CA Access Control

업그레이드 안내서

12.7

타사 고지 사항

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
- 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 - \ProgramFiles\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/worldwide 에서 기술 지원팀에 문의하십시오.

목차

제 1 장: 안내서 정보

이 안내서는 CA Access Control 서버 및 끝점 구성 요소를 업그레이드하는 방법과 PMD 를 고급 정책 환경으로 마이그레이션하는 방법을 설명합니다.

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

제 2 장: 서버 및 끝점 구성 요소 업그레이드

이 섹션은 다음 항목을 포함하고 있습니다.

시작하기 전에

업그레이드 프로세스를 시작하기 전에 다음 항목을 검토하십시오.

기존 중앙 데이터베이스를 Microsoft SQL Server 2008 로 업그레이드

CA Access Control 엔터프라이즈 관리 중앙 데이터베이스가 Microsoft SQL Server 2005 에서 구성되었고 Microsoft SQL Server 2008 로 업그레이드하려는 경우 이 새 서버와 동작하도록 엔터프라이즈 관리 서버를 구성합니다.

다음 단계를 수행하십시오.

1. 엔터프라이즈 관리 서버에서 모든 CA Access Control 서비스를 중지합니다.
2. JBoss 를 중지합니다. 다음 단계 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.
3. Microsoft SQL Server 2008 로 업그레이드합니다.
4. Microsoft 웹 사이트에서 Microsoft SQL Server JDBC 드라이버 2.0 을 다운로드합니다.
5. 엔터프라이즈 관리 서버의 임시 디렉터리에 이 파일의 압축을 풉니다.

6. 다음 단계 중 *하나*를 수행합니다.
   - JDK 버전 1.5 를 사용하는 경우 sqljdbc.jar 파일을 찾습니다.
   - JDK 버전 1.6 이상을 사용하는 경우 sqljdbc4.jar 파일을 찾아 이름을 sqljdbc.jar 로 변경합니다.
7. 엔터프라이즈 관리 서버의 다음 디렉터리로 파일을 복사합니다.

   JBoss_HOME/server/default/lib

   참고: 이 디렉터리의 기존 파일을 덮어쓰십시오.
8. Microsoft SQL Server 2008 서비스를 시작합니다.
9. JBoss 를 시작합니다.
10. CA Access Control 엔터프라이즈 관리를 시작합니다.

엔터프라이즈 관리를 위해 CA Access Control 끝점을 준비합니다.

CA Access Control 끝점에 엔터프라이즈 관리 서버를 설치할 수 있습니다. 이 끝점은 엔터프라이즈 관리 서버에 필요한 모든 구성 요소를 포함하고 있지 않습니다. 끝점에 엔터프라이즈 관리 서버를 설치하려면 먼저 끝점을 준비합니다.

다음 단계를 수행하십시오.

1. 끝점에서 모든 CA Access Control 서비스(Windows) 또는 데몬(UNIX)을 중지합니다.
2. 끝점에 엔터프라이즈 관리 서버를 설치합니다.

   웹 기반 응용 프로그램과 배포 서버가 설치됩니다. 이미 설치되지 않았으면 CA Access Control 의 최신 버전도 설치됩니다.
3. 엔터프라이즈 관리 서버에서 DMS 를 만듭니다.

   엔터프라이즈 관리 서버 설치는 끝점에 DMS 를 만들지 않습니다. dmsmgr 유틸리티를 사용하여 DMS 를 만드십시오.
4. 엔터프라이즈 관리 서버 서비스 또는 데몬을 시작합니다.
5. ADMIN, AUDITOR, Logical 권한 부여 특성을 사용하여 사용자 계정을 만듭니다.

   CA Access Control 엔터프라이즈 관리에서 DMS 연결 설정을 정의할 때 논리적 사용자 계정을 사용합니다.

6. DMS 에 호스트 그룹을 만듭니다.
7. dmsmgr 유틸리티를 사용하여 DMS 에 노드를 추가합니다.
8. 엔터프라이즈 관리 서버를 설치할 때 지정한 관리 사용자 계정을 사용하여 CA Access Control 엔터프라이즈 관리에 로그인합니다.
9. CA Access Control 엔터프라이즈 관리에서 DMS 연결 설정을 정의합니다.

   끝점에서 만든 DMS 를 지정합니다.

   만든 DMS 를 사용하도록 엔터프라이즈 관리 서버가 설치 및 구성되었습니다.

참고: dmsmgr 유틸리티에 대한 자세한 내용은 *참조 안내서*를 참조하십시오. selang 을 사용하여 사용자를 만들고 구성하는 방법에 대한 자세한 내용은 *selang 참조 안내서*를 참조하십시오.

엔터프라이즈 관리 서버의 업그레이드 준비

설치된 r12.5.x 엔터프라이즈 관리 서버를 r12.6.1 로 업그레이드하기 전에 다음 정보를 수집합니다.

- 메시지 큐 암호

  관리 사용자, reportserver 사용자, +reportagent 사용자 암호를 획득합니다.

- 데이터베이스 연결 정보

  호스트 이름, 포트 번호, 데이터베이스 이름, 사용자 이름, 암호를 획득합니다.

- Java Connector Server 암호

  CA Access Control 엔터프라이즈 관리의 이전 설치 중 사용한 통신 암호를 획득합니다.

- (선택 사항) Java Connector Server(JCS) SSL 인증서

  사용자 지정 SSL 인증서를 사용한 경우에만 CA Access Control 엔터프라이즈 관리 r12.5.x 로 업그레이드한 이후에 새 SSL 인증서를 가져오십시오.

업그레이드 후 Java Connector Server SSL 인증서 가져오기

CA Access Control r12.5 SP3 에서 Java Connector Server(JCS) SSL 인증서의 변경 사항으로 인해 CA Access Control r12.5.x 에서 업그레이드한 이후에 새 SSL 인증서를 가져와야 합니다.

중요! 사용자 지정 JCS SSL 인증서를 사용한 경우에만 이 절차를 완료하십시오. 기본 SSL 인증서를 사용한 경우 이 절차를 수행할 필요가 없습니다.

다음 단계를 수행하십시오.

1. JBoss Application Server 를 중지합니다.
2. 다음 디렉터리로 이동합니다. 여기서 *JBOSS_HOME* 은 JBoss 를 설치한 디렉터리를 나타냅니다.

   ```
   JBOSS_HOME/server/default/deploy/IdentityMinder.ear/custom/ppm/trusttore/
   ```

3. ssl.keystore 파일을 백업합니다.
4. 앞에서 탐색한 디렉터리에서 명령 프롬프트 창을 엽니다.
5. keytool 유틸리티를 실행하여 가져올 사용자 지정 SSL 키 저장소를 지정합니다. 여기서 *JAVA_HOME* 은 JDK 가 설치된 디렉터리를 나타냅니다. 예:

   ```
   JAVA_HOME\bin\keytool.exe -import -alias eta_client -file c:\custom_certificate.der -keystore ssl.keystore
   ```

   암호 프롬프트가 나타납니다.
6. 키 저장소 암호를 입력합니다. 기본 암호는 *secret* 입니다.

   keytool 은 인증서 정보와 지문을 표시합니다.
7. 인증서를 키 저장소에 추가하려면 'Yes'를 입력합니다.

   keytool 이 새 인증서를 추가합니다.
8. JBoss Application Server 를 시작합니다.

   새 JCS SSL 인증서 파일을 CA Access Control 엔터프라이즈 관리에 로드했습니다.

CA Access Control r5.3 에서 업그레이드하는 방법

배포에 추가된 구성 요소 및 변경 사항으로 인해 CA Access Control r5.3 에서 CA Access Control r12.6.1 로 업그레이드할 수 없습니다. 먼저 기존 CA Access Control r5.3 배포를 CA Access Control r8.0Sp1 로 업그레이드한 다음 CA Access Control r12.6.1 로 업그레이드합니다.

다음 단계를 수행하여 기존 CA Access Control r5.3 배포를 업그레이드합니다.

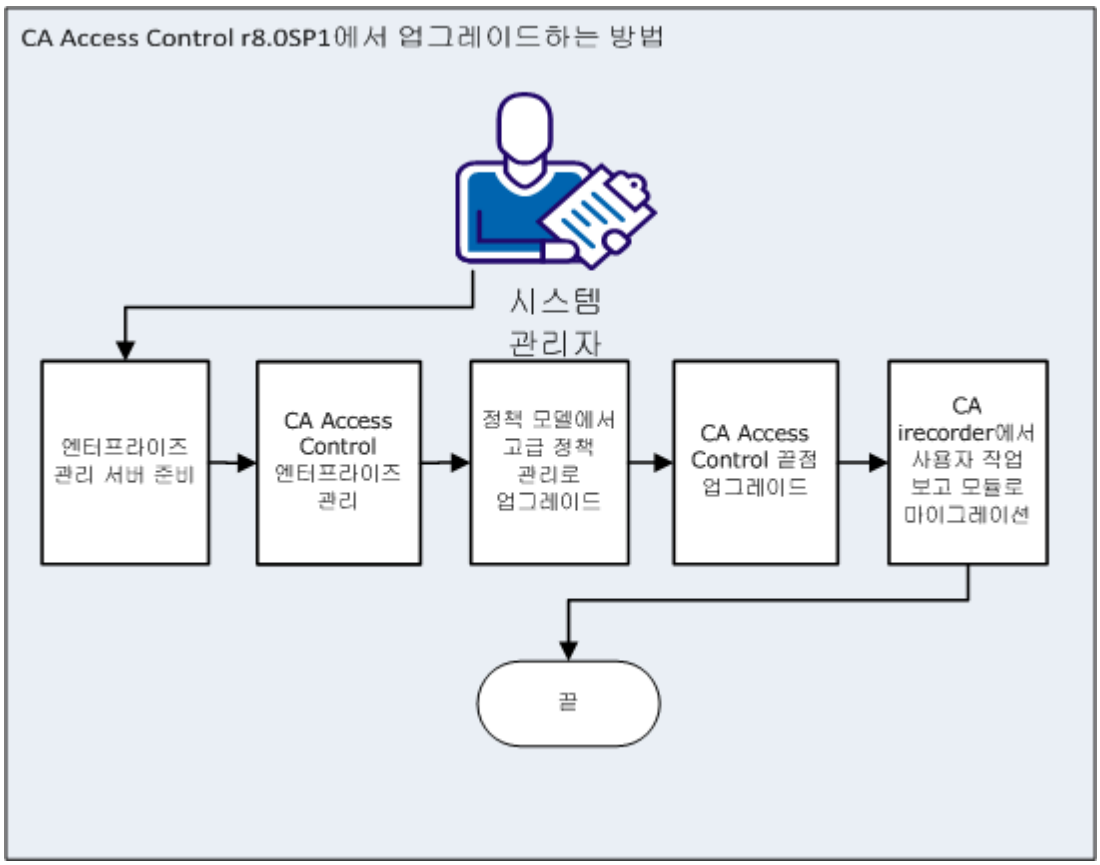
1. 업그레이드 프로세스를 시작하기 전에 모든 CA Access Control 구성 요소를 백업합니다.
2. CA Access Control r8.0SP1 로 업그레이드합니다. (페이지 19)
3. CA Access Control r12.6.1 로 업그레이드

제 3 장: CA Access Control r8.0SP1 에서 업그레이드

이 시나리오의 목적은 CA Access Control r8.0SP1 에서 업그레이드하기 위해 수행하는 단계를 설명하는 것입니다. 이 장의 업그레이드 프로세스는 CA Access Control r8.0SP1 구성 요소가 서로 다른 컴퓨터에 설치되었다고 가정합니다.

이 시나리오의 정보는 CA Access Control 을 관리하는 시스템 또는 CA Access Control 관리자를 위해 제공됩니다.

다음 다이어그램은 CA Access Control r8.0SP1 에서 업그레이드하기 위해 수행하는 단계를 설명합니다.



중요!

