

CA Access Control Premium Edition

엔터프라이즈 관리 안내서

12.6.02



포함된 도움말 시스템 및 전자적으로 배포된 매체를 포함하는 이 문서(이하 "문서")는 정보 제공의 목적으로만 제공되며 CA 에 의해 언제든지 변경 또는 취소될 수 있습니다.

CA 의 사전 서면 동의 없이 본건 문서의 전체 혹은 일부를 복사, 전송, 재생, 공개, 수정 또는 복제할 수 없습니다. 이 문서는 CA 의 기밀 및 독점 정보이며, 귀하는 이 문서를 공개하거나 다음에 의해 허용된 경우를 제외한 다른 용도로 사용할 수 없습니다: (i) 귀하가 이 문서와 관련된 CA 소프트웨어를 사용함에 있어 귀하와 CA 사이에 별도 동의가 있는 경우, 또는 (ii) 귀하와 CA 사이에 별도 기밀 유지 동의가 있는 경우.

상기 사항에도 불구하고, 본건 문서에 기술된 라이선스가 있는 사용자는 귀하 및 귀하 직원들의 해당 소프트웨어와 관련된 내부적인 사용을 위해 합당한 수의 문서 복사본을 인쇄 또는 제작할 수 있습니다. 단, 이 경우 각 복사본에는 전체 CA 저작권 정보와 범례가 첨부되어야 합니다.

본건 문서의 사본 인쇄 또는 제작 권한은 해당 소프트웨어의 라이선스가 전체 효력을 가지고 유효한 상태를 유지하는 기간으로 제한됩니다. 어떤 사유로 인해 라이선스가 종료되는 경우, 귀하는 서면으로 문서의 전체 또는 일부 복사본이 CA 에 반환되거나 파괴되었음을 입증할 책임이 있습니다.

CA 는 관련법의 허용 범위 내에서, 상품성에 대한 묵시적 보증, 특정 목적에 대한 적합성 또는 권리 위반 보호를 비롯하여(이에 제한되지 않음) 어떤 종류의 보증 없이 본 문서를 "있는 그대로" 제공합니다. CA 는 본 시스템의 사용으로 인해 발생하는 직, 간접 손실이나 손해(수익의 손실, 사업 중단, 영업권 또는 데이터 손실 포함)에 대해서는 (상기 손실이나 손해에 대해 사전에 명시적으로 통지를 받은 경우라 하더라도) 귀하나 제 3 자에게 책임을 지지 않습니다.

본건 문서에 언급된 모든 소프트웨어 제품의 사용 조건은 해당 라이선스 계약을 따르며 어떠한 경우에도 이 문서에서 언급된 조건에 의해 라이선스 계약이 수정되지 않습니다.

본 문서는 CA 에서 제작되었습니다.

본 시스템은 "제한적 권리"와 함께 제공됩니다. 미합중국 정부에 의한 사용, 복제 또는 공개는 연방조달규정(FAR) 제 12.212 조, 제 52.227-14 조, 제 52.227-19(c)(1)호 - 제(2)호 및 국방연방구매규정(DFARS) 제 252.227-7014(b)(3)호 또는 해당하는 경우 후속 조항에 명시된 제한 사항을 따릅니다.

Copyright © 2012 CA. All rights reserved. 본 시스템에서 언급된 모든 상표, 상호, 서비스 표시 및 로고는 각 해당 회사의 소유입니다.

타사 고지 사항

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

(c) Copyright IBM Corporation 1999, 2002

All Rights Reserved.

샘플 스크립트와 샘플 SDK 코드

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

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

CA Technologies 제품 참조

이 문서는 다음 CA Technologies 제품을 참조합니다 :

- CA Access Control Premium Edition
- CA Access Control
- CA Single Sign-On(CA 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)
- CA Service Desk Manager(이전 이름: Unicenter Service Desk)
- CA User Activity Reporting Module (이전 명칭: CA Enterprise Log Manager)
- CA Identity Manager

설명서 규칙

CA Access Control 설명서는 다음과 같은 규칙을 따릅니다.

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

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

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

예제: 명령 표기 규칙

다음 코드는 이 안내서에서 명령 규칙이 사용되는 방식을 보여 줍니다.

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

설명:

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

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

파일 위치 규칙

CA Access Control 설명서는 다음과 같은 파일 위치 규칙을 따릅니다.

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

CA 에 문의

기술 지원팀에 문의

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

설명서 변경 사항

이 설명서가 마지막으로 릴리스된 이후에 다음과 같이 업데이트되었습니다.

- PUPM 구현 계획 - 이 장에서 다음 섹션이 변경되었습니다.
 - 공유 계정 관리
 - 공유 계정이란?
 - 권한 있는 액세스 역할이 작업 체크 아웃 및 체크 인에 주는 영향
 - 권한 있는 액세스 역할이 공유 계정 요청 작업에 주는 영향
 - PUPM 끝점과 CA User Activity Reporting Module 을 통합하는 방법
 - 공유 계정 암호의 전자 메일 알림
 - 고급 CA Access Control 와 PUPM 통합 제한
- 공유 계정 구현 - 이 장에서 다음 섹션이 변경되었습니다.
 - 공유 계정 설정 방법
 - 암호 정책 만들기
 - PUPM 끝점 및 공유 계정 만들기
 - VMware ESX/ESXi 연결 정보
 - Windows Agentless Connection 정보
 - 로컬 Windows 계정 관리
 - Active Directory 계정 관리
 - Windows Agentless 끝점의 방화벽 구성
 - SSH 및 네트워크 장치 XML 구성 파일의 유형
 - SSH 장치 XML 파일 사용자 지정
 - 로그인 응용 프로그램 만들기
 - PUPM 끝점 및 공유 계정을 가져오는 방법
 - 끝점 CSV 파일 만들기
 - 공유 계정 CSV 파일 만들기
 - PUPM 자동 로그인 응용 프로그램 Visual Basic 스크립트
- PUPM 끝점 구성 - 이 장에서 다음과 같은 섹션이 변경되었습니다.

- 터미널 통합 구성
- 공유 계정 관리 - 장 제목이 업데이트되었습니다.

목차

제 1 장: 소개 17

안내서 정보.....	17
본 안내서의 사용자	17
엔터프라이즈 관리	18
엔터프라이즈 관리 인터페이스	18
중앙 정책 관리	18
엔터프라이즈 뷰	19
권한 있는 사용자 암호 관리	19
UNAB 관리	20
엔터프라이즈 보고서	20

제 2 장: CA Access Control 엔터프라이즈 관리 관리 21

관리 범위 지정	21
CA Access Control 엔터프라이즈 관리의 관리 역할	22
관리자 역할 만들기	23
권한 있는 액세스 역할	25
권한 있는 액세스 역할 만들기	26
사용자에게 역할을 할당하는 방법	28
관리 작업 만들기	32
사용자, 그룹, 관리 역할	35
Active Directory 제한	36
사용자 만들기	37
사용자 암호 다시 설정	39
사용자 활성화 또는 비활성화	40
그룹 유형	41
감사 데이터	46
제출된 작업 검색	47
작업 상세 정보 보기	51
이벤트 상세 정보 보기	51
제출된 작업 정리	52
메시지 큐 감사 메시지를 Windows 이벤트 로그로 라우팅	54
메시지 큐 감사 메시지를 UNIX Syslog 로 라우팅	56
전자 메일 알림	58
전자 메일 템플릿	58

전자 메일 알림 작동 방법	62
전자 메일 템플릿 사용자 지정	63

제 3 장: 기업 구현 보기 65

월드 뷰	65
회사의 CA Access Control 구현 보기	66
CA Access Control 끝점 관리를 열어 끝점 관리	67
CA Access Control 끝점 관리 SSO 를 위해 UNIX 끝점 구성	68
PUPM 끝점 수정	69

제 4 장: 중앙에서 정책 관리 71

정책 유형	71
중앙에서 정책을 관리하기 위한 방법	72
고급 정책 관리	72
고급 정책 기반 관리 작동 방법	73
배포 방법이 배포 작업에 주는 영향	74
DMS 가 수록한 끝점 데이터	76
끝점이 DMS 를 업데이트하는 방법	77
고급 정책 관리 통신 계층 수정	78
고급 정책 관리 클래스	78
호스트 및 호스트 그룹	81
끝점을 기업의 호스트로 정의	81
자동 호스트 그룹 할당이 작동하는 방법	83
논리 호스트 그룹 정의	87
호스트 그룹 가져오기	89
할당 경로	90
정책 생성 및 배포 방법	91
관리 요구 사항	92
정책 종속성	93
정책 확인	93
정책 버전 생성 및 저장	95
변수를 정의하는 정책 만들기	97
정책과 연관된 규칙 보기	99
정책 가져오기	100
저장된 정책 버전 할당	102
정책 유지 관리	103
할당된 정책 할당 취소	103
할당된 호스트를 최신 정책 버전으로 업그레이드	104

할당된 호스트를 특정 정책 버전으로 다운그레이드	105
삭제된 정책	105
변수	108
변수 작성 방법	109
변수 유형	109
변수 사용 지침	111
끝점이 변수를 해석하는 방법	114
정책 배포 문제 해결	114
사용하지 않는 끝점 제거 방법	116
배포 감사 정보 보기	116
정책 위반 계산 작동 방법	117
위반 계산 트리거	118
정책 위반 로그 및 오류 파일	119
정책 위반 데이터 파일	119

제 5 장: PUPM 구현 계획 125

공유 계정 관리	125
공유 계정이란?	125
권한 있는 액세스 역할 및 권한 있는 계정	126
권한 있는 액세스 역할 사용	126
권한 있는 액세스 역할이 작업 체크 아웃 및 체크 인에 주는 영향	128
권한 있는 액세스 역할이 공유 계정 요청 작업에 주는 영향	130
Break Glass 프로세스가 작동하는 방법	134
암호 소비자	135
암호 소비자의 유형	136
요청 시 암호 소비자가 암호를 가져오는 방법	137
PUPM 이 암호 변경에 대해 암호 소비자에게 통보하는 방법	139
암호 소비자에 대한 구현 고려 사항	140
PUPM 감사 레코드	141
암호 소비자 감사 레코드	142
PUPM 피더 감사 레코드	142
PUPM 끝점의 이벤트 감사	143
PUPM 끝점과 CA User Activity Reporting Module 을 통합하는 방법	144
CA Service Desk Manager 통합	144
CA Service Desk Manager 와 권한 있는 계정 요청을 통합하는 방법	145
CA Service Desk Manager 에 대한 연결 구성	146
구현 고려 사항	148
공유 계정 암호의 전자 메일 알림	148
Windows Agentless 끝점의 도메인 사용자에 대한 제한 사항	148

Active Directory 끝점을 관리하기 위한 최소 권한	149
고급 CA Access Control 와 PUPM 통합 제한	152
커넥터 서버	152
PUPM SDK	162

제 6 장: 공유 계정 구현 171

공유 계정 설정 방법	171
권한 있는 계정 검색	174
권한 있는 계정 또는 서비스 계정 만들기	177
암호 정책 만들기	180
암호 조합 규칙	182
PUPM 끝점 및 공유 계정 만들기	184
끝점 만들기	184
로그인 응용 프로그램 만들기	230
PUPM 끝점 및 공유 계정을 가져오는 방법	234
PUPM 피더가 동작하는 방법	235
끝점 CSV 파일 만들기	237
공유 계정 CSV 파일 만들기	244
직접 폴링 작업을 시작합니다.	247
암호 소비자를 설정하는 방법	248
서비스 계정 검색	252
암호 소비자 만들기	254
암호 소비자 예제: Windows Run As	257
암호 소비자 예제: Windows 예약된 작업	259
PUPM 자동 로그인	260
자동 로그인이 작동하는 방법	261
PUPM 자동 로그인 응용 프로그램 스크립트를 사용자 지정하는 방법	262
PUPM 원격 데스크톱 스크립트 사용자 지정	269
고급 로그인	272
터미널 통합	273

제 7 장: PUPM 끝점 구성 277

데이터베이스(JDBC) 암호 소비자를 사용하도록 JBoss Application 준비	277
Microsoft SQL Server 에 대한 데이터 원본 구성 파일 사용자 지정	279
Oracle 에 대한 데이터 원본 구성 파일 사용자 지정	279
암호 소비자 예제: JDBC 데이터베이스	280
Oracle 데이터베이스에 대한 추가 정보	282
데이터베이스(ODBC, OLEDB, OCI) 암호 소비자를 사용하도록 끝점 구성	284

데이터베이스(.NET) 암호 소비자를 사용하기 위한 끝점 구성	285
CLI 암호 소비자를 사용하기 위한 끝점 구성	287
CLI 암호 소비자가 작동하는 방식	288
예제: 암호를 가져오는 스크립트	289
암호 소비자 SDK 응용 프로그램을 사용하도록 끝점을 구성하는 방법	290
Java PUPM SDK 응용 프로그램 실행	291
웹 서비스 PUPM SDK 응용 프로그램을 사용하도록 끝점을 구성하는 방법	293
터미널 통합 구성	294

제 8 장: 공유 계정 관리 297

권한 있는 계정 암호의 강제 체크 인	297
권한 있는 계정 암호를 자동으로 다시 설정	298
권한 있는 계정 암호 직접 다시 설정	299
공유 계정 요청 관리	299
수동 암호 추출	300
권한 있는 계정 감사	302
권한 있는 계정 감사를 위한 검색 특성	302
작업 상태 설명	305
PUPM 끝점에서 감사 이벤트 보기	306
암호 소비자 동기화	307
끝점 관리자 암호 복원	309
이전 권한 있는 계정 암호 표시	310

제 9 장: UNAB 사용 311

UNAB 구성 요소	311
UNAB 설정 방법	312
UNAB 가 사용자를 인증하는 방법	313
UNAB 끝점에 저장된 정보	313
호스트 액세스를 제어하고 UNAB 를 구성하는 방법	314
UNAB 로그인 권한 부여 관리	315
UNAB 호스트 또는 호스트 그룹 구성	317
CA Access Control 엔터프라이즈 관리가 호스트에 정책을 커밋했는지 확인	318
사용자 및 그룹을 Active Directory 로 마이그레이션하는 방법	319
마이그레이션 충돌 해결	320
사용자 정보 표시	326
UNAB 중지	326
UNAB 상태 보기	327
UNAB 디버그 파일	327

제 10 장: 보고서 작성

329

보안 표준	329
보고서 유형	330
보고 서비스	330
보고 서비스 구성 요소	331
보고 서비스 작동 방법	332
끝점 스냅샷을 배포 서버로 보내기	334
CA Access Control 엔터프라이즈 관리에서 보고서를 보는 방법	336
스냅샷 데이터 캡처	336
CA Access Control 엔터프라이즈 관리에서 보고서 실행	337
보고서 보기	339
스냅샷 관리	340
BusinessObjects InfoView 보고서 포털	340
표준 보고서	345
보고서 모양	346
계정 관리 보고서	347
권한 보고서	351
기타 보고서	353
정책 관리 보고서	356
암호 정책 보고서	360
권한 있는 계정 관리 보고서	361
UNIX 인증 브로커 보고서	367
CA Enterprise Log Manager 보고서	371
사용자 지정 보고서	372
BusinessObjects 용 CA Access Control Universe	372
CA Access Control Universe 보기	372
표준 보고서 사용자 지정	373
사용자 지정 보고서 게시	374

제 11 장: 예제 및 모범 사례 정책 배포

375

예제 정책	375
예제 정책이 저장되는 위치	376
예제 정책 스크립트	377
컴플라이언스 및 모범 사례 정책	381
컴플라이언스 및 모범 사례 정책이 저장되는 위치	382
컴플라이언스 및 모범 사례 정책 스크립트	383
정책 배포	386
정책 배포를 위한 끝점 준비 방법	386

단계적으로 정책을 배포하는 방법	388

제 1 장: 소개

이 섹션은 다음 항목을 포함하고 있습니다.

[안내서 정보](#) (페이지 17)

[본 안내서의 사용자](#) (페이지 17)

[엔터프라이즈 관리](#) (페이지 18)

안내서 정보

이 안내서는 CA Access Control Premium Edition 의 엔터프라이즈 관리 및 보고 기능과 CA Access Control 엔터프라이즈 관리 웹 기반 인터페이스에 대한 정보를 제공합니다. CA Access Control 의 엔터프라이즈 관리 및 보고 기능에는 고급 정책 관리, 보고, 월드 뷰 엔터프라이즈 뷰어가 포함되어 있습니다.

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

본 안내서의 사용자

이 안내서는 다음과 같은 CA Access Control 의 엔터프라이즈 관리 및 보고 기능을 사용하려는 보안 및 시스템 관리자로 작성되었습니다.

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

엔터프라이즈 관리

CA Access Control 엔터프라이즈 관리는 회사 전체에서 액세스 관련 관리 작업을 수행할 수 있게 해주는 웹 기반 사용자 인터페이스입니다. CA Access Control 엔터프라이즈 관리를 사용하여 여러 관리 작업을 수행할 수 있습니다. 예를 들어, 중앙 위치에서 회사 전체에 액세스 정책을 배포하거나, 개별 호스트를 관리하거나, 권한 있는 계정을 관리하거나, 엔터프라이즈 보고서를 작성하는 등의 작업을 수행할 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.

중앙 정책 관리

회사의 호스트 또는 호스트 그룹에 일관된 정책을 만들어 할당하려면 CA Access Control 엔터프라이즈 관리의 중앙 정책 관리 기능을 사용하십시오. CA Access Control 엔터프라이즈 관리 인터페이스에서는 마법사를 사용하여 회사 전체에 적용되는 정책을 할당하고 모든 호스트에서 배포 프로세스 상태를 확인할 수 있습니다.

또한 CA Access Control 엔터프라이즈 관리 중앙 정책 관리 기능을 사용하여 정책 배포 프로세스의 문제를 해결하고, 기존 정책을 할당 취소하거나 업그레이드/다운그레이드할 수 있습니다.

엔터프라이즈 뷰

CA Access Control 엔터프라이즈 관리를 사용하여 중앙 위치에서 CA Access Control, PUPM, UNAB 호스트에 대한 정보를 보고 관리할 수 있습니다. CA Access Control 엔터프라이즈 관리 월드 뷰는 각 호스트 유형, 마지막 업데이트된 날짜, 각 호스트에 구성된 장치 유형에 대한 세부 정보를 표시하고, 호스트 설정을 수정하고 원격으로 관리할 수 있게 해 줍니다.

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.

UNAB 관리

UNIX 인증 브로커(UNAB)는 Active Directory 데이터 저장소를 사용하여 UNIX 컴퓨터에 로그인할 수 있게 해 줍니다. 즉, 모든 사용자에게 대해 단일 리포지토리를 사용할 수 있으므로 사용자들이 동일한 사용자 이름과 암호를 사용하여 모든 플랫폼에 로그인할 수 있게 됩니다.

UNIX 계정을 Active Directory 와 통합하면 엄격한 인증 및 암호 정책을 시행하고, 기본 UNIX 사용자 및 그룹 속성을 Active Directory 로 전송할 수 있습니다. 이렇게 하면 Windows 사용자와 그룹을 관리할 때처럼 단일 지점에서 UNIX 사용자 및 그룹을 관리할 수 있게 됩니다.

일련의 로그인 규칙을 포함하는 로그인 정책을 만들어 할당하는 방법으로 UNIX 호스트에 대한 액세스를 제어하려면 CA Access Control 엔터프라이즈 관리 중앙 정책 관리 기능을 사용하십시오.

엔터프라이즈 보고서

CA Access Control 엔터프라이즈 관리 보고 옵션을 사용하면 한 위치에서 각 끝점(사용자, 그룹, 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 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](#) (페이지 21)

[사용자, 그룹, 관리 역할](#) (페이지 35)

[감사 데이터](#) (페이지 46)

[전자 메일 알림](#) (페이지 58)

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** - 호스트 및 로컬 호스트 그룹을 정의합니다.

이 관리 역할이 있는 사용자는 호스트 및 호스트 그룹을 만들고, 호스트를 호스트 그룹에 할당하고, 이들을 수정할 수 있습니다. 이 역할의 사용자는 정책 또는 배포 정책을 정의할 수는 없지만 이러한 정책을 보고 월드 뷰에 액세스할 수 있습니다.

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

이 관리 역할이 있는 사용자는 정책을 호스트 및 호스트 그룹에 할당하고, 정책을 업그레이드/다운그레이드하고, 구성을 다시 설정하고, 배포 감사에 액세스할 수 있습니다. 이 역할의 사용자는 정책 및 호스트를 볼 수 있지만 정의할 수는 없으며 월드 뷰에 액세스할 수 있습니다.

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

이 관리 역할이 있는 사용자는 정책을 만들고, 수정하고, 보고, 삭제할 수 있습니다. 이 역할의 사용자는 호스트 또는 호스트 그룹에 정책을 배포할 수는 없지만 이들을 보고 월드 뷰에 액세스할 수 있습니다.

- **CA Access Control 사용자 관리자** - CA Access Control 엔터프라이즈 관리에서 사용자를 관리합니다. 즉, 사용자 및 그룹을 만들고 관리하며 CA Access Control 엔터프라이즈 관리 역할을 사용자에게 할당합니다.

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.

이 관리 역할이 있는 사용자는 CA Access Control 엔터프라이즈 관리에 있는 모든 작업을 수행하고, 만들고, 관리할 수 있습니다.

회사에서 실제 관리 역할을 정의하는 구현 단계와 비상 상황에 이 역할을 사용하십시오. 이 역할을 최소한의 사용자에게 할당하고(사용자 한 명이 적합함) 이 사용자의 동작을 자세히 모니터링하는 것이 좋습니다.

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

- **UNAB 관리자** - UNAB 를 관리합니다. 이 역할이 있는 사용자는 UNAB 호스트 및 호스트 그룹을 구성하고, 로그인 권한 부여 정책을 관리하고, 마이그레이션 충돌을 해결할 수 있습니다.
참고: 시스템 관리자 역할이 할당된 사용자에게는 UNAB 관리자 역할도 함께 할당됩니다.
- **CA Enterprise Log Manager 사용자** - CA Enterprise Log Manager 보고서를 볼 수 있습니다. 이 역할이 있는 사용자는 CA Enterprise Log Manager 보고서를 볼 수 있습니다.
- **CA Enterprise Log Manager 관리자** - 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 자신의 계정에서 계정 암호 변경, 자신의 사용자 프로필 수정, 자신의 할당된 역할/제출된 작업/승인 대기 중인 항목 보기와 같은 관리 작업을 수행할 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. b에서 c 단계를 반복하여 역할에 작업을 더 추가합니다.
7. [구성원 및 범위 규칙을 추가합니다](#) (페이지 28).
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.

사용자에게 권한 있는 액세스 역할을 할당할 때는 다음 사항에 주의해야 합니다.

- 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)을 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. b에서 c 단계를 반복하여 역할에 작업을 더 추가합니다.
7. [구성원 및 범위 규칙을 추가합니다](#) (페이지 28).
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 사용자에게 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 30)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 30)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 31)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 30)를 지정합니다.

역할의 관리 정책이 만들어집니다.

3. "소유자" 탭을 클릭한 다음 "추가"를 클릭하고 [소유자 역할](#) (페이지 31)을 지정한 다음 "확인"을 클릭합니다.

정책의 소유자 규칙이 만들어집니다.

구성원 정책

구성원 정책은 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 33)

[탭 추가](#) (페이지 34)

[필드, 이벤트, 역할 사용 구성](#) (페이지 34)

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 37)

[그룹 유형](#) (페이지 41)

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 사용자에게 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 구성된 LDAP 디렉터리 내에서 수행됩니다.

예: 예제 LDAP 쿼리

샘플 LDAP 쿼리는 다음과 같습니다.

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

설명	쿼리
뉴욕 서부 지사에 있는 모든 관리자	ldap:///o=MyCorporation??one?(&(title=Manager)(office=NYWest))
휴대폰이 있는 모든 기술자	ldap:///o=MyCorporation??one?(&(employee=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 Manager에 라우트하도록 감사 수집기를 구성할 수 있습니다..

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

추가 정보:

[제출된 작업 검색](#) (페이지 47)

[작업 상세 정보 보기](#) (페이지 51)

[이벤트 상세 정보 보기](#) (페이지 51)

[제출된 작업 정리](#) (페이지 52)

[메시지 큐 감사 메시지를 Windows 이벤트 로그로 라우팅](#) (페이지 54)

[메시지 큐 감사 메시지를 UNIX Syslog 로 라우팅](#) (페이지 56)

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 48)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 50)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

작업 흐름의 일부로 승인되어야 하는 작업을 식별합니다.

추가 정보:

[작업 상태 설명](#) (페이지 50)

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 보여줍니다.

```
<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. ■ CheckOutAccountPassswordEvent.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: 기업 구현 보기

이 섹션은 다음 항목을 포함하고 있습니다.

[월드 뷰](#) (페이지 65)

[회사의 CA Access Control 구현 보기](#) (페이지 66)

[CA Access Control 끝점 관리를 열어 끝점 관리](#) (페이지 67)

[CA Access Control 끝점 관리 SSO 를 위해 UNIX 끝점 구성](#) (페이지 68)

[PUPM 끝점 수정](#) (페이지 69)

월드 뷰

CA Access Control 엔터프라이즈 관리의 월드 뷰를 통해 연결된 DMS 에서 관리하고 있는 회사의 CA Access Control 구현을 볼 수 있습니다.

월드 뷰를 사용하여 다음을 수행할 수 있습니다.

- 연결된 DMS 에 보고하는 끝점을 식별합니다.
- CA Access Control, PMDB, PUPM, UNAB 중 하나인 끝점 유형을 식별합니다.
- 각 끝점에서 마지막으로 DMS 로 하트비트를 전송한 시간을 식별합니다.
- 배포된 정책, 운영 체제, 끝점에 있는 관리되는 장치와 같은 끝점에 대한 보다 자세한 정보를 봅니다.
- CA Access Control 끝점을 관리하기 위해 CA Access Control 끝점 관리를 엽니다.
- UNAB 호스트 또는 PUPM 관리되는 장치를 수정합니다.

회사의 CA Access Control 구현 보기

CA Access Control 엔터프라이즈 관리를 사용하여 회사의 CA Access Control 구현을 표시할 수 있습니다. 이 엔터프라이즈 "월드 뷰"는 모든 끝점, 끝점이 그룹화된 논리적 호스트 그룹, 끝점에 있는 배포된 정책, 끝점에 있는 관리되는 장치의 스냅샷입니다.

회사의 CA Access Control 구현을 보려면

1. CA Access Control 엔터프라이즈 관리에서 "월드 뷰" 탭을 클릭하고 왼쪽에 있는 작업 메뉴에서 "월드 뷰" 링크를 클릭합니다.
"월드 뷰" 페이지가 나타나고 "검색" 섹션이 표시됩니다.
2. (선택 사항) 검색 조건을 정의합니다.
다음과 같이 두 가지 검색 유형을 사용할 수 있습니다.
 - **단순** - 단순 검색을 사용하여 호스트 이름 마스크를 정의하고 결과를 필터링할 끝점의 유형을 지정합니다.
 - **고급** - "고급" 링크를 클릭하면 지정된 호스트 그룹, 할당된 정책, 관리되는 장치 이름 마스크, 관리되는 장치 유형을 기준으로 결과를 필터링할 수 있습니다.

참고: 기본적으로 월드 뷰에는 CA Access Control 엔터프라이즈 관리가 연결되어 있는 DMS 에 정의된 모든 끝점에 대한 결과가 표시됩니다.
3. "실행"을 클릭합니다.
다음 범주 중 하나로 정의한 조건과 일치하는 결과가 표시됩니다.
 - **호스트 이름별 결과** - DMS 에 정의하는 호스트(끝점)입니다. 이 범주는 결과를 표시할 때 사용되는 기본 범주입니다.
 - **호스트 그룹별 결과** - 정의하는 논리적 호스트 그룹입니다.
 - **정책별 결과** - 끝점에 배포된 정책입니다.
 - **관리되는 장치별 결과** - 끝점에 있는 관리되는 장치입니다.

CA Access Control 끝점 관리를 열어 끝점 관리

CA Access Control 엔터프라이즈 관리는 CA Access Control 끝점 관리에 쉽게 로그인하여 CA Access Control 엔터프라이즈 관리가 관리하는 모든 끝점을 관리할 수 있도록 SSO(Single-Sign On)를 지원합니다.

Windows 끝점을 관리하기 위해 자동 로그인을 설정하려면 CA Access Control 엔터프라이즈 관리 및 CA Access Control 끝점에서 동일한 사용자 이름과 암호를 사용하는지 확인하고, CA Access Control 끝점 관리를 사용하여 끝점을 관리하기 위한 터미널 액세스 권한이 있는지 확인하십시오.

참고: UNIX 끝점을 관리하기 위해 자동 로그인을 설정하려면 CA Access Control 끝점 관리 SSO 에 대한 끝점을 구성해야 합니다.

CA Access Control 끝점 관리를 열어 끝점을 관리하려면

1. 월드 뷰를 사용하여 관리할 끝점 하나 이상을 표시합니다.
2. "작업" 열에서 "관리"를 클릭합니다.

CA Access Control 끝점 관리가 열리고 끝점의 호스트 이름과 사용자의 자격 증명이 자동으로 입력됩니다. 로그인하는 데 사용한 CA Access Control 엔터프라이즈 관리 사용자 계정이 CA Access Control 끝점 관리에 없으면 자격 증명을 직접 입력해야 합니다.

추가 정보:

[회사의 CA Access Control 구현 보기](#) (페이지 66)

[CA Access Control 끝점 관리 SSO 를 위해 UNIX 끝점 구성](#) (페이지 68)

CA Access Control 끝점 관리 SSO 를 위해 UNIX 끝점 구성

CA Access Control 엔터프라이즈 관리를 사용하면 CA Access Control 끝점 관리에 쉽게 로그인하여 CA Access Control 엔터프라이즈 관리에서 관리하는 모든 끝점을 관리할 수 있습니다. 자동 로그인에서는 사용자 자신의 Active Directory 자격 증명을 사용하여 CA Access Control 엔터프라이즈 관리에 로그인합니다. CA Access Control 엔터프라이즈 관리는 이 자격 증명을 보존하며 사용자가 끝점을 관리하기 위해 CA Access Control 끝점 관리를 열 때 끝점에 이 자격 증명을 제공합니다. CA Access Control 끝점 관리를 사용한 CA Access Control 자동 로그인은 CA Access Control 엔터프라이즈 관리에 대해 인증하기 위해 사용하는 사용자 계정에 의존합니다.

참고: UNAB 끝점에 대한 자동 로그인을 구성하려면 CA Access Control 엔터프라이즈 관리와 UNAB 가 동일한 Active Directory 를 사용해야 합니다.

중요! Active Directory 에서 UNIX 사용자로 사용할 사용자를 구성합니다.

CA Access Control 끝점 관리 SSO 를 위해 UNIX 끝점을 구성하려면

1. CA Access Control 끝점에서 seos.ini 파일을 열고 [OS_User] 섹션을 찾은 다음 osuser_enabled 토큰의 값을 **1** 로 설정합니다.
엔터프라이즈 사용자 및 그룹이 활성화됩니다.
2. [seos] 섹션을 찾아 auth_login 토큰의 값을 **pam** 으로 설정합니다.
사용되는 로그인 권한 방법은 PAM 입니다.
3. CA Access Control 끝점 관리 컴퓨터에 대한 TERMINAL 레코드를 만듭니다.
CA Access Control 끝점 관리 컴퓨터에는 TERMINAL 액세스가 부여됩니다.

4. CA Access Control 엔터프라이즈 관리에 로그인하는 데 사용하는 사용자 계정을 XUSER 로 구성하고 여기에 admin 특성을 부여합니다. 다음 형식을 사용하십시오: <DOMAIN-NAME>user_account.
5. TERMINAL 클래스에서 읽기 및 쓰기 액세스 권한을 사용하여 superadmin 사용자에게 대한 ACL 을 정의합니다. 예:

Defaccess : R, W

ACLs :

Accessor	Access

DOMAIN\user(XUSER)	R, W

사용자는 CA Access Control 엔터프라이즈 관리 서버를 사용하여 끝점을 관리할 수 있습니다.

PUPM 끝점 수정

CA Access Control 엔터프라이즈 관리 월드 뷰를 사용하여 PUPM 끝점의 관리되는 장치에 대한 설정을 수정할 수 있습니다. 관리되는 장치는 권한 있는 계정을 사용하여 관리하는 응용 프로그램입니다. PUPM 끝점은 계정에 대한 액세스를 부여하는 역할 기반 관리 시스템을 사용하여 권한 있는 계정을 암호 데이터베이스에 저장합니다. 관리되는 장치는 PUPM 끝점 자체에 설치되거나 엔터프라이즈에 설치할 수 있습니다.

PUPM 끝점을 수정하려면

1. "월드 뷰", "월드 뷰" 작업을 차례로 선택합니다.
월드 뷰 검색 화면이 나타납니다.
2. 쿼리를 입력한 다음 "실행"을 클릭합니다.
쿼리에 대한 검색 결과가 표시됩니다.
3. 수정할 PUPM 끝점의 행에 있는 아래쪽 화살표(보기) 아이콘을 클릭합니다.
확장된 정보에 끝점에 있는 관리되는 장치가 표시됩니다.
4. "수정"을 클릭하여 끝점 설정을 수정합니다.
"끝점 수정" 창이 나타나고 여기에 끝점 설정이 표시됩니다.
5. 끝점 설정을 수정하고 "제출"을 클릭합니다.
작업이 완료되었음을 알리는 메시지가 표시됩니다.

추가 정보:

[끝점 만들기](#) (페이지 184)

제 4 장: 중앙에서 정책 관리

이 섹션은 다음 항목을 포함하고 있습니다.

- [정책 유형 \(페이지 71\)](#)
- [중앙에서 정책을 관리하기 위한 방법 \(페이지 72\)](#)
- [고급 정책 관리 \(페이지 72\)](#)
- [고급 정책 기반 관리 작동 방법 \(페이지 73\)](#)
- [호스트 및 호스트 그룹 \(페이지 81\)](#)
- [정책 생성 및 배포 방법 \(페이지 91\)](#)
- [정책 유지 관리 \(페이지 103\)](#)
- [변수 \(페이지 108\)](#)
- [정책 배포 문제 해결 \(페이지 114\)](#)
- [사용하지 않는 끝점 제거 방법 \(페이지 116\)](#)
- [배포 감사 정보 보기 \(페이지 116\)](#)
- [정책 위반 계산 작동 방법 \(페이지 117\)](#)

정책 유형

CA Access Control 엔터프라이즈 관리에서는 CA Access Control 정책, UNAB 구성 정책, UNAB 로그인 정책의 세 가지 정책 유형을 사용하여 CA Access Control 끝점 및 UNAB 호스트를 관리합니다.

CA Access Control 정책은 회사 전체에서 CA Access Control 끝점에 대한 접근자의 권한을 설정하고 리소스에 대한 액세스를 제어하기 위한 통일된 정책을 만들 때 사용합니다.

UNAB 로그인 정책은 회사 내의 UNIX 호스트에 대한 액세스를 관리할 때 사용합니다. 로그인 정책은 UNAB가 실행되는 UNIX 호스트에 대한 사용자의 로그인을 제어합니다. CA Access Control 엔터프라이즈 관리는 전파한 권한 부여 목록을 기반으로 자동으로 로그인 정책을 만들고, 할당하고, 배포합니다.

UNAB 구성 정책은 조직 내에서 UNAB 호스트를 배포 및 구성하기 위해 원격 UNAB 호스트의 구성 파일에 있는 토큰 값을 설정할 때 사용합니다.

추가 정보:

[UNAB 로그인 권한 부여 관리](#) (페이지 315)

[UNAB 호스트 또는 호스트 그룹 구성](#) (페이지 317)

중앙에서 정책을 관리하기 위한 방법

CA Access Control 을 사용하면 다음 방법으로 단일 컴퓨터에서 여러 데이터베이스를 관리할 수 있습니다.

- **자동 규칙 기반 정책 업데이트** - 중앙 데이터베이스(PMDB)에서 정의한 일반 규칙은 구성된 계층의 데이터베이스에 자동으로 전파됩니다.

참고: 이중 제어는 이 방법으로만, UNIX 에서만 사용할 수 있습니다. 자동 규칙 기반 정책 업데이트의 이중 제어에 대한 자세한 내용은 *UNIX 용 끝점 관리 안내서*를 참조하십시오. 자동 규칙 기반 정책 업데이트에 대한 자세한 내용은 *Windows 용 끝점 관리 안내서*를 참조하십시오.

- **고급 정책 관리** - 사용자가 배포하는 정책(규칙 그룹)은 호스트 또는 호스트 그룹 할당에 따라 모든 데이터베이스에 전파됩니다. 정책을 배포 취소(제거)하고 배포 상태와 배포 위반을 확인할 수도 있습니다. 이 기능을 사용하려면 추가 구성 요소를 설치하고 구성해야 합니다.

참고: 고급 정책 관리에 대한 자세한 내용은 *엔터프라이즈 관리 안내서*를 참조하십시오.

고급 정책 관리

정책(selang 명령)을 작성하여 저장한 후, 사용자가 정의하는 방식으로 기업에 배포할 수 있습니다. 이 정책 기반 방법을 사용하여 정책을 저장한 다음 호스트 또는 그룹 호스트에 할당할 수 있습니다. 할당된 정책은 배포를 위해 큐에 추가됩니다. 또는 호스트나 그룹 호스트에 직접 정책 버전을 배포 및 배포 취소할 수 있습니다.

중앙 데이터베이스인 DMS(Deployment Map Server)에서는 기업 정책, 버전, 할당 및 배포에 대한 모든 정보를 수집합니다. 따라서 배포 상태, 배포 위반 및 배포 계층에 대해 쉽게 보고할 수 있습니다.

참고: 이중 제어는 이 방법에서 사용할 수 없으며 UNIX 에서만 사용할 수 있습니다. 자세한 내용은 *UNIX 용 끝점 관리 안내서*를 참조하십시오.

고급 정책 기반 관리 작동 방법

고급 정책 기반 관리를 통해 정책 버전을 저장, 배포 및 배포 취소하고 나중에 배포 상태, 배포 위반 및 배포 분산을 확인할 수 있습니다.

고급 정책 기반 관리는 다음 방식으로 작동합니다.

1. 정책을 만듭니다.

각 정책은 **selang** 명령 스크립트 쌍으로 포함합니다. 첫 번째 스크립트는 **배포 스크립트**라고 하며 정책을 구성하는 **selang** 명령 집합을 포함하고 있습니다. 두 번째 스크립트는 **배포 취소 스크립트**라고 하며 끝점 데이터베이스에서 정책의 배포를 취소(제거)하는 데 필요한 명령을 포함하고 있습니다.

2. CA Access Control 엔터프라이즈 관리 또는 **policydeploy** 유틸리티를 사용하여 DMS에 정책 세부 정보를 저장하면 CA Access Control은 자동 버전 제어 기능을 사용하여 정책을 저장합니다.

정책 세부 정보에는 정책 설명, 배포 및 배포 취소 스크립트, 정책 종속성 등이 포함됩니다.

3. DMS에 정책이 이미 있는지 여부에 따라 CA Access Control은 다음 중 하나를 수행합니다.

- DMS에 정책 이름이 없으면 CA Access Control은 정책의 첫 번째 버전(**policy_name#01**)과 논리적 정책 개체(GPOLICY 클래스)를 만든 다음 정책 버전을 논리적 정책의 구성원으로 추가합니다.
- DMS에 정책 이름이 이미 있으면 CA Access Control은 검색된 가장 높은 정책 버전에 한 버전을 증가시켜 새 정책 버전을 만들고 이 정책 버전을 논리적 정책(GPOLICY 개체)의 구성원으로 추가합니다.

4. 준비가 되었다고 판단되면 CA Access Control 엔터프라이즈 관리나 **policydeploy** 유틸리티를 사용하여 저장된 정책을 대상 데이터베이스에 배포합니다. CA Access Control은 DMS에서 자동으로 배포 작업(DEPLOYMENT 개체)을 만듭니다.

참고: CA Access Control은 저장된 정책의 최종 완료된 정책 버전을 배포합니다. 만드는 새 정책 버전은 자동으로 할당된 호스트에 전달되지 않습니다. 할당된 호스트를 최신 정책 버전으로 수동으로 업그레이드해야 합니다.

참고: 정책을 만든 이후에 CA Access Control 엔터프라이즈 관리는 UNAB 로그인 및 프로시저 정책을 자동으로 배포합니다. 사용자는 UNAB 로그인 및 구성 정책만 UNAB 호스트에 할당할 수 있습니다.

5. CA Access Control 은 DMS 에서 배포 패키지(GDEPLOYMENT 개체)를 자동으로 만듭니다.
배포 패키지는 이전 단계에서 작성된 모든 배포 작업을 그룹화합니다.
6. DMS 가 배포 작업을 DH(배포 호스트)로 보냅니다.
7. 끝점은 policyfetcher 를 통해 새 정책 배포 작업이 있는지 정기적으로 확인하고, 보류 중인 배포 작업을 DH 에서 가져오고, 각 규칙(배포 스크립트에 지정된 selang 명령)을 대상 데이터베이스에서 실행합니다.
8. 끝점은 DH 의 배포 작업 상태(실패, 성공), 실패한 명령에 대해 생성되는 selang 결과 메시지 및 HNODE 의 정책 상태를 업데이트합니다.
참고: 배포된 정책에 오류가 있는 경우 CA Access Control 엔터프라이즈 관리의 배포 감사를 사용하여 실패한 명령에 대한 자세한 selang 출력을 볼 수 있습니다. 그렇지 않으면 오류가 있는 정책이 배포된 컴퓨터에서 로그 파일을 확인해야 합니다.
9. DH 가 이 정보가 저장된 DMS 에서 배포 작업 상태와 정책 상태를 업데이트합니다.

참고: UNAB 로그인 정책 및 UNAB 구성 정책은 고급 정책 기반 관리와 같은 방식으로 작동하지 않습니다.

추가 정보:

[정책 종속성](#) (페이지 93)

[정책 확인](#) (페이지 93)

[할당 경로](#) (페이지 90)

[호스트 액세스를 제어하고 UNAB 를 구성하는 방법](#) (페이지 314)

배포 방법이 배포 작업에 주는 영향

저장된 정책을 대상 데이터베이스로 배포할 때 CA Access Control 은 DMS 에 배포 작업을 자동으로 만듭니다. 배포 작업(DEPLOYMENT 개체)은 끝점에서 실행할 작업 지시로서 DMS 에서 생성됩니다. 각 배포 작업은 한 끝점에만 사용되며 끝점에 배포하는 데 필요한 정책 버전 정보를 포함하고 있습니다.

참고: CA Access Control 은 다른 배포 방법을 사용하여 UNAB 로그인 및 구성 정책을 배포합니다.

저장된 정책을 배포하기 위해 사용하는 방법은 **CA Access Control** 이 만드는 배포 작업에 영향을 줍니다. 다음은 다른 방법을 선택할 때의 결과에 대해 설명합니다.

- 정책(GPOLICY 개체)을 하나 이상의 호스트에 할당
CA Access Control 은 호스트별로 정책의 최종 완료된 버전에 대한 배포 작업을 만듭니다.
- 정책(GPOLICY 개체)을 하나 이상의 호스트 그룹에 할당
CA Access Control 은 호스트 그룹 중 하나의 구성원인 호스트별로 정책의 최종 완료된 버전에 대한 배포 작업을 만듭니다.
- 저장된 정책(GPOLICY 개체)이 할당된 호스트 그룹에 호스트 추가
CA Access Control 은 새 호스트에 대해 정책의 최종 완료된 버전에 대한 배포 작업을 만듭니다.
- 호스트에 정책 다시 배포
CA Access Control 은 호스트별로 정책의 최종 완료된 버전에 대한 배포 작업을 만듭니다.
- HNODE 에서 정책 복원(호스트에 배포해야 하는 정책 재배포)
CA Access Control 은 호스트에 배포해야 하는 정책별로 해당 호스트에서 유효한 정책 버전에 대한 배포 작업을 만듭니다.
- 하나 이상의 호스트에서 배포된 정책 업그레이드
호스트에 저장된 버전이 호스트에 배포된 것보다 최신 버전인 경우 CA Access Control 은 호스트별로 최종 완료된 정책 버전에 대한 배포 작업을 만듭니다.

예: 호스트에 정책 할당

정책 IIS 를 호스트 `host1.comp.com` 및 `host2.comp.com` 에 할당하는 경우 CA Access Control 은 최신 IIS 정책 버전을 `host1.comp.com` 에 배포하기 위한 작업과 최신 IIS 정책 버전을 `host2.comp.com` 에 배포하기 위한 작업의 두 가지 배포 작업을 만듭니다.

예: 호스트 그룹에 정책 할당

호스트 그룹 서버에 `hostA.comp.com` 및 `hostB.comp.com` 의 두 개의 구성원이 있습니다. 정책 IIS 를 호스트 그룹 서버에 할당하는 경우 CA Access Control 은 최신 IIS 정책 버전을 `hostA.comp.com` 에 배포하는 작업과 최신 IIS 정책 버전을 `hostB.comp.com` 에 배포하는 두 개의 배포 작업을 만듭니다.

예: 할당된 정책이 있는 호스트 그룹에 호스트 추가

호스트 그룹 서버에는 두 개의 할당된 정책(IIS 및 ORACLE)이 있습니다. 호스트 `test.comp.com` 을 호스트 그룹에 추가하는 경우 CA Access Control 은 최신 IIS 정책 버전을 `test.comp.com` 에 배포하는 작업과 최신 ORACLE 정책 버전을 `test.comp.com` 에 배포하는 두 가지 배포 작업을 만듭니다.

예: 호스트 복원

호스트에 `policy1` 과 `policy2` 의 두 개의 할당된 정책이 있습니다. 호스트를 복원하는 경우 CA Access Control 은 호스트에서 최종 완료된 `policy1` 버전을 배포하는 작업과 최종 완료된 `policy2` 버전을 배포하는 두 가지 배포 작업을 만듭니다.

예: 배포된 정책 업그레이드

정책 IIS 가 `host1.comp.com` 및 `host2.comp.com` 의 두 개 호스트에 배포되었지만 정책 IIS 의 최종 버전은 `host1.comp.com` 에 배포되지 않았습니다. 두 호스트 모두에서 정책 IIS 를 업그레이드하는 경우 CA Access Control 은 최신 IIS 정책 버전을 `host1.comp.com` 에 배포하는 하나의 배포 작업만 만듭니다.

추가 정보:

[호스트 액세스를 제어하고 UNAB 를 구성하는 방법](#) (페이지 314)

DMS 가 수록한 끝점 데이터

회사 환경에 고급 정책 관리를 구성할 때 회사의 끝점은 구성된 DH 를 통해 다음 세 가지 영역의 상태 변경 사항을 DMS 에 통보합니다.

■ 정책 배포 및 배포 취소

정책이 배포 또는 배포 취소될 때 끝점은 알람을 보냅니다. 그러면 작업 결과에 따라 다음 세부 정보가 업데이트됩니다.

- 정책 세부 정보
- 배포 상태(성공, 실패 등)
- 실행하지 못한 정책 명령의 `selang` 명령 출력
- HNODE 정책 상태(배포됨, 배포 실패 등)

- 호스트 하트비트

일반 구성 가능한 간격으로 각 끝점은 온라인 상태의 호스트에 대한 계정으로 하트비트를 전달합니다.

- 위반 상태

각 하트비트 이후에 끝점은 정책 위반을 계산하여 그 결과(위반 발견 여부)를 보냅니다.

참고: `policyfetcher` 가 끝점과 DH 사이에서 배포 및 위반 상태 충돌을 발견하면 끝점에서 받은 정보를 기준으로 이 충돌을 해결합니다.

끝점이 DMS 를 업데이트하는 방법

각 끝점은 사용자가 구성한 DH 를 통해 하트비트(호스트 상태), 정책 상태 및 위반 상태 알림을 DMS 에 보냅니다. 해당 DMA 알림은 다음과 같은 방법으로 처리됩니다.

1. DH 가 업데이트 파일에 알림 메시지를 저장합니다.

이러한 알림은 끝점에서 보내는 하트비트 및 정책 배포/배포 취소 알림입니다.

2. DH 에서 구독자인 DMS 에 연결합니다.

- DMS 를 사용할 수 없는 경우 DH 는 모든 메시지를 성공적으로 보낼 때까지 정기적으로 DMS 와 통신하려고 시도합니다.

- DMS 를 사용할 수 있는 경우 DH 는 저장된 알림을 보냅니다.

3. DMS 가 나중에 사용할 수 있도록 각 DH 에서 받은 정보를 저장합니다.

보고서를 작성할 때마다 CA Access Control 은 DMS 에서 정보를 검색합니다.

참고: UNAB 끝점은 다른 프로세스를 사용하여 DMS 를 업데이트합니다.

추가 정보:

[호스트 액세스를 제어하고 UNAB 를 구성하는 방법](#) (페이지 314)

고급 정책 관리 통신 계층 수정

CA Access Control 12.6.01 부터, DMS 와 배포 호스트 사이의 고급 정책 관리 통신 계층은 메시지 큐 서버를 사용하도록 수정되었습니다. 메시지 큐 서버를 사용하기 위해 기존 끝점 통신 방법을 수정할 수 있습니다.

다음 단계를 수행하십시오.

1. DMS 가 있는 엔터프라이즈 관리 서버에서 모든 구독자가 DMS 와 동기화되었는지 확인합니다.

참고: DH 구독자 오프셋이 전역 오프셋과 일치하는지 확인하십시오.

2. DMS 에서 모든 구독자를 제거합니다. 예:

```
sepmc -u DMS__DH__@dhname
```

3. 다음과 같이 메시지 큐 구독자를 DMS 에 추가합니다.

