CA Access Control for Virtual Environments

엔터프라이즈 관리 안내서

r2.0

ca technologies

타사 고지 사항

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

샘플 스크립트와 샘플 SDK 코드

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

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

CA 제품 참조

이 문서는 다음 CA Technologies 제품을 참조합니다 :

- [set the eACee variable for your book]
- CA Access Control
- CA User Activity Reporting Module
- CA Identity Manager

설명서 규칙

CA Access Control 설명서는 다음과 같은 규칙을 따릅니다.

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

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

형식	의미
기울임꼴	반드시 입력해야 하는 정보
대괄호([ ]) 사이	선택적 피연산자
중괄호({ }) 사이	필수 피연산자 집합
파이프(|)로 구분된 선택 사항	대체 피연산자(하나 선택)를 구분합니다. 예를 들어, 다음은 사용자 이름 *또는* 그룹 이름 중 *하나*라는 의미입니다. {*username*|*groupname*}

형식	의미
...	앞의 항목 또는 항목 그룹이 반복될 수 있음을 나타냅니다.
밑줄	기본값
줄 마지막에 공백 다음의 백슬래시(\)	때때로 이 안내서에서 명령이 한 줄에 모두 표시되지 않는 경우가 있습니다. 이런 경우에는 줄 끝에 공백과 백슬래시(\)를 표시하여 명령이 다음 줄에서 계속됨을 나타냅니다. **참고:** 실제 명령을 입력할 때는 이러한 백슬래시를 포함하지 말고 줄바꿈 없이 명령을 한 줄에 입력하십시오. 백슬래시 및 줄바꿈은 실제 명령 구문에 포함되지 않습니다.

예제: 명령 표기 규칙

다음 코드는 이 안내서에서 명령 규칙이 사용되는 방식을 보여 줍니다.

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

설명:

- 표시되는 그대로 입력해야 하는 명령 이름(ruler)은 일반 고정 폭 글꼴로 표시됩니다.
- *className* 옵션은 클래스 이름(예: USER)이 들어갈 자리이므로 기울임꼴로 표시됩니다.
- 대괄호로 묶인 두 번째 부분은 선택적 피연산자를 의미하므로 이 부분 없이 명령을 실행할 수도 있습니다.
- 옵션 매개 변수(props)를 사용할 때 키워드 *all*을 선택하거나 하나 이상의 속성 이름을 쉼표로 구분하여 지정할 수 있습니다.

파일 위치 규칙

CA Access Control 설명서는 다음과 같은 파일 위치 규칙을 따릅니다.

- *ACVEInstallDir* - 기본 CA Access Control for Virtual Environments 설치 디렉터리:
  - /opt/CA/AccessControlServer/VirtualAppliance
- *ACInstallDir* - 기본 CA Access Control 설치 디렉터리입니다.
  - [set the alternate Installation Path variable]
- *ACSharedDir* - UNIX 에서 CA Access Control 에 의해 사용되는 기본 디렉터리입니다.
  - /opt/CA/SharedComponents
- *ACServerInstallDir* - 기본 CA Access Control 엔터프라이즈 관리 설치 디렉터리입니다.
  - /opt/CA/AccessControlServer
- *JBoss_HOME* - 기본 JBoss 설치 디렉터리입니다.
  - /opt/jboss-4.2.3.GA

CA 에 문의

기술 지원팀에 문의

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

목차

제 1 장: 소개

이 섹션은 다음 항목을 포함하고 있습니다.

안내서 정보

이 안내서는 엔터프라이즈 관리 및 보고 기능과 CA Access Control 엔터프라이즈 관리 웹 기반 인터페이스에 대한 정보를 제공합니다. CA Access Control 엔터프라이즈 관리의 엔터프라이즈 관리 및 보고 기능에는 권한 있는 계정 암호 관리, 보고, 월드 뷰 엔터프라이즈 뷰어가 포함되어 있습니다.

용어를 간단히 하기 위해 이 안내서에서는 제품을 CA Access Control 이라고 칭합니다.

본 안내서의 사용자

이 안내서는 CA Access Control for Virtual Environments 와 이 제품의 엔터프라이즈 관리, 타사 프로그램 통합, 보고 기능을 사용하려는 보안, 시스템, 가상화 관리자를 위한 안내서입니다.

- 엔터프라이즈 정책 관리
- 엔터프라이즈 보고
- 엔터프라이즈 호스트 액세스 관리 처리를 위한 웹 기반 인터페이스
- 권한 있는 사용자 암호 관리(PUPM)
- 타사 프로그램과의 통합

엔터프라이즈 관리

CA Access Control 엔터프라이즈 관리는 회사 전체에서 액세스 관련 관리 작업을 수행할 수 있게 해주는 웹 기반 사용자 인터페이스입니다. 여러 관리 작업을 수행할 수 있습니다. 예를 들어, 중앙 위치에서 기업 전체에 액세스 정책을 배포하고, 개별 호스트를 관리하고, 권한 있는 계정을 관리하고, 엔터프라이즈 보고서를 생성하는 등의 작업을 할 수 있습니다.

엔터프라이즈 관리 인터페이스

CA Access Control 엔터프라이즈 관리 인터페이스는 회사를 관리하는 데 필요한 모든 것을 수록하고 있는 엔터프라이즈 관리 도구입니다. CA Access Control 엔터프라이즈 관리 인터페이스에는 호스트를 구성하고, 정책을 만들어 할당하고, 사용자/그룹/관리 작업을 관리하고, 회사 전체에서 권한 있는 계정에 대한 액세스를 구성/관리하기 위한 도구가 포함되어 있습니다. 또한 엔터프라이즈 보고 및 감사 기능도 포함되어 있습니다.

엔터프라이즈 뷰

중앙 위치에서 가상/물리 컴퓨터 및 PUPM 끝점에 대한 정보를 보고 이 컴퓨터를 관리하려면 CA Access Control 엔터프라이즈 관리를 사용하십시오. CA Access Control 엔터프라이즈 관리 월드 뷰는 마지막 업데이트되었을 때 각 관리되는 장치에 대한 세부 정보를 표시합니다. 월드 뷰에서는 또한 관리되는 장치 및 보안 그룹에 대한 설정을 수정할 수 있습니다.

권한 있는 사용자 암호 관리

권한 있는 사용자 암호 관리(PUPM)는 회사에서 가장 강력한 계정과 관련된 모든 활동을 추적하고, 관리하고, 보안을 유지하기 위한 프로세스입니다.

CA Access Control 엔터프라이즈 관리를 사용하면 중앙 위치에서 관리되는 장치에 있는 권한 있는 계정의 액세스 권한을 역할에 기반하여 관리할 수 있습니다. CA Access Control 엔터프라이즈 관리는 권한 있는 계정 및 응용 프로그램 ID 암호를 안전하게 저장하고 정책에 기반하여 권한 있는 계정 및 암호에 대한 액세스를 제어합니다.

또한 CA Access Control 엔터프라이즈 관리를 사용하여 권한 있는 계정 및 응용 프로그램 암호를 관리하고 구성 파일 및 스크립트에서 암호를 제거할 수 있습니다.

엔터프라이즈 보고서

CA Access Control 엔터프라이즈 관리 보고 옵션을 사용하면 중앙 위치에서 각 PUPM 끝점 및 관리되는 장치의 보안 상태를 볼 수 있습니다. 끝점 및 관리되는 장치로부터 데이터의 수집은 예약하거나 필요할 때 수행할 수 있습니다. 어떤 사용자가 어떤 리소스에 액세스할 수 있는 권한이 있는지 확인하기 위해 각 끝점에 일일이 연결할 필요가 없습니다.

CA Access Control for Virtual Environments 보고 서비스는 한 번 설치되면 각 끝점에서 데이터를 수집하여 중앙 서버에 보고하기 위해 독립적으로 작동하며 사용자가 수동 작업을 할 필요 없이 끝점 상태를 계속 보고합니다. 즉 수집 서버가 가동되고 있는지 또는 중지되었는지에 관계없이 각 끝점에서 해당 상태를 보고합니다.

CA Access Control 엔터프라이즈 관리에는 즉시 사용할 수 있도록 각 끝점에 대한 일련의 정보를 표시하는 미리 정의된 보고서가 포함되어 있습니다. 또한 기존 보고서를 사용자 지정하여 원하는 정보를 수록하는 새 보고서를 만들 수 있습니다.

제 2 장: CA Access Control 엔터프라이즈 관리 관리

이 섹션은 다음 항목을 포함하고 있습니다.

관리 범위 지정

CA Access Control 엔터프라이즈 관리에서는 관리 및 권한 있는 액세스 역할을 할당하여 사용자 및 관리자에게 사용 권한을 할당합니다. 역할은 CA Access Control 엔터프라이즈 관리의 응용 프로그램 기능에 해당하는 작업을 포함하고 있습니다.

역할은 사용함으로써 사용 권한을 쉽게 관리할 수 있습니다. 사용자에게 수행할 각 작업을 할당하지 않고 대신 사용자에게 역할을 할당할 수 있습니다. 사용자는 자신의 할당된 역할에 있는 모든 작업을 수행할 수 있습니다. 그런 다음 작업을 추가하여 역할을 수정할 수 있습니다. 그러면 이 역할이 있는 모든 사용자는 이제 새 작업을 수행할 수 있게 됩니다. 역할에서 하나의 작업을 제거하면 해당 사용자는 더 이상 이 작업을 수행할 수 없습니다.

사용자가 CA Access Control 엔터프라이즈 관리에 로그인하면 자신의 역할에 해당하는 탭을 보게 됩니다. 사용자는 자신의 역할에 할당된 탭 및 작업만 볼 수 있습니다.

하나의 사용자가 모든 작업을 수행하는 것을 방지하려면 다른 여러 사용자에게 다른 역할을 할당할 수 있습니다. 이렇게 하면 회사의 권한 분리 원칙을 충족시키는 데 도움이 됩니다. 하지만 한 사용자에게 여러 역할을 할당할 수 있습니다.

CA Access Control 엔터프라이즈 관리의 관리 역할

CA Access Control 엔터프라이즈 관리의 미리 정의된 관리 역할은 필요에 따라 회사의 관리자에게 할당할 수 있는 기본 관리 역할 세트를 제공합니다. CA Access Control 엔터프라이즈 관리에는 다음과 같은 즉시 사용 가능한 관리 역할이 기본적으로 포함되어 있습니다.

- **CA Access Control 호스트 관리자** - 관리되는 장치 및 논리적 보안 그룹을 정의합니다.

  CA Access Control 호스트 관리자는 관리되는 장치 및 보안 그룹을 만들고, 장치를 보안 그룹에 할당하고, 그룹을 수정할 수 있습니다. CA Access Control 호스트 관리자는 정책을 정의하거나 배포할 수는 없지만 월드 뷰를 사용하여 정책을 볼 수 있습니다.

- **CA Access Control 정책 배포자** - 환경 내에서 정책을 배포합니다.

  CA Access Control 정책 배포자는 호스트 및 호스트 그룹에 정책을 할당하고, 정책을 다운그레이드하고, 호스트 구성을 다시 설정합니다. CA Access Control 정책 배포자는 배포 감사에 액세스할 수 있습니다. 이들은 정책과 호스트를 볼 수 있지만 정의할 수는 없습니다. 이들은 월드 뷰에 액세스할 수 있습니다.

- **CA Access Control 정책 관리자** - 정책을 만듭니다.

  CA Access Control 정책 관리자는 정책을 만들고, 수정하고, 보고, 삭제합니다. 이들은 호스트 또는 호스트 그룹에 정책을 배포할 수 없지만 정책을 보고 월드 뷰에 액세스할 수 있습니다.

- **CA Access Control 사용자 관리자** - CA Access Control 엔터프라이즈 관리의 사용자 및 그룹을 관리합니다. 이들은 또한 사용자에게 CA Access Control 엔터프라이즈 관리 역할을 할당할 수도 있습니다.

  참고: CA Access Control 사용자 관리자는 새 관리 역할을 만들 수 없습니다. 시스템 관리자만 새 관리 역할을 만들 수 있습니다.

- **시스템 관리자** - CA Access Control 엔터프라이즈 관리를 관리합니다.

  CA Access Control 엔터프라이즈 관리에서 모든 작업을 수행하고, 만들고, 관리할 수 있습니다.

  회사에서 실제 관리 역할을 정의하는 구현 단계와 비상 상황에 이 역할을 사용하십시오. 이 역할은 최소 인원(가급적 한 사람)에게 할당하고 이러한 사용자의 작업을 긴밀히 모니터링하는 것이 좋습니다.

- **보고** - 영어 보고서를 관리합니다. 이 역할이 있는 사용자는 보고서를 예약하고 볼 수 있습니다.

- **CA Enterprise Log Manager 사용자** - CA Enterprise Log Manager 보고서를 검토합니다. 이 역할이 있는 사용자는 CA Enterprise Log Manager 보고서를 볼 수 있습니다.
- **CA Enterprise Log Manager 관리** - CA Enterprise Log Manager 보고서를 관리합니다. 이 역할이 있는 사용자는 CA Access Control 엔터프라이즈 관리에서 CA Enterprise Log Manager 보고서를 관리하고 CA Enterprise Log Manager 서버에 대한 연결을 관리할 수 있습니다.
- **위임 관리자** - 작업 항목을 위임합니다. 이 역할이 있는 사용자는 작업 항목을 사용자에게 위임할 수 있습니다.
- **자체 관리자** - 자신의 사용자 계정을 관리합니다. 이 역할이 있는 사용자는 자산의 계정에서 관리 작업을 수행할 수 있습니다. 이 사용자는 계정 암호를 변경하고, 자신의 사용자 프로필을 수정하고, 자신의 할당된 역할, 제출된 작업, 승인을 기다리는 항목을 볼 수 있습니다.

  참고: 기본적으로 시스템 모든 사용자에게는 자체 관리자 역할이 할당됩니다.

관리자 역할 만들기

CA Access Control 엔터프라이즈 관리에 있는 미리 정의된 관리 역할이 조직 요구 사항에 적합하지 않은 경우 새 역할을 만들 수 있습니다.

관리자 역할을 만들려면

1. CA Access Control 엔터프라이즈 관리에서 다음을 수행합니다.
   a. "사용자 및 그룹"을 클릭합니다.
   b. "역할" 하위 탭을 클릭합니다.
   c. 작업 메뉴에서 왼쪽에 있는 "관리 역할" 트리를 확장합니다.

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

   "관리 역할 만들기: 관리 역할 선택" 페이지가 나타납니다.

3. (선택 사항) 다음과 같이 새 관리 역할을 만들 때 복사하여 사용할 기존 관리 역할을 선택합니다.
   a. "역할 복사본 만들기"를 선택합니다.
   b. 검색 특성을 선택하고 필터 값을 입력한 다음 "검색"을 클릭합니다.

      필터 조건에 일치하는 관리 역할의 목록이 나타납니다.
   c. 새 관리 역할을 만들 때 기초로 사용할 개체를 선택합니다.
4. "확인"을 클릭합니다.

   "관리 역할 만들기" 작업 페이지가 나타납니다. 기존 개체에서 관리 역할을 만든 경우 대화 상자 필드에는 기존 개체에서 가져온 값이 자동으로 입력됩니다.
5. 대화 상자의 "프로필" 탭에서 다음 필드를 완성합니다.

   이름

   역할의 이름을 정의합니다.

   설명

   역할에 대한 설명합니다.

   사용

   역할이 사용자 및 그룹에 할당될 수 있는지 여부를 지정합니다.
6. 다음과 같이 역할에 작업을 추가합니다.
   a. "작업" 탭을 클릭합니다.
   b. (선택 사항) "필터" 작업 드롭다운 목록에서 작업 범주를 선택합니다.

      이 범주의 작업이 로드됩니다.

      참고: 작업 범주는 이 범주의 작업이 CA Access Control 엔터프라이즈 관리에 나타나는 탭과 일치합니다.
   c. "작업 추가" 드롭다운 목록에서 작업을 선택합니다.

      작업이 역할에 추가됩니다.
   d. b 에서 c 단계를 반복하여 역할에 작업을 더 추가합니다.
7. 구성원 및 범위 규칙을 추가합니다 (페이지 22).
8. "제출"을 클릭합니다.

   이렇게 하면 역할이 만들어집니다.

권한 있는 액세스 역할

CA Access Control 엔터프라이즈 관리의 권한 있는 액세스 역할은 필요에 따라 회사의 관리자 및 사용자에게 할당할 수 있는 기본 규칙 세트를 제공합니다. CA Access Control 엔터프라이즈 관리에는 다음과 같은 즉시 사용 가능한 권한 있는 액세스 역할이 기본적으로 포함되어 있습니다.

- **Break Glass** - 이 역할이 있는 사용자는 Break Glass 권한 있는 계정 암호 체크 아웃을 시작할 수 있습니다. Break Glass 체크 아웃을 사용하면 사용자에게 액세스 권한이 없는 끝점에 즉시 액세스할 수 있습니다. 이 역할은 기본적으로 CA Access Control 엔터프라이즈 관리의 모든 사용자에게 할당됩니다.
- **끝점 권한 있는 액세스 규칙** - 이 역할이 있는 사용자는 지정된 끝점 유형에서 권한 있는 액세스 작업을 수행할 수 있습니다. 새 끝점 유형을 처음 정의할 때 CA Access Control 은 해당 끝점 권한 있는 액세스 역할을 만듭니다. 예를 들어, CA Access Control 엔터프라이즈 관리에 처음 Windows 끝점을 만들면 CA Access Control 이 Windows Agentless Connection 끝점 권한 있는 액세스 역할을 만듭니다.
- **권한 있는 계정 요청** - 이 역할이 있는 사용자는 권한 있는 계정 암호에 대한 요청을 제출 또는 삭제할 수 있습니다. 이 역할은 기본적으로 CA Access Control 엔터프라이즈 관리의 모든 사용자에게 할당됩니다.
- **PUPM 승인자** - 이 역할이 있는 사용자는 CA Access Control 엔터프라이즈 관리 사용자가 제출한 권한 있는 액세스 요청에 응답할 수 있습니다. 이 역할은 기본적으로 CA Access Control 엔터프라이즈 관리의 모든 사용자에게 할당됩니다.
- **PUPM 감사 관리자** - 이 역할이 있는 사용자는 권한 있는 계정 활동을 감사하고 CA Enterprise Log Manager 감사 수집 매개 변수를 관리할 수 있습니다.
- **PUPM 정책 관리자** - 이 역할이 있는 사용자는 역할 구성원과 구성원 정책을 관리할 수 있고, 역할 소유자를 할당할 수 있고, 역할을 생성 및 삭제할 수 있습니다.
- **PUPM 대상 시스템 관리자** - 이 역할이 있는 사용자는 암호 정책 및 권한 있는 계정을 관리할 수 있고, 끝점에서 권한 있는 계정을 검색하기 위해 권한 있는 계정 검색 마법사를 실행할 수 있습니다.
- **PUPM 사용자** - 이 역할이 있는 사용자는 사용이 허가된 권한 있는 계정 암호를 체크 인 및 체크 아웃할 수 있습니다. 이 역할은 기본적으로 CA Access Control 엔터프라이즈 관리의 모든 사용자에게 할당됩니다.

- **PUPM 사용자 관리자** - 이 역할이 있는 사용자는 CA Access Control 엔터프라이즈 관리 사용자, 그룹, 암호 정책을 관리하고 사용자의 작업 항목을 관리할 수 있습니다.

다음에 주의하십시오.

- 권한 있는 계정 요청에 응답하려면 사용자에게 PUPM 승인자 역할이 있어야 하며 요청하는 사용자의 관리자여야 합니다.
- 사용자에게 Break Glass, 권한 있는 계정 요청 또는 PUPM 사용자 역할이 있지만 끝점 권한 있는 액세스 역할이 없는 경우 이 사용자는 어떠한 끝점에도 액세스할 수 없습니다. 결과적으로 이 사용자는 어떠한 작업도 수행 수 없게 됩니다.
- 사용자에게 끝점 권한 있는 액세스 역할이 있지만 다른 역할이 없는 경우 이 사용자는 어떠한 작업도 수행할 수 없습니다.

권한 있는 액세스 역할 만들기

권한 있는 액세스 역할은 역할 구성원, 관리자, 소유자가 PUPM 을 사용할 때 수행할 수 있는 작업(예: 권한 있는 계정 체크 인 및 체크 아웃)를 정의합니다. CA Access Control 엔터프라이즈 관리에 있는 미리 정의된 권한 있는 액세스 역할이 조직 요구 사항에 적합하지 않은 경우 새 역할을 만들 수 있습니다.

권한 있는 액세스 역할을 만들려면

1. CA Access Control 엔터프라이즈 관리에서 다음을 수행합니다.
   a. "사용자 및 그룹"을 클릭합니다.
   b. "역할" 하위 탭을 클릭합니다.
   c. 작업 메뉴에서 왼쪽에 있는 "권한 있는 액세스 역할" 트리를 확장합니다.

      사용 가능한 작업 목록에 "권한 있는 액세스 역할 만들기" 작업이 나타납니다.
2. "권한 있는 액세스 역할 만들기"를 클릭합니다.

   "역할 만들기: 권한 있는 액세스 역할 선택" 페이지가 나타납니다.

3. (선택 사항) 다음과 같이 새 역할을 만들 때 복사하여 사용할 기존 권한 있는 액세스 역할을 선택합니다.
   a. "역할 복사본 만들기"를 선택합니다.
   b. 검색 특성을 선택하고 필터 값을 입력한 다음 "검색"을 클릭합니다.

      필터 조건에 일치하는 권한 있는 액세스 역할의 목록이 나타납니다.
   c. 새로운 권한 있는 액세스 역할을 만들 때 기초로 사용할 개체를 선택합니다.
4. "확인"을 클릭합니다.

   "관리 역할 만들기" 작업 페이지가 나타납니다. 기존 개체에서 관리 역할을 만든 경우 대화 상자 필드에는 기존 개체에서 가져온 값이 자동으로 입력됩니다.
5. 대화 상자의 "프로필" 탭에서 다음 필드를 완성합니다.

   이름

   역할의 이름을 정의합니다.

   설명

   역할에 대한 설명합니다.

   사용

   역할이 사용자 및 그룹에 할당될 수 있는지 여부를 지정합니다.
6. 다음과 같이 역할에 작업을 추가합니다.
   a. "작업" 탭을 클릭합니다.
   b. (선택 사항) "필터" 작업 드롭다운 목록에서 작업 범주를 선택합니다.

      이 범주의 작업이 로드됩니다.

      참고: 작업 범주는 이 범주의 작업이 CA Access Control 엔터프라이즈 관리에 나타나는 탭과 일치합니다.
   c. "작업 추가" 드롭다운 목록에서 작업을 선택합니다.

      작업이 역할에 추가됩니다.
   d. b 에서 c 단계를 반복하여 역할에 작업을 더 추가합니다.
7. 구성원 및 범위 규칙을 추가합니다 (페이지 22).
8. "제출"을 클릭합니다.

   이렇게 하면 역할이 만들어집니다.

사용자에게 역할을 할당하는 방법

다음 방법을 사용하여 사용자에게 역할을 할당할 수 있습니다:

- "역할 구성원/관리자 수정" 작업을 사용하여 역할에서 여러 사용자를 추가 또는 제거할 수 있습니다.
- "사용자 수정" 작업의 "권한 있는 액세스 역할" 탭 또는 "관리 역할" 탭을 사용하여 한 사용자에 대해 역할을 추가 또는 제거할 수 있습니다.
- "권한 있는 액세스 역할 수정" 탭 또는 "관리 역할 수정" 작업에 있는 "구성원" 탭을 사용하여 역할에 대한 구성원 정책을 수정합니다.

사용자를 관리 역할에 추가하는 방법

관리 역할을 만든 다음에는 이 역할에 구성원과 관리자를 추가할 수 있습니다. 역할의 구성원인 사용자는 해당 역할에 부여된 권한을 할당합니다. 다음 단계는 역할에 구성원을 추가하기 위한 사전 요구 사항입니다.

1. 이 규칙의 구성원을 정의하기 위해 관리 역할 구성원 정책 정의를 수정합니다.

   다른 역할의 구성원인 사용자를 수정하는 역할에 추가하도록 허용하는 역할 구성원 정책을 수정합니다.

   예: *where Logon Name = "Administrator" or Admin roles = "SystemManager"*

2. 관리자(administrator)가 이 역할에서 구성원을 추가 또는 제거할 수 있는지 확인합니다.
3. 이 역할에서 사용자가 추가 또는 제거될 때 발생하는 동작을 정의합니다.

   예: *Add SystemManager to Admin Roles, Remove SystemManager from Admin Roles*.

4. 사용자를 관리 규칙에 있는 이 역할에 관리자로 추가하고 사용자에게 관리자 권한을 할당하기 위해 관리 정책을 수정합니다.

   역할 관리자로 할당한 사용자가 이 역할에 구성원을 추가하도록 권한 부여됩니다.

   이제 이 역할에 구성원을 추가할 수 있습니다.

구성원 및 범위 규칙 추가

역할의 프로필과 작업을 정의한 다음에는 구성원, 관리자, 소유자를 추가합니다.

구성원 및 범위 규칙을 추가하려면

1. "구성원" 탭을 클릭한 후 다음 중 하나를 수행합니다.
   a. "추가"를 클릭합니다.
   b. 구성원 정책 (페이지 24)에 대한 구성원 규칙과 범위 규칙을 지정한 다음 "확인"을 클릭합니다.
   c. (선택 사항) 관리자가 이 역할의 구성원을 추가 및 제거할 수 있도록 선택하고 작업 추가 및 작업 제거 (페이지 24)를 지정합니다.

   역할의 구성원 정책이 만들어집니다.
2. "관리자" 탭을 클릭한 후 다음 중 하나를 수행합니다.
   a. "추가"를 클릭합니다.
   b. 관리 규칙과 범위 규칙을 지정하고 관리 정책 (페이지 25)에 대한 관리자 권한을 지정한 다음 "확인"을 클릭합니다.
   c. (선택 사항) 관리자가 이 규칙의 관리자를 추가 및 제거할 수 있도록 선택하고 작업 추가 및 작업 제거 (페이지 24)를 지정합니다.

   역할의 관리 정책이 만들어집니다.
3. "소유자" 탭을 클릭한 다음 "추가"를 클릭하고 소유자 역할 (페이지 25)을 지정한 다음 "확인"을 클릭합니다.

   정책의 소유자 규칙이 만들어집니다.

구성원 정책

*구성원 정책*은 역할에서 작업을 수행할 수 있는 사용자를 정의합니다. 구성원 정책에는 다음이 포함되어 있습니다.

- **구성원 규칙** - 역할을 수행할 수 있는 사용자를 정의합니다.
- **범위 규칙** - 사용자가 관리할 수 있는 개체를 정의합니다.

예를 들어, 관리 역할, 연결, 권한 있는 계정, 정책은 모두 개체입니다. 범위 규칙에 많은 다른 개체를 지정할 수 있습니다. 각 구성원 정책에는 둘 이상의 구성원 규칙이 있을 수 있으며 각 구성원 규칙에는 둘 이상의 범위 규칙이 있을 수 있습니다.

예: 뉴욕 CA Access Control 호스트 관리자의 구성원 정책

Don Hailey 는 Forward, Inc 의 IT 관리자로서 시스템 관리자 관리자 역할을 가지고 있습니다. Don 은 뉴욕 사무소에서 CA Access Control 호스트 관리자 관리 역할이 있는 직원이 Forward, Inc 뉴욕 사무소에 있는 호스트 및 호스트 그룹만 관리하는 관리 역할을 만들려고 합니다. 모든 뉴욕 직원들은 NY 직원 그룹의 구성원이며 뉴욕의 모든 호스트 및 호스트 그룹의 이름은 NY 라는 문자로 시작합니다.

Don 이 다음과 같이 구성원 정책을 작성합니다. 구성원 정책에는 두 개의 구성원 규칙이 포함되어 있습니다. 첫 번째 구성원 규칙에는 범위 규칙이 없습니다. 두 번째 구성원 규칙에 다음과 같은 두 개의 범위 규칙이 포함되어 있습니다.

- 구성원 규칙 1 - 관리자 역할에 "AC 호스트 관리자"가 포함됩니다.
- 구성원 규칙 2 - "NY 직원" 그룹의 구성원인 사용자. 범위 규칙 - 이름이 "NY"로 시작하는 호스트 및 이름이 "NY"로 시작하는 호스트 그룹

추가 및 제거 동작

관리자 역할의 관리자가 사용자를 해당 역할에 할당하거나 해당 역할에서 할당 취소할 수 있도록 지정하는 경우 관리자 역할에 대한 추가 및 제거 동작을 지정해야 합니다.

추가 및 제거 동작에는 다음이 포함됩니다.

- **추가 동작**—사용자가 역할의 구성원 규칙 중 하나에 포함된 기준을 충족해야 합니다.
- **제거 동작**—사용자가 역할의 구성원 규칙 중 하나에 포함된 기준을 더 이상 충족하지 않아야 합니다.

관리자 정책

*관리자 정책*은 관리자 역할의 관리자인 사용자를 지정합니다. 관리자 역할 관리자는 관리자 역할의 구성원 정책을 관리하고, 사용자 및 그룹을 관리자 역할에 추가하거나 관리자 역할에서 제거합니다.

관리자 역할에는 다음이 포함되어 있습니다.

- **관리자 규칙**—역할의 관리자인 사용자를 정의합니다.
- **범위 규칙**—관리자가 관리할 수 있는 사용자를 정의합니다.
- **관리자의 권한**—관리자가 해당 관리자 역할의 구성원 및 관리자를 관리할 수 있는지 여부를 지정합니다.

역할 소유자

역할 소유자는 작업을 관리자 역할에 추가하거나 관리자 역할에서 제거합니다. 하나의 소유자 역할만 정의할 수 있지만 소유자 규칙 내에 있는 다른 그룹의 구성원을 지정할 수 있습니다.

관리 작업 만들기

CA Access Control 엔터프라이즈 관리에 있는 미리 정의된 관리 작업이 조직 요구 사항에 적합하지 않은 경우 새 관리 작업을 만들 수 있습니다.

관리 작업을 만들려면

1. "사용자 및 그룹" 탭을 선택하고 "작업" 링크를 선택한 다음 "관리 작업 만들기"를 클릭합니다.

   "관리 작업 만들기: 관리 작업 선택" 페이지가 나타납니다.

2. 새 관리 작업을 만들도록 선택한 다음 "확인"을 클릭합니다.

   "관리 작업 만들기" 페이지의 "프로필" 탭이 나타납니다.

   참고: 기존 관리 작업의 복사본을 만들려면 관리 작업의 복사본을 만들도록 선택하고, 복사할 관리 작업을 검색하고, 관리 작업을 선택한 다음 "확인"을 클릭합니다.

3. 작업 이름과 설명을 입력합니다. 필드에 커서를 가져가면 태그 필드에 이름이 표시됩니다.
4. 메뉴의 작업 목록에서 작업의 위치를 선택합니다.
5. 이 작업이 속한 범주를 선택합니다.
6. (선택 사항) 최대 3 개까지 작업의 순서 및 범주 이름을 선택합니다.
7. 이 작업이 속한 주 개체를 선택합니다. 주 개체는 이 작업에 대한 가장 높은 범주입니다.
8. 작업과 연계할 동작을 선택합니다.
9. 사용자와 계정을 작업과 동기화할지 여부를 선택합니다.
10. 다음 옵션 중 하나를 선택합니다.

    메뉴에서 숨기기

    작업을 표시하지 않습니다.

    공용 작업

    모든 사용자가 작업을 사용할 수 있도록 선택합니다.

    감사 사용

    이 작업에 대해 감사 이벤트 로깅을 사용하도록 선택합니다.

    작업흐름 사용

    작업흐름을 사용하도록 설정합니다.

웹 서비스 사용

웹 서비스를 사용하여 이 작업에 액세스할 수 있도록 선택합니다.

워크플로 프로세스

작업과 연계할 작업흐름 프로세스를 선택합니다.

11. 작업 우선 순위를 선택합니다.
12. "제출"을 선택합니다.

    CA Access Control 엔터프라이즈 관리가 관리 작업을 만듭니다.

추가 정보:

검색 화면 추가 (페이지 27)
탭 추가 (페이지 28)
필드, 이벤트, 역할 사용 구성 (페이지 28)

검색 화면 추가

이 작업과 연계할 검색 화면을 선택합니다. 이 탭에서는 이 작업에서 기존 검색 화면을 사용하거나, 정보를 표시하고 이 작업에 고유한 검색 옵션을 제공하는 새 검색 화면을 만들 수 있습니다.

검색 화면을 추가하려면

1. 찾아보기 단추를 클릭하여 기존 검색 화면을 찾거나 새 검색 화면을 만듭니다.

   참고: 기존 검색 화면의 복사본을 만들려면 다른 작업에서 범위를 복사하고, 복사할 관리 작업을 검색하고, 관리 작업을 선택한 다음 "확인"을 클릭합니다.
2. "새로 만들기"를 선택하여 새 검색 화면을 만듭니다.
3. 만들 검색 화면의 유형을 선택합니다.
4. 필요한 정보를 입력한 다음 "확인"을 클릭합니다.

   작업에 새 검색 화면이 추가됩니다.

탭 추가

이 작업에 사용할 탭 컨트롤러를 선택하고 작업에 표시될 탭을 선택하려면 탭 화면을 사용하십시오.

탭을 추가하려면

1. 이 작업에 사용할 탭 컨트롤러를 선택합니다.

   참고: 기존 탭 정의의 복사본을 만들려면 다른 작업에서 탭을 복사하도록 선택하고, 복사할 관리 작업을 검색하고, 관리 작업을 선택한 다음 "확인"을 클릭합니다.

2. 메뉴에서 이 작업에 표시될 탭을 선택합니다.
3. "제출"을 클릭합니다.

   CA Access Control 엔터프라이즈 관리가 해당 탭을 새 작업에 추가합니다.

필드, 이벤트, 역할 사용 구성

필드, 이벤트, 역할 사용 탭은 이 작업이 액세스하는 필드, 작업에 연결된 이벤트, 이 작업을 볼 수 있는 사용자 역할과 관련된 정보를 표시합니다. 이 필드에 표시된 정보는 변경할 수 없습니다.

설정을 변경하여 이 탭에 표시되는 정보를 변경할 수 있습니다. 예를 들어, 이 작업이 표시되는 관리 역할을 변경하려면 이 작업을 포함 또는 제외하도록 관리 역할 설정을 수정하십시오.

사용자, 그룹, 관리 역할

사용자를 만들 때 하나 이상의 *관리 역할* 또는 *권한 있는 액세스 역할*을 할당합니다. 관리자 역할에는 CA Access Control 엔터프라이즈 관리의 응용 프로그램 기능에 해당하는 작업이 포함되어 있습니다. 관리자 역할을 사용자에게 할당하면 이 사용자가 관리자 역할에 포함된 작업을 수행할 수 있습니다. 사용자는 이러한 작업을 통해 정책 작성, 정책 배포, 호스트 그룹 작성 및 기타 사용자 관리 등 CA Access Control 기능을 수행할 수 있습니다.

권한 있는 액세스 역할은 관리되는 끝점에서 권한 있는 계정 관리에 해당하는 작업을 정의합니다. 권한 있는 액세스 역할을 사용자에게 할당하면 이 사용자는 권한 있는 계정 암호 검사와 같은 권한 있는 계정 관리 작업을 수행할 수 있습니다.

더 쉽게 관리할 수 있도록 사용자 그룹을 작성하고 관리자 역할을 그룹에 할당할 수 있습니다. 그러면 그룹의 각 사용자가 해당 관리 역할의 모든 작업을 수행할 수 있습니다.

추가 정보:

사용자 만들기 (페이지 31)
그룹 유형 (페이지 35)

Active Directory 제한

사용자 저장소로 Active Directory 를 사용하는 경우 CA Access Control 엔터프라이즈 관리에서 사용자 및 그룹을 만들거나 삭제할 수 없습니다. 인터페이스에서 다음 작업을 볼 수 없으며 이러한 작업을 관리 역할 또는 권한 있는 액세스 역할에 할당할 수 없습니다.

- 사용자 만들기
- 사용자 삭제
- 역할 구성원/관리자 수정
- 그룹 작성
- 그룹 삭제

Active Directory 사용자에 관리 역할을 할당할 때 CA Access Control 엔터프라이즈 관리는 사용자 프로필을 수정하고 주소 필드에 이 사용자에게 할당된 관리 역할을 나타냅니다.

참고: 사용자 DN: 매개 변수에서 사용자를 읽기 전용 권한으로 정의하도록 선택할 수 있습니다. 하지만 읽기 전용 권한 가진 사용자를 정의하면 CA Access Control 엔터프라이즈 관리의 사용자에게 관리자 역할이나 권한 있는 액세스 역할을 할당할 수 없습니다. 대신, Active Directory 그룹을 가리키도록 각 역할에 대한 구성원 정책을 수정합니다.)

사용자 만들기

사용자는 CA Access Control 엔터프라이즈 관리에서 작업을 수행합니다. CA Access Control 엔터프라이즈 관리를 설치할 때 시스템 관리자 역할이 있는 사용자를 만듭니다. CA Access Control 엔터프라이즈 관리를 시작하여 권한 분리를 시행할 때 추가 사용자를 만드십시오.

참고: 사용자 저장소로 Active Directory 를 사용하는 경우 CA Access Control 엔터프라이즈 관리에 사용자를 만들 수 없습니다.

사용자를 만들려면

1. CA Access Control 엔터프라이즈 관리에서 "사용자 및 그룹"을 클릭합니다.

   사용 가능한 작업 목록에 "사용자 만들기" 작업이 나타납니다.

2. "사용자 만들기"를 클릭합니다.

   "사용자 만들기: 사용자 선택" 창이 나타납니다.

3. (선택 사항) 다음과 같이 새 사용자를 만들 때 복사하여 사용할 기존 사용자를 선택합니다.

   a. 사용자의 복사본 만들기를 선택합니다.

   b. 검색 특성을 선택하고 필터 값을 입력한 다음 "검색"을 클릭합니다.

      필터 조건에 일치하는 사용자의 목록이 표시됩니다.

   c. 새 사용자를 만들 때 기초로 사용할 개체를 선택합니다.

4. "확인"을 클릭합니다.

   "사용자 만들기" 작업 페이지가 나타납니다. 기존 개체에서 사용자를 만든 경우 기존 개체의 값이 대화 상자 필드에 미리 입력됩니다.

5. "프로필" 탭에서 이 필드를 완성합니다. 다음 필드는 자동으로 채워지지 않습니다.

   사용자 ID

   CA Access Control 엔터프라이즈 관리에서 사용자를 식별하는 문자열을 정의합니다. 이 문자열은 로그인하는 데 사용하는 사용자의 이름입니다.

   암호를 반드시 변경

   사용자가 처음 로그인할 때 암호를 반드시 변경하도록 지정합니다.

   사용

   사용자가 CA Access Control 엔터프라이즈 관리에 로그인할 수 있는지 여부를 지정합니다.

6. (선택 사항) "관리 역할"을 클릭하여 다음과 같이 사용자에게 관리 역할을 할당합니다.

   a. 관리 역할 추가를 클릭합니다.

      "관리 역할 선택" 섹션이 나타납니다.

   b. 필터 값을 입력한 다음 "검색"을 클릭합니다.

      필터 조건에 일치하는 역할의 목록이 표시됩니다.

   c. 사용자에게 할당할 관리 역할을 선택한 다음 "선택"을 클릭합니다.

   사용자에게 관리 역할이 할당됩니다.

7. (선택 사항) "권한 있는 액세스 역할" 탭을 클릭하여 다음과 같이 사용자에게 권한 있는 액세스 역할을 할당합니다.

   a. 권한 있는 액세스 역할 추가를 클릭합니다.

      "권한 있는 액세스 역할 선택" 섹션이 나타납니다.

   b. 필터 값을 입력한 다음 "검색"을 클릭합니다.

      필터 조건에 일치하는 역할의 목록이 표시됩니다.

   c. 사용자에게 할당할 권한 있는 액세스 역할을 선택한 다음 "선택"을 클릭합니다.

   사용자에게 권한 있는 액세스 역할이 할당됩니다.

8. (선택 사항) "그룹" 탭을 클릭하여 다음과 같이 사용자를 그룹에 추가합니다.
   a. 그룹 추가를 클릭합니다.

      "그룹 선택" 섹션이 나타납니다.

   b. 필터 값을 입력한 다음 "검색"을 클릭합니다.

      필터 조건에 일치하는 그룹의 목록이 표시됩니다.

   c. 사용자에게 할당할 그룹을 선택한 다음 "선택"을 클릭합니다.

   그룹에 사용자가 추가됩니다.
9. "제출"을 클릭합니다.

   사용자가 만들어집니다.

사용자 암호 다시 설정

여러 번 로그인 시도가 실패하여 사용자 계정이 잠기거나 암호를 잊어버린 경우 사용자 암호를 다시 설정합니다.

사용자 암호를 다시 설정하려면

1. CA Access Control 엔터프라이즈 관리에서 "사용자 및 그룹"을 클릭합니다.

   사용 가능한 작업의 목록에 "사용자 암호 다시 설정"이 표시됩니다.
2. "사용자 암호 다시 설정"을 클릭합니다.

   "사용자 암호 다시 설정" 검색 페이지가 열립니다.
3. 검색 쿼리를 입력한 다음 "검색"을 클릭합니다.

   검색 조건에 따라 쿼리 결과가 표시됩니다.
4. 사용자 계정을 선택하고 "선택"을 클릭합니다.

   암호 다시 설정 창이 열립니다.
5. "암호 확인" 필드에 계정 암호를 입력합니다.
6. (선택 사항) "암호를 반드시 변경" 옵션을 선택합니다.
7. "제출"을 클릭합니다.

   CA Access Control 엔터프라이즈 관리가 사용자 암호를 다시 설정합니다.

사용자 활성화 또는 비활성화

사용자가 계정 자격 증명을 사용하여 CA Access Control 엔터프라이즈 관리에 로그인할 수 있도록 하려면 사용자를 활성화합니다. 사용자가 CA Access Control 엔터프라이즈 관리에 액세스할 수 없도록 하고 시스템에 사용자 프로필을 유지하려면 사용자 계정을 비활성화합니다.

사용자를 활성화 또는 비활성화하려면

1. CA Access Control 엔터프라이즈 관리에서 "사용자 및 그룹"을 클릭합니다.

   사용 가능한 작업 목록에 "사용자 활성화/비활성화" 작업이 나타납니다.

2. "사용자 활성화/비활성화"를 클릭합니다.

   "사용자 활성화/비활성화" 페이지가 나타납니다.

3. 검색 쿼리를 정의하고 "검색"을 클릭합니다.

   검색 쿼리에 일치하는 사용자의 목록이 표시됩니다.

4. 다음과 같이 활성화 및 비활성화할 사용자 계정을 지정합니다.
   - 계정을 비활성화할 사용자를 지웁니다.
   - 계정을 활성화할 사용자를 선택합니다.

5. 선택을 클릭합니다.

   지정한 변경 내용을 요약하는 화면이 표시됩니다.

6. "예"를 클릭하여 수정 내용을 승인합니다.

   CA Access Control 엔터프라이즈 관리는 작업을 제출하여 요청된 변경을 수행합니다.

그룹 유형

여러 유형의 그룹이나 이러한 유형의 조합을 만들 수 있습니다.

- **정적 그룹**

  대화형으로 추가된 일련의 사용자입니다.

- **동적 그룹**

  LDAP 쿼리를 충족하는 경우 그룹에 속하는 사용자입니다. 사용자 저장소로 LDAP 디렉터리가 요구됩니다.

  참고: 동적 그룹 쿼리 필드를 보려면 관련 프로필 화면을 편집하여 이 필드를 작업에 포함시켜야 합니다.

- **중첩 그룹**

  다른 그룹을 포함하는 그룹입니다. 사용자 저장소로 LDAP 디렉터리가 요구됩니다.

  참고: 사용자가 속한 정적, 동적, 중첩 그룹을 보려면 "사용자" 개체의 "그룹" 탭을 사용하십시오. 이 탭은 "사용자 보기" 및 "사용자 수정" 작업에 있습니다.

정적 또는 동적 그룹 만들기

사용자 모음을 정적 그룹으로 연결할 수 있습니다. 그룹의 구성원 자격 목록에서 사용자를 추가하거나 제거하여 그룹을 관리합니다. 그룹의 구성원 자격을 보려면 "그룹 보기" 또는 "그룹 수정" 작업에서 "구성원 자격" 탭을 사용하십시오.

CA Access Control 엔터프라이즈 관리를 사용하여 LDAP 필터 쿼리를 정의하는 방법으로 동적 그룹을 만들면 런타임에 그룹 구성원 자격을 파악할 수 있습니다.

참고: "구성원 자격" 탭에는 명시적으로 그룹에 추가된 구성원만 표시됩니다. 사용자 저장소로 Active Directory 를 사용하는 경우 CA Access Control 엔터프라이즈 관리에 그룹을 만들 수 없습니다.

정적 또는 동적 그룹을 만들려면

1. 그룹 관리 권한이 있는 사용자로 CA Access Control 엔터프라이즈 관리에 로그인합니다.
2. "그룹", "그룹 만들기"를 차례로 선택합니다.

   그룹 만들기 검색 화면이 나타납니다.
3. 그룹을 만들도록 선택하고 "확인"을 클릭합니다.

   그룹 프로필 탭이 나타납니다.
4. 그룹 이름과 설명을 입력합니다.
5. "구성원 자격" 탭으로 이동합니다.

   참고: "그룹 수정" 작업이 있는 관리자만 그룹 동적 구성원 자격을 변경할 수 있습니다.
6. "사용자 추가"를 클릭합니다.

   사용자 선택 검색 창이 열립니다.
7. 검색 쿼리를 입력하고 "검색"을 클릭합니다.

   검색 조건에 따라 쿼리 결과가 반환됩니다.
8. 사용자를 선택하고 "선택"을 클릭합니다.

   "관리자" 탭으로 이동합니다.
9. "제출"을 클릭합니다.

   프로세스가 성공적으로 완료되었음을 알리는 메시지가 표시됩니다.