- 업그레이드 프로세스를 시작하기 전에 모든 CA Access Control 구성 요소를 백업합니다.
- 소프트웨어 패키지를 사용자 지정하여 'eTrustAccessControl' 경로를 지정하십시오. r8 SP1 패키지는 제품 이름에 eTrust 가 포함되어 있었고 따라서 eTrustAccessControl 하위 디렉터리에 설치되었습니다. 최신 버전은 AccessControl 하위 디렉터리에 설치됩니다.

다음 단계를 수행하여 기존 CA Access Control r8.0SP1 배포를 업그레이드합니다.

1. 엔터프라이즈 관리 서버를 준비합니다.

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

2. CA Access Control 엔터프라이즈 관리를 설치합니다. (페이지 23)
3. 정책 모델 환경에서 고급 정책 관리 환경으로 업그레이드합니다 (페이지 69).
4. CA Access Control 끝점 업그레이드:
   - Windows - 제품 탐색기를 사용하여 설치 (페이지 28)
   - UNIX - install_base 스크립트를 사용하여 설치 (페이지 30)

   참고: 이 설치는 또한 암호 PMD 를 업그레이드합니다.
5. (선택 사항) iRecorder product 를 CA User Activity Reporting Module 으로 마이그레이션합니다.

참고: 정책 관리자는 업그레이드할 수 없습니다. 끝점에서 정책을 관리하려면 [set value for eACEMI variable for your book]를 사용하십시오.

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 중앙 데이터베이스에 대한 사용자를 만듭니다.

     이 사용자는 다음과 같은 권한과 설정이 있어야 합니다.

     - CONNECT (다음과 같은 시스템 권한 부여: ALTER SESSION, CREATE CLUSTER, CREATE DATABASE LINK, CREATE SEQUENCE, CREATE SESSION, CREATE SYNONYM, CREATE TABLE, CREATE VIEW)
     - RESOURCE (다음과 같은 시스템 권한 부여: CREATE CLUSTER, CREATE INDEXTYPE, CREATE OPERATOR, CREATE PROCEDURE, CREATE SEQUENCE, CREATE TABLE, CREATE TRIGGER, CREATE TYPE)
     - CA Access Control 엔터프라이즈 관리 서버를 호스트하는 테이블스페이스에서 무제한 할당량.

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

       데이터베이스에는 정렬 순서 SQL_Latin1_General_CP1_CI_AS 가 있어야 합니다.
     - 새 사용자를 만들고, 새 데이터베이스를 사용자의 기본 데이터베이스로 만들고, 사용자에게 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.

      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. 자세한 내용은 *구현 안내서*를 참조하십시오.

   b. 배포 스크립트를 배포합니다.

   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

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 준비합니다.

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.

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 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.

   InstallAnywhere 설치 프로그램이 시작됩니다.

   a. (선택 사항) 설치 중 사용할 사용자 지정 FIPS 키의 전체 경로 이름을 지정합니다.

   b. 명령 프롬프트 창을 열고 Windows 용 CA Access Control 서버 구성 요소 DVD 에 있는 CA Access Control 엔터프라이즈 관리 설치 실행 파일로 이동합니다. 이 파일은 다음 위치에 있습니다.

      ```
      \EnterpriseMgmt\Disk1\InstData\NoVM
      ```

   c. 다음 인수를 사용하여 CA Access Control 엔터프라이즈 관리 설치 실행 파일을 실행합니다.

      ```
      -DFIPS_KEY=full_pathname_to_FIPS_key
      ```

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

      ```
      E:\EnterpriseMgmt\Dis1\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.

   InstallAnywhere 설치 프로그램이 시작됩니다.

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

JDK(Java Development Kit)

기존 JDK 의 위치를 정의합니다.

참고: CA Access Control 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

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.

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 [assign the value for unab in your book]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. [assign the value for unab in your book] 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.

CA Access Control 엔터프라이즈 관리는 이 마법사를 완료한 이후에 설치됩니다. CA Access Control 엔터프라이즈 관리 설치를 완료하려면 컴퓨터를 다시 시작하십시오.

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

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

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.

다음 단계를 수행하십시오.

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 워크시트를 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 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.

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 명령을 검토하여 그러한 기능의 설치를 시작하는 방법을 알아두십시오. install_base 스크립트의 작동 방식을 먼저 알아두는 것도 좋습니다.

다음 단계를 수행하십시오.

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.

예: 자동 설치를 사용하여 UNIX 용 CA Access Control r12.6SP1 로 업그레이드

이 예는 기존 CA Access Control r8.0SP1 끝점을 UNIX 용 CA Access Control r12.6SP1 로 업그레이드하는 방법을 보여줍니다. 이 예에서는 끝점에 새 기능을 설치할 수 있게 해 주는 매개 변수 파일을 사용하여 CA Access Control 을 설치합니다.

1. install_base script 명령을 검토합니다.

   install_base 스크립트를 사용하여 자동 모드로 CA Access Control r12.6SP1 을 설치합니다. 자세한 내용은 *구현 안내서*를 참조하십시오.

2. UNIX 용 CA Access Control 끝점 구성 요소 미디어에 있는 tar 압축 파일로부터 매개 변수 파일을 추출합니다. 이 파일은 다음 디렉터리에 있습니다.

   ```
   \Unix\Access-Control\
   ```

3. install_base 스크립트를 사용하여 CA Access Control 을 설치합니다.

   -autocfg 명령을 사용하고 사용자 지정한 매개 변수 파일을 사용하도록 지정하십시오.

   지정한 옵션을 사용하여 CA Access Control r12.6SP1 이 설치됩니다.

예: 매개 변수 파일

매개 변수 파일을 사용하면 끝점에 추가할 소프트웨어 구성 요소를 선택할 수 있습니다. 네이티브 설치 모드로 CA Access Control 을 설치하는 경우 설치를 시작하기 전에 이 파일을 사용자 지정합니다. 대화형 모드로 CA Access Control 을 설치하는 경우 설치 매개 변수를 한 파일에 추출한 다음 설치 매개 변수를 사용자 지정할 수 있습니다.

다음은 매개 변수 파일에서 가져온 코드 조각입니다.

```
#  Specifies whether you want to configure PUPM Agent
#  Values: "yes", "no"
#  Default: "no"
INSTALL_PUPM="yes"

# Specifies whether  enables KBL audit records management
# Values: yes, no
# Default: no
ENABLE_KBL=yes
```

이 예에서는 [assign the pupm variable value for your book] 통합을 설치하도록 지정하고(INSTALL_PUPM=yes), 끝점에서 키보드 로깅을 활성화했습니다(ENABLE_KBL=yes).