```
sepmc -smc DMS__ -predefined ServerToServerBroadcast -destination DH
```

4. 각 배포 서버에서 다음 명령을 사용하여 DMS 구독자가 DH__WRITER 와 동기화되었는지 확인합니다.

```
sepmc -L DH__WRITER
```

참고: DMS 구독자 오프셋이 전역 오프셋과 일치하는지 확인하십시오.

5. DH__WRITER 에서 DMS 구독자를 제거합니다. 예:

```
sepmc -u DH__WRITER DMS__@dmsname
```

6. 다음과 같이 메시지 큐 구독자를 추가합니다.

```
sepmc -smc DH__WRITER -predefined ServerToServer -destination DMS
```

고급 정책 관리 클래스

CA Access Control 은 특수 클래스를 사용하여 DMS 에서 다음을 가능하게 합니다.

- 각 컴퓨터에 배포된 정책 상태의 최신 맵을 유지합니다.
- 끝점이 포함해야 할 관련 정책 배포 정보를 끝점이 가져올 수 있도록 DH 에 배포 정보를 보냅니다.

참고: 이러한 클래스가 포함하는 속성에 대한 자세한 내용은 *selang* 참조 안내서를 참조하십시오.

DEPLOYMENT 클래스

DEPLOYMENT 클래스의 각 개체는 정책 배포 작업을 나타냅니다. CA Access Control에서는 사용자가 호스트에 정책을 할당 또는 할당 취소하거나 정책을 직접 배포 또는 배포 취소할 때 DMS에서 배포 작업을 자동으로 작성합니다. 사용자가 정책이 할당된 호스트 그룹에서 호스트를 추가(할당) 또는 제거(할당 취소)하고, 호스트에서 정책을 다운그레이드 또는 업그레이드하고, 호스트를 재설정 또는 복원할 때에도 배포 작업이 작성됩니다.

끝점은 이 개체를 작업 지시로 사용하여 보류 중인 DEPLOYMENT 개체의 정보에 따라 정책 버전을 배포 또는 배포 취소합니다. 각 작업 지시는 한 끝점에만 사용되며 끝점에 배포하는 데 필요한 정책 버전 정보를 포함하고 있습니다. 또한 DEPLOYMENT 개체에는 배포의 성공 여부를 나타내는 상태 속성과 정책 배포 작업의 `selang` 명령 출력이 포함된 결과 속성(`result_message`)이 있습니다.

참고: 다른 할당 경로로 인해 HNODE에 이미 정책이 있는 경우에는 배포 작업이 비어 있을 수 있습니다(작업 없음 상태).

추가 정보:

[저장된 정책 버전 할당](#) (페이지 102)

[할당된 정책 할당 취소](#) (페이지 103)

[할당된 호스트를 특정 정책 버전으로 다운그레이드](#) (페이지 105)

GDEPLOYMENT 클래스

GDEPLOYMENT 클래스의 각 개체는 배포 패키지를 나타냅니다. 배포 패키지는 동일한 트랜잭션(정책 할당, 업그레이드 등)의 결과로 특정 호스트에 대해 작성되는 모든 배포 작업과 함께 DMS 및 그룹에 자동으로 작성됩니다. 즉, 사용자가 만드는 각 트랜잭션은 필요한 수만큼의 배포 작업을 생성하며(DEPLOYMENT 개체) 이들을 호스트별로 그룹화합니다(GDEPLOYMENT 개체).

배포 패키지는 정책 배포를 추적하고 문제를 해결할 수 있게 해주며 배포가 시작된 이유인 트리거를 기록합니다.

HNODE 클래스

HNODE 클래스의 각 개체는 회사 내에 있는 각 끝점을 나타냅니다. 이 개체에는 개체가 나타내는 특정 노드, 개체가 속한 호스트 그룹 및 개체가 마지막으로 온라인에서 검색된 시간에 대한 정보가 포함되어 있습니다. 또한 각 HNODE 개체에는 개체가 직접 또는 간접 할당을 통해 나타내는 노드에서 유효한 정책 버전과 각 정책의 상태(배포됨, 배포되었지만 오류 발생 등)에 대한 정보가 포함되어 있습니다.

HNODE 개체 이름은 실제 호스트 이름입니다. 예: myhost.mydomain.com

GHNODE 클래스

GHNODE 클래스의 각 개체는 CA Access Control 노드(HNODE 개체)의 그룹을 나타냅니다. 이 개체를 사용하면 정책을 배포하기 위해 끝점을 논리적 그룹으로 그룹화할 수 있습니다. 각 GHNODE 개체에는 개체가 나타내는 노드에 할당된 정책에 대한 정보가 포함되어 있습니다.

POLICY 클래스

POLICY 클래스의 각 개체는 호스트(HNODE 개체) 또는 호스트의 논리적 그룹(GHNODE 개체)에 배포할 수 있는 정책(GPOLICY 개체)의 버전을 나타냅니다. 이 개체에는 연관된 정책 스크립트가 저장되어 있는 위치(RULESET 개체) 및 개체를 배포해야 하는 노드 또는 노드 그룹에 대한 정보가 포함되어 있습니다.

이 개체의 이름은 정책 이름이며 버전 번호가 접미사로 사용됩니다(policy_name#xx).

GPOLICY 클래스

GPOLICY 클래스의 각 개체는 논리 정책을 나타냅니다. 이 개체에는 이 정책에 속한 정책 버전(POLICY 개체)과 개체가 할당된 호스트 및 호스트 그룹에 대한 정보가 포함되어 있습니다.

이 개체의 이름은 논리 정책 이름입니다.

RULESET 클래스

RULESET 클래스의 각 개체에는 정책 버전과 연관된 배포 스크립트와 배포 취소(제거) 스크립트가 모두 포함되어 있습니다.

이 개체의 이름은 각 POLICY 개체 이름에 따라 다릅니다.

호스트 및 호스트 그룹

고급 정책 관리를 사용하려면 기업의 CA Access Control 구현을 정의해야 합니다. 이렇게 하려면 끝점이나 호스트를 나타내는 HNODE 개체와 논리 호스트 그룹을 나타내는 GHNODE 개체를 작성합니다. 호스트는 해당 속성과 정책 요구에 따라 여러 논리 호스트 그룹의 구성원이 될 수 있습니다. 예를 들어 호스트에서 Red Hat 운영 체제와 Oracle 을 실행하는 경우 호스트는 기본 Red Hat 액세스 제어 정책을 가져오기 위한 Red Hat 논리 호스트 그룹의 구성원인 동시에 Oracle 액세스 제어 정책을 가져오기 위한 Oracle 논리 호스트 그룹의 구성원이 될 수 있습니다.

끝점을 기업의 호스트로 정의

끝점에 정책을 배포하고 해당 배포 상태를 표시하려면 DMS(Deployment Map Server)에서 기업 관리에 사용되는 끝점을 정의해야 합니다. 고급 정책 관리를 활성화하여 끝점에 CA Access Control 을 설치하면 끝점을 나타내는 HNODE 레코드가 DMS 에 자동으로 작성됩니다. 끝점에 CA Access Control 을 설치하기 전에 환경을 모델링하고자 하는 경우에만 DMS 에서 끝점을 수동으로 정의해야 합니다.

중요! HNODE 이름에는 정규화된 호스트 이름을 사용해야 합니다. 그렇지 않으면 끝점이 배포를 수집하지 않습니다.

끝점을 기업의 호스트로 정의하려면

1. CA Access Control 엔터프라이즈 관리에서 "정책 관리", "호스트" 하위 탭을 차례로 클릭하고 왼쪽에 있는 작업 메뉴에서 "호스트" 트리를 확장합니다.

사용 가능한 작업 목록에 "호스트 만들기" 작업이 나타납니다.

2. "호스트 만들기"를 클릭합니다.

"호스트 만들기: 호스트 검색" 화면이 나타납니다.

3. "호스트" 유형의 새 개체 만들기가 선택되었는지 확인하고 "확인"을 클릭합니다.

"호스트 만들기" 작업 페이지가 나타납니다.

4. 대화 상자에서 다음 필드를 채웁니다.

이름

끝점(HNODE 개체)의 이름을 정의합니다. 이 이름은 DMS 에서
고유해야 합니다(필수).

설명

(선택 사항) 호스트의 비즈니스 설명(자유 텍스트)을 정의합니다. 이
필드를 사용하여 끝점을 식별하는 데 도움이 되는 정보를
기록하십시오.

IP 주소

(선택 사항) 호스트의 IP 주소를 정의합니다.

5. "제출"을 클릭합니다.

작업이 성공적으로 제출되면 새 호스트(HNODE)가 만들어졌음을 알리는
메시지가 바로 나타납니다.

자동 호스트 그룹 할당이 작동하는 방법

고급 정책 관리를 활성화하여 CA Access Control 을 끝점에 설치하면 CA Access Control 엔터프라이즈 관리가 자동으로 호스트를 호스트 그룹에 할당합니다. CA Access Control 엔터프라이즈 관리는 호스트 유형, 운영 체제, 설치된 CA Access Control 버전 또는 정의하는 기타 일반 특성과 같은 기준에 기반하여 호스트를 호스트 그룹에 할당합니다. 그 이후에 호스트 그룹에 정책을 할당할 수 있습니다.

참고: Linux 끝점에 CA Access Control 을 설치하면 이 끝점은 자동으로 "모든 Linux 호스트" 호스트 그룹에 자동으로 할당됩니다. 이 끝점에 UNAB 를 설치하면 이 끝점도 "모든 UNAB 호스트" 호스트 그룹에 자동으로 할당됩니다.

CA Access Control 엔터프라이즈 관리는 다음 방법으로 호스트를 호스트 그룹에 자동으로 할당합니다.

1. 고급 정책 관리가 구성된 끝점은 엔터프라이즈 관리 서버로 하트비트를 보냅니다.

하트비트에는 끝점 특성에 대한 정보가 포함되어 있습니다.

2. 엔터프라이즈 관리 서버는 호스트 그룹 할당 조건에 대해 끝점 특성을 평가하고 호스트를 적절한 호스트 그룹에 할당합니다.

월드 뷰를 사용하여 각 호스트 그룹에 할당된 호스트를 볼 수 있습니다.

기본 제공되는 호스트 그룹

다음 표는 CA Access Control 엔터프라이즈 관리에서 기본 제공되는 호스트 그룹을 나타냅니다.

호스트 그룹 이름	설명
AIX 5.2	모든 AIX 5.2 호스트에 대한 기본 호스트 그룹
AIX 5.3	모든 AIX 5.3 호스트에 대한 기본 호스트 그룹
AIX 6.1	모든 AIX 6.1 호스트에 대한 기본 호스트 그룹

호스트 그룹 이름	설명
모든 Linux 호스트	모든 Linux 호스트에 대한 기본 호스트 그룹
모든 UNAB 호스트	모든 UNIX 호스트에 대한 기본 호스트 그룹
모든 Windows 호스트	모든 Windows 호스트에 대한 기본 호스트 그룹
ESX Server 3.x	모든 ESX Server 3.x 호스트에 대한 기본 호스트 그룹
ESX Server 4.x	모든 ESX Server 4.x 호스트에 대한 기본 호스트 그룹
HP-UX 11.23	모든 HP-UX 11.23 호스트에 대한 기본 호스트 그룹
HP-UX 11.31	모든 HP-UX 11.31 호스트에 대한 기본 호스트 그룹
RedHat 3	모든 RedHat 3 호스트에 대한 기본 호스트 그룹
RedHat 4	모든 RedHat 4 호스트에 대한 기본 호스트 그룹
RedHat 5	모든 RedHat 5 호스트에 대한 기본 호스트 그룹
SLES 9	모든 SLES 9 호스트에 대한 기본 호스트 그룹
SLES 10	모든 SLES 10 호스트에 대한 기본 호스트 그룹
SLES 11	모든 SLES 11 호스트에 대한 기본 호스트 그룹
Solaris 8	모든 Solaris 8 호스트에 대한 기본 호스트 그룹
Solaris 9	모든 Solaris 9 호스트에 대한 기본 호스트 그룹
Solaris 10	모든 Solaris 10 호스트에 대한 기본 호스트 그룹

호스트 그룹 이름	설명
Windows Server 2003	모든 Windows Server 2003 호스트에 대한 기본 호스트 그룹
Windows Server 2003 R2	모든 Windows Server 2003 R2 호스트에 대한 기본 호스트 그룹
Windows Server 2008	모든 Windows Server 2008 호스트에 대한 기본 호스트 그룹
Windows Server 2008 R2	모든 Windows Server 2008 R2 호스트에 대한 기본 호스트 그룹

자동 호스트 그룹 할당 조건 수정

CA Access Control 엔터프라이즈 관리는 미리 정의된 조건(예: 운영 체제 유형)을 사용하여 호스트 그룹에 호스트를 할당합니다. 기본적으로 CA Access Control 엔터프라이즈 관리는 호스트 운영 체제에 해당하는 호스트 그룹에 각 호스트를 자동으로 추가합니다. 예를 들어, CA Access Control 엔터프라이즈 관리는 Windows Server 2003 R2 호스트를 모든 Windows 호스트 및 Windows Server 2003 R2 호스트 그룹에 추가합니다. CA Access Control 엔터프라이즈 관리가 호스트를 호스트 그룹에 추가하기 위해 사용하는 조건을 추가로 지정할 수 있습니다.

자동 호스트 그룹 할당 조건을 수정하려면

1. 엔터프라이즈 관리 서버에서 **selang** 창을 열고 DMS 에 연결합니다.
2. 다음 **selang** 명령을 사용하여 호스트 그룹을 편집하고 할당 조건을 지정합니다.

```
editres GHNODE host_group_name criteria+(attribute=value)
editres GHNODE host_group_name criteria+(attribute!=value)
editres GHNODE host_group_name criteria+(attribute=value)&&(attribute=value)
editres GHNODE host_group_name criteria+(attribute1=value1)
editres GHNODE host_group_name criteria+(attribute2=value2)
editres GHNODE host_group_name criteria-(attribute=value)
```

host_group_name

이 조건을 할당하는 호스트 그룹의 이름을 지정합니다.

attribute=value

호스트 그룹 할당 특성 및 값을 지정합니다. 이 매개 변수를 다음 값을 가질 수 있습니다.

HNODE_IP=IP_address

CA Access Control 엔터프라이즈 관리가 정의된 IP 주소를 호스트 그룹 할당 조건에 추가하도록 지정합니다.

예: HNODE_IP=172.24.123.456

NODE_TYPE={AC Windows | AC UNIX | AC UNAB}

CA Access Control 엔터프라이즈 관리가 지정된 끝점 유형을 호스트 그룹 할당 조건에 추가하도록 지정합니다.

HNODE_VERSION={ACW | ACU | ACUNAB}:version

CA Access Control 엔터프라이즈 관리가 정의된 끝점 버전을 호스트 그룹 할당 조건에 추가하도록 지정합니다.

예: HNODE_VERSION=ACW:12.53

이 예는 CA Access Control 엔터프라이즈 관리가 CA Access Control Windows 끝점 버전 12.53.1178을 호스트 그룹 할당 조건에 추가하도록 지정합니다.

ATTRIBUTES=("attribute")

CA Access Control 엔터프라이즈 관리가 정의된 특성 정보를 호스트 그룹 할당 조건에 추가하도록 지정합니다.

예: ATTRIBUTES=(Microsoft_Windows_Server_2003_R2)

참고: 값 필드에 별표를 지정할 수 있습니다.

지정된 호스트 그룹의 할당 조건을 수정했습니다.

예: 버전을 기준으로 호스트를 그룹에 할당

이 예에서는 "All Windows 12.53 Hosts"란 이름의 호스트 그룹의 할당 조건을 수정하여 CA Access Control 버전 12.53 을 설치한 이러한 Windows 호스트만 자동으로 할당하도록 만듭니다.

```
editres GHNODE ("All Windows 12.53 hosts") criteria+(HNODE_VERSION=ACW:12.53)
```

예: 유형 및 버전을 기준으로 호스트를 그룹에 할당

이 예에서는 유형(ACUNIX) 및 CA Access Control 버전을 기준으로 호스트를 자동 할당하도록 "All UNIX hosts"란 이름의 호스트 그룹의 할당 조건을 수정합니다.

```
editres GHNODE ("All UNIX hosts") criteria+(NODE_TYPE=AC
UNIX&&HNODE_VERSION=ACU:12.53)
```

예: 유형 또는 버전을 기준으로 호스트를 그룹에 할당

이 예에서는 유형(UNAB) 또는 UNAB 버전을 기준으로 호스트를 자동 할당하도록 "All UNAB Hosts"란 이름의 호스트 그룹의 할당 조건을 수정합니다.

```
editres GHNODE ("All UNAB Hosts") criteria+(NODE_TYPE=ACUNAB)
editres GHNODE ("All UNAB Hosts") criteria+(HNODE_VERSION=ACUNAB:12.53)
```

예: 유형을 기준으로 호스트 제외

이 예에서는 AC UNIX 유형의 모든 호스트를 자동으로 제외하도록 "Non UNIX Hosts"란 이름의 호스트 그룹의 할당 조건을 수정합니다.

```
editres GHNODE ("Non UNIX Hosts") criteria+(NODE_TYPE!=AC UNIX)
```

예: 할당된 조건 제거

이 예에서는 이전에 "All Windows Hosts"란 이름의 호스트 그룹에 할당한 NODE_TYPE 조건을 제거합니다.

```
editres GHNODE ("All Windows Hosts") criteria-(NODE_TYPE=AC Windows)
```

참고: 호스트의 유효한 특성을 표시하기 위해 DMS 감사 파일을 보고 호스트 하트비트를 찾을 수 있습니다. DMS 감사 파일을 표시하려면 `seaudit -a -fn pmd.audit` 명령을 사용하십시오.

논리 호스트 그룹 정의

관련 끝점 그룹에서 정책을 관리하려면 끝점을 논리 호스트 그룹으로 정의하고 전체 그룹에서 고급 정책 관리 작업을 수행하십시오. 의미 있는 호스트 그룹을 작성하려면 먼저 DMS에서 끝점을 정의해야 합니다.

참고: 이 절차에서는 CA Access Control 엔터프라이즈 관리를 사용하여 DMS에서 논리 호스트 그룹을 정의하는 방법에 대해 설명합니다.

논리 호스트 그룹을 정의하려면

1. CA Access Control 엔터프라이즈 관리에서 "정책 관리", "호스트" 하위 탭을 차례로 클릭하고 왼쪽에 있는 작업 메뉴에서 "호스트 그룹" 트리를 확장합니다.

사용 가능한 작업 목록에 "호스트 그룹 만들기"가 나타납니다.

2. "호스트 그룹 만들기"를 클릭합니다.

"호스트 그룹 만들기: 호스트 그룹 검색" 화면이 나타납니다.

3. "호스트 그룹" 유형의 새 개체 만들기가 선택되었는지 확인하고 "확인"을 클릭합니다.

"호스트 그룹 만들기" 작업 페이지가 나타납니다.

4. 대화 상자에서 다음 필드를 채웁니다.

이름

논리 호스트 그룹(GHNODE 개체)의 이름을 정의합니다.

설명

(선택 사항) 호스트 그룹의 비즈니스 설명(자유 텍스트)을 정의합니다. 이 필드를 사용하여 호스트 그룹을 식별하는 데 도움이 되는 정보를 기록하십시오.

5. "호스트 선택"을 클릭한 다음 "추가"를 클릭합니다.

"구성원 추가" 대화 상자가 나타납니다.

6. 호스트 그룹에 추가할 끝점을 선택하고 "선택"을 클릭합니다.

"구성원 추가" 대화 상자가 닫히고 선택한 끝점이 정의 중인 논리적 그룹 호스트의 "구성원 목록"에 추가됩니다.

7. "제출"을 클릭합니다.

작업이 성공적으로 제출되면 새 그룹 호스트(GHNODE)가 만들어졌음을 알리는 메시지가 바로 나타납니다.

호스트 그룹 가져오기

호스트 그룹을 가져오면 기존 PMDB 구조를 고급 정책 관리로 마이그레이션하는 데 도움이 됩니다. 호스트 그룹을 가져올 때는 호스트 그룹에 호스트를 만들거나 호스트를 조인합니다. 호스트는 PMDB의 구독자에 해당합니다.

참고: 고급 정책 관리는 계층적 호스트 그룹을 지원하지 않습니다. PMDB에서 호스트 그룹을 가져올 때는 모든 구독자의 계층을 동일한 호스트 그룹으로 단일화합니다. CA Access Control 엔터프라이즈 관리는 구독자 PMDB에 해당하는 호스트를 만들지 않습니다.

호스트 그룹에 조인하는 각 PMDB 구독자에 대해 CA Access Control 엔터프라이즈 관리는 구독자에 해당하는 호스트(HNODE 개체)가 이미 DMS에 있는지 여부를 확인합니다. 해당 호스트가 DMS에 있으면 CA Access Control은 이 호스트를 호스트 그룹에 추가합니다. 해당 호스트가 DMS에 없으면 CA Access Control은 새 호스트를 만들어 호스트 그룹에 추가합니다.

액세스 권한이 없는 끝점은 마법사에 표시되지 않으며 해당 호스트를 호스트 그룹에 추가할 수 없습니다.

호스트 그룹을 가져오려면

1. CA Access Control 엔터프라이즈 관리에서 다음을 수행합니다.
 - a. "정책 관리"를 클릭합니다.
 - b. "호스트" 하위 탭을 클릭합니다.
 - c. 작업 메뉴에서 왼쪽에 있는 "호스트 그룹" 트리를 확장합니다.
사용 가능한 작업 목록에 "호스트 그룹 가져오기" 작업이 나타납니다.

2. "호스트 그룹 가져오기"를 클릭합니다.

PMDB 호스트 로그인 페이지가 나타납니다.

3. 사용자 이름, 암호, PMDB 이름을 입력한 다음 "로그인"을 클릭합니다.

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

"일반" 작업 단계에 "호스트 그룹 가져오기" 마법사가 나타납니다.

4. 마법사를 완료하고 요약을 읽은 후에 "마침"을 클릭합니다.

CA Access Control 이 호스트를 호스트 그룹에 추가합니다. DMS 에 호스트가 없으면 CA Access Control 은 호스트를 호스트 그룹(GHNODE)에 추가하기 전에 호스트에 대한 HNODE 개체를 만듭니다.

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

할당 경로

할당 경로는 특정 호스트나 호스트 그룹에 대한 정책 할당을 설명합니다. 정책은 다음과 같은 두 가지 경로로 호스트에 할당할 수 있습니다.

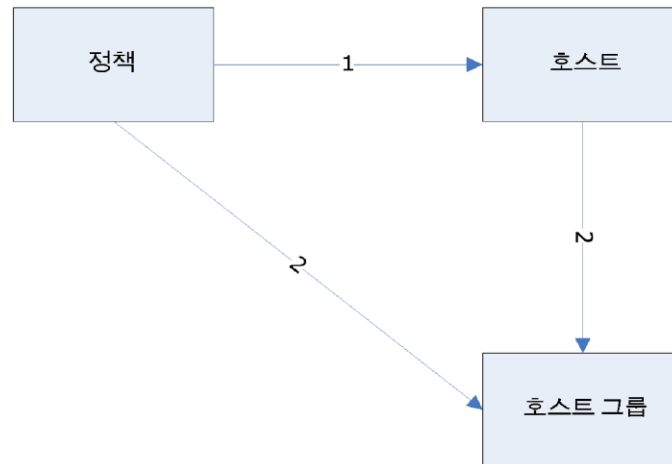
- 정책이 호스트에 직접 할당됩니다.
- 정책이 호스트가 구성원인 호스트 그룹에 할당됩니다.
- 호스트가 하나 이상의 정책이 할당된 호스트 그룹에 조인됩니다.

할당 경로는 여러 개일 경우 다음과 같이 고급 정책 관리에 영향을 미치기 때문에 중요합니다.

- 할당 경로를 하나 제거해도 호스트와 정책 사이에 다른 할당 경로가 있기 때문에 CA Access Control 이 정책을 배포 취소하지 않습니다.
- 할당 경로를 추가하면 추적 및 관리 용도로 배포 패키지와 배포 작업이 생성됩니다. 그러나 배포 작업의 상태는 *작업 없음*이므로 끝점에서 정책 배포가 시작되지 않습니다.

예: 정책 IIS 에 대한 다중 할당 경로

다음 그림은 정책 IIS 에 대한 다중 할당 경로의 예를 설명합니다. 호스트 host1.comp.com 은 호스트 그룹 "Servers"의 구성원입니다. 경로 1 은 정책 IIS 를 호스트 host1.comp.com 에 직접 할당할 때의 할당 경로입니다. 경로 2 는 정책 IIS 를 호스트 그룹 "Servers"에 할당할 때의 할당 경로입니다.



예: 할당 경로 제거

앞의 그림에서 정책 IIS 는 호스트 그룹 "Servers" 및 호스트 host1.comp.com 에 할당되었습니다. "Servers" 호스트 그룹에서 host1.comp.com 을 제거하면 경로 2 가 제거됩니다. 하지만 CA Access Control 은 정책 IIS 가 아직 호스트(경로 1)에 직접 할당되어 있으므로 host1.comp.com 에서 정책 IIS 를 배포 취소하지 않습니다.

정책 생성 및 배포 방법

고급 정책 기반 관리를 사용하여 정책의 초안 버전을 저장하고 필요에 따라 검토 및 수정한 다음 승인된 버전을 배포할 수 있습니다.

CA Access Control 엔터프라이즈 관리를 사용하여 승인된 정책 버전을 배포하려면 다음 작업을 수행하십시오.

1. 정책 버전을 DMS 에 저장합니다.

정책 버전을 저장한 다음 정책을 검토하고 배포할 수 있습니다.

2. 정책을 검토합니다.

정책 버전이 저장된 이후에는 검토한 정책과 관련된 규칙이 있어야 합니다.

3. 정책을 완료합니다.

정책을 완료한 후에는 정책을 배포할 호스트 및 호스트 그룹에 정책을 할당할 수 있습니다.

4. 사용 가능한 할당 경로 중 하나를 통해 정책을 끝점에 할당합니다.

- 저장된 정책을 호스트 또는 호스트 그룹에 할당합니다.
- 정책이 이미 할당된 호스트의 논리 그룹에 호스트를 할당합니다.

정책이 할당되면 **CA Access Control** 은 최근에 완료된 정책 버전을 배포하기 위한 작업을 자동으로 수행합니다.

참고: UNAB 로그인과 구성 정책을 만들고 배포하려면 다른 프로세스를 따르십시오.

추가 정보:

[UNAB 로그인 권한 부여 관리](#) (페이지 315)

[UNAB 호스트 또는 호스트 그룹 구성](#) (페이지 317)

[할당 경로](#) (페이지 90)

관리 요구 사항

DMS 에 정책을 저장하거나 이러한 정책을 할당하려면 사용자 및 사용자가 작업 중인 컴퓨터에 적절한 사용 권한이 있어야 합니다.

DMS 에 정책을 저장하려면

- DMS 를 관리하고 있는 *컴퓨터*나 **policydeploy** 유틸리티를 실행하고 있는 컴퓨터에 DMS 에 대한 터미널 권한(**TERMINAL** 클래스)이 있어야 합니다.
- *사용자*는 DMS 의 **POLICY**, **GPOLICY** 및 **RULESET** 클래스에 대해 하위 관리 권한이 있어야 합니다.

호스트 또는 호스트 그룹에 정책을 할당하려면:

- DMS 를 관리하는 데 사용하는 *컴퓨터*에 DMS 에 대한 터미널 권한(TERMINAL 클래스)이 있어야 합니다.
- *사용자*는 DMS 의 DEPLOYMENT, GDEPLOYMENT, POLICY, GPOLICY, HNODE 및 GHNODE(호스트 그룹에 정책을 할당하는 경우) 클래스에 대해 하위 관리 권한이 있어야 합니다.

참고: 터미널 권한 및 하위 관리 권한에 대한 자세한 내용은 *UNIX 용 끝점 관리 안내서* 및 *Windows 용 끝점 관리 안내서*를 참조하십시오.

정책 종속성

고급 정책 관리를 사용하면 정책이 배포 또는 배포 취소되는 순서를 적용할 수 있습니다.

정책 종속성을 사용하면 하나 이상의 다른 정책에 종속된 정책이 필수 정책이 배포될 때까지 배포되지 않도록 정의할 수 있습니다. 마찬가지로 의존적인 정책이 하나 이상 배포되어 있는 경우에는 필수 구성 요소 정책을 배포 취소할 수 없습니다.

정책을 만들거나 수정할 때 정책 종속성을 정의합니다.

정책 확인

정책 확인이 활성화되면 CA Access Control 은 정책을 배포하기 전에 정책에 오류가 없는지 검사합니다. CA Access Control 이 정책 배포 스크립트에서 오류를 발견하면 이 정책 스크립트는 끝점에서 실행되지 않습니다. 이렇게 하면 오류 있는 정책이 배포되지 않고 끝점에서 스크립트 오류를 추적할 수 있게 됩니다. 정책 확인은 기본적으로 비활성화되어 있습니다.

정책 확인이 활성화되어 있지 않을 때 오류 있는 정책이 배포되는 경우 다른 명령의 오류에도 불구하고 일부 정책 명령이 여전히 실행될 수 있습니다.

정책 확인은 CA Access Control 데이터베이스 명령(AC 환경의 `selang` 명령)만 검사합니다. 정책 확인은 네이티브, 구성, 정책 모델 환경에서 명령을 검사하지 않습니다. 정책에 AC 환경의 명령과 다른 환경의 명령이 모두 포함되어 있으면 정책 확인은 AC 환경의 명령만 검사합니다.

정책 확인은 배포 취소 스크립트를 검사할 수 없습니다.

정책 확인 작동 방법

정책 확인 기능은 끝점에 실제로 정책을 배포하기 전에 오류가 없는지 확인합니다.

참고: 정책 확인은 기본적으로 활성화되어 있지 않습니다.

다음 프로세스는 정책 확인의 작동 방법을 설명한 것입니다.

1. 사용자가 호스트 또는 호스트 그룹에 정책을 할당합니다.
2. 각 끝점에서 CA Access Control 엔터프라이즈 관리는 정책을 확인합니다.
3. 다음 중 *한 가지* 결과가 나타납니다.

- 정책에 오류가 없으면 CA Access Control 엔터프라이즈 관리가 정책을 끝점에 배포합니다.

끝점은 정책 상태가 *배포됨*인 DMS 를 업데이트합니다.

- 정책 스크립트에 오류가 있으면 CA Access Control 엔터프라이즈 관리는 정책을 끝점에 배포하지 *않습니다*.

끝점은 정책 상태가 *실행되지 않음*인 DMS 를 업데이트합니다.

DMS 는 또한 스크립트 오류가 있는 정책에 해당하는 각 배포 작업의 상태를 *실패*로 업데이트합니다.

참고: CA Access Control 엔터프라이즈 관리의 배포 감사 기능을 사용하여 오류가 있는 스크립트를 볼 수 있습니다.

정책 확인 활성화

정책 확인은 끝점에서 정책이 실제로 배포되기 전에 정책이 오류 없이 배포될 수 있도록 합니다.

정책 확인을 활성화하려면 `policyfetcher` 섹션의 `policy_verification` 구성 설정 값을 1로 설정하십시오.

정책 확인이 활성화됩니다.

정책 버전 생성 및 저장

만들어 DMS 에 저장하는 모든 정책에는 자동으로 버전 번호가 지정됩니다. 처음 정책을 저장하면 버전 번호 "01"이 지정됩니다. 예를 들어 정책 *myPolicy* 를 처음 저장할 때 CA Access Control 엔터프라이즈 관리는 *myPolicy* 라는 GPOLICY 개체와 *myPolicy#01* 이라는 POLICY 개체를 만듭니다. DMS 에 이미 있는 정책을 저장할 때마다 저장된 최신 정책 버전이 한 버전씩 증가하면서 새로운 정책 버전이 작성됩니다. 예를 들어 *myPolicy* 버전을 28 번째 저장할 때 CA Access Control 엔터프라이즈 관리는 *myPolicy#28* 이라는 POLICY 개체를 작성합니다.

참고: 이 절차에서는 CA Access Control 엔터프라이즈 관리를 사용하여 정책 버전을 만들고 저장하는 방법에 대해 설명합니다. 이 절차는 UNAB 로그인 및 구성 정책에는 적용되지 않습니다.

정책 버전을 만들어 저장하려면

1. (선택 사항) *selang* 배포 명령을 사용하여 새 스크립트 파일을 작성합니다.

이러한 명령은 기업의 끝점에 배포할 정책을 구성하는 데 필요한 명령입니다.

중요! 정책 배포에서는 사용자 암호를 설정하는 명령을 지원하지 않으므로 배포 스크립트 파일에 이러한 명령을 포함시키지 마십시오. 기본 *selang* 명령이 지원되지만 위반 보고서에는 표시되지 않습니다.
2. (선택 사항) *selang* 배포 취소 명령을 사용하여 새 스크립트 파일을 작성합니다.

이러한 명령은 기업의 끝점에서 정책을 배포 취소(제거)하는 데 필요한 명령입니다.
3. CA Access Control 엔터프라이즈 관리에서 "정책 관리", "정책" 작업을 차례로 클릭하고 왼쪽에 있는 작업 메뉴에서 "정책" 트리를 확장합니다. 정책 작업이 나타납니다.
4. "정책 만들기"를 클릭합니다.

"정책 만들기: 정책 검색" 화면이 나타납니다.

참고: 기존 정책에 대한 새 버전을 작성하려면 대신 "정책 수정"을 클릭하고 수정할 정책을 검색합니다.
5. "확인"을 클릭합니다.

"정책 만들기" 작업 페이지가 나타납니다.

6. 대화 상자에서 다음 필드를 채웁니다.

이름

정책(GPOLICY 개체)의 이름을 정의합니다. 이 이름은 DMS 및 기업에서 고유해야 합니다. DMS의 경우 이 사항이 강제 적용되며, 기업의 경우 강제 적용되지 않지만 동일한 이름의 정책이 이미 있으면 정책을 호스트에 배포할 수 없습니다.

설명

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

7. "정책 스크립트" 탭을 클릭하고 다음 방법 중 *하나*를 사용하여 배포 및 배포 취소 스크립트를 제공합니다.
- 배포 및 배포 취소 스크립트를 해당 필드에 입력합니다.
배포 명령으로 스크립트 파일을 작성하지 않은 경우 이 옵션을 사용합니다.
 - 기존 **selang** 스크립트 파일에서 명령을 로드합니다.
 - a. "찾아보기"를 클릭하고 사용할 **selang** 스크립트가 포함된 파일을 찾습니다.
 - b. "로드"를 클릭하여 스크립트 필드를 선택한 파일의 내용으로 채웁니다.
8. (선택 사항) 이 정책 버전에 대한 설명을 제공합니다.
이 옵션을 사용하여 이 정책 버전에 사용할 배포 스크립트에 대한 특정 정보를 제공합니다.
9. (선택 사항) "제출 시 완료"를 선택합니다.
이 옵션은 작성한 새 정책을 배포할 수 있도록 지정합니다. 배포 스크립트 작성을 완료하지 않은 경우에는 이 옵션의 선택을 취소합니다.
- 참고:** 이 옵션을 선택하지 않으면 새 정책 버전을 작성하지 않고 배포 스크립트를 수정할 수 있습니다. 그러나 완료되지 않은 정책 버전은 배포할 수 없습니다.
10. "정책 종속성" 탭을 클릭한 다음 "추가"를 클릭합니다.
"구성원 추가" 대화 상자가 나타납니다.

11. 정책에 대한 사전 요구 사항으로 추가할 정책을 선택한 다음 "선택"을 클릭합니다.

"구성원 추가" 대화 상자가 닫히고 선택한 정책이 생성 중인 정책의 "구성원 목록"에 추가됩니다.

12. "제출"을 클릭합니다.

작업이 성공적으로 제출되면 새 정책 버전이 만들어졌음을 알리는 메시지가 바로 나타납니다. UNAB 로그인과 구성 정책을 만들고 배포하려면 다른 프로세스를 따르십시오.

참고: 또한 `policydeploy` 유틸리티를 사용하여 이 작업을 수행할 수도 있습니다. `policydeploy` 유틸리티에 대한 자세한 내용은 [참조 안내서](#)를 참조하십시오.

추가 정보:

[UNAB 로그인 권한 부여 관리](#) (페이지 315)

[UNAB 호스트 또는 호스트 그룹 구성](#) (페이지 317)

변수를 정의하는 정책 만들기

변수를 정의하는 정책을 만들어 배포하면 동일한 변수를 여러 끝점에서 정의할 수 있습니다.

변수를 정의하는 정책을 만들려면

1. 변수를 정의하는 `selang` 배포 명령을 사용하여 스크립트 파일을 만듭니다. 다음 `selang` 명령을 사용하여 각 변수를 정의합니다.

```
editres ACVAR ("variable_name") value("variable_value")
```

2. (선택 사항) 변수를 사용하는 `selang` 명령을 스크립트 파일에 추가합니다.

참고: 정책의 이후 규칙에서 변수를 참조하려면 정책의 각 변수를 정의해야 합니다. 변수를 참조할 때는 다음 형식을 사용하십시오:
`"<!variable>"`

3. 정책을 DMS에 저장합니다.

예: 변수를 정의하는 정책 만들기

이 예에서 다음 정책은 값이 `/opt/jboss` 이고 이름이 `jboss_home` 인 변수를 정의하고, 사용자 `Mark` 가 `JBoss` 를 통해 액세스하는 `/opt` 디렉터리에 있는 모든 리소스에 액세스하도록 허용하는 규칙을 만듭니다.

```
editres ACVAR ("jboss_home") value("/opt/jboss")
authorize FILE /opt/* uid(Mark) access(all) via(pgm("<jboss_home>/jboss"))
```

끝점이 정책을 컴파일할 때 다음과 같은 규칙을 만듭니다.

```
authorize FILE /opt/* uid(Mark) access(all) via(pgm(/opt/jboss/jboss))
```

예: 여러 변수 값을 정의하는 정책 만들기

다음 정책은 다음과 같이 값이 `C:\JBoss` 이고 이름이 `jboss_home` 인 변수를 정의하고, `C:\Program Files\JBoss` 값을 `jboss_home` 변수에 추가하고, 액세스 규칙을 만듭니다.

```
editres ACVAR ("jboss_home") value("C:\JBoss")
editres ACVAR ("jboss_home") value+("C:\Program Files\JBoss")
editres FILE ("<jboss_home>\bin") defacc(none) audit(a)
```

끝점이 정책을 컴파일할 때 다음과 같은 규칙을 만듭니다.

```
editres FILE ("C:\JBoss\bin") defacc(none) audit(a)
editres FILE ("C:\Program Files\JBoss\bin") defacc(none) audit(a)
```

예: 변수를 사용하여 동일한 정책을 Windows 및 UNIX 끝점에 배포

다음 예는 운영 체제에서 JBoss 설치 위치가 다른 경우에도 변수를 사용하여 동일한 JBoss 정책을 Windows 및 UNIX 끝점에 배포하는 방법을 설명합니다. 이 예는 각 운영 체제에서 JBoss 설치 위치를 정의하는 두 개의 `jboss_home` 변수를 정의합니다.

1. 각 운영 체제의 JBoss 설치 위치를 정의하는 두 개의 `jboss_home` 변수를 정의합니다.

- Windows 에서 JBoss 설치 위치를 정의하는 정책을 만들어 Windows 끝점에 배포합니다.

```
editres ACVAR ("jboss_home") value("C:\JBoss")
```

- UNIX 에서 JBoss 설치 위치를 정의하는 정책을 만들어 UNIX 끝점에 배포합니다.

```
editres ACVAR ("jboss_home") value("/opt/jboss")
```

2. JBoss 설치 위치를 보호하기 위해 `jboss_home` 변수를 사용하는 정책을 만들어 Windows 및 UNIX 끝점에 배포합니다.

```
editres FILE "<!jboss_home>" defacc(none) audit(all)
```

- Windows 끝점이 이 정책을 컴파일할 때 다음 규칙을 만듭니다.

```
editres FILE "C:\JBoss" defacc(none) audit(all)
```

- UNIX 끝점이 이 정책을 컴파일할 때 다음 규칙을 만듭니다.

