CA Identity Manager™

구현 안내서

12.6.4

ca technologies

CA Technologies 제품 참조

이 문서는 다음 CA Technologies 제품을 참조합니다 :

- CA CloudMinder™ Identity Management
- CA Directory
- CA Identity Manager ™
- CA Identity Governance(이전 명칭 CA GovernanceMinder)
- CA SiteMinder®
- CA User Activity Reporting
- CA AuthMinder ™

CA 에 문의

기술 지원팀에 문의

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

목차

제 1 장: ID 및 액세스 관리

이 섹션은 다음 항목을 포함하고 있습니다.

사용자 관리 및 응용 프로그램 액세스

일반적인 IT(정보 기술) 부서는 사용자 계정을 유지 관리해야 하는 지속적인 요구에 직면하고 있습니다. IT 관리자는 잊어버린 암호 다시 설정, 새 계정 만들기, 사무용품 및 장비 제공 등과 같은 사용자의 긴급한 요구를 해결해야 합니다.

동시에 IT 관리자는 사용자에게 응용 프로그램에 대한 다양한 액세스 수준을 제공해야 합니다. 예를 들어 구매 주문을 생성하는 부서 관리자는 재무 응용 프로그램의 계정이 필요합니다.

점점 늘어나는 IT 수요를 충족하기 위해 CA CA Identity Manager 는 사용자 및 응용 프로그램에 대한 사용자 액세스를 관리할 수 있는 통합된 방법을 제공합니다. 여기에는 다음이 포함됩니다.

- 역할을 통한 권한 할당. 구체적으로 말하면 다음과 같습니다.
  - 관리자가 사용자 계정을 만들고 유지 관리할 수 있게 해주는 역할
  - 기존 사용자에게 추가 계정을 프로비저닝하는 역할(프로비저닝 지원 필요)
- 사용자 및 응용 프로그램 액세스 관리 위임
- 사용자가 자신의 계정을 관리할 수 있도록 하는 자체 서비스 옵션
- 비즈니스 응용 프로그램과 CA CA Identity Manager 통합
- CA CA Identity Manager 를 사용자 지정 및 확장하는 옵션

역할 기반 권한

역할을 할당하여 사용자에게 권한을 할당합니다. *역할*에는 CA Identity Manager 의 응용 프로그램 기능에 해당하는 태스크(예: "사용자 만들기" 태스크), 응용 프로그램 기능(예: "구매 주문 만들기" 기능) 또는 사용자 계정(예: SAP 계정)을 제공하는 계정 템플릿이 포함됩니다. 역할이 할당된 경우 사용자가 해당 권한을 받습니다.

CA Identity Manager 는 다음과 같은 유형의 역할을 제공합니다.

- *관리자 역할*이라고 하는 사용자 관리 역할.

  관리자 역할에는 사용자 콘솔에 나타나는 태스크가 포함될 수도 있습니다.
- *프로비저닝 역할*이라고 하는 계정 할당 역할
- *액세스 역할*이라고 하는 응용 프로그램 기능 역할

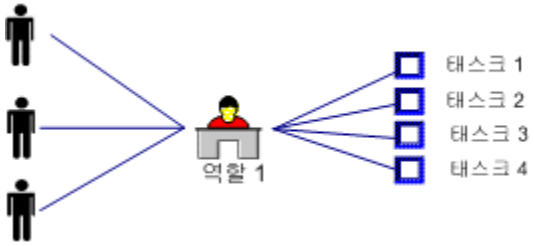
역할에서 태스크 또는 계정 템플릿을 제거하면 사용자가 더 이상 해당 태스크를 수행하거나 끝점 계정을 사용하거나 응용 프로그램 기능을 사용할 수 없습니다.

관리자 역할

관리자 역할은 사용자가 CA Identity Manager 에서 수행할 수 있는 작업을 제어합니다. 시스템 관리자가 사용자에게 역할을 할당하면 해당 역할은 사용자가 수행할 수 있는 태스크 집합을 정의합니다. 사용자는 사용자 계정에서 암호 변경, 작업 제목 업데이트 등의 관리 *태스크*를 수행할 수 있습니다.

사용자마다 해당 태스크에 대한 액세스 수준이 다릅니다. 예를 들어 "직원" 역할은 사용자에게 이름과 주소를 수정할 수 있는 기능을 제공하는 태스크를 포함할 수 있는 반면에 "인사 담당 매니저" 역할은 사용자의 직위와 급여를 수정하는 태스크를 포함합니다.

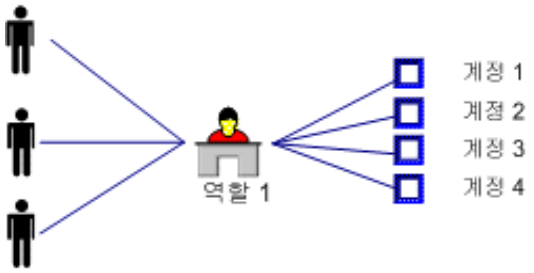
다음 그림에서는 하나의 관리자 역할로 결합되어 세 명의 사용자에게 할당되는 네 개의 태스크를 보여 줍니다.



프로비저닝 역할

전자 메일 시스템과 같은 추가 응용 프로그램의 계정에 사용자가 액세스할 수 있도록 하려면 프로비저닝 역할을 할당합니다. 프로비저닝 역할에는 계정의 한 유형으로 존재하는 특성을 정의하는 계정 템플릿이 수록되어 있습니다. 예를 들어 Exchange 계정의 계정 템플릿은 사서함 크기와 같은 특성을 정의합니다. 계정 템플릿은 계정에 CA Identity Manager 사용자 특성이 매핑되는 방법도 정의합니다.

다음 그림에서는 하나의 프로비저닝 역할로 결합되어 세 명의 사용자에게 할당되는 네 개의 계정을 보여 줍니다. 해당 사용자에게 프로비저닝 역할을 할당하면 각 사용자가 네 개의 계정을 받습니다.



액세스 역할

액세스 역할은 CA Identity Manager 또는 다른 응용 프로그램에서 권한을 제공하는 추가적인 방법을 제공합니다. 예를 들어 액세스 역할을 사용하여 다음을 수행할 수 있습니다.

- 사용자 특성에 대한 간접 액세스 제공
- 복합 식 만들기
- 다른 응용 프로그램에서 권한을 결정하는 데 사용되는 사용자 프로필의 특성 설정

액세스 역할은 일련의 비즈니스 변경 내용을 사용자나 사용자 그룹에 적용한다는 점에서 ID 정책과 유사합니다. 그러나 액세스 역할을 사용하여 비즈니스 변경 내용을 적용하면 액세스 역할의 구성원을 확인하여 변경 내용이 적용되는 사용자를 알 수 있습니다.

대부분의 경우 액세스 역할은 태스크와 관련되지 않습니다.

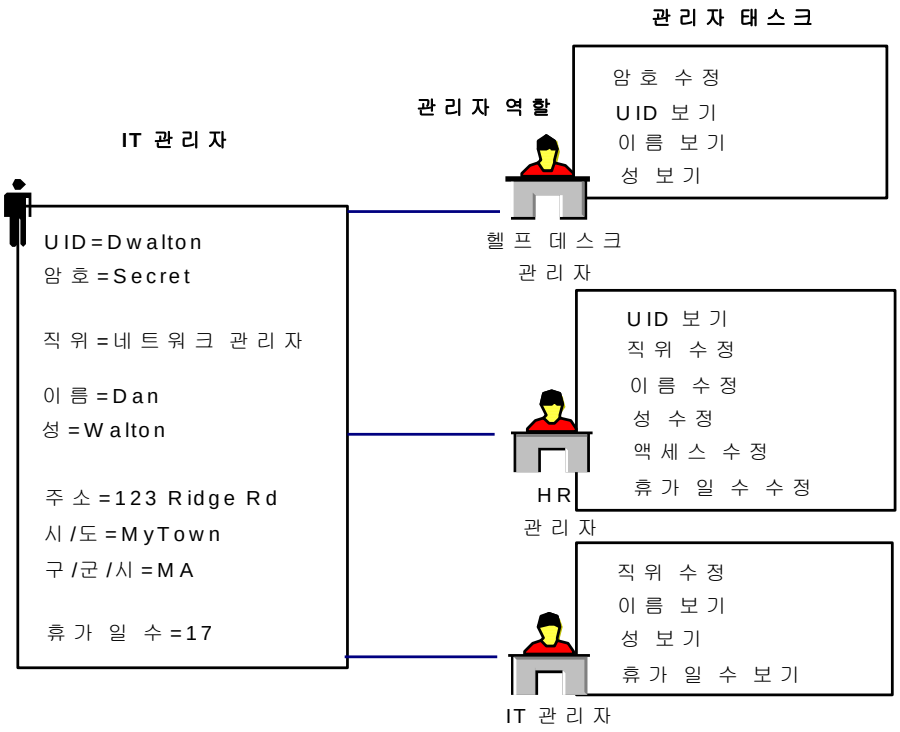
참고: CA Identity Manager 가 CA SiteMinder 와 통합된 경우 액세스 역할이 CA SiteMinder 로 보호된 응용 프로그램에 대한 액세스를 제공할 수도 있습니다. 이 경우 액세스 역할에는 액세스 태스크가 포함됩니다. 자세한 내용은 *Configuration Guide*(구성 안내서)의 SiteMinder 통합 장을 참조하십시오.

사용자 계정 관리를 위한 관리자 역할

CA CA Identity Manager 에서는 관리자 역할을 통해 사용자 저장소 개체(사용자, 그룹 및 조직)를 관리합니다. 또한 사용자 저장소 개체를 관리하는 데 사용하는 역할 및 태스크를 관리하는 데에도 관리자 역할을 사용할 수 있습니다. 예를 들어 사용자의 프로필 특성을 수정하고, 사용자에게 자신의 계정을 관리하기 위한 옵션을 제공하고, 워크플로를 사용하는 태스크를 승인하는 등의 작업에 관리자 역할을 사용합니다.

특성 수준에서 프로필 관리

서로 다른 프로필 특성을 읽거나 써야 하는 여러 관리자를 위한 관리자 역할을 만들 수 있습니다. 예를 들어 회사에서 사용자 프로필의 오퍼레이션을 수행하는 여러 직원이 각각 서로 다른 특성에 액세스할 수 있습니다. 다음 그림에서는 세 가지 역할 및 관련 태스크를 보여 줍니다. 각 역할의 프로필 특성에 대한 액세스는 서로 다릅니다.



이 예에서는 세 역할이 동일한 사용자 Dan Walton 에 대해 서로 다른 특성을 관리할 수 있습니다.

- 헬프 데스크 관리자는 사용자 이름과 주소를 보고 사용자 암호를 다시 설정합니다.
- HR 관리자는 사용자 ID, 사용자 이름, 주소, 직함 및 휴가 일 수를 수정합니다.
- IT 관리자는 사용자 직함을 수정하고 사용자 이름과 휴가 일 수를 봅니다.

어떤 역할로 CA CA Identity Manager 에 로그인하든 자신의 CA CA Identity Manager 계정에 할당된 관리자 역할에 따라 범주라는 일련의 탭이 표시됩니다. 탭을 클릭하면 다음 그림과 같이 해당 범주에서 수행할 수 있는 태스크가 표시됩니다.

범주와 사용자에게 표시되는 해당 범주의 태스크는 사용자의 관리자 역할에 따라 결정됩니다.

관리자 태스크에 대한 워크플로 승인

비즈니스 프로세스를 자동화할 수 있도록 워크플로 프로세스를 생성하는 관리자 태스크를 설계할 수 있습니다. *워크플로 프로세스*는 회사에서 자주 반복되고 잘 정의된 절차를 자동화합니다. CA CA Identity Manager 에는 WorkPoint 워크플로 엔진이 포함되어 있습니다.

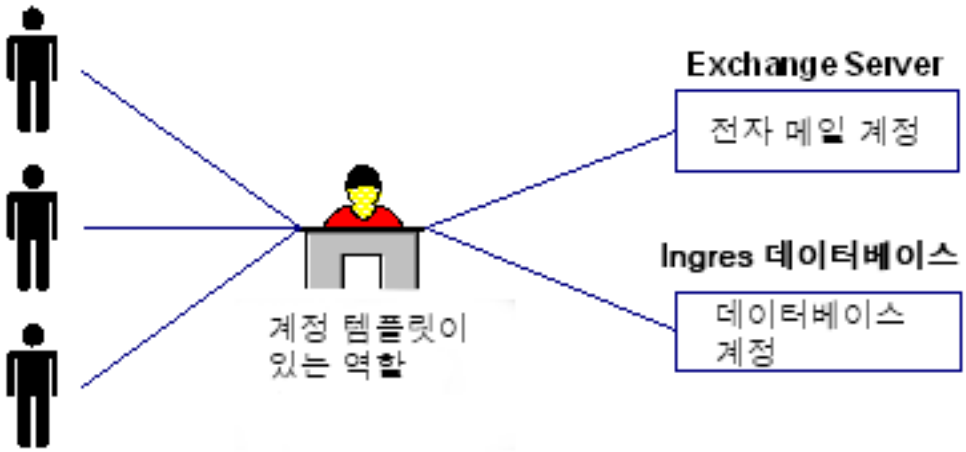
워크플로 프로세스는 관리자 태스크의 일부인 CA CA Identity Manager 이벤트에 의해 트리거됩니다. 예를 들어 "사용자 만들기" 태스크에는 CreateUserEvent 및 AddToGroupEvent 라는 이벤트가 포함되어 있습니다. 이벤트가 발생하면 워크플로 엔진은 다음을 수행할 수 있습니다.

- 승인 요구 - 승인자가 사용자 프로필 수정과 같은 이벤트를 승인해야만 CA CA Identity Manager 가 사용자 저장소를 업데이트할 수 있습니다. 승인자는 특정 태스크에 대한 승인자 역할을 가진 관리자입니다.
- 알림 보내기 - 워크플로 엔진은 사용자가 이벤트를 시작한 경우나 이벤트가 승인된 경우와 같은 여러 프로세스 단계에서 이벤트의 상태를 사용자에게 알릴 수 있습니다.
- 작업 목록 생성 - 작업 목록은 특정 사용자가 수행해야 하는 태스크를 지정합니다. 워크플로 엔진은 관리자의 작업 목록을 자동으로 업데이트합니다.

일반 이벤트의 경우 CA CA Identity Manager 와 함께 제공되는 워크플로 프로세스를 사용할 수 있습니다. 또는 사용자 지정 워크플로 프로세스를 만들 수 있습니다.

추가 계정의 프로비저닝 역할

CA CA Identity Manager 에서는 프로비저닝 역할을 사용하여 사용자에게 추가 계정을 제공합니다. 프로비저닝 역할에는 전자 메일 서버와 같은 관리 끝점에 있는 계정을 정의하는 계정 템플릿이 포함되어 있습니다. CA CA Identity Manager 에 사용자가 있는 경우 이러한 사용자 중 일부에 프로비저닝 역할을 할당할 수 있습니다. 사용자는 역할의 템플릿에 정의된 계정을 받습니다.



계정 템플릿은 계정의 특성을 정의합니다. 예를 들어 Exchange 계정의 계정 템플릿은 사서함 크기를 정의할 수 있습니다. 이 계정 템플릿은 또한 계정에 사용자 특성이 매핑되는 방법을 정의합니다.

프로비저닝 역할을 사용할 수 있으려면 Identity Manager 서버와 함께 프로비저닝 서버를 설치해야 합니다. 그런 다음 사용자 콘솔에서 계정 템플릿을 만듭니다.

암호 관리

Identity Manager 에는 사용자 암호를 관리하기 위한 여러 기능이 포함되어 있습니다.

- 암호 정책 - 이 정책은 암호 만료, 컴퍼지션 및 사용을 제어하는 규칙과 제한을 적용하여 사용자 암호를 관리합니다.

  참고: 고급 암호 정책의 경우 SiteMinder 와의 통합을 구성합니다. 자세한 내용은 *설치 안내서*를 참조하십시오.

- 암호 매니저 - 암호 매니저 역할을 가진 관리자는 사용자가 헬프 데스크에 문의하면 암호를 다시 설정할 수 있습니다.

- 자체 서비스 암호 관리 - Identity Manager 에는 사용자가 자신의 암호를 관리할 수 있게 해 주는 여러 개의 자체 서비스 태스크가 포함되어 있습니다. 이러한 작업의 예는 다음과 같습니다.
  - 자체 등록 - 사용자가 회사 웹 사이트에 등록할 때 암호를 지정합니다.
  - 내 암호 변경 - IT 또는 헬프 데스크 직원의 도움 없이 사용자가 자신의 암호를 수정할 수 있습니다.
  - 잊어버린 암호 - Identity Manager 가 ID 를 확인한 후 사용자가 잊어버린 암호를 다시 설정하거나 검색할 수 있습니다.
  - 잊어버린 사용자 ID - Identity Manager 가 ID 를 확인하고 나면 사용자가 잊어버린 사용자 ID 를 검색할 수 있습니다.
- 암호 동기화(프로비저닝에만 사용) - Identity Manager 와 끝점이라는 대상 시스템의 계정에서 암호 변경 내용이 동기화됩니다. 새 암호는 Identity Manager 암호 정책과 비교하여 확인됩니다.

사용자의 자체 서비스 옵션

IT 작업 부하를 더욱 줄일 수 있도록 CA CA Identity Manager 에는 새 사용자를 등록하고 잊어버린 암호를 제공하는 기능이 있습니다. 이러한 기능은 관리자 개입 없이 사용할 수 있습니다. 사용자는 로그인 계정이 필요하지 않은 *공용 콘솔*을 통해 CA CA Identity Manager 에 액세스합니다. 이 콘솔을 통해 사용자는 사이트에 자체 등록하거나 잊어버린 암호에 대한 미리 알림을 요청할 수 있습니다.

IT 관리자의 시간을 절약할 수 있도록 CA CA Identity Manager 사용자는 계정을 직접 관리할 수 있습니다. 사용자는 자체 관리 역할이 있으므로 다음을 수행할 수 있습니다.

- 개인 정보 유지 관리
- 자신의 암호 변경
- 자체 구독 그룹에 참가

Identity Manager 사용자 지정 및 확장

다음 CA CA Identity Manager 기능을 사용자 지정합니다.

- Identity Manager 디렉터리 - CA CA Identity Manager 에 사용자 저장소 구조를 설명합니다.
- 사용자 인터페이스의 모양과 기능
- 사용자 항목 화면 - 각 태스크 화면의 필드와 레이아웃을 결정합니다.
- 정규식, JavaScript 또는 Java 구현을 통한 사용자 데이터 항목에 대한 유효성 검사
- 워크플로 - 자동화된 워크플로 프로세스를 정의합니다. WorkPoint Process Designer 에서 승인자와 동작을 연결하여 프로세스를 만들거나 수정합니다.
- 전자 메일 메시지 - 사용자에게 태스크의 상태를 알립니다.
- 태스크 제출 - 타사 응용 프로그램이 Identity Manager TEWS(태스크 실행 웹 서비스)로 태스크를 보낼 수 있습니다. TEWS 는 원격 태스크 요청을 처리합니다. 원격 태스크 요청은 WSDL 표준을 준수합니다.

다음 API 를 사용하여 CA CA Identity Manager 의 기능을 확장할 수 있습니다.

- 논리적 특성 API - 특성이 사용자 디렉터리에 실제로 저장된 방식과 다르게 특성을 표시할 수 있습니다.
- 비즈니스 로직 태스크 처리기 API - 데이터 유효성 검사 또는 변환 오퍼레이션 중에 사용자 지정 비즈니스 로직을 실행할 수 있습니다.
- 워크플로 API - 워크플로 프로세스의 사용자 지정 스크립트에 정보를 제공합니다. 스크립트에서 정보를 평가하고 워크플로 프로세스의 경로를 적절히 결정합니다.
- 참여자 해결 프로그램 API - 워크플로 활동을 승인할 권한이 있는 참여자 목록을 지정할 수 있습니다.
- 이벤트 수신기 API - 특정 Identity Manager 이벤트 또는 이벤트 그룹을 수신하는 사용자 지정 이벤트 수신기를 만들 수 있습니다. 이벤트가 발생하면 이벤트 수신기는 사용자 지정 비즈니스 로직을 실행할 수 있습니다.

- 알림 규칙 API - 전자 메일 알림을 수신해야 하는 사용자를 결정할 수 있습니다.
- 전자 메일 템플릿 API - 전자 메일 알림에 이벤트 관련 정보를 포함합니다.

참고: CA CA Identity Manager API 에 대한 자세한 내용은 *Programming Guide for Java*(Java 프로그래밍 안내서)를 참조하십시오.

CA Identity Manager 에 프로비저닝이 포함된 경우 다음과 같이 프로비저닝 기능을 확장할 수도 있습니다.

- 사용자 지정 커넥터 - 프로비저닝 서버와 끝점 시스템 간의 통신을 활성화합니다. 커넥터를 구성하는 코드에는 GUI 플러그 인, 서버 플러그 인 및 에이전트 플러그 인이 포함될 수 있습니다.

  동적 커넥터는 Connector Xpress 에서 생성할 수 있고 사용자 지정 정적 커넥터는 Java 또는 C++로 개발할 수 있습니다.
- 프로그램 종료 - 프로비저닝 서버 프로세스 흐름에서 사용자 지정 코드를 참조할 수 있습니다.

참고: 프로비저닝 기능 확장에 대한 자세한 내용은 *Programming Guide for Provisioning*(프로비저닝 프로그래밍 안내서)을 참조하십시오.

CA Identity Governance 통합

CA Identity Governance 은 역할 모델을 신속 정확하게 개발, 유지 관리, 분석할 수 있게 해 주는 ID 수명 주기 관리 제품입니다. 또한 이 제품을 사용하면 중앙화된 ID 규정 준수 정책을 제어하고 규정 준수 및 보안 요구 사항의 충족과 관련된 프로세스를 자동화합니다. CA Identity Governance 을 사용하여 다음을 수행할 수 있습니다.

- 비즈니스 규정 준수 정책에 따라 CA Identity Manager 사용자 권한이 부여되었는지 확인합니다.
- CA Identity Manager 사용자, 역할 및 계정을 만들거나 수정할 때 제안된 역할 및 규정 준수 검사 기능을 사용합니다.
- 조직에 있는 역할을 이해하고, 조직에 맞는 역할 모델을 설정하고, CA Identity Manager 내에서 원하는 역할 모델을 다시 만듭니다.
- 비즈니스가 성장함에 따라 역할 모델을 분석 및 유지 관리합니다.

CA Identity Manager 는 두 가지 방법으로 CA Identity Governance 과 통합됩니다.

- CA Identity Manager 용 CA Identity Governance 커넥터

  CA Identity Manager 와 CA Identity Governance 사이에서 권한 데이터를 자동으로 동기화하는 특별한 유형의 커넥터입니다. 이 커넥터를 사용하여 CA Identity Manager 에서 CA Identity Governance 로 데이터를 가져오거나 CA Identity Governance 에서 CA Identity Manager 로 데이터를 내보낼 수 있습니다.

- 스마트 프로비저닝

  CA Identity Manager 가 CA Identity Governance 과 통합될 때 일상적인 ID 관리 오퍼레이션을 지원하기 위해 역할 모델에 있는 역할 및 규정 준수 정보를 사용할 수 있도록 해 주는 추가 기능을 구성할 수 있습니다. CA Identity Manager 에서 변경하면 CA Identity Governance 에서 역할 모델이 동적으로 업데이트됩니다.

참고: CA Identity Manager 와의 CA Identity Governance 통합에 대한 자세한 내용은 CA Identity Governance 북셸프에 있는 *CA Identity Manager Integration Guide*(CA Identity Manager 통합 안내서)를 참조하십시오.

CA 사용자 활동 보고 통합

CA Identity Manager r12.6 부터 CA Enterprise Log Manager 의 명칭이 CA User Activity Reporting(CA UAR)으로 변경되었습니다.