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
```

CA Access Control r12.0 SP1 에서 업그레이드

이 절은 기존 CA Access Control r12.0 SP1 배포를 업그레이드하기 위해 CA Access Control 또는 시스템 관리자가 수행하는 단계에 대해 설명합니다. 이 장에 설명된 과정은 관리자가 별도의 컴퓨터에 CA Access Control r12.0 SP1 을 설치했다고 가정합니다.

예를 들어, 엔터프라이즈 관리 서버가 하나의 컴퓨터에 설치되어 있고 DMS, DH, 보고서 서버가 또한 별도 컴퓨터에 설치되어 있습니다.

이 장에 설명된 업그레이드 프로세스는 각 구성 요소를 별도로 업그레이드하는 방법에 대해 설명합니다.

참고: CA Access Control 엔터프라이즈 관리 r12.0 SP1 에서만 업그레이드할 수 있습니다.

시작하기 전에

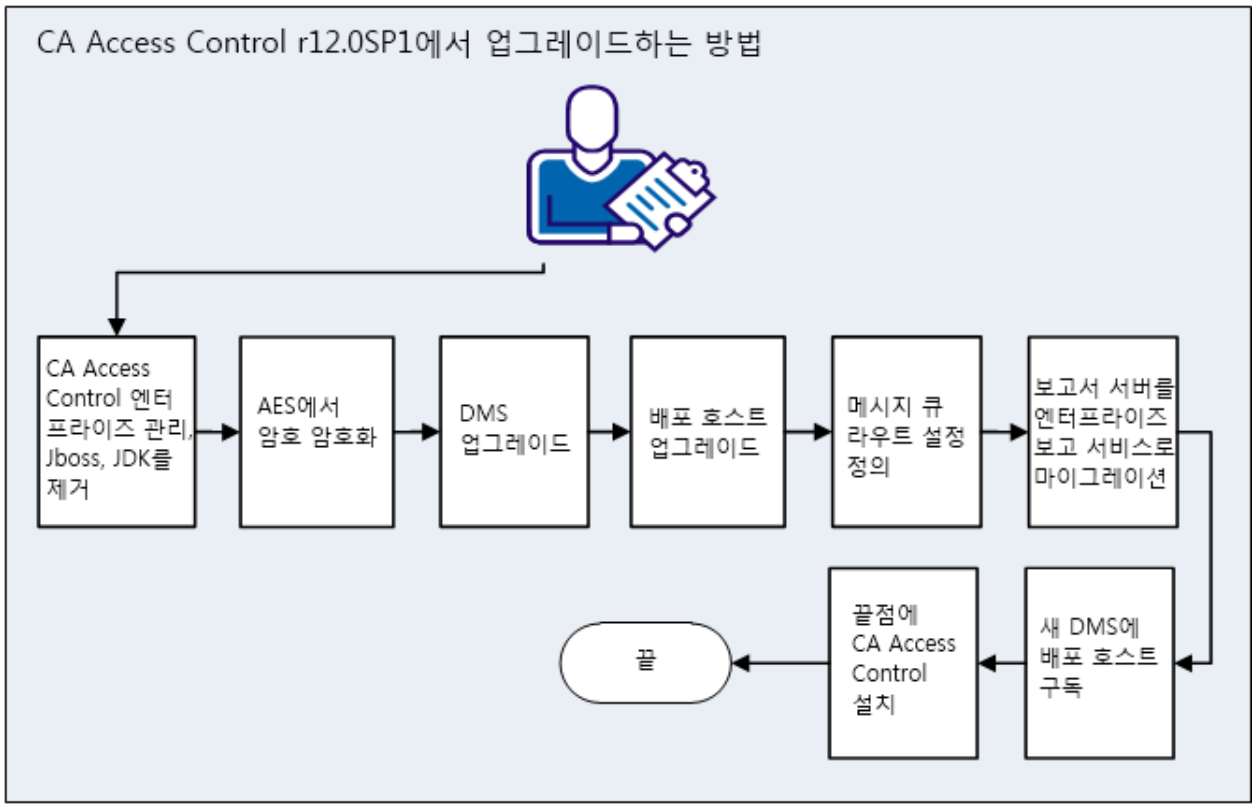
현재 설치된 CA Access Control 을 업그레이드하는 프로세스를 시작하기 전에 다음 사항을 고려하십시오.

- 업그레이드 프로세스를 시작하기 전에 CA Access Control 구성 요소를 백업하는 것이 좋습니다. 업그레이드 프로세스를 시작하기 전에 모든 데이터베이스를 포함하여 시스템 파일을 백업하는 것이 좋습니다.
- CA Access Control 엔터프라이즈 관리는 관리 서버, CA Access Control, 배포 서버, 엔터프라이즈 보고 서비스의 구성 요소를 설치합니다.
- 업그레이드 이후에는 이전 DMS 를 사용할 수 없습니다. 서버를 시작하기 전에 엔터프라이즈 관리 서버, DMS, DH 를 업그레이드해야 합니다.
- 엔터프라이즈 관리 서버를 설치할 때 포함된 사용자 저장소를 사용하도록 지정하십시오.

  중요! 포함된 사용자 저장소에 엔터프라이즈 관리 서버를 설치할 때는 [assign the value for unab in your book] 보고서와 로그인 권한 부여 정책을 사용할 수 없습니다. [assign the value for unab in your book] 보고서를 생성하고 로그인 권한 부여 정책을 구성하려면 Active Directory 를 설치해야 합니다.

r12.0 SP1 에서 업그레이드하는 방법

다음 단계는 기본 CA Access Control r12.0 SP1 배포를 업그레이드하는 방법을 설명합니다.



1. 엔터프라이즈 관리 서버를 업그레이드합니다.
   a. CA Access Control 엔터프라이즈 관리 r12.0 SP1, JBoss, JDK 를 제거합니다.
   b. 필수 프로그램 설치 관리자를 사용하여 JDK 1.5.0 및 JBoss 4.2.3 을 설치합니다 (페이지 37).
   c. CA Access Control 엔터프라이즈 관리를 설치합니다.
2. AES 에서 기존 암호를 암호화합니다 (페이지 47).

   CA Access Control 엔터프라이즈 관리 r12.5 SP1 에서 암호화 방법이 RC2 에서 AES 로 변경되었습니다.
3. DMS 컴퓨터를 업그레이드합니다 (페이지 49).

   참고: CA Access Control 엔터프라이즈 관리가 설치된 동일한 컴퓨터에 DMS 가 설치된 경우 이 단계를 수행할 필요가 없습니다.
4. 배포 호스트를 업그레이드합니다 (페이지 53).

   참고: 회사에 있는 모든 DH 를 업그레이드하십시오. 엔터프라이즈 관리 서버가 설치된 동일한 컴퓨터에 DH 가 설치된 경우 이 단계를 수행할 필요가 없습니다.
5. 메시지 큐(MQ) 라우트 설정을 정의합니다 (페이지 54).
6. 보고서 서버를 엔터프라이즈 보고 서비스로 마이그레이션합니다 (페이지 67).
7. 새 DMS 에 DH 를 구독시킵니다 (페이지 68).
8. (선택 사항) CA Access Control 끝점을 업그레이드합니다 (페이지 68).

엔터프라이즈 관리 서버 업그레이드

이 절차는 엔터프라이즈 서버의 업그레이드를 위한 단계와 필요한 설치 후 단계에 대해 설명합니다.

다음 단계를 수행하십시오.

1. CA Access Control 엔터프라이즈 관리 r12.0 SP1 을 제거합니다.

   참고: CA Access Control 엔터프라이즈 관리 r12.0 SP1 설치에 대한 자세한 내용은 해당 릴리스의 *구현 안내서*를 참조하십시오.
2. 기존 JDK 및 JBoss 를 제거합니다.

3. 필수 소프트웨어를 설치합니다. (페이지 37)
4. CA Access Control 엔터프라이즈 관리를 설치합니다. (페이지 23)

   CA Access Control 엔터프라이즈 관리는 또한 다음 항목을 설치합니다.

   - 엔터프라이즈 관리 서버
   - CA Access Control
   - 엔터프라이즈 보고 서비스
   - 배포 서버

   중요! CA Access Control 엔터프라이즈 관리를 설치할 때 포함된 사용자 저장소를 사용하도록 지정해야 합니다.
5. 보고 데이터베이스 스키마가 CA Access Control 엔터프라이즈 관리의 스키마와 다른 경우 제공된 스크립트를 실행하여 데이터베이스 스키마를 업데이트합니다.
6. (선택 사항) JBoss 에 대한 보안 통신을 구성합니다 (페이지 43).
7. CA Access Control 엔터프라이즈 관리에서 DMS 와 DH 를 비활성화합니다. 다음 명령을 실행합니다.

   ```
   dmsmgr -remove -auto
   ```

   중요! DMS 가 CA Access Control 엔터프라이즈 관리와 다른 컴퓨터에 설치된 경우에만 이 단계를 수행하십시오.

   참고: 업그레이드한 이후에는 기존 DMS 를 더 이상 사용할 수 없게 됩니다. 새 엔터프라이즈 관리 서버를 설치한 이후에 DMS 를 업그레이드하십시오. dmsmgr 유틸리티에 대한 자세한 내용은 *참조 안내서*를 참조하십시오.

새 엔터프라이즈 관리 서버가 설치되었습니다. CA Access Control 엔터프라이즈 관리를 시작하기 전에 이제 DMS 및 배포 호스트를 업그레이드해야 합니다.

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 "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 "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 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.

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 서버 구성 요소 DVD 의 Disk 1 디렉터리에 있는 전체 콘텐츠를 설치 디렉터리에 복사하거나 드라이브를 DVD 에 매핑하십시오.

Windows 에 CA Access Control 엔터프라이즈 관리를 설치하려면

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 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.

   InstallAnywhere 설치 프로그램이 시작됩니다.
5. (선택 사항) 설치 중 사용할 사용자 지정 FIPS 키의 전체 경로 이름을 지정합니다.

   a. 명령 프롬프트 창을 열고 Windows 용 CA Access Control 서버 구성 요소 DVD 에 있는 CA Access Control 엔터프라이즈 관리 설치 실행 파일로 이동합니다. 이 파일은 다음 위치에 있습니다.

      ```
      \EnterpriseMgmt\Disk1\InstData\NoVM
      ```

   b. 다음 인수를 사용하여 CA Access Control 엔터프라이즈 관리 설치 실행 파일을 실행합니다.

      ```
      -DFIPS_KEY=full_pathname_to_FIPS_key
      ```

      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.

   InstallAnywhere 설치 프로그램이 시작됩니다.
6. 필요에 따라 마법사를 완료합니다. 다음 설치 입력 항목은 자동으로 채워지지 않습니다.

   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 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 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.

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 [assign the value for unab in your book]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. [assign the value for unab in your book] 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.

CA Access Control 엔터프라이즈 관리는 이 마법사를 완료한 이후에 설치됩니다. CA Access Control 엔터프라이즈 관리 설치를 완료하려면 컴퓨터를 다시 시작하십시오.

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

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

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.se
    rver.home.dir}/deploy/IdentityMinder.ear/custom/ppm/truststore/keystore.passw
    ord</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.

AES 암호화 방법으로 암호 암호화

CA Access Control r12.0 SP1 에서 암호는 RC2 암호화 방법을 사용하여 암호화되었습니다. CA Access Control r12.0 SP1 에서 암호 암호화 방법이 AES 로 변경되었습니다. 따라서 RC2 암호화 방법을 사용하여 암호화되었던 암호는 CA Access Control 의 이후 새 버전에서 동작하지 않습니다. 이 문제를 해결하려면 CA Access Control r12.0SP1 에서 업그레이드한 이후에 AES 에서 기존 암호를 암호화하십시오.

다음 단계를 수행하십시오.

1. 모든 CA Access Control 서비스를 중지합니다.
2. 다음 작업을 수행하십시오.
   a. 읽기 및 쓰기 액세스 권한이 있는 사용자로 엔터프라이즈 관리 서버 데이터베이스에 연결합니다.
   b. 다음 쿼리를 실행하여 CA Access Control 엔터프라이즈 관리가 사용자 저장소에 연결하기 위해 사용하는 암호를 제거합니다.

      ```
      update IM_DIR_CONNECTION set password=null where
      connection_name='java:/userstore';
      ```

3. pwdtools 유틸리티를 사용하여 데이터베이스의 모든 암호를 암호화합니다.

   tlbusers 테이블의 각 항목에 대해 암호를 생성하는 암호화된 암호로 변경합니다.
4. 연결 테이블에서 DMS 설정을 제거합니다. 다음 쿼리를 실행합니다.

   ```
   DELETE FROM connection WHERE connection_name='con1';
   ```

