CA Access Control

통합 안내서

12.7

타사 고지 사항

샘플 스크립트와 샘플 SDK 코드

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

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

CA Technologies 제품 참조

이 문서는 다음 CA Technologies 제품을 참조합니다 :

- CA Access Control
- CA ControlMinder
- CA Single Sign-On(eTrust SSO)
- CA Top Secret®
- CA ACF2™
- CA Audit
- CA NSM(CA Network and Systems Management, 이전의 Unicenter NSM 및 Unicenter TNG)
- CA Software Delivery(이전의 Unicenter Software Delivery)
- Unicenter Service Desk(이전 이름: Unicenter Service Desk)
- CA User Activity Reporting Module (이전 명칭: [set the CALM variable for your book])
- CA Identity Manager

설명서 규칙

CA ControlMinder 설명서는 다음과 같은 규칙을 따릅니다.

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

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

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

예제: 명령 표기 규칙

다음 코드는 이 안내서에서 명령 규칙이 사용되는 방식을 보여 줍니다.

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

설명:

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

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

파일 위치 규칙

CA ControlMinder 설명서는 다음과 같은 파일 위치 규칙을 따릅니다.

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

CA 에 문의

기술 지원팀에 문의

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

설명서 변경 사항

이 설명서가 마지막으로 릴리스된 이후에 다음과 같이 업데이트되었습니다.

- CA ControlMinder REST API - 엔터프라이즈 관리 서버 사용자 인터페이스를 바이패스하여 공유 계정 관리 데이터베이스를 사용하여 사용자 지정 또는 타사 프로그램 간 통신하기 위한 REST 요청이 추가되었습니다.

목차

제 1 장: 안내서 정보

이 안내서는 CA Access Control 과 타사 소프트웨어를 통합하는 방법에 대한 정보를 제공합니다. 여기에는 CA User Activity Reporting Module, CA 디렉터리, CA SiteMinder, RSA SecurID, ObserveIT Enterprise 가 포함됩니다. 이 안내서의 장은 CA Access Control 에만 적용됩니다.

용어를 간단히 나타내기 위해 이 안내서에서는 제품을 CA ControlMinder 이라고 합니다.

제 2 장: CA User Activity Reporting Module 과 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. [set the CALM variable for your book]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.

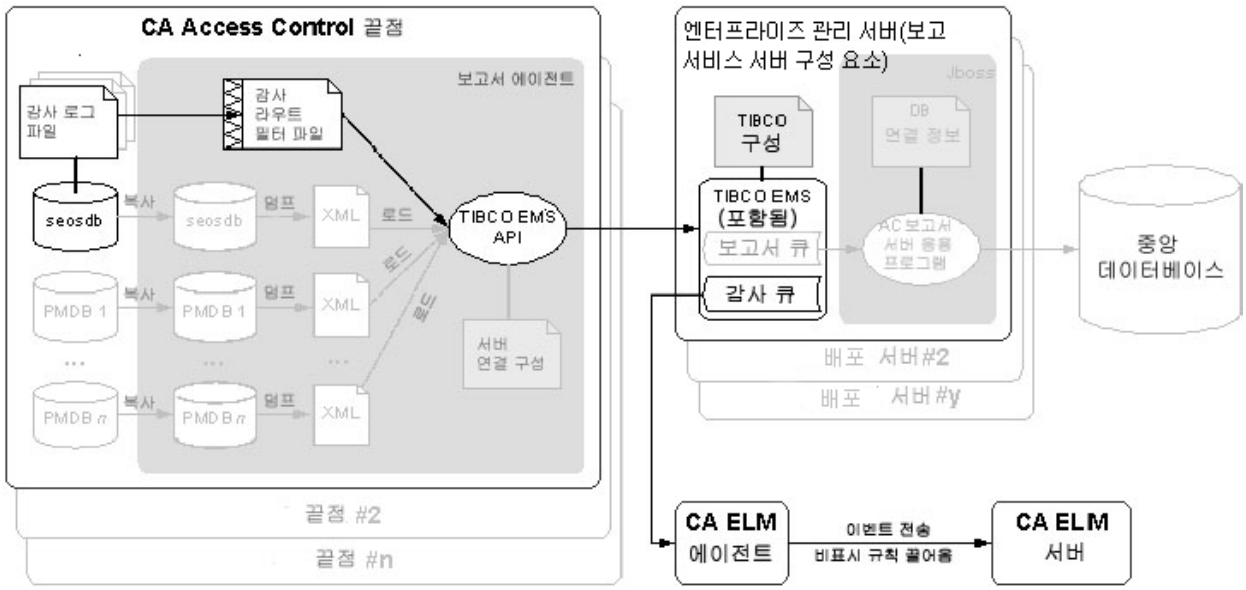
CA User Activity Reporting Module 통합 아키텍처

CA User Activity Reporting Module 와 통합하면 CA User Activity Reporting Module 가 수집하고 보고할 수 있도록 각 끝점에서 CA ControlMinder 감사 이벤트를 보낼 수 있습니다.

로컬 끝점의 감사 파일에서 배포 서버의 원격 감사 큐로 감사 이벤트를 보내도록 CA ControlMinder 을 구성할 수 있습니다. 그런 다음 감사 큐와 연결하고 감사 큐에서 이벤트(메시지)를 끌어오도록 CA User Activity Reporting Module 커넥터를 구성할 수 있습니다. CA User Activity Reporting Module 는 이러한 이벤트를 처리하고 CA User Activity Reporting Module 서버로 보냅니다.

CA ControlMinder 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.

- 하나의 CA ControlMinder 데이터베이스(seosdb)가 들어 있는 각 끝점에 보고서 에이전트 구성 요소가 설치되어 있습니다.
- 보고서 에이전트가 끝점에서 감사 데이터를 수집하여 보고서 서버로 보냅니다.

- 배포 서버는 감사 데이터를 감사 큐에 누적합니다.
- CA User Activity Reporting Module 에이전트는 감사 큐에서 이벤트를 수집하여 처리를 위해 CA User Activity Reporting Module 서버로 보냅니다.

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.

참고: CA Access Control 엔터프라이즈 관리는 기본적으로 배포 서버를 엔터프라이즈 관리 서버에 설치합니다. 가용성을 높이기 위해 다른 컴퓨터에 배포 서버를 설치할 수도 있습니다.

CA User Activity Reporting Module 통합 구성 요소

CA User Activity Reporting Module 통합에서는 다음과 같은 CA ControlMinder 구성 요소를 사용합니다. 이러한 구성 요소는 CA ControlMinder 엔터프라이즈 보고 서비스의 일부입니다.

- *보고서 에이전트*는 각각의 CA ControlMinder 또는 UNAB 에서 실행되는 Windows 서비스 또는 UNIX 데몬이며, 배포 서버에 있는 구성된 메시지 큐의 큐로 정보를 보냅니다. CA User Activity Reporting Module 통합에 대해 보고서 에이전트는 정기적으로 감사 로그 파일에서 끝점 감사 메시지를 수집하고 이러한 이벤트를 예약된 보고서 서버의 감사 큐로 보냅니다.
- *메시지 큐*는 보고서 에이전트가 보내는 끝점 정보를 받기 위해 구성된 배포 서버의 구성 요소입니다. 보고를 위해 메시지 큐는 CA ControlMinder 웹 서비스를 사용하여 중앙 데이터베이스에 전달합니다. 중복 및 장애 조치를 위해 정보를 수집하고 전달하는 여러 개의 보고서 서버를 사용할 수 있습니다.

참고: CA Access Control 엔터프라이즈 관리는 기본적으로 배포 서버를 엔터프라이즈 관리 서버에 설치합니다.

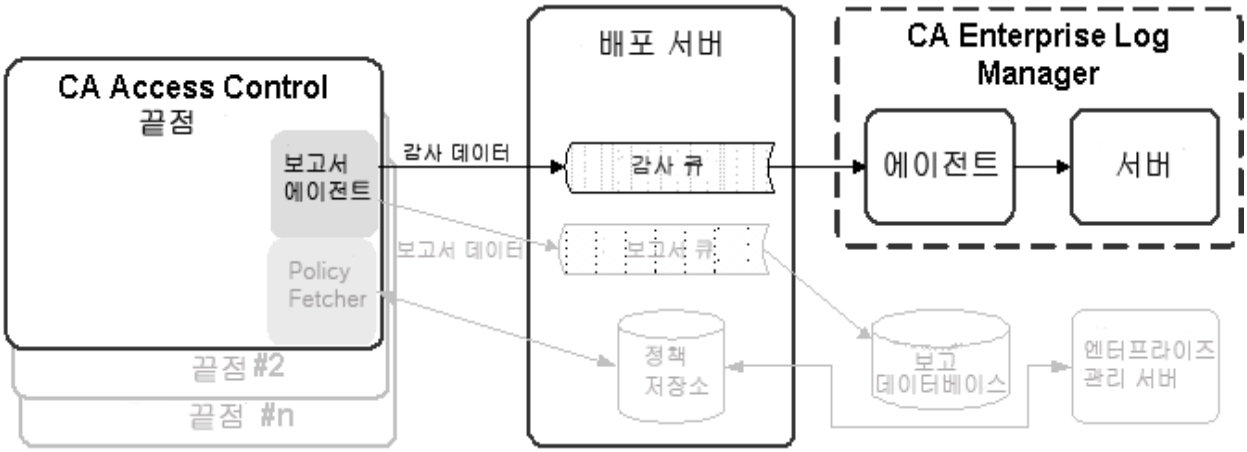
CA User Activity Reporting Module 통합에서는 다음과 같은 CA User Activity Reporting Module 구성 요소도 사용합니다.

- *CA User Activity Reporting Module 에이전트*는 각각 단일 이벤트 소스에서 원시 이벤트를 수집한 다음 처리를 위해 이벤트를 CA User Activity Reporting Module 서버로 보내는 커넥터를 사용하여 구성된 일반 서비스입니다. CA ControlMinder 감사 데이터의 경우 에이전트에서 CA ControlMinder 커넥터를 배포합니다.
- *CA ControlMinder 커넥터*는 CA ControlMinder 감사 이벤트 원본에 즉시 사용 가능한 CA User Activity Reporting Module 통합입니다. 이 커넥터를 사용하면 CA ControlMinder 보고서 서버에서 원시 이벤트를 수집하고 변환된 이벤트를 규칙에 따라 이벤트 로그 저장소(핫 데이터베이스에 삽입됨)로 전송할 수 있습니다.
- *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 ControlMinder 에서 CA User Activity Reporting Module 로 전달되는 방법

CA ControlMinder 이 CA User Activity Reporting Module 와 통합되는 방법과 이 통합을 구성할 때 고려해야 할 사항을 이해하려면 먼저 CA ControlMinder 과 CA User Activity Reporting Module 간의 감사 데이터 흐름을 고려해야 합니다. 다음 그림에서는 CA ControlMinder 이 감사 이벤트를 배포 서버의 메시징 큐로 라우팅하는 방법에 대해 설명합니다. 여기서 CA User Activity Reporting Module 에이전트의 CA ControlMinder 커넥터가 이벤트를 끌어오고 매핑 및 변환한 다음 CA User Activity Reporting Module 서버로 보냅니다.



1. 보고서 에이전트는 로컬 끝점의 감사 파일에서 감사 이벤트를 수집하고, 필터링 정책을 적용한 다음 보고서 서버에 있는 감사 큐에 이벤트를 배치합니다.
2. CA User Activity Reporting Module 에이전트에 의해 배포된 CA User Activity Reporting Module 커넥터는 감사 큐와 연결하고 감사 큐에서 이벤트(메시지)를 끌어옵니다.
3. CA User Activity Reporting Module 커넥터 및 에이전트는 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 ControlMinder 에 대해 CA User Activity Reporting Module 를 설정하는 방법

CA User Activity Reporting Module 를 사용하여 모든 CA ControlMinder 끝점에 있는 감사 데이터를 수록하는 보고서를 만들려면 우선 엔터프라이즈 보고를 구현하십시오. 엔터프라이즈 보고 기능을 구현하면 끝점에서 보고서 에이전트가 활성화되므로 CA User Activity Reporting Module 와 통합하기 전에 엔터프라이즈 보고 기능을 구현해야 합니다. 엔터프라이즈 보고가 구현되면 CA ControlMinder 에 대해 CA User Activity Reporting Module 를 설정하십시오.

CA ControlMinder 에 대해 CA User Activity Reporting Module 를 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. 배포 서버나 그 근처에 CA User Activity Reporting Module 에이전트를 설치합니다.

   에이전트는 배포 서버에 액세스할 수 있고 지정된 포트를 통해 보고서 서버와 통신해야 합니다. 또한 CA User Activity Reporting Module 서버에 액세스할 수 있어야 합니다.

   참고: 설치하기 전에 운영 체제에서 CA User Activity Reporting Module 에이전트가 지원되는지 확인하십시오. 에이전트 설치에 대한 자세한 내용은 *CA User Activity Reporting Module 에이전트 설치 안내서*를 참조하십시오.

3. CA Access Control 엔터프라이즈 관리를 설치합니다.

   참고: 자세한 내용은 *구현 안내서*를 참조하십시오.

4. 에이전트에 대한 커넥터를 만듭니다.

   CA User Activity Reporting Module 에이전트를 설치했으며 CA User Activity Reporting Module 서버와 통신하도록 설정했으면 커넥터를 만들고 CA ControlMinder 이벤트 원본(보고서 서버의 감사 큐)에 액세스할 수 있도록 구성해야 합니다.

참고: 다음 항목은 커넥터 세부 정보와 성공적인 통합을 위해 구성해야 하는 커넥터 구성 요구 사항을 포함하여, CA ControlMinder 이벤트 수집을 위해 요구되는 설정에 대해 설명합니다. 커넥터를 만드는 방법에 대한 자세한 내용은 *CA User Activity Reporting Module 관리 안내서* 및 *온라인 도움말*을 참조하십시오.

