CA Identity Manager™

구성 안내서

12.6.5

ca technologies

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.

CA Technologies 제품 참조

이 문서에서 참조하는 CA 제품은 다음과 같습니다.

- CA Identity Manager
- CA Siteminder®
- CA Directory
- CA User Activity Reporting
- CA Identity Governance

목차

제 1 장: CA Identity Manager 환경 소개

이 섹션은 다음 항목을 포함하고 있습니다.

CA Identity Manager 환경 구성 요소

CA Identity Manager *환경*은 CA Identity Manager 관리자가 사용자, 그룹, 조직 등의 개체를 관리하는 데 사용할 수 있는 관리 네임스페이스 보기입니다. 이러한 개체는 연결된 역할 및 태스크 집합과 함께 할당됩니다. 디렉터리의 관리와 시각적 표시는 CA Identity Manager 환경에 의해 제어됩니다.

단일 사용자 저장소는 여러 CA Identity Manager 환경 (페이지 20)에 연결되어 디렉터리에 대한 다양한 보기를 정의할 수 있습니다. 그러나 한 CA Identity Manager 환경에는 하나의 사용자 저장소만 연결됩니다.

CA Identity Manager 환경은 다음 요소로 구성됩니다.

디렉터리

CA Identity Manager 에 대한 사용자 저장소를 설명합니다. 디렉터리 요소에는 다음이 포함됩니다.

- 사용자, 그룹 및 조직 같은 관리 개체를 저장하는 사용자 저장소에 대한 포인터
- 관리 개체가 디렉터리에 저장되고 해당 표시가 CA Identity Manager 에 저장되는 방식을 설명하는 메타데이터

프로비저닝 디렉터리(선택 사항)

관리 끝점에서 추가 계정을 관리하기 위한 프로비저닝 서버 관련 데이터를 저장합니다. 한 환경에 하나의 프로비저닝 디렉터리만 연결될 수 있습니다.

참고: 프로비저닝 서버 또는 프로비저닝 디렉터리에 대한 자세한 내용은 *설치 안내서*를 참조하십시오.

사용자 콘솔

CA Identity Manager 관리자가 CA Identity Manager 환경에서 태스크를 수행하는 데 사용됩니다.

태스크 및 역할 정의

CA Identity Manager 및 다른 응용 프로그램에서 사용자 권한을 결정합니다. 처음에 이러한 태스크 및 역할 정의는 해당 항목을 사용자에게 할당할 수 있는 CA Identity Manager 환경에서 사용할 수 있습니다.

사용자 콘솔을 사용하여 기본 역할 및 태스크를 사용자 지정할 수 있습니다.

자체 서비스

사용자가 고객 웹 사이트 같은 리소스에 액세스하기 위한 자신의 고유한 계정을 만들고 유지 관리할 수 있도록 합니다. 또한 사용자는 현재 암호를 잊어버렸을 경우 자체 서비스를 통해 임시 암호를 요청할 수 있습니다.

워크플로 정의

CA Identity Manager 에는 사용자 프로필 만들기나 역할 또는 그룹에 사용자 할당 등의 사용자 관리 태스크에 대한 승인 및 알림을 자동화하는 기본 워크플로 정의가 포함되어 있습니다. CA Identity Manager 에서 기본 워크플로 프로세스를 수정하여 각 엔터프라이즈 요구 사항을 지원할 수 있습니다.

스킨

CA Identity Manager 사용자 인터페이스의 모습을 결정합니다.

사용자 지정 기능

CA Identity Manager API 를 사용하여 비즈니스 요구 사항에 맞게 CA Identity Manager 를 수정할 수 있습니다. *Programming Guide for Java*(Java 프로그래밍 안내서)를 참조하십시오.

각 CA Identity Manager 환경에는 사용자 콘솔을 사용하여 초기 역할 및 태스크를 사용자 지정할 시스템 매니저가 한 명 이상 필요합니다. 시스템 매니저는 초기 역할 및 태스크를 만든 후 해당 환경의 사용자에게 관리 권한을 부여할 수 있습니다. 이러한 사용자는 사용자, 그룹 및 조직을 관리하는 관리자가 됩니다. *관리 안내서*를 참조하십시오.

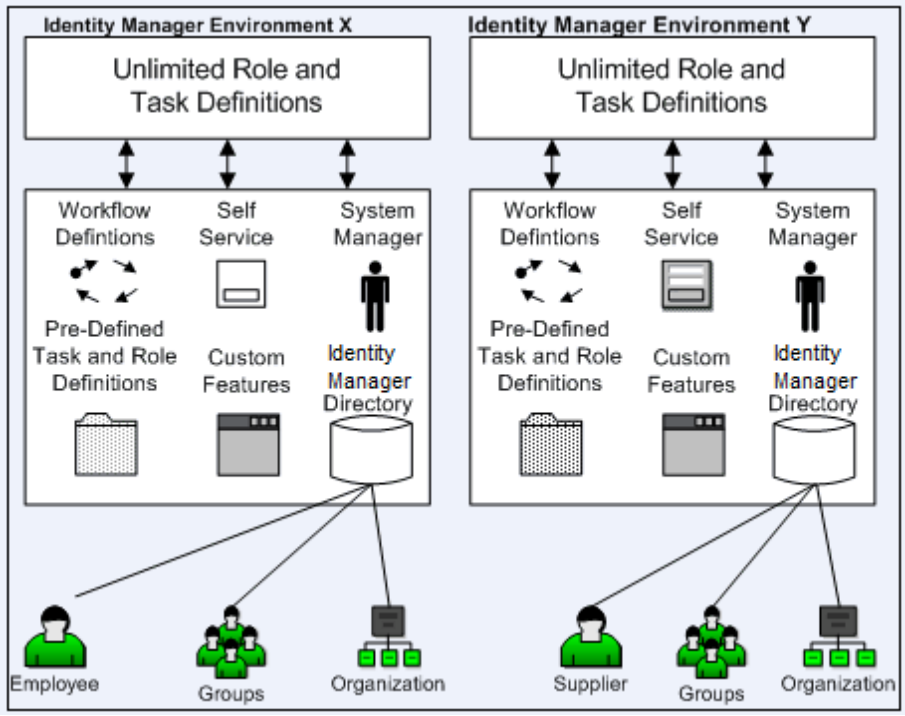
여러 CA Identity Manager 환경

다음 작업을 수행하려는 경우 CA Identity Manager 환경을 여러 개 만드십시오.

- 추가 사용자 저장소 관리 - 사용자를 다른 유형의 사용자 저장소에서 관리할 수 있습니다. 예를 들어 회사에서 모든 사용자 프로필을 Sun Java 시스템 LDAP 디렉터리에 저장하는데, Oracle 데이터베이스에 사용자 정보를 저장하는 파트너와 합작 투자를 진행하려고 합니다. 따라서 사용자 집합에 대해 각기 다른 CA Identity Manager 환경이 필요합니다.

- 다양한 LDAP 개체 클래스를 갖는 개체 관리 - CA Identity Manager 가 LDAP 디렉터리를 관리하고 있다고 간주하면 동일한 디렉터리 내에서 다양한 개체 클래스 및 특성을 갖는 동일한 유형의 개체를 관리할 수 있습니다. 예를 들어 다음 그림은 두 가지 유형의 사용자를 포함하는 디렉터리를 보여 줍니다.
  - Employee - 직원 ID 를 가짐
  - Supplier - 공급업체 번호로 식별됨

수식 1: 직원 및 공급업체를 포함하는 디렉터리가 있는 두 개의 Identity Manager 환경을 보여 주는 다이어그램



CA Identity Manager 관리 콘솔

CA Identity Manager 시스템 관리자의 역할은 다음과 같습니다.

- CA Identity Manager 디렉터리 만들기
- 프로비저닝 디렉터리 구성
- CA Identity Manager 환경 구성
- 시스템 매니저 할당
- 초기 사용을 위한 사용자 지정 기능 활성화

CA Identity Manager 환경을 구성하려면 웹 기반 응용 프로그램인 관리 콘솔을 사용하십시오.

관리 콘솔은 다음 두 섹션으로 구분됩니다.

- Directories(디렉터리) - 이 섹션에서는 사용자 저장소를 CA Identity Manager 에 설명하는 CA Identity Manager 디렉터리 및 프로비저닝 디렉터리를 만들고 관리할 수 있습니다.
- Environments(환경) - 이 섹션에서는 디렉터리의 관리 및 시각적 표시를 제어하는 CA Identity Manager 환경을 만들고 관리할 수 있습니다.

CA Identity Manager 관리 콘솔에 액세스하는 방법

관리 콘솔에 액세스하려면 브라우저에 다음 URL 을 입력하십시오.

http://*hostname:port*/iam/immanage

hostname

CA Identity Manager 가 설치된 서버의 정규화된 도메인 이름 또는 IP 주소를 정의합니다.

참고: Internet Explorer 7 을 사용하여 관리 콘솔에 액세스하는데 hostname 에 IPv6 주소가 포함되어 있으면 관리 콘솔이 잘못 표시될 수 있습니다. 이 문제를 방지하려면 정규화된 호스트 이름 또는 IPv4 주소를 사용하십시오.

port

응용 프로그램 서버 포트를 정의합니다.

참고: 웹 에이전트를 사용하여 CA Identity Manager 에 대해 고급 인증을 제공하는 경우에는 포트를 지정할 필요가 없습니다.

참고: 관리 콘솔에 액세스하는 데 사용할 브라우저에서 Javascript 가 사용되도록 설정해야 합니다.

관리 콘솔의 경로 예제는 다음과 같습니다.

- Geologic Weblogs:
  http://myserver.mycompany.org:7001/iam/immanage
- JBoss:
  http://myserver.mycompany.org:8080/iam/immanage
- WebSphere:
  http://myserver.mycompany.org:9080/iam/immanage

CA Identity Manager 환경을 만드는 방법

CA Identity Manager 환경을 만들려면 관리 콘솔에서 다음 단계를 완료해야 합니다.

1. 디렉터리 구성 마법사 (페이지 212)를 사용하여 CA Identity Manager 디렉터리를 만듭니다.
2. 환경에 프로비저닝이 포함되어 있을 경우 디렉터리 구성 마법사를 다시 사용하여 프로비저닝 디렉터리를 만듭니다 (페이지 232).
3. CA Identity Manager 환경을 만듭니다.
4. 환경에 액세스하여 (페이지 266) 실행되고 있는지 확인합니다.

제 2 장: 샘플 CA Identity Manager 환경

이 섹션은 다음 항목을 포함하고 있습니다.

샘플 CA Identity Manager 환경 개요

CA Identity Manager 에는 CA Identity Manager 를 배워 보고 테스트해 볼 수 있는 샘플 환경이 포함되어 있습니다.

샘플 환경은 NeteAuto 라는 자동차 무역 회사를 기반으로 합니다. NeteAuto 관리자는 CA Identity Manager 를 사용하여 직원, 공급업체 및 지역 대리점을 관리합니다.

샘플 NeteAuto 환경을 사용하는 사용자 저장소 구성은 다음과 같습니다.

- 조직을 지원하는 LDAP 사용자 저장소
- 조직을 지원하지 않는 LDAP 사용자 저장소
- 조직을 지원하는 관계형 데이터베이스 사용자 저장소
- 조직을 지원하지 않는 관계형 데이터베이스 사용자 저장소

참고: 이 환경에는 프로비저닝 디렉터리가 없으므로 프로비저닝 기능을 사용할 수 없습니다.

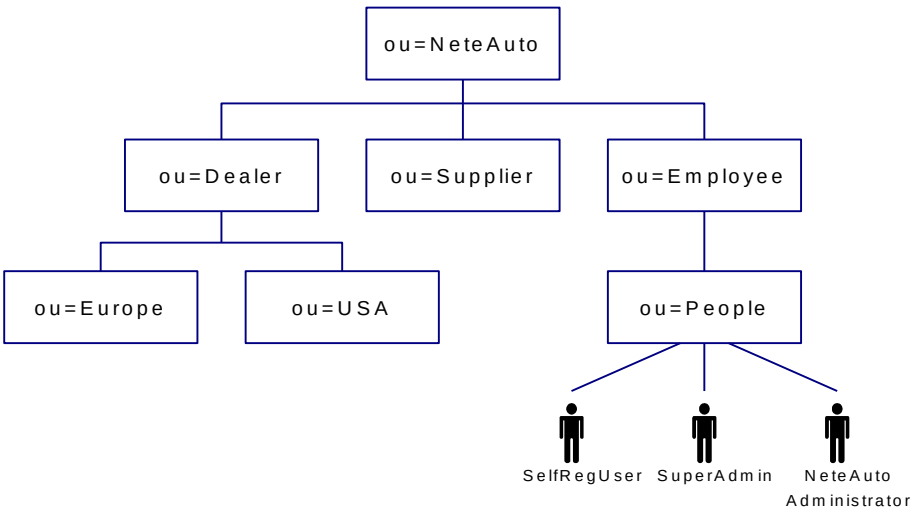
조직 지원과 함께 NeteAuto 샘플을 구성하는 방법

조직 지원과 함께 NeteAuto 샘플을 구성하는 과정에는 다음 단계가 포함됩니다.

- 필수 소프트웨어 설치
- 샘플 CA Identity Manager 환경 설치
- LDAP 사용자 디렉터리 구성
- 관계형 데이터베이스 구성
- CA Identity Manager 디렉터리 만들기
- NeteAuto CA Identity Manager 환경 만들기

NeteAuto 의 LDAP 디렉터리 구조

다음 그림은 LDAP 디렉터리에 대한 NeteAuto 샘플을 보여 줍니다.



샘플 CA Identity Manager 환경에는 다음 사용자가 포함되어 있습니다.

- Superadmin 은 이 CA Identity Manager 환경에 대한 시스템 매니저 역할을 가진 관리자 계정입니다. superadmin 은 모든 기본 관리자 태스크를 수행할 수 있습니다.

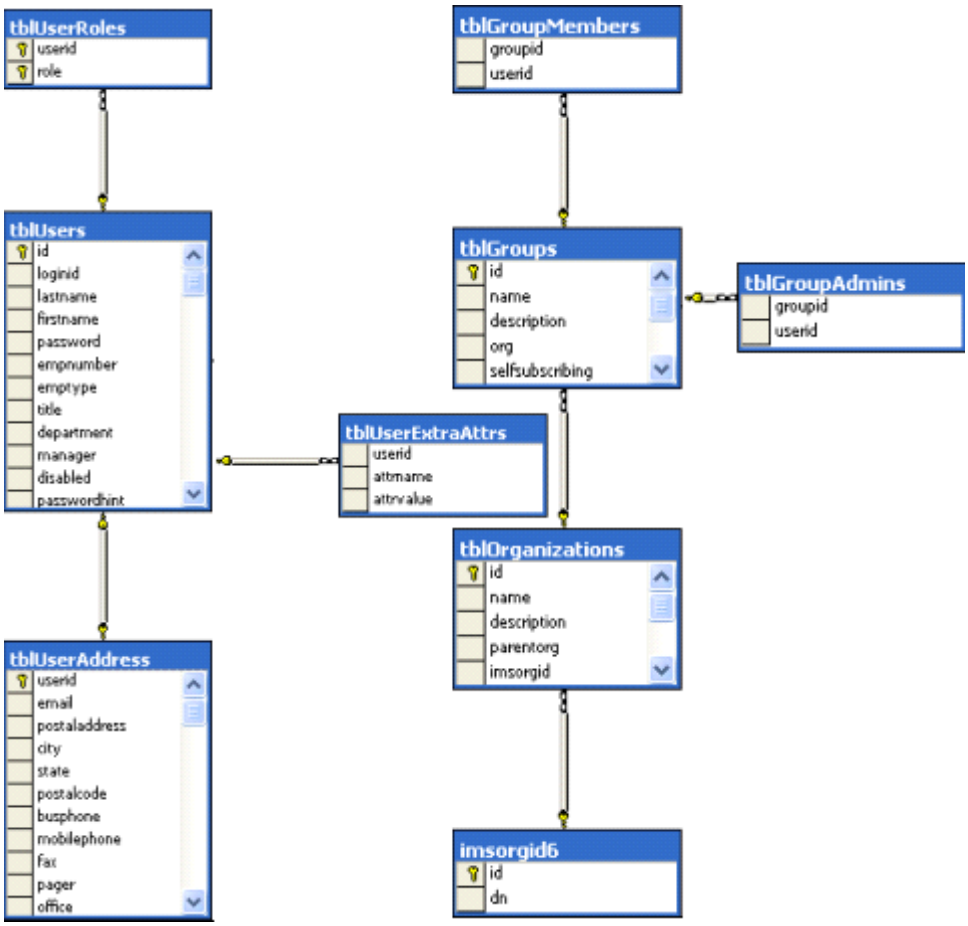
  참고: 기본 관리자 태스크에 대한 설명은 *관리 안내서*를 참조하십시오.

- SelfRegUser 는 CA Identity Manager 가 이 CA Identity Manager 환경에 대해 자체 등록을 활성화하기 위해 사용하는 관리자 계정입니다.

- NeteAuto Administrator 는 NeteAuto 환경을 설치할 때 어떤 권한도 갖지 않습니다. 그룹 매니저 역할 할당에 설명된 대로 사용자 역할로 그룹 매니저를 할당할 수 있습니다.

NeteAuto 의 관계형 데이터베이스

다음 그림은 조직 테이블을 포함한 NeteAuto 샘플의 관계형 데이터베이스를 보여 줍니다.



NeteAuto 의 필수 소프트웨어

NeteAuto CA Identity Manager 환경의 필수 구성 요소는 다음과 같습니다.

- *설치 안내서*에 설명된 대로 CA Identity Manager 를 설치합니다. CA Identity Manager 관리 도구를 설치해야 합니다.
- Sun Java 시스템(Sun ONE 또는 iPlanet) Directory Server 또는 Microsoft SQL Server 데이터베이스에 대한 액세스 권한이 있어야 합니다.

NeteAuto 환경의 설치 파일

CA Identity Manager 에는 샘플 CA Identity Manager 환경을 설정하는 데 사용할 수 있는 일련의 파일이 포함되어 있습니다. CA Identity Manager 환경은 CA Identity Manager 관리자가 사용자, 그룹, 조직 등의 개체를 관리하는 데 사용할 수 있는 관리 네임스페이스 보기입니다. 이러한 개체는 관련된 역할 및 태스크 집합과 함께 관리됩니다. 디렉터리의 시각적 표시 및 관리는 CA Identity Manager 환경에 의해 제어됩니다.

샘플 CA Identity Manager 환경에는 다음 요소가 포함되어 있습니다.

- 사용자 및 조직과 같은 샘플 개체
- 역할, 태스크 및 화면 정의

  태스크는 사용자 콘솔에서 "사용자" 또는 "그룹" 등의 탭을 클릭할 때 표시됩니다. 할당된 역할에 따라 사용자가 로그인할 때 관련 태스크가 나타납니다.

  참고: 역할 및 태스크에 대한 자세한 내용은 *관리 안내서*를 참조하십시오.
- NeteAuto 사용자에 대해 사용자 콘솔을 사용자 지정하는 샘플 스킨
- CA Identity Manager 디렉터리를 만드는 데 사용하는 디렉터리 구성 파일

샘플 CA Identity Manager 환경을 만들기 위한 파일은 다음 위치에 설치됩니다.

admin_tools\samples\NeteAuto

이 경로에서 *admin_tools* 는 관리 도구를 나타냅니다. 기본적으로 관리 도구는 다음 위치에 설치됩니다.

- **Windows:** C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools
- **UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

NeteAuto 환경 설치

NeteAuto 환경을 설치하려면 다음 프로세스를 수행하십시오.

다음 단계를 수행하십시오.

1. 필수 소프트웨어가 설치 (페이지 29)되었는지 확인합니다.
2. 사용자 저장소를 구성하고 샘플 데이터를 가져옵니다.
   - LDAP 사용자: LDAP 사용자 디렉터리 구성 (페이지 31)
   - 관계형 데이터베이스 사용자: 관계형 데이터베이스 구성
3. NeteAuto CA Identity Manager 디렉터리를 만듭니다.
4. NeteAuto CA Identity Manager 환경을 만듭니다.
5. NeteAuto 사용자에 대한 CA Identity Manager 사용자 인터페이스의 모양을 구성합니다 (페이지 52).

LDAP 사용자 디렉터리 구성

설치 환경에 따라 LDAP 디렉터리를 사용할 수 있습니다. 다음 절차에 따라 이 디렉터리가 있는지 확인하거나 이 디렉터리를 만듭니다.

다음 단계를 수행하십시오.

1. 디렉터리 서버 콘솔에서 다음 루트를 사용하여 LDAP 인스턴스를 만듭니다.

   ```
   dc=security,dc=com
   ```

   이후에 참조할 수 있도록 포트 번호를 적어 둡니다.

2. 관리 도구의 samples\NeteAuto 에서 디렉터리 서버로 NeteAuto.ldif 파일을 가져옵니다.

   관리 도구는 다음 기본 위치에 설치됩니다.

   - **Windows:** C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools
   - **UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

참고: LDIF 파일을 가져오거나 CA Identity Manager 디렉터리를 만들 때 문제가 발생하면 다음 텍스트를 LDIF 파일의 시작 부분에 추가하십시오.

```
dn: dc=security, dc=com
objectClass: top
objectClass: domain
dc: security
```

파일을 저장하고 1 단계와 2 단계를 반복합니다.

관계형 데이터베이스 구성

관계형 데이터베이스를 구성하려면 다음 절차를 수행하십시오.

다음 단계를 수행하십시오.

1. 이름이 NeteAuto 인 데이터베이스 인스턴스를 만듭니다.

2. 암호로 test 를 사용하여 neteautoadmin 이라는 사용자를 만듭니다. 사용자의 속성을 편집하여 NeteAuto 에 대한 neteautoadmin 권한(예: public 및 db_owner 권한)을 부여합니다.

   참고: NeteAuto 데이터베이스를 만들려면 neteautoadmin 역할이 .sql 스크립트에서 생성되는 모든 테이블에 대해 최소 권한(선택, 삽입, 업데이트 및 삭제) 이상을 가져야 합니다. 또한 이러한 스크립트에 저장 프로시저가 정의되어 있을 경우 모든 정의된 저장 프로시저를 실행할 수 있어야 합니다.

3. 사용자 속성을 편집할 때 NeteAuto 를 neteautoadmin 의 기본 데이터베이스로 설정합니다.

4. 다음 스크립트를 나열된 순서대로 실행합니다.

   - *db_type*-rdbuserdirectory.sql - NeteAuto 샘플의 테이블을 구성하고 사용자 항목을 만듭니다.
   - ims_*db_type*_rdb.sql - 조직에 대한 지원을 구성합니다.

     db_type

     구성하려는 데이터베이스 유형에 따라 Microsoft SQL 또는 Oracle 을 정의합니다.

   이러한 스크립트 파일은 *admin_tools*\samples\NeteAutoRDB\Organization 폴더에 있습니다. 이 예에서 *admin_tools* 는 다음 기본 위치에 설치된 관리 도구를 나타냅니다.

   - **Windows:** C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools
   - **UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

5. NeteAuto 데이터베이스를 가리키며 이름이 neteautoDS 인 JDBC 데이터 원본을 정의합니다.

   데이터 원본을 구성하는 절차는 CA Identity Manager 가 설치된 응용 프로그램 서버의 유형에 따라 달라집니다. JDBC 데이터 원본을 만드는 방법 (페이지 144) 단원에는 JDBC 데이터 원본을 만들기 위한 응용 프로그램 서버 관련 지침이 나와 있습니다.

CA Identity Manager 디렉터리 만들기

CA Identity Manager 디렉터리를 만들려면 다음 절차를 수행하십시오.

다음 단계를 수행하십시오.

1. 브라우저에 다음 URL 을 입력하여 관리 콘솔을 엽니다.

   http://*im_server:port*/iam/immanage

   im_server

   CA Identity Manager 가 설치된 서버의 정규화된 도메인 이름을 정의합니다.

   port(포트)

   응용 프로그램 서버 포트 번호를 정의합니다.

2. "Directories"(디렉터리)를 클릭합니다.
3. "Create from Wizard"(마법사에서 만들기)를 클릭하여 CA Identity Manager 디렉터리 마법사를 시작합니다.
4. 해당 디렉터리 구성 .xml 파일을 찾고 "Next"(다음)를 클릭합니다.

   디렉터리 구성 파일은 다음 폴더에 있습니다.

   - Sun Java System Directory Server 사용자 디렉터리:

     admin_tools\samples\NeteAuto\Organization\directory.xml

- 관계형 데이터베이스:

  admin_tools\samples\NeteAutoRDB\Organization*db_type* directory.xml

  admin_tools

  관리 도구가 설치된 위치를 정의합니다.

  관리 도구는 다음 기본 위치에 설치됩니다.

  Windows: C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools

  UNIX: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

  db_type

  구성하려는 데이터베이스의 유형 Microsoft SQL 또는 Oracle 을 지정합니다.

상태 정보가 "Directory Configuration Output"(디렉터리 구성 출력) 화면에 표시됩니다.

5. 마법사의 두 번째 페이지에서 다음 값을 제공합니다.

- Sun Java System Directory Server

  Name(이름)

  NeteAuto Directory

  Description(설명)

  Sample NeteAuto directory

  Connection Object Name(연결 개체 이름)

  NeteAuto Users

  Host(호스트)

  사용자 저장소가 설치된 시스템의 컴퓨터 이름 또는 IP 주소

  Port(포트)

  사용자 저장소의 포트 번호

Search root(검색 루트)

dc=security, dc=com

Username(사용자 이름)

사용자 저장소에 액세스할 수 있는 계정의 사용자 이름

Password(암호) 및 Confirm Password(암호 확인)

사용자 계정의 암호

- Microsoft SQL Server 및 Oracle 데이터베이스

Name(이름)

NeteAutoRDB Directory

Description(설명)

Sample NeteAuto directory

Connection Object Name(연결 개체 이름)

NeteAutoRDB

JDBC Data Source(JDBC 데이터 원본)

neteautoDS

Username(사용자 이름)

Neteautoadmin

Password(암호)

Test

6. "Next"(다음)를 클릭합니다.
7. "Finish"(마침)를 클릭하여 마법사를 종료합니다.

NeteAuto CA Identity Manager 환경 만들기

NeteAuto CA Identity Manager 환경을 만들려면 다음 절차를 수행하십시오.

다음 단계를 수행하십시오.

1. 관리 콘솔에서 "Environments"(환경)를 클릭합니다.
2. CA Identity Manager 환경 화면에서 "New"(새로 만들기)를 클릭합니다.

   CA Identity Manager 환경 마법사가 나타납니다.
3. 마법사의 첫 번째 페이지에서 다음 값을 입력합니다.

   Environment name(환경 이름)

   NeteAuto Environment(NeteAuto 환경)

   Description(설명)

   Sample Environment(샘플 환경)

   Alias(별칭)

   Neteauto

   별칭은 CA Identity Manager 환경에 액세스하기 위한 URL 에 추가됩니다. 예를 들어 neteauto 환경에 액세스하기 위한 URL 이 다음과 같을 수 있습니다.

   http://*server_name*/iam/im/neteauto

   server_name

   CA Identity Manager 가 설치된 서버의 정규화된 도메인 이름을 정의합니다. 예를 들어 다음과 같습니다.

   http://myserver.mycompany.org/iam/im/neteauto

   참고: 별칭은 대소문자를 구분합니다.

   "Next"(다음)를 클릭합니다.

4. 만들려는 환경과 연결할 CA Identity Manager 디렉터리를 선택합니다.
   - Sun Java System Directory Server 의 경우 NeteAuto Directory 를 사용합니다.
   - Microsoft SQL Server 또는 Oracle 데이터베이스의 경우 NeteAutoRDB Directory 를 사용합니다.

   "Next"(다음)를 클릭합니다.
5. 다음과 같이 자체 등록 및 잊어버린 암호 태스크 같은 공용 태스크에 대한 지원을 구성합니다.
   a. 공용 태스크에 대한 다음 별칭을 입력합니다.

      Neteautopublic
   b. 익명 사용자 계정으로 SelfRegUser 를 입력합니다.
   c. "Validate"(유효성 검사)를 클릭하여 사용자 고유 식별자를 확인합니다.

   참고: 사용자가 공용 태스크를 사용하기 위해 로그인할 필요가 없습니다.
6. NeteAuto 환경에 대해 만들 태스크 및 역할을 선택합니다.
   a. "Import roles from the file"(파일에서 역할 가져오기)를 선택합니다.
   b. 다음 위치 중 하나로 이동합니다.
      - Sun Java System Directory Server 사용자 저장소:

        admin_tools\samples\NeteAuto\RoleDefinitions.xml
      - Microsoft SQL Server 사용자 저장소:

        admin_tools\samples\NeteAutoRDB\Organization\mssqlRoleDefinitions.xml

- Oracle 사용자 저장소:

  admin_tools\samples\NeteAutoRDB\Organization\oracleRoleDefinitions.xml

admin_tools 는 기본적으로 다음 위치에 설치되는 관리 도구를 나타냅니다.

Windows: C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools

UNIX: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

7. 이 환경에 대해 시스템 매니저 역할을 할 사용자를 지정하고 "Next"(다음)를 클릭합니다.
   a. "System Manager"(시스템 매니저) 필드에 SuperAdmin 을 입력합니다.
   b. "Add"(추가)를 클릭합니다.

      CA Identity Manager 가 Superadmin 사용자의 고유 식별자를 사용자 목록에 추가합니다.
   c. "Next"(다음)를 클릭합니다.
8. 환경에 대한 설정을 검토하고 다음 테스트를 수행합니다.
   - (선택 사항) "Previous"(이전)를 클릭하여 설정을 수정합니다.
   - "Finish"(마침)를 클릭하여 현재 설정으로 CA Identity Manager 환경을 만듭니다.

     "Environment Configuration Output"(환경 구성 출력) 화면에 환경 만들기 진행 상황이 표시됩니다.
9. "Continue"(계속)를 클릭하여 CA Identity Manager 환경 마법사를 종료합니다.
10. CA Identity Manager 환경을 시작합니다.

NeteAuto 환경을 만든 후에는 다음을 수행할 수 있습니다.

- 이 CA Identity Manager 환경에 대한 스킨을 만듭니다 (페이지 52).
- 환경에 액세스합니다. (페이지 50)

조직 지원 없이 NeteAuto 샘플을 구성하는 방법

조직 지원 없이 NeteAuto 샘플을 구성하는 과정에는 다음 단계가 포함됩니다.

- 필수 소프트웨어 (페이지 29) 설치
- 샘플 CA Identity Manager 환경 설치
- 데이터베이스 구성
- JDBC 데이터 원본 만들기
- CA Identity Manager 디렉터리 만들기
- NeteAuto CA Identity Manager 환경 만들기

샘플 CA Identity Manager 환경 설명

Microsoft SQL Server 및 Oracle 데이터베이스의 경우 CA Identity Manager 에 조직이 있지 않은 NeteAuto 환경 버전이 포함되어 있습니다. 이 CA Identity Manager 환경에는 다음 세 가지 사용자가 있습니다.

- Superadmin 은 이 CA Identity Manager 환경에 대한 시스템 매니저 역할을 가진 관리자 계정입니다. Superadmin 은 모든 기본 관리자 태스크를 수행할 수 있습니다.

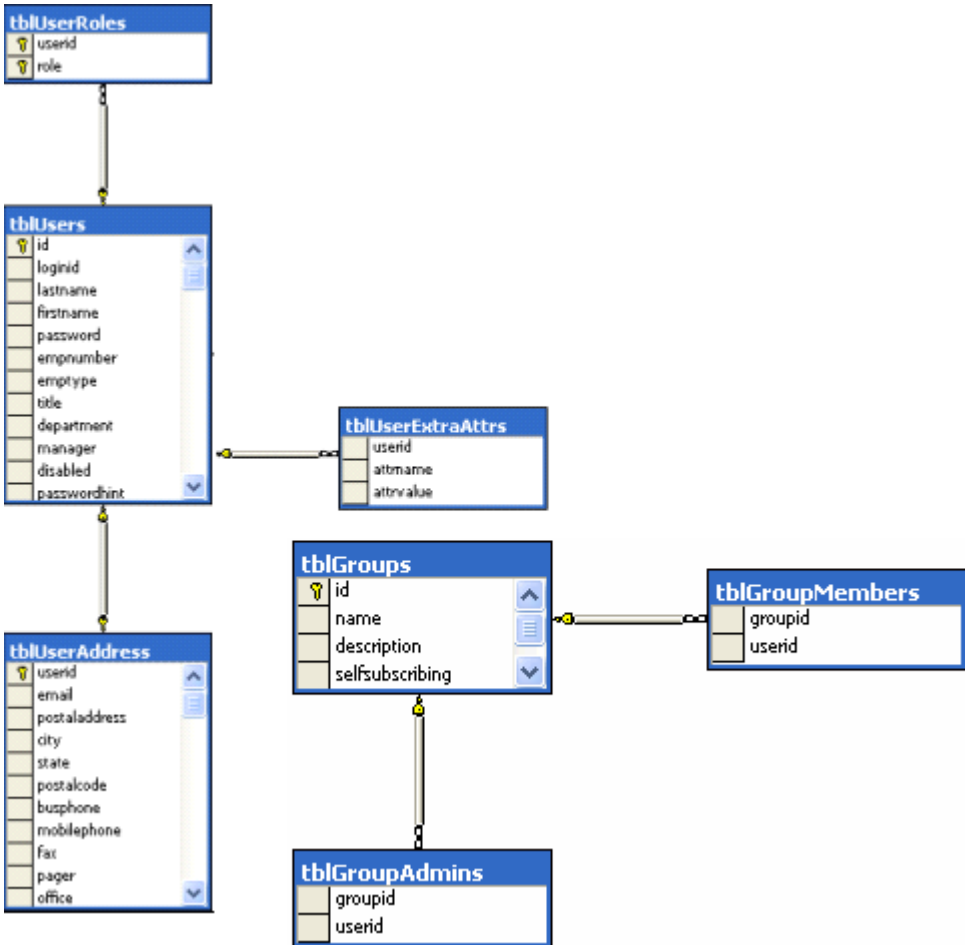
  참고: 기본 관리자 태스크에 대한 설명은 *관리 안내서*를 참조하십시오.

- SelfRegUser 는 CA Identity Manager 가 이 CA Identity Manager 환경에 대해 자체 등록을 활성화하기 위해 사용하는 관리자 계정입니다.

- NeteAuto Administrator 는 NeteAuto 환경을 설치할 때 어떤 권한도 갖지 않습니다.

  그러나 NeteAuto Administrator 계정에 그룹 매니저 역할을 할당할 수 있습니다.

다음 그림은 조직 없는 관계형 데이터베이스에 대한 NeteAuto 샘플을 보여 줍니다.



NeteAuto 환경의 설치 파일

CA Identity Manager 에는 샘플 CA Identity Manager 환경을 설정하는 데 사용할 수 있는 일련의 파일이 포함되어 있습니다. CA Identity Manager 환경은 CA Identity Manager 관리자가 개체를 관리하는 데 사용할 수 있는 관리 네임스페이스 보기입니다. 사용자 및 그룹과 같은 이러한 개체는 일련의 역할 및 태스크와 함께 제공됩니다. 사용자 저장소의 관리와 시각적 표시는 CA Identity Manager 환경에 의해 제어됩니다.

샘플 CA Identity Manager 환경에는 다음 요소가 포함되어 있습니다.

- 샘플 사용자
- 역할, 태스크 및 화면 정의

  태스크는 사용자 콘솔에서 사용자 또는 그룹과 같은 범주를 클릭할 때 표시됩니다. 태스크는 해당 사용자에게 할당된 역할을 기반으로 표시됩니다.

  참고: 역할 및 태스크에 대한 자세한 내용은 *관리 안내서*를 참조하십시오.
- NeteAuto 사용자에 대해 사용자 콘솔을 사용자 지정하는 샘플 스킨
- CA Identity Manager 디렉터리를 만드는 데 사용하는 디렉터리 구성 파일

샘플 CA Identity Manager 환경을 만들기 위한 파일은 다음 위치에 설치됩니다.

admin_tools\samples\NeteAutoRDB\NoOrganization

이 경로에서 *admin_tools* 는 관리 도구를 나타냅니다.

기본적으로 관리 도구는 다음 위치에 설치됩니다.

- **Windows:** C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools
- **UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

NeteAuto 환경을 설치하는 방법 - 조직 지원 없음

NeteAuto 환경을 설치하려면 다음 프로세스를 수행하십시오.

다음 단계를 수행하십시오.

1. 필수 소프트웨어 (페이지 42)가 설치되었는지 확인합니다.
2. 데이터베이스를 구성합니다 (페이지 31).
3. CA Identity Manager 디렉터리를 만듭니다. (페이지 45)
4. NeteAuto CA Identity Manager 환경을 만듭니다 (페이지 47).
5. NeteAuto 사용자에 대한 CA Identity Manager 사용자 인터페이스 (페이지 52)의 모양을 구성합니다.

필수 소프트웨어

NeteAuto CA Identity Manager 환경의 필수 구성 요소는 다음과 같습니다.

- *설치 안내서*에 설명된 대로 CA Identity Manager 를 설치합니다. CA Identity Manager 관리 도구가 설치되었는지 확인합니다.
- Microsoft SQL Server 또는 Oracle 데이터베이스에 액세스할 수 있어야 합니다.

관계형 데이터베이스 구성

관계형 데이터베이스를 구성하려면 다음 절차를 수행하십시오.

다음 단계를 수행하십시오.

1. 이름이 NeteAuto 인 데이터베이스 인스턴스를 만듭니다.
2. 암호로 test 를 사용하여 neteautoadmin 이라는 사용자를 만듭니다. 사용자의 속성을 편집하여 NeteAuto 에 대한 neteautoadmin 권한(예: public 및 db_owner 권한)을 부여합니다.

   참고: NeteAuto 데이터베이스를 만들려면 neteautoadmin 역할이 .sql 스크립트에서 생성되는 모든 테이블에 대해 최소 권한(선택, 삽입, 업데이트 및 삭제) 이상을 가져야 합니다. 또한 이러한 스크립트에 저장 프로시저가 정의되어 있을 경우 모든 정의된 저장 프로시저를 실행할 수 있어야 합니다.
3. 사용자 속성을 편집할 때 NeteAuto 를 neteautoadmin 의 기본 데이터베이스로 설정합니다.

4. 다음 스크립트를 나열된 순서대로 실행합니다.

   - *db_type*-rdbuserdirectory.sql - NeteAuto 샘플의 테이블을 구성하고 사용자 항목을 만듭니다.
   - ims_*db_type*_rdb.sql - 조직에 대한 지원을 구성합니다.

     db_type

     구성하려는 데이터베이스 유형에 따라 Microsoft SQL 또는 Oracle 을 정의합니다.

   이러한 스크립트 파일은 *admin_tools*\samples\NeteAutoRDB\Organization 폴더에 있습니다. 이 예에서 *admin_tools* 는 다음 기본 위치에 설치된 관리 도구를 나타냅니다.

   - **Windows:** C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools
   - **UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

5. NeteAuto 데이터베이스를 가리키며 이름이 neteautoDS 인 JDBC 데이터 원본을 정의합니다.

   데이터 원본을 구성하는 절차는 CA Identity Manager 가 설치된 응용 프로그램 서버의 유형에 따라 달라집니다. JDBC 데이터 원본을 만드는 방법 (페이지 144) 단원에는 JDBC 데이터 원본을 만들기 위한 응용 프로그램 서버 관련 지침이 나와 있습니다.

CA Identity Manager 디렉터리 만들기

CA Identity Manager 디렉터리를 만들려면 다음 절차를 수행하십시오.

다음 단계를 수행하십시오.

1. 브라우저에 다음 URL 을 입력하여 관리 콘솔을 엽니다.

   http://*im_server*:*port*/iam/immanage

   im_server

   CA Identity Manager 가 설치된 서버의 정규화된 도메인 이름을 정의합니다.

   port

   응용 프로그램 서버 포트 번호를 정의합니다.

2. "Directories"(디렉터리)를 클릭합니다.

   CA Identity Manager 디렉터리 화면이 나타납니다.

3. "New"(새로 만들기)를 클릭하여 CA Identity Manager 디렉터리 마법사를 시작합니다.

4. 다음 디렉터리 구성 XML 파일 중 하나를 찾고 "Next"(다음)를 클릭합니다.

   - Sun Java 시스템:

     admin_tools\samples\NeteAuto\NoOrganization\directory.xml

   - SQL Server 데이터베이스:

     admin_tools\samples\NeteAuto\NoOrganization\mssql-directory.xml

   - Oracle 데이터베이스:

     admin_tools\samples\NeteAuto\NoOrganization\oracle-directory.xml

   admin_tools 는 기본적으로 다음 위치에 설치되는 관리 도구를 나타냅니다.

   - **Windows:** C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools
   - **UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

   상태 정보가 "Directory Configuration Output"(디렉터리 구성 출력) 화면에 표시됩니다.

5. 마법사의 두 번째 페이지에서 다음 값을 제공합니다.

   Name(이름)

   NeteAutoRDB Directory

   Description(설명)

   Sample NeteAuto directory with no organization support

   Connection Object Name(연결 개체 이름)

   NeteAutoRDB

JDBC Data Source(JDBC 데이터 원본)

neteautoDS

Username(사용자 이름)

neteautoadmin

Password(암호)

test

6. "Next"(다음)를 클릭합니다.
7. "Finish"(마침)를 클릭하여 마법사를 종료합니다.

NeteAuto CA Identity Manager 환경 만들기

NeteAuto CA Identity Manager 환경을 만들려면 다음 절차를 수행하십시오.

다음 단계를 수행하십시오.

1. 관리 콘솔에서 "Environments"(환경)를 클릭합니다.
2. CA Identity Manager 환경 화면에서 "New"(새로 만들기)를 클릭합니다.

   CA Identity Manager 환경 마법사가 열립니다.
3. 마법사의 첫 번째 페이지에서 다음 값을 입력합니다.
   - Environment name(환경 이름) - NeteAuto 환경
   - Description(설명) - NeteAuto 는 샘플 환경입니다.

- Alias(별칭) - neteautoRDB

  별칭은 CA Identity Manager 환경에 액세스하기 위한 URL 에 추가됩니다. 예를 들어 neteauto 환경에 액세스하기 위한 URL 이 다음과 같을 수 있습니다.

  `http://domain/iam/im/neteautoRDB`

  이 경로에서 *domain* 은 다음 예제에서처럼 CA Identity Manager 가 설치된 서버의 정규화된 도메인 이름을 정의합니다.

  `http://myserver.mycompany.org/iam/im/neteautoRDB`

  참고: 별칭은 대소문자를 구분합니다.

"Next"(다음)를 클릭합니다.

4. 만들려는 환경과 연결할 NeteAutoRDB Directory CA Identity Manager 디렉터리를 선택하고 "Next"(다음)를 클릭합니다.
5. 자체 등록 및 잊어버린 암호 태스크 같은 공용 태스크에 대한 지원을 구성합니다.

   참고: 사용자가 공용 태스크에 액세스하기 위해 로그인할 필요가 없습니다.

   a. 공용 태스크에 대한 다음 별칭을 입력합니다.

      neteautoRDBpublic

   b. 익명 사용자 계정으로 SelfRegUser 를 입력합니다.

   c. "Validate"(유효성 검사)를 클릭하여 사용자 고유 식별자를 확인합니다(이 경우 2).
6. NeteAuto 환경에 대해 만들 태스크 및 역할을 선택합니다.

   - "Import roles from the file"(파일에서 역할 가져오기)를 선택합니다.

- 다음 위치로 이동합니다.

  im_admin_tools_dir\samples\NeteAutoRDB\NoOrganizations\RoleDefinitions.xml

  이 경로에서 *im_admin_tools_dir* 은 CA Identity Manager 관리 도구의 설치 위치를 정의합니다.

7. 이 환경에 대해 시스템 매니저 역할을 할 사용자를 지정하고 "Next"(다음)를 클릭합니다.
   a. "System Manager"(시스템 매니저) 필드에 SuperAdmin 을 입력합니다.
   b. "Add"(추가)를 클릭합니다.
   c. "Next"(다음)를 클릭합니다.
8. 환경 관련 설정을 검토합니다.
   - "Previous"(이전)를 클릭하고 설정을 수정합니다.
   - "Finish"(마침)를 클릭하여 현재 설정으로 CA Identity Manager 환경을 만듭니다.

     "Environment Configuration Output"(환경 구성 출력) 화면에 환경 만들기 진행 상황이 표시됩니다.
9. "Finish"(마침)를 클릭하여 CA Identity Manager 환경 마법사를 종료합니다.
10. CA Identity Manager 환경을 시작합니다.

NeteAuto 환경을 만든 후 다음을 수행할 수 있습니다.

- NeteAuto 스킨 설정 (페이지 52)에 설명된 대로 이 CA Identity Manager 환경의 스킨을 만듭니다.
- "NeteAuto CA Identity Manager 환경을 사용하는 방법"에 설명된 대로 이 환경에 액세스합니다.

NeteAuto CA Identity Manager 환경을 사용하는 방법

NeteAuto CA Identity Manager 환경을 사용하여 자체 서비스 태스크 및 사용자를 관리할 수 있습니다.

자체 서비스 태스크 관리

자체 서비스 태스크에는 다음이 포함됩니다.

- 새 사용자로 등록
- 자체 등록된 사용자로 로그인
- 잊어버린 암호 기능 사용

새 사용자로 등록

새 사용자로 등록하려면 다음 절차를 수행하십시오.

다음 단계를 수행하십시오.

1. 브라우저에서 다음 URL 을 입력합니다.

   `http://hostname/iam/im/neteautopublic/index.jsp?task.tag=SelfRegistration`

   hostname

   CA Identity Manager 가 실행되고 있는 시스템의 정규화된 도메인 이름을 정의합니다.

   참고: Neteauto 스킨을 구성 (페이지 52)하지 않은 경우 다음과 같이 URL 에서 imcss 를 생략할 수 있습니다.

   http://*hostname*/iam/im/neteautopublic/index.jsp?task.tag=SelfRegistration

이 URL 은 기본 ca 콘솔로 리디렉션됩니다.

"Self-Registration: End-User License Agreement"(자체 등록: 최종 사용자 사용권 계약) 페이지에 CA 웹 사이트가 표시됩니다.

참고: 사용자 지정 최종 사용자 사용권 계약을 표시하도록 기본 자체 등록 태스크를 구성할 수 있습니다. 자세한 지침은 *관리 안내서*를 참조하십시오.

2. "승인"을 클릭하고 진행합니다.
3. "프로필" 탭에서 다음 정보를 제공합니다.
   a. 별표(*)로 표시된 필수 필드의 값을 입력합니다.
   b. 암호 힌트와 대답을 입력합니다.

      암호를 잊어버릴 경우 CA Identity Manager 에서 암호 힌트를 제공하고 대답을 요청합니다. 대답이 맞을 경우 CA Identity Manager 는 사용자에게 새 암호를 지정하고 확인하도록 요구합니다.
4. "그룹" 탭은 변경하지 않고 그대로 둡니다.
5. "제출"을 클릭합니다.

자체 등록된 사용자로 로그인

자체 등록된 사용자로 로그인하려면 다음 절차를 수행하십시오.

다음 단계를 수행하십시오.

1. 브라우저에서 NeteAuto CA Identity Manager 환경에 대한 다음 URL 을 입력합니다.

   `http://hostname/iam/im/neteauto/imcss/index.jsp`

   hostname

   CA Identity Manager 가 실행되고 있는 시스템의 정규화된 도메인 이름을 정의합니다.
2. 등록할 때 지정한 사용자 이름 및 암호를 사용하여 로그인합니다.

NeteAuto 스킨 설정

NeteAuto 스킨을 설정하려면 SiteMinder 정책 서버에서 SiteMinder 응답을 만들어야 합니다.

다음 단계를 수행하십시오.

1. 도메인 권한을 가진 관리자로 다음 인터페이스 중 하나에 로그인합니다.
   - CA SiteMinder Web Access Manager r12 이상의 경우 관리 UI 에 로그인합니다.
   - CA eTrust SiteMinder 6.0 SP5 의 경우 정책 서버 사용자 인터페이스에 로그인합니다.

   참고: 이러한 인터페이스를 사용하는 방법에 대한 내용은 사용 중인 SiteMinder 버전의 설명서를 참조하십시오.
2. neteautoDomain 을 엽니다.
3. neteautoDomain 에서 "영역"을 선택합니다.

   다음 영역이 표시됩니다.

   neteauto_ims_realm

   CA Identity Manager 환경을 보호합니다.

   neteauto_pub_realm

   자체 등록 및 잊어버린 암호 태스크 같은 공용 태스크에 대한 지원을 활성화합니다.
4. 각 영역에서 규칙을 만듭니다. 다음 정보를 지정합니다.
   - 리소스: *
   - 동작: GET, POST

   관리를 간소화하기 위해 NeteAuto 스킨을 규칙 이름에 포함하십시오.

5. 다음 응답 특성을 사용하여 도메인에 대한 응답을 만듭니다.
   - 특성: WebAgent-HTTP-Header-Variable

     이 특성은 새 HTTP 헤더를 응답에 추가합니다.
   - 특성 종류: 정적
   - 변수 이름: skin

     변수 값: neteauto
6. CA Identity Manager 가 neteautoDomain 에서 만든 정책을 수정합니다. 다음 정보를 지정합니다.
   - 사용자
     - LDAP:"사용 가능한 구성원"에서 ou=People, ou=Employees, ou=NeteAuto 를 선택하고 "현재 구성원"에 추가합니다. "확인"을 클릭합니다.
     - 관계형 데이터베이스: id 특성이 *인 사용자를 검색합니다. "사용 가능한 구성원"에서 모든 사용자를 선택하고 "현재 구성원"에 추가합니다. "확인"을 클릭합니다.
   - 규칙:
     - 4 단계에서 만든 규칙을 추가합니다.
     - 각 규칙에 대해 "응답 설정"을 클릭합니다. 각 규칙을 5 단계에서 만든 응답과 연결합니다.

참고: neteauto 스킨은 imcss 콘솔을 기반으로 합니다. 스킨을 보려면 다음과 같이 /imcss/index.jsp 를 NeteAuto CA Identity Manager 환경의 URL 에 추가하십시오.

http://*hostname*/iam/im/neteauto/imcss/index.jsp

NeteAuto CA Identity Manager 환경 액세스 (페이지 55)에서는 Neteauto 환경에 액세스하기 위한 완전한 지침을 제공합니다.

잊어버린 암호 기능 사용

잊어버린 암호 기능을 사용하려면 다음 절차를 수행하십시오.

다음 단계를 수행하십시오.

1. 브라우저에서 다음 URL 을 입력합니다.

   `http://hostname/iam/im/neteautopublic/index.jsp?task.tag=ForgottenPasswordReset`

   hostname

   CA Identity Manager 가 실행되고 있는 시스템의 정규화된 도메인 이름을 정의합니다.

2. Register as a New User (페이지 50)(새 사용자로 등록)에서 만든 자체 등록된 사용자의 고유 식별자를 입력하고 "다음"을 클릭합니다.
3. 메시지가 표시될 때마다 확인 질문에 대답합니다. 대답은 등록 중에 제공한 것입니다.

   참고: 각 질문에 대해 올바른 응답이 필요합니다. 태스크를 취소하거나 브라우저를 닫는 경우 실패한 시도로 계산됩니다.
4. "제출"을 클릭합니다.

   새 암호를 제공하라는 메시지가 표시됩니다.

사용자 관리

사용자 관리에는 다음 오퍼레이션이 포함됩니다.

- NeteAuto CA Identity Manager 환경 액세스
- 사용자 수정
- 그룹 매니저 역할 할당
- 그룹 만들기
- 자체 등록된 사용자 관리

NeteAuto CA Identity Manager 환경 액세스

NeteAuto CA Identity Manager 환경에 액세스하려면 다음 절차를 수행하십시오.

다음 단계를 수행하십시오.

1. 브라우저에서 다음 URL 을 입력합니다.

   `http://hostname/iam/im/neteauto/imcss/index.jsp`

   hostname

   다음 예제와 같이 정규화된 도메인 이름을 정의합니다.

   http://myserver.mycompany.com/iam/im/neteauto/imcss/index.jsp.

   참고: Neteauto 스킨을 구성하지 않은 경우 다음 URL 을 사용하여 Neteauto 환경에 액세스할 수 있습니다.

   http://*hostname*/iam/im/neteauto

2. 로그인 화면에 다음 자격 증명을 입력합니다.

   사용자 이름

   SuperAdmin

   암호

   test

사용자 수정

사용자를 수정하려면 다음 절차를 수행하십시오.

다음 단계를 수행하십시오.

1. 암호 test 를 사용하여 SuperAdmin 으로 NeteAuto 환경에 로그인합니다.
2. "사용자", "사용자 관리", "사용자 수정"을 차례로 선택합니다.

   "사용자 선택" 화면이 나타납니다.

3. "검색"을 클릭합니다.

   NeteAuto 환경의 사용자 목록이 표시됩니다.

4. 다음과 같이 NeteAuto 관리자를 선택합니다.

   - LDAP 디렉터리의 경우 "NeteAuto Administrator"
   - 관계형 데이터베이스의 경우 "NeteAuto Admin"

   "선택"을 클릭합니다. NeteAuto 관리자의 프로필이 표시됩니다.

5. "제목" 필드에 "Manager"를 입력합니다. "제출"을 클릭합니다.

   태스크 제출이 확인됩니다.

6. "확인"을 클릭하여 기본 화면으로 돌아갑니다.

그룹 매니저 역할 할당

그룹 매니저 역할 할당이 필요합니다. 그룹 매니저를 할당하려면 다음 절차를 수행하십시오.

다음 단계를 수행하십시오.

1. SuperAdmin 으로 "역할 및 태스크" 탭을 선택하고 "관리자 역할", "관리자 역할 수정"을 차례로 선택합니다.
2. "그룹 매니저" 역할을 선택하고 "선택"을 클릭합니다.

   "그룹 매니저" 역할의 프로필이 나타납니다.

3. "구성원" 탭을 클릭하고 "구성원 정책"에서 "추가"를 클릭합니다.

   "구성원 정책" 화면이 나타납니다.

4. "구성원 규칙"의 "사용자" 필드에서 아래쪽 화살표를 클릭합니다.

   드롭다운 목록에서 "조건: <사용자-필터>"를 선택합니다.

   규칙의 필터를 입력할 수 있도록 "사용자" 필드가 변경됩니다.

5. 다음과 같이 구성원 자격 규칙을 입력합니다.
   a. 첫 번째 필드의 드롭다운 목록에서 "제목"을 선택합니다.
   b. 두 번째 필드에서 등호(=)가 선택되었는지 확인합니다.
   c. 세 번째 필드에 "Manager"를 입력합니다.
6. "범위 규칙" 섹션에서 다음과 같이 사용자, 그룹 및 조직(지원되는 경우)에 대한 규칙을 정의합니다.
   a. "사용자" 필드에서 아래쪽 화살표를 클릭하여 옵션 목록을 표시합니다. 목록에서 "(모두)"를 선택합니다.
   b. "그룹" 및 "조직" 필드(지원되는 경우)에서 'a' 단계를 반복합니다.
   c. "액세스 태스크" 필드는 비워 둡니다.
7. "확인"을 클릭합니다.

   만든 구성원 정책이 표시됩니다.
8. "제출"을 클릭합니다.

   태스크 제출이 확인됩니다.
9. "확인"을 클릭하여 기본 화면으로 돌아갑니다.
10. CA Identity Manager 를 닫습니다.

그룹 만들기

그룹을 만들려면 다음 절차를 수행하십시오.

다음 단계를 수행하십시오.

1. 다음과 같이 NeteAuto 관리자로 CA Identity Manager 에 로그인합니다.
   - LDAP 디렉터리의 경우 사용자 이름 "NeteAuto Administrator"와 암호 "test"를 입력합니다.
   - 관계형 데이터베이스의 경우 사용자 이름 "NeteAuto Admin"과 암호 "test"를 입력합니다.

   NeteAuto 관리자가 수행할 수 있는 태스크 목록이 나타납니다. NeteAuto 관리자는 제한된 수의 태스크만 수행할 수 있기 때문에 범주 대신 태스크가 나열됩니다.
2. "그룹 만들기"를 클릭합니다.
3. "새 그룹 만들기"가 선택되었는지 확인하고 "확인"을 클릭합니다.
4. 다음 중 경우에 맞는 단계를 구현합니다.
   - NeteAuto 환경에서 조직을 지원하는 경우
     a. "조직 이름" 필드에서 줄임표 기호(...)를 클릭하여 CA Identity Manager 가 그룹을 만드는 조직을 선택합니다.
     b. "조직 선택" 화면의 맨 아래에서 "NeteAuto"를 확장합니다.
     c. "Dealer"(딜러) 조직을 선택합니다.
   - NeteAuto 환경에서 조직을 지원하지 않는 경우 다음 단계로 이동합니다.
5. 다음 그룹 정보를 입력합니다.
   - 그룹 이름: Dealer Administrators
   - 그룹 설명: Administrators for NeteAuto dealerships

6. "구성원 자격" 탭을 클릭하고 "사용자 추가"를 클릭합니다.

   "사용자 선택" 화면이 나타납니다.

7. "검색"을 클릭합니다.
8. NeteAuto 관리자를 선택하고 "선택"을 클릭합니다.
9. "제출"을 클릭하여 그룹을 만듭니다.

자체 등록된 사용자 관리

자체 등록된 사용자를 관리하려면 다음 절차를 수행하십시오.

다음 단계를 수행하십시오.

1. 다음 자격 증명을 사용하여 NeteAuto 관리자로 CA Identity Manager 에 로그인합니다.

   - LDAP 디렉터리의 경우

     사용자 이름

     NeteAuto Administrator

     암호

     test

   - 관계형 데이터베이스:

     사용자 이름

     NeteAuto Admin

     암호

     test

   NeteAuto 관리자가 수행할 수 있는 태스크 목록이 사용자 콘솔의 왼쪽에 나타납니다. NeteAuto 관리자는 제한된 수의 태스크만 수행할 수 있기 때문에 범주 대신 태스크가 나열됩니다.

2. "그룹 수정"을 클릭합니다.

3. "검색"을 클릭합니다.

   그룹 목록이 표시됩니다.

4. "Dealer Administrators"를 선택하고 "선택"을 클릭합니다.
5. "구성원 자격" 탭을 클릭하고 "사용자 추가"를 클릭합니다.

   "사용자 선택" 화면이 나타납니다.

6. "검색"을 클릭합니다.
7. "사용자 검색" 화면에서 Register as a New User (페이지 50)(새 사용자로 등록)에 입력한 사용자를 선택합니다. "선택"을 클릭합니다.
8. "제출"을 클릭합니다.

   태스크 제출이 확인됩니다.

9. "확인"을 클릭하여 기본 화면으로 돌아갑니다.

사용자가 만들어진 그룹의 구성원인지 확인하려면 "그룹 보기" 태스크를 사용하십시오.

추가 기능을 구성하는 방법

NeteAuto 샘플을 설치하고 기본 CA Identity Manager 기능을 실습했으면 NeteAuto 환경을 사용하여 전자 메일 알림, 워크플로 등의 추가 CA Identity Manager 기능을 실습 및 테스트하십시오.

참고: 이러한 기능에 대한 자세한 내용은 *관리 안내서*를 참조하십시오.

전역 사용자 이름에 대한 SiteMinder 로그인 이름 제한

사용자가 SiteMinder 정책 서버에 로그인해야 하는 경우 전역 사용자 이름에 다음 문자 또는 문자열을 포함할 수 없습니다.

&
*
:
()

해결 방법

전역 사용자 이름에 이러한 문자를 사용하지 마십시오.

제 3 장: LDAP 사용자 저장소 관리

이 섹션은 다음 항목을 포함하고 있습니다.

CA Identity Manager 디렉터리

*CA Identity Manager 디렉터리*는 사용자, 그룹 및 조직 같은 개체가 사용자 디렉터리에 저장되는 방법과 CA Identity Manager 에 표현되는 방법을 설명합니다. CA Identity Manager 디렉터리는 하나 이상의 CA Identity Manager 환경과 연결됩니다.

CA Identity Manager 디렉터리를 만드는 방법

LDAP 사용자 저장소의 CA Identity Manager 디렉터리 만들기에는 다음 단계가 포함됩니다.

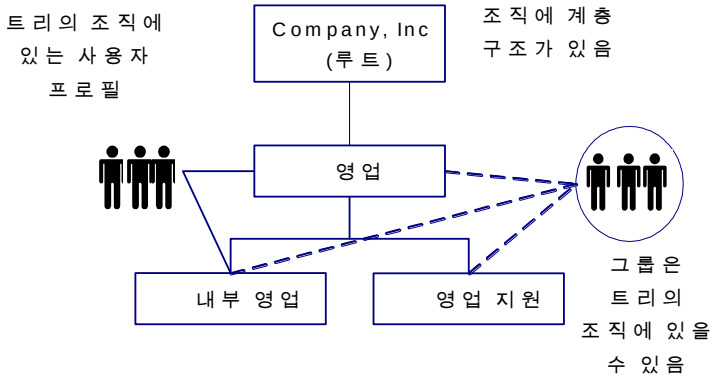
1. 디렉터리 구조를 결정합니다.
2. 디렉터리 구성 파일(directory.xml) (페이지 71)을 수정하여 사용자 저장소의 개체를 설명합니다.
3. 디렉터리 구성 파일을 가져오고 디렉터리를 만듭니다 (페이지 210).

참고: SiteMinder 를 사용하는 경우 CA Identity Manager 디렉터리를 만들기 전에 정책 저장소 스키마를 적용했는지 확인하십시오. 특정 정책 저장소 스키마와 해당 스키마를 적용하는 방법에 대한 자세한 내용은 *설치 안내서*를 참조하십시오.

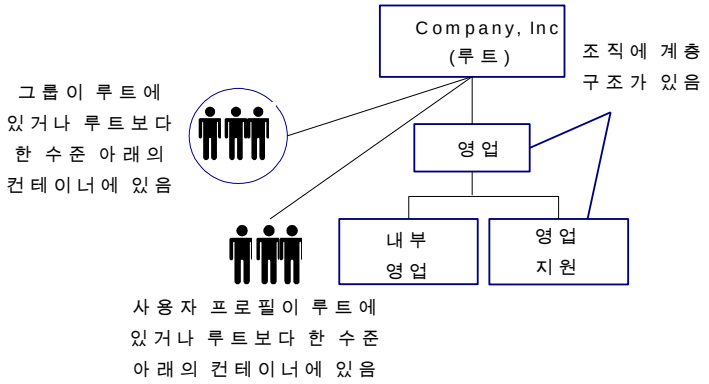
디렉터리 구조

CA Identity Manager 는 다음 디렉터리 구조를 지원합니다.

- 계층적 - 상위 조직(루트)과 하위 조직을 포함합니다. 다음 그림과 같이 하위 조직에 하위 조직이 포함될 수도 있는데, 이 경우 다단계 구조가 만들어집니다.

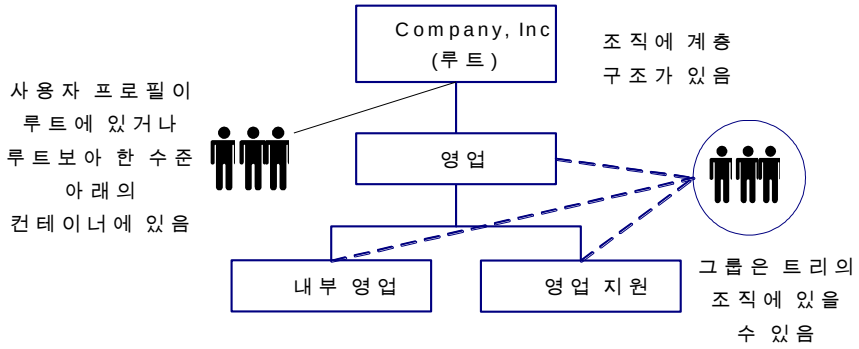


- 비계층적 - 사용자와 그룹이 검색 루트에 저장되거나 검색 루트보다 한 수준 아래의 컨테이너에 저장됩니다. 비계층적 디렉터리 구조를 보여주는 다음 그림과 같이 조직에는 계층적 구조가 있습니다.



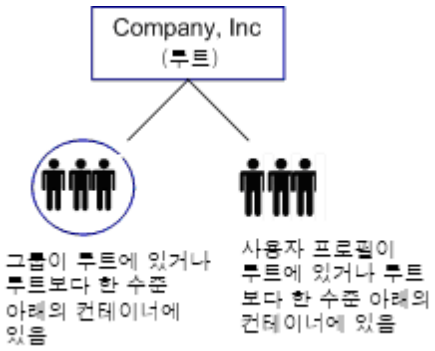
비계층적 디렉터리 구조에서 사용자 관리와 위임을 쉽게 수행하기 위해 사용자와 그룹은 논리적 조직에 속합니다. 논리적 조직은 사용자와 그룹 프로필에 특성으로 저장됩니다.

- 비계층적 사용자 - 조직과 그룹은 계층적으로 저장되지만 사용자는 검색 루트에 저장되거나 검색 루트보다 한 수준 아래의 컨테이너에 저장됩니다. 다음 다이어그램에 비계층적 사용자 디렉터리 구조가 나와 있습니다.



비계층적 사용자 디렉터리 구조에서 사용자는 논리적 조직에 속합니다. 사용자의 논리적 조직은 사용자 프로필에 특성으로 저장됩니다.

- 무조직 - 디렉터리에 조직이 포함되지 않습니다. 사용자와 그룹이 검색 루트에 저장되거나 검색 루트보다 한 수준 아래의 컨테이너에 저장됩니다. 다음 그림에 무조직 디렉터리 구조가 나와 있습니다.



참고: 한 디렉터리가 두 개 이상의 구조 유형을 포함할 수 있습니다. 예를 들어 사용자 프로필이 디렉터리의 한 부분에는 비계층적 구조로 저장되고 다른 부분에는 계층적 구조로 저장될 수 있습니다. 하이브리드 디렉터리 구조를 지원하려면 여러 CA Identity Manager 환경을 만드십시오.

디렉터리 구성 파일

CA Identity Manager 를 대상으로 사용자 디렉터리 구조를 설명하려면 디렉터리 구성 파일을 만드십시오.

디렉터리 구성 파일에는 다음과 같은 섹션이 하나 이상 포함됩니다.

CA Identity Manager Directory Information(CA Identity Manager 디렉터리 정보)

CA Identity Manager 디렉터리 정보를 포함합니다.

참고: 이 섹션의 정보는 수정하지 마십시오. 관리 콘솔에서 CA Identity Manager 디렉터리를 만들 때 이 정보를 제공하라는 메시지가 표시됩니다.

Attribute Validation(특성 유효성 검사)

CA Identity Manager 디렉터리에 적용되는 유효성 검사 규칙을 정의합니다.

Provider Information(공급자 정보)

CA Identity Manager 에서 관리하는 사용자 저장소에 대해 설명합니다.

Directory Search Information(디렉터리 검색 정보)

CA Identity Manager 가 사용자 저장소를 검색하는 방법을 지정할 수 있습니다.

User Object(사용자 개체)

사용자가 사용자 저장소에 저장되는 방법과 CA Identity Manager 에 표현되는 방법을 설명합니다.

Group Object(그룹 개체)

그룹이 사용자 저장소에 저장되는 방법과 CA Identity Manager 에 표현되는 방법을 설명합니다.

Organization Object(조직 개체)

조직이 저장되는 방법과 CA Identity Manager 에 표현되는 방법을 설명합니다. 조직 개체는 사용자 저장소에 조직이 포함되는 경우에만 상세 정보를 제공합니다.

Self-Subscribing Object(자체 구독 그룹)

자체 서비스 사용자가 참가할 수 있는 그룹에 대한 지원을 구성합니다.

Directory Groups Behavior(디렉터리 그룹 동작)

CA Identity Manager 디렉터리가 동적 그룹과 중첩된 그룹을 지원하는지 여부를 지정합니다.

디렉터리 구성 파일을 만들려면 구성 템플릿을 수정합니다.

디렉터리 구성 템플릿을 선택하는 방법

CA Identity Manager 는 다양한 디렉터리 유형과 구조를 지원하는 디렉터리 구성 템플릿을 제공합니다. CA Identity Manager 디렉터리를 만들려면 사용 중인 디렉터리 구조와 가장 근접하게 일치하는 템플릿을 수정하십시오.

다음 표에 설명된 템플릿은 관리 도구와 함께 설치됩니다.

admin_tools\directoryTemplates*directory_type*\

기본적으로 관리 도구는 다음 위치에 설치됩니다.

- **Windows:** C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools
- **UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

디렉터리 유형과 해당 구성 템플릿이 다음 표에 나와 있습니다.

디렉터리 유형	템플릿
계층적 구조가 있는 Active Directory(ADSI) LDAP 디렉터리	ActiveDirectory\directory.xml
계층적 구조가 있는 Microsoft ADAM 디렉터리	ADAM\directory.xml
계층적 구조가 있는 IBM Directory Server 디렉터리	IBMDirectoryServer\directory.xml
계층적 구조가 있는 Novell eDirectory 사용자 디렉터리	eDirectory\directory.xml
계층적 구조가 있는 Oracle Internet Directory	OracleInternetDirectory\directory.xml

디렉터리 유형	템플릿
계층적 구조가 있는 Sun Java System(SunOne 또는 iPlanet) LDAP 디렉터리	IPlanetHierarchical\directory.xml
비계층적 구조가 있는 Sun Java System(SunOne 또는 iPlanet) LDAP 디렉터리	IPlanetFlat\directory.xml
계층적 구조가 있는 CA Directory 사용자 저장소	eTrustDirectory\directory.xml
프로비저닝 디렉터리 이 템플릿은 CA Identity Manager 환경에 대해 프로비저닝 디렉터리를 구성합니다. **참고:** 이 구성 템플릿은 설치된 대로 사용할 수 있습니다. 이 템플릿은 수정할 필요가 없습니다.	ProvisioningServer\directory.xml
사용자 지정 디렉터리	사용 중인 디렉터리와 가장 비슷한 템플릿을 사용하십시오.

구성 템플릿을 덮어쓰지 않도록 새 디렉터리에 복사하거나 다른 이름으로 저장하십시오.

CA Identity Manager 를 대상으로 사용자 디렉터리를 설명하는 방법

디렉터리를 관리하려면 CA Identity Manager 가 디렉터리의 구조 및 콘텐츠를 이해해야 합니다. CA Identity Manager 를 대상으로 디렉터리를 설명하려면 적절한 템플릿 디렉터리에서 디렉터리 구성 파일(directory.xml)을 수정하십시오.

디렉터리 구성 파일에는 다음과 같은 중요한 규칙이 있습니다.

- ## - 필수 값을 나타냅니다.

  필요한 정보를 모두 제공하려면 이중 파운드 기호(##)를 모두 찾아 적절한 값으로 바꾸십시오. 예를 들어 ##DISABLED_STATE 는 사용자의 계정 상태를 저장하기 위해 특성을 제공해야 함을 나타냅니다.

- @ - CA Identity Manager 가 채우는 값을 나타냅니다. 디렉터리 구성 파일에서 이러한 값을 수정하지 마십시오. 디렉터리 구성 파일을 가져올 때 값을 제공하라는 메시지가 표시됩니다.

디렉터리 구성 파일을 수정하기 전에 알아 두어야 할 정보는 다음과 같습니다.

- 사용자, 그룹 및 조직 개체에 대한 LDAP 개체 클래스
- 사용자, 그룹 및 조직 프로필의 특성 목록

디렉터리 구성 파일을 수정하는 방법

디렉터리 구성 파일을 수정하려면 다음 단계를 수행하십시오.

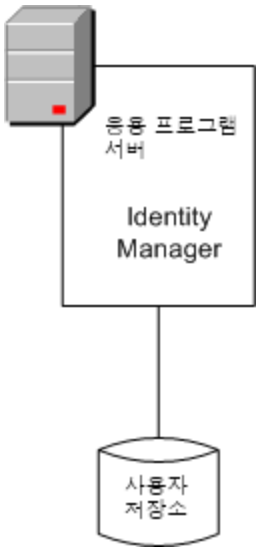
참고: 필수 단계는 그에 따라 설명되어 있습니다.

1. 검색 결과 (페이지 79)의 크기를 제한합니다.
2. 기본 사용자, 조직 또는 그룹 관리 개체를 수정합니다.
3. 기본 특성 설명을 변경합니다.
4. Well-Known 특성 (페이지 107)을 수정합니다. (필수)

   Well-Known 특성은 CA Identity Manager 에서 암호 특성과 같은 특수한 특성을 식별합니다.
5. 사용 중인 디렉터리 구조에 대해 CA Identity Manager 를 구성합니다 (페이지 117)(필수).
6. 사용자가 그룹을 구독 (페이지 118)하도록 설정합니다.

사용자 디렉터리에 대한 연결

다음 그림과 같이 CA Identity Manager 는 사용자 디렉터리에 연결하여 사용자, 그룹 및 조직 정보 같은 정보를 저장합니다.



새 디렉터리나 데이터베이스가 필요하지 않습니다. 하지만 기존 디렉터리나 데이터베이스가 FQDN(정규화된 도메인 이름)을 가진 시스템에 있어야 합니다.

지원되는 디렉터리 및 데이터베이스 유형 목록은 CA Support 사이트의 CA Identity Manager 지원표를 참조하십시오.

관리 콘솔에서 CA Identity Manager 디렉터리를 만들 때 사용자 저장소에 대한 연결을 구성합니다.

CA Identity Manager 디렉터리를 만든 후 디렉터리 구성을 내보내면 사용자 디렉터리 연결 정보가 디렉터리 구성 파일의 Provider 요소에 표시됩니다.

Provider 요소

구성 정보는 directory.xml 파일의 Provider 요소와 해당 하위 요소에 저장됩니다.

참고: CA Identity Manager 디렉터리를 만드는 경우 directory.xml 파일에서 디렉터리 연결 정보를 제공할 필요가 없습니다. 관리 콘솔의 CA Identity Manager 디렉터리 마법사에서 연결 정보를 제공하십시오. 업데이트하려는 경우에만 Provider 요소를 수정하십시오.

Provider 요소에는 다음과 같은 하위 요소가 있습니다.

LDAP

연결하고 있는 사용자 디렉터리를 설명합니다.

Credentials(자격 증명)

LDAP 사용자 저장소에 액세스하기 위한 사용자 이름과 암호를 제공합니다.

Connection(연결)

사용자 저장소가 있는 컴퓨터의 호스트 이름과 포트를 제공합니다.

Provisioning Domain(프로비저닝 도메인)

CA Identity Manager 가 관리하는 프로비저닝 도메인을 정의합니다(프로비저닝 사용자만 해당).

완료된 Provider 요소는 다음 코드와 비슷합니다.

```
<Provider type="LDAP" userdirectory="@SMDirName">
   <LDAP searchroot="@SMDirSearchRoot" secure="@SMDirSecure" />
   <Credentials user="@SMDirUser"
     cleartext="true">@SMDirPassword</Credentials>
   <Connection host="@SMDirHost" port="@SMDirPort" />
   <eTrustAdmin domain="@SMDirETrustAdminDomain" />
</Provider>
```

Provider 요소에는 다음 매개 변수가 포함됩니다.

type

데이터베이스의 유형을 지정합니다. 모든 LDAP 사용자 저장소의 경우 "LDAP"(기본값)를 지정하십시오.

userdirectory

사용자 디렉터리 연결의 이름을 지정합니다.

참고: directory.xml 파일에 사용자 디렉터리 연결의 이름을 지정하지 마십시오. 관리 콘솔에서 CA Identity Manager 디렉터리를 만들 때 이름을 제공하라는 메시지가 표시됩니다.

참고: 매개 변수는 선택 사항입니다.

LDAP 하위 요소

LDAP 하위 요소에는 다음 매개 변수가 포함됩니다.

searchroot

디렉터리의 시작점 역할을 하는 LDAP 디렉터리의 위치를 지정합니다. 주로 조직(o) 또는 조직 단위(ou)입니다.

secure

다음과 같이 LDAP 사용자 디렉터리에 대한 SSL(Secure Sockets Layer) 연결을 강제 적용합니다.

- true - CA Identity Manager 가 보안 연결을 사용합니다.
- false - CA Identity Manager 가 SSL 없이 사용자 디렉터리에 연결합니다(기본값).

참고: 매개 변수는 선택 사항입니다.

Credentials 하위 요소

LDAP 디렉터리에 연결하려면 CA Identity Manager 가 유효한 자격 증명을 제공해야 합니다. 자격 증명은 다음 코드와 비슷한 Credentials 하위 요소에서 정의됩니다.

```
<Credentials user="@SMDirUser" cleartext="true">
  "MyPassword"
</Credentials>
```

Credentials 하위 요소에서 암호를 지정하지 않으면 관리 콘솔에서 CA Identity Manager 디렉터리를 만들 때 암호를 제공하라는 메시지가 표시됩니다.

참고: 관리 콘솔에서 암호를 지정하는 것이 좋습니다.

관리 콘솔에서 암호를 지정하면 CA Identity Manager 에서 자동으로 암호를 암호화합니다. 그렇지 않은 경우 암호를 일반 텍스트로 표시하지 않으려면 CA Identity Manager 와 함께 설치된 암호 도구를 사용하여 암호를 암호화하십시오.

참고: 자격 증명 세트는 하나만 지정할 수 있습니다. Connection 하위 요소에 설명된 대로 여러 디렉터리를 정의하는 경우에는 지정하는 자격 증명이 모든 디렉터리에 적용되어야 합니다.

Credentials 하위 요소에는 다음 매개 변수가 포함됩니다.

user

디렉터리에 액세스할 수 있는 계정의 로그인 ID 를 지정합니다.

프로비저닝 사용자의 경우 지정하는 사용자 계정은 프로비저닝 서버에서 "도메인 관리자" 프로필이나 해당 권한 세트를 가져야 합니다.

참고: directory.xml 파일에서 사용자 매개 변수의 값을 지정하지 마십시오. 관리 콘솔에서 CA Identity Manager 디렉터리를 만들 때 로그인 ID 를 제공하라는 메시지가 표시됩니다.

cleartext

다음과 같이 암호가 directory.xml 파일에 일반 텍스트로 표시되는지 여부를 결정합니다.

- true - 암호가 일반 텍스트로 표시됩니다.
- false - 암호가 암호화됩니다(기본값).

참고: 매개 변수는 선택 사항입니다.

Connection 하위 요소

Connection 하위 요소는 CA Identity Manager 가 관리하는 사용자 저장소의 위치를 설명합니다. 이 하위 요소에는 다음 매개 변수가 포함됩니다.

host

사용자 디렉터리가 있는 시스템의 호스트 이름이나 IP 주소를 지정합니다.

참고: 연결하는 시스템에 IPv6 주소가 있는 경우 다음과 같이 IP 주소를 괄호([ ])로 묶으십시오.

<Connection host="[2::9255:214:22ff:fe72:525a]" port="20389"
failover="[2::9255:214:22ff:fe72:525a]:20389"/>

port

사용자 디렉터리의 포트 번호를 지정합니다.

failover

기본 시스템을 사용할 수 없는 경우 중복 사용자 저장소가 있는 시스템의 호스트 이름과 IP 주소를 지정합니다. 기본 시스템을 다시 사용할 수 있게 되더라도 장애 조치 시스템이 계속해서 사용됩니다. 기본 시스템 사용으로 돌아가려면 보조 시스템을 다시 시작하십시오. 여러 서버가 나열된 경우 CA Identity Manager 는 나열된 순서대로 시스템에 연결하려고 시도합니다.

다음과 같이 failover 특성에서 *공백으로 구분된* 목록으로 호스트 이름과 IP 주소를 지정하십시오.

failover="IPaddress:port IPaddress:port"

예:

<Connection host="123.456.789.001" port="20389"
failover="123.456.789.002:20389 123.456.789.003:20389"/>

참고: 포트 20389 는 프로비저닝 서버의 기본 포트입니다.

참고: 매개 변수는 선택 사항입니다.

Provisioning 하위 요소

CA Identity Manager 환경에 프로비저닝이 포함된 경우 다음과 같이 프로비저닝 도메인을 정의하십시오.

```
<eTrustadmin domain="@SMDirProvisioningDomain" />
```

Provisioning 하위 요소에는 다음 매개 변수가 포함됩니다.

domain

CA Identity Manager 가 관리하는 프로비저닝 도메인의 이름을 포함합니다.

관리 콘솔에서 CA Identity Manager 디렉터리를 만들 때 도메인 이름을 제공하라는 메시지가 표시됩니다. 따라서 디렉터리 구성 파일(directory.xml)에서 domain 매개 변수의 값을 지정하십시오.

디렉터리 검색 매개 변수

DirectorySearch 요소에서 다음 검색 매개 변수를 설정할 수 있습니다.

maxrows

사용자 디렉터리를 검색할 때 CA Identity Manager 가 반환할 수 있는 최대 개체 수를 지정합니다. 개체 수가 한도를 초과하면 오류가 표시됩니다.

maxrows 매개 변수의 값을 설정하여 검색 결과를 제한하는 LDAP 디렉터리의 설정을 재정의할 수 있습니다. 충돌하는 설정이 적용되는 경우 LDAP 서버는 가장 낮은 설정을 사용합니다.

참고: maxrows 매개 변수는 CA Identity Manager 태스크 화면에 표시되는 개체 수를 제한하지 않습니다. 표시 설정을 구성하려면 CA Identity Manager 사용자 콘솔에서 목록 화면 정의를 수정하십시오. 지침은 *User Console Design Guide*(사용자 콘솔 디자인 안내서)를 참조하십시오.

maxpagesize

단일 검색에서 반환될 수 있는 개체 수를 지정합니다. 개체 수가 페이지 크기를 초과하는 경우 다중 검색이 수행됩니다.

maxpagesize 를 지정할 때는 다음 사항에 주의하십시오.

- maxpagesize 옵션을 사용하려면 CA Identity Manager 가 관리하는 사용자 저장소가 페이지 단위 처리를 지원해야 합니다. 일부 사용자 저장소 유형의 경우 페이지 단위 처리를 지원하려면 추가 구성이 필요합니다. 자세한 내용은 대규모 검색 성능을 개선하는 방법 (페이지 131)을 참조하십시오.
- 사용자 저장소가 페이지 단위 처리를 지원하지 않는 경우 maxrows 의 값이 지정되면 CA Identity Manager 가 maxrows 값만 사용하여 검색 크기를 제어합니다.

timeout

검색을 종료하기 전에 CA Identity Manager 가 디렉터리를 검색하는 최대 시간(초)을 결정합니다.

참고: DirectorySearch 요소는 선택 사항입니다. 하지만 디렉터리가 페이지 단위 처리 (페이지 131)를 지원하므로 DirectorySearch 요소를 지정하는 것이 좋습니다.

추가 정보:

디렉터리 검색 성능을 개선하는 방법 (페이지 129)
대규모 검색 성능을 개선하는 방법 (페이지 131)

사용자, 그룹 및 조직 관리 개체 설명

CA Identity Manager 에서 사용자 디렉터리의 항목에 해당하는 다음 개체 유형을 관리해야 합니다.

사용자

엔터프라이즈의 사용자를 나타냅니다. 사용자는 단일 조직에 속합니다.

그룹

공통 사항을 가지고 있는 사용자의 연결을 나타냅니다.

조직

비즈니스 단위를 나타냅니다. 조직은 사용자, 그룹 및 다른 조직 같은 상세 정보를 포함합니다.

개체 설명에는 다음과 같은 정보가 포함되어 있습니다.

- LDAP 개체 클래스, 개체가 저장된 컨테이너 같은 개체 (페이지 157) 정보
- 항목에 대한 정보를 저장하는 특성 (페이지 163). 예를 들어 호출기 특성은 호출기 번호를 저장합니다.

참고: CA Identity Manager 환경은 사용자, 그룹 및 조직 개체 유형을 하나만 지원합니다. 예를 들어 모든 사용자 개체는 동일한 개체 클래스를 가집니다.

관리 개체 설명

관리 개체는 디렉터리 구성 파일의 User Object, Group Object 및 Organization Object 섹션에서 개체 정보를 지정하여 설명됩니다.

참고: 구성 템플릿(directory.xml 파일)을 사용하는 경우 조직을 지원하지 않는 사용자 디렉터리에 대해서는 Organization Object 섹션을 사용할 수 없습니다.

이러한 각 섹션에는 다음 예제와 같이 ImsManagedObject 요소가 포함됩니다.

```
<ImsManagedObject name="User" description="My Users"
objectclass="top,person,organizationalperson,inetorgperson" objecttype="USER">
```

선택적으로 ImsManagedObject 요소에는 다음 예제와 같이 Container 요소가 포함될 수 있습니다.

```
<Container objectclass="top,organizationalUnit" attribute="ou" value="people" />
```

개체 정보 지정

개체 정보는 다양한 매개 변수의 값을 제공하는 방법으로 지정됩니다.

다음 단계를 수행하십시오.

1. User Object, Organization Object 또는 Group Object 섹션에서 ImsManagedObject 요소를 찾습니다.
2. 다음 매개 변수의 값을 제공합니다.

   name

   관리 개체의 고유 이름을 지정합니다.

   참고: 이 매개 변수는 필수 사항입니다.

   description

   관리 개체에 대한 설명을 포함합니다.

   objectclass

   개체 유형(사용자, 그룹 또는 조직)에 대한 LDAP 개체 클래스의 이름을 지정합니다. 개체 클래스는 개체의 사용 가능한 특성 목록을 결정합니다.

   여러 개체 클래스의 특성이 개체 유형에 적용되는 경우 쉼표로 구분된 목록으로 개체 클래스를 나열하십시오. 예를 들어 개체가 person, organizationalperson 및 inetorgperson 개체 클래스의 특성을 포함하는 경우 다음과 같이 해당 개체 클래스를 추가하십시오.

   objectclass="top,person,organizationalperson,inetorgperson"

   각 LDAP 디렉터리에는 미리 정의된 개체 클래스 세트가 포함됩니다. 미리 정의된 개체 클래스에 대한 자세한 내용은 디렉터리 서버 설명서를 참조하십시오.