참고: 사용자를 그룹 관리자로 할당하는 경우 관리자가 그룹 관리에 적합한 범위가 있는 역할을 가지고 있는지 확인하십시오.

LDAP 필터 쿼리 - 동적 그룹 쿼리 매개 변수 정의

CA Access Control 엔터프라이즈 관리를 사용하여 LDAP 필터 쿼리를 정의하는 방법으로 동적 그룹을 만들면 런타임에 그룹 구성원 자격을 파악할 수 있습니다.

이 필터 쿼리의 형식은 다음과 같습니다.

LDAP:///*search_base_DN*??*search_scope*?*searchfilter*

search_base_DN

LDAP 디렉터리에서 검색을 시작하는 지점을 정의합니다. 쿼리에 기본 DN 을 지정하지 않으면 그룹 조직이 기본 DN 이 됩니다.

search_scope

검색 범위를 지정하며 다음을 포함합니다.

- **sub** - 기본 DN 수준 및 그 아래의 항목을 반환합니다.
- **one** - URL 에 지정하는 기본 DN 보다 한 수준 아래의 항목을 반환합니다.
- **base** - 검색 옵션으로 base 를 무시하고 one 을 대신 사용합니다.

one 또는 *base* 를 사용하면 기본 DN 조직의 사용자만 반환됩니다.

sub 를 사용하면 기본 DN 조직 및 트리에서 모든 하위 조직의 사용자가 모두 반환됩니다.

searchfilter

검색 범위 내의 항목에 적용할 필터를 정의합니다. 검색 필터를 입력하는 경우 다음과 같은 표준 LDAP 쿼리 구문을 사용합니다.

([*logical_operator*]*Comparison*)

logical operator

논리 연산자를 정의합니다. 다음 중 하나일 수 있습니다.

- **|** - 논리적 OR
- **&** - 논리적 AND
- **!** - 논리적 NOT

Comparison

AttributeOperatorValue 를 정의합니다.

- *Attribute* - LDAP 특성의 이름을 정의합니다.
- *Operator* - 비교 연산자를 지정합니다. 다음 중 하나: **=** (같음), **<=** (작거나 같음), **>=** (크거나 같음), **~=** (비슷함)
- *Value* - 특성 데이터의 값을 정의합니다.

예: (&(city=Boston)(state=Massachusetts))

기본값: (objectclass=*)

동적 쿼리를 만들 때 다음 사항에 주의하십시오.

- "LDAP" 접두사는 다음과 같이 소문자여야 합니다.

  ldap:///o=MyCorporation??sub?(title=Manger)

- LDAP 서버 호스트 이름이나 포트 번호를 지정할 수 없습니다. 모든 검색은 사용자의 환경에 대해 구성한 LDAP 디렉터리 내에서 수행됩니다.

예: 예제 LDAP 쿼리

샘플 LDAP 쿼리는 다음과 같습니다.

설명	쿼리
관리자인 모든 사용자	ldap:///o=MyCorporation??sub?(title=Manger)

설명	쿼리
뉴욕 서부 지사에 있는 모든 관리자	ldap:///o=MyCorporation??one?(&(title=Manager) (office=NYWest))
휴대폰이 있는 모든 기술자	ldap:///o=MyCorporation??one? (&(employeetype=technician) (mobile=*))
사원 번호가 1000 - 2000 사이인 모든 사원	ldap:///o=MyCorporation, (& (ou=employee) (employeenumber >=1000) (employeenumber <=2000))
회사에서 6 개월 이상 근무한 모든 헬프 데스크 관리자	ldap:///o=MyCorporation,(& (cn=helpdeskadmin) (DOH => 2004/04/22) **참고:** 이 쿼리를 사용하려면 사용자의 고용 날짜에 대해 DOH 특성을 만들어야 합니다.

참고: > 및 <(보다 큼 및 보다 작음) 비교는 산술적이 아니라 사전순입니다. 이러한 비교 연산자 사용에 대한 자세한 내용은 LDAP 디렉터리 서버 설명서를 참조하십시오.

그룹 구성원 수정

구성원 및 그룹을 추가 또는 제거하려면 이 옵션을 사용하십시오. 이 절차를 통해 구성원의 그룹 목록을 수정할 수 있습니다.

그룹 구성원을 수정하려면

1. 그룹 관리 권한이 있는 사용자로 CA Access Control 엔터프라이즈 관리에 로그인합니다.
2. "그룹", "그룹 구성원 수정"을 차례로 선택합니다.

   그룹 구성원 수정 화면이 나타납니다.
3. 그룹을 선택하고 "선택"을 클릭합니다.

   그룹 구성원 목록이 열립니다.

4. 구성원을 제거하려면 구성원 이름 옆의 확인란의 선택을 취소합니다.
5. 구성원을 추가하려면 "사용자 추가"를 클릭합니다.
   a. 검색 쿼리를 입력한 다음 "검색"을 클릭합니다.
      검색 조건에 따라 검색 쿼리 결과가 표시됩니다.
   b. 사용자를 선택하고 "선택"을 클릭합니다.
      사용자가 그룹 구성원으로 추가됩니다.
6. 그룹을 추가하려면 "그룹 추가" 단추를 클릭합니다.
   a. 검색 쿼리를 입력한 다음 "검색"을 클릭합니다.
      검색 조건에 따라 검색 쿼리 결과가 표시됩니다.
   b. 그룹을 선택하고 "선택"을 클릭합니다.
      그룹이 추가됩니다.
7. "제출"을 클릭합니다.
   작업이 성공적으로 완료되었음을 알리는 확인 메시지가 표시됩니다.

감사 데이터

감사 데이터는 CA Access Control 엔터프라이즈 관리 환경에서 발생하는 작업의 내역을 제공합니다. 감사 데이터의 예는 아래와 같습니다.

- 특정 기간에 대한 시스템 활동
- 특정 기간 중에 수정된 개체의 목록
- 사용자에게 할당된 역할
- 특정 사용자 계정에 대해 수행된 작업

감사 데이터는 *이벤트*에 대해 생성됩니다. 이벤트는 CA Access Control 엔터프라이즈 관리 작업에서 생성된 작업입니다. 예를 들어, "사용자 만들기" 작업은 AssignAccessRoleEvent 이벤트를 포함할 수 있습니다.

CA Access Control 엔터프라이즈 관리는 감사 데이터를 중앙 데이터베이스에 저장합니다. 감사 데이터를 CA Enterprise Log Manager 에 라우트하도록 감사 수집기를 구성할 수 있습니다..

참고: CA Enterprise Log Manager 와의 통합에 대한 자세한 내용은 *구현 안내서*를 참조하십시오.

추가 정보:

제출된 작업 검색 (페이지 41)
작업 상세 정보 보기 (페이지 45)
이벤트 상세 정보 보기 (페이지 45)
제출된 작업 정리 (페이지 46)
메시지 큐 감사 메시지를 Windows 이벤트 로그로 라우팅 (페이지 48)
메시지 큐 감사 메시지를 UNIX Syslog 로 라우팅 (페이지 50)
감사 수집기 구성 (페이지 192)

제출된 작업 검색

제출된 작업은 CA Access Control 엔터프라이즈 관리 환경의 작업에 대한 정보를 제공합니다. CA Access Control 엔터프라이즈 관리가 수행하는 작업에 대한 매우 자세한 정보를 검색하여 볼 수 있습니다. 세부 정보 화면은 각 작업과 이벤트에 대한 추가 정보를 제공합니다.

작업의 상태를 기반으로 작업을 취소하거나 다시 제출할 수 있습니다.

제출된 작업을 사용하여 시작부터 끝까지 작업의 처리를 추적할 수 있습니다.

제출한 작업을 검색하려면

1. CA Access Control 엔터프라이즈 관리에서 "시스템", "감사" 하위 탭을 차례로 클릭합니다.

   사용 가능한 작업 목록에 "제출된 작업 보기" 작업이 나타납니다.

2. "제출된 작업 보기"를 클릭합니다.

   "제출한 작업 보기" 페이지가 나타납니다.

3. 검색 조건 (페이지 42)을 지정하고, 표시할 행 수를 입력한 다음 "검색"을 클릭합니다.

   검색 조건에 맞는 작업이 표시됩니다.

제출한 작업 보기의 검색 특성

처리를 위해 제출된 작업을 검토하려면 "제출한 작업 보기"의 검색 기능을 사용할 수 있습니다. 다음 조건을 기반으로 작업을 검색할 수 있습니다.

시작자

작업을 시작한 사용자의 이름을 검색 조건으로 식별합니다. 사용자 이름을 기반으로 검색이 수행됩니다. 유효한 사용자 이름을 입력했는지 확인하려면 "유효성 검사" 단추를 사용합니다.

승인한 사람

작업 승인자의 이름을 검색 조건으로 식별합니다. 사용자 이름을 기반으로 검색이 수행됩니다. 유효한 사용자 이름을 입력했는지 확인하려면 "유효성 검사" 단추를 사용합니다.

참고: "다음에 의해 승인된 작업" 조건을 선택하여 작업을 필터링하는 경우 "승인 작업 표시" 조건도 기본적으로 활성화됩니다.

작업 이름

작업 이름을 검색 조건으로 식별합니다. 같음, 포함, 다음으로 시작 또는 다음으로 끝남과 같은 조건을 "작업 이름 위치" 필드 값과 함께 지정하여 검색을 구체화할 수 있습니다. 예를 들어, 같음 조건을 선택하고 텍스트 필드에 "사용자 만들기"를 입력하여 "작업 이름 같음 사용자 만들기"라는 검색 조건을 지정할 수 있습니다.

작업 상태

작업 상태 (페이지 44)를 검색 조건으로 식별합니다. "작업 상태", 같음, 조건을 선택하여 작업 상태를 선택할 수 있습니다. 다음 조건을 기반으로 검색을 구체화할 수 있습니다.

- 완료함
- 진행 중
- 실패
- 거부됨
- 부분 완료됨
- 취소
- 예약됨

작업 우선 순위

작업 우선 순위를 검색 조건으로 식별합니다. "작업 우선 순위", 같음, 조건을 선택하여 작업 우선 순위를 선택할 수 있습니다. 다음 조건을 기반으로 검색을 구체화할 수 있습니다.

낮음

낮은 우선 순위를 가진 작업을 검색할 수 있도록 지정합니다.

중간

중간 우선 순위를 가진 작업을 검색할 수 있도록 지정합니다.

높음

높은 우선 순위를 가진 작업을 검색할 수 있도록 지정합니다.

다음에서 수행됨

선택한 개체 인스턴스에서 수행된 작업을 식별합니다. 개체 인스턴스를 선택하지 않으면 해당 개체의 모든 인스턴스에서 수행된 작업이 표시됩니다.

참고: 이 필드는 "제출한 작업 구성" 화면의 "다음에서 수행됨 구성" 필드가 채워진 경우에만 나타납니다. 이 화면을 사용하여 "제출한 작업" 탭을 구성합니다.

날짜 범위

제출한 작업을 검색할 날짜 범위를 식별합니다. "시작 날짜" 및 "종료 날짜"를 제공해야 합니다.

제출되지 않은 작업 표시

"감사 마침" 상태의 작업을 식별합니다. 제출되지 않은 다른 작업을 시작한 작업을 식별합니다. 이 탭을 선택하면 이러한 작업이 모두 감사 및 표시됩니다.

승인 작업 표시

작업흐름의 일부로 승인되어야 하는 작업을 식별합니다.

추가 정보:

작업 상태 설명 (페이지 44)

작업 상태 설명

제출한 작업은 아래에 설명된 상태 중 하나에 있습니다. 작업 상태를 기반으로 작업 취소 또는 작업 다시 제출과 같은 동작을 수행할 수 있습니다.

참고: 작업을 취소하거나 다시 제출하려면 작업 상태를 기반으로 취소 및 다시 제출 단추를 표시하도록 "제출한 작업 보기"를 구성해야 합니다.

진행 중

다음 중 하나가 발생하는 경우에 표시됩니다.

- 작업흐름이 시작되었지만 완료되지 않았음
- 현재 작업보다 먼저 시작된 작업이 진행 중임
- 중첩된 작업이 시작되었지만 완료되지 않았음
- 주 이벤트가 시작되었지만 완료되지 않았음
- 보조 이벤트가 시작되었지만 완료되지 않았음

이 상태의 작업은 취소할 수 있습니다.

참고: 작업을 취소하면 현재 작업의 불완전한 모든 중첩된 작업과 이벤트가 취소됩니다.

취소

진행 중인 작업이나 이벤트를 취소한 경우에 표시됩니다.

거부됨

CA Access Control 엔터프라이즈 관리가 작업흐름 프로세스의 일부인 이벤트나 작업을 거부하는 경우에 표시됩니다. 거부된 작업은 다시 제출할 수 있습니다.

참고: 작업을 다시 제출하면 CA Access Control 엔터프라이즈 관리는 실패 또는 거부한 중첩 작업과 이벤트를 모두 다시 제출합니다.

부분 완료됨

이벤트나 중첩된 작업 중 일부를 취소한 경우에 표시됩니다. 부분 완료된 이벤트나 중첩된 작업은 다시 제출할 수 있습니다.

완료함

작업이 완료된 경우에 표시됩니다. 현재 작업의 중첩된 작업 및 중첩된 이벤트가 완료되면 작업이 완료됩니다.

실패

작업, 중첩된 작업 또는 현재 작업에 중첩된 이벤트가 유효하지 않은 경우에 표시됩니다. 이 상태는 작업이 실패한 경우에 표시됩니다. 실패한 작업은 다시 제출할 수 있습니다.

예약됨

작업이 이후 날짜에 실행되도록 예약된 경우에 표시됩니다. 이 상태의 작업은 취소할 수 있습니다.

작업 상세 정보 보기

CA Access Control 엔터프라이즈 관리는 제출된 작업의 상태, 중첩 작업, 작업 관련 이벤트와 같은 작업 상세 정보를 제공합니다.

제출한 작업의 상세 정보를 보려면

1. "제출된 작업 보기" 탭에서 선택한 작업 옆에 있는 오른쪽 화살표 아이콘을 클릭합니다.

   작업 상세 정보가 나타납니다.

   참고: 이벤트 및 중첩된 작업(있는 경우)이 "작업 상세 정보" 페이지에 표시됩니다. 각 작업 및 이벤트에 대해 작업 상세 정보를 볼 수 있습니다.

2. "닫기"를 클릭합니다.

   "작업 세부 정보" 탭이 닫히고 작업 목록이 포함된 "제출된 작업 보기" 탭이 CA Access Control 엔터프라이즈 관리에서 표시됩니다.

이벤트 상세 정보 보기

CA Access Control 엔터프라이즈 관리는 제출된 이벤트의 상태, 이벤트 특성, 이벤트에 대한 모든 추가 정보와 같은 이벤트 상세 정보를 제공합니다.

제출한 이벤트의 상세 정보를 보려면

1. "작업 상세 정보 보기" 페이지에서 이벤트 옆에 있는 오른쪽 화살표 아이콘을 클릭합니다.

   이벤트 상세 정보가 나타납니다.

2. "닫기"를 클릭합니다.

   "이벤트 상세 정보" 페이지가 닫힙니다.

제출된 작업 정리

CA Access Control 엔터프라이즈 관리는 PUPM 감사 데이터를 포함하여 감사 데이터를 중앙 데이터베이스에 저장합니다. 하지만 중앙 데이터베이스에 큰 감사 데이터를 저장하면 데이터베이스 성능에 영향을 줄 수 있습니다. 데이터베이스 성능을 높이려면 제출된 작업 정리 마법사를 사용하여 중앙 데이터베이스에서 제출된 작업을 제거할 수 있습니다.

중요! 제출된 작업을 삭제하면 데이터베이스에서 감사 데이터가 삭제됩니다. 데이터 손실을 방지하기 위해 정리 작업을 실행하기 전에 감사 이벤트를 CA Enterprise Log Manager 에 라우트하는 것이 좋습니다.

정리 작업은 즉시 실행하거나 주기적으로 반복하여 실행하도록 예약할 수 있습니다. 제출된 작업을 정리할 때 많은 시스템 메모리가 사용될 수 있습니다. 이 작업은 업무 시간 이후에 수행하도록 예약하는 것이 좋습니다.

제출된 작업을 정리하려면

1. CA Access Control 엔터프라이즈 관리에서 다음을 수행합니다.
   a. "시스템"을 클릭합니다.
   b. "작업" 하위 탭을 클릭합니다.
   c. "제출된 작업 정리"를 클릭합니다.

      "제출된 작업 정리: 되풀이" 페이지가 나타납니다.
2. 다음 작업 중 *하나*를 수행합니다.
   - 작업을 즉시 실행하려면 "지금 실행"을 선택하고 "다음"을 클릭합니다.

     "제출된 작업 정리: 제출된 작업 정리" 페이지가 나타납니다.
   - 되풀이 일정을 만들려면 "새 작업 예약"을 선택하고 표시되는 필드를 완성하십시오. 다음 필드는 자동으로 채워지지 않습니다.

     시간대

     엔터프라이즈 관리 서버의 시간대를 지정합니다.

     서버와 다른 시간대에 있는 경우 새 작업을 예약할 때 현재 위치의 시간대 또는 서버 시간대를 선택할 수 있습니다. 기존 작업을 수정할 때는 시간대를 변경할 수 없습니다.

주별 일정

작업이 지정된 날 또는 요일의 지정된 시간에 실행되도록 지정합니다.

17:15 같이 24시간 형식으로 시간을 지정합니다.

고급 일정

cron 식을 사용하여 작업이 실행되는 시간을 지정할 수 있습니다.

"다음"을 클릭합니다.

"제출된 작업 정리: 제출된 작업 정리" 페이지가 나타납니다.

3. 다음 필드를 완료하십시오.

최소 사용 기간

CA Access Control 엔터프라이즈 관리가 중앙 데이터베이스에서 제거하는 최종 단계(완료됨, 실패함. 거부됨, 취소됨, 중지됨)에 있는 작업에 대한 최소 사용 기간을 지정합니다.

감사 만료

(선택 사항) CA Access Control 엔터프라이즈 관리가 중앙 데이터베이스에서 제거하는 감사 상태에 있는 작업에 대한 최소 사용 기간을 지정합니다.

참고: 감사 상태에 있는 작업은 제출되지 않았습니다.

시간 제한

(선택 사항) CA Access Control 엔터프라이즈 관리가 정리 작업을 수행하는 데 걸리는 최소 시간을 지정합니다.

작업 제한

(선택 사항) CA Access Control 엔터프라이즈 관리가 중앙 데이터베이스에서 제거하는 최대 작업 수를 지정합니다.

"마침"을 클릭합니다.

CA Access Control 엔터프라이즈 관리는 지정한 시간에 중앙 데이터베이스에서 제출된 작업을 제거합니다.

메시지 큐 감사 메시지를 Windows 이벤트 로그로 라우팅

Windows 에 해당

엔터프라이즈 관리 서버를 구성하여 메시지 큐 감사 메시지를 Windows 이벤트 로그로 라우팅할 수 있습니다. 엔터프라이즈 관리 서버가 감사 로그에 감사 메시지를 기록할 때마다 해당 이벤트가 이벤트 로그로 전달됩니다.

메시지 큐 감사 메시지를 Windows 이벤트 로그로 라우팅하려면

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

   JBOSS_HOME\server\default\conf\

3. jboss-log4j.xml 파일을 엽니다.
4. 클래스에 "ENTM_NTEventLog"란 접미사를 추가합니다.

   이 접미사는 감사에 사용할 클래스와 데이터를 표시하는 방법을 지정합니다.

5. "EventLog"란 이름의 로거를 만듭니다.

   감사 메시지에 대한 입력 채널로서 접미사가 바인딩하는 로거를 지정합니다.

6. 파일을 저장한 후 닫습니다.
7. NTEventLogAppender.dll 파일을 Windows System32 디렉터리에 복사합니다.

   참고: NTEventLogAppender.dll 파일은 Apache log4j 1.2.16 번들에 있습니다. Apache log4j 1.2.16 은 Apache 로깅 서비스 웹 사이트에서 다운로드할 수 있습니다.

8. JBoss Application Server 를 시작합니다.

   엔터프라이즈 관리 서버는 이제 메시지 큐 감사 메시지를 Windows 이벤트 로그로 라우팅합니다.

예: 메시지 큐 감사 메시지를 Windows 이벤트 로그로 전달하도록 jboss-log4j.xml 파일 수정

다음 코드 조각은 메시지 큐 감사 메시지를 Windows 이벤트 로그로 라우팅하도록 구성된 jboss-log4j.xml 파일을 보여 줍니다.

```
<appender name="ENTM_NTEventLog"
                class="org.apache.log4j.nt.NTEventLogAppender">
  <param name="Source" value="CA Access Control Enterprise Management"/>
  <layout class="org.apache.log4j.SimpleLayout"/>
</appender>

<logger name="EventLog">
  <appender-ref ref="ENTM_NTEventLog"/>
</logger>
```

이 예에서 다음과 같은 변경을 수행했습니다.

- "ENTM_NTEventLog"란 이름의 새 접미사를 추가했습니다.
- "org.apache.log4j.nt.NTEventLogAppender"란 이름으로 클래스를 추가했습니다.
- 매개 변수 이름을 정의했습니다: "Source"
- 값을 정의했습니다: "CA Access Control Enterprise Management"
- 레이아웃 클래스를 정의했습니다:"org.apache.log4j.SimpleLayout"
- 로거 이름을 정의했습니다: "EventLog"
- 접미사 참조를 정의했습니다: "ENTM_NTEventLog"

메시지 큐 감사 메시지를 UNIX Syslog 로 라우팅

UNIX 에 해당

엔터프라이즈 관리 서버를 구성하여 메시지 큐 감사 메시지를 UNIX syslog 로 라우팅할 수 있습니다. 엔터프라이즈 관리 서버가 감사 로그에 감사 메시지를 기록할 때마다 해당 이벤트가 syslog 로 전달됩니다.

메시지 큐 감사 메시지를 UNIX Syslog 로 라우팅하려면

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

   JBOSS_HOME\server\default\conf\
3. jboss-log4j.xml 파일을 엽니다.
4. 클래스에 "ENTM_UNIXEventLog"란 접미사를 추가합니다.

   이 접미사는 감사에 사용할 클래스와 데이터를 표시하는 방법을 지정합니다.
5. "EventLog"란 이름의 로거를 만듭니다.

   감사 메시지에 대한 입력 채널로서 접미사가 바인딩하는 로거를 지정합니다.
6. 파일을 저장한 후 닫습니다.
7. /etc/syslog.conf 파일을 열고 syslog 가 메시지를 /var/log/messages 파일로 라우팅하는지 확인합니다.
8. /etc/sysconfig/syslog 매개 변수 파일을 열고 원격 모드 옵션이 다음 항목에 있는지 확인합니다.

   SYSLOGD_OPTIONS="-m 0-r"
9. syslog 데몬을 다시 시작합니다. 다음 명령을 실행합니다.

   /etc/rc.d/init.d/syslog restart

   syslog 데몬이 시작됩니다.
10. JBoss Application Server 를 시작합니다.

    엔터프라이즈 관리 서버는 이제 메시지 큐 감사 메시지를 UNIX syslog 로 라우팅합니다.

예: 메시지 큐 감사 메시지를 UNIX syslog 로 전달하도록 jboss-log4j.xml 파일 수정

다음 코드 조각은 LogAppender 개체가 생성된 후 jboss-log4j.xml 파일을 보여 줍니다.

```
<appender name="ENTM_UNIXSysLog"3
                class="org.apache.log4j.net.SyslogAppender">
  <param name="Facility" value="USER"/>
  <param name="FacilityPrinting" value="false"/>
  <param name="SyslogHost" value="localhost"/>
  <layout class="org.apache.log4j.PatternLayout">
    <param name="ConversionPattern" value="%p - [CA AC ENTM]: %m%n"/>
  </layout>
</appender>

<logger name="EventLog">
  <appender-ref ref="ENTM_UNIXSysLog"/>
</logger>
```

이 예에서 다음을 수행했습니다.

- 접미사를 추가했습니다:"ENTM_UNIXSysLog"
- 클래스를 만들었습니다: "org.apache.log4j.net.SyslogAppender"
- 매개 변수 이름을 정의했습니다: "Facility" and the value "USER"
- 매개 변수 이름을 정의했습니다: "FacilityPrinting". 값 "false"
- 매개 변수 이름을 정의했습니다: "SyslogHost". 값 "localhost"
- 레이아웃 클래스를 정의했습니다: "org.apache.log4j.PatternLayout"
- 매개 변수 이름을 정의했습니다: "ConversionPattern". 값: "%p - [CA AC ENTM]: %m%n"
- 로거 이름을 정의했습니다: "EventLog"
- 접미사 참조를 정의했습니다: ref="ENTM_UNIXSysLog"

전자 메일 알림

전자 메일 알림은 전자 메일 템플릿에서 생성되며 CA Access Control 엔터프라이즈 관리 사용자에게 시스템의 이벤트에 대해 알립니다. 전자 메일 알림을 사용하는 경우 CA Access Control 엔터프라이즈 관리는 다음 중 하나가 발생할 때 전자 메일 알림을 생성할 수 있습니다.

- 승인 또는 거부를 요구하는 이벤트가 보류 중인 경우
- 승인자가 이벤트를 승인하는 경우
- 승인자가 이벤트를 거부하는 경우
- 이벤트가 시작, 실패, 완료되는 경우
- CA Access Control 엔터프라이즈 관리 사용자가 생성되거나 수정되는 경우

참고: 전자 메일 알림을 사용하는 방법에 대한 자세한 내용은 *구현 안내서*를 참조하십시오.

전자 메일 템플릿

CA Access Control 엔터프라이즈 관리는 전자 메일 템플릿에서 전자 메일 알림을 생성합니다. 각 전자 메일 템플릿은 다음 정보를 포함하고 있습니다.

- **배달 정보** - 전자 메일 받는 사람의 목록입니다.
- **제목** - 전자 메일의 제목 줄에 사용되는 텍스트입니다.
- **내용** - 전자 메일 본문입니다. 본문은 주로 전자 메일을 트리거하는 작업 또는 이벤트를 기반으로 CA Access Control 엔터프라이즈 관리가 처리하는 변수 및 정적 텍스트를 모두 포함합니다.

전자 메일 템플릿은 다음 디렉터리에 있습니다. 여기서 *JBoss_home* 은 JBoss 를 설치한 디렉터리입니다.

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

emailTemplates 디렉터리는 5 개의 하위 디렉터리를 포함하고 있습니다. 각 폴더는 이벤트 상태와 연결되어 있습니다. 다음 표는 각 하위 디렉터리의 전자 메일 템플릿의 용도를 나열합니다.

Subdirectory	목차
승인됨	■ CertifyRoleEvent.tmpl - 더 이상 사용되지 않습니다. ■ CheckOutAccountPasswordEvent.tmpl - 받는 사람에게 권한 있는 계정 암호 요청이 승인되었음을 알립니다. ■ CreatePrivilegedAccountExceptionEvent.tmpl - 받는 사람에게 권한 있는 계정 암호 요청이 지정된 기간 동안 승인되었음을 알립니다(이 템플릿은 권한 있는 계정 요청 작업에 해당). ■ defaultEvent.tmpl - 받는 사람에게 이벤트가 승인되었음을 알립니다. ■ defaultTask.tmpl - 받는 사람에게 작업이 승인되었음을 알립니다. ■ ForgottenPasswordEvent.tmpl - 더 이상 사용되지 않습니다. ■ SelfRegisterUserEvent.tmpl - 더 이상 사용되지 않습니다.

Subdirectory	목차
완료함	■ AccumulatedProvisioningRolesEvent.tmpl - 더 이상 사용되지 않습니다. ■ CertificationNonCertifiedActionCompletedNotificationEvent.tmpl - 더 이상 사용되지 않습니다. ■ CertificationNonCertifiedActionPendingNotificationEvent.tmpl - 더 이상 사용되지 않습니다. ■ CertificationRequiredFinalReminderNotificationEvent.tmpl - 더 이상 사용되지 않습니다. ■ CertificationRequiredNotificationEvent.tmpl - 더 이상 사용되지 않습니다. ■ CertificationRequiredReminderNotificationEvent.tmpl - 더 이상 사용되지 않습니다. ■ CheckOutAccountPasswordEvent.tmpl - 받는 사람에게 체크 아웃한 권한 있는 계정의 암호에 대해 알립니다. ■ CreateProvisioningUserNotificationEvent.tmpl - 더 이상 사용되지 않습니다. ■ defaultEvent.tmpl - 받는 사람에게 CA Access Control 엔터프라이즈 관리가 이벤트를 완료했음을 알립니다. ■ defaultTask.tmpl - 받는 사람에게 CA Access Control 엔터프라이즈 관리가 작업을 완료했음을 알립니다. ■ ForgottenPassword.tmpl - 더 이상 사용되지 않습니다. ■ ForgottenUserID.tmpl - 더 이상 사용되지 않습니다. ■ Self Registration.tmpl - 더 이상 사용되지 않습니다.
오류	■ AssignProvisioningRoleEvent.tmpl - 더 이상 사용되지 않습니다. ■ DefaultEvent.tmpl - 받는 사람에게 이벤트가 실패했음을 알립니다. ■ DefaultTask.tmpl - 받는 사람에게 작업이 실패했음을 알립니다.

Subdirectory	목차
보류	■ BreakGlassCheckOutAccountEvent.tmpl - 승인자에게 Break Glass 체크 아웃이 수행되었음을 알립니다. ■ CertifyRoleEvent.tmpl - 더 이상 사용되지 않습니다. ■ CheckOutAccountPasswordEvent.tmpl - 승인자에게 권한 있는 계정 체크 아웃 요청의 검토가 필요함을 알립니다. ■ defaultEvent.tmpl - 승인자에게 작업 목록 항목의 검토가 필요함을 알립니다. ■ defaultTask.tmpl - 승인자에게 작업의 검토가 필요함을 알립니다. ■ ModifyUserEvent.tmpl - 더 이상 사용되지 않습니다.
거부됨	■ CertifyRoleEvent.tmpl - 더 이상 사용되지 않습니다. ■ CheckOutPasswordEvent.tmpl - 받는 사람에게 권한 있는 계정 암호 요청이 거부되었음을 알립니다. ■ CreatePrivilegedAccountExceptionEvent.tmpl - 받는 사람에게 지정된 기간 동안의 권한 있는 계정 액세스에 대한 사용자 요청이 거부되었음을 알립니다(이 템플릿은 권한 있는 계정 요청 작업에 해당) ■ defaultEvent.tmpl - 받는 사람에게 이벤트가 거부되었음을 알립니다. ■ defaultTask.tmpl - 받는 사람에게 작업이 거부되었음을 알립니다. ■ ForgottenPasswordEvent.tmpl - 더 이상 사용되지 않습니다. ■ SelfRegisterUserEvent - 더 이상 사용되지 않습니다.

전자 메일 알림 작동 방법

전자 메일은 CA Access Control 엔터프라이즈 관리 사용자에게 시스템의 이벤트에 대해 알립니다. 다음 프로세스는 전자 메일 알림이 작동하는 방법에 대해 설명합니다.

1. 이벤트가 발생하면 CA Access Control 엔터프라이즈 관리는 전자 메일 알림이 이벤트에 대해 사용되는지 여부를 확인합니다.
2. 전자 메일 알림이 사용되는 경우 CA Access Control 엔터프라이즈 관리는 적절한 하위 디렉터리에서 이벤트 유형을 찾습니다.

   예를 들어, 권한 있는 계정 요청의 승인에 대해 전자 메일을 보내는 경우 CA Access Control 엔터프라이즈 관리는 "승인됨" 하위 디렉터리에서 찾습니다.
3. CA Access Control 엔터프라이즈 관리는 하위 디렉터리에서 이벤트와 이름이 같은 전자 메일 템플릿을 찾고 다음 중 하나를 수행합니다.
   - 이벤트와 이름이 같은 전자 메일 템플릿이 있으면 CA Access Control 엔터프라이즈 관리는 이 전자 메일 템플릿을 받는 사람에게 보냅니다.
   - 이벤트와 이름이 같은 전자 메일 템플릿이 없으면 CA Access Control 엔터프라이즈 관리는 defaultEvent.tmpl 전자 메일 템플릿을 받는 사람에게 보냅니다.

참고: 전자 메일 알림 설정을 구성하는 방법에 대한 자세한 내용은 *구현 안내서*를 참조하십시오.

전자 메일 템플릿 사용자 지정

CA Access Control 엔터프라이즈 관리는 전자 메일 템플릿에서 전자 메일 알림을 생성합니다. 회사의 요구 사항에 맞게 전자 메일 템플릿을 사용자 지정할 수 있습니다.

전자 메일 템플릿을 사용자 지정하려면

1. 편집 가능한 형식으로 템플릿을 엽니다.
2. 다음 중 하나 또는 모두를 수행하여 전자 메일 템플릿을 편집합니다.
   - 템플릿의 본문에 정적 텍스트를 입력합니다.
   - 전자 메일 템플릿 API 에서 변수를 사용하여 템플릿의 동적 콘텐츠를 지정합니다.
3. 템플릿을 저장한 후 닫습니다.

참고: 전자 메일 템플릿 API 에 대한 자세한 내용은 *CA Identity Manager 관리 안내서*를 참조하십시오.

제 3 장: PUPM 구현 계획

이 섹션은 다음 항목을 포함하고 있습니다.

권한 있는 사용자 암호 관리

권한 있는 사용자 암호 관리(PUPM)는 회사에서 가장 강력한 계정과 관련된 모든 활동을 추적하고, 관리하고, 보안을 유지하기 위한 프로세스입니다.

PUPM 을 사용하면 중앙 위치에서 대상 끝점에 있는 권한 있는 계정의 액세스 권한을 역할에 기반하여 관리할 수 있습니다. PUPM 은 권한 있는 계정 및 응용 프로그램 ID 암호를 안전하게 저장하고, 정의하는 정책에 기반하여 권한 있는 계정 및 암호에 대한 액세스를 제어합니다. 그 외에도 PUPM 을 사용하면 권한 있는 계정과 응용 프로그램 암호 수명 주기를 관리하고 구성 파일 및 스크립트에서 암호를 제거할 수 있습니다.

권한 있는 계정이란?

권한 있는 계정은 개별 계정에 할당되지 않고 업무에 핵심적인 데이터 및 프로세스에 액세스할 수 있는 계정입니다. 시스템 관리자는 권한 있는 계정을 사용하여 대상 끝점에서 관리 작업을 수행하거나 무인 모드에서 처리하기 위해 서비스 파일, 스크립트, 구성 파일에 관리 작업을 포함시킬 수 있습니다.

권한 있는 계정은 식별 가능한 사용자에게 할당되지 않으므로 감사 및 추적이 어렵고, 따라서 통제하는 데 어려움이 있습니다. 이로 인해 업무에 핵심적인 시스템이 실수나 악의적인 행위로 의해 손상될 수 있는 취약점이 생기게 됩니다. 회사나 조직은 업무에 차질이 없는 한도 내에서 이러한 권한 있는 계정의 수를 최소한 줄여야 합니다.

관리자(Administrator)는 기밀 정보 액세스에 대한 대부분의 내부 제어를 바이패스할 수 있으며 응용 프로그램을 삭제하거나 작용 불능 상태로 만들어 서비스 거부(DOS) 공격을 유발할 수도 있습니다. 더 나아가, 권한 있는 계정을 사용하여 수행된 이러한 작업이 실제 어떤 사용자 계정에 의해 수행되었는지 파악하기가 어렵습니다.

권한 있는 액세스 역할 및 권한 있는 계정

권한 있는 액세스 역할을 사용하여 각 사용자가 CA Access Control 엔터프라이즈 관리에서 수행하는 PUPM 작업과 각 사용자가 체크 인 및 체크 아웃할 수 있는 권한 있는 계정을 지정합니다. CA Access Control 엔터프라이즈 관리에는 미리 정의된 권한 있는 액세스 역할이 포함되어 있습니다. 용도에 맞게 이 미리 정의된 역할을 수정하거나 새 역할을 만들 수 있습니다.

사용자가 CA Access Control 엔터프라이즈 관리에 로그인하면 자신의 역할과 일치하는 작업 및 권한 있는 계정만 볼 수 있습니다.

권한 있는 액세스 역할 사용

회사에서 PUPM 을 설정하기 전에 다음 사항을 고려해야 합니다.

- 사용자 저장소로 Active Directory 를 사용하고 Active Directory 의 그룹을 가리키도록 각 역할에 대한 구성원 정책을 수정하는 것이 좋습니다. 이 방법으로 설정하는 역할에서 사용자를 추가 또는 제거하려면 Active Directory 그룹에서 사용자를 추가 또는 제거합니다. 이렇게 하면 관리 오버헤드를 줄일 수 있습니다.
- 사용자 저장소로 Active Directory 를 사용하는 경우 CA Access Control 엔터프라이즈 관리를 사용하여 사용자 또는 그룹을 만들거나 삭제할 수 없습니다. Active Directory 에서만 사용자 및 그룹을 만들고 삭제할 수 있습니다.

- 역할에 정의된 구성원 정책이 있고 PUPM 사용자 관리자가 사용자에게 특정 역할을 할당하지만 사용자가 구성원 정책의 범위에 맞지 않는 경우 CA Access Control 은 역할을 사용자에게 할당하지 않습니다. 구성원 정책에 정의된 규칙은 PUPM 사용자 관리자 할당보다 우선 순위가 높습니다.
- 권한 있는 계정 요청에 응답하려면 사용자에게 PUPM 승인자 역할이 있어야 하며 요청하는 사용자의 관리자여야 합니다. 포함된 사용자 저장소를 사용하는 경우 CA Access Control 엔터프라이즈 관리의 "사용자 만들기" 및 "사용자 수정" 작업에서 사용자의 관리자를 지정할 수 있습니다.
- 기본적으로 CA Access Control 은 모든 사용자에게 Break Glass, PUPM 승인자, 권한 있는 계정 요청, PUPM 사용자 역할을 할당합니다. 이 설정을 변경하려면 각 역할에 대한 구성원 정책을 수정하십시오.
- 특정 끝점 및 역할이 액세스할 수 있는 권한 있는 계정을 정의하기 위해 역할에 대한 범위 규칙을 수정할 수 있습니다. 범위 규칙을 사용하면 회사 전체에서 권한 있는 계정에 대한 세부적인 액세스를 구현할 수 있습니다. 범위 규칙은 역할의 구성원 정책에 정의됩니다.

추가 정보:

구성원 정책 (페이지 24)

권한 있는 액세스 역할이 작업 체크 아웃 및 체크 인에 주는 영향

끝점에서 관리 작업을 수행하기 위해 권한 있는 계정을 체크 아웃하고 끝점에서 작업을 완료한 다음 권한 있는 계정을 체크 인합니다.

중요! 사용자에게는 끝점 유형에서 작업을 수행하기 위한 끝점 권한 있는 액세스 역할이 있어야 합니다. 끝점 권한 있는 액세스 역할은 권한 있는 액세스 계정을 사용하여 사용자가 작업을 수행할 수 있는 끝점의 유형을 지정합니다. 예를 들어, 사용자에게 Windows Agentless 끝점 권한 있는 액세스 역할을 할당하면 사용자는 권한 있는 계정을 사용하는 Windows 끝점에서 끝점 작업을 수행할 수 있습니다. Break Glass, 권한 있는 계정 요청 또는 PUPM 사용자 역할을 사용자에게 할당하는 경우 사용자에게 끝점 권한 있는 액세스 역할도 할당해야 합니다. 그렇지 않으면 사용자가 어떠한 작업도 완료할 수 없습니다.

다음 프로세스는 권한 있는 액세스 역할이 사용자가 수행하는 작업의 체크 아웃 및 체크 인에 주는 영향에 대해 설명합니다.

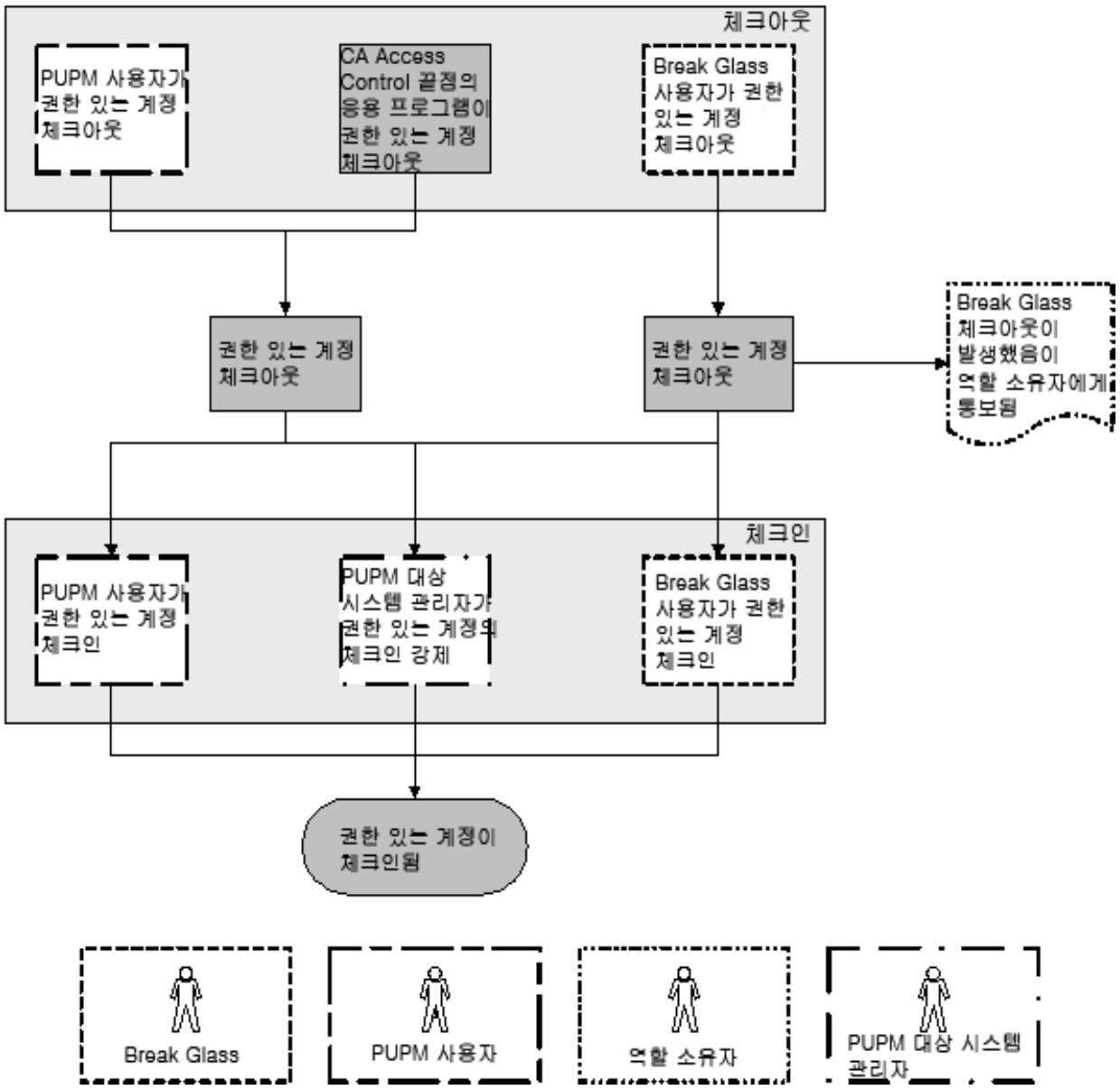
1. 사용자는 다음 방법 중 하나를 사용하여 권한 있는 계정을 체크 아웃합니다.
   - PUPM 사용자 역할이 있는 사용자가 권한 있는 계정을 체크 아웃합니다.
   - Break Glass 역할이 있는 사용자가 break glass 체크 아웃을 수행합니다.
   - CLI 암호 소비자와 같은 응용 프로그램이 CA Access Control 끝점에서 권한 있는 계정을 체크 아웃합니다.

   권한 있는 계정이 체크 아웃됩니다.

   참고: 사용자가 break glass 체크 아웃을 수행하면 CA Access Control 은 역할 소유자에게 알림 메시지를 보냅니다. 역할 소유자는 감사를 위해 이 메시지에 정보를 추가할 수 있습니다.
2. 사용자는 다음 방법 중 하나를 사용하여 권한 있는 계정을 체크 인합니다.
   - PUPM 사용자 역할이 있는 사용자가 권한 있는 계정을 체크 인합니다.
   - Break Glass 역할이 있는 사용자가 권한 있는 계정을 체크 인합니다.
   - CA Access Control 끝점에 있는 응용 프로그램이 권한 있는 계정을 체크 인합니다.
   - PUPM 대상 시스템 관리자 역할이 있는 사용자가 권한 있는 계정을 강제로 체크 인합니다.

   권한 있는 계정이 체크 인됩니다.

다음 다이어그램은 권한 있는 액세스 역할이 사용자가 수행하는 작업의 체크 인 및 체크 아웃에 주는 영향을 설명합니다.



예: 권한 있는 계정 체크 아웃

본인에게 시스템 관리자 역할이 있습니다. Joe 에게 PUPM 사용자 역할과 Windows Agentless 연결 끝점 권한 있는 액세스 역할을 할당합니다. Joe 가 CA Access Control 엔터프라이즈 관리에 로그인하고 Windows 끝점에서 권한 있는 계정을 체크 아웃하고 체크 인할 수 있는 작업만 살펴봅니다.

예: 권한 있는 계정에 대한 Break Glass

본인에게 시스템 관리자 역할이 있습니다. Fiona 에게 Break Glass 역할과 Oracle 서버 연결 끝점 권한 있는 액세스 역할을 할당합니다. Fiona 는 Oracle 끝점에 즉시 액세스해야 합니다. Fiona 가 CA Access Control 엔터프라이즈 관리에 로그인하여 Oracle 끝점에서 계정에 대한 break glass 체크 아웃을 수행할 수 있는 작업만 살펴봅니다. Fiona 는 Oracle 권한 있는 계정에 대해 break glass 체크 아웃을 수행하고 CA Access Control 은 Break Glass 역할 소유자에게 알림 메시지를 보냅니다.

참고: 기본적으로 Break Glass 역할 소유자는 시스템 관리자 관리 역할입니다.