5. CA Access Control 엔터프라이즈 관리에서 CA User Activity Reporting Module 로의 연결을 만듭니다.
6. (선택 사항) 감사 수집기를 구성합니다.
7. 감사 수집을 위해 CA ControlMinder 끝점을 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 ControlMinder 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 ControlMinder 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 ControlMinder 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 ControlMinder"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 ControlMinder 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 ControlMinder 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 ControlMinder 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 ControlMinder 이 지정된 감사 이벤트를 배포 서버로 보내지 않도록 만들지만 CA ControlMinder 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 ControlMinder 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 ControlMinder 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 ControlMinder 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 ControlMinder 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 ControlMinder 을 설정하는 것이 좋습니다. 이렇게 하면 CA ControlMinder 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 ControlMinder 은 다음과 같은 logmgr 섹션 구성 설정을 지정합니다.

```
BackUp_Date=yes
audit_max_files=50
```

이 경우 CA ControlMinder 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 ControlMinder 은 백업 파일을 삭제하지 않고 파일 누적을 계속합니다. 외부 절차를 통해 백업 파일을 관리하려는 경우 CA ControlMinder 에서 기본적으로 이러한 파일을 보호한다는 것을 기억하십시오.

CA User Activity Reporting Module 통합을 위한 기존 Windows 끝점 구성

CA Access Control 엔터프라이즈 관리가 설치되어 구성된 다음에는 보고서 에이전트를 활성화 및 구성하여 배포 서버로 감사 데이터를 보내기 위해 끝점을 구성할 수 있습니다.

참고: CA ControlMinder 을 설치할 때 감사 데이터를 수집하고 보내기 위해 끝점을 구성할 수 있습니다. 이 절차에서는 설치 시 이 옵션을 구성하지 않은 경우 감사 데이터 전송을 위해 기존 끝점을 구성하는 방법에 대해 설명합니다.

CA User Activity Reporting Module 통합을 위해 기존 Windows 끝점을 구성하려면

1. "시작", "제어판", "프로그램 추가/제거"를 차례로 클릭합니다.

   "프로그램 추가/제거" 대화 상자가 나타납니다.

2. 프로그램 목록을 스크롤하여 CA ControlMinder 를 선택합니다.

3. "변경"을 클릭합니다.

   CA ControlMinder 설치 마법사가 나타납니다.

   마법사 프롬프트에 따라 보고서 에이전트 기능과 감사 라우팅 하위 기능이 활성화되도록 CA ControlMinder 설치를 수정합니다.

   또한 타임스탬프가 지정된 감사 로그 파일 백업을 유지하도록 지정하는지도 확인하십시오.

참고: 보고서 에이전트 및 감사 라우팅을 활성화한 후 CA ControlMinder 구성 설정을 수정하여 성능 관련 설정을 변경할 수 있습니다. 이 작업을 수행하기 전에 보고서 에이전트가 감사 이벤트를 수집하여 배포 서버로 라우팅하는 방법 (페이지 24)을 이해해야 합니다. 보고서 에이전트 구성 설정에 대한 자세한 내용은 *참조 안내서*를 참조하십시오.

CA User Activity Reporting Module 통합을 위한 기존 UNIX 끝점 구성

CA Access Control 엔터프라이즈 관리가 설치되어 구성된 다음에는 보고서 에이전트를 활성화 및 구성하여 배포 서버로 감사 데이터를 보내기 위해 끝점을 구성할 수 있습니다.

참고: CA ControlMinder 을 설치할 때 감사 데이터를 수집하고 보내기 위해 끝점을 구성할 수 있습니다. 이 절차에서는 설치 시 이 옵션을 구성하지 않은 경우 감사 데이터 전송을 위해 기존 끝점을 구성하는 방법에 대해 설명합니다.

다음 단계를 수행하십시오.

1. *ACSharedDir*/lbin/report_agent.sh 를 실행합니다.

   ```
   report_agent config -server hostname [-proto {ssl|tcp}] [-port port_number
   [-rqueue queue_name] -audit -bak
   ```

   구성 옵션을 생략하면 기본 설정이 사용됩니다.

   참고: report_agent.sh 스크립트에 대한 자세한 내용은 *참조 안내서*를 참조하십시오.

2. 데이터베이스에서 *+reportagent* 사용자를 작성합니다.

   사용자는 ADMIN 과 AUDITOR 특성 및 로컬 터미널에 대한 *쓰기* 액세스 권한을 가지고 있어야 합니다. 또한 배포 서버 설치 시 정의한 보고서 에이전트 공유 암호에 대해 epassword 를 설정해야 합니다.

3. 보고서 에이전트 프로세스에 대해 SPECIALPGM 을 작성합니다.

   SPECIALPGM 은 루트 사용자를 +reportagent 사용자로 매핑합니다.

참고: 보고서 에이전트 및 감사 라우팅을 활성화한 후 CA ControlMinder 구성 설정을 수정하여 성능 관련 설정을 변경할 수 있습니다. 이 작업을 수행하기 전에 보고서 에이전트가 감사 이벤트를 수집하여 배포 서버로 라우팅하는 방법 (페이지 24)을 이해해야 합니다. 보고서 에이전트 구성 설정에 대한 자세한 내용은 *참조 안내서*를 참조하십시오.

예: selang 을 사용하여 CA User Activity Reporting Module 통합을 위해 UNIX 끝점 구성

다음 selang 명령은 보고서 에이전트를 활성화 및 구성했다고 가정하여 필요한 보고서 에이전트 사용자를 만들고 보고서 에이전트 프로세스에 대한 특별한 보안 권한을 지정하는 방법을 보여 줍니다.

```
eu +reportagent admin auditor logical epassword(Report_Agent) nonative
auth terminal (terminal101) uid( +reportagent) access(w)
er specialpgm (/opt/CA/AcessControl/bin/ReportAgent) Seosuid(+reportagent) \

Nativeuid(root) pgmtype(none)
```

CA ControlMinder 이벤트에 대한 쿼리 및 보고서

CA ControlMinder 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/support 에서 CA User Activity Reporting Module 제품 페이지를 참조하십시오.

CA ControlMinder 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. (페이지 32)
3. [set the CALM variable for your book]에 대한 연결을 구성합니다 (페이지 34).
4. (선택 사항) 감사 수집기를 구성합니다 (페이지 36).

   공유 계정 관리 감사 이벤트를 CA User Activity Reporting Module 로 보내려면 감사 수집기를 구성하십시오.

[set the CALM variable for your book] 트러스트되는 인증서를 키 저장소에 추가

[set the CALM variable for your book] 보고서는 트러스트된 인증서를 사용하여 인증됩니다. 인증서는 보고서에 표시된 정보가 트러스트된 [set the CALM variable for your book] 출처(데이터의 진위를 검증하는 출처)에서 전달되었는지 확인합니다.

CA Access Control 엔터프라이즈 관리에서 [set the CALM variable for your book] 보고서를 보려면 먼저 인증서를 내보낸 다음 키 저장소에 추가해야 합니다.

[set the CALM variable for your book] 트러스트되는 인증서를 키 저장소에 추가하려면

1. 다음 형식으로 웹 브라우저에 [set the CALM variable for your book] 서버의 URL 을 입력합니다: https://*host*:*port*

   보안 경고 대화 상자가 나타납니다.
2. "인증서 보기"를 클릭합니다.

   "인증서" 대화 상자가 나타납니다.

3. "자세히", "파일에 복사"를 차례로 클릭합니다.

   인증서 내보내기 마법사가 나타납니다.

4. 다음 지시를 따라 마법사를 완료합니다.

   - **내보내기 파일 형식** - Base-64 로 인코딩된 X.509(.CER)를 선택합니다.
   - **내보낼 파일** - 내보낸 인증서 파일의 전체 경로 이름을 정의합니다.

     예: C:\certificates\computer.base64.cer

   성공적으로 내보냈음을 알리는 메시지가 표시됩니다.

5. 인증서를 키 저장소로 가져옵니다. 예:

   ```
   C:\jdk1.5.0\jre\lib\security>c:\jdk1.5.0\bin\keytool.exe -import -file
   computer.base64.cer -keystore
   C:\jboss-4.2.3.GA\server\default\deploy\IdentityMinder.ear\custom\ppm\truststore\ssl.keystore
   ```

6. 키 저장소 암호를 입력합니다. 기본 암호는 'secret'입니다.
7. "예"를 클릭하여 인증서를 트러스트합니다.

   인증서가 키 저장소에 추가됩니다.

CA User Activity Reporting Module 에 대한 연결 구성

CA Access Control 엔터프라이즈 관리는 CA ControlMinder 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.

CA User Activity Reporting Module 에 대한 연결을 구성하려면

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

   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

인증 기관 서명된 SSL 인증서

CA User Activity Reporting Module 에 대한 연결이 인증 기관이 서명한 SSL 인증서를 사용할지 여부를 지정합니다.

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 공유 계정 관리 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 3 장: ObserveIT Enterprise 와 통합

이 섹션은 다음 항목을 포함하고 있습니다.

안내서 정보

이 장에서는 CA Access Control 과 ObserveIT Enterprise 세션 기록 프로그램을 통합하는 방법에 대해 설명합니다. 이 장에서는 공유 계정 관리 세션을 기록하기 위해 수행하는 프로세스 및 절차에 대해 설명합니다.

이 장은 CA ControlMinder 을 관리하며 ObserveIT Enterprise 세션 기록 기능을 사용하려는 보안 및 시스템 관리자를 위해 제공됩니다.

용어를 간단히 나타내기 위해 이 안내서에서는 제품을 CA ControlMinder 이라고 합니다.

ObserveIT 통합 정보

CA ControlMinder 과 ObserveIT Enterprise 를 통합하면 권한 있는 계정을 사용하여 조직 내 서버에 액세스하려는 시도를 폭넓게 제어할 수 있습니다. ObserveIT Enterprise 세션 로깅 소프트웨어는 대상 시스템에서 사용자의 활동을 기록합니다. 사용자가 권한 있는 계정 암호를 체크 아웃하고 끝점에 로그인하면 기록이 시작되어 세션이 종료(예: 사용자가 권한 있는 암호를 체크 인할 때)되면 기록이 종료됩니다.

기록된 세션은 준비한 전용 데이터베이스에 저장됩니다. ObserveIT 뷰어를 사용하여 CA Access Control 엔터프라이즈 관리에서 직접 기록된 세션을 재생할 수 있습니다.

다음 링크의 ObserveIT Systems 에서 ObserveIT Enterprise 세션 로깅 프로그램을 얻을 수 있습니다.

http://www.observeit-sys.com/download.asp

다음 링크에서 ObserveIT Enterprise 설명서를 찾을 수 있습니다:

https://support.ca.com/cadocs/

참고: ObserveIT 에 대한 자세한 내용은 ObserveIT Enterprise 설치 미디어에 있는 ObserveIT 설명서를 참조하십시오.

통합을 설정하는 방법

CA ControlMinder 을 ObserveIT Enterprise 세션 기록 소프트웨어와 통합하기 위해 수행해야 하는 몇 가지 단계가 있습니다. 통합의 마지막에 모든 공유 계정 관리 세션은 ObserveIT Enterprise 소프트웨어에 의해 기록됩니다.

참고: 1-5 단계를 완료하는 방법에 대한 자세한 내용은 ObserveIT 설치 미디어에 있는 ObserveIT Enterprise 설명서를 참조하십시오.

통합을 설정하려면 다음을 수행하십시오.

1. ObserveIT Enterprise 시스템 및 설치 요구 사항을 검토합니다.

   사용하는 서버가 ObserveIT Enterprise 를 설치하기 위한 최소 시스템 요구 사항을 충족하는지 확인합니다.

2. 중앙 데이터베이스를 준비합니다.

   기록된 세션은 전용 Microsoft SQL Server 에 저장됩니다.

3. Internet Information Server(IIS)를 구성합니다.

   ObserveIT Enterprise 응용 프로그램 서버는 IIS 를 사용하여 에이전트가 보내는 메타데이터를 처리합니다.

4. ObserveIT Enterprise 서버 구성 요소를 설치합니다.

   ObserveIT 응용 프로그램 서버, 에이전트, 관리 콘솔도 또한 설치됩니다.

5. ObserveIT Enterprise 응용 프로그램 서버를 구성합니다.

   기록 설정을 구성합니다.

6. 엔터프라이즈 관리 서버에서 세션 기록 스크립트를 배포합니다.

   이 스크립트는 세션 기록을 트리거하는 공유 계정 관리 자동 로그인을 활성화합니다.

7. 서비스 계정을 만듭니다.

   사용할 엔터프라이즈 관리 서버에 대한 서비스 계정을 만듭니다.

8. CA Access Control 엔터프라이즈 관리에서 ObserveIT Enterprise 응용 프로그램 서버에 대한 연결을 정의합니다.

   세션 로깅을 사용하도록 연결 설정을 구성합니다.

통합을 준비하는 방법

ObserveIT Enterprise 응용 프로그램 서버의 설치를 완료한 이후에 CA ControlMinder 과의 통합을 위해 서버를 준비합니다. ObserveIT Enterprise 응용 프로그램 서버를 준비하면 서버가 공유 계정 관리 세션의 기록 및 저장을 시작하도록 구성됩니다.

이 통합을 준비하려면 다음을 수행하십시오.

1. 관리 콘솔을 엽니다.
2. 서비스 계정을 만듭니다.

   CA ControlMinder 은 서비스 계정을 사용하여 ObserveIT Enterprise 응용 프로그램 서버에 연결합니다.

관리 콘솔을 엽니다.

ObserveIT Enterprise 를 설치 및 시작하면 웹 기반 관리 콘솔을 시작할 수 있습니다.