   참고: 이 매개 변수는 필수 사항입니다.

objecttype

관리 개체의 유형을 지정합니다. 유효한 값은 다음과 같습니다.

- 사용자
- 조직
- 그룹

참고: 이 매개 변수는 필수 사항입니다.

maxrows

사용자 디렉터리를 검색할 때 CA Identity Manager 가 반환할 수 있는 최대 개체 수를 지정합니다. 개체 수가 한도를 초과하면 오류가 표시됩니다.

maxrows 매개 변수의 값을 설정하여 검색 결과를 제한하는 LDAP 디렉터리의 설정을 재정의할 수 있습니다. 충돌하는 설정이 적용되는 경우 LDAP 서버는 가장 낮은 설정을 사용합니다.

참고: maxrows 매개 변수는 CA Identity Manager 태스크 화면에 표시되는 개체 수를 제한하지 않습니다. 표시 설정을 구성하려면 CA Identity Manager 사용자 콘솔에서 목록 화면 정의를 수정하십시오. 지침은 *User Console Design Guide*(사용자 콘솔 디자인 안내서)를 참조하십시오.

maxpagesize

단일 검색에서 반환될 수 있는 개체 수를 지정합니다. 개체 수가 페이지 크기를 초과하는 경우 다중 검색이 수행됩니다.

"Search Page Size"(검색 페이지 크기)를 지정할 때는 다음 사항에 주의하십시오.

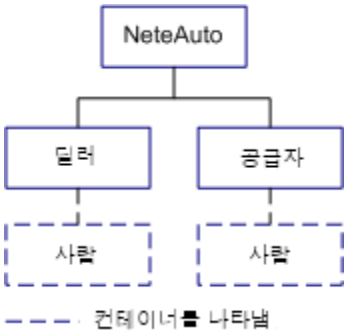
- "Search Page Size"(검색 페이지 크기) 옵션을 사용하려면 CA Identity Manager 가 관리하는 사용자 저장소가 페이지 단위 처리를 지원해야 합니다. 일부 사용자 저장소 유형의 경우 페이지 단위 처리를 지원하려면 추가 구성이 필요합니다. 자세한 내용은 대규모 검색 성능을 개선하는 방법 (페이지 131)을 참조하십시오.
- 사용자 저장소가 페이지 단위 처리를 지원하지 않는 경우 maxrows 의 값이 지정되면 CA Identity Manager 가 maxrows 값만 사용하여 검색 크기를 제어합니다.

3. 선택적으로 컨테이너 정보를 제공합니다.

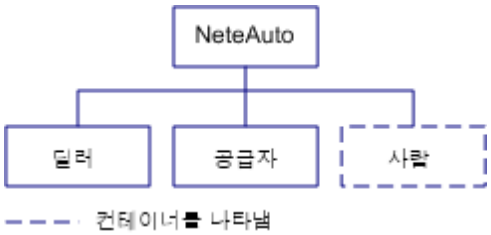
컨테이너

관리를 단순화하기 위해 특정 유형의 개체를 컨테이너로 그룹화할 수 있습니다. 디렉터리 구성 파일에서 컨테이너를 지정하는 경우 CA Identity Manager 는 컨테이너의 항목만 관리합니다. 예를 들어 People 이라는 사용자 컨테이너를 지정하는 경우 CA Identity Manager 는 다음 그림과 같이 People 컨테이너의 사용자를 관리합니다.

- 계층적 디렉터리



- 비계층적 디렉터리



이러한 예제에서 모든 사용자는 People 컨테이너에 있습니다.

컨테이너를 지정하는 경우 다음 사항에 주의하십시오.

- 조직에 컨테이너가 없으면 첫 번째 항목이 추가되는 즉시 CA Identity Manager 가 컨테이너를 만듭니다. 계층적 디렉터리의 경우 CA Identity Manager 는 항목이 추가된 조직에 컨테이너를 만듭니다. 비계층적 디렉터리와 조직을 지원하지 않는 디렉터리의 경우 CA Identity Manager 는 CA Identity Manager 디렉터리를 만들 때 지정하는 검색 루트 아래에 컨테이너를 만듭니다.
- CA Identity Manager 는 지정된 컨테이너에 없는 항목을 무시합니다. 예를 들어 People 컨테이너를 지정하면 People 컨테이너 외부에 있는 사용자를 관리할 수 없습니다.

  참고: 지정된 컨테이너에 없는 사용자를 관리하기 위해 다른 CA Identity Manager 환경을 만들 수 있습니다.

컨테이너 및 Well-Known 특성

Well-Known 특성은 CA Identity Manager 에서 특수한 의미를 가지는 특성입니다. CA Identity Manager 가 컨테이너를 포함하는 사용자 저장소를 관리하는 경우 다음과 같은 Well-Known 특성이 컨테이너 정보를 식별합니다.

%ORG_MEMBERSHIP%

컨테이너의 DN(전체 이름)을 저장하는 특성을 식별합니다.

예를 들어 전체 이름은 다음과 비슷합니다.

ou=People, ou=Employee, ou=NeteAuto, dc=security, dc=com

%ORG_MEMBERSHIP_NAME%

특성의 사용자에게 친숙한 이름을 저장하는 특성을 식별합니다.

예를 들어 이전 예제에서 컨테이너의 사용자에게 친숙한 이름은 People 입니다.

이러한 Well-Known 특성은 다음과 같이 directory.xml 파일의 User Object 및 Group Object 섹션에 있는 특성 설명에 나타납니다.

```
 <ImsManagedObjectAttr physicalname="someattribute" description="Organization"
displayname="Organization" valuetype="String" required="true"
wellknown="%ORG_MEMBERSHIP%" maxlength="0" permission="WRITEONCE"
searchable="false" />
```

계층적 사용자 저장소 구조의 경우 physicalname 및 wellknown 매개 변수는 다음과 같이 Well-Known 특성에 매핑됩니다.

```
<ImsManagedObjectAttr physicalname="%ORG_MEMBERSHIP%" description="Organization"
displayname="Organization" valuetype="String" required="true"
wellknown="%ORG_MEMBERSHIP%" maxlength="0" permission="WRITEONCE"
searchable="false" />
```

예제에서는 CA Identity Manager 가 directory.xml 파일의 다른 정보에서 컨테이너 DN 과 사용자에게 친숙한 이름을 자동으로 파생합니다.

비계층적 사용자 저장소 구조의 경우 물리적 특성 이름을 제공하십시오.

참고: 지침은 비계층적 사용자 디렉터리 구조를 설명하는 방법 (페이지 117)을 참조하십시오.

사용자 또는 그룹 컨테이너 지정

사용자 또는 그룹 컨테이너를 지정하려면 다음 절차를 수행하십시오.

다음 단계를 수행하십시오.

1. User Object 또는 Group Object 섹션에서 Container 요소를 찾습니다.
2. 다음 매개 변수의 값을 제공합니다.

objectclass

특정 유형의 개체가 만들어지는 컨테이너의 LDAP 개체 클래스를 결정합니다. 예를 들어 사용자 컨테이너의 기본값은 "top,organizationalUnit"인데, 이는 사용자가 LDAP 조직 단위(ou)에 만들어짐을 나타냅니다.

동적 또는 중첩된 그룹을 관리하고 있는 경우 해당 그룹 유형을 지원하는 (페이지 120) 개체 클래스를 지정해야 합니다.

참고: 이 매개 변수는 필수 사항입니다.

attribute

컨테이너 이름을 저장하는 특성(예: ou)을 지정합니다.

다음 예제와 같이 특성은 값과 쌍으로 연결되어 컨테이너의 상대 DN 을 형성합니다.

ou=People

참고: 이 매개 변수는 필수 사항입니다.

value

컨테이너의 이름을 지정합니다.

참고: 이 매개 변수는 필수 사항입니다.

참고: 조직에 대해서는 컨테이너를 지정할 수 없습니다.

특성 설명

특성은 전화 번호, 주소 같은 항목 정보를 저장합니다. 항목 특성은 해당 프로필을 결정합니다.

디렉터리 구성 파일에서 특성은 ImsManagedObjectAttr 요소에서 설명됩니다. 디렉터리 구성 파일의 User Object, Group Object 및 Organization Object 섹션에서 다음 동작을 수행할 수 있습니다.

- 기본 특성 설명을 수정하여 사용자 저장소의 특성을 설명합니다.
- 기존 설명을 복사하고 필요에 따라 값을 수정하여 새 특성 설명을 지정합니다.

사용자, 그룹 및 조직 프로필의 각 특성마다 ImsManagedObjectAttr 요소가 하나씩 있습니다. 예를 들어 ImsManagedObjectAttr 요소는 사용자 ID 로 설명됩니다.

ImsManagedObjectAttr 요소는 다음 코드와 유사합니다.

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

ImsManagedObjectAttr 에는 다음 매개 변수가 있습니다.

physicalname

이 매개 변수는 다음 항목 중 하나를 포함해야 합니다.

- 프로필 값이 저장되는 LDAP 특성의 이름. 예를 들어 사용자 ID 는 사용자 디렉터리의 uid 특성에 저장됩니다.

  참고: 성능을 개선하려면 사용자 콘솔에서 검색 쿼리에 사용되는 LDAP 특성을 색인화하십시오.

- Well-Known 특성 (페이지 107) Well-Known 특성을 제공하는 경우 값이 자동으로 계산됩니다. 예를 들어 Well-Known 특성 %ORG_MEMBERSHIP%를 지정하는 경우 CA Identity Manager 는 항목의 DN 을 기반으로 해당 항목이 속한 조직을 결정합니다.

description

특성에 대한 설명을 포함합니다.

displayname

특성의 고유 이름을 지정합니다.

사용자 콘솔에서 태스크 화면에 추가할 수 있는 특성 목록에 표시 이름이 나타납니다. 이 매개 변수는 필수 사항입니다.

참고: 디렉터리 구성 파일(directory.xml)에서 특성의 표시 이름을 수정하지 마십시오. 태스크 화면에서 특성의 이름을 변경하려면 태스크 화면 정의에서 특성에 대한 레이블을 지정하면 됩니다. 자세한 내용은 *관리 안내서*를 참조하십시오.

valuetype

특성의 데이터 유형을 지정합니다. 유효한 값은 다음과 같습니다.

String(문자열)

값이 임의의 문자열일 수 있습니다.

이것이 기본값입니다.

Integer(정수)

값이 정수여야 합니다.

참고: 정수는 소수를 지원하지 않습니다.

Number(숫자)

값이 정수여야 합니다. 숫자 옵션은 소수를 지원합니다.

Date(날짜)

값이 다음 패턴을 사용하여 유효한 날짜로 구문 분석되어야 합니다.

yyyy/MM/dd

ISODate(ISO 날짜)

값이 yyyy-MM-dd 패턴을 사용하여 유효한 날짜로 구문 분석되어야 합니다.

UnicenterDate(Unicenter 날짜)

값이 YYYYYYYDDD 패턴을 사용하여 유효한 날짜로 구문 분석되어야 합니다.

여기서 YYYYYYY 는 세 개의 0 으로 시작하는 7 자리 숫자의 연도 표현입니다. 예: 0002008

DDD 는 필요에 따라 0 으로 시작하는 3 자리 숫자의 날짜 표현입니다. 유효한 값의 범위는 001 - 366 입니다.

Structured(구조화됨)

이 유형의 특성은 단일 특성 값으로 여러 관련 값을 저장하는 데 사용되는 구조화된 데이터로 구성됩니다. 예를 들어 구조화된 특성은 이름, 성 및 전자 메일 주소 값 같은 값을 포함합니다.

특정 끝점 유형은 이러한 특성을 사용하지만 CA Identity Manager 를 통해 관리됩니다.

참고: CA Identity Manager 는 구조화된 특성을 사용자 콘솔에 표 형식으로 표시할 수 있습니다. 사용자가 표에서 값을 편집하면 해당 값이 사용자 저장소에 저장되면서 끝점으로 다시 전파됩니다. 다중값 특성 표시에 대한 자세한 내용은 *관리 안내서*를 참조하십시오.

required

다음과 같이 특성이 필수 사항인지 여부를 나타냅니다.

- true - 특성이 필수 사항입니다.
- false - 특성이 선택 사항입니다(기본값).

참고: 특성이 LDAP 디렉터리 서버에 대한 필수 사항인 경우 required 매개 변수를 true 로 설정하십시오.

multivalued

특성이 다중 값을 가질 수 있는지 여부를 나타냅니다. 예를 들어 "그룹 구성원 자격"은 각 그룹 구성원의 사용자 DN 을 저장하는 다중값 특성입니다. 유효한 값은 다음과 같습니다.

- true - 특성이 다중 값을 가질 수 있습니다.
- false - 특성이 단일 값만 가질 수 있습니다(기본값).

중요! 사용자 개체 정의의 "그룹 구성원 자격" 및 "관리자 역할"은 다중값 특성이어야 합니다.

wellknown

Well-Known 특성의 이름을 정의합니다.

Well-Known 특성은 CA Identity Manager 에서 특정한 의미를 가집니다 (페이지 107). 이러한 특성은 다음 구문에서 식별됩니다.

%ATTRIBUTENAME%

maxlength

특성의 값이 가질 수 있는 최대 길이를 정의합니다. 길이를 무제한으로 지정하려면 maxlength 매개 변수를 0 으로 설정하십시오.

참고: 이 매개 변수는 필수 사항입니다.

permission

태스크 화면에서 특성의 값을 수정할 수 있는지 여부를 나타냅니다. 유효한 값은 다음과 같습니다.

READONLY

값이 표시되기는 하지만 수정할 수는 없습니다.

WRITEONCE

개체가 만들어진 후에는 값을 수정할 수 없습니다. 예를 들어 사용자가 만들어진 후에는 사용자 ID 를 변경할 수 없습니다.

READWRITE

값을 수정할 수 있습니다(기본값).

hidden

특성이 CA Identity Manager 태스크 양식에 표시되는지 여부를 나타냅니다. 유효한 값은 다음과 같습니다.

- true - 사용자에게 특성이 표시되지 않습니다.
- false - 사용자에게 특성이 표시됩니다(기본값).

논리적 특성은 숨겨진 특성을 사용합니다.

참고: 자세한 내용은 *Programming Guide for Java*(Java 프로그래밍 안내서)를 참조하십시오.

system

CA Identity Manager 전용 특성을 지정합니다. 사용자 콘솔에서 사용자가 특성을 수정할 수 없습니다. 유효한 값은 다음과 같습니다.

- true - 사용자가 특성을 수정할 수 없습니다. CA Identity Manager 사용자 인터페이스에서 특성이 숨겨집니다.
- false - 사용자가 이 특성을 수정할 수 있습니다. CA Identity Manager 사용자 인터페이스에서 특성을 태스크 화면에 추가할 수 있습니다. (기본값)

validationruleset

유효성 검사 규칙 세트를 특성과 연결합니다.

지정하는 유효성 검사 규칙 세트가 디렉터리 구성 파일의 ValidationRuleSet 요소에 정의되었는지 확인하십시오.

objectclass

특성이 ImsManagedObject 요소에 지정된 기본 개체 클래스의 일부가 아닐 때 사용자, 그룹 또는 조직 특성의 LDAP 보조 클래스를 나타냅니다.

예를 들어 사용자의 기본 개체 클래스가 다음 사용자 특성을 정의하는 top, person 및 organizationalperson 이라고 가정하십시오.

- 일반 이름(cn)
- 성(sn)
- 사용자 ID(uid)
- 암호(userPassword)

이 경우 Employee 보조 클래스에 정의된 employeeID 특성을 포함하려면 다음 특성 설명을 추가합니다.

```
<ImsManagedObjectAttr physicalname="employeeID" displayname="Employee ID"
description="Employee ID" valuetype="String" required="true" multivalued="false"
maxlength="0" objectclass="Employee"/>
```

특성 설명 지정

특성 설명에는 다음 단계가 포함됩니다.

1. 다음 항목 중에서 관련 단원을 읽어 보십시오.
   - CA Directory 고려 사항 (페이지 104)
   - Microsoft Active Directory 고려 사항 (페이지 105)
   - IBM Directory Server 고려 사항 (페이지 105)
   - Oracle Internet Directory 고려 사항 (페이지 106)
2. 디렉터리 구성 파일의 User Object, Group Object 및 Organization Object 섹션에서 다음 동작을 수행합니다.
   - 디렉터리 특성을 설명하는 내용으로 기본 특성 설명을 수정하십시오.
   - 기존 설명을 복사하고 필요에 따라 값을 수정하여 새 특성 설명을 지정합니다.

   참고: 새 특성 설명이 지정되었고 물리적 특성이 지정되었다고 가정하겠습니다. 개체 유형에 대해 지정한 개체 클래스에 물리적 특성이 있어야 합니다.
3. (선택 사항) 사용자 콘솔에서 암호, 급여 같은 중요한 정보가 표시되지 않도록 특성의 표시 설정을 변경합니다 (페이지 98).
4. (선택 사항) 기본 정렬 순서를 구성합니다.
5. 비계층적 또는 비계층적 사용자 구조가 있는 디렉터리나 조직을 제외한 디렉터리를 관리하고 있는 경우 사용자 디렉터리 구조 설명 (페이지 117)으로 이동합니다.

중요한 특성 관리

CA Identity Manager 는 중요한 특성을 관리하기 위한 다음과 같은 방법을 제공합니다.

- 특성에 대한 데이터 분류

  데이터 분류를 사용하여 특성에 대한 표시 및 암호화 속성을 디렉터리 구성 파일(directory.xml)에 지정할 수 있습니다.

  다음과 같이 중요한 특성을 관리하는 데이터 분류를 정의할 수 있습니다.

  - CA Identity Manager 태스크 화면에서 일련의 별표로 특성의 값을 표시합니다.

    예를 들어 암호를 일반 텍스트로 표시하지 않고 별표로 표시할 수 있습니다.

  - "제출한 태스크 보기" 화면에서 특성 값을 숨깁니다.

    이 옵션을 사용하면 특성을 관리자로부터 숨길 수 있습니다. 예를 들어 CA Identity Manager 에서 태스크 상태는 보지만 월급 관련 세부 정보는 볼 필요가 없는 관리자에게 월급 등의 월급 관련 세부 정보가 표시되지 않도록 숨깁니다.

  - 기존 개체의 사본을 만들 때 특정 특성을 무시합니다.

  - 특성을 암호화합니다.

- 태스크 프로필 화면의 필드 스타일

  directory.xml 파일에서 특성을 수정하지 않으려면 중요한 특성이 나타나는 화면 정의에서 특성에 대한 표시 속성을 설정하십시오.

  필드 스타일을 사용하면 암호 등의 특성을 일반 텍스트 대신 일련의 별표로 표시할 수 있습니다.

  참고: 중요한 특성의 필드 스타일에 대한 자세한 내용을 보려면 사용자 콘솔 도움말에서 필드 스타일을 검색하십시오.

데이터 분류 특성

데이터 분류 요소는 추가 속성을 특성 설명과 연결하는 방법을 제공합니다. 이 요소의 값에 따라 CA Identity Manager 가 해당 특성을 처리하는 방식이 결정됩니다. 이 요소는 다음 매개 변수를 지원합니다.

- sensitive

  이 매개 변수를 설정하면 CA Identity Manager 가 "View Submitted Tasks"(제출한 태스크 보기) 화면에 특성을 일련의 별표(*)로 표시합니다. 이 매개 변수는 특성의 이전 값과 새 값이 "View Submitted Tasks"(제출한 태스크 보기) 화면에 일반 텍스트로 표시되지 않도록 합니다.

  또한 사용자 콘솔에서 기존 사용자에 대한 사본을 만들 경우 이 매개 변수를 설정하면 특성이 새 사용자에게 복사되지 않습니다.

- vst_hide

  "View Submitted Tasks"(제출한 태스크 보기) 탭의 "Event Details"(이벤트 정보) 화면에서 특성을 숨깁니다. 별표로 표시되는 sensitive 특성과 다르게 vst_hidden 특성은 아예 표시되지 않습니다.

  이 매개 변수를 사용하여 월급과 같은 특성의 변경 사항이 "View Submitted Tasks"(제출한 태스크 보기)에 표시되지 않도록 할 수 있습니다.

- ignore_on_copy

  이 매개 변수를 설정하면 관리자가 사용자 콘솔에서 개체 사본을 만들 때 CA Identity Manager 가 특성을 무시합니다. 예를 들어 사용자 개체의 암호 특성에 대해 ignore_on_copy 를 지정했다고 가정합니다. 사용자 프로필을 복사할 때 CA Identity Manager 는 현재 사용자의 암호를 새 사용자 프로필에 적용하지 않습니다.

- AttributeLevelEncrypt

  사용자 저장소에 저장되는 특성 값을 암호화합니다. CA Identity Manager 에서 FIPS 140-2 가 활성화되었을 경우 CA Identity Manager 는 RC2 암호화 또는 FIPS 140-2 암호화를 사용합니다.

  CA Identity Manager 의 FIPS 140-2 지원에 대한 자세한 내용은 *구성 안내서*를 참조하십시오.

  런타임에는 특성이 일반 텍스트로 표시됩니다.

  참고: 특성이 화면에 일반 텍스트로 표시되지 않도록 하기 위해 암호화된 특성에 sensitive 데이터 분류 요소를 추가할 수도 있습니다. 자세한 내용은 특성 수준 암호화를 추가하는 방법 (페이지 101)을 참조하십시오.

- PreviouslyEncrypted

  이 매개 변수를 설정하면 CA Identity Manager 가 사용자 저장소의 개체에 액세스할 때 특성의 암호화된 값을 감지하고 암호 해독합니다.

  이 데이터 분류를 사용하여 이전에 암호화된 값을 암호 해독할 수 있습니다.

  개체를 저장할 때 일반 텍스트 값이 저장소에 저장됩니다.

데이터 분류 특성 구성

다음 단계를 수행하십시오.

1. 디렉터리 구성 파일에서 특성을 찾습니다.
2. 특성 설명 뒤에 다음 특성을 추가합니다.

   <DataClassification name="*parameter*">

   parameter

   다음 매개 변수 중 하나를 나타냅니다.

   sensitive

   vst_hide

   ignore_on_copy

   AttributeLevelEncrypt

   PreviouslyEncrypted

   예를 들어 vst_hide 데이터 분류 특성을 포함하는 특성 설명은 다음 코드와 비슷합니다.

```
<ImsManagedObjectAttr physicalname="salary" displayname="Salary"
description="salary" valuetype="String" required="false" multivalued="false"
maxlength="0">
    <DataClassification name="vst_hide"/>
```

특성 수준 암호화

디렉터리 구성 파일(directory.xml)의 특성에 대해 AttributeLevelEncypt 데이터 분류를 지정하여 사용자 저장소에서 특성을 암호화할 수 있습니다. 특성 수준 암호화가 활성화되면 CA Identity Manager 가 특성의 값을 사용자 저장소에 저장하기 전에 암호화합니다. 특성은 사용자 콘솔에서 일반 텍스트로 표시됩니다.

참고: 특성이 화면에 일반 텍스트로 표시되지 않도록 하기 위해 암호화된 특성에 sensitive 데이터 분류 요소를 추가할 수도 있습니다. 자세한 내용은 특성 수준 암호화를 추가하는 방법 (페이지 101)을 참조하십시오.

FIPS 140-2 지원이 활성화된 경우 RC2 암호화 또는 FIPS 140-2 암호화를 사용하여 특성이 암호화됩니다.

특성 수준 암호화를 구현하려면 먼저 다음 사항에 주의하십시오.

- CA Identity Manager 는 검색에서 암호화된 특성을 찾을 수 없습니다.

  암호화된 특성이 구성원, 관리자, 소유자 정책 또는 ID 정책에 추가되었다고 가정합니다. CA Identity Manager 는 이 특성을 검색할 수 없기 때문에 해당 정책을 제대로 확인하지 못합니다.

  directory.xml 파일에서 특성을 searchable="false"로 설정해 봅니다. 예를 들면 다음과 같습니다.

  ```
  <ImsManagedObjectAttr physicalname="title" description="Title"
  displayname="Title" valuetype="String" maxlength="0" searchable="false">
  <DataClassification name="AttributeLevelEncrypt"/>
  </ImsManagedObjectAttr>
  ```

- CA Identity Manager 에서 공유 사용자 저장소와 프로비저닝 디렉터리를 사용하는 경우 프로비저닝 서버 특성을 암호화하지 마십시오.
- 다음 조건을 만족하는 환경의 사용자 암호에 대해서는 AttributeLevelEncrypt 를 활성화하지 마십시오.
  - CA SiteMinder 통합 포함
  - 관계형 데이터베이스에 사용자 저장

  CA Identity Manager 가 CA SiteMinder 와 통합되는 경우 암호를 암호화하면 새 사용자가 로그인하고 암호를 일반 텍스트로 입력하려고 할 때 문제가 발생합니다.
- CA Identity Manager 이외의 응용 프로그램에서 사용하는 사용자 저장소에 대해 특성 수준 암호화를 활성화하면 다른 응용 프로그램에서 암호화된 특성을 사용할 수 없습니다.

특성 수준 암호화를 추가하는 방법

특성 수준 암호화를 CA Identity Manager 디렉터리에 추가했다고 가정합니다. 그러면 해당 특성과 연결된 개체를 저장할 때 CA Identity Manager 가 자동으로 기존 일반 텍스트 특성 값을 암호화합니다. 예를 들어 암호 특성을 암호화하면 이 특성에서 사용자 프로필을 저장할 때 암호가 암호화됩니다.

참고: 특성 값을 암호화하려면 개체를 저장하는 데 사용할 태스크에 해당 특성이 포함되어야 합니다. 이전 예제의 암호 특성을 암호화하려면 개체를 저장하는 데 사용할 태스크(예: "사용자 수정" 태스크)에 암호 필드가 추가되어야 합니다.

모든 새 개체가 사용자 저장소에서 암호화된 값으로 생성됩니다.

다음 단계를 수행하십시오.

1. 다음 태스크 중 하나를 완료하십시오.
   - CA Identity Manager 디렉터리 만들기
   - 디렉터리 설정을 내보내어 기존 디렉터리 업데이트
2. 다음 데이터 분류 특성을 directory.xml 파일에서 암호화할 특성에 추가합니다.

   AttributeLevelEncrypt

   특성 값을 암호화된 형식으로 사용자 저장소에 보존합니다.

   sensitive(선택 사항)

   특성 값을 CA Identity Manager 화면에서 숨깁니다. 예를 들어 암호는 별표(*)로 표시됩니다.

   예:

```
<ImsManagedObjectAttr physicalname="salary" displayname="Salary"
description="salary" valuetype="String" required="false"
multivalued="false" maxlength="0" searchable="false">
<DataClassification name="AttributeLevelEncrypt"/>
<DataClassification name="sensitive"/>
```

3. CA Identity Manager 디렉터리를 만든 경우 이 디렉터리를 환경과 연결합니다.
4. CA Identity Manager 가 모든 값을 즉시 암호화하도록 하려면 대량 로더를 사용하여 모든 개체를 수정합니다.

   참고: 대량 로더에 대한 자세한 내용은 *관리 안내서*를 참조하십시오.

특성 수준 암호화를 제거하는 방법

암호화된 특성이 CA Identity Manager 디렉터리에 있고 일반 텍스트 형식의 이 특성 값과 함께 저장된 경우 AttributeLevelEncrypt 데이터 분류를 제거할 수 있습니다.

데이터 분류가 제거되면 CA Identity Manager 가 더 이상 새 특성 값을 암호화하지 않습니다. 특성과 연결된 개체를 저장하면 기존 값이 암호 해독됩니다.

참고: 특성 값을 암호 해독하려면 개체를 저장하는 데 사용할 태스크에 해당 특성이 포함되어야 합니다. 예를 들어 기존 사용자의 암호를 해독하려면 암호 필드를 포함하는 태스크(예: "사용자 수정" 태스크)와 함께 사용자 개체를 저장해야 합니다.

CA Identity Manager 가 특성에 대해 사용자 저장소에서 유지되는 암호화된 값을 감지하고 암호 해독하도록 하려면 다른 데이터 분류 PreviouslyEncrypted 를 지정하면 됩니다. 개체를 저장할 때 일반 텍스트 값이 사용자 저장소에 저장됩니다.

참고: PreviouslyEncrypted 데이터 분류를 추가하면 각 개체 로드에서 추가 처리가 늘어납니다. 성능 문제를 방지하려면 PreviouslyEncrypted 데이터 분류를 추가하고 해당 특성과 연결된 각 개체를 로드 및 저장한 후 데이터 분류를 제거하는 것이 좋습니다. 이 방법을 사용하면 모든 저장된 암호화된 값이 저장된 일반 텍스트로 자동으로 변환됩니다.

다음 단계를 수행하십시오.

1. 해당 CA Identity Manager 디렉터리의 디렉터리 설정을 내보냅니다.
2. directory.xml 파일을 열고 암호 해독할 특성에서 데이터 분류 AttributeLevelEncrypt 를 제거합니다.

3. CA Identity Manager 가 이전에 암호화된 값을 제거하도록 하려면 PreviouslyEncrypted 데이터 분류 특성을 추가합니다.

   예:

   ```
   <ImsManagedObjectAttr physicalname="salary" displayname="Salary"
   description="salary" valuetype="String" required="false" multivalued="false"
   maxlength="0" searchable="false">
   <DataClassification name="PreviouslyEncrypted"/>
   ```

4. CA Identity Manager 가 모든 값을 즉시 암호 해독하도록 하려면 대량 로더를 사용하여 모든 개체를 수정합니다.

   참고: 대량 로더에 대한 자세한 내용은 *관리 안내서*를 참조하십시오.

CA Directory 고려 사항

CA Directory 사용자 저장소에 대한 특성을 설명하는 경우 다음 사항에 주의하십시오.

- 특성 이름은 대소문자를 구분합니다.
- seeAlso 특성을 자체 구독 그룹을 나타내는 특성으로 사용하는 경우 관리자가 그룹을 만들 때 오류가 발생할 수 있습니다.

photo 특성을 사용자 계정 상태(enabled 또는 disabled)를 나타내는 특성으로 사용하는 경우 관리자가 사용자를 만들 때 오류가 발생할 수 있습니다.

참고: CA Directory 요구 사항에 대한 자세한 내용은 CA Directory 설명서를 참조하십시오.

Microsoft Active Directory 고려 사항

Active Directory 에 대한 특성을 설명하는 경우 다음 사항에 주의하십시오.

- 특성 설명에 지정된 특성의 대소문자는 Active Directory 에 있는 특성의 대소문자와 일치해야 합니다. 예를 들어 unicodePwd 특성을 사용자 암호를 저장하는 특성으로 선택하는 경우 디렉터리 구성 파일에서 unicodePwd(대문자 P 사용)를 지정하십시오.
- 사용자 및 그룹 개체의 경우 sAMAccountName 특성을 포함해야 합니다.

IBM Directory Server 고려 사항

IBM Directory Server 사용자 디렉터리에 대한 특성을 설명하는 경우 다음 단원을 참조하십시오.

- Directory Server 디렉터리의 그룹 (페이지 105)
- 조직 개체 설명의 개체 클래스 "top" (페이지 106)

Directory Server 디렉터리의 그룹

IBM Directory Server 의 경우 그룹에 구성원이 하나 이상 포함되어야 합니다. 이 요구 사항을 충족하기 위해 CA Identity Manager 는 그룹이 만들어질 때 *더미 사용자*를 새 그룹의 구성원으로 추가합니다.

더미 사용자 구성

다음 단계를 수행하십시오.

1. 디렉터리 구성 파일의 Group Object 섹션에서 다음 요소를 찾습니다.

```
<PropertyDict name="DUMMY_USER">
    <Property name="DUMMY_USER_DN">##DUMMY_USER_DN</Property>
</PropertyDict>
```

참고: 이러한 요소가 디렉터리 구성 파일에 없는 경우 여기에 표시된 대로 정확히 추가하십시오.

2. ##DUMMY_USER_DN 을 사용자 DN 으로 바꿉니다. CA Identity Manager 는 이 DN 을 모든 새 그룹의 구성원으로 추가합니다.

   참고: 기존 사용자의 DN 을 지정하는 경우 해당 사용자가 모든 CA Identity Manager 그룹의 구성원으로 나타납니다. *더미 사용자*가 그룹 구성원으로 나타나지 않도록 하려면 디렉터리에 없는 DN 을 지정하십시오.

3. 디렉터리 구성 파일을 저장합니다.

조직 개체 설명의 개체 클래스 "top"

중요! 디렉터리 구성 파일의 조직 개체 설명에 개체 클래스 top 를 포함하지 마십시오.

예를 들어 조직 개체의 개체 클래스가 top, organizationalUnit 인 경우 다음과 같이 개체 클래스를 지정하십시오.

```
<ImsManagedObject name="Organization" description="My Organizations"
objectclass="organizationalUnit" objecttype="ORG">
```

top 를 포함하는 경우 예상하지 못한 검색 결과가 발생할 수 있습니다.

Oracle Internet Directory 고려 사항

OID(Oracle Internet Directory) 사용자 저장소에 대한 특성을 설명하는 경우 소문자만 사용하여 LDAP 특성을 지정하십시오.

LDAP 사용자 저장소에 대한 Well-Known 특성

CA Identity Manager 에서 Well-Known 특성은 특별한 의미를 갖습니다. 이 특성은 다음 구문으로 식별됩니다.

%ATTRIBUTENAME%

이 구문에서 *ATTRIBUTENAME* 은 대문자여야 합니다.

Well-Known 특성은 특성 설명 (페이지 163)을 사용하여 하나의 물리적 특성에 매핑됩니다.

다음 특성 설명에서 userpassword 특성은 다음과 같이 CA Identity Manager 가 userpassword 의 값을 암호로 처리하도록 Well-Known 특성 %PASSWORD%에 매핑됩니다.

```
<ImsManagedObjectAttr
        physicalname="userpassword"
        displayname="Password"
        description="Password"
        valuetype="String"
        required="false"
        multivalued="false"
        wellknown="%PASSWORD%"
        maxlength="0" />
```

Well-Known 특성은 필수 사항일 수도 있고 선택 사항일 수도 있습니다.

사용자 Well-Known 특성

사용자 Well-Known 특성 및 해당 특성이 매핑되는 항목 목록은 다음과 같습니다.

%ADMIN_ROLE_CONSTRAINT%

관리자의 관리자 역할 목록에 매핑됩니다.

%ADMIN_ROLE_CONSTRAINT%에 매핑되는 물리적 특성은 다중값 특성이어야 여러 역할을 수용할 수 있습니다.

%ADMIN_ROLE_CONSTRAINT%에 매핑되는 LDAP 특성을 색인화하는 것이 좋습니다.

%CERTIFICATION_STATUS%

사용자의 인증 상태에 매핑됩니다.

이 특성은 사용자 인증 기능을 사용하는 데 필요합니다.

참고: 사용자 인증에 대한 자세한 내용은 *관리 안내서*를 참조하십시오.

%DELEGATORS%

작업 항목을 현재 사용자에게 위임한 사용자의 목록에 매핑됩니다.

이 특성은 위임을 사용하는 데 필요합니다. %DELEGATORS%에 매핑되는 물리적 특성은 문자열을 포함할 수 있는 다중 값이어야 합니다.

중요! CA Identity Manager 태스크 또는 외부 도구를 사용하여 이 필드를 직접 편집하면 보안에 중요한 영향을 미칠 수 있습니다.

%EMAIL%

사용자의 전자 메일 주소에 매핑됩니다.

전자 메일 알림 기능을 사용하는 데 필요합니다.

%ENABLED_STATE%

(필수)

사용자의 상태에 매핑됩니다.

참고: 이 특성은 SiteMinder 사용자 디렉터리 연결의 "비활성화된 플래그" 사용자 디렉터리 특성과 일치해야 합니다.

%FIRST_NAME%

사용자의 이름에 매핑됩니다.

%FULL_NAME%

사용자의 이름 및 성에 매핑됩니다.

%IDENTITY_POLICY%

사용자 계정에 적용된 ID 정책 목록과 사용자 개체에 대해 추가 또는 제거 동작을 수행한 고유 Policy Xpress 정책 ID 목록을 지정합니다.

CA Identity Manager 는 이 특성을 사용하여 ID 정책을 사용자에게 적용해야 하는지 여부를 결정합니다. 정책에 "Apply Once"(한 번 적용) 설정이 사용되도록 설정되어 있고 %IDENTITY_POLICY% 특성에 정책이 나열되어 있다고 가정하십시오. CA Identity Manager 는 정책의 변경 내용을 사용자에게 적용하지 않습니다.

참고: ID 정책에 대한 자세한 내용은 *관리 안내서*를 참조하십시오.

%LAST_CERTIFIED_DATE%

역할이 사용자에 대해 인증되는 날짜에 매핑됩니다.

사용자 인증 기능을 사용하는 데 필요합니다.

참고: 사용자 인증에 대한 자세한 내용은 *관리 안내서*를 참조하십시오.

%LAST_NAME%

사용자의 성에 매핑됩니다.

%MEMBER_OF%

사용자가 구성원으로 속한 그룹 목록에 매핑됩니다.

%MEMBER_OF%에 매핑되는 물리적 특성은 다중값 특성이어야 여러 그룹을 수용할 수 있습니다.

이 특성을 사용하는 경우 사용자 그룹을 검색할 때 응답 시간이 개선됩니다.

이 특성은 Active Directory 나 사용자 개체에서 사용자의 그룹 구성원 자격을 유지 관리하는 모든 디렉터리 스키마와 함께 사용할 수 있습니다.

%ORG_MEMBERSHIP%

(필수)

사용자가 속한 조직의 DN 에 매핑됩니다.

CA Identity Manager 는 이 Well-Known 특성을 사용하여 디렉터리 구조 (페이지 117)를 결정합니다.

사용자 디렉터리에 조직이 포함되지 않는 경우에는 이 특성이 필요하지 않습니다.

%ORG_MEMBERSHIP_NAME%

(필수)

사용자의 프로필이 있는 조직의 사용자에게 친숙한 이름에 매핑됩니다.

사용자 디렉터리에 조직이 포함되지 않는 경우에는 이 특성이 필요하지 않습니다.

%PASSWORD%

사용자의 암호에 매핑됩니다.

이 특성은 SiteMinder 사용자 디렉터리 연결의 "암호" 특성과 일치해야 합니다.

참고: 특성 또는 필드가 암호를 숨기도록 설정되어 있지 않더라도 %PASSWORD% 특성 값은 CA Identity Manager 화면에서 항상 일련의 별표(*) 문자로 표시됩니다.

%PASSWORD_DATA%

(암호 정책 지원 시 필수)

암호 정책 정보를 추적하는 특성을 지정합니다.

참고: 특성 또는 필드가 암호를 숨기도록 설정되어 있지 않더라도 %PASSWORD_DATA% 특성 값은 CA Identity Manager 화면에서 항상 일련의 별표(*) 문자로 표시됩니다.

%PASSWORD_HINT%

(필수)

사용자가 지정한 질문 및 대답 쌍에 매핑됩니다. 질문 및 대답 쌍은 사용자가 암호를 잊어버린 경우에 사용됩니다.

여러 질문 및 대답 쌍을 지원하려면 %PASSWORD_HINT% 특성이 다중값 특성인지 확인하십시오.

SiteMinder 의 "암호 서비스" 기능을 사용하여 암호를 관리하고 있는 경우 "암호 힌트" 특성은 SiteMinder 사용자 디렉터리의 "챌린지/응답" 특성과 일치해야 합니다.

참고: 특성 또는 필드가 암호를 숨기도록 설정되어 있지 않더라도 %PASSWORD% 특성 값은 CA Identity Manager 화면에서 항상 일련의 별표(*) 문자로 표시됩니다.

%USER_ID%

(필수)

사용자의 ID 에 매핑됩니다.

그룹 Well-Known 특성

다음 항목은 그룹 Well-Known 특성 목록입니다.

%GROUP_ADMIN_GROUP%

그룹의 관리자인 그룹 목록을 저장하는 특성을 나타냅니다. 예를 들어 그룹 1 이 그룹 A 의 관리자인 경우 그룹 1 은 %GROUP_ADMIN_GROUP% 특성에 저장됩니다.

참고: %GROUP_ADMIN_GROUP% 특성을 지정하지 않으면 관리자 그룹이 %GROUP_ADMIN% 특성에 저장됩니다.

참고: 그룹을 다른 그룹의 관리자로 추가하려면 *관리 안내서*를 참조하십시오.

%GROUP_ADMIN%

그룹 관리자의 DN 을 포함하는 특성을 나타냅니다.

%GROUP_ADMIN%에 매핑되는 물리적 특성은 다중값 특성이어야 합니다.

%GROUP_DESC%

그룹에 대한 설명을 포함하는 특성을 나타냅니다.

%GROUP_MEMBERSHIP%

(필수)

그룹의 구성원 목록을 포함하는 특성을 나타냅니다.

%GROUP_MEMBERSHIP%에 매핑되는 물리적 특성은 다중값 특성이어야 합니다.

프로비저닝 사용자 디렉터리에 대해서는 Well-Known 특성 %GROUP_MEMBERSHIP%가 필요하지 않습니다.

%GROUP_NAME%

(필수)

그룹 이름을 저장하는 특성을 나타냅니다.

%ORG_MEMBERSHIP%

(필수)

그룹이 속한 조직의 DN 을 포함하는 특성을 나타냅니다.

CA Identity Manager 는 이 Well-Known 특성을 사용하여 디렉터리 구조 (페이지 117)를 결정합니다.

사용자 디렉터리에 조직이 포함되지 않는 경우에는 이 특성이 필요하지 않습니다.

%ORG_MEMBERSHIP_NAME%

그룹이 있는 조직의 사용자에게 친숙한 이름을 포함하는 특성을 나타냅니다.

조직이 포함되지 않는 사용자 디렉터리에 대해서는 이 특성이 유효하지 않습니다.

%SELF_SUBSCRIBING%

사용자가 그룹 (페이지 116)을 구독할 수 있는지 여부를 결정하는 특성을 나타냅니다.

%NESTED_GROUP_MEMBERSHIP%

그룹의 구성원인 그룹 목록을 저장하는 특성을 나타냅니다. 예를 들어 그룹 1 이 그룹 A 의 구성원인 경우 그룹 1 은 %NESTED_GROUP_MEMBERSHIP% 특성에 저장됩니다.

%NESTED_GROUP_MEMBERSHIP% 특성을 지정하지 않으면 중첩된 그룹이 %GROUP_MEMBERSHIP% 특성에 저장됩니다.

그룹을 다른 그룹의 구성원으로 포함하려면 "동적 그룹과 중첩된 그룹 구성"에 설명된 지침에 따라 중첩된 그룹에 대한 지원을 구성하십시오.

%DYNAMIC_GROUP_MEMBERSHIP%

동적 그룹 (페이지 197)을 생성하는 LDAP 쿼리를 저장하는 특성을 나타냅니다.

참고: 보조 개체 클래스를 사용하여 %NESTED_GROUP_MEMBERSHIP% 및 %DYNAMIC_GROUP_MEMBERSHIP% 특성을 포함하도록 그룹 개체에 대해 사용할 수 있는 특성을 확장할 수 있습니다.

조직의 Well-Known 특성

다음 Well-Known 특성은 조직을 지원하는 환경에만 적용됩니다.

%ORG_DESCR%

조직에 대한 설명을 포함하는 특성을 나타냅니다.

%ORG_MEMBERSHIP%

(필수)

조직의 상위 조직의 DN 을 포함하는 특성을 나타냅니다.

%ORG_MEMBERSHIP_NAME%

조직의 상위 조직의 사용자에게 친숙한 이름을 포함하는 특성을 나타냅니다.

%ORG_NAME%

(필수)

조직의 이름을 포함하는 특성을 나타냅니다.

%ADMIN_ROLE_CONSTRAINT% 특성

관리자 역할을 만드는 경우 역할 구성원 자격에 대한 규칙을 하나 이상 지정하십시오. 구성원 자격 규칙을 충족하는 사용자에게 역할이 부여됩니다. 예를 들어 "사용자 매니저" 역할에 대한 구성원 자격 규칙이 "title=User Manager"인 경우 직함이 "사용자 매니저"인 사용자에게 "사용자 매니저" 역할이 부여됩니다.

참고: 규칙에 대한 자세한 내용은 *관리 안내서*를 참조하십시오.

%ADMIN_ROLE_CONSTRAINT%를 사용하면 관리자의 관리자 역할을 저장하는 프로필 특성을 지정할 수 있습니다.

%ADMIN_ROLE_CONSTRAINT% 특성을 사용하는 방법

%ADMIN_ROLE_CONSTRAINT%를 모든 관리자 역할에 대한 제약 조건으로 사용하려면 다음 태스크를 수행하십시오.

- 여러 역할을 수용하도록 %ADMIN_ROLE_CONSTRAINT% Well-Known 특성을 다중 값 프로필 특성과 연결합니다.

- 사용자 콘솔에서 관리자 역할을 구성하는 경우 다음 제약 조건에 대해 아래 사항을 확인하십시오.

  관리자 역할이 *role name* 과 같음

  role name

  다음 예제와 같이 제약 조건을 제공하고 있는 역할의 이름을 정의합니다.

  관리자 역할이 사용자 매니저와 같음

참고: 관리자 역할은 %ADMIN_ROLE_CONSTRAINT% 특성의 기본 표시 이름입니다.

Well-Known 특성 구성

Well-Known 특성을 구성하려면 다음 절차를 수행하십시오.

다음 단계를 수행하십시오.

1. 디렉터리 구성 파일에서 다음 기호를 검색합니다.

   ##

2. ##으로 시작하는 값을 적절한 LDAP 특성으로 바꿉니다.
3. 필수 값을 모두 바꿀 때까지 1 단계와 2 단계를 반복합니다.
4. 필요에 따라 선택적 Well-Known 특성을 물리적 특성에 매핑합니다.
5. 디렉터리 구성 파일을 저장합니다.

사용자 디렉터리 구조 설명

CA Identity Manager 는 Well-Known 특성 %ORG_MEMBERSHIP%를 사용하여 사용자 디렉터리 구조를 결정합니다.

사용자 디렉터리 구조를 설명하는 절차는 디렉터리 구조 유형에 따라 다릅니다.

계층적 디렉터리 구조를 설명하는 방법

계층적 디렉터리 구조에 대해서는 디렉터리 구성 파일이 이미 구성되어 있습니다. 따라서 %ORG_MEMBERSHIP% 특성 설명을 수정하지 않아도 됩니다.

비계층적 사용자 디렉터리 구조를 설명하는 방법

다음 단계를 수행하십시오.

1. directory.xml 파일의 User Object 섹션에서 %ORG_MEMBERSHIP% 특성 설명을 찾습니다.
2. physicalname 매개 변수에서 %ORG_MEMBERSHIP%를 사용자가 속한 조직을 저장하는 특성의 이름으로 바꿉니다.

비계층적 디렉터리 구조를 설명하는 방법

다음 단계를 수행하십시오.

1. directory.xml 파일의 User Object 섹션에서 %ORG_MEMBERSHIP% 특성 설명을 찾습니다.
2. physicalname 매개 변수에서 %ORG_MEMBERSHIP%를 사용자가 속한 조직을 저장하는 특성의 이름으로 바꿉니다.

3. Group Object 섹션에서 1 단계를 반복합니다.
4. physicalname 매개 변수에서 %ORG_MEMBERSHIP%를 그룹이 속한 조직을 저장하는 특성의 이름으로 바꿉니다.

조직을 지원하지 않는 사용자 디렉터리를 설명하는 방법

조직에 대해 정의된 개체 설명이나 Well-Known 특성이 directory.xml 에 없는지 확인하십시오.

그룹을 구성하는 방법

구성을 위해 다음과 같이 그룹을 나눌 수 있습니다.

- 자체 구독 그룹
- 동적 그룹과 중첩된 그룹

자체 구독 그룹 구성

디렉터리 구성 파일에서 자체 구독 그룹에 대한 지원을 구성하여 자체 서비스 사용자가 그룹에 참가하도록 설정할 수 있습니다.

사용자가 자체 등록하는 경우 CA Identity Manager 는 지정된 조직에서 그룹을 찾은 다음 사용자에게 자체 구독 그룹을 표시합니다.

다음 단계를 수행하십시오.

1. "Self-Subscribing Groups"(자체 구독 그룹) 섹션에서 다음과 같이 SelfSubscribingGroups 요소를 추가합니다.

   <SelfSubscribingGroups type=*search_type* org=*org_dn*>

2. 다음 매개 변수의 값을 추가합니다.

type

다음과 같이 CA Identity Manager 가 자체 구독 그룹을 검색하는 위치를 나타냅니다.

- NONE - CA Identity Manager 가 그룹을 검색하지 않습니다. 사용자가 그룹을 구독하지 않게 하려면 "NONE"을 지정하십시오.
- ALL - CA Identity Manager 가 루트에서 그룹 검색을 시작합니다. 사용자가 계층적 디렉터리 전체에서 그룹을 구독할 수 있는 경우 "ALL"을 지정하십시오.
- INDICATEDORG - CA Identity Manager 가 사용자의 조직과 해당 하위 조직에서 자체 구독 그룹을 검색합니다. 예를 들어 사용자 프로필이 Marketing 조직에 있는 경우 CA Identity Manager 는 Marketing 조직 및 모든 하위 조직에서 자체 구독 그룹을 검색합니다.
- SPECIFICORG - CA Identity Manager 가 특정 조직에서 검색을 수행합니다. org 매개 변수에서 특정 조직의 DN(고유 이름)을 제공합니다.

org

CA Identity Manager 가 자체 구독 그룹을 검색하는 조직의 고유 식별자를 지정합니다.

참고: type=SPECIFICORG 인 경우 org 매개 변수를 지정해야 합니다.

CA Identity Manager 디렉터리에서 자체 구독 그룹에 대한 지원이 구성된 경우 CA Identity Manager 관리자는 사용자 콘솔에서 자체 구독 그룹을 지정할 수 있습니다.

참고: 그룹 관리에 대한 자세한 내용은 *관리 안내서*를 참조하십시오.

동적 그룹과 중첩된 그룹 구성

LDAP 사용자 저장소를 관리하고 있는 경우 디렉터리 구성 파일에서 다음 그룹 유형에 대한 지원을 구성할 수 있습니다.

동적 그룹

동적으로 사용자 콘솔에서 LDAP 필터 쿼리를 지정하여 그룹 구성원 자격을 정의할 수 있습니다. 동적 그룹을 사용하는 경우에는 관리자가 개별적으로 그룹 구성원을 검색 및 추가하지 않아도 됩니다.

중첩된 그룹

그룹을 다른 그룹의 구성원으로 추가할 수 있습니다.

디렉터리 구성 파일을 사용하여 동적 그룹과 중첩된 그룹이 사용되도록 설정할 수 있습니다.

다음 단계를 수행하십시오.

1. 필요에 따라 다음 Well-Known 특성 (페이지 112)을 그룹 관리 개체의 물리적 특성에 매핑합니다.
   - %DYNAMIC_GROUP_MEMBERSHIP%
   - %NESTED_GROUP_MEMBERSHIP%

   참고: 선택하는 물리적 특성은 다중 값을 지원해야 합니다.
2. "Directory Groups Behavior"(디렉터리 그룹 동작) 섹션에서 다음 GroupTypes 요소를 추가합니다.

   ```
   <GroupTypes type=group>
   ```

   참고: GroupTypes 는 대/소문자를 구분합니다.

3. 다음 매개 변수의 값을 입력합니다.

group

동적 그룹과 중첩된 그룹에 대한 지원이 사용되도록 설정합니다. 유효한 값은 다음과 같습니다.

- NONE - CA Identity Manager 가 동적 그룹과 중첩된 그룹을 지원하지 않습니다.
- ALL - CA Identity Manager 가 동적 그룹과 중첩된 그룹을 지원합니다.
- DYNAMIC - CA Identity Manager 가 동적 그룹만 지원합니다.
- NESTED - CA Identity Manager 가 중첩된 그룹만 지원합니다.

CA Identity Manager 디렉터리에서 동적 그룹과 중첩된 그룹에 대한 지원이 구성된 후에는 CA Identity Manager 관리자가 사용자 콘솔에서 동적 그룹과 중첩된 그룹을 지정할 수 있습니다.

참고: Well-Known 매개 변수 %NESTED_GROUP_MEMBERSHIP%를 *설정하지 않고* 그룹 유형을 NESTED 또는 ALL 로 설정했다고 가정하십시오. 이 경우 CA Identity Manager 는 Well-Known 매개 변수 %GROUP_MEMBERSHIP%에 중첩된 그룹과 사용자를 모두 저장합니다. 그룹 구성원 자격 처리가 약간 느려질 수 있습니다.

그룹의 관리자 역할을 하는 그룹에 대한 지원 추가

LDAP 사용자 저장소를 관리하고 있는 경우 그룹이 다른 그룹의 관리자 역할을 하도록 설정할 수 있습니다. 그룹을 관리자로 할당하면 해당 그룹의 관리자만 지정된 그룹의 관리자입니다. 지정하는 관리자 그룹의 구성원에게는 그룹을 관리할 권한이 없습니다.

다음 단계를 수행하십시오.

1. Well-Known 특성 %GROUP_ADMIN_GROUP%를 관리자 역할을 하는 그룹 목록을 저장하는 물리적 특성에 매핑합니다.

   참고: 선택하는 물리적 특성은 다중 값을 지원해야 합니다.

   그룹 Well-Known 특성 (페이지 112)은 %GROUP_ADMIN_GROUP% 특성에 대한 추가 정보를 제공합니다.

   참고: Well-Known 특성 %GROUP_ADMIN_GROUP%를 설정하지 않고 관리자 그룹 유형을 ALL 로 설정하는 경우 CA Identity Manager 는 관리자 그룹을 %GROUP_ADMIN% 특성에 저장합니다.

2. Directory AdminGroups Behavior 섹션에서 다음과 같이 AdminGroupTypes 요소를 구성합니다.

   <AdminGroupTypes type="ALL">

   기본 AdminGroupTypes 는 NONE 입니다.

   참고: "AdminGroupTypes"는 대/소문자를 구분합니다.

CA Identity Manager 디렉터리에서 관리자 역할을 하는 그룹에 대한 지원이 구성된 후에는 CA Identity Manager 관리자가 사용자 콘솔에서 그룹을 다른 그룹의 관리자로 지정할 수 있습니다.

유효성 검사 규칙

유효성 검사 규칙은 사용자가 태스크 화면 필드에 입력하는 데이터에 대한 요구 사항을 적용합니다. 요구 사항은 데이터 유형이나 형식을 적용할 수 있습니다. 따라서 태스크 화면에 있는 다른 데이터의 컨텍스트에서 데이터가 유효한지 확인하십시오.

유효성 검사 규칙은 프로필 특성과 연결됩니다. CA Identity Manager 는 태스크를 처리하기 전에 프로필 특성에 대해 입력된 데이터가 연결된 유효성 검사 규칙을 모두 충족하는지 확인합니다.

디렉터리 구성 파일에서 유효성 검사 규칙을 정의하고 프로필 특성과 연결할 수 있습니다.

추가 CA Identity Manager 디렉터리 속성

다음 추가 속성을 구성할 수 있습니다.

- 검색 결과의 정렬 순서
- 새 사용자가 아직 없는지 확인하기 위해 개체 클래스에서 검색
- 마스터 LDAP 디렉터리에서 슬레이브 LDAP 디렉터리로의 데이터 복제가 완료되기 전에 시간 만료를 방지하기 위해 CA Identity Manager 가 대기하는 시간

정렬 순서 구성

사용자, 그룹, 조직 같은 각 관리 개체에 대해 정렬 특성을 지정할 수 있습니다. CA Identity Manager 는 이 특성을 사용하여 CA Identity Manager API 로 만드는 사용자 지정 비즈니스 로직에서 검색 결과를 정렬합니다.

참고: 정렬 특성은 사용자 콘솔의 검색 결과 표시 방식에 영향을 주지 않습니다.

예를 들어 사용자 개체에 대해 cn 특성을 지정하면 CA Identity Manager 가 cn 특성을 기반으로 사용자 검색 결과를 사전순으로 정렬합니다.

다음 단계를 수행하십시오.

1. 정렬 순서가 적용되는 관리 개체에 대한 섹션의 마지막 IMSManagedObjectAttr 요소 뒤에 다음 문을 추가합니다.

```
<PropertyDict name="SORT_ORDER">
    <Property name="ATTR">your_sort_attribute
    </Property>
</PropertyDict>
```

2. *your_sort_attribute* 를 CA Identity Manager 가 검색 결과를 정렬하는 특성으로 바꿉니다.

참고: 물리적 특성을 하나만 지정하십시오. Well-Known 특성을 지정하지 마십시오.

예를 들어 cn 특성의 값을 기반으로 사용자 검색 결과를 정렬해야 한다고 가정하십시오. 이 경우 디렉터리 구성 파일의 User Object 섹션에 있는 마지막 IMSManagedObjectAttr 요소 뒤에 다음 요소를 추가하십시오.

```
<!-- ******************** User Object ******************** -->
   <ImsManagedObject name="User" description="My Users"
      objectclass="top,person,organizationalperson,user"
      objecttype="USER">
   .
   .
   .
        <ImsManagedObjectAttr physicalname="departmentnumber"
                displayname="Department" description="Department"
                valuetype="String" required="true"
                multivalued="false" maxlength="0" />
        <PropertyDict name="SORT_ORDER">
                <Property name="ATTR">cn</Property>
        </PropertyDict>
  </ImsManagedObject>
```

개체 클래스에서 검색

CA Identity Manager 는 사용자를 만들 때 기존 사용자가 있는지 확인하기 위해 사용자 저장소를 검색합니다. 이 검색은 개체 클래스가 디렉터리 구성 파일(directory.xml)의 사용자 개체 정의에 지정되어 있는 사용자로 제한됩니다. 이러한 개체 클래스에서 기존 사용자를 찾을 수 없는 경우 CA Identity Manager 는 사용자를 만들려고 합니다.

고유 식별자(사용자 ID)는 같지만 개체 클래스는 다른 사용자가 있는 경우에는 LDAP 서버가 사용자를 만들지 못합니다. 오류가 LDAP 서버에서 보고되지만 CA Identity Manager 가 오류를 인식하지 못합니다. CA Identity Manager 가 사용자를 성공적으로 만드는 것처럼 나타납니다.

SEARCH_ACROSS_CLASSES 속성을 구성하여 이 문제를 방지할 수 있습니다. 그러면 기존 사용자가 있는지 확인할 때 CA Identity Manager 가 모든 개체 클래스 정의에서 사용자를 검색합니다.

참고: 이 속성은 사용자 만들기 같은 태스크를 수행할 때의 중복 사용자 검색에만 영향을 줍니다. 다른 모든 검색의 경우 개체 클래스 제약 조건이 적용됩니다.

다음 단계를 수행하십시오.

1. 디렉터리 구성 파일(directory.xml)에서 사용자 개체를 설명하는 ImsManagedObject 요소를 찾습니다.
2. 다음 PropertyDict 요소를 추가합니다.

```
<PropertyDict name="SEARCH_ACROSS_CLASSES" description="allowing checking an
attribute across classes ">
<Property name="ENABLE">true</Property>
</PropertyDict>
```

참고: 다음 예제와 같이 PropertyDict 요소는 ImsManagedObject 요소의 마지막 요소여야 합니다.

```
<ImsManagedObject name="User" description="My Users"
objectclass="top,person,organizationalperson,inetorgperson,customClass"
objecttype="USER">
<ImsManagedObjectAttr physicalname="departmentnumber" displayname="Department"
description="Department" valuetype="String" required="true"
multivalued="false" maxlength="0" />
.
.
.
<PropertyDict name="SEARCH_ACROSS_CLASSES" description="allow checking an
attribute across classes ">
<Property name="ENABLE">true</Property>
</PropertyDict>
```

복제 대기 시간 지정

마스터 LDAP 디렉터리와 슬레이브 LDAP 디렉터리 간의 복제가 포함된 배포에서 슬레이브 디렉터리와 통신하도록 SiteMinder 정책 서버를 구성할 수 있습니다. 이 구성에서 정책 서버는 LDAP 디렉터리에 데이터를 쓰는 오퍼레이션 중에 마스터 디렉터리를 가리키는 조회를 자동으로 검색합니다. 데이터는 마스터 LDAP 디렉터리에 저장되고 사용 중인 네트워크 리소스의 복제 체계에 따라 슬레이브 LDAP 디렉터리에 복제됩니다.

이 구성의 경우 CA Identity Manager 에서 개체를 만들면 해당 개체가 마스터 디렉터리에 만들어지고 슬레이브 디렉터리에도 복제됩니다. 복제 프로세스 중에 지연이 발생하여 CA Identity Manager 에서 만들기 동작이 실패할 수 있습니다.

이 문제를 방지하기 위해 REPLICATION_WAIT_TIME 속성에서 "시간 만료" 전에 CA Identity Manager 가 대기하는 시간(초)을 지정할 수 있습니다.

다음 단계를 수행하십시오.

1. 디렉터리 구성 파일(directory.xml)에서 사용자 개체를 설명하는 ImsManagedObject 요소를 찾습니다.
2. 다음 PropertyDict 요소를 추가합니다.

```
<PropertyDict name="REPLICATION_WAIT_TIME" description="time delay in seconds
for LDAP provider to allow replication to propagate from master to slave">
<Property name=REPLICATION_WAIT_TIME"><time in seconds></Property>
</PropertyDict>
```

참고: 다음 예제와 같이 PropertyDict 요소는 ImsManagedObject 요소의 마지막 요소여야 합니다.

```
<ImsManagedObject name="User" description="My Users"
objectclass="top,person,organizationalperson,inetorgperson,customClass"
objecttype="USER">
<ImsManagedObjectAttr physicalname="departmentnumber" displayname="Department"
description="Department" valuetype="String" required="true"
multivalued="false" maxlength="0" />
.
.
.
<PropertyDict name="REPLICATION_WAIT_TIME" description="time delay in seconds
for LDAP provider to allow replication to propagate from master to slave">
<Property name=REPLICATION_WAIT_TIME">800</Property>
</PropertyDict>
```

복제 대기 시간을 정의하지 않은 경우 기본값 0 이 사용됩니다.

LDAP 연결 설정 지정

성능을 개선하기 위해 디렉터리 구성 파일(directory.xml)에서 다음 매개 변수를 지정할 수 있습니다.

Connection Timeout(연결 시간 만료)

검색을 종료하기 전에 CA Identity Manager 가 디렉터리를 검색하는 최대 시간(밀리초)을 지정합니다.

이 속성은 다음과 같이 디렉터리 구성 파일에서 지정됩니다.

com.sun.jndi.ldap.connect.timeout

Connection Pool Max Size(연결 풀 최대 크기)

CA Identity Manager 가 LDAP 디렉터리에 대해 설정할 수 있는 최대 연결 수를 지정합니다.

이 속성은 다음과 같이 디렉터리 구성 파일에서 지정됩니다.

com.sun.jndi.ldap.connect.pool.maxsize

Connection Pool Default Size(연결 풀 기본 크기)

CA Identity Manager 와 LDAP 디렉터리 간의 기본 연결 수를 지정합니다.

이 속성은 다음과 같이 디렉터리 구성 파일에서 지정됩니다.

com.sun.jndi.ldap.connect.pool.prefsize

다음 단계를 수행하십시오.

1. 디렉터리 구성 파일(directory.xml)에서 사용자 개체를 설명하는 ImsManagedObject 요소를 찾습니다.
2. 다음 PropertyDict 요소를 추가합니다.

```
<PropertyDict name="LDAP_CONNECTION_SETTINGS" description="LDAP Connection
Settings">
    <Property name="com.sun.jndi.ldap.connect.timeout">5000</Property>
    <Property name="com.sun.jndi.ldap.connect.pool.maxsize">200</Property>
    <Property name="com.sun.jndi.ldap.connect.pool.prefsize">10</Property>
</PropertyDict>
```

3. directory.xml 파일을 저장합니다.

   이 파일을 사용하여 CA Identity Manager 디렉터리를 만들 때 CA Identity Manager 가 해당 설정을 구성합니다.

디렉터리 검색 성능을 개선하는 방법

사용자, 조직 및 그룹에 대한 디렉터리 검색 성능을 개선하려면 다음 사항을 수행하십시오.

- 관리자가 검색 쿼리에서 지정할 수 있는 특성을 색인화합니다.

  참고: Oracle Internet Directory 의 경우 검색 쿼리에 있는 특성이 색인화되지 않았으면 검색이 실패할 수 있습니다.

- 페이지 크기 및 최대 행 설정을 구성 (페이지 131)하여 CA Identity Manager 의 대규모 검색 처리 방식을 결정합니다.

- 사용자 디렉터리를 조정합니다. 사용 중인 사용자 디렉터리 설명서를 참조하십시오.

대규모 검색 성능을 개선하는 방법

CA Identity Manager 가 대규모 사용자 저장소를 관리하는 경우 많은 결과가 반환되는 검색으로 인해 시스템의 메모리가 부족해질 수 있습니다. 메모리 문제를 방지하기 위해 대규모 검색에 대한 한도를 정의할 수 있습니다.

다음 2 가지 설정에 따라 CA Identity Manager 가 대규모 검색을 처리하는 방식이 결정됩니다.

- Maximum number of rows(최대 행 수)

  사용자 디렉터리를 검색할 때 CA Identity Manager 가 반환할 수 있는 최대 결과 수를 지정합니다. 결과 수가 이 제한을 초과하면 오류가 표시됩니다.

- Page size(페이지 크기)

  단일 검색에서 반환될 수 있는 개체 수를 지정합니다. 개체 수가 페이지 크기를 초과하는 경우 다중 검색이 수행됩니다.

  페이지 크기를 지정하는 경우 다음 사항에 주의하십시오.

  - "Search Page Size"(검색 페이지 크기) 옵션을 사용하려면 CA Identity Manager 가 관리하는 사용자 저장소가 페이지 단위 처리를 지원해야 합니다. 일부 사용자 저장소 유형의 경우 페이지 단위 처리를 지원하려면 추가 구성이 필요합니다. 자세한 내용은 다음 항목을 참조하십시오.

    Sun Java System Directory Server 페이지 단위 처리 지원 구성 (페이지 134)

    Active Directory 페이지 단위 처리 지원 구성

  - 사용자 저장소가 페이지 단위 처리를 지원하지 않지만 maxrows 값이 지정된 경우 CA Identity Manager 는 maxrows 값만 사용하여 검색 크기를 제어합니다.

다음 위치에서 최대 행 제한 및 페이지 크기를 구성할 수 있습니다.

- 사용자 저장소

  대부분의 사용자 저장소 및 데이터베이스에서 검색 제한을 구성할 수 있습니다.

  참고: 자세한 내용은 현재 사용하고 있는 사용자 저장소 또는 데이터베이스 설명서를 참조하십시오.

- CA Identity Manager 디렉터리

  디렉터리 구성 파일(directory.xml)에서 CA Identity Manager 디렉터리를 만드는 데 사용하는 DirectorySearch 요소를 구성 (페이지 79)할 수 있습니다.

  기본적으로 기존 디렉터리에는 최대 행 및 페이지 크기의 값에 제한이 없지만, 새 디렉터리의 경우에는 최대 행 값에는 제한이 없고 페이지 크기는 2000 으로 설정됩니다.

- 관리 개체 정의

  전체 디렉터리 대신 단일 개체 유형에 적용되는 최대 행 제한과 페이지 크기를 설정하려면 CA Identity Manager 디렉터리를 만드는 데 사용하는 directory.xml 파일에서 *관리 개체 정의를* 구성 (페이지 82)하십시오.

  특정 관리 개체 유형에 대한 제한을 설정하면 비즈니스 요구 사항을 기준으로 조정할 수 있습니다. 예를 들어 대부분의 회사에는 그룹보다 사용자가 많습니다. 이런 경우 사용자 개체 검색에 대한 제한만 설정하면 됩니다.

- 태스크 검색 화면

  사용자 콘솔에서 검색 및 목록 화면에 표시되는 검색 결과 수를 제어할 수 있습니다. 결과 수가 태스크에 대해 정의된 페이지당 결과 수를 초과하면 추가 결과 페이지에 대한 링크가 사용자에게 표시됩니다.

  이 설정은 검색에서 반환되는 결과의 수에는 영향을 미치지 않습니다.

  참고: 검색 및 목록 화면에서 페이지 크기를 설정하는 방법에 대한 자세한 내용은 *관리 안내서*를 참조하십시오.

최대 행 제한 및 페이지 크기가 여러 위치에서 정의된 경우 가장 구체적인 설정이 적용됩니다. 예를 들어 관리 개체 설정이 디렉터리 수준 설정보다 우선합니다.

Sun Java System Directory Server 페이지 단위 처리 지원 구성

Sun Java System Directory Server 는 특정 순서나 특정 하위 집합으로 검색 결과를 전달하는 방법인 VLV(가상 목록 뷰)를 지원합니다. 이 방법은 CA Identity Manager 가 예상하는 단순 페이지 단위 처리 결과와 다릅니다.

VLV 를 사용하려면 사용 권한을 설정하고 색인을 만듭니다. CA Identity Manager 에는 페이지 단위 처리 지원을 구성해야 하는 다음 파일이 포함됩니다.

- vlvcntrl.ldif
- vlvindex.ldif
- runvlvindex.cmd, runvlvindex.sh

이러한 파일은 관리 도구의 samples\NeteAuto 에 NeteAuto 샘플의 일부로 포함됩니다.

관리 도구는 다음 기본 위치에 설치됩니다.

Windows: C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager

UNIX: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/

다음 단계를 수행하십시오.

1. 다음과 같이 아래 매개 변수를 CA Identity Manager 디렉터리의 directory.xml 파일에 있는 DirectorySearch 요소 (페이지 79)에 추가합니다.

   ```
   minsortrules="1"
   ```

   참고: 기존 CA Identity Manager 디렉터리를 수정하고 있는 경우 CA Identity Manager 디렉터리에 대한 설정을 업데이트하는 방법 (페이지 251)을 참조하십시오.

2. 다음과 같이 vlvcntrl.ldif 파일에 대한 사용 권한을 설정합니다.

   ```
   ldapmodify -D "cn=Directory Manager" -w password -p port -f
   vlvcntrl.ldif
   ```

3. 다음과 같이 VLV 검색 및 색인 정의를 가져옵니다.

   ```
   ldapmodify -D "cn=Directory Manager" -w password -p port -f
   vlvindex.ldif
   ```

4. 다음과 같이 디렉터리를 중지합니다.

   ```
   stop-slapd
   ```

5. runvlvindex 를 사용하여 색인을 작성합니다.

6. 다음과 같이 디렉터리를 시작합니다.

   ```
   start-slapd
   ```

Active Directory 페이지 단위 처리 지원 구성

Active Directory 에서 페이지 단위 처리 지원을 구성하려면 다음 상위 수준의 단계를 완료하십시오.

- 가상 목록 뷰에 대한 지원을 구성합니다 (페이지 136).
- Active Directory MaxPageSize 를 구성합니다 (페이지 137). (**CA Identity Manager r12.5 SP7 이전에 만들어진 디렉터리만 해당**)

VLV(가상 목록 뷰)에 대한 지원 구성

Active Directory 는 특정 순서나 특정 하위 집합으로 검색 결과를 전달하는 방법인 VLV(가상 목록 뷰)를 지원합니다. 이 방법은 CA Identity Manager 가 예상하는 단순 페이지 단위 처리 결과와 다릅니다.

VLV 를 사용하려면 사용 권한을 설정하고 색인을 만듭니다. CA Identity Manager 에는 페이지 단위 처리 지원을 구성해야 하는 다음 파일이 포함됩니다.

- vlvcntrl.ldif
- vlvindex.ldif
- runvlvindex.cmd, runvlvindex.sh

이러한 파일은 관리 도구의 samples\NeteAuto 에 NeteAuto 샘플의 일부로 포함됩니다.

관리 도구는 다음 기본 위치에 설치됩니다.

Windows: C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager

UNIX: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/

다음 단계를 수행하십시오.

1. 다음과 같이 아래 매개 변수를 CA Identity Manager 디렉터리의 directory.xml 파일에 있는 DirectorySearch 요소 (페이지 79)에 추가합니다.

   ```
   minsortrules="1"
   ```

   참고: 기존 CA Identity Manager 디렉터리를 수정하고 있는 경우 CA Identity Manager 디렉터리에 대한 설정을 업데이트하는 방법 (페이지 251)을 참조하십시오.

2. 다음과 같이 vlvcntrl.ldif 파일에 대한 사용 권한을 설정합니다.

   ```
   ldapmodify -D "cn=Directory Manager" -w password -p port -f
   vlvcntrl.ldif
   ```

3. 다음과 같이 VLV 검색 및 색인 정의를 가져옵니다.

   ```
   ldapmodify -D "cn=Directory Manager" -w password -p port -f
   vlvindex.ldif
   ```

4. 다음과 같이 디렉터리를 중지합니다.

   ```
   stop-slapd
   ```

5. runvlvindex 를 사용하여 색인을 작성합니다.

6. 다음과 같이 디렉터리를 시작합니다.

   ```
   start-slapd
   ```

Active Directory MaxPageSize 구성

Active Directory 는 1000 을 기본 MaxPageSize 로 사용합니다. directory.xml 의 maxpagesize 특성 값이 1000 보다 크거나 같다고 가정하십시오. 이 경우 검색 결과 수가 directory.xml 의 maxrows 값을 초과해도 CA Identity Manager 가 경고를 표시하지 못합니다. 따라서 검색을 수행하는 관리자는 일부 검색 결과가 누락되었음을 알 수 없습니다.

이 문제를 방지하려면 디렉터리와 각 관리 개체의 maxpagesize 특성 값이 Active Directory MaxPageSize 보다 작은지 확인하십시오.

CA Identity Manager 12.5 SP7 이상 버전에 설치된 directory.xml 파일 템플릿을 사용하여 CA Identity Manager 디렉터리를 만든다고 가정합니다. 이 경우 페이지 단위 처리 지원을 위한 추가 단계를 수행하지 않아도 됩니다. directory.xml 의 maxpagesize 특성은 기본적으로 설정되어 있습니다.

기존 CA Identity Manager 디렉터리에 페이지 단위 처리 지원을 추가하는 경우 directory.xml 의 maxpagesize 특성은 1000 보다 작아야 합니다.

또한 Active Directory MaxPageSize 가 1000 인 경우에는 CA Identity Manager 디렉터리 및 모든 관리 개체에 적절하게 maxpagesize 특성을 설정해야 합니다.

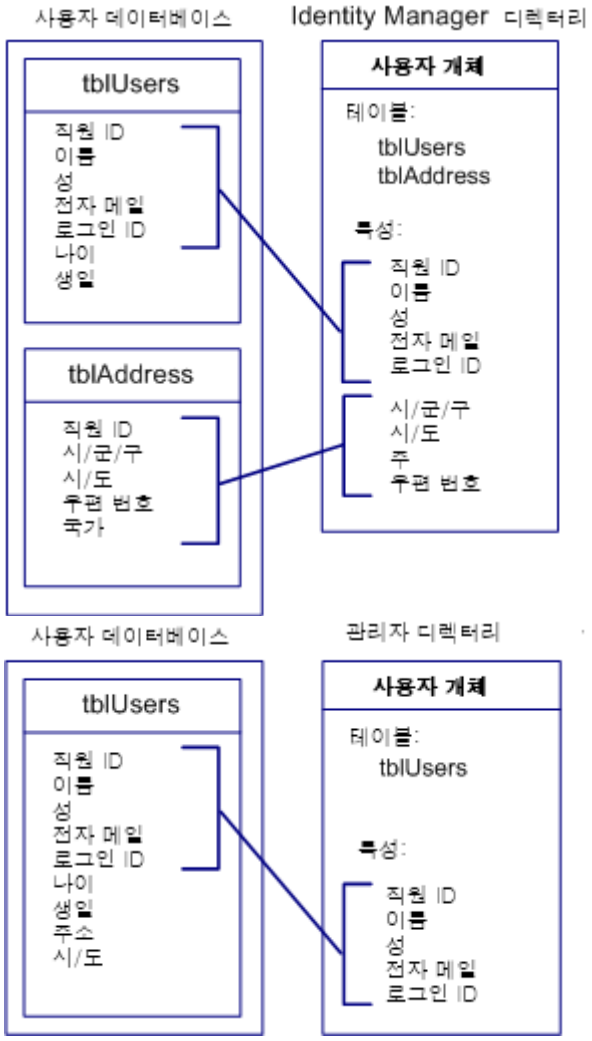
제 4 장: 관계형 데이터베이스 관리

이 섹션은 다음 항목을 포함하고 있습니다.

CA Identity Manager 디렉터리

*CA Identity Manager 디렉터리*는 사용자, 그룹 및 조직(선택 사항)과 같은 개체가 사용자 저장소에 저장되는 방식 및 CA Identity Manager 에 표시되는 방식을 설명합니다. CA Identity Manager 디렉터리는 하나 이상의 CA Identity Manager 환경과 연결됩니다.

다음 그림에는 CA Identity Manager 디렉터리와 사용자 저장소의 관계가 나와 있습니다.



참고: 데이터베이스의 일부 사용자 특성은 CA Identity Manager 디렉터리에 포함되어 있지 않습니다. 따라서 CA Identity Manager 는 해당 특성을 관리하지 않습니다.

관계형 데이터베이스를 위해 CA Identity Manager 를 구성할 때 중요한 참고 사항

관계형 데이터베이스를 관리하도록 CA Identity Manager 를 구성하기 전에 데이터베이스가 다음 요구 사항을 충족하는지 확인하십시오.

- 데이터베이스는 JDBC 드라이버 또는 ODBC(Open Database Connectivity) 드라이버를 통해 액세스할 수 있어야 합니다(CA Identity Manager 가 SiteMinder 와 통합된 경우). 드라이버가 외부 조인을 지원해야 합니다. 관리 개체를 나타내는 데 3 개 이상의 테이블이 사용되는 경우 드라이버는 중첩된 외부 조인도 지원해야 합니다.

  참고: 드라이버가 외부 조인을 지원하지 않는 경우 CA Identity Manager 는 데이터베이스를 쿼리할 때 내부 조인을 사용합니다. 이로 인해 예상치 못한 쿼리 결과가 발생할 수 있습니다.

- 사용자, 그룹 또는 조직(지원되는 경우)과 같이 CA Identity Manager 가 관리하는 각 개체를 고유하게 식별합니다. 예를 들어 사용자의 고유 식별자는 로그인 ID 일 수 있습니다.

  참고: 고유 식별자는 하나의 열에 저장되어야 합니다.

- CA Identity Manager 에는 개별 테이블의 여러 행이나 단일 셀에 구분된 목록으로 저장될 수 있는 다중 값 특성이 일부 필요합니다. 예를 들어 다음과 같은 tblGroupMembers 테이블에는 특정 그룹의 구성원이 저장됩니다.

ID	구성원
Research	dmason
Research	rsavory
Marketing	dmason
Marketing	awelch

ID 열에는 그룹의 고유 식별자가 들어 있고 구성원 열에는 그룹 구성원의 고유 식별자가 들어 있습니다. 예를 들어 dmason 및 rsavory 는 Research 그룹의 구성원입니다. 새 구성원을 해당 그룹에 추가하면 다른 행이 tblGroupMembers 에 추가됩니다.

- 사용자 환경에 조직이 포함된 경우 다음 태스크를 수행하십시오.
  - 데이터베이스에 대해 CA Identity Manager 와 함께 포함된 SQL 스크립트를 편집 및 실행하여 조직 지원을 구성 (페이지 200)합니다.
  - CA Identity Manager 에는 루트라는 최상위 조직이 있어야 합니다. 기타 모든 조직은 루트 조직과 관련이 있습니다.

    조직 요구 사항에 대한 자세한 내용은 조직 관리 (페이지 199)를 참조하십시오.

WebSphere 용 Oracle 데이터 원본 만들기

다음 단계를 수행하십시오.

1. WebSphere Administrative Console 에서 JDBC 드라이버를 구성할 때 만든 JDBC 공급자로 이동합니다.
2. 다음 속성을 사용하여 데이터 원본을 만들고 "Apply"(적용)를 클릭합니다.

   Name(이름): 사용자 저장소 데이터 원본

   JNDI Name(JNDI 이름): userstore

   URL: jdbc:oracle:thin:@*db_systemname*:1521:*oracle_sid*

3. 사용자 저장소 데이터 원본에 대한 새 J2C 인증 데이터 항목을 구성합니다.

   a. 다음 속성을 입력합니다.

      Alias(별칭): 사용자 저장소

      User ID(사용자 ID): *username*

      password(암호): *password*

      여기서 *username* 및 *password* 는 데이터베이스를 만들 때 계정에 대해 지정한 사용자 이름 및 암호입니다.

   b. "OK"(확인)를 클릭한 다음 화면 위쪽에 있는 탐색 링크를 사용하여 만들려는 데이터 원본으로 돌아갑니다.

4. 다음 필드의 목록 상자에서 앞서 만든 사용자 저장소 J2C 인증 데이터 항목을 선택합니다.

   - Component-managed Authentication Alias(구성 요소 관리 인증 별칭)
   - Container-managed Authentication Alias(컨테이너 관리 인증 별칭)

5. "OK"(확인)를 클릭한 다음 구성을 저장합니다.

   참고: 데이터 원본이 올바르게 구성되었는지 확인하려면 데이터 원본의 구성 화면에서 "Test Connection"(연결 테스트)을 클릭하십시오. 연결 테스트가 실패하는 경우 WebSphere 를 다시 시작하고 연결을 다시 테스트합니다.

CA Identity Manager 디렉터리를 만드는 방법

다음 단계를 수행하십시오.

1. SiteMinder 를 사용하고 있는 경우 CA Identity Manager 디렉터리를 만들기 전에 먼저 정책 저장소 스키마를 적용합니다.

   참고: 특정 정책 저장소 스키마 및 이를 적용하는 방법에 대한 자세한 내용은 *설치 안내서*를 참조하십시오.

2. SiteMinder 를 사용하고 있는 경우 SiteMinder 에 사용할 ODBC 데이터 원본을 만듭니다 (페이지 153).

3. CA Identity Manager 가 관리하는 사용자 데이터베이스에 대한 데이터 원본을 만듭니다.

4. 디렉터리 구성 파일(directory.xml)을 수정하여 CA Identity Manager 에 데이터베이스를 설명합니다. 자세한 내용은 디렉터리 구성 파일에서 데이터베이스를 설명하는 방법을 참조하십시오.

5. 관리 콘솔에서 디렉터리 구성 파일을 가져오고 디렉터리를 만듭니다.

JDBC 데이터 원본을 만드는 방법

CA Identity Manager 에서 사용자 저장소에 연결하려면 CA Identity Manager 가 설치되어 있는 응용 프로그램 서버에 JDBC 데이터 원본이 있어야 합니다. 데이터 원본을 만드는 지침은 응용 프로그램 서버마다 각기 다릅니다.

JBoss Application Server 용 JDBC 데이터 원본 만들기

다음 단계를 수행하십시오.

1. 다음 파일의 사본을 만듭니다.

   jboss_home\server\default\deploy\objectstore-ds.xml

   jboss home

   CA Identity Manager 가 설치되어 있는 JBoss Application Server 가 설치된 위치입니다.

   새 파일은 동일한 위치에 있어야 합니다.

2. 파일의 이름을 userstore-ds.xml 로 바꿉니다.

3. userstore-ds.xml 을 다음과 같이 편집합니다.

   a. <jndi-name> 요소를 찾습니다.

   b. <jndi-name> 요소 값을 다음과 같이 jdbc/objectstore 에서 userstore 로 변경합니다.

      <jndi-name>userstore</jndi-name>

   c. <connection-url> 요소에서 다음과 같이 DatabaseName 매개 변수를 사용자 저장소로 사용되는 데이터베이스의 이름으로 변경합니다.

      <connection-url>

      jdbc:sqlserver://*ipaddress:port*;selectMethod=cursor;DatabaseName=*userstore_name*

      </connection-url>

      ipaddress

      사용자 저장소가 설치되어 있는 시스템의 IP 주소를 지정합니다.

      port

      데이터베이스의 포트 번호를 지정합니다.

      userstore_name

      사용자 저장소로 사용되는 데이터베이스의 이름을 지정합니다.

4. FIPS 지원에 필요한 JBoss 보안 영역을 만들려면 다음 단계를 수행하십시오.
   a. 보안 도메인의 이름을 <security-domain>imuserstoredb</security-domain>으로 바꿉니다.
   b. 파일을 저장합니다.
   c. 나머지 단계는 생략합니다. 대신, JDBC 데이터 원본에 JBoss 보안 영역 사용 (페이지 147)에 나와 있는 단계를 완료하십시오.
5. 다음과 같이 userstore-ds.xml 의 내용을 추가로 변경합니다.
   a. 사용자 저장소에 대한 읽기 및 쓰기 권한이 있는 계정에 대한 <user-name> 요소 값을 사용자 이름으로 변경합니다.
   b. <user-name> 요소에 지정된 계정에 대한 <password> 요소 값을 암호로 변경합니다.

   참고: 사용자 이름 및 암호는 이 파일에서 일반 텍스트로 표시됩니다. 따라서 userstore-ds.xml 을 편집하는 대신 JBoss 보안 영역을 만들 수 있습니다.
6. 파일을 저장합니다.

JDBC 데이터 원본에 JBoss 보안 영역 사용

JBoss Application Server 에서 JDBC 데이터 원본을 만들어야 합니다. 데이터 원본은 사용자 이름 및 암호를 사용하도록 구성할 수도 있고, 보안 영역을 사용하도록 구성할 수도 있습니다.

중요! FIPS 를 사용하고 있는 경우에는 JBoss 보안 영역 옵션을 사용해야 합니다.

다음 단계를 수행하십시오.