CA UAR 는 CEG(CA Common Event Grammar)를 사용하여 다양한 시스템에서 표준 형식으로 발생한 이벤트를 매핑하고 모든 이벤트(아직 매핑되지 않은 이벤트 포함)를 검토 및 분석을 위해 저장합니다. 또한 CA UAR 는 다양한 유형의 정보 및 이벤트를 검색할 수 있는 구성 가능한 데이터베이스 쿼리 및/또는 보고서를 사용하여 사용자가 수집된 데이터를 매핑 및 보고할 수 있게 해주는 대용량 솔루션을 제공합니다.

CA UAR 는 관리되지 않는 시스템 및 CA Identity Manager 의 미리보기 및 제어 범위 밖의 시스템에 대한 더 높은 수준의 통찰력을 제공하며 ID 를 보다 상세히 조사할 수 있게 해줍니다.

CA Identity Manager 와 통합하면 CA Identity Manager 사용자 콘솔을 사용하여 CA UAR ID 중심 보고서 및/ 또는 사용자 콘솔에 대한 동적 쿼리를 볼 수 있습니다. 사용자 콘솔에서 기존 CA Identity Manager/CA UAR 보고서 및/또는 쿼리를 보고 수정하는 방법을 구성하고 특정 ID 를 자세히 조사할 수 있습니다.

CA UAR 보고서

다음 CA UAR 보고서는 CA UAR 역할 정의와 함께 기본적으로 제공됩니다.

태스크	보고서 호출
사용자별 시스템 모든 이벤트	CA Identity Manager - 사용자 ID 별로 필터링된 시스템 모든 이벤트
호스트별 계정 관리	호스트별 계정 관리
계정별 계정 만들기	계정별 계정 만들기
계정별 계정 삭제	계정별 계정 삭제
계정별 계정 잠금	계정별 계정 잠금
호스트별 인증서 프로세스 활동	CA Identity Manager - 호스트별 프로세스 활동
암호 정책 수정 활동	CA Identity Manager - 정책 수정 활동

제 2 장: 비즈니스 요구 사항 해결

이 섹션은 다음 항목을 포함하고 있습니다.

비즈니스 변경 내용 저장

ID 정책을 사용하여 특정 ID 관리 태스크 처리를 자동화할 수 있습니다. ID 정책은 사용자가 특정 조건이나 규칙을 충족할 때 발생하는 일련의 비즈니스 변경 내용입니다. ID 정책 세트를 사용하여 다음 작업을 수행할 수 있습니다.

- 역할 및 그룹 구성원 자격 할당, 리소스 할당 또는 사용자 프로필 특성 수정과 같은 ID 관리 태스크를 자동화합니다.
- 직무 분리를 적용합니다 (페이지 29). 예를 들어, 수표 서명자 역할의 구성원이 수표 승인자 역할을 갖지 못하도록 금지하고 회사의 모든 직원이 $10,000 이상의 수표를 쓰지 못하도록 제한하는 ID 정책 세트를 만들 수 있습니다.
- 규정 준수를 적용합니다. 예를 들어, 특정 직함을 가지고 있으며 $100,000 이상의 수입이 있는 사용자를 감사할 수 있습니다.

  규정 준수를 적용하는 ID 정책을 *규정 준수 정책*이라고 합니다.

ID 정책과 연결된 비즈니스 변경에는 다음이 포함됩니다.

- 프로비저닝 역할을 비롯한 역할 할당 또는 해지(CA Identity Manager 에 프로비저닝이 포함된 경우)
- 그룹 구성원 자격 할당 또는 해지
- 사용자 프로필의 특성 업데이트

예를 들어, 회사에서 모든 부사장이 컨트리 클럽 구성원 그룹에 속하고 급여 승인자 역할을 갖도록 규정하는 ID 정책을 만들 수 있습니다. 사용자 직함이 부사장으로 변경되고 해당 사용자가 ID 정책과 동기화되면 CA Identity Manager 에서 이 사용자를 적절한 그룹과 역할에 추가합니다. 부사장이 CEO 로 승진되면 더 이상 부사장 ID 정책의 조건을 충족하지 않으므로 해당 정책에 의해 적용되는 변경이 해지되고 CEO 정책을 기반으로 하는 새 변경이 적용됩니다.

ID 정책을 기반으로 수행되는 변경 동작에는 워크플로 제어를 적용하고 감사할 수 있는 이벤트가 포함되어 있습니다. 앞의 예에서 급여 승인자 역할은 구성원에게 상당한 권한을 부여합니다. 급여 승인자 역할을 보호하기 위해 회사에서 역할이 할당되기 전에 승인이 필요한 워크플로 프로세스를 만들 수 있으며, 역할 할당을 감사하도록 CA Identity Manager 를 구성할 수 있습니다.

ID 정책 관리를 단순화하기 위해 ID 정책은 ID 정책 세트로 그룹화되어 있습니다. 예를 들어, 부사장 및 CEO 정책은 임원 권한 ID 정책 세트에 포함될 수 있습니다.

비즈니스 정책 준수

규정 준수는 회사 및 해당 직원이 비즈니스 정책을 준수하도록 하는 광범위한 절차가 포함된 회사 규정입니다. 이러한 규정 준수 절차에는 대체로 응용 프로그램 및 시스템에 대한 자격 할당을 문서화, 자동화 및 감사하는 작업이 포함됩니다.

CA Identity Manager 에는 규정 준수 관리를 지원하는 다음과 같은 기능이 있습니다.

- **스마트 프로비저닝**

  스마트 프로비저닝은 CA Identity Manager 가 CA Identity Governance 과 통합될 때 프로비저닝 역할을 쉽게 할당할 수 있게 도와 주는 기능의 모음입니다. 이 기능은 다음을 포함합니다.

  - 제안된 프로비저닝 역할

    CA Identity Manager 는 관리자가 사용자에게 할당하기에 적절한 프로비저닝 역할 목록을 제공할 수 있습니다. 프로비저닝 역할 목록은 관리자가 입력한 조건을 기준으로 CA Identity Governance 에 의해 결정됩니다.

    제안된 프로비저닝 역할은 회사의 역할 모델을 유지 관리하는 동시에 사용자에게 올바른 권한이 할당될 수 있도록 도움을 줍니다.

  - 규정 준수 및 패턴 메시지

    CA Identity Manager 관리자는 변경 내용을 커밋하기 전에 CA Identity Governance 의 역할 모델에 대해 제안된 변경 내용의 유효성을 검사할 수 있습니다. 변경 사항을 확인하기 전에 유효성을 검사하면 회사가 오퍼레이션에 대해 정의한 역할 모델을 유지관리하는 데 도움을 줍니다.

    사용자는 프로비저닝 역할에 제안된 변경 사항(할당 또는 제거) 또는 사용자 특성의 변경 사항에 대해 유효성을 검사할 수 있습니다.

CA Identity Manager 는 다음 두 가지 유형의 정책 유효성 검사를 수행합니다.

- 컴플라이언스

  CA Identity Governance 의 명시적이고 미리 정의된 비즈니스 정책 규칙을 위반하는지 여부를 확인하기 위해 CA Identity Governance 역할 모델에 대해 제안된 변경 사항의 유효성을 검사합니다.

- 패턴

  제안된 변경 내용을 CA Identity Governance 역할 모델과 비교하여 변경 내용의 대상이 "패턴 불일치"가 되는지 확인합니다. 또한 CA Identity Manager 는 변경 내용이 역할 모델에서 설정한 패턴을 크게 변경하지 않음을 확인합니다.

  사용자가 특정 태스크를 수행할 때 자동으로 이러한 유효성 검사를 수행하거나 사용자가 수동으로 유효성 검사를 시작할 수 있도록 CA Identity Manager 를 구성할 수 있습니다.

CA Identity Governance 에 CA Identity Manager 데이터를 기준으로 설정된 역할 모델이 있으면 CA Identity Manager 환경에 스마트 프로비저닝을 구현할 수 있습니다.

참고: 자세한 내용은 *관리 안내서*를 참조하십시오.

- **ID 정책**

  사용자에게 다른 권한이 있는 경우 사용자가 특정 권한을 갖지 못하도록 하는 ID 정책 (페이지 23) 유형인 규정 준수 정책을 만들 수 있습니다. 예를 들어, 확인을 승인할 수 있는 사용자가 확인을 통보하지 못하도록 금지할 수 있습니다.

  규정 준수 정책은 환경에서 직무 분리를 적용합니다.

- **규정 준수 보고서**

  CA Identity Manager 에는 환경의 사용자에 대한 규정 준수 상태를 표시하는 샘플 보고서가 포함되어 있습니다. 이 보고서를 사용하여 비즈니스 정책을 준수하지 않는 사용자를 확인할 수 있습니다.

규정 준수 보고서

CA Identity Manager 에는 회사 비즈니스 정책 준수를 모니터링하는 데 사용할 수 있는 다음 표의 샘플 보고서가 포함되어 있습니다.

보고서	설명
역할 구성원	보고서 데이터베이스의 역할을 표시하고 이러한 역할의 구성원을 나열합니다.
역할	보고서 데이터베이스의 각 역할에 대해 다음 정보를 표시합니다. ■ 역할과 관련된 태스크 ■ 구성원 정책 및 역할 구성원 ■ 관리자 정책 및 역할 관리자 ■ 소유자 정책 및 역할 소유자
태스크 역할	보고 데이터베이스의 태스크와 이 태스크가 연결된 역할을 표시합니다.
사용자 역할	보고 데이터베이스의 사용자를 표시하고 각 사용자의 역할을 나열합니다.
비표준 계정 추세	고아 계정, 시스템 계정, 예외 계정에 대한 비표준 계정 추세를 표시합니다.
비표준 계정	모든 고아, 시스템 및 예외 계정을 표시합니다.
고아 계정	프로비저닝 서버에서 전역 사용자가 없는 모든 끝점 계정을 표시합니다.
정책	모든 ID 정책을 표시합니다.

보고서	설명
사용자 프로필	사용자에 대한 다음 정보를 표시합니다. ■ 이름 ■ 사용자 ID ■ 사용자가 구성원 또는 관리자인 그룹 ■ 사용자가 구성원, 관리자, 소유자인 역할
Endpoint Accounts(끝점 계정)	끝점별 계정을 표시합니다(보려는 끝점 선택 가능).
역할 관리자	역할 및 그 관리자를 표시합니다.
역할 소유자	역할 및 그 소유자를 표시합니다.
스냅숏	내보낸 모든 스냅숏을 표시합니다.
사용자 계정	사용자 및 그 계정의 목록을 표시합니다.
사용자 권한	사용자의 역할, 그룹 및 계정을 표시합니다.
사용자 정책 동기화 상태	정책(할당, 할당 취소 또는 재할당되어야 하는 정책)별 사용자의 상태를 표시합니다.

참고: 보고서에 대한 자세한 내용은 *관리 안내서*를 참조하십시오.

직무 분리 요구 사항 적용

SOD(직무 분리) 요구 사항은 사용자가 이해의 충돌이나 사기 행위를 유발할 수 있는 권한을 받지 못하도록 합니다. CA Identity Manager 는 SOD 를 지원하기 위해 다음 기능을 제공합니다.

- **보호 ID 정책**

  관리자는 태스크가 제출되기 전에 실행되는 이 정책을 사용하여 권한을 할당하거나 프로필 특성을 변경하기 전에 정책 위반을 확인할 수 있습니다. 위반이 존재하는 경우 관리자가 태스크를 제출하기 전에 위반을 삭제할 수 있습니다.

  예를 들어, 회사에서 "사용자 관리자" 역할을 맡은 사용자가 "사용자 승인자" 역할도 맡지 못하도록 금지하는 보호 ID 정책을 만들 수 있습니다. 이 경우 관리자가 "사용자 수정" 태스크를 사용하여 "사용자 매니저"에게 "사용자 승인자" 역할을 부여하면 CA Identity Manager 에서 위반 메시지를 표시합니다. 관리자는 태스크를 제출하기 전에 위반을 삭제하기 위해 역할 할당을 변경할 수 있습니다.

- **스마트 프로비저닝을 통한 정책 유효성 검사**

  CA Identity Manager 관리자는 변경 내용을 커밋하기 전에 CA Identity Governance 의 BPR(비즈니스 정책 규칙)를 기준으로 프로비저닝 역할 및 사용자 특성에 대해 제안된 변경 내용의 유효성을 검사할 수 있습니다. BPR 는 권한에 대한 다양한 제약 조건을 나타냅니다. 예를 들어 BPR 가 구성원이 하도급업체에 물품을 주문할 수 있도록 허용하는 구매 부서 역할을 가진 사용자는 하도급업체 지불 역할을 갖지 못하도록 금지할 수 있습니다. 시스템 관리자, 비즈니스 매니저, 감사자 또는 역할 엔지니어가 CA Identity Governance 에서 BPR 를 만듭니다.

  참고: BPR 에 대한 자세한 내용은 *CA Identity Governance Sage DNA User Guide*(CA Identity Governance Sage DNA 사용자 안내서)를 참조하십시오.

참고: 보호 ID 정책 및 스마트 프로비저닝에 대한 자세한 내용은 *CA Identity Manager 관리 안내서*를 참조하십시오.

사용자 저장소에서 데이터 변환

경우에 따라 데이터를 사용자 저장소에 저장하기 전에 CA Identity Manager 에서 데이터를 변환하도록 구성할 수 있습니다. 예를 들어 정보를 입력한 형식과 다른 형식으로 저장하거나 특정 유형의 정보를 표시할 때 변경 내용이 적용되도록 할 수 있습니다.

CA Identity Manager 에는 데이터를 변환하기 위한 다음과 같은 기능이 포함되어 있습니다.

- ID 정책
- 논리적 특성 처리기

참고: 또한 ID 정책 및 논리적 특성 처리기를 사용하여 사용자 지정 비즈니스 로직을 구현할 수도 있습니다.

논리적 특성 처리기

논리적 특성 처리기는 CA Identity Manager 태스크 화면에서 사용되는 사용자 특성 값을 변환하는 사용자 지정 Java 코드입니다. 논리적 특성 처리기를 사용하면 태스크 화면에서 물리적 특성이 표시되는 방식을 제어할 수 있습니다. 또한 논리적 특성 처리기를 사용하여 태스크 화면에서 비용과 같은 표시 값을 사용자 저장소에 저장되는 단가 및 수량과 같은 하나 이상의 물리적 특성으로 변환할 수 있습니다.

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

사용자 지정 비즈니스 로직 적용

CA Identity Manager 를 사용자 지정하여 회사에 필요한 비즈니스 로직을 구현할 수 있습니다. CA Identity Manager 에는 사용자 지정 비즈니스 로직을 구현하기 위한 다음과 같은 옵션이 포함되어 있습니다.

- ID 정책 - ID 정책을 사용하면 사용자가 특정 조건이나 규칙을 충족할 경우 발생하는 일련의 비즈니스 변경 내용을 정의할 수 있습니다. 예를 들어 ID 정책은 역할 할당과 같은 특정 ID 관리 태스크를 자동화하거나 사용자가 20,000 달러가 넘는 수표를 서명 및 승인하지 못하게 하는 등의 비즈니스 규칙을 적용할 수 있습니다.

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

- 논리적 특성 처리기 - 이러한 처리기를 CA Identity Manager 태스크 화면과 연결하여 특성 값의 표시 및 수정을 제어할 수 있습니다.

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

- 비즈니스 로직 태스크 처리기 - CA Identity Manager 태스크에 대한 데이터 유효성 검사 오퍼레이션을 수행하는 동안 다음과 같은 사용자 지정 비즈니스 로직을 수행할 수 있습니다.
  - 사용자 지정 비즈니스 규칙(예: 관리자가 6 개 이상의 그룹을 관리할 수 없음) 적용
  - 고객 관련 태스크 화면 필드의 유효성 검사(예: "직원 ID" 필드 값은 마스터 인사 데이터베이스에 있어야 함)

  비즈니스 로직 태스크 처리기는 Java 또는 JavaScript 로 구현할 수 있습니다.

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

- 워크플로 - CA Identity Manager 이벤트와 연결된 사용자 지정 프로세스 정의를 만들 수 있습니다.

참고: 비즈니스 로직을 비즈니스 로직 태스크 처리기에서 구현할지 또는 워크플로 프로세스에서 구현할지 결정하려면 다음 단원을 참조하십시오.

- 비즈니스 로직 태스크 처리기 고려 사항 (페이지 32)
- 워크플로 프로세스 고려 사항 (페이지 32)

비즈니스 로직 태스크 처리기 고려 사항

비즈니스 로직 태스크 처리기는 이벤트 생성 전에 발생하는 태스크의 동기식 처리 단계 동안 비즈니스 로직 유효성 검사를 수행합니다. 따라서 다음을 수행할 수 있습니다.

- 태스크 수준 유효성 검사 수행. 예를 들어 사용자 프로필 화면에 지정된 그룹 구성원의 사무실 위치에 따라 구성원을 추가하거나 제거할 수 있습니다.
- 유효성 검사에 실패하는 경우 태스크가 제출되지 않도록 방지
- 태스크 제출 전에 태스크 화면의 모든 정보를 비즈니스 정책에 맞게 자동으로 변환

참고: 완료하는 데 오래 걸리는 활동은 비즈니스 로직 태스크 처리기에서 구현하지 않아야 합니다. 오래 실행되는 활동은 태스크 제출을 지연시키며 사용자 상호 작용이 일어나는 동기식 단계에 적합하지 않습니다. 대신 태스크의 비동기식 단계 중 실행되는 워크플로 프로세스를 사용하십시오.

워크플로 프로세스 고려 사항

워크플로 프로세스는 태스크의 비동기식 단계 중 호출되며 개별 이벤트 실행과 연결됩니다. 따라서 다음을 수행할 수 있습니다.

- 개별 이벤트 데이터를 기준으로 승인 활동 실행
- 오래 실행되는 사용자 지정 비즈니스 로직 활동 실행

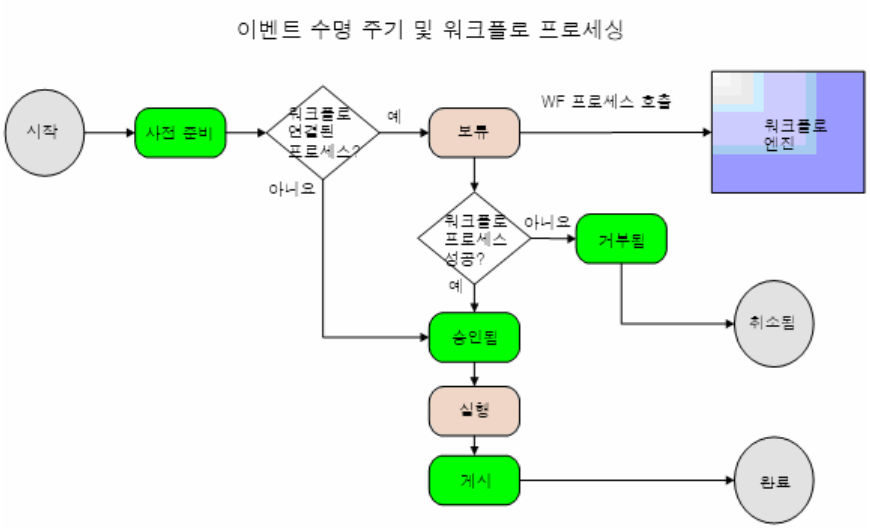
워크플로 API 를 사용하면 워크플로 활동에서 태스크 수준 데이터를 얻을 수 있지만 일반적으로 워크플로 아래의 해당하는 특정 이벤트의 컨텍스트에서 작업합니다.

비즈니스 변경 내용 승인

워크플로는 고용 절차 실행 또는 외부 시스템에서 사용자의 신용 점수 가져오기와 같은 일부 비즈니스 목표를 달성하기 위해 수행해야 하는 하나 이상의 단계로 구성되는 프로세스를 설명합니다. 일반적으로 워크플로 프로세스의 단계 중 하나에는 비즈니스 변경 내용의 승인 또는 거부가 포함됩니다.

CA Identity Manager 에서 워크플로 프로세스는 태스크 처리 중 발생하는 동작인 이벤트와 연결되어 있습니다. 이벤트가 수명 주기에서 "보류 중" 상태가 되면 CA Identity Manager 는 연결된 워크플로 프로세스를 호출하고 프로세스가 완료될 때까지 이벤트 실행을 일시 중지합니다. 그런 다음 CA Identity Manager 는 워크플로 프로세스의 결과에 따라 이벤트를 수행하거나 거부합니다.

이 순서는 다음 다이어그램에 나와 있습니다.



CA Identity Manager 에는 워크플로 프로세스를 만들고 관리하기 위한 InSession WorkPoint 워크플로 엔진이 포함되어 있습니다.

참고: 자세한 내용은 *관리 안내서*를 참조하십시오.

제 3 장: CA Identity Manager 아키텍처

이 섹션은 다음 항목을 포함하고 있습니다.

CA Identity Manager 구성 요소

CA Identity Manager 구현에는 다음 구성 요소의 일부 또는 전부가 포함될 수 있습니다.

- 서버
- 사용자 저장소
- 데이터베이스
- 커넥터

서버

CA Identity Manager 구현에는 필요한 기능에 따라 하나 이상의 서버 유형이 포함됩니다.

CA Identity Manager 서버(필수)

CA Identity Manager 내의 태스크를 실행합니다. J2EE CA Identity Manager 응용 프로그램에는 관리 콘솔과 사용자 콘솔이 포함됩니다.

CA Identity Manager 프로비저닝 서버

끝점 시스템의 계정을 관리합니다.

CA Identity Manager 설치에서 계정 프로비저닝을 지원할 경우 이 서버가 필요합니다.

참고: 프로비저닝 서버를 설치하려면 먼저 CA Directory Server 에서 원격으로나 로컬로(데모 환경에만 해당) 프로비저닝 디렉터리를 설치해야 합니다.

SiteMinder 정책 서버

CA Identity Manager 에 대한 고급 인증을 제공하고 암호 서비스 및 싱글 사인온과 같은 SiteMinder 기능에 대한 액세스를 지원합니다.

이 서버는 선택 사항입니다.

사용자 저장소 및 프로비저닝 디렉터리

CA Identity Manager 는 다음 두 사용자 저장소를 조율합니다.

- CA Identity Manager 가 유지 관리하는 사용자 저장소인 *CA Identity Manager 사용자 저장소*. 일반적으로 회사에서 관리해야 하는 사용자 ID 를 포함하는 기존 저장소입니다.

  사용자 저장소는 LDAP 디렉터리나 관계형 데이터베이스일 수 있습니다.

  관리 콘솔에서 CA Identity Manager 디렉터리 개체를 만들어 사용자 저장소에 연결하고 CA CA Identity Manager 가 유지 관리할 사용자 저장소 개체를 설명합니다.

- 프로비저닝 서버가 유지 관리하는 사용자 저장소인 *프로비저닝 디렉터리*.

  이 저장소는 CA Directory 의 인스턴스이며 프로비저닝 디렉터리의 사용자를 Microsoft Exchange, Active Directory 및 SAP 와 같은 끝점의 계정과 연결하는 전역 사용자를 포함합니다.

  일부 CA Identity Manager 사용자에게만 해당하는 전역 사용자가 있습니다. CA Identity Manager 사용자가 프로비저닝 역할을 받는 경우 프로비저닝 서버는 전역 사용자를 만듭니다.

분리된 사용자 저장소 및 프로비저닝 디렉터리

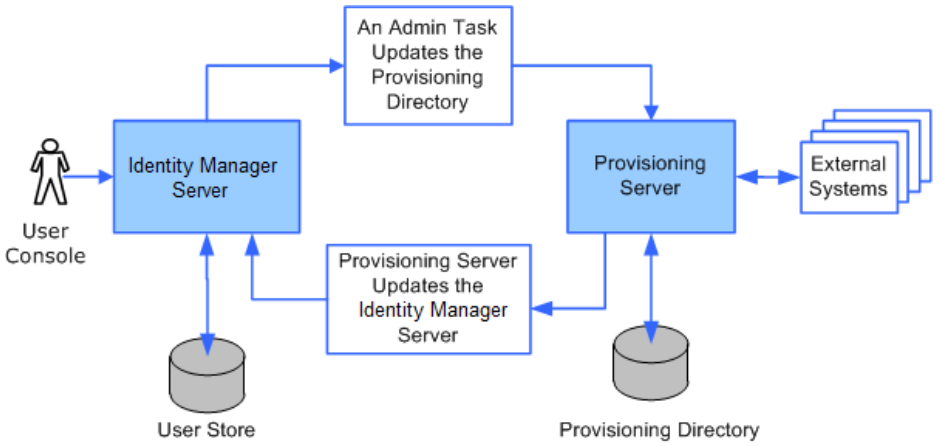
다음 그림은 CA Identity Manager 의 신규 설치에 대해 지원되는 시나리오인 별도 사용자 저장소와 프로비저닝 디렉터리를 보여 줍니다. 이 그림에서,

- CA Identity Manager 관리자는 사용자 저장소의 사용자를 편집하며, 이에 따라 프로비저닝 디렉터리에 영향을 주는 관리자 태스크를 사용합니다.