```
editres FILE "/opt/jboss" defacc(none) audit(all)
```

정책과 연관된 규칙 보기

DMS 에 정책이 저장되면 각 정책 버전에 대한 배포 및 배포 취소 스크립트에서 규칙을 볼 수 있습니다.

정책과 연관된 규칙을 보려면

1. CA Access Control 엔터프라이즈 관리에서 "정책 관리", "정책" 하위 탭을 차례로 클릭하고 왼쪽에 있는 작업 메뉴에서 "정책" 트리를 확장합니다. 정책 작업이 나타납니다.
2. "정책 보기"를 클릭합니다.
"정책 보기: 정책 검색" 화면이 나타납니다.

3. 검색 범위를 정의하고 "검색"을 클릭합니다.
정의한 검색 범위와 일치하는 정책 목록이 나타납니다.
4. 볼 정책을 선택하고 "선택"을 클릭합니다.
"정책 보기: *policyName*" 페이지가 나타납니다. 다양한 탭에서 정책 이름 및 설명, 최신 버전의 배포 및 배포 취소 스크립트, 이 정책에 대해 존재하는 모든 정책 버전 목록, 모든 정책 종속성, 정책 작성 및 업데이트 이벤트에 대한 일반적인 정보를 비롯한 정책 속성을 볼 수 있습니다.
5. 버전 기록 탭을 누릅니다.
정책 버전 목록이 나타나고 각 버전에는 배포 및 배포 취소 스크립트 링크가 포함되어 있습니다.
6. 다음 중 하나를 수행합니다.
 - "배포 스크립트" 링크를 클릭합니다.
배포 스크립트가 포함된 팝업 창이 나타납니다.
 - "배포 취소 스크립트" 링크를 클릭합니다.
배포 취소 스크립트가 포함된 팝업 창이 나타납니다.

참고: 또한 `policydeploy` 유틸리티를 사용하여 이 작업을 수행할 수도 있습니다. `policydeploy` 유틸리티에 대한 자세한 내용은 [참조 안내서](#)를 참조하십시오.

정책 가져오기

정책을 가져올 때 CA Access Control 엔터프라이즈 관리는 로컬 CA Access Control 데이터베이스 또는 PMDB에서 `selang` 규칙을 내보내 DMS에 이 규칙을 포함하는 정책을 만들어 저장합니다. 이렇게 하면 한 끝점을 보호하는 규칙을 여러 끝점을 보호할 수 있는 정책으로 변환할 수 있으므로 PMDB를 고급 정책 관리로 마이그레이션하는 데 도움이 됩니다.

참고: 규칙을 내보내는 끝점 또는 PMDB는 CA Access Control r12.0 이상이 설치된 호스트에 있어야 합니다. 이전 CA Access Control 버전에서 정책을 가져오려면 우선 끝점을 업그레이드하십시오.

정책을 가져오려면

1. CA Access Control 엔터프라이즈 관리에서 다음을 수행합니다.

- a. "정책 관리"를 클릭합니다.
- b. "정책" 하위 탭을 클릭합니다.
- c. 작업 메뉴에서 왼쪽에 있는 "정책" 트리를 확장합니다.

사용 가능한 작업 목록에 "정책 가져오기" 작업이 나타납니다.

2. "정책 가져오기"를 클릭합니다.

"호스트 로그인" 페이지가 나타납니다.

3. 사용자 이름, 암호, 규칙을 내보낼 원본 PMDB 또는 호스트의 이름을 입력한 다음 "로그인"을 클릭합니다.

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

"일반" 작업 단계에 "정책 가져오기 프로세스" 마법사가 나타납니다.

4. 다음 필드를 완성하고 "다음"을 클릭합니다.

이름

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

설명

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

정책 클래스

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

종속된 클래스 내보내기

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

"정책 스크립트" 단계가 나타납니다.

5. 내보낸 규칙을 검토하고 필요한 경우 이 규칙을 수정한 후 "다음"을 클릭합니다.
"요약" 단계가 나타납니다.
6. "마침"을 클릭합니다.
정책이 만들어집니다.

저장된 정책 버전 할당

특정 호스트나 호스트 그룹에 정책의 완료된 최신 버전을 할당할 수 있습니다. 할당된 정책은 자동으로 배포되며 **DMS** 에서 해당 상태를 모니터링할 수 있습니다.

참고: 이 절차는 로그인 및 구성 정책에는 적용되지 않습니다.

저장된 정책 버전을 할당하려면

1. **CA Access Control** 엔터프라이즈 관리에서 "정책 관리", "정책" 하위 탭을 차례로 클릭하고 왼쪽에 있는 작업 메뉴에서 "할당" 트리를 확장한 다음 "정책 할당"을 클릭합니다.
정책 선택 작업 단계에서 "정책 할당" 마법사가 나타납니다.
2. 마법사를 완료하고 요약을 읽은 후에 "마침"을 클릭합니다.
CA Access Control 이 정책 할당 작업을 제출합니다. 정책이 호스트에 직접 할당되거나 논리 호스트 그룹 구성원을 통해 할당되면 **CA Access Control**에서는 검색할 각 호스트에 대해 **DEPLOYMENT** 작업을 생성합니다.

참고: 또한 **policydeploy** 유틸리티를 사용하여 이 작업을 수행할 수도 있습니다. **policydeploy** 유틸리티에 대한 자세한 내용은 *참조 안내서*를 참조하십시오.

정책 유지 관리

배포된 정책에 대해 다음 작업을 수행할 수 있습니다.

- 할당된 호스트에서 정책 할당 취소
- 호스트를 최신 정책 버전으로 업그레이드
- 호스트를 이전 정책 버전으로 다운그레이드
- 배포된 정책의 오류 검사
- 정책 또는 정책 버전 삭제

이러한 작업은 CA Access Control 엔터프라이즈 관리에서 수행하거나 `policydeploy` 유틸리티를 사용하여 수행합니다.

할당된 정책 할당 취소

특정 호스트에서 또는 호스트 그룹으로 할당된 정책을 할당 취소할 수 있습니다. 할당 취소된 정책은 자동으로 배포 취소됩니다.

할당된 정책을 할당 취소하려면

1. CA Access Control 엔터프라이즈 관리에서 "정책 관리", "정책" 하위 탭을 차례로 클릭하고 왼쪽에 있는 작업 메뉴에서 "할당" 트리를 확장한 다음 "정책 할당 취소"를 클릭합니다.

정책 선택 작업 단계에서 "정책 할당 취소" 마법사가 나타납니다.

2. 마법사를 완료하고 요약을 읽은 후에 "마침"을 클릭합니다.

CA Access Control 이 정책 할당 작업을 제출합니다. 정책이 호스트에서 직접 할당 취소되거나 논리 호스트 그룹 구성원을 통해 할당 취소되면 CA Access Control에서는 검색할 각 호스트에 대해 DEPLOYMENT 작업을 생성합니다.

참고: 또한 `policydeploy` 유틸리티를 사용하여 이 작업을 수행할 수도 있습니다. `policydeploy` 유틸리티에 대한 자세한 내용은 [참조 안내서](#)를 참조하십시오.

할당된 호스트를 최신 정책 버전으로 업그레이드

새 정책 버전은 할당된 호스트나 정책이 배포된 호스트로 자동으로 전송되지 않습니다. 정책이 배포된 호스트를 최신 정책 버전으로 수동으로 업그레이드하십시오.

중요! 최신 정책 버전으로 업그레이드하면 이전 버전의 정의된 사용자, 그룹, 리소스는 삭제됩니다.

다음 단계를 수행하십시오.

1. CA Access Control 엔터프라이즈 관리에서 "정책 관리", "정책"을 클릭하고 왼쪽에 있는 태스크 메뉴에서 "할당" 트리를 확장한 다음 "정책 업그레이드"를 클릭합니다.

정책 선택 작업 단계에서 "정책 업그레이드" 마법사가 나타납니다.

2. 마법사를 완료하고 요약을 읽은 후에 "마침"을 클릭합니다.

CA Access Control 이 정책 업그레이드 작업을 제출합니다. 호스트의 정책을 업그레이드하기 위해 CA Access Control 에서는 검색할 호스트에 대해 DEPLOYMENT 작업을 생성합니다.

참고: 업그레이드할 호스트 그룹을 선택할 때 CA Access Control 엔터프라이즈 관리는 배포된 정책의 오래된 버전이 있는 호스트를 수록한 호스트 그룹에서만 선택할 수 있게 합니다.

참고: 또한 `policydeploy` 유틸리티를 사용하여 이 작업을 수행할 수도 있습니다. `policydeploy` 유틸리티에 대한 자세한 내용은 [참조 안내서](#)를 참조하십시오.

할당된 호스트를 특정 정책 버전으로 다운그레이드

잘못된 정책 버전을 하나 이상의 호스트에 실수로 할당했거나 특정 호스트에서 이전 정책 버전으로 돌아가려는 경우 정책을 다운그레이드할 수 있습니다.

할당된 호스트를 특정 정책 버전으로 다운그레이드하려면

1. CA Access Control 엔터프라이즈 관리에서 "정책 관리", "정책" 하위 탭을 차례로 클릭하고 왼쪽에 있는 작업 메뉴에서 "할당" 트리를 확장한 다음 "정책 다운그레이드"를 클릭합니다.

정책 선택 작업 단계에서 "정책 다운그레이드" 마법사가 나타납니다.

2. 마법사를 완료하고 요약을 읽은 후에 "마침"을 클릭합니다.

CA Access Control 이 정책 다운그레이드 작업을 제출합니다. 호스트의 정책을 다운그레이드하기 위해 CA Access Control에서는 검색할 호스트에 대해 DEPLOYMENT 작업을 생성합니다.

참고: 또한 `policydeploy` 유틸리티를 사용하여 이 작업을 수행할 수도 있습니다. `policydeploy` 유틸리티에 대한 자세한 내용은 [참조 안내서](#)를 참조하십시오.

삭제된 정책

논리 정책(GPOLICY 개체) 또는 정책 버전(POLICY 개체)을 DMS에서 삭제할 수 있습니다. 정책 버전을 삭제할 때 CA Access Control 엔터프라이즈 관리는 또한 해당 정책 버전과 관련된 배포 및 배포 취소 스크립트(RULESET 개체)도 삭제합니다. 논리 정책을 삭제하면 논리 정책과 관련된 모든 정책 버전 및 관련 스크립트도 삭제됩니다.

삭제된 논리 정책 또는 정책 버전은 복원할 수 없습니다.

삭제할 수 없는 정책

다음의 경우에는 정책을 삭제할 수 없습니다.

- 하나 이상의 정책의 정책 버전을 삭제할 수 없는 경우
- 정책이 다른 정책의 사전 요구 사항인 경우
정책을 삭제하기 전에 해당 정책에 대한 모든 종속성을 제거해야 합니다.
- 호스트에 정책이 할당 또는 배포된 경우
정책을 삭제하기 전에 호스트에서 정책을 할당 취소 또는 배포 취소해야 합니다.

삭제할 수 없는 정책 버전

다음 중 하나 이상에 해당하는 경우 정책 버전을 삭제할 수 없습니다.

- 정책 버전이 호스트에 할당 또는 배포된 경우
정책 버전을 삭제하기 전에 호스트에서 정책 버전을 할당 취소 또는 배포 취소해야 합니다.
- 정책 버전이 DMS 에서 상태가 있는 경우
정책 버전을 삭제하기 전에 호스트에서 정책 버전을 할당 취소 또는 배포 취소해야 합니다. 정책 버전을 할당 취소 또는 배포 취소할 수 없는 경우 호스트에서 직접 제거해야 합니다.
- 정책의 상태가 "배포 취소되었지만 오류 발생"인 경우
정책 버전을 삭제하기 전에 이 상태를 제거해야 합니다.

예제: 삭제할 수 없는 정책 버전

다음은 DMS 에 상태가 있지만 호스트에 적용되지 않으므로 삭제할 수 없는 정책 버전의 예제입니다.

- 배포됨(오류 발생)
- 실행되지 않음

이러한 두 경우, 정책 버전을 삭제하기 전에 호스트에서 직접 정책 버전을 제거해야 합니다.

참고: 호스트(HNODE)에서의 정책 상태에 대한 자세한 내용은 [참조 안내서](#)를 참조하십시오. 정책 버전의 제거에 대한 자세한 내용은 [문제 해결 안내서](#)를 참조하십시오.

정책 삭제

정책이 호스트 또는 호스트 그룹에 더 이상 할당되어 있지 않은 경우 CA Access Control 엔터프라이즈 관리에서 이 정책을 삭제할 수 있습니다.

중요! 정책(GPOLICY 개체)을 삭제할 때 CA Access Control 엔터프라이즈 관리는 모든 정책 버전(POLICY 개체)과 각 정책 버전과 연계된 RULESET 개체를 삭제합니다.

정책을 삭제하려면

1. CA Access Control 엔터프라이즈 관리에서 "정책 관리", "정책" 하위 탭을 차례로 클릭하고 왼쪽에 있는 작업 메뉴에서 "정책" 트리를 확장합니다.
정책 작업이 나타납니다.
2. "정책 삭제"를 클릭합니다.
"정책 삭제: 정책 검색" 화면이 나타납니다.
3. 검색 범위를 정의하고 "검색"을 클릭합니다.
정의한 검색 범위와 일치하는 정책 목록이 나타납니다.
4. 삭제할 정책을 선택하고 "선택"을 클릭합니다.
정책을 삭제할 것인지 묻는 메시지가 나타납니다.
5. "예"를 클릭합니다.
정책이 삭제됩니다.

참고: 또한 `policydeploy` 유틸리티를 사용하여 이 작업을 수행할 수도 있습니다. `policydeploy` 유틸리티에 대한 자세한 내용은 [참조 안내서](#)를 참조하십시오.

추가 정보:

[삭제할 수 없는 정책](#) (페이지 106)

정책 버전 삭제

더 이상 필요 없는 저장된 정책 버전(POLICY 개체)을 삭제할 수 있습니다. 정책 버전(POLICY 개체)을 삭제할 때 CA Access Control 엔터프라이즈 관리가 이 정책 버전과 연계된 모든 배포 및 배포 취소 스크립트를 삭제합니다.

정책 버전을 삭제하려면 다음 명령을 실행하십시오.

```
policydeploy -delete name#xx [-dms list]
```

-delete name#xx

지정한 정책 버전을 삭제합니다.

-dms list

(선택 사항) 정책 버전을 삭제할 DMS 노드의 목록을 쉼표로 구분하여 지정합니다. DMS 노드를 지정하지 않으면 policydeploy 유틸리티는 로컬 CA Access Control 데이터베이스에 지정된 DMS 노드의 목록을 사용합니다.

예: IIS 5 보호 정책 버전 삭제

다음 예는 할당 취소된 정책 버전 IIS5#05 를 DMS 에서 삭제하는 방법에 대해 설명합니다. 이 예에서 정책 버전 IIS5#05 는 어떠한 호스트 또는 호스트 그룹에도 할당되지 않았으며 crDMS@cr_host.company.com DMS 노드에 저장되어 있습니다.

IIS 5 보호 정책 버전을 삭제하려면 명령 프롬프트 창을 연 다음 policydeploy 유틸리티를 실행하십시오.

```
policydeploy -delete IIS5#05
```

정책 버전 IIS5#05 가 crDMS@cr_host.company.com DMS 노드에서 삭제됩니다.

변수

변수는 다른 구성 및 운영 체제를 사용하는 끝점에 동일한 정책을 배포할 수 있게 해 줍니다. 예를 들어, 변수를 사용하여 운영 체제의 다른 위치에 CA Access Control 이 설치되어 있는 경우라도 동일한 정책을 Windows 및 Solaris 끝점에 배포할 수 있습니다.

변수 작성 방법

변수는 ACVAR 클래스의 개체이고 하나 이상의 값을 가질 수 있습니다. 끝점에 있는 각 변수와 정책의 각 변수에는 고유한 이름을 사용해야 합니다. 다음 중 한 방법으로 변수를 만들 수 있습니다.

- CA Access Control 끝점 관리를 사용하여 끝점에서 변수를 정의합니다.
- 변수를 정의하는 정책을 만들어 여러 끝점에 배포합니다.

중요! 정책의 변수를 사용하는 규칙만 만들 수 있습니다. 변수를 포함하는 규칙을 사용하여 CA Access Control 데이터베이스를 직접 업데이트하면 데이터베이스가 규칙을 컴파일할 수 없고 CA Access Control 이 이 규칙을 시행할 수 없습니다. 정책 스크립트에서 변수를 참조하기 전에 변수를 정의해야 합니다.

변수 유형

CA Access Control 은 사용자 정의된 변수 및 기본 제공되는 변수를 지원합니다.

- 사용자 정의된 변수는 CA Access Control 데이터베이스에 정의하는 변수입니다.
- 기본 제공되는 변수는 CA Access Control 이 설치 중 생성하는 변수입니다. 기본 제공되는 변수는 수정할 수 없습니다.

사용자 정의된 변수

CA Access Control 은 다음과 같은 사용자 정의된 변수를 지원합니다.

정적 변수

CA Access Control 끝점의 고정된 위치를 정의합니다.

이름이 같지만 값이 다른 정적 변수를 여러 개 정의할 수 있지만 각 변수는 반드시 다른 끝점 및 다른 정책에 존재해야 합니다.

참고: 변수를 만들 때 변수 유형을 지정하지 않으면 CA Access Control 은 정적 변수를 만듭니다.

레지스트리 값 변수

(Windows) 레지스트리 값을 기반으로 CA Access Control 끝점의 위치를 정의합니다.

참고: REG_SZ 또는 REG_EXPAND_SZ 레지스트리 유형을 가리키는 레지스트리 변수만 정의할 수 있습니다.

예: 다음 규칙은 이름이 jboss_home 인 레지스트리 변수를 정의합니다.

```
editres ACVAR ("jboss_home") value("HKLM\Software\Jboss\home") type(regval)
```

정책에 이 규칙을 배포할 때 Windows 끝점은

HKLM\Software\Jboss\home 레지스트리 키를 사용하여 변수 값을 가져옵니다.

운영 체제 변수

운영 체제 환경 값을 기반으로 CA Access Control 끝점의 위치를 정의합니다.

예: 다음 규칙은 이름이 jboss_home 인 운영 체제 변수를 정의합니다.

```
editres ACVAR ("jboss_home") value("JBoss_HOME") type(osvar)
```

정책에 이 규칙을 배포할 때 끝점은 JBoss_HOME 운영 체제 환경 변수의 값을 사용하여 변수 값을 가져옵니다.

기본 제공되는 변수

CA Access Control 은 설치 프로세스 중 CA Access Control 데이터베이스에 기본 제공되는 변수를 만듭니다. 기본 제공되는 변수를 수정하거나 삭제할 수 없지만 기본 제공되는 변수를 정책에 사용할 수 있습니다. 기본 제공되는 변수는 동적 변수이며 CA Access Control 끝점의 시스템 설정에 종속됩니다. 기본 제공되는 변수의 값은 해당 시스템 설정이 변경될 때 함께 변경됩니다.

참고: CA Access Control 데이터베이스를 내보낼 때 기본 제공되는 변수는 출력에 포함되지 않습니다. CA Access Control 은 DMS 또는 PMDB 를 만들 때 기본 제공되는 변수를 만들지 않습니다.

CA Access Control 은 다음과 같은 기본 제공되는 변수를 지원합니다.

<!HOSTNAME>

로컬 컴퓨터의 정규화된 호스트 이름을 식별합니다.

<!HOSTIP>

하나 이상의 호스트 IP 주소를 식별합니다.

<!AC_ROOT_PATH>

CA Access Control 설치 경로를 식별합니다.

<!AC_REGISTRY_KEY>

(Windows) CA Access Control 루트 레지스트리 키를 식별합니다.

<!USER_OS_ADMIN>

로컬 컴퓨터 운영 체제의 관리자를 식별합니다.

<!DOMAINNAME>

로컬 컴퓨터의 도메인 이름을 식별합니다.

<!DNSDOMAINNAME>

로컬 컴퓨터의 DNS 이름을 식별합니다.

예: 정책에 기본 제공되는 변수 사용

이 예는 다음과 같이 네트워크 리소스 규칙을 만듭니다.

```
authorize TCP 8333 uid(*) host(<!HOSTNAME>) access(WRITE)
```

이 정책을 끝점 host1.example.com 과 이 정책을 준수하는 끝점에 배포하면 다음 규칙이 만들어집니다.

```
authorize TCP 8333 uid(*) host(host1.example.com) access(WRITE)
```

변수 사용 지침

변수를 사용할 때 다음과 같은 지침을 따라야 합니다.

- 다른 변수나 정책이 사용하는 변수는 삭제할 수 없습니다.
- 변수는 여러 값을 가질 수 있습니다. 변수 값을 추가 또는 제거할 수 있습니다.
- 변수는 중첩될 수 있습니다. 예를 들어, 다음 규칙은 기본 제공되는 <!AC_ROOT_PATH> 변수를 포함하는 ac_data 란 이름의 변수를 정의합니다.

```
editres ACVAR ac_data value("<!AC_ROOT_PATH>\data")
```

기본 설치된 CA Access Control 이 있는 Windows 끝점이 이 규칙을 준수하면 다음 규칙이 만들어집니다.

```
editres ACVAR ac_data value("C:\Program Files\CA\AccessControl\data")
```

- 각 변수는 하나의 유형만 가질 수 있으므로, 예를 들어 변수를 정적 변수인 동시에 레지스트리 값 변수로 정의할 수 없습니다.
- 정의되지 않은 변수를 포함하는 정책을 배포할 수 없습니다. 정의되지 않은 변수를 포함하는 정책을 배포하면 CA Access Control 이 이 정책의 배포 상태를 "배포 보류"로 변경합니다. 정책을 배포하려면 우선 정의되지 않은 변수를 정의한 다음 정책을 다시 배포해야 합니다.

참고: 정책에서 정의되지 않은 변수를 찾으려면 정책의 DEPLOYMENT 개체를 검토하십시오. CA Access Control 은 정책 감사의 활성화 여부에 관계없이 정의되지 않은 변수를 검사합니다.

- CA Access Control 은 CA Access Control 변수와 Windows 시스템 변수를 결합하는 규칙을 해석할 수 없습니다. 예를 들어, CA Access Control 은 이름이 var1 인 변수를 정의하는 다음 규칙을 해석할 수 없습니다.

```
editres ACVAR var1 value("%SYSTEMROOT%\temp")
```

%SYSTEMROOT%를 CA Access Control 변수로 정의하고 %SYSTEMROOT%\temp 를 보호하는 정책을 만들려면 다음 규칙을 사용하십시오.

```
editres ACVAR var1 value("SYSTEMROOT") type(osvar)
editres ACVAR var2 value("<!var1>\temp")
```

- CA Access Control 은 서로 종속된 변수를 확인할 수 없습니다. 예를 들어, CA Access Control 은 다음 예에서 변수 var1 과 var2 를 해석할 수 없습니다.

```
editres ACVAR var1 value("<!var2>")
editres ACVAR var2 value("<!var1>")
```

- 슬래시를 사용하여 변수에서 디렉터리를 정의할 때 CA Access Control 은 Windows 와 UNIX 끝점에 대해 슬래시를 올바른 방향으로 해석합니다.
- selang 규칙을 사용하여 변수를 정의하는 경우 정책을 사용하여 규칙을 끝점에 배포해야 합니다. selang 규칙을 사용하여 끝점에 있는 CA Access Control 데이터베이스를 직접 업데이트하면 CA Access Control 은 이 규칙을 컴파일할 수 없습니다. 예를 들어, 끝점에서 jboss_home 이란 이름의 변수를 정의하고 다음 selang 규칙으로 데이터베이스를 직접 업데이트했다고 가정합니다.

```
editres FILE <!jboss_home> audit(all)
```

CA Access Control 은 이 규칙을 컴파일할 수 없지만 대신 데이터베이스에 <!jboss_home>이란 이름의 FILE 개체를 만듭니다.

UNIX 끝점에서 운영 체제 변수를 사용하기 위한 지침

UNIX 에 해당

CA Access Control 운영 체제 변수(osvar 유형의 ACVAR 개체)는 UNIX 환경 변수의 값을 사용합니다. 각 UNIX 프로세스는 자체 환경 변수 세트가 있으므로 UNIX 끝점에서 운영 체제 변수를 사용하지 않는 것이 좋습니다.

UNIX 끝점에서 운영 체제 변수를 사용하는 경우에는 CA Access Control 을 시작하기 전에 반드시 필요한 환경 변수를 설정하고 내보내야 합니다. UNIX 끝점에서 운영 체제 변수를 사용할 때는 다음 지침을 준수해야 합니다.

- 컴퓨터가 시작되었을 때 CA Access Control 을 시작하기 위해 rc startup 스크립트를 사용하는 경우 이 스크립트가 CA Access Control 을 시작하기 전에 환경 변수를 설정하고 내보내는지 확인하십시오.
- 사용자가 CA Access Control 을 중지하고 다시 시작하는 경우 사용자는 CA Access Control 을 다시 시작하기 전에 자신의 세션에서 환경 변수를 설정하고 내보내야 합니다.

Windows 끝점에서 운영 체제 변수를 사용하기 위한 지침

Windows 에 해당

CA Access Control 운영 체제 변수(osvar 유형의 ACVAR 개체)는 Windows 환경 변수의 값을 사용합니다.

Windows 끝점에서 운영 체제 변수를 사용할 때는 다음 지침을 준수해야 합니다.

- 환경 변수는 시스템 변수여야 합니다.
- Windows 환경 변수의 값을 변경하면 CA Access Control 은 다시 시작할 때까지 변경 사항을 인식하지 않습니다. 또한 Windows 의 일부 릴리스에서는 Windows 서비스와 CA Access Control 이 변경 사항을 인식하도록 하려면 컴퓨터를 다시 시작해야 합니다.

끝점이 변수를 해석하는 방법

변수는 다른 구성 및 운영 체제를 사용하는 끝점에 동일한 정책을 배포할 수 있게 해 줍니다. 다음 프로세스는 정책을 만들어 배포한 이후에 **CA Access Control** 끝점이 정책에 있는 변수를 해석하는 방법을 설명합니다.

1. **policyfetcher** 가 정책을 가져오면 **CA Access Control** 은 이 정책에 있는 변수가 정책 또는 **CA Access Control** 데이터베이스에 정의되어 있는지 확인합니다. 다음 중 *하나*가 발생합니다.
 - 변수가 정책 또는 데이터베이스에 정의되어 있지 않으면 **CA Access Control** 이 정책 상태를 "배포 보류"로 변경합니다.
참고: 정책을 배포하려면 우선 정의되지 않은 변수를 정의한 다음 정책을 다시 배포해야 합니다.
 - 변수가 정책 또는 데이터베이스에 정의되어 있으면 **CA Access Control** 은 이 정책을 컴파일하고 포함된 규칙을 시행합니다.
2. 하트비트때마다 **policyfetcher** 는 **CA Access Control** 데이터베이스에서 변수 값이 변경되었는지 확인합니다. 다음 중 *하나*가 발생합니다.
 - 변수 값이 변경되지 않았으면 **policyfetcher** 는 2 단계를 반복합니다.
 - 변수 값이 변경되었으면 **CA Access Control** 은 변경된 변수를 사용하는 끝점에 있는 모든 정책에 대해 정책 상태를 "동기화되지 않음"으로 변경합니다.
참고: 정책에 대한 "동기화되지 않음" 상태를 지우려면 정책을 다시 배포해야 합니다.

정책 배포 문제 해결

호스트에 정책을 할당할 때 **policyfetcher** 가 배포 작업을 검색하고 정책 스크립트를 실행할 때까지 정책은 할당된 끝점에 배포되지 않습니다. 따라서 정책이 전송되거나 끝점에 배포될 때 다양한 이유로 배포 오류가 발생할 수 있습니다.

정책 배포 오류를 해결하기 위해 고급 정책 관리에는 문제 해결 작업을 제공합니다. 이러한 작업은 **CA Access Control** 엔터프라이즈 관리 또는 **policydeploy** 유틸리티를 사용하여 수행할 수 있습니다. **CA Access Control** 엔터프라이즈 관리에서 문제 해결 작업은 "정책 관리" 탭의 "정책" 하위 탭에 있습니다.

문제 해결 작업은 다음과 같습니다.

- **재배포** - 정책 스크립트를 포함하는 새 배포 작업을 만들어 끝점에 배포합니다.

정책을 끝점에 배포할 때 오류가 발생하는 경우 이 옵션을 사용하십시오. 즉, **selang** 정책 스크립트 실행이 실패하는 경우입니다. 정책을 재배포하려면 먼저 끝점에서 스크립트 오류의 원인을 수동으로 수정해야 합니다.

참고: 이 옵션은 **CA Access Control** 엔터프라이즈 관리에서만 사용할 수 있으며 **policydeploy** 유틸리티에서는 지원되지 않습니다.

- **배포 취소** - 해당 호스트에서 정책을 할당 취소하지 않고 지정된 끝점에서 정책의 배포를 취소합니다.

DMS 에 있는 호스트에 할당되지 않은 끝점에서 정책을 제거하려면 이 옵션을 사용하십시오.

- **다시 설정** - 끝점을 다시 설정합니다. **CA Access Control** 은 호스트 상태를 재설정하고, 모든 유효 정책을 배포 취소하며, 모든 **GPOLICY**, **POLICY**, **RULESET** 개체를 삭제합니다.

DMS 에서 끝점과 그 상태를 삭제하려면 모든 정책 배포에서 이 옵션을 사용하십시오.

참고: 감사를 위해 필요할 수도 있으므로 이 옵션은 끝점 또는 DMS 에서 **DEPLOYMENT** 또는 **GDEPLOYMENT** 개체를 제거하지 않습니다. 끝점을 다시 설정한 후에 **dmsmgr -cleanup** 기능을 사용하여 **DEPLOYMENT** 및 **GDEPLOYMENT** 개체를 제거할 수 있습니다. 끝점을 다시 설정한 이후에 정상적으로 끝점에 정책을 할당할 수 있습니다.

- **복원** - 지정된 호스트에서 모든 정책의 배포를 취소한 다음, 새 배포 작업을 만들어 실행을 위해 호스트에 이 작업을 전달함으로써 호스트에 배포(할당 또는 직접 배포됨)해야 할 모든 정책을 복원합니다.

DMS 가 해당 끝점에서 유효한 것으로 나타내는 모든 정책을 다시 배포하려면 끝점에서 **CA Access Control** 또는 운영 체제를 다시 설치할 때 또는 백업에서 끝점을 복원할 때 이 옵션을 사용하십시오.

사용하지 않는 끝점 제거 방법

DMS에서는 기업에 대한 정보를 저장합니다. 기업에서 컴퓨터를 제거하는 경우 이 컴퓨터에서 CA Access Control 을 제거해도 DMS에는 해당 노드에 대한 참조가 계속 포함되어 있습니다. 일상적인 유지 관리 절차로서 DMS에서 이런 사용하지 않는 노드를 정리해야 합니다.

사용하지 않는 노드를 제거하려면 다음 중 하나를 수행하십시오.

- DMS 컴퓨터에서 다음과 같이 **dmsmgr** 유틸리티를 실행하여 일상적인 정리 작업을 수행합니다.

```
dmsmgr -cleanup number_of_days -dms name  
number_of_days
```

CA Access Control 노드를 사용할 수 없는 최소 일 수를 정의합니다.

- DMS 컴퓨터에서 다음 **selang** 명령을 실행하여 특정 노드를 수동으로 삭제합니다.

```
rr HNODE HNODE_name
```

중요! 노드를 삭제하면 CA Access Control에서는 모든 HNODE 관련 배포 작업을 제거하고, 패키지에 다른 배포 작업 구성원이 포함되지 않은 한 모든 배포 작업의 패키지를 제거한 다음, HNODE 개체만 제거합니다.

배포 감사 정보 보기

CA Access Control 엔터프라이즈 관리에서는 정책 배포 감사 기능을 제공합니다. 이 감사는 배포 작업의 설명 목록인 정책 배포 보기를 제공합니다. 이 목록에는 각 배포 작업을 트리거한 항목, 작업이 생성된 시간 및 관련된 배포 유형이 자세히 설명되어 있습니다. 각 배포 작업에 대해 배포 작업이 생성된 호스트 및 정책 쌍, 배포된 정책 버전, 배포 작업 상태(큐에 추가, 성공 또는 실패) 및 **selang** 출력(명령 배포 결과) 등의 세부 정보를 추가로 탐색할 수 있습니다.

배포 감사 정보를 보려면

1. CA Access Control 엔터프라이즈 관리에서 다음을 수행합니다.
 - a. "정책 관리"를 클릭합니다.
 - b. "정책" 하위 탭을 클릭합니다.
 - c. 작업 메뉴에서 왼쪽에 있는 "배포" 트리를 확장합니다.

사용 가능한 작업 목록에 "배포 감사" 작업이 나타납니다.

2. "배포 감사"를 클릭합니다.

"배포 감사" 페이지가 나타납니다.

3. 배포 감사 범위를 정의하고 "실행"을 클릭합니다.

CA Access Control 엔터프라이즈 관리는 정의된 범위 내에 있는 배포 정보를 검색하고 잠시 후 결과를 표시합니다.

4. (선택 사항) 연관된 배포 작업에 대한 자세한 내용을 보려면 배포의 트리거를 클릭합니다.

정책 위반 계산 작동 방법

고급 정책 관리를 사용하면 정책 배포의 결과로 끝점에 배포되어야 하는 액세스 규칙과 동일한 끝점에 성공적으로 배포된 실제 규칙 사이의 차이점을 확인할 수 있습니다. 또한 정책 개체에 추가된 속성과 변경된 속성을 확인합니다. 이 정보를 사용하면 정책 배포와 연관된 문제를 해결할 수 있습니다.

끝점에서 정책 위반 계산기를 실행하면 다음 작업이 수행됩니다.

1. 끝점에 배포해야 하는 규칙 목록을 로컬 호스트에서 검색합니다.

이러한 규칙은 배포된 각 정책 버전의 **POLICY** 개체와 연관된 로컬 **RULESET** 개체에 지정된 대로 각 배포 정책에 지정된 규칙입니다.

2. 이러한 각 규칙이 끝점에 적용되는지 확인합니다.

중요! 위반 계산에서는 기본 규칙이 적용되는지 여부를 확인하지 않습니다. 또한 데이터베이스에서 개체(사용자 또는 개체 특성, 사용자 또는 리소스 권한 부여, 실제 사용자 또는 리소스)를 제거하는 규칙을 무시합니다. 예를 들어 위반 계산에서는 다음 규칙이 적용되는지 여부를 확인할 수 없습니다.

`rr FILE /etc/passwd`

3. (선택 사항) 로컬 정책 개체와 DMS 의 정책 개체를 비교합니다.
일반적으로 위반 계산기는 로컬 호스트에서만 위반을 확인합니다.
-strict 옵션을 지정하면 위반 계산기가 로컬 HNODE 개체와 연관된 정책과 DMS 에 있는 HNODE 개체와 연관된 정책도 비교합니다.
비교하는 내용은 다음과 같습니다.
 - a. 로컬 호스트를 나타내는 HNODE 개체와 연관된 정책 목록
 - b. HNODE 개체와 연관된 각 POLICY 개체의 정책 상태
 - c. HNODE 개체와 연관된 각 POLICY 개체의 정책 서명
4. 다음 두 개의 파일이 출력됩니다.
 - ACInstallDir/data/devcalc/deviation.log
마지막 위반 계산 시 수집된 로그 및 오류 메시지입니다.
 - ACInstallDir/data/devcalc/deviation.dat
정책 및 해당 위반 목록입니다. 끝점에서 selang 명령 `get devcalc` 를 사용하여 이 파일의 내용을 가져올 수 있습니다.

참고: CA Access Control 은 `seaudit -a` 를 사용하여 볼 수 있는 감사 이벤트도 전송합니다. `seaudit` 유틸리티에 대한 자세한 내용은 [참조 안내서](#)를 참조하십시오.
5. 위반이 있음을 DMS 에 알립니다.
알림은 로컬 CA Access Control 데이터베이스에 대해 지정된 DH 를 통해 DMS 에 전달됩니다.

위반 계산 트리거

DMS 에 정책 위반 상태에 대한 최신 정보가 포함되도록 위반 계산을 정기적으로 수행해야 합니다. 끝점에서 고급 정책 관리가 비활성화된 경우 `policyfetcher` 가 각 하트비트 이후에 위반 계산을 트리거합니다.

참고: 기본적으로 실행되는 위반 계산은 끝점에 추가된 항목을 고려하지 않습니다. 이러한 항목을 보려면 `정밀한` 모드에서 위반 계산을 실행하도록 `devcalc_command` 구성을 변경하십시오.

원하는 간격으로 정책 위반 계산이 수행되도록 `policyfetcher` 설정을 수정하는 것이 좋습니다.

정책 위반 로그 및 오류 파일

정책 위반을 계산하면 각 위반 계산 중에 새 로그가 작성됩니다. 오류 메시지도 포함되어 있는 이 로그는 `ACInstallDir\data/devcalc/deviation.log`에 저장되어 있습니다.

DMS에서 가져온 보고서에 표시되는 위반이 마지막으로 실행된 위반 계산에서 수집되지 않은 경우 이 로그를 사용합니다. 이 로그는 위반 계산 결과가 DMS로 전송되지 않은 이유를 진단하는 데 도움이 됩니다.

예: 위반 로그 및 오류 파일

다음은 예제 위반 로그와 오류 파일입니다.

```
시작 시간: Mon Jan 23 13:04:48 2006
경고,\"DH 호스트 이름을 검색하지 못했습니다. 위반이 로컬에 저장됩니다.\"
'iis8#02' 정책에 대한 위반을 찾았습니다.
종료 시간: Mon Jan 23 13:05:04 2006
```

정책 위반 데이터 파일

정책 위반을 계산하면 정책 및 정책 위반 목록이 포함된 데이터 파일이 작성됩니다. 이 데이터 파일은 `ACInstallDir\data/devcalc/deviation.dat`에 저장되어 있습니다.

참고: 데이터 파일에 포함되는 정책 목록은 위반을 계산하는 정책에 따라 다릅니다. 기본적으로 끝점의 모든 정책과 모든 정책 버전이 포함됩니다.

중요! 위반 계산에서는 기본 규칙이 적용되는지 여부를 확인하지 않습니다. 또한 데이터베이스에서 개체(사용자 또는 개체 특성, 사용자 또는 리소스 권한 부여, 실제 사용자 또는 리소스)를 제거하는 규칙을 무시합니다. 예를 들어 위반 계산에서는 다음 규칙이 적용되는지 여부를 확인할 수 없습니다.
`rr FILE /etc/passwd`

위반이 있는지 여부에 관계없이 위반 상태는 DMS로 전송되지만 실제 위반은 로컬에 저장됩니다. 보고서 작성 시 이 파일에서 실제 위반 결과를 가져와서 보고서에 추가할 수 있습니다.

정책 위반 데이터 파일에 나타날 수 있는 행은 다음과 같습니다.

날짜

위반 계산의 타임스탬프를 표시합니다. 날짜 행은 항상 위반 보고서의 첫 번째 행입니다.

형식: DATE, *DDD MMM DD hh:mm:ss YYYY*

Strict

-strict 옵션을 사용하여 위반 계산이 실행되었음을 지정합니다.

형식: STRICT, *DMS@hostname, policy_name#xx*, [1|0]

[1|0]은 로컬 HNODE 개체와 연관된 정책과 *DMS@hostname* 의 HNODE 개체와 연관된 정책 사이에 위반이 있는지(1) 또는 없는지(0) 여부를 나타냅니다.

Policy Start

이 정책 버전에 대한 위반을 정의하는 정책 블록을 시작합니다.

형식: POLICYSTART, *policy_name#xx*

차이

정책에 대해 발견된 위반을 설명합니다. 위반이 적용되는 정책 이름은 이 행 위에서 가장 가까운 정책 행입니다.

다음 표에는 누락 요소를 나타내는 위반 네 개 및 추가 요소를 나타내는 위반 네 개의 위반 유형 여덟 개가 설명되어 있습니다.

위반 유형	형식
클래스를 찾을 수 없습니다.	DIFF, <i>-(class_name)</i> , (*), (*), (*)
개체를 찾을 수 없습니다.	DIFF, <i>(class_name)</i> , <i>-(object_name)</i> , (*), (*)
개체가 추가되었습니다.	DIFF, <i>(class_name)</i> , <i>+(object_name)</i> , (*), (*)
속성을 찾을 수 없습니다.	DIFF, <i>(class_name)</i> , <i>(object_name)</i> , <i>-(property_name)</i> , (*)
속성이 추가되었습니다.	DIFF, <i>(class_name)</i> , <i>(object_name)</i> , <i>+(property_name)</i> , (*)

위반 유형	형식
속성 값이 없습니다.	DIFF, (class_name), (object_name), (property_name), -(expected_value)
속성 값이 추가되었습니다.	DIFF, (class_name), (object_name), (property_name), +(value)

참고: 위반 계산기는 누락된 클래스를 발견하면 누락된 모든 개체, 속성 및 값에 대한 위반 행을 생성합니다.

Policy End

이 정책에 대한 위반을 정의하는 정책 블록을 종료합니다.

형식: POLICYEND, policy_name#xx, [1|0]

{1|0}은 위반이 있는지(1) 또는 없는지(0) 여부를 나타냅니다.

경고

경고를 설명합니다.

형식: WARNING, "warning_text"

예: 위반 데이터 파일

다음 예는 위반 데이터 파일의 내용을 보여 줍니다.

```
날짜: Sun Mar 19 08:30:00 2006
경고, "DH 호스트 이름을 검색하지 못했습니다. 위반이 로컬에 저장됩니다."
POLICYSTART, iis8#02
DIFF, (USER), (iis8pers), (*), (*)
POLICYEND, iis8#02, 1
```

누락된 요소를 나타내는 위반

위반 계산기는 누락된 요소와 추가된 새 요소를 구별합니다. 누락된 요소는 지정된 정책에 명시적으로 정의되어 있지만 로컬 호스트에 없는 CA Access Control 요소입니다. 이러한 누락된 요소는 클래스, 개체, 속성 및 값이 될 수 있습니다.

누락된 요소 조합은 계층적 요구 사항을 정의합니다. 예를 들어 Policy1 에는 다음 규칙이 있습니다.

eu mytestuser2 operator

위반 계산기는 다음 암시적 요구 사항이 충족된다고 가정합니다.

- USER 클래스가 있어야 합니다.
규칙은 USER 클래스에 속한 사용자를 정의합니다.
- USER 개체 mytestuser2 가 있어야 합니다.
USER 클래스의 mytestuser2 개체가 규칙에 명시적으로 정의됩니다.
- OBJ_TYPE 속성이 있어야 합니다.
규칙은 operator 매개 변수를 사용하여 USER 개체의 OBJ_TYPE 매개 변수를 설정합니다.
- 값 Operator 가 OBJ_TYPE 속성에 할당됩니다.
규칙은 이 값을 명시적으로 설정합니다.

추가된 요소를 나타내는 위반

위반 계산기는 누락된 요소와 추가된 새 요소를 구별합니다. 추가된 요소는 로컬로 정의되었지만 지정된 정책에는 없는 CA Access Control 요소입니다. 이러한 추가된 요소는 클래스, 개체, 속성 및 값이 될 수 있습니다.

다음과 같은 경우 추가 위반이 포함됩니다.

- 로컬 예외로 인해 정책 내에서 설명한 개체의 속성에 새 값이 추가된 경우
- 로컬 예외로 인해 정책 내에서 설명한 개체에 새 속성이 추가된 경우

참고: 정책 내에서 설명하지 않은 새 개체는 추가 요소로 고려되지 않으며 새 클래스의 경우에도 마찬가지입니다.

수정된 요소를 나타내는 위반

수정된 요소를 표시하는 위반은 위반 데이터 파일의 어떠한 위반 줄에도 수정 사항이 표시되지 않을 때 발생합니다. 수정 사항을 식별하려면 동일한 요소에 적용되는 순차적 제거 및 추가 줄을 찾아야 합니다. 예를 들어 다음은 위반 데이터 파일에서 추출한 내용입니다. 여기에서 **mytestuser** 값이 **Operator** 에서 **Auditor** 및 **Administrator** 로 수정되었습니다.