5. 모든 CA Access Control 서비스를 시작합니다.
6. CA Access Control 엔터프라이즈 관리에서 DMS 연결 설정을 구성합니다.

   참고: DMS 연결 설정에 대한 자세한 내용은 *온라인 도움말*을 참조하십시오.

예: pwdtools 유틸리티를 사용하여 암호 암호화

이 예는 pwdtools 유틸리티를 사용하여 AES 암호화 모드에서 사용자 암호를 암호화하고 엔터프라이즈 관리 서버 데이터베이스에서 암호화된 암호를 설정하는 방법을 보여줍니다.

1. 편집을 위해 pwdtool.bat 을 엽니다. 이 파일은 아래 디렉터리에 있습니다. 여기서 *ACServerInstallDir* 는 엔터프라이즈 서버가 설치된 디렉터리입니다.

   ACServerInstallDir/IAM_Suite/Access_Control/tools/PasswordTool/

2. "::SET JAVA_HOME=<enter valid java home here>" 토큰에 JAVA_HOME 경로를 입력합니다. 예:

   ```
   SET JAVA_HOME=C:\jdk1.5.0
   ```

3. 명령줄 창에서 다음 명령을 실행합니다. 여기서 *password* 는 일반 텍스트 암호이며 *JBOSS_Home* 은 JBoss 가 설치된 디렉터리입니다.

   ```
   pwdtools -FIPS -p <"password"> -k
   JBOSS_HOME\server\default\deploy\IdentityMinder.ear\config\com\
   netegrity\config\keys\FIPSkey.dat
   ```

   암호화된 암호가 표시됩니다. 암호를 클립보드에 복사합니다.

4. 데이터베이스에 대한 액세스 권한이 있는 사용자로 엔터프라이즈 관리 서버에 연결합니다.

5. 다음 쿼리를 실행합니다. 여기서 *encrypted password* 는 이전에 클립보드에 복사한 암호화된 암호이고 *username* 은 사용자 계정의 이름입니다.

   ```
   update tblusers set password = '<encrypted password>' where
   loginid='<username>';
   ```

암호화된 암호를 사용하여 계정 암호를 설정했습니다.

DMS 업그레이드

새 CA Access Control 엔터프라이즈 관리 서버를 설치한 이후에 기존 DMS 를 업그레이드해야 합니다. 업그레이드 전에 기존에 설치된 DMS 를 제거할 필요는 없습니다.

중요! DMS 가 CA Access Control 엔터프라이즈 관리와 다른 컴퓨터에 설치된 경우에만 이 단계를 수행하십시오.

DMS 를 업그레이드하려면 DMS 컴퓨터에 CA Access Control 을 설치하십시오 (페이지 28).

이제 DMS 에 연결하기 위해 CA Access Control 엔터프라이즈 관리를 구성할 수 있습니다 (페이지 51).

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 워크시트를 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 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.

DMS 의 연결 구성

설치 중 CA Access Control 엔터프라이즈 관리는 엔터프라이즈 서버에 설치된 DMS(Deployment Map Server)와 동작하도록 구성됩니다. 다른 DMS 로의 사용자 지정 연결을 만들려면 사용자 지정 DMS 에 대한 연결을 구성하여 사용하는 환경에 맞게 연결을 구성해야 합니다.

참고: 설치 중에 CA Access Control 엔터프라이즈 관리는 *ac_entm_pers* 사용자 계정을 사용하여 엔터프라이즈 관리 서버에 있는 DMS 에 대한 기본 연결을 만듭니다.

DMS 에 대한 연결을 구성하려면

1. CA Access Control 엔터프라이즈 관리에서 다음을 수행합니다.
   a. "시스템"을 클릭합니다.
   b. "연결 관리" 하위 탭을 클릭합니다.
   c. 작업 메뉴에서 왼쪽에 있는 DMS 트리를 확장합니다.

   사용 가능한 작업 목록에 "연결 만들기" 작업이 나타납니다.
2. "연결 만들기"를 클릭합니다.

   "연결 만들기" 작업 페이지가 나타납니다.
3. 대화 상자의 필드를 입력합니다. 다음 필드는 자동으로 채워지지 않습니다.

   연결 이름

   이 연결에 사용할 이름을 정의합니다.

   연결 유형

   만들고 있는 연결 유형을 나타냅니다(AC).

   설명

   (선택 사항) 이 연결에 대한 설명을 정의합니다.

   호스트 이름

   CA Access Control 엔터프라이즈 관리가 작업할 DMS 의 이름을 정의합니다.

   형식: DMS*Name*@*hostName*

   예를 들어 host1.comp.com 호스트에 CA Access Control 엔터프라이즈 관리를 설치할 때 설치되는 기본 DMS 를 사용하려면 DMS__@host1.comp.com 을 입력하십시오.

사용자 ID

DMS 에 대한 관리 권한이 있는 사용자의 이름을 정의합니다.

작성한 전용 프록시 사용자를 사용하는 것이 좋으며, 로그인한 사용자를 대신하여 CA Access Control 엔터프라이즈 관리 작업 수행에 기본 관리 사용자를 사용하지 않는 것이 좋습니다.

참고: DMS 감사 레코드가 CA Access Control 엔터프라이즈 관리에 로그인한 사용자를 대신하여 정의된 프록시 사용자가 데이터베이스 명령을 실행했음을 보여줍니다.

암호

DMS 에 대한 관리 권한이 있는 사용자의 암호를 정의합니다.

기본 연결

로그인할 때 CA Access Control 엔터프라이즈 관리가 기본값으로 사용한 연결인지 지정합니다.

참고: 기본 연결을 지정하는 경우 로그아웃한 후 연결하기 전에 다시 로그인해야 합니다.

"제출"을 클릭합니다.

CA Access Control 엔터프라이즈 관리는 사용자가 지정한 정보를 사용하여 DMS 에 로그인을 시도합니다. 정보가 정확하면 연결이 성공하고 CA Access Control 엔터프라이즈 관리를 사용하여 CA Access Control 의 엔터프라이즈 배포를 관리할 수 있게 됩니다. 정보가 정확하지 않아 CA Access Control 엔터프라이즈 관리가 DMS 에 로그인할 수 없으면 오류 메시지가 표시되어 연결이 실패한 원인을 보여 줍니다.

배포 호스트(DH) 업그레이드

DMS 를 성공적으로 업그레이드한 다음에는 배포 호스트(DH)를 업그레이드합니다. 배포 호스트를 실행하는 모든 컴퓨터에 배포 서버를 설치하여 DH 를 업그레이드합니다.

배포 서버를 설치한 다음에는 배포 서버와 CA Access Control 엔터프라이즈 관리 사이에서 메시지를 주고받기 위한 라우트를 구성하기 위해 메시지 큐 라우팅 설정을 구성합니다.

중요! DH 가 CA Access Control 엔터프라이즈 관리와 다른 컴퓨터에 설치된 경우에만 이 단계를 수행하십시오.

배포 호스트를 업그레이드하려면

1. DH 컴퓨터에 배포 서버를 설치합니다 (페이지 53).

   배포 서버는 JCS(Java Connector Server), DH, 메시지 큐를 설치합니다.

2. 배포 서버와 CA Access Control 엔터프라이즈 관리 사이의 메시지 큐 라우팅 설정을 정의 (페이지 54)합니다.

   배포 서버가 이제 구성되었습니다.

배포 서버 설치

재해 복구 또는 고가용성 환경에서 동작하도록 CA Access Control 를 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 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.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.

메시지 라우팅 설정 구성 방법

엔터프라이즈 관리 서버의 단일 인스턴스와 여러 배포 서버로 구성된 환경에서 작업할 때는 엔터프라이즈 관리 서버의 MQ 를 가리키도록 모든 배포 서버에서 MQ 라우팅 설정을 구성해야 합니다. 이렇게 하면 CA Access Control 끝점이 보내는 모든 메시지가 궁극적으로 엔터프라이즈 관리 서버에 있는 단일 MQ 로 라우팅됩니다.

모든 배포 서버에 있는 MQ 에서 엔터프라이즈 관리 서버로 메시지를 라우팅하려면 다음을 수행하십시오.

- 환경에 있는 각 배포 서버에서 다음을 수행합니다.
  - 메시지 큐 서비스를 중지합니다.
  - 엔터프라이즈 관리 서버 메시지 큐에 대한 라우팅을 수정합니다.
  - 엔터프라이즈 관리 서버 메시지 큐의 매개 변수를 정의합니다.
  - 배포 서버 메시지 큐의 이름을 구성합니다.
  - 엔터프라이즈 관리 서버 메시지 큐의 위치를 지정합니다.
  - 메시지 큐 서비스를 시작합니다.
- 엔터프라이즈 관리 서버에서 다음을 수행하십시오.
  - 메시지 큐 서비스를 중지합니다.
  - 배포 서버 메시지 큐에 대한 라우팅을 수정합니다.
  - 배포 서버 메시지 큐의 매개 변수를 정의합니다.
  - 엔터프라이즈 관리 서버 메시지 큐의 이름을 구성합니다.
  - 엔터프라이즈 관리 서버 메시지 큐의 위치를 지정합니다.
  - 메시지 큐 서비스를 시작합니다.

참고: 메시지 라우팅에 대한 자세한 내용은 *TIBCO Enterprise Message Server User's Guide* 를 참조하십시오. Tibco 설명서는 메시지 큐의 일부로서 설치되며 *ACServerInstallDir*/MessageQueue/tibco/ems/5.1/doc 에 있습니다.

배포 서버에서 메시지 큐 설정 수정

기본적으로 모든 배포 서버는 해당 서버에서 실행 중인 메시지 큐와 동작하도록 구성되어 있습니다. 메시지를 또 다른 메시지 큐로 라우팅하려면 메시지 큐 설정을 다시 구성해야 합니다.

이 절차는 CA Access Control 엔터프라이즈 관리 메시지 큐와의 통신을 활성화하기 위해 배포 서버에서 메시지 큐 설정을 수정하는 방법을 보여줍니다. 환경에 있는 모든 배포 서버에 대해 이 절차를 완료하십시오.

배포 서버에서 메시지 큐 설정을 수정하려면

1. CA Access Control 메시지 큐 서비스를 중지합니다.

   중요! CA Access Control 메시지 큐 서비스를 중지하면 CA DSM r11 Common Application Framework 서비스 또한 중지됩니다.

2. 배포 서버에서 tibemsd.conf 파일을 엽니다. 이 파일은 기본적으로 아래 디렉터리에 있습니다. 여기서 *DistServerInstallDir* 는 배포 서버를 설치한 디렉터리를 나타냅니다.

   DistServerInstallDir/ACMQ/tibco/cfgmgmt/ems/data

3. 'server' 매개 변수에 배포 서버의 약식 호스트 이름을 입력합니다.
4. 'routing' 매개 변수 값을 활성화되도록 변경합니다.
5. CA Access Control 메시지 큐 서비스를 시작합니다.

   배포 서버에서 메시지 큐 설정을 수정했습니다.

참고: 메시지 라우팅에 대한 자세한 내용은 *TIBCO Enterprise Message Server User's Guide* 를 참조하십시오. Tibco 설명서는 메시지 큐의 일부로서 설치되며 *ACServerInstallDir*/MessageQueue/tibco/ems/5.1/doc 에 있습니다.

예: tibemsd.conf 파일

이 예제는 DS_Example 이란 이름의 배포 서버에 대한 라우팅 설정을 수정한 이후의 tibemsd.conf 파일의 코드 조각을 보여줍니다.