권한 있는 액세스 역할이 권한 있는 계정 요청 작업에 주는 영향

사용자가 권한 있는 계정을 체크 아웃할 수 없고 계정에 즉시 액세스할 필요가 없는 경우 사용자는 권한 있는 계정 요청을 제출할 수 있습니다. 사용자의 관리자는 권한 있는 계정 요청을 승인 또는 거부할 수 있습니다. 이 항목에서는 사용자가 권한 있는 계정 요청 작업을 수행하기 위해 필요한 권한 있는 액세스 역할에 대해 설명합니다.

중요! 사용자에게는 끝점 유형에서 작업을 수행하기 위한 끝점 권한 있는 액세스 역할이 있어야 합니다. 끝점 권한 있는 액세스 역할은 권한 있는 액세스 계정을 사용하여 사용자가 작업을 수행할 수 있는 끝점의 유형을 지정합니다. 예를 들어, 사용자에게 Windows Agentless 끝점 권한 있는 액세스 역할을 할당하면 사용자는 권한 있는 계정을 사용하는 Windows 끝점에서 끝점 작업을 수행할 수 있습니다. Break Glass, 권한 있는 계정 요청 또는 PUPM 사용자 역할을 사용자에게 할당하는 경우 사용자에게 끝점 권한 있는 액세스 역할도 할당해야 합니다. 그렇지 않으면 사용자가 어떠한 작업도 완료할 수 없습니다.

다음 프로세스는 권한 있는 액세스 역할이 사용자가 수행할 수 있는 권한 있는 액세스 요청 작업에 주는 영향에 대해 설명합니다.

1. 권한 있는 액세스 요청 역할이 있는 사용자가 권한 있는 계정에 대한 액세스를 요청합니다.
2. CA Access Control 은 권한 있는 계정 요청을 사용자의 관리자(PUPM 승인자 역할도 필요함)에게 보냅니다.

   참고: 권한 있는 계정 요청을 받으려면 PUPM 승인자 역할이 있어야 하는 *동시에* 해당 사용자의 관리자여야 합니다.

3. PUPM 승인자 역할이 있는 사용자가 권한 있는 계정 요청에 응답하고 다음 중 *하나*를 수행합니다.
   - 권한 있는 계정 요청을 거부합니다.

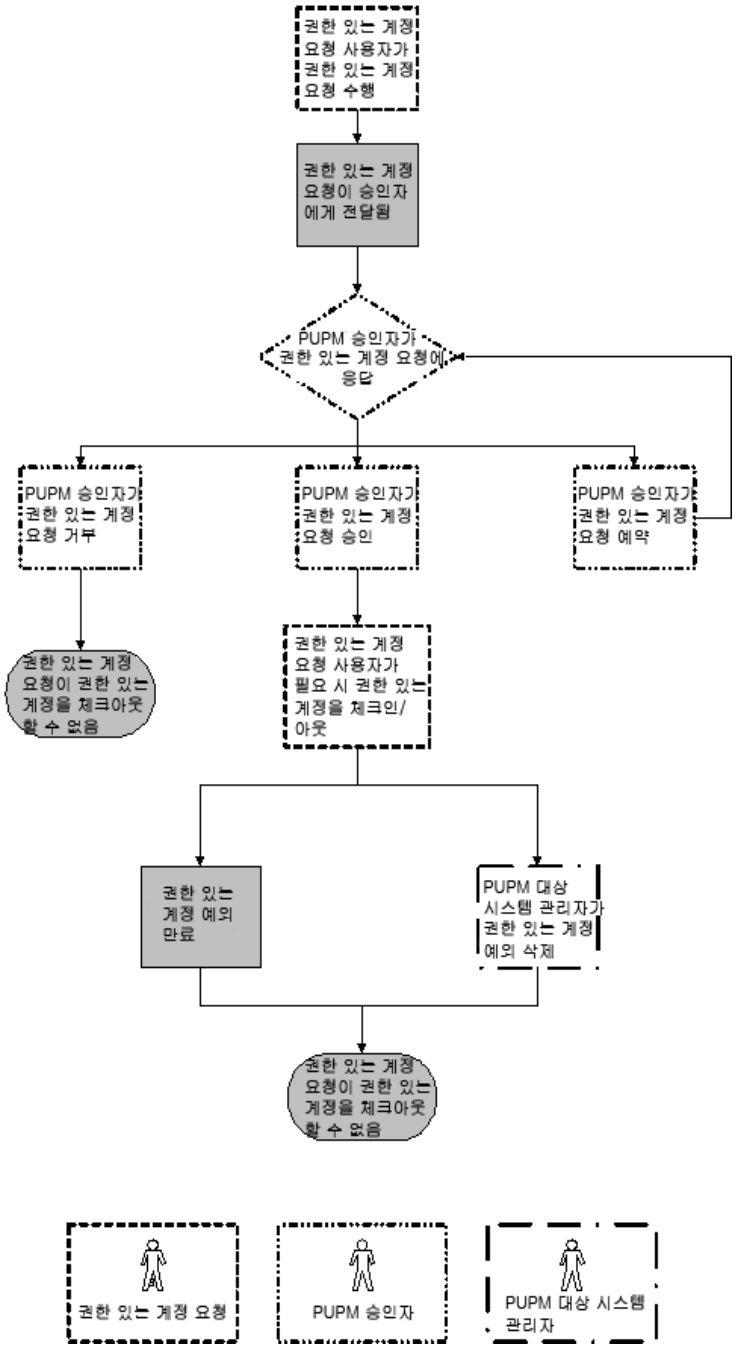
     권한 있는 계정 요청 역할이 있는 사용자가 권한 있는 계정을 체크 아웃할 수 없습니다.
   - 권한 있는 계정 요청을 예약합니다.

     다른 사용자가 이 권한 있는 계정 요청을 승인 또는 거부할 수 없습니다. PUPM 승인자가 요청을 승인할 때까지 권한 있는 계정 요청 역할이 있는 사용자가 권한 있는 계정을 체크 아웃할 수 없습니다.
   - 권한 있는 계정 요청을 승인합니다.

     권한 있는 요청 역할이 있는 사용자에게 권한 있는 계정 예외가 부여되어 사용자가 권한 있는 계정을 체크 아웃 및 체크 인할 수 있습니다.
4. 다음 이유 중 하나로 인해 권한 있는 계정 예외가 만료됩니다.
   - 권한 있는 계정 예외에 지정된 만료 시간에 도달했습니다.
   - PUPM 대상 시스템 관리자 역할이 있는 사용자가 권한 있는 계정 예외를 삭제했습니다.

   권한 있는 계정 요청 역할이 있는 사용자가 더 이상 권한 있는 계정을 체크 아웃할 수 없습니다.

다음 다이어그램은 권한 있는 액세스 역할이 사용자가 수행할 수 있는 권한 있는 계정 요청 작업에 주는 영향에 대해 설명합니다.



예: 권한 있는 계정 요청 및 이 요청에 응답

본인에게 시스템 관리자 역할이 있습니다. Alice 에게 권한 있는 계정 요청 역할과 SSH 장치 연결 끝점 권한 있는 액세스 역할을 할당합니다. Alice 의 관리자인 Bob 에게 PUPM 승인자 역할을 할당합니다.

Alice 가 CA Access Control 엔터프라이즈 관리에 로그인하고 UNIX 끝점의 계정에 대한 권한 있는 계정 요청을 제출할 수 있는 작업만 살펴봅니다. Alice 가 UNIX 끝점의 example_ux 계정에 대한 권한 있는 계정 요청을 제출합니다.

Bob 이 CA Access Control 엔터프라이즈 관리에 로그인하여 권한 있는 계정 요청에 응답할 수 있는 작업만 살펴봅니다. Bob 이 Alice 의 권한 있는 액세스 요청을 승인하고 권한 있는 계정 예외가 오후 6 시까지 유효하도록 지정합니다. Alice 는 이제 example_ux 권한 있는 계정에 체크 인 및 체크 아웃할 수 있습니다. 오후 6 시에 권한 있는 계정 예외가 만료되고 Alice 는 더 이상 example_ux 권한 있는 계정을 체크 아웃할 수 없게 됩니다.

Break Glass 프로세스가 작동하는 방법

사용자가 관리 권한이 없는 계정에 즉시 액세스해야 하는 경우 Break Glass 체크 아웃을 수행합니다.

Break Glass 계정은 사용자 역할에 따라 사용자에게 할당되지 않은 권한 있는 계정입니다. 하지만 사용자는 필요한 경우 이 계정 암호를 획득할 수 있습니다.

Break Glass 체크 아웃 프로세스 중에 Break Glass 체크 아웃 프로세스가 발생했음을 알리는 알림 메시지가 역할 관리자에게 전달되지만 이 관리자는 이 프로세스를 승인 또는 중단시킬 수 없습니다.

체크 아웃된 Break Glass 계정이 "홈" 탭의 "Break Glass" 옵션에 있는 "내 체크 아웃한 권한 있는 계정" 탭에 추가됩니다.

참고: Break Glass 권한 있는 액세스 역할이 있는 사용자만 Break Glass 프로세스를 수행할 수 있습니다.

PUPM 감사 레코드

CA Access Control 엔터프라이즈 관리는 이벤트(예: 사용자가 권한 있는 계정 암호를 체크 인할 때)에 대한 감사 데이터를 기록합니다. CA Access Control 엔터프라이즈 관리는 또한 실패한 이벤트에 대한 감사 데이터를 기록합니다. 예를 들어, 권한 있는 계정 암호를 체크 아웃할 때 자동 로그인을 선택했지만 ActiveX 다운로드를 허용하지 않으면 CA Access Control 엔터프라이즈 관리는 자동 로그인이 실패한 이유를 기록합니다. CA Access Control 엔터프라이즈 관리는 PUPM 감사 데이터를 중앙 데이터베이스에 저장합니다.

추가 정보:

감사 데이터 (페이지 40)
권한 있는 계정 감사 (페이지 158)

PUPM 피더 감사 레코드

PUPM 피더는 다음 작업을 수행합니다. CA Access Control 엔터프라이즈 관리는 PUPM 피더가 수행하는 각 작업에 대한 감사 레코드를 만듭니다.

- 피더 폴더 폴링 - PUPM 피더가 CA Access Control 엔터프라이즈 관리에 대한 폴링 폴더에 CSV 파일을 성공적으로 업로드했는지 여부를 지정합니다.
- 피더 프로세스 csv 파일 - CA Access Control 엔터프라이즈 관리가 업로드된 CSV 파일을 성공적으로 처리했는지 여부를 지정하고, CA Access Control 엔터프라이즈 관리가 CSV 파일에서 처리한 줄 수를 추적하는 진행 상황 표시기를 제공합니다.

또한 CA Access Control 엔터프라이즈 관리는 가져온 CSV 파일의 각 줄에 대한 감사 레코드를 만듭니다. 각 줄은 PUPM 끝점 또는 권한 있는 계정을 만들거나 수정하기 위한 작업을 나타냅니다. 감사 레코드는 각 작업의 상태가 추적합니다. 이러한 추적은 다음과 같은 상태를 가질 수 있습니다.

- **완료** - CA Access Control 엔터프라이즈 관리가 작업을 완료했습니다(예: 권한 있는 계정을 만듦).
- **실패** - CA Access Control 엔터프라이즈 관리가 작업을 처리했지만 완료하지 못했습니다(예: 존재하지 않는 끝점에서 권한 있는 계정을 만들지 못함).
- **감사됨** - CA Access Control 엔터프라이즈 관리가 작업을 처리 또는 완료하지 못했습니다(예: ACCOUNT_NAME 특성이 지정되지 않아 권한 있는 계정을 만들지 못함)

시스템 관리자 역할이 있는 사용자는 "제출된 작업 보기" 작업을 사용하여 각 작업의 상태를 볼 수 있습니다.

PUPM 끝점의 이벤트 감사

CA Access Control 엔터프라이즈 관리는 엔터프라이즈 관리 서버에서 발생하는 이벤트에 대한 감사 데이터를 기록합니다. PUPM 끝점을 CA Enterprise Log Manager 와 통합하면 각 권한 있는 계정 세션에 대해 끝점에서 감사 이벤트도 기록할 수 있습니다.

이 통합을 사용하면 사용자가 권한 있는 계정을 체크 아웃하고 이 계정을 사용하여 끝점에 로그인한 이후에 권한 있는 계정이 끝점에서 수행하는 작업을 추적할 수 있습니다. 이러한 작업은 CA Enterprise Log Manager 보고서에 수집되는 감사 이벤트에 기록됩니다. 이러한 CA Enterprise Log Manager 보고서는 CA Access Control 엔터프라이즈 관리에서 볼 수 있습니다.

예를 들어, privileged1 이란 이름의 계정을 체크 아웃한 이후에 사용자가 수행한 작업을 검토하려고 합니다. CA Access Control 엔터프라이즈 관리에서 "권한 있는 계정 감사" 작업을 사용하여 privileged1 계정 체크 아웃에 대한 감사 레코드를 찾습니다. 그런 다음 이 감사 레코드에서 드릴다운하여 privileged1 계정이 끝점에서 수행한 작업(예: 프로그램 열기 및 닫기)에 대한 CA Enterprise Log Manager 보고서를 검토합니다.

추가 정보:

PUPM 끝점에서 감사 이벤트 보기 (페이지 162)

PUPM 끝점과 CA User Activity Reporting Module 을 통합하는 방법

PUPM 끝점을 CA User Activity Reporting Module 과 통합하면 각 권한 있는 계정 세션에 대해 끝점의 감사 이벤트를 기록할 수 있습니다. 이 통합을 통해 또한 CA Access Control 엔터프라이즈 관리에서 PUPM 끝점의 권한 있는 계정 감사 이벤트에 대한 CA Enterprise Log Manager 보고서를 볼 수 있습니다.

다음 단계를 수행하십시오.:

1. CA Access Control 엔터프라이즈 관리에서:
   a. CA User Activity Reporting Module 에 대한 연결을 구성합니다.
   b. 각 PUPM 끝점에 대해 CA User Activity Reporting Module 호스트 이름과 이벤트 로그 이름을 지정합니다.

      호스트 이름과 이벤트 로그 이름을 지정하려면 "끝점 만들기" 또는 "끝점 수정" 작업의 CA User Activity Reporting Module 탭을 사용하십시오.
2. PUPM 에서 지속적으로 정보를 수집하려면 CA User Activity Reporting Module 을 구성합니다.

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

추가 정보:

PUPM 끝점에서 감사 이벤트 보기 (페이지 162)

구현 고려 사항

다음은 PUPM 을 구현하기 전에 고려해야 할 항목을 나열합니다.

권한 있는 계정 암호의 전자 메일 알림

때때로 CA Access Control 엔터프라이즈 관리는 사용자가 암호를 체크아웃할 때 (예를 들어 네트워크가 느릴 때) 20 초 이상 응답하지 않을 수 있습니다. CA Access Control 엔터프라이즈 관리가 20 초 이상 응답하지 않는 경우 화면이 만료되어 암호가 사용자에게 표시되지 않습니다. CA Access Control 엔터프라이즈 관리는 대신 암호를 사용자에게 전자 메일로 발송합니다.

사용자가 확실히 암호를 받을 수 있도록 다음을 수행하십시오.

- CA Access Control 엔터프라이즈 관리에 대한 전자 메일 알림 설정을 구성하십시오.
- 각 PUPM 사용자에 대해 사용자 저장소에 올바른 전자 메일 주소가 기록되었는지 확인하십시오.

참고: 전자 메일 알림 구성에 대한 자세한 내용은 *구현 안내서*를 참조하십시오.

Windows Agentless 끝점의 도메인 사용자에 대한 제한 사항

로컬 컴퓨터에서 도메인 사용자를 구성하는 경우 PUPM 은 도메인 사용자의 암호를 변경할 수 없습니다. 이 제한 사항은 Windows 의 특성에 기인합니다.

커넥터 서버

CA Access Control 엔터프라이즈 관리는 PUPM 끝점에서 권한 있는 계정을 검색하고 관리하기 위해 커넥터 서버와 통신합니다. CA Access Control 엔터프라이즈 관리는 Java Connector Server(JCS)를 사용하여 PUPM 끝점에 대한 CA Access Control 과 통신합니다. 기본적으로 JCS 는 CA Access Control 엔터프라이즈 관리를 설치할 때 배포 서버의 일부로 설치됩니다.

PUPM 을 사용하여 CA Identity Manager 프로비저닝 끝점을 관리하려면 CA Access Control 엔터프라이즈 관리에 Identity Manager 프로비저닝 유형 커넥터 서버를 만들어야 합니다.

참고: 커넥터 서버 생성에 대한 자세한 내용은 *온라인 도움말*을 참조하십시오.

Connector Xpress 개요

Connector Xpress 는 동적 커넥터를 관리하고, 끝점에 동적 커넥터를 매핑하고, 끝점에 대한 라우팅 규칙을 구성하기 위한 CA Identity Manager 유틸리티입니다. 이 유틸리티를 사용하여 SQL 데이터베이스를 제공하고 관리하기 위해 동적 커넥터를 구성할 수 있습니다.

Connector Xpress 를 사용하면 프로비저닝 관리자에 의해 관리되는 커넥터를 만들 때 요구되는 기술 지식 없이도 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.

참고: Connector Xpress 에 대한 자세한 내용은 *Connector Xpress Guide*(Connector Xpress 안내서)를 참조하십시오.

PUPM 에 대해 Connector Xpress 를 구현하는 방법

기본 PUPM 끝점 유형이 아닌 끝점을 관리하려면 Connector Xpress 를 사용하여 새 끝점 유형을 만들고 권한 있는 계정 암호를 관리할 수 있습니다. 예를 들어, Microsoft SQL Server 데이터베이스에 있는 권한 있는 계정 암호를 관리하려면 SQL 유형의 끝점을 만듭니다. 기본 PUPM SQL 끝점 유형은 데이터베이스 내의 개별 테이블을 관리하는 것이 아니라 SQL Server 에서 권한 있는 계정을 관리하기 위해 고안되었습니다.

다음 단계를 수행하십시오.

1. Connector Xpress 를 설치합니다.

   참고: Connector Xpress 의 설치 방법에 대한 자세한 내용은 CA Support에서 CA Identity Manager 북셸프에 있는 *Connector Xpress Guide*(Connector Xpress 안내서)를 참조하십시오.

2. Connector Xpress 에서 새 끝점 유형을 구성합니다.

3. 새 끝점 유형을 Java Connector Server 에 등록합니다.

   새 끝점 유형을 등록하는 것은 Java Connector Server 가 끝점 유형을 관리할 수 있도록 하기 위해서 입니다.

4. 새 끝점 유형을 엔터프라이즈 관리 서버로 로드합니다.

   새 끝점 유형을 로드하는 것은 끝점 유형을 CA Access Control 엔터프라이즈 관리에서 사용할 수 있도록 하기 위해서 입니다.

5. CA Access Control 엔터프라이즈 관리에서 새 끝점 유형에 대한 PUPM 끝점을 만듭니다.

6. 새 끝점에서 권한 있는 계정 암호를 검색합니다.

Connector Xpress 예제: JDBC 끝점 구성

이 예에서 시스템 관리자인 Steve 는 Microsoft SQL Server 에 연결하기 위해 Connector Xpress 에서 JDBC 끝점을 만듭니다.

Steve 는 엔터프라이즈 관리 서버 호스트에 Connector Xpress 를 설치했습니다. Steve 는 다음과 같은 작업을 수행합니다.

1. "시작" 메뉴에서 "프로그램", "CA, Identity Manager", "Connector Xpress"를 선택합니다.

   Identity Manager Connector Xpress 기본 메뉴가 나타납니다.

2. "Setup Data Sources"(데이터 원본 설정)를 클릭합니다.

   "Setup Data Sources"(데이터 원본 설정) 창이 열립니다.

3. "Add"(추가)를 클릭합니다.

   "Source Types"(원본 유형) 창이 열리고 사용 가능한 원본이 표시됩니다.

4. JDBC 를 선택하고 "확인"을 클릭합니다.

   "Edit Source"(원본 편집" 창이 열립니다.

5. 다음 세부 정보를 입력합니다.

   - 데이터 원본 이름 - SQL Server
   - 데이터베이스 유형 - Microsoft SQL Server
   - 사용자 이름 - sa
   - 서버 이름 - mysql
   - 포트 - 1433
   - 데이터베이스 - users

6. "Test"(테스트)를 클릭하여 연결 설정을 검사합니다.

   데이터 원본에 대한 암호 입력 창이 열립니다.

7. sa 사용자 계정 암호를 입력한 다음 "확인"을 클릭합니다.

   오류가 발견되지 않으면 확인 메시지가 표시됩니다. 새 데이터 원본이 만들어졌습니다. Steve 는 이제 새 끝점 유형을 구성합니다.

8. Identity Manager Connector Xpress 기본 메뉴로 돌아가 "New Project"(새 프로젝트)를 선택합니다.

   "Select Data Source for New Project"(새 프로젝트를 위한 데이터 원본 선택) 창이 열립니다.

9. 만든 데이터 원본을 선택하고 "확인"을 클릭합니다.

   "Endpoint Type Details"(끝점 유형 정보) 창이 열립니다.

10. 끝점 이름과 설명을 입력하고 "Classes"(클래스) 아이콘을 두 번 클릭한 다음 "User Details"(사용자 정보) 옵션을 선택합니다.

    "Map Class and Attributes"(클래스 및 특성 매핑) 창이 열립니다.

11. "Select Schema and Table"(스키마 및 테이블 선택) 섹션에서 다음을 선택합니다.

    - "Schema"(스키마)에 대해 dbo 를 선택합니다.
    - "Table"(테이블)에 대해 sqlConnector 테이블을 선택합니다.

    매핑된 열이 표시됩니다.

12. "Map Columns"(열 매핑) 섹션에서 "Name"(이름) 열에 다음 값을 입력합니다.

    - uname 행에 "Account ID"(계정 ID)를 입력합니다.
    - upassword 행에 "Password"(암호)를 입력합니다.

13. "Project"(프로젝트), "Save"(저장)를 선택하여 끝점 유형 정의를 저장합니다.

Steve 는 Connector Xpress 에서 새 JDBC 끝점 유형을 구성했습니다. Steve 는 이제 끝점 유형을 Java Connector Server 에 등록합니다.

Connector Xpress 예제: Java Connector Server 에서 JDBC 끝점 등록

이 예에서 시스템 관리자인 Steve 는 Connector Xpress 에서 만든 끝점 유형을 Java Connector Server 에 등록합니다. Steve 는 새 끝점 유형이 CA Access Control 엔터프라이즈 관리에 표시되도록 이 유형을 등록합니다. Steve 는 다음과 같은 작업을 수행합니다.

1. Identity Manager Connector Xpress 프로젝트 창에서 "Connector Server"(커넥터 서버) 옵션을 마우스 오른쪽 단추로 클릭한 다음 "Add Server"(서버 추가)를 선택합니다.

   "Connector Server Details"(커넥터 서버 정보) 창이 열립니다.

2. Java Connector Server 호스트 이름을 지정하고 "확인"을 클릭합니다.

   참고: Java Connector Server 는 배포 서버의 일부입니다. 엔터프라이즈 관리 서버는 기본적으로 이 서버에 배포 서버를 설치합니다. "Connector Server Password Required"(커넥터 서버 암호가 필요함) 창이 열립니다.

3. 엔터프라이즈 관리 서버 통신 암호를 입력합니다.

   엔터프라이즈 관리 서버를 설치했을 때 통신 암호를 지정했습니다. 기존 끝점 유형의 목록이 표시됩니다.

4. "Endpoint Types"(끝점 유형)를 마우스 오른쪽 단추로 클릭하고 "Create New Endpoint Type"(새 끝점 유형 만들기)을 선택합니다.

   "Create New Endpoint Type"(새 끝점 유형 만들기) 창이 열립니다.

5. 끝점 유형 이름을 입력하고 "확인"을 클릭합니다.

   오류가 발견되지 않으면 Connector Xpress 가 새 끝점 유형을 만듭니다.

Steve 가 새 끝점은 Java Connector Server 에 등록했습니다. Steve 는 이제 새 끝점 유형을 엔터프라이즈 관리 서버로 로드합니다.

Connector Xpress 예제: 끝점 유형을 엔터프라이즈 관리 서버로 로드

이 예에서 시스템 관리자인 Steve 는 만든 새 끝점 유형을 엔터프라이즈 관리 서버로 로드합니다. 새 끝점 유형을 로드한 후에 Steve 는 CA Access Control 엔터프라이즈 관리에서 이 끝점을 구성하고 관리할 수 있습니다. Steve 는 다음과 같은 작업을 수행합니다.

1. JBoss Application Server 를 중지합니다.
2. 다음 중 *하나*를 수행합니다.
   - (JDBC) conXpressnamespace_config.xml.template 파일을 편집합니다.
   - (SUN One) iplanetnamespace_config.xml 을 편집합니다.

   이 파일은 다음 디렉터리에 있습니다. 여기서 *JBoss_HOME* 은 JBoss 를 설치한 디렉터리를 나타냅니다.

   JBOSS_HOME/server/default/deploy/IdentityMinder.ear/custom/ppm/namespaceConfigs/
3. <endpointType> 매개 변수를 찾아 기본값 'REPLACE_WITH_ENDPOINT_TYPE'을 제거합니다.
4. 끝점 유형 이름을 Connector Xpress 에 지정한 그대로 입력합니다.
5. 다음 디렉터리에 conXpress_*Endpoint_Type*_namespace_config.xml 이란 이름으로 파일을 저장합니다.

   JBOSS_HOME/server/default/deploy/IdentityMinder.ear/custom/ppm/namespaceConfigs/
6. JBoss Application Server 를 시작합니다.

Steve 가 새 끝점 유형을 엔터프라이즈 관리 서버로 로드했습니다. Steve 는 이제 CA Access Control 엔터프라이즈 관리에서 이 유형의 끝점을 정의하고 끝점에서 권한 있는 계정을 검색할 수 있습니다.

Connector Xpress 제한 사항

Connector Xpress 에서 만든 끝점 유형에서 권한 있는 계정 검색 마법사를 실행하기 전에 다음 사항을 고려해야 합니다.

- Connector Xpress 에서 만든 동일한 유형의 끝점(예: SQL Server 끝점)을 정의하고 끝점 관리자 계정 자격 증명을 제공합니다. CA Access Control 엔터프라이즈 관리가 끝점을 만들 때는 연결이 해제된 권한 있는 계정도 만듭니다.
- 끝점 유형 메뉴에서 Connector Xpress 에서 만든 끝점 유형을 지정합니다. URL 필드에서 아래 예와 같이 데이터베이스 이름을 지정하십시오.
- 사용자 로그인 및 암호 필드는 비워두십시오. "Use the following privileged account"(다음 권한 있는 계정 사용)을 선택하고 끝점에 연결하기 위한 권한이 있는 권한 있는 계정을 선택하십시오. CA Access Control 엔터프라이즈 관리가 이전에 정의한 끝점에 대해 만든 연결 해제된 권한 있는 계정을 사용하십시오.

예: 끝점 URL 필드의 SQL Server 데이터베이스 이름

다음 예는 SQL Server 데이터베이스 이름을 포함하는 URL 필드를 나타냅니다.

```
jdbc:sqlserver://server.company.com:1433;database=database_name
```

PUPM SDK

PUPM SDK 를 사용하면 권한 있는 계정 암호를 체크 아웃/체크 인하는 응용 프로그램을 작성할 수 있습니다. PUPM SDK 에는 암호 소비자 SDK 와 웹 서비스 SDK 의 두 가지 종류가 있습니다.

다음 표는 두 가지 종류의 SDK 사이의 차이점을 요약합니다.

기능	암호 소비자 SDK	웹 서비스 SDK
프로그래밍 언어	Java .NET	Java
사용자 인증	예	아니요
암호 캐싱	예	아니요
끝점에서 CA Access Control 필요	예	아니요

사용 사례: PUPM SDK

PUPM SDK 를 사용하면 스크립트의 권한 있는 계정 암호의 관리를 자동화할 수 있습니다. 하드 코드된 암호가 들어 있는 스크립트를 수정하고 싶지 않으면 스크립트에서 암호를 주기적으로 대체하는 응용 프로그램을 작성할 수 있습니다.

예를 들어, 동일한 권한 있는 계정에 대한 하드 코드된 암호를 수록하는 끝점에 10 개의 스크립트가 있다고 가정합니다. 이 스크립트들은 수정하고 싶지 않습니다. PUPM SDK 를 사용하여 적절한 다운타임 중에 권한 있는 계정 암호를 체크 아웃하고 각 스크립트에서 암호를 업데이트한 다음 암호를 체크 인하는 응용 프로그램을 작성할 수 있습니다. 암호를 주기적으로 변경하면 권한 있는 계정의 보안을 높이는 데 도움이 됩니다.

이 작업을 수행하기 위해 응용 프로그램을 만드는 경우 CA Access Control 엔터프라이즈 관리가 체크 아웃 또는 체크 인 시 권한 있는 계정 암호를 변경하지 않는지 확인하십시오. "권한 있는 계정 보기" 작업을 사용하여 이 정보를 확인할 수 있습니다.

참고: 또한 CLI 암호 소비자를 사용하여 스크립트에서 하드 코드된 암호를 대체할 수도 있습니다. 예를 들어, 파일에서 하드 코드된 암호를 수동으로 업데이트하려면 CLI 암호 소비자를 사용하십시오.

암호 소비자 SDK 응용 프로그램이 암호를 가져오는 방법

암호 소비자 SDK 는 권한 있는 계정 암호를 가져오고 체크 인/체크 아웃하는 응용 프로그램을 작성할 수 있게 해 줍니다. 암호 소비자 SDK 를 사용하려면 다음을 수행해야 합니다.

- 응용 프로그램이 실행되는 끝점에 CA Access Control 을 설치합니다.
- CA Access Control 엔터프라이즈 관리의 응용 프로그램에 대한 암호 소비자를 정의합니다.

암호 소비자 SDK 에는 두 가지 종류가 있습니다.

- Java PUPM SDK
- .NET PUPM SDK

암호 소비자 SDK 응용 프로그램은 PUPM 에이전트와 통신하고, 그런 다음 메시지 큐를 사용하여 CA Access Control 엔터프라이즈 관리와 통신합니다. PUPM 에이전트는 SSL 통신 및 포트 7243 을 사용하여 메시지 큐와 통신합니다.

다음 프로세스는 암호 소비자 SDK 응용 프로그램이 암호를 가져오는 방법을 설명합니다.

1. 이 응용 프로그램은 암호 요청을 PUPM 에이전트로 보냅니다.
2. PUPM 에이전트는 암호 요청을 받습니다. CA Access Control 은 응용 프로그램을 실행하는 사용자를 식별하고 캐시를 검사합니다. 다음 중 *한 가지* 결과가 나타납니다.
   - 암호 요청이 캐시에 저장되어 있으면 PUPM 에이전트는 권한 있는 계정 암호를 응용 프로그램으로 전달합니다. 이 단계에서 프로세스가 끝납니다. CA Access Control 엔터프라이즈 관리는 암호 요청에 대한 감사 레코드를 작성하지 않습니다.
   - 암호 요청이 캐시에 저장되어 있지 않으면 PUPM 에이전트는 암호 요청과 응용 프로그램을 실행하는 사용자의 이름을 CA Access Control 엔터프라이즈 관리로 보냅니다.
3. CA Access Control 엔터프라이즈 관리는 요청을 받고 암호 소비자가 존재하는지 확인하여 응용 프로그램이 권한 있는 계정 암호를 획득하도록 허가합니다.

   암호 소비자는 응용 프로그램의 경로, 응용 프로그램이 요청할 수 있는 권한 있는 계정, 응용 프로그램을 실행할 수 있는 사용자, 응용 프로그램이 실행될 수 있는 호스트를 지정합니다.

4. 다음 중 *한 가지* 결과가 나타납니다.
   - 응용 프로그램이 암호를 받도록 허가된 경우 CA Access Control 엔터프라이즈 관리는 권한 있는 계정 암호를 PUPM 에이전트로 보냅니다.
   - 응용 프로그램이 암호를 받도록 허가되지 않은 경우 CA Access Control 엔터프라이즈 관리는 오류 메시지를 PUPM 에이전트로 보냅니다.

   두 경우 모두, CA Access Control 엔터프라이즈 관리가 이벤트에 대한 감사 레코드를 작성합니다.
5. PUPM 에이전트가 권한 있는 계정 암호 또는 오류 메시지를 응용 프로그램으로 보냅니다.

   응용 프로그램이 권한 있는 계정 암호를 처음으로 획득한 경우, PUPM 에이전트가 암호를 캐시에 저장합니다.

참고: 권한 있는 계정의 암호가 변경되면 CA Access Control 엔터프라이즈 관리가 암호 변경 이벤트를 끝점으로 브로드캐스트합니다. 끝점이 브로드캐스트 메시지를 받으면 PUPM 에이전트는 권한 있는 계정 암호를 캐시에서 제거합니다.

Java PUPM SDK

Java PUPM SDK 는 권한 있는 계정 암호를 획득하고 체크 아웃/체크 인하는 Java 응용 프로그램을 작성할 수 있는 암호 소비자 SDK 입니다. Java PUPM SDK 는 CA Access Control 이 설치된 Windows 및 UNIX 끝점에서 사용할 수 있습니다. 작성하는 Java 응용 프로그램은 JRE 1.5 이상을 사용해야 합니다.

Java PUPM SDK 는 다음 디렉터리에 있습니다.

ACInstallDir/SDK/JAVA

이 디렉터리에는 다음 항목이 들어 있습니다.

- PupmJavaSDK.jar - Java 응용 프로그램에 포함하는 SDK 라이브러리
- CAPUPMCLientCommons.jar - 응용 프로그램을 실행할 때 classpath 에 반드시 포함해야 하는 지원 라이브러리
- jsafeFIPS.jar - 응용 프로그램을 실행할 때 classpath 에 반드시 포함해야 하는 지원 라이브러리

- CAPUPM.properties.SAMPLE - 기본 응용 프로그램 속성을 변경하기 위해 편집할 수 있는 샘플 파일

  이 파일을 편집하는 경우 새 파일의 이름을 CAPUPM.properties 로 지정해야 하고, 응용 프로그램을 실행할 때 classpath 에 이 파일 이름을 포함해야 합니다.

  참고: 이 파일을 수정하기 전에 CA Support 에 문의하는 것이 좋습니다. 도움이 필요한 경우 기술 지원부(http://ca.com/support)에 문의하십시오.

- Samples - 권한 있는 계정 암호를 체크 아웃/체크 인하는 샘플 Java 응용 프로그램을 포함하는 폴더

응용 프로그램이 런타임 이벤트 및 정보를 로깅하도록 하려면 classpath 에 log4j 라이브러리도 포함해야 합니다. 응용 프로그램이 권한 있는 계정 암호를 획득하고 체크 아웃/체크 인할 수 있도록 하려면 먼저 CA Access Control 엔터프라이즈 관리에서 응용 프로그램에 대한 소프트웨어 개발자 키트(SDK/CLI) 암호 소비자를 만들어야 합니다.

.NET PUPM SDK

Windows 에 해당

.NET PUPM SDK 는 권한 있는 계정 암호를 획득하고 체크 아웃/체크 인하는 C# 응용 프로그램을 작성할 수 있는 암호 소비자 SDK 입니다. 다른 운영 체제에 있는 권한 있는 계정에 대한 암호를 획득하고 체크 아웃/체크 인할 수 있지만 .NET PUPM SDK 는 CA Access Control 이 설치된 Windows 끝점에서만 사용할 수 있습니다. .NET PUPM SDK 를 사용하려면 끝점에 .NET Framework 2.0 이상을 설치해야 합니다.

.NET PUPM SDK 는 다음 디렉터리에 있습니다.

ACInstallDir\SDK\DOTNET

이 디렉터리에는 다음 항목이 들어 있습니다.

- Pupmcsharpsdk.dll - C# 응용 프로그램에 포함하는 SDK 라이브러리
- Examples - 권한 있는 계정 암호를 체크 아웃/체크 인하는 샘플 응용 프로그램이 들어 있는 폴더

  각 샘플 응용 프로그램은 컴파일되지 않은 샘플(.cs 파일)과 컴파일된 샘플(.exe 파일)을 포함합니다.

응용 프로그램이 권한 있는 계정 암호를 획득하고 체크 아웃/체크 인할 수 있도록 하려면 먼저 CA Access Control 엔터프라이즈 관리에서 응용 프로그램에 대한 소프트웨어 개발자 키트(SDK/CLI) 암호 소비자를 만들어야 합니다.

웹 서비스 PUPM SDK

웹 서비스 PUPM SDK 는 권한 있는 계정 암호를 체크 인/체크 아웃하는 Java 응용 프로그램을 작성할 수 있게 해 줍니다. 웹 서비스 PUPM SDK 는 CA Access Control 이 설치되지 않은 끝점(예: 메인프레임 끝점)에서 사용할 수 있습니다.

웹 서비스 PUPM SDK 응용 프로그램을 사용하여 권한 있는 계정 암호를 체크 아웃 또는 체크 인할 수 있으려면 먼저 CA Access Control 엔터프라이즈 관리에 응용 프로그램을 나타내는 사용자를 만든 다음 이 사용자에게 적절한 권한 있는 액세스 역할을 할당해야 합니다.

웹 서비스 PUPM SDK 를 사용하려면 끝점에서 다음과 같은 구성 요소를 설치해야 합니다.

- Apache Ant 1.7
- Apache Axis 1.4
- Java SDK 1.4.2
- (선택 사항) 통합된 개발 환경(IDE). 예: Eclipse

웹 서비스 PUPM SDK 는 다음 디렉터리에 있습니다.

ACServerInstallDir/IAM Suite/Access Control/tools/samples/webservice/Axis

이 디렉터리에는 웹 서비스 PUPM SDK 에 대한 다음과 같은 구성 요소가 포함되어 있습니다.

- Readme.txt - 환경을 구성하고, Java 샘플을 만들고, Java 샘플을 실행하는 방법에 대한 지침이 수록된 파일.
- build.xml - Apache Ant 빌드 스크립트
- build.properties - build.xml 에서 속성을 설정하는 파일
- CheckInPrivilegedAccount.java - 권한 있는 계정 암호를 체크 인하는 샘플 Java 응용 프로그램
- CheckOutPrivilegedAccount.java - 권한 있는 계정 암호를 체크 아웃하는 샘플 Java 응용 프로그램
- client-config.wsdd - 들어오고 나가는 모든 XML 메시지를 axis.log 란 이름의 파일에 저장하기 위해 Axis 를 구성하는 파일

  참고: 이 디렉터리에는 또한 다른 관리 작업(예: 권한 있는 계정 생성 또는 삭제)을 수행할 수 있게 해 주는 샘플 Java 응용 프로그램도 포함되어 있습니다.

웹 서비스 SDK 응용 프로그램이 암호를 가져오는 방법

웹 서비스 PUPM SDK 는 권한 있는 계정 암호를 체크 인/체크 아웃하는 Java 응용 프로그램을 작성할 수 있게 해 줍니다. 웹 서비스 PUPM SDK 응용 프로그램이 실행되는 끝점에 CA Access Control 을 설치할 필요는 없습니다. 하지만 암호 소비자 SDK 와 달리, 웹 서비스 PUPM SDK 는 암호를 캐싱하거나 사용자를 인증하지 않습니다.

웹 서비스 PUPM SDK 응용 프로그램은 SOAP(Simple Object Access Protocol) 및 포트 18080 을 사용하여 엔터프라이즈 관리 서버와 직접 통신합니다.

중요! 응용 프로그램과 엔터프라이즈 관리 서버 사이의 연결을 인증하려면 NTLM 과 같은 강력한 인증 프로토콜을 사용하는 것이 좋습니다.

다음 프로세스는 웹 서비스 PUPM SDK 응용 프로그램이 암호를 가져오는 방법을 설명합니다.

1. 응용 프로그램이 CA Access Control 엔터프라이즈 관리에 로그인합니다.

   응용 프로그램이 로그인하는 사용자 이름과 암호는 응용 프로그램에 정의되어 있습니다.
2. 응용 프로그램이 권한 있는 계정의 암호를 요청합니다.

3. CA Access Control 엔터프라이즈 관리가 응용 프로그램을 나타내는 사용자에 할당된 권한 있는 액세스 역할을 검사합니다.
4. 다음 중 *한 가지* 결과가 나타납니다.
   - 해당 권한 있는 액세스 역할이 있는 사용자가 권한 있는 계정 암호를 획득할 수 있으면 CA Access Control 엔터프라이즈 관리는 암호를 응용 프로그램으로 보냅니다.
   - 해당 권한 있는 액세스 역할이 있는 사용자가 권한 있는 계정 암호를 획득할 수 없으면 CA Access Control 엔터프라이즈 관리가 오류 메시지를 응용 프로그램으로 보냅니다.
5. 응용 프로그램이 CA Access Control 엔터프라이즈 관리에서 로그아웃합니다.

제 4 장: 권한 있는 계정 구현

이 섹션은 다음 항목을 포함하고 있습니다.

권한 있는 계정 설정 방법

권한 있는 사용자 암호 관리(PUPM)는 회사에서 가장 강력한 계정과 관련된 모든 활동을 추적하고, 관리하고, 보안을 유지하기 위한 프로세스입니다. 권한 있는 계정 암호를 사용하려면 먼저 PUPM 에 대해 CA Access Control 엔터프라이즈 관리를 설정하는 일부 단계를 완료해야 합니다. 그런 다음 사용자들이 정의된 권한 있는 계정을 사용하여 작업을 시작할 수 있게 됩니다.

다음 프로세스는 권한 있는 계정을 설정하기 위해 회사의 사용자들이 반드시 완료해야 하는 작업에 대해 설명합니다. 사용자에게는 각 프로세스 단계를 완료하기 위한 지정된 역할이 있어야 합니다. 시스템 관리자 관리 역할이 있는 사용자는 이 프로세스에서 모든 CA Access Control 엔터프라이즈 관리 작업을 수행할 수 있습니다.

참고: 이 프로세스를 시작하기 전에 CA Access Control 엔터프라이즈 관리에서 전자 메일 알림이 활성화되었는지 확인하십시오. CA Access Control 엔터프라이즈 관리가 사용자에게 암호를 표시할 수 없으면 대신 사용자에게 전자 메일로 암호를 보냅니다.

권한 있는 계정을 설정하려면 사용자가 다음을 수행해야 합니다.

1. PUPM 대상 시스템 관리자가 암호 정책을 만듭니다. 암호 정책은 권한 있는 계정에 대한 암호 규칙 및 제한을 설정합니다.
2. PUPM 대상 시스템 관리자가 CA Access Control 엔터프라이즈 관리에 끝점을 만듭니다. 끝점은 권한 있는 계정이 관리하는 장치입니다. CA Access Control 엔터프라이즈 관리에 끝점을 만들거나 PUPM 피더를 사용하여 끝점을 가져올 수 있습니다.

3. PUPM 대상 시스템 관리자는 각 끝점에 대한 권한 있는 계정을 만듭니다. 권한 있는 계정을 만들면 CA Access Control 엔터프라이즈 관리가 계정을 관리할 수 있습니다. CA Access Control 엔터프라이즈 관리에 권한 있는 계정을 만들거나 PUPM 피더를 사용하여 권한 있는 계정을 가져올 수 있습니다.

4. (선택 사항) 시스템 관리자가 로그인 응용 프로그램을 만들고 PUPM 대상 시스템 관리자가 로그인 응용 프로그램을 사용하기 위해 PUPM 끝점을 수정합니다. 로그인 응용 프로그램이 사용자가 CA Access Control 엔터프라이즈 관리에서 권한 있는 계정에 로그인할 수 있게 합니다.

5. PUPM 정책 관리자가 권한 있는 액세스 역할의 구성원 정책을 수정합니다. 구성원 정책은 역할에서 작업을 수행할 수 있는 사용자를 정의합니다.

   참고: 사용자 저장소로 Active Directory 를 사용하는 경우 해당 Active Directory 그룹을 가리키도록 각 구성원 정책을 수정하는 것이 좋습니다. 그런 다음 해당 Active Directory 그룹에서 추가 또는 제거하는 방법으로 역할에서 사용자를 추가 또는 제거할 수 있습니다. 이렇게 하면 관리 오버헤드를 크게 줄일 수 있습니다.

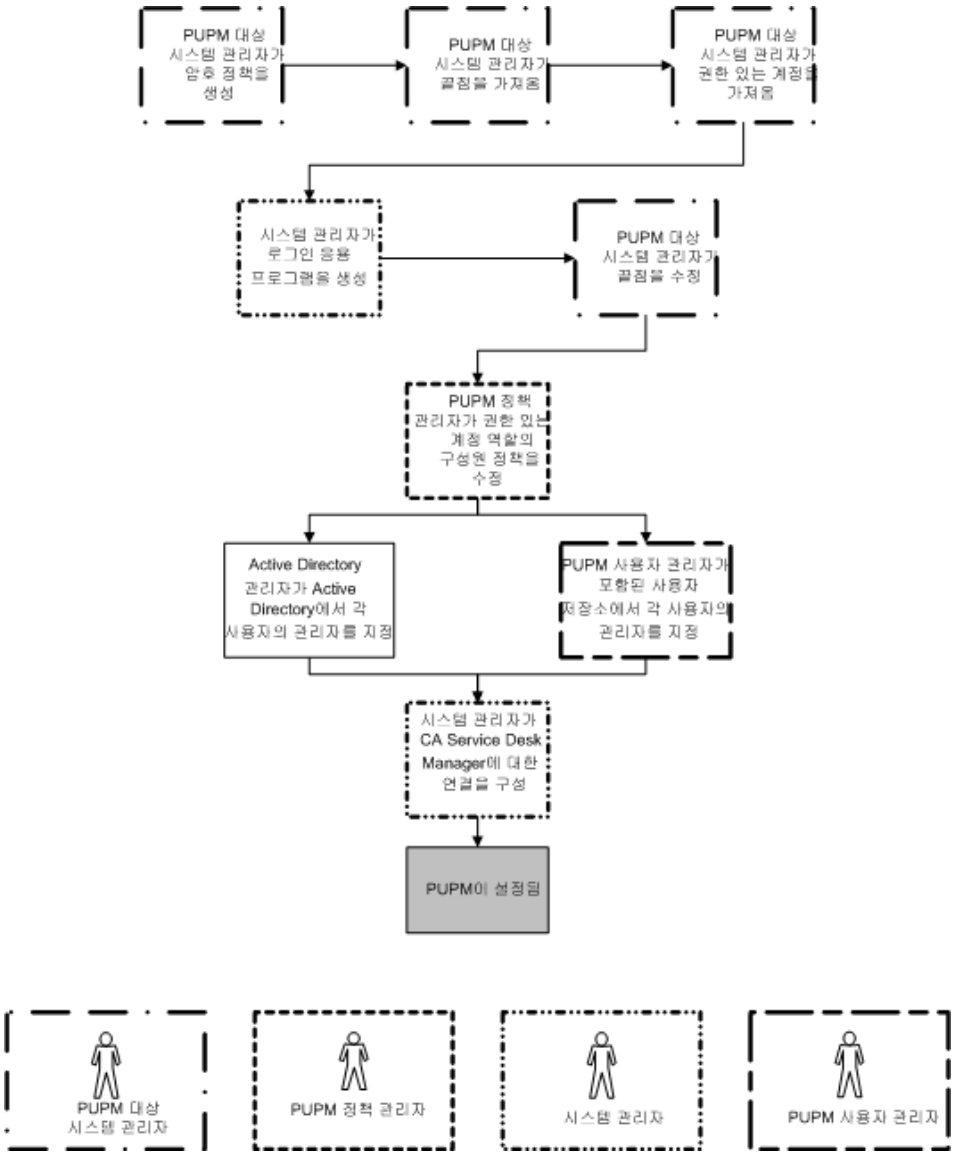
6. (포함된 사용자 저장소) PUPM 사용자 관리자는 각 사용자의 관리자를 지정합니다.