1. JBoss Application Server 용 JDBC 데이터 원본 만들기 (페이지 145)에 나와 있는 단계를 완료하십시오.

   4 단계에서 설명한 대로 userstore-ds.xml 에서 사용자 이름 및 암호를 지정하지 마십시오.

2. *jboss_home*\server\default\conf 에서 login-cfg.xml 을 엽니다.

3. 파일에서 다음 항목을 찾습니다.

```
<application-policy name="imobjectstoredb">
  <authentication>
    <login-module
code="com.netegrity.jboss.datasource.PasswordEncryptedLogin" flag="required">
      <module-option name="userName">fwadmin</module-option>
      <module-option
name="password">{PBES}:gSex2/BhDGzEKWvFmzca4w==</module-option>
      <module-option
name="managedConnectionFactoryName">jboss.jca:name=jdbc/objectstore,service=N
oTxCM</module-option>
    </login-module>
  </authentication>
</application-policy>
```

4. 전체 항목을 복사하고 이를 login-cfg.xml 파일의 <policy> 및 </policy> 태그 안에 붙여넣습니다.

5. 파일에 붙여넣은 항목에서 다음과 같이 변경합니다.

   a. 다음과 같이 이름 특성 값을 imobjectstoredb 에서 imuserstoredb 로 변경합니다.

```
<application-policy name="imuserstoredb">
```

b. 사용자 저장소 인증에 사용되는 사용자의 이름을 다음과 같이 지정합니다.

```
<module-option name="userName">user_store_user</module-option>
```

c. 이전 단계에서 다음과 같이 사용자의 암호를 지정합니다.

```
<module-option name="password">user_store_user_password</module-option>
```

참고: 사용자 저장소 암호를 암호화하려면 CA Identity Manager 와 함께 설치된 암호 도구(pwdtools)를 사용하십시오.

d. <module-option name="managedConnectionFactoryName"> 요소에서 다음과 같이 적절한 jdbc.jca:name 을 지정합니다.

```
<module-option name="managedConnectionFactoryName">
   jboss.jca:name=userstore,service=NoTxCM
</module-option>
```

6. 파일을 저장합니다.
7. 응용 프로그램 서버를 다시 시작합니다.

WebLogic 용 JDBC 데이터 원본 만들기

WebLogic Administration Console 에서 데이터 원본을 만들어야 합니다.

참고: Weblogic 연결 풀에 대한 자세한 정보는 Oracle WebLogic 11 Documentation (Oracle WebLogic 11 설명서)을 참조하십시오.

다음 단계를 수행하십시오.

1. WebLogic Administration Console 에서 다음 매개 변수를 사용하여 JDBC 데이터 원본을 만듭니다.

   Name(이름): 사용자 저장소 데이터 원본

   JNDI Name(JNDI 이름): userstore

2. 다음 정보를 사용하여 데이터 원본에 대한 연결 풀을 만듭니다.

- SQL Server 2005 데이터베이스의 경우 다음과 같은 값을 사용합니다.

  URL: jdbc:sqlserver://*db_systemName*:1433

  Driver Class Name(드라이버 클래스 이름):
  com.microsoft.sqlserver.jdbc.SQLServerDriver

  Properties(속성): user=*username*

  databaseName=*user store name*

  selectMethod=cursor

  Password(암호): *password*

- Oracle 데이터베이스의 경우 다음과 같은 값을 사용합니다.

  URL: jdbc:oracle:thin:@*tp_db_systemname*:1521:*oracle_SID*

  Driver Class Name(드라이버 클래스 이름):
  oracle.jdbc.driver.OracleDriver

  Properties(속성): user=*username*

  Password(암호): *password*

3. 구성을 마친 경우 풀의 대상을 서버 인스턴스 *wl_server_name* 으로 설정합니다.

   풀을 배포하고 나면 콘솔을 통해 오류가 발생했는지 확인하십시오.

   참고: 존재하지 않는 풀로 인해 데이터 원본을 만들 수 없다는 내용의 오류가 표시될 수 있습니다. 이 오류를 해결하려면 WebLogic 을 다시 시작하십시오.

WebSphere 데이터 원본

다음 단원에서는 WebSphere 응용 프로그램 서버용 SQL 또는 Oracle 데이터 원본을 만드는 방법에 대해 설명합니다.

WebSphere 용 SQL Server 데이터 원본 만들기

다음 단계를 수행하십시오.

1. WebSphere Administrative Console 에서 JDBC 드라이버를 구성할 때 만든 JDBC 공급자로 이동합니다.
2. "Additional Properties"(추가 속성) 섹션에서 "Data Sources"(데이터 원본)를 선택합니다.
3. 다음 속성을 사용하여 데이터 원본을 만들고 "Apply"(적용)를 클릭합니다.

   Name(이름): 사용자 저장소 데이터 원본

   JNDI Name(JNDI 이름): userstore

   databaseName(데이터베이스 이름): *userstore_name*

   serverName(서버 이름): *db_systemname*
4. selectMethod 속성을 다음과 같이 구성합니다.
   a. "Additional Properties"(추가 속성) 섹션에서 "Custom Properties"(사용자 지정 속성)를 선택합니다.
   b. selectMethod 사용자 지정 속성을 클릭합니다.
   c. "Value"(값) 필드에 다음 텍스트를 입력합니다.

      cursor
   d. "OK"(확인)를 클릭한 다음 화면 위쪽에 있는 탐색 링크를 사용하여 만들려는 데이터 원본으로 돌아갑니다.

5. 사용자 저장소 데이터 원본에 대한 새 J2C 인증 데이터 항목을 구성합니다.

   a. "Related Items"(관련 항목) 섹션에서 J2EE Connector Architecture(J2C) 인증 데이터 항목을 선택합니다.

   b. "New"(새로 만들기)를 클릭합니다.

   c. 다음 속성을 입력합니다.

      Alias(별칭): 사용자 저장소

      User ID(사용자 ID): *username*

      password(암호): *password*

      여기서 *username* 및 *password* 는 데이터베이스를 만들 때 계정에 대해 지정한 사용자 이름 및 암호입니다.

   d. "OK"(확인)를 클릭한 다음 화면 위쪽에 있는 탐색 링크를 사용하여 만들려는 데이터 원본으로 돌아갑니다.

6. "Component-managed Authentication Alias"(구성 요소 관리 인증 별칭) 필드의 목록 상자에서 앞서 만든 사용자 저장소 J2C 인증 데이터 항목을 선택합니다.

7. "OK"(확인)를 클릭한 다음 구성을 저장합니다.

   참고: 데이터 원본이 올바르게 구성되었는지 확인하려면 데이터 원본의 구성 화면에서 "Test Connection"(연결 테스트)을 클릭하십시오. 연결 테스트가 실패하는 경우 WebSphere 를 다시 시작하고 연결을 다시 테스트합니다.

WebSphere 용 Oracle 데이터 원본 만들기

다음 단계를 수행하십시오.

1. WebSphere Administrative Console 에서 JDBC 드라이버를 구성할 때 만든 JDBC 공급자로 이동합니다.

2. 다음 속성을 사용하여 데이터 원본을 만들고 "Apply"(적용)를 클릭합니다.

   Name(이름): 사용자 저장소 데이터 원본

   JNDI Name(JNDI 이름): userstore

   URL: jdbc:oracle:thin:@*db_systemname*:1521:*oracle_sid*

3. 사용자 저장소 데이터 원본에 대한 새 J2C 인증 데이터 항목을 구성합니다.

   a. 다음 속성을 입력합니다.

      Alias(별칭): 사용자 저장소

      User ID(사용자 ID): *username*

      password(암호): *password*

      여기서 *username* 및 *password* 는 데이터베이스를 만들 때 계정에 대해 지정한 사용자 이름 및 암호입니다.

   b. "OK"(확인)를 클릭한 다음 화면 위쪽에 있는 탐색 링크를 사용하여 만들려는 데이터 원본으로 돌아갑니다.

4. 다음 필드의 목록 상자에서 앞서 만든 사용자 저장소 J2C 인증 데이터 항목을 선택합니다.

   - Component-managed Authentication Alias(구성 요소 관리 인증 별칭)
   - Container-managed Authentication Alias(컨테이너 관리 인증 별칭)

5. "OK"(확인)를 클릭한 다음 구성을 저장합니다.

   참고: 데이터 원본이 올바르게 구성되었는지 확인하려면 데이터 원본의 구성 화면에서 "Test Connection"(연결 테스트)을 클릭하십시오. 연결 테스트가 실패하는 경우 WebSphere 를 다시 시작하고 연결을 다시 테스트합니다.

SiteMinder 에 사용할 ODBC 데이터 원본을 만드는 방법

CA Identity Manager 가 SiteMinder 와 통합된 경우 SiteMinder 시스템에서 데이터베이스를 가리키는 ODBC 데이터 원본을 정의해야 합니다. 나중에 사용할 수 있도록 데이터 원본의 이름을 기록해 둡니다. 다음과 같이 진행하십시오.

- **Windows:** 시스템 DN 으로 ODBC 데이터 원본을 구성합니다. 자세한 지침은 Windows 운영 체제 설명서를 참조하십시오.
- **UNIX:** *policy_server_installation*/db 에 있는 system_odbc.ini 파일에서 ODBC 데이터 원본에 대한 매개 변수를 지정하는 항목을 추가합니다.

디렉터리 구성 파일에서 데이터베이스를 설명하는 방법

데이터베이스를 관리하려면 CA Identity Manager 가 데이터베이스 구조 및 콘텐츠를 알아야 합니다. CA Identity Manager 에 데이터베이스를 설명하려면 디렉터리 구성 파일(directory.xml)을 만드십시오.

디렉터리 구성 파일에는 다음과 같은 섹션이 하나 이상 포함됩니다.

CA Identity Manager Directory Information(CA Identity Manager 디렉터리 정보)

CA Identity Manager 에서 사용하는 CA Identity Manager 디렉터리에 대한 정보를 포함합니다.

Attribute Validation(특성 유효성 검사)

CA Identity Manager 디렉터리에 적용되는 유효성 검사 규칙을 정의합니다.

Provider Information(공급자 정보)

CA Identity Manager 에서 관리하는 사용자 저장소에 대해 설명합니다.

Directory Search Information(디렉터리 검색 정보)

CA Identity Manager 가 사용자 저장소를 검색하는 방법을 지정할 수 있습니다.

User Object(사용자 개체) (페이지 157)

사용자가 사용자 저장소에 저장되는 방식과 CA Identity Manager 에서 표시되는 방식을 설명합니다.

Group Object(그룹 개체) (페이지 157)

그룹이 사용자 저장소에 저장되는 방식과 CA Identity Manager 에서 표시되는 방식을 설명합니다.

Organization Object(조직 개체) (페이지 157)

조직에 저장되는 방식 및 CA Identity Manager 에 표시되는 방식을 설명합니다.

Self-Subscribing Groups(자체 구독 그룹)

자체 서비스 사용자가 참가할 수 있는 그룹에 대한 지원을 구성합니다.

CA Identity Manager 용 관리 도구를 설치한 디렉터리에는 관계형 데이터베이스에 대한 다음과 같은 디렉터리 구성 파일 템플릿이 포함되어 있습니다.

admin_tools\directoryTemplates\RelationalDatabase\directory.xml

admin_tools

다음 예와 같이 CA Identity Manager 관리 도구가 설치된 위치를 정의합니다.

- **Windows:** C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools
- **UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

참고: directoryTemplates\RelationalDatabase 의 디렉터리 구성 파일 템플릿은 조직을 지원하는 환경에 대해 구성되어 있습니다. 조직이 포함되지 않은 환경에 대한 디렉터리 구성 파일을 확인하려면 *admin_tools*\samples\Nete AutoRDB\NoOrganization 에 있는 NeteAuto 샘플용 directory.xml 파일을 살펴보면 됩니다.

구성 템플릿을 덮어쓰지 않도록 새 디렉터리에 복사하거나 다른 이름으로 저장하십시오. 그런 다음 데이터베이스 구조를 반영하도록 템플릿을 수정합니다.

디렉터리 구성 파일에는 다음과 같은 2 가지 중요한 규칙이 있습니다.

- ## - 필수 값을 나타냅니다.

  필요한 정보를 모두 제공하려면 이중 파운드 기호(##)를 모두 찾아 적절한 값으로 바꾸십시오. 예를 들어 ##PASSWORD_HINT 는 암호를 잊어버린 경우 임시 암호를 받기 위해 사용자가 대답할 질문을 저장하기 위한 특성을 제공해야 함을 나타냅니다.

- @ - CA Identity Manager 가 채우는 값을 나타냅니다. 디렉터리 구성 파일에서 이러한 값을 수정하지 마십시오. 디렉터리 구성 파일을 가져올 때 값을 제공하라는 메시지가 표시됩니다.

디렉터리 구성 파일을 수정하기 전에 알아 두어야 할 정보는 다음과 같습니다.

- 사용자, 그룹 및 조직 개체에 대한 테이블 이름(구조에 조직이 포함된 경우)
- 사용자, 그룹 및 조직 프로필의 특성 목록(구조에 조직이 포함된 경우)

디렉터리 구성 파일 수정

디렉터리 구성 파일을 수정하려면 다음 절차를 수행하십시오.

다음 단계를 수행하십시오.

1. 데이터베이스에 대한 연결을 구성합니다.
2. 검색을 종료하기 전까지 CA Identity Manager 에서 디렉터리를 검색하는 시간을 지정합니다.
3. CA Identity Manager 가 관리하는 사용자 및 그룹 관리 개체 (페이지 157)를 정의합니다.
4. Well-Known 특성을 수정합니다.

   Well-Known 특성은 CA Identity Manager 에서 암호 특성과 같은 특수한 특성을 식별합니다.
5. 자체 구독 그룹에 대한 지원을 구성합니다.
6. 사용자 환경에 조직이 포함된 경우 조직 지원을 구성합니다.

추가 정보:

관리 개체 설명 (페이지 157)
조직 관리 (페이지 199)
자체 구독 그룹을 구성하는 방법 (페이지 197)
관계형 데이터베이스의 Well-Known 특성 (페이지 190)

관리 개체 설명

CA Identity Manager 에서는 사용자 저장소의 항목에 따라 다음과 같은 유형의 개체를 관리할 수 있습니다.

- 사용자 - 엔터프라이즈의 사용자를 나타냅니다.
- 그룹 - 공통점이 있는 사용자들의 연결을 나타냅니다.
- (선택 사항) 조직 - 비즈니스 단위를 나타냅니다. 조직에는 사용자, 그룹 및 기타 조직이 포함될 수 있습니다.

  참고: 조직 관리 (페이지 199)에서는 조직 구성에 대한 정보를 제공합니다.

개체 설명에는 다음과 같은 정보가 포함되어 있습니다.

- 개체에 대한 정보 (페이지 157)(예: 개체가 저장된 테이블)
- 항목에 대한 정보를 저장하는 특성 (페이지 163). 예를 들어 호출기 특성은 호출기 번호를 저장합니다.

중요! CA Identity Manager 환경은 한 가지 유형의 사용자, 그룹 및 조직 개체만 지원합니다.

관리 개체를 설명하는 방법

관리 개체는 디렉터리 구성 파일의 User Object(사용자 개체), Group Object(그룹 개체) 및 Organization Object(조직 개체) 섹션(데이터베이스에 조직이 포함된 경우)에서 개체 정보를 지정하는 방식으로 설명됩니다.

이러한 각 섹션에는 다음 코드와 같이 ImsManagedObject 요소가 들어 있습니다.

```
<ImsManagedObject name="User" description="My Users">
```

ImsManagedObject 요소에는 다음과 같은 요소가 포함될 수 있습니다.

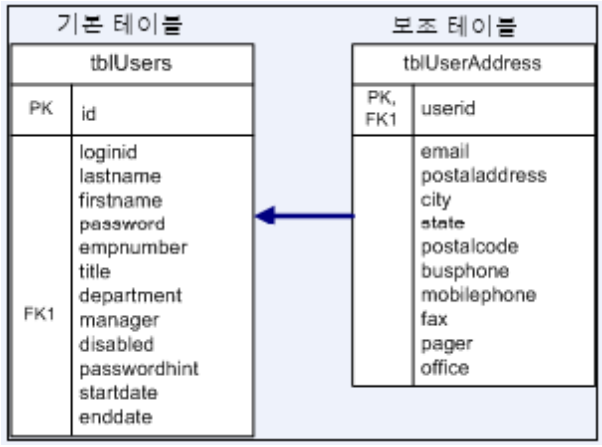
- Table(필수)
- UniqueIdentifier(필수)
- ImsManagedObjectAttr(필수)
- RootOrg(조직 개체만 해당)

데이터베이스 테이블

디렉터리 구성 파일의 Table 요소를 사용하여 관리 개체에 대한 정보를 저장하는 테이블을 정의할 수 있습니다.

각 관리 개체에는 개체에 대한 고유 식별자가 들어 있는 하나의 기본 테이블이 있어야 합니다. 추가 정보는 보조 테이블에 저장될 수 있습니다.

다음 그림에는 기본 및 보조 테이블에 사용자 정보를 저장하는 데이터베이스가 나와 있습니다.



개체 정보가 여러 테이블에 저장된 경우 각 테이블에 대해 Table 요소를 하나씩 만듭니다. Table 요소에서 보조 테이블에 대한 Reference 요소를 사용하여 기본 테이블과의 관계를 정의합니다.

예를 들어 사용자에 대한 기본 정보가 tblUsers 에 저장되고 주소 정보는 tblUserAddress 에 저장된 경우 User 관리 개체에 대한 테이블 정의는 다음 항목과 유사합니다.

```
<Table name="tblUsers" primary="true" />
<Table name="tblUserAddress">
  <Reference childcol="userid" primarycol="id" />
</Table name>
```

Table 요소

Table 요소의 매개 변수는 다음과 같습니다.

name

(필수)

개체의 관리 프로필에 특성 중 일부 또는 모두를 저장하는 테이블의 이름을 지정합니다.

primary

테이블이 관리 개체의 기본 테이블인지 여부를 나타냅니다. 기본 테이블에는 다음과 같이 개체의 고유 식별자가 포함됩니다.

- True - 테이블이 기본 테이블입니다.
- False - 테이블이 보조 테이블입니다(기본값).

기본 매개 변수를 지정하지 않는 경우 CA Identity Manager 는 테이블을 보조 테이블로 간주합니다.

참고: 테이블 하나만 기본 테이블이 될 수 있습니다.

filter

관리 개체에 적용되는 테이블 항목의 하위 집합을 식별합니다.

선택적 필터 매개 변수는 다음 예와 유사할 수 있습니다.

```
filter="ORG=2"
```

참고: 필터는 CA Identity Manager 가 생성하는 쿼리에만 적용됩니다. 생성된 쿼리를 사용자 지정 쿼리로 덮어쓰는 경우 사용자 지정 쿼리에 필터를 지정합니다.

fullouterjoin

외부 조인이 완전 외부 조인인지 여부를 나타냅니다.

- True - 외부 조인이 완전 외부 조인입니다. 이 경우 조인에 포함된 양쪽 테이블 모두에서 조건이 발견되어야 올바른 행이 반환됩니다.
- False - 외부 조인이 기본 테이블을 기준으로 왼쪽 우선 조인입니다. 이 경우 쿼리에서 한 테이블의 행만 조건을 충족해야 합니다(기본값).

참고: 달리 지정하지 않는 한 매개 변수는 선택 사항입니다.

Table 매개 변수는 기본 테이블을 보조 테이블과 연결하는 Reference 요소를 하나 이상 포함할 수 있습니다.

Reference 요소

Reference 요소의 매개 변수는 다음과 같습니다.

childcol

기본 테이블의 열에 매핑되는 보조 테이블(해당 Table 요소에 지정됨)의 열을 나타냅니다.

primarycol

보조 테이블의 열에 매핑되는 기본 테이블의 열을 나타냅니다.

참고: 달리 지정하지 않는 한 매개 변수는 선택 사항입니다.

개체 정보 지정

개체 정보는 다양한 매개 변수의 값을 제공하는 방법으로 지정됩니다.

다음 단계를 수행하십시오.

1. User Object(사용자 개체), Group Object(그룹 개체) 또는 Organization Object(조직 개체) 섹션에서 ImsManagedObject 요소를 찾습니다.
2. 다음 매개 변수의 값을 제공합니다.

   name

   (필수)

   관리 개체의 고유 이름을 제공합니다.

   description

   관리 개체에 대한 설명을 제공합니다.

   objecttype

   (필수)

   관리 개체의 유형을 지정합니다. 유효한 값은 다음과 같습니다.

   - USER
   - GROUP
   - ORGANIZATION

   ImsManagedObject 요소는 다음 코드와 유사해야 합니다.

   ```
   <ImsManagedObject name="User" description="My  Users" objecttype="USER">
   ```

3. 데이터베이스 테이블 (페이지 158)에 설명된 대로 테이블 정보를 제공합니다.
4. 개체의 고유 식별자 (페이지 162)를 포함하는 열을 지정합니다.
5. 개체 프로필을 구성하는 특성 (페이지 163)을 설명합니다.
6. 조직 개체를 구성하는 경우 조직 관리 (페이지 199)로 이동합니다.

관리 개체의 고유 식별자를 지정하는 방법

CA Identity Manager 가 관리하는 개체에는 각각 고유 식별자가 있어야 합니다. 고유 식별자는 관리 개체의 기본 테이블에서 하나의 열에 저장되어야 합니다. 기본 테이블은 데이터베이스 테이블 (페이지 158)에서 설명합니다.

UniqueIdentifier 및 UniqueIdentifierAttr 요소를 사용하여 다음과 같이 고유 식별자를 정의합니다.

```
<UniqueIdentifier>
  <UniqueIdentifierAttr name="tablename.columnname" />
</UniqueIdentifier>
```

UniqueIdentifierAttr 요소에는 name 매개 변수가 필요합니다. name 매개 변수의 값은 고유 식별자가 저장되는 특성입니다. 이 값은 물리적 특성 또는 Well-Known 특성 (페이지 107)일 수 있습니다.

물리적 특성을 지정하는 경우 다음 사항에 주의하십시오.

- 지정하는 특성은 데이터베이스에 있어야 하고 특성 설명을 수정하는 방법 (페이지 163)에 설명된 대로 디렉터리 구성 파일에서 정의합니다. 세션 중에 고유 식별자가 변경되지 않게 하려면 특성 설명에서 읽기 전용 또는 한 번 쓰기 권한을 지정해야 합니다.
- 다음 구문을 사용하여 물리적 특성을 지정하십시오.

  tablename.columnname

  tablename

  특성이 있는 테이블의 이름을 정의합니다. 지정하는 테이블은 기본 테이블이어야 합니다.

  columnname

  특성을 저장하는 열의 이름을 정의합니다.

- 데이터베이스에서 고유 식별자를 생성하면 특성에 대한 사용자 지정 오퍼레이션 (페이지 178)을 지정합니다. 예를 들어 데이터베이스에서 마지막으로 생성된 식별자를 가져오는 오퍼레이션을 지정해야 할 수 있습니다.

특성 설명을 수정하는 방법

특성은 전화 번호 또는 주소와 같은 사용자, 그룹 또는 조직 엔터티에 대한 정보를 저장합니다. 엔터티 특성에 따라 프로필이 결정됩니다.

디렉터리 구성 파일에서 특성은 ImsManagedObjectAttr 요소에서 설명됩니다. 디렉터리 구성 파일의 User Object(사용자 개체), Group Object(그룹 개체) 및 Organization Object(조직 개체) 섹션에서 다음을 수행하십시오.

- 데이터베이스 특성을 설명하도록 기본 특성 설명을 수정합니다.
- 기존 설명을 복사하고 필요에 따라 값을 수정하여 새 특성 설명을 지정합니다.

사용자, 그룹 및 조직 프로필에 있는 각 특성의 경우 하나의 ImsManagedObjectAttr 요소만 있습니다. 예를 들어 ImsManagedObjectAttr 요소는 사용자 ID 를 설명할 수 있습니다.

ImsManagedObjectAttr 요소는 다음 코드와 유사합니다.

```
<ImsManagedObjectAttr
 physicalname="tblUsers.id"
 displayname="User Internal ID"
 description="User Internal ID"
 valuetype="Number"
 required="false"
 multivalued="false"
 maxlength="0"
 hidden="false"
 permission="READONLY">
```

참고: Oracle 데이터베이스를 사용하는 경우 관리 개체 특성을 구성할 때는 다음 사항에 주의하십시오.

- Oracle 데이터베이스는 기본적으로 대소문자를 구분합니다. 디렉터리 구성 파일에서 특성 및 테이블 이름의 대소문자는 Oracle 의 특성 대소문자와 일치해야 합니다.

  문자열 데이터 형식이 잘리지 않게 하려면 최대 길이를 지정하십시오. 문자열의 길이를 제한하려면 사용자가 최대 길이를 초과하여 문자열을 입력할 때 오류를 표시하도록 유효성 검사 규칙을 만들면 됩니다.

ImsManagedObjectAttr 매개 변수는 다음과 같습니다.

참고: 달리 지정하지 않는 한 매개 변수는 선택 사항입니다.

physicalname

(필수)

특성의 물리적 이름을 지정하되, 다음과 같은 정보 중 하나를 포함해야 합니다.

- 값이 저장된 이름과 위치

  형식: *tablename.columnname*

  예를 들어 특성이 tblUsers 테이블의 id 열에 저장된 경우 이 특성의 물리적 이름은 다음과 같습니다.

  tblUsers.id

  Table 요소 (페이지 158)에서 특성을 포함하는 각 테이블을 정의해야 합니다.

- Well-Known 특성

  Well-Known 특성은 계산된 값을 나타낼 수 있습니다. 예를 들어 사용자 지정 오퍼레이션 (페이지 178)을 사용하여 계산된 특성을 나타낼 때 Well-Known 특성을 사용할 수 있습니다

displayname

(필수)

특성의 고유 이름을 지정합니다.

사용자 콘솔에서 태스크 화면에 추가할 수 있는 특성 목록에 표시 이름이 나타납니다.

참고: 디렉터리 구성 파일(directory.xml)에서 특성의 표시 이름을 수정하지 마십시오. 태스크 화면에서 특성의 이름을 변경하려면 태스크 화면 정의에서 특성에 대한 레이블을 지정하면 됩니다. 자세한 내용은 *관리 안내서*를 참조하십시오.

description

특성에 대한 설명을 제공합니다.

valuetype

특성의 데이터 형식을 지정합니다. 유효한 값은 다음과 같습니다.

String(문자열)

값이 임의의 문자열일 수 있습니다.

이것이 기본값입니다.

Integer(정수)

값이 정수여야 합니다.

참고: 정수는 소수를 지원하지 않습니다.

Number(숫자)

값이 정수여야 합니다. 숫자 옵션은 소수를 지원합니다.

Date(날짜)

값이 다음 패턴을 사용하여 유효한 날짜로 구문 분석되어야 합니다.

yyyy/MM/dd

ISODate(ISO 날짜)

값이 yyyy-MM-dd 패턴을 사용하여 유효한 날짜로 구문 분석되어야 합니다.

UnicenterDate(Unicenter 날짜)

값이 YYYYYYYDDD 패턴을 사용하여 유효한 날짜로 구문 분석되어야 합니다.

YYYYYYY 는 세 개의 0 으로 시작하는 연도를 나타내는 7 자리 숫자 표시입니다. 예: 0002008

DDD 는 필요한 경우 0 으로 시작하는 날짜를 나타내는 3 자리 숫자 표시입니다. 유효한 값은 001 에서 366 사이입니다.

특성의 valuetype 이 올바르지 않으면 CA Identity Manager 쿼리가 실패할 수 있습니다.

특성이 데이터베이스에 올바로 저장되었는지 확인하려면 이 특성을 유효성 검사 규칙과 연결하십시오.

required

다음과 같이 특성 값을 지정해야 하는지 여부를 나타냅니다.

- True - 필수
- False - 선택 사항(기본값)

multi-valued

다음과 같이 특성이 다중 값을 가질 수 있는지 여부를 나타냅니다.

- True - 특성이 다중 값을 가질 수 있습니다.
- False - 특성이 하나의 값만 가질 수 있습니다(기본값).

예를 들어 사용자 프로필의 그룹 구성원 자격 특성은 사용자가 속한 여러 그룹을 저장할 수 있도록 다중 값을 갖습니다.

복수 행 테이블이 아니라 구분된 목록으로 다중 값 특성을 저장하려면 delimiter 매개 변수에서 구분 기호 문자를 정의해야 합니다.

열에서 지원되는 가능한 값의 수와 각 값의 길이가 충분하지 확인하십시오.

중요! 사용자 개체 정의의 그룹 구성원 자격 특성은 다중 값을 가져야 합니다.

wellknown

Well-Known 특성의 이름을 제공합니다.

Well-Known 특성은 CA Identity Manager 에서 특정한 의미를 가집니다.

형식: %*ATTRIBUTENAME*%

참고: 사용자 지정 오퍼레이션이 특성과 관련된 경우 Well-Known 특성 (페이지 107)을 지정해야 합니다.

maxlength

열의 최대 크기를 결정합니다.

permission

태스크 화면에서 다음과 같이 특성 값을 수정할 수 있는지 여부를 나타냅니다.

READONLY

값이 표시되기는 하지만 수정할 수는 없습니다.

WRITEONCE

개체가 만들어진 후에는 값을 수정할 수 없습니다. 예를 들어 사용자가 만들어진 후에는 사용자 ID 를 변경할 수 없습니다.

READWRITE

값을 수정할 수 있습니다(기본값).

hidden

다음과 같이 특성이 CA Identity Manager 태스크 화면에 표시되는지 여부를 나타냅니다.

- true - 사용자에게 특성이 표시되지 않습니다.
- false - 사용자에게 특성이 표시됩니다(기본값).

논리적 특성은 숨겨진 특성을 사용합니다.

참고: 논리적 특성에 대한 자세한 내용은 *Programming Guide for Java*(Java 프로그래밍 안내서)를 참조하십시오.

system

CA Identity Manager 전용 특성을 지정합니다. 다음과 같이 사용자 콘솔에서 사용자가 특성을 수정할 수 없습니다.

- true - 사용자가 특성을 수정할 수 없습니다. 사용자 콘솔에 특성이 표시되지 않습니다.
- false - 사용자가 이 특성을 수정할 수 있으며 사용자 콘솔에서 태스크 화면에 추가할 수 있습니다(기본값).

validationruleset

유효성 검사 규칙 세트를 특성과 연결합니다.

지정하는 유효성 검사 규칙 세트가 디렉터리 구성 파일의 ValidationRuleSet 요소에 정의되어 있는지 확인하십시오.

delimiter

하나의 열에 다중 값이 저장된 경우 값을 구분하는 문자를 정의합니다.

중요! delimiter 매개 변수를 적용하려면 multivalued 매개 변수가 true 로 설정되었는지 확인하십시오.

참고: 암호 또는 급여와 같이 중요한 정보가 표시되지 않게 하려면 사용자 콘솔에서 DataClassification (페이지 98) 매개 변수를 지정하십시오.

중요한 특성 관리

CA Identity Manager 는 중요한 특성을 관리하기 위한 다음과 같은 방법을 제공합니다.

- 특성에 대한 데이터 분류

  데이터 분류를 사용하여 특성에 대한 표시 및 암호화 속성을 디렉터리 구성 파일(directory.xml)에 지정할 수 있습니다.

  다음과 같이 중요한 특성을 관리하는 데이터 분류를 정의할 수 있습니다.

  - CA Identity Manager 태스크 화면에서 일련의 별표로 특성의 값을 표시합니다.

    예를 들어 암호를 일반 텍스트로 표시하지 않고 별표로 표시할 수 있습니다.

  - "제출한 태스크 보기" 화면에서 특성 값을 숨깁니다.

    이 옵션을 사용하면 특성을 관리자로부터 숨길 수 있습니다. 예를 들어 CA Identity Manager 에서 태스크 상태는 보지만 월급 관련 세부 정보는 볼 필요가 없는 관리자에게 월급 등의 월급 관련 세부 정보가 표시되지 않도록 숨깁니다.

  - 기존 개체의 사본을 만들 때 특정 특성을 무시합니다.

  - 특성을 암호화합니다.

- 태스크 프로필 화면의 필드 스타일

  directory.xml 파일에서 특성을 수정하지 않으려면 중요한 특성이 나타나는 화면 정의에서 특성에 대한 표시 속성을 설정하십시오.

  필드 스타일을 사용하면 암호 등의 특성을 일반 텍스트 대신 일련의 별표로 표시할 수 있습니다.

  참고: 중요한 특성의 필드 스타일에 대한 자세한 내용을 보려면 사용자 콘솔 도움말에서 필드 스타일을 검색하십시오.

데이터 분류 특성

데이터 분류 요소는 추가 속성을 특성 설명과 연결하는 방법을 제공합니다. 이 요소의 값에 따라 CA Identity Manager 가 해당 특성을 처리하는 방식이 결정됩니다. 이 요소는 다음 매개 변수를 지원합니다.

- sensitive

  이 매개 변수를 설정하면 CA Identity Manager 가 "View Submitted Tasks"(제출한 태스크 보기) 화면에 특성을 일련의 별표(*)로 표시합니다. 이 매개 변수는 특성의 이전 값과 새 값이 "View Submitted Tasks"(제출한 태스크 보기) 화면에 일반 텍스트로 표시되지 않도록 합니다.

  또한 사용자 콘솔에서 기존 사용자에 대한 사본을 만들 경우 이 매개 변수를 설정하면 특성이 새 사용자에게 복사되지 않습니다.

- vst_hide

  "View Submitted Tasks"(제출한 태스크 보기) 탭의 "Event Details"(이벤트 정보) 화면에서 특성을 숨깁니다. 별표로 표시되는 sensitive 특성과 다르게 vst_hidden 특성은 아예 표시되지 않습니다.

  이 매개 변수를 사용하여 월급과 같은 특성의 변경 사항이 "View Submitted Tasks"(제출한 태스크 보기)에 표시되지 않도록 할 수 있습니다.

- ignore_on_copy

  이 매개 변수를 설정하면 관리자가 사용자 콘솔에서 개체 사본을 만들 때 CA Identity Manager 가 특성을 무시합니다. 예를 들어 사용자 개체의 암호 특성에 대해 ignore_on_copy 를 지정했다고 가정합니다. 사용자 프로필을 복사할 때 CA Identity Manager 는 현재 사용자의 암호를 새 사용자 프로필에 적용하지 않습니다.

- AttributeLevelEncrypt

  사용자 저장소에 저장되는 특성 값을 암호화합니다. CA Identity Manager 에서 FIPS 140-2 가 활성화되었을 경우 CA Identity Manager 는 RC2 암호화 또는 FIPS 140-2 암호화를 사용합니다.

  CA Identity Manager 의 FIPS 140-2 지원에 대한 자세한 내용은 *구성 안내서*를 참조하십시오.

  런타임에는 특성이 일반 텍스트로 표시됩니다.

  참고: 특성이 화면에 일반 텍스트로 표시되지 않도록 하기 위해 암호화된 특성에 sensitive 데이터 분류 요소를 추가할 수도 있습니다. 자세한 내용은 특성 수준 암호화를 추가하는 방법 (페이지 101)을 참조하십시오.

- PreviouslyEncrypted

  이 매개 변수를 설정하면 CA Identity Manager 가 사용자 저장소의 개체에 액세스할 때 특성의 암호화된 값을 감지하고 암호 해독합니다.

  이 데이터 분류를 사용하여 이전에 암호화된 값을 암호 해독할 수 있습니다.

  개체를 저장할 때 일반 텍스트 값이 저장소에 저장됩니다.

데이터 분류 특성 구성

다음 단계를 수행하십시오.

1. 디렉터리 구성 파일에서 특성을 찾습니다.
2. 특성 설명 뒤에 다음 특성을 추가합니다.

   <DataClassification name="*parameter*">

   parameter

   다음 매개 변수 중 하나를 나타냅니다.

   sensitive

   vst_hide

   ignore_on_copy

   AttributeLevelEncrypt

   PreviouslyEncrypted

   예를 들어 vst_hide 데이터 분류 특성을 포함하는 특성 설명은 다음 코드와 비슷합니다.

```
<ImsManagedObjectAttr physicalname="salary" displayname="Salary"
description="salary" valuetype="String" required="false" multivalued="false"
maxlength="0">
    <DataClassification name="vst_hide"/>
```

특성 수준 암호화

디렉터리 구성 파일(directory.xml)의 특성에 대해 AttributeLevelEncypt 데이터 분류를 지정하여 사용자 저장소에서 특성을 암호화할 수 있습니다. 특성 수준 암호화가 활성화되면 CA Identity Manager 가 특성의 값을 사용자 저장소에 저장하기 전에 암호화합니다. 특성은 사용자 콘솔에서 일반 텍스트로 표시됩니다.

참고: 특성이 화면에 일반 텍스트로 표시되지 않도록 하기 위해 암호화된 특성에 sensitive 데이터 분류 요소를 추가할 수도 있습니다. 자세한 내용은 특성 수준 암호화를 추가하는 방법 (페이지 101)을 참조하십시오.

FIPS 140-2 지원이 활성화된 경우 RC2 암호화 또는 FIPS 140-2 암호화를 사용하여 특성이 암호화됩니다.

특성 수준 암호화를 구현하려면 먼저 다음 사항에 주의하십시오.

- CA Identity Manager 는 검색에서 암호화된 특성을 찾을 수 없습니다.

  암호화된 특성이 구성원, 관리자, 소유자 정책 또는 ID 정책에 추가되었다고 가정합니다. CA Identity Manager 는 이 특성을 검색할 수 없기 때문에 해당 정책을 제대로 확인하지 못합니다.

  directory.xml 파일에서 특성을 searchable="false"로 설정해 봅니다. 예를 들면 다음과 같습니다.

  ```
  <ImsManagedObjectAttr physicalname="title" description="Title"
  displayname="Title" valuetype="String" maxlength="0" searchable="false">
  <DataClassification name="AttributeLevelEncrypt"/>
  </ImsManagedObjectAttr>
  ```

- CA Identity Manager 에서 공유 사용자 저장소와 프로비저닝 디렉터리를 사용하는 경우 프로비저닝 서버 특성을 암호화하지 마십시오.
- 다음 조건을 만족하는 환경의 사용자 암호에 대해서는 AttributeLevelEncrypt 를 활성화하지 마십시오.
  - CA SiteMinder 통합 포함
  - 관계형 데이터베이스에 사용자 저장

  CA Identity Manager 가 CA SiteMinder 와 통합되는 경우 암호를 암호화하면 새 사용자가 로그인하고 암호를 일반 텍스트로 입력하려고 할 때 문제가 발생합니다.
- CA Identity Manager 이외의 응용 프로그램에서 사용하는 사용자 저장소에 대해 특성 수준 암호화를 활성화하면 다른 응용 프로그램에서 암호화된 특성을 사용할 수 없습니다.

특성 수준 암호화를 추가하는 방법

특성 수준 암호화를 CA Identity Manager 디렉터리에 추가했다고 가정합니다. 그러면 해당 특성과 연결된 개체를 저장할 때 CA Identity Manager 가 자동으로 기존 일반 텍스트 특성 값을 암호화합니다. 예를 들어 암호 특성을 암호화하면 이 특성에서 사용자 프로필을 저장할 때 암호가 암호화됩니다.

참고: 특성 값을 암호화하려면 개체를 저장하는 데 사용할 태스크에 해당 특성이 포함되어야 합니다. 이전 예제의 암호 특성을 암호화하려면 개체를 저장하는 데 사용할 태스크(예: "사용자 수정" 태스크)에 암호 필드가 추가되어야 합니다.

모든 새 개체가 사용자 저장소에서 암호화된 값으로 생성됩니다.

다음 단계를 수행하십시오.

1. 다음 태스크 중 하나를 완료하십시오.
   - CA Identity Manager 디렉터리 만들기
   - 디렉터리 설정을 내보내어 기존 디렉터리 업데이트
2. 다음 데이터 분류 특성을 directory.xml 파일에서 암호화할 특성에 추가합니다.

   AttributeLevelEncrypt

   특성 값을 암호화된 형식으로 사용자 저장소에 보존합니다.

   sensitive(선택 사항)

   특성 값을 CA Identity Manager 화면에서 숨깁니다. 예를 들어 암호는 별표(*)로 표시됩니다.

   예:

```
<ImsManagedObjectAttr physicalname="salary" displayname="Salary"
description="salary" valuetype="String" required="false"
multivalued="false" maxlength="0" searchable="false">
<DataClassification name="AttributeLevelEncrypt"/>
<DataClassification name="sensitive"/>
```

3. CA Identity Manager 디렉터리를 만든 경우 이 디렉터리를 환경과 연결합니다.
4. CA Identity Manager 가 모든 값을 즉시 암호화하도록 하려면 대량 로더를 사용하여 모든 개체를 수정합니다.

   참고: 대량 로더에 대한 자세한 내용은 *관리 안내서*를 참조하십시오.

특성 수준 암호화를 제거하는 방법

암호화된 특성이 CA Identity Manager 디렉터리에 있고 일반 텍스트 형식의 이 특성 값과 함께 저장된 경우 AttributeLevelEncrypt 데이터 분류를 제거할 수 있습니다.

데이터 분류가 제거되면 CA Identity Manager 가 더 이상 새 특성 값을 암호화하지 않습니다. 특성과 연결된 개체를 저장하면 기존 값이 암호 해독됩니다.

참고: 특성 값을 암호 해독하려면 개체를 저장하는 데 사용할 태스크에 해당 특성이 포함되어야 합니다. 예를 들어 기존 사용자의 암호를 해독하려면 암호 필드를 포함하는 태스크(예: "사용자 수정" 태스크)와 함께 사용자 개체를 저장해야 합니다.

CA Identity Manager 가 특성에 대해 사용자 저장소에서 유지되는 암호화된 값을 감지하고 암호 해독하도록 하려면 다른 데이터 분류 PreviouslyEncrypted 를 지정하면 됩니다. 개체를 저장할 때 일반 텍스트 값이 사용자 저장소에 저장됩니다.

참고: PreviouslyEncrypted 데이터 분류를 추가하면 각 개체 로드에서 추가 처리가 늘어납니다. 성능 문제를 방지하려면 PreviouslyEncrypted 데이터 분류를 추가하고 해당 특성과 연결된 각 개체를 로드 및 저장한 후 데이터 분류를 제거하는 것이 좋습니다. 이 방법을 사용하면 모든 저장된 암호화된 값이 저장된 일반 텍스트로 자동으로 변환됩니다.

다음 단계를 수행하십시오.

1. 해당 CA Identity Manager 디렉터리의 디렉터리 설정을 내보냅니다.
2. directory.xml 파일을 열고 암호 해독할 특성에서 데이터 분류 AttributeLevelEncrypt 를 제거합니다.

3. CA Identity Manager 가 이전에 암호화된 값을 제거하도록 하려면 PreviouslyEncrypted 데이터 분류 특성을 추가합니다.

   예:

   ```
   <ImsManagedObjectAttr physicalname="salary" displayname="Salary"
   description="salary" valuetype="String" required="false" multivalued="false"
   maxlength="0" searchable="false">
   <DataClassification name="PreviouslyEncrypted"/>
   ```

4. CA Identity Manager 가 모든 값을 즉시 암호 해독하도록 하려면 대량 로더를 사용하여 모든 개체를 수정합니다.

   참고: 대량 로더에 대한 자세한 내용은 *관리 안내서*를 참조하십시오.

사용자 지정 오퍼레이션

다음 태스크를 수행하려면 특정 관리 개체에 대해 사용자 지정 오퍼레이션을 정의할 수 있습니다.

- 저장 프로시저 사용
- 데이터베이스 구조에 대한 쿼리 최적화
- 데이터베이스에서 생성된 고유 식별자 검색

사용자 지정 오퍼레이션은 특성에만 적용됩니다.

사용자 지정 오퍼레이션을 지정하는 경우 다음 사항을 고려하십시오.

- 사용자 지정 오퍼레이션을 지정하는 사용자는 SQL 에 익숙해야 합니다.
- CA Identity Manager 는 사용자 지정 오퍼레이션의 유효성을 검사하지 않습니다. 런타임까지 구문 오류 및 잘못된 쿼리는 보고되지 않습니다.

- 특성에 대한 사용자 지정 오퍼레이션을 지정하는 경우 CA Identity Manager 태스크의 검색 필터에서 해당 특성을 사용할 수 없습니다.
- 사용자 지정 오퍼레이션은 XML 표준을 따라야 합니다. XML 구문을 사용하여 특수 문자를 나타냅니다. 예를 들어 '로 작은따옴표(')를 지정합니다.

사용자 지정 오퍼레이션을 지정하려면 Operation 요소를 사용하십시오.

Operation 요소

Operation 요소는 사용자 지정 쿼리를 실행할 수 있는 SQL 문을 정의하거나 특성을 생성, 검색, 수정 또는 삭제하기 위한 저장 프로시저를 호출합니다. Operation 요소는 다음 예에 나와 있는 것처럼 IMSManagedObjectAttr 요소의 하위 요소입니다.

```
<ImsManagedObjectAttr physicalname="tblUsers.id" displayname="User Internal ID"
description="User Internal ID" valuetype="Number" required="false"
multivalued="false" maxlength="0" hidden="false" permission="READONLY">
  <Operation name="GetDb" value="select @@identity" />
```

Operation 요소 매개 변수는 다음과 같습니다.

name

오퍼레이션에 대해 미리 정의된 이름을 지정합니다. 유효한 오퍼레이션은 다음과 같습니다.

- Create
- Get
- Set
- Delete
- GetDB

  데이터베이스를 통해서나 저장 프로시저에서 고유 식별자가 생성되는 경우 GetDB 오퍼레이션은 Create 태스크 중에 데이터베이스에서 고유 식별자를 검색합니다.

value

실행할 SQL 문 또는 저장 프로시저를 정의합니다. 유효한 값은 다음과 같습니다.

- INSERT
- SELECT
- UPDATE
- DELETE
- CALL(저장 프로시저 전용)

참고: 달리 지정하지 않는 한 매개 변수는 선택 사항입니다.

Operation 요소는 하나 이상의 Parameter 요소를 포함할 수 있습니다.

Parameter 요소

Parameter 요소는 쿼리에 전달되는 값을 지정합니다. 여러 Parameter 요소가 정의된 경우 값은 목록에 지정된 순서대로 쿼리에 전달됩니다.

Parameter 요소에는 name 매개 변수가 필요합니다. name 매개 변수의 값은 물리적 특성 또는 Well-Known 특성 (페이지 107)일 수 있습니다.

참고: CA Identity Manager 는 Parameter 요소에서 쿼리에 전달된 값을 알아야 합니다. 예를 들어 값은 ImsManagedObjectAttr 특성에 정의된 물리적 이름 또는 Well-Known 특성일 수 있습니다.

물리적 특성을 지정하는 경우 다음 사항에 주의하십시오.

- 다음 구문을 사용하여 물리적 특성을 지정하십시오.

  tablename.columnname

  - *tablename*

    특성이 있는 테이블의 이름을 제공합니다. 지정하는 테이블은 기본 테이블이어야 합니다.

  - *columnname*

    특성을 저장하는 열의 이름을 제공합니다.

- 지정하는 특성은 데이터베이스에 있어야 하고 특성 설명을 수정하는 방법 (페이지 163)에 설명된 대로 디렉터리 구성 파일에서 정의합니다.

예: Business Number 특성에 대한 사용자 지정 오퍼레이션

다음 예에서 Business Number 특성은 저장 프로시저를 호출하여 생성되었으며, 데이터베이스에서 물리적 특성이 아닙니다.

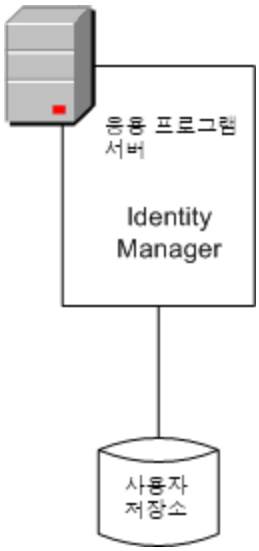
```
<ImsManagedObjectAttr wellknown="%BUSINESS_NUMBER%"     displayname="Business
Number" description="Business Number"     valuetype="String" required="false"
multivalued="false"     maxlength="0">
<Operation name="Get" value="call sp_getbusinessnumber(?)">
    <Parameter name="%USER_ID%"/>
</Operation>
<Operation name="Set" value="call sp_setbusinessnumber(?,?)">
    <Parameter name="%USER_ID%"/>
    <Parameter name="%BUSINESS_NUMBER%"/>
</Operation>
<Operation name="Delete" value="call sp_deletebusinessnumber(?)">
    <Parameter name="%USER_ID%"/>
</Operation>
```

다음에 주의하십시오.

- sp_getbusinessnumber, sp_setbusinessnumber 및 sp_deletebusinessnumber 는 사용자 정의 저장 프로시저입니다.
- Get 오퍼레이션에서 반환되는 값은 %BUSINESS_NUMBER% 특성에 매핑됩니다.
- 물음표(?)는 대체를 나타내며, 이 대체 작업은 쿼리가 실행되기 전 런타임에 수행됩니다. 예를 들어 Get 오퍼레이션에서 %USER_ID% Well-Known 특성은 sp_getbusinessnumber 저장 프로시저로 전달됩니다.

사용자 디렉터리에 대한 연결

다음 그림과 같이 CA Identity Manager 는 사용자 디렉터리에 연결하여 사용자, 그룹 및 조직 정보 같은 정보를 저장합니다.



새 디렉터리나 데이터베이스가 필요하지 않습니다. 하지만 기존 디렉터리나 데이터베이스가 FQDN(정규화된 도메인 이름)을 가진 시스템에 있어야 합니다.

지원되는 디렉터리 및 데이터베이스 유형 목록은 CA Support 사이트의 CA Identity Manager 지원표를 참조하십시오.

관리 콘솔에서 CA Identity Manager 디렉터리를 만들 때 사용자 저장소에 대한 연결을 구성합니다.

CA Identity Manager 디렉터리를 만든 후 디렉터리 구성을 내보내면 사용자 디렉터리 연결 정보가 디렉터리 구성 파일의 Provider 요소에 표시됩니다.

데이터베이스 연결 설명

데이터베이스 연결을 설명하려면 directory.xml 파일에서 Provider 요소 및 해당 하위 요소를 사용하십시오.

참고: CA Identity Manager 디렉터리를 만드는 경우 directory.xml 파일에서 디렉터리 연결 정보를 제공할 필요가 없습니다. 관리 콘솔의 CA Identity Manager 디렉터리 마법사에서 연결 정보를 제공하십시오.

업데이트하려는 경우에만 Provider 요소를 수정하십시오.

Provider 요소

Provider 요소에는 다음과 같은 하위 요소가 있습니다.

JDBC(필수)

사용자 저장소에 연결할 때 사용할 JDBC 데이터 원본을 식별합니다. JDBC 데이터 원본을 만들 때 (페이지 144) 제공한 JNDI 이름을 지정합니다.

Credentials(필수)

데이터베이스에 액세스하는 데 필요한 사용자 이름 및 암호를 제공합니다.

DSN

사용자 저장소에 연결할 때 사용할 ODBC 데이터 원본을 식별합니다.

참고: 이 하위 요소는 CA Identity Manager 가 SiteMinder 와 통합된 경우에만 적용됩니다. SiteMinder 가 포함되어 있지 않은 CA Identity Manager 환경에서는 이 하위 요소가 무시됩니다.

SiteMinderQuery

관계형 데이터베이스에서 사용자 정보를 찾는 데 사용할 사용자 지정 쿼리 체계를 지정합니다.

참고: 이 하위 요소는 CA Identity Manager 가 SiteMinder 와 통합된 경우에만 적용됩니다. SiteMinder 가 포함되어 있지 않은 CA Identity Manager 환경에서는 이 하위 요소가 무시됩니다.

완성된 데이터베이스 연결은 다음 예와 유사합니다.

```
<Provider type="RDB" userdirectory="@SMDirName">
        <JDBC datasource="@SMDirJDBCDataSource"/>
        <Credentials user="@SMDirUser"
                cleartext="true">@SMDirPassword</Credentials>
        <DSN name="@SMDirDSN" />
        <SiteMinderQuery name="AuthenticateUser" query="SELECT TBLUSERS.LOGINID
FROM    TBLUSERS WHERE TBLUSERS.LOGINID='%s' AND TBLUSERS.PASSWORD='%s'" />
</provider>
```

Provider 요소의 특성은 다음과 같습니다.

type

데이터베이스의 유형을 지정합니다. Microsoft SQL Server 및 Oracle 데이터베이스의 경우 RDB(기본값)를 지정합니다.

userdirectory

사용자 디렉터리 연결의 이름을 지정합니다. 이 매개 변수는 디렉터리 생성 과정에서 제공하는 연결 개체 이름에 해당합니다.

인증을 위해 CA Identity Manager 가 SiteMinder 와 통합된 경우 SiteMinder 에서 설치 중에 연결 개체에 지정한 이름을 사용하여 사용자 디렉터리 연결이 생성됩니다. 기존 SiteMinder 사용자 디렉터리에 연결하려는 경우 연결 개체를 요구하는 메시지가 표시되면 해당 사용자 디렉터리의 이름을 입력합니다. CA Identity Manager 는 userdirectory 매개 변수를 지정한 이름으로 채웁니다.

CA Identity Manager 가 SiteMinder 와 통합되지 않은 경우 userdirectory 매개 변수의 값은 사용자 저장소에 대한 JDBC 연결을 제공하는 모든 이름입니다.

참고: directory.xml 파일에 사용자 디렉터리 연결의 이름을 지정하지 마십시오. CA Identity Manager 에서 디렉터리를 만드는 중에 이름을 제공하라는 메시지가 표시됩니다.

데이터베이스 자격 증명

데이터베이스에 연결하려면 CA Identity Manager 는 데이터 원본에 대해 올바른 자격 증명을 제공해야 합니다. 자격 증명은 Credentials 요소에서 정의되며, 이는 다음 예와 유사합니다.

```
<Credentials user="@SMDirUser" cleartext="true">
  "MyPassword"
</Credentials>
```

Credentials 요소에서 암호를 지정하지 않고 관리 콘솔에서 CA Identity Manager 디렉터리를 만들려고 하면 암호 자격 증명을 요구하는 메시지가 표시됩니다.

참고: 관리 콘솔에서 암호를 지정하는 것이 좋습니다.

관리 콘솔에서 암호를 지정하면 CA Identity Manager 에서 자동으로 암호를 암호화합니다. 그렇지 않은 경우 암호를 일반 텍스트로 표시하지 않으려면 CA Identity Manager 와 함께 설치된 암호 도구를 사용하여 암호를 암호화하십시오. SiteMinder 암호에서 암호 도구 사용에 대한 지침을 확인할 수 있습니다.

참고: 자격 증명 세트는 하나만 지정할 수 있습니다. 여러 데이터 원본을 정의하는 경우 지정하는 자격 증명이 모든 데이터 원본에 적용되어야 합니다.

자격 증명 매개 변수는 다음과 같습니다.

user

데이터 원본에 액세스할 수 있는 계정의 로그인 ID 를 정의합니다.

directory.xml 파일에서 user 매개 변수에 대한 값을 지정하지 마십시오. 관리 콘솔에서 CA Identity Manager 디렉터리를 만들 때 로그인 ID 를 제공하라는 메시지가 표시됩니다.

cleartext

directory.xml 파일에서 암호를 일반 텍스트로 표시할지 여부를 결정합니다.

- True - 암호가 일반 텍스트로 표시됩니다.
- False - 암호가 암호화됩니다(기본값).

참고: 이러한 매개 변수는 선택 사항입니다.

DSN(데이터 원본 이름)

directory.xml 파일의 DSN 요소에는 CA Identity Manager 가 데이터베이스에 연결할 때 사용하는 ODBC 데이터 원본의 이름에 해당하는 매개 변수가 하나 있습니다. name 매개 변수의 값은 기존 데이터 원본의 이름과 일치해야 합니다.

참고: 이 요소는 CA Identity Manager 가 SiteMinder 와 통합된 경우에만 적용됩니다. CA Identity Manager 가 SiteMinder 와 통합되지 않은 경우 이 요소는 무시됩니다.

name 매개 변수의 값이 @SmDirDSN 인 경우 directory.xml 파일에서 DSN 이름을 지정할 필요가 없습니다. CA Identity Manager 에서 directory.xml 파일을 가져올 때 DSN 이름을 제공하라는 메시지를 표시합니다.

장애 조치를 구성하려면 여러 DSN 요소를 정의하십시오. 기본 데이터 원본이 요청에 응답하지 못할 경우 정의된 다음 데이터 원본이 요청에 응답합니다.

예를 들어 다음과 같은 방법으로 장애 조치를 구성했다고 가정합니다.

```
<DSN name="DSN1">
<DSN name="DSN2">
```

CA Identity Manager 는 데이터 원본 DSN1 을 사용하여 데이터베이스에 연결합니다. DSN1 에 문제가 발생한 경우 CA Identity Manager 는 DSN2 를 사용하여 데이터베이스에 연결하려고 시도합니다.

참고: Credentials 요소 (페이지 185)에서 지정하는 자격 증명이 정의하는 모든 DSN 에 적용되어야 합니다.

SQL 쿼리 체계

CA Identity Manager 는 쿼리 체계를 사용하여 관계형 데이터베이스에서 사용자 및 그룹 정보를 찾습니다.

참고: 이 요소는 CA Identity Manager 가 SiteMinder 와 통합된 경우에만 적용됩니다. SiteMinder 가 포함되어 있지 않은 환경에서는 이 매개 변수가 무시됩니다.

관리 콘솔에서 CA Identity Manager 디렉터리를 만드는 경우 CA Identity Manager 가 SiteMinder 의 필수 쿼리 체계를 기반으로 하는 쿼리 체계 집합을 생성합니다. SiteMinder 쿼리 체계에 대한 자세한 정보는 *CA SiteMinder Web Access Manager Policy Server Configuration Guide*(CA SiteMinder Web Access Manager 정책 서버 구성 안내서)를 참조하십시오. SiteMinder 쿼리 체계의 테이블 및 열 이름은 디렉터리 구성 파일에서 지정하는 데이터로 바뀝니다.

사용자 지정 쿼리 체계를 정의하는 방법

쿼리 체계는 디렉터리 구성 파일의 SiteMinderQuery 요소에서 정의됩니다. SiteMinderQuery 요소는 다음과 같습니다.

```
<SiteMinderQuery name="SetUserProperty" query="update tblUsers set %s =
&apos;%s&apos; where loginid = &apos;%s&apos;" />
```

참고: 샘플 쿼리에서 '는 작은따옴표(')에 해당하는 XML 구문입니다.

SiteMinderQuery 요소는 CA Identity Manager 가 SiteMinder 와 통합된 경우에만 적용됩니다.

쿼리 체계 매개 변수는 다음과 같습니다.

name

SiteMinder 쿼리 체계의 다시 정의된 이름을 지정합니다.

이 값을 수정하지 마십시오.

query

실행할 SQL 문 또는 저장 프로시저를 지정합니다. 유효한 값은 다음과 같습니다.

- INSERT
- SELECT
- UPDATE
- DELETE
- CALL(저장 프로시저 전용)

참고: 이러한 매개 변수는 SiteMinderQuery 요소에 필요합니다.

쿼리 체계를 사용자 지정하려면 먼저 다음을 수행해야 합니다.

- 기본 쿼리 체계에 익숙해야 합니다.

  참고: SQL 쿼리 체계에 대한 자세한 내용은 *CA SiteMinder Web Access Manager Policy Server Configuration Guide*(CA SiteMinder Web Access Manager 정책 서버 구성 안내서)를 참조하십시오.

- SQL 쿼리 개발에 대한 폭넓은 경험을 갖추어야 합니다.

기본 쿼리 체계 수정

기본 쿼리 체계를 수정하려면 다음 절차를 수행하십시오.

다음 단계를 수행하십시오.

1. 디렉터리 구성 파일을 내보냅니다.

   CA Identity Manager 에서 생성된 쿼리 체계를 비롯하여 CA Identity Manager 디렉터리에 대한 현재의 모든 설정이 포함된 디렉터리 구성 파일을 생성합니다.

2. 디렉터리 구성 파일을 저장합니다.

   참고: 원본 디렉터리 구성 파일의 백업을 만들려면 내보낸 파일을 저장하기 전에 먼저 파일을 다른 이름으로 저장하거나 다른 위치에 저장하십시오.

3. 수정하려는 CA Identity Manager 생성 쿼리 체계를 찾습니다.
4. query 매개 변수에 실행할 쿼리 체계 또는 저장 프로시저를 입력합니다.

   참고: 쿼리 이름을 수정하지 마십시오.

5. 필요에 따라 내용을 변경한 후 디렉터리 구성 파일을 저장합니다.

   CA Identity Manager 디렉터리를 업데이트 (페이지 252)할 파일을 가져옵니다.

관계형 데이터베이스의 Well-Known 특성

CA Identity Manager 에서 Well-Known 특성은 특별한 의미를 갖습니다. 이 특성은 다음 구문으로 식별됩니다.

%ATTRIBUTENAME%

이 구문에서 *ATTRIBUTENAME* 은 대문자여야 합니다.

Well-Known 특성은 특성 설명 (페이지 163)을 사용하여 하나의 물리적 특성에 매핑됩니다.

다음 특성 설명에서 tblUsers.password 특성은 CA Identity Manager 가 tblUsers.password 의 값을 암호로 처리하도록 Well-Known 특성 %PASSWORD%에 매핑됩니다.

```
<ImsManagedObjectAttr
        physicalname="tblUsers.password"
        displayname="Password"
        description="Password"
        valuetype="String"
        required="false"
        multivalued="false"
        wellknown="%PASSWORD%"
        maxlength="0" />
```

Well-Known 특성은 필수 사항일 수도 있고 선택 사항일 수도 있습니다.

사용자 Well-Known 특성

사용자 Well-Known 특성 목록은 다음과 같습니다.

%ADMIN_ROLE_CONSTRAINT%

관리자 (페이지 195)에게 할당된 관리자 역할 (페이지 195) 목록을 포함합니다.

%ADMIN_ROLE_CONSTRAINT%에 매핑된 물리적 특성은 여러 역할을 수용할 수 있도록 다중 값을 가져야 합니다.

%ADMIN_ROLE_CONSTRAINT%에 매핑된 특성을 색인화하는 것이 좋습니다.

%CERTIFICATION_STATUS%

(사용자 인증 기능을 사용하는 경우 필수)

사용자의 인증 상태를 포함합니다.

참고: 사용자 인증에 대한 자세한 내용은 *관리 안내서*를 참조하십시오.

%DELEGATORS%

작업 항목을 현재 사용자에게 위임한 사용자의 목록에 매핑됩니다.

이 특성은 위임을 사용하는 데 필요합니다. %DELEGATORS%에 매핑되는 물리적 특성은 문자열을 포함할 수 있는 다중 값이어야 합니다.

중요! CA Identity Manager 태스크 또는 외부 도구를 사용하여 이 필드를 직접 편집하면 보안에 중요한 영향을 미칠 수 있습니다.

%EMAIL%

(전자 메일 알림 기능이 사용되도록 설정하는 경우 필수)

사용자의 전자 메일 주소를 저장합니다.

%ENABLED_STATE%

(필수)

사용자의 상태를 추적합니다.

참고: %ENABLED_STATE%에 매핑되는 물리적 특성의 데이터 형식은 문자열이어야 합니다.

%FIRST_NAME%

사용자의 이름을 포함합니다.

%FULL_NAME%

(필수)

사용자의 성과 이름을 포함합니다.

%IDENTITY_POLICY%

사용자 계정에 적용된 ID 정책 목록을 포함합니다.

CA Identity Manager 는 이 특성을 사용하여 ID 정책을 사용자에게 적용해야 할지 여부를 결정합니다. 정책에서 "Apply Once"(한 번 적용) 설정이 사용되도록 설정되어 있고 정책이 %IDENTITY_POLICY% 특성에 나열되어 있으면 정책 변경 내용이 사용자에게 적용되지 않습니다.

참고: ID 정책에 대한 자세한 내용은 *관리 안내서*를 참조하십시오.

%LAST_CERTIFIED_DATE%

(사용자 인증 기능을 사용하는 경우 필수)

사용자 역할이 인증된 날짜를 포함합니다.

참고: 사용자 인증에 대한 자세한 내용은 *관리 안내서*를 참조하십시오.

%LAST_NAME%

사용자의 성을 포함합니다.

%ORG_MEMBERSHIP%

(조직이 지원되는 경우 필수)

사용자가 속한 조직의 고유 식별자를 포함합니다.

%ORG_MEMBERSHIP_NAME%

(조직이 지원되는 경우 필수)

사용자가 속한 조직의 이름(사용자에게 친숙한 이름)을 포함합니다.

%PASSWORD%

사용자 암호를 포함합니다.

참고: 특성 또는 필드가 암호를 숨기도록 설정되어 있지 않더라도 %PASSWORD% 특성 값은 CA Identity Manager 화면에서 항상 일련의 별표(*) 문자로 표시됩니다.

%PASSWORD_DATA%

(암호 정책 지원 시 필수)

암호 정책 정보를 추적하는 특성을 지정합니다.

참고: 특성 또는 필드가 암호를 숨기도록 설정되어 있지 않더라도 %PASSWORD_DATA% 특성 값은 CA Identity Manager 화면에서 항상 일련의 별표(*) 문자로 표시됩니다.

%PASSWORD_HINT%

(필수)

사용자가 지정한 질문 및 대답 쌍을 포함합니다. 질문 및 대답 쌍은 사용자가 암호를 잊어버린 경우에 사용됩니다.

참고: 특성 또는 필드가 암호를 숨기도록 설정되어 있지 않더라도 %PASSWORD_HINT% 특성 값은 CA Identity Manager 화면에서 항상 일련의 별표(*) 문자로 표시됩니다.

%USER_ID%

(필수)

사용자 로그인 ID 를 저장합니다.

그룹 Well-Known 특성

그룹 Well-Known 특성 목록은 다음과 같습니다.

%GROUP_ADMIN%

그룹의 관리자를 포함합니다.

참고: %GROUP_ADMIN% 특성은 다중 값을 가져야 합니다.

%GROUP_DESC%

그룹에 대한 설명을 포함합니다.

%GROUP_ID%

그룹의 고유 식별자를 포함합니다.

%GROUP_MEMBERSHIP%

(필수)

그룹의 구성원 목록을 포함합니다.

참고: %GROUP_MEMBERSHIP% 특성은 다중 값을 가져야 합니다.

%GROUP_NAME%

(필수)

그룹의 이름을 저장합니다.

%ORG_MEMBERSHIP%

(조직이 지원되는 경우 필수)

그룹이 속한 조직의 고유 식별자를 포함합니다.

%ORG_MEMBERSHIP_NAME%

(조직이 지원되는 경우 필수)

그룹이 속한 조직의 이름(사용자에게 친숙한 이름)을 포함합니다.

%SELF_SUBSCRIBING%

사용자가 그룹을 구독할지 여부를 결정합니다.

%Admin_Role_Constraint% 특성

관리자 역할을 만드는 경우 역할 구성원 자격에 대한 규칙을 하나 이상 지정하십시오. 구성원 자격 규칙을 충족하는 사용자에게 해당 역할이 부여됩니다. 예를 들어 사용자 매니저 역할에 대한 구성원 자격 규칙이 title=User Manager 인 경우 직책이 사용자 매니저인 사용자에게 사용자 매니저 역할이 부여됩니다.

참고: 규칙에 대한 자세한 내용은 *관리 안내서*를 참조하십시오.

%ADMIN_ROLE_CONSTRAINT%를 사용하면 관리자의 모든 관리자 역할을 저장할 프로필 특성 하나를 지정할 수 있습니다.

%ADMIN_ROLE_CONSTRAINT% 특성을 사용하는 방법

%ADMIN_ROLE_CONSTRAINT%를 모든 관리자 역할의 제약 조건으로 사용하려면 다음 태스크를 수행하십시오.

- 여러 역할을 수용하도록 %ADMIN_ROLE_CONSTRAINT% Well-Known 특성을 다중 값 프로필 특성과 연결합니다.
- CA Identity Manager 사용자 인터페이스에서 관리자 역할을 구성하는 경우 다음과 같은 시나리오가 제약 조건이 될 수 있습니다.

  관리자 역할이 *role name* 과 같음

  role name

  제약 조건을 제공하는 역할의 이름을 정의합니다.

  예: 관리자 역할이 사용자 매니저와 같음

참고: 관리자 역할은 %ADMIN_ROLE_CONSTRAINT% 특성의 기본 표시 이름입니다.

Well-Known 특성 구성

Well-Known 특성을 구성하려면 다음 절차를 수행하십시오.

다음 단계를 수행하십시오.

1. 디렉터리 구성 파일에서 다음 기호를 검색합니다.

   ##

   필수 값은 2 개의 파운드 기호(##)로 식별됩니다.

2. ##로 시작하는 값을 데이터베이스에 있는 특성의 물리적 이름으로 바꿉니다. 다음 형식을 사용하여 특성 이름을 제공합니다.

   tablename.columnname

   예를 들어 암호 특성이 tblUsers 테이블의 암호 열에 저장된 경우 다음과 같은 방법으로 이름을 지정합니다.

   tblUsers.password

3. 모든 필수 값을 바꾸고 원하는 선택적 값이 모두 포함될 때까지 1~2 단계를 반복합니다.
4. 필요에 따라 선택적 Well-Known 특성을 물리적 특성에 매핑합니다.
5. 디렉터리 구성 파일을 저장합니다.

자체 구독 그룹을 구성하는 방법

디렉터리 구성 파일에서 자체 구독 그룹에 대한 지원을 구성하여 자체 서비스 사용자가 그룹에 참가하도록 설정할 수 있습니다.

다음 단계를 수행하십시오.

1. "Self-subscribing Groups"(자체 구독 그룹) 섹션에서 다음과 같이 SelfSubscribingGroups 요소를 추가합니다.

   <SelfSubscribingGroups type=*search_type* org=*org_dn*>

2. 다음 매개 변수의 값을 입력합니다.

   type

   CA Identity Manager 가 자체 구독 그룹을 검색하는 위치를 나타냅니다. 유효한 값은 다음과 같습니다.

   - NONE - CA Identity Manager 가 그룹을 검색하지 않습니다. 사용자가 그룹을 구독하지 않게 하려면 "NONE"을 지정하십시오.
   - ALL - 사용자 저장소에서 모든 그룹을 검색합니다. 사용자가 모든 그룹을 구독할 수 있는 경우 "ALL"을 지정하십시오.
   - INDICATEDORG(*조직을 지원하는 환경만 해당*) - CA Identity Manager 가 사용자의 조직과 해당 하위 조직에서 자체 구독 그룹을 검색합니다. 예를 들어 사용자 프로필이 Marketing 조직에 있는 경우 CA Identity Manager 는 Marketing 조직 및 모든 하위 조직에서 자체 구독 그룹을 검색합니다.
   - SPECIFICORG(*조직을 지원하는 환경만 해당*) - CA Identity Manager 가 특정 조직에서 검색을 수행합니다. org 매개 변수에서 특정 조직의 고유 식별자를 제공합니다.

   org

   CA Identity Manager 가 자체 구독 그룹을 검색하는 조직의 고유 식별자를 정의합니다.

   참고: type=SPECIFICORG 인 경우 org 매개 변수를 지정해야 합니다.

3. 다음 항목 중 하나를 변경한 경우 SiteMinder 정책 서버를 다시 시작하십시오.
   - type 매개 변수를 SPECIFICORG 로 변경한 경우 또는 그 반대의 경우
   - org 매개 변수의 값

CA Identity Manager 디렉터리에서 자체 구독 그룹에 대한 지원이 구성된 경우 CA Identity Manager 관리자는 사용자 콘솔에서 자체 구독 그룹을 지정할 수 있습니다.

사용자가 자체 등록하는 경우 CA Identity Manager 는 지정된 조직에서 그룹을 검색하여 자체 구독 그룹을 사용자에게 표시합니다.

유효성 검사 규칙

유효성 검사 규칙은 사용자가 태스크 화면 필드에 입력하는 데이터에 대한 요구 사항을 적용합니다. 이 요구 사항으로 데이터 형식 또는 형식을 적용할 수도 있고, 태스크 화면의 다른 데이터 맥락에서 데이터가 올바른지 확인할 수도 있습니다.

유효성 검사 규칙은 프로필 특성과 연결됩니다. 태스크가 처리되기 전에 먼저 CA Identity Manager 는 프로필 특성에 대해 입력된 데이터가 모든 관련 유효성 검사 규칙을 충족하는지 확인합니다.

유효성 검사 규칙을 정의하고, 이를 디렉터리 구성 파일의 프로필 특성에 연결할 수 있습니다.

조직 관리

관계형 데이터베이스의 경우 CA Identity Manager 에는 조직을 관리할 수 있는 옵션이 있습니다. 데이터베이스가 조직을 지원하는 경우 다음 사항이 적용됩니다.

- 조직은 계층적 구조를 갖습니다.
- 사용자, 그룹, 기타 조직과 같은 모든 관리 개체는 조직에 속해 있습니다.

- 조직을 삭제하면 해당 조직에 속해 있는 개체도 삭제됩니다.

몇 가지 추가 단계를 수행하여 사용자 및 그룹 개체를 구성하는 것과 동일한 방법으로 조직 개체를 구성할 수 있습니다.

조직 지원을 설정하는 방법

조직 지원을 설정하려면 다음 단계를 수행하십시오.

1. 데이터베이스에서 조직 지원을 구성 (페이지 200)합니다.
2. ImsManagedObject (페이지 157)에서 조직 개체를 설명합니다.

   Table 및 UniqueIdentifier 하위 요소를 구성해야 합니다.
3. 최상위 조직 (페이지 200)을 구성합니다.
4. 조직을 구성하는 특성을 설명 (페이지 163)합니다.
5. 조직 개체 (페이지 202)의 Well-Known 특성을 정의합니다.

데이터베이스에서 조직 지원 구성

다음 단계를 수행하십시오.

1. 편집기에서 다음 SQL 스크립트 중 하나를 엽니다.
   - Microsoft SQL Server 데이터베이스:

     ims_mssql_rdb.sql

- Oracle 데이터베이스:

  ims_oracle_rdb.sql

  이러한 파일은 다음 위치에 있습니다.

  admin_tools\directoryTemplates\RelationalDatabase

  admin_tools 는 관리 도구가 설치된 위치를 나타내며, 기본적으로 다음 위치 중 하나에 설치됩니다.

  Windows: C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools

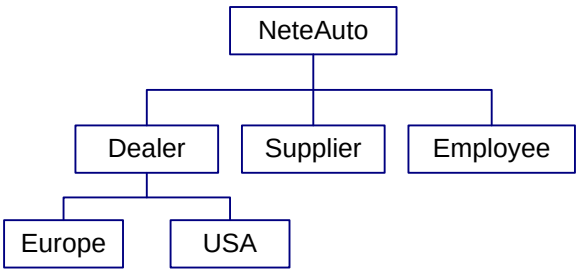
  UNIX: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

2. SQL 스크립트에서 <@primary organization table@>을 검색하고 이를 조직 개체의 기본 테이블의 이름으로 바꿉니다. SQL 스크립트를 저장합니다.
3. 데이터베이스에 대해 SQL 스크립트를 실행합니다.

루트 조직 지정

루트 조직은 디렉터리에서 최상위 또는 부모 조직으로 사용됩니다. 모든 조직은 루트 조직과 관련이 있습니다.

다음 그림에서 NeteAuto 는 루트 조직입니다. 나머지 조직은 NeteAuto 의 하위 조직입니다.



전체 루트 조직 정의는 다음 샘플과 유사합니다.

```
<ImsManagedObject name="Organization" description="My  Organizations"
objecttype="ORG">
   <RootOrg value="select orgid from tblOrganizations where parentorg is null">
      <Result name="%ORG_ID%" />
   </RootOrg>
```

조직 프로필 및 조직 개체의 고유 식별자를 구성하는 테이블을 포함하여 조직 개체에 대한 기본 정보를 정의하고 나면 directory.xml 파일에서 다음과 같이 루트 조직을 지정합니다.

- 다음 예와 같이 RootOrg 요소의 value 매개 변수에서 CA Identity Manager 가 루트 조직을 검색하는 데 사용하는 쿼리를 정의합니다.

  ```
  <RootOrg value="select orgid from tblOrganizations where parentorg  is null">
  ```

- 다음 예와 같이 Result 요소의 name 매개 변수에 조직의 고유 식별자를 입력합니다.

  ```
  <Result name="%ORG_ID%" />
  ```

  참고: name 매개 변수의 값은 조직 개체의 고유 식별자여야 합니다.

조직의 Well-Known 특성

Well-Known 특성 (페이지 107)에 설명된 대로 조직 프로필의 프로필에서 특성에 대한 Well-Known 특성을 정의합니다.

필수 조직 Well-Known 특성과 선택적 조직 Well-Known 특성은 다음과 같습니다.

%ORG_DESCR%

조직에 대한 설명을 포함합니다.

%ORG_MEMBERSHIP%

(필수)

조직의 부모 조직을 포함합니다.

참고: %ORG_MEMBERSHIP% 특성에 대한 자세한 내용은 "조직 계층을 정의하는 방법"을 참조하십시오.

%ORG_MEMBERSHIP_NAME%

(필수)

조직의 부모 조직 (페이지 203) 이름(사용자에게 친숙한 이름)을 포함합니다.

%ORG_NAME%

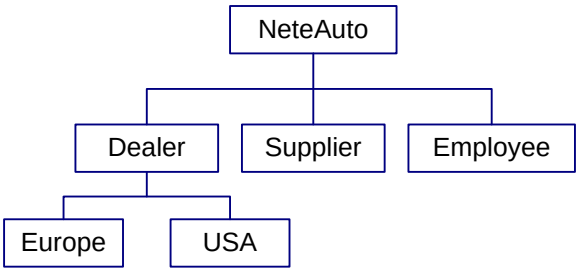
(필수)

조직의 이름을 포함합니다.

조직 계층을 정의하는 방법

CA Identity Manager 에서 조직은 루트 조직 및 하위 조직이 포함되어 있는 계층적 구조를 갖습니다. 하위 조직에는 또 다른 하위 조직이 포함될 수 있습니다.

루트 조직을 제외한 각 조직에는 부모 조직이 있습니다. 예를 들어 다음 그림에서 Dealer 는 USA 및 Europe 조직의 부모 조직입니다.



부모 조직의 고유 식별자는 조직 프로필의 특성에 저장됩니다. CA Identity Manager 는 이 특성의 정보를 사용하여 조직 계층을 구성할 수 있습니다.

부모 조직이 저장되는 특성을 지정하려면 다음과 같이 특성 설명에서 부모 조직의 이름을 저장하는 물리적 특성과 함께 %ORG_MEMBERSHIP% 및 %ORG_MEMBERSHIP_NAME% Well-Known 특성을 사용하십시오.

```
<ImsManagedObjectAttr physicalname="tblOrganizations.parentorg"
displayname="Organization" description="Parent Organization" valuetype="Number"
required="false" multivalued="false" wellknown="%ORG_MEMBERSHIP%" maxlength="0" />
```

디렉터리 검색 성능을 개선하는 방법

사용자, 조직 및 그룹에 대한 디렉터리 검색 성능을 향상시키려면 다음 태스크를 수행하십시오.

- 관리자가 검색 쿼리에서 지정할 수 있는 특성을 색인화합니다.
- 디렉터리 구성 파일(directory.xml)에서 시간 만료 검색 매개 변수 값을 지정하여 기본 디렉터리 시간 만료 설정을 재정의합니다.
- 사용자 디렉터리를 조정합니다. 사용 중인 데이터베이스 설명서를 참조하십시오.

ODBC 데이터 원본에서 데이터베이스 관련 옵션을 구성합니다. 자세한 내용은 데이터 원본 설명서를 참조하십시오.

대규모 검색 성능을 개선하는 방법

CA Identity Manager 가 대규모 사용자 저장소를 관리하는 경우 많은 결과가 반환되는 검색으로 인해 시스템의 메모리가 부족해질 수 있습니다.

다음 2 가지 설정에 따라 CA Identity Manager 가 대규모 검색을 처리하는 방식이 결정됩니다.

- Maximum number of rows(최대 행 수)

  사용자 디렉터리를 검색할 때 CA Identity Manager 가 반환할 수 있는 최대 결과 수를 지정합니다. 결과 수가 이 제한을 초과하면 오류가 표시됩니다.

- Page size(페이지 크기)

  단일 검색에서 반환될 수 있는 개체 수를 지정합니다. 개체 수가 페이지 크기를 초과하는 경우 다중 검색이 수행됩니다.

  참고: 사용자 저장소가 페이지 단위 처리를 지원하지 않지만 maxrows 값이 지정된 경우 CA Identity Manager 는 maxrows 값만 사용하여 검색 크기를 제어합니다.

다음 위치에서 최대 행 제한 및 페이지 크기를 구성할 수 있습니다.

- 사용자 저장소

  대부분의 사용자 저장소 및 데이터베이스에서 검색 제한을 구성할 수 있습니다.

  참고: 자세한 내용은 현재 사용하고 있는 사용자 저장소 또는 데이터베이스 설명서를 참조하십시오.

- CA Identity Manager 디렉터리

  디렉터리 구성 파일(directory.xml)에서 CA Identity Manager 디렉터리를 만드는 데 사용하는 DirectorySearch 요소를 구성 (페이지 79)할 수 있습니다.

  기본적으로 기존 디렉터리에는 최대 행 및 페이지 크기의 값에 제한이 없지만, 새 디렉터리의 경우에는 최대 행 값에는 제한이 없고 페이지 크기는 2000 으로 설정됩니다.

- 관리 개체 정의

  전체 디렉터리 대신 단일 개체 유형에 적용되는 최대 행 제한과 페이지 크기를 설정하려면 CA Identity Manager 디렉터리를 만드는 데 사용하는 directory.xml 파일에서 *관리 개체 정의*를 구성 (페이지 82)하십시오.

  특정 관리 개체 유형에 대한 제한을 설정하면 비즈니스 요구 사항을 기준으로 조정할 수 있습니다. 예를 들어 대부분의 회사에는 그룹보다 사용자가 많습니다. 이런 경우 사용자 개체 검색에 대한 제한만 설정하면 됩니다.

- 태스크 검색 화면

  사용자 콘솔에서 검색 및 목록 화면에 표시되는 검색 결과 수를 제어할 수 있습니다. 결과 수가 태스크에 대해 정의된 페이지당 결과 수를 초과하는 경우 결과에 대한 추가 페이지로 연결되는 링크가 표시됩니다.

  이 설정은 검색에서 반환되는 결과의 수에는 영향을 미치지 않습니다.

  참고: 검색 및 목록 화면에서 페이지 크기를 설정하는 방법에 대한 자세한 내용은 *관리 안내서*를 참조하십시오.

최대 행 제한 및 페이지 크기가 여러 위치에서 정의된 경우 가장 구체적인 설정이 적용됩니다. 예를 들어 관리 개체 설정이 디렉터리 수준 설정보다 우선합니다.

제 5 장: CA Identity Manager 디렉터리

CA Identity Manager 디렉터리에서는 CA Identity Manager 가 관리하는 사용자 디렉터리에 대한 정보를 제공합니다. 이 정보는 사용자, 그룹 및 조직과 같은 개체가 사용자 저장소에 저장되고 CA Identity Manager 에서 표시되는 방식을 설명합니다.

관리 콘솔의 CA Identity Manager 디렉터리 섹션에서 CA Identity Manager 디렉터리를 만들고, 보고, 내보내고, 업데이트하고, 삭제할 수 있습니다.

참고: CA Identity Manager 가 SiteMinder 정책 서버의 클러스터를 사용하는 경우 CA Identity Manager 디렉터리를 만들거나 업데이트하기 전에 정책 서버 하나를 제외하고 모두 중지하십시오.

이 섹션은 다음 항목을 포함하고 있습니다.

CA Identity Manager 디렉터리를 만들기 위한 사전 요구 사항

CA Identity Manager 디렉터리를 만들려면 먼저 다음을 수행해야 합니다.

- CA Identity Manager 디렉터리를 만들거나 수정하기 전에 CA Identity Manager 노드를 하나만 제외하고 모두 중지합니다.

  참고: CA Identity Manager 노드의 클러스터가 있는 경우 관리 콘솔에서 변경할 때 하나의 CA Identity Manager 노드만 사용되도록 설정할 수 있습니다.

- CA Identity Manager 디렉터리를 만들거나 업데이트하기 전에 정책 서버를 하나만 제외하고 모두 중지합니다.

  참고: SiteMinder 정책 서버의 클러스터가 있는 경우 관리 콘솔에서 변경할 때 하나의 SiteMinder 정책 서버만 사용되도록 설정할 수 있습니다.

디렉터리를 만드는 방법

관리 콘솔에서 사용자 저장소의 구조 및 콘텐츠를 설명하는 CA Identity Manager 디렉터리와 프로비져닝 서버에 필요한 정보를 저장하는 프로비져닝 디렉터리를 만듭니다. 이러한 디렉터리는 CA Identity Manager 환경과 연결되어 있습니다.

다음 방법 중 하나를 사용하여 디렉터리를 만들 수 있습니다.

- 디렉터리 구성 마법사 사용

  관리자가 자신의 사용자 저장소에 대한 디렉터리를 만드는 과정을 안내합니다. 이 방법을 사용하면 발생할 수 있는 구성 오류를 줄일 수 있습니다.

  참고: LDAP 사용자 저장소에 대한 디렉터리를 새로 만들 경우에만 디렉터리 구성 마법사를 사용하십시오. 관계형 데이터베이스에 대한 디렉터리를 만들거나 기존 디렉터리를 업데이트하려면 directory.xml 파일을 직접 가져오십시오.

- XML 구성 파일 사용

  관리자가 완전하게 구성된 XML 파일을 선택하여 사용자 저장소 또는 프로비져닝 서버를 만들거나 수정할 수 있습니다.

  관계형 데이터베이스에 대한 디렉터리를 만들거나 기존 디렉터리를 업데이트하는 경우 이 방법을 선택하십시오.

