 수 없습니다.
- 암호는 로컬 CA Access Control 데이터베이스인 seosdb 에 저장됩니다.

중요! 이 사용자가 CA Access Control 데이터베이스에 로그인할 수 없도록 하려면 이 사용자에 대한 암호를 설정하지 않는 것이 좋습니다.

+policyfetcher 암호를 변경하려면 selang 을 사용하여 암호를 변경 (페이지 451)하십시오.

예: +policyfetcher 암호 변경

이 명령은 +policyfetcher 사용자에 대한 암호를 변경합니다. 암호는 "secret"이며, 큰따옴표로 둘러싼 일반 텍스트여야 합니다.

```
AC> cu +policyfetcher password("secret") grace- nonative
(localhost)
USER +policyfetcher 를 성공적으로 업데이트했습니다.
```

+devcalc 암호 변경

+devcalc 계정은 정책 위반 계산을 실행합니다. 이 계산은 (정책 배포의 결과로) 끝점에 배포될 예상된 액세스 규칙과 동일한 끝점에 성공적으로 배포된 실체 규칙의 차이를 계산합니다. CA Access Control 은 SPECIALPGM 규칙을 사용하여 +devcalc 를 시스템 사용자로 정의합니다. +devcalc 는 Windows 에서 NT Authority\System 사용자로 실행됩니다.

조직의 보안 및 암호 정책에 따라 +devcalc 암호를 정기적으로 변경해야 할 수 있습니다.

+devcalc 암호를 변경하기 전에 다음 사항에 주의하십시오.

- 이 계정에 대한 기본 암호는 없습니다. CA Access Control 은 설치 중 +devcalc 에 대한 암호를 설정하지 않습니다.
- 이 암호는 다음과 같은 제한이 있습니다.
  - 길이는 1–240 자여야 합니다.
  - 높은 ASCII 문자를 포함할 수 없습니다.
  - 큰따옴표("")를 포함할 수 없습니다.
- 암호는 로컬 CA Access Control 데이터베이스인 seosdb 에 저장됩니다.

중요! 이 사용자가 CA Access Control 데이터베이스에 로그인할 수 없도록 하려면 이 사용자에 대한 암호를 설정하지 않는 것이 좋습니다.

+devcalc 암호를 변경하려면 selang 을 사용하여 암호를 변경 (페이지 451)하십시오.

예: +devcalc 암호 변경

이 명령은 +devcalc 사용자에 대한 암호를 변경합니다. 암호는 "secret"이며, 큰따옴표로 둘러싼 일반 텍스트여야 합니다.

```
AC> cu +devcalc password("secret") grace- nonative
(localhost)
USER +devcalc 를 성공적으로 업데이트했습니다.
```

ac_entm_pers 암호 변경

ac_entm_pers 계정은 DMS 와 엔터프라이즈 관리 서버 사이의 통신을 인증합니다.

조직의 보안 및 암호 정책에 따라 ac_entm_pers 암호를 정기적으로 변경해야 할 수 있습니다. RDBMS 및 DMS 모두에서 암호를 변경해야 합니다.

ac_entm_pers 암호를 변경하기 전에 다음을 고려하십시오.

- 기본 암호는 설치 중 CA Access Control 이 임의로 생성한 암호입니다.
- 이 암호는 다음과 같은 제한이 있습니다.
  - 길이는 1-48 자여야 합니다.
  - 큰따옴표("")를 포함할 수 없습니다.
  - 높은 ASCII 문자를 포함할 수 없습니다.
- 암호는 RDBMS 및 DMS 에 저장됩니다.

ac_entm_pers 암호를 변경하려면

1. selang 을 사용하여 DMS 에서 ac_entm_pers 암호를 변경합니다 (페이지 451).
2. CA Access Control 엔터프라이즈 관리에서 DMS 에 대한 연결을 구성하고 새 암호를 지정합니다.

   ac_entm_pers 암호가 모든 위치에서 변경됩니다.

   참고: DMS 에 대한 연결을 구성하는 방법에 대한 자세한 내용은 *CA Access Control 엔터프라이즈 관리 온라인 도움말*을 참고하십시오.

예: selang 을 사용하여 ac_entm_pers 암호 변경

이 명령은 DMS 에 연결하고 ac_entm_pers 사용자에 대한 암호를 변경합니다. 암호는 "secret"이며, 큰따옴표로 둘러싼 일반 텍스트여야 합니다.

```
AC> host DMS__@example.com
(DMS__@example.com)
연결했습니다.
AC> cu ac_entm_pers password("secret") grace- nonative
(localhost)
USER ac_entm_per 를 성공적으로 업데이트했습니다.
```

ADS_LDAP_bind_user 암호 변경

ADS_LDAP_bind_user 계정은 CA Access Control 엔터프라이즈 관리가 Active Directory 에서 LDAP 쿼리를 수행할 수 있게 해 줍니다. 이 계정은 ADS_LDAP_bind_user 로 명명되지 않습니다. 이 계정의 이름은 CA Access Control 엔터프라이즈 관리를 설치할 때 Active Directory 설정 마법사 페이지에서 지정하는 사용자 DN 입니다.