```
DIFF, (USER), (mytestuser2), (OBJ_TYPE), -(Operator)
DIFF, (USER), (mytestuser2), (OBJ_TYPE), +(Auditor)
DIFF, (USER), (mytestuser2), (OBJ_TYPE), +(Administrator)
```


제 5 장: PUPM 구현 계획

이 섹션은 다음 항목을 포함하고 있습니다.

[공유 계정 관리](#) (페이지 125)

[공유 계정이란?](#) (페이지 125)

[권한 있는 액세스 역할 및 권한 있는 계정](#) (페이지 126)

[암호 소비자](#) (페이지 135)

[PUPM 감사 레코드](#) (페이지 141)

[CA Service Desk Manager 통합](#) (페이지 144)

[구현 고려 사항](#) (페이지 148)

공유 계정 관리

공유 계정 관리(SAM)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.

공유 계정이란?

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

공유 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 공유 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, 공유 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.

추가 정보:

[권한 있는 액세스 역할](#) (페이지 25)

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 30)

권한 있는 액세스 역할이 작업 체크 아웃 및 체크 인에 주는 영향

끝점에서 관리 작업을 수행하기 위해 공유 계정을 체크 아웃하고 끝점에서 작업을 완료한 다음 공유 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 끝점 권한 있는 액세스 역할을 할당하면 사용자는 공유 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 공유 계정을 체크 아웃합니다.
 - PUPM 사용자 역할이 있는 사용자가 계정을 체크 아웃합니다.
 - Break Glass 역할이 있는 사용자가 break glass 체크 아웃을 수행합니다.
 - CLI 암호 소비자와 같은 응용 프로그램이 CA Access Control 끝점에서 계정을 체크 아웃합니다.

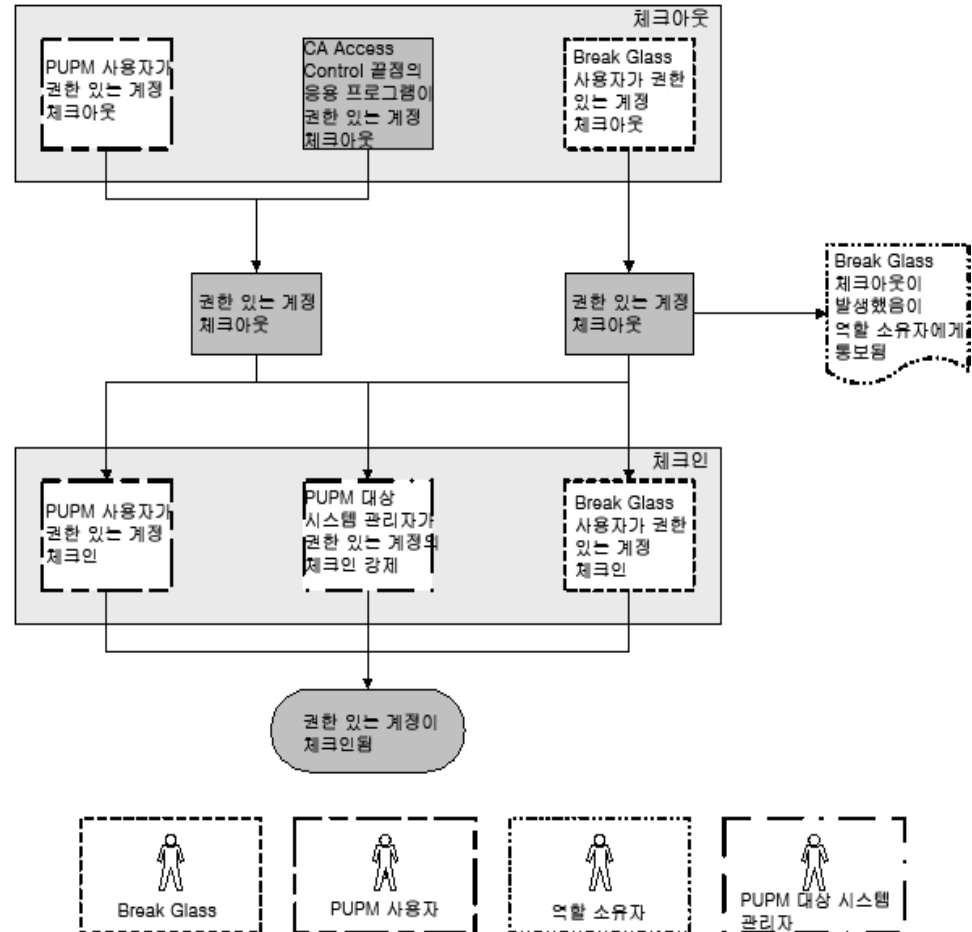
공유 계정이 체크 아웃됩니다.

참고: 사용자가 Break Glass 체크 아웃을 수행하면 CA Access Control 은 역할 소유자에게 알립니다. 역할 소유자는 감사를 위해 이 메시지에 정보를 추가할 수 있습니다.

2. 사용자는 다음 방법 중 하나를 사용하여 공유 계정을 체크 인합니다.
 - PUPM 사용자 역할이 있는 사용자가 계정을 체크 인합니다.
 - Break Glass 역할이 있는 사용자가 계정을 체크 인합니다.
 - CA Access Control 끝점에 있는 응용 프로그램이 계정을 체크 인합니다.
 - PUPM 대상 시스템 관리자 역할이 있는 사용자가 계정을 강제로 체크 인합니다.

공유 계정이 체크 인됩니다.

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



예: 공유 계정 체크 아웃

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

예: 공유 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 공유 계정 요청 작업에 주는 영향

사용자가 공유 계정을 체크 아웃할 수 없고 계정에 즉시 액세스할 필요가 없는 경우 사용자는 공유 계정 요청을 제출할 수 있습니다. 관리자는 이 요청을 승인 또는 거부할 수 있습니다. 이 항목에서는 사용자가 공유 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 끝점 권한 있는 액세스 역할을 할당하면 사용자는 공유 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 공유 액세스 요청 작업에 주는 영향에 대해 설명합니다.

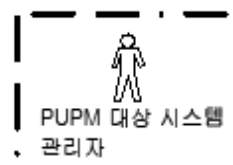
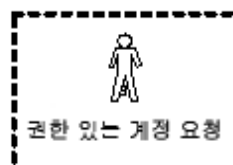
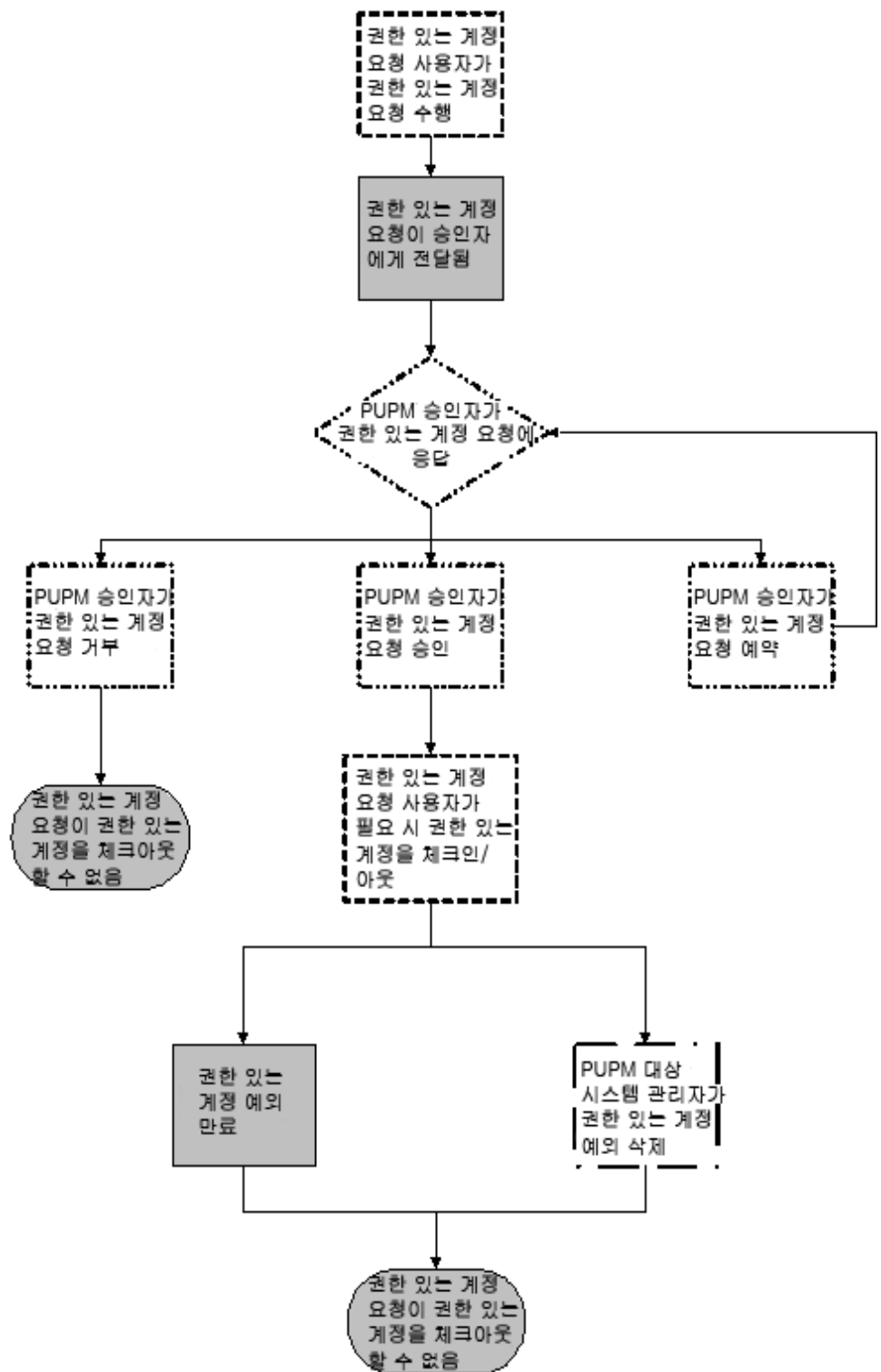
1. 공유 액세스 요청 역할이 있는 사용자가 권한 있는 계정에 대한 액세스를 요청합니다.
2. CA Access Control 은 공유 계정 요청을 사용자의 관리자(PUPM 승인자 역할도 필요함)에게 보냅니다.

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

3. PUPM 승인자 역할이 있는 사용자가 요청에 응답하고 다음 중 *하나*를 수행합니다.
 - 공유 계정 요청을 거부합니다.
권한 있는 계정 요청 역할이 있는 사용자가 공유 계정을 체크 아웃할 수 없습니다.
 - 공유 계정 요청을 예약합니다.
다른 사용자가 이 요청을 승인 또는 거부할 수 없습니다. PUPM 승인자가 요청을 승인할 때까지 권한 있는 계정 요청 역할이 있는 사용자가 공유 계정을 체크 아웃할 수 없습니다.
 - 공유 계정 요청을 승인합니다.
권한 있는 요청 역할이 있는 사용자에게 공유 계정 예외가 부여되어 사용자가 계정을 체크 아웃 및 체크 인할 수 있습니다.
4. 다음 이유 중 하나로 인해 공유 계정 예외가 만료됩니다.
 - 공유 계정 예외에 지정된 만료 시간에 도달했습니다.
 - PUPM 대상 시스템 관리자 역할이 있는 사용자가 공유 계정 예외를 삭제했습니다.

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

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



예: 공유 계정 요청 및 이 요청에 응답

본인에게 시스템 관리자 역할이 있습니다. Alice에게 공유 계정 요청 역할과 SSH 장치 연결 끝점 권한 있는 액세스 역할을 할당합니다. Alice의 관리자인 Bob에게 PUPM 승인자 역할을 할당합니다.

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

Bob이 CA Access Control 엔터프라이즈 관리에 로그인하여 공유 계정 요청에 응답할 수 있는 작업만 살펴봅니다. Bob이 Alice의 공유 액세스 요청을 승인하고 공유 계정 예외가 오후 6시까지 유효하도록 지정합니다. Alice는 이제 example_ux 계정에 체크인 및 체크아웃할 수 있습니다. 오후 6시에 공유 계정 예외가 만료되고 Alice는 더 이상 example_ux 계정을 체크아웃할 수 없게 됩니다.

Break Glass 프로세스가 작동하는 방법

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

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

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

체크아웃된 Break Glass 계정이 "홈" 탭의 "Break Glass" 옵션에 있는 "내 체크아웃한 권한 있는 계정" 탭에 추가됩니다.

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

암호 소비자

암호 소비자는 스크립트를 실행하고, 데이터베이스에 연결하거나 Windows 서비스, 예약된 작업 또는 RunAs 명령을 관리하기 위해 권한 있는 계정 및 서비스 계정을 사용하는 응용 프로그램, Windows 서비스, Windows 예약된 작업입니다. **서비스 계정**은 Windows 서비스에서 사용되는 내부 계정입니다. 예를 들어, Windows 서비스는 운영 체제에 로그인하기 위해 NT AUTHORITY\LocalService 서비스 계정을 사용할 수 있습니다.

암호 소비자는 응용 프로그램 스크립트에서 하드 코드된 암호를 제거하고 끝점에서 암호 정책을 시행하도록 할 수 있습니다. 예를 들어, Windows 끝점에서 각 예약된 작업에 대한 암호 소비자를 만들고 각 암호 소비자가 동일한 암호 정책을 사용하도록 지정할 수 있습니다. 그런 다음 PUPM 은 암호 정책에 지정된 간격으로 각 예약된 작업의 암호를 변경합니다.

PUPM 은 다음과 같은 방식으로 권한 있는 계정 암호를 암호 소비자에게 제공합니다.

- 요청 시 - 암호 소비자가 권한 있는 계정 암호에 대한 요청을 보낼 때. 예: 권한 있는 계정이 ODBC 를 사용하여 인증을 요구하는 데이터베이스 연결하는 경우

참고: 필요 시 암호를 가져오는 암호 소비자를 사용하려면 PUPM 통합 기능을 활성화하여 PUPM 끝점에 CA Access Control 을 설치해야 합니다.

- 암호가 변경될 때 - CA Access Control 엔터프라이즈 관리에서 암호 소비자에 대한 암호 변경 이벤트가 발생할 때. 예: 암호 정책이 서비스 계정에 대한 암호가 지정된 시간 이후 반드시 변경되도록 지정하는 경우

참고: 암호 변경 시 암호를 가져오는 암호 소비자를 사용하기 위해 PUPM 끝점에 CA Access Control 을 설치할 필요는 없습니다.

암호 소비자의 유형

암호 소비자는 PUPM 끝점에서 실행하는 응용 프로그램, Windows 서비스, Windows 예약된 작업을 의미합니다. 소프트웨어 개발 키트 암호 소비자를 제외하고, 모든 기타 암호 소비자는 권한 있는 계정 암호를 받지만 이 암호를 체크 아웃 또는 체크 인하지 않습니다.

PUPM 은 요청 시 권한 있는 계정 암호를 다음 암호 소비자에게 제공합니다.

- **소프트웨어 개발 키트(SDK/CLI)** - 소프트웨어 개발 키트 암호 소비자는 끝점에서 스크립트에 의해 실행될 때 권한 있는 계정 암호를 요청합니다.

스크립트에서 하드 코드된 암호를 대체하려면 소프트웨어 개발 키트 암호 소비자를 사용하십시오.

참고: 다른 암호 소비자와 달리, 소프트웨어 개발 키트 암호 소비자는 권한 있는 계정 암호를 체크 아웃 및 체크 인할 수 있습니다.

- **데이터베이스(ODBC, JDBC, OLEDB, OCI, .NET)** - 데이터베이스 암호 소비자는 끝점에서 실행 중인 프로그램이 데이터베이스에 연결할 때 권한 있는 계정 암호를 요청합니다.

데이터베이스에 연결하는 프로그램에서 하드 코드된 암호를 대체하려면 데이터베이스 암호 소비자를 사용하십시오.

- **Windows Run As** - Windows Run As 암호 소비자는 사용자가 권한 있는 계정으로 전환하여 특정 명령을 실행하기 위해 RunAs 응용 프로그램 실행할 때 암호를 요청합니다.

사용자가 권한 있는 계정으로 전환하여 권한 있는 계정 암호 없이 명령을 실행하도록 하려면 Windows Run As 암호 소비자를 사용하십시오.

참고: 필요 시 암호를 가져오는 암호 소비자를 사용하려면 PUPM 통합 기능을 활성화하여 PUPM 끝점에 CA Access Control 을 설치해야 합니다.

PUPM 은 암호 변경 시 권한 있는 계정 암호를 다음 암호 소비자에게 제공합니다.

- **Windows 예약된 작업** - Windows 예약된 작업 암호 소비자는 서비스 계정을 사용하여 예약된 작업을 관리합니다. PUPM 은 CA Access Control 엔터프라이즈 관리에서 암호 변경 이벤트가 발생할 때마다 작업에 대한 암호 변경을 강제합니다.

암호 정책을 설정하고 예약된 작업에 대한 암호 변경을 자동화하려면 Windows 예약된 작업 암호 소비자를 사용하십시오.

- **Windows 서비스** - Windows 서비스 암호 소비자는 서비스 계정을 사용하여 Windows 서비스를 실행합니다. PUPM 은 CA Access Control 엔터프라이즈 관리에서 암호 변경 이벤트가 발생할 때마다 서비스 계정에 대한 암호 변경을 강제합니다.

암호 정책을 설정하고 Windows 서비스에 대한 암호 변경을 자동화하려면 Windows 서비스 암호 소비자를 사용하십시오. 서비스는 암호를 변경할 수 있는 계정(예: 컴퓨터의 Administrator 계정 또는 도메인 계정)에 의해 실행되어야 합니다.

참고: 암호 변경 시 암호를 가져오는 암호 소비자를 사용하기 위해 PUPM 끝점에 CA Access Control 을 설치할 필요는 없습니다.

추가 정보:

[암호 소비자 만들기](#) (페이지 254)

요청 시 암호 소비자가 암호를 가져오는 방법

암호 소비자는 연결된 권한 있는 계정이 다른 응용 프로그램으로 인증될 때 PUPM 에서 암호를 가져옵니다. 요청 시 암호를 가져오는 암호 소비자는 암호 요청을 PUPM 에이전트에게 전달하고, 이 에이전트는 메시지 큐를 사용하여 CA Access Control 엔터프라이즈 관리와 통신합니다.

소프트웨어 개발 키트, 데이터베이스, Windows Run As 암호 소비자가 요청 시 암호를 받습니다. 요청 시 암호를 가져오는 암호 소비자를 사용하여 스크립트에서 하드 코드된 암호를 대체합니다. 응용 프로그램이 인증을 위한 암호를 제공할 때마다 PUPM 은 하드 코드된 암호를 권한 있는 계정 암호로 대체합니다.

참고: 필요 시 암호를 가져오는 암호 소비자를 사용하려면 PUPM 통합 기능을 활성화하여 PUPM 끝점에 CA Access Control 을 설치해야 합니다.

다음 프로세스는 요청 시 암호 소비자가 권한 있는 계정 암호를 가져오는 방법을 설명합니다.

1. 응용 프로그램은 하드 코드된 암호를 사용하여 사용자 인증을 요구하는 시스템에 연결하려고 시도합니다.
2. 암호 소비자가 연결 시도를 가로칩니다.

예를 들어, OCI 암호 소비자는 Oracle 데이터베이스에 연결하려는 시도를 가로칩니다.

3. PUPM 에이전트가 캐시를 확인합니다. 다음 중 *한 가지* 결과가 나타납니다.
 - 요청이 캐시에 저장되어 있으면 PUPM 에이전트는 권한 있는 계정 암호를 암호 소비자에게 전달합니다. 암호 소비자는 하드 코드된 암호를 권한 있는 계정 암호로 대체합니다. 응용 프로그램은 권한 있는 계정 암호를 사용하여 시스템에 로그인합니다. 이 단계에서 프로세스가 끝납니다. CA Access Control 엔터프라이즈 관리는 암호 검색에 대한 감사 레코드를 작성하지 않습니다.
 - 요청이 캐시에 저장되어 있지 않으면 PUPM 에이전트가 암호 요청을 CA Access Control 엔터프라이즈 관리로 전달합니다.
4. CA Access Control 엔터프라이즈 관리는 메시지를 받고 암호 소비자가 권한 있는 계정 암호를 받도록 허가되었는지 확인합니다.
5. 다음 중 *한 가지* 결과가 나타납니다.
 - 암호 소비자가 암호를 받도록 허가된 경우 CA Access Control 엔터프라이즈 관리는 권한 있는 계정 암호를 PUPM 에이전트로 보냅니다. PUPM 에이전트는 하드 코드된 암호를 권한 있는 계정 암호로 대체합니다. 응용 프로그램은 권한 있는 계정 암호를 사용하여 시스템에 로그인합니다. CA Access Control 엔터프라이즈 관리가 이벤트에 대한 감사 레코드를 작성합니다.
 - 암호 소비자가 암호를 받도록 허가되지 않은 경우 CA Access Control 엔터프라이즈 관리는 오류 메시지를 PUPM 에이전트로 보냅니다. PUPM 에이전트가 암호를 응용 프로그램으로 전달하지 않으므로 응용 프로그램은 하드 코드된 암호를 사용하여 시스템에 로그인합니다.

PUPM 이 암호 변경에 대해 암호 소비자에게 통보하는 방법

PUPM 은 CA Access Control 엔터프라이즈 관리에서 암호 변경 이벤트가 발생할 때(예: 지정된 기간 이후에 암호를 반드시 변경하도록 암호 정책이 지정하는 경우) 암호 소비자에 대한 암호 변경을 강제합니다. CA Access Control 엔터프라이즈 관리는 JCS 를 사용하여 암호 변경 시 암호를 가져오는 암호 소비자와 통신합니다.

Windows 예약된 작업 및 Windows 서비스 암호 소비자만 암호 변경 시 암호를 받습니다.

참고: 암호 변경 시 암호를 가져오는 암호 소비자를 사용하기 위해 PUPM 끝점에 CA Access Control 을 설치할 필요는 없습니다.

다음 프로세스는 PUPM 이 암호 소비자에게 암호 변경에 대해 통보하는 방법을 설명합니다.

1. 암호 변경 이벤트가 새 암호를 생성합니다.
2. CA Access Control 엔터프라이즈 관리가 이 암호를 사용하는 암호 소비자를 중앙 데이터베이스에서 찾습니다.
3. 끝점을 만들 때 제공한 관리자 자격 증명을 사용하여 JCS 가 영향을 받는 각 끝점에 로그인합니다.
4. JCS 는 끝점에서 암호 소비자의 암호를 변경하려고 시도합니다. 다음 중 한 가지 결과가 나타납니다.
 - JCS 는 끝점에서 암호 소비자의 암호를 변경하고 선택한 경우 서비스를 다시 시작합니다.
5. CA Access Control 엔터프라이즈 관리가 암호 변경에 대한 감사 레코드를 작성합니다.

참고: 암호 소비자를 만들 때 JCS 가 서비스를 다시 시작할지 여부를 지정합니다.

- JCS 는 끝점에서 암호 소비자의 암호를 변경할 수 없습니다. CA Access Control 엔터프라이즈 관리는 암호 변경 이벤트를 시작한 작업에서 알림 메시지를 작성합니다.

참고: "제출된 작업 보기"를 사용하여 PUPM 감사 레코드를 볼 수 있습니다. JCS 가 암호 소비자의 암호를 변경할 수 없으면 "암호 소비자 동기화"를 사용하여 암호 변경을 다시 시도할 수 있습니다.

추가 정보:

[암호 소비자 동기화](#) (페이지 307)

암호 소비자에 대한 구현 고려 사항

암호 소비자를 구현하기 전에 다음 사항을 고려하십시오.

- 소프트웨어 개발 키트, 데이터베이스, Windows Run As 암호 소비자를 사용하려면 PUPM 통합 기능을 활성화하여 PUPM 끝점에 CA Access Control 을 설치해야 합니다.
- JDBC 데이터베이스 암호 소비자를 사용하려면 데이터베이스에 연결하는 응용 프로그램이 JRE 1.5 또는 이상을 사용해야 합니다.
- OCI 데이터베이스 암호 소비자를 사용하려면 데이터베이스에 연결하는 응용 프로그램이 OCI8 또는 이상을 사용해야 합니다.
- 비기본 드라이버를 갖는 ODBC 또는 OLEDB 데이터베이스 암호 소비자를 사용하려면 CA Technologies Support 에 문의해야 합니다.

참고: 기본 드라이버는 ODBC 또는 OLEDB 플러그 인의 레지스트리 하위 키에 있는 ApplyOnProcess 레지스트리 항목에 정의되어 있습니다. 도움이 필요한 경우 기술 지원부(<http://ca.com/support>)에 문의하십시오.

- Java PUPM SDK 암호 소비자를 사용하려면 작성하는 Java 응용 프로그램이 JRE 1.5 또는 이상을 사용해야 합니다.
- .NET PUPM SDK 암호 소비자를 사용하려면 끝점에 .NET Framework 2.0 또는 이상을 설치해야 합니다.
- Windows 서비스 또는 Windows 예약된 작업 암호 소비자를 만들기 위해 서비스 계정을 검색할 때 CA Access Control 은 사용자가 암호를 변경할 수 있는 계정으로 실행되는 서비스만 검색합니다.

- 도메인 계정인 서비스 계정을 검색하려면 계정이 있는 도메인 컨트롤러(DC)를 나타내는 PUPM 끝점을 만들어야 합니다. 이 끝점에는 다음과 같은 특성이 있어야 합니다.

- 끝점 유형 - Windows Agentless
- Active Directory - True
- 호스트 도메인 - DC가 구성원인 도메인 이름
- 사용자 도메인 - DC에 정의된 사용자가 구성원인 도메인 이름

참고: 계정이 있는 도메인이 아닌 다른 도메인에서 관리 계정이 온 경우에만 사용자 도메인을 지정하십시오.

추가 정보:

[서비스 계정 검색](#) (페이지 252)

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 46)

[권한 있는 계정 감사](#) (페이지 302)

암호 소비자 감사 레코드

CA Access Control 엔터프라이즈 관리는 암호 소비자가 암호를 요청하고 PUPM 에이전트가 엔터프라이즈 관리 서버에서 암호를 가져올 때마다 감사 레코드를 작성합니다. CA Access Control 엔터프라이즈 관리는 또한 암호 소비자가 암호를 요청하고 이 요청이 실패할 때(예: 암호 소비자가 액세스 권한이 없는 암호를 요청한 경우) 감사 레코드를 작성합니다.

CA Access Control 엔터프라이즈 관리는 암호 소비자가 암호를 요청하고 끝점의 PUPM 에이전트가 캐시에서 암호를 가져올 때 감사 레코드를 작성하지 않습니다.

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 만들).
- 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 306)

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.

PUPM 끝점을 CA User Activity Reporting Module 과 통합하려면 다음과 같이 합니다.

1. CA Access Control 엔터프라이즈 관리에서:
 - a. CA User Activity Reporting Module 에 대한 연결을 구성합니다.
 - b. 각 PUPM 끝점에 대해 CA Enterprise Log Manager 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 에 대한 연결을 구성하는 방법에 대한 자세한 내용은 [구현 안내서](#)를 참조하십시오. CA User Activity Reporting Module 구성 방법에 대한 자세한 내용은 CA User Activity Reporting Module 설명서를 참조하십시오.

추가 정보:

[끝점 만들기](#) (페이지 184)

[PUPM 끝점에서 감사 이벤트 보기](#) (페이지 306)

CA Service Desk Manager 통합

PUPM 은 CA Service Desk Manager 와 통신하여 권한 있는 계정 요청 및 승인 프로세스의 일부로서 티켓을 승인하고 유효성을 검사할 수 있습니다. CA Service Desk Manager 와 통합되면 PUPM 은 권한 있는 계정 암호에 대한 각 요청을 활성 티켓에 대해 유효성을 검사합니다. PUPM 과 CA Service Desk Manager 를 통합하면 여러 승인 프로세스를 포함하는 권한 있는 계정 요청에 대한 유효성 검사 프로세스를 만들 수 있습니다.

CA Service Desk Manager 와 권한 있는 계정 요청을 통합하는 방법

CA Service Desk Manager 와 PUPM 을 통합하는 방법을 이해하면 CA Service Desk Manager 에 대한 연결을 설정하고 유효성 검사 프로세스를 구현하는데 도움이 됩니다.

CA Service Desk Manager 와 PUPM 을 통합하려면 다음을 수행하십시오.

1. CA Service Desk Manager 를 배포하고 구성합니다.
2. CA Access Control 엔터프라이즈 관리에서 CA Service Desk Manager 에 대한 연결을 구성합니다.
3. CA Service Desk Manager 를 사용하여 권한 있는 계정에 대한 액세스를 요청하는 서비스 데스크 티켓을 개설합니다.
4. CA Service Desk Manager 를 사용하여 서비스 데스크 요청을 승인합니다.
5. CA Access Control 엔터프라이즈 관리에서 권한 있는 계정 요청을 만들고 CA Service Desk Manager 티켓 번호를 제공합니다.
6. 권한 있는 계정 요청을 승인 또는 거부합니다.

CA Service Desk Manager 에 대한 연결 구성

PUPM 을 CA Service Desk Manager 와 통합하기 위해 CA Access Control 엔터프라이즈 관리에서 CA Service Desk Manager 에 대한 연결을 정의합니다.

CA Service Desk Manager 에 대한 연결을 구성하려면

1. CA Access Control 엔터프라이즈 관리에서 "시스템", "연결 관리", CA Service Desk Manager, 관리되는 CA Service Desk Manager 연결을 선택합니다.

"관리되는 CA Service Desk Manager 연결" 창이 열립니다.

2. 다음을 사용하여 양식을 완료합니다.

연결 이름

연결 이름을 정의합니다.

기본값: 주 CA Service Desk Manager 연결

연결 유형

연결 유형을 지정합니다.

기본값: CA Service Desk Manager

연결 설명

연결에 대한 설명을 지정합니다.

호스트 이름

CA Service Desk Manager 웹 서비스 URL 을 정의합니다.

기본값:

`http://host_name:8080/axis/services/USD_R11_WebService?wsdl`

사용자 ID

CA Service Desk Manager 에 연결할 때 사용한 사용자 ID 를 정의합니다.

참고: 웹 서비스 API 를 통해 서비스 데스크 티켓을 쿼리하려면 사용자에게 권한이 있어야 합니다.

암호

사용자 ID 의 암호를 정의합니다.

필수

권한 있는 계정에 대한 액세스를 요청할 때 사용자가 티켓 번호를 입력해야 하는지 여부를 지정합니다.

참고: 선택하지 않는 경우 권한 있는 계정에 대한 액세스를 요청할 때 티켓 번호를 입력하는 것이 강제되지 않습니다.

사용

연결의 활성화 여부를 지정합니다.

참고: 선택하지 않은 경우 티켓 번호 필드는 요청 권한 있는 계정 작업에 표시되지 않습니다.

고급

고급 설정을 정의할지 여부를 지정합니다. 이 옵션을 선택하면 다음 필드가 나타납니다.

티켓 유형

권한 있는 계정 암호를 요청하는 데 사용되는 CA Service Desk Manager 티켓의 유형을 정의합니다.

제한: cr, iss, chg

기본값: cr

참고: 이 필드는 대/소문자를 구분합니다.

티켓 쿼리

티켓의 유효성을 검사하는 데 사용된 사용자 지정 쿼리를 정의합니다. 모든 올바른 CA Service Desk Manager 쿼리를 지정합니다.

예: active=1 AND status='OP

참고: 이 필드가 비어 있으면 CA Access Control 엔터프라이즈 관리는 요청자 티켓의 유효성을 검사하기 위해 모든 서비스 데스크 티켓을 열거합니다.

3. "제출"을 클릭합니다.

CA Access Control 엔터프라이즈 관리는 연결 설정을 테스트하고 커넥터 서버를 만듭니다.

참고: CA Service Desk Manager 에 대한 자세한 내용은 CA Service Desk Manager 설명서를 참조하십시오.

추가 정보:

[CA Service Desk Manager 와 권한 있는 계정 요청을 통합하는 방법](#) (페이지 145)

구현 고려 사항

다음은 PUPM 을 구현하기 전에 고려해야 할 항목을 나열합니다.

공유 계정 암호의 전자 메일 알림

때때로 CA Access Control 엔터프라이즈 관리는 사용자가 암호를 체크 아웃할 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 사용자에게 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 사용자에게 대한 제한 사항

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

Active Directory 끝점을 관리하기 위한 최소 권한

Windows 에 해당

Active Directory 를 관리하기 위해 PUPM Windows Agentless 끝점을 사용하려고 하지만 도메인 관리자 계정을 지정하고 싶지 않은 경우 일반 사용자 계정을 관리하는 데 필요한 최소 권한을 갖는 위임된 사용자를 지정할 수 있습니다.

예: Active Directory 사용자에게 Windows Server 2008 에서 다른 Active Directory 사용자를 관리하는 권한 위임

다음 예는 Windows Server 2008 에서 다른 일반 Active Directory 사용자를 관리하기 위해 일반 사용자에게 권한을 위임하는 방법을 설명합니다.

1. "시작", "관리 도구", "구성 요소 서비스"를 선택합니다.
"구성 요소 서비스" 콘솔이 열립니다.
2. "구성 요소 서비스" 목록을 확장하고 "컴퓨터"를 선택한 다음 "내 컴퓨터"를 마우스 오른쪽 단추로 클릭하고 "속성"을 선택합니다.
"내 컴퓨터" 속성 창이 열립니다.
3. "COM 보안" 탭으로 이동하여 다음을 수행합니다.
 - a. "액세스 권한" 섹션에서 "기본값 편집"을 클릭합니다.
 - b. "추가"를 클릭하여 액세스 권한을 할당할 사용자 계정을 찾습니다.
 - c. "시작 및 활성화 권한" 섹션에서 "기본값 편집"을 선택합니다.
 - d. "추가"를 클릭하여 액세스 권한을 할당할 사용자 계정을 찾습니다.
 - e. "허용" 열 아래에서 "로컬 액세스"와 "원격 액세스" 및 "로컬 활성화"와 "원격 활성화" 옵션을 선택합니다.
 - f. "확인"을 클릭하고 속성 창을 종료합니다.

4. "시작", "관리 도구", "Active Directory 사용자 및 컴퓨터"를 차례로 선택합니다. 다음 작업을 수행하십시오.
 - a. "사용자" 목록에서 사용자 계정을 마우스 오른쪽 단추로 클릭합니다.
 - b. "소속 그룹" 탭으로 이동한 다음 "그룹에 추가"를 선택합니다.
 - c. 사용자를 다음 그룹의 구성원으로 추가한 다음 "확인"을 클릭합니다.

- Domain Users

- Distributed COM Users

위임된 사용자에게 대한 보안 특성을 구성했습니다. 이제 이 사용자가 관리할 컨테이너의 보안 특성을 구성합니다.

5. "Active Directory 사용자 및 그룹" 콘솔에서 "사용자" 폴더를 마우스 오른쪽 단추로 클릭한 다음 "속성"을 선택합니다.
6. "보안" 탭으로 이동한 다음 "사용자 추가"를 선택하고 "고급"을 클릭합니다.

고급 보안 설정 창이 열립니다. 다음 작업을 수행하십시오.

- a. "권한" 탭에서 사용자를 선택하고 "편집"을 클릭합니다.
권한 항목 창이 열립니다.
- b. "적용 대상" 목록에서 "하위 사용자 개체"를 선택하고 다음 권한을 적용합니다.

- 내용 보기
- 모든 속성 읽기
- 모든 속성 쓰기
- 권한 읽기
- 권한 수정
- 암호 변경
- 암호 다시 설정

- c. "확인"을 클릭하고 속성 창을 종료합니다.

"사용자" 컨테이너의 사용자에게 대한 보안 특성을 구성했습니다.

7. "명령 프롬프트" 창에서 `wmimgmt` 명령을 실행하여 WMI 컨트롤 콘솔을 엽니다. 다음 작업을 수행하십시오.

- a. "WMI 컨트롤"을 마우스 오른쪽 단추로 클릭한 다음 "속성"을 선택합니다.

WMI 컨트롤 속성 창이 열립니다.

- b. "보안" 탭으로 이동하여 루트 디렉터리를 확장합니다.
- c. 디렉터리를 선택한 다음 "보안" 단추를 클릭합니다.
- d. "추가"를 클릭하여 편집할 사용자 계정을 추가한 다음 루트 네임스페이스와 하위 네임스페이스에 대해 다음 권한을 추가합니다.

- 일부 쓰기
- 공급자 쓰기
- 계정 사용
- 원격으로부터 사용 가능

- e. WMI 컨트롤 콘솔을 닫습니다.

8. "명령 프롬프트" 창에서 **regedit** 유틸리티를 실행하고 다음 레지스트리 항목을 찾습니다.

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

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

9. 각 레지스트리 키를 마우스 오른쪽 단추로 클릭한 다음 "사용 권한"을 선택합니다.

사용 권한 창이 열립니다.

10. 사용자를 목록에 추가하고 해당 키와 자식 개체에 "모든 권한"을 할당합니다.

11. "확인"을 클릭하여 **regedit** 유틸리티를 닫습니다.

일반 Active Directory 사용자에게 다른 일반 Active Directory 사용자를 관리하는 권한을 위임했습니다.

고급 CA Access Control 와 PUPM 통합 제한

고급 CA Access Control 와 PUPM 통합(터미널 통합)을 사용하면 권한 있는 계정으로 사용하여 CA Access Control 끝점에 로그인하는 사용자의 원래 사용자 이름을 추적할 수 있습니다.

사용자들이 자동 로그인을 사용하여 CA Access Control 엔터프라이즈 관리에서 권한 있는 계정을 체크 아웃하는 경우에만 고급 CA Access Control 와 PUPM 통합을 사용할 수 있습니다.

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 Support](#)에서 CA Identity Manager 북셀프에 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: SUN ONE 끝점 구성

이 예에서 시스템 관리자인 Steve 는 SUN ONE 디렉터리에 연결하기 위해 Connector Xpress 에서 SUN ONE 끝점을 만듭니다.

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

1. "시작" 메뉴로 이동하여 "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. JNDI 를 선택하고 "확인"을 클릭합니다.

"Edit Source"(원본 편집) 창이 열립니다.

5. 다음 세부 정보를 입력합니다.

- 이름 - SUN ONE
- 서버 이름 - server1
- 포트 - 389
- 바이트 DN -
uid=user1,ou=cont1,ou=ldapConnector,dc=company,dc=com

중요! 디렉터리 관리자 계정이 아닌 기존 디렉터리 사용자 계정을 지정하십시오. 이 계정은 기본 DN 바로 아래에 있지 않습니다.

- Base DN - ou=ldapConnector,dc=company,dc=com

6. "Test"(테스트)를 클릭하여 연결 설정을 검사합니다.

데이터 원본에 대한 암호 입력 창이 열립니다.

7. administrator 계정 암호를 입력한 다음 "확인"을 클릭합니다.

오류가 발견되지 않으면 확인 메시지가 표시됩니다. 새 데이터 원본이 만들어졌습니다. Steve 는 이제 새 프로젝트를 만듭니다.

8. 프로젝트, 새로 만들기, 데이터 원본, 편집을 선택하고 administrator 계정 암호를 입력합니다.

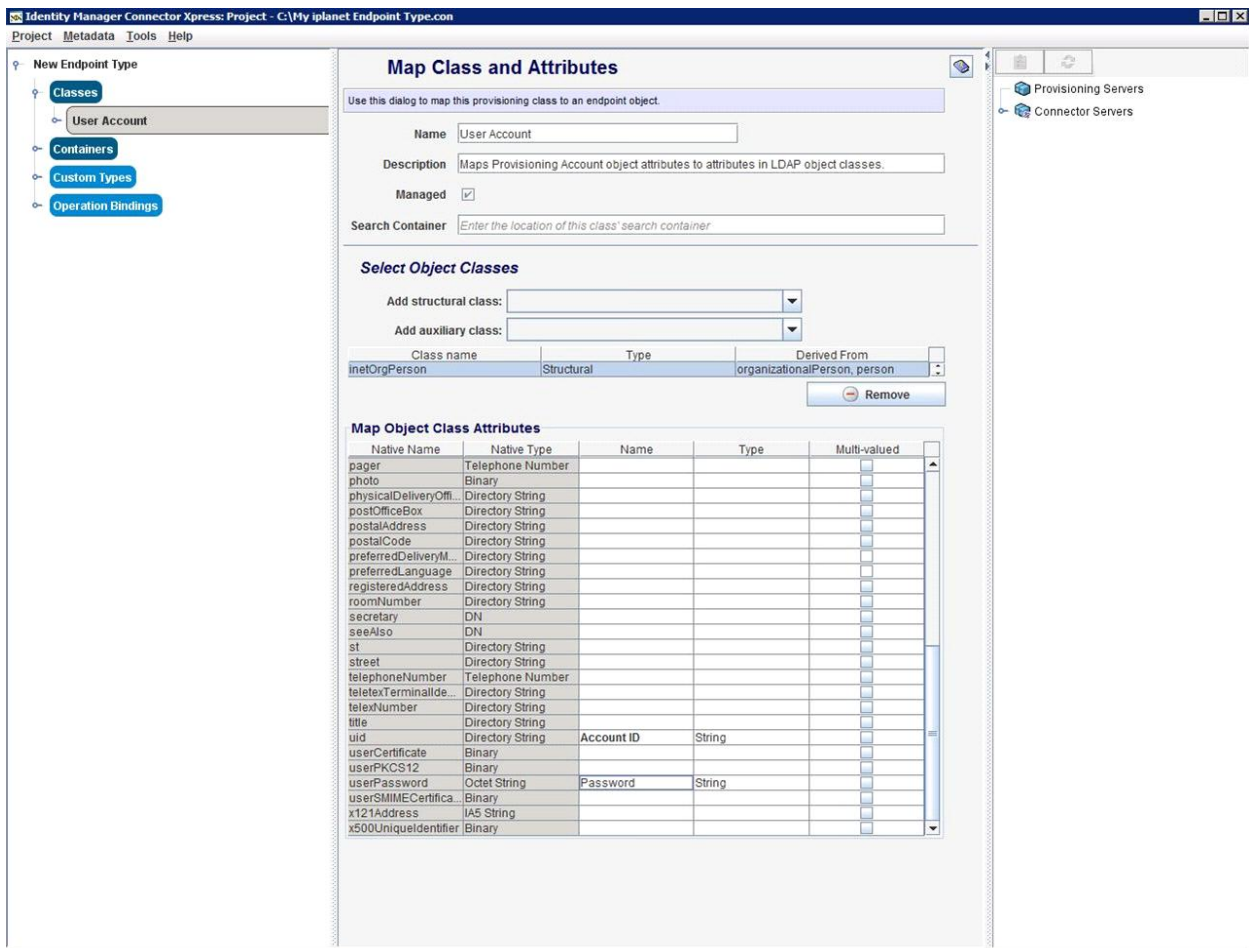
"Endpoint Type Details"(끝점 유형 정보) 화면이 열립니다.

9. 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.

10. "Select Object Classes"(개체 클래스 선택)에서 구조 클래스 inetOrgPerson 을 추가하고 다음 특성을 매핑합니다.

- cn - AccountID
- sn - 성(이름)
- uid -AccountID
- userPassword - 사용자 계정 암호



11. 프로젝트를 저장하여 끝점 유형 정의를 저장합니다.

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

Connector Xpress 예제: Java Connector Server 에서 SUN One 끝점 유형 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.

추가 정보:

[Connector Xpress 예제: 끝점 유형을 엔터프라이즈 관리 서버로 로드](#) (페이지 161)

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.

추가 정보:

[암호 소비자 SDK 응용 프로그램을 사용하도록 끝점을 구성하는 방법](#)
(페이지 290)

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 디렉터리에 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.

추가 정보:

[암호 소비자 SDK 응용 프로그램을 사용하도록 끝점을 구성하는 방법](#)
(페이지 290)

.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.

추가 정보:

[암호 소비자 SDK 응용 프로그램을 사용하도록 끝점을 구성하는 방법](#)
(페이지 290)

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.

추가 정보:

[웹 서비스 PUPM SDK 응용 프로그램을 사용하도록 끝점을 구성하는 방법](#)
(페이지 293)

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 사용자에게 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.

추가 정보:

[웹 서비스 PUPM SDK 응용 프로그램을 사용하도록 끝점을 구성하는 방법](#)
(페이지 293)

제 6 장: 공유 계정 구현

이 섹션은 다음 항목을 포함하고 있습니다.

[공유 계정 설정 방법](#) (페이지 171)

[암호 정책 만들기](#) (페이지 180)

[PUPM 끝점 및 공유 계정 만들기](#) (페이지 184)

[PUPM 끝점 및 공유 계정을 가져오는 방법](#) (페이지 234)

[암호 소비자를 설정하는 방법](#) (페이지 248)

[PUPM 자동 로그인](#) (페이지 260)

공유 계정 설정 방법

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

다음 프로세스는 공유 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.

공유 계정을 설정하려면 사용자가 다음을 수행해야 합니다.

1. PUPM 대상 시스템 관리자가 암호 정책을 만듭니다. 암호 정책은 공유 계정에 대한 암호 규칙 및 제한을 설정합니다.
2. PUPM 대상 시스템 관리자가 CA Access Control 엔터프라이즈 관리에 끝점을 만듭니다. 끝점은 공유 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 공유 계정을 만듭니다. 공유 계정을 만들면 PUPM 이 계정을 관리할 수 있습니다. CA Access Control 엔터프라이즈 관리에 공유 계정을 만들거나 PUPM 피더를 사용하여 공유 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 공유 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.

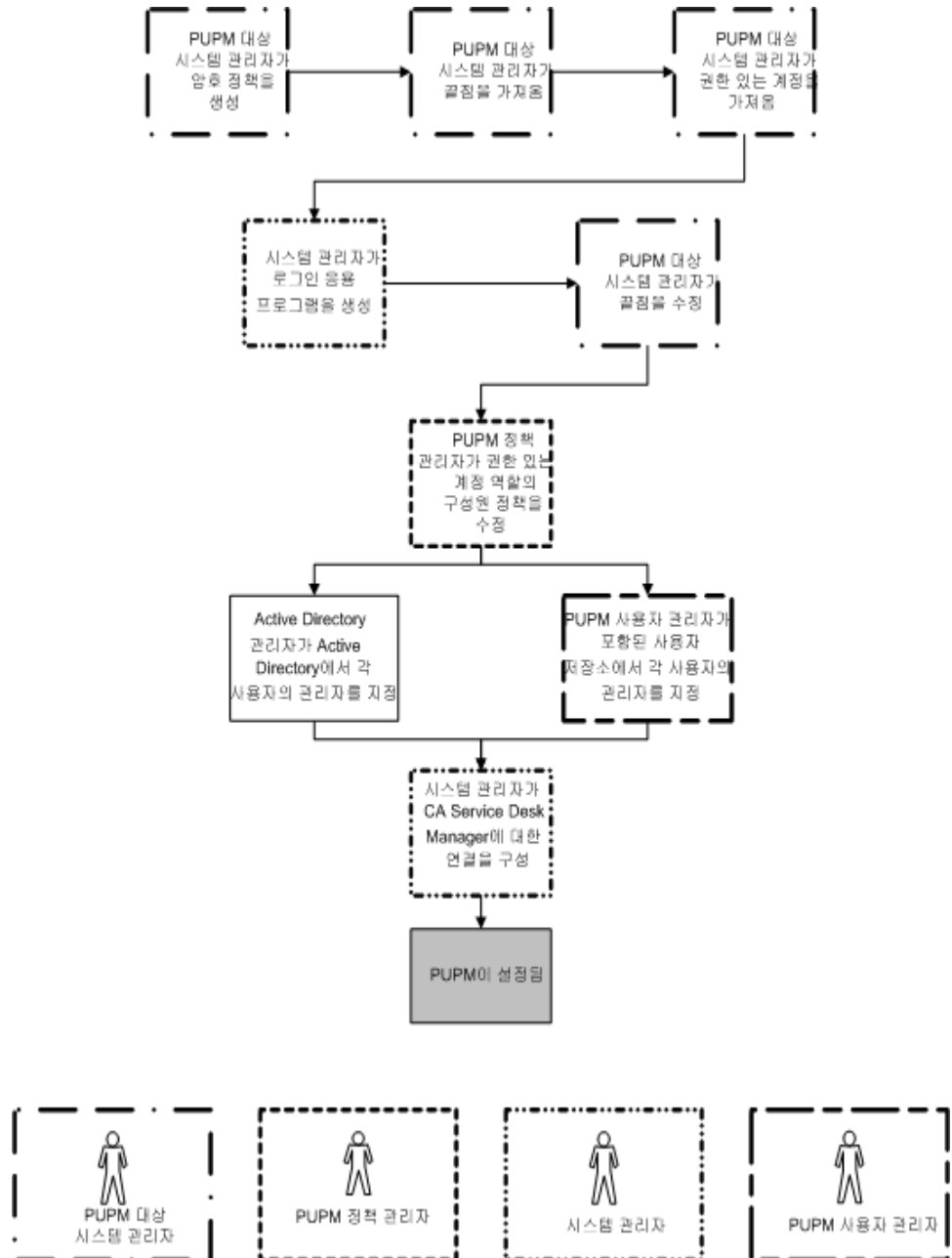
6. (포함된 사용자 저장소) PUPM 사용자 관리자는 각 사용자의 관리자를 지정합니다.

참고: 관리자만 사용자의 공유 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 CA Service Desk Manager 에 대한 연결을 구성합니다.

CA Service Desk Manager 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.

권한 있는 계정을 검색하려면

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.

배타적 세션은 끝점에서 현재 실행 중인 열린 세션이 없는 경우 단 하나의 사용자만 계정을 사용할 수 있도록 지정합니다.

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.

서비스 계정

검색한 계정이 서비스 계정인지 여부를 지정합니다.

참고: 서비스 계정 검색 마법사를 사용하여 서비스 계정을 검색할 수도 있습니다.

"마침"을 클릭합니다.

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

추가 정보:

[서비스 계정 검색](#) (페이지 252)

권한 있는 계정 또는 서비스 계정 만들기

관리되는 시스템 및 연결 해제된 시스템에서 계정 암호를 관리하기 위해 권한 있는 계정 및 서비스 계정을 만듭니다. 권한 있는 계정 및 서비스 계정은 다른 용도로 사용됩니다.

- 사용자가 권한 있는 계정 암호를 체크 아웃 및 체크 인하도록 하려면 권한 있는 계정을 만듭니다.
- CLI, 데이터베이스 또는 Windows RunAs 암호 소비자를 설정하려면 권한 있는 계정을 만듭니다.
- Windows 서비스 및 Windows 예약된 작업 암호 소비자를 설정하려면 서비스 계정을 만듭니다.

참고: 서비스 계정 암호는 체크 아웃 및 체크 인할 수 없습니다.

여러 계정을 만들려면 권한 있는 계정 검색 마법사와 서비스 계정 검색 마법사를 사용하여 끝점에서 권한 있는 계정 및 서비스 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 직접 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 계정 또는 서비스 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 계정에 사용할 암호를 정의합니다.

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.

배타적 세션은 끝점에서 현재 실행 중인 열린 세션이 없는 경우 단 하나의 사용자만 계정을 사용할 수 있도록 지정합니다.

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.

5. (선택 사항) "암호 소비자" 탭으로 이동합니다.

구성된 경우 CA Access Control 엔터프라이즈 관리는 권한 있는 계정을 사용하는 암호 소비자를 표시합니다.

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 관리가 새 권한 있는 계정 또는 서비스 계정을 만듭니다.

암호 정책 만들기

권한 있는 계정에 대한 암호 정책은 허용되는 권한 있는 계정 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 PUPM 이 계정에 대한 새 암호를 자동으로 만드는 간격을 결정합니다.

참고: PUPM 에는 사용 가능한 미리 정의된 암호 정책이 포함되어 있습니다. 회사의 보안 요구 사항을 충족하고 각 끝점에 적절한 암호 정책을 정의하여 사용하는 것이 좋습니다.

다음 단계를 수행하십시오.

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. (선택 사항) 계정 암호 시도에 대한 유예 기간(일)을 정의합니다. 이 기간이 경과하면 PUPM 은 암호 변경 실패를 추적합니다. 기본적으로 유예 기간은 0 으로 설정됩니다.

참고: "암호 변경 실패" 화면에서 검토할 수 있도록 암호 변경 실패를 CSV 파일로 내보낼 수 있습니다.

10. "제출"을 클릭합니다.

CA Access Control 엔터프라이즈 관리가 암호 정책을 만듭니다.

추가 정보:

[암호 조합 규칙](#) (페이지 182)

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

- ***** - lkl&5Jj@ 또는 sffIU*&1 에 일치
- llllaaaa - yuUI1Uo3 또는 qWcV1Er6 에 일치

금지된 문자

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

PUPM 끝점 및 공유 계정 만들기

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

여러 PUPM 끝점 또는 공유 계정을 만들거나 수정하려면 PUPM 피더의 사용을 고려하십시오. PUPM 피더를 사용하면 한 단계로 많은 끝점 및 공유 계정을 가져올 수 있으며, PUPM 끝점 및 공유 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 끝점에 대한 기준으로 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 기록할 정보(일반 텍스트)를 정의합니다.

끝점 유형

권한 있는 계정 또는 서비스 계정이 있는 끝점의 유형을 지정합니다.

참고: 끝점 유형을 선택할 때는 해당 끝점 유형에서 권한 있는 계정을 관리하기 위해 PUPM 이 요구하는 자격 증명을 제공할 수 있는 추가 대화 상자가 열립니다. 선택하는 끝점 유형은 제공해야 하는 연결 정보에 영향을 줍니다.

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.

고급 로그인 사용 안 함

이 끝점에 대해 고급 로그인 옵션을 사용하지 않도록 지정합니다.

6. (선택 사항) CA Enterprise Log Manager 탭을 클릭하고 탭에 있는 필드를 완성합니다.

이 탭을 사용하여 CA Access Control 엔터프라이즈 관리에서 PUPM 끝점의 권한 있는 계정 감사 이벤트에 대한 CA Enterprise Log Manager 보고서를 볼 수 있습니다. CA Enterprise Log Manager 에 대한 연결을 구성하지 않은 경우 이 탭은 표시되지 않습니다.

Host Name(호스트 이름)

CA Enterprise Log Manager 에 지정된 대로 호스트 이름을 정의합니다.

이 필드에 값을 입력하지 않으면 CA Access Control 엔터프라이즈 관리의 "일반" 탭의 "이름" 필드에 지정하는 호스트 이름을 사용합니다.

이벤트 로그 이름

CA Enterprise Log Manager 에 지정된 대로 이벤트 로그 이름을 정의합니다. 예를 들어, Windows Agentless 끝점의 이벤트 로그 이름은 NT-Security 와 같을 수 있습니다..

이 필드에 값을 입력하지 않으면 CA Access Control 엔터프라이즈 관리에서 권한 있는 계정 감사 이벤트의 보고서를 볼 때 모든 끝점 유형의 감사 이벤트가 표시됩니다.

참고: 이벤트 로그 이름에 대한 자세한 내용은 CA Enterprise Log Manager 설명서를 참조하십시오.

7. (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.

8. "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 187)

[VMware ESX/ESXi 연결 정보](#) (페이지 199)

[Windows Agentless Connection 정보](#) (페이지 199)

[SSH 장치 연결 정보](#) (페이지 212)

[SAP R3 연결 정보](#) (페이지 223)

[CA Identity Manager 프로비저닝 연결 정보](#) (페이지 226)

[연결 해제된 끝점 연결 정보](#) (페이지 230)

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.

다음에 주의하십시오.

"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

향상된 기능 사용

권한 있는 계정 및 서비스 계정을 관리하기 위해 끝점에서 CA Access Control 을 사용하도록 지정합니다.

참고: CA Access Control r12.6.01 및 이상 버전에서만 지원됩니다.

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.

배타적 세션 비활성화

이 끝점에서 배타적 세션 검사를 비활성화할지 여부를 지정합니다. 선택하면 PUPM 이 끝점에서 열린 세션을 검사하지 않습니다.

배타적 Break-Glass 거부

배타적 계정에 대해 Break-Glass 체크 아웃 작업을 차단하도록 지정합니다.

ACF2 연결 정보

ACF2 끝점을 사용하면 권한 있는 ACF2 계정을 관리할 수 있습니다.

이 유형의 끝점을 만들 때는 Enterprise Management Server 가 이 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.

다음에 주의하십시오.

"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.

예: `cn=user1,acf2admingrp=lids,host=ACF2,o=company,c=com`

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.

참고: 자신 및 다른 사용자 계정에 대한 관리 권한으로 사용자 계정을 지정합니다.

IBM OS/400 연결 정보

IBM OS/400 끝점 유형을 사용하면 권한 있는 IBM OS/400 관리되는 계정을 관리할 수 있습니다.

IBM OS/400 끝점에 대해 지정하는 관리 사용자는 다음 권한이 있어야 합니다.

- 다른 사용자 계정 보기
- 자체 사용자 계정 보기
- 다른 사용자 계정 암호 보기

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

이름

끝점의 이름을 지정합니다.

중요! 끝점 이름은 호스트 이름과 일치해야 합니다.

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.

다음에 주의하십시오.

"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.

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.

중요! 호스트 이름은 끝점 이름과 일치해야 합니다.

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.

다음에 주의하십시오.

"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.

배타적 세션 비활성화

이 끝점에서 배타적 세션 검사를 비활성화할지 여부를 지정합니다. 선택하면 PUPM 이 끝점에서 열린 세션을 검사하지 않습니다.

배타적 Break-Glass 거부

배타적 계정에 대해 Break-Glass 체크 아웃 작업을 차단하도록 지정합니다.

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.

다음에 주의하십시오.

"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:drvertype:@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.

배타적 세션 비활성화

이 끝점에서 배타적 세션 검사를 비활성화할지 여부를 지정합니다. 선택하면 PUPM 이 끝점에서 열린 세션을 검사하지 않습니다.

배타적 Break-Glass 거부

배타적 계정에 대해 Break-Glass 체크 아웃 작업을 차단하도록 지정합니다.

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.

다음에 주의하십시오.

"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.

배타적 세션 비활성화

이 끝점에서 배타적 세션 검사를 비활성화할지 여부를 지정합니다. 선택하면 PUPM 이 끝점에서 열린 세션을 검사하지 않습니다.

배타적 Break-Glass 거부

배타적 계정에 대해 Break-Glass 체크 아웃 작업을 차단하도록 지정합니다.

RACF 연결 정보

RACF 끝점을 사용하면 권한 있는 RACF 계정을 관리할 수 있습니다.

RACF 끝점을 만드는 경우 끝점에 엔터프라이즈 관리 서버를 연결하기 위한 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.

다음에 주의하십시오.

- "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.

중요! "IBM LDAP 사용" 옵션을 지정하는 경우 IBM LDAP 사용자 로그인을 입력하십시오.

예: (CA LDAP) cn=user1,host=RACF,o=company,c=com

예: (IBM LDAP) racfid=user1,profiletype=user,host=RACF,o=company,c=com

중요! 관리자 권한에는 PASSWORD 또는 PHRASE 옵션이 할당된 NOEXPIRES 피연산자가 있어야 합니다.

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.

예: (CA LDAP) ldap://host_name.company.com:1589

예: (IBM LDAP) ldap://host_name.company.com:389

IBM LDAP 사용

IBM LDAP 가 RACF 를 관리할지 여부를 지정합니다.

참고: "IBM LDAP 사용" 옵션을 지정하는 경우 IBM LDAP 사용자 로그인, 암호, URL 을 각각 입력하십시오.

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.

참고: 자신 및 다른 사용자 계정에 대한 관리 권한으로 사용자 계정을 지정합니다.

RACF 커넥터에 대한 SSL 통신 구성

SSL 을 통해 RACF 와 CA Access Control 사이의 연결 보안을 유지할 것을 권장합니다. SSL 을 사용하면 데이터를 암호화할 수 있고 보안 위험을 줄일 수 있습니다. 엔터프라이즈 관리 서버에 RACF 인증서를 설치함으로써 엔터프라이즈 관리 서버가 SSL 을 통해 RACF 끝점과 통신하도록 구성할 수 있습니다.

참고: 이 절차는 RACF 끝점에서 SSL 을 구성했고 RACF 인증서를 획득했다고 가정합니다.

중요! 고가용성을 위해 구성된 환경에서 이 절차를 모든 배포 및 커넥터 서버(주, 보조, 배포 서버)에 대해 수행하십시오.

다음 단계를 수행하십시오.

1. Windows 시작 메뉴, "설정", "제어판", "서비스"를 클릭합니다.
"Windows 서비스" 대화 상자가 표시됩니다.
2. "CA Identity Manager - Connector Server (Java)" 서비스를 중지합니다.
3. RACF 인증서를 다음 위치에 복사합니다.

`CA_home\AccessControlServer\Connector Server\conf`

CA_home

CA 제품을 설치한 디렉터리를 지정합니다.

4. 명령 프롬프트 창을 엽니다.
5. `CA_home\AccessControlServer\Connector Server\conf` 로 이동합니다.
6. 다음 명령을 실행합니다.