추가 정보:

XML 구성 파일을 사용하여 디렉터리 만들기 (페이지 229)
디렉터리 구성 마법사를 사용하여 디렉터리 만들기 (페이지 212)

디렉터리 구성 마법사를 사용하여 디렉터리 만들기

디렉터리 구성 마법사는 관리자가 사용자 저장소에 대한 디렉터리를 만드는 과정을 안내하고 구성 오류를 줄이는 데 도움이 됩니다. 마법사를 시작하기 전에 먼저 CA Identity Manager LDAP 디렉터리 구성 템플릿을 업로드해야 합니다. 이러한 템플릿은 필수 Well-Known 특성을 사용하여 미리 구성되어 있습니다. LDAP 사용자 저장소 또는 프로비저닝 디렉터리에 대한 연결 세부 정보를 입력한 다음에는 LDAP 특성을 선택하고, Well-Known 특성을 매핑하고, 이 특성에 대한 메타데이터를 입력할 수 있습니다. 특성 매핑이 끝났으면 "마침"을 클릭하여 디렉터리를 만드십시오.

디렉터리 구성 마법사 시작

디렉터리 구성 마법사를 사용하면 관리자가 CA Identity Manager 템플릿을 선택하고 이 템플릿을 사용자 환경에 맞게 수정할 수 있습니다.

다음 단계를 수행하십시오.

1. 관리 콘솔에서 "Directories"(디렉터리)를 클릭하고 "Create from Wizard"(마법사에서 만들기)를 선택합니다.

   사용자 저장소를 구성할 디렉터리 구성 파일을 선택하라는 메시지가 표시됩니다.

2. "Browse"(찾아보기)를 클릭하여 다음 기본 위치에서 사용자 저장소 또는 프로비저닝 서버를 구성할 구성 파일을 선택하고 "Next"(다음)를 클릭합니다.

   ```
   admin_tools\directoryTemplates\directory\
   ```

   참고: admin_tools 는 관리 도구가 설치된 디렉터리를 지정하고 directory 는 LDAP 공급업체의 이름을 지정합니다.

   기본적으로 관리 도구는 다음 위치에 설치됩니다.

   - Windows: C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools
   - UNIX: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

3. "Connection Details"(연결 정보) 화면에서 LDAP 디렉터리 또는 프로비저닝 서버에 대한 연결 정보, 디렉터리 검색 매개 변수 및 장애 조치 연결 정보를 지정하고 "Next"(다음)를 클릭합니다.

4. "Configure Managed Object"(관리 개체 구성) 화면에서 구성할 개체를 지정하고 "Next"(다음)를 클릭합니다. 다음 개체 중에서 선택할 수 있습니다.

   - Configure User Managed Object(사용자 관리 개체 구성)
   - Configure Group Managed Object(그룹 관리 개체 구성)
   - Configure Organization Object(조직 개체 구성)
   - Show summary and deploy directory(요약 표시 및 디렉터리 배포)

     참고: 디렉터리 구성을 마친 경우에만 "Summary and Deploy Directory"(요약 및 디렉터리 배포)를 선택하십시오.

   a. "Select Attribute"(특성 선택) 화면에서 필요에 따라 구조 및 보조 클래스를 보고 수정한 후 "Next"(다음)를 클릭합니다.

   b. "Select Attributes: Mapping Well-Knowns"(특성 선택: Well-Known 매핑) 화면에서 CA Identity Manager well-known 별칭을 선택한 LDAP 특성에 매핑하고 "Next"(다음)를 클릭합니다.

   c. (선택 사항) "Describe User Attributes"(사용자 특성 설명) 화면에서 특성 정의를 보고 수정한 후 Next"(다음)를 클릭합니다. 표시 이름과 설명을 수정할 수 있습니다.

   d. (선택 사항) "User Attribute Details"(사용자 특성 정보) 화면에서 관리할 선택한 특성 각각에 대한 메타데이터를 정의하고 Next"(다음)를 클릭합니다.

      "Managed Object Selection"(관리 개체 선택 내용) 화면이 나타납니다.

      그룹 또는 조직을 구성하려면 해당 관리 개체를 선택하고 Next"(다음)를 클릭한 후 각 개체에 대한 특성 화면을 반복하십시오.

5. 목록에서 "Show summary and deploy directory"(요약 표시 및 디렉터리 배포)를 선택하고 Next"(다음)를 클릭합니다.

   "Confirmation"(확인) 화면이 나타납니다.

6. 디렉터리 세부 정보를 확인합니다.

   오류가 있을 경우 "Back"(뒤로) 단추를 클릭하여 해당 화면에서 수정합니다. "Finish"(마침)를 클릭하여 변경 사항을 적용합니다.

   구성의 유효성이 검사되고 디렉터리가 생성됩니다. 그런 다음 새 디렉터리를 확인할 수 있는 "Directories"(디렉터리) 목록으로 다시 돌아갑니다.

Select Directory Template(디렉터리 템플릿 선택) 화면

이 화면에서 사용자 저장소 또는 프로비저닝 서버를 구성할 LDAP 에 대한 디렉터리 XML 파일을 선택할 수 있습니다.

"Browse"(찾아보기) 단추를 클릭하여 다음 기본 위치에서 사용자 저장소 또는 프로비저닝 서버를 구성할 구성 파일을 선택합니다.

```
admin_tools\directoryTemplates\directory\
```

참고: admin_tools 는 관리 도구가 설치된 디렉터리를 지정하고 directory 는 LDAP 공급업체의 이름을 지정합니다.

기본적으로 관리 도구는 다음 위치에 설치됩니다.

- Windows: C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools
- UNIX: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

디렉터리 XML 파일을 선택한 후 "Next"(다음)를 클릭하여 "Connection Details"(연결 정보) 화면으로 계속합니다.

"Connection Details"(연결 정보) 화면

이 화면에서 사용자 저장소에 대한 구성 자격 증명을 입력할 수 있습니다. 또한 디렉터리 검색 매개 변수를 입력하고 장애 조치 연결을 추가할 수 있습니다. 연결 정보를 입력한 후 "Next"(다음)를 클릭하여 관리할 개체를 선택합니다.

참고: 이 화면에 나타나는 필드는 사용자 저장소 유형 및 연결을 만들 때 디렉터리 구성 마법사를 사용하는지, 아니면 XML 파일을 직접 가져오는지에 따라 달라집니다.

이 화면에는 다음 필드가 있습니다.

Name(이름)

연결하려는 사용자 디렉터리의 이름을 지정합니다.

Description(설명)

사용자 디렉터리에 대한 설명을 지정합니다.

Host(호스트)

사용자 저장소가 위치한 컴퓨터의 호스트 이름을 지정합니다.

Port(포트)

사용자 저장소가 위치한 컴퓨터의 포트를 지정합니다.

User DN(사용자 DN)

LDAP 사용자 저장소에 액세스하는 데 사용할 사용자 도메인 이름을 지정합니다.

JDBC Data Source JNDI Name(JDBC 데이터 원본 JNDI 이름)

CA Identity Manager 가 데이터베이스에 연결하는 데 사용하는 기존 JDBC 데이터 원본의 이름을 지정합니다.

Username(사용자 이름)

프로비저닝 서버에 액세스하는 데 사용할 사용자 이름을 지정합니다.

참고: 프로비저닝 서버에만 해당됩니다.

Domain(도메인)

프로비저닝 서버에 액세스하는 데 사용할 도메인 이름을 지정합니다.

참고: 프로비저닝 서버에만 해당됩니다.

Password(암호)

LDAP 사용자 저장소/프로비저닝 서버에 액세스하는 데 사용할 암호를 지정합니다.

Confirm Password(암호 확인)

LDAP 사용자 저장소/프로비저닝 서버에 액세스하는 데 사용할 암호를 확인합니다.

Secure Connection(보안 연결)

선택할 경우 LDAP 사용자 디렉터리에 대한 SSL(Secure Sockets Layer) 연결을 강제 적용합니다.

Search Root(검색 루트)

디렉터리의 시작점 역할을 하는 LDAP 디렉터리의 위치를 지정합니다. 주로 조직(o) 또는 조직 단위(ou)입니다.

참고: LDAP 사용자 저장소에만 해당됩니다.

Search Maximum Rows(최대 검색 행 수)

사용자 디렉터리를 검색할 때 CA Identity Manager 가 반환할 수 있는 최대 결과 수를 지정합니다. 결과 수가 이 제한을 초과하면 오류가 표시됩니다.

최대 행 수 설정은 검색 결과를 제한하는 LDAP 디렉터리의 설정을 무시할 수 있습니다. 충돌하는 설정이 적용되는 경우 LDAP 서버는 가장 낮은 설정을 사용합니다.

Search Page Size(검색 페이지 크기)

단일 검색에서 반환될 수 있는 개체 수를 지정합니다. 개체 수가 페이지 크기를 초과하는 경우 다중 검색이 수행됩니다.

"Search Page Size"(검색 페이지 크기)를 지정할 때는 다음 사항에 주의하십시오.

- "Search Page Size"(검색 페이지 크기) 옵션을 사용하려면 CA Identity Manager 가 관리하는 사용자 저장소가 페이지 단위 처리를 지원해야 합니다. 일부 사용자 저장소 유형의 경우 페이지 단위 처리를 지원하려면 추가 구성이 필요할 수 있습니다. 자세한 내용은 *구성 안내서*를 참조하십시오.
- 사용자 저장소가 페이지 단위 처리를 지원하지 않고 "Search Maximum Rows"(최대 검색 행 수)의 값이 지정된 경우 CA Identity Manager 는 "Search Maximum Rows"(최대 검색 행 수) 값만 사용하여 검색 크기를 제어합니다.

Search Timeout(검색 시간 만료)

CA Identity Manager 가 검색을 종료하기 전에 디렉터리를 검색하는 최대 시간(초)을 지정합니다.

Failover Host(장애 조치 호스트)

기본 시스템을 사용할 수 없을 경우 이중화된 사용자 저장소 또는 대체 프로비저닝 서버가 있는 시스템의 호스트 이름을 지정합니다. 서버가 여러 개 있을 경우 CA Identity Manager 는 나열된 순서대로 시스템에 연결하려고 시도합니다.

Failover Port(장애 조치 포트)

기본 시스템을 사용할 수 없을 경우 이중화된 사용자 저장소 또는 대체 프로비저닝 서버가 있는 시스템의 포트를 지정합니다. 서버가 여러 개 있을 경우 CA Identity Manager 는 나열된 순서대로 시스템에 연결하려고 시도합니다.

Add(추가) 단추

다른 장애 조치 호스트 이름 및 포트 번호를 추가하려면 클릭하십시오.

Configure Managed Objects(관리 개체 구성) 화면

이 화면에서 구성할 개체를 선택할 수 있습니다.

다음 목록에는 이 화면에 나타나는 필드가 나와 있습니다.

Configure User Managed Object(사용자 관리 개체 구성)

사용자가 사용자 저장소에 저장되는 방식과 CA Identity Manager 에서 표시되는 방식을 설명합니다.

Configure Group Managed Object(그룹 관리 개체 구성)

그룹이 사용자 저장소에 저장되는 방식과 CA Identity Manager 에서 표시되는 방식을 설명합니다.

Configure Organization Managed Object(조직 관리 개체 구성)

사용자 저장소에 조직이 포함될 경우 조직이 CA Identity Manager 에서 저장되고 표시되는 방식을 설명합니다.

Show Summary and Deploy Directory(요약 표시 및 디렉터리 배포)

모든 관리 개체가 정의되었고 디렉터리를 배포하려고 함을 지정합니다. "Show summary and deploy directory"(요약 표시 및 디렉터리 배포)를 선택한 후 "Next"(다음)를 클릭하여 요약 페이지로 이동합니다.

Save(저장) 단추

xml 파일을 저장하려면 클릭하십시오.

Back(뒤로) 단추

"Connection Details"(연결 정보) 화면으로 돌아가서 수정하려면 클릭하십시오.

Next(다음) 단추

"Select Attributes"(특성 선택) 화면으로 계속하여 구성할 사용자, 그룹 또는 조직 특성을 선택하려면 클릭하십시오.

Select Attributes(특성 선택) 화면

이 화면에서 사용자, 그룹 또는 조직 개체에 대한 구조 및 보조 클래스를 변경하거나 추가할 수 있습니다. 이 화면은 사용하려는 디렉터리 유형에 대한 일반 디렉터리 스키마와 모범 사례에 기반한 값으로 미리 정의되어 있습니다. 관리자는 드롭다운 메뉴에서 새 클래스를 선택하여 구조 클래스를 변경할 수 있습니다. 클래스를 선택하면 새로운 구조 클래스에 속한 특성으로 테이블이 업데이트됩니다.

보조 클래스는 드롭다운 메뉴에서 선택하여 추가할 수 있습니다. 보조 클래스를 선택하면 새로운 보조 클래스에 속한 특성으로 테이블이 업데이트됩니다.

다음 목록에는 이 화면에 나타나는 필드가 나와 있습니다.

Structural Class Name(구조 클래스 이름)

구성할 특성의 구조 클래스를 지정합니다.

Change(변경) 단추

구조 클래스를 변경하려면 클릭하십시오.

Auxiliary Class Name(보조 클래스 이름)

구성할 특성의 보조 클래스를 지정합니다.

Add(추가) 단추

구성할 보조 클래스를 추가하려면 클릭하십시오.

Object Class(개체 클래스)

컨테이너 개체 클래스를 지정합니다.

ID

컨테이너 ID 를 지정합니다.

Name(이름)

컨테이너 이름을 지정합니다.

Attributes Table(특성 테이블)

물리적 이름, 개체 클래스, 특성이 다중 값인지 여부 및 선택한 특성의 데이터 형식을 지정합니다. 이 테이블의 특성은 "Selected"(선택됨), "Object Class"(개체 클래스), "Multi-Valued"(다중 값) 및 "Data Type"(데이터 형식)을 기준으로 정렬할 수 있습니다.

Back(뒤로) 단추

"Configure Managed Objects"(관리 개체 구성) 화면으로 돌아가려면 클릭하십시오.

Next(다음)

"Well-Known Mapping"(Well-Known 매핑) 화면으로 계속하여 필수 well-known 별칭 및 선택적 well-known 별칭을 매핑하려면 클릭하십시오.

Well-Known Mapping(Well-Known 매핑) 화면

이 화면에서 CA Identity Manager Well-Known 특성을 선택한 LDAP 특성에 매핑할 수 있습니다. 관리자는 새로운 Well-Known 특성이 사용자 지정 코드에 필요한 경우 해당 특성을 텍스트 필드에 입력하고 "Add"(추가) 단추를 클릭하여 Well-Known 특성 목록에 추가할 수 있습니다. 화면이 새로 고쳐지므로 Well-Known 특성을 필요한 만큼 계속 추가할 수 있습니다.

다음 목록에는 이 화면에 나타나는 필드가 나와 있습니다.

Required Well-Knowns(필수 Well-Known)

LDAP 특성에 매핑해야 하는 사용자, 그룹 또는 조직(해당되는 경우)에 대한 Well-Known 특성을 지정합니다.

Optional Well-Knowns(선택적 Well-Known)

필요한 경우 매핑할 수 있는 사용자, 그룹 또는 조직(해당되는 경우)에 대한 Well-Known 특성을 지정합니다.

New Well-Known(새 Well-Known)

사용자 지정 코드에서 참조되는 Well-Known 특성을 지정합니다.

Add(추가) 단추

새로운 Well-Known 특성을 "Optional Well-Knowns"(선택적 Well-Known)에 추가하려면 클릭하십시오.

Back(뒤로) 단추

"Select User Attributes"(사용자 특성 선택) 화면으로 돌아가서 추가 특성을 선택하려면 클릭하십시오. 이 화면으로 돌아가면 이미 설정한 매핑이 저장되어 사용 가능해집니다.

Next(다음) 단추

"Basic Object Attribute Definition"(기본 개체 특성 정의) 화면으로 계속하여 기본 특성 정의를 지정하려면 클릭하십시오.

More information(추가 정보)

LDAP 사용자 저장소에 대한 Well-Known 특성 (페이지 107)
그룹 Well-Known 특성 (페이지 112)
사용자 Well-Known 특성 (페이지 108)
조직의 Well-Known 특성 (페이지 114)

Basic Object Attribute Definition(기본 개체 특성 정의) 화면

이 화면에서 일반적으로 정의된 정의, 즉 표시 이름 및 설명을 보고 수정할 수 있습니다.

다음 목록에는 이 화면에 나타나는 필드가 나와 있습니다.

Managed Object Table(관리 개체 테이블)

관리 개체의 표시 이름, 물리적 이름, well-known 이름 및 설명을 지정합니다. 필요한 경우 드롭다운 메뉴를 사용하여 설명을 변경할 수 있습니다. 변경을 마치면 "Next"(다음)를 클릭하여 계속합니다.

Back(뒤로) 단추

"Well-Known Mapping"(Well-Known 매핑) 화면으로 돌아가서 매핑 세부 정보를 수정하려면 클릭하십시오.

Next(다음) 단추

추가 특성 정의를 지정할 수 있는 "Detailed Object Attribute Definition"(자세한 개체 특성 정의) 화면으로 계속하려면 클릭하십시오.

Detailed Object Attribute Definition(자세한 개체 특성 정의) 화면

이 화면에서 다른 특성 정의를 지정할 수 있습니다. 관리자는 표시 이름, 사용자 콘솔 화면의 특성 관리, 값의 데이터 형식, 최대 길이 및 유효성 검사 규칙 세트를 수정하여 선택한 각 특성에 대한 메타데이터를 정의할 수 있습니다. 특성 정의를 지정한 후 "Next"(다음)를 클릭하여 계속합니다.

이 화면의 필드가 아래에 나열되어 있습니다.

Display Name(표시 이름)

관리 개체 특성의 고유 이름을 지정합니다. 이 이름은 사용자 콘솔에 표시되는 이름입니다.

Tags(태그)

관리 개체 특성 값에 대한 데이터 분류 태그를 지정합니다. 태그는 모두 선택 사항이고 Searchable 을 제외하고 모든 태그의 기본값은 false 입니다. 다음 태그를 선택할 수 있습니다.

Required(필수)

개체를 만들 때 특성이 필수임을 나타냅니다.

Multiple Values(다중 값)

특성이 다중 값으로 표시됨을 나타냅니다.

Hidden(숨김)

특성이 숨겨짐을 나타냅니다.

System(시스템)

특성이 시스템 특성이고 태스크 화면에 추가되지 않음을 나타냅니다.

Searchable(검색 가능)

특성이 검색 필터에 추가됨을 나타냅니다. 기본값은 true 입니다.

Sensitive Encrypt(중요 특성 암호화)

특성이 중요 특성이고 일련의 별표(*)로 표시됨을 나타냅니다.

Hide in VST(VST 에서 숨김)

"View Submitted Tasks"(제출한 태스크 보기)에 대한 "Event Details"(이벤트 정보) 화면에서 특성을 숨김을 나타냅니다.

Do not copy(복사 안 함)

관리자가 개체의 사본을 만들 때 특성을 무시해야 함을 나타냅니다.

Previously encrypted(이전에 암호화됨)

사용자 저장소에서 액세스하려는 특성이 이전에 암호화되었고 암호 해독이 필요함을 나타냅니다. 개체를 저장할 때 일반 텍스트 값이 사용자 저장소에 저장됩니다.

Untagged encrypted(태그 없이 암호화됨)

특성이 사용자 저장소에서 이전에 암호화되었고 암호화된 텍스트의 시작 부분에 암호화 알고리즘 태그 이름이 없음을 나타냅니다.

Data Type(데이터 형식)

사용자 콘솔에서 관리 개체 특성의 값에 대한 데이터 형식을 지정합니다. 다음 목록에서 선택할 수 있습니다.

- READONLY
- WRITEONCE
- READWRITE

Maximum Length(최대 길이)

관리 개체 특성 값의 최대 길이를 지정합니다.

기본값: 0

Validation Rule Set(유효성 검사 규칙 세트)

관리 개체 특성 값의 유효성을 검사하기 위한 유효성 검사 규칙 세트를 지정합니다. 다음 목록에서 선택할 수 있습니다.

- User Validation(사용자 유효성 검사)
- Phone Format(전화 번호 형식)
- International Phone Format(국제 전화 번호 형식)

Back(뒤로) 단추

"Basic Object Attribute Definition"(기본 개체 특성 정의) 화면으로 돌아가서 수정하려면 클릭하십시오.

Next(다음) 단추

"Configure Managed Objects"(관리 개체 구성) 화면으로 계속하려면 이 단추를 클릭하십시오. 이 화면에서 구성할 다음 관리 개체를 선택할 수 있습니다. 관리 개체를 구성한 후 "Show summary and deploy directory"(요약 표시 및 디렉터리 배포)를 선택하여 디렉터리 정보를 표시하고 디렉터리를 배포합니다.

More information(추가 정보)

중요한 특성 관리 (페이지 95)

Confirmation(확인) 화면

이 화면에서는 디렉터리 정보에 대한 요약을 보여 줍니다.

다음 목록에는 이 화면에 나타나는 필드가 나와 있습니다.

Connection Details(연결 정보)

사용자 디렉터리에 대한 연결 정보를 지정합니다.

User/Group/Organization Details(사용자/그룹/조직 정보)

directory.xml 에 대한 변경 사항을 지정합니다.

Back(뒤로) 단추

마법사에서 정보를 수정하려면 클릭하십시오.

Save(저장) 단추

선택 내용을 저장하려면 클릭하십시오.

Finish(마침) 단추

디렉터리 정보가 모두 올바르고 마법사를 종료하려면 클릭하십시오.

구성의 유효성이 검사되고 디렉터리가 생성됩니다. 그런 후 새 디렉터리가 나열되는 "Directories"(디렉터리) 목록 페이지로 이동됩니다. 새 디렉터리를 편집하거나 내보내려면 디렉터리 목록에서 선택하십시오.

XML 구성 파일을 사용하여 디렉터리 만들기

관리 콘솔에서 완료된 directory.xml 파일을 가져와 CA Identity Manager 디렉터리를 만들거나 업데이트할 수 있습니다.

참고: 디렉터리 구성 마법사를 사용하지 않고 directory.xml 파일을 사용하여 디렉터리를 만드는 경우에는 기본 구성 템플릿을 수정해야 합니다. 자세한 내용은 *구성 안내서*를 참조하십시오.

다음 단계를 수행하십시오.

1. 브라우저에 다음 URL 을 입력하여 관리 콘솔을 엽니다.

   http://*hostname*:*port*/iam/immanage

   hostname

   CA Identity Manager 가 설치된 서버의 정규화된 도메인 이름을 정의합니다.

   port

   응용 프로그램 서버 포트 번호를 정의합니다.

2. "Directories"(디렉터리)를 클릭합니다.

   CA Identity Manager 디렉터리 창이 열립니다.

3. "Create"(만들기) 또는 "Update from XML"(XML 에서 업데이트)을 클릭합니다.

4. CA Identity Manager 디렉터리를 만들기 위한 디렉터리 구성 XML 파일의 경로와 파일 이름을 입력하거나 파일을 찾습니다. "Next"(다음)를 클릭합니다.

5. 이 창에서 필드 값을 다음과 같이 제공합니다.

   참고: 이 창에 표시되는 필드는 4 단계에서 디렉터리 구성 파일에 제공한 정보 및 사용자 저장소 유형에 따라 달라집니다. 디렉터리 구성 파일에서 이러한 필드에 대한 값을 제공한 경우 CA Identity Manager 에서는 이러한 값을 다시 제공하라는 메시지를 표시하지 않습니다.

   Name(이름)

   만들려는 CA Identity Manager 디렉터리의 이름을 결정합니다.

   Description(설명)

   (선택 사항) CA Identity Manager 디렉터리를 설명합니다.

   Connection Object Name(연결 개체 이름)

   CA Identity Manager 디렉터리가 설명하는 사용자 디렉터리의 이름을 지정합니다. 다음 정보 중 *하나*를 입력합니다.

   - CA Identity Manager 가 SiteMinder 와 통합되지 않은 경우에는 CA Identity Manager 가 사용자 저장소에 연결하는 데 사용하는 개체에 대한 의미 있는 이름을 지정합니다.
   - CA Identity Manager 가 SiteMinder 와 통합되어 있고 SiteMinder 에서 사용자 디렉터리 연결 개체를 만들려는 경우에는 원하는 의미 있는 이름을 지정합니다. CA Identity Manager 는 지정한 이름을 사용하여 SiteMinder 에서 사용자 디렉터리 연결 개체를 만듭니다.
   - CA Identity Manager 가 SiteMinder 와 통합되어 있고 기존 SiteMinder 사용자 디렉터리에 연결하려는 경우에는 SiteMinder 사용자 디렉터리 연결 개체의 이름을 정책 서버 사용자 인터페이스에 표시된 대로 지정합니다.

JDBC Data Source JNDI Name(JDBC 데이터 원본 JNDI 이름)(관계형 디렉터리에만 해당)

CA Identity Manager 가 데이터베이스에 연결하는 데 사용하는 기존 JDBC 데이터 원본의 이름을 지정합니다.

Host(호스트) (LDAP 디렉터리에만 해당)

사용자 디렉터리가 설치된 시스템의 IP 주소 또는 호스트 이름을 지정합니다.

CA Directory 사용자 저장소의 경우 호스트 시스템의 전체 도메인 이름을 사용합니다. localhost 를 사용하지 마십시오.

Active Directory 사용자 저장소의 경우 IP 주소가 아니라 도메인 이름을 지정하십시오.

Port(포트) (LDAP 디렉터리에만 해당)

사용자 디렉터리의 포트 번호를 지정합니다.

Provisioning Domain(프로비저닝 도메인)

CA Identity Manager 가 관리하는 프로비저닝 도메인입니다.

참고: 프로비저닝 도메인 이름은 대소문자를 구분합니다.

Username(사용자 이름) / User DN(사용자 DN)

사용자 저장소에 액세스할 수 있는 계정의 사용자 이름을 지정합니다.

프로비저닝 사용자 저장소의 경우 지정하는 사용자 계정에는 도메인 관리자 프로필이 있거나 그에 상응하는 프로비저닝 도메인 권한 세트가 있어야 합니다.

Password(암호)

"Username"(사용자 이름)(관계형 데이터베이스의 경우) 또는 "User DN"(사용자 DN) 필드(LDAP 디렉터리의 경우)에 지정한 사용자 계정의 암호를 지정합니다.

Confirm Password(암호 확인)

확인을 위해 "Password"(암호) 필드에 입력한 암호를 다시 입력합니다.

Secure Connection(보안 연결) (LDAP 디렉터리에만 해당)

CA Identity Manager 가 보안 연결을 사용하는지 여부를 지정합니다.

Active Directory 사용자 저장소의 경우 이 옵션을 선택해야 합니다.

"Next"(다음)를 클릭합니다.

6. CA Identity Manager 디렉터리에 대한 설정을 검토합니다. "Finish"(마침)를 클릭하여 현재 설정으로 CA Identity Manager 디렉터리를 만들거나 "Previous"(이전)를 클릭하여 수정합니다.

   "Directory Configuration Output"(디렉터리 구성 출력) 창에 상태 정보가 표시됩니다.

7. "Continue"(계속)를 클릭하여 종료합니다.

   CA Identity Manager 가 디렉터리를 만듭니다.

프로비져닝 서버 액세스 사용

관리 콘솔에서 "Directories"(디렉터리) 링크를 사용하여 프로비져닝 서버에 대한 액세스가 사용되도록 설정합니다.

참고: 이 절차의 사전 요구 사항은 CA Directory 에 프로비져닝 디렉터리를 설치하는 것입니다. 자세한 내용은 *설치/ 안내서*를 참조하십시오.

다음 단계를 수행하십시오.

1. 브라우저에 다음 URL 을 입력하여 관리 콘솔을 엽니다.

   `http://hostname:port/iam/immanage`

   hostname

   CA Identity Manager 서버가 설치된 시스템의 정규화된 호스트 이름을 정의합니다.

   port

   응용 프로그램 서버 포트 번호를 정의합니다.

2. "Directories"(디렉터리)를 클릭합니다.

   CA Identity Manager 디렉터리 창이 열립니다.

3. "Create from Wizard"(마법사에서 만들기)를 클릭합니다.

4. 프로비져닝 디렉터리를 구성하기 위한 디렉터리 XML 파일의 경로와 파일 이름을 입력합니다. 이 파일은 관리 도구 폴더의 directoryTemplates\ProvisioningServer 에 저장됩니다. 이 폴더의 기본 위치는 다음과 같습니다.

   - Windows: C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools
   - UNIX: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

   참고: 이 디렉터리 구성 파일을 설치된 그대로 수정 없이 사용할 수 있습니다.

5. "Next"(다음)를 클릭합니다.

6. 이 창에서 필드 값을 다음과 같이 제공합니다.

Name(이름)

구성하는 프로비져닝 서버와 연결된 프로비져닝 디렉터리의 이름입니다.

- CA Identity Manager 가 SiteMinder 와 통합되지 않은 경우에는 CA Identity Manager 가 사용자 디렉터리에 연결하는 데 사용하는 개체에 대한 의미 있는 이름을 지정합니다.
- CA Identity Manager 가 SiteMinder 와 통합된 경우에는 두 가지 선택 사항이 있습니다.

  SiteMinder 에서 사용자 디렉터리 연결 개체를 만들려는 경우 의미 있는 이름을 지정합니다. CA Identity Manager 는 지정된 이름으로 SiteMinder 에서 이 개체를 만듭니다.

  기존 SiteMinder 사용자 디렉터리에 연결하려는 경우 SiteMinder 사용자 디렉터리 연결 개체의 이름을 정책 서버 사용자 인터페이스에 표시된 대로 지정합니다.

Description(설명)

(선택 사항) CA Identity Manager 디렉터리를 설명합니다.

Host(호스트)

사용자 디렉터리가 설치된 시스템의 IP 주소 또는 호스트 이름을 지정합니다.

Port(포트)

사용자 디렉터리의 포트 번호를 지정합니다.

Domain(도메인)

CA Identity Manager 가 관리하는 프로비져닝 도메인의 이름을 지정합니다.

중요! 관리 콘솔을 통해 외국어 문자를 도메인 이름으로 사용하여 프로비져닝 디렉터리를 만드는 경우 프로비져닝 디렉터리 만들기가 실패합니다.

설치할 때 지정한 프로비져닝 도메인의 이름과 일치하는 이름을 사용해야 합니다.

참고: 도메인 이름은 대소문자를 구분합니다.

Username(사용자 이름)

프로비져닝 매니저에 로그인할 수 있는 사용자를 지정합니다.

이 사용자에게는 도메인 관리자 프로필이나 그에 상응하는 프로비져닝 도메인 권한 세트가 있어야 합니다.

Password(암호)

"Username"(사용자 이름) 필드에 지정한 전역 사용자의 암호를 지정합니다.

Confirm Password(암호 확인)

확인을 위해 "Password"(암호) 필드에 입력한 암호를 다시 입력합니다.

보안 연결

CA Identity Manager 가 보안 연결을 사용하는지 여부를 지정합니다.

Active Directory 사용자 저장소의 경우 이 옵션을 선택해야 합니다.

Directory Search Parameters(디렉터리 검색 매개 변수)

maxrows 는 사용자 디렉터리를 검색할 때 CA Identity Manager 가 반환할 수 있는 최대 결과 수를 정의합니다. 이 값은 LDAP 디렉터리에서 설정한 제한을 무시합니다. 충돌하는 설정이 적용되는 경우 LDAP 서버는 가장 낮은 설정을 사용합니다.

참고: maxrows 매개 변수는 CA Identity Manager 태스크 화면에 표시되는 결과 수를 제한하지 않습니다. 표시 설정을 구성하려면 CA Identity Manager 사용자 콘솔에서 목록 화면 정의를 수정하십시오. 지침은 *User Console Design Guide*(사용자 콘솔 디자인 안내서)를 참조하십시오.

timeout 은 CA Identity Manager 가 검색을 종료하기 전까지 디렉터리를 검색하는 최대 시간(초)을 결정합니다.

Failover Connections(장애 조치 연결)

대체 프로비저닝 서버로 사용되는 하나 이상의 선택적 시스템에 대한 호스트 이름 및 포트 번호입니다. 여러 서버가 나열된 경우 CA Identity Manager 는 나열된 순서대로 시스템에 액세스하려고 합니다.

기본 프로비저닝 서버가 실패하는 경우 대체 프로비저닝 서버가 사용됩니다. 기본 프로비저닝 서버를 다시 사용할 수 있게 되어도 대체 프로비저닝 서버가 계속 사용됩니다. 기본 프로비저닝 서버를 다시 사용하려면 대체 프로비저닝 서버를 다시 시작하십시오.

7. "Next"(다음)를 클릭합니다.
8. 관리할 개체(사용자, 그룹 등)를 선택합니다.
9. 개체를 필요한 대로 구성한 후 "Show summary deploy directory"(요약 표시 및 디렉터리 배포)를 클릭하고 프로비저닝 디렉터리에 대한 설정을 검토합니다.
10. 다음 동작 중 하나를 클릭합니다.
    a. 수정하려면 "Back"(뒤로)을 클릭합니다.
    b. 나중에 돌아와 배포하려는 경우 "Save"(저장)를 클릭하여 디렉터리 정보를 저장합니다.
    c. 이 절차를 완료하고 프로비저닝을 사용하여 환경 구성 (페이지 267)을 시작하려면 "Finish"(마침)를 클릭합니다.

CA Identity Manager 디렉터리 보기

CA Identity Manager 디렉터리를 보려면 다음 절차를 수행하십시오.

다음 단계를 수행하십시오.

1. CA Identity Manager 관리 콘솔에서 "Directories"(디렉터리)를 클릭합니다.
2. 보려는 CA Identity Manager 디렉터리의 이름을 클릭합니다. "Directory Properties"(디렉터리 속성) 창에 CA Identity Manager 디렉터리 속성이 표시됩니다.

CA Identity Manager Directory Properties(디렉터리 속성)

CA Identity Manager Directory Properties(디렉터리 속성)는 다음과 같습니다.

참고: CA Identity Manager 디렉터리와 연결된 디렉터리 또는 데이터베이스의 유형에 따라 표시되는 속성이 달라집니다.

Name(이름)

CA Identity Manager 디렉터리의 고유 이름을 정의합니다.

Description(설명)

CA Identity Manager 디렉터리에 대한 설명을 제공합니다.

Type(유형)

디렉터리 공급자의 유형을 정의합니다.

Connection Object Name(연결 개체 이름)

CA Identity Manager 디렉터리가 설명하는 사용자 디렉터리의 이름을 표시합니다.

CA Identity Manager 가 SiteMinder 와 통합된 경우 연결 개체 이름은 SiteMinder 사용자 디렉터리 연결의 이름과 일치합니다.

Root Organization(루트 조직) (조직을 포함하는 사용자 저장소의 경우)

사용자 저장소에 대한 진입점을 지정합니다.

LDAP 디렉터리의 경우 루트 조직은 DN 으로 지정됩니다. 관계형 데이터베이스의 경우 루트 조직의 고유 식별자가 표시됩니다.

JDBC Data Source(JDBC 데이터 원본)

CA Identity Manager 가 데이터베이스에 연결하는 데 사용하는 JDBC 데이터 원본의 이름을 지정합니다.

URL

사용자 저장소의 URL 또는 IP 주소를 제공합니다.

Username(사용자 이름)

사용자 저장소에 액세스할 수 있는 계정의 사용자 이름을 지정합니다.

Search Maximum Rows(최대 검색 행 수)

검색 결과로 반환된 행의 최대 수를 나타냅니다.

Search Page Size(검색 페이지 크기)

단일 검색에서 반환될 수 있는 개체 수를 지정합니다. 개체 수가 페이지 크기를 초과하는 경우 다중 검색이 수행됩니다.

참고: CA Identity Manager 가 관리하는 사용자 저장소에서 페이지 단위 처리를 지원해야 합니다. 일부 사용자 저장소 유형의 경우 페이지 단위 처리를 지원하려면 추가 구성이 필요할 수 있습니다. 자세한 내용은 *구성 안내서*를 참조하십시오.

Supports Paging(페이지 단위 처리 지원)

디렉터리가 페이지 단위 처리를 지원함을 나타냅니다.

Search Timeout(검색 시간 만료)(LDAP 디렉터리에만 해당)

CA Identity Manager 가 검색을 종료하기 전까지 사용자 저장소를 검색하는 최대 시간(초)을 지정합니다.

Provisioning Domain(프로비저닝 도메인)(프로비저닝 서버 디렉터리에만 해당)

CA Identity Manager 가 관리하는 프로비저닝 도메인입니다.

CA Identity Manager Directory Properties(디렉터리 속성) 창

CA Identity Manager 디렉터리에 대한 일반 정보가 선택하는 디렉터리의 속성 창에 표시됩니다. "Directory Properties"(디렉터리 속성) 창은 다음 섹션으로 분류됩니다.

Directory Properties(디렉터리 속성)

CA Identity Manager 디렉터리(환경에 대해 프로비저닝이 사용되도록 설정한 경우 연결된 프로비저닝 도메인도 포함)에 대한 기본 속성을 표시합니다.

Managed Objects(관리 개체) (페이지 242)

CA Identity Manager 가 관리하는 사용자 저장소 개체의 유형에 대한 설명을 제공합니다.

Validation Rule Sets(유효성 검사 규칙 세트) (페이지 248)

CA Identity Manager 디렉터리에 적용되는 유효성 검사 규칙 세트를 나열합니다.

Environments(환경)

CA Identity Manager 디렉터리와 연결된 환경을 나열합니다. 하나의 디렉터리를 여러 CA Identity Manager 환경과 연결할 수 있습니다.

CA Identity Manager 환경에 대한 자세한 내용을 보려면 환경 이름을 클릭합니다.

CA Identity Manager 디렉터리에서 속성을 수정하려면 CA Identity Manager 디렉터리 업데이트 (페이지 252)에 설명된 대로 디렉터리 구성 파일을 가져옵니다.

속성을 보는 것 외에도 다음 작업을 수행할 수 있습니다.

Update Authentication(인증 업데이트)

관리자가 CA Identity Manager 에서 관리 콘솔 관리자를 인증하는 데 사용하는 디렉터리를 변경할 수 있습니다. 또한 관리자는 기존 인증 디렉터리에서 관리 콘솔 관리자를 추가할 수도 있습니다.

참고: "Update Authentication"(인증 업데이트) 옵션은 네이티브 CA Identity Manager 보안으로 관리 콘솔이 보호되는 경우에만 적용됩니다. 네이티브 보안이 사용되도록 설정하거나 다른 보안 방법을 사용하는 방법에 대한 자세한 내용은 *구성 안내서*를 참조하십시오.

Export(내보내기) (페이지 251)

디렉터리 정의를 XML 파일로 내보냅니다. 디렉터리 설정을 내보낸 후 XML 파일을 수정한 다음 다시 가져와 디렉터리를 업데이트할 수 있습니다. XML 파일을 다른 디렉터리로 가져와 해당 디렉터리 설정을 동일하게 구성할 수도 있습니다.

Update(업데이트) (페이지 252)

관리자가 개체의 특성과 같은 관리 개체 정의를 추가 또는 변경하고, 검색 매개 변수를 설정하고, 디렉터리 속성을 변경할 수 있습니다.

관리 개체 속성 및 특성을 보는 방법

관리 개체는 사용자 저장소에 있는 항목의 유형(사용자, 그룹, 조직 등)을 설명합니다. 관리 개체에 적용되는 속성 및 특성은 해당 유형의 모든 항목에 적용됩니다. 예를 들어 사용자 프로필은 사용자 관리 개체의 모든 속성 및 특성으로 구성됩니다.

관리 개체에 대한 정보를 보려면 개체 이름을 클릭하여 "Managed Object Properties"(관리 개체 속성) 창을 엽니다.

Managed Object Properties(관리 개체 속성)

"Managed Object Properties"(관리 개체 속성) 창에서는 관리 개체 유형에 대한 속성 및 특성을 설명합니다.

관리하려는 사용자 저장소 유형에 따라 "Managed Object Properties"(관리 개체 속성) 창에 대한 정보가 달라집니다. 개체의 관리 속성은 다음과 같습니다.

Description(설명)

관리 개체에 대한 설명을 제공합니다.

Type(유형)

관리 개체가 나타내는 항목의 유형을 표시합니다. 개체 유형은 다음 유형 중 하나일 수 있습니다.

- User(사용자)
- Group(그룹)
- Organization(조직)

Object Class(개체 클래스) (LDAP 디렉터리에만 해당)

관리 개체의 개체 클래스를 지정합니다. 관리 개체에는 여러 개체 클래스가 있을 수 있습니다.

Sort Order(정렬 순서) (LDAP 디렉터리에만 해당)

CA Identity Manager 가 사용자 지정 비즈니스 로직에서 검색 결과를 정렬하는 데 사용하는 특성을 지정합니다. 정렬 순서는 사용자 콘솔의 검색 결과 순서에는 영향을 미치지 않습니다.

예를 들어 사용자 개체에 대해 cn 특성을 지정하면 CA Identity Manager 가 cn 특성을 기반으로 사용자 검색 결과를 사전순으로 정렬합니다.

Primary Table(기본 테이블) (관계형 데이터베이스에만 해당)

관리 개체의 고유 식별자를 포함하는 테이블을 지정합니다.

Maximum Rows(최대 행 수)

이 유형의 개체를 검색할 때 CA Identity Manager 가 반환할 수 있는 최대 결과 수를 지정합니다. 결과 수가 이 제한을 초과하면 오류가 표시됩니다.

최대 행 수 설정은 검색 결과를 제한하는 LDAP 디렉터리의 설정을 무시할 수 있습니다. 충돌하는 설정이 적용되는 경우 LDAP 서버는 가장 낮은 설정을 사용합니다.

Page size(페이지 크기)

단일 검색에서 반환될 수 있는 개체 수를 지정합니다. 개체 수가 페이지 크기를 초과하는 경우 다중 검색이 수행됩니다.

참고: CA Identity Manager 가 관리하는 사용자 저장소에서 페이지 단위 처리를 지원해야 합니다. 일부 사용자 저장소 유형의 경우 페이지 단위 처리를 지원하려면 추가 구성이 필요할 수 있습니다. 자세한 내용은 *구성 안내서*를 참조하십시오.

Container Properties(컨테이너 속성)(LDAP 디렉터리에만 해당)

LDAP 디렉터리에서 *컨테이너* 그룹에는 특정 유형의 개체가 포함됩니다. 컨테이너를 지정하는 경우 CA Identity Manager 는 컨테이너의 항목만 처리합니다. 예를 들어 컨테이너 ou=People 을 지정하는 경우 CA Identity Manager 는 People 컨테이너에 있는 사용자만 처리합니다.

참고: LDAP 디렉터리에는 있지만 정의된 컨테이너에는 없는 사용자 및 그룹이 사용자 콘솔에 표시될 수 있습니다. 이러한 사용자 및 그룹을 관리할 경우 문제가 발생할 수 있습니다.

컨테이너에서는 사용자 및 그룹만 그룹화합니다. 조직의 컨테이너는 지정할 수 없습니다.

컨테이너 속성은 다음과 같습니다.

objectclass

특정 유형의 개체가 만들어지는 컨테이너의 LDAP 개체 클래스를 지정합니다. 예를 들어 사용자 컨테이너의 기본값은 "top,organizationalUnit"인데, 이는 사용자가 LDAP 조직 단위(ou)에 만들어짐을 나타냅니다.

ID

컨테이너 이름을 저장하는 특성(예: ou)을 지정합니다. 다음 예제와 같이 특성은 이름 값과 쌍으로 연결되어 컨테이너의 상대 DN 을 형성합니다.

ou=People

Name(이름)

컨테이너 이름을 지정합니다.

Secondary Table Properties(보조 테이블 속성) (관계형 데이터베이스에만 해당)

보조 테이블에는 관리 개체에 대한 추가 특성이 포함됩니다. 예를 들어 tblUserAddress 라는 보조 테이블에는 사용자 관리 개체의 상세 주소, 구/군/시, 시/도 및 우편 번호가 포함될 수 있습니다.

보조 테이블에는 다음 속성이 표시됩니다.

Table(테이블)

테이블의 이름을 지정합니다.

Reference(참조)

기본 테이블과 보조 테이블 간의 매핑을 설명합니다.

참조는 다음 형식을 사용하여 표시됩니다.

primarytable.attribute=secondarytable.attribute

예를 들어 tblUsers.id = tblUserAddress.userid 는 기본 테이블 tblUsers 의 id 특성이 tblUserAddress 테이블의 userid 특성에 매핑됨을 나타냅니다.

Managed Object Properties(관리 개체 속성) 창의 Attribute Properties(특성 속성)

"Managed Object Properties"(관리 개체 속성) 창의 특성에는 다음 속성이 표시됩니다.

Display Name(표시 이름)

사용자에게 친숙한 특성 이름입니다. 이 이름은 사용자 콘솔에서 특정 태스크의 태스크 창을 설계할 때 사용 가능한 특성 목록에 표시됩니다.

Physical Name(물리적 이름)

사용자 저장소에 있는 특성의 이름입니다.

Well-Known Name(Well-Known 이름)

Well-Known 이름은 CA Identity Manager 에서 특별한 의미를 갖는 특성(예: 사용자 암호를 저장하는 데 사용되는 특성)을 나타냅니다.

Attribute Properties(특성 속성) 창의 특성 속성

특성 이름을 클릭하여 "Attribute Properties"(특성 속성) 창을 열면 특성에 대한 추가 정보를 볼 수 있습니다.

"Attribute Properties"(특성 속성) 창에는 다음과 같은 특성 속성이 표시됩니다.

Description(설명)

특성에 대한 설명을 제공합니다.

Physical Name(물리적 이름)

사용자 저장소에 있는 특성의 이름을 지정합니다.

Object Class(개체 클래스)(LDAP 디렉터리의 사용자, 그룹 및 조직 특성에만 해당)

특성이 사용자 개체에 대해 지정된 기본 개체 클래스의 일부가 아닌 경우 사용자 특성에 대한 LDAP 보조 클래스입니다.

사용자 및 그룹 개체에 대해서만 보조 개체 클래스를 지정할 수 있습니다.

Well-Known Name(Well-Known 이름)

CA Identity Manager 에서 특별한 의미를 갖는 특성(예: 사용자 암호를 저장하는 데 사용되는 특성)을 나타냅니다.

Required(필수)

다음과 같이 특성에 값이 필요한지 여부를 나타냅니다.

- True 이면 특성에 값이 있어야 합니다.
- False 이면 값이 선택 사항임을 나타냅니다.

Read Only(읽기 전용)

다음과 같이 특성에 대한 권한 수준을 나타냅니다.

- True 이면 특성을 수정할 수 없습니다.
- False 이면 특성을 수정할 수 있습니다.

Hidden(숨김)

특정 태스크의 태스크 창에 특성을 표시할 수 있는지 여부를 나타냅니다.

숨겨진 특성은 종종 논리 특성 체계에서 사용됩니다.

참고: 자세한 내용은 *Programming Guide for Java*(Java 프로그래밍 안내서)를 참조하십시오.

Supports Multiple Values(다중 값 지원)

다음과 같이 특성에 여러 값을 사용할지 있는지 여부를 나타냅니다. 예를 들어 그룹 구성원을 저장하는 데 사용되는 특성은 다중 값을 가질 수 있습니다.

- True 이면 특성은 여러 값을 지원할 수 있습니다.
- False 이면 특성은 단일 값만 가질 수 있습니다.

Multiple Value Delimiter(다중 값 구분 기호) (관계형 데이터베이스에만 해당)

하나의 열에 여러 값을 저장할 때 값을 구분하는 문자입니다.

System Attribute(시스템 특성)

특성이 CA Identity Manager 에서만 사용되지는 여부를 다음과 같이 나타냅니다.

- True 이면 특성이 시스템 특성입니다. 즉, 특성을 태스크 창에 추가할 수 없습니다.
- False 이면 사용자가 이 이 특성을 사용할 수 있습니다. 즉, 특성이 태스크 창에 표시될 수 있습니다.

Data Type(데이터 형식)

특성의 데이터 형식을 지정합니다. 기본값은 "String"(문자열)입니다.

Maximum Length(최대 길이)

특성 값의 최대 길이를 지정합니다. 0 으로 설정하는 경우 값의 길이에 제한이 없습니다.

Validation Rule Set(유효성 검사 규칙 세트)

특성이 유효성 검사 규칙 세트와 연결된 경우 유효성 검사 규칙 세트의 이름을 지정합니다.

Validation Rule Sets(유효성 검사 규칙 세트)

유효성 검사 규칙은 사용자가 태스크 창 필드에 입력하는 데이터에 대한 요구 사항을 적용합니다. 요구 사항에 따라 데이터 유형 또는 형식을 적용하거나 태스크 창에 있는 다른 데이터의 컨텍스트에서 데이터가 올바른지 확인할 수 있습니다.

하나 이상의 유효성 검사 규칙이 유효성 검사 규칙 세트로 그룹화됩니다. 그런 다음 유효성 검사 규칙 세트가 프로필 특성과 연결됩니다. 예를 들어 yyyy-mm-dd 의 날짜 형식을 적용하는 날짜 형식 유효성 검사 규칙이 포함된 유효성 검사 규칙 세트를 만들 수 있습니다. 그런 다음 이 유효성 검사 규칙 세트를 직원의 시작 날짜를 저장하는 특성과 연결할 수 있습니다.

참고: 유효성 검사 규칙 및 규칙 세트는 디렉터리 구성 파일이나 사용자 콘솔에서 만듭니다.

"Managed Object Properties"(관리 개체 속성) 창에는 CA Identity Manager 디렉터리에 적용되는 유효성 검사 규칙 세트 목록이 표시됩니다. 유효성 검사 규칙 세트에 대한 상세 정보를 보려면 규칙 세트 이름을 클릭하여 "Validation Rule Set Properties"(유효성 검사 규칙 세트 속성) 창을 엽니다.

Validation Rule Properties(유효성 검사 규칙 속성)

"Validation Rule Properties"(유효성 검사 규칙 속성) 창에는 다음 정보가 표시됩니다.

Name(이름)

유효성 검사 규칙의 이름을 제공합니다.

Description(설명)

규칙에 대한 설명을 제공합니다.

Class(클래스)

유효성 검사 규칙을 구현하는 Java 클래스의 이름을 제공합니다.

유효성 검사 규칙을 Java 클래스로 정의하지 않은 경우 이 필드가 표시되지 않습니다.

Filename(파일 이름)

유효성 검사 규칙의 JavaScript 구현이 포함된 파일의 이름을 제공합니다.

유효성 검사 규칙을 파일에 정의하지 않은 경우 이 필드가 표시되지 않습니다.

Regular Expression(정규식)

유효성 검사 규칙을 구현하는 정규식을 제공합니다.

유효성 검사 규칙을 정규식으로 정의하지 않은 경우 이 필드가 표시되지 않습니다.

"Validation Rule Set Properties"(유효성 검사 규칙 세트 속성)

"Validation Rule Set Properties"(유효성 검사 규칙 세트 속성) 창에는 다음 정보가 표시됩니다.

Name(이름)

유효성 검사 규칙 세트의 이름을 지정합니다.

Description(설명)

유효성 검사 규칙 세트에 대한 설명을 제공합니다.

"Validation Rule Set Properties"(유효성 검사 규칙 세트 속성) 창에는 세트의 유효성 검사 규칙 목록도 포함되어 있습니다. 유효성 검사 규칙의 이름을 클릭하여 "Validation Rule Properties"(유효성 검사 규칙 속성) 창을 열 수 있습니다.

CA Identity Manager 디렉터리에 대한 설정을 업데이트하는 방법

CA Identity Manager 디렉터리에 대한 현재 설정을 보려면 디렉터리 설정을 내보내 XML 파일로 저장합니다.

디렉터리 설정을 내보낸 후에는 XML 파일을 수정한 다음 다시 가져와 디렉터리를 업데이트할 수 있습니다. XML 파일을 다른 디렉터리로 가져와 해당 디렉터리 설정을 동일하게 구성할 수도 있습니다.

CA Identity Manager 디렉터리 내보내기

CA Identity Manager 디렉터리를 내보내려면 다음 절차를 수행하십시오.

다음 단계를 수행하십시오.

1. "Directories"(디렉터리)를 클릭합니다.

   CA Identity Manager 디렉터리 목록이 표시됩니다.

2. 내보낼 CA Identity Manager 디렉터리의 이름을 클릭합니다.

   CA Identity Manager 디렉터리에 대한 속성 창이 나타납니다.

3. 속성 창의 맨 아래에서 "Export"(내보내기)를 클릭합니다.

4. 요청을 받으면 XML 파일을 저장합니다.

CA Identity Manager 디렉터리 업데이트

CA Identity Manager 디렉터리를 업데이트하는 목적은 다음과 같습니다.

- 개체의 특성을 비롯한 관리 개체 정의 추가 또는 변경
- 검색 매개 변수 설정
- 디렉터리 속성 변경

참고: CA Identity Manager 는 개체 또는 특성 정의를 삭제하지 않습니다.

디렉터리 구성 파일에는 변경할 내용만 포함할 수 있습니다. 이미 정의한 속성 또는 특성은 포함하지 않아도 됩니다.

참고: CA Identity Manager 노드의 클러스터가 있는 경우 관리 콘솔에서 변경할 때 하나의 CA Identity Manager 노드만 사용되도록 설정할 수 있습니다. CA Identity Manager 디렉터리를 만들거나 수정하기 전에 CA Identity Manager 노드를 하나만 제외하고 모두 중지합니다.

다음 단계를 수행하십시오.

1. 현재 CA Identity Manager 디렉터리 설정을 XML 파일로 내보냅니다.
2. XML 파일을 수정하여 변경 내용을 반영합니다.
3. "Directories"(디렉터리)를 클릭합니다.

   CA Identity Manager 디렉터리 목록이 표시됩니다.
4. 업데이트할 CA Identity Manager 디렉터리의 이름을 클릭합니다.

   CA Identity Manager 디렉터리에 대한 속성이 나타납니다.
5. 속성 창의 아래쪽에서 "Update"(업데이트)를 클릭합니다.

6. CA Identity Manager 디렉터리를 업데이트하기 위한 XML 파일의 경로와 파일 이름을 입력하거나 파일을 찾습니다. "Finish"(마침)를 클릭합니다.

   상태 정보는 "Directory Configuration Output"(디렉터리 구성 출력)에 표시됩니다.

7. "Continue"(계속)를 클릭합니다.

CA Identity Manager 디렉터리 삭제

CA Identity Manager 디렉터리를 삭제하려면 먼저 이 디렉터리와 연결된 CA Identity Manager 환경을 삭제합니다.

다음 단계를 수행하십시오.

1. 관리 콘솔에서 "Directories"(디렉터리)를 클릭합니다.

   CA Identity Manager 디렉터리 목록이 표시됩니다.

2. 삭제할 디렉터리 왼쪽의 확인란을 선택합니다.
3. "Delete"(삭제)를 클릭합니다.

   확인 메시지가 나타납니다.

4. "OK"(확인)를 클릭하여 삭제를 확인합니다.

제 6 장: CA Identity Manager 환경

이 섹션은 다음 항목을 포함하고 있습니다.

CA Identity Manager 환경

CA Identity Manager 환경은 사용자 저장소의 뷰입니다. CA Identity Manager 환경에서 사용자, 그룹, 조직, 태스크 및 역할을 관리할 수 있습니다. 또한 사용자에게 전자 메일 계정이나 기타 응용 프로그램과 같은 관리되는 끝점의 계정을 부여할 수 있습니다.

관리 콘솔을 사용하여 다음과 같은 태스크를 수행할 수 있습니다.

- CA Identity Manager 환경 만들기, 수정 또는 삭제
- CA Identity Manager 환경 내보내기 및 가져오기
- 고급 설정 구성

- 역할 및 태스크 가져오기
- 시스템 매니저 계정 다시 설정

CA Identity Manager 환경을 만들기 위한 사전 요구 사항

시작하기 전에 다음 표의 워크시트를 사용하여 필요한 정보를 수집하십시오.

CA Identity Manager 환경 구성 워크시트	
필요한 정보	**값**
직접 선택하는 의미 있는 CA Identity Manager 환경 이름 예: MyEnvironment	
CA Identity Manager 가 해당 환경의 기본 암호 정책에 대한 리디렉션 URL 을 구성하는 데 사용하는 기본 URL 예: http://server.yourcompany.org	
해당 환경에서 보호된 태스크에 액세스하기 위한 URL 에 추가할 별칭 예: http://server.yourcompany.org/iam/im/alias	

CA Identity Manager 환경 구성 워크시트	
필요한 정보	**값**
자체 등록 및 잊어버린 암호 태스크 같은 공용 태스크에 액세스하기 위한 URL 에 추가할 별칭 예: http://server.yourcompany.org/iam/im/public_alias/index.jsp?task.tag=SelfRegistration **참고:** 해당 환경에 공용 태스크가 없을 경우 공용 별칭을 지정할 필요가 없습니다.	
공용 별칭을 제공했을 경우 공용 사용자 역할을 하는 기존 사용자의 이름. CA Identity Manager 는 공용 태스크에 액세스할 때 사용자 제공 자격 증명 대신 공용 사용자의 자격 증명을 사용합니다.	
CA Identity Manager (페이지 139)의 이름	
CA Identity Manager 환경이 프로비저닝을 지원하는 경우 프로비저닝 디렉터리의 이름	
CA Identity Manager 환경을 관리하는 기존 사용자의 고유 식별자 예: myadmin	

CA Identity Manager 환경 구성 워크시트	
필요한 정보	**값**
CA Identity Manager 가 SiteMinder 와 통합되는 경우 CA Identity Manager 환경을 보호하는 SiteMinder 에이전트 또는 에이전트 그룹의 이름	

CA Identity Manager 환경 만들기

CA Identity Manager 환경에서는 일련의 역할 및 태스크와 함께 디렉터리의 개체를 관리할 수 있습니다. CA Identity Manager 환경 마법사는 CA Identity Manager 환경을 만드는 단계를 안내합니다.

CA Identity Manager 환경을 만들기 전에 다음 사항에 주의하십시오.

- LDAP 사용자 저장소를 사용하고 있고 CA Identity Manager 디렉터리에 대한 디렉터리 구성 파일(directory.xml)에 사용자 컨테이너(예: ou=People)를 구성했다고 가정합니다. CA Identity Manager 환경을 만들 때 선택하는 사용자가 이 컨테이너에 있는지 확인합니다. 사용자 컨테이너에 없는 사용자 계정을 선택하면 오류가 발생할 수 있습니다.
- 비계층적 구조 또는 비계층적 사용자 구조의 LDAP 사용자 디렉터리를 관리하기 위해 CA Identity Manager 환경을 구성하는 경우 선택한 사용자의 프로필에 해당 사용자의 조직이 포함되어야 합니다. 사용자 프로필을 올바르게 구성하기 위해서는 사용자의 조직 이름을 directory.xml 파일 (페이지 117)의 %ORG_MEMBERSHIP% Well-Known 특성에 해당하는 물리적 특성에 추가합니다. 예를 들어 물리적 특성 설명이 directory.xml 파일의 %ORG_MEMBERSHIP% Well-Known 특성에 매핑되어 있고 사용자가 "Employees" 조직에 속하는 경우 사용자의 프로필에 특성/값 쌍 description=Employees 가 포함되어야 합니다.

다음 단계를 수행하십시오.

1. CA Identity Manager 가 정책 서버 클러스터를 사용하는 경우 하나만 제외하고 정책 서버를 모두 중지합니다.
2. CA Identity Manager 노드 클러스터가 있을 경우 CA Identity Manager 노드 하나만 제외하고 모두 중지합니다.
3. 관리 콘솔에서 "Environments"(환경)를 클릭합니다.
4. "New"(새로 만들기)를 클릭합니다.

   CA Identity Manager 환경 마법사가 열립니다.
5. 다음 정보를 제공합니다.

   - **Environment name(환경 이름)**

     환경에 대한 고유 이름을 지정합니다.

   - **Description(설명)**

     환경에 대해 설명합니다.

   - **Protected alias(보호 별칭)**

     "employees" 같은 고유 이름을 지정합니다. 이 별칭은 CA Identity Manager 환경에서 보호된 태스크에 액세스하기 위한 URL 에 추가됩니다. 예를 들어 별칭이 employees 일 경우 직원 환경에 액세스하기 위한 URL 은 http://my*server.mycompany.com*/iam/im/employees 가 됩니다.

     참고: 이 별칭은 대소문자를 구분하며 공백을 포함할 수 없습니다. 이 별칭을 지정할 때 문장 부호나 공백 없이 소문자를 사용하는 것이 좋습니다.

- **Base URL(기본 URL)**

  CA Identity Manager 에 대한 URL 을 지정합니다. URL 에는 호스트 이름이 필요하며 localhost 를 포함할 수 없습니다. 또한 별칭(예: http://*myserver.mycompany.com*/iam/im)을 포함하지 마십시오.

  웹 에이전트를 사용하는 경우 웹 에이전트의 URL 을 반영하도록 기본 URL 을 변경해야 합니다.

  참고: 웹 에이전트를 사용하여 CA Identity Manager 리소스를 보호하는 경우 "Base URL"(기본 URL) 필드에 포트 번호를 지정하지 마십시오. 웹 에이전트를 사용하는데 기본 URL 에 포트 번호를 포함하면 CA Identity Manager 태스크에 대한 링크가 올바로 작동하지 않습니다.

  CA Identity Manager 리소스 보호에 대한 자세한 내용은 해당 응용 프로그램 서버의 *설치/ 안내서*를 참조하십시오.

  "Next"(다음)를 클릭합니다.

6. 만들려는 환경과 연결할 CA Identity Manager 디렉터리를 선택하고 "Next"(다음)를 클릭합니다.
7. CA Identity Manager 환경에서 프로비져닝을 지원할 경우 사용할 적절한 프로비져닝 서버를 선택합니다.

   참고: CA Identity Manager 디렉터리로 프로비져닝 디렉터리를 선택한 경우에는 프로비져닝 서버를 선택하라는 메시지가 표시되지 않습니다.

8. 공용 태스크에 대한 지원을 구성합니다. 일반적으로 공용 태스크는 자체 등록 또는 잊어버린 암호 태스크와 같은 자체 서비스 태스크입니다. 사용자가 공용 태스크에 액세스하기 위해 로그인할 필요가 없습니다.

   참고: 사용자가 자체 서비스 태스크를 사용하도록 하려면 공용 태스크 지원을 구성하십시오.

   a. 공용 태스크에 액세스하기 위한 URL 에 추가할 고유 이름을 지정합니다.

      예: 다음 URL 을 사용하여 기본 자체 등록 태스크에 액세스할 수 있습니다.

      http://*myserver.mycompany.com*/iam/im/*alias*/index.jsp?task.tag=SelfRegistration

      이 URL 에서 *alias* 는 직접 제공하는 고유 이름입니다.

   b. 공용 사용자 계정 역할을 하는 다음의 기존 사용자 계정 중 하나를 지정합니다. CA Identity Manager 는 이 계정을 사용하여 알 수 없는 사용자가 자격 증명을 제공하지 않고도 공용 태스크에 액세스할 수 있도록 허용합니다.

      - LDAP 사용자는 공용 사용자 계정의 상대 DN 또는 고유 식별자를 입력합니다. 이 값이 %USER_ID% well-known (페이지 107)에 매핑되는지 확인합니다. 예를 들어 사용자 DN 의 상대 DN 이 uid=Admin1, ou=People, ou=Employees, ou=NeteAuto 일 경우 Admin1 을 입력합니다.
      - 관계형 데이터베이스 사용자는 디렉터리 구성 파일의 %USER_ID% Well-Known 특성에 매핑되는 값이나 해당 사용자의 고유 식별자를 입력합니다.

   "Validate"(유효성 검사)를 클릭하여 사용자의 전체 식별자를 확인합니다.

9. 이 환경에 대해 만들 태스크 및 역할을 선택합니다. 다음과 같은 태스크를 수행할 수 있습니다.

   - **Create default roles(기본 역할 만들기)**

     해당 환경에서 처음에 사용할 수 있는 일련의 기본 태스크와 역할을 만듭니다. 관리자는 사용자 콘솔에서 이러한 태스크와 역할을 템플릿으로 사용하여 새로운 태스크와 역할을 만들 수 있습니다.

   - **Create only the system manager role(시스템 매니저 역할만 만들기)**

     시스템 매니저 역할 및 이 역할과 관련된 태스크만 만듭니다.

     시스템 매니저 역할은 해당 환경에 액세스하는 데 필요합니다.

     시스템 매니저는 사용자 콘솔에서 새로운 태스크와 역할을 만들 수 있습니다.

   - **Import roles from the file(파일에서 역할 가져오기)**

     다른 CA Identity Manager 환경에서 내보낸 역할 정의 파일을 가져옵니다.

     참고: CA Identity Manager 환경을 사용하려면 역할 정의 파일에 적어도 시스템 매니저 역할 또는 유사한 태스크를 포함하는 역할이 있어야 합니다.

     "Import roles from the file"(파일에서 역할 가져오기) 옵션 단추를 선택하고 역할 정의 파일의 경로와 파일 이름을 입력하거나 가져올 파일을 찾습니다.

10. 역할 정의 파일을 선택하여 해당 환경에서 사용할 일련의 기본 태스크를 만들고 "Next"(다음)를 클릭합니다.

    역할 정의 파일은 특정 기능을 지원하기 위해 필요한 여러 가지 태스크와 역할을 정의하는 XML 파일입니다. 예를 들어 Active Directory 및 UNIX NIS 끝점을 관리하려는 경우 이러한 역할 정의 파일을 선택합니다.

    참고: 이 단계는 선택 사항입니다. 새 기능을 지원하기 위해 기본 태스크를 추가로 만들지 않으려는 경우 이 화면을 건너뛰십시오.

11. 다음과 같이 이 환경의 시스템 매니저 역할을 할 사용자를 정의합니다.

    a. "System Manager"(시스템 매니저) 필드에 디렉터리 구성 파일의 %USER_ID% Well-Known 특성에 매핑되는 값을 입력하거나 다음 사용자 계정 중 하나를 지정합니다.

       - LDAP 사용자는 사용자의 상대 DN 또는 고유 식별자를 입력합니다. 예를 들어 사용자 DN 의 상대 DN 이 uid=Admin1, ou=People, ou=Employees, ou=NeteAuto 일 경우 Admin1 을 입력합니다.
       - 관계형 데이터베이스 사용자는 사용자의 고유 식별자를 입력합니다.

b. "Add"(추가)를 클릭합니다.

사용자의 전체 식별자가 사용자 목록에 추가됩니다.

c. "Next"(다음)를 클릭합니다.

시스템 매니저를 지정하는 경우 다음 사항에 주의하십시오.

- 시스템 매니저는 사용자 저장소의 관리자와 동일한 사용자가 *아니어야* 합니다.
- 해당 환경에 대해 여러 시스템 매니저를 지정할 수 있습니다. 그러나 관리 콘솔에서는 최초 시스템 매니저만 지정할 수 있습니다. 시스템 매니저를 추가로 지정하려면 사용자 콘솔에서 시스템 매니저 역할을 해당 사용자에 할당하십시오.

12. "Inbound Administrator"(인바운드 관리자) 필드에서 인바운드 매핑에 매핑되는 관리 태스크를 실행할 수 있는 CA Identity Manager 관리자 계정을 지정합니다.

이 사용자는 모든 사용자에 대해 이러한 모든 태스크를 실행할 수 있어야 합니다. "Provisioning Synchronization Manager"(프로비저닝 동기화 매니저) 역할은 기본 인바운드 매핑에 있는 프로비저닝 태스크를 포함합니다.

13. 데이터를 암호화 및 암호 해독하는 키의 데이터베이스인 키 저장소의 암호를 입력합니다.

    동적 키를 정의하려면 먼저 이 암호를 정의해야 합니다. 환경을 만든 이후 "System"(시스템), "Secret Keys"(암호 키) 태스크를 사용하여 암호를 수정할 수 있습니다.

    환경에 대한 설정을 요약하는 페이지가 표시됩니다.

14. 환경 관련 설정을 검토합니다. "Previous"(이전)를 클릭하고 수정하거나 "Finish"(마침)를 클릭하여 현재 설정으로 CA Identity Manager 환경을 만듭니다.

    "Environment Configuration Output"(환경 구성 출력) 화면에 환경 만들기 진행 상황이 표시됩니다.

15. "Continue"(계속)를 클릭하여 CA Identity Manager 환경 마법사를 종료합니다.

16. 환경을 시작합니다.

    환경 이름을 클릭한 후 "Start"(시작)를 클릭합니다.

17. 1 단계에서 정책 서버를 중지했을 경우 지금 다시 시작합니다.

CA Identity Manager 환경에 액세스하는 방법

CA Identity Manager 환경을 만든 후에는 브라우저에서 URL 을 입력하여 액세스할 수 있습니다.

참고: 관리 콘솔에 액세스하는 데 사용할 브라우저에서 Javascript 가 사용되도록 설정해야 합니다.

URL 형식은 환경을 구성한 방식과 액세스할 태스크의 유형에 따라 달라집니다.

- 사용자 콘솔에서 보호되는 태스크에 액세스하려면 다음 URL 을 사용해야 합니다.

  `http://`*`hostname`*`/iam/im/`*`alias`*

  hostname

  CA Identity Manager 가 설치된 서버의 정규화된 도메인 이름(예: myserver.mycompany.com)을 정의합니다.

  alias

  환경의 별칭(예: employees)을 정의합니다.

  CA Identity Manager 환경에 대해 만든 시스템 매니저 계정과 같은 권한 있는 관리자 계정을 사용하여 CA Identity Manager 환경에 로그인합니다.

  참고: 공용 태스크를 구성하는 경우를 제외하고 모든 CA Identity Manager 태스크는 보호됩니다.

- 사용자가 자격 증명을 제공할 필요가 없는 공용 태스크에 액세스하려면 다음과 같은 형식으로 URL 을 사용해야 합니다.

  `http://`*`hostname`*`/iam/im/`*`alias`*`/index.jsp?task.tag=`*`tasktag`*

  hostname

  CA Identity Manager 가 설치된 서버의 정규화된 도메인 이름(예: myserver.mycompany.com)을 정의합니다.

alias

공용 태스크의 별칭(예: self-service)을 정의합니다.

task_tag

호출할 태스크의 태그를 정의합니다.

사용자 콘솔에서 태스크를 구성할 때 태스크 태그를 지정합니다.

기본 자체 등록 태스크와 잊어버린 암호 다시 설정 태스크의 태스크 태그는 각각 SelfRegistration 및 ForgottenPasswordReset 입니다.

참고: 자세한 내용은 *관리 안내서*를 참조하십시오.

프로비져닝을 위해 환경을 구성하는 방법

프로비져닝 서버에 액세스할 수 있도록 설정 (페이지 232)한 후에는 프로비져닝을 위해 환경을 구성할 수 있습니다.

그런 다음 인바운드 관리자라는 특별한 CA Identity Manager 사용자를 만들고 프로비져닝 서버에 대한 연결을 설정하고 프로비져닝 매니저에서 인바운드 동기화를 구성합니다.

참고: 환경에 대한 프로비져닝 속성을 수정할 때마다 항상 응용 프로그램 서버를 다시 시작해야만 변경 사항이 적용됩니다.

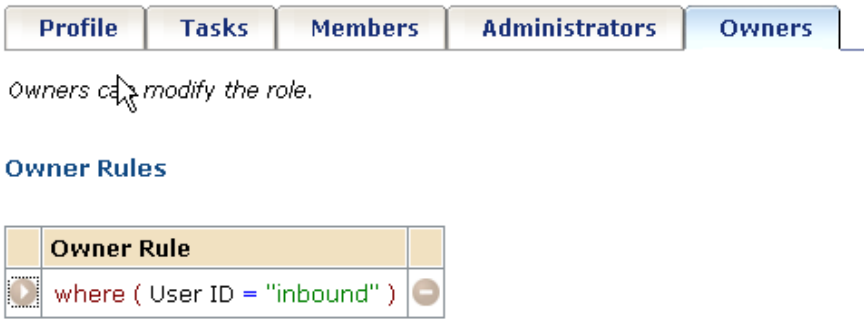
인바운드 관리자 구성

인바운드 동기화가 작동하려면 *인바운드 관리자*라는 특수한 CA Identity Manager 사용자를 만들어야 합니다. 이전 CA Identity Manager 릴리스에서는 인바운드 관리자를 *회사 사용자*라고 했습니다. 이 사용자 계정은 아무도 로그인하지 않고 CA Identity Manager 가 내부적으로 사용합니다. 하지만 이 사용자 계정을 만들고 적절한 태스크를 부여해야 합니다.

다음 단계를 수행하십시오.

1. 시스템 매니저 역할이 부여된 사용자로 CA Identity Manager 환경에 로그인합니다.
2. 사용자를 만듭니다. 용도를 상기시키기 위해 사용자의 이름을 **inbound** 로 지정할 수도 있습니다.
3. "관리자 역할", "관리자 역할 수정"을 선택하고 동기화에 사용할 태스크를 포함하는 역할을 선택합니다.
   - 프로비져닝 사용자 만들기
   - Provisioning Enable/Disable User(프로비져닝 사용자 활성화/비활성화)
   - 프로비져닝 사용자 수정

   참고: 기본 동기화 태스크를 수정하지 않은 경우에는 프로비져닝 동기화 매니저 역할을 사용하십시오.
4. "구성원" 탭에서 다음을 포함하는 구성원 정책을 추가합니다.
   - 새 사용자가 충족시키는 구성원 규칙
   - 인바운드 동기화를 유발하는 프로비져닝 디렉터리 변경 사항의 영향을 받는 모든 사용자에게 액세스를 제공하는 범위 규칙



5. 관리 콘솔에서 다음을 수행하십시오.

   a. "Environment"(환경)를 선택합니다.

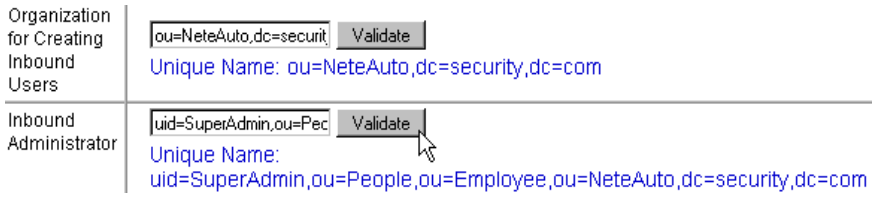
   b. "Advanced Settings"(고급 설정), "Provisioning"(프로비져닝)을 차례로 선택합니다.

   c. CA Identity Manager 디렉터리에 조직이 포함될 경우 "Organization for Creating Inbound Users"(인바운드 사용자를 만들기 위한 조직) 필드를 완성합니다.

      이 조직은 인바운드 동기화가 수행될 때 사용자가 만들어지는 위치입니다. 예를 들어 사용자를 프로비져닝 디렉터리에 추가하면 사용자가 이 조직에 추가됩니다.

   d. "Inbound Administrator"(인바운드 관리자) 필드를 2 단계에서 만든 사용자의 사용자 ID 로 채웁니다.

   e. "Validate"(유효성 검사)를 클릭하여 사용자 ID 가 허용되는지 확인합니다. 즉, 아래의 예제에 표시된 것과 같이 입력한 사용자 ID 아래에 완전한 사용자 ID 가 표시되는지 확인하십시오.



   f. 이 화면의 다른 필드를 수정합니다. 변경이 반드시 필요하지는 않습니다.

      수정할 경우 필드의 상호 작용 방식을 이해해야 합니다. 각 필드에 대한 자세한 내용을 보려면 화면에서 "Help"(도움말) 링크를 클릭하십시오.

프로비져닝 서버에 환경 연결

다음 단계를 수행하십시오.

1. 관리 콘솔에서 "Environments"(환경)를 클릭합니다.

   기존 환경 목록이 나타납니다.

2. 프로비져닝 서버에 연결할 환경의 이름을 클릭합니다.

3. "Provisioning Server"(프로비져닝 서버) 필드에서 오른쪽 화살표 아이콘을 클릭합니다.

   "Provisioning Properties"(프로비져닝 속성) 화면이 열립니다.

4. 프로비져닝 서버를 선택합니다.

5. 화면의 아래에서 "Save"(저장)를 클릭합니다.

6. 프로비져닝 매니저에서 동기화를 구성합니다 (페이지 270).

프로비져닝 매니저에서 동기화 구성

인바운드 동기화는 프로비져닝 디렉터리에서 발생한 변경 내용을 적용하여 CA Identity Manager 를 최신 상태로 유지하는 기능입니다. 변경 내용으로는 프로비져닝 매니저를 사용하여 수행된 변경 내용과 프로비져닝 서버의 커넥터가 연결되는 끝점의 변경 내용이 있습니다. 각각의 프로비져닝 서버는 단일 환경을 지원합니다. 하지만 현재 환경을 사용할 수 없을 경우에 대비하여 클러스터의 여러 시스템에 백업 환경을 구성할 수 있습니다.

다음 단계를 수행하십시오.

1. "시작", "CA Identity Manager", "Provisioning Manager"(프로비져닝 매니저)를 선택합니다.
2. "시스템", "CA Identity Manager Setup"(CA Identity Manager 설정)을 클릭합니다.
3. "호스트 이름" 필드를 CA Identity Manager 서버가 설치된 시스템의 이름으로 채웁니다.
4. "포트" 필드를 응용 프로그램 서버 포트 번호로 채웁니다.
5. "Environment name"(환경 이름) 필드를 환경의 별칭으로 채웁니다.
6. HTTP 를 사용하고 개별 알림을 암호화하는 대신 HTTPS 프로토콜을 사용하여 CA Identity Manager 서버와 통신하려면 "보안된 연결"을 선택합니다.
7. "추가"를 클릭합니다.
8. 각 백업 버전 환경에 대해 3~6 단계를 반복합니다.

   현재 환경의 응용 프로그램 서버를 사용할 수 없을 경우 백업 환경으로 장애 조치됩니다. 현재 및 백업 환경의 순서를 다시 지정하여 장애 조치 순서를 설정할 수 있습니다.
9. 첫 번째 환경일 경우 포함된 구성 요소의 사용자에 대해 CA Identity Manager 를 설치할 때 입력한 암호를 사용하여 "공유 암호" 필드를 채웁니다.

   참고: 이 설치 환경에서 FIPS 가 사용되도록 설정한 경우 이러한 필드가 적용되지 않습니다.

10. 다음과 같이 "Log Level"(로그 수준)을 설정합니다.
    - No Log(로그 없음) - 정보가 로그 파일에 기록되지 않습니다.
    - 오류 - 오류 메시지만 기록됩니다.
    - 정보 - 오류 및 정보 메시지가 기록됩니다(기본값).
    - 경고 - 오류, 경고 및 정보 메시지가 기록됩니다.
    - 디버그 - 모든 정보가 기록됩니다.
11. 환경에 로그인하기 전에 응용 프로그램 서버를 다시 시작합니다.

참고: 인바운드 동기화 오퍼레이션 및 동기화 중 발생한 문제에 대한 로그는 다음 파일을 참조하십시오.

PSHOME\logs\etanotify<date>.log

사용자 지정 프로비져닝 역할 가져오기

환경을 만들 때 기본 역할을 사용할 수도 있고 직접 만든 사용자 지정 역할 정의 파일을 사용할 수도 있습니다. 사용자 지정 역할 정의를 가져올 경우 "프로비져닝 전용" 역할 정의도 가져와야 합니다. 환경을 만든 후 다음 폴더 중 하나에 위치한 ProvisioningOnly-RoleDefinitions.xml 파일에서 역할 정의를 가져옵니다.

admin_tools/ProvisioningOnlyRoleDefinitions/Organization
admin_tools/ProvisioningOnlyRoleDefinitions/NoOrganization

admin_tools 의 기본 위치는 다음과 같습니다.

- **Windows**: C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools
- **UNIX**: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

사용자 암호 재설정 작업을 위해 계정 동기화

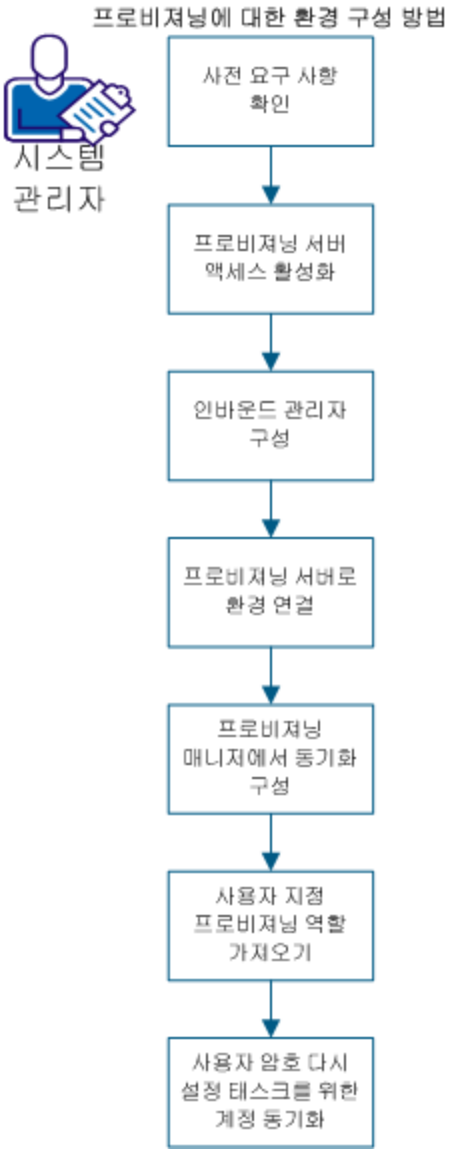
CA Identity Manager 환경에서 프로비저닝을 활성화하려면 사용자 프로비저닝을 위한 역할과 작업을 만드는 ProvisioningOnly-RoleDefinitions.xml 이라는 구성 파일을 가져옵니다.

이 파일에서는 "사용자 암호 재설정" 작업에 대한 기본 계정 동기화 설정이 "끄기"로 설정되어 있습니다. 프로비저닝을 활성화하려면 먼저 동기화 설정을 "작업 완료시"로 설정합니다.

"사용자 암호 재설정"을 사용하여 계정 동기화를 트리거하려면 ProvisioningOnly-RoleDefinitions.xml 을 가져와 계정 동기화 옵션을 설정하여 프로비저닝을 활성화합니다.

Connector Xpress 를 사용하여 연결을 생성 및 배포하는 방법

다른 시스템의 계정을 CA Identity Manager 에 의해 관리되는 사용자에게 제공하기 위해 환경에 대한 프로비저닝을 구성할 수 있습니다. 계정이 있는 사용자는 전자 메일 계정과 같은 추가 리소스에 액세스할 수 있습니다. 이러한 추가 계정은 CA Identity Manager 를 통해 만드는 프로비저닝 역할을 할당하여 제공합니다.



관리자로서 다음 단계를 수행하십시오.

1. 사전 요구 사항 확인 (페이지 275)
2. 프로비져닝 서버 액세스 사용 (페이지 232)
3. 인바운드 관리자 구성 (페이지 267)
4. 프로비져닝 서버에 환경 연결 (페이지 270)
5. 프로비져닝 매니저에서 동기화 구성 (페이지 270)
6. 사용자 지정 프로비져닝 역할 가져오기 (페이지 272)
7. 사용자 암호 다시 설정 태스크를 위한 계정 동기화 (페이지 273)

사전 요구 사항 확인

프로비져닝을 위한 환경을 구성하기 전에 CA Directory 에 프로비져닝 디렉터리가 설치되어 있는지 확인하십시오. 자세한 내용은 *설치/ 안내서*를 참조하십시오.

프로비져닝 서버 액세스 사용

관리 콘솔에서 "Directories"(디렉터리) 링크를 사용하여 프로비져닝 서버에 대한 액세스가 사용되도록 설정합니다.

참고: 이 절차의 사전 요구 사항은 CA Directory 에 프로비져닝 디렉터리를 설치하는 것입니다. 자세한 내용은 *설치/ 안내서*를 참조하십시오.

다음 단계를 수행하십시오.

1. 브라우저에 다음 URL 을 입력하여 관리 콘솔을 엽니다.

   `http://hostname:port/iam/immanage`

   hostname

   CA Identity Manager 서버가 설치된 시스템의 정규화된 호스트 이름을 정의합니다.

   port

   응용 프로그램 서버 포트 번호를 정의합니다.

2. "Directories"(디렉터리)를 클릭합니다.

   CA Identity Manager 디렉터리 창이 열립니다.

3. "Create from Wizard"(마법사에서 만들기)를 클릭합니다.

4. 프로비져닝 디렉터리를 구성하기 위한 디렉터리 XML 파일의 경로와 파일 이름을 입력합니다. 이 파일은 관리 도구 폴더의 directoryTemplates\ProvisioningServer 에 저장됩니다. 이 폴더의 기본 위치는 다음과 같습니다.

   - Windows: C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools
   - UNIX: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

   참고: 이 디렉터리 구성 파일을 설치된 그대로 수정 없이 사용할 수 있습니다.

5. "Next"(다음)를 클릭합니다.

6. 이 창에서 필드 값을 다음과 같이 제공합니다.

Name(이름)

구성하는 프로비저닝 서버와 연결된 프로비저닝 디렉터리의 이름입니다.

- CA Identity Manager 가 SiteMinder 와 통합되지 않은 경우에는 CA Identity Manager 가 사용자 디렉터리에 연결하는 데 사용하는 개체에 대한 의미 있는 이름을 지정합니다.
- CA Identity Manager 가 SiteMinder 와 통합된 경우에는 두 가지 선택 사항이 있습니다.

  SiteMinder 에서 사용자 디렉터리 연결 개체를 만들려는 경우 의미 있는 이름을 지정합니다. CA Identity Manager 는 지정된 이름으로 SiteMinder 에서 이 개체를 만듭니다.

  기존 SiteMinder 사용자 디렉터리에 연결하려는 경우 SiteMinder 사용자 디렉터리 연결 개체의 이름을 정책 서버 사용자 인터페이스에 표시된 대로 지정합니다.