  이 변경으로 인해 프로비저닝 서버에 대한 커넥터를 포함하는 끝점(예: 전자 메일 서버)도 업데이트됩니다.

  프로비저닝 서버(또는 프로비저닝 서버에 대한 커넥터가 있는 끝점)에서 변경하면 CA Identity Manager 사용자 저장소와 프로비저닝 디렉터리가 업데이트됩니다.

예를 들어 인사 응용 프로그램과 같은 끝점이 사용자의 전자 메일 주소를 업데이트할 수 있습니다.



데이터베이스

CA Identity Manager 는 CA Identity Manager 기능을 지원하는 데 필요한 정보를 저장하는 데이터베이스에 데이터 원본을 사용하여 연결합니다. 이러한 데이터베이스는 데이터베이스의 물리적 인스턴스 하나 또는 별도의 인스턴스에 있을 수 있습니다.

Object Database(개체 데이터베이스)(필수)

CA Identity Manager 구성 정보를 포함합니다.

Task Persistence Database(태스크 지속 데이터베이스) (필수)

시간에 따른 CA Identity Manager 활동 및 이와 연관된 이벤트에 대한 정보를 유지합니다. 이렇게 하면 CA Identity Manager 서버를 다시 시작하더라도 시스템에서 CA Identity Manager 활동을 정확히 추적할 수 있습니다.

Archive Database(아카이브 데이터베이스) (필수)

태스크 지속 데이터베이스의 데이터를 아카이브합니다.

Workflow Database(워크플로 데이터베이스)

워크플로 프로세스 정의, 작업, 스크립트 및 워크플로 엔진에 필요한 기타 데이터를 저장합니다.

Audit Database(감사 데이터베이스)

CA Identity Manager 환경에서 발생하는 오퍼레이션의 내역을 제공합니다.

참고: CA Identity Manager 가 감사 데이터베이스에 저장하는 정보의 양과 유형을 구성할 수 있습니다. 자세한 내용은 *구성 안내서*를 참조하십시오.

Reporting Database(보고 데이터베이스)

CA Identity Manager 에서 스냅숏을 생성한 시점의 개체 상태를 나타내는 스냅숏 데이터를 저장합니다. 이 정보로 보고서를 생성하여 사용자 및 역할과 같은 개체 간의 관계를 볼 수 있습니다.

설치 관리자를 사용하는 경우 CA Identity Manager 는 각 데이터베이스 유형에 대한 테이블이 포함된 CA Identity Manager 데이터베이스라는 단일 데이터베이스 연결을 구성합니다.

참고: 태스크 지속, 워크플로, 감사 또는 보고에 대한 데이터 저장소를 별도의 데이터베이스에 만들고 CA Identity Manager 가 해당 데이터베이스에 연결하도록 구성할 수 있습니다. 자세한 내용은 *설치 안내서*를 참조하십시오.

커넥터 구성 요소

커넥터는 끝점에 대한 소프트웨어 인터페이스입니다. 프로비저닝 서버는 커넥터를 사용하여 끝점과 통신합니다. 커넥터는 프로비저닝 서버 동작을 "Microsoft Exchange 끝점에서 새 전자 메일 계정 만들기"와 같은 끝점의 변경 내용으로 변환합니다.

끝점의 예로는 UNIX 워크스테이션, Windows PC 또는 Microsoft Exchange(전자 메일용)와 같은 응용 프로그램을 들 수 있습니다.

커넥터 서버

커넥터 서버는 커넥터를 관리하는 프로비저닝 서버 구성 요소입니다. 이 서버는 프로비저닝 서버 시스템이나 원격 시스템에 설치할 수 있습니다.

커넥터 서버 한 대가 여러 끝점과 함께 사용됩니다. 예를 들어 여러 UNIX 워크스테이션 끝점이 있는 경우 UNIX 계정을 관리하는 모든 커넥터를 처리하는 커넥터 서버 한 대가 있을 수 있습니다. 또 다른 커넥터 서버는 Windows 계정을 요청하는 모든 커넥터를 처리할 수 있습니다.

배포된 커넥터 서버는 여러 커넥터 서버와 함께 작동합니다. 커넥터 서버 한 대가 사용 중일 경우 부하 분산을 제공하고 커넥터 서버가 중단된 경우 고가용성을 제공합니다.

커넥터 서버에는 두 가지 유형이 있습니다.

- CA IAM CS(CA IAM 커넥터 서버) - Java 로 작성된 커넥터를 관리합니다.
- CCS(C++ 커넥터 서버) - C++로 작성된 커넥터를 관리합니다.

C++ 커넥터 서버

*C++ 커넥터 서버*는 C++ 커넥터를 관리하는 커넥터 서버입니다. 이 서버는 프로비저닝 서버나 원격 시스템에 설치할 수 있습니다. C++ 커넥터 서버는 C++ 커넥터 서버와 끝점 간의 통신을 담당하는 커넥터를 쉽게 개발할 수 있도록 하는 개체 지향 응용 프로그램 프레임워크를 제공합니다.

CA IAM CS

CA IAM CS 는 Java 커넥터의 호스팅, 라우팅 및 관리를 처리하는 서버 구성 요소입니다. CA IAM CS 는 C++ 커넥터 서버에 대한 Java 용 대안입니다. 아키텍처와 기능 면에서 C++ 커넥터 서버와 유사하지만 C++ API 대신 Java API 를 사용하므로 커넥터를 Java 로 구현할 수 있습니다. 또한 CA IAM CS 는 코드 기반이 아니라 데이터 기반이므로 커넥터 자체가 아니라 컨테이너(또는 CA IAM CS)에서 더 많은 기능을 처리할 수 있습니다.

프로비저닝 서버는 사용자 프로비저닝을 처리한 다음 C++ 커넥터 서버나 CA IAM CS 를 사용하여 커넥터에 끝점 계정 및 그룹 관리를 위임합니다.

커넥터 및 에이전트

CA Identity Manager 커넥터는 광범위한 프로비저닝 서버 아키텍처의 일부로 실행되며 환경에서 관리되는 시스템과 통신합니다. 커넥터는 네이티브 끝점 유형 시스템 기술의 게이트웨이 역할을 합니다. 예를 들어 ADS(Active Directory 서비스)를 실행 중인 시스템은 프로비저닝 서버가 통신할 수 있는 커넥터 서버에 ADS 커넥터가 설치된 경우에만 관리할 수 있습니다. 커넥터는 시스템에 있는 개체를 관리합니다. 관리 개체에는 계정, 그룹 및 끝점 유형 관련 개체(선택 사항)가 포함됩니다.

커넥터는 커넥터 서버에 설치되며 일부 구성 요소는 프로비저닝 서버(예: 서버 플러그 인)나 프로비저닝 매니저(예: 사용자 인터페이스 플러그 인)에 설치됩니다.

일부 커넥터는 관리하는 시스템에 에이전트가 있어야만 통신 주기를 완료할 수 있으므로 프로비저닝 설치 관리자를 사용하여 설치할 수 있습니다. 에이전트는 다음과 같은 범주로 구분할 수 있습니다.

원격 에이전트

관리 끝점 시스템에 설치됩니다.

환경 에이전트

CA ACF2, CA Top Secret 및 RACF 와 같은 시스템에 설치됩니다.

다음과 같은 C++ 커넥터 서버 기반 옵션과 같은 특정 구성 요소는 UNIX 와 Windows 에서 작동합니다.

- UNIX(ETC, NIS)
- ACC(액세스 제어)

  참고: UNIX ACC 커넥터는 UNIX ACC 끝점만 관리할 수 있습니다. Windows ACC 끝점을 관리하려면 Windows ACC 커넥터가 필요하지만 이 커넥터는 UNIX ACC 끝점도 관리할 수 있습니다.
- CA-ACF2
- RACF
- CA-Top Secret

다른 C++ 커넥터 서버 기반 커넥터는 Solaris 프로비저닝 서버에서 CSF(Connector Server Framework)를 사용하여 액세스할 수 있습니다. CSF 를 통해 Solaris 의 프로비저닝 서버가 Windows 에서 실행 중인 커넥터와 통신할 수 있습니다.

참고: 이러한 커넥터를 사용하려면 CSF 가 Windows 에서 실행되고 있어야 합니다.

Connector Xpress

Connector Xpress 는 동적 커넥터를 관리하고, 끝점에 동적 커넥터를 매핑하고, 끝점에 대한 라우팅 규칙을 설정하기 위한 CA Identity Manager 유틸리티입니다. 이 유틸리티를 사용하여 SQL 데이터베이스 및 LDAP 디렉터리를 제공하고 관리할 수 있는 동적 커넥터를 구성할 수 있습니다.

Connector Xpress 를 사용하면 프로비저닝 매니저에 의해 관리되는 커넥터를 만들 때 일반적으로 필요한 전문 기술 지식이 없어도 사용자 지정 커넥터를 만들고 배포할 수 있습니다.

또한 Connector Xpress 를 사용하여 커넥터 서버 구성(Java 및 C++ 모두)을 설정, 편집, 제거할 수도 있습니다.

Connector Xpress 로의 주요 입력은 끝점 시스템의 네이티브 스키마입니다. 예를 들어 Connector Xpress 를 사용하여 RDBMS 에 연결하고 데이터베이스의 SQL 스키마를 검색할 수 있습니다. 그런 다음 Connector Xpress 를 사용하여 ID 관리 및 프로비저닝과 관련된 네이티브 스키마의 해당 부분에서 매핑을 구성할 수 있습니다. 매핑은 프로비저닝 계층이 네이티브 스키마의 요소를 나타내는 방법을 설명합니다.

Connector Xpress 는 동적 커넥터에 대상 시스템에 대한 런타임 매핑을 설명하는 메타데이터를 생성합니다.

Connector Xpress 의 출력은 매핑을 완료할 때 생성되는 메타데이터 문서입니다. 이 메타데이터는 CA IAM CS 에 대한 커넥터의 구조를 설명하는 XML 파일입니다.

프로비저닝 서버 클래스 및 특성과 이들이 네이티브 스키마에 매핑되는 방식을 설명합니다.

이 메타데이터는 하나 이상의 프로비저닝 서버에서 동적 끝점 유형을 만드는 데 사용됩니다.

참고: Connector Xpress 사용에 대한 자세한 내용은 *CA Identity Manager bookshelf*(CA Identity Manager 북셸프)에서 *Connector Xpress Guide*(Connector Xpress 안내서)를 참조하십시오.

추가 구성 요소

CA Identity Manager 에는 CA Identity Manager 기능을 지원하는 몇 가지 추가 구성 요소가 포함되어 있습니다. 이 구성 요소 중 일부는 CA Identity Manager 와 함께 설치되고 일부는 별도로 설치해야 합니다.

WorkPoint 워크플로

WorkPoint 워크플로 엔진 및 WorkPoint Designer 는 CA Identity Manager 를 설치할 때 자동으로 설치됩니다.

이러한 구성 요소를 사용하면 CA Identity Manager 태스크를 워크플로 제어하에 두고 기존 워크플로 프로세스 정의를 수정하거나 새 정의를 만들 수 있습니다.

참고: 워크플로에 대한 자세한 내용은 *관리 안내서*를 참조하십시오.

프로비저닝 관리자

CA Identity Manager 프로비저닝 매니저는 그래픽 인터페이스를 통해 프로비저닝 서버를 관리합니다. 이 구성 요소는 프로비저닝 서버 옵션 관리와 같은 관리 태스크에 사용됩니다. 경우에 따라 CA Identity Manager 사용자 콘솔에서 관리할 수 없는 특정 끝점 특성을 관리하는 데에도 프로비저닝 매니저를 사용할 수 있습니다.

프로비저닝 매니저는 CA Identity Manager 관리 도구의 일부로 설치됩니다.

참고: 이 응용 프로그램은 Windows 시스템에서만 실행됩니다.

프로비저닝 매니저에 대한 자세한 내용은 *Provisioning Reference Guide*(프로비저닝 참조 안내서)를 참조하십시오.

IAM 보고서 서버

CA Identity Manager 에서는 CA Identity Manager 환경의 상태를 모니터링하는 데 사용할 수 있는 보고서를 제공합니다. CA Identity Manager 에서 제공되는 보고서를 사용하려면 CA Identity Manager 에 포함되어 있는 IAM 보고서 서버를 설치합니다.

IAM 보고서 서버는 Business Objects Enterprise XI 를 기반으로 합니다. 기존 Business Objects 서버가 있는 경우 IAM 보고서 서버 대신 이 서버를 사용하여 CA Identity Manager 보고서를 생성할 수 있습니다.

참고: 설치 지침은 *설치 안내서*를 참조하십시오.

샘플 CA Identity Manager 설치

CA Identity Manager 를 사용하면 사용자 ID 및 사용자의 응용 프로그램 액세스와 끝점 시스템의 계정을 제어할 수 있습니다. 필요한 기능에 따라 설치할 CA Identity Manager 구성 요소를 선택합니다.

모든 CA Identity Manager 설치에서 CA Identity Manager 서버는 응용 프로그램 서버에 설치됩니다. 필요한 다른 구성 요소는 CA Identity Manager 설치 관리자를 사용하여 설치합니다.

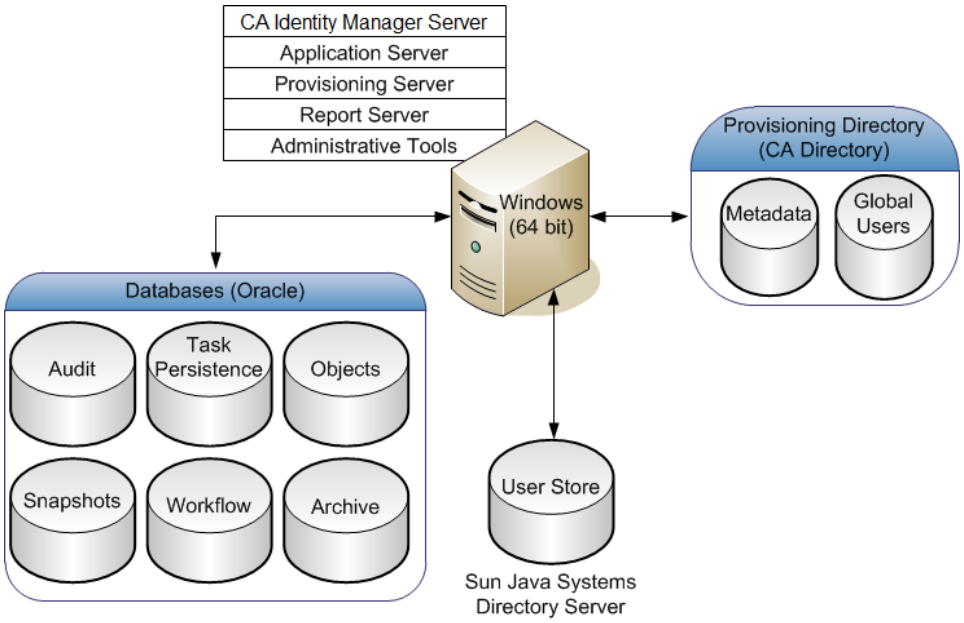
다음 단원에서는 CA Identity Manager 구현의 몇 가지 예를 개괄적으로 설명합니다.

프로비저닝 구성 요소를 사용한 설치

CA Identity Manager 프로비저닝을 사용하면 다양한 끝점 시스템에 계정을 프로비저닝하기 위해 프로비저닝 서버에 연결하는 환경을 만들 수 있습니다. CA Identity Manager 를 통해 만드는 사용자에게 프로비저닝 역할을 할당할 수 있습니다. 프로비저닝 역할은 사용자가 끝점 시스템에서 받을 수 있는 계정을 정의하는 계정 템플릿이 있는 역할입니다. 계정이 있는 사용자는 전자 메일 계정과 같은 추가 리소스에 액세스할 수 있습니다.

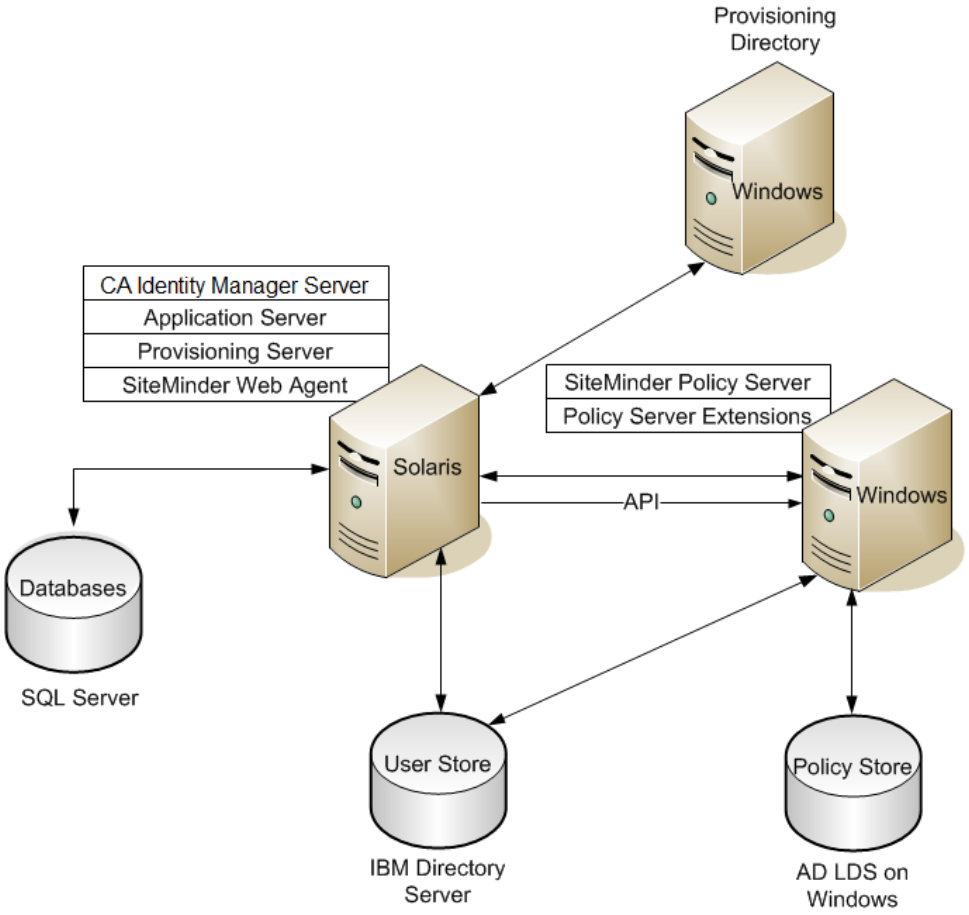
사용자에게 프로비저닝 역할을 할당하면 해당 사용자는 역할의 계정 템플릿에 정의된 계정을 받습니다. 이 계정 템플릿은 또한 계정에 사용자 특성이 매핑되는 방법을 정의합니다. 계정은 계정 템플릿에 정의된 관리 끝점에 만들어집니다.

다음 그림은 프로비저닝을 사용한 CA Identity Manager 설치의 예입니다.



SiteMinder 정책 서버를 사용한 설치

SiteMinder 정책 서버는 CA Identity Manager 환경에 대한 고급 인증과 보호를 제공합니다. 다음 그림은 SiteMinder 정책 서버를 사용한 CA Identity Manager 설치의 예입니다.



SiteMinder 를 포함하는 CA Identity Manager 구현에는 기본 설치나 프로비저닝을 사용한 설치의 모든 구성 요소 외에 다음과 같은 추가 구성 요소가 포함됩니다.

SiteMinder 웹 에이전트

SiteMinder 정책 서버와 함께 작동하여 사용자 콘솔을 보호합니다. 웹 에이전트는 CA Identity Manager 서버가 있는 시스템에 설치됩니다.

SiteMinder 정책 서버

CA Identity Manager 에 대한 고급 인증 및 권한 부여와 암호 서비스, 싱글 사인온 등의 기타 기능을 제공합니다.

SiteMinder 정책 서버에 대한 확장

SiteMinder 정책 서버가 CA Identity Manager 를 지원할 수 있도록 합니다. CA Identity Manager 구현의 각 SiteMinder 정책 서버 시스템에 확장을 설치합니다.

SiteMinder 정책 저장소

SiteMinder 가 웹 리소스에 대한 액세스를 관리하는 데 필요한 정보를 저장합니다.

CA Identity Manager 가 SiteMinder 와 통합되는 경우 SiteMinder 가 고급 인증을 제공할 수 있도록 CA Identity Manager 디렉터리 및 환경에 대한 정보도 정책 저장소에 포함됩니다.

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.

제 4 장: 구현 계획

CA Identity Manager 구현을 계획하려면 CA Identity Manager 가 사용자를 관리하는 방법과 비즈니스 목표를 달성하는 데 필요한 기능을 결정합니다. 고려할 몇 가지 사항은 다음과 같습니다.

- 사용자를 어떻게 관리합니까?
- 계정 프로비저닝이 필요합니까?
- 사용자 지정 비즈니스 요구 사항은 무엇이고 이 요구 사항을 워크플로를 사용하여 구현합니까?

결정 사항에 따라 환경에 맞게 CA Identity Manager 를 구현하는 최상의 방법을 결정할 수 있습니다.

이 섹션은 다음 항목을 포함하고 있습니다.

관리할 대상 결정

관리할 대상을 결정하면 설치할 구성 요소를 결정하는 데 도움이 됩니다. CA Identity Manager 를 사용하여 다음을 관리할 수 있습니다.

- 사용자 ID
- 끝점 시스템의 계정에 대한 액세스

사용자 ID

사용자 ID 는 직원, 계약자, 공급업체 등 회사가 관리해야 하는 사용자를 나타냅니다.

사용자 ID 를 관리하려면 CA Identity Manager 서버 및 관리 도구만 설치하면 됩니다.

사용자 관리 지원을 구성하는 방법

CA Identity Manager 에서 관리자가 수행할 수 있는 CA Identity Manager 태스크를 결정하는 관리자 역할이 있는 사용자를 관리합니다.

참고: CA Identity Manager 에서 사용자 관리를 구현하기 전에 필요한 기능을 결정하고 해당 기능을 단계적으로 구현하기 위한 계획을 개발 (페이지 66)해야 합니다.

사용자 관리 지원을 구성하려면 다음과 같은 상위 수준의 단계를 완료하십시오.

1. CA Identity Manager 서버 및 관리 도구를 설치합니다.

   관리 사용자에게 계정을 프로비저닝해야 하는 경우 프로비저닝 (페이지 51)에 대한 지원도 설치해야 합니다.

   참고: 자세한 내용은 *설치 안내서*를 참조하십시오.

2. CA Identity Manager 관리 콘솔에서 다음을 만듭니다.

   - **CA Identity Manager 디렉터리**

     CA Identity Manager 에 대한 사용자 저장소를 설명합니다. 여기에는 다음이 포함됩니다.

     - 사용자, 그룹 및 조직 같은 관리 개체를 저장하는 사용자 저장소에 대한 포인터
     - 관리 개체가 디렉터리에 저장되고 CA Identity Manager 에서 표시되는 방식을 설명하는 메타데이터

- **CA Identity Manager 환경**

  CA Identity Manager 관리자가 연결된 역할 및 태스크 세트로 사용자, 그룹 및 조직과 같은 개체를 관리할 수 있는 관리 네임스페이스를 제공합니다. 디렉터리의 관리와 시각적 표시는 CA Identity Manager 환경에 의해 제어됩니다.