```
keytool -importcert -trustcacerts -file your_RACF_certificate -keystore  
ssl.keystore
```

참고: 암호를 묻으면 통신 암호를 입력하십시오.

RACF 인증서가 JCS 에 등록되었습니다.

7. "Windows 서비스" 대화 상자를 엽니다.
8. "CA Identity Manager - Connector Server (Java)" 서비스를 시작합니다.

RACF 와 CA Access Control 사이의 연결 보안을 성공적으로 구성했습니다.

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 엔터프라이즈 관리가 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 PUPM은 관리 작업을 수행하기 위해 "사용자 로그인" 계정을 사용하지 않습니다. 대신, PUPM은 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 PUPM은 관리 작업을 수행하기 위해 "사용자 로그인" 계정을 사용하지 않습니다.

Windows Agentless Connection 정보

Windows Agentless 끝점 유형을 사용하면 원격 끝점에 CA Access Control을 설치하지 않고도 로컬 Windows 계정 및 Active Directory 계정을 모두 관리할 수 있습니다.

권한 있는 계정 암호를 관리하기 위해 CA Access Control은 관리 계정을 사용하여 원격 컴퓨터에서 끝점에 연결합니다. 관리되는 끝점에 정의된 로컬 관리자 계정이나 Active Directory 계정을 사용할 수 있습니다.

로컬 Windows 계정 관리

PUPM은 Windows 서버 로컬 리포지토리에 정의된 로컬 관리자 계정을 사용하여 로컬 Windows 계정을 관리할 수 있게 해 줍니다. 로컬 Windows 계정을 관리하려면 Windows Agentless 끝점을 정의하고 다음 정보를 제공하십시오.

사용자 로그인

끝점을 관리하는 관리 사용자의 이름을 정의합니다. PUPM은 이 계정을 사용하여 끝점에서 관리 작업(끝점에 연결하고, 계정을 검색하고, 암호를 변경하는 등의 작업)을 수행합니다.

이 필드에 *사용자 이름*을 지정하십시오. *컴퓨터 이름/사용자 이름* 형식 또는 *도메인 이름/사용자 이름* 형식을 사용하지 마십시오.

예: Administrator.

참고: "고급" 옵션을 지정하면 PUPM은 관리 작업을 수행하기 위해 "사용자 로그인" 계정을 사용하지 않습니다. 대신, PUPM은 "고급" 옵션 아래에 지정된 계정을 사용하여 끝점에서 관리 작업을 수행합니다.

암호

끝점의 관리 사용자 암호를 정의합니다.

참고: "고급" 옵션을 사용하는 경우 암호를 제공하지 마십시오.

호스트

이 옵션은 Windows 끝점의 호스트 DNS 이름을 정의합니다.

예: myhost-ac-1.ca.com

참고: IP 주소를 호스트 이름으로 사용할 수도 있습니다.

호스트 도메인

호스트 이름(NETBIOS 이름)을 지정합니다.

참고: DNS 이름(computer1.ca.com)을 사용하지 말고 대신 NETBIOS 이름(computer1)을 사용하십시오.

Active Directory

이 옵션을 선택하지 마십시오. 이 옵션은 Active Directory 계정을 관리할 때만 유효합니다.

사용자 도메인

"고급" 옵션이 선택된 경우 이 필드를 지정하십시오. "고급" 필드에 설명된 권한 있는 계정의 NETBIOS 도메인 이름을 제공합니다.

고급

끝점에서 관리 작업을 수행하기 위해 이전에 정의된 권한 있는 관리 계정을 사용할지 여부를 지정합니다. 예를 들어, PUPM은 "사용자 로그인" 필드에 지정된 계정을 사용하지 않고 "고급" 필드에 정의된 계정을 사용하여 이 끝점을 관리합니다. 이 옵션은 동일한 권한 있는 계정을 사용하여 여러 끝점을 관리할 때 유용합니다.

참고: 이 옵션을 지정하면 PUPM은 관리 작업을 수행하기 위해 "사용자 로그인" 계정을 사용하지 않습니다.

배타적 세션 비활성화

이 옵션은 이 끝점에서 배타적 세션 검사를 비활성화할지 여부를 지정합니다. 선택하면 PUPM이 끝점에서 열린 세션을 검사하지 않습니다.

Active Directory 계정 관리

PUPM은 Active Directory의 사용자를 관리할 수 있습니다. Active Directory 계정을 관리하려면 Windows Agentless 끝점을 정의하고 다음 정보를 제공하십시오.

사용자 로그인

끝점을 관리하는 관리 사용자의 이름을 정의합니다. PUPM은 이 계정을 사용하여 끝점에서 관리 작업(끝점에 연결하고, 계정을 검색하고, 암호를 변경하는 등의 작업)을 수행합니다.

이 필드에 *사용자 이름*을 지정하십시오. *컴퓨터 이름/사용자 이름* 형식 또는 *도메인 이름/사용자 이름* 형식을 사용하지 마십시오.

예: Administrator.

참고: "고급" 옵션을 지정하면 PUPM은 관리 작업을 수행하기 위해 "사용자 로그인" 계정을 사용하지 않습니다. 대신, PUPM은 "고급" 옵션 아래에 지정된 계정을 사용하여 끝점에서 관리 작업을 수행합니다.

암호

끝점의 관리 사용자 암호를 정의합니다.

참고: "고급" 옵션을 사용하는 경우 암호를 제공하지 마십시오.

호스트

Active Directory DNS 도메인 이름을 정의합니다.

예: ca.com

참고: PUPM은 도메인 이름에서 Active Directory 도메인 컨트롤러를 확인하려고 시도합니다. PUPM이 이 이름을 확인하지 못하면 Active Directory 도메인 컨트롤러(DC) DNS 이름 또는 IP 주소를 지정하십시오.

호스트 도메인

도메인 이름(NETBIOS 이름)을 지정합니다.

예: domain1

참고: DNS 이름(domain1.ca.com)을 사용하지 말고 대신 NETBIOS 이름(domain1)을 사용하십시오.

Active Directory

Active Directory를 지정하려면 이 옵션을 선택하십시오.

사용자 도메인

"사용자 로그인" 필드 또는 "고급" 필드("고급"이 사용되는 경우)에 지정된 사용자의 도메인 이름(NETBIOS 도메인 이름)을 지정합니다.

예: domain1

참고: DNS 이름(domain1.ca.com)을 사용하지 말고 대신 NETBIOS 이름(domain1)을 사용하십시오.

고급

끝점에서 관리 작업을 수행하기 위해 이전에 정의된 권한 있는 관리 계정을 사용할지 여부를 지정합니다. 예를 들어, PUPM은 "사용자 로그인" 필드에 지정된 계정을 사용하지 않고 "고급" 필드에 정의된 계정을 사용하여 이 끝점을 관리합니다. 이 옵션은 동일한 권한 있는 계정을 사용하여 여러 끝점을 관리할 때 유용합니다.

참고: 이 옵션을 지정하면 PUPM은 관리 작업을 수행하기 위해 "사용자 로그인" 계정을 사용하지 않습니다.

배타적 세션 비활성화

이 옵션은 이 끝점에서 배타적 세션 검사를 비활성화할지 여부를 지정합니다. 선택하면 PUPM이 끝점에서 열린 세션을 검사하지 않습니다.

PUPM에 대한 Windows Agentless 끝점 구성

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

추가 정보:

[Windows Agentless 끝점의 도메인 사용자에 대한 제한 사항](#) (페이지 148)

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. 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 204)

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.

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.
8. "시작", "관리 도구", "로컬 보안 정책"을 클릭합니다.
 "로컬 보안 정책" 관리 콘솔이 열립니다.

9. "로컬 정책", "보안 옵션"을 선택합니다.

사용 가능한 보안 옵션의 목록이 표시됩니다.

10. 다음 보안 정책을 찾습니다.

- 네트워크 보안: NTLM SSP 기반(보안 RPC 포함) 클라이언트에 대한 최소 세션 보안
- 네트워크 보안: NTLM SSP 기반(보안 RPC 포함) 클라이언트에 대한 최소 세션 보안

11. 각 정책을 마우스 오른쪽 단추로 클릭하고 "속성"을 선택합니다.

로컬 보안 설정 탭이 열립니다.

12. 128 비트 암호화 요구 옵션이 선택되지 않았는지 확인합니다.

13. "확인"을 클릭하여 종료합니다.

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.

관리자 승인 모드 수정

Windows Server 2008 및 Windows 7 에 해당

PUPM 끝점 관리 작업은 백그라운드로 실행되며 네이티브 관리자 계정의 액세스 권한이 필요합니다. PUPM 끝점 관리자가 이 네이티브 관리자 계정에 대한 액세스 권한이 없는 경우 모든 끝점 관리자가 관리자 승인 모드에서 실행하도록 허용해야 합니다.

중요: 이 정책 설정이 비활성화되면 보안 센터에서 운영 체제의 전체적인 보안이 낮아졌음을 알리는 통보를 보냅니다.

다음 단계를 수행하십시오.

1. "제어판", "관리 도구", "로컬 보안 정책"을 선택합니다.
"로컬 보안" 창이 열립니다.
2. "로컬 정책", "보안 옵션"으로 이동합니다.
"정책" 창이 열립니다.

3. "사용자 계정 컨트롤: 관리 승인 모드에서 모든 관리자 실행"을 마우스 오른쪽 단추로 클릭하고 "속성"을 선택합니다.
"속성" 대화 상자가 나타납니다.
4. 실행 모드를 "사용 안 함"으로 변경하고 "확인"을 클릭합니다.
"속성" 대화 상자가 닫힙니다.
5. 변경 사항이 적용되도록 컴퓨터를 다시 시작합니다.
백그라운드 끝점 관리 작업이 이제 성공적으로 실행됩니다.

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. PUPM은 이 계정을 사용하여 끝점에서 관리 작업(끝점에 연결하고, 계정을 검색하고, 암호를 변경하는 등의 작업)을 수행합니다.

다음에 주의하십시오.

"고급" 옵션을 지정하면 PUPM은 관리 작업을 수행하기 위해 "사용자 로그인" 계정을 사용하지 않습니다. 대신, PUPM은 지정된 권한 있는 계정을 사용하여 끝점에서 관리 작업을 수행합니다. 작업 관리자 계정을 지정하는 경우 PUPM은 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. PUPM은 이 계정을 사용하여 끝점에서 관리 작업(예: 권한 있는 계정의 암호 검색 및 변경)을 수행합니다. 작업 관리자 사용자를 지정하지 않으면 PUPM은 사용자 로그인 계정을 사용하여 끝점에서 관리 작업을 수행합니다.

Check Point Firewall을 사용하는 SSH 끝점에 대해 작업 관리자 사용자를 지정하는 경우 전문가 사용자를 지정하십시오. 하지만 PUPM을 사용하여 끝점에서 전문가 계정의 암호를 변경할 수 없습니다. 즉, 전문가 계정은 PUPM에서 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 PUPM은 관리 작업을 수행하기 위해 "사용자 로그인" 계정을 사용하지 않습니다.

배타적 세션 비활성화

이 끝점에서 배타적 세션 검사를 비활성화할지 여부를 지정합니다. 선택하면 PUPM이 끝점에서 열린 세션을 검사하지 않습니다.

배타적 Break-Glass 거부

배타적 계정에 대해 Break-Glass 체크 아웃 작업을 차단하도록 지정합니다.

PUPM이 UNIX 끝점에 연결하는 방법

끝점을 만들 때 끝점에 연결하기 위해 PUPM이 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 PUPM은 SSH를 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. (PUPM은 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 184). 만든 XML 파일의 이름을 "구성 파일" 필드에 입력합니다.

사용자 지정 설정을 사용하여 SSH 장치 끝점이 만들어집니다.

3. 만든 끝점에서 권한 있는 계정 검색 마법사를 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.

참고: SSH 장치 XML 파일의 형식에 대한 자세한 내용은 [참조 안내서](#)를 참조하십시오.

SSH 및 네트워크 장치 XML 구성 파일의 유형

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

SSH 장치 XML 파일:

- **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.
- **F5_BigIP.xml** - F5 BIG-IP 부하 분산 시스템인 SSH 장치에 대한 구성 설정을 정의합니다.
- **Macintosh_connector_conf.xml** - iOS 운영 체제를 사용하는 SSH 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 단계를 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** - passwd 명령을 사용하여 계정 암호를 변경하는 SSH 장치에 대한 구성 설정을 정의합니다.

참고: 로컬 사용자(예: root)를 연결된 사용자로 지정하십시오.

- **sudo_connector_conf.xml** - sudo 및 passwd 명령을 사용하는 SSH 장치에 대한 구성 설정을 정의합니다.
- **vms_connector_conf.xml** - VMS 끝점인 SSH 장치에 대한 구성 설정을 정의합니다.

네트워크 장치 XML 파일:

- **Cisco_3750_default.xml** - Cisco 3750 네트워크 장치인 네트워크 장치에 대한 구성 설정을 정의합니다.
- **Cisco_ASA_default.xml** - Cisco ASA 네트워크 장치인 네트워크 장치에 대한 구성 설정을 정의합니다.
- **Cisco_PIX_default.xml** - Cisco PIX 네트워크 장치인 네트워크 장치에 대한 구성 설정을 정의합니다.
- **netdevice_connector_conf.xml** - Cisco 2600 네트워크 장치인 네트워크 장치에 대한 구성 설정을 정의합니다.
- **Checkpoint_SPLAT.xml** - Checkpoint SPLAT 네트워크 장치인 네트워크 장치에 대한 구성 설정을 정의합니다.
- **Juniper_ISG.xml** - Juniper ISG 네트워크 장치인 네트워크 장치에 대한 구성 설정을 정의합니다.
- **Juniper_NetScreen.xml** - Juniper NetScreen 네트워크 장치인 네트워크 장치에 대한 구성 설정을 정의합니다.
- **Nokia_IPSO.xml** - Nokia IPSO 네트워크 장치인 네트워크 장치에 대한 구성 설정을 정의합니다.

SSH 장치 XML 파일 사용자 지정

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

SSH 장치 또는 네트워크 장치 끝점이 다른 방법으로 권한 있는 계정 암호를 변경하는 경우, 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.

SSH 장치:

`ACServerInstallDir/conf/override/sshdyn`

네트워크 장치:

`ACServerInstallDir/conf/override/netdevicedyn`

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 장치 XML 파일을 사용자 지정했습니다.

참고: SSH 장치 XML 파일의 형식에 대한 자세한 내용은 [참조 안내서](#)를 참조하십시오.

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.

네트워크 장치 연결 정보

네트워크 장치 끝점 유형은 네트워크 장치에서 권한 있는 계정 암호를 관리할 수 있게 해 줍니다.

참고: 현재까지 끝점 유형은 Cisco 2600 네트워크 장치에서만 동작하도록 구성할 수 있습니다.

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

사용자 인증

로그인 시 사용자 인증 모드를 지정합니다.

- 익명 - 로그인 시 사용자 이름이나 암호가 요구되지 않습니다.
- 암호만 - 로그인하기 위해 암호가 요구됩니다.
- 사용자 이름 및 암호 - 로그인하려면 사용자 이름과 암호가 필요합니다.

모드 인증 사용

모드를 사용하도록 장치를 설정하기 위해 인증 모드를 지정합니다.

- 익명 - 로그인 시 사용자 이름이나 암호가 요구되지 않습니다.
- 암호만 - 로그인하기 위해 암호가 요구됩니다.
- 사용자 이름 및 암호 - 로그인하려면 사용자 이름과 암호가 필요합니다.

참고: 익명 인증 모드에서 다음 필드는 비활성화되어 있습니다: 사용자 이름, 암호, 모든 사용자 이름 사용

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.

다음에 주의하십시오.

"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.

로그인 사용

모드를 사용하도록 장치를 설정할 수 있는 권한이 있는 관리 사용자의 이름을 정의합니다. 모드를 사용하면 네트워크 장치 설정을 수정할 수 있습니다.

호스트

끝점의 호스트 이름을 정의합니다.

포트

서버 수신 포트 번호를 지정합니다.

기본값: 23

텔넷 사용

SSH 장치에 연결하기 위해 SSH 대신 텔넷을 사용하도록 지정합니다.

참고: Cisco 2600 네트워크 장치에 연결하려면 텔넷 프로토콜만 사용하십시오.

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 netdevice_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 PUPM은 관리 작업을 수행하기 위해 "사용자 로그인" 계정을 사용하지 않습니다.

배타적 세션 비활성화

이 끝점에서 배타적 세션 검사를 비활성화할지 여부를 지정합니다. 선택하면 PUPM이 끝점에서 열린 세션을 검사하지 않습니다.

배타적 Break-Glass 거부

배타적 계정에 대해 Break-Glass 체크 아웃 작업을 차단하도록 지정합니다.

추가 정보:

[예: SSH 장치 XML 파일이 PUPM 명령을 정의하는 방법](#) (페이지 218)

SAP R3 연결 정보

PUPM SAP R3 끝점 유형을 사용하면 권한 있는 SAP R3 계정을 관리할 수 있습니다. PUPM 에서 SAP R3 끝점을 만들기 전에 SAP R3 커넥터를 구성해야 합니다.

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.

다음에 주의하십시오.

"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.

시스템 ID

SAP R3 시스템 ID 를 정의합니다.

시스템 번호

SAP R3 시스템 번호를 정의합니다.

클라이언트 번호

SAP R3 시스템 클라이언트 번호를 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.

참고: 시스템 ID, 시스템 번호, 클라이언트 번호에 대한 자세한 내용은 SAP R3 설명서를 참조하십시오.

SAP R3 커넥터 구성

PUPM 을 사용하여 SAP R3 끝점에서 권한 있는 계정을 관리하기 전에 SAP R3 커넥터를 구성해야 합니다.

SAP R3 커넥터를 구성하려면 엔터프라이즈 관리 서버 또는 Java Connector Server(JCS)가 설치된 모든 서버에 SAP JCo 라이브러리를 설치하십시오.

사용자 본인의 SAP 로그인을 사용하여 SAP 마켓플레이스에서 SAP JCo 라이브러리를 다운로드할 수 있습니다. 사용하는 시스템 플랫폼에 적합한 SAP JCo 라이브러리를 선택하십시오.

예: Windows 에 SAP JCo 라이브러리 설치

다음 예는 x86 Windows 2003 Server 에 SAP JCo 라이브러리를 설치하는 방법에 대해 설명합니다.

1. sapjco-ntamd64-2.1.9.zip 을 임시 디렉터리에 압축을 풉니다.
2. sapjcorfc.dll 및 librfc32.dll 파일을 Windows system32 디렉터리에 복사합니다.

참고: 이 디렉터리에 있는 기존 파일을 덮어쓸지 묻으면 모든 파일을 덮어쓰십시오.
3. sapjco.jar 파일을 Java Connector Server extlib 디렉터리에 복사합니다. 이 디렉터리는 다음 위치에 있습니다.

[set the Access Path variable]\Connector Server\extlib

4. "CA Identity Manager - 커넥터 서버" 서비스를 다시 시작합니다.

이제 PUPM 을 사용하여 SAP R3 끝점에서 권한 있는 계정을 관리할 수 있습니다.

추가 정보:

[SAP R3 연결 정보](#) (페이지 223)

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 프로비저닝 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 227)

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 작업 중 *하나*를 수행합니다.

- a. Windows 에서 "서비스" 창을 열고 "CA Identity Manager - Connector Server (Java)" 서비스를 선택한 다음 "중지"를 클릭합니다.
- b. UNIX 에서 다음 디렉터리로 이동합니다. 여기서 *ACServerInstallDir* 는 엔터프라이즈 관리 서버가 설치된 디렉터리를 나타냅니다.

ACServerInstallDir/Connector_Server/bin

- c. 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.

- JUNIPER_NETSCREEN_WEB.vbs - Juniper Netscreen 방화벽의 웹 인터페이스에 자동 로그인할 수 있게 합니다.
- MSSQL2005Studio.vbs - Microsoft SQL Server 2005 Management Studio 에 자동 로그인할 수 있게 합니다.

참고: MSSQL2005Studio 로그인 응용 프로그램을 사용하려면 컴퓨터에 Microsoft SQL Server 2005 Management Studio 를 설치하십시오.

- MSSQL2008Studio.vbs - Microsoft SQL Server 2008 Management Studio 에 자동 로그인할 수 있게 합니다.

참고: MSSQL2005Studio 로그인 응용 프로그램을 사용하려면 컴퓨터에 Microsoft SQL Server 2005 Management Studio 를 설치하십시오.

- NOKIA_IPSO_WEB.vbs - Check Point 방화벽에 있는 Nokia IPSO 운영 체제에 자동 로그인할 수 있게 합니다.
- 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 설치하십시오.
- RDP.vbs - Windows 끝점에 자동으로 로그인할 수 있게 합니다.
- RDP_Ad.vbs - Active Directory 관리 콘솔에 자동 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 다음 사항을 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.

기본적으로 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 응용 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 필드에는 기존 개체에서 가져온 값이 자동으로 입력됩니다.
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. 사용자가 로그인 응용 프로그램을 사용할 수 있도록 하려면 먼저 로그인 응용 프로그램을 사용하도록 **CA Access Control** 엔터프라이즈 관리에서 끝점을 수정하십시오. 터미널 통합을 사용하고 **Windows Server 2008** 끝점에서 로그인 응용 프로그램을 사용하려면 끝점에서 추가 구성 단계를 수행하십시오.

추가 정보:

[로그인 응용 프로그램을 사용하도록 Windows Server 2008 끝점 수정](#)
(페이지 208)

PUPM 끝점 및 공유 계정을 가져오는 방법

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

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

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

PUPM 끝점 및 공유 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.
- 공유 계정 CSV 파일을 만듭니다.

CSV 파일의 각 줄은 PUPM 끝점 또는 공유 계정을 만들거나 수정하기 위한 작업을 나타냅니다. 별도의 끝점 및 공유 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 공유 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.

끝점 CSV 파일 만들기

끝점 CSV 파일의 각 행 또는 줄(머리글 행 또는 줄 다음)은 CA Access Control 엔터프라이즈 관리에서 끝점을 만들고, 수정하고, 삭제하는 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.

DO_NOT_VALIDATE

(선택 사항) 끝점이 오프라인인지, 그리고 CA Access Control 엔터프라이즈 관리가 끝점을 만드는 동안 끝점의 유효성을 검사해야 하는지 여부를 지정합니다.

값: TRUE, FALSE

기본값: TRUE

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 PUPM은 LOGIN_USER를 사용하여 끝점에 연결하고 이 끝점에서 관리 작업(예: 계정 검색 및 암호 변경)을 수행합니다.
- 권한 있는 관리 계정을 지정하면 PUPM은 LOGIN_USER에 대한 모든 값을 무시합니다.

SSH 장치 끝점의 경우:

- 작업 관리자(OPERATION_ADMIN_USER_NAME) 또는 권한 있는 관리 계정을 지정하지 않으면 PUPM은 LOGIN_USER를 사용하여 끝점에 연결하고 이 끝점에서 관리 작업을 수행합니다.
- 작업 관리자를 지정하면 PUPM은 LOGIN_USER를 사용하여 끝점에 연결하고 작업 관리자를 사용하여 이 끝점에서 관리 작업을 수행합니다.
- 권한 있는 관리 계정을 지정하면 PUPM은 LOGIN_USER에 대한 모든 값을 무시합니다.

PASSWORD

LOGIN_USER의 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 URL을 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:driver~~type~~:@*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_USER가 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 지정하십시오. 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 지정하십시오.

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.

OWNER_INFO

끝점 소유자의 이름을 지정합니다.

DEPARTMENT_INFO

부서의 이름을 지정합니다.

CUSTOM1....5_INFO

최대 5 개까지 고객 관련 특성을 지정합니다.

ADMIN_ACCOUNT_IS_DISCONNECTED

끝점 관리자 계정의 연결이 해제되었는지 여부를 지정합니다.

값: TRUE, FALSE

기본값: TRUE

DISABLE_EXCLUSIVE_SESSIONS

이 끝점에서 배타적 세션 옵션을 비활성화할지 여부를 지정합니다.

값: TRUE, FALSE

기본값: FALSE

DENY_BREAKGLASS_EXCLUSIVE

Break Glass 를 사용하여 작업 중인 배타적 계정에 대한 액세스를 방지할지 여부를 지정합니다.

값: TRUE, FALSE

기본값: FALSE

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:

[사용자 지정된 SSH 장치 끝점을 만드는 방법](#) (페이지 214)

공유 계정 CSV 파일 만들기

권한 있는 계정 CSV 파일의 각 행 또는 줄(머리글 행 또는 줄 다음)은 CA Access Control 엔터프라이즈 관리에서 공유 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.

다음 단계를 수행하십시오.

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 *ACServerInstallDir* 는 엔터프라이즈 관리 서버를 설치한 디렉터리입니다.

ACServerInstallDir/IAMSuite/AccessControl/tools/samples/feeder

2. 공유 계정 특성의 이름을 지정하는 머리글 행 또는 줄을 만듭니다.

공유 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 공유 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

공유 계정이 있는 끝점의 이름을 지정합니다. 끝점에 대한 공유 계정을 만들려면 먼저 CA Access Control 엔터프라이즈 관리에서 끝점을 정의하십시오.

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 만드십시오.

CONTAINER

공유 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

공유 계정이 연결이 끊긴 시스템의 계정인지 여부를 지정합니다.

TRUE 로 지정하면 PUPM 이 이 계정을 관리하지 않습니다. 대신, 연결 해제된 시스템의 공유 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 사용자가 계정을 체크 아웃할 수 있는지 여부를 지정합니다.

EXCLUSIVE 로 지정하면 PUPM 은 한 번에 하나의 사용자가 계정을 체크 아웃하도록 허용합니다. EXCLUSIVE_SESSIONS 을 지정하면 PUPM 은 열린 세션 배타적 계정으로의 체크 인을 거부합니다. NONE 을 지정하면 PUPM 은 여러 사용자가 동시에 체크 아웃하도록 허용합니다.

값: EXCLUSIVE_SESSIONS, EXCLUSIVE, NONE

NEW_PASSWORD

공유 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

공유 계정의 암호 정책을 지정합니다.

참고: 존재하지 않는 암호 정책을 지정하면 작업이 실패하고 CA Access Control 엔터프라이즈 관리가 계정을 만들지 않습니다.

OWNER_INFO

계정 소유자의 이름을 지정합니다.

DEPARTMENT_INFO

부서의 이름을 지정합니다.

CUSTOM1....5_INFO

최대 5 개까지 고객 관련 특성을 지정합니다.

CHANGE_PASSWORD_ON_CHECKOUT

권한 있는 계정이 체크 아웃될 때마다 CA Access Control 엔터프라이즈 관리가 계정의 암호를 변경할지 여부를 지정합니다.

값: TRUE, FALSE

기본값: FALSE

CHANGE_PASSWORD_ON_CHECKIN

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

값: TRUE, FALSE

기본값: TRUE

3. 작업 줄을 CSV 파일에 추가합니다.

각 줄은 공유 계정을 만들거나 수정하는 작업을 나타내며, 머리글과 동일한 수의 특성 값을 가져야 합니다. 줄에 특성 값이 없는 경우 필드를 비워두십시오.

4. 파일을 폴링 폴더에 저장합니다.

공유 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/waiting
ToBeProcessed
```

예: 공유 계정 CSV 파일 만들기

다음은 샘플 공유 계정 CSV 파일입니다. 추가 샘플 공유 계정 CSV 파일은 *ACServerInstallDir\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.

암호 소비자를 설정하는 방법

암호 소비자는 스크립트를 실행하고, 데이터베이스에 연결하거나 Windows 서비스, 예약된 작업 또는 RunAs 명령을 관리하기 위해 권한 있는 계정 및 서비스 계정을 사용하는 응용 프로그램, Windows 서비스, Windows 예약된 작업입니다. 암호 소비자는 응용 프로그램 스크립트에서 하드 코드된 암호를 제거하고 서비스 계정에 암호 정책을 시행하도록 할 수 있습니다.

암호 소비자에는 두 개의 그룹이 있습니다.

- 필요 시 암호를 가져오는 암호 소비자 - 데이터베이스, Windows Run As, 소프트웨어 개발 키트
- 암호 변경 시 암호를 가져오는 암호 소비자 - Windows 예약된 작업, Windows 서비스

소프트웨어 개발 키트 암호 소비자는 권한 있는 계정 암호를 가져오고, 체크 아웃하고, 체크 인합니다. 모든 다른 유형의 암호 소비자는 권한 있는 계정 암호를 가져오지만 암호를 체크 아웃 또는 체크 인하지 않습니다.

다음 프로세스는 암호 소비자를 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.

암호 소비자를 설정하려면 사용자가 다음을 수행해야 합니다.

1. 시스템 관리자가 다음과 같이 끝점을 구성합니다.

- a. 데이터베이스, Windows Run As, 소프트웨어 개발 키트 암호 소비자를 사용하는 끝점에 CA Access Control 을 설치합니다.

설치 프로세스 중 시스템 관리자가 PUPM 통합 기능을 활성화합니다.

참고: Windows 예약된 작업 또는 Windows 서비스 암호 소비자를 사용하기 위해 끝점에 CA Access Control 을 설치할 필요는 없습니다.

- b. 다음 암호 소비자를 사용하는 끝점에서 추가 구성 단계를 수행합니다.

- 데이터베이스(JDBC) - [데이터베이스\(JDBC\) 암호 소비자를 사용하도록 끝점을 준비합니다](#) (페이지 277).
- 데이터베이스(ODBC, OLEDB, OCI) - [데이터베이스\(ODBC, OLEDB, OCI\) 암호 소비자를 사용하도록 끝점을 구성합니다](#) (페이지 284).
- 데이터베이스(.NET) - [데이터베이스\(.NET\) 암호 소비자를 사용하도록 끝점을 구성합니다](#) (페이지 285).
- 소프트웨어 개발 키트(CLI) - [CLI 암호 소비자를 사용하도록 끝점을 구성합니다](#) (페이지 287).
- 소프트웨어 개발 키트(SDK) - [PUPM SDK 를 사용하도록 끝점을 구성합니다](#) (페이지 290).

끝점이 암호 소비자를 사용하도록 구성됩니다.

- 2. PUPM 대상 시스템 관리자 역할은 CA Access Control 엔터프라이즈 관리에 암호 정책을 만듭니다. 암호 정책이 권한 있는 계정 및 서비스 계정에 대한 암호 규칙 및 암호 만료 주기를 설정합니다.
- 3. PUPM 대상 시스템 관리자가 CA Access Control 엔터프라이즈 관리에 끝점을 만듭니다. 끝점은 권한 있는 계정 및 서비스 계정이 관리하는 장치입니다. CA Access Control 엔터프라이즈 관리에 끝점을 만들거나 PUPM 피더를 사용하여 끝점을 가져올 수 있습니다.

참고: 권한 있는 계정을 설정할 때 이미 끝점을 만든 경우, 이 단계를 수행하지 마십시오.

4. 데이터베이스, Windows Run As, 소프트웨어 개발 키트 암호 소비자를 만들려면 사용자가 다음을 수행해야 합니다.

- a. PUPM 대상 시스템 관리자가 CA Access Control 엔터프라이즈 관리에서 권한 있는 계정을 검색하거나 만듭니다.

이 사용자는 CA Access Control 엔터프라이즈 관리에서 권한 있는 계정을 검색 및 생성하거나 PUPM 피더를 사용하여 권한 있는 계정을 가져올 수 있습니다.

- b. 시스템 관리자가 CA Access Control 엔터프라이즈 관리에서 데이터베이스, Windows Run As, 소프트웨어 개발 키트 암호 소비자를 만듭니다.

시스템 관리자가 암호 소비자 생성 작업의 일부로서 데이터베이스, Windows Run As, 소프트웨어 개발 키트 암호 소비자를 권한 있는 계정과 연결합니다.