Description(설명)

(선택 사항) CA Identity Manager 디렉터리를 설명합니다.

Host(호스트)

사용자 디렉터리가 설치된 시스템의 IP 주소 또는 호스트 이름을 지정합니다.

Port(포트)

사용자 디렉터리의 포트 번호를 지정합니다.

Domain(도메인)

CA Identity Manager 가 관리하는 프로비져닝 도메인의 이름을 지정합니다.

중요! 관리 콘솔을 통해 외국어 문자를 도메인 이름으로 사용하여 프로비져닝 디렉터리를 만드는 경우 프로비져닝 디렉터리 만들기가 실패합니다.

설치할 때 지정한 프로비져닝 도메인의 이름과 일치하는 이름을 사용해야 합니다.

참고: 도메인 이름은 대소문자를 구분합니다.

Username(사용자 이름)

프로비져닝 매니저에 로그인할 수 있는 사용자를 지정합니다.

이 사용자에게는 도메인 관리자 프로필이나 그에 상응하는 프로비져닝 도메인 권한 세트가 있어야 합니다.

Password(암호)

"Username"(사용자 이름) 필드에 지정한 전역 사용자의 암호를 지정합니다.

Confirm Password(암호 확인)

확인을 위해 "Password"(암호) 필드에 입력한 암호를 다시 입력합니다.

보안 연결

CA Identity Manager 가 보안 연결을 사용하는지 여부를 지정합니다.

Active Directory 사용자 저장소의 경우 이 옵션을 선택해야 합니다.

Directory Search Parameters(디렉터리 검색 매개 변수)

maxrows 는 사용자 디렉터리를 검색할 때 CA Identity Manager 가 반환할 수 있는 최대 결과 수를 정의합니다. 이 값은 LDAP 디렉터리에서 설정한 제한을 무시합니다. 충돌하는 설정이 적용되는 경우 LDAP 서버는 가장 낮은 설정을 사용합니다.

참고: maxrows 매개 변수는 CA Identity Manager 태스크 화면에 표시되는 결과 수를 제한하지 않습니다. 표시 설정을 구성하려면 CA Identity Manager 사용자 콘솔에서 목록 화면 정의를 수정하십시오. 지침은 *User Console Design Guide*(사용자 콘솔 디자인 안내서)를 참조하십시오.

timeout 은 CA Identity Manager 가 검색을 종료하기 전까지 디렉터리를 검색하는 최대 시간(초)을 결정합니다.

Failover Connections(장애 조치 연결)

대체 프로비져닝 서버로 사용되는 하나 이상의 선택적 시스템에 대한 호스트 이름 및 포트 번호입니다. 여러 서버가 나열된 경우 CA Identity Manager 는 나열된 순서대로 시스템에 액세스하려고 합니다.

기본 프로비져닝 서버가 실패하는 경우 대체 프로비져닝 서버가 사용됩니다. 기본 프로비져닝 서버를 다시 사용할 수 있게 되어도 대체 프로비져닝 서버가 계속 사용됩니다. 기본 프로비져닝 서버를 다시 사용하려면 대체 프로비져닝 서버를 다시 시작하십시오.

7. "Next"(다음)를 클릭합니다.
8. 관리할 개체(사용자, 그룹 등)를 선택합니다.
9. 개체를 필요한 대로 구성한 후 "Show summary deploy directory"(요약 표시 및 디렉터리 배포)를 클릭하고 프로비져닝 디렉터리에 대한 설정을 검토합니다.
10. 다음 동작 중 하나를 클릭합니다.
    a. 수정하려면 "Back"(뒤로)을 클릭합니다.
    b. 나중에 돌아와 배포하려는 경우 "Save"(저장)를 클릭하여 디렉터리 정보를 저장합니다.
    c. 이 절차를 완료하고 프로비져닝을 사용하여 환경 구성 (페이지 267)을 시작하려면 "Finish"(마침)를 클릭합니다.

인바운드 관리자 구성

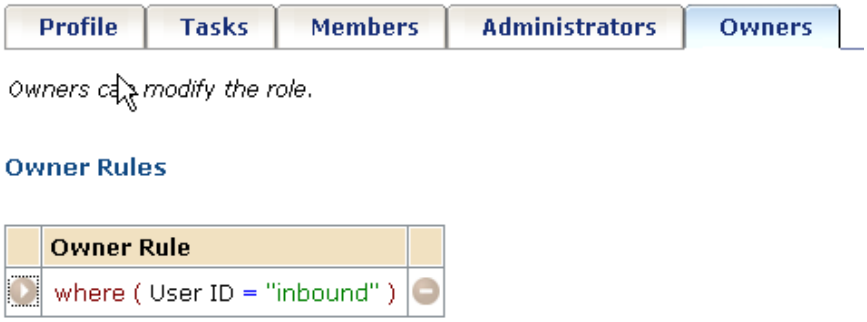
인바운드 동기화가 작동하려면 *인바운드 관리자*라는 특수한 CA Identity Manager 사용자를 만들어야 합니다. 이전 CA Identity Manager 릴리스에서는 인바운드 관리자를 *회사 사용자*라고 했습니다. 이 사용자 계정은 아무도 로그인하지 않고 CA Identity Manager 가 내부적으로 사용합니다. 하지만 이 사용자 계정을 만들고 적절한 태스크를 부여해야 합니다.

다음 단계를 수행하십시오.

1. 시스템 매니저 역할이 부여된 사용자로 CA Identity Manager 환경에 로그인합니다.
2. 사용자를 만듭니다. 용도를 상기시키기 위해 사용자의 이름을 **inbound** 로 지정할 수도 있습니다.
3. "관리자 역할", "관리자 역할 수정"을 선택하고 동기화에 사용할 태스크를 포함하는 역할을 선택합니다.
   - 프로비져닝 사용자 만들기
   - Provisioning Enable/Disable User(프로비져닝 사용자 활성화/비활성화)
   - 프로비져닝 사용자 수정

   참고: 기본 동기화 태스크를 수정하지 않은 경우에는 프로비져닝 동기화 매니저 역할을 사용하십시오.

4. "구성원" 탭에서 다음을 포함하는 구성원 정책을 추가합니다.
   - 새 사용자가 충족시키는 구성원 규칙
   - 인바운드 동기화를 유발하는 프로비져닝 디렉터리 변경 사항의 영향을 받는 모든 사용자에게 액세스를 제공하는 범위 규칙

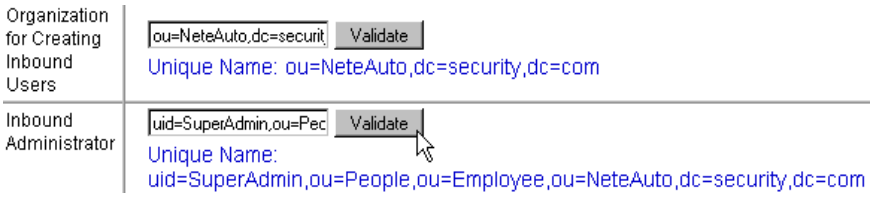


5. 관리 콘솔에서 다음을 수행하십시오.
   a. "Environment"(환경)를 선택합니다.
   b. "Advanced Settings"(고급 설정), "Provisioning"(프로비져닝)을 차례로 선택합니다.
   c. CA Identity Manager 디렉터리에 조직이 포함될 경우 "Organization for Creating Inbound Users"(인바운드 사용자를 만들기 위한 조직) 필드를 완성합니다.

      이 조직은 인바운드 동기화가 수행될 때 사용자가 만들어지는 위치입니다. 예를 들어 사용자를 프로비져닝 디렉터리에 추가하면 사용자가 이 조직에 추가됩니다.

d. "Inbound Administrator"(인바운드 관리자) 필드를 2 단계에서 만든 사용자의 사용자 ID 로 채웁니다.

e. "Validate"(유효성 검사)를 클릭하여 사용자 ID 가 허용되는지 확인합니다. 즉, 아래의 예제에 표시된 것과 같이 입력한 사용자 ID 아래에 완전한 사용자 ID 가 표시되는지 확인하십시오.



f. 이 화면의 다른 필드를 수정합니다. 변경이 반드시 필요하지는 않습니다.

수정할 경우 필드의 상호 작용 방식을 이해해야 합니다. 각 필드에 대한 자세한 내용을 보려면 화면에서 "Help"(도움말) 링크를 클릭하십시오.

프로비져닝 서버에 환경 연결

다음 단계를 수행하십시오.

1. 관리 콘솔에서 "Environments"(환경)를 클릭합니다.

   기존 환경 목록이 나타납니다.

2. 프로비져닝 서버에 연결할 환경의 이름을 클릭합니다.

3. "Provisioning Server"(프로비져닝 서버) 필드에서 오른쪽 화살표 아이콘을 클릭합니다.

   "Provisioning Properties"(프로비져닝 속성) 화면이 열립니다.

4. 프로비져닝 서버를 선택합니다.

5. 화면의 아래에서 "Save"(저장)를 클릭합니다.

6. 프로비져닝 매니저에서 동기화를 구성합니다 (페이지 270).

프로비져닝 매니저에서 동기화 구성

인바운드 동기화는 프로비져닝 디렉터리에서 발생한 변경 내용을 적용하여 CA Identity Manager 를 최신 상태로 유지하는 기능입니다. 변경 내용으로는 프로비져닝 매니저를 사용하여 수행된 변경 내용과 프로비져닝 서버의 커넥터가 연결되는 끝점의 변경 내용이 있습니다. 각각의 프로비져닝 서버는 단일 환경을 지원합니다. 하지만 현재 환경을 사용할 수 없을 경우에 대비하여 클러스터의 여러 시스템에 백업 환경을 구성할 수 있습니다.

다음 단계를 수행하십시오.

1. "시작", "CA Identity Manager", "Provisioning Manager"(프로비져닝 매니저)를 선택합니다.
2. "시스템", "CA Identity Manager Setup"(CA Identity Manager 설정)을 클릭합니다.
3. "호스트 이름" 필드를 CA Identity Manager 서버가 설치된 시스템의 이름으로 채웁니다.

4. "포트" 필드를 응용 프로그램 서버 포트 번호로 채웁니다.
5. "Environment name"(환경 이름) 필드를 환경의 별칭으로 채웁니다.
6. HTTP 를 사용하고 개별 알림을 암호화하는 대신 HTTPS 프로토콜을 사용하여 CA Identity Manager 서버와 통신하려면 "보안된 연결"을 선택합니다.
7. "추가"를 클릭합니다.
8. 각 백업 버전 환경에 대해 3~6 단계를 반복합니다.

   현재 환경의 응용 프로그램 서버를 사용할 수 없을 경우 백업 환경으로 장애 조치됩니다. 현재 및 백업 환경의 순서를 다시 지정하여 장애 조치 순서를 설정할 수 있습니다.
9. 첫 번째 환경일 경우 포함된 구성 요소의 사용자에 대해 CA Identity Manager 를 설치할 때 입력한 암호를 사용하여 "공유 암호" 필드를 채웁니다.

   참고: 이 설치 환경에서 FIPS 가 사용되도록 설정한 경우 이러한 필드가 적용되지 않습니다.
10. 다음과 같이 "Log Level"(로그 수준)을 설정합니다.
    - No Log(로그 없음) - 정보가 로그 파일에 기록되지 않습니다.
    - 오류 - 오류 메시지만 기록됩니다.
    - 정보 - 오류 및 정보 메시지가 기록됩니다(기본값).
    - 경고 - 오류, 경고 및 정보 메시지가 기록됩니다.
    - 디버그 - 모든 정보가 기록됩니다.
11. 환경에 로그인하기 전에 응용 프로그램 서버를 다시 시작합니다.

참고: 인바운드 동기화 오퍼레이션 및 동기화 중 발생한 문제에 대한 로그는 다음 파일을 참조하십시오.

PSHOME\logs\etanotify<date>.log

사용자 지정 프로비저닝 역할 가져오기

환경을 만들 때 기본 역할을 사용할 수도 있고 직접 만든 사용자 지정 역할 정의 파일을 사용할 수도 있습니다. 사용자 지정 역할 정의를 가져올 경우 "프로비저닝 전용" 역할 정의도 가져와야 합니다. 환경을 만든 후 다음 폴더 중 하나에 위치한 ProvisioningOnly-RoleDefinitions.xml 파일에서 역할 정의를 가져옵니다.

admin_tools/ProvisioningOnlyRoleDefinitions/Organization
admin_tools/ProvisioningOnlyRoleDefinitions/NoOrganization

admin_tools 의 기본 위치는 다음과 같습니다.

- **Windows**: C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools
- **UNIX**: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

사용자 암호 재설정 작업을 위해 계정 동기화

CA Identity Manager 환경에서 프로비저닝을 활성화하려면 사용자 프로비저닝을 위한 역할과 작업을 만드는 ProvisioningOnly-RoleDefinitions.xml 이라는 구성 파일을 가져옵니다.

이 파일에서는 "사용자 암호 재설정" 작업에 대한 기본 계정 동기화 설정이 "끄기"로 설정되어 있습니다. 프로비저닝을 활성화하려면 먼저 동기화 설정을 "작업 완료시"로 설정합니다.

"사용자 암호 재설정"을 사용하여 계정 동기화를 트리거하려면 ProvisioningOnly-RoleDefinitions.xml 을 가져와 계정 동기화 옵션을 설정하여 프로비저닝을 활성화합니다.

환경 관리

이 단원에서는 환경을 관리하는 방법에 대해 설명합니다.

CA Identity Manager 환경 속성 수정

관리 콘솔의 "CA Identity Manager Environment Properties"(환경 속성) 화면에서 다음 태스크를 수행할 수 있습니다.

- 환경의 현재 설정 보기
- 설명, 기본 URL 및 보호 별칭과 공용 별칭 수정
- 업그레이드 후 기존 CA Identity Manager 환경 가져오기

  참고: 기존 CA Identity Manager 환경을 가져오는 방법에 대한 자세한 내용은 *설치 안내서*의 업그레이드 단원을 참조하십시오.
- 환경 시작 및 중지
- 다음 태스크를 구성하기 위한 페이지에 액세스
  - **Advanced Settings(고급 설정)**

    CA Identity Manager API 를 사용하여 구현된 기능을 비롯한 고급 기능을 구성합니다.
  - **Role and Task Settings(역할 및 태스크 설정)**

    다른 CA Identity Manager 환경에서 내보낸 역할 정의 파일을 가져옵니다.
  - **System Manager(시스템 매니저)**

    시스템 매니저 역할을 할당합니다.

다음 단계를 수행하십시오.

1. CA Identity Manager 가 SiteMinder 정책 서버 클러스터를 사용하는 경우 하나만 제외하고 정책 서버를 모두 중지합니다.
2. CA Identity Manager 노드 클러스터가 있을 경우 CA Identity Manager 노드 하나만 제외하고 모두 중지합니다.

3. "Environments"(환경)를 클릭합니다.

   CA Identity Manager 환경 화면이 나타나고 CA Identity Manager 환경 목록이 표시됩니다.

4. 수정할 CA Identity Manager 환경의 이름을 클릭합니다.

   CA Identity Manager 속성 화면이 나타나고 다음 속성이 표시됩니다.

   OID

   환경의 고유 식별자를 정의합니다. CA Identity Manager 환경을 만들면 이 식별자가 생성됩니다.

   태스크 지속 데이터베이스에서 태스크 제거를 구성할 때 OID 를 사용합니다. *설치 안내서*를 참조하십시오.

   Name(이름)

   CA Identity Manager 환경의 고유 이름을 지정합니다.

   Description(설명)

   CA Identity Manager 환경에 대한 설명을 제공합니다.

   CA Identity Manager Directory(CA Identity Manager 디렉터리)

   환경이 연결되는 CA Identity Manager 디렉터리를 지정합니다.

   Enable Verbose Log Output(자세한 로그 출력 사용)

   환경을 가져올 때 CA Identity Manager 가 환경 로그에 기록하고 표시하는 정보의 양을 제어합니다. 환경을 가져오거나 파일에서 다른 개체 정의를 가져오면 관리 콘솔의 상태 창에 환경 로그가 표시됩니다.

   참고: 이 확인란을 선택하면 성능에 큰 영향을 줄 수 있습니다.

   자세한 로그에는 환경의 각 개체(태스크, 화면, 역할 및 정책)와 해당 특성에 대한 유효성 검사 및 배포 메시지가 포함됩니다.

자세한 로그를 보려면 이 확인란을 선택하고 환경 속성을 저장하십시오. 역할을 가져오거나 파일에서 다른 설정을 가져오면 자세한 정보가 로그에 표시됩니다.

Provisioning Server(프로비저닝 서버)

프로비저닝 사용자 저장소로 사용되는 프로비저닝 디렉터리를 지정합니다.

오른쪽 화살표 단추를 클릭하고 "Provisioning Properties"(프로비저닝 속성) 페이지에서 프로비저닝 디렉터리를 구성합니다.

Version(버전)

CA Identity Manager 의 버전 번호를 정의합니다.

Base URL(기본 URL)

환경에 대한 보호 별칭 또는 공용 별칭을 포함하지 않는 CA Identity Manager URL 의 부분을 지정합니다.

CA Identity Manager 는 기본 URL 을 사용하여 환경에 대한 기본 암호 정책의 암호 서비스 태스크를 가리키는 리디렉션 URL 을 구성합니다.

Protected alias(보호 별칭)

CA Identity Manager 환경에 대한 사용자 콘솔에서 보호된 태스크에 액세스하기 위한 기본 URL 이름을 정의합니다.

Public Alias(공용 별칭)

자체 등록 태스크 및 잊어버린 암호 태스크와 같은 공용 태스크에 액세스하기 위한 기본 URL 이름을 정의합니다.

Public User(공용 사용자)

CA Identity Manager 가 공용 태스크에 액세스하기 위해 사용자 제공 자격 증명 대신 사용하는 사용자 계정을 정의합니다.

Job Timeout(작업 시간 만료)

태스크가 제출된 후 상태 메시지를 표시하기 전에 CA Identity Manager 가 대기하는 시간을 지정합니다.

이 값은 "Advanced Settings"(고급 설정)의 "User Console"(사용자 콘솔) 페이지에서 설정합니다.

Status(상태)

CA Identity Manager 환경을 중지 또는 다시 시작합니다.

Migrate Task Persistence Data from CA Identity Manager 8.1(CA Identity Manager 8.1 에서 태스크 지속 데이터 마이그레이션)

CA Identity Manager 8.1 태스크 지속 데이터베이스에서 CA Identity Manager 12.6.5 태스크 지속 데이터베이스로 데이터를 마이그레이션합니다.

자세한 내용은 *설치 안내서*를 참조하십시오.

참고: "Migrate Task Persistence Data from CA Identity Manager 8.1"(CA Identity Manager 8.1 에서 태스크 지속 데이터 마이그레이션) 단추는 이전 버전의 CA Identity Manager 에서 만들고 CA Identity Manager 12.6.5 로 마이그레이션한 환경에서만 표시됩니다.

5. 필요한 경우 설명, 기본 URL, 보호 별칭 또는 공용 별칭을 수정합니다.
6. 환경 속성을 수정한 경우 CA Identity Manager 환경을 다시 시작합니다.
7. 1 단계에서 정책 서버를 중지했을 경우 지금 다시 시작합니다.

환경 설정

환경 관련 정보는 다음 세 개의 환경 설정 파일에 저장됩니다.

- *alias*_environment_roles.xml
- *alias*_environment_settings.xml
- *alias*_environment.xml

참고: *alias* 는 환경의 별칭을 나타냅니다. 환경을 만들 때 별칭을 지정합니다.

환경 설정을 내보낼 때 현재 구성을 반영하는 이 세 파일이 포함된 ZIP 파일을 생성합니다.

환경 설정을 내보낸 후에는 설정을 가져와 다음 태스크 중 하나를 수행할 수 있습니다.

- 유사한 설정으로 여러 환경을 관리합니다. 이 경우 필요한 설정으로 한 환경을 만들고 이 설정을 다른 환경으로 가져온 다음 필요에 따라 각 환경에서 설정을 사용자 지정합니다.
- 개발 환경에서 프로덕션 환경으로 환경을 마이그레이션합니다.
- 새 버전의 CA Identity Manager 로 업그레이드한 후 기존 환경을 업데이트합니다.

CA Identity Manager 환경 내보내기

프로덕션 시스템에서 CA Identity Manager 환경을 배포하려면 개발 또는 준비 시스템에서 환경을 내보내고 프로덕션 시스템으로 가져와야 합니다.

참고: 이전에 내보낸 환경을 가져올 경우 CA Identity Manager 에서 관리 콘솔의 상태 창에 로그를 표시합니다. 이 로그에 있는 각 관리 개체와 해당 특성에 대한 유효성 검사 및 배포 정보를 보려면 환경을 내보내기 *전에* "Environment Properties"(환경 속성) 페이지에서 "Enable Verbose Log Output"(자세한 로그 출력 사용) 필드를 선택하십시오. "Enable Verbose Log Output"(자세한 로그 출력 사용) 필드를 선택하면 가져오기 중에 중대한 성능 문제가 발생할 수 있습니다.

다음 단계를 수행하십시오.

1. 관리 콘솔에서 "Environments"(환경)를 클릭합니다.

   CA Identity Manager 환경 화면이 나타나고 CA Identity Manager 환경 목록이 표시됩니다.

2. 내보낼 환경을 선택합니다.
3. "Export"(내보내기) 단추를 클릭합니다.

   "File Download"(파일 다운로드) 화면이 나타납니다.

4. ZIP 파일을 프로덕션 시스템에서 액세스할 수 있는 위치에 저장합니다.
5. "Finish"(마침)를 클릭합니다.

다른 환경으로 가져올 수 있는 ZIP 파일로 환경 정보를 내보냈습니다.

CA Identity Manager 환경 가져오기

CA Identity Manager 환경 설정을 가져와 다음 태스크 중 하나를 수행할 수 있습니다.

- 유사한 설정으로 여러 환경을 관리합니다. 이 경우 필요한 설정으로 한 환경을 만들고 이 설정을 다른 환경으로 가져온 다음 필요에 따라 각 환경에서 설정을 사용자 지정합니다.
- 개발 환경에서 프로덕션 환경으로 환경을 마이그레이션합니다.
- 새 버전의 CA Identity Manager 로 업그레이드한 후 기존 환경을 업데이트합니다.

다음 단계를 수행하십시오.

1. 관리 콘솔에서 "Environments"(환경)를 클릭합니다.

   CA Identity Manager 환경 화면이 나타나고 CA Identity Manager 환경 목록이 표시됩니다.

2. "Import"(가져오기) 단추를 클릭합니다.

   "Import Environment"(환경 가져오기) 화면이 나타납니다.

3. 환경을 가져오는 데 필요한 ZIP 파일을 찾습니다.
4. "Finish"(마침)를 클릭합니다.

환경을 CA Identity Manager 로 가져왔습니다.

CA Identity Manager 환경 다시 시작

다음 단계를 수행하십시오.

1. 관리 콘솔에서 "Environments"(환경)를 클릭합니다.

   CA Identity Manager 환경 화면이 나타나고 CA Identity Manager 환경 목록이 표시됩니다.

2. 시작할 CA Identity Manager 환경의 이름을 클릭합니다.

   "CA Identity Manager Environment Properties"(환경 속성) 화면이 나타납니다.

3. 다음 옵션 중 하나를 선택합니다.

   Restart Environment(환경 다시 시작)

   환경을 중지했다가 시작합니다.

   Stop(중지)

   현재 실행 중인 환경을 중지합니다.

   Start(시작)

   현재 실행 중이지 않은 환경을 시작합니다.

CA Identity Manager 환경 삭제

CA Identity Manager 환경을 제거하려면 이 절차를 따르십시오.

참고: CA Identity Manager 가 고급 인증을 위해 SiteMinder 와 통합되는 경우 CA Identity Manager 는 환경을 보호하는 SiteMinder 정책 도메인과 환경에 대해 생성된 기본 인증 체계도 삭제합니다.

다음 단계를 수행하십시오.

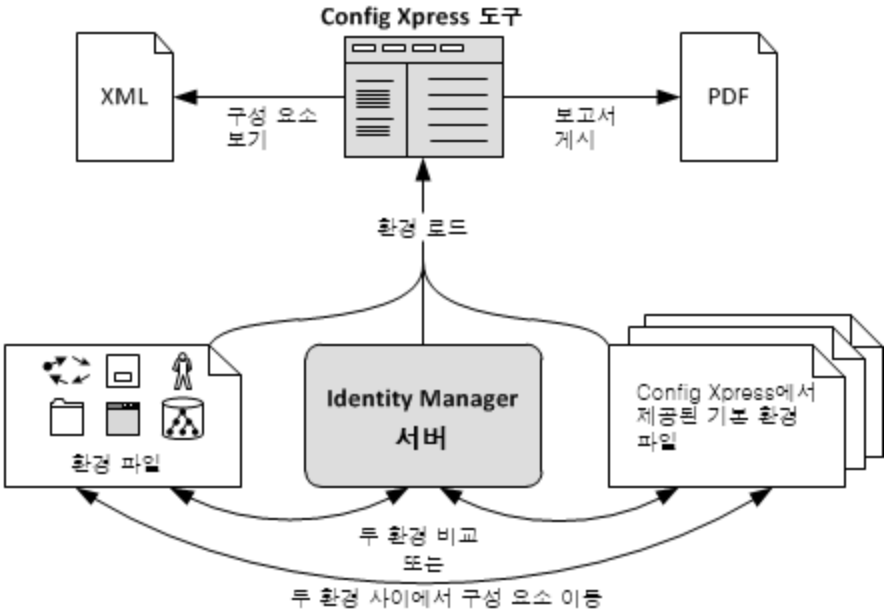
1. "Environments"(환경) 화면에서 삭제할 CA Identity Manager 환경의 확인란을 선택합니다.
2. "Delete"(삭제)를 클릭합니다.

   확인 메시지가 표시됩니다.
3. "OK"(확인)를 클릭하여 삭제를 확인합니다.

구성 관리

Config Xpress 는 CA Identity Manager 에 포함된 도구입니다. 이 도구를 통해 CA Identity Manager 환경의 구성을 분석하고 사용할 수 있습니다.

가장 중요한 것은 이 도구를 통해 환경 간에 구성 요소를 이동할 수 있다는 점입니다. Config Xpress 는 다른 필요한 구성 요소를 자동으로 감지할 뿐 아니라 이러한 요소를 이동하도록 사용자에게 메시지를 표시합니다. 이러한 지원을 통해 수작업이 감소하고 문제 위험이 줄어듭니다.



다음 단계를 수행하십시오.

1. Config Xpress 를 설정합니다 (페이지 298).
2. 이 도구를 사용하려면 먼저 분석을 위해 CA Identity Manager 환경을 (페이지 299) Config Xpress 로 로드합니다.
3. Config Xpress 를 사용하여 로드된 환경으로 다음 태스크를 수행합니다.
   - 환경 간에 구성 요소를 이동할 수 있습니다 (페이지 302).
   - 시스템 구성 요소에 대한 PDF 보고서를 게시할 수 있습니다 (페이지 304).
   - 특정 구성 요소에 대한 XML 구성을 표시할 수 있습니다 (페이지 305).

Config Xpress 설정

Config Xpress 의 설치 파일은 설치 드라이브에 포함되어 있지만 이 도구가 설치되어 있지는 않습니다.

Config Xpress 를 사용하려면 다음 소프트웨어 요구 사항을 충족해야 합니다.

- CA Identity Manager r12.0 이상
- Windows 운영 체제
- Adobe Air Runtime
- 보고서를 보기 위한 PDF Reader

다음 단계를 수행하십시오.

1. Adobe Air Runtime 을 http://get.adobe.com/air 에서 다운로드한 다음 설치합니다.
2. "Administration Tools"(관리 도구)가 설치되었는지 확인합니다.
3. 다음 위치에서 Config Xpress 의 설치 파일을 찾습니다.

   ```
   C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\ConfigXpress
   ```

4. Config Xpress.air 를 실행하여 Config Xpress 를 설치합니다.
5. 설치가 완료되면 Config Xpress 가 시작됩니다.

환경을 Config Xpress 에 로드

Config Xpress 를 사용하려면 먼저 하나 이상의 환경을 이 도구에 로드해야 합니다. 이 태스크를 수행하면 Config Xpress 에서 해당 환경으로 작업할 수 있습니다.

라이브 CA Identity Manager 서버에서 직접 Config Xpress 로 환경을 로드하거나 환경 파일에서 로드할 수 있습니다. Config Xpress 와 함께 설치되는 기본 환경 파일 중 하나를 사용할 경우 이 기본 제공 구성을 기준으로 기존 환경을 비교할 수 있습니다.

환경을 로드하는 프로세스는 몇 분 정도 걸릴 수 있습니다.

다음 단계를 수행하십시오.

1. Config Xpress 를 엽니다.
2. CA Identity Manager 서버에서 직접 **라이브 환경**을 로드하려면 다음을 수행합니다.
   a. "Server (Network)"(서버(네트워크)) 탭을 클릭합니다.
   b. CA Identity Manager 서버의 이름과 포트를 입력합니다. 예:
      `servername.ca.com:8080`
   c. HTTPS 만 허용하도록 서버를 설정하는 경우 "HTTPS 사용"을 선택합니다.
   d. 서버의 버전이 r12.5 SP6 이후일 경우 12.5 SP7 을 선택합니다.
   e. "Connect"(연결)를 클릭합니다.
   f. *Choose Environment to load*(로드할 환경 선택)에서 원하는 환경을 선택하고 "Load"(로드)를 클릭합니다.
3. CA Identity Manager 환경에서 내보낸 **환경 파일**을 로드하려면 다음을 수행합니다.
   a. CA Identity Manager 환경을 내보냅니다.

b. Config Xpress 에서 "File System"(파일 시스템) 탭을 클릭합니다.

c. 해당 버전을 선택하고 환경 파일을 찾은 다음 "Load"(로드)를 클릭합니다.

4. Config Xpress 와 함께 설치된 **기본 환경 파일**을 로드하려면 다음을 수행합니다.

a. "Base Versions"(기본 버전) 탭을 클릭합니다.

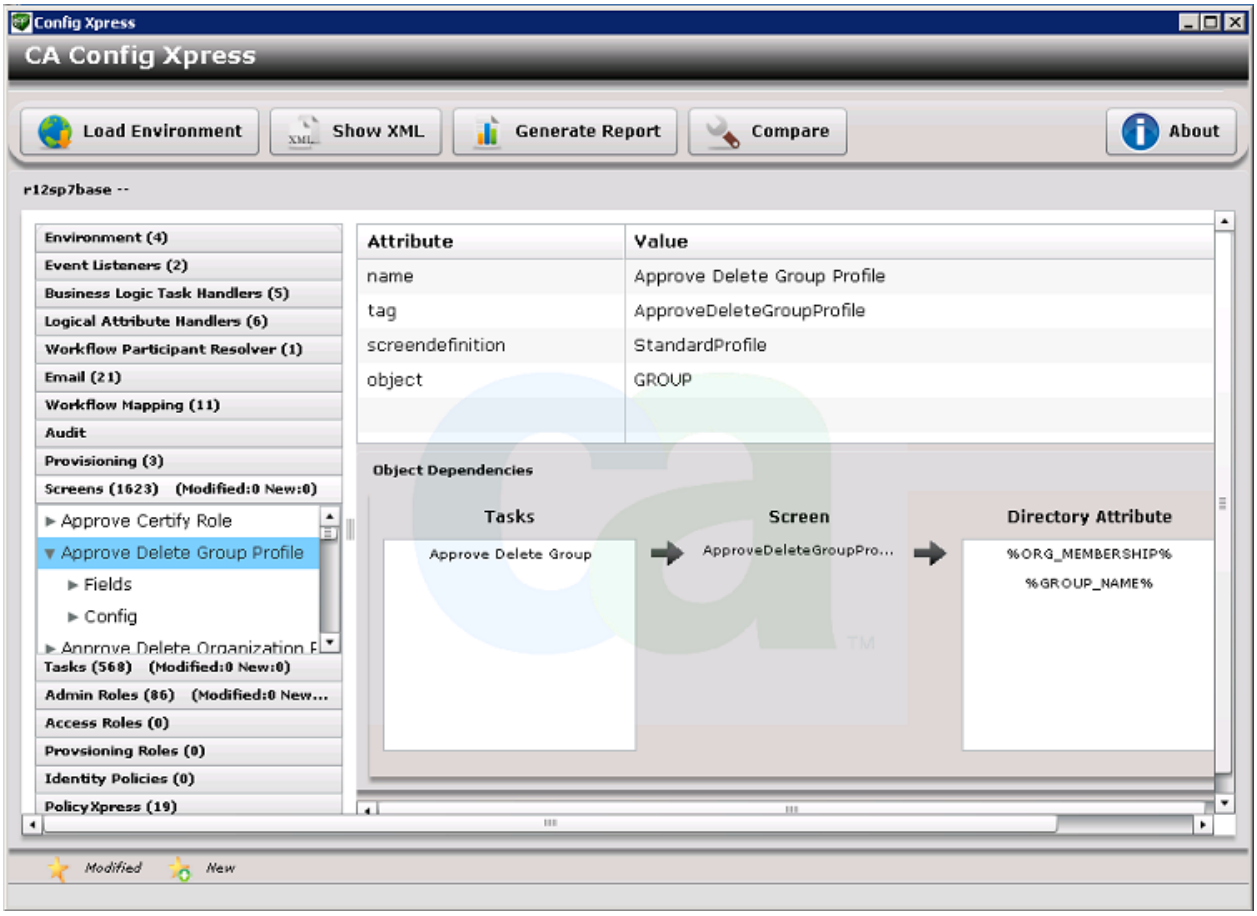
b. 필요한 버전을 선택한 다음 "Select"(선택)를 클릭합니다.

Config Xpress 에서 해당 환경을 분석한 다음 환경 세부 정보를 표시합니다.

이제 환경 일부 또는 전체를 PDF (페이지 304) 또는 XML (페이지 305)로 게시할 수 있습니다. 두 번째 환경을 로드하면 두 환경을 비교하고 두 환경 간에 구성 요소를 이동 (페이지 302)할 수 있습니다.

예: 기본 구성 파일을 로드한 후 Config Xpress

이 스크린샷은 Config Xpress 가 종속 개체를 표시하는 방법을 보여 줍니다.



한 환경에서 다른 환경으로 구성 요소 이동

Config Xpress 를 사용하지 않을 경우 준비 영역 간에 구성 요소를 이동하는 태스크가 복잡해지고 실패하기 쉽습니다.

Config Xpress 를 사용하여 구성 요소를 이동하면 이 도구는 모든 필요한 개체도 함께 이동합니다. 예를 들어 화면이 필요한 태스크를 이동할 경우 Config Xpress 는 필요한 구성 요소도 선택할 것인지 묻는 메시지를 표시합니다. Config Xpress 는 해당 태스크가 이 화면을 사용할 뿐 아니라 대상 환경으로 이동되어야 함을 인식합니다.

구성 요소를 라이브 환경으로 이동하려는 경우 Config Xpress 는 이를 즉시 업로드합니다. 구성 요소를 환경 파일로 이동하려는 경우에는 구성 요소를 XML 파일로 저장한 다음 이 파일을 환경으로 가져와야 합니다.

다음 단계를 수행하십시오.

1. 이동할 구성 요소가 포함된 환경을 로드합니다.
2. 이 환경을 두 번째 환경과 비교합니다.
   a. "Compare"(비교)를 클릭합니다.
   b. 대상 환경을 로드합니다.

      두 환경 간의 차이점 목록이 표시됩니다.
3. 차이점 목록에서 이동할 구성 요소를 찾습니다. "Name"(이름) 열을 클릭하여 목록을 정렬할 수 있습니다.
4. 각 구성 요소에 대해 다음 단계를 수행하십시오.
   a. "Action"(동작) 열에서 항목을 선택합니다.

      Config Xpress 가 구성 요소를 분석합니다. 분석하는 데 어느 정도 시간이 걸릴 수 있습니다.

b. 구성 요소에 종속 구성 요소가 있을 경우 "Add Modified Dependant Screens"(수정된 종속 화면 추가) 상자가 표시됩니다. "Yes"(예) 또는 "No"(아니요)를 클릭하여 계속합니다.

이동할 구성 요소를 모두 선택하고 나면 업데이트된 구성 요소를 이동할 준비가 된 것입니다.

5. 구성 요소를 라이브 서버로 이동하는 경우 "Upload To"(다음으로 업로드)를 클릭합니다.

   구성 요소가 즉시 이동됩니다.

6. 구성 요소를 환경 파일로 이동하려는 경우 다음을 수행합니다.

   a. "Save"(저장)를 클릭합니다.

   b. 파일 이름을 입력하고 "Save"(저장)를 다시 클릭합니다.

      Config Xpress 가 선택된 모든 구성 요소를 XML 파일에 저장합니다. 이제 이 XML 파일을 실제 대상 환경으로 가져올 수 있습니다.

PDF 보고서 게시

Config Xpress 에서 CA Identity Manager 환경의 현재 상태를 설명하는 보고서를 생성할 수 있습니다. 이 보고서를 사용하여 프로덕션 환경에 대한 스냅숏을 생성할 수 있습니다. 보고서를 생성할 때 전체 구성을 포함할지, 아니면 설치 후 변경된 사항만 포함할지를 선택할 수 있습니다.

이 보고서는 이후 참조하는 데 유용할 뿐만 아니라 시스템 복구 계획에도 활용할 수 있습니다.

다음 단계를 수행하십시오.

1. 환경을 Config Xpress 에 로드합니다.
2. "Generate Report"(보고서 생성)를 클릭합니다.

   "Generate PDF Report"(PDF 보고서 생성) 대화 상자에서 글자 크기를 변경할 수 있으며 제목 또는 표지 텍스트를 입력할 수 있습니다. 또한 모든 구성 항목만 포함할지, 아니면 새 항목 또는 수정된 항목만 포함할지를 선택할 수도 있습니다.

   중요! *Only include details of new or modified tasks, screens, roles*(새로 추가되었거나 수정된 태스크, 화면, 역할에 대한 세부 정보만 포함) 상자를 클릭하지 않을 경우 보고서에 전체 환경이 포함됩니다. PDF 파일은 약 2000 페이지로 구성되며 크기가 40 MB 를 넘습니다.
3. "OK"(확인)를 클릭합니다.
4. 파일 이름을 입력하고 보고서를 저장합니다. 저장하는 데 몇 분 정도 걸릴 수 있으며, 전체 환경을 게시하는 경우에는 시간이 더 걸릴 수 있습니다.

   PDF Reader 에서 보고서가 열립니다.

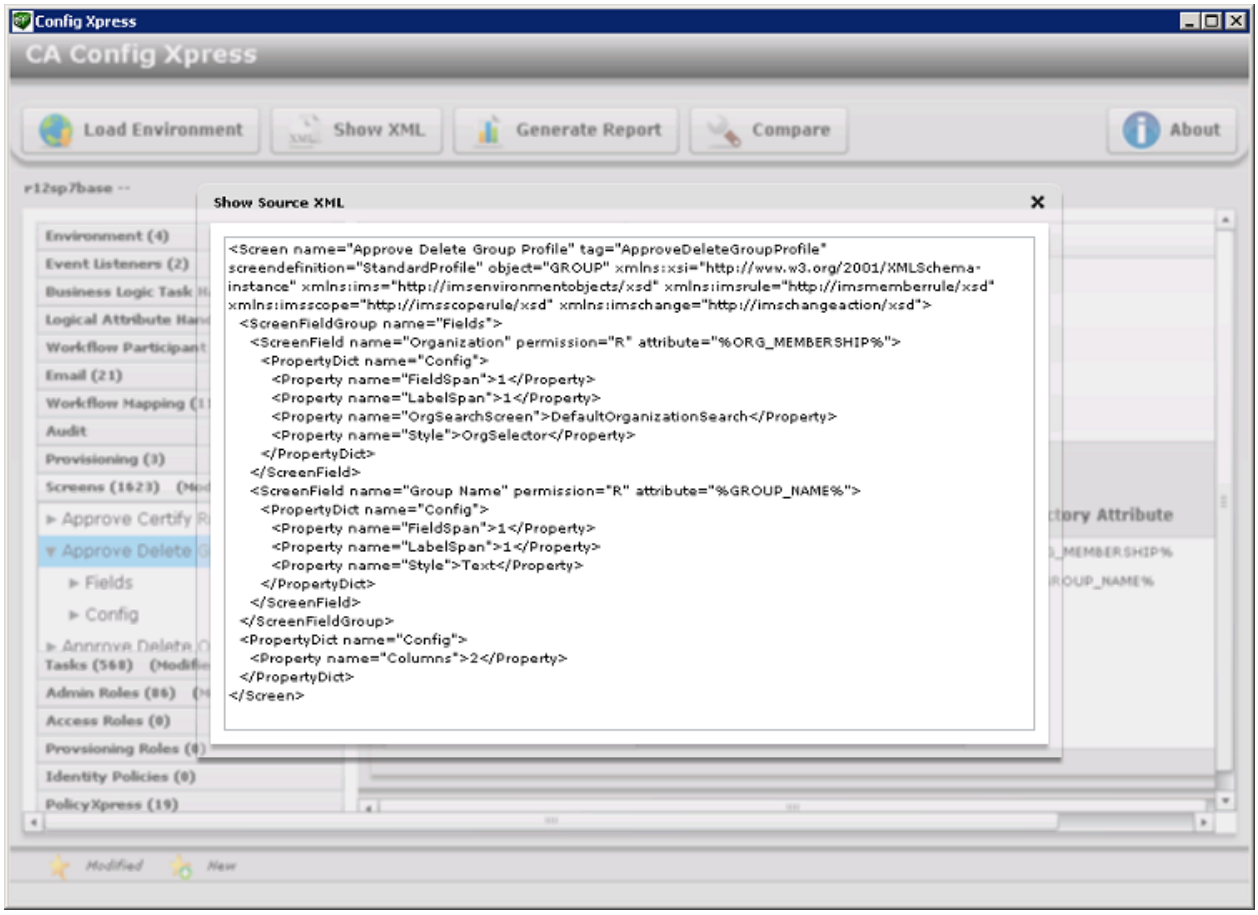
XML 구성 표시

Config Xpress 는 특정 구성 요소에 대한 XML 구성을 표시할 수 있습니다. 이 XML 파일을 검토하면 시스템을 이해하는 데 도움이 됩니다.

다음 단계를 수행하십시오.

1. 환경을 Config Xpress 에 로드합니다.
2. Config Xpress 화면에서 구성 요소를 클릭합니다.
3. "Show XML"(XML 표시)을 클릭합니다.

   XML 구성이 나타납니다.



정책 규칙 평가 최적화

사용자 집합을 동적으로 식별하는 정책 규칙은 역할 구성원, 관리자 및 소유자 정책과 ID 정책의 평가에 사용됩니다. 이러한 규칙의 평가는 대규모 CA Identity Manager 구현 환경에서는 상당히 오래 걸릴 수 있습니다.

참고: 구성원, 관리자, 소유자 및 ID 정책에 대한 자세한 내용은 *관리 안내서*를 참조하십시오.

메모리 내 평가 옵션을 사용하여 사용자 특성이 포함된 규칙에 대한 평가 시간을 줄일 수 있습니다. 메모리 내 평가 옵션이 사용되도록 설정하면 CA Identity Manager 가 평가할 사용자에 대한 정보를 사용자 저장소에서 검색하여 해당 사용자의 표현을 메모리에 저장합니다. CA Identity Manager 에서는 메모리 내 표현을 사용하여 정책 규칙과 특성 값을 비교합니다. 이를 통해 CA Identity Manager 가 사용자 저장소에 대해 직접 실행하는 호출 수가 제한됩니다.

관리 콘솔에서 환경에 대한 메모리 내 평가 옵션이 사용되도록 설정할 수 있습니다.

다음 단계를 수행하십시오.

1. 관리 콘솔을 엽니다.
2. "Environments"(환경), *Environment Name*, "Advanced Settings"(고급 설정), "Miscellaneous"(기타)를 선택합니다.

   "User Defined Properties"(사용자 정의 속성) 페이지가 열립니다.
3. "Property"(속성) 필드에 다음 텍스트를 입력합니다.

   UseInMemoryEvaluation
4. "Value"(값) 필드에 다음 숫자 중 *하나*를 입력합니다.

   0

   메모리 내 평가가 비활성화됩니다.

1

메모리 내 평가가 활성화됩니다. 이 옵션을 지정할 경우 특성 비교는 대소문자를 구분합니다.

3

메모리 내 평가가 활성화됩니다. 이 옵션을 지정할 경우 특성 비교는 대소문자를 구분하지 않습니다.

5. "Add"(추가)를 클릭합니다.

   새 속성이 환경의 기존 속성 목록에 추가됩니다.

6. "Save"(저장)를 클릭합니다.

Role and Task Settings(역할 및 태스크 설정)

관리 콘솔의 "Role and Task Settings"(역할 및 태스크 설정) 화면에서 화면, 탭, 역할 및 태스크 설정을 역할 정의 파일이라고 하는 XML 파일로 가져오거나 내보낼 수 있습니다. CA Identity Manager 는 기능 세트를 위한 화면, 탭, 역할 및 태스크를 만드는 사전 정의된 역할 정의 파일을 제공합니다. 예를 들어 스마트 프로비저닝을 지원하는 역할 정의 파일과 끝점 관리 화면을 지원하는 다른 파일이 있습니다.

또한 역할 정의 파일을 사용하여 특정 환경의 설정을 여러 환경에 적용할 수 있습니다. 다음 단계를 수행하십시오.

- 특정 환경에서 화면, 탭, 태스크 및 역할 설정을 구성합니다.
- 이 설정을 XML 파일로 내보냅니다.
- XML 파일을 필요한 환경으로 가져옵니다.

역할 및 태스크 설정 내보내기

역할 및 태스크 설정을 내보내려면 다음 절차를 수행하십시오.

다음 단계를 수행하십시오.

1. 관리 콘솔에서 "Environments"(환경)를 클릭합니다.

   CA Identity Manager 환경 목록이 나타납니다.

2. 해당 CA Identity Manager 환경의 이름을 클릭합니다.

   해당 환경에 대한 속성 화면이 나타납니다.

3. "Role and Task Settings"(역할 및 태스크 설정)를 클릭하고 "Export"(내보내기)를 클릭합니다.

4. "Open"(열기)을 클릭하여 파일을 브라우저 창에서 표시하거나 "Save"(저장)를 클릭하여 설정을 XML 파일에 저장합니다.

역할 및 태스크 설정 가져오기

역할 및 태스크 설정은 역할 정의 파일이라는 XML 파일에 정의됩니다. 사전 정의된 역할 정의 파일을 가져와서 특정한 CA Identity Manager 기능 집합(예: 스마트 프로비저닝)을 지원하거나, 특정 환경에서 다른 환경으로 역할 정의 파일을 가져올 수 있습니다.

참고: Connector Xpress 를 사용하여 생성된 사용자 지정 커넥터에 대한 역할 정의를 가져올 수도 있습니다. 이러한 역할 정의 파일은 역할 정의 생성기를 사용하여 만듭니다. 자세한 내용은 *Connector Xpress Guide*(Connector Xpress 안내서)를 참조하십시오.

역할 및 태스크 설정을 가져오려면 다음 절차를 수행하십시오.

다음 단계를 수행하십시오.

1. 관리 콘솔에서 "Environments"(환경)를 클릭합니다.

   CA Identity Manager 환경 목록이 나타납니다.

2. 역할 및 태스크 설정을 가져올 CA Identity Manager 환경의 이름을 클릭합니다.

   해당 환경에 대한 속성 화면이 나타납니다.

3. "Role and Task Settings"(역할 및 태스크 설정)를 클릭하고 "Import"(가져오기)를 클릭합니다.

4. 다음 작업 중 하나를 완료하십시오.

   - 하나 이상의 역할 정의 파일을 선택하여 환경의 기본 역할 및 태스크를 만듭니다.

     사용 가능한 역할 정의 파일을 모두 선택하려면 "Select/Deselect All"(모두 선택/선택 취소)을 클릭하십시오.

   - 가져올 역할 정의 파일의 경로와 파일 이름을 입력하거나 파일을 찾습니다. "Finish"(마침)를 클릭합니다.

5. "Finish"(마침)를 클릭합니다.

   "Role Configuration Output"(역할 구성 출력) 창에 상태가 표시됩니다.

6. "Continue"(계속)를 클릭하여 종료합니다.

동적 끝점에 대한 역할 및 태스크를 만드는 방법

Connector Xpress 를 사용하여 SQL 데이터베이스 및 LDAP 디렉터리에 대한 프로비저닝 및 관리를 허용하도록 동적 커넥터를 구성할 수 있습니다. 각 동적 커넥터에 대해 역할 정의 생성기를 사용하여 사용자 콘솔에 나타나는 계정 관리 화면에 대한 태스크 및 화면 정의를 만들 수 있습니다.

역할 정의 생성기를 실행한 후 관리 콘솔에서 생성된 역할 정의 파일을 가져옵니다 (페이지 308).

참고: 역할 정의 생성기에 대한 자세한 내용은 *Connector Xpress Guide*(Connector Xpress 안내서)를 참조하십시오.

시스템 매니저 계정 수정

시스템 매니저는 CA Identity Manager 환경을 설정하고 유지 관리하는 역할을 담당합니다. 일반적으로 시스템 매니저의 태스크는 다음과 같습니다.

- 초기 환경 만들기 및 관리
- 관리자 역할 만들기 및 수정
- 다른 관리자 계정 만들기 및 수정

CA Identity Manager 환경을 만들 때 시스템 매니저 계정을 만듭니다. 시스템 매니저가 암호를 잊어버리는 경우와 같이 이 계정이 "잠기면" System Manager(시스템 매니저) 마법사를 사용하여 계정을 다시 만들 수 있습니다.

System Manager(시스템 매니저) 마법사는 시스템 관리 역할을 사용자에게 할당하는 단계를 안내합니다.

시스템 매니저 계정을 수정하기 전에 다음 사항에 주의하십시오.

- LDAP 사용자 저장소를 사용하고 있고 CA Identity Manager 디렉터리에 대한 디렉터리 구성 파일(directory.xml)에 사용자 컨테이너(예: ou=People)를 구성했는지 확인합니다. 선택한 사용자가 시스템 매니저를 구성하는 동일한 컨테이너에 있어야 합니다. 사용자 컨테이너에 없는 사용자 계정을 선택하면 오류가 발생할 수 있습니다.
- CA Identity Manager 환경에서 비계층적 구조 또는 비계층적 사용자 구조의 사용자 디렉터리를 관리하는 경우 선택한 사용자의 프로필에 해당 조직이 포함되어야 합니다. 사용자 프로필을 올바르게 구성하려면 사용자의 조직 이름을 directory.xml file (페이지 117)의 %ORG_MEMBERSHIP% Well-Known 특성과 일치하는 물리적 특성에 추가하십시오. 예를 들어 물리적 특성 설명이 directory.xml 파일의 %ORG_MEMBERSHIP% Well-Known 특성에 매핑되어 있고 사용자가 "Employees" 조직에 속하는 경우 사용자의 프로필에 특성/값 쌍 description=Employees 가 포함되어야 합니다.

다음 단계를 수행하십시오.

1. CA Identity Manager 환경 화면에서 해당 CA Identity Manager 환경의 이름을 클릭합니다.

   이 특정 환경의 속성 화면이 표시됩니다.

2. "System Manager"(시스템 매니저)를 클릭합니다.

   System Manager(시스템 매니저) 마법사가 나타납니다.

3. 다음과 같이 시스템 매니저 역할을 가진 사용자의 고유 이름을 입력합니다.
   - 관계형 데이터베이스 사용자의 경우 디렉터리 구성 파일의 %USER_ID% Well-Known 특성에 매핑된 값 또는 사용자의 고유 식별자를 입력합니다.
   - LDAP 사용자의 경우 사용자의 상대 DN 을 입력합니다. 예를 들어 사용자의 DN 이 uid=Admin1, ou=People, ou=Employees, ou=NeteAuto 일 경우 Admin1 을 입력합니다.

   참고: 시스템 매니저는 사용자 저장소의 관리자와 동일하지 *않아야* 합니다.
4. "Validate"(유효성 검사)를 클릭하여 사용자의 전체 식별자를 표시합니다.
5. "Next"(다음)를 클릭합니다.
6. 마법사의 두 번째 페이지에서 다음과 같이 사용자에게 할당할 역할을 선택합니다.
   - 시스템 매니저 역할을 할당하려면 다음 태스크를 수행하십시오.
     a. 시스템 매니저 역할 옆의 라디오 단추를 선택합니다.
     b. "Finish"(마침)를 클릭합니다.
   - 시스템 매니저 역할 이외의 역할을 할당하려면 다음 태스크를 수행하십시오.
     a. 첫 번째 목록에서 조건을 선택합니다.
     b. 두 번째 목록 상자에서 역할 이름의 일부나 전체 또는 별표(*)를 입력합니다. "Search"(검색)를 클릭합니다.

c. 검색 결과 목록에서 할당할 역할을 선택합니다.

d. "Finish"(마침)를 클릭합니다.

"System Manager Configuration Output"(시스템 매니저 구성 출력) 화면에 상태 정보가 표시됩니다.

7. "Continue"(계속)를 클릭하여 System Manager(시스템 매니저) 마법사를 닫습니다.

CA Identity Manager 환경의 상태 액세스

CA Identity Manager 에는 다음과 같은 상태를 확인하는 데 사용할 수 있는 상태 페이지가 포함되어 있습니다.

- CA Identity Manager 디렉터리가 올바로 로드되었습니다.
- CA Identity Manager 가 사용자 저장소에 연결할 수 있습니다.
- CA Identity Manager 환경이 올바로 로드됩니다.

상태 페이지에 액세스하려면 브라우저에서 다음 URL 을 입력하십시오.

`http://hostname/iam/im/status.jsp`

hostname

CA Identity Manager 가 설치된 서버의 정규화된 도메인 이름(예: myserver.mycompany.com)을 지정합니다.

CA Identity Manager 환경이 올바르게 시작되고 모든 연결이 성공적으로 실행되는 경우 상태 페이지는 다음 그림과 비슷합니다.

상태 페이지는 해당 환경이 FIPS 140-2 를 준수하는 환경인지도 표시합니다.

CA Identity Manager 환경 문제 해결

다음 표에는 가능한 오류 메시지와 문제 해결 프로세스가 설명되어 있습니다.

메시지	설명	문제 해결
Not Loaded(로드되지 않음)	CA Identity Manager 가 시작될 때 환경과 연결된 CA Identity Manager 디렉터리가 로드되지 않았습니다.	1. 사용자 저장소가 실행 중인지 확인합니다. CA Identity Manager 가 SiteMinder 와 통합되는 경우 SiteMinder 가 사용자 저장소에

메시지	설명	문제 해결
Not OK(정상이 아님)	CA Identity Manager 가 CA Identity Manager 디렉터리에 연결할 수 없습니다.	연결할 수 있는지 확인합니다. 정책 서버 사용자 인터페이스에서 사용자 저장소와 연결된 SiteMinder 사용자 디렉터리 연결의 속성 페이지를 열고 "콘텐츠 보기" 단추를 클릭하여 연결을 확인할 수 있습니다. 사용자 저장소의 콘텐츠가 표시되면 SiteMinder 가 성공적으로 연결할 수 있는 것입니다. 정책 서버에 대한 자세한 내용은 *CA SiteMinder Web Access Manager Policy Server Configuration Guide*(CA SiteMinder Web Access Manager 정책 서버 구성 안내서)를 참조하십시오. 2. CA Identity Manager 및 정책 서버를 다시 시작합니다.

메시지	설명	문제 해결
SM connection is not OK(SM 연결이 정상이 아님)	CA Identity Manager 가 SiteMinder 정책 서버에 연결할 수 없습니다(SiteMinder 를 포함하는 구현 환경의 경우).	1. 다음 조건을 확인합니다. ■ 정책 서버가 실행 중입니다. ■ 웹 에이전트가 리소스를 보호하고 있습니다. 정책 서버 사용자 인터페이스에 액세스하여 웹 에이전트가 올바로 실행되고 있는지 확인할 수 있습니다. 자격 증명을 요구하는 메시지가 표시되면 웹 에이전트가 제대로 작동하고 있는 것입니다. 2. CA Identity Manager 및 정책 서버를 다시 시작합니다.
IMS is not available now(지금 IMS 를 사용할 수 없음)	CA Identity Manager 에서 오류가 발생했습니다.	오류 세부 정보는 응용 프로그램 서버 로그에서 확인합니다.
Windows 500 오류 메시지	LDAP 사용자 디렉터리와의 연결을 제거하는 동안 액세스할 경우 상태 페이지가 표시되지 않습니다.	상태 페이지를 표시하려면 인터넷 브라우저 옵션 "Show friendly error message"(오류 메시지 표시)를 해제하십시오.

제 7 장: Advanced Settings(고급 설정)

관리 콘솔의 "Advanced Settings"(고급 설정) 창에서 다음과 같은 설정을 지정할 수 있습니다.

- 고급 설정을 구성하기 위한 화면 액세스
- 사용자 지정 설정 가져오기/내보내기 (페이지 337)에 설명된 대로 고급 설정 가져오기 및 내보내기

이 섹션은 다음 항목을 포함하고 있습니다.

감사

감사 로그에는 CA Identity Manager 환경에서 수행된 오퍼레이션의 레코드가 유지됩니다. 감사 로그의 데이터를 사용하여 시스템 활동을 모니터링할 수 있습니다.

CA Identity Manager 에서는 *이벤트*를 감사합니다. 이벤트는 CA Identity Manager 태스크에서 생성되는 오퍼레이션입니다. 한 태스크에서 여러 이벤트를 생성할 수 있습니다. 예를 들어 CreateUser 태스크는 CreateUserEvent 및 AddToGroupEvent 이벤트를 생성할 수 있습니다.

기본적으로 CA Identity Manager 는 모든 이벤트 정보를 감사 데이터베이스로 내보냅니다. CA Identity Manager 가 기록하는 이벤트 정보의 유형 및 양을 제어하려면 다음 태스크를 수행하십시오.

- CA Identity Manager 관리자 태스크에 대한 감사가 사용되도록 설정합니다.
- 관리자 태스크에서 생성되는 CA Identity Manager 이벤트의 일부 또는 전부에 대해 감사가 사용되도록 설정합니다.
- 이벤트가 완료 또는 취소되었을 때와 같은 특정 상태의 이벤트 정보를 기록합니다.
- 이벤트와 관련된 특성에 대한 정보를 로깅합니다. 예를 들어 ModifyUserEvent 이벤트 중에 변경되는 특성을 로깅할 수 있습니다.
- 이벤트 및 특성에 대한 감사 수준을 설정합니다.

비즈니스 로직 태스크 처리기

비즈니스 로직 태스크 처리기는 CA Identity Manager 태스크가 처리되도록 제출되기 전에 먼저 사용자 지정 비즈니스 로직을 실행합니다. 일반적으로 사용자 지정 비즈니스 로직은 데이터의 유효성을 검사합니다. 예를 들어 비즈니스 로직 태스크 처리기는 CA Identity Manager 가 구성원을 그룹에 추가하기 전에 먼저 그룹의 구성원 자격 제한을 검사할 수 있습니다. 그룹 구성원 자격 제한에 도달하는 경우 새 구성원을 추가할 수 없음을 그룹 관리자에게 알리는 메시지가 표시됩니다.

미리 정의된 비즈니스 로직 태스크 처리기를 사용할 수도 있고, 비즈니스 로직 태스크 처리기 API 를 사용하여 사용자 지정 처리기를 만들 수도 있습니다.

참고: 사용자 지정 비즈니스 로직 만들기에 대한 자세한 내용은 *Programming Guide for Java*(Java 프로그래밍 안내서)를 참조하십시오.

비즈니스 로직 태스크 처리기 화면에는 기존 전역 비즈니스 로직 태스크 처리기 목록이 있습니다. 목록에는 CA Identity Manager 에 포함된 미리 정의된 처리기와 사이트에서 정의된 모든 사용자 지정 처리기가 들어 있습니다. CA Identity Manager 는 이 목록에 표시된 순서대로 처리기를 실행합니다.

전역 비즈니스 로직 태스크 처리기는 Java 에서만 구현될 수 있습니다.

사용자 암호 다시 설정 태스크에서 자동으로 암호 필드 내용 지우기

이전에 입력한 값이 암호 정책을 위반하거나 "암호" 및 "암호 확인" 필드의 값이 서로 일치하지 않을 경우 자동으로 암호 필드의 내용을 지우도록 CA Identity Manager 를 구성할 수 있습니다.

다음 단계를 수행하십시오.

1. 관리 콘솔을 시작합니다.
2. 관리할 환경을 선택한 다음 "Advanced Settings"(고급 설정)를 클릭합니다.

   "Advanced Settings"(고급 설정) 페이지가 표시됩니다.
3. 비즈니스 로직 태스크 처리기인 BlthPasswordServices 를 클릭합니다.

   "Business Logic Handler Properties"(비즈니스 로직 처리기 속성) 페이지가 표시됩니다.
4. 다음 속성을 만듭니다.

   ClearPwdIfInvalid=true

   PwdConfirmAttrName=|passwordConfirm|
5. 다음과 같이 ConfirmPasswordHandler 설정을 확인합니다.
   - Object type – User
   - Class – ConfirmPasswordHandler
   - ConfirmationAttributeName = |passwordConfirm|
   - OldPasswordAttributeName = |oldPassword|
   - passwordAttributeName = %PASSWORD%

   이제 "Reset User Password"(사용자 암호 다시 설정) 태스크에서 암호 필드의 내용을 지울 수 있습니다.

Event List(이벤트 목록)

관리자 태스크에는 CA Identity Manager 에서 태스크를 완료하기 위해 수행하는 동작인 *이벤트*가 포함되어 있습니다. 한 태스크에 여러 이벤트가 포함될 수도 있습니다. 예를 들어 "Create User"(사용자 만들기) 태스크에는 사용자 프로필을 만들고 사용자를 그룹에 추가하며 역할을 할당하는 이벤트가 포함될 수 있습니다.

CA Identity Manager 는 이벤트를 감사하고, 이벤트와 연관된 고객별 비즈니스 규칙을 적용하며, 이벤트가 워크플로 프로세스에 매핑된 경우 이벤트에 대한 승인을 요구합니다.

이 페이지를 사용하여 CA Identity Manager 에서 사용할 수 있는 이벤트 목록을 볼 수 있습니다.

전자 메일 알림

CA Identity Manager 는 태스크 또는 이벤트가 완료되는 경우 또는 워크플로 제어를 받는 이벤트가 특정 상태에 도달하는 경우 전자 메일 알림을 보낼 수 있습니다. 예를 들어 전자 메일을 통해 승인자에게 이벤트 승인이 필요함을 알릴 수 있습니다.

전자 메일 알림의 콘텐츠를 지정하려면 미리 정의된 전자 메일 템플릿을 사용하면 됩니다. 또는 사용자 요구에 맞게 템플릿을 사용자 지정할 수도 있습니다.

관리 콘솔을 사용하여 다음과 같은 태스크를 수행할 수 있습니다.

- CA Identity Manager 환경에 전자 메일 알림이 사용되도록 설정합니다.
- 전자 메일 메시지를 만드는 데 사용할 템플릿 집합을 지정합니다.
- 전자 메일 알림을 보낼 이벤트 및 태스크를 지정합니다.

이벤트 수신기

CA Identity Manager 태스크는 태스크 실행 중에 수행되는 이벤트라고 하는 하나 이상의 동작으로 구성됩니다. 예를 들어 "Create User"(사용자 만들기) 태스크에는 다음과 같은 이벤트가 포함될 수 있습니다.

- CreateUserEvent - 조직에서 사용자 프로필을 만듭니다.
- AddToGroupEvent - (선택 사항) 그룹 구성원으로 사용자를 추가합니다.
- AssignAccessRole - (선택 사항) 사용자에게 액세스 역할을 할당합니다.

*이벤트 수신기*는 특정 이벤트를 "수신 대기"한 다음 이벤트 수명 주기의 특정 시점에 사용자 지정 비즈니스 로직을 실행합니다. 예를 들어 CA Identity Manager 에서 새 사용자를 만들고 나면 이벤트 수신기가 사용자 정보를 다른 응용 프로그램의 데이터베이스에 추가할 수 있습니다.

참고: 이벤트 수신기 구성에 대한 자세한 내용은 *Programming Guide for Java*(Java 프로그래밍 안내서)를 참조하십시오.

ID 정책

ID 정책은 특정 규칙 또는 조건을 충족하는 사용자에게 일련의 비즈니스 변경 내용을 적용합니다. ID 정책을 사용하여 다음 태스크를 수행할 수 있습니다.

- 역할 및 그룹 구성원 자격 할당, 리소스 할당 또는 사용자 프로필 특성 수정과 같은 ID 관리 태스크를 자동화합니다.
- 직무 분리를 적용합니다. 예를 들어 수표 서명자 역할의 구성원이 수표 승인자 역할을 맡지 못하도록 금지하는 ID 정책을 만들 수 있습니다.

- 규정 준수를 적용합니다. 예를 들어 $100,000 가 넘는 수준의 수입을 얻을 수 있는 특정 직책의 사용자를 감사할 수 있습니다.

사용자 콘솔에서 ID 정책 세트를 만들고 관리할 수 있습니다. ID 정책에 대한 자세한 내용은 *관리 안내서*를 참조하십시오.

ID 정책을 사용하려면 관리 콘솔을 사용하여 다음 태스크를 수행하십시오.

- CA Identity Manager 환경에 ID 정책이 사용되도록 설정합니다.
- 재귀 수준을 설정합니다(선택 사항).

논리적 특성 처리기

CA Identity Manager 논리적 특성을 사용하면 태스크 화면에서 사용자에게 친숙한 형식으로 사용자 저장소의 특성(즉, *물리적 특성*)을 표시할 수 있습니다. CA Identity Manager 관리자는 태스크 화면을 사용하여 CA Identity Manager 의 기능을 수행합니다.

논리적 특성은 사용자 저장소에 없으며, 일반적으로 표현을 단순화하기 위해 하나 이상의 물리적 특성을 나타냅니다. 예를 들어 논리적 특성 *날짜*는 물리적 특성 *월, 일* 및 *연도*를 나타낼 수 있습니다.

논리적 특성은 논리적 특성 API 를 사용하여 작성된 Java 개체인 논리적 특성 처리기에서 처리됩니다. 예를 들어 태스크 화면이 표시되면 논리적 특성 처리기가 사용자 저장소의 물리적 특성 데이터를 논리적 특성 데이터로 변환할 수 있습니다.

CA Identity Manager 에 포함된 미리 정의된 논리적 특성 및 논리적 특성 처리기를 사용하거나 논리적 특성 API 를 사용하여 새로 만들 수 있습니다.

참고: 자세한 내용은 *Programming Guide for Java*(Java 프로그래밍 안내서)를 참조하십시오.

Miscellaneous(기타)

이 화면에서 정의된 사용자 정의 속성은 전체 CA Identity Manager 환경에 적용됩니다. 이러한 사용자 정의 속성은 CA Identity Manager API 를 사용하여 만드는 모든 사용자 지정 Java 개체의 init() 메서드에 이름/값 쌍으로 전달됩니다. 사용자 지정 개체는 개체의 비즈니스 로직에서 요구하는 방식으로 이 데이터를 사용할 수 있습니다.

특정 사용자 지정 개체에 대한 사용자 정의 속성도 정의됩니다. 예를 들어 속성 화면에서 MyListener 라는 이벤트 수신기에 대한 사용자 정의 속성이 정의되었다고 가정합니다. "Miscellaneous"(기타) 화면에서 정의된 개체 관련 사용자 정의 속성 및 환경 수준의 속성은 MyListener.init()에 대한 단일 호출에서 전달됩니다.

사용자 정의 속성을 추가하려면 속성 이름 및 값을 지정하고 "Add"(추가)를 클릭하십시오.

하나 이상의 사용자 정의 속성을 삭제하려면 삭제할 각 이름/값 쌍 옆에 있는 확인란을 선택하고 "Delete"(삭제)를 클릭하십시오.

변경을 마쳤으면 "Save"(저장)를 클릭하십시오. 변경 사항을 적용하려면 응용 프로그램 서버를 다시 시작해야 합니다.

참고: 모든 기타 속성은 대소문자를 구분합니다. 따라서 SelfRegistrationLogoutUrl 이라는 속성과 selfregistrationlogouturl 이라는 속성을 정의하는 경우 두 속성이 모두 추가됩니다.

알림 규칙

알림 규칙에 따라 전자 메일 알림을 수신할 사용자가 결정됩니다. 태스크가 완료된 경우 또는 태스크의 이벤트가 승인 보류, 승인됨 또는 거부됨과 같은 특정 상태에 도달하는 경우 사용자는 알림 규칙에 따라 전자 메일 알림을 받습니다.

참고: 전자 메일 알림 기능에 대한 자세한 내용은 *관리 안내서*를 참조하십시오.

CA Identity Manager 에는 다음과 같이 미리 정의된 알림 규칙이 있습니다.

ADMIN_ADAPTER

태스크를 시작하는 관리자에게 전자 메일 메시지를 보냅니다.

USER_ADAPTER

태스크의 영향을 받는 사용자에게 전자 메일 메시지를 보냅니다.

USER_MANAGER

현재 컨텍스트에서 사용자의 매니저에게 전자 메일을 보냅니다.

사용자 지정 알림 규칙을 만들려면 알림 규칙 API 를 사용하십시오.

참고: 알림 규칙에 대한 자세한 내용은 *Programming Guide for Java*(Java 프로그래밍 안내서)를 참조하십시오.

조직 선택기

조직 선택기는 CA Identity Manager 가 등록 중에 사용자가 제공하는 정보를 기반으로 자체 등록된 사용자의 프로필을 만들 위치를 결정하는 사용자 지정 논리적 특성 처리기입니다. 예를 들어 등록 시 프로모션 코드를 제공하는 사용자의 프로필은 프로모션 사용자 조직에 추가될 수 있습니다.

Provisioning(프로비져닝)

프로비져닝과 함께 CA Identity Manager 를 사용하는 경우 이 화면을 사용할 수 있습니다.

참고: 세부적인 절차인 프로비져닝을 위해 환경을 구성하는 방법 (페이지 267)에 단계별 지침이 나와 있습니다.

"Provisioning Properties"(프로비져닝 속성) 옵션은 다음과 같습니다.

Enabled(사용)

두 사용자 저장소, 즉 CA Identity Manager 에 사용할 사용자 저장소와 프로비져닝 계정에 사용할 별도의 사용자 저장소(프로비져닝 디렉터리라고 함)를 사용하도록 지정합니다. 이 옵션이 사용되지 않도록 설정하면 CA Identity Manager 사용자 저장소만 사용됩니다.

Use Session Pool(세션 풀 사용)

세션 풀이 사용되도록 설정합니다.

Session Pool Initial Sessions(세션 풀 초기 세션 수)

시작할 때 풀에서 사용할 수 있는 최소 세션 수를 정의합니다.

기본값: 8

Session Pool Maximum Sessions(세션 풀 최대 세션 수)

풀의 최대 세션 수를 정의합니다.

기본값: 32

Enable Password Changes from Endpoint Accounts(끝점 계정에서 암호 변경 사용)

프로비져닝 서버의 각 사용자에 대해 "Enable Password Synchronization Agent"(암호 동기화 에이전트 사용)의 설정을 정의합니다. 이 옵션을 사용하면 CA Identity Manager 사용자와 연결된 끝점 계정 간에 암호를 동기화할 수 있습니다.

Enable Accumulation of Provisioning Role Membership Events(프로비져닝 역할 구성원 자격 이벤트 누적 사용)

이 옵션을 선택하면 CA Identity Manager 가 프로비져닝 역할 구성원 자격과 관련된 이벤트를 특정 순서대로 실행합니다. 모든 추가 동작은 단일 오퍼레이션으로 결합되어 처리를 위해 프로비져닝 서버로 보내집니다. 추가 동작의 처리가 완료되면 CA Identity Manager 가 제거 동작을 단일 오퍼레이션으로 결합하여 프로비져닝 서버로 보냅니다. 이 순서로 이벤트를 실행하기 위해 AccumulatedProvisioningRoleEvent 라는 단일 이벤트가 생성됩니다.

참고: AccumulatedProvisioningRoleEvent 에 대한 자세한 내용은 *관리 안내서*를 참조하십시오.

Organization for Creating Inbound Users(인바운드 사용자를 만들기 위한 조직)

CA Identity Manager 가 사용하는 사용자 저장소의 정규화된 경로를 정의합니다. 이 필드는 사용자 저장소에 조직이 포함되어 있는 경우에만 나타납니다.

Inbound Administrator(인바운드 관리자)

인바운드 매핑에 매핑되는 태스크를 실행할 수 있는 CA Identity Manager 관리자 계정을 정의합니다. 이러한 태스크는 "Provisioning Synchronization Manager"(프로비져닝 동기화 매니저) 역할에 포함됩니다. 관리자가 모든 CA Identity Manager 사용자에 대해 각 태스크를 실행할 수 있어야 합니다.

프로비져닝 디렉터리

프로비져닝 디렉터리는 도메인, 전역 사용자, 끝점 유형, 끝점, 계정 및 계정 템플릿을 포함한 프로비져닝 정보의 리포지토리입니다. 이 옵션을 선택하면 CA Identity Manager 사용자 저장소를 프로비져닝 디렉터리에 매핑하기 위한 다른 옵션이 나타납니다.

Enable Session Pooling(세션 풀링 사용)

성능 향상을 위해 CA Identity Manager 는 프로비져닝 서버와 통신할 때 풀링에 사용할 세션 여러 개를 미리 할당할 수 있습니다.

"Session Pools"(세션 풀) 옵션이 사용되지 않으면 CA Identity Manager 가 필요에 따라 세션을 만들고 삭제합니다.

새 환경의 경우 "Session Pools"(세션 풀)은 기본적으로 사용됩니다. 기존 환경의 경우 "Session Pools"(세션 풀)이 사용되도록 설정할 수 있습니다.

다음 단계를 수행하십시오.

1. 관리 콘솔에서 "Advanced Settings"(고급 설정), "Provisioning"(프로비져닝)을 선택합니다.
2. "Use Session Pool"(세션 풀 사용)을 선택합니다.
3. 시작 시 풀의 최소 세션 수를 정의합니다.
4. 풀의 최대 세션 수를 정의합니다.
5. "Save"(저장)를 클릭합니다.
6. 응용 프로그램 서버를 다시 시작합니다.

   정의한 설정에 따라 세션 풀이 사용됩니다.

Enable Password Synchronization(암호 동기화 사용)

프로비져닝 서버는 CA Identity Manager 사용자와 관련 끝점 사용자 계정 사이에서 암호를 동기화할 수 있게 해 줍니다. 즉, 프로비져닝 역할을 가지고 있는 사용자가 CA Identity Manager 에서 만들어지거나 수정되면 프로비져닝 사용자가 끝점 계정의 암호 변경을 허용하도록 설정됩니다.

참고: 관리 콘솔에서 이 기능이 사용되도록 설정하면 환경의 *모든* 사용자가 끝점 계정의 암호 변경을 허용하도록 설정됩니다.

암호 동기화를 사용하려면

1. 관리 콘솔에서 "Advanced Settings"(고급 설정), "Provisioning"(프로비져닝)을 선택합니다.
2. "Enable Password Changes from Endpoint Accounts"(끝점 계정에서 암호 변경 사용)를 선택합니다.
3. "저장"을 클릭합니다.
4. 응용 프로그램 서버를 다시 시작합니다.

Attribute Mappings(특성 매핑)

특성 매핑은 "프로비져닝 사용자 만들기" 같은 프로비져닝 관련 관리자 태스크의 사용자 특성을 프로비져닝 서버의 해당 특성과 연결합니다. 단일 프로비져닝 특성을 CA Identity Manager 사용자 저장소의 여러 특성에 매핑할 수 있습니다.

기본 태스크의 특성에 대한 기본 매핑이 있는데, 이는 "Inbound Mappings"(인바운드 매핑) 섹션에 나열되어 있습니다. 다른 특성을 사용하도록 이러한 관리자 태스크 중 하나를 수정하는 경우 필요에 따라 특성 매핑을 업데이트하십시오.

Inbound Mappings(인바운드 매핑)

인바운드 매핑은 프로비져닝 서버에서 생성되는 이벤트를 관리자 태스크에 매핑합니다. 이러한 매핑은 미리 설정되어 있으며 수정할 수 없습니다.

Outbound Mappings(아웃바운드 매핑)

아웃바운드 매핑은 관리자 태스크에서 생성되는 이벤트를 프로비져닝 디렉터리에 적용되는 이벤트와 연결합니다. 사용자 특성에 영향을 주는 이벤트에 대한 기본 매핑이 있습니다.

사용자 콘솔

사용자가 관리자 태스크를 수행할 수 있게 해 주는 웹 응용 프로그램인 사용자 콘솔을 사용하여 CA Identity Manager 환경에 액세스합니다. 관리 콘솔의 "User Console"(사용자 콘솔) 페이지에서 관리자가 환경에 액세스하는 데 사용하는 사용자 콘솔의 특정 속성을 정의합니다.

"User Console"(사용자 콘솔) 페이지에는 다음 필드가 포함되어 있습니다.

General Properties(일반 속성)

환경에 적용되는 속성을 정의하십시오.

Show Recently Completed Tasks(최근에 완료된 태스크 표시)

태스크 완료 시 CA Identity Manager 가 상태 메시지를 표시하는지 여부를 결정합니다.

이 옵션을 선택하면 사용자가 "OK"(확인)를 클릭해야 CA Identity Manager 가 표시하는 상태 메시지가 지워집니다.

메시지가 사용되지 않도록 설정하고 각 상태 메시지가 나타날 때 사용자가 "OK"(확인)를 클릭하지 않아도 되도록 설정하려면 이 옵션을 선택 취소하십시오.

Show About Link(정보 링크 표시)

"About"(정보) 링크가 사용자 콘솔의 오른쪽 아래에 나타나는지 여부를 결정합니다. 이 옵션을 선택하면 CA Identity Manager 사용자가 "About"(정보) 링크를 클릭하여 CA Identity Manager 구성 요소의 버전 정보를 볼 수 있습니다.

Enable Language Switching(언어 전환 사용)

CA Identity Manager 가 로그인 화면과 사용자 콘솔에 "Choose Language"(언어 선택) 드롭다운 목록을 포함하는지 여부를 결정합니다. 이 필드를 선택하면 CA Identity Manager 사용자가 목록에서 새 언어를 선택하여 사용자 콘솔의 언어를 변경할 수 있습니다.

참고: "Choose Language"(언어 선택) 필드를 표시하려면 "Enable Language Switching"(언어 전환 사용) 필드를 선택함과 *동시에* 여러 언어를 지원하도록 CA Identity Manager 를 구성해야 합니다.

자세한 내용은 *User Console Design Guide*(사용자 콘솔 디자인 안내서)를 참조하십시오.

Job Timeout(작업 시간 만료)

태스크가 제출된 후 상태 메시지를 표시하기 전에 CA Identity Manager 가 대기하는 시간을 지정합니다.

태스크가 지정된 시간 내에 완료되는 경우 CA Identity Manager 는 다음 메시지를 표시합니다.

"태스크 완료"

태스크 완료에 더 오랜 시간이 걸리거나 태스크가 워크플로 제어하에 있는 경우에는 CA Identity Manager 가 다음 메시지를 표시합니다.

"Task has been submitted for processing on the *current date*"(태스크가 current date 에 처리를 위해 제출되었습니다.)

참고: 변경 내용이 즉시 적용되지 않을 수도 있습니다.

Theme Properties(테마 속성)

환경에 있는 사용자 콘솔의 아이콘과 제목을 사용자 지정할 수 있습니다. 예를 들어 사용자 콘솔 화면에 회사 로고와 회사 이름을 추가할 수 있습니다.

테마 속성에는 다음 설정이 포함되어 있습니다.

Icon (URI)(아이콘(URI))

URI 를 사용하여 응용 프로그램 서버가 사용할 수 있는 이미지에 대한 아이콘을 정의합니다.

예: http://myserver.mycompany.com/images/front/logo.gif

Icon Link (URI)(아이콘 링크(URI))

URI 를 사용하여 이미지에 대한 탐색 링크를 정의합니다.

Icon Title(아이콘 제목)

마우스 포인터를 아이콘 위로 이동하면 나타나는 도구 설명을 정의합니다.

제목

사용자 콘솔의 맨 위에 있는 아이콘 옆에 표시되는 사용자 지정 텍스트를 지정합니다.

참고: 사용자 지정 스킨을 정의한 경우 스킨에 대한 속성 파일을 참조하여 아이콘이나 제목을 지정할 수 있습니다. 예를 들어 사용자 지정 스킨에 대한 속성 파일의 아이콘 이미지에 대한 항목이 image/logo.gif 인 경우 "Icon"(아이콘) 필드에 동일한 문자열을 입력할 수 있습니다.

Login Properties(로그인 속성)

사용자가 환경에 액세스할 때 리디렉션되는 로그인 페이지의 인증 방법과 위치를 지정하십시오.

Authentication Provider module class name(인증 공급자 모듈 클래스 이름)

인증 공급자 모듈의 클래스 이름을 지정합니다.

로그인 페이지

사용자가 환경에 액세스할 때 리디렉션되는 페이지를 지정합니다.

웹 서비스

CA Identity Manager TEWS(태스크 실행 웹 서비스)를 사용하면 원격 실행을 위해 타사 클라이언트 응용 프로그램에서 CA Identity Manager 로 CA Identity Manager 태스크를 제출할 수 있습니다.

"Web Services Properties"(웹 서비스 속성) 화면에서는 환경에 대해 TEWS 를 구성할 수 있습니다. 이 화면에서 다음 태스크를 수행할 수 있습니다.

- CA Identity Manager 환경에 대해 TEWS 가 사용되도록 설정합니다.
- 태스크 관련 WSDL(Web Services Definition Language) 문서를 생성합니다.
- 가장을 허용합니다.
- 관리자 암호가 인증에 필요하도록 지정합니다.
- SiteMinder 인증을 구성합니다.
- CA Identity Manager 가 SiteMinder 와 통합되는 경우 웹 서비스 URL 을 보호하도록 SiteMinder 를 구성합니다.
- 웹 보안 서비스 사용자 이름 토큰 인증을 지정합니다.
- 가능한 인증 유형 세 가지 중 하나 이상을 지정합니다.

태스크 실행 웹 서비스를 통한 CA Identity Manager 원격 요청 실행에 대한 자세한 내용은 *Programming Guide for Java*(Java 프로그래밍 안내서)를 참조하십시오.

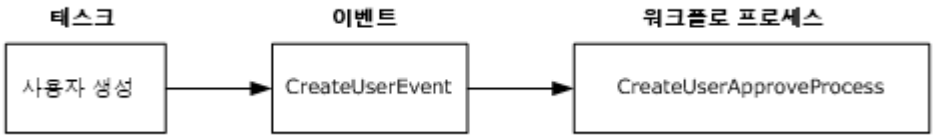
Workflow Properties(워크플로 속성)

이 옵션이 사용되도록 설정하면 워크플로 기능이 워크플로 프로세스와 연결된 CA Identity Manager 태스크의 실행을 제어합니다.

워크플로 프로세스는 사용자 계정 만들기와 같이 비즈니스 목표를 달성하기 위해 수행되는 일련의 단계입니다. 일반적으로 이러한 단계 중 하나에는 태스크 승인 또는 거부가 포함됩니다.

관리자 태스크는 하나 이상의 워크플로 프로세스를 트리거할 수 있는 하나 이상의 이벤트와 연결됩니다. 워크플로 프로세스가 완료된 후 CA Identity Manager 는 워크플로 프로세스 결과에 기반한 태스크를 수행하거나 거부합니다.

다음 그림에서는 CA Identity Manager 태스크, 관련 이벤트 및 워크플로 프로세스 간의 관계를 보여 줍니다.



Workflow Properties(워크플로 속성)

CA Identity Manager 환경에서 워크플로 사용 여부를 설정하려면 이 확인란을 사용하십시오.

Work Item Delegation(작업 항목 위임)

작업 항목 위임이 사용되도록 설정하면 참여자(위임자)가 다른 사용자(피위임자)에게 위임자의 작업 목록에 있는 태스크를 승인할 권한을 위임할 수 있습니다. 참여자는 위임자가 "사무실을 벗어난" 기간 동안 다른 승인자에게 작업 항목을 할당할 수 있습니다. 이 경우 위임자는 위임 기간 동안 해당 작업 항목에 대한 전체 액세스 권한을 계속 보유합니다.

위임에서는 다음과 같이 Well-Known 특성을 사용합니다.

%DELEGATORS%

이 Well-Known 특성은 위임이 만들어진 시간뿐 아니라 특성과 함께 사용자에게 위임하고 있는 사용자의 이름도 저장합니다.

참고: 작업 항목 위임에 대한 자세한 내용은 *관리 안내서*를 참조하십시오.

Workflow Participant Resolvers(워크플로 참여자 해결 프로그램)

태스크 승인 또는 거부 같은 워크플로 프로세스 내 활동은 *참여자*가 수행합니다.

"Workflow Participant Resolvers"(워크플로 참여자 해결 프로그램) 화면을 사용하여 사용자 지정 참여자 해결 프로그램을 정규화된 참여자 해결 프로그램 Java 클래스에 매핑합니다.

사용자 지정 *참여자 해결 프로그램*은 워크플로 활동의 참여자를 확인하고 목록을 CA Identity Manager 에 반환하는 Java 개체입니다. 그런 다음 CA Identity Manager 가 목록을 워크플로 엔진에 전달합니다.

일반적으로 표준 참여자 해결 프로그램에서 활동에 필요한 참여자 목록을 제공할 수 없는 경우에만 사용자 지정 참여자 해결 프로그램을 작성합니다.