조직의 보안 및 암호 정책에 따라 ADS_LDAP_bind_user 암호를 정기적으로 변경해야 할 수 있습니다. Active Directory 및 RDBMS 모두에서 암호를 변경해야 합니다.

ADS_LDAP_bind_user 암호를 변경하기 전에 다음 사항에 주의하십시오.

- 기본 암호는 CA Access Control 엔터프라이즈 관리를 설치할 때 Active Directory 설정 마법사에서 지정한 암호입니다.
- 이 암호는 다음과 같은 제한이 있습니다.
  - 길이는 7-120 자여야 합니다.
  - 높은 ASCII 문자를 포함할 수 없습니다.
  - 콜론(:)은 사용할 수 없습니다.
  - Active Directory 암호 규칙을 따라야 합니다.
- 암호는 Active Directory 및 RDBMS 에 저장됩니다.

ADS_LDAP_bind_user 암호를 변경하려면

1. Active Directory 도구를 사용하여 Active Directory 에서 암호를 변경합니다.

   참고: 암호를 변경하는 방법에 대한 자세한 내용은 Active Directory 설명서를 참조하십시오.

2. CA Identity Manager 관리 콘솔에서 사용자 디렉터리 암호를 변경합니다 (페이지 460).

   ADS_LDAP_bind_user 암호가 모든 위치에서 변경됩니다.

JNDI 연결 계정 변경

JNDI 연결 계정의 이름은 guest 가 되며 메시지 큐 서버에서 메시지 큐를 찾습니다. 기본적으로 이 계정에는 암호가 없습니다.

JNDI 가 메시지 큐 서버에서 메시지 큐를 찾는 데 사용하는 계정을 변경할 수 있습니다. 이 계정의 이름은 메시지 큐와 다음 XML 파일에 저장됩니다. *JBoss_home* 은 JBoss 를 설치한 디렉터리입니다.

JBoss_home/server/default/deploy/jms/tibco-jms-ds.xml

JNDI 연결 계정을 변경하려면

1. 메시지 큐 사용자를 만듭니다.
2. 다음과 같이 JNDI 연결 계정을 변경합니다.
   a. JBoss Application Server 를 중지합니다.
   b. tibco-jms-ds.xml 파일에서 계정 이름을 앞에서 만든 메시지 큐 사용자의 이름으로 대체합니다.
   c. JBoss Application Server 를 다시 시작합니다.
   d. CA Access Control 엔터프라이즈 관리에 로그인할 수 있는지 확인합니다.

      JBoss 가 성공적으로 시작되고 JNDI 연결 계정이 변경됩니다.

메시지 큐 사용자 만들기

JNDI 연결 계정을 변경할 때 메시지 큐 사용자를 만듭니다.

메시지 큐 사용자를 만들려면

1. 다음 디렉터리로 이동합니다. 여기서 *DistServer* 는 배포 서버를 설치한 디렉터리를 나타냅니다.

   DistServer/MessageQueue/tibco/ems/5.1/bin

2. (UNIX) 다음 명령을 입력합니다.

   tibemsadmin

   Tibco EMS 관리 도구가 시작됩니다.

3. (Windows) 다음 명령을 입력합니다.

   tibemsadmin.exe

   Tibco EMS 관리 도구가 시작됩니다.

4. 다음 명령 중 하나를 사용하여 현재 환경에 연결합니다.

   - 배포 서버가 7222 포트(기본 포트)에서 보고서 에이전트를 수신하는 경우 다음 명령을 사용하십시오.

     connect

   - 배포 서버가 7243 포트에서 SSL 모드로 보고서 에이전트를 수신하는 경우 다음 명령을 사용하십시오.

     connect SSL://7243

5. 사용자 이름과 암호를 입력합니다.

   참고: 기본 사용자 이름은 admin 이고 암호는 CA Access Control 엔터프라이즈 관리를 설치할 때 지정한 통신 암호입니다.

   메시지 큐에 연결되었습니다.

6. 다음 명령을 입력합니다.

   create user *username*

   username

   새 메시지 큐 사용자의 이름을 지정합니다.

   새 사용자가 만들어집니다.

예: 메시지 큐 사용자 만들기

이 Tibco EMS 관리 도구 명령은 'example'이란 이름의 메시지 큐 사용자를 만듭니다.

```
> connect SSL://7243
로그인 이름(관리자): admin
암호:
연결됨: ssl://localhost:7243
ssl://localhost:7243> create user example
사용자 'example'이 만들어졌습니다.
ssl://localhost:7243>
```

tibco-jms-ds.xml 파일에서 계정 변경

JNDI 연결 계정을 변경할 때 tibco-jms-ds.xml 파일에서 계정을 변경합니다.

tibco-jms-ds.xml 파일에서 계정을 변경하려면

1. 이미 중지되지 않은 경우 JBoss Application Server 를 중지합니다.
2. 다음 디렉터리로 이동합니다. 여기서 *JBoss_home* 는 JBoss 를 설치한 디렉터리입니다.