CA Identity Manager 디렉터리 및 환경에 대한 자세한 내용은 *구성 안내서*를 참조하십시오.

3. 비즈니스 요구 사항에 맞게 기본 관리자 역할 및 태스크를 수정합니다.

   일반적인 역할 수정 사항으로는 기존 관리자 역할에서 기본 태스크 추가 또는 제거, 기본 역할을 기반으로 하는 새 관리자 역할 만들기 등을 들 수 있습니다.

   일반적인 태스크 수정 사항으로는 관리할 정보만 포함하도록 기본 사용자 프로필 탭 사용자 지정을 들 수 있습니다. (기본 프로필 탭에는 사용자에 대해 정의된 모든 특성이 포함됩니다.)

   기본 관리자 역할 및 태스크 수정에 대한 자세한 내용은 *User Console Design Guide*(사용자 콘솔 디자인 안내서)를 참조하십시오.

4. 사용자 관리 태스크를 수행할 사용자에게 관리자 역할을 할당합니다.

다른 응용 프로그램에서 계정 프로비저닝

프로비저닝을 구현하는 결정은 관리해야 하는 정보 유형에 따라 달라집니다. 중앙 사용자 디렉터리를 관리하고 있고 다른 시스템에서는 사용자 계정을 관리하지 않으려는 경우 프로비저닝이 필요하지 않습니다. 다양한 시스템에서 사용자 계정을 관리하려는 경우에는 프로비저닝 지원을 구현해야 합니다.

프로비저닝 기능은 CA Identity Manager 와 통합되어 있는 프로비저닝 서버를 통해 제공됩니다. 프로비저닝 서버는 계정 프로비저닝을 위해 다음과 같은 기능을 제공합니다.

- 끝점 관리
- 계정 동기화
- 계정 템플릿
- 탐색 및 상관 관계 지정 기능

참고: 프로비저닝 정보는 프로비저닝 디렉터리에 저장됩니다. CA Identity Manager 가 다른 유형의 디렉터리에서 사용자를 유지 관리하는 경우 배포에 CA Identity Manager 사용자 저장소 및 프로비저닝 디렉터리가 포함됩니다.

끝점 관리

계정을 프로비저닝하려면 CA Identity Manager 사용자 콘솔에서 끝점을 정의 및 관리합니다. *끝점*은 사용자가 액세스해야 하는 시스템입니다. 끝점의 예로는 Oracle 데이터베이스, UNIX NIS 서버, Windows 서버 및 Microsoft Exchange 서버를 들 수 있습니다. *계정 템플릿* (페이지 52)을 사용하여 계정을 만들고 관리 끝점에서 사용자 기능을 결정하십시오.

참고: 또한 프로비저닝 매니저를 사용하여 끝점을 정의하고 관리할 수 있습니다. 대부분의 끝점 관리 태스크에 사용자 콘솔을 사용하는 것이 좋지만 특정 끝점 특성 관리 및 계정 외의 끝점 개체 관리와 같은 일부 태스크에는 프로비저닝 매니저가 필요합니다. 프로비저닝 매니저에 대한 자세한 내용은 *Provisioning Reference*(프로비저닝 참조)를 참조하십시오.

계정 동기화

여러 관리 끝점에서 사용자 계정을 동기화할 수 있습니다. 계정 동기화가 사용되도록 설정하는 경우 프로비저닝 서버의 사용자 프로필 변경 내용이 해당 사용자의 계정이 있는 모든 끝점으로 전파됩니다.

참고: 계정 동기화 설정은 CA Identity Manager 태스크의 "프로필" 탭에서 지정합니다. 계정 동기화 구성에 대한 자세한 내용은 *관리 안내서*를 참조하십시오.

계정 템플릿

계정 템플릿은 관리 끝점에서 사용자가 표시되는 방식을 정의합니다. 예를 들어 Exchange 계정의 템플릿에서는 사용자 전자 메일 주소의 형식(예: <첫 번째 이니셜><성>@mycompany.com)을 정의할 수 있습니다.

계정 템플릿에서는 관리 시스템 내의 사용자가 가지는 권한도 결정합니다. 예를 들어 Exchange 계정의 템플릿에서는 전자 메일 주소 형식을 정의하는 것 외에 사용자의 사서함 크기를 제한할 수도 있습니다.

계정 템플릿은 사용자 콘솔에서 만들고 관리합니다.

탐색 및 상관 관계 지정 기능

"탐색 및 상관 관계 지정" 기능은 관리 시스템의 변경 내용을 검색 및 동기화하여 끝점 관리를 간소화합니다.

"탐색" 기능은 끝점에서 계정을 비롯한 개체를 찾고 이 개체에 대한 참조를 프로비져닝 디렉터리에 저장합니다. "탐색" 기능을 사용하여 관리할 새 개체를 검색할 수 있습니다. 예를 들어 LDAP 디렉터리에서 계정을 프로비져닝하고 해당 디렉터리에 새 조직이 추가되는 경우 "탐색" 기능을 사용하여 이러한 새 조직을 가져와서 계정 템플릿에 사용할 수 있습니다.

"상관 관계 지정" 기능은 관리 끝점의 계정을 프로비져닝 디렉터리의 전역 사용자와 연결합니다. 끝점을 통해 계정을 변경하면 "상관 관계 지정" 기능은 이러한 변경 내용을 전역 사용자 계정과 동기화할 수 있습니다.

참고: "탐색 및 상관 관계 지정" 기능에 대한 자세한 내용은 *관리 안내서*를 참조하십시오.

프로비져닝에 대한 지원을 구성하는 방법

프로비져닝을 구현하기로 결정한 후 다음과 같은 상위 수준의 단계를 완료하십시오.

1. CA Identity Manager 서버 설치 관리자를 사용하여 CA Identity Manager 서버, 프로비져닝 서버, 프로비져닝 디렉터리 초기화 및 관리 도구를 설치합니다.

   참고: CA Identity Manager 구성 요소 설치에 대한 자세한 내용은 *설치 안내서*를 참조하십시오.

2. CA Identity Manager 서버에 연결하도록 프로비져닝 매니저를 구성합니다.

3. CA Identity Manager 관리 콘솔에서 프로비져닝을 구성합니다.
   a. 프로비져닝이 사용되도록 설정합니다.
   b. 다음을 완료하여 프로비져닝에 대한 환경을 구성합니다.
      - 사용자 지정 역할 정의 가져오기
      - 인바운드 관리자 구성
      - 환경을 프로비져닝 서버에 연결

   참고: 자세한 내용은 *구성 안내서*를 참조하십시오.

4. 사용자 콘솔에서 끝점을 만듭니다.

   그러면 CA Identity Manager 가 끝점을 관리할 수 있습니다.

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

5. 끝점을 탐색하고 상관 관계를 지정합니다.

   끝점을 탐색할 때 CA Identity Manager 는 끝점에 있는 개체를 찾고 이 개체의 인스턴스를 프로비저닝 디렉터리에 저장합니다. 이 동작으로 프로비저닝 디렉터리에 계정과 끝점에서 찾은 다른 개체가 채워집니다.

   끝점에서 계정의 상관 관계를 지정하면 CA Identity Manager 는 계정을 프로비저닝 디렉터리의 전역 사용자와 연결합니다. 상관 관계 지정 기능에서 존재하지 않는 전역 사용자를 만들지 또는 일치하는 전역 사용자가 없는 계정을 [기본 사용자] 전역 사용자와 연결할지를 선택할 수 있습니다.

6. 계정을 만드는 데 사용되는 특성을 포함하는 계정 템플릿을 사용하여 끝점 계정을 만들고 유지 관리합니다.

7. 계정 템플릿을 프로비저닝 역할과 연결합니다.

   사용자에게 프로비저닝 역할을 할당하면 CA Identity Manager 는 해당 사용자에 대해 연결된 끝점에서 계정을 만듭니다.

   참고: 계정 템플릿 및 프로비저닝 역할에 대한 자세한 내용은 *관리 안내서*를 참조하십시오.

감사 요구 사항 결정

CA Identity Manager 에는 CA Identity Manager 환경에서 활동을 모니터링할 수 있는 감사 기능이 포함되어 있습니다.

이 정보는 감사 데이터베이스에 저장됩니다. 감사 데이터베이스에 저장되는 정보의 양과 유형을 구성할 수 있습니다.

사용자 콘솔에서 "View Submitted Tasks"(제출한 태스크 보기)라는 태스크를 통해 감사 데이터를 볼 수 있습니다. 이 태스크를 사용하면 관리자가 시스템에서 발생하는 태스크를 검색하고 볼 수 있습니다. 관리자는 태스크 정보를 개괄적으로 보거나 태스크 및 이벤트 상세 정보를 볼 수 있습니다.

CA Identity Manager 감사 고려 사항

감사 데이터는 CA Identity Manager 환경에서 발생하는 오퍼레이션의 내역을 제공합니다. CA Identity Manager 에서 데이터를 감사하려면 다음이 필요합니다.

- 감사 데이터베이스
- 감사 설정 파일

감사 데이터베이스

CA Identity Manager 설치 관리자를 사용하는 경우 CA Identity Manager 는 CA Identity Manager 데이터베이스라는 단일 데이터베이스에 대한 연결을 구성하고 감사용 데이터베이스 테이블에 연결하기 위한 데이터 원본을 만듭니다.

참고: CA Identity Manager 데이터베이스에는 태스크 지속, 워크플로 및 보고를 비롯한 다른 CA Identity Manager 기능에 사용되는 데이터도 포함됩니다. 확장성을 위해 별도의 감사용 데이터베이스 인스턴스를 새로 만들 수 있습니다.

참고: 감사 데이터베이스에 대한 자세한 내용은 *설치 안내서*를 참조하십시오.

감사 설정

감사 설정 파일에서 감사 설정을 구성합니다. 감사 설정 파일은 CA Identity Manager 가 감사하는 정보의 양과 유형을 결정합니다. 감사 설정 파일을 구성하면 다음을 수행할 수 있습니다.

- CA Identity Manager 환경에 대해 감사가 사용되도록 설정합니다.
- 관리자 태스크에서 생성되는 CA Identity Manager 이벤트의 일부 또는 전부에 대해 감사가 사용되도록 설정합니다.
- 이벤트가 완료되거나 취소될 때와 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.

참고: 감사 구성에 대한 자세한 내용은 *구성 안내서*를 참조하십시오.

CA Audit 고려 사항

CA Audit 은 감사, 보고, 규정 준수 확인 및 이벤트 모니터링을 위해 보안 관련 데이터를 수집 및 저장할 수 있는 감사 관리 시스템입니다.

CA Audit 과 통합하려면 CA Identity Manager 서버를 설치할 때 iRecorder 구성 요소를 설치합니다. iRecorder 는 CA Identity Manager 에서 이벤트를 검색합니다. iRecorder 는 CA Audit 정책 매니저의 정책을 기반으로 이벤트를 무시하거나 CA Audit 으로 라우팅합니다.

사용자 저장소 요구 사항 결정

CA Identity Manager 구현에는 CA Identity Manager 가 유지 관리하는 사용자 ID 를 포함하는 사용자 저장소가 포함되어 있어야 합니다. 일반적으로 이 저장소는 엔터프라이즈에서 직원 및 고객과 같은 사용자에 대한 정보를 저장하는 데 사용하는 기존 사용자 저장소입니다.

구현에 프로비저닝이 포함된 경우 CA Identity Manager 에는 Microsoft Exchange, Active Directory 및 Oracle 과 같은 끝점의 계정과 연결된 전역 사용자를 포함하는 프로비저닝 디렉터리도 필요합니다.

여러 사용자 저장소 관리

엔터프라이즈에서 여러 사용자 저장소를 유지 관리할 수 있습니다. 각 사용자 저장소에서 사용자 ID 를 사용하여 서로 다른 회사 리소스에 액세스할 수 있습니다. 다음 방법 중 하나를 사용하여 여러 사용자 저장소를 관리할 수 있습니다.

- CA Identity Manager 를 사용하여 프로비저닝 디렉터리를 직접 관리하고 프로비저닝 서버를 사용하여 다른 사용자 저장소의 사용자 및 계정을 간접적으로 관리합니다.

  이 접근 방식을 사용하면 다음을 수행할 수 있습니다.

  - 다양한 엔터프라이즈 리소스가 할당될 수 있는 사용자를 중앙의 한 위치에서 관리합니다.
  - 전체 엔터프라이즈 리소스에서 공용 보안 및 비즈니스 규칙을 구현합니다. 여기에는 다음이 포함될 수 있습니다.
    - 역할 기반 액세스 제어
    - 위임된 관리

- 관리하는 회사 ID 의 유형에 따라 사용자 지정된 태스크 및 화면
- 규칙 기반 ID 관리를 위한 ID 정책
- 사용자 지정 및 확장

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

- 별도의 CA Identity Manager 환경을 만들어 각 사용자 저장소를 관리합니다.

  이 방법을 사용하면 환경 간에 정보가 공유되지 않습니다.

설치할 구성 요소 선택

다음 표에는 구현할 기능을 지원하기 위해 설치할 구성 요소가 나와 있습니다.

참고: 이러한 구성 요소를 설치하는 방법에 대한 자세한 내용은 *설치 안내서*를 참조하십시오.

필요한 기능...	설치할 구성 요소
기존 회사 사용자 저장소에서 사용자 ID 관리	■ CA Identity Manager 서버
끝점 시스템에서 계정 프로비저닝	■ 프로비저닝 서버 ■ 프로비저닝 디렉터리 ■ 프로비저닝 관리자 ■ 커넥터 ■ 커넥터 서버 **참고**: 커넥터를 설치하는 방법에 대한 자세한 내용은 설치할 커넥터 유형에 대한 *커넥터 안내서*를 참조하십시오.

필요한 기능...	설치할 구성 요소
다음 기능 중 하나 이상 구현 ■ 고급 인증 ■ 고급 암호 정책 ■ 사용자 세트에 따라 다른 콘솔 스킨 ■ 사용자의 로캘 기본 설정 구성	■ SiteMinder 정책 서버 ■ 정책 저장소 ■ SiteMinder 웹 에이전트 ■ 정책 서버에 대한 CA Identity Manager 확장 **참고**: SiteMinder 정책 서버 및 정책 저장소를 설치하는 방법에 대한 자세한 내용은 *CA SiteMinder Web Access Manager Policy Server Installation Guide* (CA SiteMinder Web Access Manager 정책 서버 설치 안내서)를 참조하십시오.웹 에이전트를 설치하는 방법에 대한 자세한 내용은 *CA SiteMinder Web Access Manager Web Agent Installation Guide* (CA SiteMinder Web Access Manager 웹 에이전트 설치 안내서)를 참조하십시오.
CA Identity Manager 활동에 대한 보고서 생성	IAM 보고서 서버

하드웨어 요구 사항 결정

CA Identity Manager 설치에 필요한 하드웨어는 구현할 기능과 배포 크기에 따라 다릅니다.

다음 단원에서는 일반적인 CA Identity Manager 구현과 각 구현에 필요한 하드웨어를 설명합니다.

배포 유형

CA Identity Manager 배포에 필요한 하드웨어를 계획할 때는 구현할 기능과 처음 배포 크기를 고려하십시오. 다음 범주 중 하나를 사용하여 배포 크기를 예상하십시오.

참고: 선택하는 배포 유형에 따라 프로비저닝 디렉터리에서 사용하는 DxGrid 파일의 크기가 결정됩니다. 배포 유형은 CA Identity Manager 서버를 설치할 때 지정합니다.

데모

개발 환경에서는 기본 테스트나 데모에서 사용하기 위한 단일 서버 배포입니다. 데모 배포에서는 최대 10,000 개의 프로비저닝된 계정을 지원합니다.

참고: 이 구현 유형에서는 프로덕션 구현을 지원하지 않습니다.

기본

대부분의 중소 규모 구현에 적합한 고가용성 구현입니다. 기본 구현에서는 최대 400,000 개의 프로비저닝된 계정을 지원합니다.

이 유형의 구현에는 CA Identity Manager 응용 프로그램과 그 구성 요소를 실행하기 위한 서버 두 대와 CA Identity Manager 데이터베이스와 사용자 저장소를 실행하기 위한 서버 두 대가 필요합니다.

중간

중간 규모 구현에 적합한 고가용성 구현입니다. 중간 배포에서는 최대 600,000 개의 프로비저닝된 계정을 지원합니다.

대규모 엔터프라이즈

추가 사용자와 증가된 수의 트랜잭션을 처리할 추가 서버 클러스터를 포함하는 고가용성 구현입니다. 대규모 배포에서는 600,000 개 이상의 프로비저닝된 계정을 지원합니다.

참고: 고가용성 구현에 대한 자세한 내용은 *설치 안내서*를 참조하십시오.

프로비저닝에 대한 추가 요구 사항

CA Identity Manager 에 프로비저닝이 포함되는 경우 기본 CA Identity Manager 구현에 필요한 구성 요소 외에 다음과 같은 추가 구성 요소가 필요합니다.

- 프로비저닝 서버

  CA Identity Manager 서버와 동일한 시스템에 설치할 수 있습니다.

- 프로비저닝 디렉터리 초기화

  중요! 프로비저닝 디렉터리 초기화는 CA Directory 에 설치해야 합니다.

- 프로비저닝 관리자

  프로비저닝 서버에 액세스할 수 있는 Windows 시스템에 설치할 수 있습니다.

참고: 개발 환경에서는 기본 설치 구성 요소도 포함하는 시스템 하나에 이러한 구성 요소를 설치할 수 있습니다.

SiteMinder 통합에 대한 추가 요구 사항

CA Identity Manager 가 SiteMinder 와 통합되는 경우에는 구현에 기본 CA Identity Manager 설치의 구성 요소뿐 아니라 다음 추가 구성 요소도 포함되어야 합니다.

- **정책 서버**

  정책 관리, 인증, 권한 부여 및 회계 서비스를 제공합니다.

  정책 서버가 CA Identity Manager 전용인 경우 정책 서버를 CA Identity Manager 서버와 동일한 시스템에 설치할 수 있습니다. 정책 서버가 다른 응용 프로그램을 보호하고 있는 경우에는 최상의 성능을 위해 별도의 시스템에 설치하는 것이 좋습니다.

- **정책 저장소**

  정책 서버 데이터를 모두 포함합니다. 지원되는 LDAP 또는 관계형 데이터베이스에 정책 저장소를 구성할 수 있습니다. 고가용성 구현에서는 정책 저장소를 별도의 서버에 설치하는 것이 좋습니다.

- **정책 서버에 대한 확장**

  SiteMinder 정책 서버가 CA Identity Manager 를 지원할 수 있도록 합니다. CA Identity Manager 구현의 각 SiteMinder 정책 서버 시스템에 확장을 설치합니다.

- **SiteMinder 웹 에이전트**

  SiteMinder 정책 서버와 함께 작동하여 사용자 콘솔을 보호합니다. 시스템에 CA Identity Manager 서버와 함께 설치됩니다.

사용자를 가져오는 방법 선택

사용자를 기존 사용자 저장소로 가져와야 하는 경우 그 방법은 비즈니스 요구 사항에 따라 선택해야 합니다.

다음 단원에서는 사용자를 가져오는 옵션에 대해 설명합니다.

새 사용자 저장소로 사용자를 가져오는 방법

사용자 데이터 저장 방법을 결정한 후 사용자를 한 저장소에서 다른 저장소로 가져와야 할 수 있습니다. 구현에 따라 다른 방법을 사용하여 사용자를 가져올 수 있습니다.

참고: 새 사용자 저장소로 사용자를 가져온 후 ID 정책 (페이지 63)을 사용하여 가져온 사용자에 변경 내용을 적용할 수 있습니다.

CA Identity Manager 를 통해 사용자 가져오기

CA Identity Manager 에서는 직접 관리하는 사용자 저장소에 사용자를 추가하는 다음과 같은 방법을 제공합니다.

방법	기능	제한
대량 로더	사용자 콘솔의 "대량 로더" 태스크를 사용하여 많은 관리 개체를 동시에 조작하는 데 사용되는 피더 파일을 업로드할 수 있습니다. "대량 로더" 방법의 장점은 정보(피더) 파일을 사용하여 많은 관리 개체를 조작하는 프로세스를 자동화할 수 있다는 것입니다. 대량 로더 태스크를 워크플로 프로세스에 매핑할 수도 있습니다.	"대량 로더"를 사용할 경우 가져오는 사용자 수에 따라 메모리 부족 예외가 발생할 수 있습니다. 이 문제를 해결하려면 JVM 메모리 설정을 늘리십시오.
TEWS(태스크 실행 웹 서비스)를 통해 원격 태스크 호출	"사용자 만들기" 태스크를 비롯해 웹 서비스에 대해 사용되도록 설정된 모든 CA Identity Manager 태스크를 실행할 수 있습니다. 이 태스크가 "사용자 동기화"에 대해 구성된 경우 CA Identity Manager 는 적용 가능한 ID 정책을 실행합니다.	웹 서비스 모델의 성능 특성은 처리량 요구 사항이 높은 대량 가져오기 오퍼레이션에는 적합하지 않을 수 있습니다.
IM API	■ Java 클라이언트를 통해 사용자를 만들기 위해 직접 호출할 수 있는 사용자 기반 API 를 제공합니다. ■ 가장 높은 처리량을 제공합니다.	■ 태스크 서버에서 제공하는 감사 및 보안 메커니즘을 건너뜁니다. ■ ID 정책 실행을 지원하지 않습니다.

참고: 대량 로더에 대한 자세한 내용은 *관리 안내서*를 참조하십시오. TEWS 및 IM API 에 대한 자세한 내용은 *Programming Guide for Java*(Java 프로그래밍 안내서)를 참조하십시오.

가져온 사용자에 대해 ID 정책 실행

*ID 정책*은 사용자가 특정 조건이나 규칙을 충족할 때 발생하는 일련의 비즈니스 변경 내용입니다. 이러한 변경에는 역할(프로비저닝 디렉터리의 사용자에 대한 프로비저닝 역할 포함) 할당 또는 해지, 그룹 구성원 자격 할당 또는 해지, 사용자 프로필의 특성 업데이트 등이 포함될 수 있습니다.

사용자 계정을 새 사용자 저장소로 가져온 후 ID 정책을 사용하여 계정에 변경 내용을 적용할 수 있습니다.

이 단원에서는 가져온 사용자에 대해 1~2 단계로 ID 정책을 실행하는 방법을 설명합니다.

1 단계 접근 방식

다음 가져오기 방법을 사용하면 한 단계로 새 사용자 저장소로 가져오는 사용자에 대해 ID 정책을 실행할 수 있습니다.

- 사용자 콘솔의 대량 로더
- TEWS 를 통해 사용자 만들기 태스크 실행
- 인바운드 동기화

2 단계 접근 방식

2 단계 접근 방식을 사용하는 경우 먼저 사용자를 가져온 다음 해당 사용자에 대해 ID 정책을 실행합니다. CA Identity Manager 가 프로비저닝 서버의 사용자를 관리하는 경우 이 방법을 사용할 수 있습니다. 가져오기 요구 사항에 따라 이 방법은 유연성을 향상시킬 수 있습니다.

1. 가져오기 도구 중 하나를 사용하여 프로비저닝 디렉터리에 사용자를 추가합니다.
2. 가져온 사용자 각각에 대해 TEWS 를 통해 CA Identity Manager "사용자 동기화" 태스크를 호출합니다.

프로비저닝 서버를 통해 사용자 가져오기

프로비저닝 서버에는 프로비저닝 디렉터리에서 사용자를 추가 및 관리하기 위한 대량 가져오기 옵션이 포함되어 있습니다. 다음 표에서는 프로비저닝 디렉터리로 사용자를 가져오는 방법을 설명합니다.