```
#####################
# Server Identification Information.
# server:    unique server name
# password:  password used to login into other routed server
#####################
server                  = DS_Example
password                =
#####################
…
#####################
# Routing. Routes configuration is in 'routes.conf'. This enables or
# disables routing functionality for this server.
#####################
routing                 = enabled
#####################
```

엔터프라이즈 관리 서버에서 메시지 큐 설정 수정

이 절차는 배포 서버와의 통신을 활성화하기 위해 엔터프라이즈 관리 서버에서 메시지 큐 설정을 수정하는 방법을 보여줍니다.

엔터프라이즈 관리 서버에서 메시지 큐 설정을 수정하려면

1. CA Access Control 메시지 큐 서비스를 중지합니다.

   중요! CA Access Control 메시지 큐 서비스를 중지하면 CA DSM r11 Common Application Framework 서비스 또한 중지됩니다.

2. 엔터프라이즈 관리 서버에서 편집을 위해 tibemsd.conf 파일을 엽니다. 이 파일은 다음 디렉터리에 있습니다. 여기서 *ACServerInstallDir* 는 엔터프라이즈 관리 서버를 설치한 디렉터리를 나타냅니다.

   ACServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data

3. 엔터프라이즈 관리 서버 약식 호스트 이름을 'server' 매개 변수에 점으로 구분하지 않고 입력합니다.

4. 'routing' 매개 변수 값을 활성화되도록 변경합니다.
5. CA Access Control 메시지 큐 서비스를 시작합니다.

   엔터프라이즈 관리 서버에서 메시지 큐 설정을 수정했습니다.

참고: 메시지 라우팅에 대한 자세한 내용은 *TIBCO Enterprise Message Server User's Guide* 를 참조하십시오. Tibco 설명서는 메시지 큐의 일부로서 설치되며 *ACServerInstallDir*/MessageQueue/tibco/ems/5.1/doc 에 있습니다.

예: tibemsd.conf 파일

이 예제는 ENTM_Example 이란 이름의 CA Access Control 엔터프라이즈 관리 서버에 대한 라우팅 설정을 수정한 이후의 tibemsd.conf 파일의 코드 조각을 보여줍니다.