   JBoss_home/server/default/deploy/jms
3. 텍스트 기반 편집기에서 tibco-jms-ds.xml 파일을 엽니다.
4. 다음 매개 변수의 끝에서 계정 이름을 변경합니다.

   java.naming.security.principal=
5. 파일을 저장한 후 닫습니다.

dP: tibco-jms-ds.xml 파일

이 tibco-jms-ds.xml 파일 조각은 변경된 JNDI 연결 계정을 보여 줍니다. 계정 이름은 'example'로 명명됩니다.

```
<!-- The JMS provider loader -->
        <mbean code="org.jboss.jms.jndi.JMSProviderLoader"
        name=":service=JMSProviderLoader,name=TibjmsProvider">
                <attribute name="ProviderName">TIBCOJMSProvider</attribute>
                <attribute name="ProviderAdapterClass">
                org.jboss.jms.jndi.JNDIProviderAdapter</attribute>
                <attribute name="FactoryRef">SSLXAQueueConnectionFactory</attribute>
                <attribute name="QueueFactoryRef">SSLXAQueueConnectionFactory</attribute>
                <attribute name="TopicFactoryRef">SSLXATopicConnectionFactory</attribute>

                <attribute name="Properties">
                        java.naming.security.principal=example
                        java.naming.factory.initial=com.tibco.tibjms.naming.TibjmsInitialContextFactory
                        java.naming.provider.url=tibjmsnaming://localhost:7243
                        java.naming.factory.url.pkgs=com.tibco.tibjms.naming
                        com.tibco.tibjms.naming.security_protocol=ssl
                        com.tibco.tibjms.naming.ssl_enable_verify_host=false
                </attribute>
        </mbean>
```

메시지 큐 통신 설정 변경

다음 메시지 큐 통신 설정을 변경할 수 있습니다.

- 메시지 큐 관리자의 암호
- 메시지 큐 서버 인증서
- 메시지 큐 URL
- 메시지 큐 SSL 키 저장소의 암호
- 끝점이 메시지 큐에 연결하기 위해 사용하는 암호

  참고: 끝점은 +reportagent 서비스 계정을 사용하여 메시지 큐에 연결합니다.
- 메시지 큐에 연결하기 위해 CA Access Control 엔터프라이즈 관리 및 DMS 가 사용하는 암호

  참고: CA Access Control 엔터프라이즈 관리 및 DMS 는 reportserver 서비스 계정을 사용하여 메시지 큐에 연결합니다.

추가 정보:

+reportagent 암호 변경 (페이지 435)
reportserver 암호 변경 (페이지 432)

메시지 큐 관리자 암호 변경

메시지 큐 관리자 계정은 *admin* 으로 명명되며, 이 계정을 사용하여 메시지 큐에서 관리 작업을 수행할 수 있습니다.

조직의 보안 및 암호 정책에 따라 admin 암호를 정기적으로 변경해야 할 수 있습니다.

메시지 큐 관리자 암호를 변경하기 전에 다음 사항에 주의하십시오.

- 이 계정의 기본 암호는 CA Access Control 엔터프라이즈 관리를 설치할 때 지정하는 통신 암호입니다.
- 이 암호는 다음과 같은 제한이 있습니다.
  - 길이는 1-240 자여야 합니다.
  - 높은 ASCII 문자를 포함할 수 없습니다.
  - 큰따옴표("")를 포함할 수 없습니다.
- 암호는 메시지 큐에 저장됩니다.

중요! 회사에 여러 대의 배포 서버가 있는 경우 엔터프라이즈 관리 서버에 설치된 배포 서버에서 암호를 먼저 변경한 다음 다른 배포 서버에서 암호를 변경하십시오. 메시지 큐는 배포 서버의 일부입니다.

메시지 큐 관리자 암호를 변경하려면 admin 사용자에 대한 메시지 큐 암호를 설정 (페이지 454)하십시오.

예: admin 사용자에 대한 메시지 큐 암호 설정

이 Tibco EMS Administration Tool 명령은 admin 사용자에 대한 메시지 큐 암호를 설정합니다. 암호는 "secret"이며, 큰따옴표로 둘러싼 일반 텍스트여야 합니다.

```
ssl://localhost:7243> set password admin "secret"
사용자 'admin'의 암호가 수정되었습니다.
ssl://localhost:7243>
```

메시지 큐 서버 인증서 변경

메시지 큐는 메시지 큐와 클라이언트 사이의 SSL 통신에 서버 인증서를 사용합니다. 메시지 큐 클라이언트는 CA Access Control 끝점 및 CA Access Control 엔터프라이즈 관리입니다.