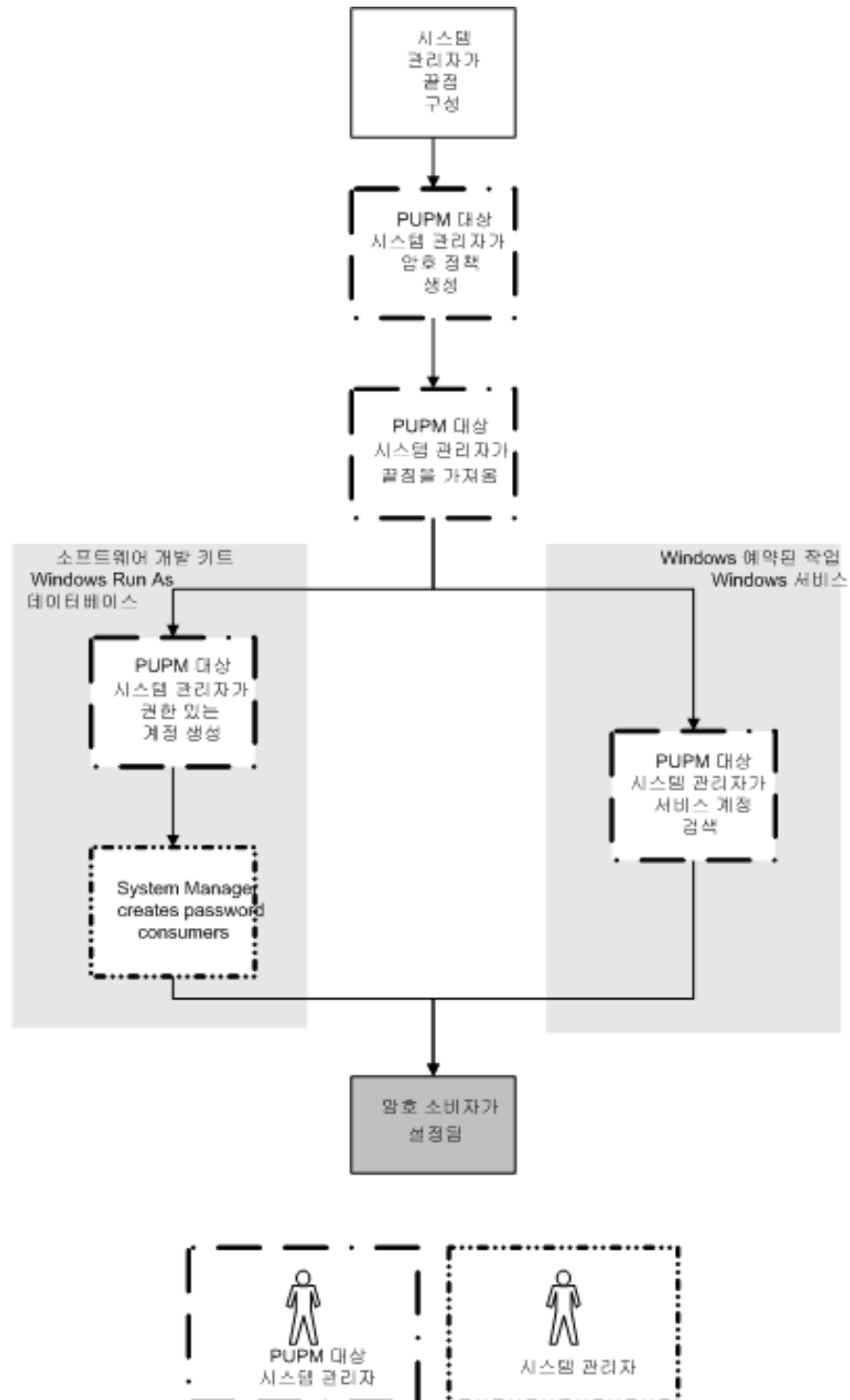
5. Windows 예약된 작업 또는 Windows 서비스 암호 소비자를 만들기 위해 PUPM 대상 시스템 관리자가 서비스 계정을 검색합니다.

CA Access Control 엔터프라이즈 관리가 검색하는 각 서비스 및 예약된 작업에 대한 암호 소비자를 만듭니다.

참고: CA Access Control 엔터프라이즈 관리는 암호를 변경할 수 있는 계정에 의해 실행되는 서비스만 검색합니다. 예를 들어, CA Access Control 엔터프라이즈 관리는 컴퓨터의 관리자 계정 또는 도메인 계정에 의해 실행되는 서비스를 검색하지만 NT AUTHORITY\Local Service 계정에 의해 실행되는 서비스는 검색하지 않습니다.

암호 소비자가 이제 회사를 위해 설정되었습니다.

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



서비스 계정 검색

*서비스 계정*은 Windows 서비스가 사용하는 내부 계정입니다. 이러한 서비스는 핵심 운영 체제 및 기타 기능을 컴퓨터에 제공합니다. CA Access Control 엔터프라이즈 관리에서 서비스 계정 암호를 관리하여 잠재적인 공격으로부터 이러한 서비스를 보호할 수 있습니다.

Windows Agentless 끝점에서 서비스와 예정된 작업을 관리하는 서비스 계정을 검색할 수 있습니다. 서비스 계정을 검색하면 동시에 CA Access Control 엔터프라이즈 관리에서 여러 서비스 계정을 만들고 암호 소비자를 서비스 계정에 할당할 수 있습니다. 서비스 계정에 대한 암호 소비자를 만들지 않으려면 "권한 있는 계정 또는 서비스 계정 만들기" 작업을 사용하여 서비스 계정을 만드십시오.

참고: 권한 있는 계정을 검색하려면 권한 있는 계정 검색 마법사를 사용하십시오.

서비스 계정 검색 마법사가 끝점에서 모든 서비스를 검색하지는 않습니다. 이 마법사는 암호를 변경할 수 있는 계정에 의해 실행되는 서비스만 검색합니다. 예를 들어, CA Access Control 엔터프라이즈 관리는 컴퓨터의 관리자 계정 또는 도메인 계정에 의해 실행되는 서비스를 검색하지만 NT AUTHORITY\Local Service 계정에 의해 실행되는 서비스는 검색하지 않습니다.

서비스 계정을 검색하려면

1. (선택 사항) 도메인 계정인 서비스 계정을 검색하려면 계정이 있는 도메인 컨트롤러가 다음 특성을 사용하여 CA Access Control 엔터프라이즈 관리에 정의되어 있는지 확인하십시오.

- 끝점 유형 - Windows Agentless
- Active Directory - True
- 호스트 도메인 - DC가 구성원인 도메인 이름
- 사용자 도메인 - DC에 정의된 사용자가 구성원인 도메인 이름

참고: 계정이 있는 도메인이 아닌 다른 도메인에서 관리 계정이 온 경우에만 사용자 도메인을 지정하십시오.

서비스 계정 검색 마법사가 이제 도메인 계정인 서비스 계정을 검색할 수 있습니다.

2. CA Access Control 엔터프라이즈 관리에서 "권한 있는 계정", "계정", "서비스 계정 검색 마법사"를 선택합니다.

서비스 계정 검색 마법사 창이 열립니다.

참고: PUPM 은 Windows Agentless 끝점에서만 서비스 계정을 관리하므로 "끝점 유형" 필드의 값은 "Windows Agentless"입니다.

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

필터 조건과 일치하는 서비스 계정의 목록과 이 서비스 계정을 사용하는 Windows 서비스 및 예약된 작업의 목록이 표시됩니다. 마법사가 알 수 없는 도메인에서 계정을 검색하면 경고 메시지가 표시됩니다.

참고: 이 프로세스는 완료될 때까지 시간이 걸릴 수 있습니다. 서비스 및 예약된 작업은 "암호 소비자" 열에 나열됩니다. 이 열의 아이콘으로 어떤 암호 소비자가 서비스인지 또는 예약된 작업인지 여부를 확인할 수 있습니다.

4. 암호 소비자를 사용하여 관리할 서비스 및 예약된 작업을 선택하고 "다음"을 클릭합니다.

"일반 계정 속성" 창이 나타납니다.

5. 서비스 및 예약된 작업에 할당할 암호 정책을 선택하고 "다음"을 클릭합니다.

"요약" 창이 나타납니다.

6. 요약 정보를 검토한 다음 "마침"을 클릭합니다.

CA Access Control 엔터프라이즈 관리는 이 작업을 제출하고 오류가 없는 경우 서비스 계정을 추가합니다. CA Access Control 엔터프라이즈 관리는 서비스 계정을 추가한 다음 선택한 각 서비스 및 예약된 작업에 대한 암호 소비자를 자동으로 만듭니다. 적절한 암호 소비자 작업을 사용하여 암호 소비자를 보고 수정할 수 있습니다.

암호 소비자 만들기

암호 소비자는 스크립트를 실행하고, 데이터베이스에 연결하거나 Windows 서비스, 예약된 작업 또는 RunAs 명령을 관리하기 위해 권한 있는 계정 및 서비스 계정을 사용하는 응용 프로그램, Windows 서비스, Windows 예약된 작업입니다.

암호 소비자에는 두 개의 그룹이 있습니다.

- 요청 시 암호를 가져오는 암호 소비자 - 소프트웨어 개발 키트, 데이터베이스, Windows Run As
참고: 필요 시 암호를 가져오는 암호 소비자를 사용하려면 PUPM 통합 기능을 활성화하여 PUPM 끝점에 CA Access Control 을 설치해야 합니다.
- 암호 변경 시 암호를 가져오는 암호 소비자 - Windows 예약된 작업, Windows 서비스

각 그룹에서 암호 소비자를 만들기 위해 다른 정보를 제공합니다. 기본적으로 암호 소비자를 만들려면 시스템 관리자 역할이 있어야 합니다.

참고: 소프트웨어 개발 키트, 데이터베이스, Windows Run As 유형의 암호 소비자를 만들려면 이 작업을 완료하십시오. 서비스 계정 검색 마법사를 사용하여 Windows 예약된 작업 또는 Windows 서비스 암호 소비자를 만들 것을 권장합니다.

암호 소비자를 만들려면

1. CA Access Control 엔터프라이즈 관리에서 "권한 있는 계정", "암호 소비자", "암호 소비자 만들기"를 클릭합니다.
암호 소비자 만들기: 암호 소비자 검색 화면 페이지가 표시됩니다.
2. (선택 사항) 다음과 같이 암호 소비자를 복사하여 만들기 위해 기존 암호 소비자를 선택합니다.
 - a. "암호 소비자" 유형의 개체 사본을 만들도록 선택합니다.
 - b. 검색 특성을 선택하고 필터 값을 입력한 다음 "검색"을 클릭합니다.
필터 조건과 일치하는 암호 소비자의 목록이 표시됩니다.
 - c. 새 암호 소비자의 기초로 사용할 개체를 선택합니다.
3. "확인"을 클릭합니다.
"암호 소비자 만들기" 작업 페이지가 나타납니다. 기존 개체에서 암호 소비자를 만든 경우 대화 상자 필드는 기존 개체의 값으로 미리 채워집니다.

4. "일반" 탭에서 다음 필드를 완성합니다.

이름

이 암호 소비자를 참조할 이름을 정의합니다.

설명

(선택 사항) 이 암호 소비자에 대해 기록할 정보(일반 텍스트)를 정의합니다.

소비자 유형

암호 소비자의 유형을 지정합니다.

응용 프로그램 경로

(소프트웨어 개발 키트, Windows Run As, Windows 예약된 작업) 끝점의 암호 소비자에 대한 전체 경로 이름을 정의합니다.

- 소프트웨어 개발 키트 암호 소비자의 경우 암호 요청을 수행하는 응용 프로그램의 경로 이름을 지정합니다.
- 데이터베이스 암호 소비자의 경우 데이터베이스에 연결하는 응용 프로그램의 경로 이름을 지정합니다.
- Windows Run As 암호 소비자의 경우 사용자가 실행하는 응용 프로그램의 경로 이름을 지정합니다.
- Windows 예약된 작업 암호 소비자의 경우 예약된 작업의 경로 이름을 지정합니다.

참고: 경로 이름에 와일드카드(*)와 CA Access Control 변수를 사용할 수 있습니다. 예: <!AC_ROOT_PATH>\bin\acpwd.exe.

서비스 이름

(Windows 서비스) Windows 서비스의 경로 이름을 정의합니다. Windows 서비스 속성 페이지에 표시되는 것과 동일하게 경로 이름을 지정하십시오.

사용

암호 소비자가 사용됨을 지정합니다. 즉, PUPM 이 이 소비자의 요청을 수락하거나 이 소비자의 암호를 변경하도록 강제합니다.

상태

(Windows 예약된 작업 또는 Windows 서비스) 마지막 암호 변경이 성공 또는 실패했는지 여부를 나타냅니다.

마지막으로 동기화된 날짜

(Windows 예약된 작업 또는 Windows 서비스) 마지막 성공한 암호 동기화를 표시합니다.

다시 시작

(Windows 서비스) 암호 변경 후 Windows 서비스를 다시 시작할지 여부를 지정합니다.

5. "권한 있는 계정" 탭을 클릭하고 암호 소비자와 연결된 권한 있는 계정을 지정합니다.

소프트웨어 개발 키트, 데이터베이스, Windows Run As 암호 소비자를 만드는 경우 지정하는 권한 있는 계정에 대한 암호를 암호 소비자가 가져올 수 있습니다.

Windows 예약된 작업 또는 Windows 서비스 암호 소비자를 만드는 경우 이러한 권한 있는 계정의 암호가 변경될 때 PUPM은 암호 소비자에 대한 암호 변경을 강제합니다.

6. 암호 소비자를 사용할 수 있는 엔터티를 지정합니다. 다음 작업 중 하나를 수행합니다.

- 소프트웨어 개발 키트, 데이터베이스, Windows Run As 암호 소비자를 만들려면 다음을 수행하십시오.
 - a. "호스트" 탭을 클릭하고 암호 소비자가 권한 있는 계정 암호를 가져올 수 있는 호스트 또는 호스트 그룹을 지정하거나, 모든 호스트 또는 호스트 그룹이 권한 있는 계정 암호에 액세스하도록 허용하려면 "모든 호스트"를 선택합니다.

참고: "이름" 필드에 호스트 또는 호스트 그룹의 이름을 입력하거나 "..."를 클릭하여 CA Access Control 호스트 또는 호스트 그룹(HNODE 또는 GHNODE 개체)을 검색할 수 있습니다.

- b. "사용자" 탭을 클릭하고 권한 있는 계정 암호를 요청할 수 있는 사용자 또는 그룹을 지정하거나, 모든 사용자가 권한 있는 계정 암호를 요청할 수 있도록 하려면 "모든 사용자"를 선택합니다.

끝점에 표시된 것과 동일하게 사용자 또는 그룹의 이름을 지정하십시오. 예: DOMAIN\user1 CA Access Control
엔터프라이즈 관리 사용자 또는 그룹을 지정하지 마십시오.

- Windows 예약된 작업 또는 Windows 서비스 암호 소비자를 만들려면 "끝점" 탭을 클릭하고 암호 소비자를 만들 끝점을 지정하십시오.

7. "제출"을 클릭합니다.

CA Access Control 엔터프라이즈 관리가 암호 소비자를 만듭니다.

추가 정보:

[암호 소비자의 유형](#) (페이지 136)

암호 소비자 예제: Windows Run As

Windows RunAs 응용 프로그램을 사용하면 사용자가 권한 있는 계정으로부터 허가를 빌려 특정 작업을 수행할 수 있습니다. 사용자가 RunAs 를 실행할 때 PUPM 에이전트가 권한 있는 계정 암호를 직접 RunAs 응용 프로그램에 제공하도록 Windows Run As 암호 소비자를 만들 수 있습니다. Windows Run As 암호 소비자를 사용하면 사용자가 관리 작업을 수행하기 위해 권한 있는 계정 암호를 알 필요가 없습니다.

Windows Run As 암호 소비자는 Windows Agentless 끝점에만 만들 수 있습니다.

다음 예에서 백업 작업은 매주 실행되도록 예약되어 있습니다. 이 작업은 C:\backup\backup.exe 에 있으며 Administrator 에 의해 실행됩니다. 예약된 백업 작업이 실패하는 경우 시스템 관리자인 Steve 는 사용자 John 이 수동으로 백업을 시작하도록 하려고 합니다. Steve 는 Windows Run As 암호 소비자를 사용하여 John 이 Administrator 암호 없이 백업 작업을 시작하도록 할 수 있습니다.

다음 프로세스는 win123_PUPM 이란 이름의 끝점에서 Windows Run As 암호 소비자를 만들고 사용하기 위해 Steve 와 John 이 수행하는 단계에 대해 설명합니다.

1. Steve 는 PUPM 통합 기능을 활성화하여 win123_PUPM 에 CA Access Control 을 설치합니다.
2. Steve 는 CA Access Control 엔터프라이즈 관리에서 다음을 수행합니다.
 - a. win123_PUPM 이란 이름으로 Windows Agentless 끝점을 만듭니다.
 - b. win123_PUPM 끝점에서 Administrator 권한 있는 계정을 검색합니다.

c. 다음 매개 변수를 사용하여 Windows Run As 암호를 만듭니다.

- 이름 - win123_PUPM Backup RunAs
- 소비자 유형 - Windows Run As
- 응용 프로그램 경로 - C:\backup\backup.exe
- 계정 - Administrator
- 호스트 - win123_PUPM
- 사용자 - Domain1\John

참고: Steve 는 끝점에 보이는 그대로 John 의 사용자 이름을 입력합니다.

Windows Run As 암호 소비자가 만들어집니다.

3. 예약된 백업 작업이 실패하고 John 이 백업을 수동으로 시작하기 위해 win123_PUPM 에 로그인합니다. 그는 백업 작업을 시작하기 위해 다음 매개 변수를 사용하여 RunAs 명령을 실행합니다.

- 계정 - Administrator
- 암호 - 암호 없음

참고: PUPM 에이전트는 John 이 암호로 제공하는 모든 값을 무시합니다.

PUPM 에이전트는 백업 작업을 시작하기 위해 John 의 이전 요청에 대한 캐시를 확인합니다. John 의 이 요청이 최초 요청이므로 요청이 캐시에 없습니다. PUPM 에이전트는 CA Access Control 엔터프라이즈 관리에서 권한 있는 계정 암호를 검색하여 RunAs 응용 프로그램에 제공합니다. 백업 작업이 시작됩니다.

암호 소비자 예제: Windows 예약된 작업

Windows 예약된 작업 및 Windows 서비스 암호 소비자는 서비스 계정에 대한 암호 변경을 자동화하는 데 도움을 줍니다. 서비스 계정은 Windows 서비스에서 사용되는 내부 계정입니다. 예를 들어, 소프트웨어 업데이트를 정기적으로 확인하기 위해 예약된 작업을 구성하는 경우, 예약된 작업은 서비스 계정을 사용하여 끝점에 로그인하고 이 작업을 수행합니다.

Windows 예약된 작업 및 Windows 서비스 암호 소비자는 Windows Agentless 끝점에서만 만들 수 있습니다. Windows 서비스 및 Windows 예약된 작업 암호 소비자를 사용하기 위해 끝점에 CA Access Control 을 설치할 필요는 없습니다.

암호를 변경할 수 있는 계정에 의해 실행되는 서비스에 대해서만 Windows 서비스 암호 소비자를 만들 수 있습니다. 예를 들어, 컴퓨터의 Administrator 계정에 의해 실행되는 서비스에 대한 암호 소비자를 만들 수는 있지만 NT AUTHORITY\Local Service 계정에 의해 실행되는 서비스에 대한 암호 소비자는 만들 수 없습니다.

다음 예에서 시스템 관리자인 Steve 는 win456 이란 이름의 Windows 끝점에서 소프트웨어 업데이트를 확인하는 예약된 작업에 대한 암호 소비자를 만들려고 합니다. 이 예약된 작업은 win456\ServiceAdmin 계정을 사용하여 끝점에 로그인합니다.

Steve 는 CA Access Control 엔터프라이즈 관리에서 다음을 수행합니다.

1. Steve 는 30days 란 이름의 암호 정책을 만듭니다. 이 암호 정책은 CA Access Control 엔터프라이즈 관리가 서비스 계정에 대한 암호를 30 일마다 변경하도록 지정하고 암호를 일요일 오전 1 시에서 오전 3 시 사이에만 변경할 수 있도록 지정합니다.
2. Steve 는 win456 이란 이름의 Windows Agentless 끝점을 만듭니다.
3. Steve 는 서비스 계정 검색 마법사를 사용하여 win456 끝점에서 win456\ServiceAdmin 계정을 검색하고 30days 암호 정책을 서비스 계정에 적용합니다.

4. CA Access Control 엔터프라이즈 관리는 다음 매개 변수를 사용하여 Windows 예약된 작업 암호 소비자를 만듭니다.

- 이름 - win456 에서 UpdateTask(C:\WINDOWS\Tasks\UpdateTask.bat)
- 소비자 유형 - Windows 예약된 작업
- 응용 프로그램 경로 - C:\WINDOWS\Tasks\UpdateTask.bat
- 권한 있는 계정 - win456\ServiceAdmin
- 끝점 - win456

Steve 가 암호 소비자를 만들었습니다. CA Access Control 엔터프라이즈 관리가 win456\ServiceAdmin 계정에 대한 암호를 변경할 때마다 JCS 는 win456 끝점에 로그인하고 소프트웨어 업데이트 예약된 작업의 암호를 변경합니다. 암호 변경이 성공하지 않으면 Steve 는 "암호 소비자 동기화" 작업을 사용하여 암호 변경을 다시 시도할 수 있습니다.

추가 정보:

[암호 소비자 동기화](#) (페이지 307)

PUPM 자동 로그인

PUPM 자동 로그인을 사용하면 권한 있는 계정 암호를 체크 아웃하고 한 단계로 PUPM 끝점에 로그인할 수 있습니다. PUPM 자동 로그인 은 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.

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.

```
Dim hwnd
Set pupmObj = CreateObject("ACLauncher.ACWebLauncher")
pupmObj.SetRDPOption "administrative session","i","1"
hwnd = pupmObj.LauncherRDP("#host#:3389", "#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.LauncherRDP("#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.

```
LauncherRDP (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.LauncherRDP("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")

LaucheProcessAsUser (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.LaucheProcessAsUser("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.LaucheRDP("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.LaucheRDP("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.LaucheRDP("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.LaucheRDP("hostname", "administrator", "password") test.SetTimeoutEvent(10)

SetWindowCloseEvent(VARIANT *phWindow);

"WaitForEvents" 메시드에 대한 창 닫기 이벤트를 지정합니다. 창이 닫힌 후에 "WaitForEvents" 메시드는 차단 호출로부터 반환되고 창이 닫혔음을 나타내는 반환 값을 표시합니다.

예: Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.LauncherRDP("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.LauncherRDP("hostname", "administrator", "password") test.SetServerCheckinEvent("http://server.com/__azy?djfhwek5jy34brfhwk eb") (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 체크 인됨

예: Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.LauncherRDP("hostname", "administrator", "password") test.SetServerCheckinEvent("http://server.com/__azy?djfhwek5jy34brfhwk eb")

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.LauncherRDP("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.LauncherRDP("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")
```

PUPM 원격 데스크톱 스크립트 사용자 지정

PUPM 원격 데스크톱 스크립트는 원격 데스크톱 설정을 구성합니다.

PUPM은 원격 데스크톱 스크립트를 실행하여 사용자를 Windows Agentless 끝점에 자동으로 로그인시킵니다. 응용 프로그램 매개 변수를 제어하기 위해 PUPM 원격 데스크톱 스크립트를 사용자 지정할 수 있습니다.

PUPM 원격 데스크톱은 다음 명령을 사용합니다.

```
SetRDPOption(BSTR bsName, BSTR bsType, BSTR bsValue)
```

bsName

수정할 매개 변수의 이름을 지정합니다.

bsType

매개 변수 유형을 지정합니다.

bsValue

매개 변수 값을 정의합니다.

예: 원격 데스크톱 응용 프로그램 설정을 구성합니다.

다음 예는 원격 데스크톱 창을 전체 화면으로 설정하고 로컬 드라이브를 원격 끝점 드라이브로 리디렉션하기 위해 사용하는 명령을 보여 줍니다.

```
Dim hwnd  
Set test = CreateObject("ACLauncher.ACWebLauncher")  
test.SetRDPOption "screen mode id","i","2"  
test.SetRDPOption "redirectdrives","i","1"  
hwnd = test.LauncherRDP("computer1", "computer1\administrator", "xxxxxx")
```

다음 표는 원격 데스크톱 스크립트를 수정하기 위해 사용할 수 있는 가능한 매개 변수와 값을 수록하고 있습니다.

	유형	값	옵션
alternate shell	문자열	c:\winnt\sys tem32\note pad.exe	터미널 서비스 세션 내에서 사용할 셸을 정의합니다. progman.exe 와 같은 대체 셸을 설정하려면 이 매개 변수를 사용하십시오. 또한 사용자가 터미널 서비스에 로그인하기 위해 사용하는 응용 프로그램을 설정하기 위해 사용할 수도 있습니다.
audiomode	정수	2	0 - 오디오를 이 컴퓨터로 가져옵니다. 1 - 원격 컴퓨터에 오디오를 남겨둡니다. 2 - 오디오를 재생하지 않습니다.
autoreconnection enabled	정수	1	파일이 열렸을 때 자동으로 연결합니다.
connect to console	정수	1	0 - 가상 세션에 연결합니다. 1 - 콘솔 세션에 연결합니다.
desktopheight	정수	768	원격 데스크톱의 높이를 픽셀로 정의합니다.
desktopwidth	정수		원격 데스크톱의 너비를 픽셀로 정의합니다.
disable full window drag	정수	1	끌어 이동하는 동안 창이 표시되지 않도록 합니다.
disable menu anims	정수	1	메뉴 애니메이션을 사용하지 않습니다.
disable themes	정수	1	세션에서 테마를 사용하지 않습니다.

	유형	값	옵션
disable wallpaper	정수	1	배경 무늬를 표시하지 않습니다.
displayconnectionbar	정수	1	전체 화면 세션에서 연결 표시줄을 표시하지 않습니다.
keyboardhook	정수	2	표준 Windows 키 조합을 적용합니다. 0 - 로컬 컴퓨터에 1 - 원격 컴퓨터에 2 - 전체 화면 모드에만
maximizeshell	정수	0	세션에 사용된 대체 셸을 최대화하도록 지정합니다.
redirectcomports	정수	1	세션에서 클라이언트 COM 포트를 리디렉션하도록 지정합니다.
redirectdrives	정수	1	세션에서 클라이언트 드라이브를 리디렉션하도록 지정합니다.
redirectprinters	정수	1	세션에서 클라이언트 프린터를 리디렉션하도록 지정합니다.
redirectsmartcards	정수	1	세션에서 클라이언트 스마트 카드를 리디렉션하도록 지정합니다.
screen mode id	정수	1	스크린 모드를 정의합니다. 1 - 윈도우 모드 2 - 전체 화면
server port	정수	3389	"full address" 매개 변수에 포트 번호를 정의합니다.
session bpp	정수	16	세션당 비트 깊이를 지정합니다. 8, 16, 24. Windows 2000 터미널 서버에는 8 비트를 사용할 수 있습니다.

유형 값		옵션
shell working directory	문자열	c:\program files\microso ft office 지정된 경우 대체 셀에 대한 작업 디렉터리를 정의합니다.
smart sizing	정수	크기를 조정할 때 바탕 화면의 클라이언트 창 표시를 크기 조정하도록 지정합니다. 0 또는 없음 - 크기 조정 안 함 1 - 크기 조정(크기 조정을 위한 추가 리소스 소비)
winposstr	문자열	0,1,0,249,80 "윈도우 모드" 크기를 지정(최대 8,876 또는 크기 지정)합니다.

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.

터미널 통합

터미널 통합을 사용하면 CA Access Control 끝점을 PUPM 과 통합하여 권한 있는 계정을 사용하는 사용자의 작업을 추적할 수 있습니다. 터미널 통합은 사용자가 권한 있는 계정 암호를 체크 아웃하고 자동 로그인을 사용하여 CA Access Control 끝점에 로그인할 때에만 사용할 수 있습니다.

터미널 통합을 사용하면 다음과 같이 보안과 신뢰성을 높일 수 있습니다.

- 보안을 높이려면 사용자가 반드시 PUPM 자동 로그인을 사용하여 끝점에 로그인하도록 지정할 수 있습니다.
- 신뢰성을 높이려면 CA Access Control 이 감사 레코드를 작성하고 권한 부여 결정을 할 때 권한 있는 사용자 이름이 아닌 원래 사용자 이름을 사용하도록 지정할 수 있습니다.

감사 레코드를 작성하고 권한 부여 결정을 할 때 CA Access Control 이 원래 사용자 이름을 사용하도록 지정하면 CA Access Control 이 로그인 세션에 대한 감사 모드를 누적합니다. 누적된 감사 모드는 원래 사용자에게 대한 감사 모드와 권한 있는 계정에 대한 감사 모드를 사용합니다. 원래 사용자가 CA Access Control 데이터베이스에 정의되어 있지 않으면 CA Access Control 은 기본 사용자에게 대한 감사 모드와 권한 있는 계정에 대한 감사 모드를 누적합니다.

예를 들어, 끝점에 대해 터미널 통합을 구성합니다. 끝점에서 user1(원래 사용자)에 대한 감사 모드가 '실패'이고 privileged_user 란 이름의 권한 있는 계정에 대한 감사 모드가 '성공'입니다. user1 이 자동 로그인을 사용하여 privileged_user 로서 끝점에 로그인하고 CA Access Control 이 로그인 세션에 대한 감사 모드를 '실패', '성공'으로 설정합니다.

터미널 통합은 CA Access Control 이 설치된 Windows Agentless 및 SSH 장치 끝점에서만 사용할 수 있습니다. 또한 사용자는 반드시 자동 로그인을 사용하여 권한 있는 계정 암호를 체크 아웃해야 합니다.

터미널 통합은 PUPM 통합 기능을 활성화하여 CA Access Control 을 설치할 때 기본적으로 활성화됩니다. CA Access Control 을 설치한 후에 CA Access Control 끝점 관리를 사용하여 끝점에서 터미널 통합을 구성합니다.

예: 로그인 이벤트 감사 레코드

다음 예는 터미널 통합을 구성한 계정에 대한 로그인 이벤트 감사 레코드를 나타냅니다. 사용자 계정이 반드시 PUPM 자동 로그인을 사용하여 끝점에 로그인하도록 지정했습니다.

이벤트 유형: 로그인 시도
Status: Denied
사용자 이름: example1\administrator
터미널: example1.domain.com
프로그램: 터미널 서비스
날짜: 2010 년 5 월 27 일
Time: 17:35
자세한 내용: 이 계정에 자동 로그인이 필요함
사용자 로그온 세션 ID: 7dd2b3dc-8a1a-4ffa-8e7d-f9bc20d2b341
감사 플래그: OS 사용자

예: 리소스 액세스 감사 레코드

다음 예는 터미널 통합을 구성한 계정에 대한 리소스 액세스 감사 레코드를 나타냅니다. CA Access Control 이 감사 레코드를 작성하고 권한 부여 결정을 할 때 권한 있는 사용자 이름이 아닌 원래 사용자 이름을 사용하도록 지정했습니다. 원래 사용자 이름(user1)이 사용자 이름 필드에 나열되고 권한 있는 계정(administrator)이 유효한 사용자 이름 필드에 나열됩니다.

Event type: Resource access
Status: Denied
Class: FILE
리소스: C:\tmp\core.txt
액세스: Exec
사용자 이름: domain\user1
터미널: example1.domain.com
프로그램: C:\WINDOWS\system32\cmd.exe
Date: 02 Feb 2010
Time: 14:20
Details: No Step that allowed access
사용자 로그온 세션 ID: 7dd2b3dc-8a1a-4ffa-8e7d-f9bc20d2b341
감사 플래그: OS 사용자
유효한 사용자 이름: example1\administrator.

추가 정보:

[터미널 통합의 구현 고려 사항](#) (페이지 276)

터미널 통합이 작동하는 방법

터미널 통합을 사용하면 CA Access Control 끝점을 PUPM 과 통합하여 보안 및 신뢰성을 높일 수 있습니다.

다음 프로세스는 터미널 통합이 작동하는 방법에 대해 설명합니다.

1. 사용자가 자동 로그인을 사용하여 CA Access Control 엔터프라이즈 관리에서 권한 있는 계정 암호를 체크 아웃합니다.
2. CA Access Control 엔터프라이즈 관리가 DMS 에서 끝점 세부 정보를 가져오고 사전 로그인 메시지를 메시지 큐로 보냅니다. 이 메시지는 권한 있는 계정의 이름, 계정을 체크 아웃한 사용자의 이름, 끝점의 이름을 포함합니다.
3. CA Access Control 끝점의 PUPM 에이전트가 메시지 큐에서 사전 로그인 메시지를 가져옵니다.
4. 사용자가 권한 있는 계정을 사용하여 끝점에 로그인하면 CA Access Control 권한 부여 엔진이 로컬 데이터베이스 레코드에서 권한 있는 계정을 확인하고 다음 작업을 수행합니다.
 - a. 엔진이 로그인 전에 계정이 계정 체크 아웃을 요구하는지 여부, 즉 사용자가 반드시 자동 로그인을 사용하여 끝점에 로그인해야 하는지 여부를 확인합니다. 다음 중 *하나*가 발생합니다.
 - 계정 체크 아웃이 요구되고 PUPM 에이전트가 권한 있는 계정에 대한 사전 로그인 메시지를 받지 않은 경우, 엔진은 로그인 시도를 거부합니다.
 - 계정 체크 아웃이 요구되고 PUPM 에이전트가 권한 있는 계정에 대한 사전 로그인 메시지를 받은 경우, 엔진은 추가 제한 사항이 없으면(예: 로그인을 금지하는 **TERMINAL** 제한 사항이 없는 경우) 로그인을 허용합니다.
 - 계정 체크 아웃이 요구되지 않는 경우 엔진은 추가 제한 사항이 없으면 로그인을 허용합니다.
 - b. 엔진은 권한 부여 결정을 내리기 위해 사용자의 원래 ID 가 사용되어야 하는지 여부를 확인합니다. 다음 중 *하나*가 발생합니다.
 - 사용자의 원래 ID 가 사용되어야 하는 경우 엔진은 원래 사용자 이름을 사용하여 리소스 액세스 요청을 평가하고 감사 레코드를 작성합니다.
 - 사용자의 원래 ID 가 사용되지 않는 경우 엔진은 권한 있는 계정 이름을 사용하여 리소스 액세스 요청을 평가하고 감사 레코드를 작성합니다.

추가 정보:

[터미널 통합의 구현 고려 사항](#) (페이지 276)

터미널 통합의 구현 고려 사항

터미널 통합을 구현하기 전에 다음 사항을 고려하십시오.

- CA Access Control 이 설치된 Windows Agentless 및 SSH 끝점 유형에서 터미널 통합을 구성할 수 있습니다. 다른 끝점 유형에서는 터미널 통합을 구현할 수 없습니다.
- (UNIX) CA Access Control 은 끝점에 연결하는 데 사용되는 로그인 프로그램에 대해 PAM 로그인 차단을 사용해야 합니다. 예를 들어, 사용자가 SSH 를 사용하여 끝점에 연결하는 경우 CA Access Control 은 PAM 로그인 차단을 사용하여 SSH 로그인을 차단해야 합니다.

CA Access Control 이 로그인 프로그램에 대해 PAM 로그인 차단을 사용하도록 지정하려면 로그인 프로그램의 LOGINAPPL 레코드에서 loginflags(pamlogin) 플래그를 설정하십시오. 예:

```
editres loginappl SSH loginflags(pamlogin)
```

- 권한 있는 계정 로그인에 대해서만 터미널 통합을 사용할 수 있습니다. 로그인 통합은 서비스 계정 로그인에 대해 사용할 수 없습니다.
- 터미널 통합은 자동 로그인을 사용하여 권한 있는 계정을 체크 아웃하는 경우에만 사용할 수 있습니다.
- (UNIX) 터미널 통합은 SSH 로그인에만 사용할 수 있습니다. 사용자가 PUPM 자동 로그인을 사용하여 권한 있는 계정 암호를 체크 아웃하고 CA Access Control 끝점에 로그인하는 경우에만 터미널 통합을 사용할 수 있고 PUPM 이 SSH 로그인에 대한 로그인 스크립트만 제공하므로 이러한 제한이 존재합니다.

사용자 지정된 스크립트를 작성하여 다른 로그인 유형에 대한 로그인 응용 프로그램을 만들고 다른 로그인 유형에 대해 터미널 통합을 사용하려면 적절한 로그인 프로그램의 LOGINAPPL 레코드에 대한 loginflags(pamlogin) 속성을 설정하십시오.

제 7 장: PUPM 끝점 구성

이 섹션은 다음 항목을 포함하고 있습니다.

[데이터베이스\(JDBC\) 암호 소비자를 사용하도록 JBoss Application 준비](#)
(페이지 277)

[Oracle 데이터베이스에 대한 추가 정보](#) (페이지 282)

[데이터베이스\(ODBC, OLEDB, OCI\) 암호 소비자를 사용하도록 끝점 구성](#)
(페이지 284)

[데이터베이스\(.NET\) 암호 소비자를 사용하기 위한 끝점 구성](#) (페이지 285)

[CLI 암호 소비자를 사용하기 위한 끝점 구성](#) (페이지 287)

[암호 소비자 SDK 응용 프로그램을 사용하도록 끝점을 구성하는 방법](#)
(페이지 290)

[웹 서비스 PUPM SDK 응용 프로그램을 사용하도록 끝점을 구성하는 방법](#)
(페이지 293)

[터미널 통합 구성](#) (페이지 294)

데이터베이스(JDBC) 암호 소비자를 사용하도록 JBoss Application 준비

데이터베이스에 연결하기 위해 JDBC 를 사용하는 응용 프로그램에서 하드 코딩된 암호를 대체하기 위해 JDBC 데이터베이스 암호 소비자를 사용할 수 있습니다. 응용 프로그램이 인증을 위한 암호를 제공할 때마다 PUPM 에이전트는 CA Access Control 엔터프라이즈 관리에서 권한 있는 계정 암호를 가져와서 하드 코딩된 암호를 이 권한 있는 계정 암호로 대체합니다.

암호 소비자가 사용하는 데이터베이스를 구성하기 전에 JDBC 암호 소비자를 사용하도록 끝점을 준비해야 합니다.

데이터베이스(JDBC) 암호 소비자를 사용하도록 JBoss Application 을 준비하려면

1. CA Access Control 이 PUPM 통합 기능을 활성화하여 끝점에 설치되었고 데이터베이스에 연결하는 응용 프로그램이 1.5 이상을 사용하는지 확인합니다.

참고: 데이터베이스에 연결하는 응용 프로그램이 설치된 끝점에 CA Access Control 을 설치하십시오. CA Access Control 을 데이터베이스 호스트에 설치할 필요는 없습니다.

2. 데이터베이스에 연결하는 응용 프로그램이 실행 중이면 중지합니다.
3. 다음 디렉터리로 이동합니다. 여기서 *ACInstallDir* 는 CA Access Control 이 설치된 디렉터리입니다.

ACInstallDir/SDK/JDBC

4. 다음 파일을 찾습니다.
 - CAJDBCService.sar
 - CAJBCDriver.jar
 - CAPUPMClientCommons.jar
 - jsafeFIPS.jar

5. CAJDBCService.sar 를 다음 디렉터리에 복사합니다. 여기서 *JBoss_HOME* 은 JBoss 를 설치한 디렉터리입니다.

JBoss_HOME/server/default/deploy

6. CAJBCDriver.jar, CAPUPMClientCommons.jar, jsafeFIPS.jar 파일을 다음 디렉터리로 복사합니다.

JBoss_HOME/server/lib

7. 엔터프라이즈 관리 서버에서 암호 소비자에 대해 정의한 데이터 원본 XML 파일을 찾습니다.

8. 편집을 위해 파일을 엽니다: 다음 작업 중 *하나*를 수행합니다.

- [Microsoft SQL Server 에 대한 데이터 원본 구성 파일 사용자 지정](#) (페이지 279)

- [Oracle 에 대한 데이터 원본 구성 파일 사용자 지정](#) (페이지 279)

데이터베이스 연결 설정 및 데이터 원본 클래스를 지정하기 위해 데이터 원본 구성 파일을 사용자 지정합니다.

9. CA Access Control 을 시작합니다.

암호 소비자를 사용하기 위해 끝점을 구성했습니다. 이제 CA Access Control 엔터프라이즈 관리에서 응용 프로그램에 대한 암호 소비자를 만들어야 합니다. 암호 소비자를 만든 이후에 응용 프로그램을 시작합니다.

추가 정보:

[암호 소비자 예제: JDBC 데이터베이스](#) (페이지 280)

[암호 소비자 만들기](#) (페이지 254)

Microsoft SQL Server 에 대한 데이터 원본 구성 파일 사용자 지정

Microsoft SQL Server 데이터베이스에 연결하기 위해 JDBC 를 사용하는 응용 프로그램에서 하드 코드된 암호를 대체하기 위해 JDBC 데이터베이스 암호 소비자를 구성할 수 있습니다. JDBC 암호 소비자를 사용하기 위해 끝점을 준비한 이후에 다음 단계를 수행하십시오.

Microsoft SQL Server 에 대한 데이터 원본 구성 파일을 사용자 지정하려면

1. <driver-class> 태그를 찾아 JDBC 드라이버 클래스 속성으로 기본값을 대체합니다. 예:

```
<driver-class>com.ca.ppm.clients.jdbc.CAJDBCDriver</driver-class>
```

2. <connection-url> 태그를 찾아 데이터베이스 연결 설정으로 기본값을 대체합니다. 예:

```
<connection-url>>@@@com.microsoft.sqlserver.jdbc.SQLServerDriver@@@jdbc:sqlserver://SQLServer1:1433;selectMethod=cursor;DatabaseName=tempdb</connection-url>
```

3. CA Access Control 을 시작하고

데이터베이스 구성 파일을 Microsoft SQL Server 로 사용자 지정했습니다. 이제 CA Access Control 엔터프라이즈 관리에서 응용 프로그램에 대한 암호 소비자를 만들어야 합니다. 암호 소비자를 만든 이후에 응용 프로그램을 시작합니다.

Oracle 에 대한 데이터 원본 구성 파일 사용자 지정

Oracle 데이터베이스에 연결하기 위해 JDBC 를 사용하는 응용 프로그램에서 하드 코드된 암호를 대체하기 위해 JDBC 데이터베이스 암호 소비자를 구성할 수 있습니다. JDBC 암호 소비자를 사용하기 위해 끝점을 준비한 이후에 다음 단계를 수행하십시오.

Oracle 에 대한 데이터 원본 구성 파일을 사용자 지정하려면

1. <xa-datasource-class> 태그를 찾아 CAJDBCDataSource 클래스 속성으로 기본값을 대체합니다. 예:

```
<xa-datasource-class>com.ca.ppm.clients.jdbc.CAJDBCDataSource</xa-datasource-class>
```

중요! 속성 이름은 기본값과 동일한 대소문자를 사용해야 합니다.

- 모든 <xa-datasource-property name=> 태그를 찾습니다. 예:

```
<xa-datasource-property
name="URL">jdbc:oracle:oci8:@tc</xa-datasource-property>
<xa-datasource-property name="User">scott</xa-datasource-property>
<xa-datasource-property name="Password">tiger</xa-datasource-property>
```

- 속성을 단일 문자열로 구성합니다. 예:

```
<xa-datasource-property
name="CAJDBCProperties">CAJDBCPropertyRealDatasourceClass="oracle.jdbc.xa.client.OracleXADataSource";URL="jdbc:oracle:oci8:@tc";User="scott";Password="tiger";</xa-datasource-property>
```

- CA Access Control 을 시작하고

Oracle 에 대한 데이터 원본 구성 파일을 사용자 지정했습니다. 이제 CA Access Control 엔터프라이즈 관리에서 응용 프로그램에 대한 암호 소비자를 만들어야 합니다. 암호 소비자를 만든 이후에 응용 프로그램을 시작합니다.

암호 소비자 예제: JDBC 데이터베이스

이 예에서 시스템 관리자인 Steve 는 JBoss 응용 프로그램 서버를 사용하여 일반 텍스트로 된 암호를 수록하는 응용 프로그램을 실행합니다. 이 응용 프로그램은 일반 텍스트로 된 암호를 사용하여 Microsoft SQL Server 데이터베이스에 대한 연결을 인증합니다. Steve 는 응용 프로그램이 데이터베이스에 연결할 때마다 응용 프로그램이 PUPM 으로부터 권한 있는 계정 암호를 받도록 JBoss 응용 프로그램 서버를 수정하려고 합니다.

Steve 는 Windows 끝점에 JBoss 응용 프로그램 서버 버전 4.2.3.GA 와 Java Development Kit(JDK) 1.6.0_19 를 설치했습니다. 끝점의 이름은 JBossEndpoint 입니다. 이름이 JBossEndpoint\Administrator 인 사용자는 run.bat 파일을 사용하여 JBoss 응용 프로그램 서버를 시작하고, 이 서버는 Microsoft SQL Server 데이터베이스에 연결하는 응용 프로그램을 실행합니다. 이 응용 프로그램은 sa 계정을 사용하여 데이터베이스에 연결합니다.

- Steve 는 JBossEndpoint 에서 다음을 수행합니다.
 - JBoss 를 중지합니다.
 - PUPM 통합 기능을 활성화하여 CA Access Control 을 설치합니다.
 - 다음 디렉터리로 이동합니다.

C:\Program Files\CA\AccessControl\SDK\JDBC

- d. 다음 파일을 찾습니다.
 - CAJDBCService.sar
 - CAJBCDriver.jar
 - CAPUPMClientCommons.jar
 - jsafeFIPS.jar
 - e. CAJDBCService.sar 파일을 다음 디렉터리로 복사합니다.
C:\jboss-4.2.3.GA\server\default\deploy
 - f. CAJBCDriver.jar, CAPUPMClientCommons.jar, jsafeFIPS.jar 파일을 다음 디렉터리로 복사합니다.
C:\jboss-4.2.3.GA\server\default\lib
 - g. 다음 디렉터리로 이동합니다.
C:\jboss-4.2.3.GA\server\default\deploy
 - h. 편집을 위해 다음 파일을 엽니다:
 - imworkflowdb-ds.xml
 - objectstore-ds.xml
 - reportsnapshot-ds.xml
 - userstore-ds.xml
 - i. <driver-class> 태그를 찾아 JDBC 드라이버 클래스 속성으로 기본값을 대체합니다. 예:
<driver-class>com.ca.ppm.clients.jdbc.CAJBCDriver</driver-class>
 - j. <connection-url> 태그를 찾아 데이터베이스 연결 설정으로 기본값을 대체합니다. 예:
<connection-url>>@@@com.microsoft.sqlserver.jdbc.SQLServerDriver@@@jdbc:sqlserver://SQLServer1:1433;selectMethod=cursor;DatabaseName=tempdb</connection-url>
 - k. 파일을 저장하고 닫습니다.
 - l. CA Access Control 을 시작합니다.
2. Steve 는 CA Access Control 엔터프라이즈 관리에서 다음을 수행합니다.
 - a. JBossEndpoint_PUPM 이란 이름으로 Windows Agentless 유형의 끝점을 만듭니다.
 - b. JBossEndpoint_PUPM 끝점에서 sa 권한 있는 계정을 검색합니다.

c. 다음 매개 변수를 사용하여 데이터베이스 암호 소비자를 만듭니다.

- 이름 - JBossEndpoint MS SQL 연결
- 소비자 유형 - 데이터베이스(ODBC/JDBC/OLEDB/OCI)
- 응용 프로그램 경로 - C:\jboss-4.2.3.GA\bin\run.bat
- 계정 - sa
- 호스트 - JBossEndpoint
- 사용자 - JBossEndpoint\Administrator

3. JBossEndpoint\Administrator 사용자는 run.bat 파일을 실행하여 끝점에서 JBoss 응용 프로그램 서버를 시작합니다.

JBoss 응용 프로그램 서버가 시작되고 이 응용 프로그램이 SQL Server 에 연결을 시도합니다. PUPM 에이전트가 연결 시도를 가로채고 권한 있는 계정 암호를 응용 프로그램에 제공합니다.

4. Steve 는 다음 디렉터리에 있는 JBoss 로그 파일에서 오류가 있는지 검사합니다.

C:\jboss-4.2.3.GA\server\default\log

Oracle 데이터베이스에 대한 추가 정보

tnsnames.ora 파일은 클라이언트가 Oracle 데이터베이스에 연결하기 위해 사용하는 데이터베이스 주소를 정의하는 Oracle 구성 파일입니다.

tnsnames.ora 파일은 여러 호스트 이름, 포트, 서비스 이름, 인스턴스 이름 SID 를 포함할 수 있습니다.

PUPM 에이전트는 tnsnames.ora 파일의 전체 경로를 확인하기 위해 \$ORACLE_HOME 및 \$TNS_ADMIN 환경 변수를 확인합니다. 이 환경 변수는 다음 레지스트리 키에 정의됩니다.

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation\Plugin\plugin\EnvironmentVariables

plugin

연결 시도를 가로채는 플러그 인의 이름을 지정합니다.

값: OCIPlg, ODBCPlg, OLEDBPlg

PUPM 에이전트는 Oracle 데이터베이스에 대한 연결 시도를 가로챌 때마다 `tnsnames.ora` 파일을 구문 분석합니다. 이 파일에 이러한 특성에 대한 값이 여러 개 포함된 경우, PUPM 에이전트는 가능한 각 특성 조합별로 별도의 네트워크 세트를 만듭니다. PUPM 에이전트는 모든 네트워크 세트를 CA Access Control 엔터프라이즈 관리에 보내고, CA Access Control 엔터프라이즈 관리는 이 네트워크 세트와 가장 가깝게 일치하는 권한 있는 계정에 대한 암호를 가져옵니다.

예: `tnsnames.ora` 파일의 네트워크 세트

다음은 `tnsnames.ora` 파일의 예입니다.