참고: 사용자 지정 참여자 해결 프로그램 개발에 대한 자세한 내용은 *Programming Guide for Java*(Java 프로그래밍 안내서)를 참조하십시오. 표준 참여자 해결 프로그램에 대한 자세한 내용은 *관리 안내서*를 참조하십시오.

사용자 지정 설정 가져오기/내보내기

관리 콘솔의 "Advanced Settings"(고급 설정) 화면에서 다음과 같이 여러 환경에 고급 설정을 적용할 수 있습니다.

- 한 환경에서 고급 설정을 구성합니다.
- 고급 설정을 XML 파일로 내보냅니다.
- XML 파일을 필요한 환경으로 가져옵니다.

Java Virtual Machine 메모리 부족 오류

증상

스트레스나 높은 부하로 인해 CA Identity Manager 서버 기능이 영향을 받는 기간 동안 JVM 메모리 부족 오류가 수신됩니다.

해결 방법

메모리 부족 상태에 대한 경고를 받도록 JVM 디버깅 옵션을 설정하는 것이 좋습니다.

참고: JVM 디버깅 옵션 설정에 대한 자세한 내용은 http://www.oracle.com 의 "Debugging Options in Java HotSpot VM Options"(Java 핫스폿 VM 옵션의 디버깅 옵션)를 참조하십시오.

제 8 장: 감사

이 섹션은 다음 항목을 포함하고 있습니다.

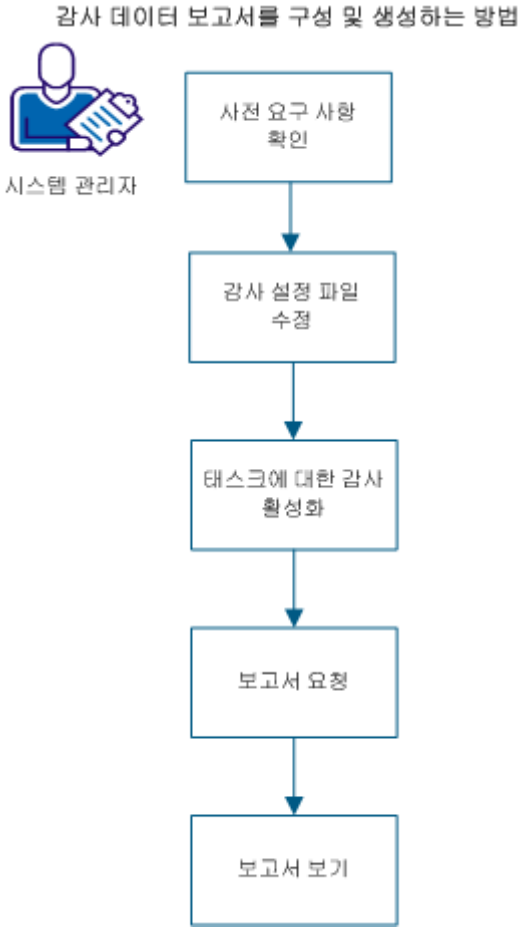
감사 데이터 보고서를 구성 및 생성하는 방법

감사 데이터는 환경에서 발생하는 작업의 내역을 제공합니다. 감사를 구성하고 활성화하면 시스템이 감사 데이터베이스에 태스크에 대한 정보를 기록합니다. 감사 정보를 사용하여 보고서를 생성할 수 있습니다. 감사 데이터의 예는 다음과 같습니다.

- 지정된 기간 동안의 시스템 활동
- 특정 환경에 액세스하는 동안의 사용자 로그인 및 로그아웃 이벤트
- 특정 사용자가 수행하는 태스크
- 특정 기간 동안 수정된 개체 목록
- 사용자에게 할당된 역할
- 특정 사용자 계정에 대해 수행된 오퍼레이션

감사 데이터는 CA Identity Manager *이벤트*에 대해 생성됩니다. 이벤트는 CA Identity Manager 태스크에서 생성되는 오퍼레이션입니다. 예를 들어 "사용자 만들기" 태스크는 AssignAccessRoleEvent 이벤트를 포함할 수 있습니다.

다음 다이어그램은 시스템 관리자가 감사를 구성하고 감사 데이터에 대한 보고서를 생성하는 방법을 설명합니다.



관리자로서 다음 단계를 수행하십시오.

1. 사전 요구 사항 확인 (페이지 341)
2. 감사 설정 파일 수정 (페이지 341)
3. 태스크에 대한 감사 활성화 (페이지 349)

4. 보고서 요청 (페이지 350)
5. 보고서 보기 (페이지 353)

사전 요구 사항 확인

감사 설정을 구성하기 전에 다음과 같은 사전 요구 사항이 충족되는지 확인하십시오.

- 감사와 관련된 데이터를 저장하기 위해 별도 데이터베이스 인스턴스가 생성됩니다. 기본적으로 CA Identity Manager 데이터베이스 스키마 파일은 다음 위치에 있습니다.
  - **Windows**: C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\Identity Manager\tools\db
- 감사 보고서를 요청하고 보려면 보고서 서버 연결을 구성하십시오.
- 감사 보고서에 대한 연결 개체를 추가하십시오. 다음 단계를 수행하십시오.
  a. 관리자 권한을 사용하여 사용자 콘솔에 로그인합니다.
  b. "역할 및 태스크", "관리자 태스크"로 이동한 다음 수정할 감사 보고서를 찾습니다.
  c. "보고서용 연결 개체" 필드에 다음과 같은 연결 이름을 입력합니다.
     `rptParamConn`

감사 설정 파일 수정

CA Identity Manager 가 반드시 감사해야 하는 정보 유형을 정의하기 위해 감사 설정 파일에서 감사 설정을 구성하십시오. 다음과 같은 태스크를 수행하도록 감사 설정 파일을 구성할 수 있습니다.

- 관리자 태스크에서 생성된 이벤트의 일부 또는 모두를 감사합니다.

- 이벤트가 완료 또는 취소되었을 때 같은 특정 상태의 이벤트 정보를 기록합니다.
- 이벤트와 관련된 특성에 대한 정보를 로깅합니다. 예를 들어 ModifyUserEvent 이벤트 중에 변경되는 특성을 로깅할 수 있습니다.

- 특성 로깅에 대한 감사 수준을 설정합니다.

감사 설정 파일은 감사 설정을 내보내어 만드는 XML 파일입니다. 파일의 스키마는 다음과 같습니다.

```
<Audit enabled="" auditlevel="" datasource="">
  <AuditEvent name="" enabled="" auditlevel="">
    <AuditProfile objecttype="" auditlevel="">
      <AuditProfileAttribute name="" auditlevel="" />
    </AuditProfile>
    <EventState name="" severity=""/>
  </AuditEvent>
</Audit>
```

감사 요소 및 스키마에 대한 자세한 내용은 감사 설정 파일의 설명을 참조하십시오.

AuditProfileAttribute 요소는 CA Identity Manager 가 감사하는 특성을 나타냅니다. 특성은 AuditProfile 요소에서 지정한 개체에 적용됩니다.

참고: 지정된 감사 프로필 특성이 없으면 AuditProfile 요소에서 지정한 개체의 모든 특성이 로깅됩니다.

다음 표에서는 CA Identity Manager 개체 유형에 대해 유효한 특성을 보여 줍니다.

CA Identity Manager 개체 유형에 대해 유효한 특성

개체 유형	유효한 특성

CA Identity Manager 개체 유형에 대해 유효한 특성	
개체 유형	**유효한 특성**
ACCESS ROLE	■ name - 사용자에게 표시되는 역할 이름입니다. ■ description - 역할의 용도에 대한 선택적 설명입니다. ■ members - 역할을 사용할 수 있는 사용자입니다. ■ administrators - 역할 구성원을 할당할 수 있는 사용자 또는 관리자입니다. ■ owners - 역할을 수정할 수 있는 사용자입니다. ■ enabled - 역할이 사용되도록 설정되었는지 여부를 나타냅니다. ■ assignable - 관리자가 역할을 할당할 수 있는지 여부를 나타냅니다. ■ tasks - 역할과 연결된 액세스 태스크입니다.
ACCESS TASK	■ name - 사용자에게 표시되는 태스크 이름입니다. ■ description - 태스크의 용도에 대한 선택적 설명입니다. ■ application - 태스크와 연결된 응용 프로그램입니다. ■ tag - 태스크의 고유 식별자입니다. ■ reserved1, reserved2, reserved3, reserved4 - 태스크에 대해 예약된 필드의 값입니다.

CA Identity Manager 개체 유형에 대해 유효한 특성

개체 유형	유효한 특성
ADMINISTRATIVE ROLE	■ name - 사용자에게 표시되는 역할 이름입니다. ■ description - 역할의 용도에 대한 선택적 설명입니다. ■ members - 역할을 사용할 수 있는 사용자입니다. ■ administrators - 역할 구성원을 할당할 수 있는 사용자 또는 관리자입니다. ■ owners - 역할을 수정할 수 있는 사용자입니다. ■ enabled - 역할이 사용되도록 설정되었는지 여부를 나타냅니다. ■ assignable - 관리자가 역할을 할당할 수 있는지 여부를 나타냅니다. ■ tasks - 역할과 연결된 태스크입니다.

CA Identity Manager 개체 유형에 대해 유효한 특성	
개체 유형	**유효한 특성**
ADMINISTRATIVE TASK	■ name - 사용자에게 표시되는 태스크 이름입니다. ■ description - 태스크의 용도에 대한 선택적 설명입니다. ■ tag - 태스크의 고유 식별자입니다. ■ category - CA Identity Manager 사용자 인터페이스에서 태스크가 나타나는 범주입니다. ■ primary_object - 태스크가 실행되는 개체입니다. ■ action - 개체에 대해 수행되는 오퍼레이션입니다. ■ hidden - 태스크가 메뉴에 나타나지 *않는지* 여부를 나타냅니다. ■ public - CA Identity Manager 에 로그인하지 않은 사용자가 태스크를 사용할 수 있는지 여부를 나타냅니다. ■ auditing - 태스크에서 감사 정보 기록이 사용되도록 설정되는지 여부를 나타냅니다. ■ external - 태스크가 외부 태스크인지 여부를 나타냅니다. ■ url - 외부 태스크가 실행될 때 CA Identity Manager 가 사용자를 리디렉션하는 URL 입니다. ■ workflow - 태스크와 연결된 CA Identity Manager 이벤트가 워크플로를 트리거하는지 여부를 나타냅니다. ■ webservice - 태스크가 CA Identity Manager 관리 콘솔에서 WSDL(Web Services Description

CA Identity Manager 개체 유형에 대해 유효한 특성

개체 유형	유효한 특성
GROUP	디렉터리 구성 파일(directory.xml)에서 GROUP 개체에 대해 정의된 모든 유효한 특성입니다.
ORGANIZATION PARENTORG	디렉터리 구성 파일(directory.xml)에서 Organization 개체에 대해 정의된 모든 유효한 특성입니다.
RELATIONSHIP	■ %CONTAINER% - 부모 개체의 고유 식별자입니다. 예를 들어 RELATIONSHIP 개체가 역할 구성원 자격을 설명하는 경우 컨테이너는 역할입니다. ■ %CONTAINER_NAME% - 사용자에게 표시되는 부모 그룹 이름입니다. ■ %ITEM% - 부모 개체에 포함된 개체의 고유 식별자입니다. 예를 들어 RELATIONSHIP 개체가 역할 구성원 자격을 설명하는 경우 항목은 역할 구성원입니다. ■ %ITEM_NAME% - 사용자에게 표시되는 중첩된 그룹 이름입니다.
USER	디렉터리 구성 파일(directory.xml)에서 USER 개체에 대해 정의된 모든 유효한 특성입니다.
NONE	특성이 없습니다.

참고: 다음 사항은 이전 테이블에 적용됩니다.

- 즉, enabled, assignable, auditable, workflow, hidden, webservice 및 public 이 true 또는 false 로 로깅됩니다.
- 역할에 대한 태스크를 감사하는 경우 사용자에게 표시되는 이름이 로깅됩니다.
- 데이터베이스에는 구성원, 관리자 및 소유자 정책이 컴파일된 XML 형식으로 저장됩니다. 이 형식은 각 정책이 식으로 나타나는 사용자 인터페이스와 다릅니다.

다음 단계를 수행하십시오.

1. 관리 콘솔에 로그인하고, 환경을 선택하고, "고급 설정"을 선택하고, "감사"를 클릭합니다.
2. "내보내기"를 클릭합니다.

   시스템이 현재 감사 설정을 감사 설정 XML 파일로 내보냅니다.

3. 이전 단계에서 내보낸 XML 파일에서 감사 설정을 수정합니다. 다음 태스크를 수행하십시오.
   a. 값 Audit enabled ="true"로 설정하고 요소 데이터 원본에 대한 "iam_im_<auditdb>.xml"의 JNDI 이름 값을 제공합니다.
   b. 다음 JNDI 이름을 지정하십시오.
      `java:/auditDbDataSource`
      참고: 이 데이터 원본은 다음 위치에 있습니다.
      `iam/im/jdbc/auditDbDataSource`
   c. 파일에서 요소를 추가, 수정, 삭제합니다.
   d. 각 이벤트에 대해 기록되는 정보 수준을 수정합니다.
4. 1 단계와 2 단계를 반복합니다. "가져오기"를 클릭하여 수정된 감사 설정 XML 파일을 업로드합니다.
5. 환경을 다시 시작합니다.

감사 설정 파일이 이제 업데이트되었습니다.

태스크에 대한 감사 활성화

감사 설정 파일에서 감사를 구성한 태스크에 대해 감사를 활성화하십시오.

다음 단계를 수행하십시오.

1. 시스템 관리자 권한을 사용하여 사용자 콘솔에 로그인합니다.
2. 감사를 활성화할 태스크를 만들거나 수정합니다.
3. "프로필" 탭에서 "감사 사용" 확인란이 선택되었는지 확인합니다.
4. "제출"을 클릭합니다.

이제 해당 태스크에 대해 감사가 활성화되었습니다.

보고서 요청

보고서를 보려면 보고서 관리 권한이 있는 사용자에게 보고서를 요청하십시오. 감사 데이터를 추적하는 적절한 보고서를 선택하십시오. 보고서 요청에 승인이 필요한 경우 시스템이 전자 메일 알림을 보냅니다.

보고서를 예약하기 전에 다음 단계를 수행하십시오.

1. 관리자 권한을 사용하여 사용자 콘솔에 로그인합니다.
2. "역할 및 태스크", "관리자 태스크 수정"로 이동한 다음 수정할 감사 보고서를 선택합니다.
3. "탭" 탭을 선택하고 편집할 IAM ReportServerScheduler 를 클릭합니다.
4. "되풀이 옵션 사용" 확인란을 선택합니다.
5. "확인" 및 "제출"을 클릭합니다.

다음 단계를 수행하십시오.

1. 보고서 태스크 사용자 권한을 사용하여 사용자 콘솔에 로그인합니다.
2. "보고서", "보고 태스크", "보고서 요청"을 선택합니다.

   보고서의 목록이 나타납니다.
3. 감사 기반 보고서를 선택합니다.

   매개 변수 화면이 나타납니다.

4. "일정 보고서"를 클릭하고 보고서의 일정을 선택합니다.

지금

보고서가 즉시 실행됨을 지정합니다.

한 번

특정 기간 동안 보고서가 한 번 실행되도록 지정합니다. 보고서를 생성할 시작 날짜, 종료 날짜, 시작 시간 및 종료 시간을 선택합니다.

(감사 보고서만) 매시간

시작 시간과 이후 'n'시간마다 보고서가 생성되도록 지정합니다. 'n'은 연속 보고서의 간격을 나타냅니다. 시작 날짜, 종료 날짜, 시작 시간, 종료 시간 및 연속 보고서의 간격을 선택합니다.

(감사 보고서만) 매일

시작 시간과 이후 'n'일마다 보고서가 생성되도록 지정합니다. 'n'은 연속 보고서의 간격을 나타냅니다. 시작 날짜, 종료 날짜, 시작 시간, 종료 시간 및 연속 보고서의 간격을 선택합니다.

(감사 보고서만) 매주

시작 날짜부터 매주 선택한 요일에 보고서가 생성되도록 지정합니다. 보고서를 생성할 시작 날짜, 종료 날짜, 시작 시간 및 종료 시간을 선택합니다.

(감사 보고서만) 매달

시작 날짜부터 매월 및 이후 'n'개월마다 보고서가 생성되도록 지정합니다. 'n'은 연속 보고서의 간격을 나타냅니다. 시작 날짜, 종료 날짜, 시작 시간, 종료 시간 및 연속 보고서의 간격을 선택합니다.

(감사 보고서만) 매달 특정 날짜에 보고서 실행

지정한 특정 날짜에 보고서가 생성되도록 지정합니다. 보고서를 생성할 시작 날짜, 종료 날짜, 시작 시간 및 종료 시간을 선택합니다.

(감사 보고서만) 첫 번째 월요일

매월 첫 번째 월요일마다 보고서가 생성되도록 지정합니다. 보고서를 생성할 시작 날짜, 종료 날짜, 시작 시간 및 종료 시간을 선택합니다.

(감사 보고서만) 매월 마지막 날

매월 마지막 날에 보고서가 생성되도록 지정합니다. 보고서를 생성할 시작 날짜, 종료 날짜, 시작 시간 및 종료 시간을 선택합니다.

(감사 보고서만) 매월 특정 주의 특정 요일

매월 특정 주의 특정 요일에 보고서가 생성되도록 지정합니다. 보고서를 생성할 시작 날짜, 종료 날짜, 시작 시간 및 종료 시간을 선택합니다. 예를 들어, 매월 셋째 주의 금요일에 보고서를 생성할 수 있습니다.

5. "제출"을 클릭합니다.

보고서 요청이 제출됩니다. 환경 구성에 따라 요청은 즉시 실행되거나 관리자가 승인한 후에 실행됩니다.

대개 시스템 관리자나 보고서 관리 권한이 있는 다른 사용자가 보고서 요청을 승인해야 해당 보고서 요청이 완료됩니다. 승인이 필요한 이유는 일부 보고서를 실행하는 데 오랜 시간이 걸리거나 상당한 시스템 리소스가 필요하기 때문입니다. 보고서 요청에 대한 승인이 필요한 경우 시스템이 전자 메일 알림을 보냅니다.

참고: 승인이 필요한 경우 환경에 대한 워크플로를 활성화하십시오.

보고서 보기

환경 구성에 따라 차이가 있지만 관리자가 해당 보고서 요청을 승인하면 보고서를 볼 수 있게 됩니다. 보고서 요청에 대한 승인이 보류 중인 경우 시스템이 전자 메일 알림을 보냅니다. 보려는 보고서는 승인된 후에야 검색 목록에 나타납니다.

참고: "내 보고서 보기" 태스크를 사용하여 CA Identity Manager 에서 보고서를 보려면 브라우저에서 타사 세션 쿠키를 사용하십시오.

다음 단계를 수행하십시오.

1. 사용자 콘솔에서 "보고서", "보고 태스크"로 이동하고 "내 보고서 보기"를 클릭합니다.
2. 생성된 보고서 중에서 보려는 보고서를 검색합니다.

   생성된 되풀이 보고서와 주문형 보고서가 모두 표시됩니다.

   참고: 보고서의 상태가 보류 중/되풀이인 경우 보고서는 생성되지 않은 것이며 완료하는 데 시간이 걸릴 수 있습니다.
3. 보려는 보고서를 선택합니다.
4. (선택 사항) 왼쪽 위에 있는 "이 보고서 내보내기"를 클릭하여 보고서를 다음 형식으로 내보냅니다.
   - Crystal Reports
   - PDF
   - Microsoft Excel(97-2003)
   - Microsoft Excel(97-2003) 데이터 전용
   - Microsoft Excel(97-2003) - 편집 가능
   - RTF(서식 있는 텍스트 형식 파일)
   - CSV(쉼표로 구분된 값)
   - XML

감사 데이터베이스 정리

감사 데이터베이스에 더 이상 필요 없는 레코드가 누적될 수 있습니다. 이러한 레코드를 제거하려면 db\auditing 디렉터리에서 다음 데이터베이스 프로시저를 실행하십시오.

`garbageCollectAuditing12 *environment-ID MM/DD/YYYY*`

environment-ID

CA Identity Manager 환경의 ID 를 정의합니다.

MM/DD/YYYY

감사 레코드 제거가 완료되어야 하는 날짜를 정의합니다.

제 9 장: 프로덕션 환경

이 단원에서는 특정 기능 요소를 마이그레이션하기 위한 단계별 기능 설명을 제공합니다. 개발 환경에서 제한된 사항이 변경되었고 이러한 변경 내용이 잘 이해된 경우에만 사용되도록 하십시오.

이 섹션은 다음 항목을 포함하고 있습니다.

관리자 역할 및 태스크 정의를 마이그레이션하려면

회사의 특정 요구 사항을 충족하도록 CA Identity Manager 역할 및 태스크를 사용자 지정할 수 있습니다. 사용자 지정에는 관리자 역할이나 태스크에 대해 만들기 또는 수정 태스크를 사용하여 관리자 역할 및 태스크를 만들거나 수정하는 작업이 포함됩니다.

roledefinition.xml 파일에서 역할 및 태스크를 수정할 수도 있지만 이 방법은 *권장되지 않습니다*. 편집 시 오류가 발생할 위험이 있으므로 매우 제한된 변경 내용에 대해서만 이 방법을 사용하십시오.

이 프로세스는 관리자 역할 및 태스크 정의만 마이그레이션합니다. 역할이 조직에 바인딩된 경우 전체 CA Identity Manager 환경 마이그레이션을 고려하십시오.

중요! 프로덕션 환경에서 역할 또는 태스크 정의를 변경한 경우 개발 환경에서 역할 또는 태스크 정의를 가져오면 이러한 변경 내용이 손실됩니다. 역할 및 태스크 정의를 가져오면 동일한 이름의 기존 역할 및 태스크 정의를 덮어씁니다.

관리자 역할 및 태스크 정의를 내보내려면

roledefinition.xml 파일을 직접 변경한 경우 이 파일을 프로덕션 환경으로 직접 가져올 수 있습니다. 그렇지 않은 경우 역할 및 태스크 정의를 내보내려면

1. 정책 서버 클러스터가 있는 경우 하나의 정책 서버만 실행되고 있는지 확인합니다.
2. 하나를 제외한 모든 CA Identity Manager 노드를 중지합니다.
3. 관리 콘솔에 로그인합니다.
4. CA Identity Manager 환경을 클릭합니다.
5. 내보낼 역할 및 태스크 정의가 있는 CA Identity Manager 환경을 선택합니다.
6. "Roles"(역할), "Export"(내보내기)를 차례로 클릭하고 파일 이름을 제공합니다.
7. 다음 절차에 나와 있는 지침을 따라 이 파일을 가져옵니다.

관리자 역할 및 태스크 정의를 가져오려면

다음 단계를 수행하십시오.

1. 앞의 절차에서 만든 파일을 프로덕션 환경에 복사합니다.
2. 프로덕션 환경의 관리 콘솔에 로그인합니다.
3. CA Identity Manager 환경을 클릭합니다.
4. 적절한 CA Identity Manager 환경을 선택합니다.
5. "Roles"(역할)를 클릭합니다.
6. "Import"(가져오기)를 클릭하고 내보내기 시 생성되는 XML 파일의 이름을 지정합니다.
7. 이러한 단계가 성공한 경우 모든 추가 정책 서버와 중지한 CA Identity Manager 노드를 시작합니다.

   참고: CA Identity Manager 환경에서 변경할 사항이 아직 있는 경우 6 단계를 반복하십시오.

역할 및 태스크 가져오기를 확인하려면

역할 및 태스크를 성공적으로 가져왔는지 확인하려면 다음 태스크를 사용할 수 있는 관리자 계정으로 CA Identity Manager 에 로그인하십시오.

- 관리자 역할 수정
- 관리자 태스크 수정

이러한 태스크를 실행하고 역할 및 태스크가 새로 가져온 역할 정의를 반영하는지 확인하십시오.

CA Identity Manager 스킨을 마이그레이션하려면

CA Identity Manager 스킨을 사용자 지정하여 응용 프로그램에 특정 모양과 느낌을 줄 수 있습니다. 사용자 세트에 대한 스킨을 수정하거나 새로 만든 경우 개발 환경에서 프로덕션 환경으로 스킨을 마이그레이션하려면 다음 단계를 수행하십시오.

스킨을 수정하고 있는 경우 수정된 파일을 복사하십시오.

다음 단계를 수행하십시오.

1. 개발 서버에서 프로덕션 서버로 이미지 파일, 스타일 시트, 속성 파일, 콘솔 페이지(index.jsp) 같은 새 파일과 수정된 파일을 복사합니다.
2. 여러 스킨이 사용되고 있는 경우 SiteMinder 응답을 구성합니다.

   참고: 여러 스킨 사용에 대한 자세한 내용은 *구성 안내서*를 참조하십시오.

스킨 마이그레이션을 확인하려면 사용자 콘솔에 로그인하고 스킨이 올바로 나타나는지 확인하십시오.

프로덕션 환경에서 CA Identity Manager 업데이트

개발 환경에서 프로덕션 환경으로 CA Identity Manager 를 마이그레이션한 후 증분 업데이트를 수행해야 할 수 있습니다. 개발 환경에서 프로덕션 환경으로 새 CA Identity Manager 기능을 마이그레이션하려면 다음 단계를 실행하십시오.

1. CA Identity Manager 환경을 마이그레이션합니다.
2. iam_im.ear 를 복사합니다.
3. 워크플로 프로세스 정의를 마이그레이션합니다.

CA Identity Manager 환경을 마이그레이션하려면

CA Identity Manager 환경은 관리 콘솔에서 만들어집니다. CA Identity Manager 환경에는 역할 및 태스크 정의 세트, 워크플로 정의, CA Identity Manager API 를 사용하여 만들어지는 사용자 지정 기능, CA Identity Manager 디렉터리 등이 포함됩니다.

다음 단계를 수행하십시오.

1. CA Identity Manager 가 SiteMinder 와 통합되고 정책 서버 클러스터가 있는 경우 하나의 정책 서버만 실행되고 있는지 확인합니다.
2. 하나를 제외한 모든 CA Identity Manager 노드를 중지합니다.
3. 개발 환경의 관리 콘솔에서 CA Identity Manager 환경을 내보냅니다.
4. 내보낸 환경을 프로덕션 환경의 관리 콘솔로 가져옵니다.
5. CA Identity Manager 가 SiteMinder 와 통합되는 경우 정책 서버 사용자 인터페이스에서 CA Identity Manager 영역을 다시 보호합니다.

   CA Identity Manager 환경을 내보내면 정책 도메인이 정책 저장소에서 내보내지지 않습니다.
6. 정책 서버와 중지한 CA Identity Manager 노드를 다시 시작합니다.

CA Identity Manager 환경을 마이그레이션하면 다음 활동이 발생합니다.

- 동일한 개체가 두 위치 모두에 있는 경우 개발 서버의 변경 내용이 프로덕션 서버의 변경 내용을 덮어씁니다.
- 새 개체가 개발 환경에 만들어지는 경우 해당 개체가 프로덕션 서버에 추가됩니다.
- 새 개체가 프로덕션 서버에 만들어지는 경우 해당 개체가 유지됩니다.

CA Identity Manager 환경을 내보내려면

프로덕션 시스템에서 CA Identity Manager 환경을 배포하려면 개발 또는 준비 시스템에서 환경을 내보내고 프로덕션 시스템으로 가져와야 합니다.

참고: 이전에 내보낸 환경을 가져올 경우 CA Identity Manager 에서 관리 콘솔의 상태 창에 로그를 표시합니다. 이 로그에 있는 각 관리 개체와 해당 특성에 대한 유효성 검사 및 배포 정보를 보려면 환경을 내보내기 *전에* "Environment Properties"(환경 속성) 페이지에서 "Enable Verbose Log Output"(자세한 로그 출력 사용) 필드를 선택하십시오. "Enable Verbose Log Output"(자세한 로그 출력 사용) 필드를 선택하면 가져오기 중에 중대한 성능 문제가 발생할 수 있습니다.

다음 단계를 수행하십시오.

1. 관리 콘솔에서 "Environments"(환경)를 클릭합니다.

   CA Identity Manager 환경 화면이 나타나고 CA Identity Manager 환경 목록이 표시됩니다.

2. 내보낼 환경을 선택합니다.
3. "Export"(내보내기) 단추를 클릭합니다.

   "File Download"(파일 다운로드) 화면이 나타납니다.

4. ZIP 파일을 프로덕션 시스템에서 액세스할 수 있는 위치에 저장합니다.
5. "Finish"(마침)를 클릭합니다.

   다른 환경으로 가져올 수 있는 ZIP 파일로 환경 정보를 내보냈습니다.

CA Identity Manager 환경을 가져오려면

개발 시스템에서 CA Identity Manager 환경을 내보낸 후 해당 환경을 프로덕션 시스템으로 가져올 수 있습니다.

다음 단계를 수행하십시오.

1. 관리 콘솔에서 "Environments"(환경)를 클릭합니다.

   CA Identity Manager 환경 화면이 나타나고 CA Identity Manager 환경 목록이 표시됩니다.

2. "Import"(가져오기) 단추를 클릭합니다.

   "Import Environment"(환경 가져오기) 화면이 나타납니다.

3. 환경을 가져오는 데 필요한 ZIP 파일을 찾습니다.

4. "Finish"(마침)를 클릭합니다.

환경을 CA Identity Manager 로 가져왔습니다.

CA Identity Manager 환경 마이그레이션을 확인하려면

CA Identity Manager 환경이 제대로 마이그레이션되었는지 확인하려면 CA Identity Manager 환경이 프로덕션 환경의 정책 서버에 대한 정책 서버 사용자 인터페이스에 나타나는지 확인하십시오.

정책 서버 사용자 인터페이스에서 다음 사항을 확인하십시오.

- CA Identity Manager 사용자 디렉터리 설정이 정확합니다.
- 새 CA Identity Manager 도메인이 있습니다.
- 올바른 인증 체계가 CA Identity Manager 영역을 보호합니다.

또한 관리 콘솔에 로그인할 때 "Environments."(환경)를 선택하면 CA Identity Manager 환경이 나타나는지 확인하십시오.

JBoss 용 iam_im.ear 마이그레이션

개발 환경에서 프로덕션 환경으로 기능이 마이그레이션될 때마다 iam_im.ear 를 다시 배포하십시오. 전체 EAR 를 마이그레이션하면 프로덕션 환경이 개발 환경과 동일해집니다.

다음 단계를 수행하십시오.

1. 개발 환경에서 프로덕션 환경이 액세스할 수 있는 위치로 iam_im.ear 를 복사합니다.
2. iam_im.ear 의 복사본에서 프로덕션 환경을 반영하도록 정책 서버 연결 정보를 편집합니다.

   이렇게 변경하려면 프로덕션 환경에서 iam_im.ear 로 *jboss_home*/server/default/iam_im.ear/policyserver_rar/META-INF/ra.xml 을 복사합니다.
3. 다음과 같이 설치된 iam_im.ear 를 2 단계의 개발 환경에 있는 iam_im.ear 의 복사본으로 바꿉니다.
   a. 프로덕션 서버에서 다음 iam_im.ear 를 삭제합니다.

      cluster_node_jboss_home\server\default\deploy\iam_im.ear
   b. 삭제된 파일을 개발 환경에 있는 iam_im.ear 의 편집된 복사본으로 바꿉니다.
4. 클러스터의 각 노드에 대해 이러한 단계를 반복합니다.

WebLogic 용 iam_im.ear 마이그레이션

개발 환경에서 프로덕션 환경으로 기능이 마이그레이션될 때마다 iam_im.ear 를 다시 배포하십시오. 전체 EAR 를 마이그레이션하면 프로덕션 환경이 개발 환경과 동일해집니다.

다음 단계를 수행하십시오.

1. 정책 서버 연결 정보를 유지합니다.

   정책 서버 연결 정보는 policyserver_rar/WEB-INF 디렉터리의 ra.xml 파일에 저장됩니다. 다시 배포하기 전에 iam_im.ear 에서 바뀔 수 있도록 이 파일을 다른 위치에 복사합니다.

2. iam_im.ear 를 WebLogic Admin Server 가 사용할 수 있는 위치에 복사합니다.

3. 정책 서버 연결 정보를 바꿉니다.

   iam_im.ear 에서 policyserver_rar/WEB-INF/ra.xml 파일을 1 단계에서 유지된 파일로 바꾸십시오.

4. iam_im.ear 를 다시 배포합니다.

   a. WebLogic 콘솔에 로그인합니다.

   b. "Deployments"(배포), "Application"(응용 프로그램), "Identity Manager"로 이동합니다.

"Deploy"(배포) 탭에서 "Deploy (Re-Deploy) Application"(응용 프로그램 배포(다시 배포))을 선택합니다.

WebSphere 용 iam_im.ear 마이그레이션

다음 단계를 수행하십시오.

1. *was_im_tools_dir**WebSphere-tools* 에서 *deployment_manager_dir* *bin* 디렉터리로 *imsInstall.jacl* 스크립트를 복사합니다.
   - 여기서 *was_im_tools_dir* 는 개발 시스템에서 WebSphere 용 CA Identity Manager 도구가 설치된 디렉터리입니다.
   - *deployment_manager_dir* 는 배포 매니저가 설치된 위치입니다.
2. CA Identity Manager 응용 프로그램을 구성한 개발 시스템에서 *was_im_tools_dir* *WebSphere-tools**imsExport.bat* 또는 *imsExport.sh* 를 *was_home**bin* 에 복사합니다.
3. 명령줄에서 *was_home**bin* 으로 이동합니다.
4. WebSphere 응용 프로그램 서버가 실행되고 있는지 확인합니다.
5. 다음과 같이 배포된 CA Identity Manager 응용 프로그램을 내보냅니다.

   Windows 의 경우 다음 명령을 입력합니다.

   ```
   imsExport.bat "path-to-exported-ear"
   ```

   여기서 *path-to-exported-ear* 는 imsExport 유틸리티가 만드는 전체 경로 및 파일 이름입니다.

   Windows 시스템의 경우 was_im.ear 의 경로를 지정할 때 백슬래시(\) 대신 슬래시(/)를 사용합니다. 예를 들면 다음과 같습니다.

   ```
   imsExport.bat "c:/program files/CA/CA Identity Manager/
   exported_ear/iam_im.ear"
   ```

   UNIX 의 경우 다음 명령을 입력합니다.

   ```
   ./wsadmin -f imsExport.jacl -conntype RMI -port 2809 path to exported ear
   ```

   여기서 *path-to-exported-ear* 는 내보낸 EAR 파일의 파일 이름을 포함한 전체 경로입니다.
6. 해당 EAR 파일을 내보낸 개발 시스템 상의 위치에서 배포 매니저가 설치된 시스템 상의 위치로 내보낸 EAR 파일을 복사합니다.

7. *was_im_tools_dir*/WebSphere-ear/iam_im.ear/policyserver_rar/META-INF/ra.xml 을 프로덕션 환경에 있는 파일로 바꿉니다.

   ra.xml 파일은 정책 서버 연결 정보를 포함합니다.

8. 배포 매니저가 설치된 시스템에서 Identity Manager EAR 를 배포합니다.

   a. 명령줄에서 다음 위치로 이동합니다.

      deployment_manager_dir \bin

   b. WebSphere 응용 프로그램 서버가 실행되고 있는지 확인합니다.

   c. 다음과 같이 imsInstall.jacl 스크립트를 실행합니다.

   참고: imsInstall.jacl 스크립트를 실행하려면 몇 분 정도 걸릴 수 있습니다.

   Windows:

   wsadmin -f imsInstall.jacl *"path-to-copied-ear" cluster_name*

   여기서 *path-to-copied-ear* 는 배포 매니저 시스템에 복사한 Identity Manager EAR 의 파일 이름을 포함한 전체 경로입니다.

   예를 들면 다음과 같습니다.

   wsadmin -f imsInstall.jacl "c:\Program Files\CA\Identity Manager\WebSphere-tools\was_im.ear" im_cluster

UNIX:

./wsadmin -f imsInstall.jacl *path-to-copied-ear cluster_name*

여기서 *path-to-copied-ear* 는 배포 매니저 시스템에 복사한 Identity Manager EAR 의 파일 이름을 포함한 전체 경로입니다.

예를 들면 다음과 같습니다.

./wsadmin -f imsInstall.jacl /opt/CA/Identity Manager/WebSphere-tools/was_im.ear im_cluster

9. CA Identity Manager 가 SiteMinder 와 통합되는 경우 다음 사항을 확인합니다.
   - SiteMinder 에이전트가 정책 저장소에 연결할 수 있습니다.
   - 정책 서버가 사용자 저장소에 연결할 수 있습니다.
   - CA Identity Manager 도메인이 만들어졌습니다.

워크플로 프로세스 정의 마이그레이션

개발 환경에서 워크플로를 사용한 경우 워크플로 정의를 내보냈다가 프로덕션 환경으로 가져오십시오. 그런 다음 각 서버 노드에서 워크플로를 구성하십시오.

프로세스 정의 내보내기

개발 환경 시스템에서 워크플로 프로세스 정의를 내보냅니다.

다음 단계를 수행하십시오.

1. 응용 프로그램 서버가 실행되고 있는지 확인합니다.
2. *admin_tools*\Workpoint\bin\으로 이동하고 다음과 같이 Archive.bat(Windows 의 경우) 또는 Archive.sh(UNIX 의 경우)를 실행합니다.
   a. "Import"(가져오기) 대화 상자에서 루트 개체를 선택합니다.
   b. "Add"(추가)를 클릭합니다.
   c. 생성할 파일의 이름을 지정합니다.
   d. "Export"(내보내기)를 클릭합니다.
   e. "Go"(실행)를 클릭합니다.

   admin_tools 는 다음 위치 중 하나에 기본적으로 설치되어 있는 관리 도구를 나타냅니다.
   - **Windows:** C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools
   - **UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools
3. 다음 단원인 프로세스 정의 가져오기 (페이지 368)에 나와 있는 지침을 따릅니다.

프로세스 정의 가져오기

프로덕션 환경 시스템에서 워크플로 프로세스 정의를 가져오십시오.

다음 단계를 수행하십시오.

1. 응용 프로그램 서버를 다시 시작합니다.
2. 선택적으로 앞의 절차를 통해 정의를 내보내어 현재 정의의 백업 복사본을 만듭니다.
3. *admin_tools*\Workpoint\bin\으로 이동하고 다음과 같이 Archive 스크립트를 실행합니다.
   a. "Import"(가져오기) 대화 상자에서 가져올 항목을 모두 선택합니다.
   b. 새 형식을 사용할지 아니면 이전 형식을 사용할지 묻는 메시지가 표시되면 이전 형식을 유지합니다.

      새 형식은 CA Identity Manager 를 지원하지 않습니다.
   c. 내보내기 시 생성되는 파일의 이름을 제공합니다.
   d. "Go"(실행)를 클릭합니다.

   admin_tools 는 다음 위치 중 하나에 기본적으로 설치되어 있는 관리 도구를 나타냅니다.

   - **Windows:** C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools
   - **UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools

제 10 장: CA Identity Manager 로그

이 섹션은 다음 항목을 포함하고 있습니다.

CA Identity Manager 에서 문제를 추적하는 방법

CA Identity Manager 에는 다음과 같은 상태 기록 및 문제 추적 방법이 포함되어 있습니다.

"View Submitted Tasks"(제출한 태스크 보기) 태스크

CA Identity Manager 환경의 모든 이벤트 및 태스크 상태를 표시합니다. 관리자는 사용자 콘솔에서 이 태스크를 사용합니다.

"View Submitted Tasks"(제출한 태스크 보기)에서는 다음 유형의 정보를 제공합니다.

- 환경에서 발생하는 이벤트 및 태스크 목록
- 이벤트와 연결된 특성 목록
- 성공한 이벤트 및 실패한 이벤트
- 보류 중이거나 중단된 상태의 이벤트
- 거부된 이벤트(거부 이유 포함)
- 계정 동기화 상태
- ID 정책 동기화 상태
- 프로비저닝 정보(프로비저닝이 사용되도록 설정된 경우)

응용 프로그램 서버 로그

CA Identity Manager 설치의 모든 구성 요소에 대한 정보를 표시하고 CA Identity Manager 의 모든 오퍼레이션에 대한 상세 정보를 제공합니다.

로그 파일 위치와 유형은 다음과 같이 사용 중인 응용 프로그램 서버 유형에 따라 다릅니다.

- WebLogic - CA Identity Manager 정보가 표준 출력에 기록됩니다. 기본적으로 표준 출력은 서버 인스턴스가 실행되고 있는 콘솔 창입니다.
- JBoss - CA Identity Manager 정보가 서버 인스턴스가 실행되고 있는 콘솔 창과 *jboss_home*\server\log\server.log 에 기록됩니다.
- WebSphere - CA Identity Manager 정보가 서버 인스턴스가 실행되고 있는 콘솔 창과 *was_home*\AppServer\logs*server_name*\SystemOut 에 기록됩니다.

자세한 내용은 응용 프로그램 서버 설명서를 참조하십시오.

디렉터리 서버 로그 파일

사용자 디렉터리에서 발생하는 활동에 대한 정보를 포함합니다.

기록되는 정보 유형과 로그 파일 위치는 사용 중인 디렉터리 서버 유형에 따라 다릅니다. 자세한 내용은 디렉터리의 서버 설명서를 참조하십시오.

정책 서버 로그 파일

CA Identity Manager 가 SiteMinder 와 통합되는 경우 다음 정보를 표시합니다.

- SiteMinder 연결 문제
- SiteMinder 인증 문제
- SiteMinder 정책 저장소의 CA Identity Manager 관리 개체에 대한 정보
- 암호 정책 평가

SiteMinder 로그 구성에 대한 자세한 내용은 *CA SiteMinder Web Access Manager Policy Server Administration Guide*(CA SiteMinder Web Access Manager 정책 서버 관리 안내서)를 참조하십시오.

정책 서버 프로파일러

CA Identity Manager 가 SiteMinder 와 통합되는 경우 CA Identity Manager 관련 기능을 포함한 내부 정책 서버 진단 및 처리 기능을 추적할 수 있습니다.

자세한 내용은 구성 요소와 데이터 필드를 추적하는 방법 (페이지 372)을 참조하십시오.

웹 에이전트 로그 파일

CA Identity Manager 가 SiteMinder 와 통합되는 경우 웹 에이전트는 다음 두 로그에 정보를 기록합니다.

- 오류 로그 파일 - 웹 에이전트가 정책 서버와 통신할 수 없는 등의 프로그램 및 오퍼레이션 수준 오류를 포함합니다.
- 추적 로그 파일 - 추적 메시지, 흐름 상태 메시지 등의 경고 및 정보 메시지를 포함합니다. 헤더 상세 정보, 쿠키 변수 등의 데이터도 포함됩니다.

참고: 웹 에이전트 로그 파일에 대한 자세한 내용은 *CA SiteMinder Web Access Manager Web Agent Configuration Guide*(CA SiteMinder Web Access Manager 웹 에이전트 구성 안내서)를 참조하십시오.

구성 요소와 데이터 필드를 추적하는 방법

CA Identity Manager 가 SiteMinder 와 통합되는 경우 SiteMinder 정책 서버 프로파일러를 사용하여 정책 서버에 대한 CA Identity Manager 확장에 있는 구성 요소와 데이터 필드를 추적할 수 있습니다. 프로파일러를 통해 구성 요소나 데이터 필드의 특정 값만 캡처하도록 추적 출력에 대한 필터를 구성할 수 있습니다.

참고: 정책 서버 프로파일러를 사용하는 방법에 대한 자세한 내용은 *CA SiteMinder Web Access Manager Policy Server Administration Guide*(CA SiteMinder Web Access Manager 정책 서버 관리 안내서)를 참조하십시오.

다음 구성 요소에 대해 추적이 사용되도록 설정할 수 있습니다.

Function_Begin_End

정책 서버에 대한 CA Identity Manager 확장에 있는 특정 메서드가 실행될 때 하위 수준 추적 문을 제공합니다.

IM_Error

SiteMinder 정책 서버에 대한 CA Identity Manager 확장에 있는 런타임 오류를 추적합니다.

IM_Info

CA Identity Manager 확장에 대한 일반 추적 정보를 제공합니다.

IM_Internal

내부 CA Identity Manager 오퍼레이션에 대한 일반 정보를 추적합니다.

IM_MetaData

CA Identity Manager 가 디렉터리 메타데이터를 처리할 때 추적 정보를 제공합니다.

IM_RDB_Sql

관계형 데이터베이스에 대한 추적 정보를 제공합니다.

IM_LDAP_Provider

LDAP 디렉터리에 대한 추적 정보를 제공합니다.

IM_RuleParser

런타임에 해석되는 XML 파일에 정의된 구성원, 소유자 및 관리자 정책의 구문 분석 및 평가 프로세스를 추적합니다.

IM_RuleEvaluation

구성원, 관리자, 소유자 및 범위 규칙의 평가를 추적합니다.

IM_MemberPolicy

구성원 자격과 범위를 포함한 구성원 정책의 평가를 추적합니다.

IM_AdminPolicy

관리자 정책의 평가를 추적합니다.

IM_OwnerPolicy

소유자 정책의 평가를 추적합니다.

IM_RoleMembership

사용자가 가지고 있는 역할 목록, 특정 역할을 맡고 있는 구성원 목록 같은 역할 구성원 자격 관련 정보를 추적합니다.

IM_RoleAdmins

사용자가 관리할 수 있는 역할 목록, 특정 역할에 대한 관리자 목록 같은 역할 관리 관련 정보를 추적합니다.

IM_RoleOwners

사용자가 소유한 역할 목록, 특정 역할에 대한 소유자 목록 같은 역할 소유권 관련 정보를 추적합니다.

IM_PolicyServerRules

정책 서버가 확인한 RoleMember, RoleAdmin, RoleOwner 같은 구성원 규칙과 AccessTask 에 대한 AII 및 AccessTaskFilter 규칙 같은 범위 규칙의 평가를 추적합니다.

IM_LLSDK_Command

내부 CA Identity Manager SDK 와 정책 서버 간의 통신을 추적합니다. 기술 지원 시 이 추적 구성 요소가 사용됩니다.

IM_LLSDK_Message

명시적으로 Java 코드를 통해 내부 CA Identity Manager SDK 에서 정책 서버로 전송되는 메시지를 추적합니다. 기술 지원 시 이 추적 구성 요소가 사용됩니다.

IM_IdentityPolicy

ID 정책의 평가 및 적용을 추적합니다.

IM_PasswordPolicy

암호 정책의 평가를 추적합니다.

IM_Version

CA Identity Manager 버전에 대한 정보를 제공합니다.

IM_CertificationPolicy

인증 정책의 평가를 추적합니다.

IM_InMemoryEval

구성원, 관리자, 소유자 및 ID 정책을 포함한 CA Identity Manager 정책의 처리를 추적합니다. 기술 지원 시 이 추적 구성 요소가 사용됩니다.

IM_InMemoryEvalDetail

구성원, 관리자, 소유자 및 ID 정책을 포함한 CA Identity Manager 정책의 처리에 대한 추가 상세 정보를 제공합니다. 기술 지원 시 이 추적 구성 요소가 사용됩니다.

추적을 구성할 수 있는 데이터 필드는 *CA SiteMinder Web Access Manager Policy Server Administration Guide*(CA SiteMinder Web Access Manager 정책 서버 관리 안내서)에 나열되어 있습니다.

제 11 장: CA Identity Manager 보호

이 섹션은 다음 항목을 포함하고 있습니다.

사용자 콘솔 보안

사용자 콘솔은 관리자가 CA Identity Manager 환경에서 사용자, 그룹, 조직 같은 개체를 관리하는 데 사용되는 사용자 인터페이스입니다. 이러한 개체는 연결된 역할 및 태스크 집합과 함께 할당됩니다. 관리자가 사용자 콘솔에 로그인하면 관리자와 관련된 태스크가 해당 환경에 표시됩니다.

기본적으로 CA Identity Manager 는 네이티브 인증을 사용하여 사용자 콘솔에 대한 액세스를 보호합니다. CA Identity Manager 관리자가 CA Identity Manager 환경에 로그인하기 위해 유효한 사용자 이름과 암호를 입력합니다. 그러면 CA Identity Manager 는 CA Identity Manager 가 관리하는 사용자 저장소를 대상으로 이름과 암호를 인증합니다.

CA Identity Manager 가 SiteMinder 와 통합되는 경우 CA Identity Manager 는 *자동으로* SiteMinder 기본 인증을 사용하여 환경을 보호합니다. 기본 인증을 사용하는 데 필요한 추가 구성은 없습니다. SiteMinder 관리 사용자 인터페이스를 사용하여 고급 인증 방법을 구성할 수 있습니다.

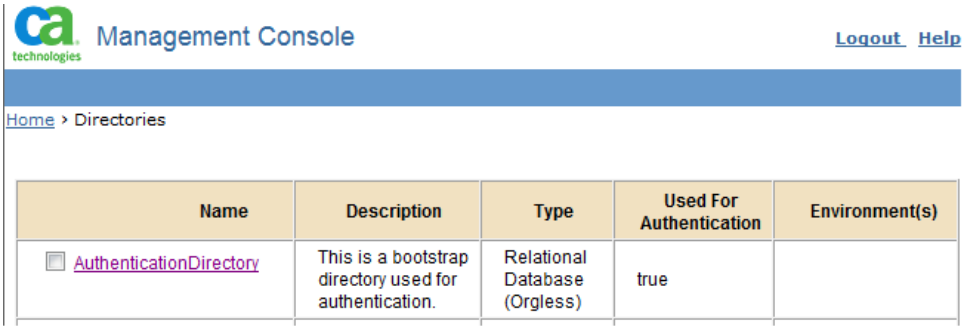
참고: 자세한 내용은 *CA SiteMinder Web Access Manager Policy Server Configuration Guide*(CA SiteMinder Web Access Manager 정책 서버 구성 안내서)를 참조하십시오.

관리 콘솔 보안

관리자가 관리 콘솔을 사용하여 CA Identity Manager 디렉터리 및 환경을 만들고 관리할 수 있습니다. 관리자가 관리 콘솔을 사용하여 환경에 대한 사용자 지정 기능을 구성할 수도 있습니다.

CA Identity Manager 설치에는 관리 콘솔 보안 옵션이 포함됩니다. 이 옵션은 기본적으로 선택되어 있습니다. 설치하는 동안 CA Identity Manager 가 관리 콘솔에 액세스할 수 있는 관리자를 인증하는 데 사용하는 자격 증명을 지정합니다. CA Identity Manager 는 AuthenticationDirectory 라는 부트스트랩 디렉터리에서 제공하는 자격 증명으로 사용자를 만듭니다. 관리 콘솔에서 이 디렉터리를 볼 수 있습니다.

참고: CA Identity Manager 가 CA SiteMinder 와 통합되는 경우에는 네이티브 보안을 사용하여 관리 콘솔을 보호할 수 없습니다.



관리 콘솔 관리자 추가

기본적으로 네이티브 CA Identity Manager 보안으로 보호되는 관리 콘솔에는 설치하는 동안 새 CA Identity Manager 디렉터리에 만들어지는 관리자 계정이 하나 있습니다.

관리자를 추가하려면 관리 콘솔에 대한 액세스 권한이 필요한 사용자를 포함하는 CA Identity Manager 디렉터리를 지정합니다. 기존 디렉터리를 사용하면 새 계정을 만들지 않고도 조직의 사용자에게 관리 콘솔 액세스 권한을 부여할 수 있습니다.

인증용 디렉터리는 하나만 지정할 수 있습니다. 인증용으로 구성된 디렉터리는 삭제할 수 없습니다.

다음 단계를 수행하십시오.

1. 설치하는 동안 제공한 사용자 자격 증명으로 관리 콘솔에 로그인합니다.
2. "Directories"(디렉터리)를 열고 관리 콘솔에 대한 액세스 권한이 필요한 사용자를 포함하는 디렉터리를 클릭합니다.
3. "Update Authentication"(인증 업데이트)을 클릭합니다.
4. "Used for Authentication"(인증에 사용됨) 옵션을 선택합니다.
5. 첫 번째 사용자의 로그인 이름을 입력하고 "Add"(추가)를 클릭합니다.
6. 모든 사용자가 추가될 때까지 관리 콘솔에 대한 액세스 권한이 필요한 사용자 추가를 계속합니다. 그런 다음 "Save"(저장)를 클릭합니다.

   이제 지정한 사용자가 해당 사용자 이름과 암호를 사용하여 관리 콘솔에 액세스할 수 있습니다.

관리 콘솔에 대해 네이티브 보안이 사용되지 않도록 설정

관리 콘솔에 대해 네이티브 보안이 사용되도록 설정한 경우 이제 다른 응용 프로그램으로 관리 콘솔을 보호하려면 다른 보안 방법을 구현하기 전에 네이티브 보안이 사용되지 않도록 설정하십시오.

다음 단계를 수행하십시오.

1. 다음과 같이 web.xml 파일에서 관리 콘솔에 대해 네이티브 보안이 사용되지 않도록 설정합니다.
   a. 텍스트 편집기에서 *CA Identity Manager_installation*\iam_im.ear\management_console.war\WEB-INF\web.xml 을 엽니다.
   b. 다음과 같이 ManagementConsoleAuthFilter 에 대한 Enable 매개변수의 값을 false 로 설정합니다.

```
<filter>
<filter-name>ManagementConsoleAuthFilter</filter-name>
<filter-class>com.netegrity.ims.manage.filter.ManagementCon
soleAuthFilter</filter-class>
<init-param>
<param-name>Enable</param-name>
<param-value>false</param-value>
</init-param>
</filter>
```

   c. web.xml 파일을 저장합니다.
2. CA Identity Manager 서버를 다시 시작합니다.

   이제 관리 콘솔이 더 이상 네이티브 보안으로 보호되지 않습니다.

SiteMinder 를 사용하여 관리 콘솔 보안

처음에 관리 콘솔을 보호하기 위해 SiteMinder 정책을 만들 수 있습니다.

SiteMinder 정책은 관리 콘솔 같이 보호할 리소스를 식별하고 사용자 세트에 해당 리소스에 대한 액세스 권한을 부여합니다.

다음 단계를 수행하십시오.

1. 관리 콘솔에 대해 네이티브 보안이 사용되지 않도록 설정 (페이지 380)합니다.
2. 도메인 권한을 가진 관리자로 다음 인터페이스 중 하나에 로그인합니다.
   - CA SiteMinder r12 이상의 경우 관리 UI 에 로그인합니다.
   - CA SiteMinder 6.0 SP*x* 의 경우 정책 서버 사용자 인터페이스에 로그인합니다.

   참고: 이러한 인터페이스를 사용하는 방법에 대한 내용은 사용 중인 SiteMinder 버전의 설명서를 참조하십시오.
3. 적절한 CA Identity Manager 환경에 대한 정책 도메인을 찾습니다.

   이 도메인은 CA Identity Manager 가 SiteMinder 와 통합될 때 자동으로 만들어집니다. 도메인 이름의 형식은 다음과 같습니다.

   *Identity Manager-environment*Domain

   이 형식에서 *Identity Manager-environment* 는 수정 중인 환경의 이름을 지정합니다. 예를 들어 이름이 *employees* 인 경우 도메인 이름은 *employees*Domain 입니다.
4. 다음 리소스 필터를 사용하여 영역을 만듭니다.

   /iam/immanage/
5. 영역에 대한 규칙을 만듭니다. 관리 콘솔의 모든 페이지를 보호하려면 별표(*)를 필터로 지정합니다.
6. 새 정책을 만들고 이전 단계에서 만든 규칙과 연결합니다.

   관리 콘솔에 액세스할 수 있는 사용자를 정책과 연결해야 합니다.
7. 응용 프로그램 서버를 다시 시작합니다.

업그레이드 후 기존 환경 보호

CA Identity Manager 12.6 이상으로 업그레이드한 후 네이티브 보안을 사용하여 관리 콘솔을 보호할 수 있습니다.

참고: CA Identity Manager 가 CA SiteMinder 와 통합되는 경우에는 네이티브 CA Identity Manager 보안을 사용하여 관리 콘솔을 보호할 수 없습니다.

다음 단계를 수행하십시오.

1. 다음과 같이 web.xml 파일에서 관리 콘솔에 대해 네이티브 보안이 사용되도록 설정합니다.
   a. 텍스트 편집기에서 *CA Identity Manager_installation*\iam_im.ear\management_console.war\WEB-INF\web.xml 을 엽니다.
   b. 다음과 같이 ManagementConsoleAuthFilter 에 대한 Enable 매개 변수의 값을 true 로 설정합니다.

```
<filter>
<filter-name>ManagementConsoleAuthFilter</filter-name>
<filter-class>com.netegrity.ims.manage.filter.ManagementCon
soleAuthFilter</filter-class>
<init-param>
<param-name>Enable</param-name>
<param-value>true</param-value>
</init-param>
</filter>
```

   c. web.xml 파일을 저장합니다.
2. CA Identity Manager 개체 저장소에 IM_AUTH_USER 테이블을 만듭니다.

   IM_AUTH_USER 테이블에는 관리 콘솔 관리자에 대한 정보가 저장됩니다.
   a. CA\Identity Manager\IAM Suite\Identity Manager\tools\db\objectstore 로 이동합니다.
   b. 개체 저장소를 대상으로 다음 스크립트 중 하나를 실행합니다.
      - sql_objectstore.sql

- oracle_objectstore.sql

참고: 기존 데이터베이스를 대상으로 한 스크립트 실행에 대한 자세한 내용은 해당 데이터베이스에 대한 공급업체 설명서를 참조하십시오.

3. 사용자 암호를 암호화하려면 암호 도구를 사용하십시오.

   암호 도구는 다음 위치에 CA Identity Manager 도구와 함께 설치됩니다.

Windows: C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\PasswordTool

UNIX: /opt/CA/IdentityManager/IAM_Suite/Identity_Manager/tools/PasswordTool

   PasswordTool

   다음 명령을 사용하여 암호 도구를 실행하십시오.

   `pwdtools -JSAFE -p anypassword`

   JSAFE 옵션은 PBE 알고리즘을 사용하여 일반 텍스트 값을 암호화합니다.

1. IM_AUTH_USER 테이블에 부트스트랩 사용자 정보를 넣습니다.

   IM_AUTH_USER 테이블의 모든 열에 대한 값을 지정합니다.

   예를 들면 다음과 같습니다.

   USER_NAME: admin1

   PASSWORD: *anypassword*

   DISABLED: 0

   ID:1

2. CA Identity Manager 서버를 다시 시작합니다.

   이제 관리 콘솔이 네이티브 보안으로 보호됩니다.

CSRF 공격으로부터 보호

CSRF(Cross-Site Request Forgery) 공격에 대한 내성을 강화하도록 CA Identity Manager 가 향상되었습니다. 기본적으로 향상된 기능은 CA Identity Manager 에서 사용되지 않도록 설정되어 있습니다.

향상된 기능이 사용되도록 설정하려면

1. 다음 위치에 있는 web.xml 파일을 엽니다.

   application-server/iam_im.ear/user_console.war/WEB-INF

2. <param-name> csrf-prevention-on 이 있는 <context-param> 요소를 찾습니다.
3. <param-value>를 true 로 설정합니다.
4. 응용 프로그램 서버를 다시 시작합니다.

제 12 장: Service Desk 통합

NIM SM(Normalized Integration Management Service Management) 통합은 정규화된 단일 RESTful API 를 통해 CA Identity Manager 를 여러 서비스 데스크 제품과 통합할 수 있도록 합니다. NIM 은 이 RESTful API 를 노출하고 모든 요청을 일련의 구성 가능한 매핑에 따라 네이티브 서비스 데스크 형식으로 내부적으로 변환하는 완전히 포함된 웹 서비스를 제공합니다.

Policy Xpress 와 해당 웹 서비스 작업을 사용하면 CA Identity Manager 내에서 태스크 및 이벤트 상태에 따라 서비스 데스크 티켓을 자동으로 만들 수 있습니다.

지원되는 서비스 데스크 제품의 전체 목록은 제품 지원표를 참조하십시오.

다음 예에서는 서비스 데스크 통합의 사용 사례를 보여 줍니다.

샘플 사용 사례: 사용할 수 없는 끝점 티켓

예를 들어 CA Identity Manager 가 끝점에 연결할 수 없는 경우와 같은 태스크 또는 이벤트 실패를 기반으로 실행되는 Policy Xpress 정책을 만들 수 있습니다. 그러면 이 Policy Xpress 정책은 NIM RESTful API 를 호출하고 서비스 데스크 티켓을 만듭니다. 실패를 조사하고 해결할 수 있도록 티켓에는 오류 메시지를 포함하여 실패에 대한 충분한 정보가 포함되며, 서비스 데스크 티켓에 의해 워크플로가 추적됩니다.

샘플 사용 사례: 수동 프로비저닝 요청 티켓

서비스 기능을 사용하여 CA Identity Manager 가 관리하지 않는 시스템에서 계정을 수동으로 프로비저닝하고 프로비저닝 해지할 수 있도록 하는 수동 프로비저닝 요청을 구현할 수 있습니다. NIM RESTful API 를 통해 서비스 데스크 티켓을 만드는 이행 및 이행 해지 작업으로 서비스를 구성할 수 있습니다. 그러면 사용자는 서비스 데스크 티켓 형식으로 해당 시스템에 대한 액세스를 요청하고 요청이 할당, 추적 및 이행되도록 할 수 있습니다.

참고: 현재 NIM SM 은 인스턴스별로 구성된 단일 서비스 데스크 연결만 지원하며 인스턴스는 서버당 하나입니다.

이 섹션은 다음 항목을 포함하고 있습니다.

NIM 자격 증명 업데이트

CA NIM SM(Normalization Integration Management Service Management)은 CA Identity Manager 를 다양한 서비스 데스크 솔루션과 통합할 수 있도록 합니다.

새로 설치할 때 NIM 은 CA 내장 구성 요소에 대해 지정한 사용자 이름과 암호를 사용하도록 구성됩니다.

이전 버전에서 CA Identity Manager 12.6.5 로 업그레이드할 경우에는 CA 내장 구성 요소의 사용자 이름과 암호를 사용할 수 없습니다. 대신 NIM 사용자 이름과 암호가 모두 기본값인 "nimadmin"으로 돌아갑니다. 다음 파일에서 사용자 이름 및 암호 값을 변경하여 NIM 자격 증명을 업데이트하는 것이 좋습니다.

- iam_im.ear/config/ca_nim.properties
- iam_im.ear/ca-nim-sm.war/WEB-INF/config/NIM-Users.xml

다음 단계를 수행하십시오.

1. 암호 도구를 사용하여 암호를 암호화합니다.

   참고: 암호 도구를 사용하기 전에 pwdtools.bat 파일에서 %JAVE_HOME% 환경 변수를 설정하십시오. 자세한 내용은 "암호 도구"를 참조하십시오.

   a. CA Identity Manager 서버가 설치된 컴퓨터에서 명령 프롬프트 창을 열고 암호 도구 디렉터리로 이동합니다.

   예:

   C:\Program Files (x86)\CA\Identity Manager\IAM Suite\Identity Manager\tools\PasswordTool

   b. 암호화 요구 사항에 따라 다음 명령 중 *하나*를 입력합니다.

   - FIPS 비호환 암호화의 경우 다음 명령을 입력하십시오.

   ```
   pwdtools -JSAFE -p password
   ```

   출력 예:

일반 텍스트: password

암호화된 값: {PBES}:WQf3wza4JfbqICD/4D8xog==

- FIPS 호환 암호화의 경우 다음 명령을 입력하십시오.

```
pwdtools –FIPS –k [FIPS 키 경로] -p password
```

출력 예:

키 파일 위치=C:/FIPSkey.dat

일반 텍스트: password

암호화된 값: {AES}:3BqepUi09EfB3IKmvBBBWg==

2. iam_im.ear/config/로 이동하여 ca_nim.properties 파일을 텍스트 편집기에서 엽니다.

   예: C:\Program Files\jboss-eap-6.2\standalone\deployments\iam_im.ear\config\ca_nim.properties

3. 다음 행을 찾습니다.

```
nimadminUser=nimadmin
nimadminPassword={PBES}:Q82YUY22ku8X04T1DyBvww==
```

4. 해당 값을 자신의 사용자 이름과 암호화된 암호로 바꿉니다.

   예:

```
nimadminUser=myusername
nimadminPassword=myencryptedpassword
```

5. ca_nim.properties 파일을 저장합니다.

6. 암호 도구를 사용하여 암호를 NIM 에 필요한 형식으로 암호화합니다. 다음 명령을 입력합니다.

```
pwdtools -CANIMSM -p password
```

출력 예:

일반 텍스트: password

암호화된 값: AAAAEM7HElhthx74qHBkjDD7L/nIthHpxl8z3piCMFyw5ctL

7. iam_im.ear/ca-nim-sm.war/WEB-INF/config/로 이동하여 NIM-Users.xml 파일을 텍스트 편집기에서 엽니다.
8. 다음 코드 행을 찾습니다.

```
<User>
<property name="username" value="nimadmin"/>
<property name="password"
value="AAAAEDFsjJUDxVV9PK+2putOEiUsoPzGAcDjnMGFie4NC01Z"/>
</User>
```

9. 해당 값을 자신의 사용자 이름과 암호화된 암호로 바꿉니다.

   예:

```
<User>
<property name="username" value="myusername"/>
<property name="password" value="myencryptedpassword"/>
</User>
```

10. 응용 프로그램 서버를 다시 시작합니다.

NIM 자격 증명을 업데이트했습니다.

Service Desk 통합을 위한 역할 정의 가져오기

현재 CA Identity Manager 환경을 서비스 데스크 솔루션과 통합하려면 CA NIM Service Management 에 대한 역할 정의를 가져오십시오. 이러한 역할 정의는 시스템 매니저 역할에 다음 태스크를 추가합니다.

- Service Desk 통합 구성
- Service Desk 필드 매핑 사용자 지정
- Service Desk 통합 REST API 설명서 보기

다음 단계를 수행하십시오.

1. 관리 콘솔에서 "환경"으로 이동하고 서비스 데스크 솔루션과 통합하려는 환경을 클릭합니다.
   "환경 속성" 화면이 나타납니다.
2. "역할 및 태스크", "가져오기"를 차례로 클릭하고 "NIM Service Management"를 선택한 다음 "가져오기"를 클릭합니다.
3. 환경을 다시 시작합니다.

서비스 데스크 통합을 위한 역할 정의를 가져왔습니다.

Service Desk 통합 구성

CA Identity Manager 가 서비스 데스크 솔루션과 통신할 수 있도록 하려면 서비스 데스크 통합을 구성하십시오.

다음 단계를 수행하십시오.

1. CA Identity Manager 사용자 콘솔에서 "시스템", "NIM SM Integration"으로 이동하고 "Service Desk 통합 구성"을 클릭합니다.
2. 드롭다운 목록에서 사용자의 서비스 데스크 솔루션을 선택합니다.
3. 서비스 데스크 솔루션에 대한 연결 설정을 입력하고 "제출"을 클릭합니다.

참고: 자세한 내용은 해당 서비스 데스크 솔루션에 대한 연결 설정 단원을 참조하십시오.

추가 정보:

CA Cloud Service Management 에 대한 연결 설정 (페이지 397)
CA Service Desk Manager 에 대한 연결 설정 (페이지 392)
HP Service Manager 에 대한 연결 설정 (페이지 393)
BMC Remedy ITSM 에 대한 연결 설정 (페이지 395)
ServiceNow 에 대한 연결 설정 (페이지 399)

CA Service Desk Manager 에 대한 연결 설정

CA Service Desk Manager 와 통합하려면 다음 매개 변수를 제공하십시오.

- Protocol_SOAP
  CA Service Desk Manager SOAP 웹 서비스에 연결하는 데 사용되는 프로토콜을 지정합니다.
  유효한 값: http, https
  기본값: http
- Host_SOAP
  CA Service Desk Manager SOAP 웹 서비스에 연결하는 데 사용되는 호스트를 지정합니다.
  예: CA-SERDESK-S1
- Port_SOAP
  CA Service Desk Manager SOAP 웹 서비스에 연결하는 데 사용되는 포트 번호를 지정합니다.
  기본값: 8080
- Protocol _REST
  CA Service Desk Manager REST 웹 서비스에 연결하는 데 사용되는 프로토콜을 지정합니다.
  예: http
- Host_REST
  CA Service Desk Manager REST 웹 서비스에 연결하는 데 사용되는 호스트를 지정합니다.
  예: CA-SERDESK-S1
- Port_REST
  CA Service Desk Manager REST 웹 서비스에 연결하는 데 사용되는 포트 번호를 정의합니다.
  기본값: 8050
  SSL 포트: 8413

- 사용자 이름

  CA Service Desk Manager 웹 서비스에 연결하는 데 사용되는 사용자 ID 를 정의합니다.

  기본값: ServiceDesk

- 암호

  CA Service Desk Manager 사용자 암호를 정의합니다.

- DefaultAttachmentRepositoryName

  CA Service Desk Manager 첨부 파일을 저장하는 데 사용되는 기본 리포지토리를 정의합니다.

  기본값: Service Desk

CA Service Desk Manager 에 대한 자세한 내용은 CA Service Desk Manager 설명서를 참조하십시오.

HP Service Manager 에 대한 연결 설정

HP Service Manager 와 통합하려면 다음 매개 변수를 제공하십시오.

- 호스트

  HP Service Manager 에 연결하는 데 사용되는 호스트를 지정합니다.

- 포트

  HP Service Manager 에 연결하는 데 사용되는 포트 번호를 지정합니다.

  예: 13080

- 사용자 이름

  HP Service Manager 에 연결하는 데 사용되는 사용자 이름을 지정합니다.

- 암호

  HP Service Manager 에 연결하는 데 사용되는 암호를 지정합니다.

- HPSMClientURL
  HP Service Manager 에 연결하는 데 사용되는 HPSMClientURL 을 지정합니다.
  기본값: http://hpsm-host-name:port-number/webtier-9.32
- (선택 사항) Service Desk ProxyServer
  환경에서 HP Service Manager 에 연결하는 데 사용되는 프록시 서버를 지정합니다.
  예: proxy.xxx.com
- (선택 사항) Service Desk ProxyPort
  HP Service Manager 에 연결하기 위해 설정 및 사용되는 프록시 포트를 지정합니다.
  예: 80
- (선택 사항) Service Desk ProxyUser
  HP Service Manager 에 연결하는 데 사용되는 프록시 사용자를 지정합니다.
- (선택 사항) Service Desk ProxyPassword
  HP Service Manager 에 연결하는 데 사용되는 프록시 암호를 지정합니다.
- EnabledProtocol
  사용 중인 프로토콜을 지정합니다.
  기본값: http

(WebLogic) IDM_OPTS 구성

기본 WebLogic SAAJ 구현의 알려진 문제로 인해 다음과 같은 오류 메시지가 생성될 수 있습니다.

java.lang.UnsupportedOperationException: This class does not support SAAJ 1.3(이 클래스는 SAAJ 1.3 을 지원하지 않습니다.)

WebLogic 설치 디렉터리/user_projects/domains/base_domain/bin/setDomainEnv.cmd 에 구성된 IDM_OPTS 변수에 다음 속성을 추가하고 WebLogic 을 다시 시작하십시오.

```
-Djavax.xml.soap.MessageFactory=weblogic.xml.saaj.MessageFactoryImpl
```

HP Service Manager 에 대한 자세한 내용은 HP Service Manager 설명서를 참조하십시오.

BMC Remedy ITSM 에 대한 연결 설정

사전 요구 사항

BMC Remedy ITSM 에 대한 설정을 구성하기 전에 BMC Remedy 시스템의 SDK jar 파일을 서버에 복사하십시오. 이러한 파일은 CA Identity Manager 와 BMC Remedy 간의 통신을 가능하게 합니다.

다음 단계를 수행하십시오.

Windows 및 Linux 에 해당

1. BMC Remedy 시스템에서 다음 파일로 이동합니다.
   \\bmc\Software\ARSystem\Arserver\api\lib
2. 다음 SDK jar 파일을 복사합니다.
   - arapi8*.jar
   - arutil81*.jar
3. 복사한 jar 파일을 CA Identity Manager 시스템의 다음 위치에 저장합니다.
   iam_im.ear/ca-nim-sm.war/WEB-INF/lib
4. 응용 프로그램 서버를 다시 시작합니다.

매개 변수

BMC Remedy ITSM 과 통합하려면 다음 매개 변수를 제공하십시오.

- 호스트

  BMC Remedy ITSM 에 연결하는 데 사용되는 호스트를 정의합니다.

  기본값: bmc_host_name

- 포트

  BMC Remedy ITSM 에 연결하는 데 사용되는 포트 번호를 정의합니다.

  기본값: 0

- 사용자 이름

  BMC Remedy ITSM 에 연결하는 데 사용되는 사용자 이름을 정의합니다.

  기본값: admin

- 암호

  BMC Remedy ITSM 에 연결하는 데 사용되는 암호를 정의합니다.

- BMCRemedyClientURL

  BMC Remedy ITSM 에 연결하는 데 사용되는 BMCRemedyClientURL 을 정의합니다.

  예: http://bmc_client_host_name:8080/arsys

CA Cloud Service Management 에 대한 연결 설정

(WebSphere) 서버에서 인증서 검색

CA Cloud Service Management 와 CA Identity Manager 간의 통신을 가능하게 하려면 서버에서 인증서를 검색하여 NodeDefaultTrustStore 에 추가하십시오.

다음 단계를 수행하십시오.

1. WebSphere 관리 콘솔에서 "Security"(보안)를 확장하고 "SSL certificate and key management"(SSL 인증서 및 키 관리)를 클릭합니다.
2. "Configuration settings"(구성 설정) 아래에서 "Manage endpoint security configurations"(끝점 보안 구성 관리)를 클릭합니다.
3. 적절한 아웃바운드 구성을 선택하여 (셀): <서버 이름>Node01Cell:(노드):<서버 이름>Node01 관리 범위로 이동합니다.
4. "Related Items"(관련 항목) 아래에서 "Key stores and certificates"(키 저장소 및 인증서)를 클릭하고 "NodeDefaultTrustStore" 키 저장소를 클릭합니다.
5. "Additional Properties"(추가 속성) 아래에서 "Signer certificates"(서명자 인증서)를 클릭하고 "Retrieve From Port"(포트에서 검색)를 클릭합니다.
6. "Host"(호스트) 필드에 다음 매개 변수를 입력합니다.

   호스트 이름: sm2t.saas.ca.com

   포트: 443

   별칭: sm2t.saas.ca.com_cert
7. "Retrieve Signer Information"(서명자 정보 검색)을 클릭합니다.
8. 인증서 정보가 신뢰할 수 있는 인증서에 대한 것인지 확인합니다.
9. "Apply"(적용), "Save"(저장)를 클릭합니다.
10. WebSphere 를 다시 시작합니다.

서버에서 인증서를 검색했습니다.

매개 변수

CA Cloud Service Management 와 통합하려면 다음 매개 변수를 제공하십시오.

- URL
  CA Cloud Service Management 시스템에 연결하는 데 사용되는 URL 을 지정합니다.
  예: https://xxx.saas.ca.com/
  기본값: https://cacsmwebservice_host_name/
- 사용자 이름
  CA Cloud Service Management 에 연결하는 데 사용되는 사용자 이름을 지정합니다.
  예: webuser@org.com
- 암호
  CA Cloud Service Management 에 연결하는 데 사용되는 암호를 지정합니다.
- CACSMClient URL
  LaunchIncontext URL 에 사용되는 CACSMClient URL 을 지정합니다. LaunchIncontext 는 최종 사용자를 특정 CA Cloud Service Management 서비스 데스크 인시던트 ID 로 리디렉션합니다.
  예: https://xxx.saas.ca.com/
  기본값: https://cacsmclient_host_name/
- (선택 사항) Service Desk ProxyServer
  환경에서 CA Cloud Service Management 에 연결하는 데 사용되는 프록시 서버를 지정합니다.
  예: proxy.xxx.com

- (선택 사항) Service Desk ProxyPort
  CA Cloud Service Management 에 연결하기 위해 설정 및 사용되는 프록시 포트를 지정합니다.
  예: 80
- (선택 사항) Service Desk ProxyUser
  프록시 서버에 사용되는 사용자 이름을 지정합니다.
- (선택 사항) Service Desk ProxyPassword
  프록시 사용자 이름의 암호를 정의합니다.

CA Cloud Service Management 에 대한 자세한 내용은 CA Cloud Service Management 설명서를 참조하십시오.

ServiceNow 에 대한 연결 설정

REST API 에 관리자가 아닌 사용자에 대한 액세스 권한을 부여하기 위해 현재 인스턴스에서 사용자에게 rest_service 역할을 할당할 수 있습니다.

매개 변수

ServiceNow 와 통합하려면 다음 매개 변수를 제공하십시오.

- URL
  ServiceNow 에 연결하는 데 사용되는 URL 을 지정합니다.
  예: https://xxx.service-now.com/
  기본값: https://servicenow-webservice-host-name
- 사용자 이름
  ServiceNow 에 연결하는 데 사용되는 사용자 이름을 지정합니다.
- 암호
  ServiceNow 에 연결하는 데 사용되는 암호를 지정합니다.

- ServiceNowClientURL
  ServiceNow 에 연결하는 데 사용되는 ServiceNowClientURL 을 지정합니다.
  기본값: https://servicenow-host-name
- useCustomEndpoint
  사용자 지정 끝점을 통해 연결할지 여부를 지정합니다.
  기본값: False

  참고: 서비스 데스크 솔루션에서 이 옵션이 사용되도록 설정되어 있으면 모든 유효성 검사는 useCustomEndpoint 설정으로 수행됩니다.
- (선택 사항) Service Desk ProxyServer
  환경에서 ServiceNow 에 연결하는 데 사용되는 프록시 서버를 지정합니다.
  예: proxy.xxx.com
- (선택 사항) Service Desk ProxyPort
  ServiceNow 에 연결하기 위해 설정 및 사용되는 프록시 포트를 지정합니다.
  예: 80
- (선택 사항) Service Desk ProxyUser
  ServiceNow 에 연결하는 데 사용되는 프록시 사용자를 지정합니다.
- (선택 사항) Service Desk ProxyPassword
  ServiceNow 에 연결하는 데 사용되는 프록시 암호를 지정합니다.

(WebSphere) 서버에서 인증서 검색

ServiceNow 와 CA Identity Manager 간의 통신을 가능하게 하려면 서버에서 인증서를 검색하여 NodeDefaultTrustStore 에 추가하십시오.

다음 단계를 수행하십시오.

1. WebSphere 관리 콘솔에서 "Security"(보안)를 확장하고 "SSL certificate and key management"(SSL 인증서 및 키 관리)를 클릭합니다.
2. "Configuration settings"(구성 설정) 아래에서 "Manage endpoint security configurations"(끝점 보안 구성 관리)를 클릭합니다.
3. 적절한 아웃바운드 구성을 선택하여 (셀): <서버 이름>Node01Cell:(노드):<서버 이름>Node01 관리 범위로 이동합니다.
4. "Related Items"(관련 항목) 아래에서 "Key stores and certificates"(키 저장소 및 인증서)를 클릭하고 "NodeDefaultTrustStore" 키 저장소를 클릭합니다.
5. "Additional Properties"(추가 속성) 아래에서 "Signer certificates"(서명자 인증서)를 클릭하고 "Retrieve From Port"(포트에서 검색)를 클릭합니다.
6. "Host"(호스트) 필드에 다음 매개 변수를 입력합니다.

   호스트 이름: service-now.com

   포트: 443

   별칭: service-now.com_cert
7. "Retrieve Signer Information"(서명자 정보 검색)을 클릭합니다.
8. 인증서 정보가 신뢰할 수 있는 인증서에 대한 것인지 확인합니다.

9. "Apply"(적용), "Save"(저장)를 클릭합니다.
10. WebSphere 를 다시 시작합니다.

서버에서 인증서를 검색했습니다.

(WebLogic) 호스트 이름 확인자 구성

기본 WebLogic 호스트 이름 확인자에는 와일드카드가 포함된 호스트 이름과 관련한 문제가 있습니다. WebLogic 서버에서 SSLWLSWildcardHostnameVerifier 를 사용하도록 구성하십시오.

다음 단계를 수행하십시오.

1. WLS 콘솔에서 "Environment"(환경), "Servers"(서버), "AdminServer"(관리 서버)로 이동합니다.
2. "SSL" 탭을 선택하고 "Advanced"(고급)를 클릭합니다.
3. "Hostname verification"(호스트 이름 확인) 항목을 "Custom Hostname Verifier"(사용자 지정 호스트 이름 확인자)로 변경합니다.
4. "Custom Hostname Verifier"(사용자 지정 호스트 이름 확인자)에 다음 텍스트를 입력합니다.
   weblogic.security.utils.SSLWLSWildcardHostnameVerifier
5. "Use JSSE SSL"(JSSE SSL 사용)을 선택합니다.
6. "Save"(저장)를 클릭하고 WebLogic 을 다시 시작합니다.

호스트 이름 확인자를 구성했습니다.

Service Desk 필드 매핑 사용자 지정

서비스 데스크 통합을 구성할 때 기본적으로 일부 NIM 필드는 서비스 데스크 솔루션의 필드에 매핑됩니다. 이러한 필드 매핑을 사용자 지정하고, 매핑을 추가하고, 사용자 지정 필드 매핑을 만들 수 있습니다. 예를 들어 심각도 또는 긴급도 수준을 추가로 만들 수 있습니다.

새 필드 매핑 정의

다음 단계를 수행하십시오.

1. "시스템", "NIM SM Integration"으로 이동하고 "Service Desk 필드 매핑 사용자 지정"을 클릭합니다.
2. 매핑할 CA NIM 필드를 선택합니다.
3. NIM 에 매핑할 Service Desk 필드를 선택합니다.
4. (선택 사항) 기본값을 추가합니다.
5. (선택 사항) 가능한 값을 추가합니다.
6. "추가"를 클릭합니다.

새 필드 매핑을 정의했습니다.

참고: 기존 필드 매핑을 사용자 지정하려면 먼저 사용자 지정할 매핑을 삭제한 다음 새 필드 매핑을 정의할 때와 동일한 방법으로 매핑을 다시 추가하십시오.

사용자 지정 필드 매핑 정의

서비스 데스크 솔루션에 NIM 에서 자동으로 감지되지 않는 사용자 지정 필드가 포함되어 있는 경우 사용자 지정 필드 매핑을 정의하십시오.

다음 단계를 수행하십시오.

1. "시스템", "NIM SM Integration"으로 이동하고 "Service Desk 필드 매핑 사용자 지정"을 클릭합니다.
2. "사용자 지정 NIM 필드 사용"을 선택합니다.
3. "사용자 지정 NIM 필드"에서 필드의 이름을 정의합니다.
4. "데이터 유형"을 선택합니다.
   값: 날짜와 시간, 문자열
5. 사용자 지정 필드를 매핑할 Service Desk 필드를 선택합니다.
6. (선택 사항) 기본값을 추가합니다.
7. (선택 사항) 가능한 값을 추가합니다.
8. "추가"를 클릭합니다.

사용자 지정 필드 매핑을 정의했습니다.

참고: REST 호출에서 사용자 지정 필드는 기본 CA NIM 필드와는 다르게 사용됩니다. 다음 예에서는 REST 호출에서 사용자 지정 필드를 사용하는 방법을 보여 줍니다.