```
######################
# Server Identification Information.
# server:    unique server name
# password:  password used to login into other routed server
######################
server                  = ENTM_Example
password                =
######################
…
######################
# Routing. Routes configuration is in 'routes.conf'. This enables or
# disables routing functionality for this server.
######################
routing                 = enabled
######################
```

메시지 큐 연결 구성

배포 서버의 메시지 큐에서 메시지를 엔터프라이즈 관리 서버로 메시지를 반대로 라우팅하려면 회사에서 기존 메시지 큐 설정을 수정합니다.

예: 배포 서버에서 메시지 큐 연결 설정 구성

이 예는 배포 서버에서 메시지 큐 서버 설정을 구성하는 방법을 보여줍니다. 엔터프라이즈 관리 서버에서 실행 중인 메시지 큐의 매개 변수를 정의하는 방법으로, 엔터프라이즈 관리 서버로 메시지를 보내도록 메시지 큐를 구성합니다.

다음 단계를 수행하십시오.

1. 배포 서버에서 다음 중 하나를 수행합니다.
   - (Windows 2003 Server) "시작", "프로그램", "TIBCO-CA_AC, TIBCO EMS 5.1", "Start EMS Administration Tool"을 차례로 선택합니다.
   - (UNIX) 다음을 수행합니다.
     a. 다음 디렉터리로 이동합니다. 여기서 *DistServerInstallDir* 는 배포 서버를 설치한 디렉터리를 나타냅니다.

        DistServerInstallDir/MessageQueue/tibco/ems/5.1/bin

     b. 다음 명령을 실행합니다.

        tibemsadmin

        TIBCO EMS Administration Tool 명령 프롬프트 창이 열립니다.
2. 다음 중 하나를 사용하여 메시지 큐에 연결합니다.
   - SSL 를 사용하여 연결하려면 다음 명령을 입력하십시오.

     connect ssl://localhost:7243
   - TCP 를 사용하여 연결하려면 다음 명령을 입력하십시오.

     connect tcp://localhost:7222

   로그인 이름 프롬프트가 나타납니다.
3. **admin** 을 입력합니다.

   암호 프롬프트가 나타납니다.
4. 배포 서버를 설치할 때 제공한 암호를 입력합니다.
5. 요청되는 경우 메시지 큐 서버에 대한 새 암호를 입력합니다.
6. 메시지 큐 암호를 정의합니다.

   set server password=

   예: set server password=*<C0mp1ex>*
7. ENTM-NAME 이란 이름의 사용자를 만들어 암호를 할당합니다.

   create user ENTM-NAME password=*acserver_user-passwd*

   예: create user EMS-SERVER password=*<acserver_user-passwd>*

   중요! 엔터프라이즈 관리 서버에 tibemsd.conf 파일의 'server' 매개 변수에 정의한 것과 동일한 이름을 지정합니다.

8. 다음 작업을 수행하십시오.
   a. 다음 명령을 입력합니다.

      ```
      add member ac_server_users ENTM_NAME
      ```

      생성한 사용자가 ac_server_users 그룹에 추가되었습니다.
   b. 다음 명령을 입력합니다.

      ```
      add member ac_endpoint_users ENTM_NAME
      ```

      생성한 사용자가 ac_endpoint_users 그룹에 추가되었습니다.
   c. 다음 명령을 입력합니다.

      ```
      add member report_publishers ENTM_NAME
      ```

      생성한 사용자에게 메시지를 읽고 CA Access Control 큐에 게시할 수 있는 권한이 부여되었습니다.
9. 배포 서버를 다시 시작합니다.

   변경 사항이 적용되었습니다.

예: 엔터프라이즈 관리 서버에서 메시지 큐 연결 설정 구성

이 예는 엔터프라이즈 관리 서버에서 메시지 큐 서버 설정을 구성하는 방법을 보여줍니다. 배포 서버로 메시지를 보내기 위해 메시지 큐를 구성합니다.

이 예제에서 *DS-NAME* 은 배포 서버 컴퓨터의 이름을 의미하며 *ENTM-NAME* 은 엔터프라이즈 관리 서버의 이름을 의미합니다. 메시지 큐 서버 설정을 정의할 때 이 이름을 *tibemsd.conf* 파일의 'server' 토큰에 정의된 서버의 실제 이름으로 대체합니다.

다음 단계를 수행하십시오.

1. 엔터프라이즈 관리 서버에서 다음 중 하나를 수행하십시오.
   - (Windows 2003 Server) "시작", "프로그램", "TIBCO-CA_AC, TIBCO EMS 5.1", "Start EMS Administration Tool"을 차례로 선택합니다.
   - (UNIX) 다음을 수행합니다.
     a. 다음 디렉터리로 이동합니다. 여기서 *ACServerInstallDir* 는 엔터프라이즈 관리 서버를 설치한 디렉터리를 나타냅니다.

        ```
        ACServerInstallDir/MessageQueue/tibco/ems/5.1/bin
        ```

     b. 다음 명령을 실행합니다.

        ```
        tibemsadmin
        ```

        TIBCO EMS Administration Tool 명령 프롬프트 창이 열립니다.
2. 다음 중 하나를 사용하여 메시지 큐에 연결합니다.
   - SSL 를 사용하여 연결하려면 다음 명령을 입력하십시오.

     ```
     connect ssl://localhost:7243
     ```
   - TCP 를 사용하여 연결하려면 다음 명령을 입력하십시오.

     ```
     connect tcp://localhost:7222
     ```

   로그인 이름 프롬프트가 나타납니다.
3. **admin** 을 입력합니다.

   암호 프롬프트가 나타납니다.
4. 엔터프라이즈 관리 서버를 설치할 때 제공한 암호를 입력합니다.
5. 메시지 큐 암호를 정의합니다.

   ```
   set server password=entm_server-passwd
   ```

   예: set server password=*<ENTM_SERVER_NAME-passwd>*

6. 각 배포 서버에 대해 DS-NAME 이란 이름의 사용자를 만들어 암호를 할당합니다.

   ```
   create user DS-NAME password=dist_server_user
   ```

   예: create user EMS-Server password=*<C0mp1ex>*

   중요! 엔터프라이즈 관리 서버에 tibemsdf.conf 파일의 'server' 매개 변수에 정의한 것과 동일한 이름을 지정합니다.

7. 다음 작업을 수행하십시오.

   a. 다음 명령을 입력합니다.

      ```
      add member ac_server_users DS_NAME
      ```

      생성한 사용자가 ac_server_users 그룹에 추가되었습니다.

   b. 다음 명령을 입력합니다.

      ```
      add member ac_endpoint_users DS_NAME
      ```

      생성한 사용자가 ac_endpoint_users 그룹에 추가되었습니다.

   c. 다음 명령을 입력합니다.

      ```
      add member report_publishers DS_NAME
      ```

      생성한 사용자에게 메시지를 읽고 CA Access Control 큐에 게시할 수 있는 권한이 부여되었습니다.

8. 변경 사항을 적용하려면 배포 서버를 다시 시작해야 합니다.

   엔터프라이즈 관리 서버에서 메시지 큐 연결 설정을 구성했습니다.

참고: 메시지 라우팅에 대한 자세한 내용은 *TIBCO Enterprise Message Server User's Guide* 를 참조하십시오. Tibco 설명서는 메시지 큐의 일부로서 설치되며 *ACServerInstallDir*/MessageQueue/tibco/ems/5.1/doc 에 있습니다.

배포 서버에서 메시지 큐의 이름 구성

배포 서버에서 엔터프라이즈 관리 서버로 메시지를 전달하려면 배포 서버의 메시지 큐에서 엔터프라이즈 관리 서버의 메시지 큐로 메시지를 전달하도록 각 메시지 경로를 구성하십시오.

이 절차는 배포 서버에서 메시지 큐 설정을 정의합니다. 엔터프라이즈 관리 서버의 메시지 큐 설정을 제공하기 위해 메시지 큐 설정 파일을 수정합니다.

배포 서버에서 메시지 큐의 이름을 구성하려면

1. 배포 서버에서 queues.conf 파일을 엽니다. 이 파일은 기본적으로 다음 디렉터리에 있습니다. 여기서 *DistServerInstallDir* 는 배포 서버를 설치한 디렉터리를 나타냅니다.

   DistServerInstallDir/ACMQ/tibco/cfgmgmt/ems/data

2. 'queue/snapshots'란 이름의 큐를 찾아 큐 이름 끝에 다음과 같이 @ 기호 뒤에 ENTM-NAME 값을 추가합니다.

   queue/snapshots*@ENTM-NAME*

   ENTM-NAME

   엔터프라이즈 관리 서버의 약식 이름을 정의합니다.

   중요! 엔터프라이즈 관리 서버에 tibemsd.conf 파일의 'server' 매개 변수에 정의한 것과 동일한 이름을 지정합니다.

3. 'queue/audit'이란 이름의 큐를 찾아 큐 이름 끝에 다음과 같이 @ 기호 뒤에 ENTM-NAME 값을 추가합니다.

   queue/audit*@ENTM-NAME*

4. 'ac_endpoint_to_server'란 이름의 큐를 찾아 큐 이름 끝에 다음과 같이 @ 기호 뒤에 ENTM-NAME 값을 추가합니다.

   ac_endpoint_to_server*@ENTM-NAME*

5. 'ac_server_to_endpoint'란 이름의 큐를 찾아 큐 이름 끝에 다음과 같이 @ 기호 뒤에 ENTM-NAME 값을 추가합니다.

   ac_server_to_endpoint*@ENTM-NAME*

6. 파일을 저장한 후 닫습니다.

참고: 메시지 라우팅에 대한 자세한 내용은 *TIBCO Enterprise Message Server User's Guide* 를 참조하십시오. Tibco 설명서는 메시지 큐의 일부로서 설치되며 *ACServerInstallDir*/MessageQueue/tibco/ems/5.1/doc 에 있습니다.

엔터프라이즈 관리 서버에서 메시지 큐의 이름 구성

이 절차에서는 엔터프라이즈 관리 서버에서 메시지 라우팅 설정을 정의합니다. 이 메시지 큐를 기본 서버로 식별하도록 엔터프라이즈 관리 서버에서 메시지 큐 설정을 구성합니다.

엔터프라이즈 관리 서버에서 메시지 큐의 이름을 구성하려면

1. 엔터프라이즈 관리 서버에서 queues.conf 파일을 편집 가능한 형식으로 엽니다. 이 파일은 다음 디렉터리에 있습니다. 여기서 *ACServerInstallDir* 는 엔터프라이즈 관리 서버를 설치한 디렉터리를 나타냅니다.

   ACServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data

2. 'queue/snapshots'란 이름의 큐를 찾아 다음과 같이 큐 이름 끝에 'secure'란 단어 다음에 'global'이란 단어를 추가합니다.

   ```
   queue/snapshot secure, global
   ```

3. 'queue/audit'이란 이름의 큐를 찾아 다음과 같이 큐 이름 끝에 'secure'란 단어 다음에 'global'이란 단어를 추가합니다.

   ```
   queue/audit secure, global
   ```

4. 'ac_endpoint_to_server'란 이름의 큐를 찾아 다음과 같이 큐 이름 끝에 'secure'란 단어 다음에 'global'이란 단어를 추가합니다.

   ```
   ac_endpoint_to_server secure, global
   ```

5. 'ac_server_to_endpoint'란 이름의 큐를 찾아 다음과 같이 큐 이름 끝에 'secure'란 단어 다음에 'global'이란 단어를 추가합니다.

   ```
   ac_server_to_endpoint secure, global
   ```

6. 파일을 저장한 후 닫습니다.

참고: 메시지 라우팅에 대한 자세한 내용은 *TIBCO Enterprise Message Server User's Guide* 를 참조하십시오. Tibco 설명서는 메시지 큐의 일부로서 설치되며 *ACServerInstallDir*/MessageQueue/tibco/ems/5.1/doc 에 있습니다.

메시지 라우팅 구성

메시지 큐 설정을 구성하고 배포 서버와 엔터프라이즈 관리 서버에서 메시지 큐 라우팅 설정을 구성한 이후에 배포 서버와 엔터프라이즈 관리 서버에서 메시지 경로를 설정합니다.

예: 배포 서버에서 메시지 라우트 설정

이 예는 배포 서버에서 메시지 라우트 설정을 구성하는 방법을 보여줍니다. CA Access Control 끝점에서 받는 메시지를 엔터프라이즈 관리 서버의 메시지 큐로 라우팅하도록 배포 서버와 엔터프라이즈 관리 서버 사이의 경로를 설정합니다. 회사에 있는 모든 배포 서버에 대해 이 절차를 완료하십시오.

1. 배포 서버에서 편집을 위해 routes.conf 파일을 엽니다. 이 파일은 기본적으로 다음 디렉터리에 있습니다. 여기서 *DistServerInstallDir* 는 배포 서버를 설치한 디렉터리를 나타냅니다.

   DistServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data

2. 다음 행을 추가합니다.

   ```
   [ENTM-NAME]
   url          = ENTM-URL
   ssl_verify_host = disabled
   ssl_verify_hostname = disabled
   ```

   ENTM-NAME

   엔터프라이즈 관리 서버의 약식 이름을 정의합니다.

   ENTM_URL

   엔터프라이즈 관리 서버 URL 을 정의합니다.

3. 파일을 저장합니다.
4. CA Access Control 메시지 큐 서비스를 다시 시작합니다.

예: 엔터프라이즈 관리 서버에서 메시지 경로 설정

이 예는 엔터프라이즈 관리 서버에서 메시지 경로 설정을 구성하는 방법을 보여줍니다. 엔터프라이즈 관리 서버에서 배포 서버로, 그리고 배포 서버에서 끝점으로 메시지를 보내도록 엔터프라이즈 관리 서버와 배포 서버 사이의 경로를 설정합니다.

1. 엔터프라이즈 관리 서버에서 routes.conf 파일을 엽니다. 이 파일은 기본적으로 다음 디렉터리에 있습니다. 여기서 *ACServerInstallDir* 는 엔터프라이즈 관리 서버를 설치한 디렉터리를 나타냅니다.

   ACServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data

2. 다음 행을 추가합니다.

   ```
   [DS-NAME]
   url          = DS-URL
   ssl_verify_host = disabled
   ssl_verify_hostname = disabled
   ```

   DS_NAME

   배포 서버의 약식 이름을 정의합니다.

   DS_URL

   배포 서버 URL 을 정의합니다.

3. 파일을 저장합니다.
4. CA Access Control 메시지 큐 서비스를 다시 시작합니다.

참고: 메시지 라우팅에 대한 자세한 내용은 *TIBCO Enterprise Message Server User's Guide* 를 참조하십시오. Tibco 설명서는 메시지 큐의 일부로서 설치되며 *ACServerInstallDir*/MessageQueue/tibco/ems/5.1/doc 에 있습니다.

보고서 서버를 엔터프라이즈 보고 서비스로 마이그레이션

엔터프라이즈 보고 서비스는 하나의 엔터프라이즈 전체 보고 서비스에 보고서 서버 기능을 추가합니다. 아키텍처 변경으로 인해 보고서 서버는 이제 CA Access Control 엔터프라이즈 관리의 일부로 포함되어 있으며 독립적인 구성 요소로 제공되지 않습니다. 보고서 서버에 배포 서버를 설치하고 메시지 큐 설정을 다시 구성하여 보고서 서버를 마이그레이션합니다.

참고: 이 마이그레이션 프로세스는 기존 끝점이 보고서 서버 컴퓨터에서 메시지 큐를 계속 사용하도록 합니다. 이 절차를 완료한 다음 끝점에서 ReportAgent 설정을 다시 구성할 필요는 없습니다.

중요! 보고서 서버가 CA Access Control 엔터프라이즈 관리와 다른 컴퓨터에 설치된 경우에만 이 단계를 수행하십시오.

다음 단계를 수행하십시오.

1. 보고서 서버 컴퓨터에 배포 서버를 설치합니다 (페이지 53).
2. JBoss 서비스를 비활성화합니다.
3. 배포 서버와 CA Access Control 엔터프라이즈 관리 사이의 메시지 큐 라우팅 설정을 정의 (페이지 54)합니다.

   엔터프라이즈 보고 서비스(보고서 서버 포함)가 설치됩니다. 이제 엔터프라이즈 보고 서버 구성 요소를 구성할 수 있습니다.

   참고: 엔터프라이즈 보고 서버 구성 요소에 대한 자세한 내용은 *엔터프라이즈 관리 안내서*를 참조하십시오.
4. 새 DMS 에 DH 를 구독합니다. (페이지 68)

DMS 에 DH 구독

CA Access Control 엔터프라이즈 관리 구성 요소의 업그레이드가 완료되면 더 이상 이전 DMS 를 사용하여 작업할 수 없게 됩니다. CA Access Control 엔터프라이즈 관리를 시작하기 전에 새 DMS 를 사용하여 작업하려면 업그레이드된 DH 를 구성해야 합니다.

중요! 보고서 서버 컴퓨터에 배포 서버를 설치한 경우에만 이 단계를 완료하십시오.

다음 단계를 수행하십시오.

1. 배포 서버에서 명령 프로그램 창을 엽니다.
2. 배포 서버에 새 DMS 를 구독합니다.

   ```
   sepmd -s DH__WRITER DMS__@<entm>
   ```

3. 새 DMS 를 배포 호스트 부모로 추가합니다.

   ```
   sepmd -s DMS__ DH__@<host_name>
   ```

4. 엔터프라이즈 관리 서버에서 명령 프롬프트 창을 열고 새 구독자를 만듭니다.

   ```
   sepmd -n DH__@<host_name>
   ```

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

CA Access Control 끝점 업그레이드

CA Access Control 엔터프라이즈 관리, DMS, 배포 호스트, 보고서 서버를 업그레이드한 다음에는 이제 기존 CA Access Control r12.0 SP1 끝점을 업그레이드할 수 있습니다.

CA Access Control 끝점을 업그레이드하려면 끝점에 CA Access Control 을 설치 (페이지 28)하십시오.

제 4 장: PMD 를 고급 정책 관리 환경으로 마이그레이션

이 섹션은 다음 항목을 포함하고 있습니다.

고급 정책 관리 환경으로 마이그레이션

PMD(정책 모델) 환경에서 고급 정책 관리 환경으로 마이그레이션하면 규칙을 끝점에 배포하는 방법이 변경됩니다.

- PMD 환경에서는 중앙 데이터베이스(PMDB)에 정의한 일반 규칙이 구성된 계층의 데이터베이스에 자동으로 전파됩니다.
- 고급 정책 관리 환경에서는 하나 이상의 호스트 또는 호스트 그룹에 정책(규칙 그룹)을 할당합니다. 정책을 배포 취소(제거)하고 배포 상태와 배포 위반을 확인할 수도 있습니다.

PMD 환경에서 고급 정책 관리 환경으로 마이그레이션하는 경우 다음을 수행합니다.

- 추가 구성 요소 설치
- PMDB 의 규칙에서 정책 만들기
- 끝점 업그레이드
- PMD 구조 평면화

고급 정책 관리는 계층적 호스트 그룹을 지원하지 않습니다. 사용하는 PMD 아키텍처가 계층적 PMDB 를 포함하는 경우 PMD 계층을 평면화해야 합니다.

참고: 고급 정책 관리에서는 암호 관리 명령이 포함된 정책을 지원하지 않습니다. 암호 PMD 를 사용하여 끝점 간에 암호를 동기화하고 암호 관리 규칙을 배포해야 합니다. 암호 PMD 는 고급 정책 관리 환경으로 마이그레이션할 수 없습니다. 대신, 암호 PMD 에 필터 파일을 적용하여 구독자에게 암호 규칙만 보내도록 할 수 있습니다.

마이그레이션 프로세스 동작 방식

고급 정책 관리 환경으로 마이그레이션하면 정책을 배포 및 배포 취소하고 정책의 배포 상태 및 위반 상태를 확인할 수 있습니다. CA Access Control 을 사용하여 대부분의 마이그레이션 작업을 수행할 수 있지만 일부 작업은 사용자가 여전히 직접 수행해야 합니다. 마이그레이션 프로세스가 동작하는 방식을 이해하면 이후 발생할 수도 있는 문제를 해결하는 데 도움이 될 것입니다.

다음 절차는 마이그레이션 프로세스의 단계에 대해 개괄적으로 설명합니다.

1. 엔터프라이즈 관리 서버 구성 요소를 설치합니다.

   엔터프라이즈 관리 설치 프로세스의 일부로 고급 정책 관리 환경이 설정됩니다.

2. PMD 를 CA Access Control r12.5 이상으로 업그레이드합니다.
3. PMD 를 구독하는 끝점을 고급 정책 관리 환경으로 마이그레이션합니다.
4. CA Access Control 엔터프라이즈 관리에서 PMDB 의 규칙을 정책 파일로 내보냅니다.
5. CA Access Control 엔터프라이즈 관리는 DMS 에 다음 항목을 만듭니다.
   - 마이그레이션된 PMDB 에 해당하는 호스트 그룹(GHNODE 개체)
   - PMDB 의 끝점 구독자에 해당하는 호스트(HNODE 개체)
   - 정책 파일에 있는 규칙을 포함하는 POLICY 개체

6. CA Access Control 엔터프라이즈 관리에서 사용자는 호스트 그룹에 호스트를 조인합니다. CA Access Control 은 POLICY 개체를 호스트 그룹에 할당하고 PMDB 의 끝점 구독자에 해당하는 호스트로 POLICY 개체를 배포합니다.
7. CA Access Control 엔터프라이즈 관리에서 다음 중 *하나*를 수행합니다.
   - PMD 가 암호 PMD 인 경우 PMD 에 필터 파일을 적용합니다.
   - PMD 가 암호 PMD 가 아닌 경우 PMD 를 삭제합니다.

참고: 또한 policydeploy 유틸리티를 사용하여 마이그레이션 작업을 수행할 수도 있습니다.

추가 정보:

고급 정책 관리로 마이그레이션하는 방법 (페이지 74)

정책을 만들어 할당하는 방법

PMD 환경에서 고급 정책 관리 환경으로 마이그레이션할 때 CA Access Control 을 사용하여 PMDB 에 있는 규칙으로부터 정책을 만든 다음 이 정책을 DMS 에 있는 호스트 그룹에 할당합니다.

다음 절차는 CA Access Control 에서 정책을 만들어 할당하는 방법을 설명합니다.

1. CA Access Control 은 PMDB 에 있는 규칙을 정책 파일로 내보냅니다.

   참고: CA Access Control 이 특정 클래스에 있는 리소스만 수정하는 규칙만 내보내도록 지정할 수 있습니다.
2. CA Access Control 은 새 리소스나 접근자를 만드는 각 규칙을 리소스나 접근자를 수정하는 규칙으로 변경합니다. 예를 들어, CA Access Control 은 모든 newres 규칙을 editres 규칙으로 변경합니다.

   이 단계는 새 리소스와 접근자를 만드는 규칙을 동일한 끝점에 여러 번 배포하는 경우 발생하는 배포 오류를 방지합니다.
3. CA Access Control 은 PMD 에 해당하는 호스트 그룹(GHNODE 개체)을 DMS 에 만듭니다.

4. PMDB 에 나열되어 있는 각 끝점 구독자에 대해 CA Access Control 은 해당 호스트(HNODE 개체)가 이미 DMS 에 있는지 여부를 검사합니다.
   - PMDB 에 나열되어 있고 DMS 에 해당 호스트가 있는 각 구독자에 대해 CA Access Control 은 3 단계에서 만든 호스트 그룹에 이 호스트를 조인합니다.
   - PMDB 에 나열되어 있고 DMS 에 해당 호스트가 없는 각 구독자에 대해 CA Access Control 은 끝점에 해당하는 호스트를 만들어 이 호스트를 3 단계에서 만든 호스트 그룹에 조인합니다.

   참고: CA Access Control 은 구독자 PMDB 에 해당하는 호스트를 만들지 않습니다.
5. CA Access Control 은 내보낸 정책 파일에 있는 규칙을 사용하여 DMS 에 POLICY 개체를 만듭니다.

   참고: CA Access Control 은 POLICY 개체에 대한 배포 취소 스크립트를 만들지 않습니다.
6. CA Access Control 은 POLICY 개체를 3 단계에서 만든 호스트 그룹에 할당합니다.

추가 정보:

PMDB 마이그레이션 (페이지 76)

처음에 정책이 마이그레이션된 끝점으로 전송되는 방법

PMD 환경에서 고급 정책 관리 환경으로 마이그레이션할 때 CA Access Control 은 PMDB 에 있는 규칙으로부터 정책을 만든 다음 마이그레이션된 끝점으로 전달합니다. CA Access Control 이 처음에 정책을 마이그레이션된 끝점으로 보내는 방법을 이해하면 마이그레이션 프로세스 중에 발생하는 오류를 해결하는 데 도움이 될 수 있습니다.

다음 프로세스에서는 끝점에서 CA Access Control 을 시작한 후 처음에 정책이 마이그레이션된 끝점으로 전송되는 방법에 대해 설명합니다.

1. CA Access Control 이 하트비트 알림을 DMS 로 보내는 policyfetcher 를 시작하고 호출합니다.
2. DMS 가 하트비트 알림을 받고 DMS 에 해당 호스트(HNODE) 개체가 있는지 확인합니다.

3. 다음 중 *한 가지* 결과가 나타납니다.
   - 해당 호스트가 DMS 에 있고 호스트가 마이그레이션한 PDM 에 해당하는 호스트 그룹의 구성원인 경우:
     a. CA Access Control 이 끝점과 호스트를 연관시킵니다.
     b. CA Access Control 이 호스트 그룹에 할당된 정책을 끝점에 배포합니다.
   - 해당 호스트가 DMS 에 없는 경우:
     a. CA Access Control 이 보고서를 만듭니다.
     b. 정책을 만들어 할당할 때 CA Access Control 은 마이그레이션한 PMD 에 해당하는 호스트 그룹에 호스트를 조인합니다.
     c. CA Access Control 이 호스트 그룹에 할당된 정책을 끝점에 배포합니다.
4. CA Access Control 은 정책에 나열된 각 리소스의 "업데이트 시간" 속성을 정책이 배포된 시간으로 수정합니다.

   참고: CA Access Control 이 개체를 만드는 명령을 개체 수정 명령으로 변경했으므로 정책에 대한 배포 오류가 표시되지 않습니다.

참고: 정책 및 호스트 그룹에 대한 자세한 내용은 *엔터프라이즈 관리 안내서*를 참조하십시오.

CA Access Control 이 암호 PMD 에 필터 파일을 적용하는 방법

고급 정책 관리에서는 암호 관리 명령을 사용한 정책을 지원하지 않습니다. 끝점 사이에서 암호를 동기화하고 암호 관리 규칙을 배포하려면 암호 PMD 를 사용해야 합니다. 암호 PMD 를 고급 정책 관리 환경으로 마이그레이션할 때는 암호 규칙만 구독자에게 배포하기 위해 암호 PMD 에 필터 파일을 적용합니다.

다음 프로세스는 CA Access Control 이 암호 PMD 에 필터 파일을 적용하는 방법에 대해 설명합니다.

1. CA Access Control 은 filter.flt 란 이름의 텍스트 파일을 만들어 다음 줄을 이 파일에 추가합니다.