   참고: 관리자만 사용자의 권한 있는 계정 요청을 승인할 수 있습니다. 사용자 저장소로 Active Directory 를 사용하는 경우 각 사용자의 관리자가 Active Directory 에 지정되어 있는지 확인하십시오.

7. (선택 사항) 시스템 관리자는 Unicenter Service Desk 에 대한 연결을 구성합니다.

   Unicenter Service Desk 와 통합하면 권한 있는 계정 요청에 대한 여러 승인 프로세스를 만들 수 있습니다.

다음 다이어그램은 각 프로세스 단계를 수행하는 권한 있는 액세스 역할을 설명합니다.



권한 있는 계정 검색

끝점에서 권한 있는 계정을 검색할 때는 권한 있는 계정 검색 프로세스를 지정된 간격으로 실행하는 것이 좋습니다. 권한 있는 계정을 검색하면 동시에 여러 권한 있는 계정을 만들 수 있습니다. CA Access Control 엔터프라이즈 관리는 검색하는 계정을 표에 나타내므로 PUPM 을 사용하여 이미 관리하는 계정을 쉽게 파악할 수 있습니다.

끝점 유형에서 권한 있는 계정을 처음 발견했을 때 CA Access Control 엔터프라이즈 관리는 해당 끝점 유형에서 권한 있는 계정을 사용하기 위한 끝점 권한 있는 액세스 역할을 자동으로 만듭니다. 예를 들어, Windows Agentless 끝점에서 권한 있는 계정을 처음 발견했을 때 CA Access Control 엔터프라이즈 관리는 자동으로 Windows Agentless Connection 끝점 권한 있는 액세스 역할을 만듭니다.

다음 단계를 수행하십시오.

1. CA Access Control 엔터프라이즈 관리에서 "권한 있는 계정", "계정", "권한 있는 계정 검색 마법사"를 클릭합니다.

   "권한 있는 계정 검색 마법사: 권한 있는 계정 선택" 페이지가 나타납니다.

2. 목록에서 "끝점 유형"을 선택합니다.
3. 검색 특성을 선택하고 필터 값을 입력한 다음 "검색"을 클릭합니다.

   필터 조건에 일치하는 끝점의 목록이 표시됩니다.

4. 관리할 권한 있는 계정을 선택합니다.

   다음 표의 열 제목은 직관적으로 이해되지 않습니다.

   검색된 계정

   계정이 이미 CA Access Control 엔터프라이즈 관리에 알려져 있는지 여부를 지정합니다. 알려진 계정에는 CA Access Control 엔터프라이즈 관리가 이미 관리하는 계정과 CA Access Control 엔터프라이즈 관리가 끝점을 관리하기 위해 사용하는 관리자 계정을 포함합니다.

끝점 관리자

CA Access Control 엔터프라이즈 관리가 끝점을 관리하기 위해 계정을 사용하는지 여부를 지정합니다.

중요! 끝점 관리자 계정을 선택할 때는 주의하십시오. CA Access Control 엔터프라이즈 관리는 관리하는 권한 있는 계정의 암호를 자동으로 변경합니다. 끝점 관리자 계정을 선택하면 끝점에 있는 권한 있는 계정에 로그인하여 관리할 수 없게 됩니다.

"다음"을 클릭합니다.

"권한 있는 계정 검색 마법사: 일반 계정 세부 정보" 페이지가 나타납니다.

5. 대화 상자의 필드를 입력합니다. 다음 필드는 자동으로 채워지지 않습니다.

연결 해제된 시스템

계정이 연결 해제된 시스템에 있는지 여부를 지정합니다.

이 옵션을 선택하면 PUPM 이 해당 계정을 관리하지 않습니다. 대신, 연결 해제된 시스템의 권한 있는 계정을 위한 암호 저장소의 역할만 수행합니다. 암호를 변경할 때마다 관리되는 끝점에서도 계정 암호를 직접 변경해야 합니다.

암호 정책

권한 있는 계정 또는 서비스 계정에 적용할 암호 정책을 지정합니다.

체크 아웃 만료

체크 아웃 계정이 만료되는 기간(분)을 정의합니다.

배타적 계정

한 번에 하나의 사용자만 계정에 액세스할 수 있는지 여부를 지정합니다. *배타적 계정*은 한 번에 하나의 사용자만 권한 있는 계정을 사용하도록 제한합니다.

체크 아웃 시 암호 변경

CA Access Control 엔터프라이즈 관리가 권한 있는 계정을 체크 아웃할 때마다 이 계정 암호를 변경할지 여부를 지정합니다.

참고: 이 옵션은 서비스 계정에 적용되지 않습니다.

체크 인 시 암호 변경

사용자 또는 프로그램이 권한 있는 계정을 체크 인할 때마다 또는 체크 아웃 기간이 만료될 때 CA Access Control 엔터프라이즈 관리가 이 계정 암호를 변경할지 여부를 지정합니다.

참고: 배타적 계정이 아닌 경우 CA Access Control 엔터프라이즈 관리는 *모든* 사용자가 계정을 체크 인한 경우에만 새 권한 있는 계정 암호를 생성합니다.

참고: 이 옵션은 서비스 계정에 적용되지 않습니다.

6. "마침"을 클릭합니다.

   CA Access Control 엔터프라이즈 관리는 이 작업을 제출하고 오류가 없는 경우 선택된 권한 있는 계정을 만듭니다.

권한 있는 계정 만들기

관리되는 시스템 및 연결 해제된 시스템에서 계정 암호를 관리하기 위해 권한 있는 계정을 만듭니다. 권한 있는 계정을 사용하여 사용자가 권한 있는 계정 암호를 체크 아웃 및 체크 인하도록 합니다.

여러 계정을 만들려면 권한 있는 계정 검색 마법사를 사용하여 끝점에서 권한 있는 계정을 검색하십시오. 하나의 계정을 만들려면 이 창에서 권한 있는 계정 또는 서비스 계정의 상세 정보를 제공하십시오.

다음 단계를 수행하십시오.

1. CA Access Control 엔터프라이즈 관리에서 "권한 있는 계정", "계정", "권한 있는 계정 만들기"를 클릭합니다.

   "권한 있는 계정 만들기: 권한 있는 계정 선택" 페이지가 나타납니다.

2. (선택 사항) 다음과 같이 권한 있는 계정을 만들 때 복사하여 사용할 기존 권한 있는 계정을 선택합니다.

   a. "권한 있는 계정" 유형의 개체에 대한 복사본을 만들도록 선택합니다.

   b. 검색 특성을 선택하고 필터 값을 입력한 다음 "검색"을 클릭합니다.

      필터 조건에 일치하는 권한 있는 계정의 목록이 표시됩니다.

   c. 새로운 권한 있는 계정을 만들 때 기초로 사용할 개체를 선택합니다.

3. "확인"을 클릭합니다.

   "권한 있는 계정 만들기" 작업 페이지의 "일반" 탭이 나타납니다. 기존 개체에서 권한 있는 계정을 만든 경우 대화 상자 필드에는 기존 개체에서 가져온 값이 자동으로 입력됩니다.

4. "일반" 탭에서 다음 필드를 완성합니다.

   계정 이름

   이 권한 있는 계정에 대한 이름을 정의합니다.

   참고: RACF, ACF, Top Secret 과 같은 메인프레임 시스템은 사용자 이름에 대/소문자를 구분합니다. 계정 이름을 대문자로 입력하십시오.

연결 해제된 계정

계정이 연결 해제된 시스템에 있는지 여부를 지정합니다.

이 옵션을 선택하면 PUPM 이 해당 계정을 관리하지 않습니다. 대신, 연결 해제된 시스템의 권한 있는 계정을 위한 암호 저장소의 역할만 수행합니다. 암호를 변경할 때마다 관리되는 끝점에서도 계정 암호를 변경해야 합니다.

계정 유형

계정이 공유 (권한 있는) 계정인지 또는 서비스 계정인지 여부를 지정합니다.

참고: 서비스 계정을 만들 때 PUPM 은 계정 암호를 변경하려고 시도하지 않습니다.

끝점 이름

권한 있는 계정이 있는 정의된 끝점의 이름을 지정합니다. CA Access Control 엔터프라이즈 관리는 지정한 유형의 끝점만 나열합니다.

끝점 유형

권한 있는 계정 또는 서비스 계정이 있는 끝점의 유형을 지정합니다.

컨테이너

권한 있는 계정 또는 서비스 계정에 대한 컨테이너의 이름을 지정합니다. *컨테이너*는 인스턴스가 다른 개체의 컬렉션인 클래스입니다. 컨테이너는 특정 액세스 규칙에 따라 개체를 체계적인 방식으로 저장하기 위해 사용됩니다.

암호 정책

권한 있는 계정 또는 서비스 계정에 적용할 암호 정책을 지정합니다.

암호

새 권한 있는 계정과 함께 사용할 암호를 정의하고 검사합니다.

참고: 새 암호는 지정하는 암호 정책을 준수해야 합니다.

체크 아웃 만료

체크 아웃 계정이 만료되는 기간(분)을 정의합니다.

배타적 계정

한 번에 하나의 사용자만 계정에 액세스할 수 있는지 여부를 지정합니다. *배타적 계정*은 한 번에 하나의 사용자만 권한 있는 계정을 사용하도록 제한합니다.

체크 아웃 시 암호 변경

CA Access Control 엔터프라이즈 관리가 권한 있는 계정을 체크 아웃할 때마다 이 계정 암호를 변경할지 여부를 지정합니다.

참고: 이 옵션은 서비스 계정에 적용되지 않습니다.

체크 인 시 암호 변경

사용자 또는 프로그램이 권한 있는 계정을 체크 인할 때마다 또는 체크 아웃 기간이 만료될 때 CA Access Control 엔터프라이즈 관리가 이 계정 암호를 변경할지 여부를 지정합니다.

참고: 배타적 계정이 아닌 경우 CA Access Control 엔터프라이즈 관리는 *모든* 사용자가 계정을 체크 인한 경우에만 새 권한 있는 계정 암호를 생성합니다.

참고: 이 옵션은 서비스 계정에 적용되지 않습니다.

로그인 응용 프로그램 체크 아웃만

로그인 응용 프로그램이 끝점에 대해 정의된 경우에만 암호 체크 아웃을 허용할지 여부를 지정합니다.

참고: 이 옵션이 사용된 경우 사용자는 암호를 클립보드에 복사하거나 표시할 수 없습니다.

"제출"을 클릭합니다.

CA Access Control 엔터프라이즈 관리가 새 권한 있는 계정을 만듭니다.

암호 정책 만들기

권한 있는 계정에 대한 암호 정책은 권한 있는 계정의 허용되는 암호를 결정하는 일련의 규칙 및 제한입니다. 예를 들어, 길이가 8 자 이상이고 숫자 및 문자를 포함하도록 암호를 규정하는 정책을 구성할 수 있습니다. 암호 정책은 또한 CA Access Control 엔터프라이즈 관리가 계정에 대한 새 암호를 자동으로 만드는 간격을 결정합니다.

참고: CA Access Control 엔터프라이즈 관리에는 미리 정의된 암호 정책이 포함되어 있습니다. 회사의 보안 요구 사항을 충족하고 각 끝점에 적절한 암호 정책을 정의하여 사용하는 것이 좋습니다.

암호 정책을 만들려면

1. CA Access Control 엔터프라이즈 관리에서 "권한 있는 계정", "암호 정책", "암호 정책 만들기"를 차례로 클릭합니다.

   "암호 정책 만들기: 표준 검색 구성 화면" 페이지가 나타납니다.

2. (선택 사항) 다음과 같이 암호 정책을 만들 때 복사하여 사용할 기존 암호 정책을 선택합니다.

   a. "권한 있는 계정 암호 정책" 유형의 개체 복사본 만들기를 선택한 다음 "검색"을 클릭합니다.

      암호 정책의 목록이 표시됩니다.

   b. 새 암호 정책을 만들 때 기초로 사용할 개체를 선택합니다.

3. "확인"을 클릭합니다.

   "암호 정책 만들기" 작업 페이지가 나타납니다. 기존 개체에서 암호 정책을 만든 경우 대화 상자 필드에는 기존 개체에서 가져온 값이 자동으로 입력됩니다.

4. 암호 정책의 이름과 선택적 설명을 입력합니다.

5. (선택 사항) 활성화 표시를 지웁니다.

   기본적으로 새 암호 정책은 활성화되어 있습니다. 만드는 정책이 아직 승인되지 않은 경우 이 확인란을 선택할 수 없으며 정책을 비활성화된 상태로 두십시오.

6. 암호 조합 규칙을 정의합니다.

7. (선택 사항) 암호 만료 간격을 정의합니다.

   이 간격은 CA Access Control 엔터프라이즈 관리가 암호를 자동으로 변경하는 일반 간격입니다. 기본적으로 만료 간격은 비활성화(0 으로 설정)되어 있습니다.

8. (선택 사항) CA Access Control 엔터프라이즈 관리가 암호를 변경할 시간을 24 시간 형식으로 정의합니다.

   예를 들어, 서비스 계정에 대한 암호 정책을 만드는 경우 CA Access Control 엔터프라이즈 관리가 일요일 오후 10:00 에서 오후 11:59 사이에만 계정의 암호를 변경하도록 지정할 수 있습니다.

9. "제출"을 클릭합니다.

   CA Access Control 엔터프라이즈 관리가 암호 정책을 만듭니다.

추가 정보:

암호 조합 규칙 (페이지 95)

암호 조합 규칙

암호 정책을 만들 때 새 암호에 대한 내용 요구 사항을 정의할 수 있습니다.

중요! 암호 조합 규칙을 구성하는 경우 요구 사항을 설정할 때 최대 암호 길이를 고려하십시오. 필요한 문자의 전체 개수가 최대 암호 길이를 초과하면 모든 암호가 거부됩니다.

CA Access Control 엔터프라이즈 관리는 권한 있는 계정에 대한 다음과 같은 암호 조합 규칙을 제공합니다.

최소 암호 길이

암호에 들어가야 하는 문자의 최소 수를 정의합니다.

최대 암호 길이

암호에 들어갈 수 있는 문자의 최대 수를 정의합니다.

최대 반복 문자

암호에 들어갈 수 있는 반복되는 문자의 최대 수를 정의합니다.

예를 들어, 이 값을 3 으로 설정하면 문자열 "aaa"는 암호에 사용될 수 없지만 "aa"는 사용될 수 있습니다.

대문자(패턴: u)

암호에 대문자를 포함할 수 있는지 여부를 지정하고, 포함할 수 있는 경우 암호에 포함해야 하는 최소 대문자 수를 정의합니다.

소문자(패턴: c)

암호에 소문자를 포함할 수 있는지 여부를 지정하고, 포함할 수 있는 경우 암호에 포함해야 하는 최소 소문자 수를 정의합니다.

문자(패턴: l)

암호에 영문자를 포함할 수 있는지 여부를 지정하고, 포함할 수 있는 경우 암호에 포함해야 하는 최소 영문자 수를 정의합니다.

숫자(패턴: d)

암호에 숫자를 포함할 수 있는지 여부를 지정하고, 포함할 수 있는 경우 암호에 포함해야 하는 최소 숫자 수를 정의합니다.

문자 또는 숫자(패턴: a)

암호에 영숫자를 포함할 수 있는지 여부를 지정하고, 포함할 수 있는 경우 암호에 포함해야 하는 최소 영숫자 수를 정의합니다.

문장 부호(패턴: p)

암호에 문장 부호 또는 특수 문자(비영숫자)를 포함할 수 있는지 여부를 지정하고, 포함할 수 있는 경우 암호에 포함해야 하는 이러한 문자 수를 정의합니다.

모두(패턴: *)

암호가 모든 문자를 포함할 수 있도록 지정합니다. 이 옵션을 선택하면 CA Access Control 엔터프라이즈 관리는 자동으로 다른 모든 문자 내용 정의를 선택합니다.

패턴 사용

문자 내용 정의를 정의하는 대신 암호에 반드시 사용해야 하는 패턴을 정의하도록 지정합니다.

예:

- **uuuuu** - ASDKF 또는 IUTYE 에 일치
- **ucdddp** - Rv671* 또는 Uc194^에 일치
- ********** - lkI&5Jj@ 또는 sffIU*&1 에 일치
- **lllaaaa** - yuUI1Uo3 또는 qWcV1Er6 에 일치

금지된 문자

권한 있는 계정 암호를 만들거나 수정할 때 사용할 수 없는 문자를 정의합니다.

PUPM 끝점 및 권한 있는 계정 만들기

다음 항목은 CA Access Control 엔터프라이즈 관리에서 끝점을 만들고, 권한 있는 계정을 만들고 검색하고, 로그인 응용 프로그램을 만드는 방법을 설명합니다.

여러 PUPM 끝점 또는 권한 있는 계정을 만들거나 수정하려면 PUPM 피더의 사용을 고려하십시오. PUPM 피더를 사용하면 한 단계로 많은 끝점 및 권한 있는 계정을 가져올 수 있으며, PUPM 끝점 및 권한 있는 계정의 관리를 자동화할 수 있습니다.

끝점 만들기

CA Access Control 엔터프라이즈 관리에 끝점 정의를 만들면 끝점을 관리하고 끝점에 있는 권한 있는 계정 및 서비스 계정을 검색할 수 있습니다.

다음 단계를 수행하십시오.

1. CA Access Control 엔터프라이즈 관리에서 "권한 있는 계정", "끝점", "끝점 만들기"를 클릭합니다.

   "끝점 만들기: 끝점 선택" 페이지가 나타납니다.

2. (선택 사항) 다음과 같이 끝점을 만들 때 복사하여 사용할 기존 끝점을 선택합니다.

   a. "끝점" 유형의 개체에 대한 복사본을 만들도록 선택합니다.

   b. 검색 특성을 선택하고 필터 값을 입력한 다음 "검색"을 클릭합니다.

      필터 조건에 일치하는 끝점의 목록이 표시됩니다.

   c. 새 끝점을 만들 때 기초로 사용할 개체를 선택합니다.

3. "확인"을 클릭합니다.

   "끝점 만들기" 작업 페이지의 "일반" 탭이 나타납니다. 기존 개체에서 끝점을 만든 경우 대화 상자 필드에는 기존 개체에서 가져온 값이 자동으로 입력됩니다.

4. 이 탭에 있는 필드를 완성합니다. 다음 필드는 자동으로 채워지지 않습니다.

   이름

   끝점의 논리적 이름을 정의합니다.

   참고: 이 필드는 끝점이 이름이 CA Access Control 엔터프라이즈 관리에 나타나는 방식을 정의합니다. 끝점 유형을 선택할 때 연결 정보를 지정합니다.

   설명

   (선택 사항) 이 끝점에 대해 기록하려는 정보(일반 텍스트)를 정의합니다.

   끝점 유형

   권한 있는 계정 또는 서비스 계정이 있는 끝점의 유형을 지정합니다.

   참고: 끝점 유형을 선택할 때 PUPM 이 해당 끝점에서 권한 있는 계정을 관리하는 데 필요한 자격 증명을 제공하도록 요청받습니다. 선택하는 끝점 유형은 제공해야 하는 연결 정보에 영향을 줍니다.

   관리되는 장치

   (선택 사항) PUPM 끝점과 CA Access Control for Virtual Environments 관리되는 장치를 연결할지 여부를 지정합니다.

5. (선택 사항) "로그인 응용 프로그램" 탭을 클릭한 다음 이 탭에 있는 필드를 완성합니다.

   로그인 응용 프로그램

   로그인 응용 프로그램을 이 끝점에 할당하도록 지정합니다.

   참고: 끝점에 할당하기 전에 로그인 응용 프로그램을 만드십시오. 동일한 끝점에 여러 개의 로그인 응용 프로그램을 할당할 수 있습니다.

6. (선택 사항) "정보" 탭을 클릭하고 탭에 있는 필드를 완성합니다.

   이 탭에서는 끝점 관련 특성을 지정하여 권한 있는 액세스 역할을 정의 또는 수정할 때 이 특성을 사용할 수 있습니다.

   액세스 권한 있는 역할의 구성원이 CA Access Control 엔터프라이즈 관리에 로그인할 때 사용자는 권한 있는 액세스 역할에 정의된 특성에 따라 권한 있는 액세스 계정에 대한 액세스를 획득합니다.

   소유자

   끝점 소유자의 이름을 지정합니다.

부서

부서의 이름을 지정합니다.

예: 개발부

사용자 지정 1...5

최대 5 개까지 사용자 지정 끝점 관련 특성을 지정합니다.

참고: 권한 있는 계정 "구성원" 탭, "구성원 정책" 섹션, "구성원 역할" 창에서 사용자 지정 특성을 정의하십시오.

7. "제출"을 클릭합니다.

CA Access Control 엔터프라이즈 관리는 제공한 자격 증명을 사용하여 끝점에 연결하려고 시도합니다. 연결이 성공하면 끝점이 만들어집니다. 연결이 실패하면 연결 오류 메시지를 받습니다.

관련 항목:

PUPM 용 Access Control 연결 정보 (페이지 99)
VMware ESX/ESXi 연결 정보 (페이지 101)
Windows Agentless Connection 정보 (페이지 106)
CA Identity Manager 프로비저닝 연결 정보 (페이지 123)
연결 해제된 끝점 연결 정보 (페이지 126)

PUPM 용 Access Control 연결 정보

PUPM 용 Access Control 끝점 유형을 사용하면 권한 있는 Access Control 계정을 관리할 수 있습니다.

이 유형의 끝점을 만들 때는 CA Access Control 엔터프라이즈 관리가 끝점에 연결할 수 있도록 다음 정보를 제공하십시오.

사용자 로그인

끝점의 관리 사용자 이름을 정의합니다. PUPM 은 이 계정을 사용하여 끝점에서 관리 작업(끝점에 연결하고, 계정을 검색하고, 암호를 변경하는 등의 작업)을 수행합니다.

참고: "고급" 옵션을 지정하면 PUPM 은 관리 작업을 수행하기 위해 "사용자 로그인" 계정을 사용하지 않습니다. 대신, PUPM 은 지정된 권한 있는 계정을 사용하여 끝점에서 관리 작업을 수행합니다.

암호

끝점의 관리 사용자 암호를 정의합니다.

호스트

끝점의 호스트 이름을 정의합니다.

호스트 도메인

이 호스트가 구성원으로 속한 도메인의 이름을 지정합니다.

예: Domain.com

고급

권한 있는 관리 계정을 사용하여 끝점에서 관리 작업(끝점에 연결하고, 계정을 검색하고, 암호를 변경하는 등의 작업)을 수행할지 여부를 지정합니다. 예를 들어, 여러 끝점에서 관리 작업을 수행할 수 있는 권한 있는 도메인 계정을 지정할 수 있습니다.

이 옵션을 지정하면 PUPM 은 관리 작업을 수행하기 위해 "사용자 로그인" 계정을 사용하지 않습니다.

VMware ESX/ESXi 연결 정보

VMware ESX/ESXi 끝점 유형을 사용하면 권한 있는 VMware ESX/ESXi 계정을 관리할 수 있습니다.

이 유형의 끝점을 만들 때는 CA Access Control for Virtual Environments 가 끝점에 연결할 수 있도록 다음 정보를 제공하십시오.

사용자 이름

끝점의 관리 사용자 이름을 정의합니다. CA Access Control 엔터프라이즈 관리는 이 계정을 사용하여 끝점에서 관리 작업(끝점에 연결하고, 계정을 검색하고, 암호를 변경하는 등의 작업)을 수행합니다.

참고: "고급" 옵션을 지정하면 PUPM 은 관리 작업을 수행하기 위해 "사용자 로그인" 계정을 사용하지 않습니다. 대신, PUPM 은 지정된 권한 있는 계정을 사용하여 끝점에서 관리 작업을 수행합니다.

암호

끝점의 관리 사용자 암호를 정의합니다.

호스트

끝점의 호스트 이름을 정의합니다.

고급

권한 있는 관리 계정을 사용하여 끝점에서 관리 작업(끝점에 연결하고, 계정을 검색하고, 암호를 변경하는 등의 작업)을 수행할지 여부를 지정합니다. 예를 들어, 여러 끝점에서 관리 작업을 수행할 수 있는 권한 있는 도메인 계정을 지정할 수 있습니다.

이 옵션을 지정하면 PUPM 은 관리 작업을 수행하기 위해 "사용자 로그인" 계정을 사용하지 않습니다.

MS SQL Server 연결 정보

MS SQL Server 끝점 유형을 사용하면 권한 있는 Microsoft SQL Server 계정을 관리할 수 있습니다.

MS SQL Server 끝점에 대해 지정하는 관리 사용자는 다음 조건을 충족해야 합니다.

- securityadmin 서버 역할이 있어야 합니다.

참고: securityadmin 서버 역할이 있는 사용자는 serveradmin 및 sysadmin 서버 역할을 수정할 수 없습니다.

이 유형의 끝점을 만들 때는 CA Access Control 엔터프라이즈 관리가 끝점에 연결할 수 있도록 다음 정보를 제공하십시오.

사용자 로그인

끝점의 관리 사용자 이름을 정의합니다. PUPM 은 이 계정을 사용하여 끝점에서 관리 작업(끝점에 연결하고, 계정을 검색하고, 암호를 변경하는 등의 작업)을 수행합니다.

참고: "고급" 옵션을 지정하면 PUPM 은 관리 작업을 수행하기 위해 "사용자 로그인" 계정을 사용하지 않습니다. 대신, PUPM 은 지정된 권한 있는 계정을 사용하여 끝점에서 관리 작업을 수행합니다.

암호

끝점의 관리 사용자 암호를 정의합니다.

URL

CA Access Control 엔터프라이즈 관리가 끝점에 연결하기 위해 사용할 수 있는 URL 을 정의합니다. URL 은 데이터베이스 서버의 특정 유형을 지정합니다.

형식: jdbc:sqlserver://*servername*:*port*

예: jdbc:sqlserver://localhost:1433

참고: URL 의 형식에 대한 자세한 내용은 끝점 설명서를 참조하십시오.

호스트

끝점의 호스트 이름을 정의합니다.

참고: CA Access Control 이 끝점에 설치된 경우 이 특성에 대해 CA Access Control 호스트 이름을 지정하는 것이 좋습니다. 월드 뷰를 사용하여 끝점의 CA Access Control 호스트 이름을 볼 수 있습니다.

포트

(선택 사항) 서버 수신 포트 번호를 지정합니다. 지정하는 포트 번호는 URL 에 지정하는 포트 번호와 일치해야 합니다.

예: 1433

인스턴스 이름

(선택 사항) 데이터베이스 인스턴스 이름을 지정합니다.

고급

권한 있는 관리 계정을 사용하여 끝점에서 관리 작업(끝점에 연결하고, 계정을 검색하고, 암호를 변경하는 등의 작업)을 수행할지 여부를 지정합니다. 예를 들어, 여러 끝점에서 관리 작업을 수행할 수 있는 권한 있는 도메인 계정을 지정할 수 있습니다.

이 옵션을 지정하면 PUPM 은 관리 작업을 수행하기 위해 "사용자 로그인" 계정을 사용하지 않습니다.

Oracle 서버 연결 정보

Oracle 서버 끝점 유형을 사용하면 권한 있는 Oracle 데이터베이스 계정을 관리할 수 있습니다.

Oracle 서버 끝점에 대해 지정하는 관리 사용자는 ALTER USER 및 SELECT ANY DIRECTORY 시스템 권한이 있어야 합니다.

이 유형의 끝점을 만들 때는 CA Access Control 엔터프라이즈 관리가 끝점에 연결할 수 있도록 다음 정보를 제공하십시오.

사용자 로그인

끝점의 관리 사용자 이름을 정의합니다. PUPM 은 이 계정을 사용하여 끝점에서 관리 작업(끝점에 연결하고, 계정을 검색하고, 암호를 변경하는 등의 작업)을 수행합니다.

참고: "고급" 옵션을 지정하면 PUPM 은 관리 작업을 수행하기 위해 "사용자 로그인" 계정을 사용하지 않습니다. 대신, PUPM 은 지정된 권한 있는 계정을 사용하여 끝점에서 관리 작업을 수행합니다.

암호

끝점의 관리 사용자 암호를 정의합니다.

URL

CA Access Control 엔터프라이즈 관리가 끝점에 연결하기 위해 사용할 수 있는 URL 을 정의합니다. URL 은 데이터베이스 서버의 특정 유형을 지정합니다.

형식: jdbc:oracle:*drivertype*:@*hostname*:*port*:*service*

예: jdbc:oracle:thin:@ora.comp.com:1521:orcl

참고: URL 의 형식에 대한 자세한 내용은 끝점 설명서를 참조하십시오.

호스트

끝점의 호스트 이름을 정의합니다. 이 이름은 정규화된 호스트 이름입니다.

참고: CA Access Control 이 끝점에 설치된 경우 이 특성에 대해 CA Access Control 호스트 이름을 지정하는 것이 좋습니다. 월드 뷰를 사용하여 끝점의 CA Access Control 호스트 이름을 볼 수 있습니다.

고급

권한 있는 관리 계정을 사용하여 끝점에서 관리 작업(끝점에 연결하고, 계정을 검색하고, 암호를 변경하는 등의 작업)을 수행할지 여부를 지정합니다. 예를 들어, 여러 끝점에서 관리 작업을 수행할 수 있는 권한 있는 도메인 계정을 지정할 수 있습니다.

이 옵션을 지정하면 PUPM 은 관리 작업을 수행하기 위해 "사용자 로그인" 계정을 사용하지 않습니다.

Sybase 서버 연결 정보

Sybase 서버 끝점 유형을 사용하면 권한 있는 Sybase 서버 계정을 관리할 수 있습니다.

중요! 데이터베이스가 적절히 구성되었고 포트 2638 이 연결에 대해 열려 있는지 확인합니다.

이 유형의 끝점을 만들 때는 CA Access Control 엔터프라이즈 관리가 끝점에 연결할 수 있도록 다음 정보를 제공하십시오.

사용자 로그인

끝점의 관리 사용자 이름을 정의합니다. PUPM 은 이 계정을 사용하여 끝점에서 관리 작업(끝점에 연결하고, 계정을 검색하고, 암호를 변경하는 등의 작업)을 수행합니다.

참고: "고급" 옵션을 지정하면 PUPM 은 관리 작업을 수행하기 위해 "사용자 로그인" 계정을 사용하지 않습니다. 대신, PUPM 은 지정된 권한 있는 계정을 사용하여 끝점에서 관리 작업을 수행합니다.

암호

끝점의 관리 사용자 암호를 정의합니다.

URL

CA Access Control 엔터프라이즈 관리가 끝점에 연결하기 위해 사용할 수 있는 URL 을 정의합니다. URL 은 데이터베이스 서버의 특정 유형을 지정합니다.

형식: jdbc:sybase:Tds:*servername*:*port*

예: jdbc:sybase:Tds:localhost:2638

참고: URL 의 형식에 대한 자세한 내용은 끝점 설명서를 참조하십시오.

호스트

끝점의 호스트 이름을 정의합니다.

참고: CA Access Control 이 끝점에 설치된 경우 이 특성에 대해 CA Access Control 호스트 이름을 지정하는 것이 좋습니다. 월드 뷰를 사용하여 끝점의 CA Access Control 호스트 이름을 볼 수 있습니다.

고급

권한 있는 관리 계정을 사용하여 끝점에서 관리 작업(끝점에 연결하고, 계정을 검색하고, 암호를 변경하는 등의 작업)을 수행할지 여부를 지정합니다. 예를 들어, 여러 끝점에서 관리 작업을 수행할 수 있는 권한 있는 도메인 계정을 지정할 수 있습니다.

이 옵션을 지정하면 PUPM 은 관리 작업을 수행하기 위해 "사용자 로그인" 계정을 사용하지 않습니다.

Windows Agentless Connection 정보

Windows Agentless 끝점 유형을 사용하면 권한 있는 Windows 계정을 관리할 수 있습니다.

참고: 로컬 컴퓨터에서 도메인 사용자를 구성하는 경우 PUPM 은 도메인 사용자의 암호를 변경할 수 없습니다. 이 제한 사항은 Windows 의 특성에 기인합니다.

이 유형의 끝점을 만들 때는 CA Access Control 엔터프라이즈 관리가 끝점에 연결할 수 있도록 다음 정보를 제공하십시오.

사용자 로그인

끝점의 관리 사용자 이름을 정의합니다. PUPM 은 이 계정을 사용하여 끝점에서 관리 작업(끝점에 연결하고, 계정을 검색하고, 암호를 변경하는 등의 작업)을 수행합니다.

참고: "고급" 옵션을 지정하면 PUPM 은 관리 작업을 수행하기 위해 "사용자 로그인" 계정을 사용하지 않습니다. 대신, PUPM 은 지정된 권한 있는 계정을 사용하여 끝점에서 관리 작업을 수행합니다.

암호

끝점의 관리 사용자 암호를 정의합니다.

호스트

끝점의 호스트 이름을 정의합니다.

예: myhost-ac-1

호스트 도메인

이 호스트가 구성원으로 포함된 도메인 이름을 지정합니다.

참고: 호스트 도메인 이름은 접두사만 사용하여 지정하십시오. 예를 들어, 전체 도메인 이름이 company.com 인 경우 접두사인 company 만 입력합니다.

Active Directory

사용자 계정이 Active Directory 계정인지 여부를 지정합니다.

사용자 도메인

사용자가 구성원으로 포함된 도메인 이름을 지정합니다.

참고: 사용자 도메인 이름은 접두사만 사용하여 지정하십시오. 예를 들어, 전체 도메인 이름이 company.com 인 경우 접두사인 company 만 입력합니다.

중요! PUPM 자동 로그인을 사용하여 끝점에 로그인하려는 경우 호스트 도메인 이름을 지정해야 합니다. 끝점이 워크그룹의 구성원인 경우 워크그룹 이름이 아닌 호스트 이름을 지정하십시오.

고급

권한 있는 관리 계정을 사용하여 끝점에서 관리 작업(끝점에 연결하고, 계정을 검색하고, 암호를 변경하는 등의 작업)을 수행할지 여부를 지정합니다. 예를 들어, 여러 끝점에서 관리 작업을 수행할 수 있는 권한 있는 도메인 계정을 지정할 수 있습니다.

이 옵션을 지정하면 PUPM 은 관리 작업을 수행하기 위해 "사용자 로그인" 계정을 사용하지 않습니다.

PUPM 에 대한 Windows Agentless 끝점 구성

다음 항목은 PUPM 을 구현하기 전에 Windows Agentless 끝점에서 수행해야 하는 추가 구성 단계에 대해 설명합니다.

추가 정보:

Windows Agentless 끝점의 도메인 사용자에 대한 제한 사항 (페이지 71)

Windows Agentless 끝점의 방화벽 구성

Windows Server 2008 및 Windows 7 Enterprise 에 해당

PUPM Windows Agentless 커넥터는 포트 135(DCOM 포트)를 사용하여 Windows Agentless 끝점에 연결합니다. PUPM Windows Agentless 커넥터는 JCS 의 일부입니다. 커넥터는 끝점에 연결한 다음 동적 포트(1000 보다 큼)를 사용하여 WMI(Windows Management Instrumentation) 서비스와 통신합니다.

Windows 방화벽이 Windows Agentless 끝점에서 사용되면 방화벽은 포트 135 와 동적 포트에 대한 연결 모두를 차단할 수 있습니다. Windows 방화벽에 의해 이러한 연결이 차단되는 경우 엔터프라이즈 관리 서버는 끝점과 통신할 수 없습니다. 따라서 끝점에서 서비스 계정 및 예약된 작업을 검색할 수 없거나 Windows Agentless 끝점을 만들 수 없습니다.

Windows 방화벽이 사용되는 경우, PUPM Windows Agentless 커넥터가 끝점에 연결할 수 있도록 방화벽을 구성하십시오. 방화벽을 구성할 때는 포트 135 를 열고 방화벽이 동적 RPC 포트에서 WMI 서비스에 도달하는 모든 트래픽을 허용하도록 지정하십시오.

추가 정보:

PUPM 에 대한 Windows 방화벽 구성 방법 (페이지 108)

PUPM 에 대한 Windows 방화벽 구성 방법

Windows Agentless 끝점에 해당

PUPM Windows Agentless 커넥터는 포트 135(DCOM 포트)를 사용하여 Windows Agentless 끝점에 연결합니다. 커넥터는 끝점에 연결한 다음 동적 포트(1000 보다 큼)를 사용하여 WMI(Windows Management Instrumentation) 서비스와 통신합니다.

Windows 방화벽이 사용되는 경우, PUPM Windows Agentless 커넥터가 끝점에 연결할 수 있도록 방화벽을 구성해야 합니다. 방화벽을 구성하지 않으면 엔터프라이즈 관리 서버는 끝점과 통신할 수 없습니다.

PUPM 에 대해 Windows 방화벽을 구성하려면 다음을 수행하십시오.

1. 포트 135 를 엽니다.
2. 방화벽이 동적 RPC 포트에서 WMI 서비스에 도달하는 모든 트래픽을 허용하도록 방화벽 규칙을 만듭니다.

   Windows 방화벽을 구성하는 데 도움이 되도록 다음 예제의 정보를 사용하십시오.

예: 포트 135 열기

다음 예는 Windows Server 2008 컴퓨터에서 포트 135 를 여는 방법을 설명합니다.

1. "시작", "제어판", "Windows 방화벽"을 차례로 클릭합니다.

   "Windows 방화벽" 대화 상자가 나타납니다.
2. "설정 변경"을 클릭합니다.

   "Windows 방화벽" 설정 대화 상자가 나타납니다.
3. "예외" 탭을 클릭한 후 "포트 추가"를 클릭합니다.

   "포트 추가" 대화 상자가 나타납니다.
4. 다음과 같이 대화 상자를 완료합니다.
   - "이름" 필드에서 **DCOM_TCP135** 를 입력합니다.
   - "포트 번호" 필드에서 **135** 를 입력합니다.
   - "프로토콜" 섹션에서 "TCP"를 선택합니다.

   "확인"을 클릭합니다.

   "예외" 탭에 "DCOM_TCP135" 규칙이 나타납니다.
5. "확인"을 클릭합니다.

   "Windows 방화벽" 설정 대화 상자가 닫힙니다. 포트 135 를 열었습니다.

예: 동적 RPC 포트에서 WMI 서비스에 도달하는 트래픽을 허용하는 방화벽 규칙 만들기

다음 예는 Windows Server 2008 컴퓨터에서 방화벽 규칙을 만드는 방법을 보여줍니다. 방화벽 규칙은 동적 RPC 포트에서 WMI 서비스에 도달하는 트래픽을 허용합니다.

1. "시작", "관리 도구", "Windows 방화벽", "고급 보안이 포함된 Windows 방화벽"을 클릭합니다.

   "고급 보안이 포함된 Windows 방화벽" 대화 상자가 열립니다.

2. 왼쪽 창에서 "인바운드 규칙"을 마우스 오른쪽 단추로 클릭하고 "새 규칙"을 클릭합니다.

   새 인바운드 규칙 마법사가 나타납니다.

3. 새 인바운드 규칙 마법사를 완료합니다. 다음을 *제외*한 모든 페이지에서 기본 설정을 선택합니다.

   a. "규칙 종류" 페이지에서 "사용자 지정"을 선택합니다.

   b. "프로그램" 페이지에서 다음을 수행합니다.

      - 모든 프로그램을 선택합니다.
      - "사용자 지정"을 클릭합니다.

        "서비스 설정 사용자 지정" 대화 상자가 열립니다.

      - "이 서비스에 적용", "Windows Management Instrumentation"을 선택한 다음 "확인"을 클릭합니다.

   c. "범위" 페이지에서 원격 IP 주소가 이 규칙 일치 섹션에서 하는 것처럼 다음을 수행합니다.

      - 이 IP 주소를 선택하고 "추가"를 클릭합니다.

        "IP 주소" 대화 상자가 나타납니다.

      - 이 IP 주소 또는 서브넷에서 배포 서버의 IP 주소를 입력하고 "확인"을 클릭합니다.

   d. "이름" 페이지에서 "이름" 필드에 새 규칙의 이름을 입력합니다.

   마법사를 완료한 이후에 방화벽이 동적 RPC 포트에서 WMI 서비스로 도달하는 모든 트래픽을 허용하도록 방화벽 규칙을 만들었습니다.

추가 정보:

Windows Agentless 끝점의 방화벽 구성 (페이지 108)

PUPM 에 대한 Windows Server 2008 R2 x64 끝점 구성

Windows Server 2008 에 해당

Windows Server 2008 R2 x64 끝점에서 PUPM 을 사용하려면 끝점에서 추가 구성 단계를 수행하십시오.

다음 단계를 수행하십시오.

1. Windows 레지스트리를 엽니다.
2. 다음 레지스트리 키로 이동하여 각 키에 대해 3-6 단계를 수행하십시오.

   HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}

   HKEY_CLASSES_ROOT\CLSID\{233664b0-0367-11cf-abc4-02608c9e7553}

   참고: "편집" 메뉴에서 "찾기" 옵션을 사용하여 이 레지스트리 키를 찾을 수 있습니다.
3. 각 키를 마우스 오른쪽 단추로 클릭한 다음 "사용 권한"을 선택합니다.

   "사용 권한" 대화 상자가 나타납니다.
4. "고급"을 클릭합니다.

   "고급 보안 설정" 대화 상자가 나타납니다.
5. "소유자" 탭을 클릭하고 "소유자를 다음으로 변경:" 필드에서 "Administrators"를 클릭한 다음 "적용", "확인"을 차례로 클릭합니다.

   "고급 보안 설정" 대화 상자가 닫힙니다.
6. "사용 권한" 대화 상자의 "그룹 또는 사용자 이름" 창에서 "Administrators"를 선택하고 Administrators 에 대한 "사용 권한" 창에서 "허용" 열의 "모든 권한" 확인란을 선택합니다.
7. "확인"을 클릭합니다.

   "사용 권한" 대화 상자가 닫힙니다. PUPM 에 대한 Windows Server 2008 R2 x64 끝점을 구성했습니다. 추가적으로 방화벽과 DCOM 에 대한 사용 권한을 구성해야 할 수도 있습니다.

로그인 응용 프로그램을 사용하도록 Windows Server 2008 끝점 수정

Windows Server 2008 에 해당

Windows Server 2008 컴퓨터에서 Microsoft 는 ActiveX 컨트롤 옵션에 대한 자동 알림의 기본값을 변경했습니다. Windows Server 2008 컴퓨터에서 이 옵션의 기본값은 "사용 안 함"입니다. Windows 의 이전 버전에서 이 옵션의 기본값은 "사용"이었습니다. 이 옵션은 로컬 인트라넷 및 신뢰하는 사이트 영역에 대한 보안 설정에 영향을 줍니다.

Windows Server 2008 끝점이 로그인 응용 프로그램을 사용하도록 수정하려면 로컬 인트라넷 및 신뢰하는 사이트 영역에 대해 ActiveX 컨트롤 옵션의 자동 알림 값을 "사용"으로 변경하십시오.

참고: 이 옵션의 값을 변경하지 않으면 Windows Server 2008 컴퓨터에서 자동 로그인을 사용할 수 없습니다.

PUPM 에 대한 Windows 7 Enterprise 끝점 구성

Windows 7 Enterprise 에 해당

Windows 7 끝점에서 PUPM 을 사용하려면 끝점에서 추가 구성 단계를 수행해야 합니다.

다음 단계를 수행하십시오.

1. Windows 레지스트리를 엽니다.
2. 다음 레지스트리 키로 이동하여 각 키에 대해 3-6 단계를 수행하십시오.

   HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}

   HKEY_CLASSES_ROOT\CLSID\{233664b0-0367-11cf-abc4-02608c9e7553}

   참고: "편집" 메뉴에서 "찾기" 옵션을 사용하여 이 레지스트리 키를 찾을 수 있습니다.
3. 키를 마우스 오른쪽 단추로 클릭한 다음 "사용 권한"을 선택합니다.

   "사용 권한" 대화 상자가 나타납니다.
4. "고급"을 클릭합니다.

   "고급 보안 설정" 대화 상자가 나타납니다.
5. "소유자" 탭을 클릭하고 "소유자를 다음으로 변경:" 필드에서 "Administrators"를 클릭한 다음 "적용", "확인"을 차례로 클릭합니다.

   "고급 보안 설정" 대화 상자가 닫힙니다.