메시지 큐 서버 인증서를 변경하려면

1. CA Access Control 메시지 큐를 중지합니다.
2. X.509 서버 인증서를 만듭니다.

   .p12 형식 인증서를 만들 것을 권장합니다.
3. 다음 디렉터리로 이동합니다. 여기서 *DistServer* 는 배포 서버를 설치한 디렉터리입니다.

   DistServer/MessageQueue/tibco/bin/ems
4. 다음 명령을 입력합니다.

   tibemsadmin -mangle *password*

   password

   서버 인증서의 암호를 지정합니다.

   서버 인증서에 대한 암호는 암호화됩니다.
5. 텍스트 기반 편집기에서 tibemsd.conf 파일을 엽니다. 이 파일은 다음 디렉터리에 있습니다.

   DistServer/MessageQueue/tibco/bin/ems
6. 다음 매개 변수의 값을 변경합니다.

   ssl_server_identity

   서버 인증서에 대한 전체 경로를 지정합니다.

   ssl_server_key

   서버 인증서 키에 대한 전체 경로를 지정합니다.

   참고: .p12 인증서를 사용하는 경우 이 매개 변수를 비워 두십시오.

   ssl_password

   서버 인증서의 암호화된 암호를 지정합니다.
7. 파일을 저장한 후 닫습니다.

   메시지 큐 서버 인증서가 변경됩니다.
8. CA Access Control 메시지 큐를 다시 시작합니다.

예: tibemsd.conf 파일

다음은 .p12 서버 인증서에 대한 tibemds.conf 파일의 메시지 큐 서버 매개 변수의 예제입니다. 암호는 }>8:Jt^+%INK&i^v 이며 암호화되었습니다. ssl_server_key 매개 변수에는 값이 없습니다.

```
ssl_server_identity    = "C:\Program Files\CA\AccessControlServer\MessageQueue\conf\keystore.p12"
ssl_server_key         =
ssl_password           = }>8:Jt^+%INK&i^v
```

메시지 큐 SSL 키 저장소의 암호 변경

메시지 큐 SSL 키 저장소는 메시지 큐가 SSL 통신을 위해 사용하는 서버 인증서를 저장합니다. 메시지 큐 SSL 키 저장소를 변경할 때 서버 인증서를 서명하는 공개/개인 키 쌍을 업데이트합니다.

회사의 보안 및 암호 정책을 따르기 위해 주기적으로 메시지 큐 SSL 키 저장소의 암호를 변경해야 할 수 있습니다.

메시지 큐 SSL 키 저장소의 암호를 변경하기 전에 다음 사항에 주의하십시오.

- 기본 암호는 CA Access Control 엔터프라이즈 관리를 설치할 때 지정하는 통신 암호입니다.
- 이 암호는 다음과 같은 제한이 있습니다.
  - 길이는 6-50 자여야 합니다.
  - 높은 ASCII 문자를 포함할 수 없습니다.
  - 큰따옴표("")를 포함할 수 없습니다.
- 암호는 다음 파일에 저장됩니다. *ACServer* 는 CA Access Control 엔터프라이즈 관리를 설치한 디렉터리입니다.

  ACServer/MessageQueue/conf/keystore.p12

중요! 회사에 여러 대의 배포 서버가 있는 경우 엔터프라이즈 관리 서버에 설치된 배포 서버에서 암호를 먼저 변경한 다음 다른 배포 서버에서 암호를 변경하십시오. 메시지 큐는 배포 서버의 일부입니다.

메시지 큐 SSL 키 저장소의 암호를 변경하려면

1. CA Access Control 메시지 큐 서비스를 중지합니다.
2. 명령 프롬프트 창을 열고 다음 디렉터리로 이동합니다. 여기서 *JDK* 는 Java Development Kit 를 설치한 디렉터리입니다.

   JDK/bin

3. 다음 명령을 실행합니다.

   keytool -genkey -keyalg RSA -keysize 1024 -keystore "keystore.p12" -storetype PKCS12 -dname "cn=acmq" -alias acmq -storepass "*password*" -keypass "*password*"

   -genkey

   명령이 키 쌍(공개 키 및 개인 키)을 생성하도록 지정합니다.

   -keyalg RSA

   RSA 알고리즘을 사용하여 키 쌍을 만들도록 지정합니다.

   -keysize 1024

   생성된 키의 크기를 1024 비트로 지정합니다.

   -storetype PKCS12

   PKCS12 파일 형식으로 키가 생성되도록 지정합니다.

   -dname "cn=acmq"

   생성된 인증서의 X.500 고유 이름을 acmq 로 지정합니다. 이 이름은 인증서의 발급자 및 주체 필드에 사용됩니다.

   -alias acmq

   키 저장소 입력 이름을 acmq 로 업데이트합니다.

   -storepass "*password*"

   메시지 큐 SSL 키 저장소를 보호하는 암호를 지정합니다. 암호는 -keypass 매개 변수에 대해 지정하는 암호와 동일해야 합니다.