```
#-------------------------------------------------------------------------
--
# access    env     class   objects properties              pass/nopass
#-------------------------------------------------------------------------
--
  *         *       USER    *       OLD_PASSWD;CLR_PASSWD   PASS
  *         *       *       *       *                       NOPASS
#-------------------------------------------------------------------------
--
```

2. CA Access Control 은 filter.flt 파일을 암호 PMD 디렉터리에 저장합니다.
3. CA Access Control 은 filter.flt 파일의 전체 경로를 다음 위치에 있는 "filter" 구성 설정에 추가합니다.
   - (UNIX) pmd.ini 파일의 [pmd] 섹션
   - (Windows) 다음 레지스트리 키

     HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Pmd*PMDB_Name*

고급 정책 관리로 마이그레이션하는 방법

고급 정책 관리 환경으로 마이그레이션하면 정책을 배포 및 배포 취소하고 정책의 배포 상태 및 위반 상태를 확인할 수 있습니다.

참고: 고급 정책 관리에서는 암호 관리 명령이 포함된 정책을 지원하지 않습니다. 암호 PMD 를 사용하여 끝점 간에 암호를 동기화하고 암호 관리 규칙을 배포해야 합니다. 암호 PMD 는 고급 정책 관리 환경으로 마이그레이션할 수 없습니다.

마이그레이션 프로세스를 시작하기 전에 다음을 확인하십시오.

- 모든 구독자가 있습니다.
- 구독자가 PMDB 에서 모든 업데이트를 받았습니다.
- PMDB 와 동기화된 구독자가 없습니다.

중요! 마이그레이션 프로세스를 시작하기 전에 PMDB 를 백업할 것을 강력히 권장합니다.

PMD 환경에서 고급 정책 관리 환경으로 마이그레이션하려면 다음을 수행합니다.

1. 엔터프라이즈 관리 서버 구성 요소를 설치합니다.

   엔터프라이즈 관리 설치 프로세스의 일부로 고급 정책 관리 환경이 설정됩니다.
2. PMD 호스트를 CA Access Control r12.5 이상으로 업그레이드합니다.
3. 끝점 마이그레이션 (페이지 76)
4. PMDB (페이지 76)를 마이그레이션합니다.

추가 정보:

마이그레이션 프로세스 동작 방식 (페이지 70)

끝점 마이그레이션

끝점 마이그레이션은 PMD 환경에서 고급 정책 관리 환경으로 마이그레이션하는 프로세스에서 세 번째 단계입니다. 앞의 단계에서 다음을 수행했습니다.

- 엔터프라이즈 관리 서버 구성 요소를 설치했습니다.
- PMD 호스트를 CA Access Control r12.5 이상으로 업그레이드했습니다.

이 단계에서는 마이그레이션된 PMDB 를 구독하는 끝점을 마이그레이션합니다.

끝점을 마이그레이션하려면

1. 끝점을 CA Access Control r12.0 이상으로 업그레이드합니다.
2. 끝점에서 다음 명령을 실행하여 고급 정책 관리 클라이언트 구성 요소를 구성합니다.

   ```
   dmsmgr -config -endpoint
   dmsmgr -config -dh dh_name@host_name
   ```

   끝점이 고급 정책 관리 환경으로 업그레이드됩니다.

PMDB 마이그레이션

PMDB 를 마이그레이션하기 전에 전체 마이그레이션 프로세스의 각 단계에서 수행해야 할 단계를 정확히 이해하는 것이 좋습니다. PMDB 를 마이그레이션하는 것은 CA Access Control 의 엔터프라이즈 배포를 고급 정책 관리 환경으로 마이그레이션하는 프로세스에서 하나의 단계에 불과합니다.

PMDB 를 마이그레이션하는 것은 PMD 환경에서 고급 정책 관리 환경으로 마이그레이션하는 프로세스에서 마지막 단계입니다. 앞의 단계에서 다음을 수행했습니다.

- 엔터프라이즈 관리 서버를 설치했습니다.
- PMD 호스트를 CA Access Control r12.5 이상으로 업그레이드했습니다.
- 끝점을 마이그레이션했습니다. 즉, 끝점을 CA Access Control r12.0 또는 이후 버전으로 업그레이드하고 고급 정책 관리 클라이언트 구성 요소를 구성했습니다.

이 단계에서 CA Access Control 엔터프라이즈 관리를 사용하여 PMDB 에 있는 규칙으로부터 정책을 만들고, 마이그레이션된 PMDB 에 대한 호스트 그룹을 만들고, PMDB 구독자에 해당하는 호스트를 이 호스트 그룹에 조인합니다. 또한 호스트 그룹에 새 정책을 할당하도록 선택할 수도 있습니다.

중요! "다음" 단추를 클릭할 때마다 CA Access Control 엔터프라이즈 관리는 DMS 또는 PMDB 에서 작업을 완료합니다. 이러한 작업은 실행 취소하기 어려울 수 있습니다.

PMDB 를 마이그레이션하려면

1. CA Access Control 엔터프라이즈 관리에서 "정책 관리" 탭을 클릭하고, "정책" 하위 탭을 클릭하고, "정책" 트리를 확장한 다음 "PMDB 마이그레이션"을 클릭합니다.

   PMDB 호스트 로그인 페이지가 나타납니다.

2. PMDB 에 액세스할 수 있는 권한이 있는 사용자 이름 및 암호를 입력하고 마이그레이션하려는 PMDB 의 이름을 입력한 다음 "로그인"을 클릭합니다.

   참고: master_pmdb@example 과 같이 *PMDBname@host* 형식으로 PMDB 이름을 지정하십시오.

   "PMDB 마이그레이션 프로세스" 페이지가 "일반" 작업 단계에 나타납니다.

3. 다음 필드를 완성하고 "다음"을 클릭합니다.

   이름

   정책 이름을 정의합니다. 이 이름은 DMS 및 회사에서 고유해야 합니다(회사에서 반드시 고유한 이름을 사용할 필요는 없지만 동일한 이름의 정책이 이미 있으면 정책을 호스트에 배포할 수 없음).

   설명

   (선택 사항) 정책의 비즈니스 설명(자유 텍스트)을 정의합니다. 이 필드를 사용하여 이 정책이 나타내는 내용과 정책을 식별하는 데 도움을 주는 기타 정보를 기록하십시오.

정책 클래스

내보내 정책에 포함할 규칙이 있는 클래스를 지정합니다. 선택 목록 열에 클래스를 지정하지 않으면 모든 클래스를 내보내 정책에 포함합니다.

종속된 클래스 내보내기

선택 목록 열에 지정하는 클래스에 종속된 모든 클래스를 내보내도록 지정합니다. 이 옵션을 선택하지 않으면 CA Access Control 은 선택 목록 열에 지정하는 클래스만 내보냅니다.

"정책 스크립트" 작업 단계가 나타납니다.

4. 내보낸 규칙을 검토하고 필요한 경우 이 규칙을 수정한 후 "다음"을 클릭합니다.

   CA Access Control 엔터프라이즈 관리가 이 규칙에서 정책을 만듭니다. "호스트 그룹" 작업 단계가 나타납니다.

5. 다음과 같이 대화 상자를 완성하고 "다음"을 클릭합니다.

   호스트 그룹

   호스트에 추가할 호스트 그룹의 이름을 지정합니다. 기존 호스트 그룹을 지정하거나 새 호스트 그룹을 만들 수 있습니다.

   참고: 호스트를 기존 호스트 그룹에 추가하면 CA Access Control 은 호스트 그룹에 할당된 모든 정책을 이 호스트에 자동으로 배포합니다.

   정책 할당

   (선택 사항) 호스트 그룹에 정책을 할당하도록 지정합니다.

   할당된 호스트

   호스트 그룹에 호스트를 추가하도록 지정합니다.

   참고: 기본적으로 이 표에는 액세스 권한이 있는 마이그레이션된 PMDB 의 모든 구독자가 포함되어 있습니다. 할당된 호스트 목록에서 호스트를 추가 및 제거할 수 있지만 호스트에 대한 액세스 권한이 없으면 호스트를 호스트 그룹에 추가할 수 없습니다.

   CA Access Control 엔터프라이즈 관리는 호스트를 호스트 그룹에 추가하고 지정된 경우 정책을 호스트 그룹에 할당합니다. PMD 옵션 작업 단계가 나타납니다.

6. 다음 중 마이그레이션된 PMDB 에 적용할 옵션을 모두 선택합니다.

   3 단계(호스트 그룹 단계)에서 지정한 호스트의 구독 취소

   이전 작업 단계에서 선택한 끝점을 마이그레이션된 PMDB 에서 구독 취소하도록 지정합니다.

   모든 PMDB 구독자의 구독 취소

   마이그레이션된 PMDB 에서 모든 구독자의 구독을 취소하도록 지정합니다.

   PMD 삭제

   마이그레이션된 PMDB 를 삭제하도록 지정합니다.

   중요! 사용자 암호 명령을 전파하기 위해 사용하는 경우 PMDB 를 삭제하지 마십시오.

   PMD 필터 파일 추가

   PMDB 가 구독자에게 사용자 암호 명령만 전파하도록 하기 위해 마이그레이션된 PMDB 에 필터 파일을 추가하도록 지정합니다. 이 옵션을 선택하면 마이그레이션된 PMDB 는 암호 PMDB 가 됩니다.

7. "다음"을 클릭합니다.

   CA Access Control 이 지정한 작업을 수행합니다. "마이그레이션 작업 요약" 작업 단계가 나타나고 마이그레이션 프로세스가 완료됩니다.

추가 정보:

정책을 만들어 할당하는 방법 (페이지 71)

클래스 종속성

PMDB 에서 지정된 클래스에 대한 규칙을 내보낼 때 종속된 클래스의 규칙도 함께 내보낼 수 있습니다. CA Access Control 이 종속된 클래스를 내보내도록 지정하는 경우 CA Access Control 은 다음 항목을 내보냅니다.

- 특정 클래스의 리소스를 수정하는 규칙을 내보내고, 이 클래스에 해당 리소스 그룹이 있는 경우 CA Access Control 은 이 리소스 그룹에 있는 리소스를 수정하는 규칙도 또한 내보냅니다.

  예를 들어, FILE 클래스 규칙을 내보내도록 지정하는 경우 CA Access Control 은 FILE 및 GFILE 클래스에 있는 리소스를 수정하는 규칙을 내보냅니다.

- 특정 리소스 그룹에 있는 리소스를 수정하는 규칙을 내보내면 CA Access Control 은 이 리소스 그룹의 구성원 리소스를 수정하는 규칙도 또한 내보냅니다.

  예를 들어, GFILE 클래스 규칙을 내보내도록 지정하는 경우 CA Access Control 은 GFILE 및 FILE 클래스에 있는 리소스를 수정하는 규칙을 내보냅니다.

- 클래스에 PACL 이 있는 특정 클래스의 리소스를 수정하는 규칙을 내보내면 CA Access Control 은 PROGRAM 클래스에 있는 리소스를 수정하는 규칙도 또한 내보냅니다.
- 클래스에 CALACL 이 있는 특정 클래스의 리소스를 수정하는 규칙을 내보내면 CA Access Control 은 CALENDAR 클래스에 있는 리소스를 수정하는 규칙도 또한 내보냅니다.
- 특정 클래스에 있는 리소스를 수정하는 규칙을 내보내고, 해당 클래스에 있는 리소스 중 하나가 CONTAINER 리소스 그룹의 구성원인 경우 CA Access Control 은 CONTAINER 클래스에 있는 리소스를 수정하고 각 CONTAINER 리소스 그룹의 구성원인 리소스를 수정하는 규칙을 내보냅니다.

  예를 들어, CONTAINER 개체에 FILE 개체가 포함되어 있는 경우 CONTAINER 클래스 규칙을 내보내도록 지정하면 CA Access Control 은 CONTAINER 및 FILE 클래스에 있는 리소스를 수정하는 규칙을 내보냅니다.

DMS 에 중복된 HNODE 가 표시됨

증상:

PMD 를 고급 정책 관리 환경으로 마이그레이션한 다음에 동일한 끝점을 나타내는 두 개의 HNODE 가 DMS 에 생성되었습니다.

해결책:

끝점의 정규화된 호스트 이름이 DMS 와 끝점에서 같지 않습니다. 이 문제를 해결하려면 DMS 에서 HNODE 개체 중 하나를 삭제하십시오.

참고: HNODE 개체 및 DMS 에 대한 자세한 내용은 *끝점 관리 안내서*를 참조하십시오.

계층적 PMDB 마이그레이션

고급 정책 관리는 계층적 호스트 그룹을 지원하지 않습니다. 사용하는 PMD 아키텍처가 계층적 PMDB 를 포함하는 경우 마이그레이션 프로세스 중 PMD 계층을 평면화해야 합니다.

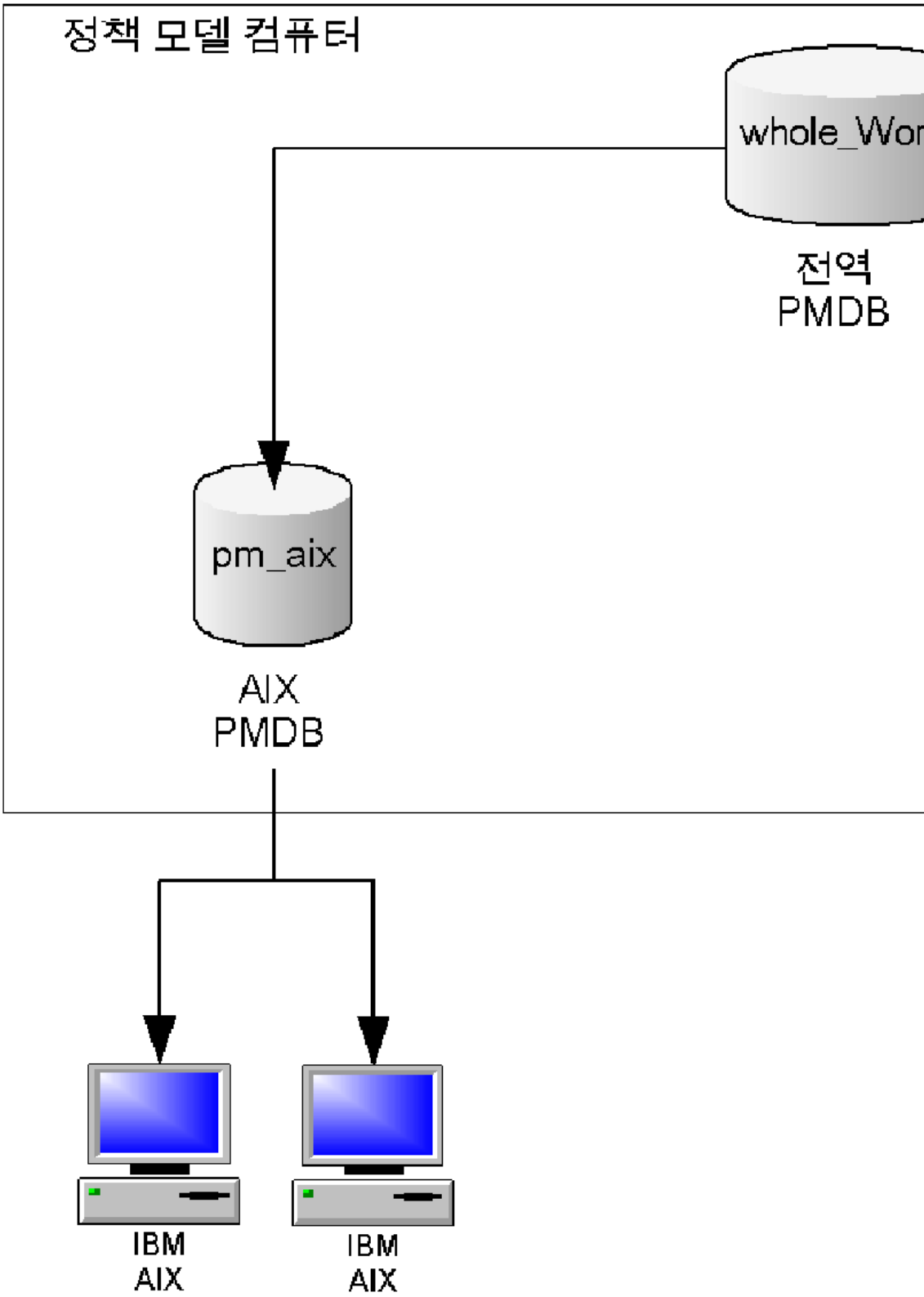
PMD 계층을 평면화할 때는 각 PMDB 를 따로 마이그레이션합니다. 마이그레이션 중에 CA Access Control 은 계층 환경에 있는 각 PMDB 에 대한 호스트 그룹을 만든 다음 각 끝점이 구독했던 PMDB 에 해당하는 모든 호스트 그룹에 각 끝점을 추가합니다.

계층적 PMDB 를 마이그레이션하려면

1. 마스터 PMDB 를 마이그레이션합니다.
2. 각 구독자 PMDB 를 마이그레이션합니다.

예: 계층적 PMDB 마이그레이션

다음 다이어그램에서는 계층 PMDB 가 있는 PMD 환경의 예를 보여 줍니다.


정책 모델 컴퓨터
whole_Wor
전역
PMDB
pm_aix
AIX
PMDB
IBM
AIX
IBM
AIX

이 예에서 pm_aix 및 pm_solaris PMDB 는 whole_world PMDB 의 구독자입니다. 모든 IBM AIX 끝점은 pm_aix 의 구독자입니다. 모든 Sun Solaris 끝점은 pm_sol 의 구독자입니다. 실제로 모든 끝점은 whole_world 의 구독자입니다.

이 PMD 환경을 고급 정책 관리 환경으로 마이그레이션할 때 다음을 수행하게 됩니다.

1. whole_world PMDB 를 마이그레이션합니다.

   CA Access Control 이 whole_world 호스트 그룹을 만듭니다. 모든 끝점은 이 호스트 그룹의 구성원입니다.

2. 구독자 PMDB 를 마이그레이션합니다.

   - pm_aix PMDB 를 마이그레이션합니다.

     CA Access Control 이 pm_aix 호스트 그룹을 만듭니다. IBM AIX 끝점은 이 호스트 그룹의 구성원입니다.

   - pm_sol PMDB 를 마이그레이션합니다.

     CA Access Control 이 pm_sol 호스트 그룹을 만듭니다. Sun Solaris 끝점은 이 호스트 그룹의 구성원입니다.

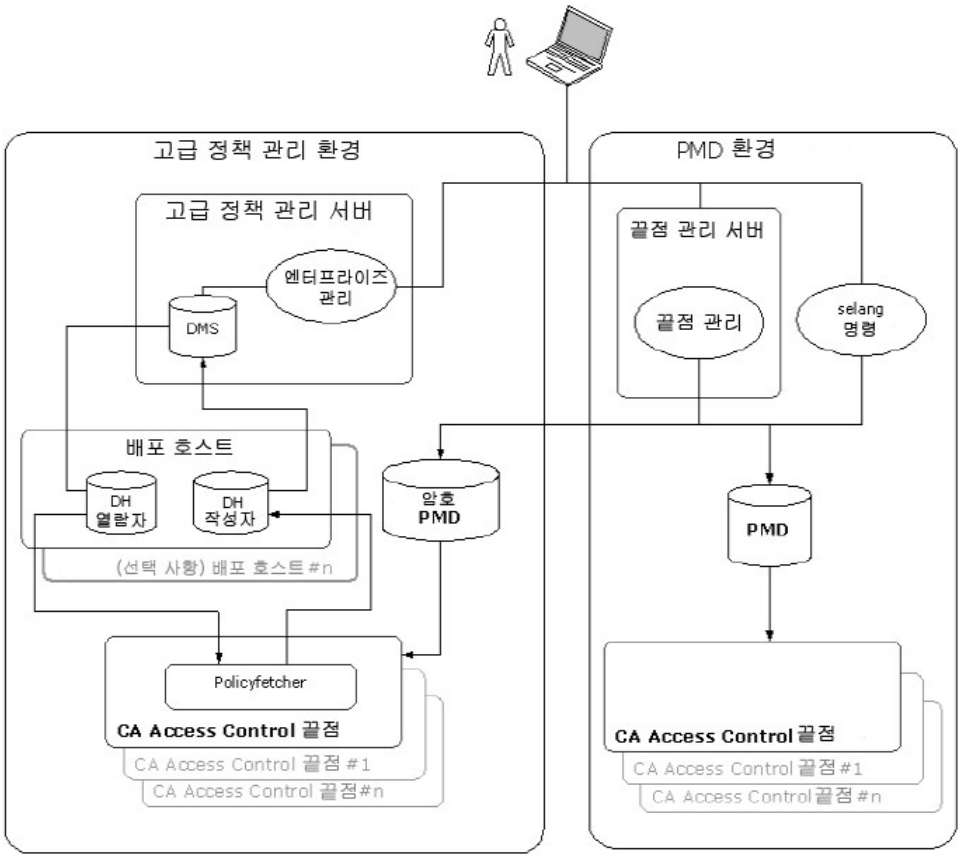
참고: PMD 환경에서 pm_aix PMDB 에 필터 파일을 적용하는 경우 필터 파일로 인해 whole_world PMDB 에서 배포하는 규칙이 IBM AIX 끝점에 도달하지 못할 수 있습니다. 고급 정책 관리 환경에서 IBM AIX 끝점은 whole_world 호스트 그룹의 구성원입니다. whole_world 호스트 그룹에 배포하는 모든 규칙은 필터링 없이 모든 끝점에 배포됩니다. 고급 정책 관리 환경에 규칙을 배포할 때는 이러한 변경된 속성을 인식하고 있어야 합니다.

혼합된 정책 관리 환경

혼합된 정책 관리 환경은 일부 끝점은 PMD 를 구독하고 일부 끝점은 고급 정책 관리 환경에 정의되어 있는 CA Access Control 배포입니다.

다음 다이어그램에서는 혼합된 정책 관리 환경을 사용한 CA Access Control 배포의 예를 보여 줍니다.

참고: 이 다이어그램에는 나와 있지 않지만 한 끝점이 PMD 를 구독하는 동시에 고급 정책 관리 환경에 정의되어 있을 수도 있습니다. 예를 들어 고급 정책 관리 환경에서 끝점에 정책을 배포하는 동시에 PMD 의 selang 규칙을 같은 끝점에 전파할 수 있습니다.



혼합된 정책 관리 환경에서 끝점 업데이트

혼합된 정책 관리 환경에서 끝점을 업데이트하는 경우 각 환경에서 개별적으로 끝점을 업데이트합니다.

참고: 끝점은 이후 CA Access Control 버전에서 추가된 클래스를 수정하는 규칙을 허용하지 않습니다. 예를 들어, r12.5 PMD 또는 DMS 로부터 규칙을 배포하는 경우에도 r8 끝점은 r8 기능을 변경하는 규칙만 허용합니다.

혼합된 정책 관리 환경에서 끝점을 업데이트하려면

1. selang 배포 명령을 사용하여 끝점에 배포할 스크립트 파일을 만듭니다.
2. CA Access Control 엔터프라이즈 관리에서 다음을 수행합니다.
   a. 정책 버전을 DMS 에 저장합니다.
   b. 저장된 정책 버전을 업데이트할 호스트 그룹에 할당합니다.

   CA Access Control 이 해당 정책을 호스트 그룹의 끝점에 배포합니다.
3. 스크립트 파일의 selang 명령을 사용하여 PMDB 를 업데이트합니다.

   PMDB 가 해당 끝점에 명령을 전파합니다.

참고: 정책을 저장하고 할당하는 방법에 대한 자세한 내용은 *엔터프라이즈 관리 안내서*를 참조하십시오. PMDB 를 업데이트하는 방법에 대한 자세한 내용은 해당 OS 의 *끝점 관리 안내서*를 참조하십시오.