6. "사용 권한" 대화 상자의 "그룹 또는 사용자 이름" 창에서 "Administrators"를 선택하고 Administrators 에 대한 "사용 권한" 창에서 "허용" 열의 "모든 권한" 확인란을 선택합니다.
7. "확인"을 클릭하여 Windows 레지스트리를 닫습니다.
8. "Windows 제어판", "관리 도구", "서비스"를 엽니다.

   Windows "서비스" 콘솔이 열립니다.
9. "Remote Registry" 서비스를 마우스 오른쪽 단추로 클릭한 다음 "속성"을 선택합니다.

   "속성" 대화 상자가 열립니다.
10. 시작 유형을 "자동"으로 변경하고 "시작"을 선택합니다.

    "Remote Registry" 서비스가 시작됩니다.
11. "실행" 명령줄 창에서 DCOMCNFG 명령을 실행합니다.

    "구성 요소 서비스" 창이 열립니다.
12. "콘솔 루트", "구성 요소 서비스", "컴퓨터"를 선택합니다.
13. "내 컴퓨터"를 마우스 오른쪽 단추로 클릭하고 "속성"을 선택합니다.

    "속성" 대화 상자가 열립니다.
14. "COM 보안" 탭을 클릭하고 "액세스 권한" 섹션 아래에서 "기본값 편집"을 클릭합니다.

    "기본 보안" 대화 상자가 열립니다.
15. "그룹 및 사용자" 창에서 "Administrators"를 선택하고 "원격 액세스"의 액세스 허용 확인란의 선택을 취소합니다.
16. "확인"을 클릭하고 "시작 및 활성화 권한" 섹션에서 14 단계와 15 단계를 반복합니다.
17. "확인"을 클릭하고 "구성 요소 서비스" 콘솔을 닫습니다.

    PUPM 에 대한 Windows 7 Enterprise 끝점을 구성했습니다. 방화벽을 구성해야 할 수도 있습니다.

질문 및 응답 인증 프로토콜 제한 사항

Windows Agentless 끝점에 해당

네트워크 로그인에 대한 질문/대답 인증 프로토콜은 끝점이 클라이언트 서버 통신에 사용하는 세션 보안과 인증 프로토콜의 수준에 영향을 줍니다. 네트워크 로그인에 대한 다음과 같은 세 가지 유형의 Windows 질문/응답 인증 프로토콜이 있습니다.

- LM - LAN Manager 질문/응답
- NTLM - Windows NT 질문/응답
- NTLMv2 - NTLM 의 두 번째 버전

LAN Manager 인증 수준 설정은 끝점이 사용하는 질문/응답 인증 프로토콜을 제어합니다. 이 설정의 기본값은 "Send LM & NTML responses"입니다. 엔터프라이즈 관리 서버는 LAN Manager 인증 수준의 값이 "Send LM & NTML responses"인 경우에만 Windows 끝점과 통신할 수 있습니다. 예를 들어, 엔터프라이즈 관리 서버는 이 설정의 값이 "Send NTLMv2 response only\refuse LM & NTLM"일 때 Windows 끝점과 통신할 수 없습니다.

Windows Agentless 끝점은 끝점의 LAN Manager 인증 수준 설정이 "Send LM & NTML responses"인 경우에만 만들 수 있습니다. Windows Agentless 끝점을 만들 수 없는 경우 해당 끝점에서 질문 및 응답 인증 프로토콜을 변경해야 할 수 있습니다.

SSH 장치 연결 정보

SSH 장치 유형을 사용하면 권한 있는 UNIX 계정을 관리할 수 있습니다.

중요! PUPM SSH 끝점을 구성하기 전에 끝점 설정을 구성하기 전에 끝점에서 터널링된 일반 텍스트 암호를 비활성화하십시오.

이 유형의 장치를 만들 때는 CA Access Control 엔터프라이즈 관리가 장치에 연결할 수 있도록 다음 정보를 제공하십시오.

사용자 로그인

끝점의 관리 사용자 이름을 정의합니다. PUPM 은 이 계정을 사용하여 끝점에서 관리 작업(끝점에 연결하고, 계정을 검색하고, 암호를 변경하는 등의 작업)을 수행합니다.

참고: "고급" 옵션을 지정하면 PUPM 은 관리 작업을 수행하기 위해 "사용자 로그인" 계정을 사용하지 않습니다. 대신, PUPM 은 지정된 권한 있는 계정을 사용하여 끝점에서 관리 작업을 수행합니다. 작업 관리자 계정을 지정하는 경우 PUPM 은 이 계정을 사용하여 끝점에서 관리 작업을 수행합니다.

암호

끝점의 관리 사용자 암호를 정의합니다.

호스트

끝점의 호스트 이름을 정의합니다.

텔넷 사용

SSH 장치에 연결하기 위해 SSH 대신 텔넷을 사용하도록 지정합니다.

작업 관리자 사용자 로그인

(선택 사항) 끝점의 작업 관리자 사용자의 이름을 정의합니다. PUPM 은 이 계정을 사용하여 끝점에서 관리 작업(예: 권한 있는 계정의 암호 검색 및 변경)을 수행합니다. 작업 관리자 사용자를 지정하지 않으면 PUPM 은 사용자 로그인 계정을 사용하여 끝점에서 관리 작업을 수행합니다.

Check Point Firewall 을 사용하는 SSH 끝점에 대해 작업 관리자 사용자를 지정하는 경우 전문가 사용자를 지정하십시오. 하지만 PUPM 을 사용하여 끝점에서 전문가 계정의 암호를 변경할 수 없습니다. 즉, 전문가 계정은 PUPM 에서 연결이 해제된 계정입니다.

작업 관리자 암호

(선택 사항) 작업 관리자 사용자의 암호를 정의합니다.

구성 파일

SSH 장치 XML 구성 파일의 이름을 지정합니다. 필요에 따라 XML 파일을 사용자 지정할 수 있습니다.

참고: 이 필드에 대한 값을 지정하지 않으면 CA Access Control 엔터프라이즈 관리는 ssh_connector_conf.xml 파일을 사용합니다.

고급

권한 있는 관리 계정을 사용하여 끝점에서 관리 작업(끝점에 연결하고, 계정을 검색하고, 암호를 변경하는 등의 작업)을 수행할지 여부를 지정합니다. 예를 들어, 여러 끝점에서 관리 작업을 수행할 수 있는 권한 있는 도메인 계정을 지정할 수 있습니다.

이 옵션을 지정하면 PUPM 은 관리 작업을 수행하기 위해 "사용자 로그인" 계정을 사용하지 않습니다.

PUPM 이 UNIX 끝점에 연결하는 방법

끝점을 만들 때 끝점에 연결하기 위해 PUPM 이 사용하는 관리자 계정을 지정하고, 권한 있는 계정의 암호를 검색 및 변경하는 것과 같은 관리 작업을 수행합니다. UNIX 계정의 경우 가장 적합한 관리자 계정은 일반적으로 root 입니다. 하지만 PUPM 은 SSH 를 사용하여 UNIX 끝점에 연결하고, 일부 조직은 사용자 및 응용 프로그램이 root 사용자로 SSH 연결을 수행하도록 허용하지 않습니다.

이 문제를 피하기 위해 SSH 장치 끝점을 만들 때 연결 계정과 작업 관리자 계정을 모두 지정할 수 있습니다. (PUPM 은 SSH 장치를 UNIX 끝점에 대한 끝점 유형으로 사용). 두 개의 계정을 사용하면 또한 작업 관리자 계정보다 더 적은 권한을 가진 연결 계정을 사용할 수 있습니다.

다음 프로세스는 PUPM 이 이러한 계정을 사용하여 SSH 장치 끝점에 연결하는 방법에 대해 설명합니다.

1. PUPM 은 연결 계정의 자격 증명을 사용하여 끝점에 연결합니다.
2. PUPM 은 작업 관리자 계정의 자격 증명을 사용하여 해당 계정으로 su 전환합니다.

   예를 들어, 작업 관리자 계정이 root 인 경우, PUPM 은 root 자격 증명을 사용하여 root 로 su 전환합니다.
3. PUPM 은 작업 관리자로서 관리 작업을 수행합니다.

   예를 들어, 작업 관리자 계정이 root 인 경우 PUPM 은 root 로서 관리 작업을 수행합니다.

SSH 장치 끝점에서 권한 있는 계정을 보면 연결 및 작업 관리자 계정이 모두 끝점 관리자 계정으로 나열되어 있습니다.

사용자 지정된 SSH 장치 끝점을 만드는 방법

PUPM 이 권한 있는 계정을 찾기 위해 사용하는 기본 설정이 SSH 장치 끝점에 적용되지 않으면 사용자 지정된 SSH 장치 끝점을 만들 수 있습니다.

사용자 지정된 SSH 장치 끝점을 만들려면 다음을 수행하십시오.

1. SSH 장치 XML 파일을 사용자 지정합니다.
2. CA Access Control 엔터프라이즈 관리에 SSH 장치 끝점을 만듭니다 (페이지 97). 만든 XML 파일의 이름을 "구성 파일" 필드에 입력합니다.

   사용자 지정 설정을 사용하여 SSH 장치 끝점이 만들어집니다.
3. 만든 끝점에서 권한 있는 계정 검색 마법사 (페이지 88)를 실행합니다.

   CA Access Control 엔터프라이즈 관리가 XML 파일에서 정의한 매개 변수를 사용하여 끝점에서 권한 있는 계정을 검색합니다.
4. JCS 커넥터 로그 파일(jcs_stdout.log)과 JCS 커넥터 오류 파일(jcs_sterr.log)을 검토합니다. 이러한 파일은 다음 위치에 있습니다.

   ACServerInstallDir/Connector Server/logs
5. 필요하면 로그 파일에 표시된 오류를 해결하기 위해 XML 파일을 수정합니다.

SSH 장치 XML 구성 파일의 유형

CA Access Control 은 다음과 같은 SSH 장치 XML 구성 파일은 제공합니다. 이러한 파일은 실제 환경의 요건에 맞게 사용자 지정합니다.

- **aix_connector_conf.xml** - AIX 끝점인 SSH 장치에 대한 구성 설정을 정의합니다.
- **checkpoint_connector_conf.xml** - Check Point Firewall 을 사용하는 SSH 장치에 대한 구성 설정을 정의합니다.
- **Cisco-UCS_connector_conf.xml** - Cisco UCS 끝점인 SSH 장치에 대한 구성 설정을 정의합니다.
- **device_connector_conf.xml** - 라우터와 같은 장치에 대한 구성 설정을 정의합니다.
- **nis_connector_conf.xml** - NIS 서버와 동작하는 SSH 장치에 대한 구성 설정을 정의합니다.

  참고: 로컬 root 계정을 연결된 사용자로 사용하십시오. 다음 작업을 수행하십시오.

  a. NIS 끝점(nis_endpoint_1)을 만들고 기본 XML 파일을 사용하여 root 계정을 정의합니다. (ssh_connector_conf.xml)

  b. 다른 NIS 끝점(nis_endpoint_2)을 만들고 "고급" 옵션을 사용하여 첫 번째 NIS 끝점의 root 계정을 정의합니다.
- **ssh_connector_conf.xml** - 계정 암호를 변경하기 위해 passwd 명령을 사용하는 SSH 장치를 구성할 때 이 파일을 사용하십시오.

  참고: 로컬 사용자(예: root)를 연결된 사용자로 지정하십시오.
- **sudo_connector_conf.xml** - sudo 및 passwd 명령을 사용하는 SSH 장치를 구성할 때 이 파일을 사용하십시오.

SSH 장치 XML 파일 사용자 지정

SSH 장치 XML 파일은 PUPM 이 SSH 장치 끝점에 연결되고, 사용자가 계정을 검색하고, 끝점에서 권한 있는 계정 암호를 변경하는 방법을 정의합니다. CA Access Control 은 여러 다른 SSH 장치 XML 파일을 제공합니다. 이러한 파일은 PUPM 이 여러 유형의 SSH 장치 끝점에 연결하기 위해 사용하는 기본 설정을 포함하고 있습니다.

SSH 장치 끝점이 다른 방법으로 권한 있는 계정 암호를 변경하는 경우, SSH 장치 XML 파일을 사용자 지정하여 이 비기본 설정을 지정합니다. 예를 들어, 사용자 계정을 검색하고 권한 있는 계정 암호를 변경하기 위해 비기본 방법을 사용하는 라우터, 스위치, 방화벽에 대한 끝점을 만들려면 SSH 장치 XML 파일을 사용자 지정하십시오.

다음 단계를 수행하십시오.

1. CA Access Control 엔터프라이즈 관리에서 사용자 지정할 XML 파일을 찾습니다. 이러한 파일은 다음 디렉터리에 있습니다.

   ACServerInstallDir/Connector Server/conf/override/sshdyn

2. 사용자 지정할 파일을 복제한 후 편집을 위해 새 파일을 엽니다.

   참고: 새 파일은 같은 디렉터리에 저장하십시오.

3. 회사의 요구 사항에 맞게 이 파일에서 매개 변수를 수정합니다.

   이 파일의 각 <item>은 특정 명령에 대한 매개 변수를 정의합니다. PUPM 은 이러한 명령을 사용하여 사용자를 가져오고 끝점에서 암호를 변경합니다. <item> 요소를 수정하여 PUPM 이 끝점으로 보내는 명령을 정의합니다. 또한 PUPM 이 끝점에 연결하기 위해 사용하는 설정을 수정할 수도 있습니다.

4. 파일을 저장한 후 닫습니다.

   끝점에 대한 SSH 장치 XML 파일을 사용자 지정했습니다.

참고: 중국어, 일본어, 한국어를 사용하여 파일을 사용자 지정하는 경우 UTF-8 인코딩으로 파일을 저장하십시오.

예: SSH 장치 XML 파일이 PUPM 명령을 정의하는 방법

이 예는 SSH 장치 XML 파일의 섹션이 PUPM 이 SSH 장치 끝점에서 실행하는 명령을 정의하는 방법을 설명합니다. 이 섹션의 각 <item>은 특정 작업에 대한 매개 변수를 정의합니다. 함께, 이 <item> 요소들은 PUPM 이 끝점과 상호 작용하는 방식을 정의하는 스크립트를 만듭니다.

각 <item> 요소는 sCommand 매개 변수로 시작합니다. sCommand 매개 변수는 PUPM 이 끝점에서 실행하는 명령을 정의합니다. sCommand 매개 변수 뒤의 매개 변수는 이 명령 후 PUPM 이 수행하는 다른 작업을 정의합니다.

이 예는 Cisco 스위치에서 권한 있는 계정 암호를 변경하기 위해 PUPM 이 사용하는 명령을 Cisco-UCS_connector_conf.xml 파일의 섹션이 정의하는 방법을 보여 줍니다. Cisco-UCS_connector_conf.xml 파일은 다음 디렉터리에 있습니다.

ACServerInstallDir/Connector Server/conf/override/sshdyn

이 예는 Cisco-UCS_connector_conf.xml 파일의 한 섹션만 보여 줍니다. 이 파일의 다른 요소들은 Cisco 스위치에 대한 연결을 구성하고 PUPM 이 사용자를 가져오기 위해 실행하는 명령을 지정합니다.

참고: SSH 장치 XML 파일의 형식에 대한 자세한 내용은 *참조 안내서*를 참조하십시오.

다음 프로세스는 Cisco 스위치에서 권한 있는 계정 암호를 변경하기 위해 PUPM 이 실행하는 명령을 보여 줍니다. PUPM 이 실행하는 명령을 <item> 요소가 구성하는 방법을 시연하기 위해 각 단계의 끝에 해당 <item> 요소가 추가되었습니다.

1. PUPM 이 권한 있는 계정의 암호를 변경하도록 지정합니다. PUPM 이 이 단계를 완료하기 위해 다음 작업을 수행합니다.

   a. PUPM 이 다음 명령을 실행합니다.

      set password

   b. PUPM 이 500 밀리초 동안 대기합니다.

   c. PUPM 이 **word:** 문자열을 받을 때까지 대기합니다. 이 문자열을 받으면 다음 단계로 진행합니다.

   다음 <item> 요소는 이 단계에서 PUPM 이 수행하는 작업을 지정합니다.

```
<item>
<param name="sCommand" value="set password" />
<param name="iWait" value="500" />
<param name="sWaitForText" value="word:" />
</item>
```

2. PUPM 이 권한 있는 계정에 대한 새 암호를 지정합니다. PUPM 이 이 단계를 완료하기 위해 다음 작업을 수행합니다.

   a. PUPM 이 새 암호를 끝점으로 보냅니다.

      PUPM 이 새 암호를 로그 파일에 기록하지 않습니다.

   b. PUPM 이 500 밀리초 동안 대기합니다.

   c. PUPM 이 **word:** 문자열을 받을 때까지 대기합니다. 이 문자열을 받으면 다음 단계로 진행합니다.

   다음 <item> 요소는 이 명령에 대한 매개 변수를 지정합니다.

```
<item>
<param name="sCommand" value="[%%password%%]" />
<param name="bHideSentLog" value="true" />
<param name="iWait" value="500" />
<param name="sWaitForText" value="word:" />
</item>
```

3. PUPM 이 권한 있는 계정에 대한 새 암호를 확인합니다. PUPM 이 이 단계를 완료하기 위해 다음 작업을 수행합니다.

   a. PUPM 이 새 암호를 끝점으로 다시 보냅니다.

      PUPM 이 새 암호를 로그 파일에 기록하지 않습니다.

   b. PUPM 이 500 밀리초 동안 대기합니다.

   c. PUPM 은 **local-user* #** 텍스트 문자열을 받을 때까지 대기합니다. 이 문자열을 받으면 다음 단계로 진행합니다.

      PUPM 이 **failure, invalid** 또는 **error** 텍스트 문자열을 받으면 암호 변경이 실패한 것입니다.

   다음 <item> 요소는 이 명령에 대한 매개 변수를 지정합니다.

```
<item>
<param name="sCommand" value="[%%password%%]" />
<param name="bHideSentLog" value="true" />
<param name="iWait" value="500" />
<param name="sWaitForText" value="local-user* #" />
<param name="sFailureResult" value="failure;invalid;error" />
</item>
```

4. PUPM 이 권한 있는 계정에 대한 새 암호를 커밋합니다. PUPM 이 이 단계를 완료하기 위해 다음 작업을 수행합니다.

   a. PUPM 이 다음 명령을 실행합니다.

      commit-buffer

      PUPM 은 이 명령을 로그 파일에 기록하지 않습니다.

   b. PUPM 이 500 밀리초 동안 대기합니다.

   c. PUPM 은 **local-user #** 텍스트 문자열을 받을 때까지 대기합니다. 이 문자열을 받으면 암호 변경이 완료됩니다.

      PUPM 이 **Error: Update failed:** 문자열을 받으면 암호 변경이 실패한 것입니다.

   다음 <item> 요소는 이 명령에 대한 매개 변수를 지정합니다.

```
<item>
<param name="sCommand" value="commit-buffer" />
<param name="bHideSentLog" value="true" />
<param name="iWait" value="500" />
<param name="sWaitForText" value="local-user #" />
<param name="sFailureResult" value="Error: Update failed:" />
</item>
```

   암호 변경이 완료되었습니다.

CA Identity Manager 프로비저닝 연결 정보

CA Identity Manager 프로비저닝 커넥터를 사용하면 프로비저닝 서버에서 정의한 CA Identity Manager 끝점을 관리할 수 있습니다. PUPM 에서 CA Identity Manager 끝점을 만들기 전에 Identity Manager 프로비저닝 유형 커넥터 서버를 만들어야 합니다.

참고: 커넥터 서버를 만드는 방법에 대한 자세한 내용은 온라인 도움말을 참고하십시오.

참고: CA Identity Manager 프로비져닝 커넥터 서버를 구성할 때는 etaadmin 의 완전 고유 이름을 지정하십시오.

예:

eTGlobalUserName=etaadmin,eTGlobalUserContainerName=Global Users,eTNamespaceName=CommonObjects,dc=ProvisioningDomainName,dc=eta

CA Identity Manager 는 대상 시스템에서 구성된 것과 다른 암호 정책을 시행할 수 있습니다. 대상 시스템에서 암호 정책을 시행하면 PUPM 은 사용자 암호를 변경합니다. 하지만 사용자는 끝점에서 이 암호를 사용할 수 없습니다. 대상 시스템에서 암호 정책이 PUPM 암호 정책을 따르는지 확인하십시오. CA Identity Manager 암호 정책 시행 옵션에 대한 자세한 내용은 *CA Identity Manager 관리 안내서*를 참조하십시오.

이 유형의 끝점을 만들 때는 CA Access Control 엔터프라이즈 관리가 끝점에 연결할 수 있도록 다음 정보를 제공하십시오.

끝점

CA Identity Manager 프로비저닝 서버에 정의한 그대로 끝점의 이름을 정의합니다.

프로비저닝 서버에서 연결을 구성한 이후에만 CA Access Control 엔터프라이즈 관리는 CA Identity Manager 끝점 유형을 표시합니다.

호스트

끝점의 호스트 이름을 정의합니다. 이 이름은 이 끝점에 할당하려는 논리적 이름입니다. CA Access Control 엔터프라이즈 관리는 이 이름을 사용하여 월드 뷰에서 끝점을 나타냅니다.

고급

권한 있는 관리 계정을 사용하여 끝점에서 관리 작업(끝점에 연결하고, 계정을 검색하고, 암호를 변경하는 등의 작업)을 수행할지 여부를 지정합니다. 예를 들어, 여러 끝점에서 관리 작업을 수행할 수 있는 권한 있는 도메인 계정을 지정할 수 있습니다.

이 옵션을 지정하면 PUPM 은 관리 작업을 수행하기 위해 "사용자 로그인" 계정을 사용하지 않습니다.

추가 정보:

PUPM 에 대한 CA Identity Manager 프로비저닝 관리자 구성 (페이지 124)

PUPM 에 대한 CA Identity Manager 프로비저닝 관리자 구성

프로비저닝 서버에서 정의하는 CA Identity Manager r12.5 및 r12.5 SP1 끝점을 PUPM 을 사용하여 관리하려면 먼저 PUPM 에 대한 CA Identity Manager 프로비저닝 관리자를 구성해야 합니다.

PUPM 에 대한 CA Identity Manager 프로비저닝 관리자를 구성하려면

1. CA Identity Manager 프로비저닝 관리자에 로그인합니다.
2. "시스템" 탭을 클릭합니다.
3. 구성할 도메인을 선택하고 왼쪽 창에서 "도메인 구성"을 클릭합니다.

   도메인 구성 트리가 나타납니다.
4. "암호" 트리를 확장하고 "동기화된 계정 암호 적용"을 선택합니다.

   "동기화된 계정 암호 적용" 매개 변수에 대한 "도메인 구성" 탭이 나타납니다.

5. "편집"을 클릭하고 값을 No 로 변경한 다음 "확인"을 클릭합니다.
6. "적용"을 클릭합니다.

   "동기화된 계정 암호 적용" 매개 변수의 값이 변경되었습니다.
7. "CA Identity Manager - 프로비저닝 서버" 및 "CA Identity Manager - 커넥터 서버(Java)" 서비스를 다시 시작합니다.

   CA Identity Manager 프로비저닝 관리자가 PUPM 에 대해 구성되었습니다.

CA Identity Manager 프로비저닝 커넥터 검색 제한 수정

권한 있는 계정 검색 마법사를 실행하면 CA Identity Manager 프로비저닝 커넥터가 CA Identity Manager 연결 관리자에 구성된 각 끝점에 대해 최대 1000 개의 결과를 반환합니다. 각 쿼리에서 더 많은 결과를 표시하도록 기본 검색 제한을 수정할 수 있습니다.

CA Identity Manager 프로비저닝 커넥터 검색 제한을 수정하려면

1. 엔터프라이즈 관리 서버에서 Java Connector Server 를 중지합니다. 다음 작업을 수행하십시오.

   a. 다음 디렉터리로 이동합니다. 여기서 *ACServerInstallDir* 는 엔터프라이즈 관리 서버가 설치된 디렉터리를 나타냅니다.

      ACServerInstallDir/Connector_Server/bin

   b. 다음 명령을 실행합니다.

      ./im_jcs stop

   Java Connector Server 가 중지됩니다.
2. 편집을 위해 im_connector_conf.xml 파일을 엽니다. 이 파일은 다음 디렉터리에 있습니다.

   ACServerInstallDir/Connector_Server/conf/override/imdyn
3. "I_SEARCH_SIZE_LIMIT" 토큰을 찾아 검색 제한을 값으로 지정합니다. 예:

   <param name="I_SEARCH_SIZE_LIMIT" value="1500" />
4. 파일을 저장한 후 닫습니다.
5. Java connector Server 를 시작합니다.

중요! 기본값보다 높은 검색 제한 값을 지정하면 시스템 성능이 저하될 수 있습니다.

연결 해제된 끝점 연결 정보

연결 해제된 끝점 유형을 사용하면 연결 해제된 끝점에 있는 권한 있는 계정에 대한 암호를 저장할 수 있습니다.

PUPM 은 연결이 해제된 끝점에 있는 계정에 로그인하거나 이 계정을 관리하지 않습니다. 대신, PUPM 은 끝점에 있는 권한 있는 계정을 위한 암호 저장소의 역할만 수행합니다. CA Access Control 엔터프라이즈 관리에서 연결이 해제된 끝점에 있는 권한 있는 계정에 대한 암호를 변경할 때마다 관리된 끝점에서 계정 암호도 직접 변경해야 합니다.

연결이 해제된 끝점에서 연결이 해제된 계정만 만들 수 있습니다. 연결이 해제된 계정은 PUPM 이 관리하지 않는 계정입니다. 예를 들어, PUPM 은 연결이 해제된 계정의 암호를 변경하지 않습니다. 또한, 권한 있는 계정 검색 마법사 또는 서비스 계정 검색 마법사를 사용하여 연결이 해제된 끝점에서 계정을 검색할 수 없습니다.

이 유형의 끝점을 만들 때는 CA Access Control 엔터프라이즈 관리가 끝점에 연결할 수 있도록 다음 정보를 제공하십시오.

호스트 이름

끝점의 호스트 이름을 정의합니다.

로그인 응용 프로그램 만들기

로그인 응용 프로그램은 스크립트를 사용하여 사용자가 권한 있는 계정 암호를 체크 아웃한 후 자동으로 권한 있는 계정에 자동으로 사용자를 로그인시키는 응용 프로그램을 끝점에서 실행합니다. 로그인 응용 프로그램을 사용하여 PUPM 자동 로그인을 구성할 수 있습니다.

다음과 같은 유형의 로그인 응용 프로그램을 만들 수 있습니다. 로그인 응용 프로그램의 각 유형은 Visual Basic 스크립트입니다.

- ORACLE_10G_WEB.vbs - Oracle 10g 데이터베이스의 엔터프라이즈 관리자 웹 인터페이스로 자동 로그인할 수 있게 합니다.
- ORACLE_10XE_WEB.vbs - Oracle XE 데이터베이스의 데이터베이스 홈 페이지 웹 인터페이스에 자동 로그인할 수 있게 합니다.
- ORACLE_11G_WEB.vbs - Oracle 11g 데이터베이스의 엔터프라이즈 관리자 웹 인터페이스로 자동 로그인할 수 있게 합니다.

- PUTTY.vbs - SSH 장치 끝점에 자동으로 로그인할 수 있게 합니다.

  참고: PuTTY 로그인 응용 프로그램을 사용하려면 컴퓨터에 PuTTY 릴리스 0.60 이상을 설치해야 합니다.

- RDP.vbs - Windows 끝점에 자동으로 로그인할 수 있게 합니다.

자동 로그인을 사용하여 Windows Agentless 끝점에서 권한 있는 계정 암호를 체크 아웃할 때 CA Access Control 엔터프라이즈 관리는 권한 있는 계정의 이름에 대한 호스트 도메인으로 가정합니다. Windows Agentless 끝점에 대한 로그인 응용 프로그램을 만들기 전에 다음을 확인하십시오.

- 끝점이 작업 그룹의 일부인 경우 컴퓨터 이름이 "호스트 도메인" 필드에 지정되어 있는지 확인합니다.
- 끝점이 도메인의 일부인 경우 도메인 이름이 "호스트 도메인" 필드에 지정되어 있는지 확인합니다.

  참고: "끝점 수정" 작업을 사용하여 "호스트 도메인" 필드를 수정할 수 있습니다.

다음을 주의하십시오.

- 로그인 응용 프로그램을 만들려면 시스템 관리자 역할이 있어야 합니다.
- 로그인 응용 프로그램은 Microsoft Internet Explorer 브라우저에서만 사용할 수 있습니다.

다음 단계를 수행하십시오.

1. CA Access Control 엔터프라이즈 관리에서 "권한 있는 계정", "로그인 응용 프로그램", "로그인 응용 프로그램 만들기" 작업을 클릭합니다.

   "로그인 응용 프로그램 만들기: 로그인 응용 프로그램 검색" 화면이 나타납니다.

2. (선택 사항) 다음과 같이 로그인 응용 프로그램을 복사하여 만들기 위해 기존 로그인 응용 프로그램을 선택합니다.

   a. "로그인 응용 프로그램" 유형의 개체 사본을 만들도록 선택합니다.

   b. 검색 특성을 선택하고 필터 값을 입력한 다음 "검색"을 클릭합니다.

      필터 조건과 일치하는 로그인 응용 프로그램의 목록이 표시됩니다.

   c. 새 로그인 용용 프로그램의 기초로 사용할 개체를 선택합니다.

3. "확인"을 클릭합니다.

   "로그인 응용 프로그램 만들기" 작업 페이지가 나타납니다. 기존 개체에서 로그인 응용 프로그램을 만든 경우 대화 상자 필드는 기존 개체의 값으로 미리 채워집니다.

4. 다음 필드를 완료하십시오.

   이름

   이 로그인 응용 프로그램을 참조하는 데 사용할 이름을 정의합니다.

   설명

   (선택 사항) 이 로그인 응용 프로그램에 대해 기록할 정보(일반 텍스트)를 정의합니다.

   스크립트

   로그인 응용 프로그램 실행하는 데 사용할 Visual Basic 스크립트를 정의합니다.

   참고: 이러한 제공된 스크립트는 사용자 지정하지 않는 것이 좋습니다.

   사용

   이 로그인 응용 프로그램이 활성화되도록 지정합니다.

   "제출"을 클릭합니다.

   CA Access Control 엔터프라이즈 관리가 로그인 응용 프로그램을 만듭니다.

   참고: 사용자가 로그인 응용 프로그램을 사용할 수 있도록 하려면 먼저 로그인 응용 프로그램을 사용하도록 CA Access Control 엔터프라이즈 관리에서 끝점을 수정해야 합니다. 터미널 통합을 사용하고 Windows Server 2008 끝점에서 로그인 응용 프로그램을 사용하려면 끝점에서 추가 구성 단계를 수행해야 합니다.

추가 정보:

로그인 응용 프로그램을 사용하도록 Windows Server 2008 끝점 수정 (페이지 112)

PUPM 끝점 및 권한 있는 계정을 가져오는 방법

PUPM 피더를 사용하여 PUPM 끝점 및 권한 있는 계정 관리를 자동화합니다. PUPM 피더를 사용하면 많은 PUPM 끝점 및 권한 있는 계정을 하나의 단계를 통해 CA Access Control 엔터프라이즈 관리로 가져올 수 있습니다. 또한 PUPM 피더를 사용하여 PUPM 끝점 및 권한 있는 계정을 만들거나 수정할 수도 있습니다.

참고: PUPM 피더를 사용하여 PUPM 끝점 및 권한 있는 계정을 삭제할 수 없습니다.

중요! 프로세스 중 오류를 방지하려면 권한 있는 계정 CSV 파일을 가져오기 전에 끝점 CSV 파일을 PUPM 으로 가져오십시오.

PUPM 끝점 및 권한 있는 계정을 CA Access Control 엔터프라이즈 관리로 가져오려면 다음을 수행하십시오.

1. 피더 속성 파일을 구성합니다.

   피더 속성 파일은 폴링 주기 및 폴링 폴더, 처리된 파일 폴더, 오류 파일 폴더의 이름과 위치를 지정합니다.

2. (선택 사항) 폴링 폴더, 처리된 파일 폴더, 오류 파일 폴더에 대한 액세스를 제한하는 CA Access Control 규칙을 작성합니다.

   이러한 폴더에 대한 액세스를 제한하면 권한 없는 사용자가 끝점 및 권한 있는 계정 CSV 파일에 있는 일반 텍스트 암호에 액세스하는 것을 방지하는 데 도움이 됩니다.

3. 다음 중 하나 이상을 수행합니다.

   - 끝점 CSV 파일을 만듭니다.
   - 권한 있는 계정 CSV 파일을 만듭니다.

   CSV 파일의 각 줄은 PUPM 끝점 또는 권한 있는 계정을 만들거나 수정하기 위한 작업을 나타냅니다. 별도의 끝점 및 권한 있는 계정 CSV 파일을 만들어야 합니다.

   참고: 다른 응용 프로그램에서 자동화된 프로세스를 구성하여 CSV 파일을 만들 수 있습니다.

4. (선택 사항) 폴링 작업을 시작합니다.

   폴링 작업이 시작되면 PUPM 피더는 폴링 폴더에 있는 CSV 파일을 CA Access Control 엔터프라이즈 관리에 업로드하여 CSV 파일을 처리합니다.

   참고: 폴링 작업을 직접 시작하지 않으면 PUPM 피더가 피더 속성 파일에 지정된 시간에 폴링 폴더에서 파일을 확인합니다.

5. CA Access Control 엔터프라이즈 관리가 CSV 파일의 처리를 완료하면 오류 파일 폴더에 있는 CSV 파일을 검토하여 실패한 작업이 있는지 확인합니다.

   이 파일은 실패한 작업 및 CA Access Control 엔터프라이즈 관리가 처리하지 못한 작업을 나열합니다.

6. 파일의 오류를 수정한 다음 폴링 폴더에 파일을 저장합니다.

7. 폴링 작업을 시작합니다.

8. 모든 PUPM 끝점 및 권한 있는 계정을 가져올 때까지 5-7 단계를 반복합니다.

PUPM 피더가 동작하는 방법

PUPM 피더를 사용하면 한 단계로 여러 PUPM 끝점 또는 권한 있는 계정을 만들거나 수정할 수 있습니다. PUPM 피더가 동작하는 방식을 이해하면 회사에 가장 적합한 방식으로 PUPM 을 구성하고 발생할 수 있는 문제를 해결하는 데 도움이 됩니다.

다음 프로세스는 PUPM 피더가 동작하는 방식을 설명합니다.

1. 사용자 또는 자동화된 프로세스가 폴링 폴더에 하나 이상의 CSV 파일을 만들어 저장합니다.

   CSV 파일의 각 줄은 PUPM 끝점 또는 권한 있는 계정을 만들거나 수정하기 위한 작업을 나타냅니다. 끝점 및 권한 있는 계정에 대해 별도의 CSV 파일을 만듭니다.

2. 폴링 작업이 시작되면 PUPM 피더는 폴링 폴더에 있는 CSV 파일을 CA Access Control 엔터프라이즈 관리에 업로드합니다. 지정된 시간에 실행되도록 폴링 작업을 구성하거나 직접 폴링 작업을 시작할 수 있습니다.

   참고: PUPM 피더가 파일의 이름을 변경할 수 없으면 파일을 처리할 수 없습니다. 처리되지 않은 CSV 파일은 폴링 폴더에 그대로 남아 있습니다.

3. CA Access Control 엔터프라이즈 관리는 CSV 파일 *original_timestamp*.csv 의 이름을 변경하고 파일을 처리된 파일 폴더로 이동합니다.

   참고: *original* 은 원래 CSV 파일의 이름이고 *timestamp* 는 파일이 처리된 시간을 나타내는 타임스탬프입니다. 예를 들어, 원래 CSV 파일의 이름이 endpoints.csv 이면 CA Access Control 엔터프라이즈 관리는 처리된 파일 폴더에서 이 파일의 이름을 endpoints_091209130256.csv 로 지정합니다.

4. CA Access Control 엔터프라이즈 관리는 차례로 CSV 파일의 각 줄을 처리합니다. CSV 파일의 각 줄에 대해 다음이 발생합니다.

   - CA Access Control 엔터프라이즈 관리가 작업을 완료할 수 있으면
     - 작업(예: 끝점 생성) 완료합니다.
     - 작업에 대한 감사 레코드를 만듭니다.
   - CA Access Control 엔터프라이즈 관리가 작업을 완료할 수 없으면
     - CSV 파일의 줄을 오류 파일 폴더의 CSV 파일에 복사합니다.
     - FAILURE_REASON 이란 이름의 열을 오류 파일 폴더의 CSV 파일에 추가합니다.
     - 작업이 실패한 이유를 FAILURE_REASON 열에 추가합니다.
     - 작업에 대한 감사 레코드를 만듭니다.

   오류 파일 폴더의 CSV 파일을 사용하면 실패한 작업을 쉽게 검토할 수 있습니다. 이 파일의 이름 또한 *original_timestamp*.csv 입니다.

   참고: 처리된 파일 폴더의 CSV 파일은 처리된 모든 작업을 나열하지만 작업의 상태는 기술하지 않습니다. 즉, 작업은 처리되었거나 실패했습니다.

5. CA Access Control 엔터프라이즈 관리는 CSV 파일의 각 줄에 대해 4 단계를 반복합니다.

피더 속성 파일 구성

피더 속성 파일은 폴링 주기 및 폴링 폴더, 처리된 파일 폴더, 오류 파일 폴더의 이름과 위치를 지정합니다. JBoss 는 시작할 때마다 피더 속성 파일을 읽습니다.

피더 속성 파일을 구성하려면

1. JBoss 응용 프로그램 서버가 실행 중이면 중지합니다.
2. 텍스트 기반 편집기에서 피더 속성 파일을 엽니다. 이 파일은 다음 위치에 있습니다. 여기서 *JBoss_home* 은 JBoss 를 설치한 위치입니다.

   JBoss_home/server/default/deploy/IdentityMinder.ear/custom/ppm/default/feeder.properties

3. 다음 매개 변수 중 *하나*를 활성화합니다.

   FOLDER_POLLING_INTERVAL_IN_MINUTES

   PUPM 피더가 폴링 폴더를 폴링하는 간격(분)을 정의합니다. 이 매개 변수는 기본적으로 활성화되어 있습니다.

   제한: 1-60

   기본값: 60

   FOLDER_POLLING_CRON_EXPR

   PUPM 피더가 폴링 폴더를 폴링하는 시간을 정의합니다. 이 매개 변수를 cron 식으로 지정하십시오.

   중요! 이 매개 변수를 사용하는 경우 FOLDER_POLLING_CRON_EXPR 줄에서 주석 표시(#)를 제거하고 FOLDER_POLLING_INTERVAL_IN_MINUTES 매개 변수 줄 앞에 주석 표시를 추가하여 이 매개 변수를 비활성화하십시오.

   예: FOLDER_POLLING_CRON_EXPR=0 0 23 ? * MON-FRI

   이 예는 PUPM 피더가 월요일에서 금요일 사이 오후 11 시에 폴링 폴더를 폴링하도록 지정합니다.

   폴링 간격이 구성됩니다.

4. (선택 사항) 다음 매개 변수를 편집합니다.

   FOLDER_FOR_POLLING

   폴링 폴더를 정의합니다. 이 폴더는 PUPM 피더가 CSV 파일을 폴링하는 폴더입니다.

   기본값:
   JBoss_home/server/default/deploy/IdentityMinder.ear/custom/ppm/feeder/waitingToBeProcessed

   참고: 이 폴더는 반드시 엔터프라이즈 관리 서버 컴퓨터에 있어야 합니다. 이 폴더에 대해 절대 파일 경로를 지정해야 합니다.

FOLDER_FOR_PROCESSED_FILES

처리된 파일 폴더를 정의합니다. 이 폴더는 PUPM 피더가 CSV 파일을 처리한 후 이 파일을 이동하는 폴더입니다.

기본값:
JBoss_home/server/default/deploy/IdentityMinder.ear/custom/ppm/feeder/processed

참고: 이 폴더는 반드시 엔터프라이즈 관리 서버 컴퓨터에 있어야 합니다. 이 폴더에 대해 절대 파일 경로를 지정해야 합니다.

FOLDER_FOR_ERROR_FILES

오류 파일 폴더를 정의합니다. 이 폴더는 PUPM 피더가 처리할 수 없는 CSV 파일을 이동하는 폴더입니다.

기본값:
JBoss_home/server/default/deploy/IdentityMinder.ear/custom/ppm/feeder/failedToSubmit

참고: 이 폴더는 반드시 엔터프라이즈 관리 서버 컴퓨터에 있어야 합니다. 이 폴더에 대해 절대 파일 경로를 지정해야 합니다.

폴링 폴더의 이름이 구성되었습니다.

5. 파일을 저장한 후 닫습니다.

   피더 속성 파일이 구성되었습니다.

6. JBoss Application Server 를 다시 시작합니다.

예: 피더 속성 파일

다음 예는 30 분마다 폴링 폴더를 폴링하는 PUPM 피더를 구성하고 폴링 폴더, 처리된 파일 폴더, 오류 파일 폴더의 위치를 정의합니다.

```
# 피더 폴더 폴링 작업 구성
# FOLDER_FOR_POLLING 으로 지정된 폴더가 FOLDER_POLLING_INTERVAL_IN_MINUTES 분마다 검사됩니다. 예: 60 은 1 시간(최대값은 매시간)과 같음
FOLDER_POLLING_INTERVAL_IN_MINUTES=30
# cron 식이 제공된 경우 FOLDER_POLLING_INTERVAL_IN_MINUTES 키를 주목하십시오.
# FOLDER_POLLING_CRON_EXPR=
FOLDER_FOR_POLLING=C:\feeder\waitingToBeProcessed
FOLDER_FOR_PROCESSED_FILES=C:\feeder\processed
FOLDER_FOR_ERROR_FILES=C:\feeder\failedToSubmit
```

끝점 CSV 파일 만들기

끝점 CSV 파일의 각 행 또는 줄(머리글 행 또는 줄 다음)은 CA Access Control 엔터프라이즈 관리에서 끝점을 만들거나 수정하기 위한 작업을 나타냅니다.

중요! CSV 파일을 만들 때는 다른 응용 프로그램이 이 파일을 사용하고 있지 않은지, 그리고 파일의 이름을 변경할 수 있는지를 확인하십시오. PUPM 피더는 이름을 변경할 수 있는 CSV 파일만 처리합니다.

다음 단계를 수행하십시오.

1. CSV 파일을 만들고 적절한 이름을 지정합니다.

   참고: 샘플 끝점 CSV 파일의 사본을 만드는 것이 좋습니다. 샘플 파일은 다음 디렉터리에 있습니다. 여기서 *ACServer* 는 엔터프라이즈 관리 서버를 설치한 디렉터리입니다.

   ACServer/IAM Suite/Access Control/tools/samples/feeder

2. 끝점 특성의 이름을 지정하는 머리글 행 또는 줄을 만듭니다.

   끝점 특성의 이름은 다음과 같습니다. 일부 끝점 특성은 특정 끝점 유형에 대해서만 유효합니다.

   OBJECT_TYPE

   가져올 개체의 유형을 지정합니다.

   값: ENDPOINT

   ACTION_TYPE

   수행할 작업 유형을 지정하십시오.

   값: CREATE, MODIFY, DELETE

   %FRIENDLY_NAME%

   CA Access Control 엔터프라이즈 관리에서 이 끝점에 대한 이름을 정의합니다.

   DESCRIPTION

   이 끝점에 대해 기록할 정보를 정의합니다.

ENDPOINT_TYPE

끝점의 유형을 지정합니다.

참고: CA Access Control 엔터프라이즈 관리에서 사용 가능한 끝점 유형을 볼 수 있습니다. CA Identity Manager 프로비저닝 유형의 끝점을 만들기 전에 CA Access Control 엔터프라이즈 관리에 Identity Manager 프로비저닝 유형 커넥터 서버를 만드십시오.

HOST

끝점의 호스트 이름을 정의합니다.

LOGIN_USER

끝점의 관리 사용자 이름을 정의합니다. 이 특성은 모든 CA Identity Manager 프로비저닝 끝점 유형에 대해 유효하지 *않지만* 모든 다른 끝점 유형에는 유효합니다.

SSH 장치를 제외한 모든 유효한 끝점 유형의 경우:

- 권한 있는 관리 계정(IS_ADVANCE attribute)을 지정하지 않으면 PUPM 은 LOGIN_USER 를 사용하여 끝점에 연결하고 이 끝점에서 관리 작업(예: 계정 검색 및 암호 변경)을 수행합니다.
- 권한 있는 관리 계정을 지정하면 PUPM 은 LOGIN_USER 에 대한 모든 값을 무시합니다.

SSH 장치 끝점의 경우:

- 작업 관리자(OPERATION_ADMIN_USER_NAME) 또는 권한 있는 관리 계정을 지정하지 않으면 PUPM 은 LOGIN_USER 를 사용하여 끝점에 연결하고 이 끝점에서 관리 작업을 수행합니다.
- 작업 관리자를 지정하면 PUPM 은 LOGIN_USER 를 사용하여 끝점에 연결하고 작업 관리자를 사용하여 이 끝점에서 관리 작업을 수행합니다.
- 권한 있는 관리 계정을 지정하면 PUPM 은 LOGIN_USER 에 대한 모든 값을 무시합니다.

PASSWORD

LOGIN_USER 의 암호를 정의합니다. 이 특성은 CA Identity Manager 프로비저닝 끝점 유형에 대해 유효하지 *않지만* 모든 다른 끝점 유형에는 유효합니다.

URL

CA Access Control 엔터프라이즈 관리가 끝점에 연결하기 위해 사용하는 URL 을 정의합니다. 이 특성은 MS SQL Server 및 Oracle Server 끝점 유형에 대해 유효합니다.

형식: (MS SQL Server) jdbc:sqlserver://*servername*:*port*

형식: (Oracle 서버) jdbc:oracle:*drivertype*:@*hostname*:*port*:*service*

DOMAIN

이 끝점이 구성원으로 속한 도메인의 이름을 지정합니다. 이 특성은 PUPM 용 Access Control 및 Windows Agentless 끝점 유형에 대해 유효합니다.

IS_ACTIVE_DIRECTORY

사용자 계정이 Active Directory 계정인지 여부를 지정합니다. 이 특성은 Windows Agentless 끝점 유형에 대해서만 유효합니다.