방법	기능	제한
일괄 처리 유틸리티(etautil)	프로비저닝 디렉터리에서 개체를 관리할 수 있는 명령줄 인터페이스 유틸리티입니다.	■ 현재 Windows 시스템에서만 지원됩니다.
탐색 및 상관 관계 지정	■ 사용자를 비롯한 알려진 끝점에서 프로비저닝 서버가 관리할 수 있는 새 개체를 검색합니다. ■ 끝점 및 프로비저닝 서버에 있는 개체 인스턴스에 대한 상관 관계 지정 기능을 제공합니다. 자세한 내용은 탐색 및 상관 관계 지정 기능을 참조하십시오.	■ 탐색 및 상관 관계 지정 기능은 기본적으로 현재 지원되는 커넥터에서 사용할 수 있지만, 사용자 지정 커넥터로 확장될 수도 있습니다. ■ 대량 사용자 파퓰레이션을 사용할 경우 "상관 관계 지정" 옵션은 확장성에 영향을 줄 수 있습니다. 이 가져오기 옵션을 선택하는 경우 성능 및 확장성 영향을 평가해야 합니다.

전역 사용자를 CA Identity Manager 사용자 저장소와 동기화

사용자를 프로비저닝 서버로 가져온 후 다음 방법을 사용하여 이 사용자를 CA Identity Manager 사용자 저장소에 추가할 수 있습니다.

- **인바운드 동기화**

  인바운드 동기화는 프로비저닝 디렉터리에서 발생하는 변경 내용을 적용하여 CA Identity Manager 사용자를 최신 상태로 유지합니다. 프로비저닝 디렉터리의 변경 내용에는 프로비저닝 매니저 또는 프로비저닝 서버에 대한 커넥터가 있는 시스템을 사용하여 수행된 변경 내용이 포함됩니다.

  인바운드 동기화를 사용하여 사용자를 가져올 때는 다음 사항에 주의하십시오.

  - CA Identity Manager 관리 콘솔에서 인바운드 요청의 특성이 CA Identity Manager 태스크의 특성에 매핑되는 방식을 사용자 지정할 수 있습니다.

    참고: 자세한 내용은 *관리 안내서*를 참조하십시오.

  - 어떤 프로비저닝 서버 변경 내용을 회사 사용자 저장소와 동기화해야 하는지 고려합니다. 많은 수의 변경 내용을 동기화하면 성능 및 확장성에 영향을 줄 수 있습니다.

- **프로비저닝 역할 및 계정 템플릿**

  프로비저닝 서버는 프로비저닝 역할 및 계정 템플릿을 사용하여 CA Identity Manager 사용자 저장소의 계정을 관리할 수 있습니다. 이를 위해서는 CA Identity Manager 사용자 저장소를 가리키는 관리 끝점을 얻어야 하고 적절한 계정 템플릿과 역할이 있어야 합니다. 이 경우 프로비저닝 서버를 통해 사용자 가져오기에서 설명하는 옵션 중 하나를 통해 만든 전역 사용자에게 CA Identity Manager 사용자 저장소에서 사용자 계정을 만드는 프로비저닝 역할을 할당할 수 있습니다.

배포 계획 개발

대규모 구현을 계획할 경우 CA Identity Manager 기능을 단계적으로 배포해야 합니다. 다음 배포 순서를 사용하면 CA Identity Manager 에서 상당한 가치를 신속하게 얻고, 시간에 따라 변경되는 구현 요구 사항을 평가하고, 최상의 성능과 확장성을 위한 환경을 신중하게 구성할 수 있습니다.

- 자체 서비스 및 암호 관리
- ID 정책
- 워크플로 승인
- 사용자, 그룹 및 조직 개체에 대한 위임된 관리
- 역할 관리에 대한 위임된 관리

각 배포 단계 후 다음 단계로 진행하기 전에 성능을 평가하고 조정해야 합니다. CA Identity Manager 최적화 (페이지 77)에서는 성능, 튜닝 및 확장성 정보를 제공합니다.

자체 서비스 및 암호 관리 배포

다른 CA Identity Manager 기능을 배포하기 전에 자체 서비스 태스크 및 암호 관리를 배포하는 이유는 다음과 같습니다.

- 자체 서비스 태스크 및 암호 관리는 배포하기 간편하고 상당한 가치를 빠르게 제공합니다.
- 이러한 기능은 위임된 관리 모델에 독립적이며 변화하는 비즈니스 요구를 처리하기 위해 필요한 경우 다시 구성할 수 있습니다.
- 일반적으로 이러한 기능은 CA Identity Manager 가 정기적으로 처리하는 태스크 볼륨 중 가장 많은 볼륨을 생성합니다. 이 때문에 이러한 기능은 추가 기능을 배포하기 전에 구현의 확장성을 테스트할 수 있는 방법을 제공합니다.

자체 서비스 태스크를 배포하려면 다음 단계를 완료하십시오.

1. 자체 등록 태스크를 구성합니다.

   설치 중 기본적으로 사용되도록 설정되는 공용 태스크입니다. 이 태스크를 구성하려면 기본 자체 등록 태스크에서 필요에 따라 필드를 추가하거나 제거합니다.

2. 자체 매니저 역할을 배포합니다.

   이 역할의 구성원 규칙을 구성하여 모든 사용자에게 적용하거나 새 사용자에게 역할을 자동으로 할당하는 구성원 규칙을 포함해야 합니다. 예를 들어 모든 상근 직원에 자체 매니저 역할을 할당하는 구성원 규칙을 만들 수 있습니다. 사용자가 자체 등록할 때 CA Identity Manager 는 직원 유형을 상근으로 설정할 수 있습니다(논리적 특성 처리기나 비즈니스 태스크 처리기 사용). 이 사용자는 구성원 규칙의 기준을 충족하고 자체 매니저 역할을 자동으로 받습니다.

   참고: 자체 매니저 역할에 대한 구성원 규칙을 구성할 때 관리자가 역할 구성원을 추가하거나 제거하도록 허용하지 마십시오. 이 역할은 자동으로 할당되므로 관리자가 역할을 명시적으로 할당할 필요가 없습니다.

암호 관리 기능을 배포하려면 다음 단계를 완료하십시오.

1. "잊어버린 암호" 태스크와 같은 공용 암호 관리 태스크를 구성합니다.
2. 암호 만들기 방법 및 암호 만료 시기를 결정하는 암호 정책을 만듭니다.
3. 역할 구성원이 사용자 암호를 다시 설정할 수 있게 하는 암호 매니저 역할을 배포합니다.

참고: 역할, 태스크 및 암호 관리에 대한 자세한 내용은 *관리 안내서*를 참조하십시오.

ID 정책 배포

ID 정책은 사용자가 특정 조건이나 규칙을 충족할 때 발생하는 일련의 비즈니스 변경 내용입니다. 전체 위임 모델을 배포하기 전에 ID 정책을 사용하여 비즈니스 기반 권한을 제공할 수 있습니다. 예를 들어 영업 응용 프로그램에 대한 액세스를 부여하는 영업 매니저 프로비저닝 역할을 직함이 영업 매니저인 모든 사용자에게 할당하는 ID 정책을 만들 수 있습니다. 영업 담당자가 영업 매니저로 승격되는 경우 관리자 개입 없이 업무 수행에 필요에 모든 시스템에 대한 액세스를 자동으로 받습니다.

ID 정책을 배포하려면 다음 단계를 완료하십시오.

1. 사용자 프로필 특성이 변경되면 트리거되는 ID 정책을 구성합니다.
2. 적은 수의 관리자가 "사용자 만들기" 및 "사용자 수정"과 같은 사용자 태스크를 사용하여 ID 정책을 트리거하는 특성을 변경할 수 있도록 사용자 매니저 역할 구성합니다.

   사용자 매니저 구성원 정책에서 범위 규칙을 구성하여 역할 구성원이 관리할 수 있는 사용자 세트를 결정해야 합니다.

ID 정책을 배포할 때는 다음 사항을 고려하십시오.

- 처음에는 워크플로 승인이 필요하지 *않은* 권한을 부여하는 ID 정책을 만드는 것이 좋습니다. 이렇게 하면 워크플로 프로세스, 승인 양식 및 승인자 모델을 정의하지 않고 ID 정책을 배포할 수 있습니다.
- ID 정책을 만들기 전에 최상의 솔루션을 제공하는 방법을 결정하기 위해 CA Identity Manager 에서 비즈니스 규칙을 구현하는 다른 방법(데이터 유효성 검사 규칙, 논리적 특성, 비즈니스 로직 태스크 처리기, 워크플로 프로세스 등)에 대해 알고 있어야 합니다.

  참고: 이러한 방법에 대한 자세한 내용은 *관리 안내서* 및 *Programming Guide for Java*(Java 프로그래밍 안내서)를 참조하십시오.
- ID 정책은 CA Identity Manager 에서 권한을 할당하는 효율적인 방법이지만 성능에 상당한 영향을 미칠 수 (페이지 95) 있습니다.
- 사용자 태스크의 초기 배포 동안은 동일한 권한을 ID 정책으로 관리하는 "Roles"(역할) 탭과 같은 관계 탭을 제거하거나 숨기는 것이 좋습니다. 이렇게 하면 무단 권한의 위험이 방지되고 잘못 구성된 역할로 인한 성능 영향이 방지됩니다.

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

워크플로 승인 배포

워크플로 승인은 CA Identity Manager 구현에 보안 및 자동화 수준을 추가할 수 있습니다.

워크플로 승인을 배포하려면 다음 태스크가 필요합니다.

1. 승인이 필요한 이벤트 또는 태스크를 결정합니다.
2. 각 워크플로 프로세스에 대해 참여자라고 하는 승인자 세트를 정의합니다.

   참고: 참여자 해결 프로그램에서 모든 참여자를 동적으로 결정합니다. 우수한 성능을 유지하려면 참여자 수를 사용자 30 명으로 제한합니다.
3. 승인 양식을 구성합니다.
4. 필요한 경우 사용자 지정 워크플로 프로세스를 정의합니다.

환경 및 태스크 수준 워크플로 승인

CA Identity Manager 에서는 환경 수준 승인과 태스크 수준 승인의 두 가지 유형의 승인을 지원합니다. 환경 수준 승인은 연결된 태스크에 관계없이 이벤트의 모든 인스턴스에 대해 정의됩니다. 태스크 수준 승인은 특정 태스크와 연결된 특정 이벤트에 대해 정의됩니다. 태스크 수준 승인이 환경 수준 승인보다 우선합니다.

연결된 태스크와 관계없이 이벤트에 대해 동일한 워크플로 활동이 발생하도록 대부분의 승인은 환경 수준에서 정의됩니다. 그러나 다음 상황에서는 태스크 수준 워크플로를 구현하는 것이 좋습니다.

- 승인이 필요하지 않은 이벤트를 생성하는 특정 비즈니스 변경 내용을 실행하는 특수 태스크가 있는 경우
- 워크플로 승인이 필요하지 않은 이벤트를 생성하는 ID 정책에 의해 트리거된 변경 동작이 있는 경우
- 특정 워크플로 프로세스를 태스크 관련 변경 내용과 연결할 수 있는 유연성이 필요한 경우

환경 수준 승인은 트랜잭션 볼륨 증가에 따라 상당한 처리와 시스템 리소스가 필요할 수 있습니다. 결과적으로 성능 및 확장성 문제를 초래할 수 있습니다. 적절한 경우 태스크 수준 승인을 사용하면 이러한 문제를 줄이거나 제거할 수 있습니다.

사용자, 그룹 및 조직에 대한 위임된 관리 배포

위임된 관리는 다른 CA Identity Manager 사용자가 역할 수정, 할당 및 사용 기능을 수행하도록 하여 사용자 및 해당 권한을 관리하는 것입니다.

참고: CA Identity Manager 구현에서 우수한 성능 및 확장성을 유지하려면 위임 모델을 주의해서 구성해야 합니다.

위임은 관리자 역할의 구성원 및 관리자 정책에 정의된 범위 규칙에 의해 적용됩니다. 범위 규칙은 역할 구성원이 역할을 사용할 수 있는 개체를 결정합니다. 예를 들어 범위 규칙은 사용자 매니저가 다른 부서가 아닌 자신의 부서에서만 사용자를 관리하도록 할 수 있습니다.

일반적으로 범위 규칙은 사용자 저장소의 논리 구조를 반영해야 합니다. 예를 들어 계층적 LDAP 사용자 저장소에서는 범위를 조직별로 정의할 수 있습니다. 관계형 데이터베이스에서는 부서 ID 와 같은 특성을 사용하여 범위를 정의할 수 있습니다.

사용자, 그룹 및 조직에 대한 위임된 관리를 배포할 때는 다음에 주의하십시오.

- 사용자 관련 태스크에서 "관리자 역할" 및 "프로비저닝 역할" 탭과 같은 관계 탭에 대한 액세스를 제한하십시오. 이러한 관계 탭은 "사용자 만들기" 및 "사용자 수정" 같은 기본 사용자 태스크에 포함되어 있습니다. 기본 태스크에서 이러한 관계 탭을 제거하고 적은 수의 관리자 역할에 연결된 특수 태스크에서만 사용하는 것이 좋습니다.
- CA Identity Manager 에서는 각 범위 규칙을 동적으로 평가합니다. 범위 정보는 캐시에 저장되지 않습니다. 따라서, 뛰어난 성능을 얻으려면 간단한 디렉터리 쿼리를 포함하는 범위 규칙을 만드는 것이 좋습니다.
- CA Identity Manager 에서 관리자가 관리할 수 있는 개체를 반환하는 데 걸리는 시간을 확인하여 범위 규칙의 성능을 평가하십시오.

역할의 위임된 관리 배포

CA Identity Manager 에서 역할의 위임된 관리는 대부분의 중요 권한을 부여하며 성능에 가장 큰 영향 (페이지 79)을 미칩니다. 이 때문에 다른 모든 기능을 배포한 후에 역할의 위임된 관리를 배포해야 합니다.

역할의 위임된 관리를 배포할 때는 다음 사항에 주의하십시오.

- 환경을 보호하고 높은 성능을 유지하려면 관리자 역할, 관리자 역할 구성원 및 관리자 역할 관리자의 수를 제한하십시오.
- 역할의 위임된 관리를 배포한 후에 성능 및 확장성 테스트를 수행하십시오. 필요한 경우 환경을 최적화하십시오.

제 5 장: SiteMinder 와 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:

SiteMinder 정책 서버를 사용한 설치 (페이지 46)

SiteMinder 인증

CA Identity Manager 에는 보호가 필요한 다음과 같은 콘솔이 포함되어 있습니다.

사용자 콘솔

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

관리 콘솔을 설치합니다.

CA Identity Manager 관리자가 CA Identity Manager 디렉터리, 프로비저닝 디렉터리 및 CA Identity Manager 환경을 만들고 구성할 수 있습니다.

CA Identity Manager 에는 기본적으로 사용자 콘솔을 보호하는 네이티브 인증이 포함되어 있습니다. 기본적으로 관리 콘솔은 보호되지 않지만 관리 콘솔을 보호하도록 CA Identity Manager 를 구성할 수 있습니다. 또한, CA SiteMinder 를 사용하여 관리 콘솔을 보호할 수도 있습니다.

사용자 콘솔에 대해 인증서 또는 키 인증과 같은 다른 유형의 인증을 구성하려면 CA Identity Manager 와 SiteMinder 를 통합해야 합니다.

참고: 자세한 내용은 *구성 안내서*를 참조하십시오.

제 6 장: CA Identity Manager 최적화

이 섹션은 다음 항목을 포함하고 있습니다.

CA Identity Manager 성능

CA Identity Manager 성능은 다양한 기능 및 구성 요소의 개별적인 성능에 영향을 받습니다.

CA Identity Manager 환경에서 다음과 같은 기능을 최적화할 수 있습니다.

- 역할
- 태스크
- 그룹 구성원 자격 및 관리
- ID 정책

다음과 같은 구성 요소를 튜닝하여 성능을 더욱 향상시킬 수 있습니다.

- 사용자 저장소
- 프로비저닝 구성 요소
- 데이터베이스(예: 태스크 지속 데이터베이스) 및 응용 프로그램 서버 설정을 포함하는 런타임 구성 요소

최상의 성능을 얻으려면 다음 단원의 지침에 따라 CA Identity Manager 기능을 구성하십시오. 그런 다음, 성능을 측정하고 필요한 경우 구성 요소를 튜닝하십시오. 구성 요소는 서로 연동하여 작동하기 때문에 환경에 가장 적합한 튜닝 설정을 찾으려면 여러 번 반복해야 할 수 있습니다.

역할 최적화

CA Identity Manager 에는 세 가지 유형의 역할이 있습니다.

- 관리자 역할

  사용자 콘솔에서 사용자에게 부여되는 권한을 결정합니다.

  사용자가 CA Identity Manager 환경에 로그인하면 사용자 계정에 하나 이상의 관리자 역할이 부여됩니다. 각 관리자 역할에는 사용자가 해당 CA Identity Manager 환경에서 완료할 수 있는 태스크(예: "사용자 만들기")가 포함되어 있습니다. 사용자가 보유한 관리자 역할에 따라 표시되는 사용자 콘솔이 달라집니다. 즉, 사용자의 역할에 연결된 태스크만 사용자에게 표시됩니다.

- 프로비저닝 역할

  사용자에게 전자 메일 시스템과 같은 관리 끝점의 계정을 제공합니다.

- 액세스 역할

  CA Identity Manager 에서 권한을 제공하는 또 다른 방법을 제공합니다.

역할에는 다음을 결정하는 정책이 포함됩니다.

- 역할을 사용할 수 있는 사용자(관리자 및 액세스 역할에만 해당) 및 역할을 사용할 수 있는 대상
- 역할 구성원 및 관리자를 관리할 수 있는 사용자
- 역할 정의를 수정할 수 있는 사용자

역할 및 관련 권한을 평가할 때 CA Identity Manager 성능에 큰 영향을 미칠 수 있습니다.

로그인 시 역할 평가가 성능에 미치는 영향

CA Identity Manager 사용자가 사용자 콘솔에 로그인할 때 다음과 같은 동작이 실행됩니다.

1. CA Identity Manager 에서 사용자 이름 및 암호와 같은 자격 증명을 제공하라는 메시지가 표시됩니다.
2. 사용자의 자격 증명은 다음 방법 중 하나를 사용하여 인증됩니다.
   - CA Identity Manager 네이티브 인증
   - SiteMinder 인증(CA Identity Manager 구현에 SiteMinder 가 포함된 경우)
3. CA Identity Manager 에서 환경의 모든 관리자 역할에 대해 모든 구성원 정책을 평가하여 사용자에게 적용할 관리자 역할을 결정합니다.

   참고: 이 평가는 지정된 사용자에 대해 한 번만 실행됩니다. 초기 평가를 수행한 후 CA Identity Manager 가 결과를 캐시에 저장합니다. 사용자 또는 구성원 정책 세트가 변경되어 CA Identity Manager 가 캐시의 정보를 새로 고칠 때까지 CA Identity Manager 는 캐시된 정보를 사용합니다.
4. CA Identity Manager 사용자 콘솔에는 사용자의 역할을 기준으로 범주가 표시됩니다.

사용자 콘솔에 로그인하는 모든 사용자에 대해 이 프로세스가 실행됩니다. CA Identity Manager 환경에 많은 수의 역할이 있거나 구성원 정책이 효율적이지 못한 경우 역할 구성원 자격 평가가 성능에 큰 영향을 미칠 수 있습니다. 이 경우 사용자가 사용자 콘솔에 로그인할 때 표시되는 초기 화면이 느리게 표시될 수 있습니다.

참고: 사용자가 자체 등록하거나 잊어버린 암호를 요청하기 위해 공용 태스크에 액세스할 때에는 CA Identity Manager 가 구성원 정책을 평가할 필요가 없습니다. 이 경우에는 전체 사용자 콘솔을 표시하지 않기 때문에 CA Identity Manager 에 사용자 역할 목록이 필요하지 않습니다.

역할 개체 및 성능

각 역할을 지원하기 위해 CA Identity Manager 에서는 역할 구성에 맞게 CA Identity Manager 개체 저장소 (페이지 37)에 많은 수의 개체를 만듭니다.

CA Identity Manager 는 역할마다 기본 개체 하나를 만듭니다. 또한 기본 개체 외에도 정책마다 개체 하나를 만듭니다.

역할 개체 수가 많으면 개체 저장소 검색 및 정책 평가 성능이 저하될 수 있습니다.

개체 저장소 성능

CA Identity Manager 는 사용자 및 권한을 관리하는 데 필요한 정보를 개체 저장소에 저장합니다. 개체 저장소에 많은 수의 역할 개체가 있으면 다음과 같은 문제가 발생할 수 있습니다.

- CA Identity Manager 태스크 화면에서 관리 개체 검색에 더 오랜 시간이 걸릴 수 있습니다.

  검색에 미치는 영향을 줄이기 위해 검색에 색인 특성이 사용됩니다 (페이지 100).
- 역할 관리 태스크가 느리게 실행될 수 있습니다.

  다음은 대규모 개체 저장소의 영향을 받는 몇 가지 역할 관리 태스크의 예입니다.

  - 개체 저장소에서 역할 이름이 고유한지 여부를 CA Identity Manager 가 확인해야 하기 때문에 "관리자 역할 만들기" 태스크가 느리게 실행됩니다.
  - "관리자 역할 삭제" 태스크에서는 역할을 지원하기 위해 만들어진 모든 개체를 제거하고 개체 캐시를 업데이트해야 합니다.
- CA Identity Manager 에서 역할 정책을 평가하는 데 오랜 시간이 걸립니다.

CA Identity Manager 에서는 성능을 향상시키기 위해 개체 저장소에 정보를 캐싱합니다.

역할 정책 평가 최적화

각 관리자 역할에 대해 세 가지 유형의 정책을 만들 수 있습니다.

- 구성원 정책

  역할을 받는 사용자를 결정하는 구성원 규칙과 역할 구성원이 관리할 수 있는 개체를 결정하는 범위 규칙을 정의합니다.

- 관리자 정책

  역할에 대한 관리자 규칙, 범위 규칙 및 관리자 권한을 정의합니다.

- 소유자 정책

  역할을 수정할 수 있는 사용자를 정의합니다.

CA Identity Manager 가 역할 정책을 평가할 때의 성능을 최적화하려면 다음 사항을 고려하십시오.

- CA Identity Manager 환경에서 관리자 역할의 수를 제한합니다.
- 정책 규칙 만들기 지침 (페이지 81)을 따릅니다.
- 사용자 저장소를 튜닝합니다.
- CA Identity Manager 에 SiteMinder 가 포함된 경우 정책 저장소를 튜닝합니다.

정책 규칙 만들기 지침

역할 정책 평가의 종합적인 성능을 결정할 때 주요한 요소 중 하나가 단일 정책 규칙을 평가하는 데 걸리는 시간입니다. 정책 규칙 평가 시간을 줄이려면 정책을 만들 때는 다음 사항에 주의하십시오.

- 가능한 경우 정책 규칙을 만들 때 복합 식을 사용하여 CA Identity Manager 가 만드는 정책 개체의 수와 수행하는 사용자 저장소 검색의 수를 제한합니다.

  복합 식을 포함하는 단일 규칙이 단순 식을 포함하는 여러 규칙보다 효율적입니다.

- 가능한 경우 가장 효율적이고 확장 가능한 정책 규칙 유형을 선택합니다.
- 정책 규칙에 대해 메모리 내 평가 옵션을 사용합니다.