관리 콘솔을 열려면

1. 브라우저를 사용하여 ObserveIT Enterprise 관리 콘솔을 엽니다. 다음 URL 을 입력합니다.

   http://observeit_server_name:port/ObserveIT

   예:

   http://observeit_server:4884/ObserveIT

2. 설치 시 지정한 administrator 자격 증명을 사용하여 로그인합니다.

   ObserveIT Enterprise 관리 콘솔이 열립니다.

참고: "시작", "프로그램", "ObserveIT", "ObserveIT WebConsole"을 클릭하여 ObserveIT Enterprise 관리 콘솔을 열 수도 있습니다.

서비스 계정 만들기

CA Access Control 엔터프라이즈 관리는 ObserveIT Enterprise 응용 프로그램 서버가 사용자 활동을 기록하도록 인증하기 위해 서비스 계정을 사용합니다. CA Access Control 엔터프라이즈 관리에서 ObserveIT Enterprise 응용 프로그램 서버 연결 설정을 구성할 때 서비스 계정 자격 증명을 제공합니다.

서비스 계정을 만들려면

1. ObserveIT Enterprise 관리 콘솔에서 "Configuration"(구성), "Console Users"(콘솔 사용자)를 선택합니다.

   콘솔 사용자 화면이 열립니다.

2. "Create User"(사용자 만들기)를 선택합니다.

   콘솔 사용자 창이 열립니다.

3. 사용자 이름, 암호를 입력하고 암호를 확인합니다.
4. 인증 방법을 ObserveIT.Authentication 으로 설정하고 사용자 역할을 "Admin"으로 설정합니다.
5. "추가"를 클릭합니다.

   서비스 계정이 만들어졌습니다.

참고: 사용자 관리에 대한 자세한 내용은 ObserveIT Enterprise 설치 미디어에 있는 *ObserveIT 설명서*를 참조하십시오.

세션 기록 스크립트 배포

사용자 세션 기록은 공유 계정 관리 자동 로그인과 결합하여 동작합니다. 사용자가 권한 있는 계정 암호를 체크 아웃하고 끝점에 로그인하도록 선택한 경우, 원격 관리 소프트웨어가 열려 자동으로 사용자를 로그인시킵니다. CA Access Control 엔터프라이즈 관리는 끝점 유형을 기반으로 세션 기록 스크립트를 사용하여 원격 관리 프로그램을 제어합니다.

예를 들어, 사용자가 Windows 끝점에 로그인하도록 선택하면 CA Access Control 엔터프라이즈 관리는 끝점에 연결하기 위한 원격 데스크톱 소프트웨어를 엽니다.

ObserveIT Enterprise 응용 프로그램 서버에서 세션을 기록하기 위해 엔터프라이즈 관리 서버에서 세션 기록 스크립트를 배포합니다.

세션 기록 스크립트를 배포하려면

1. CA Support 웹 사이트에서 세션 기록 스크립트를 다운로드하여 임시 디렉터리에 저장합니다.
2. 엔터프라이즈 관리 서버에서 다음 디렉터리로 이동합니다. 여기서 *JBoss_HOME* 은 JBoss 가 설치된 디렉터리를 지정합니다.

   JBoss_HOME/server/default/deploy/IdentityMinder.ear/config/sso_scripts
3. 세션 기록 스크립트를 sso_scripts 디렉터리에 복사합니다.

   덮어쓰기 전에 디렉터리에 있는 파일을 백업하는 것이 좋습니다.
4. 기존 파일을 새 파일로 덮어쓰도록 선택합니다.

이제 연결 설정을 ObserveIT Enterprise 응용 프로그램 서버로 구성할 수 있습니다.

ObserveIT 에 대한 연결 정의

ObserveIT Enterprise 와의 통합을 완료하기 위해 CA Access Control 엔터프라이즈 관리에서 ObserveIT Enterprise 응용 프로그램 서버에 대한 연결 설정을 구성합니다.

ObserveIT 에 대한 연결을 정의하려면

1. CA Access Control 엔터프라이즈 관리에서 "시스템", "연결 관리", "세션 기록", "연결 만들기"를 선택합니다.

   "연결 만들기" 화면이 나타납니다.
2. 다음 세부 정보를 입력합니다.

   연결 설명

   연결의 일반 텍스트 설명을 정의합니다.

   재생 URL

   ObserveIT Enterprise 응용 프로그램 서버 URL 정의

   예:http://observeit_host:4884/observeit/

   사용자 ID

   서비스 계정 사용자 이름 정의

   암호

   서비스 계정 암호 정의

고급

다음 고급 연결 설정을 지정합니다.

뷰어 페이지

세션이 기록되었음을 나타내는 메시지를 화면 맨 위에 표시할지 여부를 지정합니다.

뷰어 매개 변수

ObserveIt 뷰어 창 너비 및 높이를 지정합니다.

ActiveX URL

ObserveIT Enterprise ActiveX 파일이 있는 위치에 대한 전체 경로 이름을 지정합니다. 기본적으로 ObserveIT 응용 프로그램 서버에 대한 URL을 지정합니다.

예:
http://observeit_host:4884/ObserveIT/AgentInstall/Agent.cab#version=1,0,0,0

서버 URL

ObserveIT Enterprise 응용 프로그램 서버가 기록된 세션을 저장하는 위치의 전체 경로 이름을 지정합니다. 기본적으로 ObserveIT 응용 프로그램 서버에 대한 URL을 지정합니다.

예: http://observeit_host:4884/ObserveITApplicationServer

3. "제출"을 클릭합니다.

CA Access Control 엔터프라이즈 관리가 연결을 생성합니다.

세션이 로깅되는 방법

각 공유 계정 관리 세션은 기록되어 ObserveIT Enterprise 데이터베이스에 저장됩니다. 각 세션은 전체 기록된 세션에서 개별적으로 응답할 수 있는 개별 슬라이드로 구분됩니다.

다음 프로세스는 공유 계정 관리 세션이 로깅되는 방법을 설명합니다.

1. 사용자가 CA Access Control 엔터프라이즈 관리에서 권한 있는 계정 암호를 체크 아웃하고 끝점에 자동으로 로깅하도록 선택합니다.

   이 옵션을 처음 사용하는 경우 ActiveX 의 설치가 요구됩니다.

2. 원격 관리 세션이 열리고 사용자가 암호를 입력할 필요 없이 로그인됩니다.
3. 끝점에 설치된 ObserveIT 에이전트가 사용자 작업의 기록을 시작하고 슬라이드를 ObserveIT Enterprise 응용 프로그램 서버로 보내면 이 서버가 데이터를 데이터베이스에 저장합니다.
4. 사용자가 원격 관리 세션을 닫고 ObserveIT 에이전트가 기록을 중지합니다.
5. CA Access Control 엔터프라이즈 관리에 기록된 세션이 표시됩니다.

중요! Internet Explorer 가 ActiveX 를 다운로드하도록 활성화하려면 "로컬 인트라넷 영역" 또는 "신뢰할 수 있는 영역"에서 ObserveIT Enterprise 호스트 이름을 지정하고 "서명된 ActiveX 컨트롤 다운로드" 보안 옵션을 "사용"으로 설정하십시오.

참고: 세션 기록에 대한 자세한 내용은 ObserveIT Enterprise 설치 미디어에 있는 *ObserveIT 설명서*를 참조하십시오.

세션이 로깅되는 장소

ObserveIT Enterprise 응용 프로그램 서버는 공유 계정 관리 세션을 전용 Microsoft SQL Server 에 로깅합니다. ObserveIT 데이터베이스 서버는 두 개의 전용 데이터베이스를 사용합니다. 첫 번째 데이터베이스의 이름은 ObserveIT 이며, 구성 및 메타데이터를 수록하고 있습니다. 두 번째 데이터베이스의 이름은 ObserveIT_Data 이며, 기록된 세션 중 ObserveIT 에이전트가 수집하는 스크린 샷을 저장합니다.

참고: 세션 로깅에 대한 자세한 내용은 ObserveIT Enterprise 설치 미디어에 있는 *ObserveIT 설명서*를 참조하십시오.

세션 재생

CA Access Control 엔터프라이즈 관리에서 기록된 공유 계정 관리 세션을 재생합니다. 세션을 재생하도록 선택하면 CA Access Control 엔터프라이즈 관리가 새 창에서 기록된 세션을 재생합니다. 플레이어 창에는 세션을 탐색하는 데 사용하는 컨트롤 단추가 포함되어 있습니다. 기록된 세션 내에서 일반 텍스트 검색을 수행할 수도 있습니다.

참고: 일반 텍스트 검색에 대한 자세한 내용은 ObserveIT Enterprise 설치 미디어에 있는 *ObserveIT 설명서*를 참조하십시오.

세션을 재생하려면

1. CA Access Control 엔터프라이즈 관리에서 "권한 있는 계정", "감사" 하위 작업을 선택합니다.

   사용 가능한 작업의 목록에 "권한 있는 계정 감사" 작업이 나타납니다.

2. "권한 있는 계정 감사"를 선택합니다.

   "권한 있는 계정 감사" 검색 창이 열립니다.

   참고: 자신에게 공유 계정 관리 감사 관리자 역할이 할당되어 있는지 확인하십시오.

3. 검색 조건을 지정하고, 표시할 행 수를 입력한 다음 "검색"을 클릭합니다.

   검색 조건에 맞는 작업이 표시됩니다.

4. 세션 정보 열에서 재생 아이콘을 클릭하여 세션을 재생합니다.

   플레이어 창이 열리고 세션의 처음부터 세션이 재생됩니다.

   참고: 세션을 탐색하려면 창의 맨 아래에 있는 컨트롤을 사용하십시오.

제 4 장: RSA SecurID 와 통합

이 섹션은 다음 항목을 포함하고 있습니다.

CA Access Control 엔터프라이즈 관리를 RSA SecurID 와 통합하는 방법

회사에서 RSA SecurID 를 사용하여 사용자를 인증하는 경우 RSA SecurID 의 기능을 사용하여 CA Access Control 엔터프라이즈 관리에 로그인하는 사용자를 인증할 수 있습니다. 엔터프라이즈 관리 서버를 RSA SecurID 와 통합하면 CA Access Control 엔터프라이즈 관리는 로그인 시 사용자를 인증하지 않습니다. CA Access Control 엔터프라이즈 관리는 타사 프로그램을 통해 사용자 인증이 수행되는지 감지합니다.

다음 프로세스는 CA Access Control 엔터프라이즈 관리와 RSA SecurID 를 통합하는 방법을 설명합니다.

1. 엔터프라이즈 관리 서버를 준비합니다.
2. 지원되는 웹 서버를 설치합니다.
   - Windows - ARR(Application Request Routing) 모듈을 사용하는 Internet Information Server 7.0
   - Linux - 프록시 모듈을 사용하는 Apache 2.2.6 웹 서버

3. 웹 서버를 리버스 프록시 서버로 구성합니다 (페이지 51).

   웹 서버는 모든 로그인 인증 요청에 대해 리버스 프록시 서버로서 동작합니다.

4. 웹 서버로부터의 액세스를 제외하고, CA Access Control 엔터프라이즈 관리에 대한 모든 네트워크 액세스를 차단하도록 RSA SecurID 를 구성합니다.

   RSA SecurID 는 사용자가 CA Access Control 엔터프라이즈 관리를 직접 액세스하는 것을 방지합니다.

5. 엔터프라이즈 관리 서버 구성 요소를 설치합니다.

6. CA Access Control 엔터프라이즈 관리에 로그인할 각 RSA SecurID 사용자에 대해 CA Access Control 엔터프라이즈 관리에서 사용자 계정을 정의합니다.

   CA Access Control 엔터프라이즈 관리에 대한 액세스를 부여할 사용자만 정의하십시오.

   중요! Active Directory 를 사용하는 경우 이 단계를 수행할 필요가 없습니다.

7. 다음 서버에 RSA 인증 에이전트를 설치합니다.

   - (Linux) 엔터프라이즈 관리 서버
   - 웹 서버

   RSA 인증 에이전트는 사용자 요청을 가로채서 RSA 인증 관리자로 전달합니다.

8. CA Access Control 엔터프라이즈 관리에 대해 SSO(Single Sign On)을 사용하도록 RSA 웹 에이전트를 구성합니다.

9. 전용 호스트에 RSA 인증 관리자를 설치합니다.

   RSA 인증 관리자가 사용자 액세스 요청을 인증합니다.

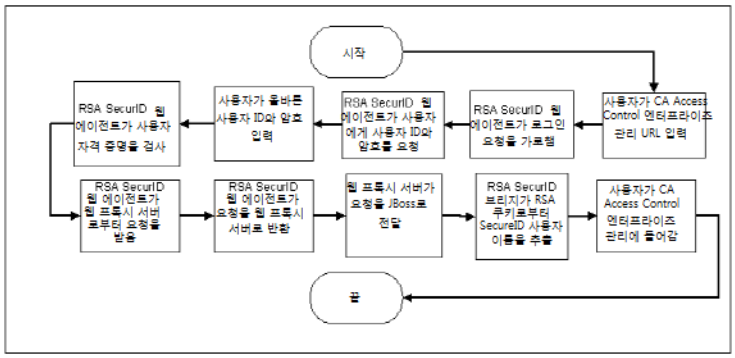
사용자가 CA Access Control 엔터프라이즈 관리에 로그인을 시도할 때마다 RSA SecurID 는 사용자에게 CA Access Control 엔터프라이즈 관리 사용자 계정 정보 대신 올바른 RSA SecurID 자격 증명을 묻습니다. 인증되면 RSA SecurID 는 CA Access Control 엔터프라이즈 관리에 사용자를 로그인시킵니다.

참고: RSA SecurID 웹 에이전트 및 인증 관리자에 대한 자세한 내용은 RSA SecurID 웹 사이트를 참조하십시오.