제한: TRUE, FALSE

USER_DOMAIN

LOGIN_USER 가 구성원으로 속한 도메인의 이름을 지정합니다. 이 특성은 Windows Agentless 끝점 유형에 대해 유효합니다.

CONFIGURATION_FILE

정의하는 SSH 장치 XML 구성 파일의 이름을 지정합니다. 이 특성은 SSH 장치 끝점 유형에 대해 유효합니다.

참고: 이 필드에 대한 값을 지정하지 않으면 CA Access Control 엔터프라이즈 관리는 기본 구성 파일(ssh_connector_conf.xml)을 사용합니다.

OPERATION_ADMIN_USER_NAME

(선택 사항) 끝점의 작업 관리자 사용자의 이름을 정의합니다. PUPM 은 이 계정을 사용하여 끝점에서 관리 작업(예: 권한 있는 계정의 암호 검색 및 변경)을 수행합니다. 이 특성은 다음과 같이 SSH 장치 끝점 유형에 대해 유효합니다.

- 권한 있는 관리 계정(IS_ADVANCE attribute) 및 작업 관리자를 지정하면 PUPM 은 권한 있는 관리 계정을 사용하여 끝점에 연결하고 작업 관리자를 사용하여 이 끝점에서 관리 작업을 수행합니다.
- LOGIN_USER 와 작업 관리자 계정을 지정하면 PUPM 은 LOGIN_USER 를 사용하여 끝점에 연결하고 작업 관리자를 사용하여 이 끝점에서 관리 작업을 수행합니다.

Check Point Firewall 을 사용하는 SSH 끝점에 대해 작업 관리자를 지정하는 경우 전문가 사용자를 지정해야 합니다. 하지만 PUPM 을 사용하여 끝점에서 전문가 계정의 암호를 변경할 수 없습니다. 즉, 전문가 계정은 PUPM 에서 연결이 해제된 계정입니다.

OPERATION_ADMIN_USER_PASSWORD

(선택 사항) 끝점의 작업 관리자 사용자의 암호를 정의합니다. 이 특성은 SSH 장치 끝점 유형에 대해 유효합니다.

ENDPOINT

CA Identity Manager 프로비저닝 서버에 정의한 그대로 끝점의 이름을 정의합니다. 이 특성은 CA Identity Manager 프로비저닝 끝점 유형에 대해 유효합니다.

IS_ADVANCE

(선택 사항) 권한 있는 관리 계정을 사용하여 끝점에 연결하고 이 끝점에서 관리 작업(예: 계정 검색 및 암호 변경)을 수행할지 여부를 지정합니다. 이 특성은 모든 끝점 유형에 대해 유효합니다.

SSH 장치를 제외한 모든 유효한 끝점 유형의 경우, 권한 있는 관리 계정(IS_ADVANCE is TRUE)을 지정하면 PUPM 이 권한 있는 관리 계정을 사용하여 끝점에 연결하고 이 끝점에서 관리 작업을 수행합니다.

SSH 장치 끝점의 경우:

- 권한 있는 관리 계정 및 작업 관리자(OPERATION_ADMIN_USER_NAME)를 지정하면 PUPM 은 권한 있는 관리 계정을 사용하여 끝점에 연결하고 작업 관리자를 사용하여 이 끝점에서 관리 작업을 수행합니다.
- 권한 있는 관리자 계정만 지정하면 PUPM 은 권한 있는 관리 계정을 사용하여 끝점에 연결하고 이 끝점에서 관리 작업을 수행합니다.

제한: TRUE, FALSE

참고: 이 특성의 값을 TRUE 로 설정하는 경우 LOGIN_USER 에 대한 값을 지정하지 마십시오. 하지만 PROPERTY_ADMIN_ACCOUNT_ENDPOINT_TYPE, PROPERTY_ADMIN_ACCOUNT_ENDPOINT_NAME, PROPERTY_ADMIN_ACCOUNT_CONTAINER, PROPERTY_ADMIN_ACCOUNT_NAME 은 반드시 지정해야 합니다.

PROPERTY_ADMIN_ACCOUNT_ENDPOINT_TYPE

(선택 사항) 권한 있는 관리 계정이 정의된 끝점의 유형을 정의합니다.

참고: 권한 있는 관리 계정을 사용하려면 IS_ADVANCE 를 TRUE 로 지정해야 합니다.

PROPERTY_ADMIN_ACCOUNT_ENDPOINT_NAME

(선택 사항) 권한 있는 관리 계정이 정의된 끝점의 이름을 정의합니다. 끝점은 반드시 CA Access Control 엔터프라이즈 관리에 있어야 합니다.

참고: 권한 있는 관리 계정을 사용하려면 IS_ADVANCE 를 TRUE 로 지정해야 합니다.

PROPERTY_ADMIN_ACCOUNT_CONTAINER

(선택 사항) 권한 있는 관리 계정이 정의된 컨테이너를 정의합니다. 컨테이너는 인스턴스가 다른 개체의 컬렉션인 클래스입니다.

값: (Windows Agentless 및 Oracle 서버): 계정

(SSH 장치): SSH 계정

(MS SQL Server): MS SQL 로그인

참고: 권한 있는 관리 계정을 사용하려면 IS_ADVANCE 를 TRUE 로 지정해야 합니다.

PROPERTY_ADMIN_ACCOUNT_NAME

(선택 사항) PUPM 이 끝점에서 관리 작업(예: 계정 검색 및 암호 변경)을 수행하기 위해 사용하는 권한 있는 관리 계정의 이름을 정의합니다. 권한 있는 계정은 반드시 CA Access Control 엔터프라이즈 관리에 있어야 합니다.

참고: 권한 있는 관리 계정을 사용하려면 IS_ADVANCE 를 TRUE 로 지정해야 합니다.

LOGIN_APPLICATION

끝점과 연계할 로그인 응용 프로그램의 이름을 지정합니다.

3. 끝점 작업 줄을 CSV 파일에 추가합니다.

   각 줄은 끝점을 만들거나 수정할 작업을 나타내며, 머리글과 동일한 특성을 사용해야 합니다. 특성은 머리글과 동일한 순서를 사용해야 합니다. 줄에 특성 값이 없는 경우 필드를 비워두십시오.

4. 파일을 폴링 폴더에 저장합니다.

   끝점 CSV 파일이 PUPM 피더에 의해 처리될 준비가 되었습니다.

   참고: 기본 폴링 폴더는 다음 위치에 있습니다. 여기서 *JBoss_home* 은 JBoss 를 설치한 디렉터리입니다.

   JBoss_home/server/default/deploy/IdentityMinder.ear/custom/ppm/feeder/waitingToBeProcessed

예: 끝점 CSV 파일 만들기

다음은 샘플 끝점 CSV 파일입니다. 추가 샘플 끝점 CSV 파일은 *ACServer*/IAM Suite/Access Control/tools/samples/feeder 디렉터리에서 찾을 수 있습니다.

```
OBJECT_TYPE,%FRIENDLY_NAME%,DESCRIPTION,ENDPOINT_TYPE,HOST,LOGIN_USER,
PASSWORD,URL,CONFIGURATION_FILE,DOMAIN,IS_ACTIVE_DIRECTORY,USER_DOMAIN,ENDPOINT

ENDPOINT,Oracle1,oracle 10g,Oracle Server,TEST10,
ORAADMIN1,ORAADMIN1,jdbc:oracle:thin:@TEST10:1521:RNDSRV,,,,,

ENDPOINT,local MSSQL1,local SQL server,MS SQL Server,
localhost,testAdmin,Password1@,jdbc:sqlserver://localhost:1433,,,,,

ENDPOINT,SSH_Device2,unix machine,SSH Device,TEST84,root,Password1@,,,,,,

ENDPOINT,IM_Access Control,Access Control via provisioning,Access Control,TEST1,,,,,,,,TEST1
```

추가 정보:

SSH 장치 XML 구성 파일의 유형 (페이지 118)

권한 있는 계정 CSV 파일 만들기

권한 있는 계정 CSV 파일의 각 행 또는 줄(머리글 행 또는 줄 다음)은 CA Access Control 엔터프라이즈 관리에서 권한 있는 계정을 만들거나 수정하기 위한 작업을 나타냅니다.

중요! CSV 파일을 만들 때는 다른 응용 프로그램이 이 파일을 사용하고 있지 않은지, 그리고 파일의 이름을 변경할 수 있는지를 확인하십시오. PUPM 피더는 이름을 변경할 수 있는 CSV 파일만 처리합니다.

권한 있는 계정 CSV 파일을 만들려면

1. CSV 파일을 만들고 적절한 이름을 지정합니다.

   참고: 샘플 권한 있는 계정 CSV 파일의 사본을 만드는 것이 좋습니다. 샘플 파일은 다음과 같이 위치해 있습니다. 여기서 *ACServer* 는 엔터프라이즈 관리 서버를 설치한 디렉터리입니다.

   ACServer/IAMSuite/AccessControl/tools/samples/feeder

2. 권한 있는 계정 특성의 이름을 지정하는 머리글 행 또는 줄을 만듭니다.

   권한 있는 계정 특성의 이름은 다음과 같습니다.

   OBJECT_TYPE

   가져올 개체의 유형을 지정합니다.

   값: ACCOUNT_PASSWORD

   ACTION_TYPE

   수행할 작업 유형을 지정하십시오.

   값: CREATE, MODIFY, DELETE

ACCOUNT_NAME

CA Access Control 엔터프라이즈 관리에서 권한 있는 계정에 대한 지정할 이름을 정의합니다.

참고: 메인프레임 시스템(예: RACF, ACF, Top Secret) 및 SSH 장치 끝점은 대/소문자를 구분하는 사용자 이름을 사용합니다. 이러한 끝점 유형에 대해 대/소문자에 주의하여 계정 이름을 입력하십시오. 메인프레임 시스템 및 Oracle 서버 끝점에서 권한 있는 계정에 대해 대문자로 계정 이름을 입력하십시오.

ENDPOINT_NAME

권한 있는 계정이 있는 끝점의 이름을 지정합니다. 끝점에 대한 권한 있는 계정을 만들려면 먼저 CA Access Control 엔터프라이즈 관리에서 끝점을 정의해야 합니다.

NAMESPACE

끝점의 끝점 유형을 지정합니다.

참고: CA Access Control 엔터프라이즈 관리에서 사용 가능한 끝점 유형을 볼 수 있습니다. CA Identity Manager 프로비저닝 유형의 끝점을 만들기 전에 CA Access Control 엔터프라이즈 관리에 Identity Manager 프로비저닝 유형 커넥터 서버를 만들어야 합니다.

CONTAINER

권한 있는 계정에 대한 컨테이너의 이름을 지정합니다. 컨테이너는 인스턴스가 다른 개체의 컬렉션인 클래스입니다. 컨테이너는 특정 액세스 규칙에 따라 개체를 체계적인 방식으로 저장하기 위해 사용됩니다.

값: (Windows Agentless 및 Oracle 서버 끝점): 계정

(SSH 장치 끝점): SSH 계정

(MS SQL Server 끝점): MS SQL 로그인

DISCONNECTED_SYSTEM

권한 있는 계정이 연결이 끊긴 시스템의 계정인지 여부를 지정합니다.

TRUE 로 지정하면 PUPM 이 이 계정을 관리하지 않습니다. 대신, 연결 해제된 시스템의 권한 있는 계정을 위한 암호 저장소의 역할만 수행합니다. PUPM 에서 암호를 변경할 때마다 관리되는 끝점에서도 계정 암호를 직접 변경하십시오.

값: TRUE, FALSE

EXCLUSIVE_ACCOUNT

한 번에 하나의 사용자만 계정을 체크 아웃할 수 있는지 여부를 지정합니다.

TRUE 로 지정하면 PUPM 은 한 번에 하나의 사용자만 계정을 체크 아웃하도록 허용합니다.

값: TRUE, FALSE

NEW_PASSWORD

권한 있는 계정의 암호를 정의합니다. 이 특성의 값을 지정하지 않으면 CA Access Control 엔터프라이즈 관리는 지정된 암호 정책을 따르는 암호를 생성합니다.

참고: 암호는 암호 정책을 준수해야 합니다.

PASSWORD_POLICY

권한 있는 계정의 암호 정책을 지정합니다.

참고: 존재하지 않는 암호 정책을 지정하면 작업이 실패하고 CA Access Control 엔터프라이즈 관리가 권한 있는 계정을 만들지 않습니다.

3. 작업 줄을 CSV 파일에 추가합니다.

   각 줄은 만들거나 수정할 작업을 나타내며, 머리글과 동일한 수의 특성 값을 가져야 합니다. 줄에 특성 값이 없는 경우 필드를 비워두십시오.

4. 파일을 폴링 폴더에 저장합니다.

   권한 있는 계정 CSV 파일이 PUPM 피더에 의해 가져올 준비가 되었습니다.

   참고: 기본 폴링 폴더는 다음 위치에 있습니다. 여기서 *JBoss_home* 은 JBoss 를 설치한 디렉터리입니다.

   JBoss_home/server/default/deploy/IdentityMinder.ear/custom/ppm/feeder/waitingToBeProcessed

예: 권한 있는 계정 CSV 파일 만들기

다음은 샘플 권한 있는 계정 CSV 파일입니다. 추가 샘플 권한 있는 계정 CSV 파일은 *ACServer*/IAMSuite/AccessControl/tools/samples/Feeder 디렉터리에서 찾을 수 있습니다.

```
OBJECT_TYPE,ACCOUNT_NAME,ENDPOINT_NAME,NAMESPACE,CONTAINER,
DISCONNECTED_SYSTEM,EXCLUSIVE_ACCOUNT,NEW_PASSWORD,PASSWORD_POLICY

ACCOUNT_PASSWORD,demo1,local windows 2003,Windows Agentless,
Accounts,FALSE,FALSE,Password1@,default password policy

ACCOUNT_PASSWORD,demo2,local windows 2003,Windows Agentless,
Accounts,FALSE,FALSE,,default password policy

ACCOUNT_PASSWORD,disconnected1,local windows 2003,Windows Agentless,
Accounts,TRUE,FALSE,Password1@,default password policy
```

직접 폴링 작업을 시작합니다.

폴링 작업이 시작되면 PUPM 피더는 폴링 폴더에 있는 CSV 파일을 업로드합니다. 그런 다음 CA Access Control 엔터프라이즈 관리는 이 CSV 파일의 각 줄을 처리합니다.

참고: 폴링 작업을 직접 시작하지 않으면 PUPM 피더가 피더 속성 파일에 지정된 시간에 폴링 폴더를 확인합니다. 폴링 작업을 시작하려면 시스템 관리자 또는 PUPM 대상 시스템 관리자 역할이 있어야 합니다.

직접 폴링 작업을 시작하려면

1. CA Access Control 엔터프라이즈 관리에서 다음을 수행합니다.
   a. "권한 있는 계정"을 클릭합니다.
   b. "계정" 하위 탭을 클릭합니다.

      사용할 수 있는 작업 목록에 "피더 폴더 폴링" 작업이 나타납니다.
2. "피더 폴더 폴링"을 클릭합니다.

   "피더 폴더 폴링" 화면이 나타납니다.
3. "제출"을 클릭합니다.

   PUPM 피더가 폴링 폴더에 있는 CSV 파일을 폴링합니다.

PUPM 자동 로그인

PUPM 자동 로그인을 사용하면 권한 있는 계정 암호를 체크 아웃하고 한 단계로 PUPM 끝점에 로그인할 수 있습니다. PUPM 자동 로그인은 암호를 체크 아웃한 이후에 암호를 표시하지 않지만 이 암호를 사용하여 끝점에서 자동으로 권한 있는 계정에 사용자를 로그인시킵니다. 암호를 체크 아웃한 이후에 CA Access Control 엔터프라이즈 관리에서 이 암호를 볼 수 있습니다.

중요! Microsoft Internet Explorer 브라우저에서만 PUPM 자동 로그인을 사용할 수 있습니다.

자동 로그인을 관리하려면 CA Access Control 엔터프라이즈 관리에 로그인 응용 프로그램 만듭니다. 로그인 응용 프로그램은 스크립트를 사용하여 사용자의 컴퓨터에서 창을 열고 체크 아웃했던 권한 있는 계정에 사용자를 로그인시킵니다. 예를 들어, PuTTY 로그인 응용 프로그램을 사용하여 SSH 장치 끝점에서 root 계정을 체크 아웃하는 경우 CA Access Control 엔터프라이즈 관리는 컴퓨터에서 PuTTY 창을 열고 이 끝점의 root 계정에 사용자를 로그인시킵니다.

자동 로그인이 작동하는 방법

PUPM 자동 로그인을 사용하면 권한 있는 계정 암호를 체크 아웃하고 한 단계로 PUPM 끝점에 로그인할 수 있습니다.

다음 프로세스는 PUPM 이 사용자를 끝점에 자동으로 로그인시키는 방법을 설명합니다. 이 프로세스를 시작하기 전에 CA Access Control 엔터프라이즈 관리에 로그인 응용 프로그램을 만들고 응용 프로그램을 PUPM 끝점에 할당해야 합니다.

1. 권한 있는 계정 암호를 체크 아웃하고 CA Access Control 엔터프라이즈 관리이 끝점에 로그인하기 위해 사용하는 로그인 응용 프로그램을 선택합니다.
2. ActiveX 가 컴퓨터에 설치되어 있지 않으면 다음이 발생합니다.
    a. CA Access Control 엔터프라이즈 관리가 ActiveX 패키지를 컴퓨터로 보냅니다.
    b. ActiveX 를 설치합니다.

    ActiveX 를 설치하지 않으면 끝점에 자동으로 로그인할 수 없습니다.

3. ActiveX 가 설치되면 ActiveX 가 로그인 응용 프로그램에 정의된 스크립트 파일을 엔터프라이즈 관리 서버에서 사용자의 컴퓨터로 다운로드합니다.

   이 스크립트 파일에는 권한 있는 계정 암호가 수록되어 있습니다. 스크립트 파일이 실행되어 끝점에 연결하고 자동으로 권한 있는 계정의 자격 증명을 입력합니다.

   참고: ActiveX 는 이 스크립트 파일을 사용자의 컴퓨터에 저장하지 않습니다.

4. 터미널, Windows 원격 데스크톱 또는 인터넷 브라우저 창이 열립니다.

   끝점에서 권한 있는 계정에 로그인됩니다.

5. 세션을 종료하면 다음 중 *하나*가 발생합니다.

   - 원격 창을 닫기 전에 권한 있는 계정 암호를 체크 인하면 PUPM 이 유예 기간이 지나면 창을 닫는다는 알림을 보냅니다. 유예 기간이 지나면 PUPM 이 창을 닫고 세션을 종료합니다.

     참고: 유예 기간은 스크립트 파일에 정의되어 있습니다. 스크립트 파일을 사용자 지정하여 유예 기간을 늘리거나 줄일 수 있습니다.

   - 원격 창을 닫고 권한 있는 계정 암호를 체크 인하지 않으면 PUPM 이 암호의 체크 인 여부를 묻는 알림을 보냅니다.

PUPM 자동 로그인 응용 프로그램 스크립트를 사용자 지정하는 방법

PUPM 자동 로그인 응용 프로그램 스크립트를 사용자 지정하여 PUPM 자동 로그인 기능을 개선할 수 있습니다. PUPM 자동 로그인 SDK 를 사용하여 사용자가 끝점에 자동으로 로그인할 수 있도록 사용자 지정 스크립트를 만듭니다.

다음 프로세스는 자동 로그인 응용 프로그램 스크립트를 사용자 지정하는 방법에 대해 설명합니다.

1. Visual Basic 스크립트를 만듭니다.

   표준 COM 개체 또는 ACLauncher ActiveX 메서드를 사용하여 스크립트를 만들 수 있습니다.

2. CA Access Control 엔터프라이즈 관리에서 로그인 응용 프로그램을 구성하고 만든 스크립트를 응용 프로그램과 연계합니다.

3. 로그인 스크립트를 끝점에 연계합니다.

추가 정보:

PUPM 자동 로그인 응용 프로그램 Visual Basic 스크립트 (페이지 146)

PUPM 자동 로그인 응용 프로그램 Visual Basic 스크립트

PUPM 자동 로그인 응용 프로그램은 Visual Basic 스크립트를 사용하여 자동 사용자 로그인을 활성화합니다. Visual Basic 스크립트를 사용자 지정하여 새 로그인 응용 프로그램을 만들거나 기존 로그인 응용 프로그램을 수정할 수 있습니다.

PUPM 자동 로그인 응용 프로그램 스크립트에는 엔터프라이즈 관리 서버에서 클라이언트 컴퓨터로 다운로드될 때 ActiveX 가 값으로 대체하는 변수가 수록되어 있습니다. 엔터프라이즈 관리 서버는 이 스크립트를 처리하고 값으로 키워드를 대체합니다. 그런 다음 ActiveX 는 클라이언트 컴퓨터에서 이 스크립트를 실행합니다.

PUPM 자동 로그인 응용 프로그램 스크립트는 다음 디렉터리에 있습니다.

JBOSS_HOME/server/default/deploy/IdentityMinder.ear/config/sso_scripts

요소

PUPM 로그인 응용 프로그램 스크립트는 다음 키를 포함합니다.

#host#

사용자가 자동으로 로그인하는 끝점의 이름을 지정합니다.

#username#

체크 아웃된 권한 있는 계정을 지정합니다.

#password#

체크 아웃할 권한 있는 계정 암호를 지정합니다.

#userdomain#

(Active Directory) 권한 있는 계정 도메인 이름을 지정합니다.

#isActiveServletUrl#

ACLauncher ActiveX 가 계정 암호 체크 인 이벤트에 대해 확인하기 위해 사용하는 URL 을 지정합니다.

#CheckinUrl#

사용자가 끝점에서 로그아웃한 경우 ACLauncher ActiveX 가 계정 암호를 체크 인하는 데 사용하는 URL 을 지정합니다.

#SessionidUrl#

세션이 ObserverIT Enterprise 에 기록된 경우 ACLauncher ActiveX 가 기록된 세션 ID 를 보내기 위해 사용하는 URL 을 지정합니다.

PUPM 자동 로그인 응용 프로그램 스크립트의 다음 코드 조각은 변수가 표시되는 방식을 보여 줍니다.

```
Set pupmObj = CreateObject("ACLauncher.ACWebLauncher")
hwnd = pupmObj.LaunchRDP("#host#", "#userDomain#\#userName#", "#password#")
' Set window close event
pupmObj.SetWindowCloseEvent(hwnd)
' Set server checkin event
pupmObj.SetServerCheckinEvent("#isActiveServletUrl#")
' Wait until one of the events signaled
rc = pupmObj.WaitForEvents()
If rc = 1 Then 'user has closed the window - notify the server side
        pupmObj.SendCheckinEvent("#CheckinUrl#")
ElseIf rc = 2 Then 'timeout elapsed - close the window
  call pupmObj.CloseWindow(hwnd, 0)
ElseIf rc = 3 Then 'the account was checkedin at the server side - close the window
  call pupmObj.CloseWindow(hwnd, 120)
End If
```

구조

PUPM 자동 로그인 응용 프로그램 스크립트 구조는 다음과 같습니다.

- COM 개체의 초기화

```
Set pupmObj = CreateObject("ACLauncher.ACWebLauncher")
```

- 자동 로그인 응용 프로그램의 실행

```
hwnd = pupmObj.LauncheRDP("#host#", "#userDomain#\#userName#", "#password#")
```

- 실행 후 작업 - 암호 체크 인, 대화형 로그인 또는 시간 만료

```
' Wait until one of the events signaled
rc = pupmObj.WaitForEvents()
If rc = 1 Then 'user has closed the window - notify the server side
        pupmObj.SendCheckinEvent("#CheckinUrl#")
ElseIf rc = 2 Then 'timeout elapsed - close the window
   call pupmObj.CloseWindow(hwnd, 0)
ElseIf rc = 3 Then 'the account was checkedin at the server side - close the window
   call pupmObj.CloseWindow(hwnd, 120)
End If
```

로그인 응용 프로그램 세션을 기록하려면 다음과 같이 스크립트에 기록 지침을 추가하십시오.

- 초기화 섹션에서 다음을 추가합니다.

```
Set observeIT = CreateObject("ObserverIT.AgentAPI.Proxy")
```

- 응용 프로그램 실행 섹션에서 다음을 추가합니다.

```
'Get application processid
processID = pupmObj.GetWindowProcessID(hwnd)
'Start recording
sessionid = observeIT.StartByProcessID(processID, true)
'Send the sessions if to the ENTM server
pupmObj.AssignSessionID "#SessionidUrl#" ,sessionId
```

- 실행 후 섹션에서 다음을 추가합니다.

```
'Stop recording

observeIT.StopBySessionId sessionId, true
```

메서드

ACLauncher ActiveX 는 다음 메서드를 사용합니다.

LaunchеRDP (BSTR bsHostName, BSTR bsUserName, BSTR bsPassword, VARIANT *phWindow);

입력 자격 증명을 사용하여 원격 데스크톱 세션을 시작하고 원격 데스크톱 창 핸들을 반환합니다.

예: Dim test Set test = CreateObject("ACLauncher.ACWebLauncher") Hwnd = test.LauncheRDP("hostname.com", "hostname\administrator", "password")

LaunchePUTTY (BSTR bsHostName, BSTR bsUserName, BSTR bsPassword, VARIANT *phWindow);

입력 자격 증명을 사용하여 PuTTY 세션을 시작하고 PuTTY 창 핸들을 반환합니다.

예: Dim test Set test = CreateObject("ACLauncher.ACWebLauncher") Hwnd = test. LaunchePUTTY ("hostname.ca.com", "root", "password")

LaunchеProcessAsUser (BSTR bsApplication, BSTR bsCommandline, BSTR bsUsername, BSTR bsPassword, VARIANT *phWindow);

입력 자격 증명을 사용하여 프로세스를 시작하고 프로세스 창 핸들을 반환합니다.

예: Dim test Set test = CreateObject("ACLauncher.ACWebLauncher") Hwnd = test.LaunchеProcessAsUser("cmd.exe", "/k echo This console is run under %USERNAME% account...", "administrator" , "password")

GetWindowProcessID(VARIANT *phWindow, LONG *pProcessID);

지정된 창 핸들의 프로세스 ID 를 반환합니다.

예: Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.LauncheRDP("hostname", "administrator", "password") id = test.GetWindowProcessID(hwnd) test.Echo "Process ID = " & id

GetWindowTitle(VARIANT *phWindow, BSTR *pbsTitle);

지정된 창 핸들의 제목을 반환합니다.

예: Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.LauncheRDP("hostname", "administrator", "password") title = test.GetWindowTitle(hwnd)

CloseWindow(VARIANT *phWindow, LONG Seconds);

창이 X 초 후에 닫힘을 나타내는 메시지가 있는 대화 상자를 표시하고 지정된 창 핸들의 창을 닫습니다.

예: Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.LauncheRDP("hostname", "administrator", "password") test.Sleep(5000) test.CloseWindow(hwnd, 60)

SetTimeoutEvent(LONG seconds);

"WaitForEvents" 메서드의 만료 시간을 지정합니다. 이 시간에 도달하면 WaitForEvents 메서드는 만료 시간에 도달했음을 나타내는 반환 값을 사용하여 차단 호출로부터 반환됩니다.

예: Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.LauncheRDP("hostname", "administrator", "password") test.SetTimeoutEvent(10)

SetWindowCloseEvent(VARIANT *phWindow);

"WaitForEvents" 메서드에 대한 창 닫기 이벤트를 지정합니다. 창이 닫힌 후에 "WaitForEvents" 메서드는 차단 호출로부터 반환되고 창이 닫혔음을 나타내는 반환 값을 표시합니다.

예: Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.LauncheRDP("hostname", "administrator", "password") test.SetWindowCloseEvent(hwnd)

SetServerCheckinEvent(BSTR bsURL);

PUPM 체크 인 이벤트를 차단 실행 조건으로 설정합니다. ActiveX 는 PUPM 을 5 초마다 쿼리합니다.

예: Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.LauncheRDP("hostname", "administrator", "password") test.SetServerCheckinEvent("http://server.com/__azy?djfhwek5jy34brfhwkeb") (replace with variable)

WaitForEvents(VARIANT *pRetVal);

등록 조건 중 하나가 맞을 때까지 스크립트 실행을 차단합니다.

옵션:1 - 사용자가 창을 닫음, 2 - 시간 만료됨, 3 - 서버측에서 암호 체크인됨

예: Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.LauncheRDP("hostname", "administrator", "password") test.SetServerCheckinEvent("http://server.com/__azy?djfhwek5jy34brfhwkeb")

test.SetWindowCloseEvent(hwnd) test.SetTimeoutEvent(360) rc = test.WaitForEvents() If rc = 3 Then call test.CloseWindow(hwnd, 10) End If

SwitchToThisWindow(VARIANT *phWindow);

Z 순서의 맨 위에 창을 배치합니다.

예: Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.LauncheRDP("hostname", "administrator", "password") test.SwitchToThisWindow(hwnd)

SendCheckinEvent(BSTR bsURL);

사용자가 창을 닫을 때 체크 인 이벤트를 보냅니다.

예: Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.LauncheRDP("hostname", "administrator", "password")

Sleep(LONG milliseconds);

스크립트 실행을 일시 중지합니다.

Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.Sleep(2000)

Echo(VARIANT* pArgs);

화면에 메시지를 출력합니다.

Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.Echo("Password Checkin")

고급 로그인

고급 로그인은 한 끝점에 정의된 권한 있는 계정을 체크 아웃하고 이 계정을 사용하여 다른 끝점에 로그인할 수 있게 해주는 자동 로그인 유형입니다. 고급 로그인을 사용하면 자동 로그인을 사용하여 Active Directory 에 정의된 권한 있는 계정을 체크 아웃할 수 있습니다.

예를 들어, Active Directory 에 'example1'이란 이름의 UNAB 끝점을 정의하고 example1 사용자 및 그룹(root 포함)을 Active Directory 로 마이그레이션합니다. CA Access Control 엔터프라이즈 관리에서 권한 있는 계정으로 root 를 정의합니다. root 를 체크 아웃할 때 자동 로그인을 사용하면 root 계정이 정의된 끝점(Active Directory 도메인 컨트롤러)에 로그인합니다. root 를 체크 아웃할 때 고급 로그인을 사용하면 example1 끝점에 로그인할지 여부를 선택할 수 있습니다.

CA Access Control 엔터프라이즈 관리는 로그인 응용 프로그램을 할당한 각 끝점에 대한 고급 로그인 옵션을 표시합니다. 끝점에 로그인 응용 프로그램을 할당한 다음에는 고급 로그인을 구성하기 위한 추가 단계를 수행할 필요가 없습니다.

제 5 장: 권한 있는 계정 관리

이 섹션은 다음 항목을 포함하고 있습니다.

권한 있는 계정 암호의 강제 체크 인

하나 이상의 사용자에 의해 현재 체크 아웃된 권한 있는 계정 암호를 강제로 체크 인할 수 있습니다.

권한 있는 계정 암호를 강제로 체크 인하려면

1. "권한 있는 계정", "계정", "강제 체크 인"을 클릭합니다.

   "강제 체크 인: 권한 있는 계정 선택" 페이지가 나타납니다.

2. 검색 특성을 선택하고 필터 값을 입력한 다음 "검색"을 클릭합니다.

   필터 조건에 일치하는 권한 있는 계정의 목록이 표시됩니다. "사용자가 체크 아웃함" 열에서 권한 있는 계정의 체크 아웃 여부 및 체크 아웃한 사람에 대한 정보를 볼 수 있습니다.

3. 체크 인할 권한 있는 계정 암호를 선택하고 "선택"을 클릭합니다.

   확인 메시지가 나타납니다.

4. 변경 사항을 승인하려면 "예"를 클릭합니다.

   CA Access Control 엔터프라이즈 관리는 이 작업을 제출하여 계정을 체크 인합니다.

권한 있는 계정 암호를 자동으로 다시 설정

선택된 권한 있는 계정의 암호를 다시 설정하려면 자동 암호 다시 설정 작업을 사용하십시오. 초기화되었을 때 CA Access Control 엔터프라이즈 관리는 계정에 할당된 암호 정책을 기반으로 선택된 계정에 대한 새 암호를 생성합니다.

중요! 계정에 대한 암호를 다시 설정하면 이전 암호는 폐기됩니다. 이전 암호를 사용하는 모든 사용자가 관리되는 장치에 계속 로그인하려면 계정에 체크 인한 다음 체크 아웃해야 합니다.

참고: 이 옵션은 연결 해제된 계정에 대해 사용할 수 없습니다.

권한 있는 계정 암호를 자동으로 다시 설정하려면

1. "권한 있는 계정", "계정", "자동 계정 다시 설정"을 클릭합니다.

   "자동 계정 다시 설정: 권한 있는 계정 선택" 페이지가 나타납니다.
2. 검색 특성을 선택하고 필터 값을 입력한 다음 "검색"을 클릭합니다.

   필터 조건에 일치하는 권한 있는 계정의 목록이 표시됩니다.
3. 다시 설정할 권한 있는 계정 암호를 선택하고 "선택"을 클릭합니다.

   확인 메시지가 나타납니다.
4. 변경 사항을 승인하려면 "예"를 클릭합니다.

   CA Access Control 엔터프라이즈 관리는 이 작업을 제출하여 계정 암호를 다시 설정합니다.

권한 있는 계정 암호 직접 다시 설정

계정 암호를 다시 설정하고 권한 있는 계정에 대한 새 암호를 직접 생성하려면 직접 암호 다시 설정 작업을 사용하십시오. 새 암호는 선택한 권한 있는 계정에 할당된 암호 정책을 준수해야 합니다.

중요! 계정에 대한 암호를 다시 설정하면 이전 암호는 폐기됩니다. 이전 암호를 사용하는 모든 사용자가 관리되는 장치에 계속 로그인하려면 계정에 체크 인한 다음 체크 아웃해야 합니다.

연결 해제된 끝점의 권한 있는 계정을 관리할 때만 직접 암호 다시 설정 기능을 사용하는 것이 좋습니다. 연결 해제된 끝점에서 암호를 변경할 때마다 CA Access Control 엔터프라이즈 관리가 저장하는 암호를 변경하십시오.

권한 있는 계정 암호를 직접 다시 설정하려면

1. "권한 있는 계정", "계정", "직접 암호 다시 설정"을 클릭합니다.

   "직접 암호 다시 설정: 권한 있는 계정 선택" 페이지가 나타납니다.

2. 검색 특성을 선택하고 필터 값을 입력한 다음 "검색"을 클릭합니다.

   필터 조건에 일치하는 권한 있는 계정의 목록이 표시됩니다.

3. 암호를 변경할 권한 있는 계정을 선택하고 "선택"을 클릭합니다.

   "직접 암호 다시 설정" 페이지가 나타납니다.

4. 새 암호를 입력하고 확인을 위해 다시 입력한 다음 "제출"을 클릭합니다.

   CA Access Control 엔터프라이즈 관리는 이 작업을 제출하여 계정 암호를 변경합니다.

권한 있는 계정 예외 삭제

*권한 있는 계정 예외*를 사용하면 사용자가 원래 체크 아웃할 수 있는 권한이 없는 계정을 체크 아웃할 수 있습니다. PUPM 승인자가 권한 있는 계정 액세스 요청을 승인하면 요청자는 요청이 유효한 기간 동안 권한 있는 계정을 체크 아웃할 수 있습니다. 예외가 적용되는 계정을 사용자가 체크 아웃하지 못하도록 방지하기 위해 권한 있는 계정 예외를 삭제할 수 있습니다. 권한 있는 계정 예외를 삭제하려면 사용하는 계정에 기본 권한 있는 계정 요청 또는 PUPM 대상 시스템 관리자 역할(또는 이 작업을 포함하는 동등한 역할)이 할당되어 있어야 합니다.

권한 있는 계정 요청을 삭제하려면

1. CA Access Control 엔터프라이즈 관리에서 "권한 있는 계정", "예외", "권한 있는 계정 예외 삭제"를 클릭합니다.

   "권한 있는 계정 예외 삭제: 권한 있는 계정 예외 선택" 페이지가 나타납니다.

2. 검색 특성을 선택하고 필터 값을 입력한 다음 "검색"을 클릭합니다.

   필터 조건에 일치하는 권한 있는 계정 예외의 목록이 표시됩니다.

3. 삭제할 권한 있는 계정 예외를 선택하고 "선택"을 클릭합니다.

   선택한 권한 있는 계정 예외의 삭제를 확인하는 확인 메시지가 나타납니다.

4. "예"를 클릭합니다.

   권한 있는 계정 요청이 삭제됩니다.

수동 암호 추출

응용 프로그램 서버가 실행되고 있지 않고 PUPM 을 사용할 수 없는 경우 PUPM 을 사용하여 권한 있는 계정을 체크 아웃할 수 없습니다. 대신, PUPM 암호 추출 유틸리티인 pwextractor 를 사용하여 데이터베이스에서 권한 있는 계정 암호를 내보낼 수 있습니다. 그런 다음 이 암호를 사용하여 이전처럼 권한 있는 계정에 로그인하거나 권한 있는 계정 암호의 백업으로 사용할 수 있습니다.

PUPM 을 사용할 수 없어 데이터베이스에서 권한 있는 계정 암호를 추출하는 경우 PUPM 이 복원되었을 때 어떠한 복원 후 단계도 수행할 필요가 없습니다.

엔터프라이즈 관리 서버를 설치할 때 pwextractor 를 설치합니다. 기본적으로 CA Access Control 규칙은 pwextractor 를 보호하지 않지만 보호하기 위한 규칙을 직접 작성할 수 있습니다.

pwextractor 를 사용하려면 다음 조건이 충족되어야 합니다.

- 데이터베이스 테이블에 대한 액세스가 필요합니다.
- 데이터베이스에 액세스하기 위해 PUPM 이 사용하는 계정의 사용자 이름과 암호를 알아야 합니다.

  참고: 엔터프라이즈 관리 서버를 설치할 때 이러한 자격 증명을 제공합니다.

CA Access Control 엔터프라이즈 관리 및 응용 프로그램 서버의 실행 여부에 관계없이 pwextractor 를 사용할 수 있습니다. pwextractor 는 또한 원격으로 실행할 수도 있습니다.

참고: pwextractor 에 대한 자세한 내용은 *참조 안내서*를 참조하십시오.

예: Oracle 데이터베이스에서 권한 있는 계정 암호 추출

다음 예는 Oracle 데이터베이스에서 권한 있는 계정 암호를 추출하여 그 출력을 C:\tmp\pwd.txt 파일에 기록합니다. 스키마 이름은 orcl 이고 데이터베이스는 호스트 myhost.example.com 에 있습니다. 엔터프라이즈 관리 서버는 Windows 컴퓨터에 설치되어 있습니다.

```
pwextractor.bat -h myhost.example.com -d orcl -t oracle -l joesmith -p P@ssw0rd -f C:\tmp\pwd.txt
-k C:\jboss-4.2.3.GA\server\default\deploy\IdentityMinder.ear\config\com\netegrity\config\keys\FipsKey.dat
```

권한 있는 계정 감사

CA Access Control 엔터프라이즈 관리가 수행하는 권한 있는 계정 작업에 대한 세부 정보를 검색하여 볼 수 있습니다. 세부 정보 화면은 각 작업과 이벤트에 대한 추가 정보를 제공합니다. 작업의 상태를 기반으로 작업을 취소하거나 다시 제출할 수 있습니다.

권한 있는 계정을 감사하려면

1. CA Access Control 엔터프라이즈 관리에서 "권한 있는 계정", "감사"를 클릭합니다.

   사용 가능한 작업 목록에 "권한 있는 계정 감사" 작업이 나타납니다.

2. "권한 있는 계정 감사"를 선택합니다.

   "권한 있는 계정 감사" 작업이 열립니다.

3. 검색 조건 (페이지 158)을 지정하고, 표시할 행 수를 입력한 다음 "검색"을 클릭합니다.

   검색 조건에 맞는 작업이 표시됩니다.

권한 있는 계정 감사를 위한 검색 특성

처리를 위해 제출된 작업을 검토하려면 "권한 있는 계정 감사"의 검색 기능을 사용할 수 있습니다. 다음 조건을 기반으로 작업을 검색할 수 있습니다.

시작한 사람

작업을 시작한 사용자의 이름을 검색 조건으로 식별합니다. 사용자 이름을 기반으로 검색이 수행됩니다. 유효한 사용자 이름을 입력했는지 확인하려면 "유효성 검사" 단추를 사용합니다.

승인한 사람

작업 승인자의 이름을 검색 조건으로 식별합니다. 사용자 이름을 기반으로 검색이 수행됩니다. 유효한 사용자 이름을 입력했는지 확인하려면 "유효성 검사" 단추를 사용합니다.

참고: "다음에 의해 승인된 작업" 조건을 선택하여 작업을 필터링하는 경우 "승인 작업 표시" 조건도 기본적으로 활성화됩니다.

작업 이름

작업 이름을 검색 조건으로 식별합니다. 같음, 포함, 다음으로 시작 또는 다음으로 끝남과 같은 조건을 "작업 이름:" 필드 값과 함께 지정하여 검색을 구체화할 수 있습니다. 예를 들어, 같음(=) 조건을 선택하고 텍스트 필드에 "끝점 만들기"를 입력하여 작업 이름 = "끝점 만들기"라는 검색 조건을 지정할 수 있습니다.

계정 이름

계정 이름을 검색 조건으로 식별합니다. 같음, 포함, 다음으로 시작 또는 다음으로 끝남과 같은 조건을 "계정 이름:" 필드 값과 함께 지정하여 검색을 구체화할 수 있습니다. 예를 들어, 같음(=) 조건을 선택하고 텍스트 필드에 "Administrator"를 입력하여 계정 이름 = "Administrator"라는 검색 조건을 지정할 수 있습니다.

끝점 유형

끝점 유형을 검색 조건으로 식별합니다. 같음, 포함, 다음으로 시작 또는 다음으로 끝남과 같은 조건을 "끝점 유형:" 필드 값과 함께 지정하여 검색을 구체화할 수 있습니다. 예를 들어, 같음(=) 조건을 선택하고 텍스트 필드에 "Windows Agentless"를 입력하여 끝점 유형 = "Windows Agentless"라는 검색 조건을 지정할 수 있습니다.

끝점 이름

끝점 이름을 검색 조건으로 식별합니다. 같음, 포함, 다음으로 시작 또는 다음으로 끝남과 같은 조건을 "끝점 이름:" 필드 값과 함께 지정하여 검색을 구체화할 수 있습니다. 예를 들어, 같음(=) 조건을 선택하고 텍스트 필드에 "exampleHost"를 입력하여 끝점 이름 = "exampleHost"라는 검색 조건을 지정할 수 있습니다.

이벤트 이름

이벤트 이름을 검색 조건으로 식별합니다. 같음, 포함, 다음으로 시작 또는 다음으로 끝남과 같은 조건을 "이벤트 이름:" 필드 값과 함께 지정하여 검색을 구체화할 수 있습니다. 예를 들어, 같음(=) 조건을 선택하고 텍스트 필드에 "CheckInAccountPasswordEvent"를 입력하여 이벤트 이름 = "CheckInAccountPasswordEvent"라는 검색 조건을 지정할 수 있습니다.

작업 상태

작업 상태를 검색 조건으로 식별합니다. "작업 상태", 같음, 조건을 선택하여 작업 상태를 선택할 수 있습니다. 다음 조건을 기반으로 검색을 구체화할 수 있습니다.

- 완료함
- 진행 중
- 실패
- 거부됨
- 부분 완료됨
- 취소
- 예약됨

작업 우선 순위

작업 우선 순위를 검색 조건으로 식별합니다. "작업 우선 순위", 같음, 조건을 선택하여 작업 우선 순위를 선택할 수 있습니다. 다음 조건을 기반으로 검색을 구체화할 수 있습니다.

낮음

낮은 우선 순위를 가진 작업을 검색할 수 있도록 지정합니다.

중간

중간 우선 순위를 가진 작업을 검색할 수 있도록 지정합니다.

높음

높은 우선 순위를 가진 작업을 검색할 수 있도록 지정합니다.

다음 사이에 제출함:

제출한 작업을 검색할 날짜 범위를 식별합니다. 필드 사이에서 "제출됨"에 시작 및 끝 날짜를 입력해야 합니다.

제출되지 않은 작업 표시

"감사 마침" 상태의 작업을 식별합니다. 제출되지 않은 다른 작업을 시작한 작업을 식별합니다. 이 확인란을 선택하면 이러한 작업이 모두 감사 및 표시됩니다.

승인 작업 표시

작업흐름의 일부로 승인되어야 하는 작업을 식별합니다.

추가 정보:

작업 상태 설명 (페이지 44)

작업 상태 설명

제출한 작업은 아래에 설명된 상태 중 하나에 있습니다. 작업 상태를 기반으로 작업 취소 또는 작업 다시 제출과 같은 동작을 수행할 수 있습니다.

참고: 작업을 취소하거나 다시 제출하려면 작업 상태를 기반으로 취소 및 다시 제출 단추를 표시하도록 "제출한 작업 보기"를 구성해야 합니다.

진행 중

다음 중 하나가 발생하는 경우에 표시됩니다.

- 작업흐름이 시작되었지만 완료되지 않았음
- 현재 작업보다 먼저 시작된 작업이 진행 중임
- 중첩된 작업이 시작되었지만 완료되지 않았음
- 주 이벤트가 시작되었지만 완료되지 않았음
- 보조 이벤트가 시작되었지만 완료되지 않았음

이 상태의 작업은 취소할 수 있습니다.

참고: 작업을 취소하면 현재 작업의 불완전한 모든 중첩된 작업과 이벤트가 취소됩니다.

취소

진행 중인 작업이나 이벤트를 취소한 경우에 표시됩니다.

거부됨

CA Access Control 엔터프라이즈 관리가 작업흐름 프로세스의 일부인 이벤트나 작업을 거부하는 경우에 표시됩니다. 거부된 작업은 다시 제출할 수 있습니다.

참고: 작업을 다시 제출하면 CA Access Control 엔터프라이즈 관리는 실패 또는 거부한 중첩 작업과 이벤트를 모두 다시 제출합니다.