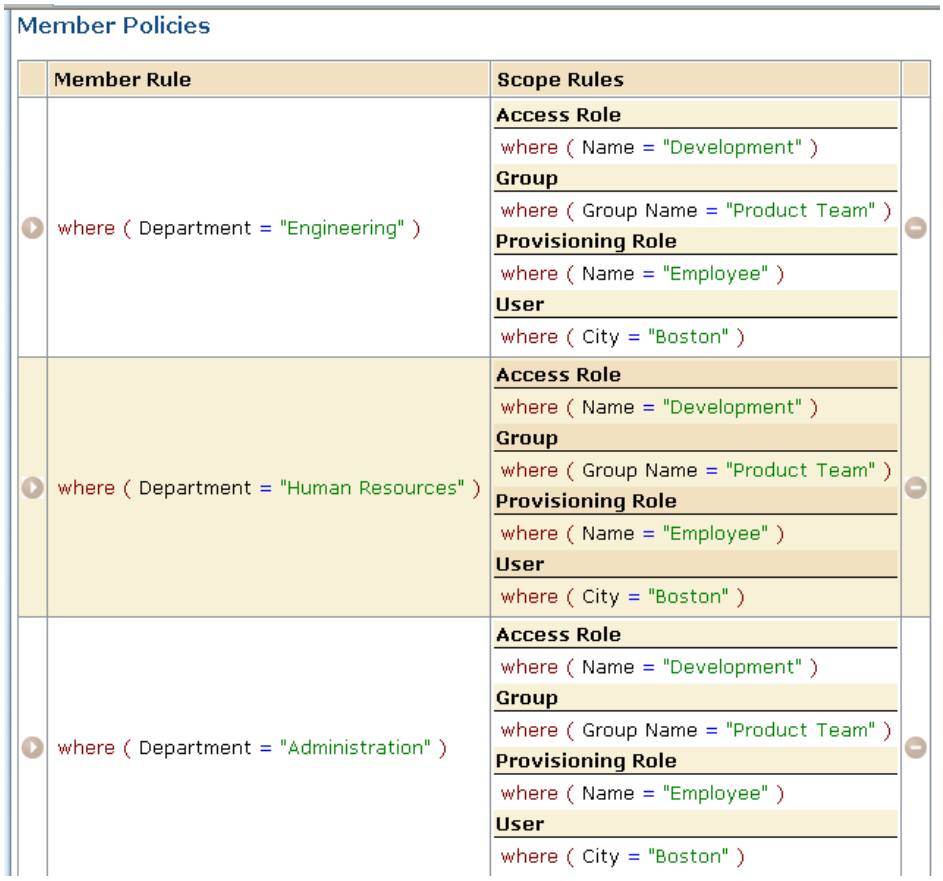
  메모리 내 평가 옵션은 평가할 사용자에 대한 정보를 사용자 저장소에서 검색하여 해당 사용자의 표현을 메모리에 저장하는 방식으로 정책 평가 시간을 크게 줄입니다. CA Identity Manager 에서는 메모리 내 표현을 사용하여 정책 규칙과 특성 값을 비교합니다.

  참고: 메모리 내 평가 옵션에 대한 자세한 내용은 *구성 안내서*를 참조하십시오.
- 사용자 저장소를 튜닝합니다.
- CA Identity Manager 구현에 SiteMinder 가 포함된 경우 정책 저장소를 튜닝합니다.

정책 개체 및 사용자 저장소 검색 제한

역할 정책의 각 규칙에는 개체 저장소의 개체 세트가 필요합니다. CA Identity Manager 가 규칙을 평가할 때 이러한 개체를 로드하고 필요한 모든 사용자 저장소 검색을 수행합니다.

다음 예에서는 세 가지 구성원 규칙을 포함하는 구성원 정책을 보여 줍니다. 각 규칙에는 네 가지 범위 규칙이 포함됩니다.


Member Policies

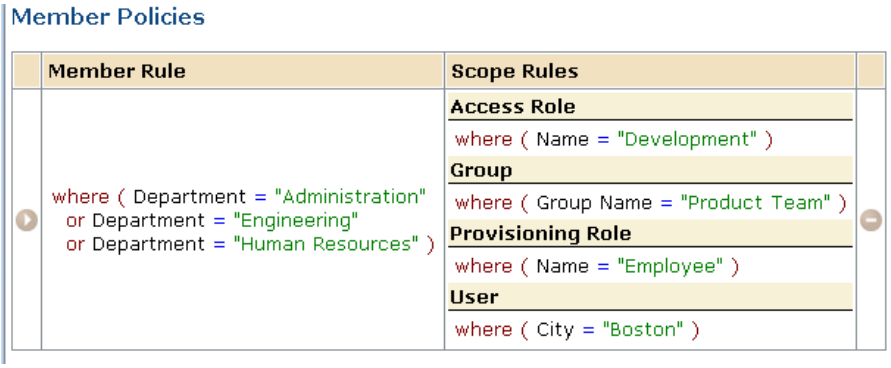
Member Rule	Scope Rules
where (Department = "Engineering")	**Access Role** where (Name = "Development") **Group** where (Group Name = "Product Team") **Provisioning Role** where (Name = "Employee") **User** where (City = "Boston")
where (Department = "Human Resources")	**Access Role** where (Name = "Development") **Group** where (Group Name = "Product Team") **Provisioning Role** where (Name = "Employee") **User** where (City = "Boston")
where (Department = "Administration")	**Access Role** where (Name = "Development") **Group** where (Group Name = "Product Team") **Provisioning Role** where (Name = "Employee") **User** where (City = "Boston")

이 예에서 CA Identity Manager 는 구성원 정책을 평가 및 적용할 때 다음 표에 설명되어 있는 개체를 만들고 사용자 저장소 검색을 수행합니다.

규칙	정책 개체	잠재적 사용자 저장소 검색
■ 구성원 규칙: 조건 (Department = "Administration") ■ 사용자 범위: 구/군/시 = "Boston" ■ 그룹 범위: 그룹 이름 = "Product Team" ■ 프로비저닝 역할 범위: 이름 = "Employee" ■ 액세스 태스크 범위: 이름 = "Development"	5	5(규칙 정의 개체마다 하나씩)
■ 구성원 규칙: 조건 (Department = "Engineering") ■ 사용자 범위: 구/군/시 = "Boston" ■ 그룹 범위: 그룹 이름 = "Product Team" ■ 프로비저닝 역할 범위: 이름 = "Employee" ■ 액세스 태스크 범위: 이름 = "Development"	5	5
■ 구성원 규칙: 조건 (Department = "Human Resources") ■ 사용자 범위: 구/군/시 = "Boston" ■ 그룹 범위: 그룹 이름 = "Product Team" ■ 프로비저닝 역할 범위: 이름 = "Employee" ■ 액세스 태스크 범위: 이름 = "Development"	5	5

이 예에서 CA Identity Manager 는 구성원 자격 및 범위를 결정하기 위해 개체 15 개를 만들고 디렉터리 검색을 15 번 수행합니다.

정책 개체의 수와 CA Identity Manager 가 수행하는 사용자 저장소 검색의 횟수를 줄이려면 규칙을 결합하여 복합 식을 만드십시오. 다음 예에서는 구성원 규칙 하나로 첫 번째 예와 동일한 권한을 지정합니다.



이 예에서는 CA Identity Manager 가 정책 개체를 10 개만 만들고 사용자 저장소 검색을 5 번만 수행합니다.

규칙	정책 개체	잠재적 사용자 저장소 검색
■ 구성원 규칙: 조건 (Department = "Administration") OR 조건 (Department = "Engineering") OR 조건 (Department = "Human Resources") ■ 사용자 범위: 구/군/시 = "Boston" ■ 그룹 범위: 그룹 이름 = "Product Team" ■ 프로비저닝 역할 범위: 이름 = "Employee" ■ 액세스 태스크 범위: 이름 = "Development"	5	5

확장 가능한 정책 규칙 유형 선택

정책 규칙의 수뿐만 아니라 정책 규칙의 유형도 성능에 영향을 미칠 수 있습니다. 일반적으로 정책 규칙은 사용자 저장소가 구조화된 방식과 권한이 결정되는 방식을 기준으로 구성됩니다. 예를 들어 그룹 구성원 자격, 조직 또는 사용자 특성을 기준으로 정책 규칙을 만들 수 있습니다. 하지만 정책 규칙을 구성하는 방법이 여러 개인 경우 다음 표에 나와 있는 성능 지침을 고려하여 구성할 규칙의 유형을 결정하십시오.

참고: 다음 표의 정책 규칙 유형은 성능순으로 나열되어 있습니다. 즉, 가장 효율적인 규칙 유형이 가장 먼저 나옵니다.

정책 규칙 유형	성능 참고 사항
조직	■ 최상의 종합적 성능 ■ LDAP 디렉터리에서 검색할 필요가 없습니다. CA Identity Manager 는 평가할 사용자의 DN 과 정책 규칙에 있는 조직의 DN 을 사용합니다.
역할	■ CA Identity Manager 는 역할 개체 정보와 개체 저장소 캐시의 이전 평가를 저장합니다. ■ 대부분의 경우 성능 수준은 조직 정책 규칙의 수준을 따릅니다.
사용자 특성	■ 가장 뛰어난 사용자 저장소 검색 성능을 제공하며 대규모 사용자 파퓰레이션의 영향을 가장 적게 받습니다. ■ 메모리 내 평가를 사용하면 성능이 크게 향상됩니다.
그룹 구성원 자격	■ 그룹 크기와 사용자 저장소 유형에 따라 성능이 결정됩니다.

태스크 최적화

CA Identity Manager 에서 사용자 콘솔에 표시되는 태스크는 사용자의 특정 권한에 따라 달라집니다. 태스크를 표시하고 실행하려면 CA Identity Manager 가 여러 번의 보안 평가를 수행해야 하며, 이러한 보안 평가를 CA Identity Manager 환경의 모든 사용자에게 적용할 경우 성능에 상당한 영향을 미칠 수 있습니다.

다음과 같은 동작이 실행될 경우 CA Identity Manager 가 보안 평가를 수행합니다.

- 사용자가 사용자 콘솔에 로그인할 경우

  이 경우 사용자 콘솔에서 사용자가 액세스할 수 있는 태스크를 결정하기 위해 CA Identity Manager 가 사용자의 역할을 평가해야 합니다.

- 사용자가 태스크를 호출할 경우

  태스크가 호출되면 CA Identity Manager 가 해당 태스크에서 사용자가 관리할 수 있는 개체를 결정해야 합니다.

- 사용자가 관계 탭에 액세스할 경우

  관계 탭은 사용자가 태스크의 대상과 권한 세트 간의 일대다 관계를 보거나 관리할 수 있는 모든 탭입니다. 관계 탭의 한 예가 사용자가 보유한 역할을 표시하는 "Admin Roles"(관리자 역할) 탭입니다.

- 사용자가 관계 탭에서 개체를 추가할 경우

  예를 들어 "Admin Roles"(관리자 역할) 탭에서 한 사용자가 다른 사용자에게 역할을 추가할 경우 CA Identity Manager 는 추가적인 보안 검사를 수행합니다.

태스크 성능은 다음과 같은 요소의 영향을 받습니다.

- 태스크 범위 - 관리자가 태스크를 사용할 수 있는 위치를 결정합니다.
- 관계 탭 - 한 개체와 다른 개체 간의 관계를 표시합니다.

태스크 범위 평가 및 성능

관리자가 사용자, 그룹, 조직, 태스크 또는 역할과 같은 관리 개체 검색을 포함하는 관리자 태스크를 사용하는 경우 CA Identity Manager 는 태스크 범위 규칙을 평가하고 적용합니다. 이러한 규칙은 CA Identity Manager 가 태스크에서 선택할 개체 목록을 표시하는 데 걸리는 시간에 상당한 영향을 미칠 수 있습니다.

참고: 구성원, 관리자 및 소유자 정책 평가와 달리 범위 규칙 평가에 대한 정보는 캐시에 저장되지 않습니다.

태스크 범위는 다음에 의해 결정됩니다.

- 태스크가 관리하는 개체의 유형
- 태스크를 포함하는 관리자 역할에 적용되는 범위 규칙. 범위 규칙은 구성원, 소유자 및 관리자 정책에서 정의합니다.
- 모든 사용자 정의 검색 조건

예를 들어 "사용자 매니저" 역할에 포함된 "사용자 수정" 태스크를 생각해 보십시오. "사용자 매니저" 역할에는 사용자 매니저가 직원 조직의 사용자를 관리할 수 있도록 허용하는 범위 규칙이 포함된 구성원 정책이 있습니다. 관리자가 "사용자 수정" 태스크를 열고 검색 조건 "성(이름) 다음으로 시작 A"를 입력합니다. 이 경우 "사용자 수정" 태스크의 범위는 성(이름)이 A 로 시작하는 직원 조직의 모든 사용자입니다.

CA Identity Manager 가 관계 탭을 표시하는 방식

관계 탭을 사용하여 사용자는 태스크의 대상과 권한 세트의 관계를 보고 관리할 수 있습니다. 예를 들어 "프로비저닝 역할" 탭에는 사용자가 소유한 프로비저닝 역할이 표시됩니다.

관계 탭에 표시할 개체를 결정하기 위해 CA Identity Manager 가 많은 수의 보안 평가를 수행하기 때문에 성능이 크게 저하될 수 있습니다.

다음 예에서는 CA Identity Manager 가 "프로비저닝 역할" 탭을 표시하기 위해 수행하는 여러 단계를 보여 줍니다.

1. 관리자가 "사용자 수정" 태스크에서 "프로비저닝 역할" 탭을 클릭합니다.
2. CA Identity Manager 는 선택된 사용자가 구성원인 프로비저닝 역할을 검색합니다.

3. 이 탭이 역할 관리자를 관리할 수 있도록 구성된 경우 CA Identity Manager 는 선택된 사용자가 관리자인 프로비저닝 역할 목록을 검색하기 위해 두 번째 호출을 수행합니다.
4. CA Identity Manager 는 사용자가 소유한 각 프로비저닝 역할을 평가하여 태스크를 시작한 관리자가 해당 역할의 구성원 자격을 관리할 수 있는지 여부를 확인합니다.

   관리자가 역할 구성원을 관리할 수 있는 경우 CA Identity Manager 는 탭의 역할 목록에서 해당 역할에 대한 "구성원 자격" 열에 활성 상태의 확인란을 표시합니다.
5. CA Identity Manager 는 사용자가 소유한 각 프로비저닝 역할을 평가하여 태스크를 시작한 관리자가 해당 역할의 관리자 권한을 관리할 수 있는지 여부를 확인합니다.

   관리자가 관리자 권한을 관리할 수 있는 경우 CA Identity Manager 는 탭의 역할 목록에서 해당 역할에 대한 "관리자" 열에 활성 상태의 확인란을 표시합니다.

   사용자가 현재 소유한 프로비저닝 역할을 표시하려면 CA Identity Manager 가 2 단계부터 5 단계까지 완료해야 합니다. 관리자가 새 프로비저닝 역할을 할당해야 하는 경우 다음과 같은 추가 단계가 필요합니다.
6. 관리자가 "추가" 단추를 클릭하여 할당할 새 프로비저닝 역할을 찾습니다.
7. 관리자가 추가할 역할을 검색하는 데 사용할 수 있는 검색 화면이 표시됩니다.
8. 관리자가 검색 필터를 입력하여 추가할 역할을 찾습니다.
9. 다음과 같은 조건을 충족하는 프로비저닝 역할 목록이 반환됩니다.
   - 역할이 관리자가 입력한 검색 필터와 일치합니다.
   - 관리자가 역할의 구성원 자격을 관리할 수 있습니다.
   - 사용자가 역할에 대한 관리자의 관리자 범위에 속합니다.
   - 사용자에게 아직 프로비저닝 역할이 없습니다.
10. CA Identity Manager 가 9 단계를 반복하여 관리자가 관리자 권한을 관리할 수 있는 역할을 결정합니다.

관계 탭 및 성능

CA Identity Manager 가 수행하는 보안 평가의 횟수로 인해 관계 탭을 표시할 때 성능에 상당한 영향을 미칠 수 있습니다. 성능을 결정하는 요소는 탭 유형에 따라 달라집니다.

역할 관계 탭의 경우 다음과 같은 요소가 성능에 영향을 미칠 수 있습니다.

- 태스크의 대상이 구성원인 역할의 수
- 태스크의 대상이 관리자인 역할의 수
- 시스템에서 CA Identity Manager 가 대상의 역할을 계산하는 데 필요한 개체의 총 수
- 역할당 구성원/관리자 정책의 수
- 구성원/관리자 정책 범위 규칙의 복잡성
- 태스크 호출자가 보안 적용의 효과를 제한할 수 있도록 캐시에 저장된 권한 부여를 유지 관리하는 기능

그룹 관계 탭에서 그룹 구성원 자격 및 관리자 권한을 결정하려면 CA Identity Manager 가 사용자 저장소에서 모든 그룹을 검색해야 합니다. 이러한 검색의 성능은 다음과 같은 요소에 따라 달라집니다.

- 사용자 저장소의 그룹 개체 수
- 개별 그룹의 구성원 수
- 사용자 저장소가 있는 데이터베이스 또는 디렉터리의 성능

태스크 처리 및 성능

관리자 태스크에는 CA Identity Manager 에서 태스크를 완료하기 위해 수행하는 동작인 이벤트가 포함되어 있습니다. 한 태스크에 여러 이벤트가 포함될 수도 있습니다. 예를 들어 "사용자 만들기" 태스크에는 사용자 프로필을 만들고 사용자를 그룹에 추가하며 역할을 할당하는 이벤트가 포함될 수 있습니다.

CA Identity Manager 는 태스크를 처리할 때 태스크와 관련된 각 이벤트를 처리합니다. 이벤트 처리 중에 각 이벤트가 네 번씩 저장됩니다. 이를 통해 CA Identity Manager 는 예기치 않은 시스템 종료가 발생하는 경우에도 처리 중인 동작을 보존할 수 있습니다.

CA Identity Manager 가 동시에 여러 이벤트를 처리하는 경우에는 이벤트가 큐에 추가됩니다. 첫 번째 이벤트가 이벤트 수명 주기의 첫 번째 단계를 완료하면 해당 이벤트가 저장된 다음 큐의 맨 뒤로 이동하여 두 번째 단계의 처리가 시작될 때까지 대기합니다. 계속해서, 큐의 다음 이벤트에 대한 첫 번째 처리 단계가 완료되면 해당 이벤트가 큐의 맨 뒤로 이동합니다. 이 프로세스가 반복되어 큐의 모든 이벤트가 첫 번째 처리 단계를 완료하게 됩니다. 그러면, 큐의 첫 번째 이벤트가 두 번째 처리 단계를 시작합니다. 큐의 모든 이벤트가 네 가지 처리 단계를 모두 완료할 때까지 이 과정이 반복됩니다.

정상적인 로드 조건에서는 이 동작이 성능에 영향을 미치지 않습니다. 하지만 대규모 사용자 파퓰레이션의 대량 로드를 처리할 때와 같이 시스템이 많은 수의 태스크와 이벤트를 처리하는 동안에는 각 이벤트와 태스크가 큐에서 훨씬 오래 대기해야 하므로 완료 시간이 더 길어집니다.

로드가 많은 상황에서 성능 문제를 방지하려면 다음과 같은 동작을 수행하는 것이 좋습니다.

- 태스크의 "프로필" 탭에 있는 "태스크 우선 순위" 설정을 사용합니다.

  "태스크 우선 순위" 설정을 사용하여 태스크의 우선 순위를 "높음", "중간" 또는 "낮음"으로 설정할 수 있습니다.

  즉시 처리해야 하는 태스크는 "높음"으로 설정해야 합니다. 대량 로드와 관련된 태스크는 "낮음"으로 설정해야 합니다.

태스크 우선 순위가 설정되어 있으면 태스크와 관련된 이벤트가 동일한 우선 순위의 다른 태스크와 함께 처리됩니다. 예를 들어 "사용자 수정" 태스크에 "높음" 우선 순위가 설정되어 있고 관리자가 사용자 프로필을 수정하는 경우 해당 태스크가 "중간" 또는 "낮음" 우선 순위의 태스크보다 먼저 처리됩니다. 다른 "높음" 우선 순위의 태스크가 있는 경우 첫 번째 "높음" 우선 순위 이벤트에 대한 첫 번째 처리 단계가 완료된 후 해당 이벤트가 다른 "높음" 우선 순위 이벤트의 목록 끝으로 이동됩니다.

- 대량 로드 오퍼레이션을 처리하는 별도의 전용 CA Identity Manager 서버를 설치합니다.

태스크 최적화 지침

CA Identity Manager 환경을 만들 때 자동으로 배포되는 기본 태스크는 광범위한 관리 사용 사례를 지원하도록 구성됩니다. 대부분의 CA Identity Manager 구현에는 기본 태스크에 제공되는 일부 기능이 필요하지 않습니다. CA Identity Manager 환경을 만든 후 특정 관리 요구 사항에 맞게 이러한 태스크를 수정하십시오.

다음 단계에서는 태스크 수정 지침을 제공합니다.

- **특수 사용자 관리 태스크 만들기**

  기본 "사용자 만들기", "사용자 수정" 및 "사용자 보기" 태스크는 전체 관리 기능을 제공합니다. 대부분의 구현에서는 소수의 관리자만 모든 기능을 사용할 수 있어야 합니다.

  필요한 기능만 포함하는 새 태스크를 만드십시오. 예를 들어 대부분의 사용자 관리 태스크에서 프로필과 그룹 관리만 수행하는 경우 "프로필" 및 "그룹" 탭만 포함하는 새로운 "사용자 수정" 태스크를 만드십시오. 기본 "사용자 수정" 태스크에서 사용할 수 있는 "관리자 역할", "액세스 역할" 및 "프로비저닝 역할" 탭을 제거하십시오.

  사용되지 않는 탭이 자주 사용하는 태스크에 남아 있으면 상당한 오버헤드가 발생할 수 있습니다. TEWS(태스크 실행 웹 서비스) 클라이언트를 사용하는 경우에는 CA Identity Manager 에 포함된 탭 java 클래스를 통해 이러한 탭이 부주의하게 활성화될 수 있으므로 특히 주의해야 합니다.

  만든 특수 태스크는 환경에 정의한 위임된 관리 모델 (페이지 71)과 일치해야 합니다.

- **관계 탭에서 "관리자 관리" 사용 안 함**

  기본적으로 모든 관계 탭에는 탭에서 관리하는 역할과 그룹 같은 개체에 대한 관리자 권한을 관리하는 기능이 있습니다. 대부분의 구현에서는 관리자에게 이 기능을 제공할 필요가 없습니다.

  이 기능이 필요하지 않은 경우 관리자 권한을 평가할 때 발생하는 추가적인 오버헤드를 제거하려면 다음과 같은 탭에서 "관리자 관리" 옵션을 해제하십시오.

  - 관리자 역할
  - 프로비저닝 역할
  - 액세스 역할
  - 그룹

  사용자가 특정 탭에서 관리자 권한을 관리할 수 있게 하려면 기본 탭의 복사본을 만든 다음 "관리자 관리" 옵션이 사용되도록 설정하고 "구성원 관리" 옵션이 사용되지 않도록 설정하십시오. 새 탭을 이 기능이 필요한 관리자만 사용하는 특수 태스크에 추가하십시오.

- **역할 관계 탭에서 범위 지정 검색 사용**

  관리자가 사용자에게 할당할 새로운 역할에 대한 조건을 지정할 수 있는 검색을 포함하도록 각 역할 탭을 구성할 수 있습니다. 역할 검색은 관리자가 사용자에게 할당할 수 있는 역할을 결정하기 위해 CA Identity Manager 가 평가해야 하는 구성원 및 관리자 정책 규칙의 수를 제한합니다.

- **태스크 동기화 옵션 설정**

  각 CA Identity Manager 태스크에 대해 사용자와 ID 정책을 동기화하는 사용자 동기화 옵션과 사용자와 프로비전된 계정을 동기화하는 프로비저닝 계정 동기화 옵션을 지정할 수 있습니다. 이러한 옵션을 사용하면 태스크가 완료되거나 이벤트가 완료될 때 사용자를 동기화할 수 있습니다.

  평가 및 처리 시간을 제거하려면 이벤트가 완료될 때가 아니라 태스크가 완료될 때 동기화가 실행되도록 설정하십시오.

그룹 구성원/관리자 최적화 지침

그룹 구성원 및 관리자에 대한 검색의 성능을 향상시키려면 다음 사항을 고려하십시오.

- 디렉터리 구성 파일(directory.xml)에서 CA Identity Manager 가 사용자 저장소 구조 및 콘텐츠를 알 수 있도록 지정하는 Well-Known 특성을 정의하십시오.

  Well-Known 특성은 CA Identity Manager 에서 특별한 의미를 갖는 특성입니다.

  그룹 구성원/관리자 검색의 성능을 향상시키려면 사용자 개체에 대해 다음과 같은 Well-Known 특성을 정의하십시오.

  %MEMBER_OF%

  사용자 개체에서 사용자가 구성원인 그룹의 목록을 저장하는 특성을 식별합니다.