   -keypass "*password*"

   새 키 쌍의 개인 키를 보호하는 암호를 지정합니다. 암호는 -storepass 매개 변수에 대해 지정하는 암호와 동일해야 합니다.

   keytool 유틸리티는 메시지 큐 SSL 키 저장소의 암호를 변경합니다.

4. 다음 디렉터리로 이동합니다. 여기서 *DistServer* 는 배포 서버를 설치한 디렉터리입니다.

   DistServer/MessageQueue/tibco/bin/ems

5. 다음 명령을 실행합니다.

   tibemsadmin -mangle *password*

   SSL 키 저장소의 암호는 암호화됩니다.

새 항목(320)

메시지 큐는 localhost 를 URL 로서 사용합니다. tibco-jms-ds.xml 을 수정하여 호스트의 정규화된 고유 이름(FQDN)을 사용하도록 이 URL 을 수정할 수 있습니다.

이 URL 정보는 메시지 큐에서 다음 XML 파일에 저장됩니다. 여기서 *JBoss_HOME* 은 JBoss 를 설치한 디렉터리입니다.

JBoss_home/server/default/deploy/jms/tibco-jms-ds.xml

다음 단계를 수행하십시오.

1. JBoss Application Server, CA Access Control 메시지 큐 및 모든 CA Access Control 서비스를 중지합니다.
2. 다음 위치에 있는 tibco-jms-ds.xml 파일을 백업합니다.

   JBoss_home\server\default\deploy\jms
3. tibco-jms-ds.xml 파일을 열고 다음 단계를 수행합니다.
   a. *localhost* 를 찾습니다.
   b. *localhost* 를 *FQDN* 으로 대체합니다.
   c. *localhost* 의 모든 인스턴스에 대해 a 와 b 단계를 수행합니다.
   d. 파일을 저장한 후 닫습니다.
4. 다음 위치로 이동하여 통신 키를 수정합니다.

   HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Common\communication
5. 키 값 *Distribution_Server* 를 찾습니다.

   기본값은 ssl://localhost:7243 입니다.
6. *ssl://localhost:7243* 값을 *ssl://<FQDN>:7243* 으로 대체합니다.
7. CA Access Control 메시지 큐 서비스를 포함하여 모든 CA Access Control 서비스를 시작합니다.
8. JBoss 서비스를 시작합니다.

   CA Access Control 메시지 큐 URL 이 변경되었습니다.

암호 변경 절차

다음 절차는 CA Access Control 암호를 변경하는 여러 다른 방법에 대해 설명합니다.

selang 을 사용하여 암호 변경

selang 을 사용하여 다음 서비스 계정에 대한 암호를 변경할 수 있습니다.

- +policyfetcher
- +devcalc
- ac_entm_pers

조직의 보안 및 암호 정책에 따라 이러한 계정의 암호를 정기적으로 변경해야 할 수 있습니다.

selang 을 사용하여 암호를 변경할 때는 다음 사항에 주의하십시오.

- 암호는 큰따옴표로 묶어야 합니다.
- 고급 정책 관리를 사용하여 암호 변경 명령을 전파할 수 없습니다.

참고: 서비스 계정이 상호 작용하는 모든 구성 요소에서 암호를 변경하려면 여러 방법을 사용해야 할 수 있습니다.

selang 을 사용하여 암호를 변경하려면 다음 명령을 실행하십시오.

cu *user* password("*password*") grace- nonative

사용자

암호를 변경하는 대상 사용자의 이름을 지정합니다.

password

새 암호를 지정합니다.

참고: 명령에 암호를 잘라내어 붙여넣는 경우 암호에 캐리지 리턴 또는 줄바꿈이 포함되지 않도록 하십시오.

예: +policyfetcher 암호 변경

이 명령은 +policyfetcher 사용자에 대한 암호를 변경합니다. 암호는 "secret"이며, 큰따옴표로 둘러싼 일반 텍스트여야 합니다.

```
AC> cu +policyfetcher password("secret") grace- nonative
(localhost)
USER +policyfetcher 를 성공적으로 업데이트했습니다.
```

추가 정보:

+policyfetcher 암호 변경 (페이지 436)
+devcalc 암호 변경 (페이지 437)
ac_entm_pers 암호 변경 (페이지 439)

sechkey 를 사용하여 메시지 큐 암호 변경

sechkey 를 사용하여 다음 서비스 계정에 대한 암호를 변경할 수 있습니다.

- reportserver
- +reportagent

조직의 보안 및 암호 정책에 따라 이러한 계정의 암호를 정기적으로 변경해야 할 수 있습니다. sechkey 를 사용하여 암호를 변경할 때는 암호를 큰따옴표로 묶어야 합니다.

참고: 서비스 계정이 상호 작용하는 모든 구성 요소에서 암호를 변경하려면 여러 방법을 사용해야 할 수 있습니다.

sechkey 를 사용하여 메시지 큐를 변경하려면 배포 서버에서 다음 명령을 실행하십시오.