부분 완료됨

이벤트나 중첩된 작업 중 일부를 취소한 경우에 표시됩니다. 부분 완료된 이벤트나 중첩된 작업은 다시 제출할 수 있습니다.

완료함

작업이 완료된 경우에 표시됩니다. 현재 작업의 중첩된 작업 및 중첩된 이벤트가 완료되면 작업이 완료됩니다.

실패

작업, 중첩된 작업 또는 현재 작업에 중첩된 이벤트가 유효하지 않은 경우에 표시됩니다. 이 상태는 작업이 실패한 경우에 표시됩니다. 실패한 작업은 다시 제출할 수 있습니다.

예약됨

작업이 이후 날짜에 실행되도록 예약된 경우에 표시됩니다. 이 상태의 작업은 취소할 수 있습니다.

PUPM 끝점에서 감사 이벤트 보기

PUPM 끝점을 CA Enterprise Log Manager 와 통합하면 각 권한 있는 계정 세션에 대해 끝점에서 감사 이벤트를 기록할 수 있습니다. 감사 이벤트는 CA Enterprise Log Manager 보고서에 수집되며, 이 내용은 CA Access Control 엔터프라이즈 관리에서 볼 수 있습니다. 이 보고서를 사용하면 사용자가 계정을 체크 아웃한 이후에 권한 있는 계정이 수행하는 작업을 추적할 수 있습니다.

CA Enterprise Log Manager 보고서는 CheckOutAccountPasswordEvent 또는 CheckInAccountPasswordEvent 이벤트에 대해서만 볼 수 있습니다.

PUPM 끝점에서 감사 이벤트를 보려면

1. CA Access Control 엔터프라이즈 관리에서 "권한 있는 계정", "감사"를 클릭합니다.

   사용 가능한 작업 목록에 "권한 있는 계정 감사" 작업이 나타납니다.

2. "권한 있는 계정 감사"를 선택합니다.

   "권한 있는 계정 감사" 작업이 열립니다.

3. 검색 조건 (페이지 158)을 지정하고, 표시할 행 수를 입력한 다음 "검색"을 클릭합니다.

   검색 조건에 맞는 작업이 표시됩니다.

4. 선택한 작업에 대해 "권한 있는 계정 감사" 페이지의 "세션 정보" 열에 있는 아이콘을 클릭합니다.

   참고: 이 아이콘은 CheckOutAccountPasswordEvent 또는 CheckInAccountPasswordEvent 이벤트에 대해서만 표시됩니다.

   CA Enterprise Log Manager 보고서가 표시됩니다. 이 보고서에는 선택한 권한 있는 계정 세션에 대한 감사 이벤트가 수록되어 있습니다.

5. "미리 보기"를 클릭합니다.

   보고서가 닫히고 CA Access Control 엔터프라이즈 관리가 작업 목록과 함께 "권한 있는 계정 감사" 페이지를 표시합니다.

추가 정보:

PUPM 끝점의 이벤트 감사 (페이지 69)

끝점 관리자 암호 복원

관리자 암호가 변경될 때마다 PUPM 은 암호가 변경된 날짜 및 시간에 따라 이전 암호를 데이터베이스에 저장합니다. 끝점에 장애가 발생하여 백업에서 끝점을 복원한 경우 현재 관리자 암호가 끝점에 설정된 관리자 암호와 다릅니다. 끝점에 연결하여 로그인하려면 사용한 백업의 기간과 일치하도록 관리자 암호를 복원해야 합니다.

끝점 관리자 암호를 복원하려면

1. CA Access Control 엔터프라이즈 관리에서 "권한 있는 계정", "끝점", "끝점 암호 복원점" 작업을 선택합니다.

   "끝점 암호 복원점: 끝점 검색" 화면이 열립니다.

2. 검색 특성을 선택하고 필터 값을 입력한 다음 "검색"을 클릭합니다.

   검색 조건에 일치하는 끝점의 목록이 표시됩니다.

3. 목록에서 끝점을 선택하고 "선택"을 클릭합니다.

   끝점 및 관리자 계정 정보가 표시됩니다.

4. "암호 날짜" 메뉴에서 복원할 관리자 암호를 선택합니다.

   "암호 날짜" 메뉴는 각 암호가 변경된 날짜와 시간을 나열합니다. 사용한 백업의 날짜에 가장 가까운 암호를 선택합니다.

5. "확인"을 클릭합니다.

   PUPM 은 암호를 확인하려고 시도합니다. 성공하는 경우 확인 메시지가 표시됩니다.

6. (선택 사항) 재설정할 추가 권한 있는 계정 암호를 선택합니다.

7. "제출"을 클릭합니다.

   PUPM 은 선택한 암호를 복원하고 암호를 현재 관리자 암호로 설정합니다. 추가 권한 있는 계정을 선택한 경우 PUPM 은 또한 이러한 계정 암호도 복원합니다.

이전 권한 있는 계정 암호 표시

끝점에 문제가 발생하여 백업에서 끝점을 복원한 경우 이 끝점의 관리자 계정 암호는 PUPM 데이터베이스에 저장된 암호와 동기화되어 있지 않습니다. 끝점에 로그인하거나 연결하려면 사용한 백업의 기간에 대한 관리자 암호가 필요합니다.

암호를 변경할 때마다 PUPM 은 이전 암호를 저장하므로 이전에 사용한 암호 중 하나를 선택하여 복원한 끝점에 연결할 수 있습니다.

이전 권한 있는 계정 암호를 표시하려면

1. CA Access Control 엔터프라이즈 관리에서 "권한 있는 계정", "계정", "이전 계정 암호 표시"를 선택합니다.

   "이전 계정 암호 표시: 권한 있는 계정 선택" 검색 화면이 열립니다.

2. 검색 특성을 선택하고 필터 값을 입력한 다음 "검색"을 클릭합니다.

   조건에 일치하는 끝점 및 권한 있는 계정의 목록이 표시됩니다.

3. 목록에서 권한 있는 계정을 선택한 다음 "선택"을 클릭합니다.

   화면이 나타나고 그 안에 날짜별로 계정 정보 및 암호 기록이 표시됩니다.

4. 목록에서 항목을 선택한 다음 "암호 표시"를 클릭합니다.

   CA Access Control 엔터프라이즈 관리는 화면의 맨 위에 권한 있는 계정 암호를 표시합니다. 이제 암호를 사용하여 끝점에 로그인할 수 있습니다.

5. "닫기"를 클릭합니다.

제 6 장: 권한 있는 계정 사용

이 섹션은 다음 항목을 포함하고 있습니다.

권한 있는 계정 암호 체크 아웃

계정이 속한 끝점에 로그인하기 위해 권한 있는 계정 암호를 체크 아웃합니다. 권한 있는 계정 암호를 체크 아웃하면 암호를 표시하고, 암호를 클립보드에 복사하고, 끝점에 로그인하도록 선택할 수 있습니다.

SSH 를 사용하여 SSH 장치 끝점에 연결하려고 하고, PUPM 이 다른 계정을 사용하여 끝점에 연결하여 관리하는 경우 두 계정을 모두 체크 아웃합니다. 연결 계정의 자격 증명을 사용하여 SSH 장치 끝점에 연결한 다음 관리 계정의 자격 증명을 사용하여 해당 계정으로 su 전환하십시오.

권한 있는 계정 암호를 체크 아웃하려면

1. "홈", "내 계정", "내 권한 있는 계정"을 클릭합니다.

   "내 계정" 페이지가 열려 체크 아웃할 수 있는 계정을 표시합니다.

2. (선택 사항) 검색 특성을 선택하고 필터 값을 입력한 다음 "검색"을 클릭합니다.

   필터 조건에 일치하는 권한 있는 계정의 목록이 표시됩니다.

3. 체크 아웃할 계정과 끝점을 선택한 다음 "작업" 메뉴에서 다음 옵션 중 *하나*를 선택합니다.
   - 암호를 체크 아웃하려면 "체크 아웃"을 선택합니다.
   - 끝점에 로그인하려면 구성한 "로그인 응용 프로그램" 선택합니다.
   - 암호를 표시하려면 "암호 표시"를 선택합니다.
   - 암호를 클립보드에 복사하려면 "클립보드에 복사"를 선택합니다.
   - 로그인할 끝점의 로그인 응용 프로그램과 호스트 이름을 구성하려면 "고급 로그인"을 선택합니다.

   선택한 옵션에 따라 CA Access Control 엔터프라이즈 관리가 작업을 제출하고 진행합니다.

   끝점에 로그인하도록 선택한 경우 CA Access Control 엔터프라이즈 관리는 확인 메시지를 표시하고, 끝점에서 창이 열려 사용자가 로그인됩니다.

   참고: 끝점에 처음 로그인하는 경우 끝점에 연결하기 전에 이 작업의 승인을 요청하는 대화 상자가 열립니다.

   중요! Microsoft Windows 2008 Server 의 경우 Microsoft Internet Explorer 브라우저 보안 설정에서 "자동 ActiveX 컨트롤 확인"을 활성화하십시오. 비활성화된 경우 브라우저가 원격 데스크톱 응용 프로그램을 실행하기 위해 필요한 ActiveX 파일을 차단합니다.

추가 정보:

PUPM 이 UNIX 끝점에 연결하는 방법 (페이지 116)

권한 있는 계정 암호 체크 인

관리되는 끝점에서 로그아웃한 다음에 권한 있는 계정 암호를 체크 인합니다. 권한 있는 계정 암호를 체크 인하면 CA Access Control 엔터프라이즈 관리가 암호를 변경할 수 있습니다(이렇게 설정된 경우).

권한 있는 계정 암호를 체크 인하려면

1. "홈", "내 계정", "내 권한 있는 계정"을 클릭합니다.

   "내 권한 있는 계정" 페이지가 열리고 체크 인할 수 있는 계정이 표시됩니다.

2. (선택 사항) 검색 특성을 선택하고 필터 값을 입력한 다음 "검색"을 클릭합니다.

   필터 조건에 일치하는 권한 있는 계정의 목록이 표시됩니다.

3. 체크 인할 계정 암호를 선택하고 "작업" 메뉴에서 "체크 인"을 선택합니다.

   CA Access Control 엔터프라이즈 관리는 이 작업을 제출하여 계정을 체크 인합니다.

추가 정보:

권한 있는 계정 암호 체크 아웃 (페이지 167)
권한 있는 계정에 대한 액세스 요청 (페이지 169)

권한 있는 계정에 대한 액세스 요청

권한 있는 계정 암호가 필요하지만 자신의 사용자 계정에 이러한 계정을 체크 아웃할 수 있는 권한이 없는 경우 계정을 체크 아웃하기 위한 요청을 제출할 수 있습니다. CA Access Control 엔터프라이즈 관리는 요청을 승인 또는 거부할 수 있는 승인자에게 이 요청을 전달합니다. 승인되면 권한 있는 계정을 체크 아웃할 수 있습니다.

권한 있는 계정에 대한 암호를 요청하려면

1. "홈", "내 계정", "권한 있는 계정 요청"을 차례로 클릭합니다.

   "권한 있는 계정 요청: 권한 있는 계정 선택" 페이지가 나타납니다.

2. 검색 특성을 선택하고 필터 값을 입력한 다음 "검색"을 클릭합니다.

   필터 조건에 일치하는 권한 있는 계정의 목록이 표시됩니다.

3. 체크 아웃할 권한 있는 계정을 선택하고 "선택"을 클릭합니다.
4. 요청을 완성하고 "제출"을 클릭합니다. 또한 Unicenter Service Desk 티켓 번호를 제공해야 합니다.

   요청이 제출되었음을 알리는 창이 열립니다.

   요청이 승인자에게 전달되고 승인 또는 거부될 때까지 보류 상태로 유지됩니다. 요청이 승인되면 권한 있는 계정을 체크 아웃할 수 있습니다.

권한 있는 계정 요청에 응답

기본 PUPM 승인자 역할이 있거나 이에 준하는 역할이 할당된 경우 사용자들이 제출한 보류 중인 권한 있는 계정 액세스 요청에 응답할 수 있습니다. 다음 작업 중 *하나*를 사용하여 응답할 수 있습니다.

- **승인** - 요청을 승인하고 사용자가 권한 있는 계정을 체크 아웃할 수 있게 허용합니다.
- **거부** - 권한 있는 계정 요청을 거부합니다.
- **항목 예약** - 나중에 고려할 수 있도록 요청을 예약합니다. 요청을 예약하면 CA Access Control 엔터프라이즈 관리는 이 작업 항목을 다른 승인자의 작업 목록에서 제거합니다. 이 항목은 나중에 승인 또는 거부할 수 있습니다.
- **항목 해제** - 다른 승인자가 응답할 수 있도록 요청의 예약을 해제합니다. 이전에 자신이 예약했던 항목만 해제할 수 있습니다.

또한 다른 승인자를 추가하고 이 승인자들도 자신의 보류 중인 승인 목록에 작업 항목을 받을 수 있도록 해당 작업 항목을 다시 할당할 수도 있습니다.

참고: Break Glass 체크 아웃 요청은 요청의 "내 승인 대기" 목록에 표시됩니다. 하지만 이러한 요청을 승인 또는 거부할 필요는 없습니다. 이러한 요청은 사용자가 Break Glass 계정을 체크 아웃했음을 알리기 위해서만 표시됩니다.

참고: 권한 있는 계정 요청에 응답하려면 사용자에게 PUPM 승인자 권한 있는 액세스 역할이 있어야 하며 요청하는 사용자의 관리자여야 합니다.

권한 있는 계정 요청에 응답하려면

1. "홈", "내 계정", "내 승인 대기"를 클릭합니다.

   보류 중인 권한 있는 계정 요청의 목록이 나타납니다.

2. 고려할 보류 승인 요청을 클릭합니다.

   "권한 있는 계정 요청 승인" 페이지가 나타납니다.

3. (선택 사항) 이 요청에 대한 승인자를 추가하려면 다음 단계를 따릅니다.

   a. "할당받은 사람 추가"를 클릭합니다.

      "사용자 선택" 검색 창이 열립니다.

   b. 검색 특성을 선택하고 필터 값을 입력한 다음 "검색"을 클릭합니다.

      필터 조건에 일치하는 사용자의 목록이 표시됩니다.

   c. 추가할 사용자를 선택하고 "선택"을 클릭합니다.

      사용자가 승인자 목록에 추가됩니다.

4. (선택 사항) 다음과 같이 요청 세부 내용을 검토하고 필요한 매개 변수를 수정합니다.

   a. "권한 있는 계정" 탭을 클릭합니다.

      "권한 있는 계정" 탭이 나타나고 이 안에 계정 및 요청의 세부 정보가 표시됩니다.

   b. "유효 날짜" 필드를 사용하여 체크 아웃 만료 시간을 다시 정의합니다.

   c. "티켓 번호" 필드를 사용하여 Unicenter Service Desk 티켓을 검토합니다.

   d. 이 요청에 대한 응답 설명을 입력합니다.

5. 다음 작업 중 *하나*를 수행합니다.

   - "승인"을 클릭합니다.

     요청이 승인되어 보류 중인 요청 목록에서 제거되며, 이제 요청자가 권한 있는 계정을 체크 아웃할 수 있게 됩니다.

   - "거부"를 클릭합니다.

     해당 요청이 거부되고 보류 중인 요청 목록에서 제거됩니다.

- "항목 예약"을 클릭합니다.

  요청이 예약되고 다른 승인자의 보류 중인 요청 목록에서 제거됩니다.

- "항목 해제"를 클릭합니다.

  요청이 해제되고 다른 승인자가 사용할 수 있게 됩니다. 자신이 예약했던 항목만 해제할 수 있습니다.

Break Glass

액세스 권한이 없는 끝점에 *즉시* 액세스해야 하는 경우 Break Glass 작업을 사용하십시오.

참고: 끝점에 즉시 액세스할 수 없는 경우 권한 있는 계정에 대한 액세스를 요청하고 요청이 승인될 때까지 기다릴 수 있습니다.

Break Glass 를 사용하려면

1. "홈", "내 계정", "내 권한 있는 계정"을 클릭합니다.

   "내 계정" 페이지가 열려 체크 아웃할 수 있는 계정을 표시합니다.

2. "계정 선택" 필드에서 "고급"을 선택합니다.

   고급 검색 옵션이 나타납니다.

3. Break Glass 계정을 포함하도록 선택하고 "검색"을 선택합니다.

   필터 조건에 일치하는 권한 있는 계정의 목록이 표시됩니다.

4. "작업" 메뉴에서 체크 아웃할 권한 있는 계정을 선택합니다.

5. 체크 아웃 사유를 입력하고 "체크 아웃"을 클릭합니다.

   CA Access Control 엔터프라이즈 관리는 작업을 제출하고 성공하는 경우 확인 메시지에 계정 암호를 표시합니다.

참고: 암호를 체크 아웃한 이후에 "작업" 메뉴에 다음 옵션이 또한 표시됩니다: 체크 아웃, 로그인 응용 프로그램, 암호 표시

Break Glass 권한 있는 계정 암호 체크 인

관리되는 끝점에서 로그아웃한 다음에 Break Glass 권한 있는 계정 암호를 체크 인합니다.

Break Glass 권한 있는 계정 암호를 체크 인하려면

1. "홈", "내 계정", "내 권한 있는 계정"을 클릭합니다.

   "내 계정" 페이지가 열려 체크 인할 수 있는 계정을 표시합니다.

2. "계정 선택" 필드에서 "고급"을 선택합니다.

   고급 검색 옵션이 나타납니다.

3. Break Glass 계정을 포함하도록 선택하고 "검색"을 선택합니다.

   필터 조건에 일치하는 권한 있는 계정의 목록이 표시됩니다.

4. 체크 인할 계정을 선택하고 "작업" 메뉴에서 "체크 인"을 클릭합니다.

   CA Access Control 엔터프라이즈 관리는 이 작업을 제출하여 계정을 체크 인합니다.

제 7 장: CA User Activity Reporting Module 와 통합

이 섹션은 다음 항목을 포함하고 있습니다.

CA User Activity Reporting Module 정보

CA User Activity Reporting Module 는 IT 준수 및 보증에 중점을 둡니다. CA Enterprise Log Manager 를 사용하면 IT 활동을 수집, 정규화, 집계 및 보고하고 가능한 준수 위반이 발생할 경우 조치를 수행하라는 알림을 생성합니다. 서로 다른 보안 장치 및 비보안 장치에서 데이터를 수집할 수 있습니다.

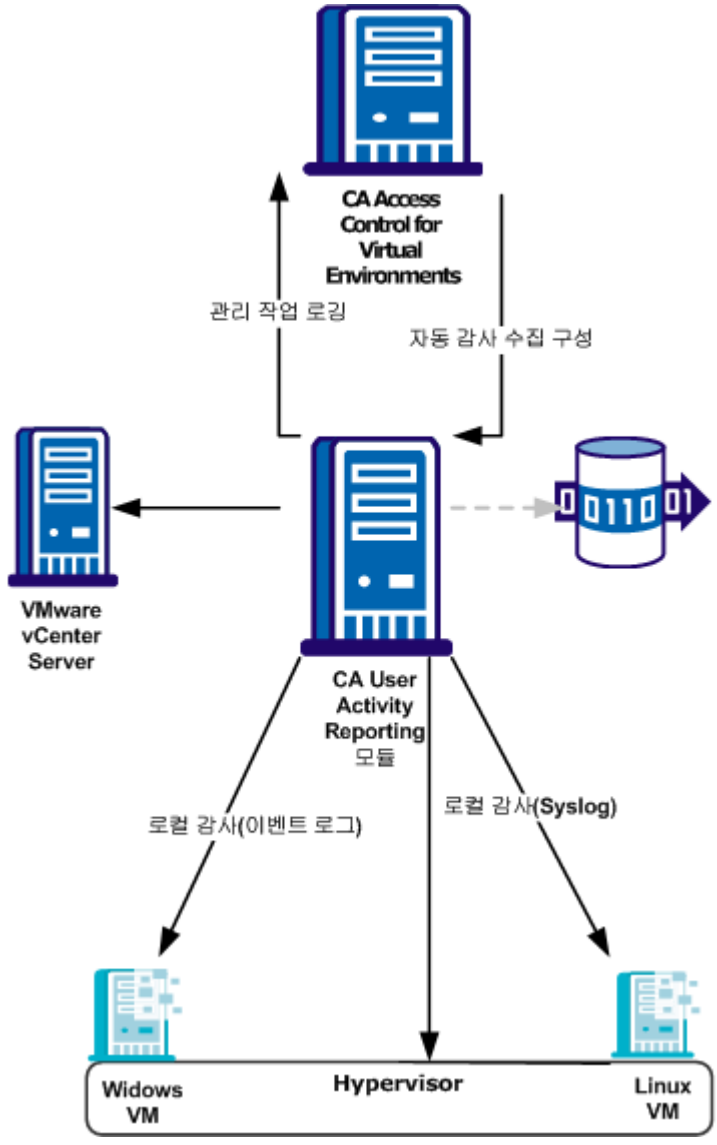
CA User Activity Reporting Module 통합 아키텍처

CA User Activity Reporting Module 과 통합되면 CA User Activity Reporting Module 이 보고할 수 있도록 각 관리되는 장치에서 감사 이벤트를 수집할 수 있습니다.

각 관리 장치를 구성하여 로컬 컴퓨터에 있는 감사 파일에 대한 감사 이벤트를 수집하도록 할 수 있습니다. 그런 다음 CA User Activity Reporting Module 을 구성하여 여기에서 이벤트(메시지)를 가져올 수 있습니다. CA User Activity Reporting Module 은 이러한 이벤트를 처리하고 CA User Activity Reporting Module 서버로 보냅니다.

CA Access Control for Virtual Environments 설치에서는 CA User Activity Reporting Module 통합을 지원합니다.

다음 다이어그램에서는 CA User Activity Reporting Module 통합 구성 요소의 아키텍처를 보여 줍니다.



앞의 다이어그램은 다음을 보여줍니다.

- 각 관리되는 장치는 로컬 파일에 대한 감사 데이터를 수집합니다.
- CA User Activity Reporting Module 은 감사 수집 정책이 적용될 때 관리되는 장치에서 감사 레코드를 가져옵니다.
- CA User Activity Reporting Module 은 CA Access Control for Virtual Environments 에서 사용자가 수행하는 관리 작업에 대한 감사 레코드를 수집합니다.
- CA User Activity Reporting Module 은 VMware vCenter Server 및 hypervisor 에서 감사 레코드를 수집합니다.

참고: CA User Activity Reporting Module 통합은 보고 서비스 구성 요소에 의존합니다. 따라서 CA User Activity Reporting Module 통합에 사용되지 않는 다른 보고 서비스 구성 요소와 기능이 아키텍처에 포함됩니다. 이러한 구성 요소와 기능은 다이어그램에서 회색으로 표시됩니다.

CA User Activity Reporting Module 통합 구성 요소

CA User Activity Reporting Module 통합에서는 다음과 같은 CA Access Control for Virtual Environments 구성 요소를 사용합니다. 이러한 구성 요소는 CA Access Control 엔터프라이즈 보고 서비스의 일부입니다.

- *보고서 에이전트*는 각 관리되는 장치에서 실행되고 VPM 서버에 있는 구성된 메시지 큐의 큐로 정보를 보냅니다. CA User Activity Reporting Module 통합을 위해, 보고서 에이전트는 정기적으로 감사 로그 파일에서 감사 메시지를 수집하여 이러한 이벤트를 구성된 보고서 서버의 감사 큐로 보냅니다.
- *메시지 큐*는 보고서 에이전트가 보내는 정보를 받도록 구성된 배포 서버의 구성 요소입니다. 보고를 위해 메시지 큐는 CA Access Control for Virtual Environments 데이터베이스 스냅숏을 중앙 데이터베이스에 전달합니다.

참고: CA Access Control for Virtual Environments 는 기본적으로 배포 서버를 CA Access Control 서버에 설치합니다.

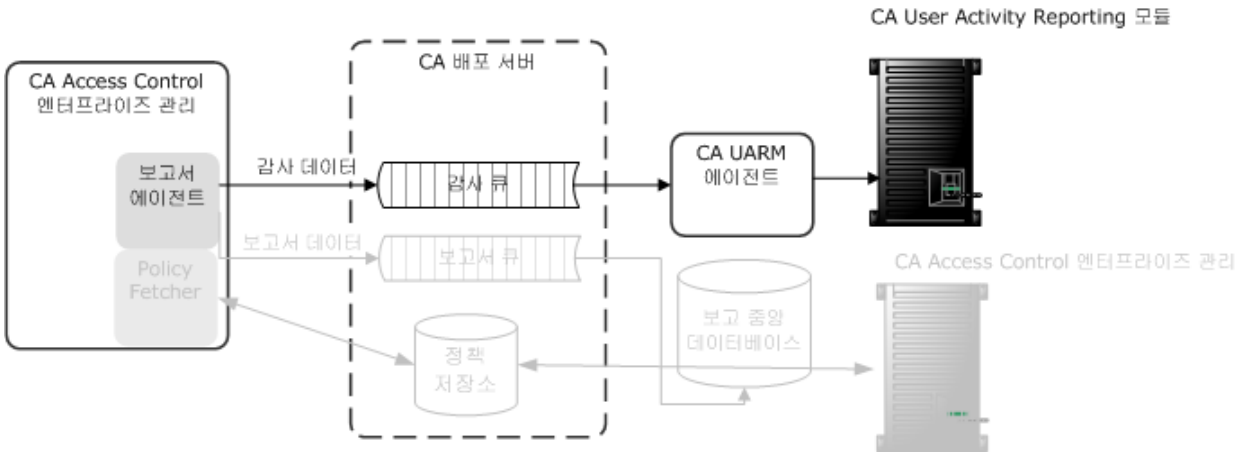
CA User Activity Reporting Module 통합에서는 다음과 같은 CA User Activity Reporting Module 구성 요소도 사용합니다.

- *CA Access Control for Virtual Environments 커넥터*는 CA Access Control 감사 이벤트 원본에 즉시 사용 가능한 CA User Activity Reporting Module 통합입니다. 이 커넥터는 배포 서버에서 원시 이벤트를 수집할 수 있게 하고, 변환된 이벤트를 이벤트 로그 저장소로 규칙에 기반하여 전송하여 핫 데이터베이스에 삽입될 수 있게 합니다.
- *수집 서버*는 들어오는 이벤트 로그를 세부적으로 조정하여 핫 데이터베이스에 삽입하고, 구성된 크기에 도달할 경우 핫 데이터베이스를 웜 데이터베이스로 압축하고, 구성된 일정에 웜 데이터베이스를 관련된 관리 서버에 자동 보관하는 CA User Activity Reporting Module 서버입니다.

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

감사 데이터가 CA Access Control for Virtual Environments 에서 CA User Activity Reporting Module 로 전달되는 방법

CA Access Control for Virtual Environments 이 CA User Activity Reporting Module 과 통합되는 방법과 이 통합을 구성할 때 고려해야 할 사항을 이해하려면 먼저 CA Access Control for Virtual Environments 과 CA User Activity Reporting Module 간의 감사 데이터 흐름을 고려해야 합니다. 다음 그림은 CA Access Control for Virtual Environments 이 감사 이벤트를 배포 서버의 메시징 큐로 라우팅하고, 여기에서 CA User Activity Reporting Module 의 CA Access Control 커넥터가 이 이벤트를 CA User Activity Reporting Module 서버로 가져오고, 매핑하고, 변환한 다음 보내는 방법을 설명합니다.



1. 보고서 에이전트는 로컬 감사 파일에서 감사 이벤트를 수집하고, 필터링 정책을 적용하고, 배포 서버에 있는 감사 큐에 이벤트를 넣습니다.
2. CA User Activity Reporting Module 커넥터는 감사 큐에 연결하여 여기에서 이벤트(메시지)를 가져옵니다.
3. CA User Activity Reporting Module 은 데이터 매핑 및 구문 분석 파일을 사용하여 이벤트를 CEG(Common Event Grammar)에 매핑한 다음 이벤트를 CA User Activity Reporting Module 서버로 라우팅하기 전에 억제 및 요약 규칙을 적용합니다.
4. CA User Activity Reporting Module 서버는 이벤트를 받은 다음 이벤트가 저장되기 전에 추가 억제 및 요약 규칙을 적용할 수 있습니다.

참고: CA User Activity Reporting Module 작동 방법에 대한 자세한 내용은 CA User Activity Reporting Module 설명서를 참조하십시오.

CA Access Control for Virtual Environments 에 대해 CA User Activity Reporting Module 을 설정하는 방법

CA User Activity Reporting Module 을 사용하여 모든 가상 컴퓨터의 감사 데이터를 수록한 보고서를 만들려면 우선 엔터프라이즈 보고 기능을 구현하십시오. 엔터프라이즈 보고 기능을 구현하면 CA Access Control 서버에서 보고서 에이전트가 활성화되므로 CA User Activity Reporting Module 과 통합하기 전에 엔터프라이즈 보고 기능을 구현해야 합니다. 엔터프라이즈 보고가 구현되면 CA Access Control for Virtual Environments 에 대해 CA User Activity Reporting Module 을 설정하십시오.

CA Access Control for Virtual Environments 에 대해 CA User Activity Reporting Module 을 설정하려면 다음 단계를 수행합니다.

1. CA User Activity Reporting Module 서버를 설치합니다.

   참고: 자세한 내용은 *CA User Activity Reporting Module 구현 안내서*를 참조하십시오.

2. CA User Activity Reporting Module 에서 CA User Activity Reporting Module API 인증서를 구성합니다.

   CA Access Control 엔터프라이즈 관리에서 CA User Activity Reporting Module 에 대한 연결을 생성할 때 인증서 정보를 지정합니다.

3. CA User Activity Reporting Module 커넥터를 구성합니다. (페이지 181)

4. CA User Activity Reporting Module 에서 감사 수집 프로필을 구성합니다.

   사용자 지정 감사 수집 프로필을 지정하거나 기본 수집 프로필을 사용할 수 있습니다.

5. CA Access Control 엔터프라이즈 관리에서 CA User Activity Reporting Module 로의 연결을 만듭니다.

   CA User Activity Reporting Module 이 관리되는 장치에서 감사 레코드를 수집하도록 연결 설정을 구성합니다.

6. CA Access Control 엔터프라이즈 관리에서 감사 수집 정책을 구성합니다.

커넥터 정보

CA User Activity Reporting Module 에이전트를 컴퓨터에 설치하면 이 컴퓨터는 CA User Activity Reporting Module 서버 관리 인터페이스에 표시됩니다. 예를 들어, "기본 에이전트 그룹"의 컴퓨터를 보려면 "관리", "로그 수집", "에이전트 탐색기", "기본 에이전트 그룹", *computer_name* 을 클릭하십시오. 이제 커넥터를 만들어야 합니다. 이 항목에서는 "커넥터 만들기" 마법사의 "커넥터 정보" 페이지에서 *구성해야 하는* 설정에 대해 설명합니다.

통합

템플릿으로 사용할 통합을 지정합니다.

적절한 CA Access Control 통합을 선택하십시오.

예: AccessControl_R12SP5_TIBCO

커넥터 이름을 선택적으로 변경하고 설명을 추가할 수 있습니다. 그런 다음 커넥터가 처리하는 이벤트에 억제 규칙을 적용할 수 있습니다.

참고: 이벤트 수집을 사용자 지정할 수 있는 기타 선택적 설정에 대한 자세한 내용은 *CA User Activity Reporting Module 관리 안내서* 및 *온라인 도움말*을 참조하십시오.

억제 및 요약 규칙

커넥터를 만들고 커넥터 정보를 지정했으면 "커넥터 만들기" 마법사의 "억제 규칙 적용" 페이지에서 억제 규칙을 선택적으로 적용할 수 있습니다.

CA Access Control 에 대한 억제 및 요약 규칙의 "이상적 모델" 이름은 "호스트 IDS/IPS"입니다. 이벤트를 식별하는 데 필요한 경우 규칙을 만들 때 "이벤트 범주", "이벤트 클래스" 및 "이벤트 동작"의 값을 선택합니다.

참고: 이벤트 수집을 사용자 지정할 수 있는 기타 선택적 설정에 대한 자세한 내용은 *CA User Activity Reporting Module 관리 안내서* 및 *온라인 도움말*을 참조하십시오. 필드 식별 또는 개별 값에 대한 자세한 내용은 *CA User Activity Reporting Module 온라인 도움말*의 "공통 이벤트 문법 참조"를 참조하십시오.

커넥터 구성 요구 사항

커넥터를 만들고 커넥터 정보를 지정했으면 커넥터를 구성할 수 있습니다. 이 항목에서는 이벤트 수집을 시작하기 위해 "커넥터 만들기" 마법사의 "커넥터 구성" 페이지에서 *구성해야 하는* 설정에 대해 설명합니다.

참고: 이벤트 수집을 사용자 지정할 수 있는 기타 선택적 설정에 대한 자세한 내용은 *CA User Activity Reporting Module 관리 안내서* 및 *온라인 도움말*을 참조하십시오.

TIBCO 서버

메시지 큐(TIBCO 서버)의 호스트 이름 또는 IP 주소를 다음 형식으로 지정합니다.

Protocol://server IP 또는 name:Port number

메시지 큐가 CA Access Control 엔터프라이즈 관리에 설치됩니다.

- 다음 값을 정의합니다.

  ssl://ACentmserver:7243

포트 값 및 통신 방법은 CA Access Control 엔터프라이즈 관리가 사용하는 기본 포트입니다. CA Access Control 엔터프라이즈 관리를 설치한 이후에 다른 값을 구성한 경우 해당 포트 및 통신 방법 값을 사용하십시오.

TIBCO 사용자

메시지 큐 인증을 위한 사용자 이름을 지정합니다. CA Access Control 은 "reportserver"란 이름의 기본 사용자를 정의합니다.

TIBCO 암호

메시지 큐 인증을 위한 암호를 지정합니다. CA Access Control 엔터프라이즈 관리를 설치할 때 "통신 암호" 대화 상자에 정의했던 암호를 입력합니다.

이벤트 로그 이름

이벤트 원본의 로그 이름을 지정합니다.

기본값인 "CA Access Control"을 선택합니다.

PollInterval

메시지 큐를 사용할 수 없거나 연결이 끊어진 경우 에이전트가 이벤트를 폴링하기 전에 기다리는 시간(초)을 지정합니다.

SourceName

메시지 큐의 식별자를 지정합니다.

기본값 "queue_audit"를 적용합니다.

TIBCO 큐

로그 센서가 메시지(이벤트)를 읽는 메시지 큐의 이름을 지정합니다.

기본값 "queue/audit"를 적용합니다.

수집 스레드 수

로그 센서가 메시지 큐 메시지를 읽기 위해 생성하는 스레드 수를 지정합니다.

이 값을 조정할 때는 메시지 큐에 있는 이벤트 수와 CA User Activity Reporting Module 에이전트 시스템의 CPU 를 고려해야 합니다.

제한: 최소값은 1 입니다. 로그 센서가 생성할 수 있는 최대 스레드 수는 20 개입니다.

구성 설정이 보고서 에이전트에 영향을 주는 방식

CA User Activity Reporting Module 통합을 위해 보고서 에이전트는 정기적으로 감사 로그 파일에서 끝점 감사 메시지를 수집하고 이러한 이벤트를 구성된 배포 서버의 감사 큐로 라우팅합니다. 보고서 에이전트 설정을 조정하여 성능에 영향을 줄 수 있습니다.

참고: 보고서 에이전트는 CA Access Control 엔터프라이즈 보고 서비스의 일부이며 끝점 보고를 위해 데이터베이스 스냅숏을 보내는 역할도 합니다. 이 프로세스에서는 보고서 에이전트가 감사 이벤트를 CA User Activity Reporting Module 로 라우팅하기 위해 수행하는 작업만 설명합니다.

감사 수집이 활성화(audit_enabled 구성 설정이 1 로 설정됨)된 경우 보고서 에이전트는 다음을 수행합니다.

- 끝점 감사 파일에서 레코드를 읽은 다음 메모리에 커밋하여 새 감사 레코드를 수집합니다.

  보고서 에이전트는 audit_read_chunk 구성 설정에 정의된 감사 레코드 수를 읽은 다음 감사 파일을 다시 읽기 전에 audit_sleep 구성 설정에 정의된 기간 동안 기다립니다. 보고서 에이전트는 활성 감사 로그 *및* 모든 백업 감사 파일에서 이전에 읽지 않은 레코드를 읽습니다. 그런 다음 감사 필터 파일(audit_filter 구성 설정)에 정의된 감사 필터를 통과하는 레코드만 메모리에 커밋합니다.

- 메모리에 있는 감사 레코드 그룹을 audit_queue 구성 설정에 정의된 보고서 서버 메시징 큐로 보냅니다.

  보고서 에이전트는 다음 중 *하나*가 적용될 때 감사 레코드를 보냅니다.

  - 메모리에 있는 레코드 수가 audit_send_chunk 구성 설정에 정의된 개수에 도달합니다.
  - 마지막 감사 레코드가 전송된 이후 경과한 시간이 audit_timeout 구성 설정에 정의된 간격과 같습니다.

예: 감사 수집 및 라우팅에 대한 기본 보고서 에이전트 설정

이 예에서는 기본 보고서 에이전트 구성 설정을 지정하는 방법, 이러한 설정이 지정되는 환경 및 성능에 미치는 영향을 보여 줍니다.

평균 환경에서는 30EPS(초당 이벤트 수)가 예상됩니다. 따라서 보고서 에이전트는 초당 30 개씩 보고서를 읽습니다. 실행 중인 다른 응용 프로그램에 미치는 영향(CPU 사용 및 컨텍스트 전환)을 줄이기 위해 다음과 같이 보고서 에이전트가 10 초당 300 개의 이벤트를 읽도록 설정했습니다.

```
audit_sleep=10
audit_read_chunk=300
```

CA Access Control 이 보고서 에이전트와 배포 서버 간에 메시지를 전송하는 데 사용하는 메시지 버스는 짧은 간격으로 전송되는 작은 패킷을 처리하는 것보다 긴 간격으로 전송되는 큰 패킷을 보다 효율적으로 처리합니다. 다음 구성 설정은 보고서 에이전트가 수집하는 감사 레코드 수가 정의된 개수에 도달하면 보고서 에이전트가 레코드를 보고서 서버로 보내도록 지정합니다. 초당 30 개 이벤트를 가정하면 보고서 에이전트가 약 1 분 간격(60 초)으로 감사 레코드를 보내도록 하려는 경우 보고서 에이전트를 다음과 같이 설정합니다.

```
audit_send_chunk=1800
```

하지만 야간이나 초당 30 개 미만의 이벤트가 있는 시간에는 분당 1800 개 미만의 이벤트가 있습니다. 보고서 에이전트가 정기적으로 감사 레코드를 보고서 서버로 보내는지 확인하기 위해 다음과 같이 감사 레코드를 보내는 최대 간격을 5 분으로 설정합니다.

```
audit_timeout=300
```

CA User Activity Reporting Module 이벤트 필터링

필터 파일을 사용하여 CA Access Control 이 로그 파일의 모든 감사 레코드를 CA User Activity Reporting Module 에 보내지 않도록 할 수 있습니다. 필터 파일은 CA User Activity Reporting Module 에 보내지 않을 감사 레코드를 지정합니다.

참고: 이 필터 파일은 CA Access Control 이 지정된 감사 이벤트를 배포 서버로 보내지 않도록 만들지만 CA Access Control 이 감사 이벤트를 로컬 파일에 기록하는 것을 방지하지는 않습니다. 로컬 감사 파일에서 감사 이벤트를 필터링하려면 logmgr 섹션의 AuditFiltersFile 구성 설정(기본적으로 audit.cfg)에 의해 정의된 파일의 규칙을 수정하십시오.

CA User Activity Reporting Module 에서 이벤트를 필터링하려면 끝점에 있는 감사 필터 파일을 편집하십시오. 여러 끝점에 동일한 필터링 규칙을 적용하려면 감사 필터링 정책을 만든 다음 적용할 끝점에 이 정책을 할당하는 것이 좋습니다.

참고: 자세한 내용은 *참조 안내서*를 참조하십시오.

예: 감사 필터 정책

이 예에서는 감사 필터링 정책이 어떻게 표시되는지 보여 줍니다.

```
env config
er config auditrouteflt.cfg line+("FILE;*;*;R;P")
```

이 정책은 auditrouteflt.cfg 파일에 다음 줄을 씁니다.

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

이 줄에서는 접근자가 파일 리소스를 읽기 위한 액세스를 허용한 시도를 기록하는 레코드를 감사합니다. CA Access Control 은 이러한 감사 레코드를 배포 서버로 보내지 않습니다.

SSL 을 사용하여 통신 보안 유지

CA Access Control 엔터프라이즈 관리를 설치할 때 SSL 을 사용하여 배포 서버와 보고서 서버 사이의 통신 보안을 유지할지 여부를 선택할 수 있습니다. 어떤 옵션을 선택하든 끝점에 보고서 에이전트를 설치할 때도 같은 옵션을 지정하십시오.

예를 들어, SSL 을 사용하여 보고서 에이전트와 배포 서버 사이의 통신을 암호화하는 경우(기본값), CA Access Control 엔터프라이즈 관리를 설치할 때 인증 정보(예: 보고서 에이전트가 배포 서버와 통신하는 데 필요한 암호)를 제공해야 합니다.

이 암호는 끝점과 CA User Activity Reporting Module 에이전트 커넥터 구성 페이지에서 CA Access Control 보고서 에이전트를 구성할 때 제공한 암호입니다.

보고서 에이전트를 설치할 때도 동일한 정보를 제공해야 합니다. 올바른 인증서와 암호 정보를 제공할 수 있는 보고서 에이전트만 배포 서버의 감사 큐에 이벤트를 쓸 수 있으므로 CA User Activity Reporting Module 에 의해 검색됩니다.

CA User Activity Reporting Module 통합에 대한 감사 로그 파일 백업

감사 데이터를 수집하기 위해 보고서 에이전트는 구성 설정에 따라 CA Access Control 감사 로그 파일을 읽습니다. 보고서 에이전트는 감사 로그 파일에서 구성된 개수의 감사 레코드를 구성된 간격으로 읽습니다. 기본 레거시 설치에서 또는 설치 중에 감사 로그 라우팅을 활성화하지 않으면 CA Access Control 은 크기 트리거된 하나의 감사 로그 백업 파일을 유지합니다. 감사 로그는 구성된 최대 크기에 도달할 때마다 백업 파일을 만들고 기존 감사 로그 백업 파일을 덮어씁니다. 따라서 보고서 에이전트가 모든 레코드를 읽기 전에 백업 파일을 덮어쓰게 될 수 있습니다.

타임스탬프가 지정된 감사 로그 파일 백업을 유지하도록 CA Access Control 을 설정하는 것이 좋습니다. 이렇게 하면 CA Access Control 에서 유지해야 하는 감사 로그 파일의 구성된 최대 개수에 도달할 때까지 백업 감사 로그 파일을 덮어쓰지 않습니다. 끝점에 설치할 때 감사 로그 라우팅 하위 기능을 활성화하는 경우 이것이 기본 설정으로 사용됩니다.

예: 감사 로그 백업 설정

이 예에서는 권장 구성 설정이 CA User Activity Reporting Module 통합에 미치는 영향을 보여 줍니다. 끝점에 설치할 때 감사 로그 라우팅 하위 기능을 활성화하면 CA Access Control 은 다음과 같은 logmgr 섹션 구성 설정을 지정합니다.

```
BackUp_Date=yes
audit_max_files=50
```

이 경우 CA Access Control 은 감사 로그 파일의 각 백업 사본에 타임스탬프를 지정하고 최대 50 개 백업 파일을 유지합니다. 이렇게 하면 보고서 에이전트가 파일에서 모든 감사 레코드를 읽을 수 있으며 필요한 경우 안전한 곳에 보관하기 위해 백업 파일을 복사할 수 있습니다.

중요! audit_max_files 를 0 으로 설정하면 CA Access Control 은 백업 파일을 삭제하지 않고 파일 누적을 계속합니다. 외부 절차를 통해 백업 파일을 관리하려는 경우 CA Access Control 에서 기본적으로 이러한 파일을 보호한다는 것을 기억하십시오.

CA Access Control 이벤트에 대한 쿼리 및 보고서

CA Access Control 에 대한 쿼리, 보고서 및 작업 경고는 CA User Activity Reporting Module 인터페이스의 "서비스 리소스 보호" 태그 아래에 그룹화되어 있습니다.

참고: 자세한 내용은 http://ca.com/support에서 CA User Activity Reporting Module 제품 페이지를 참조하십시오.

CA Access Control 에서 CA User Activity Reporting Module 보고서를 활성화하는 방법

CA Access Control 엔터프라이즈 관리에서 CA User Activity Reporting Module 보고서를 보려면 먼저 CA User Activity Reporting Module 보고 기능을 활성화하고, CA User Activity Reporting Module 인증서를 내보내 추가하고, CA Access Control 엔터프라이즈 관리에서 CA User Activity Reporting Module 로의 연결을 구성해야 합니다.

1. 고급 설정을 구성하여 CA User Activity Reporting Module 보고 기능을 활성화합니다.
2. CA User Activity Reporting Module 트러스트되는 인증서를 내보내 키 저장소에 추가합니다.
3. CA Enterprise Log Manager 에 대한 연결을 구성합니다.
4. (선택 사항) 감사 수집기를 구성합니다 (페이지 192).

   PUPM 감사 이벤트를 CA User Activity Reporting Module 로 보내려면 감사 수집기를 구성하십시오.

CA User Activity Reporting Module 트러스트되는 인증서를 키 저장소에 추가

CA User Activity Reporting Module 보고서는 트러스트된 인증서를 사용하여 인증됩니다. 인증서는 보고서에 표시된 정보가 트러스트된 CA User Activity Reporting Module 출처(데이터의 진위를 검증하는 출처)에서 전달되었는지 확인합니다.

참고: 이 절차를 시작하기 전에 CA User Activity Reporting Module 트러스트된 인증서를 획득하여 설치하십시오. CA User Activity Reporting Module 트러스트된 인증서의 설치에 대한 자세한 내용은 CA User Activity Reporting Module 설명서를 참조하십시오.

다음 단계를 수행하십시오.