RSA SecurID 가 사용자 로그인을 인증하는 방법

엔터프라이즈 관리 서버와 RSA SecurID 를 통합하면 사용자가 CA Access Control 엔터프라이즈 관리에 로그인할 때마다 RSA SecurID 는 로그인 요청을 인증합니다. RSA SecurID 가 사용자 로그인의 유효성을 확인하는 경우 사용자는 자동으로 CA Access Control 엔터프라이즈 관리에 대한 액세스 권한을 얻습니다.

다음 다이어그램은 RSA SecurID 가 CA Access Control 엔터프라이즈 관리에 대한 사용자 로그인을 인증하는 방법을 설명합니다.



웹 서버를 리버스 프록시 서버로 구성

사용자가 CA Access Control 엔터프라이즈 관리에 로그인을 시도하면 RSA SecurID 는 이 요청을 가로채고 사용자에게 올바른 SecurID 사용자 이름 및 암호를 묻습니다. 설치한 웹 서버는 엔터프라이즈 관리 서버에 있는 RSA 인증 웹 에이전트에서 로그인 요청을 받아 RSA 인증 관리자로 전달하는 리버스 프록시 서버의 역할을 합니다.

*리버스 프록시*는 다른 서버에 대한 게이트웨이로서, 한 웹 서버가 다른 웹 서버의 콘텐츠를 제공할 수 있게 해줍니다.

예: Windows Server 2008 에서 Internet Information Services 7.0 을 리버스 프록시 서버로 구성

이 예에서, 시스템 관리자인 Steve 는 엔터프라이즈 관리 서버와 Internet Information Services(IIS) 7.0 을 ARR(Application Request Routing) 모듈이 설치된 Windows Server 2008 에 설치했습니다. ARR 모듈은 IIS 가 프록시 서버로 동작할 수 있도록 해 줍니다.

1. Steve 는 Internet Information Services 서버에서 IIS 프록시 설정을 활성화합니다.
   a. "시작", "관리 도구", "IIS(인터넷 정보 서비스) 관리자"를 선택합니다.

      "IIS(인터넷 정보 서비스) 관리자" 콘솔이 열립니다.
   b. 왼쪽 창에서 호스트를 선택하여 작업 창을 확장한 다음 ARR 캐시 아이콘을 선택합니다.

      ARR 캐시 관리 콘솔이 열립니다.
   c. 작업 창에서 "서버 프록시 설정"을 선택합니다.
   d. "프록시 사용" 확인란을 선택하고 "적용"을 클릭합니다.

      Steve 는 IIS 프록시 설정을 활성화했습니다.

2. Steve 는 요청을 엔터프라이즈 관리 서버로 전달하도록 IIS 를 구성합니다.
   a. "사이트" 메뉴를 확장하고 기본 웹 사이트를 선택합니다.
   b. URL 다시쓰기 아이콘을 강조 표시하고 "작업" 메뉴에서 "기능 열기"를 선택합니다.

      URL 다시쓰기 구성 콘솔이 열립니다.
   c. "작업" 메뉴에서 "규칙 추가"를 선택합니다.

      "규칙 추가" 창이 열립니다.
   d. "인바운드 규칙" 아래에서 "빈 규칙"을 선택하고 "확인"을 클릭합니다.

      "인바운드 규칙 편집" 구성 창이 열립니다.
   e. 규칙 이름을 지정하고 "패턴" 메뉴에서 (iam.+)를 선택합니다.
   f. "작업" 섹션으로 스크롤한 다음 작업 유형 메뉴에서 "다시쓰기"를 선택합니다.
   g. 다음 형식으로 "URL 다시쓰기" 필드에 CA Access Control 엔터프라이즈 관리 URL 을 입력합니다.

      ```
      http://enterprise_host:8080/{R:0}
      ```
   h. "적용"을 클릭하여 규칙을 만듭니다.

      새 인바운드 규칙이 만들어졌습니다.
   i. "패턴" 메뉴에서 (castyles.+)를 사용하여 c - h 단계를 반복합니다.

      Steve 는 요청을 엔터프라이즈 관리 서버로 전달하도록 IIS 를 구성했습니다.
3. Steve 는 웹 서버의 보안을 유지하기 위해 RSA SecurID 를 구성합니다.
   a. Internet Information Services(IIS) 관리자 콘솔에서 "기본 웹 사이트"를 선택하고 RSA SecurID 아이콘을 두 번 클릭합니다.

      RSA SecurID 설정 창이 열립니다.
   b. 다음 확인란을 선택합니다.
      - 이 서버에서 RSA SecurID 웹 액세스 인증 기능 사용
      - 이 리소스 보호
   c. "작업" 메뉴에서 적용을 선택합니다.

4. Steve 는 CA Access Control 엔터프라이즈 관리에 대해 SSO(Single Sign On)을 사용하도록 RSA 웹 에이전트를 구성합니다.

   a. regedit 유틸리티를 열고 다음 위치로 이동합니다.

      HKEY_LOCAL_MACHINE\SOFTWARE\SDTI\RSAWebAgent

   b. RSAUSERCustomHeader 란 이름으로 DWORD 유형의 레지스트리 키를 만듭니다.

   c. 레지스트리 키 값을 1 로 설정합니다.

   Steve 는 Internet Information Services 를 리버스 프록시 서버로 설정했습니다.

예: Red Hat Enterprise Linux 5.0 에서 리버스 프록시 서버로 Apache Web Server 2.2.6 구성

이 예에서 시스템 관리자인 Steve 는 Red Hat Enterprise Linux 5.0 에 엔터프라이즈 관리 서버를 설치했습니다. Steve 는 이제 리버스 프록시 서버로서 Apache Web Server 2.2.6 을 설치 및 구성해야 합니다.

1. Steve 는 프록시 모듈을 사용하는 Apache Web Server 2.2.6 을 설치 및 구성하기 위해 다음을 수행합니다.

   a. 다음과 같이 프록시 모듈을 설치하기 위해 Apache Web Server 2.2.6 설치를 구성합니다.

   ```
   tar -zxvf httpd_2.2.6.tar.gz
   ./configure --prefix=/usr/local/apache --enable-proxy --enable-proxy-http
   make
   make install
   ```

   Apache Web Server 2.2.6 이 프록시 모듈과 함께 설치됩니다.

2. Steve 는 리버스 프록시를 구성하기 위해 다음을 수행합니다.

   a. Apache Web Server 의 conf 디렉터리로 이동합니다.

   b. 편집을 위해 httpd.conf 파일을 엽니다.

   c. 항목의 LoadModule 목록을 찾아 다음 섹션을 추가합니다.

   ```
   # Used for proxy to the Enterprise Management Server
   ProxyPass       /iam http://196.168.1.1:8080/iam
   ProxyPass       /castylesr5.1.1 http://192.168.1.1:8080/castylesr5.1.1
   ProxyPassReverse/iam http://192.168.1.1:8080/iam
   ```

   d. 파일을 저장하고 닫습니다.

   e. Apache Web Server 를 다시 시작합니다.

   Steve 는 리버스 서버로 동작하도록 Apache Web Server 2.2.6 을 구성했습니다.

3. Steve 는 쿠키 검사를 위한 웹 브라우저 IP 주소를 무시하도록 RSA 웹 에이전트를 구성합니다.

   a. RSA 웹 에이전트 설치 디렉터리로 이동합니다.

      ```
      /usr/local/apache/rsawebagent/
      ```

   b. RSA 웹 에이전트 구성 유틸리티를 실행합니다.

   c. 목록에서 현재 사용 중인 RSA 서버를 선택합니다.

   d. 두 번째 구성 화면으로 이동합니다.

   e. 쿠키 검사를 위한 브라우저 IP 주소 무시가 활성화되어 있는지 확인합니다.

   Steve 는 쿠키 검사를 위한 웹 브라우저 IP 주소를 무시하도록 RSA 웹 에이전트를 구성했습니다.

4. Steve 는 CA Access Control 엔터프라이즈 관리에 대해 SSO(Single Sign On)을 사용하도록 RSA 웹 에이전트를 구성합니다.

   a. Linux 웹 에이전트 배포를 열고 다음 파일을 찾습니다.

      ```
      rsacookieapi.tar
      ```

   b. 이 파일을 임시 디렉터리에 복사한 다음 파일의 콘텐츠를 추출합니다.

   c. 다음 파일을 찾습니다.

      - RSACookieAPI.jar
      - librsacookieapi.so

   d. librsacookieapi.so 파일을 다음 위치에 복사합니다. 여기서 *JBOSS_HOME* 은 Steve 가 Jboss 를 설치한 위치를 나타냅니다.

      ```
      JBOSS_HOME/server/default/deploy/IderntityMinder.ear/library
      ```

   e. RSACookieAPI.jar 파일을 다음 위치로 복사합니다.

      ```
      JBOSS_HOME/server/default/deploy/IderntityMinder.ear/user_console.war/WEB
      -INF/lib/
      ```

   Steve 는 CA Access Control 엔터프라이즈 관리에 대한 SSO 를 활성화하도록 RSA 웹 에이전트를 구성했습니다.

제 5 장: 다중 LDAP 서버를 사용하여 작업

이 섹션은 다음 항목을 포함하고 있습니다.

소개

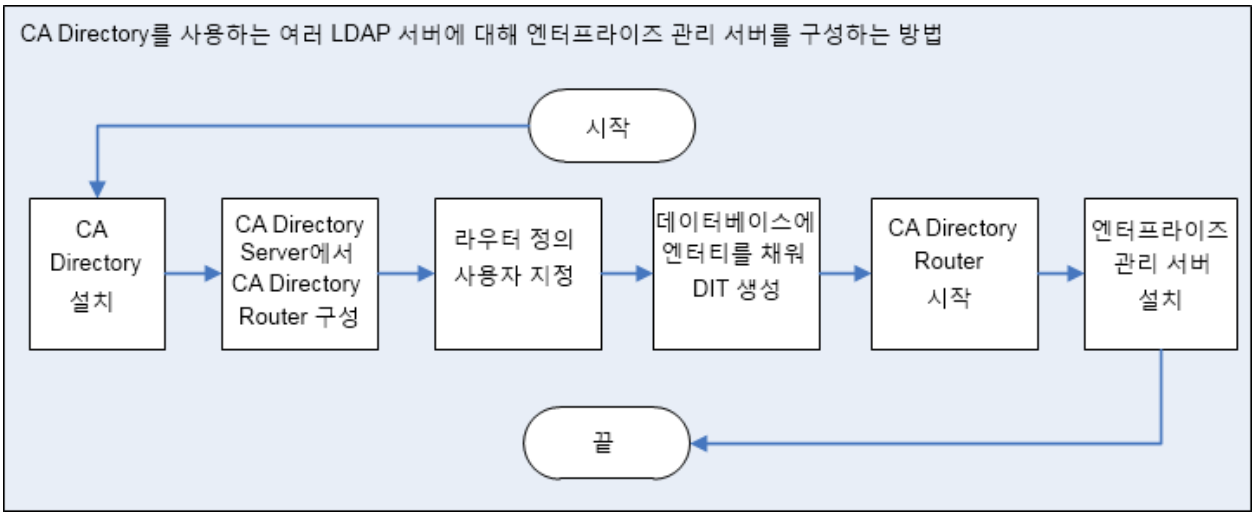
이 장의 정보는 시스템 또는 데이터베이스 관리자가 CA 디렉터리를 사용하는 여러 LDAP 서버로 CA Access Control 엔터프라이즈 관리를 구성하는 방법에 대해 설명합니다. 여러 LDAP 서버를 사용하여 작업하면 관리자가 여러 LDAP 사용자 저장소를 하나의 기업 전체 사용자 저장소로 통합할 수 있습니다.

여러 LDAP 서버를 구성하는 방법

CA 디렉터리는 LDAP 서버를 분산된 디렉터리 백본으로 통합하는 것을 지원합니다.

CA 디렉터리는 여러 LDAP 디렉터리 서버에서 검색할 수 있게 하는 DXlink 란 이름의 유틸리티를 제공합니다.

다음 다이어그램은 CA 디렉터리를 사용하는 여러 LDAP 서버에 대해 CA Access Control 엔터프라이즈 관리를 구성하는 방법을 보여 줍니다.



다음 단계를 수행하여 CA 디렉터리를 사용하는 여러 LDAP 서버에 대해 엔터프라이즈 관리 서버를 구성합니다.

1. CA 디렉터리를 설치합니다.
2. CA 디렉터리 라우터를 구성합니다. (페이지 60)
3. CA 디렉터리 라우터 정의를 사용자 지정합니다. (페이지 63)
4. 데이터베이스에 엔터티를 채워 DIT 를 만듭니다. (페이지 66)
5. CA 디렉터리를 시작합니다.
6. Active Directory 를 사용자 저장소로 사용하여 엔터프라이즈 관리 서버를 설치합니다.

   중요! 엔터프라이즈 관리 서버를 설치할 때 다음을 지정하십시오.

   - 호스트 이름 - CA 디렉터리 호스트 이름
   - 포트 번호 - 25389
   - 기본 DN - 환경에서 모든 Active Directory 서버에 공통적인 DN 을 지정합니다. 해당되지 않는 경우 이 필드는 비워두십시오.
   - (Linux) 검색 루트 - 환경에서 모든 Active Directory 서버에 공통적인 DN 을 지정합니다. 해당되지 않는 경우 이 필드는 비워두십시오.
   - 관리 계정 - Active Directory 도메인 중 하나에서 온 관리 계정입니다.

참고: CA Access Control 엔터프라이즈 관리에 로그인할 때는 사용하는 관리 계정이 구성원으로 등록된 도메인 이름을 지정해야 합니다.