{sechkey | acuxchkey} -t [-server] -pwd "*password*"

sechkey

CA Access Control 끝점에서 암호를 변경하도록 지정합니다.

acuxchkey

UNAB 끝점에서 암호를 변경하도록 지정합니다.

-server

DMS 에서 암호를 변경하도록 지정합니다.

참고: 이 매개 변수는 sechkey 매개 변수를 사용할 때만 유효합니다.

password

새 암호를 지정합니다.

참고: 명령에 암호를 잘라내어 붙여넣는 경우 암호에 캐리지 리턴 또는 줄바꿈이 포함되지 않도록 하십시오.

예: UNAB 끝점에서 메시지 큐 암호 변경

이 명령은 배포 서버와 통신하는 모든 UNAB 끝점에 메시지 암호를 전파합니다. 암호는 "secret"이며, 큰따옴표로 둘러싼 일반 텍스트여야 합니다.

acuxchkey -t -pwd "secret"

예: DMS 에서 메시지 큐 암호 변경

이 명령은 DMS 에서 메시지 큐 암호를 변경합니다. 암호는 "secret"이며, 큰따옴표로 둘러싼 일반 텍스트여야 합니다.

sechkey -t -server -pwd "secret"

추가 정보:

reportserver 암호 변경 (페이지 432)
+reportagent 암호 변경 (페이지 435)

메시지 큐 암호 설정

메시지 큐 암호를 설정하여 다음 서비스 계정의 암호를 변경합니다.

- reportserver
- +reportagent

조직의 보안 및 암호 정책에 따라 이러한 계정의 암호를 정기적으로 변경해야 할 수 있습니다. 메시지 큐 암호를 설정할 때는 암호를 큰따옴표로 묶어야 합니다.

참고: 서비스 계정이 상호 작용하는 모든 구성 요소에서 암호를 변경하려면 여러 방법을 사용해야 할 수 있습니다.

메시지 큐 암호를 설정하려면

1. 다음 디렉터리로 이동합니다. 여기서 *DistServer* 는 배포 서버를 설치한 디렉터리입니다.

   DistServer/MessageQueue/tibco/ems/5.1/bin

2. (UNIX) 다음 명령을 입력합니다.

   tibemsadmin

   Tibco EMS 관리 도구가 시작됩니다.

3. (Windows) 다음 명령을 입력합니다.

   tibemsadmin.exe

   Tibco EMS 관리 도구가 시작됩니다.

4. 다음 명령 중 하나를 사용하여 현재 환경에 연결합니다.

   - 배포 서버가 7222 포트(기본 포트)에서 보고서 에이전트를 수신하는 경우 다음 명령을 사용하십시오.

     connect

   - 배포 서버가 7243 포트에서 SSL 모드로 보고서 에이전트를 수신하는 경우 다음 명령을 사용하십시오.

     connect SSL://7243

5. 사용자 이름과 암호를 입력합니다.

   참고: 기본 사용자 이름은 admin 이고 암호는 CA Access Control 엔터프라이즈 관리를 설치할 때 지정하는 통신 암호입니다.

   메시지 큐에 연결되었습니다.

6. 다음 명령을 실행합니다.

   set password *user* "*password*"

   사용자

   암호를 변경하는 대상 사용자의 이름을 지정합니다.

   "*password*"

   새 암호를 지정합니다.

   사용자에 대한 암호가 메시지 큐에서 변경됩니다.

   참고: 명령에 암호를 잘라내어 붙여넣는 경우 암호에 캐리지 리턴 또는 줄바꿈이 포함되지 않도록 하십시오.

예: reportserver 사용자에 대한 메시지 큐 암호 설정

이 Tibco EMS Administration Tool 명령은 reportserver 사용자에 대한 메시지 큐 암호를 설정합니다. 암호는 "secret"이며, 큰따옴표로 둘러싼 일반 텍스트여야 합니다.

```
> connect SSL://7243
로그인 이름(관리자): admin
암호:
연결됨: ssl://localhost:7243
ssl://localhost:7243> set password reportserver "secret"
사용자 'reportserver'의 암호가 수정되었습니다.
ssl://localhost:7243>
```

추가 정보:

reportserver 암호 변경 (페이지 432)
+reportagent 암호 변경 (페이지 435)

일반 텍스트 암호 암호화

다음 서비스 계정의 일반 텍스트 암호를 암호화합니다.

- RDBMS_service_user
- reportserver

암호는 JBoss 디렉터리에서 일반 텍스트 XML 로 저장되므로 암호를 암호화합니다. pwdtools 유틸리티를 사용하여 일반 텍스트 암호를 암호화합니다.