1. 엔터프라이즈 관리 서버에서 명령 프롬프트 창을 열고 다음 디렉터리로 이동합니다.

jbossInstallDir/server/default/deploy/IdentityMinder.ear/custom/ppm/truststore

1. 다음 명령을 입력합니다.

   keytool -import -file <*certificate.cert*> -keystore

   -import

   유틸리티가 인증서를 읽어 키 저장소에 저장하도록 지정합니다.

   -file

   트러스트된 인증서 파일의 전체 경로 이름을 지정합니다.

   암호 프롬프트가 나타납니다.

2. 키 저장소 암호를 입력합니다. 기본 암호는 'secret'입니다.
3. "예"를 클릭하여 인증서를 트러스트합니다.

   인증서가 키 저장소에 추가됩니다.

CA User Activity Reporting Module 에 대한 연결 구성

CA Access Control 엔터프라이즈 관리는 CA Access Control 관련 정보를 포함한 보고서를 표시하기 위해 CA User Activity Reporting Module 와 통신합니다. 이러한 보고서를 표시하려면 CA User Activity Reporting Module 에 대한 연결을 구성해야 합니다.

다음 단계를 수행하십시오.

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

   사용 가능한 작업 목록에 "CA User Activity Reporting Module 연결 관리" 작업이 나타납니다.
2. "CA User Activity Reporting Module 연결 관리"를 클릭합니다.

   "CA User Activity Reporting Module 연결 관리: *PrimaryCALMServer*" 작업 페이지가 나타납니다.
3. 대화 상자의 필드를 입력합니다. 다음 필드는 자동으로 채워지지 않습니다.

   연결 이름

   CA User Activity Reporting Module 연결의 이름을 식별합니다.

   설명

   (선택 사항) 이 연결에 대한 설명을 정의합니다.

   Host Name(호스트 이름)

   CA Access Control 엔터프라이즈 관리가 작업할 CA User Activity Reporting Module 호스트의 이름을 정의합니다.

   예: host1.comp.com

   포트 번호

   CA User Activity Reporting Module 호스트가 통신에 사용하는 포트를 정의합니다.

   기본값: 5250

트러스트된 루트 인증서 유효성 검사

CA User Activity Reporting Module 에 대한 연결이 인증 기관이 서명한 트러스트된 루트 인증서를 사용하도록 지정합니다.

참고: 기능이 올바로 작동하려면 CA User Activity Reporting Module 트러스트된 루트 인증서를 설치해야 합니다.

인증서 이름

인증서의 이름을 정의합니다.

암호

인증서 암호를 정의합니다.

4. "제출"을 클릭합니다.

   CA Access Control 엔터프라이즈 관리는 CA User Activity Reporting Module 연결 설정을 저장합니다.

예: CA User Activity Reporting Module 인증서 정보 가져오기

다음 예는 CA Access Control 엔터프라이즈 관리에서 CA User Activity Reporting Module 연결 설정을 만들어 관리할 때 제공해야 하는 CA User Activity Reporting Module 인증서 정보를 획득하는 방법을 설명합니다.

1. 다음 형식으로 웹 브라우저에 CA User Activity Reporting Module URL 을 입력합니다.

   https://*host*:*port*/spin/calmapi/products.csp

   예: https://localhost:5250/spin/calmapi/products.csp

2. CA User Activity Reporting Module 에 로그인하기 위한 올바른 사용자 이름 및 암호를 입력합니다.

3. CA User Activity Reporting Module 에 인증서를 등록하기 위한 등록 옵션을 선택합니다.

   "새 제품 등록" 화면이 나타납니다.

4. 인증 이름 및 암호를 입력하고 "등록"을 선택합니다.

   인증서가 성공적으로 등록되었음을 알리는 메시지가 표시됩니다.

감사 수집기 구성

CA Access Control 엔터프라이즈 관리는 PUPM 감사 이벤트를 포함하여 감사 이벤트를 수집한 다음 중앙 데이터베이스에 저장합니다. CA Access Control 엔터프라이즈 관리를 구성하여 감사 이벤트를 CA User Activity Reporting Module 에 보내도록 할 수 있습니다.

감사 수집기를 구성하려면

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

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

   "감사 수집기 만들기: 감사 수집기 검색 화면"이 나타납니다.
3. (선택 사항) 다음과 같이 기존 감사 수집기의 사본을 만듭니다.
   a. "UARM 전송자" 유형의 개체에 대한 복사본을 만들도록 선택합니다.
   b. 검색 특성을 선택하고 필터 값을 입력한 다음 "검색"을 클릭합니다.

      필터 조건에 일치하는 UARM 전송자의 목록이 나타납니다.
   c. 새 감사 수집기를 만들 때 기초로 사용할 개체를 선택합니다.
4. "확인"을 클릭합니다.

   "감사 수집기 만들기" 작업 페이지가 나타납니다. 기존 개체에서 감사 수집기를 만든 경우 대화 상자 필드에는 기존 개체에서 가져온 값이 자동으로 입력됩니다.
5. 대화 상자의 필드를 입력합니다. 다음 필드는 자동으로 채워지지 않습니다.

   작업 활성화

   감사 수집기의 활성화 여부를 지정합니다.

   이름

   감사 수집기의 이름을 정의합니다.

큐 JNDI

CA Access Control 엔터프라이즈 관리가 감사 이벤트 메시지를 보내는 "메시지 큐" 큐의 이름을 정의합니다.

예: *queue/audit*

대기

데이터베이스 쿼리 간격(분)을 정의합니다.

기본값: 1

시간 만료

감사 이벤트 메시지를 메시지 큐로 보낼 때 수집기의 시간 만료 기간(분)을 정의합니다.

기본값: 10

참고: 시간 만료 기간이 지나면 큐에 있는 메시지 수가 메시지 블록 크기 필드에 정의된 수준에 도달하지 않더라도 수집기가 메시지를 발송합니다.

메시지 블록 크기

메시지를 큐에 보내기 전에 데이터베이스에 누적되는 최대 메시지 수를 정의합니다.

기본값: 100

6. "제출"을 클릭합니다.

CA Access Control 엔터프라이즈 관리가 감사 수집기를 만듭니다.

제 8 장: 보고서 작성

이 섹션은 다음 항목을 포함하고 있습니다.

보안 표준

여러 기업들이 문서 기반 작업 환경에서 전자 미디어 중심의 작업 환경으로 마이그레이션하는 과정에서 관련 데이터에 대한 로컬 및 원격 공격에 더욱 많이 노출되고 있습니다. 이러한 문제를 해결하기 위해 일반적인 전역 보안, 재무 정확도 및 보고, 개인 금융 정보 및 개별 ID 의 안전한 보호, 의료 관련 정보 보호, 미국 정부 차원의 보안 모범 사례 표준화 등 여러 영역에서 몇몇 보안 이니셔티브가 구현되었습니다.

아래의 보안 표준, 법령 및 요구 사항은 CA Access Control 보고 서비스에서 실행되고 있는 모범 사례 보고의 본질적인 내용을 효과적으로 요약해서 설명합니다.

PCI DSS(Payment Card Industry Data Security Standards)

PCI DSS 는 사기 및 해킹을 비롯한 보안 문제를 방지하기 위해 주요 신용 카드 회사에서 개발한 업계 표준입니다. 신용 카드 및 직불 카드 데이터를 수락, 캡처, 저장, 전송 또는 처리하는 회사는 PCI DSS 를 준수해야 합니다.

HIPAA(Health Insurance Portability and Accountability Act)

HIPAA 는 근로자가 이직하거나 실직하는 경우에도 건강 보험을 적용받을 수 있게 해주는 미국 연방법입니다. HIPAA 는 또한 보건 데이터의 보안 및 개인 정보 보호 문제를 다룹니다.

SOX(Sarbanes-Oxley Act)

SOX 는 재무 보고 표준을 규정하는 미국 연방법입니다. 이 법은 모든 미국 공개된 회사의 이사회 및 경영진에 적용됩니다.

보고서 유형

두 가지 다른 보고서 유형으로 CA Access Control for Virtual Environments 데이터 및 이벤트에 대한 정보를 볼 수 있습니다.

- CA Access Control for Virtual Environments 보고서 - 누가 무엇을 할 수 있는지 설명합니다.

  CA Access Control 보고서는 각 관리되는 장치에 있는 CA Access Control for Virtual Environments 데이터베이스의 데이터에 대한 정보(즉, 끝점에 배포하는 정책 및 정책 위반)를 제공합니다. CA Access Control for Virtual Environments 보고서는 [assign the value for cabi in your book] 및 CA Access Control 엔터프라이즈 관리에서 볼 수 있습니다.

- 감사 보고서 - 누가 무엇을 했는지 설명합니다.

  감사 보고서는 각 관리되는 장치의 데이터에 대한 정보, 즉 끝점에서 어떤 사용자가 어떤 작업을 수행했는지에 대한 정보를 제공합니다. 감사 보고서는 VMware vSphere 클라이언트 및 CA Access Control 엔터프라이즈 관리의 CA User Activity Reporting Module 에서 볼 수 있습니다.

  참고: CA User Activity Reporting Module 에서 감사 보고서를 보는 방법에 대한 자세한 내용은 *CA User Activity Reporting Module Overview Guide*(CA Enterprise Log Manager 개요 안내서)를 참조하십시오.

참고: CA Access Control for Virtual Environments 보고서 및 CA Access Control for Virtual Environments 감사 보고서를 보기 위한 추가 구성 요소를 반드시 설치해야 합니다. 자세한 내용은 *제품 안내서*를 참조하십시오.

보고 서비스

CA Access Control for Virtual Environments 보고 서비스를 사용하면 한 위치에서 각 끝점(사용자, 그룹 및 리소스)의 보안 상태를 볼 수 있습니다. 예약을 통해 또는 요청 시에 각 끝점에서 데이터를 수집할 수 있습니다. 어떤 사용자가 어떤 리소스에 액세스할 수 있는 권한이 있는지 확인하기 위해 각 끝점에 일일이 연결할 필요가 없습니다. CA Access Control for Virtual Environments 보고 서비스는 한 번 설치되면 각 끝점에서 데이터를 수집하여 중앙 서버에 보고하기 위해 독립적으로 작동하며 사용자가 수동 작업을 할 필요 없이 끝점 상태를 계속 보고합니다.

CA Access Control 보고 서비스는 BS 7799/ISO 17799, SOX(Sarbanes-Oxley), PCI(Payment Card Industry), HIPAA(Health Insurance Portability and Accountability Act), FISMA(Federal Information Security Management Act) 환경 등에 유용하며 수천 개의 끝점에서 사용자, 그룹 및 리소스 액세스의 상태를 확인해야 하는 경우에 도움이 됩니다.

보고 서비스는 각 끝점에서 수집한 데이터를 검색할 수 있도록 구성되어 있습니다. 다양한 용도에 맞게 사용자 지정 보고서를 작성하거나 CA Access Control for Virtual Environments 에서 기본적으로 제공하는 기존 보고서를 사용할 수 있습니다. 보고 서비스는 서버를 기반으로 하므로, 이 서비스를 사용하면 한 곳에서 보고서를 저장하고 관리할 수 있으며 보고서에 안전하게 액세스(SSL)할 수 있습니다. 항상 사용 가능하도록 보고 서비스를 구성할 수 있습니다. 단일 서버나 분산 구성에서 보고 서비스 구성 요소를 설치할 수 있습니다.

참고: 보고 서비스 구성 요소는 CA Access Control for Virtual Environments 적용 시스템 외부에서 작동하므로, 기존 구현을 다시 구성할 필요 없이 효율적으로 사용할 수 있습니다.

보고 서비스 구성 요소

보고 서비스는 다음 핵심 구성 요소로 구성됩니다.

- *보고서 에이전트*는 CA Access Control 서버에 있는 구성된 메시지 큐의 큐로 정보를 보내는 Windows 서비스 또는 UNIX 데몬입니다.
- *메시지 큐*는 보고서 에이전트가 보내는 끝점 정보를 받기 위해 구성된 CA Access Control 서버의 구성 요소입니다. 보고를 위해 메시지 큐는 중앙 데이터베이스와 끝점 데이터베이스 스냅숏을 주고 받습니다.
- *중앙 데이터베이스*는 보고를 포함한 CA Access Control 엔터프라이즈 관리의 기능에 대한 정보를 수록하는 관계형 데이터베이스 관리 시스템(RDBMS)입니다. 다양한 도구를 사용하여 데이터베이스에 저장된 데이터에서 CA Access Control 구현에 대한 정보를 검색할 수 있습니다.
- *보고서 포털*은 CA Access Control 보고서를 제공하는 응용 프로그램 서버입니다. 이 서버는 BusinessObjects InfoView 포털을 사용하므로 사용자가 중앙 데이터베이스에 저장된 보고 정보를 활용할 수 있습니다.
- 엔터프라이즈 관리 서버는 메시지 큐에서 보고 데이터를 읽고 이 데이터를 중앙 데이터베이스에 쓰기 위해 사용됩니다.
- 일반적인 보고 시나리오의 경우 데이터를 쉽게 작성할 수 있도록 기본 제공 보고서가 포함되어 있습니다.

보고 서비스 작동 방법

보고 서비스를 사용하여 각 관리되는 장치, 사용자 저장소, PUPM 정책 저장소에서 수집된 데이터를 검사할 수 있습니다. 보고 서비스를 제대로 설정하려면 보고 서비스가 어떤 방식으로 데이터를 수집 및 저장하고 해당 데이터에서 보고서를 생성하는지 알아야 합니다.

보고 서비스는 다음 작업을 수행합니다.

- 각 관리되는 장치에서 데이터를 수집합니다.

  각 관리되는 장치는 메시지 큐에 보고서 데이터를 보냅니다.
- 중앙 데이터베이스에 데이터를 저장합니다.

  CA Access Control for Virtual Environments 는 메시지 큐에서 보고서 데이터를 가져와 중앙 데이터베이스에 저장합니다.
- 보고서 데이터의 스냅숏을 캡처하여 중앙 데이터베이스에 저장합니다.

  CA Access Control for Virtual Environments 는 스냅숏의 일부로 PUPM 보고서 데이터를 캡처합니다.
- 저장된 데이터에서 보고서를 생성합니다.

  중앙 데이터베이스에 데이터가 있으면 보고서 포털을 사용하여 보고서를 생성하고 저장된 데이터를 쿼리할 수 있습니다. 보고서 포털은 CA Technologies 버전의 BusinessObjects InfoView 포털로서, 중앙 데이터베이스에 연결되도록 구성되었으며 미리 구성된 CA Access Control for Virtual Environments 보고서에 포함되어 제공됩니다.

보고를 위한 데이터가 수집되는 방법

보고서를 생성하려면 각 관리되는 장치에서 데이터를 수집해야 합니다. 보고 서비스는 보고서 에이전트를 사용하여 지정된 시간 또는 요청 시에 관리되는 장치에서 데이터를 수집합니다.

보고서 에이전트는 각 끝점에서 다음 작업을 수행합니다.

1. 위반 계산을 수행하고 그 결과를 CA Access Control 서버로 보냅니다.
2. 관리되는 장치에 CA Access Control 데이터베이스의 복사본을 만듭니다.

   이 복사본은 성능에 영향을 주지 않고 데이터를 처리할 수 있도록 보고서 에이전트가 사용하는 임시 복사본입니다.

3. 각 데이터베이스에서 XML 구조로 데이터를 덤프합니다.

   이 덤프는 데이터베이스에 있는 모든 개체의 덤프이므로 모든 데이터가 캡처됩니다.

4. 데이터베이스의 XML 버전을 CA Access Control 서버로 보냅니다.

   보고서 에이전트가 데이터를 CA Access Control 서버에 있는 보고 큐로 보냅니다.

추가 정보:

구성 설정이 보고서 에이전트에 영향을 주는 방식 (페이지 183)

데이터가 처리되고 저장되는 방법

각 관리되는 장치에서 데이터가 수집되면 CA Access Control 서버에서 처리되도록 전달됩니다. 처리된 데이터는 보고서 생성을 위해 중앙 데이터베이스에 전송되어 저장됩니다.

CA Access Control 서버는 다음 작업을 수행합니다.

1. 보고서 에이전트로부터 전체 데이터베이스의 XML 덤프를 받습니다.
2. 데이터베이스 스키마에 따라 MDB(Message Driven Bean)를 사용하여 XML 덤프를 처리합니다.

   들어오는 각 XML 덤프는 중앙 데이터베이스에 배치할 수 있도록 Java 개체로 변환됩니다.

3. 각 Java 개체를 중앙 데이터베이스에 삽입합니다.

   이제 중앙 데이터베이스에서 각 끝점의 데이터를 검색할 수 있습니다.

참고: 끝점 데이터는 보고서에 포함하기 전에 보고서 포털에서 가져와야 합니다(즉 스냅숏에서 캡처).

CA Access Control 엔터프라이즈 관리가 스냅숏을 캡처하는 방법

CA Access Control 엔터프라이즈 관리는 끝점 덤프를 포함하여 데이터가 보고서에 표시되기 전에 스냅숏에서 보고서 데이터를 캡처해야 합니다. CA Access Control 엔터프라이즈 관리가 스냅숏을 캡처한 다음에 CA Access Control 보고서를 생성하고 볼 수 있습니다.

스냅숏 정의에 지정된 시간에 CA Access Control 엔터프라이즈 관리는 스냅숏을 캡처하기 위해 다음 작업을 수행합니다.

- 사용자 저장소의 데이터를 중앙 데이터베이스로 추출합니다.
- PUPM 정책 저장소의 데이터를 중앙 데이터베이스로 추출합니다.
- 중앙 데이터베이스에 있는 최신 끝점 스냅숏을 스냅숏에 포함하도록 플래그 지정합니다.

CA Access Control 엔터프라이즈 관리에서 보고서를 보는 방법

이 프로세스는 관리되는 장치에 대한 정보를 제공하는 CA Access Control for Virtual Environments 보고서를 만들고 보는 방법에 대해 설명합니다. CA Access Control for Virtual Environments 보고서는 [assign the value for cabi in your book]에서도 볼 수 있습니다.

CA Access Control 엔터프라이즈 관리에서 보고서를 보려면 다음을 수행하십시오.

1. 스냅숏 정의를 만듭니다.

   스냅숏 정의는 CA Access Control for Virtual Environments 이 수집하는 보고서 데이터를 지정하고 스냅숏 일정을 정의합니다.

2. 보고를 위해 관리되는 장치를 구성했는지 확인합니다.
3. (선택 사항) 스냅숏 데이터를 캡처합니다.

   예약된 스냅숏을 기다리고 싶지 않으면 "스냅숏 데이터 캡처" 작업을 사용하여 스냅숏을 지금 수집할 수 있습니다.

4. 보고서를 실행합니다.

   보고서가 만들어집니다.

5. 보고서를 봅니다.

스냅샷 데이터 캡처

일반적으로 보고서 데이터는 예약된 간격으로 스냅숏에 캡처됩니다. 필요할 때 스냅숏 데이터를 캡처하려면 "스냅숏 데이터 캡처" 작업을 사용하여 데이터를 중앙 데이터베이스로 즉시 내보내십시오.

중요! 많은 양의 데이터를 내보내는 경우 스냅숏 데이터를 내보내는 데 시간이 오래 걸릴 수 있습니다. 보고 스냅숏에 많은 양의 데이터가 포함되는 경우 스냅숏을 예약하기 위한 스냅숏 정의를 만드는 것이 좋습니다.

참고: 기본적으로, 스냅숏 정의를 캡처하려면 시스템 관리자 역할이 있어야 합니다.

다음을 수행하십시오.

1. CA Access Control 엔터프라이즈 관리에서 다음을 수행합니다.
   a. "보고서"를 클릭합니다.
   b. "작업" 하위 탭을 클릭합니다.
   c. "스냅숏 데이터 캡처"를 클릭합니다.

      "스냅숏 데이터 캡처" 페이지가 표시됩니다.
2. 캡처할 스냅숏 정의의 이름을 선택하고 "제출"을 클릭합니다.

   CA Access Control 엔터프라이즈 관리가 스냅숏 데이터를 중앙 데이터베이스로 내보냅니다.

참고: "제출된 작업 보기" 작업을 사용하여 작업의 진행 상황을 확인할 수 있습니다. 스냅숏 정의를 만드는 방법에 대한 자세한 내용은 *온라인 도움말*을 참조하십시오.

CA Access Control 엔터프라이즈 관리에서 보고서 실행

보고서는 CA Access Control for Virtual Environments 가 스냅숏에서 캡처하는 데이터로 구성되어 있습니다. CA Access Control for Virtual Environments 가 스냅숏을 캡처한 이후에 스냅숏에 있는 데이터는 보고서에 사용할 수 있습니다. 보고서를 보려면 먼저 보고서를 실행해야 합니다. 기본적으로, 보고서를 실행하려면 시스템 관리자 또는 보고 역할이 있어야 하며, 실행할 보고서에 대한 특정 보고 역할이 있어야 합니다.

참고: CA Access Control 엔터프라이즈 관리에서 되풀이 보고서를 예약할 수 없습니다. 하지만 [assign the value for cabi in your book]에서는 되풀이 보고서를 예약할 수 있습니다. [assign the value for cabi in your book]에서 보고서를 예약하는 경우 CA Access Control 엔터프라이즈 관리에서 이 보고서를 볼 수 없지만 CA Access Control 엔터프라이즈 관리에서 보고서를 실행하면 [assign the value for cabi in your book]에서 이 보고서를 볼 수 있습니다.

다음을 수행하십시오.

1. CA Access Control 엔터프라이즈 관리에서 다음을 수행합니다.
   a. "보고서"를 클릭합니다.
   b. 언어 하위 탭을 클릭합니다.

      언어 하위 탭은 CA Access Control 엔터프라이즈 관리를 설치할 때 사용한 언어의 이름입니다. 예를 들어, CA Access Control 엔터프라이즈 관리를 영어로 설치한 경우 "영어" 하위 탭이 표시됩니다.
   c. 왼쪽의 작업 메뉴에서 실행할 보고서 유형의 트리를 확장합니다.

      보고서의 목록이 나타납니다.
2. 실행할 보고서를 선택합니다.

   매개 변수 화면이 나타납니다.

3. 필요한 매개 변수 정보를 제공합니다.

   매개 변수 정보를 입력할 때 다음 사항을 고려하십시오.

   - 매개 변수를 지정했는데 중앙 데이터베이스가 이 매개 변수에 대한 어떠한 값도 없는 경우 보고서가 실패합니다.

     예를 들어, 하나 이상의 사용자에 대해 보고서를 정의했는데 중앙 데이터베이스에 어떠한 사용자 데이터도 없는 경우, 보고할 사용자 데이터가 없으므로 보고서가 비어 있게 됩니다.

   참고: 여러 매개 변수를 선택하려면 Ctrl 키를 누른 채 클릭하십시오.

4. "제출"을 클릭합니다.

   보고서가 보고서 서버로 제출됩니다.

추가 정보:

보고서 예약 (페이지 206)

보고서 보기

CA Access Control for Virtual Environments 보고서는 관리되는 장치에 대한 정보를 제공합니다. 보고서를 보려면 먼저 CA Access Control 보고서를 실행해야 합니다.

참고: CA Access Control 엔터프라이즈 관리에서 보고서를 보려면 브라우저에서 타사 세션 쿠키를 활성화하십시오. 기본적으로 보고서를 보려면 시스템 관리자 또는 보고 역할이 있어야 합니다.

다음을 수행하십시오.

1. CA Access Control 엔터프라이즈 관리에서 다음을 수행합니다.
   a. "보고서"를 클릭합니다.
   b. "작업" 하위 탭을 클릭합니다.
   c. "내 보고서 보기"를 클릭합니다.

      "내 보고서: 보고서 관리 구성 화면"이 나타납니다.

2. 보려는 보고서를 검색합니다.

   검색 조건과 일치하는 보고서의 목록이 표시됩니다.

3. 보려는 보고서를 선택합니다.

   보고서가 표시됩니다.

4. (선택 사항) 왼쪽 위에 있는 "이 보고서 내보내기"를 클릭하여 보고서를 다음 형식으로 내보냅니다.

   - Crystal Reports
   - Excel
   - PDF
   - Word
   - RTF

   보고서가 추출됩니다.

스냅숏 관리

CA Access Control 엔터프라이즈 관리를 사용하여 스냅숏 정의를 보고, 수정하고, 삭제할 수 있습니다. 스냅숏 정의를 보거나 수정할 때 "프로필", "되풀이" 및 "유지 관리" 탭이 표시됩니다. "유지 관리" 탭은 스냅숏을 한 번 캡처한 후에만 표시됩니다.

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

스냅숏 정의를 보거나, 수정하거나, 삭제하려면 "보고서", "작업", "스냅숏 정의 관리"로 이동하여 실행할 작업을 클릭하십시오.

참고: 데이터를 중앙 데이터베이스로 내보내기 위해 스냅숏 정의가 사용되고 있는 경우에는 해당 스냅숏 정의를 삭제할 수 없습니다. 사용되는 스냅숏 정의를 삭제하면 중앙 데이터베이스로 데이터를 내보내는 작업이 중지되지만 스냅숏 정의는 계속 사용할 수 있습니다.

BusinessObjects InfoView 보고서 포털

*보고서 포털*은 CA Access Control 보고서를 제공하는 응용 프로그램 서버입니다. 이 서버는 BusinessObjects InfoView 포털을 사용하므로 사용자가 중앙 데이터베이스에 저장된 보고 정보를 활용할 수 있습니다.

보고서 작업을 위해 InfoView 열기

BusinessObjects InfoView 를 사용하여 CA Access Control 보고서에 액세스합니다. 다음 절차에서는 보고 인터페이스(BusinessObjects InfoView)에 액세스하는 방법에 대해 설명합니다.

다음 단계를 수행하십시오.

1. 다음 방법 중 *하나*를 사용하여 InfoView 를 시작합니다.
   - BusinessObjects InfoView 가 설치된 컴퓨터에서 "시작", "프로그램", "BusinessObjects XI Release 2", "BusinessObjects Enterprise", "BusinessObjects Enterprise Java InfoView"를 차례로 선택합니다.
   - 컴퓨터의 브라우저에서 다음 URL 로 이동합니다.

     http://*ACRPTGUI_host*:*ACRPTGUI_port*/businessobjects/enterprise115

     ACRPTGUI_host - InfoView 가 설치된 컴퓨터의 이름 또는 IP 주소(보고서 포털).

     ACRPTGUI_port - InfoView 에 액세스하는 데 사용되는 포트 번호(기본값 9085).

   InfoView 로그온 페이지가 나타납니다.
2. InfoView 를 설치할 때 설정한 자격 증명을 입력하고 "로그온"을 클릭합니다.

   InfoView 홈 페이지가 나타납니다.

보고서 실행

보고 인터페이스(BusinessObjects InfoView)를 연 후 보고서를 선택하고 실행할 수 있습니다.

다음 단계를 수행하십시오.

1. InfoView 를 엽니다.

   InfoView 홈 페이지가 나타납니다.
2. "홈", "공용 폴더", "CA Reports(CA 보고서)"를 확장하고 왼쪽 프레임에서 CA Access Control 을 클릭합니다.

   CA Access Control 페이지가 나타납니다.

3. 표시할 보고서의 링크 제목을 클릭합니다.

   추가 값을 입력하여 표시할 보고서의 범위를 정의할 수 있는 보고서 페이지가 나타납니다.

4. 양식 필드를 입력하여 가져오려는 보고서 범위를 정의하고 "확인"을 클릭합니다.

   보고서 출력 페이지가 나타납니다.

   추가 쿼리를 수행하여 보고서 생성에 영향을 줄 수 있습니다. 예를 들어 모두 포함하도록 선택하거나 호스트를 선택하여 알려진 모든 호스트 또는 단일 호스트에서 보고서를 생성할 수 있습니다. 또한 과거의 모든 데이터를 표시하거나 특정 날짜 범위의 데이터만 표시하도록 날짜 범위를 지정할 수 있습니다.

   참고: %(퍼센트) 기호를 사용하여 와일드카드 값을 지정할 수 있습니다. %는 표준 SQL 선택 표기법에 따라 사용하며 일반적으로 와일드카드 지정에서 수행하는 것처럼 단일 문자를 나타내지 *않습니다*.

보고서 예약

다양한 방법으로 보고서를 실행할 수 있습니다. 보고서 제목을 클릭하고 값을 지정하여 보고서를 실행하거나 다양한 옵션을 선택하여 보고서를 예약할 수 있습니다.

보고서를 예약하려면

1. InfoView 를 엽니다.

   InfoView 홈 페이지가 나타납니다.

2. "홈", "공용 폴더", "CA Reports(CA 보고서)"를 확장하고 왼쪽 프레임에서 CA Access Control 을 클릭합니다.

   CA Access Control 페이지가 나타납니다.

3. 예약할 보고서의 제목 아래에서 "일정"을 클릭합니다.

   선택한 보고서의 "일정" 페이지가 나타납니다.

4. "Run object(개체 실행)" 드롭다운 목록 선택을 수정하여 예약된 보고서를 실행할 시간을 지정합니다.
5. "매개 변수" 섹션을 확장하여 보고서 실행에 대해 값을 지정합니다.
   a. "비어 있음"을 클릭하여 각 매개 변수에 대해 값을 정의합니다.

      "Enter prompt values(프롬프트 값 입력)" 섹션 필드가 나타납니다.

   b. 필요에 따라 값을 정의하고 "확인"을 클릭합니다.

      보고서 실행에 사용할 수 있도록 정의한 값이 저장됩니다.
6. "일정"을 클릭하여 선택한 일정 옵션에 따라 보고서를 실행합니다.

   설정한 보고서 일정 인스턴스를 확인하는 "기록" 페이지가 나타납니다.

참고: BusinessObjects InfoView 사용에 대한 자세한 내용은 *BusinessObjects Enterprise XI Release 2 InfoView 사용자 안내서*를 참조하십시오.

생성된 보고서 보기

보고서가 생성된 후 CA Access Control 보고서 목록에서 다음 중 하나를 수행하여 보고서를 표시할 수 있습니다.

- 표시할 보고서의 "View Latest Instance(최신 인스턴스 보기)"를 클릭합니다.
- "기록"을 클릭한 다음 날짜와 시간을 클릭하여 표시할 보고서 인스턴스를 선택합니다.

참고: BusinessObjects InfoView 사용에 대한 자세한 내용은 *BusinessObjects Enterprise XI Release 2 InfoView 사용자 안내서*를 참조하십시오.

보고서 상태 보기

보고서의 상태를 확인하여 보고서가 성공적으로 실행되었는지 여부를 확인할 수 있습니다.

보고서 상태를 보려면

1. InfoView 를 엽니다.

   InfoView 홈 페이지가 나타납니다.

2. "홈", "공용 폴더", "CA Reports(CA 보고서)"를 확장하고 왼쪽 프레임에서 CA Access Control 을 클릭합니다.

   CA Access Control 페이지가 나타납니다.

3. 표시할 보고서의 "기록" 링크를 클릭합니다.

   보고서가 실행된 날짜 및 시간 목록을 볼 수 있는 보고서의 "기록" 페이지가 나타납니다.

   목록의 각 항목에 다음 내용이 표시됩니다.

   - 인스턴스 시간 - 보고서가 실행된 날짜 및 시간
   - 제목 - 보고서 제목
   - 실행한 사람 - 보고서를 실행한 사용자 이름
   - 매개 변수 - 해당 보고서 실행을 위해 선택한 매개 변수
   - 형식 - 보고서의 출력 형식
   - 상태 - 보고서의 현재 상태(예: 성공)
   - 다시 예약 - 보고서를 다시 실행할 수 있는 링크

참고: BusinessObjects InfoView 사용에 대한 자세한 내용은 *BusinessObjects Enterprise XI Release 2 InfoView 사용자 안내서*를 참조하십시오.

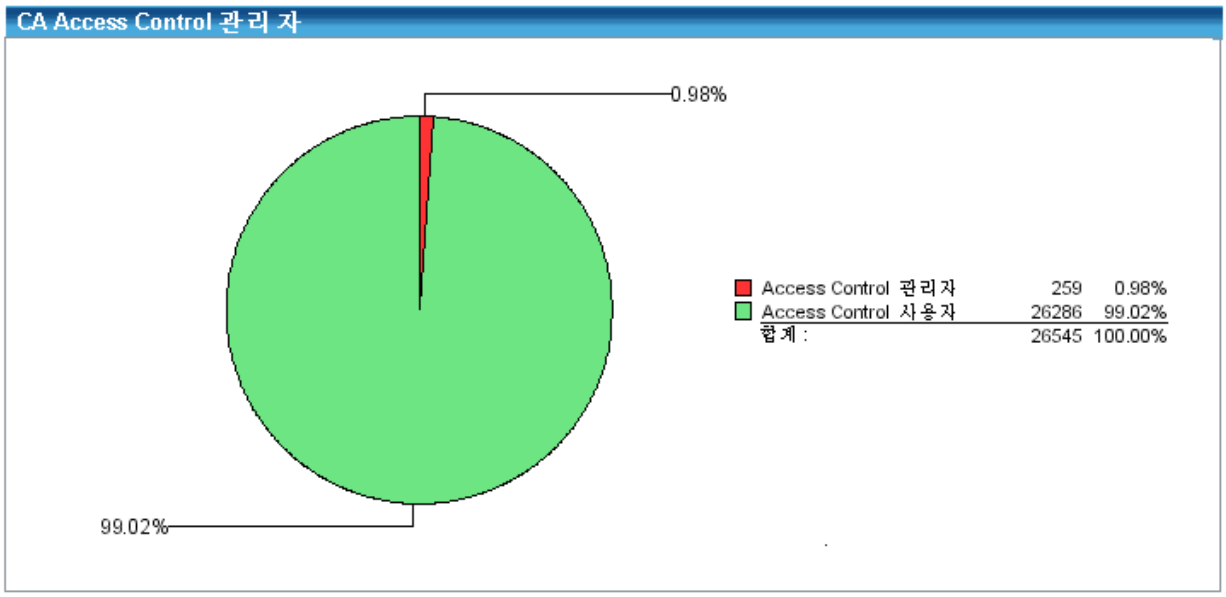
표준 보고서

기본적으로 CA Access Control for Virtual Environments 보고 서비스는 보고서 포털 설치의 일부로 배포되는 표준 보고서와 함께 제공됩니다.

표준 보고서 이외에도 보고서를 확장하고 다른 기능이 포함된 비슷한 보고서를 만들거나 완전히 새로운 보고서를 생성할 수 있습니다.

보고서 모양

보고서 출력에는 필요에 따라 표와 그래픽이 적절하게 사용됩니다. 예를 들어, 일부 보고서는 이해하기 쉬운 원형 차트와 함께 관련 세부 정보를 제공합니다. 아래 그림과 같이 CA Access Control 관리자 보고서에는 CA Access Control 관리자 역할을 수행하는 끝점 사용자의 수를 나타내는 파이형 차트가 제공됩니다. 일반 사용자에 비해 관리자의 비율이 높으면 보안상 위험할 수 있으므로 그래픽을 통해 보안 노출이 있는지 여부를 신속하게 알 수 있습니다. 이 예제 차트에서 커다란 빨간색 쐐기 모양은 현재 엔터프라이즈 사용자 기반의 거의 1%가 CA Access Control 관리를 수행할 수 있음을 나타내기 때문에 보안상 위험하다는 것을 나타냅니다.



그래픽 이외에도 각 보고서에는 실제 끝점 값에 대해 연관된 목록이 있습니다. 다음은 CA Access Control 관리자 보고서에서 가져온 이 표의 예제입니다.

CA Access Control 관리자

사용자 이름	전체 이름	호스트 ID	관리자 모드 사용	암호 관리자 모드 사용	운영자 모드 사용
_seagent					
		SYSTEMA	예		
		SYSTEMB	예		
		SYSTEMC	예		

권한 있는 계정 관리 보고서

권한 있는 계정 관리 보고서를 사용하면 권한 있는 계정 관리의 세부 정보를 볼 수 있습니다.

다음은 표준 권한 있는 계정 관리 보고서의 목록입니다.

CA Access Control 끝점별 권한 있는 계정

이 보고서는 끝점 유형과 끝점 이름별로 권한 있는 계정의 목록을 표시합니다. 이 보고서를 사용하면 끝점 유형과 이름별로 권한 있는 계정을 볼 수 있습니다. 이 보고서를 검토한 다음에는 각 끝점에 연계된 권한 있는 계정의 수를 파악할 수 있습니다.

이 보고서는 다음 정보를 표시합니다.

- 스냅숏 시간
- 끝점 유형 및 이름
- 계정 이름
- 마지막 체크 아웃 사용자
- 마지막 체크 아웃
- 마지막 암호 변경

CA Access Control 사용자별 PUPM 역할 및 권한 있는 계정

이 보고서는 사용자 계정별로 권한 있는 액세스 역할 및 권한 있는 계정의 목록을 표시합니다. 이 보고서를 사용하면 연계된 역할 및 사용자 계정별로 권한 있는 계정을 검토할 수 있습니다.

이 보고서는 다음 정보를 표시합니다.

- 스냅숏 시간
- 사용자 ID
- 끝점 시간 및 이름
- 역할 이름 및 설명
- 계정 이름
- 예외
- 마지막 암호 변경

CA Access Control 끝점별 권한 있는 계정 요청

이 보고서는 끝점 유형 및 끝점 이름별로 권한 있는 계정 요청의 목록을 표시합니다. 이 보고서를 사용하여 권한 있는 계정을 체크 아웃하기 위한 요청 및 해당 끝점 유형과 이름을 검토할 수 있습니다.

이 보고서는 다음 정보를 표시합니다.

- 스냅숏 시간
- 끝점 유형 및 이름
- 계정
- 요청자
- 요청 정당화
- 유효 날짜
- 승인자
- 승인자 설명

참고: 이 보고서는 활성화된 권한 있는 계정 요청만 표시합니다.

CA Access Control 승인자별 권한 있는 계정 요청

이 보고서는 승인자별로 권한 있는 계정 요청의 목록을 표시합니다. 이 보고서를 사용하면 요청을 승인한 사용자별로 권한 있는 계정 요청을 검토할 수 있습니다. 보고서를 검토한 다음에는 승인자 역할을 변경하고, 사용자를 추가로 할당하고, 역할에서 사용자를 제거할 수 있습니다.

이 보고서는 다음 정보를 표시합니다.

- 스냅숏 시간
- 승인자 사용자 ID
- 끝점 유형 및 이름
- 계정
- 요청자 이름 및 ID
- 요청 정당화
- 유효 날짜
- 승인자 설명

참고: 이 보고서는 활성화된 권한 있는 계정 요청만 표시합니다.

CA Access Control 요청자별 권한 있는 계정 요청

이 보고서는 권한 있는 계정의 암호를 요청한 사용자별로 권한 있는 계정 요청을 표시합니다. 이 보고서를 사용하면 권한 있는 계정을 체크 아웃하기 위한 다른 사용자의 요청을 검토할 수 있습니다. 이 보고서를 검토한 다음에는 체크 아웃 요청 수와 요청한 사용자를 파악할 수 있습니다.

이 보고서는 다음과 같은 정보를 수록합니다.

- 스냅숏 이름
- 승인자 사용자 ID
- 끝점 유형 및 이름
- 계정
- 요청 정당화
- 유효 날짜
- 승인자
- 승인자 설명

참고: 이 보고서는 활성화된 권한 있는 계정 요청만 표시합니다.

CA Access Control 권한 있는 계정별 PUPM 사용자

이 보고서는 끝점 유형 및 이름별로 권한 있는 계정에 액세스할 수 있는 사용자의 목록을 표시합니다. 이 보고서를 사용하면 사용자가 권한 있는 계정에 액세스하는 방법과 각 권한 있는 계정의 원래 이름 및 끝점 유형을 파악할 수 있습니다.

이 보고서는 다음 정보를 표시합니다.

- 스냅숏 유형
- 끝점 유형 및 이름
- 권한 있는 계정 이름
- 사용자 이름
- 사용자 ID
- Request

CA Access Control 역할별 PUPM 사용자

이 보고서는 사용자의 목록 및 각각의 연계된 권한 있는 계정 역할을 표시합니다. 이 보고서를 사용하면 사용자가 권한 있는 계정 역할에 연계된 방식과 현재 상태가 회사의 보안 표준에 부합하는지 여부를 파악할 수 있습니다.

이 보고서는 다음 정보를 표시합니다.

- 스냅숏 시간
- 역할 이름
- 구성원 수
- 사용자 이름
- 사용자 ID
- 전자 메일 주소

CA User Activity Reporting Module 보고서

CA User Activity Reporting Module 보고서는 CA Access Control for Virtual Environments 작업, 리소스 관리 등에 대한 자세한 정보를 표시합니다.

CA User Activity Reporting Module 보고서에 대한 자세한 내용은 CA User Activity Reporting Module 설명서를 참조하십시오.

사용자 지정 보고서

CA Access Control 보고서는 모두 Crystal Reports Designer XI 를 사용하여 작성되었습니다. 그런 다음 BusinessObjects InfoView 를 통해 웹 기반 형식으로 제공됩니다. 제공된 보고서를 사용자 지정하려면 Crystal Reports Designer XI 가 설치되어 있어야 합니다.

참고: 이 안내서의 지침은 처음으로 보고서를 사용자 지정할 때 도움이 되는 몇 가지 힌트를 제공합니다. Crystal Reports Designer XI 에 대한 자세한 내용은 *BusinessObjects Enterprise XI Release 2 디자이너 안내서*를 참조하십시오.

BusinessObjects 용 CA Access Control Universe

BusinessObjects 용 CA Access Control Universe 는 CA Access Control 보고 서비스 중앙 데이터베이스를 간단하게 표시합니다. Universe 는 데이터베이스의 데이터에 매핑되는 의미 체계 계층입니다. 이 계층은 최종 사용자를 복잡한 데이터베이스 구조에서 분리합니다. Universe 는 클래스 및 개체 집합입니다.

Universe 는 BusinessObjects Enterprise Designer 를 사용하여 작성됩니다. CA Access Control Universe 는 CA Technologies 에서 제공되며 이를 통해 CA Access Control 보고 서비스 중앙 데이터베이스에서 간단하게 보고서를 작성할 수 있습니다. CA Technologies 에서 개발한 CA Access Control Universe 를 수정하면 안 됩니다. 필요한 경우 자체 universe 를 위한 기반으로 사본을 작성할 수 있습니다.

CA Access Control Universe 보기

BusinessObjects Designer 를 사용하여 CA Access Control Universe 를 볼 수 있습니다.

CA Access Control Universe 를 보려면

1. "시작", "프로그램", "BusinessObjects XI Release 2", "BusinessObjects Enterprise", "Designer"를 차례로 선택합니다.

   BusinessObjects Designer 에 로그인할 수 있는 "User Identification(사용자 ID)" 대화 상자가 나타납니다.

2. 자격 증명을 입력하고 "OK(확인)"를 클릭합니다.

   "Quick Design(빠른 디자인)" 마법사의 시작 화면이 나타납니다.

3. "Run this Wizard at Startup(시작 시 이 마법사 실행)" 확인란의 선택을 취소하고 "Cancel(취소)"을 클릭합니다.

   비어 있는 디자이너 세션이 열립니다. 사용자 이름과 리포지토리 이름이 제목 표시줄에 나타납니다.

4. "파일", "열기"를 클릭하고 CA Access Control Universe 가 포함된 디렉터리로 이동하여 *CA Access Control.unv* 파일을 선택하고 "열기"를 클릭합니다.

   CA Access Control Universe 가 현재 디자이너 창에서 열립니다.

   참고: CA Access Control Universe 는 기본 universe 파일 저장소로 지정된 디렉터리의 *CA Universe\CA Access Control* 에 저장됩니다.

표준 보고서 사용자 지정

모든 표준 보고서를 사용자 지정할 수 있습니다. 예를 들어 필요에 따라 제목, 색상, 로고 및 글꼴을 변경할 수 있습니다. 내용을 변경하려면 Crystal Reports Designer XI 에서 보고서를 열어야 합니다. 모든 보고서에는 해당 .rpt 파일이 있습니다. 이 파일을 열어 보고서를 사용자 지정합니다.

표준 보고서를 사용자 지정하려면

1. 디자이너에서 사용자 지정할 .rpt 파일을 엽니다.

   보고서의 디자인 보기가 나타납니다.

2. 다음 중 *하나*를 수행하십시오.
   - 보고서 제목을 변경하려면 "파일", "요약 정보"를 클릭하고 "제목" 필드에 제목을 입력합니다.
   - 텍스트를 사용자 지정하려면 디자인 보기에서 원하는 텍스트를 강조 표시하고 두 번 클릭하여 편집합니다.
   - 텍스트 모양을 변경하려면 열린 보고서에서 텍스트를 마우스 오른쪽 버튼으로 클릭하고 "Format text(텍스트 형식 지정)"를 선택하고 원하는 대로 속성을 변경합니다.
3. 사용자 지정 .rpt 파일을 저장합니다.

   새 사용자 지정 보고서가 저장되고 게시할 준비가 완료되었습니다.

사용자 지정 보고서 게시

사용자 지정 보고서는 BusinessObjects InfoView 를 사용하여 게시해야 합니다.

사용자 지정 보고서를 게시하려면

1. BusinessObjects InfoView 를 열고 관리자로 로그인합니다.

   InfoView 홈 페이지가 나타납니다.

2. "새로 만들기", "폴더"를 클릭하고 공용 폴더에서 새 폴더를 만듭니다.

   "새 폴더 만들기" 작업 페이지가 나타납니다.

3. 사용자 지정 보고서 폴더의 이름과 설명을 입력하고 "확인"을 클릭합니다.

   새 폴더가 만들어집니다.

4. "새로 만들기", "Document from local computer(로컬 컴퓨터의 문서)"를 클릭하고 생성한 새 폴더에서 Crystal Report 를 클릭합니다.

   "Add a document from your local computer(로컬 컴퓨터에서 문서 추가)" 작업 페이지가 나타납니다.

5. 사용자 지정된 rpt 파일의 보고서 제목과 경로 이름을 입력하고 "확인"을 클릭합니다.

   사용자 지정 보고서가 게시되며 이제 BusinessObjects InfoView 에서 볼 수 있습니다. 다른 보고서와 마찬가지로 예약도 가능합니다.