CA 디렉터리 라우터 구성

CA 디렉터리는 클라이언트 요청에 정의된 접미사에 일치하는 Active Directory 에 대한 요청을 CA ControlMinder 에서 사용되는 Active Directory 로 라우트합니다. CA 디렉터리는 DXlink 유틸리티를 사용하여 요청을 라우트합니다.

이 절차를 완료하기 전에 두 개의 Active Directory 사용자 저장소(예: acdir1 및 acdir2)와 명명된 dsarouter 인 CA 디렉터리를 설치했습니다.

다음 단계를 수행하십시오.

1. CA 디렉터리 서버에서 "명령 프롬프트" 창을 엽니다.
2. 다음 명령을 실행합니다.

   ```
   dxnewdsa -s 1 cadirhost-adrouter 25389
   ```

   -s *1*

   데이터베이스 크기를 1MB 로 지정합니다.

   cadirhost -adrouter

   라우터의 이름을 정의합니다.

   25389

   라우터 포트를 지정합니다.
3. 다음 명령을 사용하여 라우터를 중지합니다.

   ```
   dxserver stop cadirhost-adrouter
   ```
4. 다음 명령을 사용하여 라우터를 설치합니다.

   ```
   dxserver install cadirhost-adrouter
   ```

5. 다음 디렉터리로 이동합니다. 여기서 *DXHOME* 은 라우터를 설치한 디렉터리의 이름입니다.

   DXHOME/config/knowledge

6. 다음과 같이 cadirhost-router.dxc 파일을 복사합니다.
   a. 한 파일의 이름을 acdir1-dxlink.dxc 로 변경합니다.
   b. 두 번째 파일의 이름을 acdir2-dxlink.dxc 로 변경합니다.
   c. acdir1-dxlink.dxc 파일을 다음과 같이 편집합니다.

```
set dsa "acdir1-dxlink" =
{
    prefix            = <dc "acdir1"><dc "com">
    dsa-name          = <cn "acdir1-dxlink">
    dsa-password      = "secret"
    ldap-dsa-name     = <dc "acdir1"><dc "com"><cn "users"><cn
"Administrator">
    ldap-dsa-password = "{CADIR}yKW2cVbG"
    address           = tcp "acdir1" port 389
    auth-levels       = clear-password
    trust-flags       = allow-check-password, no-server-credentials
    link-flags        = dsp-ldap, ms-ad
};
```

ldap-dsa-name

Active Directory에 바인딩하는 데 사용하는 DN(Distinguished Named)을 지정합니다.

ldap-dsa-password

DN의 암호화된 암호를 정의합니다..

참고: dxpassword 유틸리티를 사용하여 암호를 암호화하십시오. 예: dxpassword -P CADIR <*password*>.

address

Active Directory 도메인 컨트롤러 주소를 지정합니다.

d. acdir2-dxlink.dxc 를 다음과 같이 편집합니다.

```
set dsa "aclabcail-dxlink" =
{
    prefix            = <dc "acdir2"><dc "com">
    dsa-name          = <cn "acdir2-dxlink">
    dsa-password      = "secret"
    ldap-dsa-name   =<dc "acl"><dc "aclab"><cn "users"><cn "Administrator">
    ldap-dsa-password = "{CADIR}yKW2cVbG"
    address           = tcp "acdir2" port 389
    auth-levels       = clear-password
    trust-flags       = allow-check-password, no-server-credentials
    link-flags        = dsp-ldap, ms-ad
};
```

CA 디렉터리 라우터를 구성했습니다.

CA 디렉터리 라우터 정의 사용자 지정

CA 디렉터리 라우터를 구성한 이후에는 CA 디렉터리 라우터 정의를 사용자 지정해야 합니다.

다음 단계를 수행하십시오.

1. 다음 디렉터리로 이동합니다. 여기서 *DXHOME* 은 CA 디렉터리를 설치한 디렉터리를 나타냅니다.

   DXHOME/config/limits

2. 다음 작업을 수행하십시오.

   a. default.dxc 파일의 사본을 만들고 원본 파일의 이름을 dsarouter-adrouter.dxc 로 변경합니다.

   b. 파일에서 ReadOnly 플래그를 제거합니다.

   c. dsarouter-adrouter.dxc 파일을 열고 아래와 같이 다음 필드를 수정합니다.

   ```
   # size limits
   set max-users = 255;
   set max-local-ops = 100;
   set max-op-size = 0;

   # time limits
   set max-bind-time = none;
   set bind-idle-time = 3600;
   set max-op-time = 600;
   ```

   파일을 저장한 후 닫습니다.

3. 다음 디렉터리로 이동합니다.

   DXHOME/config/settings

4. 다음 작업을 수행하십시오.

   a. default.dxc 파일의 사본을 만들고 원본 파일의 이름을 dsarouter-adrouter.dxc 로 변경합니다.

   b. 파일에서 ReadOnly 플래그를 제거합니다.

   c. dsarouter-adrouter.dxc 파일을 열고 아래와 같이 다음 필드를 수정합니다.

   ```
   # directory information base
   set alias-integrity = true;
   # distribution controls
   set multi-casting = true;
   set always-chain-down = false;
   ```

```
# security controls
set min-auth = clear-password;
set allow-binds = true;
set ssl-auth-bypass-entry-check = false;
# general controls
set op-attrs = true;
set transparent-routing = true;
```

파일을 저장한 후 닫습니다.

5. 다음 디렉터리로 이동합니다.

   ```
   DXHOME/config/knowledge
   ```

6. dsarouter-adrouter.dxc 파일을 열거나 만들고 auth-levels 문자열 값 "anonymous"를 제거하여 명확한 암호 로그인만 허용합니다. 예:

   ```
   set dsa "cadirhost-adrouter" =
   {
   prefix        = <>
   dsa-name      = <cn "cadirhost-adrouter">
   dsa-password  = "secret"
   address       = tcp "cadirhost" port 25389
   disp-psap     = DISP
   snmp-port     = 25389
   console-port  = 25390
    auth-levels   = clear-password
   ```

   파일을 저장한 후 닫습니다.

   중요! IPv4 및 IPv6 주소가 모두 정의된 서버에 CA 디렉터리를 설치한 경우 tcp 값에 IPv4 및 IPv6 주소 유형을 지정하십시오. 예: address = tcp "fe80::20d:56ff:fed4:8300%5" port 19389, tcp "192.168.1.1" port 19389

7. adrouter.dxa 란 이름의 파일을 만들고 다음 줄을 추가한 다음 파일을 저장하고 닫습니다.

   ```
   source "dsarouter-adrouter.dxc";
   source "acdir1-dxlink.dxc";
   source "acdir2-dxlink.dxc";
   ```

8. 다음 디렉터리로 이동합니다.

   ```
   DXHOME/config/logging
   ```

9. 다음 작업을 수행하십시오.
   a. default.dxc 파일의 사본을 만듭니다.
   b. 원본 파일의 이름을 dsarouter-adrouter.dxc 로 변경합니다.
   c. ReadOnly 태그를 제거합니다.
10. 다음 디렉터리로 이동합니다.

    ```
    DXHOME/config/servers
    ```

11. 다음 작업을 수행하십시오.
    a. *cadirhost*-adrouter.dxi 를 편집하고 아래와 같이 다음 줄을 편집한 다음 파일을 저장하고 닫습니다.

    ```
    #
    # Initialization file written by DXnewdsa
    #
    # logging and tracing
    source "../logging/cadirhost-adrouter.dxc";
    # schema
    clear schema;
    source "../schema/default.dxg";
    # knowledge
    clear dsas;
    source "../knowledge/adrouter.dxg";
    # operational settings
    source "../settings/cadirhost-adrouter.dxc";
    # service limits
    source "../limits/cadirhost-adrouter.dxc";
    # access controls
    clear access;
    source "../access/default.dxc";
    # ssl
    source "../ssld/default.dxc";
    # replication agreements (rarely used)
    # source "../replication/";
    # multiwrite DISP recovery
    set multi-write-disp-recovery = false;
    # grid configuration
    set dxgrid-db-location = "data";
    set dxgrid-db-size = 1;
    set cache-index = all-attributes;
    set lookup-cache = true;
    ```

참고: *cadirhost* 를 CA 디렉터리 호스트 이름으로 대체하십시오.

CA 디렉터리 라우터 정의를 사용자 지정했습니다.

CA 디렉터리 데이터베이스를 채워 DIT 만들기

디렉터리 정보 트리(DIT)를 만들기 위해 CA 디렉터리 데이터베이스를 엔터티로 채우도록 선택할 수 있습니다. DIT 는 하향식(톱다운)으로 조직 계층 구조를 탐색할 수 있게 해 줍니다.

다음 단계를 수행하십시오.

1. CA 디렉터리 라우터를 호스팅하는 서버에서 input.ldif 란 이름의 파일을 만들고 아래와 같이 다음 엔터티를 추가합니다.

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

dn: dc=company,dc=com
objectClass: domain
objectClass: top
dc: company

dn: dc=demo
objectClass: domain
objectClass: top
dc: demo
```

2. 파일을 저장한 후 닫습니다.
3. "명령 프롬프트" 창을 열고 다음 명령을 실행합니다.

```
dxloaddb cadirhost-adrouter input.ldif
```

4. 다음 명령을 실행하여 CA 디렉터리 라우터를 시작합니다.