암호화된 암호에서 실수로 캐리지 브레이크를 선택하지 않도록 암호화된 암호(이 유틸리티의 출력)를 텍스트 파일로 내보내는 것이 좋습니다. 그렇지 않으면 암호화된 암호가 한 줄보다 길 경우 캐리지 브레이크가 발생할 수 있습니다.

pwdtools 를 사용하여 일반 텍스트 암호를 암호화하는 경우 암호를 큰따옴표로 묶어야 합니다.

일반 텍스트 암호를 암호화하려면

1. 명령 프롬프트 창을 엽니다.
2. 다음 디렉터리로 이동합니다. 여기서 *ACServerInstallDir* 는 CA Access Control 엔터프라이즈 관리이 설치된 디렉터리입니다.

   ACServerInstallDir/IAM Suite/Access Control/tools/PasswordTool
3. 다음 명령을 실행합니다.

   pwdtools -FIPS -p "*password*" -*k* [*filename*]

   password

   일반 텍스트 암호를 지정합니다.

   filename

   pwdtools 가 암호화된 암호를 출력하는 파일의 이름을 지정합니다.

   pwdtools 가 암호를 암호화합니다.

예: 일반 텍스트 암호 암호화

이 명령은 일반 텍스트 암호를 암호화하여 pw.txt 파일로 내보냅니다. 일반 텍스트 암호는 "secret"이며 큰따옴표로 묶어야 합니다.

```
C:\Program Files\CA\AccessControlServer\IAM Suite\Access Control\tools\PasswordTool>
pwdtools.bat -FIPS -p "secret" -key
C:\jboss-4.2.3.GA\server\default\deploy\IdentityMinder.ear\config\com\netegrity\config\keys\FIPSkey.dat"
```

추가 정보:

RDBMS_service_user 암호 변경 (페이지 430)
reportserver 암호 변경 (페이지 432)

properties-service.xml 파일에서 암호 변경

properties-service.xml 파일에서 암호를 변경하여 reportserver 계정에 대한 암호를 변경합니다. 조직의 보안 및 암호 정책에 따라 이 계정의 암호를 정기적으로 변경해야 할 수 있습니다.

참고: 서비스 계정이 상호 작용하는 모든 구성 요소에서 암호를 변경하려면 여러 방법을 사용해야 할 수 있습니다.

properties-service.xml 파일에서 암호를 변경하려면

1. JBoss Application Server 를 중지합니다.
2. 다음 디렉터리로 이동합니다. 여기서 *JBoss_home* 는 JBoss 를 설치한 디렉터리입니다.

   JBoss_home/server/default/deploy
3. 텍스트 기반 편집기에서 properties-service.xml 파일을 엽니다.
4. SamMDB.mdb-passwd 매개 변수에서 암호를 변경합니다.
5. 파일을 저장한 후 닫습니다.

예: properties-service.xml 파일에서 암호 변경

properties-service.xml 파일의 이 조각은 변경된 reportserver 암호를 보여 줍니다. 암호는 }>8:Jt^+%INK&i^v 이며 암호화되었습니다.

```
<attribute name="Properties">
        SamMDB.mdb-user=reportserver
        <!-- encoded tibco password -->
        SamMDB.mdb-passwd={AES}:}>8:Jt^+%INK&i^v==
</attribute>
```

추가 정보:

reportserver 암호 변경 (페이지 432)

login-config.xml 파일에서 암호 변경

다음 서비스 계정의 암호를 변경할 때는 login-config.xml 파일에서 암호를 변경합니다.

- RDBMS_service_user
- reportserver

조직의 보안 및 암호 정책에 따라 이러한 계정의 암호를 정기적으로 변경해야 할 수 있습니다.

참고: 서비스 계정이 상호 작용하는 모든 구성 요소에서 암호를 변경하려면 여러 방법을 사용해야 할 수 있습니다. 암호가 일반 텍스트 암호인 경우 login-config.xml 파일에서 암호를 변경하기 전에 pwdtools 유틸리티를 사용하여 암호를 암호화하십시오.

login-config.xml 파일에서 암호를 변경하려면

1. JBoss Application Server 를 중지합니다.
2. 다음 디렉터리로 이동합니다. 여기서 *JBoss_home* 는 JBoss 를 설치한 디렉터리입니다.

   JBoss_home/server/default/conf
3. 텍스트 기반 편집기에서 login-config.xml 파일을 엽니다.

4. RDBMS_service_user 암호 변경:
   a. 파일에서 RDBMS_service_user 계정의 이름에 대한 각 인스턴스를 찾습니다.

      이 파일에는 6 개의 인스턴스가 있습니다. 이 계정의 이름은 CA Access Control 엔터프라이즈 관리에 대한 데이터베이스를 준비하기 위해 사용자를 만들 때 지정합니다.

   b. 이름의 각 인스턴스 바로 뒤에 있는 매개 변수에서 암호를 변경합니다.

      매개 변수는 <module-option name="password"> 및 </module-option> 태그로 둘러 싸입니다.