XML 요청 본문

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<incident>
   <description>test incident</description>
   <impact>high</impact>
   <label>label_change</label>
   <priority>critical</priority>
   <severity>high</severity>
   <status>new</status>
   <urgency>high</urgency>
   <customproperties>
      <property>
        <name>customField1</name>
        <value>10</value>
      </property>
   </customproperties>
</incident>
```

JSON 요청 본문

```
{
   "description": "test incident",
   "category": "inquiry",
   "customproperties": {
     "property": [
     {
       "name": "customField1",
       "value": "10"
     }
  ]
  },
  "impact": "high",
  "label": "label_change",
  "priority": "critical",
  "severity": "high",
  "status": "new",
  "urgency": "high"
}
```

Service Desk 통합 REST API 설명서

NIM 용 REST API 설명서는 CA Identity Manager 사용자 콘솔 내에서 사용할 수 있습니다.

"시스템", "NIM SM Integration"으로 이동하고 "Service Desk 통합 REST API 설명서 보기"를 클릭합니다. 열린 프레임에서 각 개체 유형의 모델을 보고, "Try it out!"(테스트) 단추를 사용하여 API 호출을 테스트할 수 있습니다.

다음에 주의하십시오.

- REST API 설명서에 액세스하려면 CA Identity Manager 서버 URL 에 전체 도메인을 사용하여 탐색해야 합니다. 예를 들어 http://myserver:8080/iam/im/env 가 아니라 http://myserver.domain.com:8080/iam/im/env 를 사용하십시오.
- "Try it out!"(테스트) 기능을 사용하려면 HTTP 기본 인증 헤더 필드에 기본 액세스 인증 정보를 입력해야 합니다. 이는 단지 표준 기본 인증 헤더입니다.

  예: 기본 인증 헤더 "Basic bmltYWRtaW46bmltYWRtaW4="에서 "bmltYWRtaW46bmltYWRtaW4="은 단순히 Base64 로 인코딩된 "사용자 이름:암호"입니다.

NIM SM Web Service 정보

NIM Web Service 를 호출하려면 다음 URL 을 사용하십시오.

- 기준 URL:
  http://myserver.domain.com:[서버 포트 번호]/iam/imnimsm/api/v1
- 기준 URL(클러스터 배포):
  http://localhost:[서버 포트 번호]/iam/imnimsm/api/v1(기준 URL)
- 특정 API 에 액세스하려면 URL 끝에 해당 이름을 추가하십시오.
  예: 인시던트 API 에 액세스하려면 다음 URL 을 사용하십시오.
  http://myserver.domain.com:[서버 포트 번호]/iam/imnimsm/api/v1/incident

NIM Web Service 는 HTTP 기본 인증을 사용하며 해당 자격 증명은 새로 설치할 때 CA 내장 구성 요소에 대해 제공된 사용자 이름과 암호이거나 업그레이드 후 설정한 업데이트된 자격 증명입니다.

NIM PolicyXpress 샘플

CA Identity Manager 12.6.5 에는 사용자 고유의 정책을 만들어야 할 때 유용한 샘플 Policy Xpress 가 포함되어 있습니다.

NimIntegrationSample.xml 에 포함된 샘플 정책을 현재 환경으로 가져올 수 있습니다. 이 파일은 CA Identity Manager 설치 디렉터리의 samples\PolicyXpress\NimIntegration 에 있습니다.

예: C:\Program Files (x86)\CA\Identity Manager\IAM Suite\Identity Manager\tools\samples\PolicyXpress\NimIntegration

자세한 내용은 샘플 정책과 같은 디렉터리에 있는 readme.txt 파일을 참조하십시오.

제 13 장: CA SiteMinder 통합

이 섹션은 다음 항목을 포함하고 있습니다.

SiteMinder 및 CA Identity Manager

CA Identity Manager 가 CA SiteMinder 와 통합되는 경우 CA SiteMinder 는 CA Identity Manager 환경에 다음 기능을 추가할 수 있습니다.

고급 인증

CA Identity Manager 에는 기본적으로 CA Identity Manager 환경에 대한 네이티브 인증이 포함되어 있습니다. CA Identity Manager 관리자가 CA Identity Manager 환경에 로그인하기 위해 유효한 사용자 이름과 암호를 입력합니다. 그러면 CA Identity Manager 는 CA Identity Manager 가 관리하는 사용자 저장소를 대상으로 이름과 암호를 인증합니다.

CA Identity Manager 가 CA SiteMinder 와 통합되는 경우 CA Identity Manager 는 CA SiteMinder 기본 인증을 사용하여 환경을 보호합니다. CA Identity Manager 환경을 만들면 해당 환경을 보호하기 위해 CA SiteMinder 에 정책 도메인과 인증 체계가 만들어집니다.

CA Identity Manager 가 CA SiteMinder 와 통합되는 경우 SiteMinder 인증을 사용하여 관리 콘솔을 보호할 수도 있습니다.

액세스 역할 및 태스크

액세스 역할을 사용하면 CA Identity Manager 관리자가 CA SiteMinder 로 보호되는 응용 프로그램 내의 권한을 할당할 수 있습니다. 액세스 역할은 재무 응용 프로그램에서 구매 주문을 생성하는 동작 같이 비즈니스 응용 프로그램에서 사용자가 수행할 수 있는 단일 동작을 나타냅니다.

디렉터리 매핑

관리자가 관리자 인증에 사용되는 것과 다른 사용자 저장소에 있는 프로필을 가지고 있는 사용자를 관리해야 하는 경우가 있습니다. 관리자가 CA Identity Manager 환경에 로그인하면 한 디렉터리를 사용하여 관리자가 인증되고 다른 디렉터리를 사용하여 관리자에게 사용자 관리 권한이 부여됩니다.

CA Identity Manager 가 CA SiteMinder 와 통합되는 경우 인증과 권한 부여에 서로 다른 디렉터리를 사용하도록 CA Identity Manager 환경을 구성할 수 있습니다.

다양한 사용자 세트에 대한 스킨

스킨은 사용자 콘솔의 모양을 변경합니다. CA Identity Manager 가 CA SiteMinder 와 통합되는 경우 다양한 사용자 세트에 서로 다른 스킨을 표시하도록 설정할 수 있습니다. 이렇게 변경하려면 SiteMinder 응답을 사용하여 스킨을 사용자 세트와 연결합니다. 응답은 사용자 세트와 연결된 정책 내의 규칙과 쌍으로 연결됩니다. 규칙이 실행되는 경우 응답이 트리거되어 스킨에 대한 정보가 CA Identity Manager 에 전달되고 사용자 콘솔이 작성됩니다.

참고: 자세한 내용은 *User Console Design Guide*(사용자 콘솔 디자인 안내서)를 참조하십시오.

지역화된 환경에 대한 로캘 기본 설정

CA Identity Manager 가 CA SiteMinder 와 통합되는 경우 imlanguage HTTP 헤더를 사용하여 사용자에 대한 로캘 기본 설정을 정의할 수 있습니다. SiteMinder 정책 서버에서 이 헤더를 SiteMinder 응답 내에 설정하고 사용자 특성을 헤더 값으로 지정합니다. 이 imlanguage 헤더는 사용자에 대해 가장 높은 우선 순위의 로캘 기본 설정 역할을 합니다.

참고: 자세한 내용은 *User Console Design Guide*(사용자 콘솔 디자인 안내서)를 참조하십시오.

추가 정보:

사용자 지정 인증 체계를 사용하여 사용자 자격 증명 수집 (페이지 484)

리소스의 보호 방식

고급 인증을 수행하려면 구현에서 SiteMinder 정책 서버를 사용해야 합니다. CA Identity Manager 서버를 호스트하는 응용 프로그램 서버는 웹 서버와 다른 운영 환경에 있습니다. 전달 서비스를 제공하려면 웹 서버에 다음 사항이 필요합니다.

- 응용 프로그램 서버 공급업체에서 제공한 플러그 인
- 사용자 콘솔, 자체 등록 및 잊어버린 암호 기능 같은 CA Identity Manager 리소스를 보호하기 위한 SiteMinder 에이전트

웹 에이전트는 CA Identity Manager 리소스를 요청하는 사용자의 액세스를 제어합니다. 사용자가 인증되고 권한이 부여된 후 웹 에이전트는 웹 서버가 요청을 처리할 수 있도록 허용합니다.

웹 서버가 요청을 받으면 응용 프로그램 서버 플러그 인이 CA Identity Manager 서버를 호스트하는 응용 프로그램 서버에 해당 요청을 전달합니다.

웹 에이전트는 사용자와 관리자에게 노출되는 CA Identity Manager 리소스를 보호합니다.

SiteMinder 및 CA Identity Manager 통합 개요

정책 관리자와 ID 관리자가 SiteMinder 를 기존 CA Identity Manager 설치에 통합하기 위해 함께 작업하는 경우 CA Identity Manager 아키텍처는 다음 구성 요소를 포함하도록 확장됩니다.

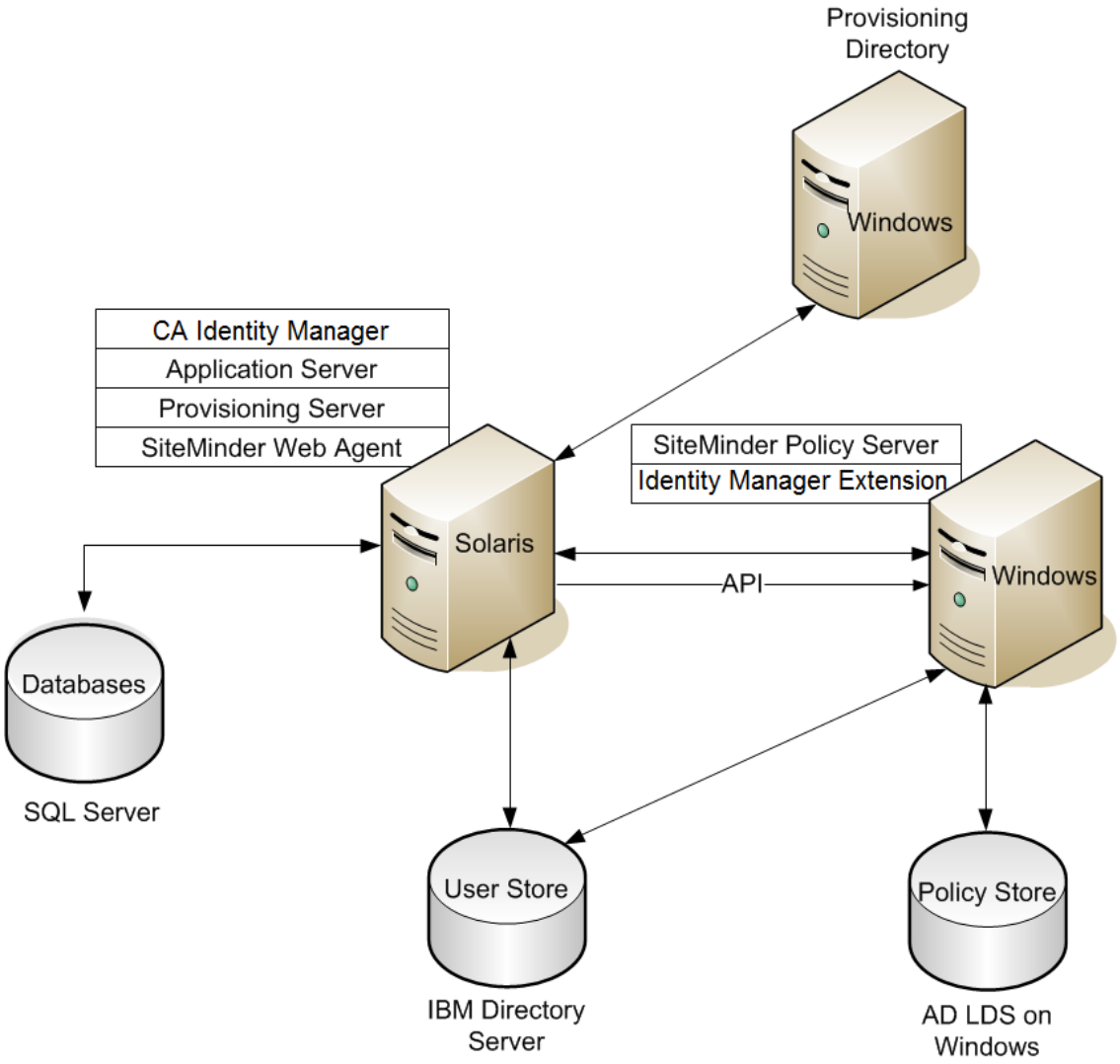
SiteMinder 웹 에이전트

CA Identity Manager 서버를 보호합니다. 웹 에이전트는 CA Identity Manager 서버가 있는 시스템에 설치됩니다.

SiteMinder 정책 서버

CA Identity Manager 에 대한 고급 인증과 권한 부여를 제공합니다.

다음 그림은 SiteMinder 정책 서버와 웹 에이전트가 있는 CA Identity Manager 설치의 예입니다.

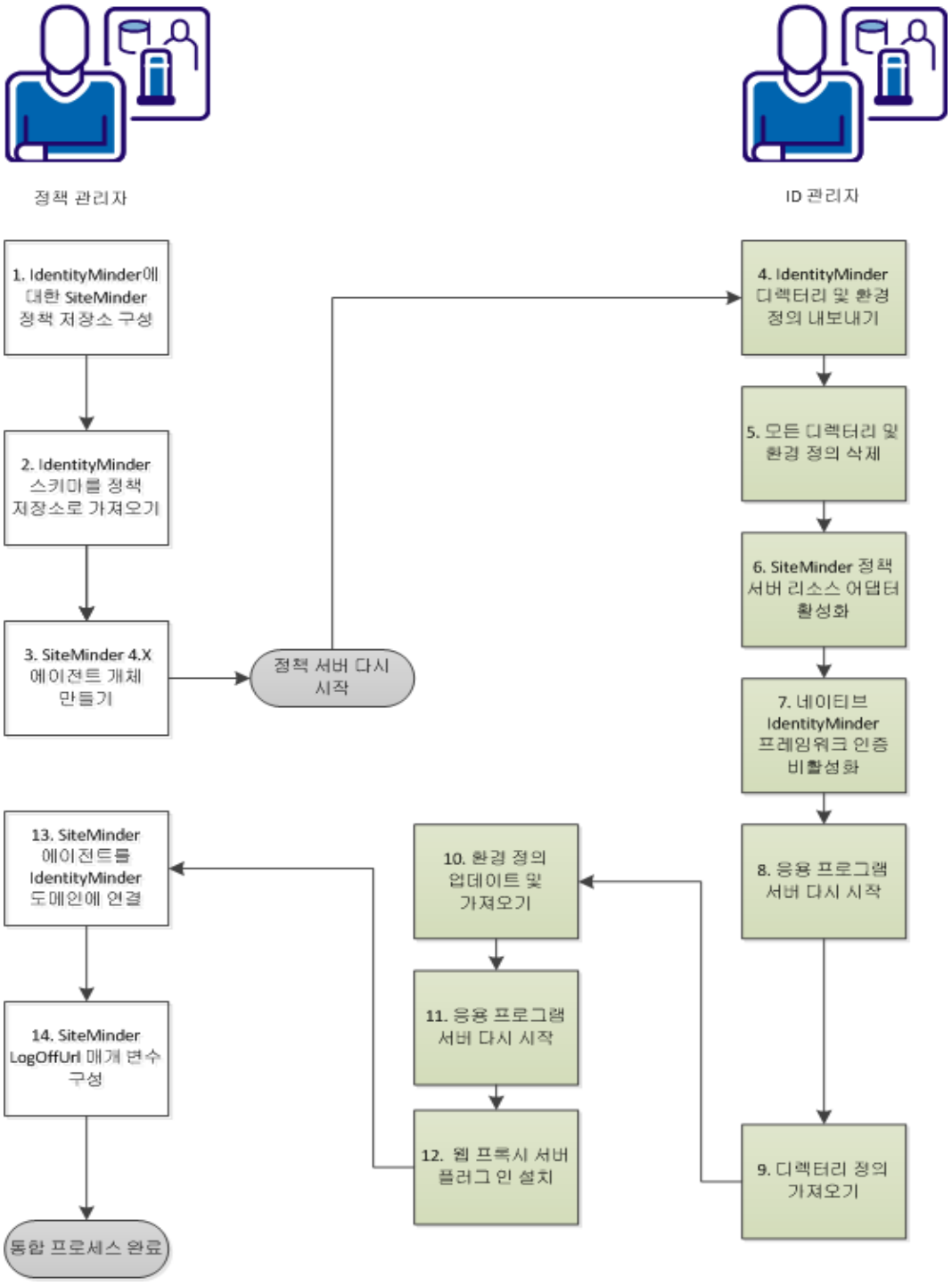


참고: 구성 요소는 예에서 볼 수 있듯이 서로 다른 플랫폼에 설치됩니다. 하지만 다른 플랫폼을 선택할 수도 있습니다. CA Identity Manager 데이터베이스는 Microsoft SQL Server 에 있고 사용자 저장소는 IBM Directory Server 에 있습니다. SiteMinder 정책 저장소는 Windows 의 AD LDS 에 있습니다.

이 프로세스를 완료하려면 CA Identity Manager ID 관리자와 SiteMinder 정책 관리자의 두 가지 역할이 필요합니다. 일부 조직에서는 한 사람이 두 역할을 모두 수행합니다. 두 사람이 관련된 경우 이 시나리오에 있는 절차를 완료하려면 긴밀한 공동 작업이 필요합니다. 정책 관리자는 이 프로세스를 시작 및 종료하고 ID 관리자는 중간의 모든 단계를 수행합니다.

중요! 릴리스 12.5 SP7 로 시작하는 CA Identity Manager 설치의 경우 Java Cryptography Extension Unlimited Strength Jurisdiction Policy Files(JCE 라이브러리)가 필요합니다. Oracle 웹 사이트에서 이러한 라이브러리를 다운로드하고 <Java_path>\<jdk_version>\jre\lib\security\ 폴더로 로드하십시오.

다음 다이어그램에서는 SiteMinder 를 CA Identity Manager 에 통합하는 전체 프로세스를 보여 줍니다.



다음 단계를 수행하십시오.

1. CA Identity Manager 에 대해 SiteMinder 정책 저장소를 구성합니다. (페이지 418)
2. CA Identity Manager 스키마를 정책 저장소로 가져옵니다. (페이지 427)
3. SiteMinder 4.x 에이전트 개체를 만듭니다. (페이지 427)
4. CA Identity Manager 디렉터리 및 환경을 내보냅니다. (페이지 429)
5. 모든 디렉터리 및 환경 정의를 삭제합니다. (페이지 430)
6. SiteMinder 정책 서버 리소스 어댑터가 사용되도록 설정합니다. (페이지 431)
7. 네이티브 CA Identity Manager 프레임워크 인증 필터가 사용되지 않도록 설정합니다. (페이지 433)
8. 응용 프로그램 서버를 다시 시작합니다. (페이지 434)
9. SiteMinder 에 대해 데이터 원본을 구성합니다. (페이지 434)
10. 디렉터리 정의를 가져옵니다. (페이지 435)
11. 환경 정의를 업데이트하고 가져옵니다. (페이지 436)
12. 응용 프로그램 서버를 다시 시작합니다. (페이지 434)
13. 웹 프록시 서버 플러그 인을 설치합니다. (페이지 436)
14. SiteMinder 에이전트를 CA Identity Manager 도메인과 연결합니다. (페이지 464)
15. SiteMinder LogOffUrl 매개 변수를 구성합니다. (페이지 465)

CA Identity Manager 에 대해 SiteMinder 정책 저장소 구성

정책 관리자는 CA Identity Manager 관리 도구를 통해 SQL 스크립트나 LDAP 스키마 텍스트에 액세스하여 IMS 스키마를 정책 저장소에 추가합니다. ID 관리자는 Admin Tools 폴더에 이러한 도구를 설치합니다. 정책 저장소를 구성하려면 다음 절차 중 *하나*를 따르십시오.

관계형 데이터베이스 구성 (페이지 419)

Sun Java Systems Directory Server 또는 IBM Directory Server 구성 (페이지 420)

Microsoft Active Directory 구성 (페이지 421)

Microsoft ADAM 구성 (페이지 422)

CA Directory Server 구성 (페이지 423)

Novell eDirectory Server 구성 (페이지 425)

OID(Oracle Internet Directory) 구성 (페이지 426)

관계형 데이터베이스 구성

구성 후 관계형 데이터베이스를 SiteMinder 정책 저장소로 사용할 수 있습니다.

다음 단계를 수행하십시오.

1. 데이터베이스를 지원되는 SiteMinder 정책 저장소로 구성합니다.

   참고: 구성 지침은 *SiteMinder Policy Server Installation Guide*(SiteMinder 정책 서버 설치 안내서)를 참조하십시오.

2. 사용 중인 데이터베이스에 적절한 다음 스크립트를 실행합니다.

   - **SQL:** C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\policystore-schemas\MicrosoftSQLServer\ims8_mssql_ps.sql
   - **Oracle:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools/policystore-schemas/OracleRDBMS/ims8_oracle_ps.sql

   앞의 경로는 기본 설치 위치입니다. 사용 중인 설치 위치가 다를 수 있습니다.

Sun Java Systems Directory Server 또는 IBM Directory Server 구성

Java 또는 IBM Directory Server 를 구성하려면 적절한 스키마 파일을 적용합니다.

다음 단계를 수행하십시오.

1. 지원되는 SiteMinder 정책 저장소로 디렉터리를 구성합니다.

   참고: 구성 지침은 *CA SiteMinder 정책 서버 설치 안내서*를 참조하십시오.

2. 디렉터리에 적절한 LDIF 스키마 파일을 추가합니다. Windows 에서 LDIF 파일의 기본 위치는 C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\policystore-schemas 입니다.

   사용 중인 디렉터리에 적절한 다음 스키마 파일을 추가합니다.

   - **IBM Directory Server:**
     IBMDirectoryServer\V3.identityminder8
   - **Sun Java Systems Directory Server(iPlanet):**
     SunJavaSystemDirectoryServer\sundirectory_ims8.ldif

Microsoft Active Directory 구성

Microsoft Active Directory 정책 저장소를 구성하려면 activedirectory_ims8.ldif 스크립트를 적용합니다.

다음 단계를 수행하십시오.

1. 지원되는 SiteMinder 정책 저장소로 디렉터리를 구성합니다.

   참고: 구성 지침은 *CA SiteMinder 정책 서버 설치 안내서*를 참조하십시오.

2. 다음과 같이 activedirectory_ims8.ldif 스키마 파일을 수정합니다.

   a. 텍스트 편집기에서 activedirectory_ims8.ldif 파일을 엽니다.
   Windows 에서 기본 위치는 다음과 같습니다.

   C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\policystore-schemas\MicrosoftActiveDirectory

   b. 모든 {root} 인스턴스를 디렉터리에 대한 루트 조직으로 바꿉니다.

   루트 조직은 정책 서버 관리 콘솔에서 정책 저장소를 구성할 때 지정한 루트 조직과 일치해야 합니다.

   예를 들어 루트가 dc=myorg,dc=com 인 경우
   dn: CN=imdomainid6,CN=Schema,CN=Configuration,{root}를 dn: CN=imdomainid6,CN=Schema,CN=Configuration,dc=myorg,dc=com 으로 바꿉니다.

   c. 파일을 저장합니다.

3. 사용 중인 디렉터리에 대한 설명서에 설명된 대로 스키마 파일을 추가합니다.

Microsoft ADAM 구성

Microsoft ADAM 정책 저장소를 구성하려면 adam_ims8.ldif 스크립트를 적용합니다.

다음 단계를 수행하십시오.

1. 지원되는 SiteMinder 정책 저장소로 디렉터리를 구성합니다.

   참고: 구성 지침은 *CA SiteMinder 정책 서버 설치 안내서*를 참조하십시오.

   CN 값(guid)을 기록해 둡니다.

2. 다음과 같이 adam_ims8.ldif 스키마 파일을 수정합니다.

   a. 텍스트 편집기에서 adam_ims8.ldif\.ldif 파일을 엽니다.
   Windows 에서 기본 위치는 다음과 같습니다.

   C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\policystore-schemas\MicrosoftActiveDirectory

   b. 모든 cn={guid} 참조를 이 절차의 1 단계에서 SiteMinder 정책 저장소를 구성할 때 찾은 문자열로 바꿉니다.

   예를 들어 guid 문자열이 CN={39BC711D-7F27-4311-B6C0-68FDEE2917B8}인 경우 모든 cn={guid} 참조를 CN={39BC711D-7F27-4311-B6C0-68FDEE2917B8}로 바꿉니다.

   c. 파일을 저장합니다.

3. 사용 중인 디렉터리에 대한 설명서에 설명된 대로 스키마 파일을 추가합니다.

CA Directory Server 구성

CA Directory Server 를 구성하려면 사용자 지정 스키마 파일을 만듭니다. 다음 단계에서 *dxserver_home* 은 CA Directory 가 설치된 디렉터리입니다. Windows 에서 이 파일의 기본 원본 위치는 C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\policystore-schemas\eTrustDirectory 입니다.

다음 단계를 수행하십시오.

1. 지원되는 SiteMinder 정책 저장소로 디렉터리를 구성합니다.

   참고: 구성 지침은 *CA SiteMinder 정책 서버 설치 안내서*를 참조하십시오.

2. etrust_ims8.dxc 를 *dxserver_home*\config\schema 에 복사합니다.

3. 다음과 같이 사용자 지정 스키마 구성 파일을 만듭니다.

   a. *dxserver_home*\config\schema\default.dxg 를 *dxserver_home*\config\schema*company_name*-schema.dxg 에 복사합니다.

   b. 다음 줄을 파일의 맨 아래에 추가하여 *dxserver_home*\config\schema*company_name*-schema.dxg 파일을 편집합니다.

   ```
   # Identity Manager Schema
   source "etrust_ims8.dxc";
   ```

4. etrust_ims_schema.txt 의 내용을 파일의 끝에 추가하여 *dxserver_home*\bin\schema.txt 파일을 편집합니다. Windows 에서 이 파일의 기본 원본 위치는 C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\policystore-schemas\eTrustDirectory 입니다.

5. 다음과 같이 사용자 지정 제한 구성 파일을 만듭니다.

   a. *dxserver_home*\config\limits\default.dxc 를 *dxserver_home*\config\limits*company_name*-limits.dxc 에 복사합니다.

   b. 다음과 같이 *dxserver_home*\config\limits*company_name*-limits.dxc 파일에서 기본 크기 제한을 5000 으로 늘립니다.

   ```
   set max-op-size=5000
   ```

   참고: CA Directory 를 업그레이드하면 limits.dxc 파일을 덮어씁니다. 따라서 업그레이드가 완료된 후 max-op-size 를 5000 으로 다시 설정해야 합니다.

6. 다음과 같이 *dxserver_home*\config\servers*dsa_name*.dxi 를 편집합니다.

   ```
   # schema
   source "company_name-schema.dxg";

   #service limits
   source "company_name-limits.dxc";
   ```

   여기서 *dsa_name* 은 사용자 지정된 구성 파일을 사용하는 DSA 의 이름입니다.

7. dxsyntax 유틸리티를 실행합니다.

8. 다음과 같이 DSA 를 중지했다가 dsa 사용자로 다시 시작하여 스키마 변경 내용을 적용합니다.

   ```
   dxserver stop dsa_name
   dxserver start dsa_name
   ```

Novell eDirectory Server 구성

Novell eDirectory Server 정책 저장소를 구성하려면 novell_ims8.ldif 스크립트를 적용합니다.

다음 단계를 수행하십시오.

1. 지원되는 SiteMinder 정책 저장소로 디렉터리를 구성합니다.

   참고: 구성 지침은 *CA SiteMinder 정책 서버 설치 안내서*를 참조하십시오.

2. 정책 서버가 설치된 시스템의 명령 창에 다음 정보를 입력하여 Novell eDirectory Server 에 대한 NCPServer 의 DN(고유 이름)을 찾습니다.

   ```
   ldapsearch -h hostname -p port -b container -s sub
   -D admin_login -w password objectClass=ncpServer dn
   ```

   예:

   ```
   ldapsearch -h 192.168.1.47 -p 389 -b "o=nwqa47container" -s sub -D
   "cn=admin,o=nwqa47container" -w password objectclass=ncpServer dn
   ```

3. novell_ims8.ldif 파일을 엽니다.

4. 모든 NCPServer 변수를 2 단계에서 찾은 값으로 바꿉니다.

   Windows 에서 novell_ims8.ldif 의 기본 위치는 다음과 같습니다.

   C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\policystore-schemas\NovelleDirectory

   예를 들어 DN 값이 cn=servername,o=servercontainer 인 경우 모든 *NCPServer* 인스턴스를 cn=servername,o=servercontainer 로 바꿉니다.

5. novell_ims8.ldif 파일로 eDirectory Server 를 업데이트합니다.

   지침은 Novell eDirectory 설명서를 참조하십시오.

OID(Oracle Internet Directory) 구성

Oracle Internet Directory 를 구성하려면 oracleoid ldif 파일을 업데이트합니다.

다음 단계를 수행하십시오.

1. 지원되는 SiteMinder 정책 저장소로 디렉터리를 구성합니다.

   참고: 구성 지침은 *CA SiteMinder 정책 서버 설치 안내서*를 참조하십시오.

2. oracleoid_ims8.ldif 파일로 Oracle Internet Directory Server 를 업데이트합니다. Window 에서 이 파일의 기본 설치 위치는 다음과 같습니다.

   install_path\policystore-schemas\OracleOID\

   지침은 Oracle Internet Directory 설명서를 참조하십시오.

정책 저장소 확인

정책 저장소를 확인하려면 다음 사항을 확인하십시오.

- 정책 서버 로그가 다음 코드로 시작하는 경고 섹션을 포함하지 않습니다.

  `*** IMS NO SCHEMA BEGIN`

  이 경고는 SiteMinder 정책 서버에 대한 확장을 설치했지만 정책 저장소 스키마를 확장하지 않은 경우에만 나타납니다.

- CA Identity Manager 개체는 정책 저장소 데이터베이스나 디렉터리에 있습니다. CA Identity Manager 개체는 ims 접두어로 시작합니다.

CA Identity Manager 스키마를 정책 저장소로 가져오기

정책 관리자가 CA Identity Manager 스키마를 정책 저장소로 가져옵니다. 이 태스크를 사용하면 CA Identity Manager 가 정책 개체를 만들고 업데이트하고 삭제할 수 있습니다. 예를 들어 디렉터리 개체, 도메인, 영역, 규칙, 정책, 액세스 역할 및 태스크가 사용되도록 설정하는 정책 개체 등이 포함됩니다.

다음 단계를 수행하십시오.

1. SiteMinder 정책 서버에서 정책 서버 서비스를 종료합니다.
2. 사용 중인 버전에 대한 CA Identity Manager 설치 관리자를 실행합니다.
3. 설치할 구성 요소를 묻는 메시지가 표시되면 "Extensions for SiteMinder"(SiteMinder 에 대한 확장)(SiteMinder 가 로컬로 설치된 경우)를 선택합니다.
4. 계속하기 전에 정책 서버 서비스가 다시 시작되었는지 확인합니다.

SiteMinder 4.x 에이전트 개체 만들기

정책 관리자가 SiteMinder 4.x 웹 에이전트를 만듭니다. 이 태스크를 사용하면 SiteMinder 와 CA Identity Manager 간에 통신할 수 있습니다. ID 관리자는 CA Identity Manager 구성 중에 이 에이전트를 참조합니다.

다음 단계를 수행하십시오.

1. SiteMinder 관리 UI 에 로그온합니다.

   관리자 권한과 관련된 탭이 표시됩니다.
2. "인프라", "에이전트", "에이전트", "에이전트 만들기"를 클릭합니다.

   "에이전트 만들기" 대화 상자가 나타납니다.

3. "에이전트 유형의 새 개체 만들기"를 선택한 다음 "확인"을 클릭합니다.

   "에이전트 만들기" 대화 상자가 나타납니다.

4. 이름과 설명(선택 사항)을 입력합니다.

   참고: 해당 SharePoint 연결 마법사와 손쉽게 연결할 수 있는 이름을 사용합니다.

5. "SiteMinder"를 선택하십시오.

6. 드롭다운 목록에서 "웹 에이전트"를 선택합니다.

7. 다음 단계를 수행하여 4.x 기능이 사용되도록 설정합니다.

   a. "4.x 에이전트 지원" 확인란을 선택합니다.

      트러스트 설정 필드가 나타납니다.

   b. 다음 필드에 정보를 입력하여 트러스트 설정을 추가합니다.

      IP 주소

      정책 서버의 IP 주소를 지정합니다.

      공유 암호

      4.x 에이전트 개체와 연결된 암호를 지정합니다. 이 암호는 SharePoint 연결 마법사에도 필요합니다.

      암호 확인

      4.x 에이전트 개체와 연결된 암호를 확인합니다. 이 암호의 확인은 SharePoint 연결 마법사에도 필요합니다.

8. "제출"을 클릭합니다.

   "Create Agent Object"(에이전트 개체 만들기) 태스크가 처리를 위해 제출되고 확인 메시지가 나타납니다.

CA Identity Manager 디렉터리 및 환경 내보내기

통합 프로세스는 현재 환경 및 디렉터리 정의를 모두 제거합니다. 이 정보가 유지되도록 하기 위해 ID 관리자는 CA Identity Manager 관리 콘솔을 사용하여 환경을 내보냅니다. 통합을 완료한 후 이러한 정의를 사용하여 디렉터리 및 환경을 복원할 수 있습니다.

다음 단계를 수행하십시오.

1. CA Identity Manager 관리 콘솔을 엽니다.
2. "Directories"(디렉터리)를 클릭합니다.
3. 목록에서 첫 번째 디렉터리를 클릭하고 "Export"(내보내기)를 클릭합니다.
4. directory xml 파일을 저장하고 보관합니다.
5. 나머지 디렉터리에 대해 이 프로세스를 반복합니다.
6. "Home"(홈), "Environments"(환경)을 차례로 클릭합니다.
7. 첫 번째 환경을 선택합니다.
8. "Export"(내보내기)를 클릭합니다.
9. 나머지 환경에 대해 이 프로세스를 반복합니다.

   참고: 이 프로세스를 완료하려면 각 환경에 대해 몇 분 정도씩 걸릴 수 있습니다.

모든 디렉터리 및 환경 정의 삭제

SiteMinder 가 CA Identity Manager 를 보호하도록 준비하기 위해 ID 관리자는 CA Identity Manager 관리 콘솔을 사용하여 디렉터리 및 환경 정의를 삭제합니다.

다음 단계를 수행하십시오.

1. CA Identity Manager 관리 콘솔을 엽니다.
2. "Environments"(환경)를 클릭합니다.
3. 첫 번째 환경을 선택합니다.
4. "Delete"(삭제)를 클릭합니다.
5. 나머지 환경 각각에 대해 이 프로세스를 반복합니다.

   참고: 환경이 디렉터리를 참조하므로 디렉터리를 삭제하기 전에 환경을 삭제하십시오.
6. "Directories"(디렉터리) 섹션으로 다시 이동합니다.
7. 나열된 디렉터리를 모두 선택합니다.
8. "Delete"(삭제)를 클릭합니다.

SiteMinder 정책 서버 리소스 어댑터가 사용되도록 설정

ID 관리자가 SiteMinder 정책 서버 리소스 어댑터가 사용되도록 설정합니다. 어댑터의 용도는 SMSESSION 쿠키의 유효성을 검사하는 것입니다. 유효성 검사 후 SiteMinder 가 사용자 컨텍스트를 만듭니다.

다음 단계를 수행하십시오.

1. CA Identity Manager 를 실행 중인 응용 프로그램 서버에서 iam_im.ear 내의 \policysever.rar\META-INF 폴더로 이동합니다.
2. 편집기에서 ra.xml 파일을 엽니다.
3. Enabled config-property 를 검색하고 다음 예제와 같이 config-property-value 를 true 로 변경합니다.

```
        <config-property-name>validateSMHeadersWithPS</config-property-name>
        <config-property-type>java.lang.String</config-property-type>
        <config-property-value>true</config-property-value>
    </config-property>
    <config-property>
        <config-property-name>Enabled</config-property-name>
        <config-property-type>java.lang.String</config-property-type>
        <config-property-value>true</config-property-value>
    </config-property>
    <!-- Set FIPS Mode to true if SiteMinder is in FIPS Only Mode -->
    <config-property>
        <config-property-name>FIPSMode</config-property-name>
```

4. ConnectionURL 속성을 찾고 SiteMinder 정책 서버의 호스트 이름을 제공합니다. FQDN(정규화된 도메인 이름)을 사용합니다.
5. UserName 속성을 찾고 SiteMinder 와의 통신에 사용할 계정을 지정합니다. SiteMinder 가 이 계정의 기본값입니다.
6. AdminSecret 속성을 찾습니다. 암호화된 암호를 제공합니다. 내보낸 directory.xml 파일에서 암호를 복사하여 ra.xml 에 붙여넣습니다. 암호가 일반 암호인지 확실하지 않을 경우 CA Identity Manager 암호 도구를 사용하여 암호를 암호화합니다.
7. 암호화된 암호를 ra.xml 파일에 붙여넣습니다.

8. 정책 관리자가 SiteMinder 구성 중에 만든 4.x 에이전트 이름을 지정합니다.
9. 암호화된 암호를 지정합니다. 필요한 경우 암호 도구를 사용하여 암호를 암호화합니다.
10. ra.xml 파일의 변경 내용을 저장합니다.

SiteMinder 정책 서버 리소스 어댑터가 사용되도록 설정되었습니다.

추가 정보:

SiteMinder 암호 또는 공유 암호 수정 (페이지 512)

네이티브 CA Identity Manager 프레임워크 인증 필터가 사용되지 않도록 설정

SiteMinder 어댑터가 있으면 프레임워크 인증 필터가 더 이상 필요하지 않습니다. ID 관리자가 필터가 사용되지 않도록 설정할 수 있습니다.

다음 단계를 수행하십시오.

1. iam_im.ear 아래의 \user_console.war\WEB-INF 폴더에서 web.xml 파일을 찾아서 편집합니다.
2. FrameworkAuthFilter 를 찾고 Enable init-param 의 값을 false 로 전환합니다.

   CA Identity Manager r12.5 SP7 이상을 사용 중인 경우 Java Cryptographic Extension Unlimited Strength Jurisdiction Policy Files(JCE)가 CA Identity Manager 환경의 \<Java_path>\<jdk_version>\jre\lib\security 로 다운로드되었는지 확인합니다. 이러한 파일을 통해 CA Identity Manager 가 SiteMinder 에 연결될 수 있습니다.

   JCE 라이브러리가 설치된 경우 CA Identity Manager 응용 프로그램을 시작하는 동안 다음 메시지가 표시됩니다.

   ```
   2012-07-06 11:23:56,079 WARN  [ims.default] (main) * Startup Step 2 : Attempting to start PolicyServerService(시작 단계 2: PolicyServerService 시작하는 중)
   2012-07-06 11:23:56,081 WARN  [ims.default] (main) Unlimited Strength Java Crypto Extensions enabled: TRUE(Java Crypto Extensions 사용: TRUE)
   ```

   그렇지 않은 경우 "Unlimited Strength Java Crypto Extensions enabled"(Unlimited Strength Java Crypto Extensions 사용) 항목에 대한 값은 false 입니다. 따라서 CA Identity Manager 가 정책 서버에 연결하지 못합니다.

응용 프로그램 서버 다시 시작

다시 시작하면 응용 프로그램 서버가 변경 내용으로 새로 고쳐집니다. ID 관리자는 전환이 성공했는지, 적절한 SiteMinder 정책 서버 연결이 있는지 검사합니다.

다음 단계를 수행하십시오.

1. 응용 프로그램 서버가 서비스로 실행되고 있는 경우 CA Identity Manager 를 다시 시작하려면 서비스 패널을 사용합니다.
2. 연결의 유효성을 검사하려면 server.log 를 참조하십시오.

SiteMinder 에 대한 데이터 원본 구성

관계형 데이터베이스가 CA Identity Manager 환경의 ID 저장소로 사용되는 경우 ID 관리자는 SiteMinder 정책 서버에서 추가 프로세스를 완료해야 합니다. SiteMinder 가 데이터베이스와 통신하려면 로컬 데이터 원본이 필요합니다.

다음 단계를 수행하십시오.

1. Windows 서버의 경우 "관리 도구" 아래의 "ODBC 데이터 원본 관리자" 콘솔을 엽니다.
2. "시스템 DSN" 탭을 클릭합니다.
3. "추가"를 클릭하고 데이터베이스에 해당하는 SiteMinder 드라이버를 선택합니다.
4. 관계형 데이터베이스 사용자 저장소를 참조하는 데 필요한 정보를 제공합니다.
5. 계속하기 전에 연결을 테스트합니다.

디렉터리 정의 가져오기

환경을 가져오도록 준비하기 위해 ID 관리자는 환경이 참조하는 디렉터리를 가져옵니다. 또한 CA Identity Manager 의 디렉터리 정의를 가져오면 디렉터리 정보가 SiteMinder 정책 저장소에 추가됩니다.

다음 단계를 수행하십시오.

1. CA Identity Manager 가 실행 중인 상태로 SiteMinder 에 연결되었는지 확인합니다.
2. CA Identity Manager 관리 콘솔로 이동합니다.
3. "Directories"(디렉터리)를 클릭하고 "Create"(만들기) 또는 "Update from XML"(XML 에서 업데이트)을 클릭합니다.
4. 디렉터리 구성 파일(directory.xml)을 선택합니다. 이 파일은 CA Identity Manager 디렉터리 및 환경 내보내기 (페이지 429)를 수행할 때 내보낸 파일입니다.
5. "Next"(다음)를 클릭합니다.
6. "Finish"(마침)를 클릭하고 로드 출력을 검토합니다. 디렉터리가 CA Identity Manager 와 SiteMinder 에 있는지 확인합니다.
7. 프로비저닝 저장소와 모든 나머지 디렉터리에 대해 이러한 단계를 반복합니다.
8. SiteMinder 관리 UI 에 로그인하여 만든 사용자 디렉터리의 유효성을 검사합니다.

환경 정의 업데이트 및 가져오기

ID 관리자가 업데이트된 환경을 CA Identity Manager 로 다시 가져옵니다.

다음 단계를 수행하십시오.

1. 디렉터리 내보내기와는 달리 환경 내보내기는 zip 파일 형식입니다. *name*.xml 파일의 사본을 zip 파일 외부로 끌어서 놓습니다.
2. *name*.xml 파일을 복사합니다. 보호 에이전트(SM 4.x 에이전트가 아님)에 대한 참조인 *agent="idmadmin"*을 ImsEnvironment 요소 끝의 닫는 /> 괄호 앞에 삽입합니다.
3. 파일을 저장하고 zip 파일에 다시 붙여넣습니다.
4. CA Identity Manager 관리 콘솔을 열고 "Environments"(환경), "Import"(가져오기)를 차례로 클릭합니다.
5. 업데이트된 환경 zip 파일의 이름을 입력합니다.
6. "Finish"(마침)를 클릭하고 가져오기 출력을 검토합니다.
7. 나머지 환경 모두에 대해 이 프로세스를 반복합니다.
8. 응용 프로그램 서버를 다시 시작합니다.

웹 프록시 서버 플러그 인 설치

설치된 응용 프로그램을 기반으로 ID 관리자는 웹 서버가 응용 프로그램 서버에 요청을 전달하는 데 사용하는 다음 플러그 인 중 하나를 설치합니다.

- WebSphere (페이지 438)
- JBoss (페이지 448)
- WebLogic (페이지 454)

WebSphere 에 프록시 플러그 인 설치

웹 에이전트가 설치된 웹 서버는 CA Identity Manager 서버를 호스트하는 응용 프로그램 서버에 요청을 전달합니다. 공급업체에서 제공한 웹 서버 프록시 플러그 인이 이러한 서비스를 제공합니다.

다음 중 배포에 해당하는 절차를 사용하십시오.

1. IBM HTTP Sever 구성 (페이지 438)(모든 웹 서버)
2. 프록시 플러그 인 구성 (페이지 439)(모든 웹 서버)
3. 다음 중 하나를 수행합니다.
   - IIS 에서 구성 완료 (페이지 444)
   - iPlanet 또는 Apache 에서 구성 완료 (페이지 447)

IBM HTTP Server 구성

모든 웹 서버의 경우 프록시 플러그 인을 설치하고 configurewebserver 명령을 사용합니다.

다음 단계를 수행하십시오.

1. WebSphere Launch Pad 에서 프록시 플러그 인을 설치합니다.
2. 다음과 같이 configurewebserver1.bat 명령을 실행하여 웹 서버를 WebSphere 셀에 추가합니다.
   a. 텍스트 편집기에서 *websphere_home*\Plugins\bin\configurewebserver1.bat/.sh 를 편집합니다.
   b. 다음과 같이 사용자 이름과 암호를 wsadmin.bat/.sh 뒤에 추가합니다.
   ```
   wsadmin.bat -user wsadmin -password password -f
   configureWebserverDefinition.jacl
   ```
   c. configurewebserver1.bat/.sh 를 실행합니다.

   참고: configurewebserver 명령에 대한 자세한 내용은 IBM WebSphere 설명서를 참조하십시오.
3. 계속해서 프록시 플러그 인 구성 (페이지 439) 절차를 진행합니다.

프록시 플러그 인 구성

모든 웹 서버의 경우 WebSphere 의 GenPluginCfg 명령을 사용하여 플러그 인을 업데이트하십시오.

다음 단계를 수행하십시오.

1. WebSphere 가 설치된 시스템에 로그인합니다.
2. 명령줄에서 *websphere_home*\bin 으로 이동합니다. 여기서 *websphere_home* 은 WebSphere 가 설치된 위치입니다.

   예:

   - **Windows:**

     C:\Program Files\WebSphere\AppServer\profile\AppSrv01\bin
   - **UNIX:**

     /*home_dir*/WebSphere/AppServer/profile/AppSrv01/bin
3. GenPluginCfg.bat 또는 GenPluginCfg.sh 명령을 실행합니다.

   이 명령을 실행하면 다음 위치에 plugin-cfg.xml 파일이 생성됩니다.

   websphere_home\AppServer\profiles\AppSrv01\config\cells
4. 계속해서 다음 절차 중 하나를 진행합니다.
   - IIS 에서 구성 완료 (페이지 444)
   - iPlanet 또는 Apache 에서 구성 완료 (페이지 447)

IIS(7.x)에서 구성 완료

이 절차를 시작하기 전에 웹 서버 플러그 인 버전 6.1.0.9 이상을 사용하고 있는지 확인하십시오. 이전 버전의 플러그 인은 Windows Server 2008 운영 체제를 지원하지 않습니다.

다음 단계를 수행하십시오.

1. IIS 버전 6.0 관리 호환성 구성 요소와 함께 IIS 버전 7.x 를 설치합니다. IIS 버전 6.0 관리 호환성 구성 요소는 기본적으로 설치되어 있지 않습니다.
2. 다음 단계를 완료하여 Windows Server 2008 에서 "서버 관리자" 창을 표시합니다.
    1. "시작", "관리 도구", "서버 관리자"를 차례로 클릭합니다.
    2. "동작", "역할 추가", "다음"을 차례로 클릭합니다.
    3. "서버 역할 선택" 페이지에서 "웹 서버(IIS)" 역할을 선택하고 "다음"을 클릭합니다.
    4. Windows Process Activation Service 기능에 대한 프롬프트가 표시되면 "기능 추가", "다음"을 차례로 클릭합니다.
    5. IIS 소개 페이지에서 "다음"을 클릭합니다.
3. "역할 서비스" 창이 표시되면 이미 선택된 기본 옵션 외에도 다음 옵션이 선택되었는지 확인합니다.
    - 인터넷 정보 서비스: 관리 도구
    - IIS 버전 6.0 관리 호환성: IIS 버전 6.0 관리 콘솔, IIS 버전 6.0 스크립팅 도구, IIS 버전 6.0 WMI 호환성, IIS 메타베이스 호환성
    - 응용 프로그램 개발: ISAPI 확장, ISAPI 필터
4. "다음"을 클릭하여 선택된 옵션이 사용되도록 설정하고 다음 창에서 "설치"를 클릭하여 설치를 수행합니다.
5. 설치가 완료되면 "설치 결과" 창에서 "닫기"를 클릭합니다.

6. 명령 프롬프트를 열고 :\Program Files\IBM\WebSphere\AppServer\profiles\Dmgr01\bin 으로 이동합니다.
7. GenPluginCfg.bat 명령을 실행합니다.

   plugin-cfg.xml 파일이 C:\Program Files\IBM\WebSphere\AppServer\profiles\Dmgr01\config\cells 위치에 생성됩니다.
8. c:\ 아래에 디렉터리(예: c:\plugin)를 만듭니다.
9. plugin-cfg.xml 파일을 c:\plugin 디렉터리에 복사합니다.
10. iisWASPlugin_http.dll 파일을 c:\plugin 디렉터리에 복사합니다.
11. Windows Server 2008 운영 체제에서 "시작", "모든 프로그램", "관리 도구", "IIS(인터넷 정보 서비스) 관리자"를 차례로 선택합니다. 이 작업을 수행하면 IIS 응용 프로그램이 시작되면서 웹 사이트 인스턴스에 대한 가상 디렉터리가 새로 만들어집니다. 이 지침에서는 기본 웹 사이트를 사용하고 있다고 가정합니다.
12. 기본 웹 사이트가 표시될 때까지 왼쪽의 트리를 확장합니다.
13. "기본 웹 사이트", "가상 디렉터리 추가"를 마우스 오른쪽 단추로 클릭하여 기본 설치가 있는 디렉터리를 만듭니다.
14. 가상 디렉터리 만들기 마법사의 "가상 디렉터리 별칭" 창에 있는 "별칭" 필드에 setPlugins 를 입력합니다.
15. 마법사의 "웹 사이트 콘텐츠 디렉터리" 창의 "실제 경로" 필드에 있는 c:\plugin 디렉터리로 이동하고 "확인"을 클릭합니다.
16. "설정 테스트" 단추를 클릭합니다. 설정 테스트가 실패하는 경우 실제 디렉터리의 사용 권한을 변경할 수 있습니다. 또는 "연결 계정"을 선택하고 IIS 가 해당 실제 경로의 파일에 대한 권한이 있는 Windows 사용자 계정으로 연결될 때까지 기다립니다.
17. "확인"을 클릭하여 setPlugins 가상 디렉터리를 웹 사이트에 추가합니다.

18. 탐색 트리에서 방금 만든 setPlugins 가상 디렉터리를 선택합니다.
19. "처리기 매핑"을 두 번 클릭하고 "동작" 패널에서 "기능 사용 권한 편집"을 클릭합니다.
20. 아직 선택되지 않은 경우 "스크립트"와 "실행"을 차례로 선택합니다.
21. "확인"을 클릭합니다.
22. "IIS 관리자" 창으로 돌아가고 해당 창의 왼쪽 탐색 트리에서 웹 사이트 폴더를 확장합니다.
23. 탐색 트리에서 "기본 웹 사이트"를 선택합니다.
24. 기본 웹 사이트의 속성 패널에서 다음 단계를 완료하여 ISAPI 필터를 추가합니다.
    1. "ISAPI 필터" 탭을 두 번 클릭합니다.
    2. 클릭하여 "필터 속성 추가/편집" 대화 상자를 엽니다.
    3. "필터 이름" 필드에 iisWASPlugin 을 입력합니다.
    4. "찾아보기"를 클릭하여 c:\plugin\iisWASPlugin_http.dll 디렉터리에 있는 플러그 인 파일을 선택합니다.
    5. "확인"을 클릭하여 "필터 속성 추가/편집" 대화 상자를 닫습니다.
25. 탐색 트리에서 최상위 서버 노드를 선택합니다.
26. "기능" 패널에서 "ISAPI 및 CGI 제한"을 두 번 클릭합니다.

    "ISAPI 또는 CGI 경로" 속성에 대해 지정할 값을 확인하려면 이전 단계에서 선택한 동일한 플러그 인 파일을 찾아서 선택하십시오. 예를 들어 c:\plugin\iisWASPlugin_http.dll 을 선택합니다.
27. "동작" 패널에서 "추가"를 클릭합니다.
28. "설명" 필드에 WASPlugin 을 입력하고 "확장 경로 실행 허용"을 선택한 다음 "확인"을 클릭하여 "ISAPI 및 CGI 제한" 대화 상자 창을 닫습니다.

29. c:\plugin 위치에 새 plugin-cfg.loc 파일을 만듭니다. plugin-cfg.loc 파일에 있는 값을 구성 파일의 위치로 설정합니다. 기본 위치는 C:\plugin\plugin-cfg.xml 입니다.

웹 에이전트 업데이트

IIS 7.x 를 구성한 후에는 웹 에이전트를 다음과 같이 변경하십시오.

1. "응용 프로그램 풀"을 클릭하고 "기본 응용 프로그램 풀"을 "클래식 모드"로 변경합니다.
2. 제출을 클릭합니다.
3. ISAPI 필터 우선 순위 목록에서 CA Identity Manager 에서 사용되는 응용 프로그램 서버의 플러그 인보다 에이전트의 우선 순위가 높게 하십시오.
4. IIS 버전 7.x 와 WebSphere 응용 프로그램 서버 프로필을 다시 시작합니다.

IIS 에서 구성 완료

IBM HTTP Server 와 프록시 플러그 인을 구성했으면 프록시 plugin-cfg.xml 이 올바른 위치에 있는지 확인하고 추가 플러그 인 파일 구성 단계를 수행하십시오.

다음 단계를 수행하십시오.

1. 다음과 같이 plugin-cfg.xml 을 복사합니다.
   a. 웹 에이전트가 설치된 시스템에 로그인합니다.
   b. C: 드라이브 아래에 공백 없이 폴더를 만듭니다. 예를 들어 C:\plugin 을 만듭니다.
   c. plugin-cfg.xml 파일을 c:\plugin 폴더에 복사합니다.
2. C:\plugin 폴더에 plugin-cfg.loc 라는 파일을 만들고 이 파일에 다음 줄을 추가합니다.

   C:\plugin\plugin-cfg.xml
3. www.ibm.com 에서 WebSphere 가 설치된 시스템으로 Websphere Plugin 설치 관리자를 다운로드합니다.
4. WebSphere Plugin 설치 관리자의 위치로 이동합니다.
5. 다음 명령을 사용하여 iisWASPlugin_http.dll 파일을 생성합니다.

   ```
   install is:javahome "c:\IBM\WebSphere\AppServer\Java
   ```

   사용 중인 구성을 기반으로 표시된 질문에 응답합니다.

   마법사가 종료되면 iisWASPlugin_http.dll 파일이 C:\IBM\WebSphere\Plugs\bin 폴더에 저장됩니다. 32 비트 또는 64 비트 하위 폴더를 찾습니다.

6. iisWASPlugin_http.dll 파일을 웹 에이전트가 있는 시스템의 C:\plugin 폴더에 복사합니다.
7. 다음과 같이 가상 디렉터리를 만듭니다.
   a. "IIS 관리자"를 엽니다.
   b. "기본 웹 사이트"를 마우스 오른쪽 단추로 클릭합니다.
   c. "새 가상 디렉터리"를 클릭하고 다음 값을 제공합니다.

      별칭: sePlugins(대소문자 구분)

      경로: c:\plugin

      사용 권한: 읽기 + 실행(ISAPI 또는 CGI)
8. 다음과 같이 ISAPI 필터를 추가합니다.
   a. "기본 웹 사이트"를 마우스 오른쪽 단추로 클릭합니다.
   b. "속성"을 클릭합니다.
   c. "ISAPI 필터" 탭에서 "추가"를 클릭합니다.
   d. 다음 값을 제공합니다.

      필터 이름: sePlugins

      실행 파일: c:\plugin\ iisWASPlugin_http.dll
9. 다음과 같이 웹 서비스 확장을 만듭니다.
   a. "IIS6 관리자"에서 컴퓨터 이름을 확장합니다.
   b. 웹 서비스 확장을 만들고 "허용됨"으로 설정합니다.

      확장 이름: WASPlugin

      경로: C:\plugin\ iisWASPlugin_http.dll
   c. 각 웹 서비스 확장을 마우스 오른쪽 단추로 클릭하여 "허용됨" 상태로 변경합니다.

10. IIS 웹 서버를 다시 시작합니다.

    마스터 WWW 서비스에서 WebSphere 플러그 인(sePlugin)이 SiteMinder 웹 에이전트 플러그 인 뒤에 나타나는지, WebSphere 플러그 인이 성공적으로 시작되는지 확인합니다.

iPlanet 또는 Apache 에서 구성 완료

IBM HTTP Server 와 프록시 플러그 인을 구성했으면 프록시 plugin-cfg.xml 이 올바른 위치에 있는지 확인하고 웹 서버를 다시 시작하십시오.

다음 단계를 수행하십시오.

1. 프록시 플러그 인을 설치한 시스템에서 다음 위치로 plugin-cfg.xml 을 복사합니다.

   websphere_home\AppServer\profiles*server_name*\config\cells*websphere_cell*\nodes\webserver1_node\servers\webserver1\

2. WebSphere 플러그 인(libns41_http.so)이 모든 iPlanet Web Server 의 SiteMinder 웹 에이전트 플러그 인(NSAPIWebAgent.so) 뒤에 로드되는지 확인합니다.

3. IPlanet 6.0 웹 서버의 경우

   iplanet_home/https-*instance*/config/magnus.conf 에서 플러그 인의 순서를 확인합니다.

4. *iplanet_home*/https-*instance*/config/magnus.conf 에서 *iplanet_home*/https-*instance*/config/obj.conf 로 다음 줄을 복사합니다(IPlanet 5.x 웹 서버).

   ```
   Init fn="load-modules" funcs="as_init,as_handler,as_term"
   shlib="/export/WebSphere/AppServer/bin/libns41_http.so"

   Init fn="as_init"
   bootstrap.properties="/export/WebSphere/AppServer/config/cells/
   plugin-cfg.xml"
   ```

   obj.conf 파일의 AuthTrans fn="SiteMinderAgent" 뒤에 다음 코드를 추가합니다.

   ```
   Service fn="as_handler"
   ```

5. SiteMinder 웹 에이전트 플러그 인(mod2_sm.so)이 Apache Web Server 의 WebSphere 플러그 인(mod_ibm_app_server_http.so) 앞에 로드되는지 확인합니다. 이 명령은 *apache_home*/config/httpd.conf 의 Dynamic Shared Object (DSO) Support 섹션에 있습니다.

6. 웹 서버를 다시 시작합니다.

JBoss 에 대한 프록시 플러그 인 설치

SiteMinder 웹 에이전트가 CA Identity Manager 리소스에 대한 요청을 인증하고 권한 부여한 후 웹 서버가 CA Identity Manager 서버를 호스트하는 응용 프로그램 서버로 요청을 전달합니다. 이러한 요청을 전달하려면 JK 커넥터를 SiteMinder 웹 에이전트가 설치된 시스템에 설치하고 구성하십시오. JK 커넥터에 대한 자세한 내용은 다음 Jakarta Project 웹 사이트를 참조하십시오.

http://community.jboss.org/wiki/usingmodjk12withjboss

CA Identity Manager 관리 도구에는 JK 커넥터를 구성하는 데 사용할 수 있는 샘플 구성 파일이 포함되어 있습니다. 지침은 다음 표에 나와 있는 디렉터리의 readme.txt 파일을 참조하십시오.

플랫폼	위치
Windows 시스템의 IIS 웹 서버	C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\samples\ConnectorConfiguration\windows\IIS_JBoss*
Solaris 시스템의 Sun Java System Web Server	/opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools/samples/ConnectorConfiguration/solaris/Iplanet_JBoss*
Solaris 시스템의 Apache Web Server	/opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools/samples/ConnectorConfiguration/solaris/apache_JBoss*

JBoss 응용 프로그램 플러그 인 설치 및 구성(IIS 7.x)

이 절차에서는 IIS 7.0 으로 시작하는 JBoss Apache 플러그 인 구성에 대해 설명합니다.

다음 단계를 수행하십시오.

1. 파일 시스템에서 ISAPI 필터를 배포하고 업데이트합니다.

   C 드라이브의 루트에 ISAPI 폴더를 배포합니다.

2. 압축을 푼 폴더에 있는 jakarta.reg 파일을 편집합니다.

   C:\의 루트에 ISAPI 폴더를 배치한 경우 이 파일을 변경하지 마십시오. 다른 폴더에 배치한 경우에는 줄 9, 줄 11 및 줄 12 에서 해당 폴더를 지정합니다.

3. 변경 내용을 저장하고 두 번 클릭하여 레지스트리를 업데이트합니다.

4. JBoss Application Server 의 위치를 지정하여 workers.properties 파일을 편집합니다. 포트와 유형은 변경할 필요가 없습니다.

5. Windows 2008 에 IIS7 또는 IIS7.5 를 설치합니다.

6. "System Manager"(시스템 매니저)를 열고 IIS ISAPI 필터와 ISAPI 확장이 설치되었는지 확인합니다.

7. "실행" 창에서 inetmgr 를 시작합니다.

8. m/c 이름을 선택하고 "ISAPI 및 CGI 제한"을 두 번 클릭합니다.

9. 오른쪽 패널에서 "추가" 단추를 클릭합니다.

10. "ISAPI 또는 CGI 제한 추가" 창이 나타납니다.

11. isapi_redirect.dll 을 선택하고 설명으로 ISAPI 를 입력합니다.

12. "확장 경로 실행 허용"을 선택합니다.

13. "ISAPI 또는 CGI 제한 추가" 창에서 "확인"을 클릭합니다.

14. "연결" 섹션에서 "사이트"를 확장하고 "기본 웹 사이트"를 선택한 다음 "가상 디렉터리 추가"를 마우스 오른쪽 단추로 클릭합니다.
15. 별칭으로 "jakarta"를 입력하고 실제 경로에 있는 isap_redirect.dll 파일의 위치(c:\ajp)를 입력합니다.
16. "설정 테스트" 단추를 클릭합니다.
    - 인증 및 권한 부여에 성공한 경우 "확인"을 클릭합니다.
    - 권한 부여에 실패한 경우 "연결 계정" 단추를 클릭합니다.
17. "특정 사용자"를 선택하고 관리 사용자 이름과 암호를 제공합니다.
18. "설정 테스트" 단추를 다시 클릭합니다. 이번에는 권한 부여가 성공합니다.
19. 왼쪽에서 "기본 웹 사이트"를 클릭하고 ISAPI 필터를 두 번 클릭합니다.
20. 오른쪽 패널에서 "추가" 단추를 클릭합니다.
21. 이름을 입력하고 isapi_redirect.dll 파일의 위치를 제공합니다.
22. "확인"을 클릭합니다.
23. "기본 웹 사이트"를 확장하고 jakarta 가상 디렉터리를 클릭합니다.
24. "처리기 매핑"을 두 번 클릭합니다.
25. ISAPI-dll 을 선택하고 "기능 사용 권한 편집"을 클릭합니다.

26. 모든 사용 권한(읽기, 스크립트, 실행)이 선택되었는지 확인합니다.
27. "확인"을 클릭합니다.

웹 에이전트 업데이트

IIS 7.x 를 구성한 후에는 웹 에이전트를 다음과 같이 변경하십시오.

1. "응용 프로그램 풀"을 클릭하고 "기본 응용 프로그램 풀"을 "클래식 모드"로 변경합니다.
2. 제출을 클릭합니다.
3. ISAPI 필터 우선 순위 목록에서 CA Identity Manager 에서 사용되는 응용 프로그램 서버의 플러그 인보다 에이전트의 우선 순위가 높게 하십시오.

JBoss 플러그 인이 구성되었습니다.

JBoss 응용 프로그램 플러그 인 설치 및 구성(IIS 6.0)

이 통합에서는 SiteMinder 가 CA Identity Manager 에 연결하기 전에 사용자를 인증하고 권한을 부여한다고 가정합니다. CA Identity Manager 에 연결하려면 SMSESSION 쿠키가 있어야 합니다. SiteMinder 웹 에이전트로 보호되는 응용 프로그램 플러그 인(프록시 리디렉션)을 사용하십시오. 이 구성을 통해 SMSESSION 쿠키가 만들어진 후 사용자가 SiteMinder 에서 인증된 다음 CA Identity Manager 로 리디렉션됩니다.

이 절차는 IIS 6.0 에 대한 JBoss Apache 플러그 인 배포 및 구성에 적용됩니다.

다음 단계를 수행하십시오.

1. 파일 시스템에서 ISAPI 필터를 배포하고 업데이트합니다.

   C 드라이브의 루트에 ISAPI 폴더를 배포해야 합니다.

2. 압축을 푼 폴더에 있는 jakarta.reg 파일을 편집합니다.

   C:\의 루트에 ISAPI 폴더를 배치한 경우 이 파일을 변경하지 마십시오. 다른 폴더에 배치한 경우에는 줄 9, 줄 11 및 줄 12 에서 해당 폴더를 지정합니다.

3. 변경 내용을 저장하고 두 번 클릭하여 레지스트리를 업데이트합니다.

4. JBoss Application Server 의 위치를 지정하여 workers.properties 파일을 편집합니다. 포트와 유형은 변경할 필요가 없습니다.

5. IIS 에서 ISAPI 필터를 배포합니다.

6. "관리 도구"에서 "인터넷 정보 서비스 관리자"를 엽니다.

7. "기본 웹 사이트"가 표시될 때까지 수준을 확장합니다. 마우스 오른쪽 단추를 클릭하고 "새로 만들기", "가상 디렉터리"를 차례로 선택합니다.

8. 별칭으로 *jakarta* 를 입력합니다.

9. ISAPI 플러그 인을 설치한 경로를 참조합니다.

10. "읽기", "스크립트 실행(예: ASP)" 및 "실행(예: ISAPI 응용 프로그램 또는 CGI)"을 선택합니다.
11. "다음"을 클릭하여 계속하고 마법사를 완료합니다.
12. "기본 웹 사이트"를 마우스 오른쪽 단추로 클릭하고 "속성", "ISAPI 필터" 탭을 차례로 선택한 다음 "추가"를 클릭합니다.
13. 필터 이름으로 *jakarta* 를 입력하고 "찾아보기"를 클릭하여 isapi_redirect.dll 을 선택합니다. 그런 다음 "확인"을 두 번 클릭합니다.
14. IIS 6.0 의 경우 "웹 서비스 확장" 아래에서 이 필터가 사용되도록 설정합니다.
15. "웹 서비스 확장" 폴더를 선택합니다. "새 웹 서비스 확장 추가" 왼쪽의 파란색 링크를 클릭합니다.
16. "Jakarta-Tomcat"을 이름으로 제공합니다. "추가"를 클릭하고 위와 동일한 dll 을 찾습니다. "확인"을 클릭하고 "확장 상태를 [허용됨]으로 설정"을 클릭한 다음 "확인"을 클릭합니다.
17. IIS 서버를 다시 시작합니다.

이제 프록시가 준비되었으므로 IIS 를 통해 CA Identity Manager 에 액세스할 수 있습니다. 예를 들어 프록시 구성 이전과 이후의 CA Identity Manager 액세스 링크는 다음과 같습니다.

이전

http://identitymgr.forwardinc.ca:8080/idmmange
http://identitymgr.forwardinc.ca:8080/idmmange

이후

http://smserver.forwardinc/idmmanage
http://smserver.forwardinc/idmmanage

참고: 프록시가 작동하려면 이 URL 의 끝에 슬래시 "/"가 필요할 수 있습니다. 관리 콘솔로 연결되지 않는 경우 프록시 로그를 참조하십시오.

WebLogic 에 프록시 플러그 인 설치

웹 에이전트가 CA Identity Manager 리소스에 대한 요청을 인증하고 권한 부여한 후 웹 서버가 CA Identity Manager 서버를 호스트하는 응용 프로그램 서버로 요청을 전달합니다.

1. WebLogic 설명서에 설명된 대로 웹 서버에 대한 WebLogic 프록시 플러그 인을 설치합니다.

   참고: IIS 사용자의 경우 프록시 플러그 인을 설치할 때 파일 확장자와 경로별로 프록시 연결을 구성해야 합니다. 파일 확장자별로 프록시를 구성하는 경우 다음 속성을 사용하여 "App Mapping"(응용 프로그램 매핑) 탭에서 응용 프로그램 매핑을 추가합니다.
   실행 파일: IISProxy.dll
   확장자: .wlforward

2. 다음 단원 중 하나에 설명된 대로 CA Identity Manager 용 프록시 플러그 인을 구성합니다.

   - IIS 프록시 플러그 인 (페이지 458)
   - iPlanet 프록시 플러그 인 (페이지 460)
   - Apache 프록시 플러그 인 (페이지 463)

IIS(7.x)용 프록시 플러그 인 구성

다음 절차에서는 IIS 7.x 에 대한 WebLogic 프록시 플러그 인을 배포하고 구성하는 과정을 단계별로 안내합니다.

참고: 이러한 지침은 32 비트 운영 환경에 적용됩니다. 64 비트 운영 환경에도 동일한 지침이 적용되지만 설치 .dll 파일의 위치는 다릅니다.

- %WL_HOME%server\plugin\win\32\
- %WL_HOME%server\plugin\win\64\

다음 단계를 수행하십시오.

1. IIS7 에 웹 에이전트를 설치하고 구성합니다.
2. 'C' 드라이브에 'plugin'이라는 폴더를 만듭니다.
3. 다음 파일을 plugin 폴더에 복사합니다.
   - lisforward.dll
   - lisproxy.dll
   - iisproxy.ini

   \\lodimmaple.ca.com\RegressionHarness\thirdparty\weblogic\Weblogic_Proxy_Files_IIS7 에서 이러한 파일을 찾을 수 있습니다.
4. IIS7 에 "응용 프로그램 개발" 및 "관리 도구" 역할 서비스를 설치합니다.
5. "Inet Manager"(Inet 관리자)를 열고 "기본 웹 사이트"를 선택합니다.
6. "처리기 매핑"을 클릭합니다.
7. "정적 파일"을 두 번 클릭하고 요청 경로를 *.*로 수정합니다.
8. "요청 제한" 단추를 클릭합니다.
9. "매핑" 탭에서 "요청이 다음에 매핑되는 경우에만 처리기 호출: 파일 또는 폴더"를 선택합니다.

10. "처리기 매핑" 대화 상자의 오른쪽 메뉴 옵션에서 "스크립트 매핑 추가..."를 클릭합니다. 다음 값을 입력합니다.
    - 요청 경로: *
    - 실행 파일: iisProxy.dll
    - 이름: proxy
11. "요청 제한" 단추를 클릭합니다.
12. "요청이 다음에 매핑되는 경우에만 처리기 호출"을 선택 취소합니다.
13. 이 IASPI 확장을 허용할지 여부에 대한 프롬프트가 표시되면 "예"를 클릭합니다.
14. "IIS 관리자" 트리의 루트 노드(컴퓨터 이름)를 클릭하고 "ISAPI 및 CGI 제한"을 클릭합니다.
15. "동작" 창에서 "추가"를 클릭하고 다음 값을 입력합니다.
    - ISAPI 또는 CGI 경로: C:\plugin\ iisproxy.dll
    - 설명: Weblogic
    - "확장 경로 실행 허용"을 선택합니다.
16. "IIS 관리자" 트리의 루트 노드(컴퓨터 이름)를 클릭하고 "ISAPI 및 CGI 제한"을 클릭합니다. Weblogic 옵션을 선택하고 오른쪽 창에서 "기능 설정 편집"을 클릭합니다.
17. "지정하지 않은 ISAPI 모듈 허용"과 "지정하지 않은 CGI 모듈 허용"을 선택합니다.
18. Webagent 에 대해 동일한 작업을 수행합니다.
19. "기능 보기"의 '기본 웹 사이트'에서 "처리기 매핑"을 두 번 클릭합니다.

20. "처리기 매핑" 페이지의 "동작" 창에서 "스크립트 매핑 추가"를 클릭하고 다음 값을 입력합니다.
    - 요청 경로: .jsp
    - 실행 파일: iisproxy.dll
    - 이름: JSP
21. "요청 제한"을 클릭합니다.
22. "매핑" 탭에서 "요청이 다음에 매핑되는 경우에만 처리기 호출: 파일"을 선택합니다.
23. "확인"을 클릭합니다.
24. "스크립트 매핑 추가"를 클릭하고 다음 값을 입력합니다.
    - 요청 경로: .do
    - 실행 파일: C:\plugin\iisproxy.dll
25. "요청 제한"을 클릭합니다. 설정은 .jsp 의 경우와 동일합니다.
26. "확인"을 클릭합니다.
27. "스크립트 매핑 추가"를 클릭하고 다음 값을 입력합니다.
    - 요청 경로: .wlforward
    - 실행 파일: C:\plugin\iisproxy.dll
28. "요청 제한"을 클릭합니다. 설정은 .jsp 의 경우와 동일합니다.
29. "기본 웹 사이트"를 클릭하고 "ISAPI 필터"를 두 번 클릭합니다.
30. 오른쪽 창에서 "View Order List"(보기 순서 목록)를 클릭합니다.

31. SiteMinder 에이전트 실행 파일을 목록의 두 번째 자리에 배치합니다. 목록에서 이 항목 뒤에는 Weblogic 실행 파일만 있습니다.

    참고: SiteMinder 에이전트 실행 파일이 Weblogic 실행 파일 뒤에 나타나는 경우 위로 이동 동작을 사용하여 SiteMinder 에이전트를 이동합니다.

32. "응용 프로그램 풀"을 클릭하고 "기본 응용 프로그램 풀"을 "클래식 모드"로 변경합니다.

WebLogic 플러그 인이 구성되었습니다.

(WL)IIS 6.0 프록시 플러그 인 구성

이 절차는 IIS 6.0.x 에 대한 WebLogic 프록시 플러그 인 구성에 적용됩니다.

다음 단계를 수행하십시오.

1. 웹 에이전트가 설치된 시스템에 폴더를 만듭니다. 예를 들어 c:\weblogic_proxy 를 만듭니다.
2. CA Identity Manager 서버가 실행되고 있는 시스템에 로그인합니다.
3. *Weblogic_Home*\wlserver_11\server\plugin 폴더로 이동합니다.
4. 다음 파일을 1 단계에서 만든 WebLogic 프록시 폴더에 복사합니다.
   - iisforward.dll
   - iisproxy.dll

5. 동일한 폴더에 iisproxy.ini 라는 파일을 만들고 다음 내용을 포함합니다.

```
# This file contains initialization name/value pairs
# for the IIS/WebLogic plug-in.
WebLogicHost=host-name
WebLogicPort=7001
ConnectTimeoutSecs=20
ConnectRetrySecs=2
WlForwardPath=/castylesr5.1.1,/iam,/im , /ca/Odata/
WLLogFile= c:\weblogic_proxy \proxy.log
DebugConfigInfo=ON
```

   host-name 을 실제 호스트 이름으로 바꿉니다.

6. "IIS 관리자"를 시작합니다.
7. "웹 사이트"를 확장합니다.
8. "기본 웹 사이트"를 마우스 오른쪽 단추로 클릭합니다.
9. "속성"을 선택합니다.
10. 다음과 같이 필터를 추가합니다.
    a. "ISAPI 필터"를 클릭합니다.
    b. "추가"를 클릭하고 다음과 같이 대화 상자에 정보를 입력합니다.

       필터 이름: WebLogic

       실행 파일: iisforward.dll 의 경로

11. 다음과 같이 iisproxy.dll 파일의 위치를 제공합니다.
    a. "홈 디렉터리"를 클릭합니다.
    b. "구성"을 클릭합니다.
    c. "추가"를 클릭합니다.
    d. iisproxy.dll 파일의 경로를 입력합니다.
    e. "확장자" 필드에 .jsp 를 입력합니다.
    f. "파일이 있는지 확인" 옵션을 선택 취소합니다.
12. .do 및 .wlforward 확장자에 대해 11 단계를 반복합니다.

13. iisforward.dll 의 위치를 가리키는 wlforward(모두 소문자)에 대한 웹 서비스 확장을 추가합니다.

    확장 상태를 "허용됨"으로 설정합니다.

14. 각 웹 서비스 확장을 마우스 오른쪽 단추로 클릭하여 "허용됨" 상태로 변경합니다.

15. IIS 웹 서버를 다시 시작합니다.

iPlanet 프록시 플러그 인 구성

플러그 인을 구성하려면 다음 iPlanet 구성 파일을 수정하십시오.

- magnus.conf
- obj.conf

iPlanet 구성 파일에는 텍스트 배치에 대한 엄격한 규칙이 있습니다. 문제를 방지하려면 다음 사항에 주의하십시오.

- 불필요한 선행 및 후행 공백을 제거하십시오. 추가 공백이 있을 경우 iPlanet 서버가 실패할 수 있습니다.
- 한 줄에 들어갈 수 있는 것보다 많은 문자를 입력해야 하는 경우 해당 줄 끝에 백슬래시(\)를 넣고 다음 줄에서 입력을 계속하십시오. 백슬래시는 첫 줄 끝을 다음 줄의 시작 부분에 직접 덧붙이는 역할을 합니다. 첫 줄을 끝내는 단어와 두 번째 줄을 시작하는 단어 사이에 공백이 필요한 경우 첫 줄 끝(백슬래시 앞)이나 두 번째 줄의 시작 부분에 하나의 공백을 사용해야 합니다.
- 특성을 여러 줄로 분할하지 마십시오.

iPlanet 인스턴스에 대한 iPlanet 구성 파일은 다음 위치에서 찾을 수 있습니다.

iplanet_home/https-*instance_name*/config/

여기서 *iplanet_home* 은 iPlanet 설치의 루트 디렉터리이고 *instance_name* 은 사용 중인 특정 서버 구성입니다.

다음 단계를 수행하십시오.

1. *weblogic_home*/server/lib 디렉터리에서 iPlanet 을 설치한 파일 시스템으로 사용 중인 iPlanet Web Server 버전에 해당하는 libproxy.so 파일을 복사합니다.
2. 텍스트 편집기에서 iPlanet magnus.conf 파일을 수정합니다.

   libproxy.so 파일을 iPlanet 모듈로 로드하도록 iPlanet 에 지시하려면 다음 줄을 magnus.conf 파일의 시작 부분에 추가하십시오.

   ```
   Init fn="load-modules" funcs="wl_proxy,wl_init"\
   shlib=path in file system from step 1/libproxy.so
   Init fn="wl_init"
   ```

   예:

   ```
   Init fn="load-modules" funcs="wl_proxy,wl_init"\
   shlib=/usr/local/netscape/plugins/libproxy.so
   Init fn="wl_init"
   ```

   load-modules 함수는 iPlanet 시작 시 로드하도록 공유 라이브러리에 태그를 지정합니다. wl_proxy 및 wl_init 값은 플러그 인이 실행하는 함수를 식별합니다.

3. 텍스트 편집기에서 다음과 같이 iPlanet obj.conf 파일을 수정합니다.

   a. 다음 텍스트로 시작하는 마지막 줄 뒤에

      NameTrans fn=....

      다음 Service 지시문을 Object name="default" 섹션에 추가합니다.

      ```
      Service method="(GET|HEAD|POST|PUT)" type=text/jsp fn="wl-proxy"
      ```

      참고: 기존 Service 지시문 뒤에 오는 줄에 이 지시문을 추가할 수 있습니다.

   b. 다음 코드를 파일 끝에 추가합니다.

      ```
      <Object name="idm" ppath="*/iam/*">">
      Service fn="wl-proxy" WebLogicHost="hostname" WebLogicPort="portnumber"
      PathTrim="/weblogic"
      </Object>
      <Object name="weblogic1" ppath="*/console*">
      Service fn="wl-proxy" WebLogicHost="hostname" WebLogicPort="portnumber"
      PathTrim="/weblogic"
      </Object>
      ```

      여기서 *hostname* 은 WebLogic 을 설치한 시스템의 서버 이름과 도메인이고 *portnumber* 는 WebLogic 포트(기본값: 7001)입니다.

      Object 항목은 둘 이상 있을 수 있습니다.

      예:

      ```
      <Object name="idm" ppath="*/iam/*">">
      Service fn="wl-proxy" WebLogicHost="MyServer.MyCompany.com"
      WebLogicPort="7001" PathTrim="/weblogic"
      <Object name="weblogic1" ppath="*/console*">
      Service fn="wl-proxy" WebLogicHost="MyServer.MyCompany.com"
      WebLogicPort="7001" PathTrim="/weblogic"
      </Object>
      ```

4. iPlanet 구성 파일을 저장합니다.

5. 웹 서버 인스턴스를 다시 시작합니다.

Apache 프록시 플러그 인 구성

Apache 프록시 플러그 인을 구성하려면 http.conf 파일을 편집해야 합니다.

다음 단계를 수행하십시오.

1. Solaris 에 웹 에이전트를 설치한 후 Apache Web Server 를 중지하고 mod_wl_20.so 파일을 다음 위치에서

   weblogic_home/server/lib/solaris

   다음과 같이 변경합니다.

   apache_home/modules

2. http.conf 파일(*apache_home*/conf 에 있음)을 편집하고 다음과 같이 변경합니다.

   a. load module 섹션에서 다음 코드를 추가합니다.

   ```
   LoadModule weblogic_module      modules/mod_wl_20.so
   ```

   b. Apache 서버 시스템의 이름을 사용하여 서버 이름을 편집합니다.

   c. 다음과 같이 파일 끝에 If 블록을 추가합니다.

   ```
   <IfModule mod_weblogic.c>
     WebLogicHost weblogic_server.com
     WebLogicPort 7001
     MatchExpression /iam
     MatchExpression /castylesr5.1.1
     MatchExpression /ca/Odata
   </IfModule>
   ```

3. http.conf 파일을 저장합니다.

4. Apache 웹 서버를 다시 시작합니다.

SiteMinder 에이전트를 CA Identity Manager 도메인과 연결

정책 관리자가 CA Identity Manager 태스크를 완료한 후 이 태스크를 수행합니다. 사용자 환경을 CA Identity Manager 로 로드하는 동안 4.X 에이전트를 참조하십시오. SiteMinder 가 SiteMinder 정책 서버에 도메인/영역을 만들 때 해당 에이전트를 사용합니다. 이 에이전트는 SMSESSION 쿠키의 유효성을 검사합니다. 도메인/영역을 업데이트하고 웹 서버에서 CA Identity Manager 에 액세스하는 데 사용되는 완전한 기능의 에이전트를 참조하십시오. 이 웹 서버는 CA Identity Manager 에 대한 액세스 지점 역할을 하고 SMSESSION 쿠키를 만듭니다.

다음 단계를 수행하십시오.

1. SiteMinder 관리 UI 에 로그인합니다.
2. "정책", "도메인"으로 이동합니다.
3. 환경에 대한 도메인을 수정합니다.
4. "영역" 탭에서 첫 번째 나열된 영역 XXX_ims_realm 을 편집합니다.
5. 프록시에서 에이전트를 검색하고 선택합니다.

   참고: 프록시 에이전트(웹 서버 에이전트)가 없으면 프록시 에이전트를 만드십시오. CA Identity Manager 앞에 웹 서버와 프록시가 있는지 확인하십시오.
6. "확인"을 두 번 클릭하고 공용 영역 XXX_pub_realm 에 대해 이 프로세스를 반복합니다.
7. 두 영역을 모두 업데이트한 후 "제출"을 클릭합니다.
8. 에이전트가 새로 고쳐질 때까지 기다리거나 프록시 에이전트가 있는 웹 서버를 다시 시작합니다.

SiteMinder LogOffUrI 매개 변수 구성

SiteMinder 를 환경에 추가한 후 CA Identity Manager 에서 로그오프하면 실제로 아무 일도 일어나지 않습니다. 이 기능이 다시 사용되도록 설정하려면 프록시 에이전트에 대한 ACO(에이전트 구성 개체)를 업데이트하십시오.

다음 단계를 수행하십시오.

1. SiteMinder 관리 UI 에 로그인합니다. "인프라" 탭, "에이전트", "Expand Agent Configuration"(에이전트 구성 확장)을 차례로 클릭한 다음 "에이전트 구성 수정"을 클릭합니다.
2. ACO 를 찾습니다. #LogoffUri 매개 변수를 찾습니다. 해당 매개 변수 왼쪽의 재생 단추(오른쪽 화살표)를 클릭합니다.
3. "값" 필드에 있는 이름에서 파운드 기호(#)를 제거하고 /idm/logout.jsp 를 입력합니다.
4. "확인", "제출"을 차례로 클릭하여 에이전트 구성 개체를 업데이트합니다.

   다음에 에이전트가 정책 서버에서 해당 구성을 검색할 때 새 설정이 전파됩니다.

문제 해결

다음 항목에서는 일반적으로 발생할 수 있는 오류에 대해 설명합니다. 가능한 모든 경우에 통합을 지원할 수 있도록 오류와 해결 방법이 쌍으로 연결되어 있습니다.

Windows DLL 누락

증상

Windows DLL(MSVCP71.dll) 누락

SiteMinder 연결이 활성화된 후 JBoss 에서 DLL(MSVCP71.dll)이 없다는 Java 오류가 나타납니다.

참고: JBoss 가 서비스로 실행되고 있는 경우에는 이 오류가 나타나지 않을 수 있습니다. 가능하다면 JBoss 를 서비스로 실행하지 않고 구성을 테스트하십시오.

해결 방법

다음 단계를 수행하십시오.

1. Windows 에서 실행되고 있는 경우 SiteMinder 정책 서버에서 MSVCP71.dll 을 찾습니다.
2. 이 DLL(MSVCP71.dll)을 \Windows\system32 폴더에 복사합니다.
3. 이 파일을 올바른 위치에 넣은 후 OS 에 등록합니다.
4. 명령 창에서 regsvr32 명령을 실행합니다. 파일이 로드되기만 하면 정상입니다.
5. 응용 프로그램 서버를 다시 시작합니다.

잘못된 SiteMinder 정책 서버 위치

증상

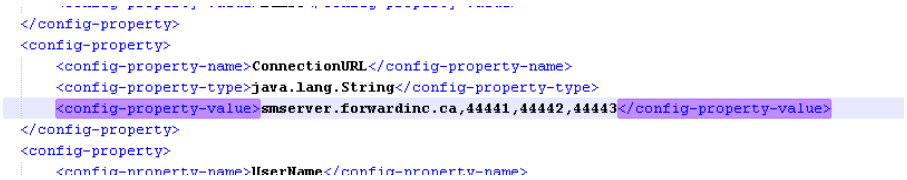
잘못된 SiteMinder 정책 서버 위치

해결 방법

잘못된 위치가 ra.xml 에서 참조되어 "Cannot connect to policy server: xxx"(정책 서버에 연결할 수 없음: xxx) 오류가 나타납니다.

다음 단계를 수행하십시오.

1. ra.xml 에서 제공된 호스트 이름을 확인합니다.



2. ConnectionURL 속성에서 SiteMinder 정책 서버 호스트 이름을 지정합니다. FQN(정규화된 이름)을 사용합니다.

잘못된 관리자 이름

증상

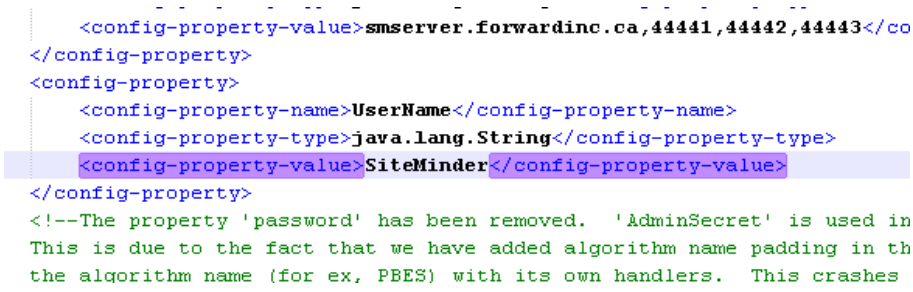
잘못된 관리자 이름

해결 방법

잘못된 관리자가 ra.xml 에서 참조되어 "Unknown administrator"(알 수 없는 관리자) 오류가 나타납니다.

다음 단계를 수행하십시오.

1. ra.xml 에서 UserName 속성을 확인합니다.



2. UserName 속성에서 CA SiteMinder 와 통신하는 데 사용되는 계정을 지정합니다. 예를 들어 SiteMinder 계정(기본값)을 사용합니다.

잘못된 관리자 암호

증상

잘못된 관리자 암호

해결 방법

잘못된 관리자 암호가 ra.xml 에서 사용되어 "Cannot connect to the policy server: Invalid credentials"(정책 서버에 연결할 수 없음: 잘못된 자격 증명) 오류가 나타납니다.

다음 단계를 수행하십시오.

1. ra.xml 에서 AdminSecret 속성을 확인합니다.