```
SAMPLE_INSTANCE=
(DESCRIPTION=
  (SOURCE_ROUTE=yes)
  (ADDRESS=(PROTOCOL=tcp)(HOST=host1)(PORT=1630))    # hop 1
  (ADDRESS_LIST=
    (FAILOVER=on)
    (LOAD_BALANCE=off)                                # hop 2
    (ADDRESS=(PROTOCOL=tcp)(HOST=host2a)(PORT=1630))
    (ADDRESS=(PROTOCOL=tcp)(HOST=host2b)(PORT=1630)))
  (ADDRESS=(PROTOCOL=tcp)(HOST=host3)(PORT=1521))    # hop 3
  (CONNECT_DATA=(SERVICE_NAME=Sales.example.com)))
```

PUPM 에이전트가 이 `tnsnames.ora` 파일을 구문 분석할 때 다음 네트워크 세트를 CA Access Control 엔터프라이즈 관리로 보냅니다.

- HOST=host1, PORT=1630
- HOST=host2a, PORT=1630
- HOST=host2b, PORT=1630
- HOST=host3, PORT=1521, SERVICE_NAME= Sales.example.com

데이터베이스(ODBC, OLEDB, OCI) 암호 소비자를 사용하도록 끝점 구성

Windows Agentless 끝점에 해당

ODBC, OLEDB 또는 OCI 데이터베이스 암호 소비자를 사용하여 ODBC, OLEDB 또는 OCI 를 사용하여 데이터베이스에 연결하는 응용 프로그램에서 하드 코드된 암호를 대체할 수 있습니다. 응용 프로그램이 데이터베이스에 대한 연결을 시도하면 PUPM 에이전트가 이 연결 시도를 가로채서 하드 코드된 암호를 CA Access Control 엔터프라이즈 관리에서 가져오는 권한 있는 계정 암호로 대체합니다.

응용 프로그램은 CA Access Control 이 설치된 Windows Agentless 끝점에 있어야 합니다. OCI 데이터베이스 암호 소비자를 만들려면 응용 프로그램이 OCI8 이상을 사용하는지 확인하십시오.

PUPM 은 다른 플러그 인을 사용하여 각 연결 시도 유형을 가로칩니다. 예를 들어, OCI 플러그 인은 OCI 를 사용하는 연결 시도를 가로칩니다. 다음 레지스트리 키는 CA Access Control 플러그 인의 동작을 제어합니다.

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation\PlugIns

각 플러그 인에 대한 설정은 다음 하위 키에 있습니다.

- OCI - Instrumentation\PlugIns\OCIPlg
- ODBC - Instrumentation\PlugIns\ODBCPlg
- OLEDB - Instrumentation\PlugIns\OLEDBPlg

데이터베이스(ODBC, OLEDB, OCI) 암호 소비자를 사용하도록 끝점 구성하려면

1. PUPM 통합 기능을 활성화하여 CA Access Control 이 끝점에 설치되었는지 확인합니다.

참고: 데이터베이스에 연결하는 응용 프로그램이 설치된 끝점에 CA Access Control 을 설치하십시오. CA Access Control 을 데이터베이스 호스트에 설치할 필요는 없습니다.

2. 끝점에서 CA Access Control 을 중지합니다.

3. 연결 유형에 대한 적절한 레지스트리 하위 키에서 다음을 수행합니다.

- **OperationMode** 레지스트리 항목의 값이 **1** 인지 확인합니다.

이 레지스트리 항목은 플러그 인을 활성화합니다.

- 응용 프로그램을 실행하는 프로세스의 이름이 **ApplyOnProcess** 레지스트리 항목의 값인지 확인합니다.

이 레지스트리 항목은 플러그 인이 적용하는 프로세스를 지정합니다. 예를 들어, IIS 응용 프로그램에 대한 암호 소비자를 만드는 경우 **w3wp.exe** 가 레지스트리 항목의 값인지 확인하십시오.

참고: 사용자가 직접 이 레지스트리 항목의 값을 변경하지 않는 것이 좋습니다. 도움이 필요한 경우 기술 지원부(<http://ca.com/support>)에 문의하십시오.

4. CA Access Control 을 시작하고

데이터베이스 암호 소비자를 사용하기 위해 끝점을 구성했습니다. 이제 CA Access Control 엔터프라이즈 관리에서 응용 프로그램에 대한 데이터베이스 암호 소비자를 만들어야 합니다.

참고: IIS 응용 프로그램에 대한 암호 소비자를 만드는 경우 **NT_AUTHORITY\NETWORK SERVICE** 및 **hostname\IUSR_hostname** 사용자가 이 암호 소비자를 사용하여 권한 있는 계정 암호를 가져올 수 있도록 지정해야 합니다. 여기서 **hostname** 은 끝점의 이름입니다.

데이터베이스(.NET) 암호 소비자를 사용하기 위한 끝점 구성

Windows Agentless 끝점에 해당

데이터베이스에 연결하기 위해 .NET 을 사용하는 응용 프로그램에서 하드 코드된 암호를 대체하기 위해 .NET 데이터베이스 암호 소비자를 사용할 수 있습니다. 응용 프로그램이 데이터베이스에 대한 연결을 시도하면 PUPM 에이전트가 이 연결 시도를 가로채서 하드 코드된 암호를 CA Access Control 엔터프라이즈 관리에서 가져오는 권한 있는 계정 암호로 대체합니다.

참고: 응용 프로그램은 CA Access Control 이 설치된 Windows Agentless 끝점에 있어야 합니다.

PUPM 은 프로파일러를 사용하여 각 연결 시도를 가로채는 플러그 인을 로드합니다. .NET 플러그 인은 .NET 을 사용하는 연결 시도를 가로챍니다. 다음 레지스트리 키는 CA Access Control .NET 의 동작을 제어합니다.

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation\ .NET \
```

프로파일러와 플러그 인의 설정은 다음 하위 키에 있습니다.

- 프로파일러 - Instrumentation\ .NET \Profiler\
- 플러그 인 - Instrumentation\ .NET \Profiler\Plugin

.NET 데이터베이스 암호 소비자를 사용하기 위해 끝점을 구성하려면

1. PUPM 통합 기능을 활성화하여 CA Access Control 이 끝점에 설치되었는지 확인합니다.
참고: 데이터베이스에 연결하는 응용 프로그램이 설치된 끝점에 CA Access Control 을 설치하십시오. CA Access Control 을 데이터베이스 호스트에 설치할 필요는 없습니다.
2. 끝점에서 CA Access Control 을 중지합니다.
3. 연결 유형에 대한 적절한 레지스트리 하위 키에서 다음을 수행합니다.

- OperationMode 레지스트리 항목의 값이 1 인지 확인합니다.
이 레지스트리 항목은 플러그 인을 활성화합니다.

중요! OperationMode 레지스트리 항목이 프로파일러 및 플러그 인에 대해 1 로 설정되어 있는지 확인하십시오.

- 응용 프로그램을 실행하는 프로세스의 이름이 ApplyOnProcess 레지스트리 항목의 값인지 확인합니다.

이 레지스트리 항목은 플러그 인이 적용하는 프로세스를 지정합니다. 예를 들어, IIS 응용 프로그램에 대한 암호 소비자를 만드는 경우 w3wp.exe 가 레지스트리 항목의 값인지 확인하십시오.

참고: 사용자가 직접 이 레지스트리 항목의 값을 변경하지 않는 것이 좋습니다. 도움이 필요한 경우 기술 지원부(<http://ca.com/support>)에 문의하십시오.

4. CA Access Control 을 시작합니다.

데이터베이스 암호 소비자를 사용하기 위해 끝점을 구성했습니다. 이제 CA Access Control 엔터프라이즈 관리에서 응용 프로그램에 대한 데이터베이스 암호 소비자를 만들어야 합니다.

참고: IIS 응용 프로그램에 대한 암호 소비자를 만드는 경우 NT_AUTHORITY\NETWORK SERVICE 및 *hostname\IUSR_hostname* 을 권한 있는 계정 암호를 가져오기 위해 암호 소비자를 사용할 수 있는 사용자로 지정하십시오. 여기서 *hostname* 은 끝점의 이름입니다.

CLI 암호 소비자를 사용하기 위한 끝점 구성

CLI 암호 소비자는 소프트웨어 개발 키트 암호 소비자의 유형입니다. CLI 암호 소비자를 사용하여 하드 코드된 암호를 권한 있는 계정 암호로 대체할 수 있습니다. CLI 암호 소비자는 권한 있는 계정 암호를 가져오고, 체크 아웃하고, 체크 인하는 스크립트를 의미합니다. 이 스크립트는 PUPM 에이전트를 호출하고, 이 에이전트는 CA Access Control 엔터프라이즈 관리에서 권한 있는 계정 암호를 가져옵니다.

다른 파일 또는 스크립트를 변경할 수 있는 권한이 제한된 .bat 또는 .sh 스크립트를 작성하려면 CLI 암호 소비자를 사용하십시오. 예를 들어, 파일에서 하드 코드된 암호를 수동으로 업데이트하기 위해 `acpwd` 유틸리티를 사용하는 스크립트를 작성할 수 있습니다. 또한 CLI 암호 소비자를 사용하여 사용자들이 끝점의 명령줄에서 `acpwd` 유틸리티를 실행하도록 할 수 있습니다.

참고: PUPM SDK 를 사용하여 스크립트의 하드 코드된 암호를 권한 있는 계정 암호로 대체할 수도 있습니다. 예를 들어, 여러 파일에서 암호를 대체하는 사용자 지정된 스크립트를 작성하려면 PUPM SDK 를 사용하십시오.

CLI 암호 소비자를 사용하기 위해 끝점을 구성하려면

1. PUPM 통합 기능을 활성화하여 CA Access Control 이 끝점에 설치되었는지 확인합니다.
2. 스크립트에 다음 명령을 추가합니다.

```
acpwd {-checkout | -get} -account name -ep name -eptype type [-container name]  
-nologo
```

참고: acpwd 유틸리티 구문에 대한 자세한 내용은 [참조 안내서](#)를 참조하십시오.

3. 명령의 출력(권한 있는 계정 암호)을 사용하도록 스크립트를 수정합니다.

CLI 암호 소비자를 사용하기 위해 끝점을 구성했습니다. 이제 CA Access Control 엔터프라이즈 관리에서 스크립트에 대한 소프트웨어 개발 키트(SDK/CLI) 암호 소비자를 만들어야 합니다.

추가 정보:

[암호 소비자 만들기](#) (페이지 254)

CLI 암호 소비자가 작동하는 방식

CLI 암호 소비자를 사용하여 하드 코드된 암호를 권한 있는 계정 암호로 대체할 수 있습니다. CLI 암호 소비자는 권한 있는 계정 암호를 가져오고, 체크 아웃하고, 체크 인하기 위해 acpwd 유틸리티를 사용하는 스크립트를 의미합니다. 또한 CLI 암호 소비자를 사용하여 사용자들이 끝점의 명령줄에서 acpwd 유틸리티를 실행하도록 할 수 있습니다. CLI 암호 소비자가 작동하는 방식을 이해하면 acpwd 유틸리티를 사용하는 데 도움이 됩니다.

참고: 스크립트 또는 명령줄에서 acpwd 유틸리티를 사용하려면 먼저 CA Access Control 엔터프라이즈 관리에서 이 스크립트 또는 유틸리티를 소프트웨어 개발 키트(SDK/CLI) 암호 소비자로 정의해야 합니다. 암호 소비자는 권한 있는 계정 암호를 획득하도록 허용된 사용자의 목록을 정의합니다.

다음 프로세스는 CLI 암호 소비자가 작동하는 방식을 설명합니다.

1. 다음 방법 중 하나로 끝점에서 **acpwd** 유틸리티가 호출됩니다.
 - 사용자가 명령줄 프롬프트 창에서 유틸리티를 실행합니다.
 - 스크립트 또는 응용 프로그램 서버가 실행되고 유틸리티를 호출합니다.
2. **acpwd** 유틸리티가 권한 있는 계정 암호를 요청합니다. **PUPM** 에이전트는 승인을 위해 요청을 **CA Access Control** 엔터프라이즈 관리에 전달합니다.
3. **CA Access Control** 엔터프라이즈 관리가 권한 있는 계정 암호를 끝점으로 보냅니다. **PUPM** 에이전트가 암호를 표시하거나 이 암호를 원래 프로그램으로 전달하고 확인 메시지를 로깅합니다.
4. 사용자, 스크립트 또는 응용 프로그램 서버, 또는 **CA Access Control** 엔터프라이즈 관리가 계정 암호를 다시 체크 인하고 **PUPM** 에이전트가 확인 메시지를 로깅합니다.
5. **PUPM** 에이전트는 체크 인이 성공했음을 알리는 확인 메시지를 로깅합니다.

참고: 숫자 0의 확인 메시지는 **PUPM** 에이전트가 성공적으로 암호를 가져오고, 체크 아웃하고, 체크 인했음을 나타냅니다. **acpwd** 유틸리티 구문에 대한 자세한 내용은 [참조 안내서](#)를 참조하십시오.

예제: 암호를 가져오는 스크립트

다음은 Windows에서 권한 있는 계정 암호를 가져오는 예제 스크립트 내용입니다. 이 예제는 **PUPM** 에이전트가 **CA Access Control** 끝점에 설치되었다고 가정합니다.

이 예제의 스크립트는 **CA Access Control** 엔터프라이즈 관리에서 가져오는 권한 있는 계정 암호를 사용하여 Windows 레지스트리에서 항목을 추가 및 삭제합니다.

```
set AdminUser=PowerUser
FOR /F "tokens=*" %i IN ('C:\Program Files\AccessControl\bin\acpwd.exe" -get
-account PowerUser
-ep compl_123 -eptype "Windows Agentless" -container "Windows Accounts" -nologo')
DO SET AdminPassword=%i
set runasadmin="C:\utils\psexec.exe" -u %AdminUser% -p
%runasadmin% %AdminPassword% REG ADD "HKLM\SOFTWARE\PUPM Registry"
%runasadmin% %AdminPassword% REG DELETE "HKLM\SOFTWARE\PUPM Registry" /F
```

이 예에서 스크립트는 PUPM 에이전트를 실행하여 권한 있는 계정 암호를 가져옵니다. 이 스크립트는 계정 이름(*PowerUser*), 끝점 이름(*comp1_123*), 끝점 유형(*Windows Agentless*), 사용자의 컨테이너 이름(*Windows Accounts*)을 포함하고 있습니다. 이 스크립트는 PUPM 에이전트가 암호만 표시하도록 지시하고, 이 암호를 사용하여 레지스트리 항목을 추가 및 삭제하기 위한 관리 사용자로서 PsExec 프로그램을 실행하기 위해 이 암호를 사용합니다.

암호 소비자 SDK 응용 프로그램을 사용하도록 끝점을 구성하는 방법

암호 소비자 SDK 를 사용하여 CA Access Control 끝점에 대한 응용 프로그램을 작성할 수 있습니다. 응용 프로그램은 권한 있는 계정 암호를 가져오고, 체크 아웃/체크 인하고, 암호 캐싱 및 사용자 인증을 제공합니다.

응용 프로그램을 실행하면 응용 프로그램은 CA Access Control 엔터프라이즈 관리에서 권한 있는 계정 암호를 가져오고 체크 아웃/체크 인하는 PUPM 에이전트를 호출합니다.

암호 소비자 SDK 에는 두 가지 종류가 있습니다.

- **Java PUPM SDK - Windows 및 UNIX** 끝점을 위한 Java 응용 프로그램을 작성하려면 이 SDK 를 사용하십시오.
작성하는 Java 응용 프로그램은 JRE 1.5 이상을 사용해야 합니다.
- **.NET PUPM SDK - Windows** 끝점을 위한 C# 응용 프로그램을 작성하려면 이 SDK 를 사용하십시오.
.NET PUPM SDK 를 사용하려면 끝점에 .NET Framework 2.0 이상을 설치해야 합니다.

암호 소비자 SDK 응용 프로그램을 사용하도록 끝점을 구성하려면 다음을 수행하십시오.

1. PUPM 통합 기능을 활성화하여 CA Access Control 이 끝점에 설치되었는지 확인합니다.
2. 암호 소비자 SDK 샘플을 사용하여 응용 프로그램을 작성합니다. 샘플은 다음 위치에 있습니다.
 - Java PUPM SDK - `ACInstallDir/SDK/JAVA/Samples/PUPMJavaSDK/src/cpm/ca/pupm/javask/Tester.java`
 - .NET PUPM SDK - `ACInstallDir/SDK/DOTNET/Examples`암호 소비자 SDK 응용 프로그램을 사용하도록 끝점을 구성했습니다. 이제 CA Access Control 엔터프라이즈 관리에서 응용 프로그램에 대한 소프트웨어 개발 키트(SDK/CLI) 암호 소비자를 만들어야 합니다.

추가 정보:

[암호 소비자 SDK 응용 프로그램이 암호를 가져오는 방법](#) (페이지 163)

[Java PUPM SDK](#) (페이지 165)

[.NET PUPM SDK](#) (페이지 166)

[암호 소비자 만들기](#) (페이지 254)

Java PUPM SDK 응용 프로그램 실행

암호 소비자 SDK 응용 프로그램을 사용하도록 끝점을 구성한 이후에 응용 프로그램을 실행하여 권한 있는 계정 암호를 가져오고 체크 아웃/체크 인할 수 있습니다.

Java PUPM SDK 응용 프로그램을 실행하려면

1. CA Access Control 엔터프라이즈 관리에서 응용 프로그램에 대한 암호 소비자를 만들었는지 확인합니다.
2. 명령 프롬프트 창을 열고 응용 프로그램이 설치된 폴더로 이동합니다.

3. 다음 명령을 실행합니다.

```
java -cp PupmJavaSDK.jar;CAPUPMClientCommons.jar;jsafeFIPS.jar;[log4jLib];.  
applicationName {explicit | keyvalues} {checkout | checkin} "endpointType"  
"endpointName" "accountName" "accountContainer" flags
```

log4jLib

(선택 사항) 런타임 이벤트와 정보를 로깅하기 위해 응용 프로그램이 사용하는 log4j 라이브러리의 이름을 정의합니다.

applicationName

Java PUPM SDK 응용 프로그램의 이름을 정의합니다.

explicit

명령이 각 매개 변수의 명시적 값을 제공하도록 지정합니다.

keyvalues

명령이 키/값 쌍을 사용하도록 지정합니다.

checkout

응용 프로그램이 권한 있는 계정 암호를 검색(가져오기 또는 체크 아웃)하도록 지정합니다.

참고: *flags* 매개 변수는 응용 프로그램이 수행하는 가져오기 또는 체크 아웃 작업을 지정합니다.

checkin

응용 프로그램이 권한 있는 계정 암호를 체크 인하도록 지정합니다.

endpointType

권한 있는 계정이 정의된 끝점의 유형을 정의합니다.

참고: CA Access Control 엔터프라이즈 관리에서 "끝점 유형 보기" 작업을 사용하여 사용 가능한 끝점 유형의 목록을 볼 수 있습니다. "프로비저닝을 통한 SAP R3"와 같이 CA Access Control 엔터프라이즈 관리에 표시되는 것과 정확하게 일치하게 끝점 유형을 정의합니다.

endpointName

권한 있는 계정이 정의된 끝점의 이름을 정의합니다.

accountName

권한 있는 계정의 이름을 정의합니다.

accountContainer

권한 있는 계정이 정의된 컨테이너의 이름을 정의합니다.

권한 있는 계정이 컨테이너에 저장되지 않았으면 이 매개 변수에 대해 "Accounts"를 지정하십시오.

flags

응용 프로그램이 권한 있는 계정 암호를 체크 아웃 또는 가져오는지 지정합니다.

값: 0 - 권한 있는 계정 암호를 체크 아웃 또는 체크 인합니다(GetOnly 플래그가 false), 1 - 권한 있는 계정 암호를 가져옵니다(GetOnly 플래그가 true).

응용 프로그램은 권한 있는 계정 암호에 대해 지정된 작업을 수행하고 그 결과를 표시합니다.

참고: semsgtool 유틸리티를 사용하여 숫자로 된 PUPM SDK 오류 코드의 구체적 설명을 볼 수 있습니다. semsgtool 유틸리티에 대한 자세한 내용은 참조 안내서를 참조하십시오.

웹 서비스 PUPM SDK 응용 프로그램을 사용하도록 끝점을 구성하는 방법

웹 서비스 PUPM SDK 를 사용하여 권한 있는 계정 암호를 체크 아웃 및 체크 인하는 Java 응용 프로그램을 작성할 수 있습니다. 응용 프로그램이 엔터프라이즈 관리 서버와 직접 통신하므로 응용 프로그램이 실행되는 끝점에서 CA Access Control 을 설치할 필요가 없습니다.

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

- Apache Ant 1.7
- Apache Axis 1.4
- Java SDK 1.4.2
- (선택 사항) 통합 개발 환경(IDE)

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

웹 서비스 PUPM SDK 를 사용하도록 끝점을 구성하려면 다음을 수행하십시오.

1. 웹 서비스 PUPM SDK 추가 정보를 검토합니다.

이 추가 정보에는 환경을 구성하고, Java 샘플을 만들고, Java 샘플을 실행하는 방법에 대한 지침이 수록되어 있습니다. 추가 정보의 위치:

`ACServerInstallDir\IAM Suite\Access Control\tools\samples\webservice\Axis`

2. SDK 응용 프로그램 작성하려면 Java 샘플을 사용합니다.

웹 서비스 PUPM SDK 응용 프로그램을 사용하도록 끝점을 구성했습니다. 이제 CA Access Control 엔터프라이즈 관리에서 응용 프로그램을 나타내는 사용자를 만들고 이 사용자에게 적절한 권한 있는 액세스 역할을 할당해야 합니다.

추가 정보:

[웹 서비스 SDK 응용 프로그램이 암호를 가져오는 방법](#) (페이지 168)

[웹 서비스 PUPM SDK](#) (페이지 167)

터미널 통합 구성

터미널 통합을 사용하면 CA Access Control 끝점을 PUPM 과 통합하여 권한 있는 계정을 체크 아웃하는 사용자의 작업을 추적할 수 있습니다. 또한 터미널 통합을 사용하면 사용자가 반드시 자동 로그인을 사용하여 권한 있는 계정으로 CA Access Control 끝점에 로그인하도록 지정할 수 있습니다.

터미널 통합을 구현하기 전에 다음을 확인하십시오.

- 터미널 통합을 구성하려는 권한 있는 계정이 CA Access Control 엔터프라이즈 관리에 있습니다.
- 끝점에서 터미널 통합이 활성화되어 있습니다. 즉, PUPM Agent 섹션의 `EnableLogonIntegration` 구성 설정의 값이 1 입니다.

참고: 터미널 통합은 PUPM 통합 기능을 활성화하여 CA Access Control 을 설치할 때 기본적으로 활성화됩니다. 터미널 통합을 활성화만 하고 구성하지 않으면 CA Access Control 이 어떠한 끝점에서도 터미널 통합을 시행하지 않습니다.

- `policyfetcher` 가 구성되고 끝점에서 실행되는지 확인하십시오.
- (UNIX) CA Access Control 이 끝점에 연결하는 데 사용되는 로그인 프로그램에 대해 PAM 로그인 차단을 사용합니다.

예를 들어, 사용자가 SSH 를 사용하여 끝점에 연결하는 경우 CA Access Control 이 PAM 로그인 차단을 사용하여 SSH 로그인을 차단하는지 확인합니다.

참고: PAM 로그인 차단 및 LOGINAPPL 클래스에 대한 자세한 내용은 *selang* 참조 안내서를 참조하십시오.

다음 절차는 하나의 권한 있는 계정에 대해 터미널 통합을 구성하는 방법에 대해 설명합니다. 여러 끝점에서 동일한 이름을 사용하는 권한 있는 계정에 대해 터미널 통합을 구성하기 위해 정책을 사용할 수 있습니다.

다음 단계를 수행하십시오.

1. CA Access Control 끝점 관리에서 "사용자" 탭, "사용자" 하위 탭을 클릭한 다음 터미널 통합을 구성하려는 권한 있는 계정을 검색합니다.

참고: CA Access Control 끝점 관리에서 사용자를 관리하는 방법에 대한 자세한 내용은 *온라인 도움말*을 참조하십시오.

2. 권한 있는 계정을 선택합니다.

"사용자 수정" 작업 페이지의 "일반" 탭이 나타납니다.

3. "계정" 섹션에서 다음 옵션 중 하나 또는 모두를 선택합니다.

원본 ID 사용

감사 레코드를 작성하고 권한 부여 의사 결정을 내릴 때 CA Access Control 이 권한 있는 계정 사용자 이름이 아닌 권한 있는 계정을 체크 아웃한 사용자의 이름을 사용하도록 지정합니다.

로그인 전에 계정 체크 아웃이 필요함

이 권한 있는 계정을 사용하여 끝점에 로그인하려면 사용자가 자동 로그인을 사용해야 함을 지정합니다. 자동 로그인 사용자는 사용자가 암호를 체크 아웃하고 CA Access Control 엔터프라이즈 관리에서 끝점에 자동으로 로그인할 수 있게 해 줍니다.

4. "저장"을 클릭합니다.

권한 있는 계정에 대한 터미널 통합을 활성화하고 구성했습니다.

예: 터미널 통합을 구성하는 정책

다음 정책은 administrator 란 이름의 계정에 대한 터미널 통합을 구성합니다. 이 정책은 CA Access Control 이 권한 부여를 결정하고 감사 레코드를 기록할 때 원래 사용자 이름을 사용하도록 지정하고, 사용자가 반드시 자동 로그인을 사용하여 administrator 로 끝점에 로그인하도록 지정합니다.

```
editusr administrator pupm_flags(use_original_identity)
editusr administrator pupm_flags(required_checkout)
```

추가 정보:

[터미널 통합](#) (페이지 273)

[터미널 통합이 작동하는 방법](#) (페이지 275)

[터미널 통합의 구현 고려 사항](#) (페이지 276)

제 8 장: 공유 계정 관리

이 섹션은 다음 항목을 포함하고 있습니다.

- [권한 있는 계정 암호의 강제 체크 인](#) (페이지 297)
- [권한 있는 계정 암호를 자동으로 다시 설정](#) (페이지 298)
- [권한 있는 계정 암호 직접 다시 설정](#) (페이지 299)
- [공유 계정 요청 관리](#) (페이지 299)
- [수동 암호 추출](#) (페이지 300)
- [권한 있는 계정 감사](#) (페이지 302)
- [암호 소비자 동기화](#) (페이지 307)
- [끝점 관리자 암호 복원](#) (페이지 309)
- [이전 권한 있는 계정 암호 표시](#) (페이지 310)

권한 있는 계정 암호의 강제 체크 인

하나 이상의 사용자에게 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.

공유 계정 요청 관리

*권한 있는 계정 요청*을 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 요청을 삭제할 수 있습니다. 권한 있는 계정 요청을 삭제하려면 사용하는 계정에 기본 권한 있는 계정 요청 또는 PUPM 대상 시스템 관리자 역할(또는 이 작업을 포함하는 동등한 역할)이 할당되어 있어야 합니다.

다음 단계를 수행하십시오.

1. "홈", "내 계정", "권한 있는 계정 요청 관리"를 차례로 클릭합니다.
"권한 있는 계정 요청 관리" 페이지가 나타납니다.
2. 검색 특성을 선택하고 필터 값을 입력한 다음 "검색"을 클릭합니다.
필터 조건에 일치하는 공유 계정 예외의 목록이 표시됩니다.
3. 삭제할 공유 계정 요청을 선택하고 "선택"을 클릭합니다.
선택한 공유 계정 요청의 삭제를 확인하는 확인 메시지가 나타납니다.
4. "예"를 클릭합니다.
공유 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\c
onfig\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 302)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 50)

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 302)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 143)

[PUPM 끝점과 CA User Activity Reporting Module 을 통합하는 방법](#) (페이지 144)

암호 소비자 동기화

CA Access Control 엔터프라이즈 관리에서 서비스 계정의 암호가 변경되면 JCS 는 이 서비스 계정과 연결된 각 암호 소비자의 암호를 변경하려고 시도합니다. JCS 가 암호 소비자의 암호를 변경하지 않으면 "암호 소비자 동기화"를 사용하여 암호 변경을 다시 시도할 수 있습니다.

암호 소비자를 동기화하려면

1. CA Access Control 엔터프라이즈 관리에서 "권한 있는 계정", "암호 소비자", "암호 소비자 동기화"를 클릭합니다.
"암호 소비자 동기화" 작업 페이지가 나타납니다.
2. 검색 특성을 선택하고 필터 값을 입력한 다음 "검색"을 클릭합니다.
필터 조건과 일치하는 암호 소비자의 목록이 표시됩니다.
참고: PUPM 은 Windows Agentless 끝점에서만 서비스 계정을 관리하므로 "끝점 유형" 필드의 값은 "Windows Agentless"입니다.
3. 동기화할 암호 소비자를 선택하고 "제출"을 클릭합니다.
JCS 가 선택한 암호 소비자에 대한 암호를 업데이트하려고 시도합니다.
참고: JCS 는 암호 소비자를 업데이트하기 위해 5 번 시도합니다. JCS 가 암호 소비자를 업데이트하지 못하면 비동기 상태로 표시되고 사용자에게 암호 소비자를 수동으로 동기화하도록 요청합니다.

추가 정보:

[PUPM 이 암호 변경에 대해 암호 소비자에게 통보하는 방법](#) (페이지 139)
[암호 소비자 예제: Windows 예약된 작업](#) (페이지 259)

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 PUPM은 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 9 장: UNAB 사용

이 섹션은 다음 항목을 포함하고 있습니다.

[UNAB 구성 요소](#) (페이지 311)

[UNAB 설정 방법](#) (페이지 312)

[UNAB 가 사용자를 인증하는 방법](#) (페이지 313)

[UNAB 끝점에 저장된 정보](#) (페이지 313)

[호스트 액세스를 제어하고 UNAB 를 구성하는 방법](#) (페이지 314)

[사용자 정보 표시](#) (페이지 326)

[UNAB 중지](#) (페이지 326)

[UNAB 상태 보기](#) (페이지 327)

[UNAB 디버그 파일](#) (페이지 327)

UNAB 구성 요소

UNIX 인증 브로커(UNAB)는 Active Directory 사용자의 UNIX 호스트에 대한 액세스를 관리하고 제어하는 여러 구성 요소로 구성되어 있습니다.

- **UNAB 인증 에이전트** - UNAB 인증 에이전트(uxauthd) 데몬은 Active Directory 와 연결하고 사용자 인증 및 로그인 권한 부여, Active Directory 에 사용자 등록, 사용자/그룹 마이그레이션, 로컬 액세스 파일 관리 등과 관련하여 Active Directory 연결의 보안을 유지할 책임이 있습니다.
- **uxconsole** - uxconsole 은 UNIX 호스트를 Active Directory 에 등록하고, 사용자/그룹을 마이그레이션하고, UNAB 를 등록 및 활성화하는 데 사용하는 UNAB 관리 콘솔입니다.
- **uxpreinstall** - uxpinstall 유틸리티는 UNIX 컴퓨터가 UNAB 시스템 요구 사항을 준수하는지 검사합니다. 가능한 문제점을 진단하고 이 문제점에 대한 제안된 해결 방법 보려면 uxpinstall 유틸리티를 사용하십시오.
- **CA Access Control 엔터프라이즈 관리** - CA Access Control 엔터프라이즈 관리는 중앙 위치에서 UNAB 호스트를 관리할 수 있게 해 줍니다. CA Access Control 엔터프라이즈 관리를 사용하여 회사의 모든 UNAB 호스트에 대한 Active Directory 사용자 액세스를 통제하고, 호스트 로그인 권한 부여를 관리하고, 호스트 마이그레이션 충돌을 해결하고, 보고서를 생성합니다.

UNAB 설정 방법

UNIX 인증 브로커(UNAB)가 UNIX 호스트에 대한 액세스를 제어하는 방식을 이해하면 구현 및 구성 프로세스 중에 도움이 됩니다.

UNIX 호스트에서 UNAB 를 설치한 이후에 UNAB 를 Active Directory 에 등록하고 UNAB 를 활성화하여 UNIX 끝점에 대한 엔터프라이즈 사용자 인증을 활성화합니다. 그런 다음에 마이그레이션 프로세스를 시작하여 로컬 사용자와 그룹을 Active Directory 로 마이그레이션할 수 있습니다.

1. Active Directory 에 UNIX 호스트를 등록합니다.

이 단계에서 UNAB 는 어떠한 로그인 요청도 차단하지 않습니다.

2. UNIX 호스트에 대한 액세스를 허용 또는 거부할 엔터프라이즈 사용자 및 그룹을 정의합니다. 이 작업은 CA Access Control 엔터프라이즈 관리에서 로그인 권한 부여 정책을 만들어 수행할 수 있습니다.
3. UNAB 를 활성화하여 UNIX 호스트에 대한 엔터프라이즈 사용자 인증을 활성화합니다.
4. 새 사용자가 로그인할 수 있게 하려면 추가 엔터프라이즈 사용자 및 그룹을 UNAB 로그인 권한 부여 정책에 추가합니다.

이 단계에서 로그인 은 로컬 사용자 저장소(예: `etc/passwd`)에 정의된 사용자와 UNAB 로그인 권한 부여 정책에서 허용된 엔터프라이즈 사용자에 대해 허용됩니다.

5. Active Directory 로 사용자와 그룹을 마이그레이션합니다.

UNAB 가 사용자를 인증하는 방법

UNIX 호스트에서 UNAB 를 설치하여 구성한 다음에는 선택한 통합 모드에 따라 사용자가 자신의 Active Directory 사용자 계정이나 로컬 사용자 계정을 사용하여 로그인할 수 있게 됩니다.

사용자가 UNAB 가 실행 중인 UNIX 호스트에 로그인하려고 시도하면 다음이 발생합니다.

1. 사용자가 Active Directory 또는 로컬 계정 사용자 이름 및 암호를 입력하도록 요청을 받습니다.
2. UNAB 가 Active Directory, 로그인 인증 정책, 로컬 호스트 액세스 파일을 사용하여 사용자의 자격 증명을 인증하고 사용자 계정에서 가져온 추가 정보를 검사합니다.
3. 사용자가 인증되면 UNAB 는 UNIX 호스트에 사용자가 액세스할 수 있도록 허용합니다. 그렇지 않은 경우 UNAB 는 호스트에 대한 사용자의 액세스를 차단합니다.

UNAB 끝점에 저장된 정보

UNAB 가 사용자를 인증한 다음에 UNAB 는 끝점에 다음 정보를 저장합니다.

- 사용자 이름
- SHA-1 에 해시된 암호
- 사용자 클래스 특성
- 사용자 계정 제어
- 마지막 유효 로그인 시간
- 마지막 실패 로그인 시간
- 마지막 유효 로그인 이후 실패 로그인 횟수

NSS 데이터베이스가 사용자 및 그룹 특성을 `nss.db` 파일에 저장하는 반면, UNAB 는 사용자 정보를 `logon.db` 파일에 저장합니다. 이 두 파일은 다음 디렉터리에 있습니다.

`/opt/CA/uxauth/etc`

호스트 액세스를 제어하고 UNAB 를 구성하는 방법

CA Access Control 엔터프라이즈 관리를 통해 UNIX 호스트에 대한 사용자 및 그룹 액세스를 제어하고 UNAB 호스트를 구성할 수 있습니다. 호스트에 로그인하도록 허가된 사용자 및 그룹에게만 액세스 권한을 부여하여 UNIX 호스트에 대한 사용자 및 그룹 액세스를 제어합니다.

호스트에 대한 통제 액세스를 구성하는 것과 같은 방법으로 UNAB 호스트를 구성합니다. CA Access Control 엔터프라이즈 관리를 사용하여 회사 내 UNAB 호스트의 기능을 먼저 제어한 다음 다른 모든 호스트에 적용합니다.

사용자 및 그룹 로그인 권한 부여를 할당하거나 구성 토큰 값을 정의한 이후에 CA Access Control 엔터프라이즈 관리는 이 정보를 정책에 적용하고 다음을 수행합니다.

1. CA Access Control 엔터프라이즈 관리는 사용자 및 그룹의 목록을 포함하거나 구성 매개 변수를 포함하는 배포 패키지를 만들어 정책을 적용할 호스트 또는 호스트 그룹에 할당합니다.
2. CA Access Control 엔터프라이즈 관리는 호스트에 배포하기 위해 이 패키지를 배포 서버에 전달합니다.
3. UNAB 는 배포 서버에서 이 패키지를 가져와 정책을 설치한 다음 CA Access Control 엔터프라이즈 관리에 확인 메시지를 보냅니다.

참고: 호스트에 엔터프라이즈 정책과 UNAB 로그인 정책을 모두 배포한 경우 엔터프라이즈 로그인 정책이 UNAB 로그인 정책보다 우선 순위가 높습니다.

UNAB 로그인 권한 부여 관리

UNAB 호스트 또는 호스트 그룹에 대한 사용자 로그인을 제어하려면 액세스 권한이 부여된 사용자 또는 그룹의 목록을 만드십시오. 이 목록은 CA Access Control 엔터프라이즈 관리가 선택된 호스트 또는 호스트 그룹에 할당 및 배포하는 정책에 작성됩니다. 로그인 정책의 이름은 `login@hostName` 으로 설정됩니다.

참고: "배포 감사" 작업을 사용하여 정책의 배포 상태를 볼 수 있습니다.

UNAB 로그인 권한 부여를 관리하려면

1. CA Access Control 엔터프라이즈 관리에서 다음을 수행합니다.
 - a. "정책 관리"를 클릭합니다.
 - b. UNIX 인증 브로커 하위 탭을 클릭합니다.
 - c. 작업 메뉴에서 왼쪽에 있는 "호스트" 또는 "호스트 그룹" 트리를 확장합니다.
사용 가능한 작업 목록이 나타납니다.
2. 다음 작업 중 *하나*를 수행합니다.
 - "호스트 로그인 권한 부여 관리"를 클릭합니다.
"호스트 로그인 권한 부여 관리: 호스트 검색" 화면이 나타납니다.
 - "호스트 그룹 로그인 권한 부여 관리"를 클릭합니다.
"호스트 그룹 로그인 권한 부여 관리: 호스트 그룹 검색" 화면이 나타납니다.
3. 수정할 호스트 또는 호스트 그룹의 이름을 입력하고 "검색"을 클릭합니다.
필터 조건과 일치하는 호스트 또는 호스트 그룹의 목록이 나타납니다.
4. 수정할 호스트 또는 호스트 그룹을 선택하고 "선택"을 클릭합니다.
"호스트 로그인 권한 부여 관리: *HostName*" 또는 "호스트 그룹 로그인 권한 부여 관리: *HostGroupName*" 페이지가 나타납니다.

5. (선택 사항) 다음과 같이 사용자를 추가합니다.
 - a. 풀다운 메뉴에서 사용자를 선택합니다.
 - b. 다음 형식으로 사용자의 이름을 입력합니다: *domain/user*.
 - c. "추가"를 클릭합니다.

추가한 사용자가 권한이 부여된 사용자 및 그룹 목록에 나타납니다.
 6. (선택 사항) 다음과 같이 그룹을 추가합니다.
 - a. 풀다운 메뉴에서 그룹을 선택합니다.
 - b. 추가할 그룹의 이름을 입력합니다.
 - c. "추가"를 클릭합니다.

추가한 그룹이 권한이 부여된 사용자 및 그룹 목록에 나타납니다.
 7. (선택 사항) 다음과 같이 사용자 및 그룹을 제거합니다.
 - a. 권한이 부여된 사용자 및 그룹 목록에서 제거할 사용자 및 그룹을 선택합니다.
 - b. "제거"를 클릭합니다.

선택한 사용자 및 그룹은 권한이 부여된 사용자 및 그룹 목록에서 제거됩니다.
 8. "제출"을 클릭합니다.
- CA Access Control 엔터프라이즈 관리는 사용자 및 그룹의 업데이트된 목록을 지정된 호스트 또는 호스트 그룹에 할당합니다.

UNAB 호스트 또는 호스트 그룹 구성

UNAB 호스트 및 호스트 그룹을 제어하는 구성 설정을 정의할 수 있습니다. CA Access Control 엔터프라이즈 관리는 UNAB 구성 파일(uxauth.ini) 또는 CA Access Control 구성 파일(acccommon.ini)의 설정 값을 설정하는 데 도움을 줍니다. 구성 설정에 값을 할당하면 CA Access Control 엔터프라이즈 관리는 업데이트된 설정 값을 포함하는 구성 정책을 만들어 호스트 또는 호스트 그룹에 할당합니다. 정책 이름은 `config@hostName` 으로 설정됩니다.

참고: "배포 감사" 작업을 사용하여 정책의 배포 상태를 볼 수 있습니다.

UNAB 호스트 또는 호스트 그룹을 구성하려면

1. CA Access Control 엔터프라이즈 관리에서 다음을 수행합니다.
 - a. "정책 관리"를 클릭합니다.
 - b. UNIX 인증 브로커 하위 탭을 클릭합니다.
 - c. 작업 메뉴에서 왼쪽에 있는 "호스트" 또는 "호스트 그룹" 트리를 확장합니다.
사용 가능한 작업 목록이 나타납니다.
2. 다음 작업 중 *하나*를 수행합니다.
 - "UNAB 호스트 구성"을 클릭합니다.
"UNAB 호스트 구성: 호스트 검색" 화면이 나타납니다.
 - "UNAB 호스트 그룹 구성"을 클릭합니다.
"UNAB 호스트 그룹 구성: 호스트 그룹 검색" 화면이 나타납니다.
3. 수정할 호스트 또는 호스트 그룹의 이름을 입력하고 "검색"을 클릭합니다.
필터 조건과 일치하는 호스트 또는 호스트 그룹의 목록이 나타납니다.
4. 수정할 호스트 또는 호스트 그룹을 선택하고 "선택"을 클릭합니다.
"UNAB 구성: HostName" 또는 "UNAB 구성: HostGroupName" 화면이 나타납니다.
5. 수정할 섹션 및 토큰을 선택하고 "토큰 추가"를 클릭합니다.
지정된 구성 토큰이 나타납니다.
6. 구성 토큰의 값을 수정합니다.
참고: 구성 토큰에 대한 자세한 내용은 *참조 안내서*를 참조하십시오.