```
dxserver start cadirhost-adrouter
```

참고: *cadirhost* 를 CA 디렉터리 호스트 이름으로 대체하십시오.

DIT 를 만들기 위해 CA 디렉터리 데이터베이스에 엔터티를 채웠습니다.

제 6 장: CA SiteMinder 와 통합

이 섹션은 다음 항목을 포함하고 있습니다.

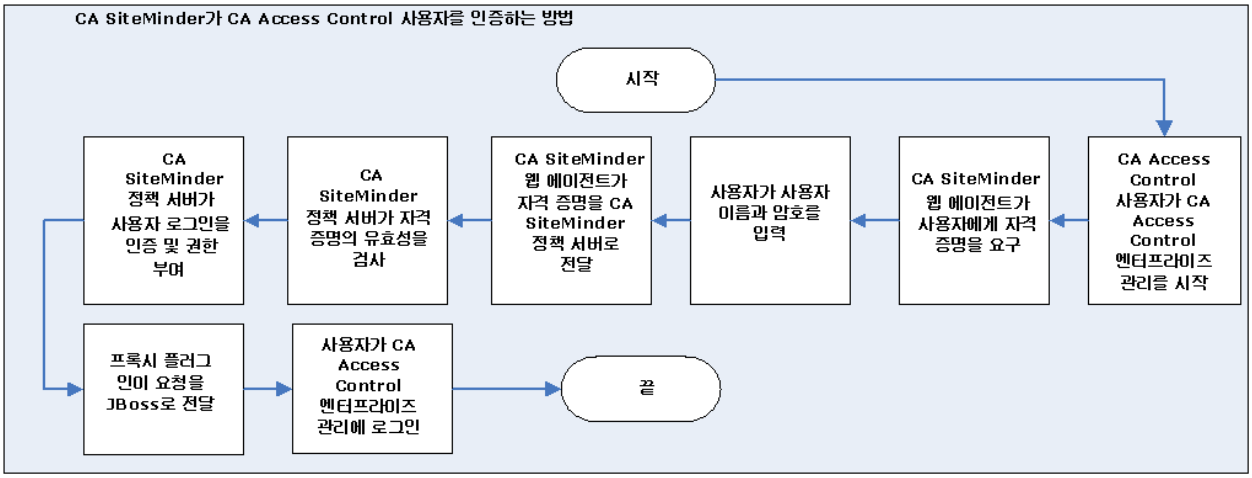
소개

이 장의 정보는 시스템, 네트워크, 보안 관리자가 CA SiteMinder 를 사용하여 CA Access Control 엔터프라이즈 관리의 보안을 유지하는 방법에 대해 설명합니다. CA SiteMinder 는 CA SiteMinder 디렉터리의 사용자를 인증할 수 있으며 CA ControlMinder 사용자만 CA Access Control 엔터프라이즈 관리에 로그인할 수 있도록 허용합니다. CA SiteMinder 를 사용하여 CA Access Control 엔터프라이즈 관리의 보안을 유지하면 관리자가 CA SiteMinder 고급 사용자 인증 방식을 사용할 수 있습니다.

CA SiteMinder 가 CA ControlMinder 사용자를 인증하는 방법

CA SiteMinder 를 사용하여 CA Access Control 엔터프라이즈 관리의 보안을 유지하는 경우, 사용자가 CA Access Control 엔터프라이즈 관리에 로그인할 때마다 CA SiteMinder 가 이 로그인 요청을 인증합니다. CA SiteMinder 가 로그인 요청을 인증하면 사용자가 CA Access Control 엔터프라이즈 관리에 대한 액세스 권한을 얻습니다.

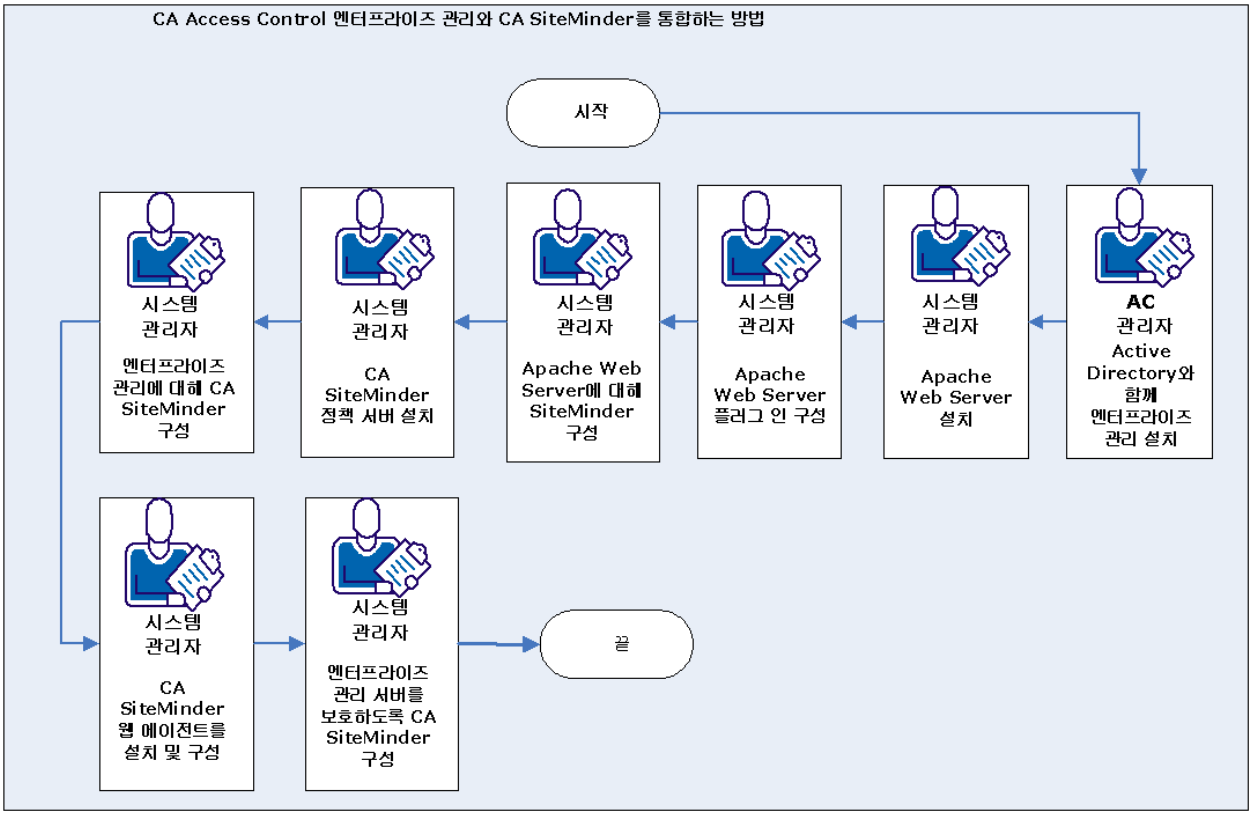
다음 다이어그램은 CA SiteMinder 가 CA Access Control 엔터프라이즈 관리에 대한 CA ControlMinder 사용자 로그인을 인증 및 권한 부여하는 방법을 보여 줍니다.



CA SiteMinder 와 통합하는 방법

CA Access Control 엔터프라이즈 관리와 CA SiteMinder 를 통합하면 CA SiteMinder 고급 사용자 인증 및 권한 부여 기능을 이용할 수 있습니다.

다음 다이어그램은 시스템 또는 보안 관리자가 CA Access Control 엔터프라이즈 관리와 CA SiteMinder 를 통합하는 방법을 보여 줍니다.



다음 프로세스는 CA SiteMinder 와 통합하는 방법을 설명합니다.

1. 엔터프라이즈 관리 서버를 설치합니다.

   모든 웹 기반 응용 프로그램, 배포 서버, DMS, CA ControlMinder 이 설치되었습니다.

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

2. 엔터프라이즈 관리 서버에서 Apache Web Server 를 구성합니다. (페이지 71)
3. CA SiteMinder 정책 서버를 설치합니다.
4. 엔터프라이즈 관리 서버에 대해 CA SiteMinder 를 구성합니다. (페이지 75)
5. CA SiteMinder 웹 에이전트를 구성합니다. (페이지 76)
6. 엔터프라이즈 관리 서버의 보안을 유지하도록 CA SiteMinder 를 구성합니다. (페이지 77)
7. CA SiteMinder 를 사용하여 사용자를 인증하도록 엔터프라이즈 관리 서버를 구성합니다. (페이지 80)

참고: CA SiteMinder 정책 서버, 웹 에이전트, Administrative UI 에 대한 자세한 내용은 CA SiteMinder 설명서를 참조하십시오.

예: 엔터프라이즈 관리 서버에서 Apahce 웹 서버 프록시 플러그 인 구성

이 예에서는 Windows 2008 Server 에 엔터프라이즈 관리 서버를 설치했습니다. 또한 SSL 지원이 활성화된 엔터프라이즈 관리 서버에 Apache Web Server 버전 2.2.19 를 설치해야 합니다. 이제 Apache Web Server 프록시 플러그 인을 구성합니다. 다음 작업을 수행하십시오.

1. 엔터프라이즈 관리 서버에서 JBoss Application Server 를 중지합니다.
2. 다음 디렉터리로 이동합니다.

   APACHE_HOME/conf

   APACHE_HOME

   Apache Web Server 가 설치된 디렉터리
3. httpd.conf 파일을 편집하여 프록시 모듈을 활성화하고 다음과 같은 프록시 구성을 편집합니다.
   a. 다음 줄의 주석 처리를 제거합니다.

      ```
      LoadModule proxy_module modules/mod_proxy.so
      LoadModule proxy_http_module modules/mod_proxy_http.so
      ```

   b. Global 구성 섹션의 끝에 다음 줄을 추가합니다.

      ```
      Include conf/extra/httpd-proxy-entm.conf
      ```
4. 다음 디렉터리로 이동합니다.

   APACHE_HOME/conf/extra
5. httpd-proxy-entm.conf 란 이름을 파일을 만들고 다음 내용을 추가한 다음 파일을 저장하고 닫습니다.

   ```
   # Proxy to CA AC ENTM
   <IfModule proxy_module>
     <IfModule proxy_http_module>
           # /iam section BEGIN
       <Proxy /iam>
         Order allow,deny
         Allow from all
       </Proxy>
       ProxyPass /iam http://acentmnode.example.com:8080/iam
       ProxyPassReverse /iam http://acentmnode.example.com:8080/iam
       ProxyPass /iam/ http://acentm.examplenode.com:8080/iam/
       ProxyPassReverse /iam/ http://acentmnode.example.com:8080/iam/

           # /iam section END
   ```

```
        # /castylesr5.1.1 section BEGIN
    <Proxy /castylesr5.1.1>
      Order allow,deny
      Allow from all
    </Proxy>
    ProxyPass /castylesr5.1.1
http://acentmnode.example.com:8080/castylesr5.1.1
    ProxyPassReverse /castylesr5.1.1
http://acentmnode.example.com:8080/castylesr5.1.1
    ProxyPass /castylesr5.1.1/
http://acentmnode.example.com:8080/castylesr5.1.1/
    ProxyPassReverse /castylesr5.1.1/
http://acentmnode.example.com:8080/castylesr5.1.1/
        # /castylesr5.1.1 section END
  </IfModule>
</IfModule>
```

참고: *acentmnode.example.com:port* 는 엔터프라이즈 관리 서버를 설치한 서버의 실제 호스트 이름과 포트로 대체하십시오.

6. Apache Web Server 를 다시 시작합니다.
7. JBoss Application Server 를 다시 시작합니다.
8. 엔터프라이즈 관리 서버를 탐색하여 Apache Web Server 가 요청을 성공적으로 전달하는지 확인합니다. 다음 URL 을 사용합니다.

   ```
   http://enterprise_host:port/iam/ac
   ```

엔터프라이즈 관리 서버에서 Apache Web Server 프록시 플러그 인을 구성했습니다.

예: Apache Web Server 에 대해 CA SiteMinder 구성

이 예에서는 엔터프라이즈 관리 서버에서 Apache Web Server 프록시 플러그인을 구성한 이후에 이제 Apache Web Server 에 대해 CA SiteMinder 를 구성합니다.

1. CA SiteMinder 관리자 인터페이스를 사용하여 다음을 수행합니다.
   a. "시작", "모든 프로그램", "CA", "CA SiteMinder", "CA SiteMinder Administrative UI"로 이동합니다..

      CA SiteMinder Administrative User Interface 가 열리고 사용자 이름과 암호를 입력하도록 요구합니다.

   b. CA SiteMinder Administrative UI 에 로그인합니다.
   c. "인프라", "호스트", "호스트 구성", "호스트 구성 만들기", "호스트 구성 유형의 개체 사본 만들기"를 선택합니다.
   d. DefaultHostSettings 개체를 선택하고 "확인"을 클릭합니다.
   e. 다음 필드를 완료하십시오.
      - **이름** - webservernode-HCO
      - **설명** - 웹 서버 호스트 구성
   f. "구성 값" 프레임으로 이동하여 "추가"를 클릭하고 다음과 같이 CA SiteMinder 정책 서버의 호스트 이름을 입력합니다.

      ```
      호스트: policyserver.company.com
      ```

   g. "제출"을 클릭합니다.

   호스트 구성 개체를 구성했습니다.
2. "인프라", "에이전트", "에이전트", "에이전트 만들기", "에이전트 유형의 새 개체 만들기"를 선택합니다.
3. 다음 필드를 완성하고 "제출"을 클릭합니다.
   - **이름** - webserver-agent
   - **설명** - 웹 서버 노드 웹 에이전트
   - **에이전트 유형 선택** - SiteMinder
   - **에이전트 유형** - 웹 에이전트
   - **4.x 에이전트 지원** - clear

   웹 에이전트 개체를 구성했습니다.

4. "에이전트 구성", "에이전트 구성 만들기", "에이전트 구성 유형의 개체 사본 만들기"를 선택합니다.
5. ApacheDefaultSettings 를 선택한 다음 "확인"을 클릭하고 다음을 수행합니다.
   a. 다음 필드를 완료합니다.
      - **Name** - webservernode-ACO
   b. 매개 변수 목록에서 #DefaultAgentName 필드를 편집하고 이름 값에서 # 문자를 제거합니다.
   c. 다음과 같이 에이전트 이름을 설정합니다.
      - **DefaultAgentName** - webserver-agent
   d. #LogoffUri 를 편집하고 이름 값에서 # 문자를 제거합니다.
   e. 값을 다음과 같이 설정합니다.
      - **LogoffUri** - /iam/logout.jsp

   참고: 에이전트 매개 변수에 대한 자세한 내용은 *CA SiteMinder Agent Configuration Guide*(에이전트 구성 안내서)를 참조하십시오.
6. "제출"을 클릭합니다.

   에이전트 구성 개체를 만들었습니다.

예: 엔터프라이즈 관리 서버에 대해 CA SiteMinder 구성

이 예에서는 엔터프라이즈 관리 서버에 대해 CA SiteMinder 를 구성합니다.

1. CA SiteMinder 관리자 인터페이스를 사용하여 다음을 완성하십시오.
2. "시작", "모든 프로그램", "CA", "CA SiteMinder", "CA SiteMinder Administrative UI"로 이동합니다..

   CA SiteMinder Administrative UI 가 열리고 사용자 이름과 암호의 입력을 요구합니다.
3. CA SiteMinder Administrative UI 에 로그인합니다.
4. "인프라", "호스트", "호스트 구성", "호스트 구성 만들기", "호스트 구성 유형의 개체 사본 만들기"를 선택합니다.
5. DefaultHostSettings 개체를 선택하고 "확인"을 클릭합니다.
6. 다음 필드를 완료하십시오.
   - **이름** - *acentmnode*-HCO
   - **설명** - ENTM 호스트 구성
7. "구성 값" 프레임으로 이동하여 "추가"를 클릭하고 다음과 같이 CA SiteMinder 정책 서버의 호스트 이름을 입력합니다.

   호스트: policyserver.company.com
8. "제출"을 클릭합니다.

에이전트 개체를 구성했습니다. 다음으로, CA SiteMinder 웹 에이전트를 설치 및 구성합니다.

예: CA SiteMinder 웹 에이전트 구성

이 예에서 시스템 관리자인 Steve 는 엔터프라이즈 관리 서버에 CA SiteMinder 웹 에이전트를 설치했습니다. Steve 는 이제 앞에서 정의한 호스트 및 에이전트 개체 구성을 사용하여 Apache Web Server 에 대한 웹 에이전트를 구성합니다.

1. 다음 작업을 수행하십시오.
   a. 다음 디렉터리로 이동합니다. 여기서 *APACHE_HOME* 은 Apache Web Server 를 설치한 디렉터리를 나타냅니다.

      ```
      APACHE_HOME/conf
      ```

   b. 다음과 같이 WebAgent.conf 파일을 편집하여 웹 에이전트를 활성화합니다.

      ```
      4$EnableWebAgent="Yes"
      ```

   c. 파일을 저장한 후 닫습니다.
2. Apache Web Server 를 다시 시작합니다.

   CA SiteMinder 웹 에이전트를 구성했습니다.

예: 엔터프라이즈 관리 서버의 보안을 유지하도록 CA SiteMinder 구성

이 예에서는 엔터프라이즈 관리 서버 로그인 세션의 보안을 유지하도록 CA SiteMinder 를 구성합니다. CA SiteMinder 가 인증 체계 및 도메인 정책의 보안을 유지하는 사용자 저장소를 구성해야 합니다.

1. 다음 작업을 수행하십시오.
   a. "시작", "모든 프로그램", CA, CA SiteMinder, CA SiteMinder Administrative UI 로 이동합니다.

      CA SiteMinder Administrative UI 가 열리고 Steve 에게 사용자 이름과 암호의 입력을 요구합니다.

   b. CA SiteMinder 관리자 사용자 계정의 자격 증명을 입력합니다.

   c. "인프라", "디렉터리", "사용자 디렉터리", "사용자 디렉터리 만들기"를 선택합니다.

   d. "일반" 프레임에서 다음 필드를 완성합니다.
      - **이름** - ac-dir
      - **설명** - Access Control 사용자 저장소

   e. "디렉터리 설정" 프레임으로 이동하여 다음 필드를 완성합니다.
      - **네임스페이스** - LDAP
      - **서버** - *directory_hostname:port*

   f. "관리자 자격 증명"으로 이동하여 다음 필드를 완성합니다.
      - **자격 증명 요구** - 선택
      - **사용자 이름** - 사용자 전체 DN 바인드
      - **암호** - *password*
      - **암호 확인** - *password*

   g. "LDAP 설정" 프레임으로 이동하여 다음 필드를 완성합니다.
      - **루트** - *searchroot*
      - **범위** - Sub-Tree
      - **시작** - (&(sAMAccountName=
      - **끝**
        -)(objectclass=top)(objectclass=person)(objectclass=organizationalperson)(objectclass=user))

   h. "사용자 특성" 프레임으로 이동하여 다음 필드를 완성합니다.

- **유니버설 ID** - %USER_ID%에 해당하는 특성 이름

2. "제출"을 클릭합니다.

   CA SiteMinder 가 사용자 디렉터리 개체를 만듭니다.

3. "사용자 디렉터리 보기", ac-dir, "내용 보기"를 선택합니다.

   사용자 저장소 항목이 표시됩니다.

4. "인프라", "인증", "인증 체계", "인증 체계 만들기"를 선택하고 다음 필드를 완성합니다.
   - **이름** - ac-basic-auth
   - **설명 -** CA Access Control 엔터프라이즈 관리 기본 인증
   - **인증 체계 유형** - 기본 템플릿
   - **보호 수준** - 5
   - **라이브러리** - smauthdir
5. "제출"을 클릭합니다.

   CA SiteMinder 가 인증 체계 개체를 만듭니다.

6. "정책", "도메인", "도메인", "도메인 만들기"를 선택합니다.
7. 도메인의 이름을 지정합니다.
8. 사용자 디렉터리 프레임으로 이동한 다음 "추가/제거"를 클릭합니다.
9. ac-dir 를 "사용 가능한 구성원" 목록에서 "선택한 구성원" 목록으로 이동한 다음 "확인"을 클릭합니다.
10. "영역", "영역 만들기"를 선택하고 다음 필드를 완성합니다.
    - **이름** - ac-realm
    - **에이전트** - *webserver*-agent
    - **리소스 필터** - /iam/
    - **기본 리소스 보호** - 보호됨
    - **인증 체계** - ac-basic-auth

11. "규칙" 프레임으로 이동한 다음 "작성"을 선택하고 다음 필드를 완성합니다.
    - **이름** - ac-rule
    - **리소스** - *
    - **액세스 허용** - 선택
    - **웹 에이전트 액션** - Get, Post
12. "확인"을 두 번 클릭합니다.
13. "정책", "작성"을 선택하고 "일반" 탭에서 다음 필드를 완성합니다.
    - **이름** - ac-policy
14. "사용자" 탭으로 이동하여 "모두 추가"를 선택합니다.
15. "규칙" 탭으로 이동하여 "규칙 추가"를 클릭하고 ac-rule 을 선택한 다음 "확인"을 클릭합니다.
16. "확인", "제출"을 클릭하여 도메인을 만듭니다.

도메인 및 영역 정책을 구성했습니다.

예: CA SiteMinder 를 사용하여 사용자를 인증하도록 엔터프라이즈 관리 서버 구성

이 예에서는 CA SiteMinder 통합을 위해 엔터프라이즈 관리 서버를 구성합니다.

1. 엔터프라이즈 관리 서버 호스트에서 다음을 수행합니다.
   a. JBoss Application Server 를 중지합니다.
   b. 다음 디렉터리로 이동합니다. 여기서 *JBOSS_HOME* 은 JBoss 를 설치한 디렉터리를 나타냅니다.

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

   c. web.xml 파일을 열고 FrameworkAuthFilter 섹션을 찾습니다.
   d. 값을 false 로 수정한 다음 파일을 저장하고 닫습니다. 예:

```
<filter>
  <filter-name>FrameworkAuthFilter</filter-name>

<filter-class>com.netegrity.webapp.authentication.FrameworkLoginFilter</filter-class>
  <init-param>
    <param-name>Enable</param-name>
    <param-value>false</param-value>
  </init-param>
</filter>
```

2. 다음 디렉터리로 이동합니다.

   JBOSS_HOME/server/default/deploy/IdentityMinder.ear/policyserver.rar/META-INF

3. 다음 작업을 수행하십시오.
   a. 다음과 같이 ra.xml 파일을 열고 값을 true 로 설정하여 연결을 활성화합니다.

```
<config-property>
 <config-property-name>Enabled</config-property-name>
 <config-property-type>java.lang.String</config-property-type>
 <config-property-value>true</config-property-value>
</config-property>
```

b. 다음과 같이 CA SiteMinder 정책 서버 구성에 따라 FIPS 모드를 구성합니다.

```
<config-property>
  <config-property-name>FIPSMode</config-property-name>
  <config-property-type>java.lang.String</config-property-type>
  <config-property-value>false</config-property-value>
</config-property>
```

c. 다음과 같이 CA SiteMinder 정책 서버 호스트 이름, IP 주소, 포트 번호를 정의합니다.

```
<config-property>
  <config-property-name>ConnectionURL</config-property-name>
  <config-property-type>java.lang.String</config-property-type>

<config-property-value>policyservernode.example.com,44441,44442,44443</co
nfig-property-value>
</config-property>
```

d. 다음과 같이 관리 사용자 계정 설정을 정의합니다.

```
<config-property>
  <config-property-name>UserName</config-property-name>
  <config-property-type>java.lang.String</config-property-type>
  <config-property-value>siteminder</config-property-value>
</config-property
```

e. 다음 디렉터리에 있는 암호 도구를 실행합니다.

```
/CA/AccessControlServer/IAMSuite/AccessControl/tools/PasswordTool
```

예:

```
pwdTools -FIPS -p <clear_text_password> -k
JBoss_HOME/server/default/deploy/IdentityMinder.ear/config/com/netegrity/
config/keys/FIPSKey.dat
```

f. 다음과 같이 AdminSecret 를 다음 암호화 명령의 출력으로 정의합니다.

```
<config-property>
  <config-property-name>AdminSecret</config-property-name>
  <config-property-type>java.lang.String</config-property-type>

<config-property-value>{AES}:gSez2/BhDGzEKWvFmzca4w==</config-property-va
lue>
</config-property>
```

g. AgentName 을 CA Access Control 엔터프라이즈 관리 노드 에이전트 이름으로 정의합니다.

```
config-property>
  <config-property-name>AgentName</config-property-name>
  <config-property-type>java.lang.String</config-property-type>
  <config-property-value>webserver-agent</config-property-value>
</config-property>
```

h. 다음 암호 도구 명령을 사용하여 CA Access Control 엔터프라이즈 관리 공유 암호를 암호화합니다.

ACServerInstallDir/IAMSuite/AccessControl/tools/Passwordtool/pwdtools.bat -FIPS -p *<your_shared_secret>* -k *JBoss_HOME*/server/default/deploy/IdentityMinder.ear/config/com/netegrity/config/keys/FIPSKey.dat

i. AgentSecret 을 다음 명령의 암호화된 출력으로 정의합니다.

```
<config-property>
  <config-property-name>AgentSecret</config-property-name>
  <config-property-type>java.lang.String</config-property-type>

<config-property-value>{AES}:gSez2/BhDGzEKWvFmzca4w==</config-property-value>
</config-property>
```

4. 파일을 저장한 후 닫습니다.
5. 다음 디렉터리로 이동합니다.

   JBoss_HOME/bin

6. run_idm.bat 를 편집하여 %PATH% 변수를 JBoss 설치 경로로 설정합니다. 예:

```
set
PATH=%PATH%;C:\jboss-4.2.3\server\default\deploy\IdentityMinder.ear\library;%SystemRoot%\SYSTEM32;%SystemRoot%;%SystemRoot%\SYSTEM32\WBEM
```

7. 파일을 저장한 후 닫습니다.
8. JBoss Application Server 를 시작합니다.

   CA SiteMinder 통합을 위해 엔터프라이즈 관리 서버를 구성했습니다. 이제 CA Access Control 엔터프라이즈 관리 URL 을 탐색하고 CA SiteMinder 가 로그인 세션의 보안을 유지하는지 확인할 수 있습니다.

제 7 장: CA ControlMinder REST API

이 섹션은 다음 항목을 포함하고 있습니다.

REST-based API

REST(Representational State Transfer)는 URL 에서 액세스 가능한 개체의 상태를 만들고 수정하기 위해 하이퍼미디어의 내재 속성에 의존하는 소프트웨어의 아키텍처 스타일 특성을 기술합니다.

REST 시나리오에서 문서(개체의 상태를 나타냄)는 클라이언트와 서비스 모두 단일 요청 또는 응답 내용 이외에는 어떠한 엔터티에 대해서도 아는 것이 없다고 가정 하에 이 둘 사이에서 주고받기됩니다.

REST 기반 API 에 대한 스키마를 얻으려면 다음 URL 을 탐색하여 빈 페이지에서 소스를 열어 보십시오.

`https://hostname:18443/iam/api/1.0/restapi/schemas`

참고: 스키마에 대한 자세한 내용은 이 섹션의 설명을 참조하십시오.

REST 요청을 사용하여 엔터프라이즈 관리 서버 사용자 인터페이스를 바이패스하고 공유 계정 관리 데이터베이스를 사용하여 사용자 지정 또는 타사 프로그램 간에 통신할 수 있습니다.

HTTP 동사

가능한 경우 CA ControlMinder REST API 는 각 작업에 대해 다음과 같은 적절한 HTTP 동사를 사용합니다.

GET

계정, 끝점, 계정 요청을 가져오는 데 사용됩니다.

POST

계정, 끝점, 계정 요청을 만드는 데 사용됩니다.

PUT

계정, 끝점, 계정 요청을 업데이트하는 데 사용됩니다.

DELETE

계정, 끝점, 계정 요청을 삭제하는 데 사용됩니다.

예: HTTP 작업

다음은 지원되는 REST 기반 API 명령의 스키마 예제입니다.

- HTTP POST:

```
POST /iam/api/1.0/restapi/environments/ac/endpoints/endpointname/accounts
HTTP/1.1
Content-type: application/xml; charset=UTF-8
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Cache-Control: no-cache
Pragma: no-cache
Host: 10.112.196.244
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
Content-Length: 79
```

다음 예는 계정을 생성하는 HTTP POST 본문 콘텐츠입니다.

```
<Account>
<Name>myaccount_name</Name>
<Disconnected>true</Disconnected>
<Type>Shared</Type>
<Container>MS SQL Logins</Container>
<PasswordPolicy>default password policy</PasswordPolicy>
<PasswordState>CheckedIn</PasswordState>
<Exclusive>false</Exclusive>
<ChangePasswordOnCheckOut>false</ChangePasswordOnCheckOut>
<ChangePasswordOnCheckIn>false</ChangePasswordOnCheckIn>
<LoginApplicationCheckoutOnly>false</LoginApplicationCheckoutOnly>
<Owner ownerType="Group">my_group</Owner>
</Account>
```

- HTTP GET:

```
GET /iam/api/1.0/restapi/environments/ac/endpoints/endpointname HTTP/1.1
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Host: 10.112.196.169:9998
```

- HTTP PUT:

```
PUT /iam/api/1.0/restapi/environments/ac/endpoints/endpointname/accounts
HTTP/1.1
Content-type: application/xml; charset=UTF-8
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Cache-Control: no-cache
Pragma: no-cache
Host: 10.112.196.244
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
Content-Length: 959
```

다음 예는 계정을 업데이트하는 HTTP PUT 본문 콘텐츠입니다.

```
<Account>
<Name>myaccount_name</Name>
<Disconnected>true</Disconnected>
<Type>Shared</Type>
<Container>MS SQL Logins</Container>
<PasswordPolicy>default password policy</PasswordPolicy>
<PasswordState>CheckedIn</PasswordState>
<Exclusive>false</Exclusive>
<ChangePasswordOnCheckOut>false</ChangePasswordOnCheckOut>
<ChangePasswordOnCheckIn>false</ChangePasswordOnCheckIn>
<LoginApplicationCheckoutOnly>false</LoginApplicationCheckoutOnly>
<Owner ownerType="Group">my_group</Owner>
</Account>
```

- HTTP DELETE:

```
DELETE /iam/api/1.0/restapi/environments/ac/endpoints/endpointname HTTP/1.1
Content-type: application/xml; charset=UTF-8
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Cache-Control: no-cache
Pragma: no-cache
Host: 10.112.196.244
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
```

REST-based 인증

CA ControlMinder REST 요청은 요청 정보의 일부로서 인증 정보를 포함합니다. CA ControlMinder 는 HTTP 기본 인증 방법을 지원합니다. 예를 들어, 다음과 같은 기본 인증을 사용할 수 있습니다.

```
Authorization: Basic
c3VwZXJhZG1pbjpkZWZhdWx0c3VwZXJhZG1pbjpkZWZhdWx0
```

앞의 예제는 사용자 “superadmin” 및 암호 “default”의 Base 64 인코딩을 나타냅니다.

스키마 가져오기

계정 요청 스키마를 가져오려면 다음 URL 로 HTTP GET 요청을 보내십시오.

`https://<host_name>:18443/iam/api/1.0/restapi/schemas`

host_name

호스트 이름을 지정합니다.

계정 만들기

계정을 만들려면 다음 URL 로 HTTP POST 요청을 보내십시오.

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts
```

host_name

호스트 이름을 지정합니다.

endpoint_name

호스트 이름을 지정합니다.