```
-->
<config-property>
    <config-property-name>AdminSecret</config-property-name>
    <config-property-type>java.lang.String</config-property-type>
    <config-property-value>{PBES}:xfx8/9xxmHD0B3Raw9VZJA==</config-property-value>
</config-property>
<config-property>
    <config-property-name>AgentName</config-property-name>
```

2. UserName 속성에서 참조된 사용자 이름에 대한 암호화된 암호를 AdminSecret 속성에 지정합니다.

추가 정보:

SiteMinder 암호 또는 공유 암호 수정 (페이지 512)

잘못된 에이전트 이름

증상

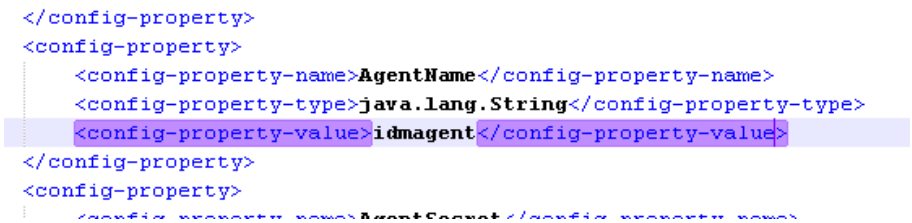
잘못된 에이전트 이름

해결 방법

잘못된 에이전트 이름이 ra.xml 에서 사용되어 "Cannot connect to the policy server: Failed to init Agent API: -1"(정책 서버에 연결할 수 없음: 에이전트 API 를 초기화하지 못했습니다: -1) 오류가 나타납니다.

다음 단계를 수행하십시오.

1. ra.xml 에서 AgentName 속성을 확인합니다.



2. SiteMinder 구성의 세 번째 단계에서 만든 4.X 에이전트 이름을 지정합니다.

잘못된 에이전트 암호

증상

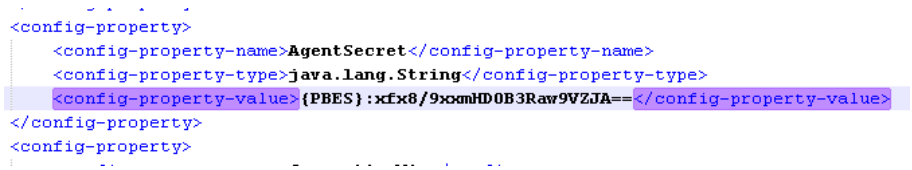
잘못된 에이전트 암호

해결 방법

잘못된 에이전트 암호가 ra.xml 에서 사용되어 앞의 암호화 처리기 오류와 함께 "Cannot connect to the policy server: Failed to init Agent API: -1"(정책 서버에 연결할 수 없음: 에이전트 API 를 초기화하지 못했습니다: -1) 오류가 나타납니다.

다음 단계를 수행하십시오.

1. ra.xml 에서 AgentSecret 속성을 확인합니다.



2. 해당 에이전트를 만들 때 사용된 암호화된 암호를 지정합니다.

추가 정보:

SiteMinder 암호 또는 공유 암호 수정 (페이지 512)

CA Identity Manager 에 사용자 컨텍스트 없음

증상

CA Identity Manager 에 사용자 컨텍스트 없음

사용자가 SMSESSION 쿠키 없이 CA Identity Manager 에 액세스하려고 하면 CA Identity Manager 가 사용자를 인증할 수 없습니다. 이 경우 빈 CA Identity Manager UI 가 표시될 수 있습니다.

사용자 환경에 대해 사용되도록 설정된 워크플로가 있는 경우 이와 유사한 오류가 나타납니다.

```
Exception during page display:

java.lang.IllegalArgumentException
        at com.netegrity.webapp.bean.WorkList.(WorkList.java:84)
        at com.netegrity.webapp.bean.WorkList.(WorkList.java:70)
        at com.netegrity.webapp.bean.WorkList.getConsoleWorkListFromRequest(WorkList.java:109)
        at com.netegrity.taglib.skin.TagUtilLocal.getWorkItems(TagUtilLocal.java:660)
        at com.netegrity.taglib.skin.TagUtilLocal.hasWorkItems(TagUtilLocal.java:846)
        at com.netegrity.taglib.skin.IfWorkItemsTag.doStartTag(IfWorkItemsTag.java:73)
        at idm_jsp.app.ca12.home_jsp._jspService(Unknown Source)
        at org.apache.jasper.runtime.HttpJspBase.service(HttpJspBase.java:70)
        at javax.servlet.http.HttpServlet.service(HttpServlet.java:803)
        at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:290)
        at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:206)
        at org.apache.catalina.core.ApplicationDispatcher.invoke(ApplicationDispatcher.java:654)
        at org.apache.catalina.core.ApplicationDispatcher.doInclude(ApplicationDispatcher.java:557)
        at org.apache.catalina.core.ApplicationDispatcher.include(ApplicationDispatcher.java:481)
        at org.apache.jasper.runtime.JspRuntimeLibrary.include(JspRuntimeLibrary.java:968)
        at idm_jsp.app.ca12.index_jsp._jspx_meth_skin_ifhomepage_0(Unknown Source)
        at idm_jsp.app.ca12.index_jsp._jspService(Unknown Source)
        at org.apache.jasper.runtime.HttpJspBase.service(HttpJspBase.java:70)
        at javax.servlet.http.HttpServlet.service(HttpServlet.java:803)
        at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:290)
        at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:206)
        at org.apache.catalina.core.ApplicationDispatcher.invoke(ApplicationDispatcher.java:654)
        at org.apache.catalina.core.ApplicationDispatcher.processRequest(ApplicationDispatcher.java:445)
        at org.apache.catalina.core.ApplicationDispatcher.doForward(ApplicationDispatcher.java:379)
        at org.apache.catalina.core.ApplicationDispatcher.forward(ApplicationDispatcher.java:292)
        at com.netegrity.webapp.filter.ConsolePageFilter.doFilter(ConsolePageFilter.java:521)
        at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:235)
        at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:206)
        at com.netegrity.webapp.page.jsf.FacesFilter.doFilter2(FacesFilter.java:180)
```

해결 방법

이 오류의 원인은 몇 가지가 있지만 일반적으로 다음 중 하나입니다.

- CA Identity Manager 에 직접 액세스했습니다.
- 프록시의 SiteMinder 에이전트가 사용되지 않도록 설정되었습니다. 즉, 아무 것도 보호되지 않으므로 SMSESSION 쿠키가 만들어지지 않습니다.
- CA Identity Manager 환경에 대한 SiteMinder 도메인이 잘못 구성되었습니다.

처음 두 가지 원인은 매우 간단한 문제입니다. 완전한 기능의 웹 에이전트가 사용되도록 설정한 상태로 웹 서버를 통해 라우트되는지 확인하십시오. 하지만 웹 서버를 통해 라우트되며 에이전트가 사용되도록 설정되어 있더라도 도메인을 수정해야 합니다.

다음 단계를 수행하십시오.

1. SiteMinder 관리 UI 에 로그인합니다.
2. CA Identity Manager 도메인을 찾고 계층을 단계별로 클릭하여 수정합니다. "영역" 탭을 클릭하고 목록의 첫 번째 영역을 클릭합니다.
3. 슬래시의 기본 위치는 영역 아래에 있습니다. 슬래시를 삭제합니다.
4. 이 영역 아래의 규칙을 클릭합니다.

   규칙에 대한 기본 유효 리소스는 별표 "*"입니다.
5. 별표 앞에 슬래시 "/"를 추가합니다.

   영역에서 규칙으로 슬래시를 이동했습니다. 보호는 같지만 SiteMinder 가 처리하는 방식은 다릅니다.

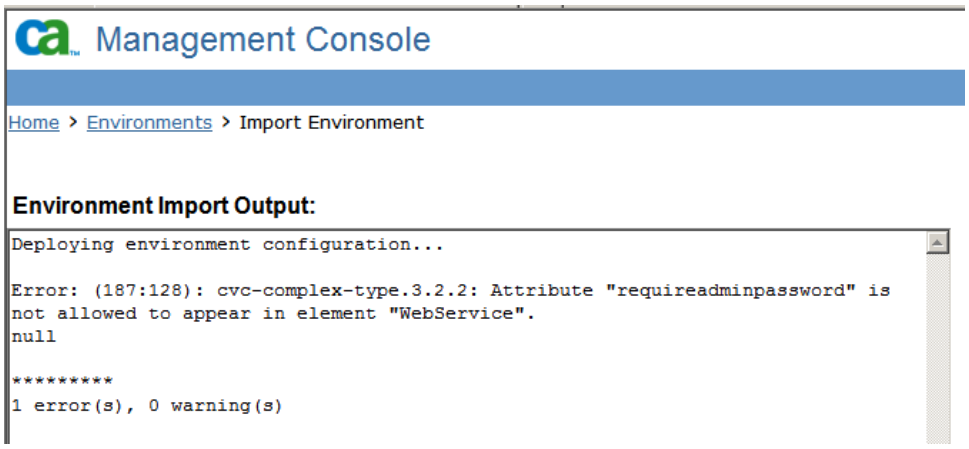
   SiteMinder 를 통해 CA Identity Manager 에 성공적으로 로그인할 수 있습니다. 적절한 보호의 유효성을 검사하려면 SiteMinder 에이전트 로그를 검토하십시오.

환경 로드 오류

증상

SiteMinder 와 통합한 후 환경을 CA Identity Manager 로 다시 가져올 때 "requireadminpassword" 특성과 "WebService" 요소에 대한 오류가 나타납니다.

참고: SiteMinder 가 배포에 포함되지 않은 경우에도 이 문제가 발생할 수 있습니다.



해결 방법

이 오류로 환경이 부분적으로 배포될 수 있습니다. 부분 배포로 인해 CA Identity Manager 개체 저장소에 빈 요소가 만들어질 수 있습니다. 환경 XML 중 하나를 수정하고 다시 가져오십시오.

다음 단계를 수행하십시오.

1. 보관된 ZIP 파일을 찾아서 탐색합니다.
2. XXX_environment_settings.xml 의 사본을 만듭니다.
3. 이 파일을 편집하고 "WebService" 요소를 찾습니다.
4. "requireadminpassword="false" 태그를 삭제합니다.

   참고: 태그와 값을 *모두* 제거합니다. 값만 제거하지 마십시오.
5. 변경 내용을 저장하고 파일을 ZIP 파일에 다시 넣습니다.
6. 보관된 환경 zip 파일을 다시 가져옵니다.

   실패한 시도에서 만들어진 환경은 삭제하지 않아도 됩니다. 수정된 파일을 다시 가져오면 실패한 시도로 인한 오류가 수정됩니다.

CA Identity Manager 디렉터리 또는 환경을 만들 수 없음

증상

SiteMinder 통합이 사용되도록 설정된 경우 CA Identity Manager 디렉터리 또는 환경을 만들 수 없습니다.

해결 방법

레지스트리에 항목이 없기 때문에 이 문제가 발생할 수 있습니다.

다음 레지스트리 설정이 SiteMinder 정책 서버 컴퓨터에 있는지 확인하십시오.

- Solaris 또는 Linux:

  다음 항목이 sm.registry 에 있는지 확인하십시오.
  ImsInstalled=8.0; REG_SZ

- Windows:

  "ImsInstalled=8.0; REG_SZ" 설정이 다음 위치에 있는지 확인하십시오.
  HKLM\SOFTWARE\Netegrity\SiteMinder\CurrentVersion

  참고: 레지스트리 경로 \Netegrity\SiteMinder\CurrentVersion 이 없으면 수동으로 만드십시오.

레지스트리를 변경한 경우에는 정책 서버를 다시 시작해야 변경 내용이 적용됩니다.

중요! 레지스트리를 수정하기 전에 전체 시스템 백업을 수행하십시오.

사용자가 로그인할 수 없음

증상

새 사용자가 일반 텍스트 암호를 사용하여 환경에 로그인할 수 없습니다.

해결 방법

다음 데이터 분류가 디렉터리 구성 파일(directory.xml)의 암호 특성 정의에 포함되지 않았는지 확인하십시오.

<DataClassification name="AttributeLevelEncrypt"/>

다음 구성 요소를 포함하는 환경에서 특성 수준 암호화가 사용되도록 설정하면 사용자가 로그인하지 못하게 됩니다.

- CA SiteMinder 및
- 관계형 데이터베이스

CA Identity Manager 에이전트 설정을 구성하는 방법

CA Identity Manager 가 SiteMinder 와 통합되는 경우 CA Identity Manager 는 기본 제공 CA Identity Manager 에이전트를 사용하여 SiteMinder 정책 서버와 통신합니다. 성능을 튜닝하려면 CA Identity Manager 에이전트에 대해 다음 연결 설정을 구성하십시오.

1. 다음 단계 중 하나를 완료하십시오.
   - CA Identity Manager 가 WebLogic 또는 WebSphere 응용 프로그램 서버에서 실행되고 있는 경우 응용 프로그램 서버 콘솔에서 policyserver_rar 커넥터 설명자의 리소스 어댑터를 편집합니다.
   - CA Identity Manager 가 JBoss Application Server 에서 실행되고 있는 경우 <JBoss_home>\server\default\deploy\iam_im.ear\policyserver_rar\META-INF 에서 policyserver-service.xml 을 엽니다.

2. 다음과 같이 설정을 구성합니다.

   ConnectionMax

   정책 서버에 대한 최대 연결 수(예: 20)를 설정합니다.

   ConnectionMin

   정책 서버에 대한 최소 연결 수(예: 2)를 설정합니다.

   ConnectionStep

   모든 에이전트 연결이 사용 중일 때 열려는 추가 연결 수를 설정합니다.

   ConnectionTimeout

   시간이 만료되기 전에 에이전트가 SiteMinder 에 연결하기 위해 대기해야 하는 시간(초)을 지정합니다.

3. 응용 프로그램 서버를 다시 시작합니다.

SiteMinder 고가용성 구성

SiteMinder 정책 서버 클러스터를 만든 경우 부하 분산과 장애 조치에 사용하도록 응용 프로그램 서버 클러스터를 구성할 수 있습니다.

다음 단계를 수행하십시오.

1. 다음 위치에 있는 ra.xml 파일을 편집합니다.

   WebSphere:
   WAS_PROFILE/config/cells/*CELL_NAME*/applications/iam_im.ear/deployments/IdentityMinder/policyserver_rar/META-INF
   Jboss: *jboss_home*/server/all/deploy/iam_im.ear/policyserver_rar/META-INF
   WebLogic: *wl_domain*/applications/iam_im.ear/policyserver_rar/META-INF

2. 다음 항목을 수정합니다. 이러한 항목은 뒤에 나오는 단원에서 설명합니다.

   - 정책 서버에 대한 연결 설정
   - 정책 서버 수
   - 클러스터에 대한 부하 분산 또는 장애 조치 선택

3. 클러스터의 각 CA Identity Manager 서버에 대해 이러한 단계를 반복합니다.

4. 응용 프로그램 서버를 다시 시작하여 변경 사항을 적용합니다.

참고: CA Identity Manager 디렉터리 또는 환경을 만들고 있거나 디렉터리 또는 환경 설정을 수정하고 있는 경우 SiteMinder Failover 및 FailoverServers 를 false 로 설정하십시오. 그렇지 않으면 디렉터리 개체가 만들어질 수 있지만 제시간에 사용되도록 복제되지는 않습니다. 예를 들어 서버 1 에 디렉터리를 만든 다음 해당 디렉터리의 개체 ID 를 사용하여 서버 2 에 특성을 만드는 경우 두 번째 디렉터리가 아직 없으므로 "개체를 찾을 수 없음" 오류가 표시됩니다.

정책 서버 연결 설정 수정

정책 서버 연결 정보는 프로덕션 환경에 대한 기본 서버를 반영해야 합니다. 이 정보는 ConnectionURL, SiteMinder 관리자 계정에 대한 사용자 이름 및 암호, 에이전트에 대한 이름 및 공유 암호 등으로 구성됩니다.

다음 예에서 편집 가능한 값은 대문자로 나타납니다.

```
<config-property>
        <config-property-name>ConnectionURL</config-property-name>
   <config-property-type>java.lang.String</config-property-type>
        <config-property-value>DEVELOPMENT.SEVERCOMPANY.COM,VALUE,VALUE,VALUE</co
nfig-
                property-value>
</config-property>

<config-property>
        <config-property-name>UserName</config-property-name>
   <config-property-type>java.lang.String</config-property-type>
        <config-property-value>SITEMINDER-ADMIN-NAME</config-property-
                value>
</config-property>

<config-property>
        <config-property-name>AdminSecret</config-property-name>
        <config-property-type>java.lang.String</config-property-type>
        <config-property-value>ENCRYPTED-PASSWORD</config-
                property-value>
</config-property>
<config-property>
        <config-property-name>AgentName</config-property-name>
        <config-property-type>java.lang.String</config-property-type>
        <config-property-value>DEVELOPMENT-AGENT-NAME</config-property-
                value>
</config-property>

<config-property>
        <config-property-name>AgentSecret</config-property-name>
        <config-property-type>java.lang.String</config-property-type>
        <config-property-value>ENCRYPTED-AGENT-SECRET</config-
                property-value>
</config-property>
```

참고: 암호화된 텍스트가 필요한 값의 경우 CA Identity Manager 암호 도구를 사용하십시오. 자세한 내용은 *구성 안내서*를 참조하십시오.

정책 서버 추가

CA Identity Manager 설치 인스턴스에 정책 서버를 더 추가하려면 ra.xml 파일에서 FailoverServers 항목을 편집하십시오.

참고: 기본 정책 서버와 모든 장애 조치 서버를 FailoverServers 항목에 포함하십시오.

각 정책 서버에 대해 인증, 권한 부여 및 계정 서비스의 IP 주소와 포트 번호를 입력하십시오. 항목이 여러 개인 경우 여기에 표시된 대로 세미콜론을 사용하여 구분하십시오.

```
<config-property>
        <config-property-name>FailoverServers</config-property-name>
        <config-property-type>java.lang.String</config-property-type>
        <config-property-value>
                172.123.123.123,44441,44442,44443;172.123.123.124,33331,
                33332,33333
        </config-property-value>
</config-property>
```

부하 분산 또는 장애 조치 선택

CA Identity Manager 의 기본 동작은 ConnectionURL 과 FailoverServers 로 식별되는 서버를 통해 라운드 로빈 부하 분산을 사용하는 것입니다. FailOver 를 false 로 설정한 상태로 두면 부하 분산이 발생합니다.

장애 조치를 선택하려면 FailOver 를 true 로 설정하십시오.

```
<config-property>
        <config-property-name>FailOver</config-property-name>
        <config-property-type>java.lang.String</config-property-type>
        <config-property-value>true</config-property-value>
</config-property>
```

기존 CA Identity Manager 배포에서 SiteMinder 제거

이 단원에서는 기존 CA Identity Manager 환경에서 CA SiteMinder 를 제거하기 위한 자세한 지침을 제공합니다.

다음 단계를 수행하십시오.

중요! 마이그레이션한 후에는 암호 기록 정보에 액세스할 수 없습니다.

1. 응용 프로그램 서버를 중지합니다.
2. \iam_im.ear\policyserver.rar\META-INF 에 있는 ra.xml 파일에서 Enabled config-property 값을 false 로 설정하여 정책 서버가 사용되지 않도록 설정합니다.
3. \iam_im.ear\User_console.war/WEB-INF 에 있는 web.xml 파일을 편집하고 FrameworkAuthFilter 속성을 Enabled = true 로 설정합니다.

   참고: WebSphere 의 경우 web.xml 파일은 *WebSphere_home*/AppServer/profiles/*Profile_name*/config/cells/*Cell_name* /applications/iam_im.ear/deployments/IdentityMinder/user_console.war/ WEB-INF 에 있습니다.
4. 응용 프로그램 서버를 시작합니다.
5. (WebSphere 에만 해당) ra.xml 파일에 있는 것과 동일한 값을 사용하여 관리 콘솔에서 policyServer 개체를 업데이트합니다.

SiteMinder 오퍼레이션

다음 단원에서는 CA Identity Manager 를 지원하기 위해 정책 도메인과 인증 체계를 포함한 SiteMinder 기능을 수정하는 방법에 대해 설명합니다.

사용자 지정 인증 체계를 사용하여 사용자 자격 증명 수집 (페이지 484)

CA Identity Manager 가 CA Identity Manager 환경에 액세스하려는 사용자의 자격 증명을 수집하는 데 사용하는 방법을 변경합니다.

액세스 역할 구성 (페이지 486)

응용 프로그램 기능에 대한 액세스를 제공합니다.

로그오프 URL 구성 (페이지 508)

전체 로그아웃을 적용하여 CA Identity Manager 환경에 대한 권한 없는 액세스를 방지합니다.

SiteMinder 영역에서 별칭 업데이트 (페이지 509)

환경의 별칭을 변경할 때 CA Identity Manager 환경을 보호하는 영역을 업데이트합니다.

SiteMinder 암호 (페이지 512)

CA Identity Manager 가 SiteMinder 와 통신하는 데 사용하는 관리자 계정의 암호와 CA Identity Manager 환경을 보호하는 SiteMinder 에이전트의 공유 암호를 변경할 수 있습니다.

CA Identity Manager 에이전트 설정 구성 (페이지 477)

SiteMinder 정책 서버와 통신하는 CA Identity Manager 에이전트의 성능을 조정합니다.

인증과 권한 부여에 서로 다른 디렉터리 사용 (페이지 514)

한 디렉터리에 프로필이 있는 관리자가 다른 디렉터리의 사용자를 관리하도록 설정합니다.

LDAP 디렉터리 오퍼레이션의 성능 개선 (페이지 516)

동일한 디렉터리에 대해 다중 연결을 열도록 SiteMinder 를 구성하여 사용자 저장소에 대한 CA Identity Manager 요청 처리량을 늘립니다.

사용자 지정 인증 체계를 사용하여 사용자 자격 증명 수집

SiteMinder 는 인증 체계를 사용하여 사용자 자격 증명을 수집하고 로그인 시 사용자 ID 를 확인합니다. 사용자가 식별되면 CA Identity Manager 가 사용자의 권한을 기반으로 개인 설정된 사용자 콘솔을 생성합니다.

모든 SiteMinder 인증 체계를 구현하여 CA Identity Manager 환경을 보호할 수 있습니다.

예를 들어 HTML 양식으로 자격 증명을 수집하는 HTML 양식 인증 체계를 구현할 수 있습니다. HTML 양식을 사용하면 회사 로고 같은 브랜딩 요소, 자체 등록 및 잊어버린 암호 페이지에 대한 링크 등을 포함할 수 있는 로그인 페이지를 만들 수 있습니다.

참고: 인증 체계에 대한 자세한 내용은 *CA SiteMinder Policy Server Configuration Guide*(CA SiteMinder 정책 서버 구성 안내서)를 참조하십시오.

다음 단계를 수행하십시오.

1. 다음 인터페이스 중 하나에 로그인합니다.
   - CA SiteMinder Web Access Manager r12 이상의 경우 관리 UI 에 로그인합니다.
   - CA eTrust SiteMinder 6.0 SP5 의 경우 정책 서버 사용자 인터페이스에 로그인합니다.

   참고: 이러한 인터페이스를 사용하는 방법에 대한 내용은 사용 중인 SiteMinder 버전의 설명서를 참조하십시오.
2. *CA SiteMinder Policy Server Configuration Guide*(CA SiteMinder 정책 서버 구성 안내서)에 설명된 대로 인증 체계를 만듭니다.
3. 1 단계에서 만든 인증 체계를 사용하도록 해당 CA Identity Manager 환경을 보호하는 영역을 수정합니다.

   영역 이름의 형식은 다음과 같습니다.

   *Identity Manager-environment*_ims_realm

   참고: 공용 태스크에 대한 지원을 구성한 경우 *Identity Manager-environment*_pub_realm 영역이 추가로 표시됩니다. 이 영역은 익명 인증 체계를 사용하여 알 수 없는 사용자가 자격 증명을 제공하지 않고 자체 등록 및 잊어버린 암호 기능이 사용되도록 설정합니다. 이러한 영역에 대해서는 인증 체계를 수정하지 마십시오.

데이터 정의를 정책 저장소로 가져오기

SiteMinder 정책을 사용하여 응용 프로그램 기능에 대한 사용자 액세스를 제어할 수 있습니다. 정책 서버 설치에는 이 제어를 허용하는 데 필요한 데이터 정의가 포함되어 있습니다. 다음 위치에서 IdmSmObjects.xdd 파일을 가져옵니다.

siteminder_home\xps\dd

siteminder_home 은 정책 서버 설치 경로입니다.

액세스 역할 계획

응용 프로그램에 대한 액세스를 제어하려면 액세스 역할 및 태스크를 만듭니다. 액세스 태스크는 응용 프로그램 기능에 대한 액세스를 제공합니다. 액세스 역할은 하나 이상의 응용 프로그램에 대한 액세스 태스크를 하나 이상 포함합니다. 사용자에게 액세스 역할이 할당된 경우 사용자는 해당 역할에 있는 기능을 사용할 수 있습니다.

응용 프로그램 액세스를 위한 액세스 역할에서는 액세스 역할의 용도에 대해 자세히 설명합니다.

액세스 역할을 사용하려면 Identity Manager 와 SiteMinder 에서 구성해야 합니다. 다음 두 관리자가 참여해야 합니다.

- Identity Manager 관리자 - Identity Manager 에서 액세스 역할 및 태스크를 만들 수 있어야 합니다. 기본 "시스템 매니저" 및 "액세스 역할 매니저" 역할에 이러한 태스크가 포함되어 있습니다.
- SiteMinder 관리자 - 시스템 범위를 가지며 시스템 및 도메인 개체를 관리할 수 있어야 합니다. 자세한 내용은 *CA eTrust SiteMinder Policy Design*(CA eTrust SiteMinder 정책 설계)을 참조하십시오.

참고: 정책 설계 사용자 인터페이스에서 사용하는 용어인 *Identity Manager 환경*이 지금은 *Identity Manager 환경*으로 바뀌었습니다. 또한 이 제품과 함께 제공된 SiteMinder 설명서에서는 이를 *Identity Manager* 라고 합니다. r8.1 의 경우 새 제품 이름은 *Identity Manager* 입니다.

다음 절차에서는 액세스 역할을 만드는 단계에 대해 설명합니다.

1. "액세스 역할 매니저" 역할이 있는 Identity Manager 관리자는
   a. 액세스 태스크를 만듭니다.
   b. 액세스 역할을 만듭니다.
   c. SiteMinder 관리자에게 역할 및 태스크 정보를 전달합니다.
2. SiteMinder 관리자는 다음을 수행하여 역할 기반 액세스 제어 정책을 만듭니다.
   a. 하나 이상의 Identity Manager 환경과 연결된 사용자 디렉터리를 정책 도메인에 할당
   b. 하나 이상의 Identity Manager 환경을 1 단계의 정책 도메인과 연결
   c. 정책 도메인에 영역 및 규칙 만들기(아직 없는 경우). 영역 및 규칙은 액세스 역할이 액세스 권한을 부여할 리소스에 해당해야 합니다.
   d. Identity Manager 환경에서 정책을 만들어 역할에 바인딩
   e. (선택 사항) 보호된 리소스에 권한 정보를 전달하는 응답 지정

   이전 단계에 대한 지침은 *CA eTrust SiteMinder Policy Design*(CA eTrust SiteMinder 정책 설계)을 참조하십시오.

SiteMinder 와 함께 액세스 역할이 사용되도록 설정

CA SiteMinder 와 함께 액세스 역할을 사용하기 위해 CA CA Identity Manager 는 SiteMinder 정책 저장소에 있는 액세스 역할과 관련된 CA Identity Manager 개체 저장소의 모든 개체를 미러링합니다. 이 동작이 발생하도록 설정하려면 CA Identity Manager 관리 콘솔에서 속성을 구성합니다.

SiteMinder 와 함께 액세스 역할이 사용되도록 설정하려면

1. 관리 콘솔을 엽니다.
2. "Environment"(환경), *Your Environment*, "Advanced Settings"(고급 설정), "Miscellaneous"(기타)를 차례로 선택합니다.
3. 다음 정보를 제공하여 새 속성을 추가합니다.
   - "Property"(속성) 필드에 다음을 입력합니다.

     EnableSMRBAC
   - "Value"(값) 필드에 다음을 입력합니다.

     true

4. "Add"(추가)를 클릭합니다. 그런 다음 "Save"(저장)를 클릭합니다.

   환경을 다시 시작해야 한다는 메시지가 나타납니다.

5. "Restart Environment"(환경 다시 시작)를 클릭합니다.

   이제 CA CA Identity Manager 가 CA SiteMinder 와 함께 사용할 액세스 역할 및 태스크를 지원합니다.

CA SiteMinder 와 함께 액세스 역할이 사용되도록 설정한 후 다음 사항에 주의하십시오.

- CA Identity Manager r8x 에서 액세스 역할을 사용한 경우 추가 마이그레이션 단계를 수행해야 현재 CA CA Identity Manager 버전에서 해당 액세스 역할을 관리할 수 있습니다. 자세한 내용은 *업그레이드 안내서*를 참조하십시오.
- SiteMinder 에서 액세스 역할에 대한 지원이 사용되지 않도록 설정하려면 SiteMinder 정책 저장소에서 CA Identity Manager 액세스 역할 및 태스크 개체를 삭제하십시오. 그런 다음 "Miscellaneous Properties"(기타 속성) 목록에서 "EnableSMRBAC" 속성을 제거하고 환경을 다시 시작하십시오.

관리자 역할에 액세스 태스크 추가

기본적으로 액세스 태스크는 "Roles and Tasks"(역할 및 태스크) 탭 아래에 나타나지 않습니다. 따라서 로그인한 사용자의 관리자 역할에 액세스 태스크를 추가해야 합니다.

다음 단계를 수행하십시오.

1. 액세스 역할을 만들기 위한 태스크가 포함된 역할이 있는 CA Identity Manager 계정에 로그인합니다.
2. "역할 및 태스크", "관리자 역할 수정"을 차례로 클릭합니다.
3. 로그인한 사용자의 관리자 역할을 선택합니다.
4. "태스크" 탭과 "범주별 필터링" 필드를 차례로 클릭한 다음 드롭다운에서 "Select Roles and Tasks"(역할 및 태스크 선택)를 선택합니다.
5. "태스크 추가" 드롭다운에서 "액세스 태스크 만들기"를 선택합니다.
6. 제출을 클릭합니다.

액세스 태스크 만들기

액세스 태스크는 재무 응용 프로그램에서 구매 주문을 생성하는 동작 같이 비즈니스 응용 프로그램에서 사용자가 수행할 수 있는 단일 동작입니다. 사용자는 액세스 태스크가 포함된 액세스 역할을 할당받은 경우 해당 동작을 수행할 수 있습니다.

중요! 액세스 태스크를 만들려면 로그인한 사용자의 관리자 역할에 액세스 태스크를 추가 (페이지 490)해야 합니다.

다음 단계를 수행하십시오.

1. "역할 및 태스크", "액세스 태스크", "액세스 태스크 만들기"를 차례로 선택합니다.
2. 다음 옵션 중 하나를 선택합니다.
   - 액세스 태스크 만들기
   - 액세스 태스크의 사본 만들기

3. 다음 필드에 정보를 입력합니다.

이름

구매 주문 생성 같이 태스크에 할당할 수 있는 고유한 이름입니다.

태그

태스크의 고유한 태그입니다. 태그는 문자나 밑줄로 시작해야 하며 문자, 숫자 또는 밑줄만 포함해야 합니다.

설명

태스크의 용도에 대한 선택적 참고 사항입니다.

응용 프로그램 ID

태스크와 연결된 응용 프로그램의 식별자(예: 응용 프로그램 이름)입니다. 응용 프로그램 ID 는 공백이나 영숫자가 아닌 문자를 포함할 수 없습니다.

이 ID 를 기록해 둡니다. SiteMinder 에서 역할이 사용되도록 설정할 때 필요합니다.

4. 액세스 태스크를 완료하려면 "제출"을 클릭합니다.

액세스 역할을 만드는 방법

액세스 역할은 응용 프로그램 기능에 대한 액세스를 제공하는 액세스 태스크를 포함합니다. 예를 들어 역할은 역할 구성원이 구매 응용 프로그램에서 주문하고 재고 관리 응용 프로그램에서 수량을 업데이트하도록 설정하는 태스크를 포함할 수 있습니다.

액세스 역할을 만들려면 다음 단계를 완료합니다.

1. 액세스 역할 만들기를 시작합니다. (페이지 493)
2. "프로필" 탭에서 액세스 역할의 기본 속성을 정의합니다. (페이지 494)
3. 역할에 대한 액세스 태스크를 선택합니다. (페이지 494)
4. 역할의 구성원 정책을 정의합니다. (페이지 495)
5. 역할의 관리자 정책을 정의합니다. (페이지 496)
6. 역할의 소유자 규칙을 정의합니다. (페이지 497)

액세스 역할 만들기 시작

1. 액세스 역할을 만드는 작업이 포함된 역할을 가진 Identity Manager 계정에 로그인합니다.
2. "액세스 역할", "액세스 역할 만들기"를 클릭합니다.

   새 역할이나 역할 사본을 만드는 옵션을 선택합니다. "복사"를 선택한 경우 역할을 검색합니다.
3. 다음 섹션인 액세스 역할의 프로필 정의로 계속 진행합니다.

액세스 역할의 프로필 정의

액세스 역할의 프로필을 정의하려면

1. 이름과 설명을 입력하고, 역할에 대해 정의된 사용자 지정 특성을 완료합니다.

   참고: "프로필" 탭에서 액세스 역할에 대한 추가 정보를 지정하는 사용자 지정 특성을 지정할 수 있습니다. 이 추가 정보를 사용하여 수많은 역할을 포함하는 환경에서 역할을 쉽게 검색할 수 있습니다.

2. 역할을 만드는 즉시 사용할 수 있게 하려면 "사용"을 선택합니다.
3. 다음 섹션인 액세스 역할의 구성원 정책 정의로 계속 진행합니다.

역할의 액세스 태스크 선택

"태스크" 탭에서 다음을 수행합니다.

1. 이 역할에 포함할 태스크를 선택합니다. 먼저 응용 프로그램을 선택한 다음 태스크를 선택합니다. 여러 응용 프로그램의 태스크를 포함할 수 있습니다.

   참고: 필요한 태스크가 다른 역할에 있으면 "다른 역할에서 태스크 복사"를 클릭합니다. 나타난 목록을 편집할 수 있습니다.

   역할이나 태스크를 만드는 경우 다음과 같이 항목을 추가, 편집 및 제거하기 위한 아이콘이 표시됩니다.

   앞으로 이동하거나 현재 항목을 선택하여 보거나 편집합니다.

   JavaScript 가 사용되지 않도록 설정된 경우 앞으로 단추를 눌러 드롭다운 목록에서 선택합니다.

   뒤로 이동하거나 이전 선택을 취소합니다.

태스크 또는 규칙 같은 요소를 삽입합니다.

현재 태스크를 삭제하거나 규칙에서 뒤에 나오는 표현식을 삭제합니다.

현재 항목을 목록에서 위로 이동합니다.

현재 항목을 목록에서 아래로 이동합니다.

2. 다음 단원인 액세스 역할의 관리자 정책 정의로 계속 진행합니다.

액세스 역할의 구성원 정책 정의

구성원 정책은 역할의 구성원 규칙과 범위 규칙을 정의합니다. 하나의 역할에 대해 여러 구성원 정책을 정의할 수 있습니다. 각 정책에 대해 구성원 규칙의 조건을 충족하는 사용자는 해당 정책에 정의된 역할을 사용하기 위한 범위를 갖습니다.

다음 단계를 수행하십시오.

1. "구성원" 탭을 선택합니다.
2. "추가"를 선택하여 구성원 정책을 정의합니다.
3. (선택 사항) "구성원 정책" 페이지에서 이 역할을 사용할 수 있어야 하는 사용자에 대한 구성원 규칙을 선택적으로 정의합니다.

   구성원 규칙을 정의하면 구성원 정책의 조건과 일치하는 사용자에게 역할이 자동으로 할당됩니다.

   참고: 디렉터리 특성(예: title=Manager)만 사용하는 구성원 규칙을 정의합니다. 관리자 역할 같이 사용자 디렉터리에 저장되지 않는 개체를 참조하는 구성원 규칙을 정의하면 SiteMinder 가 참조를 확인할 수 없습니다.

4. 구성원 정책이 "구성원" 탭에 나타나는지 확인합니다.

   정책을 편집하려면 왼쪽의 화살표 기호를 클릭하십시오. 정책을 제거하려면 빼기 기호 아이콘을 클릭하십시오.

5. "구성원" 탭에서 "관리자가 이 역할의 구성원을 추가하거나 제거할 수 있습니다." 확인란이 사용되도록 설정합니다.

   이 기능이 사용되도록 설정한 후 "추가 동작" 및 "제거 동작"을 정의합니다. 이러한 동작은 사용자가 역할의 구성원으로 추가되거나 제거될 때 발생하는 결과를 정의합니다.

액세스 역할의 관리자 정책 정의

관리자 정책은 역할의 관리자 규칙, 범위 규칙 및 관리자 권한을 정의합니다. 하나의 역할에 대해 여러 관리자 정책을 정의할 수 있습니다. 각 정책에 대해 관리자 규칙의 조건을 충족하는 관리자는 해당 정책에 대해 정의된 범위와 관리자 권한을 갖습니다.

다음 단계를 수행하십시오.

1. 액세스 역할의 "관리자" 탭을 선택합니다.
2. "관리자 관리" 옵션을 사용할 수 있도록 설정하려면 "관리자가 이 역할의 관리자를 추가하거나 제거할 수 있습니다." 확인란을 선택합니다.

   이 기능이 사용되도록 설정한 후 사용자가 역할의 관리자로 추가되거나 제거될 때 발생하는 동작을 정의합니다.

3. "관리자" 탭에서 관리자 및 범위 규칙과 관리자 권한이 포함된 관리자 정책을 추가합니다. 각 정책마다 하나 이상의 권한("구성원 관리" 또는 "관리자 관리")이 필요합니다.

   규칙을 충족하는 관리자에 대해 규칙과 권한이 각기 다른 관리자 정책을 여러 개 추가할 수 있습니다.

   참고: 디렉터리 특성(예: title=Manager)만 사용하는 관리자 정책을 정의합니다. 관리자 역할 같이 사용자 디렉터리에 저장되지 않는 개체를 참조하는 구성원 정책을 정의하면 SiteMinder 가 참조를 확인할 수 없습니다.

4. 정책을 편집하려면 왼쪽의 화살표 기호를 클릭하십시오. 정책을 제거하려면 빼기 기호 아이콘을 클릭하십시오.

5. 다음 단원인 액세스 역할의 소유자 정책 정의로 계속 진행합니다.

액세스 역할의 소유자 규칙 정의

소유자 규칙은 역할을 수정할 수 있는 사용자를 정의합니다. 하나의 역할에 대해 여러 소유자 규칙을 정의할 수 있습니다.

다음 단계를 수행하십시오.

1. 액세스 역할의 "소유자" 탭을 선택합니다.

2. 역할을 수정할 수 있는 사용자를 결정하는 소유자 규칙을 정의합니다.

   참고: 디렉터리 특성(예: title=Manager)만 사용하는 소유자 규칙을 정의합니다. 관리자 역할 같이 사용자 디렉터리에 저장되지 않는 개체를 참조하는 소유자 규칙을 정의하면 SiteMinder 가 참조를 확인할 수 없습니다.

3. "제출"을 클릭합니다.

   태스크가 제출되었다는 메시지가 나타납니다. 사용자가 역할을 사용할 수 있기 전에 일시 지연이 발생할 수 있습니다.

SiteMinder 에서 액세스 역할이 사용되도록 설정

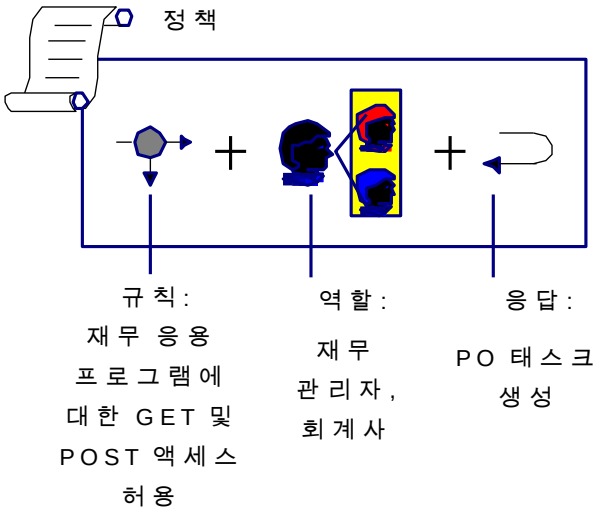
SiteMinder 관리자는 사용자가 리소스와 상호 작용하는 방식을 정의하는 보안 정책에 역할을 바인딩합니다. 정책에서 다음 개체를 연결할 수 있습니다.

- 사용자 및 사용자 그룹 - 정책의 영향을 받는 일련의 사용자를 식별합니다.
- 역할 - Identity Manager 에서 일련의 권한이 할당된 사용자를 식별합니다.
- 규칙 - 리소스와 해당 리소스에 대해 허용되거나 거부되는 동작을 식별합니다. 리소스는 대개 URL, 응용 프로그램 또는 스크립트입니다.
- 응답 - 규칙에 대한 반응을 결정합니다. 규칙이 실행되면 응답이 SiteMinder 에이전트에 반환됩니다.

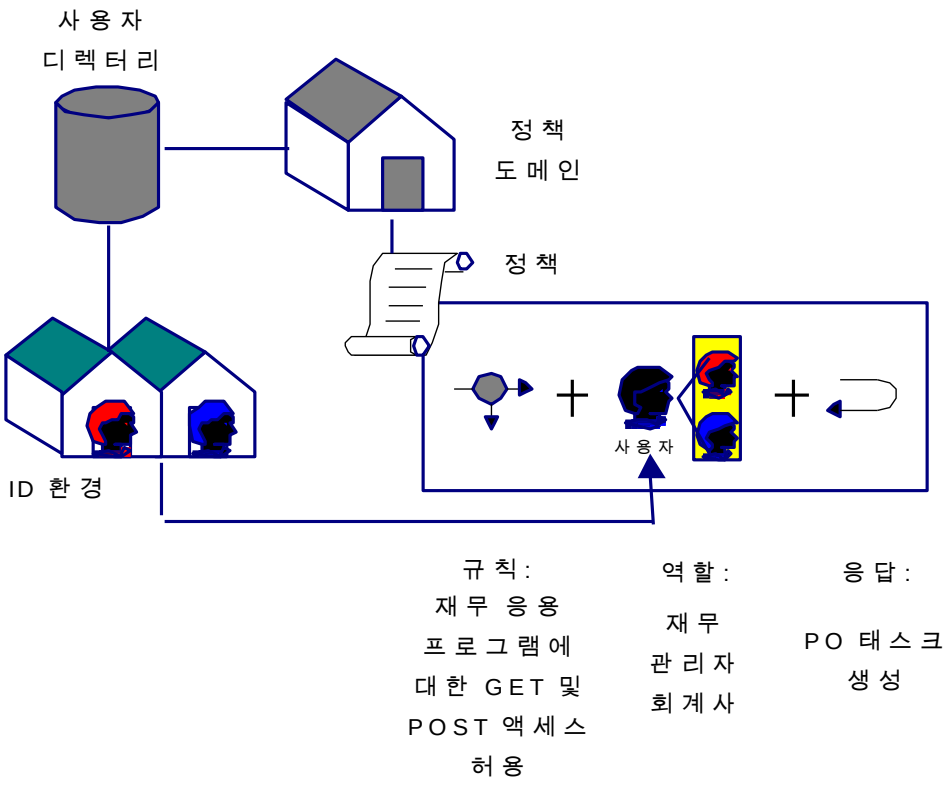
  Identity Manager 는 SiteMinder 응답을 사용하여 보호된 리소스에 특정 태스크 및 역할 정보를 전달합니다.

SiteMinder 정책을 사용자, 역할 또는 사용자 *및*/역할에 바인딩할 수 있습니다. 사용자나 역할 구성원이 보호된 리소스에 액세스하려고 하면 SiteMinder 가 정책에 있는 정보를 사용하여 액세스 권한 부여 여부를 결정하고 응답을 트리거합니다.

다음 그림에서는 역할 기반 정책에 있는 정책 개체의 관계를 보여 줍니다.



사용자 디렉터리를 보호된 리소스에 논리적으로 연결하는 정책 도메인에서 SiteMinder 정책이 만들어집니다. 다음 그림에서는 역할 기반 정책에 있는 정책 개체의 관계를 보여 줍니다.



사용자에게 보호된 응용 프로그램에 대한 권한을 제공하기 위해 SiteMinder 관리자가 응용 프로그램의 정책에 있는 규칙과 응답을 쌍으로 연결합니다. 응답은 SiteMinder 에서 생성되고 Identity Manager 에서 권한 정보를 검색하는 응답 특성을 포함합니다.

SiteMinder 가 역할 구성원에게 보호된 리소스에 대한 권한을 부여하는 경우 다음 이벤트가 발생합니다.

1. 정책의 규칙이 SiteMinder 에서 실행되어 쌍으로 연결된 응답을 트리거합니다.
2. 정책 서버가 Identity Manager 에서 응답에 포함할 권한 정보를 얻습니다.

3. 응답 특성이 정책 서버에서 웹 에이전트로 전달됩니다.
4. 웹 에이전트가 권한 정보를 HTTP 헤더 변수나 쿠키로 응용 프로그램에 제공합니다.

SiteMinder 에서 생성되는 응답 특성

Identity Manager 는 SiteMinder 웹 에이전트 응답을 통해 응용 프로그램에 권한 정보를 전달합니다. 이러한 응답은 응용 프로그램이 사용자의 액세스 권한을 결정하는 데 사용될 수 있는 응답 특성에 HTTP 헤더 변수를 포함합니다. 응답은 사용자가 보호된 리소스와 상호 작용하는 방식을 결정하는 SiteMinder 정책에 포함됩니다.

SiteMinder 관리자는 응용 프로그램에 정보를 전달하도록 다음 두 가지 응답 특성 유형이 포함된 응답을 구성할 수 있습니다.

- SM_USER_APPLICATION_ROLES[:*application id*] - 사용자에게 할당된 역할 목록을 반환합니다.
- SM_USER_APPLICATION_TASKS[:*application id*] - 사용자가 자신에게 할당된 역할을 기반으로 수행할 수 있는 태스크 목록을 반환합니다.

응용 프로그램 ID 는 요청된 역할 및 태스크 세트를 특정 응용 프로그램으로 제한합니다. 예를 들어 다음 응답 특성을 만드는 경우

SM_USER_APPLICATION_ROLES:Finance_application

SiteMinder 는 재무 응용 프로그램에 태스크가 있는 역할을 웹 에이전트에 반환합니다. 그러면 정보가 웹 에이전트에서 재무 응용 프로그램으로 전달됩니다.

참고: 제공하는 *application id* 는 Identity Manager 에서 "액세스 태스크 만들기"를 사용할 때 제공한 *application id* 와 일치해야 합니다. 태스크를 아직 만들지 않은 경우 응용 프로그램 ID 로 모든 이름을 선택할 수 있지만 공백이나 영숫자가 아닌 문자를 포함할 수 없습니다.

쉼표로 구분된 목록으로 여러 응용 프로그램 ID 를 지정하여 단일 응답 특성에서 여러 응용 프로그램의 역할 및 태스크 세트를 반환할 수 있습니다. 예를 들어 사용자가 재무 및 구매 응용 프로그램에서 소유하고 있는 역할 목록을 반환하려면 다음을 지정하십시오.

SM_USER_APPLICATION_ROLES:Finance, Purchasing

SiteMinder 에서 액세스 역할이 사용되도록 설정하기 위한 체크리스트

참고: 다음 단계에서는 만들고 있는 액세스 역할이 적용되는 응용 프로그램이 이미 SiteMinder 로 보호되고 있다고 가정합니다. SiteMinder 로 보호되지 않는 응용 프로그램의 액세스 역할을 만들려는 경우 SiteMinder 에서 응용 프로그램을 구성하는 데 필요한 지침은 *CA eTrust SiteMinder Policy Design*(CA eTrust SiteMinder 정책 설계) 안내서를 참조하십시오.

✓	단계	참조
	1. 정책 서버 사용자 인터페이스에서 Identity Manager 환경과 연결된 사용자 디렉터리를 정책 도메인에 할당합니다.	*CA eTrust SiteMinder Policy Design(CA eTrust SiteMinder 정책 설계)*
	2. 액세스 역할이 적용되는 응용 프로그램을 보호하는 SiteMinder 도메인에 Identity Manager 환경을 추가합니다.	*CA eTrust SiteMinder Policy Design(CA eTrust SiteMinder 정책 설계)*
	3. 정책 도메인에서 액세스 역할이 액세스 권한을 부여할 리소스에 해당하는 영역 및 규칙(아직 없는 경우)을 만듭니다.	*CA eTrust SiteMinder Policy Design(CA eTrust SiteMinder 정책 설계)*

✓	단계	참조
	4. 리소스에 권한 정보를 전달하기 위한 응답을 만듭니다.	SiteMinder 응답 만들기 (페이지 504)
	5. 정책을 만들어 다음과 연결합니다. ■ Identity Manager 에서 만든 역할 ■ 2 단계에서 만든 영역 및 규칙 ■ 4 단계에서 만든 응답	*CA eTrust SiteMinder Policy Design(CA eTrust SiteMinder 정책 설계)*

정책 도메인에 Identity Manager 환경 추가

SiteMinder 가 액세스 역할을 지원하도록 설정하려면 SiteMinder 에서 CA Identity Manager 환경을 사용자 디렉터리 및 정책 도메인과 연결하십시오.

참고: 정책 도메인에 CA Identity Manager 환경과 연결된 사용자 저장소를 추가한 *후*에야 정책 도메인에 CA Identity Manager 환경을 추가할 수 있습니다.

정책 도메인에 CA Identity Manager 환경을 추가하려면

1. 정책 서버 사용자 인터페이스의 "Policy Domain"(정책 도메인) 대화 상자에서 다음과 같이 정책 도메인에 CA Identity Manager 환경과 연결된 사용자 저장소를 추가합니다.
   a. "사용자 디렉터리" 탭을 선택합니다.
   b. 탭의 하단에 있는 드롭다운 목록 상자에서 정책 도메인에 포함할 사용자 디렉터리를 선택합니다.
   c. '추가' 단추를 클릭합니다.

      정책 서버 사용자 인터페이스가 "사용자 디렉터리" 탭에 표시된 목록에 디렉터리를 추가합니다.
   d. "적용"을 클릭합니다.

2. 다음과 같이 정책 도메인에 CA Identity Manager 환경을 추가합니다.
   a. CA Identity Manager 환경 탭을 선택합니다.
   b. 탭의 하단에 있는 드롭다운 목록에서 정책 도메인과 연결할 CA Identity Manager 환경을 선택합니다.
   c. "추가"를 클릭합니다.

      정책 서버 사용자 인터페이스가 탭의 상단에 있는 CA Identity Manager 환경 목록에 선택 항목을 추가합니다.
3. "확인"을 클릭하여 선택 사항을 저장하고 대화 상자를 닫습니다.

   이제 정책을 만들 때 선택한 CA Identity Manager 환경을 사용할 수 있습니다.

SiteMinder 응답 만들기

1. 정책 서버 사용자 인터페이스에 로그인합니다.
2. 관리 권한에 따라 다음 중 하나를 수행합니다.
   - "시스템 및 도메인 개체 관리" 권한이 있는 경우
     a. "개체" 창에서 "도메인" 탭을 클릭합니다.
     b. 응답을 추가할 정책 도메인을 선택합니다.
   - "도메인 개체 관리" 권한이 있는 경우 "개체" 창에서 응답을 추가할 정책 도메인을 선택합니다.
3. 메뉴 표시줄에서 "편집", <domain name>, "응답 만들기"를 차례로 선택합니다.

   "SiteMinder 응답" 대화 상자가 열립니다("응답" 대화 상자 참조).
4. 새 응답의 이름과 설명을 입력합니다.
5. "에이전트 유형" 그룹 상자에서 SiteMinder 라디오 단추를 선택합니다.

6. "에이전트 유형" 그룹 상자의 드롭다운 목록에서 "웹 에이전트" 옵션을 선택하고 "적용"을 클릭하여 변경 내용을 저장합니다.
7. "만들기"를 클릭합니다.

   "SiteMinder 응답 특성 편집기" 대화 상자가 열립니다.
8. "특성" 드롭다운 목록에서 "WebAgent-HTTP-Header-Variable" 응답 특성을 선택합니다.
9. "특성 설정" 탭에서 "사용자 특성" 라디오 단추를 선택합니다.
10. "변수" 필드에 응용 프로그램에 전달될 변수의 이름을 입력합니다.

    예를 들어 TASKS 변수를 지정하면 다음 헤더가 응용 프로그램에 반환됩니다.

    HTTP_TASKS
11. "특성 이름" 필드에서 다음과 같이 응답 특성을 지정합니다.
    - SM_USER_APPLICATION_ROLES[:*application id1, application_id2, ...application_idn*]--사용자에게 할당된 역할 목록을 반환합니다.
    - SM_USER_APPLICATION_TASKS[:*application id1, application_id2, ...application_idn*]

    SiteMinder 생성 응답 특성 (페이지 501)에서는 추가 정보를 제공합니다.
12. "확인"을 클릭하여 변경 내용을 저장하고 SiteMinder 관리 창으로 돌아갑니다.

SiteMinder 정책에 역할 추가

적절한 액세스 역할이 할당된 사용자가 보호된 리소스에 액세스하려고 하면 SiteMinder 정책 서버는 사용자에게 액세스 역할이 할당되었는지 확인한 다음 정책에 포함된 규칙을 실행하여 사용자가 리소스에 액세스할 수 있는지 확인합니다.

SiteMinder 정책에 액세스 역할을 추가하려면

1. SiteMinder 정책 대화 상자에서 "사용자" 탭을 클릭합니다.

   "사용자" 탭에는 정책 도메인에 포함된 각 사용자 디렉터리 및 CA Identity Manager 환경에 대한 탭이 포함되어 있습니다.

2. 정책에 추가할 역할이 포함된 CA Identity Manager 환경을 선택합니다.
3. "추가/제거" 단추를 클릭합니다.

   "SiteMinder Policy Identity Manager Role"(SiteMinder 정책 Identity Manager 역할) 대화 상자가 열립니다.

4. 정책에 역할을 추가하려면 "사용 가능한 구성원" 목록에서 항목을 선택하고 "현재 구성원" 목록으로 이동합니다.
5. "확인"을 클릭하여 변경 내용을 저장하고 SiteMinder 정책 대화 상자로 돌아갑니다.

정책에서 역할 제외

액세스 역할을 사용하여 응용 프로그램에 대한 액세스 권한을 부여하는 것 외에, 액세스 역할을 사용하여 액세스 역할의 구성원이 응용 프로그램에 액세스하지 못하게 할 수도 있습니다. 액세스 역할 구성원이 응용 프로그램에 액세스하지 못하게 하려면 SiteMinder 정책에서 역할을 제외하십시오. CA Identity Manager 에서 제외된 액세스 역할이 할당된 사용자가 보호된 리소스에 액세스하려고 하면 정책 서버는 할당된 사용자에 대해 CA Identity Manager 역할이 제외되었는지 확인합니다. 확인되면 리소스에 대한 액세스가 차단됩니다.

다음 단계를 수행하십시오.

1. SiteMinder 정책 대화 상자에서 "사용자" 탭을 클릭합니다.

   "사용자" 탭에는 정책 도메인에 포함된 각 사용자 디렉터리 및 CA Identity Manager 환경에 대한 탭이 포함되어 있습니다.

2. 정책에서 제외할 역할이 포함된 CA Identity Manager 환경을 클릭합니다.

3. "추가/제거" 단추를 클릭합니다.

   SiteMinder 정책 CA Identity Manager 역할 대화 상자가 열립니다.

4. 정책에 역할을 추가하려면"사용 가능한 구성원" 목록에서 항목을 선택하고 "현재 구성원" 목록을 가리키는 왼쪽 화살표 단추를 클릭합니다.

   반대로 절차를 수행하면 "현재 구성원" 목록에서 역할이 제거됩니다.

5. "현재 구성원" 목록에서 제외할 역할을 선택하고 목록 아래에 있는 "제외" 단추를 클릭합니다.

   슬래시가 포함된 빨간색 원이 제외된 역할 왼쪽에 표시됩니다.

6. "확인"을 클릭하여 변경 내용을 저장하고 SiteMinder 정책 대화 상자로 돌아갑니다.

로그오프 URI 구성

CA Identity Manager 환경을 보호하려면 사용자가 CA Identity Manager 에서 로그오프하고 나면 환경을 보호하는 SiteMinder 웹 에이전트가 사용자 세션을 종료하도록 구성해야 합니다.

웹 에이전트는 웹 브라우저에서 SiteMinder 세션 및 인증 쿠키를 삭제하고 세션 정보를 모두 제거하도록 정책 서버에 지시하여 사용자 세션을 종료합니다.

SiteMinder 세션을 종료하려면 CA Identity Manager 환경을 보호하는 SiteMinder 에이전트의 에이전트 구성 개체에 있는 LogOffURI 필드에서 로그아웃 기능을 구성합니다.

참고:

- SiteMinder 에이전트에는 하나의 로그오프 URI 가 있습니다. 에이전트에서 보호하는 모든 응용 프로그램은 동일한 로그아웃 페이지를 사용합니다.
- 로그아웃 페이지 구성에 설명된 대로 관리 콘솔에서 사용자 지정 로그아웃 페이지를 구성하면 CA Identity Manager 는 로그아웃 요청을 사용자 지정 로그아웃 페이지 *및*/로그오프 URI 에 보냅니다. 그러나 사용자에게는 사용자 지정 로그아웃 페이지만 표시됩니다.

다음 단계를 수행하십시오.

1. 다음 인터페이스 중 하나에 로그인합니다.
   - CA SiteMinder r12 이상의 경우 관리 UI 에 로그인합니다.
   - CA eTrust SiteMinder 6.0 SP5 의 경우 정책 서버 사용자 인터페이스에 로그인합니다.

   참고: 이러한 인터페이스를 사용하는 방법에 대한 내용은 사용 중인 SiteMinder 버전의 설명서를 참조하십시오.

2. CA Identity Manager 환경을 보호하는 에이전트의 에이전트 구성 개체에서 #LogOffUri 속성을 다음과 같이 수정합니다.
   - 파운드 기호(#)를 제거합니다.
   - "값" 필드에 다음 URI 를 지정합니다.

     /iam/im/logout.jsp

   참고: 웹 에이전트를 설치할 때 에이전트 구성 개체를 선택합니다. 자세한 내용은 *CA SiteMinder Web Access Manager 정책 서버 설치 안내서*를 참조하십시오.
3. 변경 내용을 저장합니다.
4. 웹 서버를 다시 시작합니다.

SiteMinder 영역의 별칭

*별칭*은 CA Identity Manager 환경에 액세스하기 위해 URL 에 추가되는 고유 문자열입니다. 예를 들어 환경의 별칭이 *employees* 인 경우 해당 환경에 액세스하기 위한 URL 은 다음과 같습니다.

`http://myserver.mycompany.org/iam/im/employees`

myserver.mycompany.org

CA Identity Manager 가 설치된 서버의 정규화된 도메인 이름을 정의합니다.

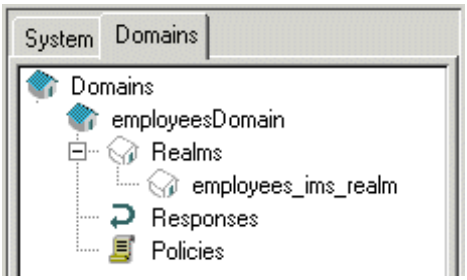
관리 콘솔에서 CA Identity Manager 환경을 만들 때 별칭을 하나 이상 지정합니다. 공용 별칭을 지정할 수도 있습니다.

SiteMinder 는 환경 이름을 사용하여 환경을 보호하는 개체의 이름을 지정합니다. 예를 들어 *employees* 라는 이름을 지정하는 경우 SiteMinder 는 *employeesobject_type* 이라는 개체를 만듭니다.

object_type

employees_ims_realm 과 같은 SiteMinder 개체를 정의합니다.

다음 그림에서는 SiteMinder 가 만드는 개체 중 2 개를 보여 줍니다.



SiteMinder 영역에서 별칭 업데이트

관리 콘솔에서 보호 별칭 또는 공용 별칭을 수정하는 경우 CA Identity Manager 는 정책 서버에서 별칭 이름을 업데이트하려고 합니다. CA Identity Manager 가 이름을 업데이트할 수 없는 경우 다음 인터페이스 중 하나에서 이름을 수동으로 업데이트할 수 있습니다.

- CA SiteMinder Web Access Manager r12 이상의 경우 관리 UI 를 사용합니다.
- CA eTrust SiteMinder 6.0 SP5 의 경우 정책 서버 사용자 인터페이스를 사용합니다.

다음 단계를 수행하십시오.

1. CA Identity Manager 환경에 대한 영역을 찾습니다.

   CA Identity Manager 가 SiteMinder 와 통합될 때 이러한 영역이 다른 필수 SiteMinder 개체와 함께 자동으로 만들어집니다.

   영역에는 다음과 같은 명명 규칙이 사용됩니다.

   - *Identity Manager-environment*_ims_realm - 사용자 콘솔을 보호합니다.
   - *Identity Manager-environment*_pub_realm - 자체 등록 및 잊어버린 암호 태스크와 같은 공용 태스크에 대한 지원이 사용되도록 설정합니다. 이 영역은 공용 별칭을 구성한 경우에만 표시됩니다.

     참고: 정책 서버 사용자 인터페이스를 사용하여 영역을 수정하는 경우에는 먼저 CA Identity Manager 환경의 정책 도메인(*Identity Manager-environment*Domain)을 찾습니다. 영역은 도메인 아래에 있습니다.

2. 영역의 리소스를 다음과 같이 수정합니다.

   /iam/im/*new_alias*

   리소스 필터에서 별칭 앞에 오는 /iam/im/을 제거하지 마십시오.

3. 변경 내용을 저장합니다.

참고: Modify CA Identity Manager Properties(CA Identity Manager 속성 수정)에서는 관리 콘솔에서 별칭을 변경하는 방법에 대한 지침을 제공합니다.

SiteMinder 암호 또는 공유 암호 수정

정책 서버에 대한 CA Identity Manager 확장을 설치할 때는 CA Identity Manager 가 정책 서버와 통신할 때 사용하는 SiteMinder 관리자 계정의 암호를 제공합니다.

이 암호를 변경할 수는 있지만 암호를 암호화해야 합니다. 암호를 암호화하려면 CA Identity Manager 와 함께 제공되는 암호 도구를 사용하십시오.

참고: SiteMinder 암호를 변경하기 전에 사용자 환경에 대해 JAVA_HOME 변수가 정의되어 있는지 확인하십시오.

다음 단계를 수행하십시오.

1. 다음과 같이 암호를 암호화합니다.
   a. 명령줄에서 *admin_tools*\PasswordTool 로 이동합니다. 여기서 *admin_tools* 는 다음 예와 같은 관리 도구의 설치 위치입니다.
      - **Windows:** C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\tools\PasswordTool
      - **UNIX:** /opt/CA/IdentityManager/IAM_Suite/Identity_Manager//tools/PasswordTool
   b. 다음 명령을 입력합니다.

      pwdtools *new_password*

      이 명령에서 *new_password* 는 암호화할 암호입니다.

      참고: pwdtools 유틸리티의 옵션에 대한 자세한 내용을 보려면 다음 명령을 입력하십시오.

      pwdtools help
   c. 암호화된 암호를 복사합니다.

2. 다음과 같이 관련 단계를 완료합니다.

   - CA Identity Manager 가 WebLogic 응용 프로그램 서버에서 실행되고 있는 경우 다음 태스크를 수행합니다.

     a. WebLogic 콘솔에서 policyserver_rar 커넥터 설명자의 WebLogic 리소스 어댑터를 편집합니다.

     b. 암호화된 암호를 암호 속성의 값으로 추가합니다.

   - CA Identity Manager 가 JBoss Application Server 에서 실행되고 있는 경우 다음 태스크를 수행합니다.

     a. *JBoss_home*\server\default\deploy\iam_im.ear\policyserver_rar\META-INF 에서 ra.xml 을 엽니다.

     b. 암호화된 암호를 암호 config-property 의 값으로 추가합니다.

   - CA Identity Manager 가 WebSphere 응용 프로그램 서버에서 실행되고 있는 경우 다음 태스크를 수행합니다.

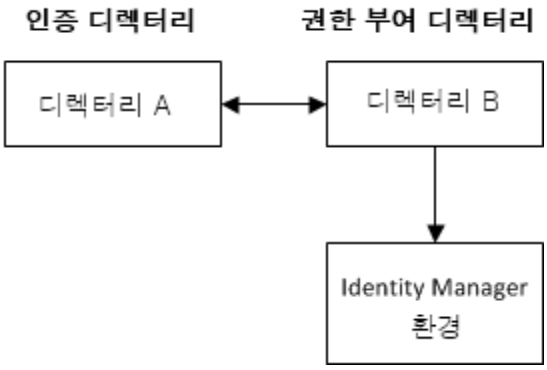
     a. WebSphere 콘솔에서 ra.xml 을 엽니다.

     b. 암호화된 암호를 암호 config-property 의 값으로 추가합니다.

3. 응용 프로그램 서버를 다시 시작합니다.

인증과 권한 부여에 서로 다른 디렉터리 사용 CA Identity Manager 환경 구성

관리자가 관리자 인증에 사용되는 것과 다른 사용자 저장소에 있는 프로필을 가지고 있는 사용자를 관리해야 하는 경우가 있습니다. 즉, 관리자가 CA Identity Manager 환경에 로그인할 때 다음 그림과 같이 하나의 디렉터리를 사용하여 인증되어야 하고 두 번째 디렉터리에서 사용자를 관리할 권한을 부여받아야 합니다.



다음 단계를 수행하십시오.

1. 다음 인터페이스 중 하나에 로그인합니다.
   - CA SiteMinder Web Access Manager r12 이상의 경우 관리 UI 에 로그인합니다.
   - CA eTrust SiteMinder 6.0 SP5 의 경우 정책 서버 사용자 인터페이스에 로그인합니다.

   참고: 이러한 인터페이스를 사용하는 방법에 대한 내용은 사용 중인 SiteMinder 버전의 설명서를 참조하십시오.
2. 두 개의 사용자 디렉터리를 만듭니다.

   한 디렉터리는 인증 데이터(관리자 프로필)를 참조하고, 다른 디렉터리는 권한 부여 데이터(사용자 프로필)를 참조합니다.
3. 관리 콘솔에서 CA Identity Manager 환경을 만듭니다.

   권한 부여 디렉터리를 CA Identity Manager 디렉터리로 선택합니다.

4. 사용되는 SiteMinder 버전의 인터페이스에서 이전 단계에서 만든 CA Identity Manager 환경의 도메인에 인증 디렉터리를 추가합니다.

   이 도메인 및 SiteMinder 에 필요한 다른 개체는 환경을 만들고 SiteMinder 가 CA Identity Manager 와 통합될 때 자동으로 만들어집니다.

   도메인은 다음 명명 규칙을 사용합니다.

   *Identity Manager-environment*Domain

5. 이 디렉터리가 도메인과 연결된 디렉터리 목록에서 처음에 표시되어야 합니다.
6. *Identity Manager-environment*_ims_realm 을 찾습니다.
7. 영역 정의의 "Advanced"(고급) 섹션에서 권한 부여 디렉터리를 인증 디렉터리에 매핑합니다.
8. 다음 *Identity Manager-environment*response_ims 응답을 찾습니다.
9. 응답에 다음과 같이 응답 특성을 추가합니다.

필드	값
특성	Web-Agent-HTTP-Header-Variable
특성 종류	사용자 특성
변수 이름	sm_userdn
특성 이름	SM_USERNAME

10. 변경 내용을 저장합니다.

    이제 CA Identity Manager 는 인증과 권한 부여에 서로 다른 디렉터리를 사용합니다.

LDAP 디렉터리 오퍼레이션의 성능을 개선하는 방법

LDAP 사용자 디렉터리에 대한 모든 CA Identity Manager 요청은 고정된 연결 세트를 통해 라우트되므로 디렉터리 오퍼레이션을 처리하는 데 오랜 시간이 걸릴 수 있습니다.

사용자 디렉터리에 대한 CA Identity Manager 요청의 처리량을 늘리려면 동일한 디렉터리에 대한 여러 연결을 열도록 SiteMinder 를 구성합니다. 이 절차를 수행하려면 정책 서버 사용자 인터페이스의 "LDAP 디렉터리 장애 조치 및 부하 분산 설정" 대화 상자에서 LDAP 서버를 여러 번 추가합니다.

LDAP 서버를 입력하는 횟수 및 설정할 연결 수는 CA Identity Manager 의 로드에 따라 다릅니다.

부록 A: FIPS 140-2 준수

이 섹션은 다음 항목을 포함하고 있습니다.

FIPS 개요

FIPS(Federal Information Processing Standards) 140-2 발행물은 제품에서 암호화를 위해 사용해야 하는 암호화 라이브러리 및 알고리즘에 대한 보안 표준입니다. FIPS 140-2 암호화는 CA 제품의 구성 요소 사이와 CA 제품 및 타사 제품 사이에 이루어지는 모든 중요한 데이터의 통신에 영향을 줍니다. FIPS 140-2 는 중요한 분류되지 않은 데이터를 보호하는 보안 시스템 내에서 암호화 알고리즘을 사용하기 위한 요구 사항을 지정합니다.

CA Identity Manager 는 미국 정부에 의해 조정된 AES(Advanced Encryption Standard)를 사용합니다. CA Identity Manager 는 암호화 모듈 관련 FIPS 140-2 보안 요구 사항을 만족하는 것으로 검증된 RSA Crypto-J v3.5 및 Crypto-C ME v2.0 암호화 라이브러리를 포함합니다.

통신

FIPS 암호화는 CA Identity Manager 와 다음 구성 요소 간의 모든 데이터 통신에 적용됩니다.

- CA Identity Manager 서버
- 프로비져닝 서버
- 프로비져닝 매니저 및 클라이언트
- C++ 커넥터 서버
- C++ 커넥터 서버 끝점(끝점에서 지원하는 경우)
- CA IAM 커넥터 서버(CA IAM CS)
- CA IAM CS 끝점(끝점에서 지원하는 경우)
- Connector Xpress(끝점에서 지원하는 경우)
- Windows 암호 동기화 에이전트
- JIAM(Java Identity and Access Management)

설치

Identity Manager 설치 관리자를 사용하여 FIPS 140-2 를 준수하도록 CA CA Identity Manager 를 구성할 수 있습니다.

Identity Manager 가 FIPS 140-2 를 지원하기 위해서는 Identity Manager 환경의 모든 구성 요소에서 FIPS 140-2 를 활성화해야 합니다. 설치 중에 FIPS 140-2 를 활성화하려면 FIPS 암호화 키가 필요합니다. FIPS 키를 생성하기 위한 암호 도구(pwdtools.bat/pwdtools.sh)는 다음 위치에 포함되어 있습니다.

```
C:\Program Files\CA\Identity Manager\IAM Suite\Identity
Manager\PasswordTool\pwdtools.bat
```

중요! 모든 설치에서 동일한 FIPS 140-2 암호화 키를 사용하고 암호 도구에서 생성된 키 파일을 안전하게 유지해야 합니다.

SiteMinder 에 연결

Identity Manager 설치 중에 CA SiteMinder 에 연결하는 경우 다음 표에 나열된 제품 버전 구성 및 FIPS 모드만 지원된다는 점에 유의하십시오.

Identity Manager r12	SiteMinder	SiteMinder 버전
FIPS 전용 모드	FIPS 전용 모드	r12
FIPS 전용 모드	FIPS 호환 모드	r12
비 FIPS 모드	FIPS 호환 모드	r12
비 FIPS 모드	비 FIPS 모드	r6

키 파일 저장소

CA CA Identity Manager 는 파일 시스템을 FIPS 암호화 키 저장소로 사용합니다. CA Identity Manager 관리자는 특정 그룹 또는 사용자 유형(예: CA CA Identity Manager 를 실행하도록 권한이 부여된 사용자)에 대해 디렉터리 액세스 권한을 설정하여 무단으로 액세스하지 못하도록 파일을 보호해야 합니다.

다음 표에는 각 CA Identity Manager 구성 요소에 대한 FIPS 키 파일의 위치가 정리되어 있습니다.

구성 요소	설치된 위치
CA Identity Manager 서버	*IdentityMinder.ear*\config\com\netegrity\config\keys\FIPSkey.dat *IdentityMinder.ear* 는 응용 프로그램 서버에서 CA CA Identity Manager 가 설치된 위치입니다.
프로비저닝 서버	*Provisioning Server install*\data\tls\keymgmt\imps_datakey
C++ 커넥터 서버	*Provisioning Server install*\data\tls\keymgmt\imps_datakey

암호 도구

FIPS 호환 암호 도구 유틸리티 pwdtools.bat(또는 pwdtools.sh)는 명령줄에서 CA Identity Manager 설치 중 암호화 키를 생성할 수 있습니다.

암호 도구를 사용하기 전에 pwdtools.bat/pwdtools.sh 파일을 편집하고 JAVA_HOME 변수를 필요에 맞게 설정합니다.

중요! CA Identity Manager 는 데이터 마이그레이션이나 재암호화를 지원하지 않습니다. 따라서 설치 후에는 암호화 키를 변경하지 않아야 합니다.

이 명령의 구문은 다음과 같습니다.

```
pwdtools -{FIPSKEY|JSAFE|FIPS|RC2} -p plain text [-k <키 파일 위치>] [-f  <암호화되는 매개 변수 파일>]
```

JSAFE

PBE 알고리즘을 사용하여 일반 텍스트 값을 암호화합니다.

예:

```
pwdtools -JSAFE –p mypassword
```

참고: 이전 버전에서 부트스트랩 관리자의 암호는 일반 텍스트로 저장되었습니다. CA Identity Manager r12.6 SP1 이상으로 업그레이드 또는 마이그레이션하는 경우 이 일반 텍스트 암호를 수동으로 암호화해야 합니다. 이 도구를 사용할 때는 JSAFE 옵션이 지정되어 있는지 확인하고 다음 단계를 수행하십시오.

1. CA Identity Manager r12.6 SP1 이상으로 업그레이드 또는 마이그레이션한 후에 CA Identity Manager 개체 저장소 데이터베이스로 이동하여 다음 테이블을 찾습니다.
   IM_AUTH_USER
2. 암호 도구와 JSAFE 를 사용하여 일반 텍스트 암호를 암호화하십시오.
3. 테이블에서 암호화된 암호로 일반 텍스트를 대체하십시오.

FIPSKEY

설치 관리자의 경우 FIPS 키 파일을 만듭니다. 이 키는 CA Identity Manager 설치 전에 생성합니다.

예:

```
pwdtools -FIPSKEY –k C:\keypath\FIPSkey.dat
```

여기서 *keypath* 는 FIPS 키를 저장할 위치의 전체 경로입니다.

암호 도구는 지정된 위치에 FIPS 키를 만듭니다. 설치 중 FIPS 키 파일의 위치를 설치 관리자에 제공합니다.

참고: CA Identity Manager 를 실행할 권한이 있는 사용자와 같은 특정 그룹 또는 사용자 유형에 대한 디렉터리 액세스 권한을 설정하여 키의 보안을 유지해야 합니다.

FIPS

FIPS 키 파일을 사용하여 일반 텍스트 값을 암호화합니다. FIPS 는 기존 FIPS 키 파일을 사용합니다.

예:

```
pwdtools -FIPS –p firewall -k C:\keypath\FIPSkey.dat
```

여기서 *keypath* 는 FIPS 키 디렉터리의 전체 경로입니다.

참고: 설치 중 지정한 것과 동일한 FIPS 키 파일을 사용합니다.

RC2

RC2 알고리즘을 사용하여 일반 텍스트 값을 암호화합니다.

중요! CA Identity Manager 는 FIPS 키 파일을 사용하여 응용 프로그램이 FIPS 모드로 시작하는지 또는 비 FIPS 모드로 시작하는지 확인합니다. 따라서 키 파일은 이름이 FIPSKey.dat 이고 다음과 같은 응용 프로그램 서버 배포 경로를 가져야 합니다.

```
iam_im.ear\config\com\netegrity\config\keys\FIPSkey.dat
```

여기서 iam_im.ear 는 응용 프로그램 서버 배포 디렉터리입니다. 예를 들면 다음과 같습니다.

```
jboss_home\server\default\deploy
```

FIPS 모드 감지

CA CA Identity Manager 가 FIPS 모드 또는 비 FIPS 모드에서 작동 중인지 확인하려면 CA Identity Manager 환경 상태 페이지를 사용하십시오.

상태 페이지를 보려면 브라우저에서 다음 URL 을 입력하십시오.

```
http://server_name/idm/status.jsp
```

server_name

CA CA Identity Manager 가 설치된 서버의 정규화된 도메인 이름(예: myserver.mycompany.com)을 지정합니다. 이 예제에서 전체 URL 은 다음과 같습니다.

http://myserver.mycompany.com/idm/status.jsp

FIPS 상태가 페이지 아래쪽에 표시됩니다.

참고: 다음 키 파일을 찾아 CA CA Identity Manager 가 FIPS 모드에서 작동 중인지 확인할 수도 있습니다.

```
/config/com/netegrity/config/keys/FIPSkey.dat
```

이 파일이 있을 경우 CA CA Identity Manager 는 FIPS 모드에서 작동 중입니다.

FIPSkey.dat 키 파일은 <CA idmgr> 설치 중에 암호 도구 유틸리티 pwdtools.bat(또는 pwdtools.sh)에 의해 생성됩니다.

암호화된 텍스트 형식

알고리즘 이름이 암호화된 텍스트에 접두어로 추가되어 암호화에 사용된 알고리즘을 CA Identity Manager 에 알려 줍니다.

FIPS 모드에서는 접두어가 {AES}입니다. 예를 들어 텍스트 "password"를 암호화하는 경우 암호화된 텍스트는 다음 예와 유사합니다.

{AES}:eolQCTq1CGPyg6qe++0asg==

비 FIPS 모드(또는 JSAFE 모드)에서는 알고리즘에 따라 접두어(알고리즘 태그)가 {PBES} 또는 {RC2}입니다. 예를 들어 텍스트 "password"를 암호화하는 경우 암호화된 텍스트는 다음과 유사합니다.

{PBES}:gSex2/BhDGzEKWvFmzca4w==

"System"(시스템)에서 "Secret Keys"(암호 키) 태스크를 사용하여 동적 키를 생성할 수 있습니다. 동적 키를 정의하는 경우 알고리즘 태그와 태그 구분 기호(':') 사이에 키 ID 가 삽입됩니다. 암호화된 데이터에 키 ID 가 없으면 암호화에 하드 코딩된 키가 사용된 것입니다. 이 키는 이전 버전과의 호환성을 위해 사용되거나 지정된 알고리즘에 대한 동적 키가 정의되지 않은 경우에 사용할 수 있습니다.

암호화되는 정보

다음 CA Identity Manager 정보가 암호화됩니다.

- Jboss 용 데이터 원본 구성의 암호
- 잊어버린 암호 복구 정보

- 프로비저닝 서버 콜백 암호
- 워크플로 세션 정보
- 정책 서버 연결 정보

FIPS 모드 로깅

다음 CA Identity Manager 구성 요소는 로그 파일에서 FIPS 모드가 활성화되었는지 여부를 나타냅니다.

- Identity Manager 서버
- 프로비저닝 서버
- C++ 커넥터 서버
- Java 커넥터 서버
- 프로비저닝 관리자
- 암호 동기화 에이전트

모든 경우에 FIPS 모드가 활성화되었음을 나타내는 로그 항목은 다음 문자열로 끝납니다.

FIPS 140-2 MODE: ON

부록 B: SHA-2 로 서명된 SSL 인증서로 CA Identity Manager 인증서 대체

SHA-2 SSL 인증서 해싱은 NIST(National Institute of Standards and Technology)와 NSA(National Security Agency)에서 개발한 암호화 알고리즘입니다. SHA2 인증서는 이전의 다른 모든 알고리즘보다 안전합니다. CA Identity Manager 에서는 SHA-1 해시 함수로 서명된 인증서 대신 SHA-2 로 서명된 SSL 인증서를 구성할 수 있습니다.

참고: SSL 인증서 구성에 대한 자세한 내용은 *설치/ 안내서*를 참조하십시오.

다음 표에서는 SHA-2 로 서명된 인증서를 배치할 수 있는 CA Identity Manager 서버의 경로 위치를 보여 줍니다.

인증서	설치 위치	설명
프로비져닝 서버 인증서	[프로비져닝 서버 설치 디렉터리]/data/tls/server/eta2_servercert.pem [프로비져닝 서버 설치 디렉터리]/data/tls/server/eta2_serverkey.pem *cs_install*/ccs/data/tls/server/eta2_servercert.pem *cs_install*/ccs/data/tls/server/eta2_serverkey.pem *cs_install*/jcs/conf/eta2_server.p12	프로비져닝 서버에서는 .pem 형식, CA IAM CS 에서는 .p12 형식으로 사용됩니다(서명된 인증서, 개인 키 및 루트 CA 인증서 포함). **참고**: eta2_server.p12 를 별칭 eta2_server 아래의 *cs_install*/jcs/conf/ssl.keystore 로 가져오고 기존 항목을 제거합니다. ssl.keystore 암호는 설치하는 동안 제공한 커넥터 서버의 암호입니다.

인증서	설치 위치	설명
프로비져닝 클라이언트 인증서	[프로비져닝 서버 설치 디렉터리]/data/tls/client/eta2_clientcert.pem [프로비져닝 서버 설치 디렉터리]/data/tls/client/eta2_clientkey.pem [프로비져닝 매니저 설치 디렉터리]/data/tls/client/eta2_clientcert.pem [프로비져닝 매니저 설치 디렉터리]/data/tls/client/eta2_clientkey.pem *cs_install*/ccs/data/tls/client/eta2_clientcert.pem *cs_install*/ccs/data/tls/client/eta2_clientkey.pem *cs_install*/jcs/conf/eta2_client.p12	프로비져닝 서버에서는 .pem 형식, CA IAM CS 에서는 .p12 형식으로 사용됩니다(서명된 인증서, 개인 키 및 루트 CA 인증서 포함).
프로비져닝 디렉터리 트러스트된 인증서	*cadir_install*/config/ssld/impd_trusted.pem	CA Directory 에서 .pem 형식으로 사용됩니다. 다음과 같은 구조의 인증서 콘텐츠를 포함해야 합니다. -----BEGIN CERTIFICATE----- 인증서 콘텐츠 -----END CERTIFICATE-----

인증서	설치 위치	설명
프로비져닝 디렉터리 개인 인증서	*cadir_install*/config/ssld/personalities/impd-co.pem *cadir_install*/config/ssld/personalities/impd-inc.pem *cadir_install*/config/ssld/personalities/impd-main.pem *cadir_install*/config/ssld/personalities/impd-notify.pem *cadir_install*/config/ssld/personalities/impd-router.pem	CA Directory 에서 .pem 형식으로 사용됩니다.
루트 CA 인증서	[프로비져닝 서버 설치 디렉터리]/data/tls/et2_cacert.pem [프로비져닝 매니저 설치 디렉터리]/data/tls/et2_cacert.pem *cs_install*/ccs/data/tls/et2_cacert.pem *conxp_install*/lib/jiam.jar [응용 프로그램 서버 설치 디렉터리]/iam_im.ear/library/jiam.jar	인증서를 [Connector Xpress 설치 디렉터리]/conf/ssl.keystore 에 있는 Connector Xpress 키 저장소로 가져옵니다. 인증서를 jiam.jar 키 저장소로도 가져와야 합니다. 가져오려면 jar 를 추출하고 인증서를 admincacerts.jks 로 가져온 다음 jar 콘텐츠를 다시 패키징합니다. admincacerts.jks 의 키 저장소 암호는 "changeit"입니다. jiam.jar 의 사본이 모두 대체되었는지 확인합니다.

유용한 명령

OpenSSL 프로그램은 OpenSSL 라이브러리의 다양한 암호화 기능을 사용하기 위한 명령줄 도구입니다. 이 도구는 [프로비져닝 서버 설치 디렉터리]/bin 에 있는 IMPS 와 함께 제공됩니다.

다음 표에서는 인증서 관리와 관련된 다양한 명령을 실행하는 OpenSSL 프로그램의 몇 가지 유용한 명령을 보여 줍니다.

명령	설명
openssl x509 –in cert.pem –text –noout	.pem 인증서의 콘텐츠를 출력합니다.
openssl.exe pkcs12 -in my.pkcs12 –info	.p12 파일의 콘텐츠를 출력합니다.
openssl.exe pkcs12 -export -chain –inkey key.pem –in cert.pem -CAfile cacert.pem -out my.p12	.pem cert/keypair 를 .p12 로 변환합니다.
keytool –list –v -keystore my.keystore	java 키 저장소의 콘텐츠를 출력합니다.
keytool –list –v –alias myalias –keystore my.keystore	java 키 저장소에 있는 특정 별칭의 콘텐츠를 출력합니다.
keytool –delete –alias myalias –keystore my.keystore	java 키 저장소에서 별칭을 삭제합니다.
keytool –importkeystore –destkeystore my.keystore –srckeystore src.p12 –srcstoretype PKCS12 –srcalias 1 –destalias myalias	.p12 파일을 java 키 저장소로 가져옵니다.

명령	설명
keytool -import -trustcacerts -alias myrootca -file rootcacert.pem -keystore my.keystore	.pem root ca 인증서를 java 키 저장소로 가져옵니다.