   RDBMS_service_user 암호가 변경됩니다.
5. reportserver 암호 변경:
   a. 파일에서 다음 매개 변수를 찾습니다:

      <module-option name="userName">reportserver</module-option>

   b. 이 매개 변수의 바로 뒤에 있는 매개 변수에서 암호를 변경합니다.

      매개 변수는 <module-option name="password"> 및 </module-option> 태그로 둘러 싸입니다.

   reportserver 암호가 변경됩니다.
6. 파일을 저장한 후 닫습니다.

예: login-config.xml 파일에서 RDBMS_service_user 암호 변경

login-config.xml 파일의 이 조각은 변경된 RDMBS_service_user 암호의 한 인스턴스를 보여 줍니다. 사용자 이름은 caidb01 입니다.
암호는 }>8:Jt^+%INK&i^v 이며 암호화되었습니다.

```
<application-policy name="imobjectstoredb">
        <authentication>
                <login-module code="com.netegrity.jboss.datasource.PasswordEncryptedLogin"
                flag="required">
                        <module-option name="userName">caidb01</module-option>
                        <module-option name="password">{AES}:}>8:Jt^+%INK&i^v==</module-option>
                        <module-option name="managedConnectionFactoryName">
                        jboss.jca:name=jdbc/objectstore,service=NoTxCM</module-option>
                </login-module>
        </authentication>
</application-policy>
```

예: login-config.xml 파일에서 reportserver 암호 변경

login-config.xml 파일의 이 조각은 변경된 reportserver 암호를 보여 줍니다. 암호는 }>8:Jt^+%INK&i^v 이며 암호화되었습니다.

```
<application-policy name="JmsXATibcoRealm">
    <authentication>
      <login-module code="com.netegrity.jboss.datasource.PasswordEncryptedLogin" flag="required">
        <module-option name="userName">reportserver</module-option>
              <module-option name="password">{AES}:}>8:Jt^+%INK&i^v==</module-option>
                    <module-option name="managedConnectionFactoryName">
                    jboss.jca:service=TxCM,name=TibcoJmsXA</module-option>
      </login-module>
    </authentication>
  </application-policy>
```

추가 정보:

RDBMS_service_user 암호 변경 (페이지 430)
reportserver 암호 변경 (페이지 432)

CA Identity Manager 관리 콘솔에서 사용자 디렉터리 암호 변경

ADS_LDAP_bind_user 암호를 변경할 때 CA Identity Manager 관리 콘솔에서 사용자 디렉터리 암호를 변경합니다. 조직의 보안 및 암호 정책에 따라 이 계정의 암호를 정기적으로 변경해야 할 수 있습니다.

참고: 서비스 계정이 상호 작용하는 모든 구성 요소에서 암호를 변경하려면 여러 방법을 사용해야 할 수 있습니다.

CA Identity Manager 관리 콘솔에서 사용자 디렉터리 암호를 변경하려면

1. 일반 텍스트 암호를 암호화합니다 (페이지 456).
2. CA Identity Manager 관리 콘솔을 엽니다 (페이지 88).
3. "디렉터리"를 클릭합니다.

   "디렉터리" 페이지가 나타납니다.
4. "ac-dir"를 클릭합니다.

   "디렉터리 속성" 페이지가 나타납니다.
5. "내보내기"를 클릭합니다.

   ac-dir.xml 파일이 내보내기됩니다.

6. 텍스트 기반 편집기에서 exported 파일을 엽니다.
7. 다음 매개 변수를 찾습니다.

   <Credentials user=

8. 다음 필드에서 <credentials> 매개 변수 뒤에 암호화된 암호를 입력합니다.

   {PBES}=

9. 파일을 저장한 후 닫습니다.
10. CA Identity Manager 관리 콘솔에 있는 "디렉터리 속성" 페이지에서 "업데이트"를 클릭합니다.

    "디렉터리 업데이트" 창이 나타납니다.

11. 편집한 XML 파일의 경로 및 파일 이름을 입력하거나 파일을 찾은 다음 "마침"을 클릭합니다.

    상태 정보는 "디렉터리 구성 출력"에 표시됩니다.

12. "계속"을 클릭하고 환경을 다시 시작합니다.

    CA Identity Manager 관리 콘솔에서 사용자 디렉터리 암호를 변경했습니다.

예: 사용자 디렉터리 암호 변경

내보낸 ac-dir.xml 파일의 이 조각은 변경된 사용자 디렉터리 암호를 보여 줍니다. 사용자 이름은 Administrator 입니다. 암호는 }>8:Jt^+%INK&i^v 이며 암호화되었습니다.

<Credentials user="CN=Administrator,cn=Users,DC=unixauthdemo,DC=co,DC=il">
{PBES}:**}>8:Jt^+%INK&i^v**==</Credentials>

추가 정보:

CA Identity Manager 관리 콘솔 활성화 (페이지 88)
CA Identity Manager 관리 콘솔 열기 (페이지 88)
ADS_LDAP_bind_user 암호 변경 (페이지 440)