다음 예는 계정을 만드는 HTTP 본문 콘텐츠를 보여 줍니다.

```
<Account>

<Name>myaccount_name</Name>

<Disconnected>true</Disconnected>

<Type>Shared</Type>

<Container>MS SQL Logins</Container>

<PasswordPolicy>default password policy</PasswordPolicy>

<PasswordState>CheckedIn</PasswordState>

<Exclusive>false</Exclusive>

<ChangePasswordOnCheckOut>false</ChangePasswordOnCheckOut>

<ChangePasswordOnCheckIn>false</ChangePasswordOnCheckIn>

<LoginApplicationCheckoutOnly>false</LoginApplicationCheckoutOnly>

<Owner ownerType="Group">my_group</Owner>

</Account>
```

Name

계정 이름을 지정합니다.

Disconnected

계정의 연결이 해제되었는지 여부를 지정합니다.

Type

계정 유형을 지정합니다.

Container

컨테이너를 지정합니다.

PasswordPolicy

계정에 대해 구현된 암호 정책을 지정합니다.

PasswordState

계정의 암호 상태를 지정합니다.

Exclusive

계정이 배타적인지 여부를 지정합니다.

ChangePasswordOnCheckOut

계정이 체크 아웃될 때 암호가 변경되는지 여부를 지정합니다.

ChangePasswordOnCheckIn

계정이 체크 인될 때 암호가 변경되는지 여부를 지정합니다.

LoginApplicationCheckoutOnly

로그인 응용 프로그램이 계정을 체크 아웃하는지 여부를 지정합니다.

Owner

소유자 유형을 지정합니다.

계정 업데이트

계정을 업데이트하려면 다음 URL 로 HTTP PUT 요청을 보내십시오.

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts/<account_name>
```

host_name

호스트 이름을 지정합니다.

endpoint_name

호스트 이름을 지정합니다.

account_name

계정 이름을 지정합니다.

다음 예는 계정을 업데이트하는 HTTP 본문 콘텐츠를 보여 줍니다.

```
<Account>
<Name>myaccount_name</Name>
<Disconnected>true</Disconnected>
<Type>Shared</Type>
<Container>MS SQL Logins</Container>
<PasswordPolicy>default password policy</PasswordPolicy>
<PasswordState>CheckedIn</PasswordState>
<Exclusive>false</Exclusive>
<ChangePasswordOnCheckOut>false</ChangePasswordOnCheckOut>
<ChangePasswordOnCheckIn>false</ChangePasswordOnCheckIn>
<LoginApplicationCheckoutOnly>false</LoginApplicationCheckoutOnly>
<Owner ownerType="Group">my_group</Owner>
</Account>
```

Name

계정 이름을 지정합니다.

Disconnected

계정의 연결이 해제되었는지 여부를 지정합니다.

Type

계정 유형을 지정합니다.

Container

컨테이너를 지정합니다.

PasswordPolicy

계정에 대해 구현된 암호 정책을 지정합니다.

PasswordState

계정의 암호 상태를 지정합니다.

Exclusive

계정이 배타적인지 여부를 지정합니다.

ChangePasswordOnCheckOut

계정이 체크 아웃될 때 암호가 변경되는지 여부를 지정합니다.

ChangePasswordOnCheckIn

계정이 체크 인될 때 암호가 변경되는지 여부를 지정합니다.

LoginApplicationCheckoutOnly

로그인 응용 프로그램이 계정을 체크 아웃하는지 여부를 지정합니다.

Owner

소유자 유형을 지정합니다.

계정 삭제

계정을 삭제하려면 다음 URL 로 HTTP DELETE 요청을 보내십시오.

`https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts/<account_name>`

host_name

호스트 이름을 지정합니다.

endpoint_name

호스트 이름을 지정합니다.

account_name

계정 이름을 지정합니다.

계정 가져오기

특정 계정을 가져오려면 GET 명령을 사용하십시오.

참고: 계정이 체크 아웃된 경우 암호를 볼 수 있습니다.

특정 계정을 가져오려면 다음 URL 로 HTTP GET 요청을 보내십시오.

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts/<account_name>
```

계정을 가져오는 동안 지원 끝점에 대한 컨테이너를 지정하려면 계정-컨테이너 쿼리 매개 변수를 사용하십시오.

Active Directory 와 같은 비기본 계정-컨테이너를 갖는 계정을 가져오려면 다음 URL 로 HTTP GET 요청을 보내십시오.

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts/<account_name>
```

host_name

호스트 이름을 지정합니다.

endpoint_name

호스트 이름을 지정합니다.

account_name

계정 이름을 지정합니다.

계정 가져오기

끝점에서 권한 있는 계정을 가져오려면 다음 URL 로 HTTP GET 요청을 보내십시오.

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts
```

host_name

호스트 이름을 지정합니다.

endpoint_name

호스트 이름을 지정합니다.

계정 체크 인

계정을 체크 인하려면 다음 URL 로 HTTP PUT 요청을 보내십시오.

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts/<account_name>
```

host_name

호스트 이름을 지정합니다.

endpoint_name

호스트 이름을 지정합니다.

account_name

계정 이름을 지정합니다.

다음 예는 계정을 체크 인하는 HTTP 본문 콘텐츠를 보여 줍니다.

```
<Account>

<PasswordState>Checked In</PasswordState>

</Account>
```

계정 체크 아웃

계정을 체크 아웃하려면 다음 URL 로 HTTP PUT 요청을 보내십시오.

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts/<account_name>
```

host_name

호스트 이름을 지정합니다.

endpoint_name

호스트 이름을 지정합니다.

account_name

계정 이름을 지정합니다.

다음 예는 계정을 체크 아웃하는 HTTP 본문 콘텐츠를 보여 줍니다.

```
<Account>

<PasswordState>Checked Out</PasswordState>

</Account>
```

계정 Break Glass

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

계정을 Break Glass 하려면 다음 URL 로 HTTP 요청을 보내십시오.

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts/<account_name>?breakglass-accounts=true
```

host_name

호스트 이름을 지정합니다.

endpoint_name

호스트 이름을 지정합니다.

account_name

계정 이름을 지정합니다.

다음 예는 계정을 Break Glass 하는 HTTP 본문 콘텐츠를 보여 줍니다.

```
<Account>

<PasswordState justification="my
justification">BreakGlass</PasswordState>

</Account>
```

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

암호 다시 설정

암호를 수동으로 다시 설정하려면 다음 URL 로 HTTP PUT 요청을 보내십시오.

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts/<account_name>
```

host_name

호스트 이름을 지정합니다.

endpoint_name

호스트 이름을 지정합니다.

account_name

계정 이름을 지정합니다.

다음 예는 암호를 다시 설정하는 HTTP 본문 콘텐츠를 보여 줍니다.

```
<Account>

<Password auto="false">password</Password>

</Account>
```

암호를 자동으로 다시 설정

계정의 암호를 자동으로 다시 설정하려면 다음 URL 로 HTTP PUT 요청을 보내십시오.

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts/<account_name>
```

host_name

호스트 이름을 지정합니다.

endpoint_name

호스트 이름을 지정합니다.

account_name

계정 이름을 지정합니다.

다음 예는 암호를 자동으로 다시 설정하는 HTTP 본문 콘텐츠를 보여 줍니다.

```
<Account>

<Password auto="true"/>

</Account>
```

끝점 만들기

끝점을 만들려면 다음 URL 로 HTTP POST 요청을 보내십시오.

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints
```

host_name

호스트 이름을 지정합니다.

다음 예는 끝점을 만드는 HTTP 본문 콘텐츠를 보여 줍니다.

```
<Endpoint>
   <Name>endpoint_name</Name>
   <EndpointType>MS SQL Server</EndpointType>
   <EndpointTypeProperties>
      <UserLogin>user1</UserLogin>
      <URL>URL Value</URL>
      <Host>Endpoint_Host_Address</Host>
      <Password>User_Password</Password>
   </EndpointTypeProperties>
   <AdministrativeAdvanced>false</AdministrativeAdvanced>

</Endpoint>
```

Name

호스트 이름을 지정합니다.

EndpointType

끝점 유형을 지정합니다.

UserLogin

끝점에 대한 사용자 로그인을 지정합니다.

URL

끝점에 대한 URL 값을 지정합니다.

Host

끝점 호스트 주소를 지정합니다.

Password

UserLogin 태그에 지정된 끝점 사용자의 암호를 지정합니다.

AdministrativeAdvanced

끝점에 고급 관리를 사용할 수 있는지 여부를 지정합니다.

참고: *EndpointTypeProperties* 태그는 동적이며 *EndpointType* 태그에 대해 지정된 입력에 의해 결정됩니다. 동적 끝점 유형 속성에 대한 속성 스키마를 가져오는 방법에 대한 설명은 끝점 유형 가져오기 (페이지 101) 절을 참조하십시오.

끝점 업데이트

끝점을 업데이트하려면 다음 URL 로 HTTP PUT 요청을 보내십시오.

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints
```

host_name

호스트 이름을 지정합니다.

다음 예는 끝점을 업데이트하는 HTTP 본문 콘텐츠를 보여 줍니다.

```
<Endpoint>
    <Name>endpoint_name</Name>
    <EndpointType>Endpoint_type</EndpointType>
    <EndpointTypeProperties>
        <UserLogin>user1</UserLogin>
        <URL>URL Value</URL>
        <Host>Endpoint_Host_Address</Host>
        <Password>User_Password</Password>
    </EndpointTypeProperties>
<AdministrativeAdvanced>false</AdministrativeAdvanced>
</Endpoint>
```

Name

호스트 이름을 지정합니다.

EndpointType

끝점 유형을 지정합니다.

UserLogin

끝점에 대한 사용자 로그인을 지정합니다.

URL

끝점에 대한 URL 값을 지정합니다.

Host

끝점 호스트 주소를 지정합니다.

Password

UserLogin 태그에 지정된 끝점 사용자의 암호를 지정합니다.

AdministrativeAdvanced

끝점에 고급 관리를 사용할 수 있는지 여부를 지정합니다.

끝점 삭제

끝점을 삭제하려면 다음 URL 로 HTTP DELETE 요청을 보내십시오.

`https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>`

host_name

호스트 이름을 지정합니다.

endpoint_name

호스트 이름을 지정합니다.

끝점 가져오기

모든 끝점을 가져오려면 다음 URL 로 HTTP GET 요청을 보내십시오.

`https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>`

host_name

호스트 이름을 지정합니다.

endpoint_name

호스트 이름을 지정합니다.

끝점 가져오기

모든 끝점을 가져오려면 GET 끝점 명령을 사용하십시오.

모든 끝점을 가져오려면 다음 URL 로 HTTP GET 요청을 보내십시오.

`https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints`

host_name

호스트 이름을 지정합니다.

끝점 유형 가져오기

모든 끝점 유형을 가져오려면 GET 끝점 유형 명령을 사용하십시오.

모든 끝점 유형을 가져오려면 다음 URL 로 HTTP GET 요청을 보내십시오.

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoint-types
```

EndpointTypeProperties 태그는 동적이며 EndpointType 태그에 대해 지정된 입력에 의해 결정됩니다. 속성 스키마를 가져오려면 다음 URL 을 사용하십시오.

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoint-types/<host_name>/properties-schema
```

host_name

호스트 이름을 지정합니다.

계정 요청 만들기

계정 요청을 만들려면 다음 URL 로 HTTP POST 요청을 보내십시오.

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts/<account_name>/accountrequest
```

host_name

호스트 이름을 지정합니다.

endpoint_name

호스트 이름을 지정합니다.

account_name

계정 이름을 지정합니다.

다음 예는 계정 요청을 만드는 HTTP 본문 콘텐츠를 보여 줍니다.

```
<AccountRequest>
    <StartTime>Start_Time</StartTime>
    <ValidUntilTime>Valid_Until_Time</ValidUntilTime>
    <User>
        <Name>user1</Name>
    </User>
    <Approver>
    <User>
        <Name>superadmin</Name>
    </User>
    </Approver>
    <Justification>user1 requests</Justification>

</AccountRequest>
```

StartTime

요청자 사용자가 공유 계정 요청 작업을 수행할 수 있는 시작 시간을 지정합니다.

날짜는 다음 형식으로 입력하십시오.

```
yyyy-mm-ddThh:mm:sec
```

ValidUntilTime

경과하면 사용자가 공유 계정 요청 작업을 수행할 수 없는 유효 시간을 지정합니다.

날짜는 다음 형식으로 입력하십시오.

```
yyyy-mm-ddThh:mm:sec
```

이름

요청자의 사용자 이름을 지정합니다.

<Approver><User>Name

승인자의 사용자 이름을 지정합니다.

Justification

사유 설명을 지정합니다.

계정 요청 삭제

계정 요청을 삭제하려면 다음 URL 로 HTTP DELETE 요청을 보내십시오.

`https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts/<account_name>/accountrequest/<account_request_name>`

host_name

호스트 이름을 지정합니다.

endpoint_name

호스트 이름을 지정합니다.

account_name

계정 이름을 지정합니다.

account_request_name

계정 요청 이름을 지정합니다.

요청에 대한 계정 암호 가져오기

사용자가 요청할 수 있는 모든 계정 암호를 가져오려면 다음 URL 로 HTTP GET 요청을 보내십시오.

`https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts?to-request=true`

host_name

호스트 이름을 지정합니다.

endpoint_name

호스트 이름을 지정합니다.

계정 요청 가져오기

특정 계정 요청(예: *exc-113*)을 가져오려면 다음 URL 로 HTTP GET 요청을 보내십시오.

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts/<account_name>/accountrequests/exc-113
```

권한 있는 계정(account_name)에 대한 액세스 권한이 있는 모든 계정 요청을 가져오려면 다음 URL 로 HTTP GET 요청을 보내십시오.

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts/<account_name>/accountrequests
```

전체 환경에서 모든 계정 요청을 가져오려면 다음 URL 로 HTTP GET 요청을 보내십시오.

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints?display=accountrequests
```

host_name

호스트 이름을 지정합니다.

endpoint_name

호스트 이름을 지정합니다.

account_name

계정 이름을 지정합니다.