  이 특성이 정의된 경우 CA Identity Manager 가 사용자 저장소에서 해당 그룹의 모든 구성원을 검색할 필요가 없습니다. 대규모 그룹의 경우 그룹 검색이 성능에 상당한 영향을 줄 수 있습니다.

  %ADMINISTRATOR_OF%

  사용자 개체에서 사용자가 관리자인 그룹의 목록을 저장하는 특성을 식별합니다.

  %MEMBER_OF% 특성과 마찬가지로, 이 Well-Known 특성은 시간이 오래 걸리는 그룹 검색을 제거할 수 있습니다.

- 디렉터리 구성 파일에서 그룹 유형 지정

  CA Identity Manager 는 표준 그룹, 중첩된 그룹 및 동적 그룹의 세 가지 그룹 유형을 지원합니다.

  디렉터리 구성 파일에서 그룹 개체를 정의할 때 사용자 저장소가 지원하는 그룹 유형을 지정할 수 있습니다. 사용 중인 구현에서 중첩된 그룹이나 동적 그룹을 지원하지 않는 경우에는 그룹 유형 특성을 다음과 같이 설정하십시오.

  GroupType = NONE

  NONE 설정은 표준 그룹에 대한 지원을 지정합니다.

  기본 그룹 유형 설정은 ALL 이기 때문에 성능에 영향을 미칠 수 있습니다.

  참고: 디렉터리 구성 파일의 Well-Known 특성 및 그룹 유형에 대한 자세한 내용은 *구성 안내서*를 참조하십시오.

- GlobalGroup 성능 향상을 위한 프로비저닝 디렉터리 캐시 색인 설정

  사용자 저장소와 프로비저닝 디렉터리가 결합된 CA Identity Manager 구현의 경우 역할 및 ID 정책에 대한 정책 규칙 평가용으로 GlobalGroup 구성원 자격을 최적화할 수 있습니다.

  이 최적화를 사용하려면 프로비저닝 서버가 그룹 구성원 자격을 확인할 때 사용할 수 있도록 프로비저닝 디렉터리 캐시에서 다음과 같은 특성을 색인화해야 합니다.

  eTID

  고유한 개체 ID 특성입니다. 그룹 구성원 자격 조회의 경우 이 값은 조회에 포함된 특정 사용자 또는 그룹입니다.

  eTPID

  구성원 자격 관계를 검색할 때 사용되는 개체의 부모 ID 입니다.

  eTCID

  구성원 자격 관계를 검색할 때 사용되는 개체의 자식 ID 입니다.

  또한 다음과 같은 해시 항목을 추가하십시오.

  eTSuperiorClass

  구성원 자격 조회에서 부모 개체의 유형입니다.

  eTSubordinateClass

  구성원 자격 조회에서 자식 개체의 유형입니다.

  참고: 프로비저닝 디렉터리 캐시에 대한 자세한 내용은 *설치 안내서*를 참조하십시오.

ID 정책 최적화

*ID 정책*은 사용자가 특정 조건이나 규칙을 충족할 때 발생하는 일련의 비즈니스 변경 내용입니다. 이러한 변경 내용에는 역할 할당 또는 해지, 그룹 구성원 자격 할당 또는 해지, 사용자 프로필의 특성 업데이트 등이 포함될 수 있습니다.

사용자 동기화가 발생하면 CA Identity Manager 가 ID 정책을 평가합니다.

ID 정책 성능은 다음과 같은 요소의 영향을 받습니다.

- ID 정책이 구성된 방식
- 사용자 동기화가 발생하는 빈도

사용자와 ID 정책의 동기화 방법

ID 정책을 사용하는 경우 CA CA Identity Manager 에서 정책을 평가하고 사용자에게 적용하는 방법을 이해하는 것이 중요합니다. 사용자 동기화 프로세스를 완전히 이해하지 않으면 예기치 않은 결과를 발생시키는 ID 정책 세트를 구성할 수 있습니다.

다음 절차는 CA CA Identity Manager 에서 ID 정책을 평가하고 적용하는 방법에 대해 설명합니다.

1. 사용자 동기화 프로세스가 시작됩니다.
   - **자동** - 사용자 동기화를 자동으로 트리거하도록 CA CA Identity Manager 태스크를 구성할 수 있습니다.
   - **수동** - 사용자 콘솔의 "사용자 동기화" 태스크를 사용하여 사용자를 동기화합니다.
2. CA CA Identity Manager 에서 사용자에게 적용할 ID 정책 세트를 확인합니다.
3. CA CA Identity Manager 에서 사용자에게 적용되는 ID 정책 세트를 이미 해당 사용자에게 적용한 정책 목록과 비교합니다.

   참고: 사용자에게 적용된 정책 목록은 사용자 프로필의 잘 알려진 %IDENTITY_POLICY% 특성에 저장됩니다. 이 특성의 구성에 대한 자세한 내용은 *Configuration Guide*(구성 안내서)를 참조하십시오.

   - ID 정책이 적용 가능한 정책 목록에 *있고* 이전에 해당 정책이 사용자에게 적용되지 *않은* 경우 CA CA Identity Manager 에서 이 정책을 할당 목록에 추가합니다.
   - ID 정책이 적용 가능한 정책 목록에 있고 이전에 해당 정책을 사용자에게 적용했으며 정책에 대해 "한 번 적용" 설정을 사용하지 않은 경우 CA CA Identity Manager 에서 이 정책을 재할당 목록에 추가합니다.

- ID 정책이 적용 가능한 정책 목록에 없고, 해당 정책이 사용자에게 적용된 경우 이 사용자는 더 이상 정책 조건에 맞지 않습니다. CA CA Identity Manager 는 이러한 정책을 할당 취소 목록에 추가합니다.

4. CA CA Identity Manager 에서 사용자에 대한 모든 정책을 평가한 후 다음 순서대로 정책을 적용합니다.
   a. 할당 취소 목록의 ID 정책
   b. 할당 목록의 ID 정책
   c. 재할당 목록의 ID 정책
5. ID 정책이 적용된 후 CA CA Identity Manager 는 정책을 재평가하여 첫 번째 동기화 프로세스(2-4 단계)에서 발생한 변경에 따라 추가 변경이 필요한지 여부를 확인합니다.

   이것은 ID 정책 적용에 의한 변경에서 다른 ID 정책을 트리거하지 않았는지 확인하기 위한 것입니다.
6. CA CA Identity Manager 는 사용자가 적용 가능한 모든 정책과 동기화되거나 CA CA Identity Manager 가 관리 콘솔에서 정의된 최대 되풀이 수준에 도달할 때까지 계속해서 ID 정책을 재평가하여 적용합니다.

   예를 들어, 사용자에게 역할이 할당되면 ID 정책이 해당 사용자의 부서를 변경할 수 있습니다. 새 부서가 다른 ID 정책을 트리거합니다. 그러나 재귀 수준이 1 로 설정되면 사용자가 다시 동기화될 때까지 후속 변경이 수행되지 않습니다.

   재귀 수준 설정에 대한 자세한 내용은 관리 콘솔 온라인 도움말을 참조하십시오.

효율적인 ID 정책 설계

ID 정책을 만들 때는 다음과 같은 지침에 따르십시오.

- **정책 개체 수 제한**

  CA Identity Manager 는 개체 저장소에서 ID 정책을 지원하는 개체를 만듭니다. 개체 저장소의 개체 수를 줄이려면 복합 식을 사용하여 ID 정책을 만드십시오.
  역할 정책 (페이지 83)에 대해서도 유사한 접근 방식이 권장됩니다.

- **ID 정책 세트 반복 제한**

  ID 정책에 대한 재귀 수준을 구성할 수 있습니다. 이러한 재귀 수준은 사용자가 동기화될 때 CA Identity Manager 가 ID 정책을 평가 및 적용하는 횟수를 결정합니다. 예를 들어, 사용자에게 역할이 할당되면 아이덴터티 정책이 해당 사용자의 부서를 변경할 수 있습니다. 새 부서가 다른 아이덴터티 정책을 트리거합니다. 그러나 재귀 수준이 1 로 설정되면 사용자가 다시 동기화될 때까지 후속 변경이 수행되지 않습니다.

  재귀 수준을 설정하여 CA Identity Manager 가 ID 정책을 평가하는 횟수를 제한합니다.

- **ID 정책 규칙 간의 종속성 제한**

  다음 표에 나와 있는 것처럼, 한 정책의 변경 동작("정책 적용 동작" 또는 "정책 제거 동작")이 또 다른 정책의 ID 정책 조건에서 사용되는 ID 정책을 만들 수 있습니다.

ID 정책 조건	정책 적용 동작	정책 제거 동작
조건 (Job Code(작업 코드) = "100")	("Account Manager" 프로비저닝 역할)의 구성원 만들기	구성원을 ("Account Manager" 프로비저닝 역할에서) 제거
다음의 구성원인 사람: (프로비저닝 역할 "Account Manager")	("Account Managers" 그룹의) 구성원 만들기	구성원을 ("Account Managers" 그룹에서) 제거

  CA Identity Manager 가 이 정책 유형을 평가할 때 두 조건을 모두 충족하려면 두 번 이상 변경 내용을 평가 및 적용해야 합니다. 전체 CA Identity Manager 환경에 대해 설정하는 재귀 수준은 1 보다 커야 하므로 각 ID 정책 세트에 대해 추가적인 평가가 발생합니다.

사용자 동기화를 트리거하는 태스크 제한

사용자 동기화 프로세스 중에 ID 정책이 평가 및 적용됩니다. 태스크에 대해 다음 사용자 동기화 옵션 중 하나를 지정하여 자동 동기화를 구성할 수 있습니다.

태스크 완료 시

태스크의 모든 이벤트가 완료된 후 CA Identity Manager 는 사용자 동기화 프로세스를 시작합니다.

모든 이벤트 발생 시

태스크의 각 이벤트가 완료될 때 CA Identity Manager 가 사용자 동기화 프로세스를 시작합니다.

최상의 성능을 얻으려면 자동 사용자 동기화를 트리거하는 태스크 수를 제한하십시오.

사용자 동기화를 구성할 때는 다음 사항을 고려하십시오.

- **암호 태스크에 대해 사용자 동기화 사용 안 함**

  대부분의 경우 ID 정책 조건에 암호가 사용되지 않습니다.

- **사용자 동기화 태스크에 대해 사용자 동기화 사용 안 함**

  "사용자 동기화" 태스크는 ID 정책 평가를 트리거하기 때문에 이 태스크에 대해 사용자 동기화 옵션이 사용되도록 설정하면 CA Identity Manager 가 평가를 다시 수행합니다.

- **특수 태스크 만들기**

  가능한 경우 ID 정책 조건을 트리거하는 수정 사항을 실행하는 태스크를 만들고 해당 태스크에 대해서만 사용자 동기화가 사용되도록 설정합니다.

ID 정책 규칙 평가 최적화

메모리 내 평가 옵션을 사용하여 사용자 특성이 포함된 ID 정책 조건에 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 정책 조건과 특성 값을 비교할 때 이 메모리 내 표현을 사용합니다. 이를 통해 CA Identity Manager 가 사용자 저장소에 대해 직접 실행하는 호출 수가 제한됩니다.

참고: 메모리 내 평가 옵션에 대한 자세한 내용은 *구성 안내서*를 참조하십시오.

사용자 저장소 튜닝

사용자 저장소 튜닝에는 다음을 비롯한 많은 단계가 포함됩니다.

- 사용자 저장소 구조 최적화
- 기반 저장소 튜닝
- 부하 분산 및 복제 구현

다음 단계는 현재 사용 중인 사용자 저장소의 유형에 따라 달라집니다. 사용자 저장소 관련 튜닝 정보는 사용자 저장소가 포함된 데이터베이스 또는 디렉터리에 대한 설명서를 참조하십시오.

CA Identity Manager 에는 일반적인 튜닝 고려 사항과 함께 다음과 같은 튜닝 고려 사항이 적용됩니다.

- **사용자 저장소 검색 성능 측정**

  최적의 성능을 얻으려면 CA Identity Manager 정책 평가 검색이 10-20 밀리초 내에 완료되어야 합니다.

  CA Identity Manager 가 이러한 검색을 지속적으로 권장된 시간 내에 완료하도록 보장하려면 다양한 부하 조건에서 검색 성능을 테스트해야 합니다.

  또한 이 측정 값을 사용하여 사용자 저장소가 물리적 제한에 도달하는 시기와 부하 분산을 위해 추가 서버가 필요한 시기를 결정할 수 있습니다.

- **특성 색인화**

  역할 정책 또는 ID 정책에 사용되는 각 특성을 색인화합니다. 특성을 색인화하면 성능이 크게 향상됩니다.

  참고: 특성 색인화에 대한 자세한 내용은 사용자 저장소가 포함된 LDAP 디렉터리 또는 관계형 데이터베이스에 대한 설명서를 참조하십시오.

- **LDAP 바인딩 캐시**

  CA Identity Manager 에서 모든 디렉터리 LDAP 바인딩은 CA Identity Manager 디렉터리 개체에 정의된 프록시 사용자에 의해 실행됩니다. 각 연결에서 이 동일한 사용자에 대해 동일한 LDAP 바인딩이 반복적으로 실행됩니다.

  사용자 저장소로 LDAP 디렉터리를 사용하고 해당 디렉터리가 캐싱을 지원하는 경우 LDAP 바인딩(또는 세션)을 캐시하는 디렉터리를 구성하십시오.

- **사용자 저장소 캐시 사용**

  CA Identity Manager 가 사용자에 대한 정책 결정 사항을 평가할 때 해당 정보가 권한 부여 캐시에 저장됩니다. 캐시된 정보가 만료되면 CA Identity Manager 가 해당 사용자에 대한 모든 정책을 다시 평가합니다.

  사용자 저장소가 캐싱을 지원하는 경우 후속 정책 규칙 평가에서 사용자 저장소 검색의 성능을 향상시키려면 사용자 저장소가 검색된 데이터를 캐시하도록 설정하십시오.

  CA Directory 에는 캐시된 데이터를 검색할 수 있는 메모리 내 데이터베이스 구현인 dxCache 라고 하는 캐시가 포함되어 있습니다.

  참고: CA Directory 에 대한 자세한 내용은 *CA Directory Administrator Guide*(CA Directory 관리자 안내서)를 참조하십시오.

프로비저닝 구성 요소 튜닝

CA Identity Manager 구현에 프로비저닝이 포함된 경우 최상의 성능을 얻으려면 다음과 같은 최적화를 수행하십시오.

- CA Identity Manager 서버와 프로비저닝 서버 간 연결 최적화

  CA Identity Manager 는 Java IAM(JIAM) API 를 사용하여 프로비저닝 서버와 통신합니다. 통신 성능을 향상시키려면 다음을 구성하십시오.

  - 프로비저닝 서버와의 다중 연결을 위한 JIAM 세션 풀

    참고: 초기 세션 값을 8 로 설정하고 최대 세션 수를 128 로 설정하는 것이 좋습니다.

  - 프로비저닝 서버에서 검색된 개체에 대한 JIAM 캐시

  참고: JIAM 구성 설정에 대한 자세한 내용은 *관리 안내서*를 참조하십시오.

- 각 이벤트가 끝날 때가 아니라 태스크가 끝날 때 계정 동기화가 실행되도록 설정 (페이지 92)
- 프로비저닝 서버 튜닝

  참고: 자세한 내용은 *관리 안내서* 및 *설치 안내서*를 참조하십시오.

런타임 구성 요소 튜닝

CA Identity Manager 에서 비즈니스 변경은 태스크를 통해 수행합니다. 태스크에는 CA Identity Manager 가 태스크를 완료하기 위해 수행하는 활동을 나타내는 이벤트가 하나 이상 포함됩니다. 예를 들어 "사용자 만들기" 태스크에는 CreateUserEvent 와 AddToGroupEvent 가 포함될 수 있습니다.

CA Identity Manager 에는 런타임 시 태스크와 이벤트를 처리하는 다음과 같은 구성 요소가 포함되어 있습니다.

- CA Identity Manager 기능을 지원하는 CA Identity Manager 데이터베이스
- 이벤트 처리를 담당하는 JMS 메시지

CA Identity Manager 데이터베이스 튜닝

태스크를 실행하면 CA Identity Manager 에서 다음과 같은 데이터베이스를 사용합니다.

- 태스크 지속

  시간에 따른 CA Identity Manager 태스크 및 이벤트에 대한 정보를 유지합니다. 시스템 오류가 발생한 경우 이 데이터베이스를 사용하여 CA Identity Manager 가 마지막으로 알려진 이벤트 및 태스크의 상태를 복원할 수 있습니다.

  참고: 상태 전환 중에 이 데이터베이스에서 태스크 및 해당 이벤트를 저장하고 검색하기 때문에 이 데이터베이스가 CA Identity Manager 성능에 가장 큰 영향을 미칩니다.

- Audit

  CA Identity Manager 환경에서 발생하는 오퍼레이션의 내역을 제공합니다.

- 워크플로

  워크플로 프로세스 정의, 작업, 스크립트 및 워크플로 엔진에 필요한 기타 데이터를 저장합니다.

- 보고

  CA Identity Manager 에서 스냅숏을 생성한 시점의 개체 상태를 나타내는 스냅숏 데이터를 저장합니다.

CA Identity Manager 는 JDBC 연결 풀을 통해 각 데이터베이스와 통신합니다. CA Identity Manager 를 호스트하는 응용 프로그램 서버에서 JDBC 연결 풀을 만들고 구성할 수 있습니다. JDBC 연결 풀을 구성할 때는 다음 사항에 주의하십시오.

- 동시에 실행될 수 있는 태스크의 수를 고려하십시오.
- JDBC 연결 풀 크기를 구성할 때 다른 런타임 구성 요소를 고려하십시오. 각 런타임 구성 요소는 다른 런타임 구성 요소와 연계되어 동작합니다.

  참고: 초기 연결 풀 값을 128 로 설정하는 것이 좋습니다.

- 태스크 지속 데이터베이스의 경우 실행되는 각 태스크에서 태스크의 전체 수명 기간 동안 태스크 및 이벤트 데이터를 검색하고 업데이트할 수 있도록 풀의 데이터베이스 연결 수가 충분해야 합니다.

- 태스크 지속 데이터베이스에서는 준비된 문을 사용합니다. 태스크 지속 데이터를 저장하는 데 사용 중인 데이터베이스에 대해 준비된 문 캐시를 구성하십시오.

  참고: 준비된 문 캐시 구성에 대한 자세한 내용은 태스크 지속용으로 사용 중인 데이터베이스의 설명서를 참조하십시오.

JMS 설정

CA Identity Manager 태스크에는 CA Identity Manager 가 태스크를 완료하기 위해 수행하는 동작에 해당하는 이벤트가 포함됩니다.

이벤트의 수명 주기 동안 이벤트는 다음과 같은 상태 전환을 거칩니다.

- BEGIN(시작)
- APPROVED(승인됨)
- EXECUTING(실행 중)
- COMPLETED(완료됨)
- INVALID(오류)

워크플로로 제어되는 이벤트에도 다음과 같은 상태가 있습니다.

- PENDING(보류 중)
- REJECTED(거부됨)

CA Identity Manager 에서는 JMS 메시지를 사용하여 이러한 상태 전환을 제어합니다.

JMS 메시지가 이벤트 전환을 제어하는 방법

CA Identity Manager 는 JMS 메시지를 사용하여 이벤트의 상태 전환을 제어합니다. 다음 절차에서는 이와 관련된 단계를 설명합니다.

1. 사용자가 태스크를 제출합니다.
2. 태스크가 하나 이상의 이벤트를 생성합니다.
3. 이벤트를 처리할 준비가 되면 CA Identity Manager 가 이벤트의 상태를 BEGIN(시작)으로 설정하고 이벤트가 태스크 지속 데이터베이스에 유지됩니다.
4. CA Identity Manager 가 이벤트 ID 를 포함하는 JMS 메시지를 만들고 해당 메시지를 이벤트 메시지 큐에 게시합니다.

5. 메시지 수신 시 JMS 가 이벤트 컨트롤러의 구현인 이벤트 MDB(메시지 구동 Bean) 인스턴스를 호출합니다.
6. 이벤트 컨트롤러는 메시지의 이벤트 ID 를 사용하여 태스크 지속 데이터베이스에서 이벤트를 검색하고 이벤트의 현재 상태에 대한 동작을 실행합니다.
7. 해당 상태가 완료되면 이벤트가 다음 상태로 설정되고 태스크 지속 데이터베이스에 상태가 유지된 후, 다음 상태를 처리할 수 있도록 새 JMS 메시지가 게시됩니다.

   이벤트가 해당 상태 시스템을 완료할 때까지 이 주기가 계속 실행됩니다.

JMS 메시지 및 성능

모든 이벤트에는 상태 전환을 위해 JMS 메시지가 필요한 다음과 같은 3~5 개의 상태가 있습니다.

- BEGIN(시작)
- PENDING(보류 중) (워크플로 제어에만 해당)
- APPROVED(승인됨) 또는 REJECTED(거부됨)
- EXECUTING(실행 중)
- COMPLETED(완료됨) 또는 INVALID(오류)

단일 이벤트를 처리할 경우 다음과 같은 동작이 실행됩니다.

- 이벤트 메시지 큐에 대한 3~5 번의 게시
- 3~5 번의 MDB(메시지 구동 Bean) 호출
- 태스크 지속 데이터베이스에 대한 6~10 개의 연결(상태별로 읽기 동작 하나와 쓰기 동작 하나)

이러한 동작은 CA Identity Manager 의 태스크 처리에 걸리는 시간에 영향을 줄 수 있습니다.

상태 전환 중에 최상의 성능을 얻으려면 CA Identity Manager 를 호스트하는 응용 프로그램 서버에서 JMS 리소스를 튜닝하여 적절한 JMS 리소스를 사용할 수 있도록 하십시오.

JMS 설정 튜닝

다음과 같은 응용 프로그램 서버의 JMS 튜닝 매개 변수는 큐 연결 및 MDB(메시지 구동 Bean) 인스턴스 풀을 정의합니다.

- **WebSphere JMS 튜닝**

  WebSphere 는 Queue Connection Factories 에 성능을 향상시키기 위해 구성할 수 있는 두 가지 매개 변수를 제공합니다. WebSphere Administration Console 을 사용하여 다음 속성을 설정하십시오.

  - "Resources"(리소스) 아래에서 두 Queue Connection Factories 매개 변수(iam-im-neteQCF 및 iam-im-wpConnectionFactory)를 찾습니다.
  - 각 매개 변수에 대해 연결 풀 속성을 편집하여 최대 연결 수를 128 로 설정합니다.

- **WebLogic 튜닝**

  WebLogic 응용 프로그램 서버에서 Queue Connection Factories 는 JMS 스레드 풀 크기에 따라 서버의 JMS 스레드 풀 또는 기본 실행 풀로부터 연결 처리 스레드를 가져옵니다. JMS 스레드 풀 크기가 0 이면 WebLogic 은 실행 풀의 스레드를 사용합니다.

  JMS 스레드 풀의 스레드 수를 CA Identity Manager 이벤트 MDB(메시지 구동 Bean)의 최대 Bean 풀 크기(기본적으로 128 로 설정됨)로 설정하는 것이 좋습니다.

  WebLogic 서버 콘솔을 사용하여 CA Identity Manager 가 설치되어 있는 도메인 및 서버에 대한 JMS 서비스 속성에서 JMS 스레드 풀 크기를 설정합니다.

  CA Identity Manager 이벤트 MDB(메시지 구동 Bean) 풀 크기는 다음 위치에 있는 설명자 파일에서 max-beans-in-free-pool 설정을 수정하여 설정합니다.

  WebLogic_home\domain\applications\iam_im.ear\identityminder_ejb.jar\META-INF\weblogic-ejb-jar.xml

```
<weblogic-enterprise-bean>
        <ejb-name>SubscriberMessageEJB</ejb-name>
        <message-driven-descriptor>
            <pool>
                <max-beans-in-free-pool>128</max-beans-in-free-pool>
                <initial-beans-in-free-pool>16</initial-beans-in-free-pool>
            </pool>

<destination-jndi-name>com.netegrity.ims.msg.queue</destination-jndi-name>
        </message-driven-descriptor>
    </weblogic-enterprise-bean>
```

- **JBoss 튜닝**

  JBoss Application Server 에서 Queue Connection Factories 는 서버의 표준 JMS 풀 세션 팩토리에서 연결 처리 스레드를 가져옵니다. 기본적으로 최대 스레드 수는 15 로 설정됩니다.

  이 값을 표준 메시지 Bean 컨테이너의 최대 크기 값과 일치하도록 설정하는 것이 좋습니다.

  JMS 세션 풀 섹션 팩토리는 다음과 같은 파일에 있는 JMSContainerInvoker 의 MaximumSize 요소에서 설정합니다.

  jboss_home\server\default\conf\standardjboss.xml

```
<invoker-proxy-binding>
         <name>message-driven-bean</name>
         ….
         <proxy-factory-config>

<JMSProviderAdapterJNDI>DefaultJMSProvider</JMSProviderAdapterJNDI>

<ServerSessionPoolFactoryJNDI>StdJMSPool</ServerSessionPoolFactoryJNDI>
            <MaximumSize>128</MaximumSize>
            <MaxMessages>1</MaxMessages>
            ….
         </proxy-factory-config>
     </invoker-proxy-binding>
```

  CA Identity Manager 이벤트 MDB(메시지 구동 Bean) 풀 크기는 다음 설명자 파일에서 최대 크기 값을 수정하여 설정합니다.

  jboss_home\server\default\conf\standardjboss.xml

```
<container-configuration>
         <container-name>Standard Message Driven Bean</container-name>
         <call-logging>false</call-logging>

<invoker-proxy-binding-name>message-driven-bean</invoker-proxy-binding-name>
        ……
         <container-pool-conf>
            <MaximumSize>128</MaximumSize>
         </container-pool-conf>
   </container-configuration>
```

JBoss 5 성능 튜닝

JBoss 5 기본 설치에서는 JBoss 핫 배포 스캐너가 5 초마다 한 번씩 실행되므로 JBoss 성능에 영향을 미칩니다. 이 기능이 필요하지 않은 경우 사용되지 않도록 설정하거나, 그렇지 않은 경우 이 기능의 실행 빈도를 변경할 수 있습니다.

핫 배포가 사용되지 않도록 설정하거나 빈도를 수정하려면

1. 다음 위치에서 hdscanner-jboss-beans.xml 을 편집합니다.

   단일 노드: *jboss_home*/server/default/deploy

   클러스터: *jboss_home*/server/all/deploy

2. 이 기능이 사용되지 않도록 설정하려면 HDScanner Bean 내부에 다음 줄을 추가하십시오.

   ```
   <attribute name="ScanEnabled">False</attribute>
   ```

3. 스캔 빈도를 수정하려면 scanPeriod 특성 값을 5000(밀리초)보다 높은 값으로 설정합니다.

참고: 자세한 내용은 http://community.jboss.org/wiki/JBossASTuningSlimming 링크를 참조하십시오.

메모리 부족 오류를 해결하려면

Java 힙 크기가 지나치게 작은 경우 "메모리 부족" 예외가 발생할 수 있습니다. 힙 크기의 초기 크기를 1024 로 설정하는 것이 좋습니다.

제 7 장: 재해 복구 계획 만들기

이 섹션은 다음 항목을 포함하고 있습니다.

재해로 인한 서비스 손실

재해가 발생하는 경우 사용자는 작업에 중요한 서비스에 액세스하지 못하게 될 수 있습니다. 결과적으로 이러한 사용자는 다른 사용자에게 서비스를 제공할 수 없습니다.

서비스에 대한 액세스 복원의 긴급성은 CA Identity Manager 의 실제 사용에 따라 달라질 수 있습니다. 일부 조직에는 CA Identity Manager 에서 제공하는 서비스에 대한 무중단 액세스를 필요로 하는 사용자가 있는 반면, 하루 동안 액세스하지 않아도 문제가 되지 않는 사용자도 있습니다. 두 경우 모두 시스템의 부분 또는 전체 손실을 초래하는 이벤트로부터 CA Identity Manager 구현을 보호하도록 준비를 갖추는 것이 좋습니다.

CA Identity Manager 에 대해 이중화된 아키텍처를 구성하면 사용자에 대한 서비스 가용성을 높일 수 있습니다. 기본 구성 요소가 실패하는 경우 대체 구성 요소가 계속 동일한 서비스를 제공합니다. 또한 중요 시스템 및 소프트웨어를 정기적으로 백업할 수 있으므로 완전히 손실된 시스템이나 데이터를 복원할 수 있습니다.

이 문서에서는 이러한 시나리오에 대한 일반적인 계획 지침을 제공합니다. 이러한 지침에 따라 조직의 요구 사항을 충족하는 특정 재해 복구 절차를 개발하는 것이 좋습니다.

재해 복구를 계획하는 방법

효과적인 재해 복구 계획을 개발하려면 이 장에서 설명하는 다음 단계를 수행하십시오.

✓	단계
	1. 재해 복구 요구 사항 정의 (페이지 111) 조직의 요구 사항을 기반으로 예측되는 재해 유형과 서비스를 얼마나 신속하게 복원해야 하는지를 식별합니다.
	2. 이중화된 아키텍처 설계 (페이지 112) 사용자 요구 사항에 따라 원격 위치에 이중화된 구성 요소를 포함하는 아키텍처를 설계합니다.
	3. 백업 계획 개발 (페이지 115) 설치를 보호하려면 구성 요소 백업을 위한 계획을 개발합니다.
	4. 복원 절차 개발 (페이지 117) 손실된 구성 요소를 복원하는 절차를 개발합니다.
	5. 복구 계획 문서화 (페이지 120) CA Identity Manager 의 재해를 복구하기 위한 계획을 문서화합니다.
	6. 복구 계획 테스트 (페이지 120) 재해 복구 절차에 따라 CA Identity Manager 구현을 이벤트 전의 상태로 복원할 수 있는지 확인합니다.
	7. 재해 복구 교육 제공 (페이지 122) 시스템 재해 복구 업무를 담당하는 직원이 복구 교육을 받도록 하여 복구 계획을 완성합니다.

재해 복구 요구 사항 정의

다음은 재해 복구 계획의 요구 사항을 정의하기 위해 고려할 몇 가지 일반적인 지침입니다.

1. 다음 정보를 숙지하고 있는 팀을 구성합니다.
   - CA Identity Manager 를 지원하는 아키텍처 및 시스템
   - CA Identity Manager 에서 사용하는 관계형 데이터베이스 및 LDAP 사용자 저장소를 백업하는 방법
2. 하나 이상의 사이트에서 부분 또는 전체적인 시스템 손실을 비롯하여 해결해야 할 잠재적인 재해 시나리오를 식별합니다.
3. 설치를 지원하기 위해 사용할 수 있어야 하는 시스템을 나열합니다.
4. 이러한 각 시스템의 허용 가능한 최대 다운타임을 정의합니다.

   예를 들어 대체 서버를 지원하는 시스템은 복원 우선 순위가 낮을 수 있습니다.

이중화된 아키텍처 설계

중요한 구성 요소 장애로부터 보호하려면 대체 구성 요소(서버 및 디렉터리)와 원격 위치에서 이중화된 데이터베이스를 사용하는 다음과 같은 보호 조치를 고려해야 합니다.

*설치 안내서*에 따라 CA Identity Manager 에 대한 이중화를 구성합니다.다음 구성 요소를 포함합니다.

- 클러스터의 일부인 이중화된 CA Identity Manager 응용 프로그램 서버 노드
- 장애 조치를 제공하는 정책 서버 클러스터(CA SiteMinder 를 사용하여 CA Identity Manager 를 보호하는 경우)
- 대체 프로비저닝 서버, 프로비저닝 디렉터리 및 커넥터 서버. 기본 구성 요소가 손실되는 경우 시스템은 대체 구성 요소로 전환됩니다.

다음을 비롯한 데이터베이스에 대한 이중화를 구성합니다.

- 워크플로 또는 감사 데이터베이스와 같이 CA Identity Manager 의 일부인 모든 런타임 데이터베이스

  ORACLE 또는 Microsoft SQL Server 와 함께 제공된 설명서를 참조하십시오.

- Business Objects 데이터베이스(보고서 서버를 사용하는 경우)

  SAP 설명서 웹 사이트에서 Business Objects Enterprise, Release 2 및 Release 2 SP4 설명서를 참조하십시오.

대체 CA Identity Manager 서버

CA Identity Manager 서버에 대해 이중화된 응용 프로그램 서버 노드를 제공하면 확장성과 성능상의 이점을 얻을 수 있고 개별 서버가 실패할 경우 재해 복구를 수행할 수 있습니다. 응용 프로그램 서버에 대한 장애 조치를 제공하는 가장 일반적인 방법은 클러스터를 만드는 것입니다. 클러스터를 만드는 절차는 *설치 안내서*의 클러스터 단원에서 다룹니다.

참고: CA Identity Manager r12.0 이상 릴리스의 경우 다중 노드 배포를 구현하는 유효한 방법은 응용 프로그램 서버 클러스터뿐입니다. CA Identity Manager 환경에서는 JMS 큐를 백본으로 사용하는 업계 표준 J2EE 클러스터 아키텍처가 필요합니다. 따라서 CA Identity Manager 구성에서 다중 노드를 사용할 수 있는 유일한 방법은 응용 프로그램 서버 클러스터입니다.

이러한 변경 사항에 대한 자세한 내용은 TechDoc 545594 를 참조하십시오.

대체 프로비저닝 구성 요소

여러 프로비저닝 구성 요소에는 고가용성을 제공하기 위한 대체 구성 요소 옵션이 있습니다. 최상의 보호를 제공하기 위해서는 대체 구성 요소가 원격 사이트에 있어야 합니다.

대체 서버 및 디렉터리의 특정 구성 정보에 대해서는 *설치 안내서*의 "High Availability Provisioning"(고가용성 프로비저닝) 장을 참조하십시오.

다중 사이트 프로비저닝 디렉터리

원격 위치의 대체 디렉터리와 함께 기본 프로비저닝 디렉터리와 대체 프로비저닝 디렉터리를 만들 수 있습니다. 세 개의 프로비저닝 디렉터리(기본 디렉터리 하나와 대체 디렉터리 두 개)를 설치하는 것이 좋습니다.

다중 사이트 프로비저닝 서버

기본 프로비저닝 서버의 실패로부터 보호하려면 대체 프로비저닝 서버를 구성할 수 있습니다. 기본 프로비저닝 서버와 대체 프로비저닝 서버의 차이점은 기본 서버를 설치하면 프로비저닝 디렉터리 컨테이너가 채워진다는 것입니다. 또한 기본 서버를 제거하면 이러한 항목도 제거됩니다. 설치와 제거를 제외하고 기본 서버와 대체 서버는 동일하게 작동합니다.

다중 사이트 커넥터 서버

Java 또는 C++ 커넥터 서버에 대해 동일한 끝점 또는 끝점 유형을 지원하도록 여러 커넥터 서버를 구성할 수 있습니다.

구성하는 각 커넥터 서버에 대해 동일한 끝점을 처리하는 대체 커넥터 서버를 원격 위치에 구성해야 합니다. 커넥터 서버가 실패하면 곧바로 대체 서버가 끝점과의 통신을 관리합니다.

이중화된 데이터베이스

지원되는 데이터베이스 소프트웨어인 Microsoft SQL Server 및 Oracle 에는 이중화된 데이터베이스를 제공하는 기능이 있습니다. 기본 데이터베이스가 실패하는 경우 이중화된 데이터베이스를 즉시 사용할 수 있습니다. 전체 사이트가 영향을 받는 경우 이중화된 데이터베이스는 원격 사이트에 있어야 합니다.

백업 계획 개발

일부 또는 모든 시스템의 손실을 방지하려면 백업하는 모든 데이터에 대한 오프사이트 저장소 및 최대 다운타임 요구 사항을 충족하는 백업 일정을 사용합니다. 백업 및 복원 절차에서는 서로 다른 응용 프로그램을 사용하므로 전체적인 CA Identity Manager 시스템 복구를 위해서는 이들 간의 조정이 필요합니다.

백업 계획에 다음 구성 요소를 포함합니다.

구성 요소	설명	백업 방법
CA Identity Manager 사용자 저장소	CA Identity Manager 사용자에 대한 레코드를 포함하는 LDAP 사용자 디렉터리 또는 관계형 데이터베이스	데이터베이스 또는 LDAP 소프트웨어와 함께 제공된 설명서를 참조하십시오.
CA Identity Manager 데이터베이스	태스크 지속, 워크플로, 감사, 개체 저장소, 보고 및 태스크 지속 아카이브에 대한 데이터베이스 워크플로, 태스크 지속 및 감사가 변경 빈도가 가장 높으므로 백업을 적절히 예약해야 합니다.	데이터베이스 소프트웨어와 함께 제공된 설명서를 참조하십시오.
SiteMinder 정책 저장소	SiteMinder 정책 서버에 대한 개체가 포함된 LDAP 사용자 디렉터리 또는 관계형 데이터베이스(SiteMinder 를 사용하는 경우)	데이터베이스 또는 LDAP 소프트웨어와 함께 제공된 설명서를 참조하십시오.
프로비저닝 디렉터리	프로비저닝 사용자 및 프로비저닝 개체에 대한 레코드를 포함하는 LDAP 사용자 디렉터리	CA Directory 설명서를 참조하십시오.
응용 프로그램 서버 JMS 영구 저장소	CA Identity Manager 태스크 이벤트 처리 메시지를 보관하는 데 사용되는 저장소	응용 프로그램 서버 설명서를 참조하십시오.

구성 요소	설명	백업 방법
보고 데이터베이스	스냅숏 데이터베이스 Business Objects 데이터베이스	데이터베이스 소프트웨어와 함께 제공된 설명서를 참조하십시오.
사용자 지정 보고서	사용자 지정 보고서 및 관련 XML 파일	SAP 설명서 웹 사이트에서 Business Objects Enterprise, Release 2 및 Release 2 SP4 설명서를 참조하십시오.

파일 시스템 백업 프로그램을 사용하여 다음 구성 요소를 백업 계획에 포함하십시오.

구성 요소	설명
웹 서버 구성 요소	응용 프로그램 서버 플러그 인 및 SiteMinder 웹 에이전트와 같이 배포된 웹 서버 구성 요소에 대한 구성. 부하 분산을 사용 중인 경우나 SiteMinder 를 사용하여 사용자 콘솔에 대한 액세스를 보호하는 경우 웹 서버 프런트 엔드가 필요합니다.
XML 데이터 파일	CA Identity Manager 개체 저장소 개체를 만들고, 유지 관리하고, 아카이브하는 데 사용되는 모든 CA Identity Manager 디렉터리 및 환경 파일
CA Identity Manager 사용자 지정 구성 요소	배포된 다음 iam_im.ear 폴더에 있는 파일 ■ 구성 ■ User_console.war WEB-INF\web.xml
스크립트 및 프로그램	TEWS 스크립트, 프로그램, 프로그램 종료
Connector Xpress 구성 요소	사용자 지정 커넥터 Connector Xpress 프로젝트 파일
재해 복구 설명서	재해 복구에 대한 설명서를 직접 작성한 경우 지침이 변경되는 경우에 대비하여 설명서를 정기적으로 백업하십시오.

복원 절차 개발

복원 절차는 백업 방법에 따라 다릅니다. 실패한 시스템의 복구 프로세스는 상황에 따라 달라집니다. 그러나 대부분의 경우에 사용되는 복원 방법은 소프트웨어를 다시 설치하는 것입니다. 자세한 내용은 *설치 안내서*의 "High Availability Provisioning"(고가용성 프로비저닝) 장을 참조하십시오.

CA Identity Manager 사용자 저장소 복원

CA Identity Manager 사용자 저장소를 복원하려면 사용하는 데이터베이스 또는 LDAP 소프트웨어와 함께 제공된 설명서를 참조하십시오. 모든 사용자 저장소에 대한 액세스를 비롯해 백업의 데이터 저장소가 변경되지 않았는지 확인하십시오.

CA Identity Manager 데이터베이스 복원

CA Identity Manager 데이터베이스를 복원하려면 사용 중인 데이터베이스와 함께 제공된 설명서를 참조하십시오. 모든 데이터베이스에 대한 액세스를 비롯해 백업의 데이터 저장소가 변경되지 않았는지 확인하십시오.

SiteMinder 정책 저장소 복원

SiteMinder 정책 저장소를 복원하려면 사용 중인 데이터베이스 또는 LDAP 소프트웨어와 함께 제공된 설명서를 참조하십시오. 모든 사용자 저장소에 대한 액세스를 비롯해 백업의 데이터 저장소가 변경되지 않았는지 확인하십시오.

CA Identity Manager 서버 복원

CA Identity Manager 서버의 클러스터 노드가 손실되는 경우 다음 단계를 수행하십시오.

1. 문서화된 표준 절차에 따라 노드를 추가합니다.

   *설치 안내서*에서 클러스터 설치 관련 장을 참조하십시오.

2. 프로비저닝 서버에 대한 연결을 업데이트합니다.

   자세한 내용은 *설치 안내서*의 "High Availability"(고가용성) 장에서 프로비저닝 장애 조치 단원을 참조하십시오.

프로비저닝 서버 및 디렉터리 복원

대체 서버를 설치하여 손실된 프로비저닝 서버를 복원할 수 있습니다. 모든 시스템이 실패한 경우 재해 복구 중에 손실된 데이터를 복원하십시오.

다음 단계를 수행하십시오.

1. 사용자 지정 스키마 파일을 CA Directory config\schema 디렉터리로 복사합니다.
2. 새 프로비저닝 디렉터리를 설치합니다.

   데이터 저장소는 비어 있습니다.

3. 백업 위치의 데이터를 복원합니다.
4. 새로 복원된 프로비저닝 디렉터리에 대한 상세 정보를 제공하는 프로비저닝 서버 설치 관리자를 사용합니다.

   도메인 정보가 이미 있어야 합니다.

5. 백업의 사용자 지정 커넥터 및 구성 파일을 복원합니다.

참고: 자세한 내용은 CA Directory 설명서를 참조하십시오.

커넥터 서버 복원

커넥터 서버가 손실되는 경우 다음 단계를 수행하십시오.

1. 커넥터 서버 설치 관리자를 사용하여 새 커넥터 서버를 설치합니다.

   설치 중 커넥터 서버를 프로비저닝 서버에 등록합니다.

2. csfconfig 또는 Connector Xpress 를 사용하여 손실된 커넥터 서버의 등록을 제거합니다.

보고서 서버 복원

보고서 서버가 손실되는 경우 Business Objects 설명서에서 적용되는 절차를 참조하십시오. SAP 설명서 웹 사이트에서 Business Objects Enterprise, Release 2 및 Release 2 SP 4 설명서를 확인하십시오.

관리자 태스크 복원

재해 발생 시 관리자 태스크가 진행 중이었으면 다음 조건하에 해당 태스크를 복구할 수 있습니다.

- 승인 대기 중인 "보류 중" 상태이던 모든 관리자 태스크는 해당 상태 정보를 유지 관리하는 데 사용되는 저장소가 유지되는 경우 계속 사용할 수 있습니다. 이 저장소에는 태스크 지속 데이터베이스, 태스크 및 이벤트 JMS 메시지를 보관하는 JMS 저장소, 워크플로 데이터베이스 등이 포함됩니다.
- "진행 중" 상태("보류 중" 외의 상태)의 태스크에는 추가 조건이 적용됩니다.

  이 상태의 태스크는 새 JMS 메시지를 CA Identity Manager 이벤트 메시지 큐에 게시해야만 계속 처리됩니다. 해당 이벤트가 큐에 게시되기 전에 중단이 발생하면 복구 시 태스크가 계속되지 않습니다.

  이 경우 태스크를 복구하는 다음과 같은 두 가지 옵션이 있습니다.

  - 태스크가 "View Submitted Tasks"(제출한 태스크 보기) 태스크에 실패한 상태로 있는 경우에는 태스크 상세 정보 페이지로 이동하고 "Resubmit Task"(태스크 다시 제출) 옵션을 사용하여 태스크를 다시 제출합니다.
  - 동일한 변경 내용을 포함하는 새 태스크를 제출합니다.

복구 계획 문서화

이 장의 지침에 따라 조직에 적용되는 특정 재해 복구 설명서를 개발하는 것이 좋습니다.

다음 접근 방식을 고려하십시오.

1. 아키텍처에 있는 시스템의 이름 및 위치와 각 시스템의 대체 구성 요소를 식별합니다.

   각 시스템에 대해 설치된 소프트웨어(예: 설치된 특정 JDK), 응용 프로그램 서버의 수정 릴리스 및 설치된 메모리 양을 나열합니다. 이 상세 정보는 완전히 다시 빌드해야 하는 것으로 결정한 모든 시스템에 필요합니다.

2. 각 구성 요소를 복구하는 절차나 필요한 경우 전체 시스템을 다시 빌드하기 위한 절차를 작성합니다.
3. 시스템 및 CA Identity Manager 사용자 인터페이스의 사용자 이름과 암호가 한 두 명의 사용자에게만 알려진 경우 이러한 항목을 찾거나 다시 설정하는 방법을 식별합니다.
4. 잘 알려진 오프사이트 위치에 저장하는 백업 복사본을 만들어 재해 복구 설명서의 손실을 방지합니다.

복구 계획 테스트

재해를 성공적으로 복구하기 위해 특정 시스템이 사용할 수 없게 되는 시뮬레이션된 재해를 예약할 수 있습니다. 다음 단원에서 설명하는 다음 테스트를 고려하십시오.

1. 장애 조치 프로세스를 테스트합니다.
2. 시스템 복원을 테스트합니다.

장애 조치 프로세스 테스트

다음 구성 요소를 비롯한 모든 서버 또는 디렉터리는 원격 사이트에 대체 서버나 디렉터리가 있어야 합니다.

- CA Identity Manager 서버
- 프로비저닝 서버
- 프로비저닝 디렉터리
- C++ 및 Java 커넥터 서버
- 보고서 서버
- 정책 서버

각 구성 요소를 수동으로 중지하고 대체 구성 요소를 사용하여 모든 오퍼레이션이 계속 작동하는지 확인하십시오. 예를 들어 프로비저닝 서버에 대한 다음 테스트를 수행할 수 있습니다.

1. 기본 프로비저닝 서버가 있는 시스템의 Windows 서비스 대화 상자에서 프로비저닝 서비스를 중지합니다.

   기본 프로비저닝 서버가 중지됩니다.

2. 사용자 콘솔에서 다음 동작을 수행합니다.

   a. 사용자에게 프로비저닝 역할을 할당합니다.

   b. 해당 사용자에 대해 끝점 계정이 만들어지는지 확인합니다.

      만들어지는 계정은 CA Identity Manager 서버와의 통신을 처리하는 대체 프로비저닝 서버에 따라 다릅니다.

이 절차는 한 가지 테스트의 예입니다. 중지하는 각 구성 요소에 대해 대체 구성 요소가 사용 중인지 확인하는 유사한 테스트를 개발하십시오.

복원 절차 테스트

재해 복구 설명서에 따라 중요한 각 구성 요소에 대한 테스트를 수행하여 손실된 시스템을 복원할 수 있는지 확인하십시오.

재해 복구 교육 제공

복구 절차가 안정적이라고 판단되면 복구를 구현해야 하는 사용자가 복구 절차를 수행할 수 있도록 도와 줍니다. 조직에 따라 다른 단계가 필요할 수 있지만 몇 가지 일반적인 지침은 다음과 같습니다.

1. 복구 설명서의 위치를 알립니다.
2. 연습 삼아 교육을 미리 수행합니다.
3. 교육의 피드백을 통합하여 최종 재해 복구 절차를 충실하게 만듭니다.

참고: 또한 복구 담당자인 한 사용자와 대체 담당자인 두 번째 사용자를 비롯한 복구 담당자를 할당할 기회로 교육을 활용할 수도 있습니다. 이러한 사용자가 문서화된 위치에서 만나 재해 복구 계획을 시작하도록 안내해야 합니다.