7. (선택 사항) 수정할 다른 섹션 및 토큰을 선택하고, "토큰 추가"를 클릭하고, 구성 토큰의 값을 필요한 대로 수정합니다.
8. "제출"을 클릭합니다.

CA Access Control 엔터프라이즈 관리는 선택한 UNAB 호스트 및 호스트 그룹의 구성 토큰 값을 설정합니다.

CA Access Control 엔터프라이즈 관리가 호스트에 정책을 커밋했는지 확인

권한 부여 및 구성 목록을 작성한 다음에는 CA Access Control 엔터프라이즈 관리가 변경 내용을 UNAB 호스트의 배포 감사 옵션에 커밋했는지 확인할 수 있습니다.

CA Access Control 엔터프라이즈 관리가 호스트에 정책을 커밋했는지 확인하려면

1. CA Access Control 엔터프라이즈 관리에서 "정책 관리" 탭, "정책" 작업을 차례로 선택한 다음 "배포" 옵션을 확장합니다.
배포 옵션 메뉴가 열립니다.
2. "배포 감사" 옵션을 선택합니다.
배포 감사 검색 화면이 열립니다.
3. 표시할 호스트 및 정책을 선택하고 "실행"을 클릭합니다.
쿼리에 대한 검색 결과가 표시됩니다.
참고: 로그인 정책의 이름은 **login@** 으로 시작됩니다.
4. 결과 줄을 클릭하여 배포 상태를 표시합니다.
CA Access Control 엔터프라이즈 관리는 배포 작업의 상태 및 출력을 표시합니다.

사용자 및 그룹을 Active Directory 로 마이그레이션하는 방법

UNIX 호스트에서 Active Directory 로 사용자를 마이그레이션하면 관리 작업이 하나의 관리 응용 프로그램으로 통합되므로 사용자 및 그룹의 관리가 단순해집니다.

사용자 및 그룹을 Active Directory 로 마이그레이션하려면 다음을 수행하십시오.

1. 에뮬레이션 모드에서 마이그레이션 프로세스를 실행합니다.

에뮬레이션 모드에서 UNAB 는 사용자 또는 그룹을 Active Directory 로 마이그레이션하지 않습니다. 충돌을 발견하면 UNAB 는 사용자 및 그룹 특성에서 가능한 충돌을 보고하는 로그 파일에 이 충돌을 로깅합니다. 기본적으로 UNAB 충돌 파일인 migrate.conflicts 는 다음 디렉터리에 있습니다.

`/opt/CA/uxauth/log`

2. 충돌 파일을 다운로드합니다.

충돌 파일은 CA Access Control 엔터프라이즈 관리로부터 CVS 형식으로 호스트에서 다운로드합니다.

참고: CSV 파일을 다운로드할 수 있으려면 다음 예약된 보고서 스냅샷이 완료될 때까지 기다려야 합니다.

3. Active Directory 로 마이그레이션할 각 로컬 계정에 대해 Active Directory 계정을 만듭니다.

UNAB 는 기존 Active Directory 사용자 계정이 있는 사용자만 마이그레이션합니다.

참고: 사용자 계정을 만들 때 UNIX 특성을 지정할 필요는 없습니다. Active Directory 에 그룹을 만들 필요는 없습니다. 마이그레이션 도구가 마이그레이션 프로세스 중에 그룹을 만듭니다.

4. 충돌을 해결하는 CSV 파일을 호스트에 업로드합니다.

UNAB 는 마이그레이션 프로세스를 다시 시작하여 해결된 계정과 그룹의 마이그레이션을 시도합니다.

5. 마이그레이션이 끝난 후 충돌 파일을 다시 검토하여 이전에 충돌 파일에서 보고된 사용자 및 그룹이 성공적으로 마이그레이션되었는지 확인합니다.

마이그레이션 충돌 해결

UNAB 는 마이그레이션 프로세스 중에 발견한 충돌을 충돌 파일에 로깅합니다. 이 파일은 로컬 호스트에서 **Active Directory** 로 사용자 및 그룹을 마이그레이션하지 못하게 만든 충돌의 원인에 대한 자세한 정보를 수록합니다.

이 충돌 파일을 **CSV** 파일로 내보내 컴퓨터로 다운한 다음 검토하여 충돌을 해결할 수 있습니다. 나중에 수정된 스프레드시트를 **CA Access Control** 엔터프라이즈 관리로 업로드하면 메시지 큐 서버로 이 시트가 전달됩니다. UNAB 는 이 파일을 검색한 다음 마이그레이션 프로세스를 다시 시작하여 이전에 마이그레이션되지 않은 사용자 및 그룹을 마이그레이션합니다.

참고: 호스트 그룹을 마이그레이션하는 경우 충돌 파일을 다운로드할 수 없습니다. 하지만 마이그레이션 프로세스의 충돌을 해결할 수 있도록 수정된 충돌 파일을 업로드할 수 있습니다.

마이그레이션 충돌을 해결하려면

1. **CA Access Control** 엔터프라이즈 관리에서 다음을 수행합니다.
 - a. "정책 관리"를 클릭합니다.
 - b. **UNIX** 인증 브로커 하위 탭을 클릭합니다.
 - c. 작업 메뉴에서 왼쪽에 있는 "호스트" 또는 "호스트 그룹" 트리를 확장합니다.
사용 가능한 작업 목록이 나타납니다.
2. 다음 작업 중 *하나*를 수행합니다.
 - "호스트 마이그레이션 충돌 해결"을 클릭합니다.
"호스트 마이그레이션 충돌 해결: 호스트 검색" 화면이 나타납니다.
 - "호스트 그룹 마이그레이션 충돌 해결"을 클릭합니다.
"호스트 그룹 마이그레이션 충돌 해결: 호스트 그룹 검색" 화면이 나타납니다.
3. 충돌을 해결할 호스트 또는 호스트 그룹의 이름을 입력한 다음 "검색"을 클릭합니다.
필터 조건과 일치하는 호스트 또는 호스트 그룹의 목록이 나타납니다.

4. 충돌을 해결할 호스트 또는 호스트 그룹을 선택하고 "선택"을 클릭합니다.
"UNAB 마이그레이션: *HostName*" 또는 "UNAB 마이그레이션: *HostGroupName*" 페이지가 나타납니다.
5. (선택 사항) 다음과 같이 호스트 마이그레이션에 대한 충돌 파일을 다운로드한 다음 충돌을 해결합니다.
 - a. "UNAB 마이그레이션 충돌 세부 정보 다운로드" 섹션에 있는 "내보내기 및 다운로드" 링크를 선택합니다.
대화 상자 창이 열립니다.
 - b. 파일을 저장할 위치로 이동한 다음 "저장"을 선택합니다.
CSV 파일이 지정된 위치로 다운로드됩니다.
 - c. 이 CSV 파일을 열고 파일에 보고된 충돌을 해결한 다음 저장하고 파일을 닫습니다.
6. (선택 사항) 호스트 그룹 마이그레이션에 대한 충돌을 해결하는 CSV 파일을 만들어 저장합니다.
7. 다음과 같이 호스트 및 호스트 그룹 마이그레이션에 대한 충돌을 해결하는 CSV 파일을 업로드합니다.
 - a. "UNAB 마이그레이션 솔루션 업로드" 섹션에서 "찾아보기" 단추를 선택합니다.
대화 상자 창이 열립니다.
 - b. 파일을 찾은 다음 "열기"를 클릭합니다.
 - c. "업로드"를 클릭합니다.
파일이 업로드됩니다.

8. "제출"을 클릭합니다.

CA Access Control 엔터프라이즈 관리는 파일을 메시지 큐로 보냅니다. UNAB 는 큐에서 파일을 검색하고 마이그레이션 프로세스를 다시 시작하여 해결된 계정과 그룹의 마이그레이션을 시도합니다.

9. 마이그레이션이 끝난 후 충돌 파일을 다시 검토하여 이전에 충돌 파일에서 보고된 사용자 및 그룹이 성공적으로 마이그레이션되었는지 확인합니다.

참고: Active Directory 에 동일한 이름의 사용자 또는 그룹이 있으면 사용자 또는 그룹을 마이그레이션할 수 없습니다. 예를 들어, 이름이 g1 인 그룹을 마이그레이션하려고 할 때 이름이 g1 인 사용자가 Active Directory 에 있으면 UNAB 가 이 그룹을 마이그레이션할 수 없습니다.

예: UNAB 충돌 파일 출력

다음 예는 마이그레이션 프로세스 중 작성된 UNAB 충돌 파일의 출력 내용입니다.

```
*** Conflict Details as found by the CA Access Control UNAB Migration tool at 12/29/10
10:49 ***

*** CRITICAL
Conflicts:

***
*** The next found conflicts prevent the user/group migration and need the
intervention ***
*** of the system administrator as they cannot be solved by the migration
tool. ***

User 'John' conflicts:
  User 'John' from domain 'development.computer.com' is assigned id '47670' and Unix
id is '300821'
  User 'John' from domain 'development.computer.com' is assigned primary group
'47670' and Unix primary group is '1011'
  User 'John' from domain 'development.computer.com' is assigned home directory
'/home/aletestu' and Unix home directory is '/home/john1'
  User 'John' from domain 'development.computer.com' is assigned shell
'/sbin/nologin' and Unix shell is '/bin/bash'

*** AUTOMATIC
Conflicts:

***
*** Migration tool will try to solve the next found conflicts when run in
"administrative mode",
***
*** if not solved this conflicts will prevent the user/group
migration
Group 'alegcheck' conflicts:
  Cannot add members to Active Directory group 'dev_users' because UNIX group
'dev_users' contains member[s] that do not exist in domain
'development.computer.com'.
  UNIX group 'alegcheck' members: aleucheck1;aleucheck2
User 'John1' conflicts:
  User 'John1' from domain 'development.computer.com' has no UNIX attributes.

*** IGNORED
Conflicts:

***
*** The next found Conflicts are shown for informational purpose, they will be
ignored for
```

```
***      while migration the
user/group
```

```
***
```

User 'John' conflicts:

User 'John' from domain 'development.computer.com' is assigned geccos '' and Unix geccos is 'gecos of John'

User 'John' primary group '1011' was not migrated

이 예에서 UNAB 는 다음과 같은 중요 충돌을 보고했습니다.

- 사용자 'john'에 다음 특성이 없습니다.
 - 사용자 id(47670)가 UNIX 사용자 id(300821)와 충돌합니다.
 - 사용자 주 그룹(47670)이 Active Directory 그룹(1011)과 충돌합니다.
 - 사용자 홈 UNIX 디렉터리(home/john1)가 Active Directory 홈 디렉터리 설정(/home/john)과 충돌합니다.
 - 사용자 UNIX 셸(/bin/bash)이 Active Directory 셸 특성(/sbin/nologin)과 충돌합니다.

UNAB 가 다음과 같은 충돌을 보고했습니다. 다음에 마이그레이션 프로세스가 실행될 때 UNAB 는 이 충돌을 해결하려고 시도합니다.

- UNIX 그룹(dev_users)이 Active Directory 에 없습니다.
- UNIX 특성이 사용자 'john1'에 대해 구성되지 않았습니다.

<una>가 마이그레이션 프로세스 중에 무시할 다음과 같은 사소한 충돌을 보고했습니다.

- The user geccos ("") conflicts with the UNIX assigned geccos (gecos for john)
- 사용자 주 그룹(1011)이 마이그레이션되지 않았습니다.

예: UNAB 충돌 해결 파일

다음 예는 UNAB 가 충돌 파일에서 보고한 충돌을 해결하기 위해 사용자가 작성하는 UNAB 충돌 해결 CSV 파일에서 가져왔습니다. CA Access Control 엔터프라이즈 관리를 사용하여 이 CSV 파일을 UNAB 호스트에 제출합니다.

솔루션 엔터티 유형	솔루션 엔터티 이름	솔루 션 작업	솔루 션 AD 매핑 이름	충돌	U I D	홈 디렉 터리	GI D	소속 그룹	구 성 원	GEC OS
USER	수퍼유 저		root	그룹 마이그 레이션, AD 없음	1	/home /super user/	1			

이 예에서 충돌 해결 CSV 파일은 다음을 포함하고 있습니다.

- 솔루션 엔터티 유형 - USER
- 솔루션 엔터티 이름 - superuser
- 솔루션 AD 매핑 이름 - root
- 충돌 - 사용자 그룹이 Active Directory 에 없습니다.
- UID - 1
- 홈 디렉터리 - /home/superuser/
- GID - 1

참고: 사용자 마이그레이션에 대한 자세한 내용은 *구현 안내서*를 참조하십시오.

사용자 정보 표시

UNAB 는 계정 유형(로컬 또는 엔터프라이즈 사용자 계정), 로그인 상태(허용 및 거부), 로그인 이유와 같은 사용자 계정에 대한 정보를 표시할 수 있습니다. 로컬 또는 엔터프라이즈 계정의 목록과 자세한 계정 정보를 표시하도록 선택할 수 있습니다.

사용자 정보를 표시하려면

1. bin 디렉터리로 이동합니다. 기본적으로 이 디렉터리는 다음 경로 아래에 있습니다.

```
/opt/CA/uxauth/bin
```

2. 다음 명령 중 하나를 입력합니다.

```
./uxconsole -manage -find -user <filter>
```

```
./uxconsole -manage -show -detail -user <filter>
```

UNAB 는 지정한 옵션에 따라 사용자의 세부 정보를 표시합니다.

참고: 와일드카드 문자(*)를 사용할 수 있습니다.

참고: uxconsole 유틸리티에 대한 자세한 내용은 [참조 안내서](#)를 참조하십시오.

UNAB 중지

UNAB 의 새 버전을 설치하거나 운영 체제를 업데이트하는 경우 UNAB 를 중지해야 합니다.

uxauthd.sh 스크립트를 중지하여 UNAB 를 중지합니다.

UNAB 를 중지하려면

1. root 로 UNIX 컴퓨터에 로그인합니다.
2. UNAB bin 디렉터리로 이동합니다.
3. 다음 명령을 입력합니다.

```
./uxauthd.sh -stop
```

UNAB 데몬이 중지됩니다.

UNAB 상태 보기

UNAB의 최신 상태를 보려면 이 옵션을 사용하십시오.

UNAB 상태를 보려면

1. 해당 컴퓨터의 관리 권한이 있는 사용자로 UNIX 컴퓨터에 로그인합니다.
2. UNAB bin 디렉터리로 이동합니다.
3. 다음 명령을 실행합니다.

```
./uxconsole -status -detail
```

UNAB의 현재 상태를 알리는 메시지가 표시됩니다.

참고: `uxconsole` 유틸리티에 대한 자세한 내용은 [참조 안내서](#)를 참조하십시오.

UNAB 디버그 파일

`uxauth.ini` 파일에 있는 UNAB 구성 파일의 에이전트 섹션은 런타임에 에이전트에 의해 수집된 디버깅 정보를 정의합니다. 기본적으로 UNAB는 다음 파일에서 디버그 정보를 수집합니다. 여기서 `UNABInstallDir`는 UNAB를 설치한 디렉터리입니다.

```
UNABInstallDir/log/debug/agent_debug
```

디버그 메커니즘이 UNAB 구성 파일에서 활성화되어 있는 한, UNAB 에이전트는 `uxauthd` 데몬이 시작할 때 디버그 파일에 디버그 메시지를 로깅합니다.

`-debug` 옵션을 사용하여 UNAB를 시작하는 경우 디버그 메시지가 사용자 콘솔에 나타납니다.

제 10 장: 보고서 작성

이 섹션은 다음 항목을 포함하고 있습니다.

[보안 표준](#) (페이지 329)

[보고서 유형](#) (페이지 330)

[보고 서비스](#) (페이지 330)

[CA Access Control 엔터프라이즈 관리에서 보고서를 보는 방법](#) (페이지 336)

[표준 보고서](#) (페이지 345)

[사용자 지정 보고서](#) (페이지 372)

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 데이터 및 이벤트에 대한 정보를 볼 수 있습니다.

- CA Access Control 보고서 - 누가 무엇을 할 수 있는지 설명합니다.

CA Access Control 보고서는 각 끝점에 있는 CA Access Control 데이터베이스의 데이터에 대한 정보(끝점 및 정책 위반에 배포하는 규칙 및 정책)를 제공합니다. CA Access Control 보고서는 CA Business Intelligence 및 CA Access Control 엔터프라이즈 관리에서 볼 수 있습니다.

- 감사 보고서 - 누가 무엇을 했는지 설명합니다.

감사 보고서는 각 끝점에 있는 감사 로그 파일(seos.audit)의 데이터에 대한 정보(어떤 사용자가 끝점에서 어떤 작업을 수행했는지에 대한 정보)를 제공합니다. 감사 보고서는 CA Enterprise Log Manager 및 CA Access Control 엔터프라이즈 관리에서 볼 수 있습니다.

참고: CA Enterprise Log Manager 에서 감사 보고서를 보는 방법에 대한 자세한 내용은 *CA Enterprise Log Manager Overview Guide*(CA Enterprise Log Manager 개요 안내서)를 참조하십시오.

참고: CA Access Control 보고서와 CA Access Control 감사 보고서를 보려면 추가 구성 요소를 설치하여 구성해야 합니다. 자세한 내용은 *구현 안내서*를 참조하십시오.

보고 서비스

CA Access Control 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 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 실제 끝점 상태를 확인해야 하는 모든 경우에 도움이 됩니다.

보고 서비스는 각 끝점에서 수집한 데이터를 검색할 수 있도록 구성되어 있습니다. 다양한 용도에 맞게 사용자 지정 보고서를 작성하거나 CA Access Control 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 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 각각의 CA Access Control 또는 UNAB 에서 실행되는 Windows 서비스 또는 UNIX 데몬이며, 배포 서버에 있는 구성된 메시지 큐의 큐로 정보를 보냅니다.
- **메시지 큐**는 보고서 에이전트가 보내는 끝점 정보를 받기 위해 구성된 배포 서버의 구성 요소입니다. 보고를 위해 메시지 큐는 중앙 데이터베이스와 끝점 데이터베이스 스냅샷을 주고 받습니다. 중복 및 장애 조치를 위해 정보를 수집하고 전달하는 여러 개의 보고서 서버를 사용할 수 있습니다.
- **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.
- CA Access Control 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.
- 보고서를 보고 관리하기 위해 웹 브라우저를 실행하는 컴퓨터

참고: CA Access Control 보고 서비스 구현 및 아키텍처에 대한 자세한 내용은 **구현 안내서**를 참조하십시오.

보고 서비스 작동 방법

보고 서비스를 사용하면 각 CA Access Control 및 UNAB 끝점, 사용자 저장소, PUPM 정책 저장소에서 수집한 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 CA Access Control 및 UNAB 끝점에서 데이터를 수집합니다.
각 끝점은 보고서 데이터를 배포 서버의 메시지 큐로 보냅니다.
- 중앙 데이터베이스에 데이터를 저장합니다.
CA Access Control 엔터프라이즈 관리는 메시지 큐에서 보고서 데이터를 가져와 중앙 데이터베이스에 저장합니다.
- 보고서 데이터의 스냅샷을 캡처하여 중앙 데이터베이스에 저장합니다.
CA Access Control 엔터프라이즈 관리는 스냅샷의 일부로 PUPM 보고서 데이터를 캡처합니다.
- 저장된 데이터에서 보고서를 생성합니다.
중앙 데이터베이스에 데이터가 있으면 보고서 포털을 사용하여 보고서를 생성하고 저장된 데이터를 검사할 수 있습니다. 보고서 포털은 CA Technologies 버전의 BusinessObjects InfoView 포털로서, 중앙 데이터베이스에 연결되도록 구성되었으며 미리 구성된 CA Access Control 보고서에 포함되어 제공됩니다.

참고: 보고서 서비스 아키텍처에 대한 자세한 내용은 *구현 안내서*를 참조하십시오.

각 끝점에서 보고용 데이터를 수집하는 방법

보고서를 생성하려면 각 끝점에서 데이터를 수집해야 합니다. 보고 서비스는 각 CA Access Control 및 UNAB 끝점에 설치된 보고서 에이전트를 사용하여 예약된 시간에 또는 요청 시 해당 끝점에서 데이터를 수집합니다.

참고: 보고서 에이전트는 CA Enterprise Log Manager 와의 통합에 대한 감사 데이터를 수집하고 라우팅하는 역할도 수행합니다. 이 프로세스에서는 보고서 에이전트가 끝점에 대한 보고를 위해 수행하는 작업만 설명합니다.

보고서 에이전트는 각 끝점에서 다음 작업을 수행합니다.

1. 위반 계산을 수행하고 그 결과를 배포 서버로 보냅니다.

중요! 보고서 에이전트를 정기적으로 실행하도록 설정하고 **DMS** 를 업데이트할 필요가 없는 경우에는 정책 위반 계산을 별도로 예약할 필요가 없습니다.

2. CA Access Control 끝점에서 각 정책 모델 데이터베이스(PMDB)와 CA Access Control 데이터베이스(seosdb)의 사본을 만들거나 UNAB 끝점에서 UNAB 데이터베이스의 사본을 만듭니다.

이 복사본은 CA Access Control 성능에 영향을 미치지 않고 데이터를 처리할 수 있도록 보고서 에이전트가 사용하는 임시 복사본입니다.

3. 각 데이터베이스에서 XML 구조로 데이터를 덤프합니다.

이 덤프는 데이터베이스에 있는 모든 개체의 덤프입니다. 즉, **selang** 같은 데이터베이스 인터페이스 유틸리티를 통해 표시되는 데이터뿐만 아니라 모든 데이터가 캡처됩니다.

4. 데이터베이스의 XML 버전을 배포 서버로 보냅니다.

보고서 에이전트는 데이터를 배포 서버의 보고 큐로 보냅니다.

참고: 보고를 위한 데이터는 PUPM 끝점에서 수집되지 않습니다.

각 끝점의 데이터를 처리 및 저장하는 방법

각 끝점에서 수집된 데이터는 처리를 위해 배포 서버로 보내집니다. 처리된 데이터는 보고서 생성을 위해 중앙 데이터베이스에 전송되어 저장됩니다.

배포 서버에서는 다음 작업을 수행합니다.

1. 각 끝점의 보고서 에이전트로부터 끝점의 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 스냅샷에서 캡처).

CA Access Control 엔터프라이즈 관리가 스냅shots을 캡처하는 방법

CA Access Control 엔터프라이즈 관리는 끝점 덤프를 포함하여 데이터가 보고서에 표시되기 전에 스냅shots에서 보고서 데이터를 캡처해야 합니다. CA Access Control 엔터프라이즈 관리가 스냅shots을 캡처한 다음에 CA Access Control 보고서를 생성하고 볼 수 있습니다.

스냅shots 정의에 지정된 시간에 CA Access Control 엔터프라이즈 관리는 스냅shots을 캡처하기 위해 다음 작업을 수행합니다.

- 사용자 저장소의 데이터를 중앙 데이터베이스로 추출합니다.
- PUPM 정책 저장소의 데이터를 중앙 데이터베이스로 추출합니다.
- 중앙 데이터베이스에 있는 최신 끝점 스냅shots을 스냅shots에 포함하도록 플래그 지정합니다.

끝점 스냅shots을 배포 서버로 보내기

보고를 위한 끝점을 구성할 때 보고서 에이전트가 로컬 CA Access Control 데이터베이스와 끝점의 모든 PMDB의 예약된 스냅shots을 수집하여 이 스냅shots을 배포 서버의 보고서 큐로 보내는 시간을 지정합니다. 예약된 시간까지 기다리지 않으려면 즉시 끝점 스냅shots을 배포 서버로 보낼 수 있습니다.

참고: `accommon.ini` 파일 또는 CA Access Control 레지스트리 키의 `ReportAgent` 섹션에서 일정 구성 설정을 변경하여 보고서 에이전트 일정을 변경할 수 있습니다.

필요 시 끝점 스냅shots을 배포 서버로 보내려면

1. 끝점에서 명령 프로그램 창을 엽니다.
2. (UNIX) 다음과 같이 라이브러리 경로 환경 변수를 설정합니다.
 - a. root 로 su 를 실행합니다.
 - b. 라이브러리 경로 환경 변수를 `ACSharedDir/lib` 로 설정합니다.
기본적으로 `ACSharedDir` 는 다음 디렉터리입니다.
`/opt/CA/AccessControlShared`
 - c. 라이브러리 경로 환경 변수를 내보냅니다.

3. (UNIX) 다음 디렉터리로 이동합니다.

`ACSharedDir/bin`

4. 끝점에서 보고서 에이전트를 실행합니다. 다음 작업 중 *하나*를 수행합니다.

- (Windows) 다음 명령을 실행합니다.

`ReportAgent -report snapshot`

- (UNIX) 다음 명령을 실행합니다.

`./ReportAgent -report snapshot`

보고서 에이전트는 CA Access Control 데이터베이스와 모든 로컬 PMDB의 스냅샷을 배포 서버의 보고서 큐로 보냅니다.

참고: 보고를 위해 끝점을 구성하는 방법에 대한 자세한 내용은 *구현 안내서*를 참조하십시오. **ReportAgent** 섹션에 대한 자세한 내용은 *참조 안내서*를 참조하십시오. 라이브러리 경로 환경 변수에 대한 자세한 내용은 *문제 해결 안내서*를 참조하십시오.

CA Access Control 엔터프라이즈 관리에서 보고서를 보는 방법

이 프로세스는 PUPM, CA Access Control 및 UNAB 끝점, 사용자 저장소에 대한 정보를 제공하는 CA Access Control 보고서를 만들고 보는 방법에 대해 설명합니다. CA Access Control 보고서는 CA Business Intelligence 에서도 볼 수 있습니다.

CA Access Control 엔터프라이즈 관리에서 보고서를 보려면 다음을 수행하십시오.

1. 스냅샷 정의를 만듭니다.

스냅샷 정의는 CA Access Control 이 수집하는 보고서 데이터를 지정하고 스냅샷 일정을 정의합니다.

2. 보고를 위해 CA Access Control 및 UNAB 끝점을 구성했는지 확인합니다.

3. (선택 사항) 스냅샷 데이터를 캡처합니다.

예약된 스냅샷을 기다리고 싶지 않으면 "스냅샷 데이터 캡처" 작업을 사용하여 스냅샷을 지금 수집할 수 있습니다.

4. 보고서를 실행합니다.

보고서가 만들어집니다.

5. 보고서를 봅니다.

참고: 스냅샷 정의를 만들고 보고를 위해 끝점을 구성하는 방법에 대한 자세한 내용은 *구현 안내서*를 참조하십시오.

스냅샷 데이터 캡처

일반적으로 보고서 데이터는 예약된 간격으로 스냅샷에 캡처됩니다. 필요할 때 스냅샷 데이터를 캡처하려면 "스냅샷 데이터 캡처" 작업을 사용하여 데이터를 중앙 데이터베이스로 즉시 내보내십시오.

중요! 많은 양의 데이터를 내보내는 경우 스냅샷 데이터를 내보내는 데 시간이 오래 걸릴 수 있습니다. 보고 스냅샷에 많은 양의 데이터가 포함되는 경우 스냅샷을 예약하기 위한 스냅샷 정의를 만드는 것이 좋습니다.

참고: 기본적으로, 스냅샷 정의를 캡처하려면 시스템 관리자 역할이 있어야 합니다.

스냅샷 데이터를 캡처하려면

1. CA Access Control 엔터프라이즈 관리에서 다음을 수행합니다.
 - a. "보고서"를 클릭합니다.
 - b. "작업" 하위 탭을 클릭합니다.
 - c. "스냅샷 데이터 캡처"를 클릭합니다.

"스냅샷 데이터 캡처" 페이지가 표시됩니다.

2. 캡처할 스냅샷 정의의 이름을 선택하고 "제출"을 클릭합니다.

CA Access Control 엔터프라이즈 관리가 스냅샷 데이터를 중앙 데이터베이스로 내보냅니다.

참고: "제출된 작업 보기" 작업을 사용하여 작업의 진행 상황을 확인할 수 있습니다. 스냅샷 정의를 만드는 방법에 대한 자세한 내용은 [구현 안내서](#)를 참조하십시오.

CA Access Control 엔터프라이즈 관리에서 보고서 실행

CA Access Control 보고서는 PUPM, CA Access Control 및 UNAB 끝점, 사용자 저장소에 있는 데이터에 대한 정보를 제공합니다.

보고서는 CA Access Control 엔터프라이즈 관리가 스냅샷에서 캡처하는 데이터로 구성되어 있습니다. CA Access Control 엔터프라이즈 관리가 스냅샷을 캡처한 이후에 스냅샷에 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 CA Business Intelligence에서는 되풀이 보고서를 예약할 수 있습니다. CA Business Intelligence에서 보고서를 예약하는 경우 CA Access Control 엔터프라이즈 관리에서 이 보고서를 볼 수 없지만 CA Access Control 엔터프라이즈 관리에서 보고서를 실행하면 CA Business Intelligence에서 이 보고서를 볼 수 있습니다.

CA Access Control 엔터프라이즈 관리에서 보고서를 실행하려면

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.

- 숫자 매개 변수를 지정했는데 이 매개 변수에 비슷자 값을 입력하면 보고서가 실패합니다.
- 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 342)

보고서 보기

CA Access Control 보고서는 PUPM, CA Access Control 및 UNAB 끝점, 사용자 저장소에 있는 데이터에 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.

보고서를 보려면

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.

스냅샷 관리

CA Access Control 엔터프라이즈 관리를 사용하여 스냅샷 정의를 보고, 수정하고, 삭제할 수 있습니다. 스냅샷 정의를 보거나 수정할 때 "프로필", "되풀이" 및 "유지 관리" 탭이 표시됩니다. "유지 관리" 탭은 스냅샷을 한 번 캡처한 후에만 표시됩니다.

중요! 여러 스냅샷 정의를 활성화하지 마십시오. 여러 스냅샷 정의가 활성화된 경우 CA Access Control 엔터프라이즈 관리는 모든 보고서를 성공적으로 실행할 수 없습니다.

스냅샷 정의를 보거나, 수정하거나, 삭제하려면 "보고서", "작업", "스냅샷 정의 관리"로 이동하여 실행할 작업을 클릭하십시오.

참고: 데이터를 중앙 데이터베이스로 내보내기 위해 스냅샷 정의가 사용되고 있는 경우에는 해당 스냅샷 정의를 삭제할 수 없습니다. 사용되는 스냅샷 정의를 삭제하면 중앙 데이터베이스로 데이터를 내보내는 작업이 중지되지만 스냅샷 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.

보고서 작업을 위해 InfoView 를 열려면

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 로그인 페이지가 나타납니다.

2. InfoView 를 설치할 때 설정한 자격 증명을 입력하고 "로그온"을 클릭합니다.

InfoView 홈 페이지가 나타납니다.

참고: BusinessObjects InfoView 사용에 대한 자세한 내용은 *BusinessObjects Enterprise XI Release 2 InfoView 사용자 안내서*를 참조하십시오.

보고서 실행

보고 인터페이스(BusinessObjects InfoView)를 연 후 보고서를 선택하고 실행할 수 있습니다.

보고서를 실행하려면

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*.

참고: BusinessObjects InfoView 사용에 대한 자세한 내용은 *BusinessObjects Enterprise XI Release 2 InfoView 사용자 안내서*를 참조하십시오.

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.
설정된 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

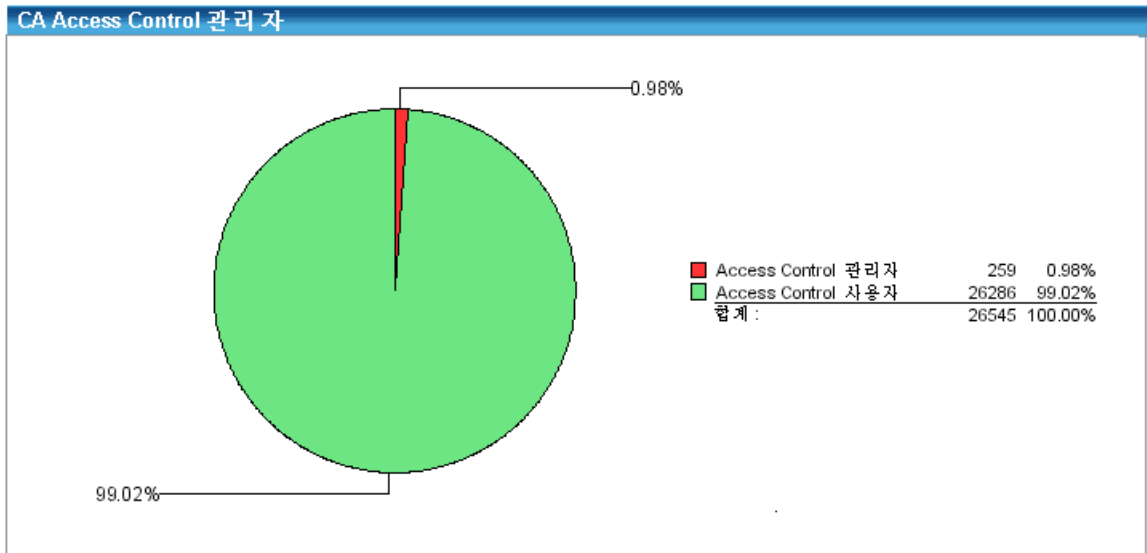
기본적으로 CA Access Control 보고 서비스는 보고서 포털 설치의 일부로 표준 보고서와 함께 제공됩니다. 보고서는 다음과 같은 범주로 구분됩니다.

- [계정 관리 보고서](#) (페이지 347)
- [허용 권한 보고서](#) (페이지 351)
- [기타 보고서](#) (페이지 353)
- [정책 관리 보고서](#) (페이지 356)
- [암호 정책 보고서](#) (페이지 360)
- [권한 있는 계정 관리 보고서](#) (페이지 361)
- [UNIX 인증 브로커 보고서](#) (페이지 367)

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 썰기 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		

계정 관리 보고서

표준 계정 관리 보고서는 사용자 계정의 개요를 제공합니다.

참고: 보고서 제목은 BusinessObjects InfoView 에 나타나는 이름입니다.

다음은 표준 계정 관리 보고서의 목록입니다.

- [CA Access Control 관리자](#) (페이지 347)
- [CA Access Control 그룹 사용자 구성원](#) (페이지 347)
- [CA Access Control 그룹](#) (페이지 348)
- [CA Access Control 비활성 기간](#) (페이지 348)
- [CA Access Control 암호 변경](#) (페이지 348)
- [CA Access Control 암호 만료](#) (페이지 349)
- [CA Access Control 암호 정책 준수\(계정\)](#) (페이지 349)
- [CA Access Control 암호 정책 준수\(호스트\)](#) (페이지 349)
- [CA Access Control 권한 분리](#) (페이지 350)
- [CA Access Control 사용자 그룹 구성원](#) (페이지 350)
- [CA Access Control 사용자 생성 날짜](#) (페이지 350)
- [CA Access Control 사용자 중단 날짜](#) (페이지 351)
- [CA Access Control 사용자 업데이트 날짜](#) (페이지 351)

CA Access Control 관리자

CA Access Control 관리자 보고서는 CA Access Control 관리 권한이 있는 모든 사용자 목록을 표시합니다. 여기에는 ADMIN, PWMANAGER 또는 OPERATOR 특성이 있는 사용자가 포함됩니다. 이 보고서는 파이형 차트로 요약 데이터를 표시하고 사용자 이름별 상세 목록을 표 형식으로 표시합니다.

CA Access Control 을 관리할 수 있는 사용자가 많으면 기업이 보안 위험에 노출될 수 있습니다. 물론 평가 중인 끝점이 개발 또는 테스트 환경에 있는 경우 시스템의 사용자 대부분이 CA Access Control 관리자가 되는 것은 정상적입니다.

CA Access Control 그룹 사용자 구성원

CA Access Control 그룹 사용자 구성원 보고서에서는 사용자 그룹 및 해당 구성원을 보여줍니다. 이 보고서에는 세부 정보가 표 형식으로 표시됩니다.

관리를 단순화하기 위해 CA Access Control 환경의 각 사용자를 현재 정의된 CA Access Control 그룹 하나 이상의 구성원으로 포함할 수 있습니다. 리소스 액세스가 일반적으로 그룹에 적용되므로 정기적으로 그룹 구성원 자격을 검토해야 합니다.

CA Access Control 그룹

CA Access Control 그룹 보고서는 그룹이 있는 정의된 호스트 및 그룹 설명뿐만 아니라 중첩 그룹으로 알려진 자식 그룹이 포함되어 있는지 여부를 표시합니다.

회사 전체에서 어떤 호스트에 어떤 그룹이 위치하는지 파악하고 있으면 환경을 관리하는 데 도움이 됩니다. 또한 다른 그룹이 포함된 그룹을 알고 있으면 특정 사용자나 그룹이 특정 리소스에 액세스할 수 있는 이유를 확인하는 데 유용합니다.

CA Access Control 비활성 기간

CA Access Control 비활성 기간 보고서는 지정된 기간(예: 90 일) 동안 로그인하지 않은 사용자를 표시합니다. 또한 해당 사용자가 일시 중단되어 있는지 또는 시스템에 계속 액세스할 수 있는지 여부를 표시합니다. 이 보고서에는 계정이 비활성 상태이고 일시 중단된 사용자와 계정이 비활성 상태이지만 일시 중단되지 않은 사용자를 비교해서 나타낸 요약 원형 차트가 포함되어 있습니다.

모든 엔터프라이즈 환경에서 감사의 주안점은 어떤 사용자가 현재 환경에 액세스할 수 있는지와 마지막으로 액세스한 시간을 파악하는 데 있습니다. 예를 들어 사용자가 마지막으로 리소스에 액세스하여 끝점에 로그인한 시간뿐 아니라 계정이 비활성 상태로 지속된 기간을 표시해야 합니다. 이 보고서는 서비스 계정의 액세스 규칙성을 증명하고 계속 열려 있지만 특정 기간 동안 액세스하지 않은 계정을 식별하는 데 유용합니다.

CA Access Control 암호 변경

CA Access Control 암호 변경 보고서는 지정된 기간 내에 암호를 변경해야 하는 사용자 계정 목록을 표시합니다. 이 보고서에는 암호를 변경할 필요가 없는 사용자 계정, 암호를 업데이트해야 하는 사용자 계정 및 암호가 만료된 사용자 계정의 요약 파이형 차트가 제공됩니다. 또한 호스트 ID 및 사용자 계정의 암호가 만료될 때까지 남은 날짜 같은 세부 정보가 제공됩니다.

유효하지 않은 암호의 상태를 파악하는 것과 유사한 감사 요구 사항은 암호 변경을 보류 중인 사용자 목록을 파악하기 위한 요구 사항입니다. 파악한 정보를 사용하여 곧 무효화될 수 있는 계정에서 보류 중인 보안 노출을 확인할 수 있습니다.

CA Access Control 암호 만료

CA Access Control 암호 만료 보고서는 지정된 일 수 내에 암호를 업데이트하지 않은 사용자 계정을 표시합니다. 이 보고서에는 암호를 업데이트한 사용자 계정, 암호가 만료되어 시스템 액세스가 일시 중단된 사용자 계정 및 암호가 만료되었지만 시스템에 계속 액세스할 수 있는 사용자 계정을 식별하는 요약 파이형 차트가 제공됩니다. 또한 호스트 ID를 포함하여 지난 x 일 내에 암호를 변경하지 않은 사용자 계정에 대한 세부 정보, 마지막 암호 변경 날짜 및 사용자 계정이 시스템에 계속 액세스할 수 있는 이유가 제공됩니다.

CA Access Control에는 추가적인 품질 확인 기능을 제공하고 이전 암호 기록을 유지하여 빈번한 재사용을 방지함으로써 끝점 암호 보안을 향상할 수 있는 기능이 있습니다. 이 구성 요소의 일부로 마지막 암호 변경 날짜가 유지됩니다. CA Access Control은 암호 품질 모델의 이 구성 요소를 사용하여 기업에서 지정된 기간 내에 암호를 변경하지 않은 사용자를 식별할 수 있습니다. 이 보고서가 특히 중요한 이유는 이 보고서를 사용하여 엔터프라이즈 로그인 환경에서 유효하지 않은 암호로 인해 발생할 수 있는 취약점을 중앙에서 확인할 수 있다는 것입니다.

CA Access Control 암호 정책 준수(계정)

CA Access Control 암호 정책 준수(계정) 보고서는 암호 정책(예: 암호 길이와 최소 숫자 및 영문자 수)에 맞지 않는 암호를 가진 사용자 계정을 표시합니다. 이 보고서에는 정책에 맞는 사용자 계정 수와 정책에 맞지 않는 사용자 계정 수를 식별하는 요약 파이형 차트가 제공됩니다. 또한 정책이 적용되지 않는 사용자 계정에 대한 세부 정보가 표 형식으로 제공됩니다.

CA Access Control 암호 정책 준수(호스트)

CA Access Control 암호 정책 준수(호스트) 보고서는 사용자 계정의 암호 정책(예: 암호 길이와 최소 숫자 및 영문자 수)에 맞지 않는 암호를 가진 호스트를 표시합니다. 이 보고서에는 정책에 맞는 호스트 수와 정책에 맞지 않는 호스트 수를 식별하는 요약 파이형 차트가 제공됩니다. 또한 정책이 적용되지 않는 호스트와 해당 호스트에 있는 사용자 계정에 대한 세부 정보가 표 형식으로 제공됩니다.

CA Access Control 권한 분리

CA Access Control 권한 분리 보고서는 권한 분리 정책(예: 사용자가 관리자 사용자 그룹과 감사자 사용자 그룹 모두의 구성원이 될 수 없음)을 위반하는 사용자 계정을 표시합니다. 이 보고서에는 정책에 맞는 사용자 수와 맞지 않는 사용자 수를 비교하는 요약 파이형 차트가 제공됩니다. 또한 정책과 호스트 ID에 맞지 않는 사용자 계정에 대한 세부 정보가 포함되어 있습니다.

모든 엔터프라이즈 환경의 모든 끝점은 OS와 응용 프로그램 구성 요소에 액세스할 수 있는 사용자가 유지 관리해야 합니다. 일반적으로 시스템 관리자는 OS 관점에서 컴퓨터를 유지 관리하고 응용 프로그램 관리자는 응용 프로그램 관점에서 컴퓨터를 유지 관리합니다. 예를 들어 Solaris 시스템 관리자는 UNIX 호스트 파일의 항목을 업데이트하고 Oracle DBA는 Oracle 데이터베이스의 테이블을 유지 관리할 수 있습니다.

이 모델의 장점은 시스템 관리자와 응용 프로그램 관리자가 각각 응용 프로그램의 가용성과 OS의 가용성을 조정하는 데 제한이 있다는 것입니다. 일반적으로 시스템 관리자가 응용 프로그램 관리자 역할까지 수행하는 것은 바람직하지 않습니다.

이 보고서는 사용자들이 서로 다른 역할을 나타내는 두 개의 그룹에 속할 때 잠재적인 충돌을 파악하는 데 도움을 줍니다. 두 그룹의 공통 부분을 검색하고 보고하는 것은 ISO7799, SOX, PCI, HIPAA 및 DoD에 대한 주요 감사 항목 중 하나를 충족하는 데 매우 유용합니다.

CA Access Control 사용자 그룹 구성원

CA Access Control 사용자 그룹 구성원 자격 보고서는 환경에 있는 각 호스트의 사용자 및 그룹 구성원 자격을 표시합니다. 이 보고서에는 사용자 및 사용자가 속한 그룹의 호스트별로 정렬된 세부 정보가 제공됩니다.

CA Access Control 사용자 생성 날짜

CA Access Control 사용자 생성 날짜 보고서는 환경에서 지정된 호스트 또는 모든 호스트에 대해 특정 기간 내에 생성된 사용자 계정을 표시합니다. 이 보고서에는 사용자 계정이 생성된 날짜에 대한 세부 정보가 호스트별로 정렬된 후 다시 사용자 계정별로 정렬되어 제공됩니다.

CA Access Control 사용자 중단 날짜

CA Access Control 사용자 중단 날짜 보고서는 환경에서 지정된 호스트 또는 모든 호스트에 대해 특정 기간 내에 일시 중단된 사용자 계정을 표시합니다. 이 보고서에는 사용자 계정이 중지된 날짜에 대한 세부 정보가 호스트별로 정렬된 후 다시 사용자 계정별로 정렬되어 제공됩니다.

CA Access Control 사용자 업데이트 날짜

CA Access Control 사용자 업데이트 날짜 보고서는 환경에서 지정된 호스트 또는 모든 호스트에 대해 특정 기간 내에 업데이트된 사용자 계정을 표시합니다. 이 보고서에는 사용자 계정이 업데이트된 날짜에 대한 세부 정보가 호스트별로 정렬된 후 다시 사용자 계정별로 정렬되어 제공됩니다.

권한 보고서

표준 권한 보고서는 사용자 및 리소스 권한의 개요를 제공합니다.

참고: 보고서 제목은 BusinessObjects InfoView 에 나타나는 이름입니다.

표준 권한 보고서의 목록입니다.

[CA Access Control 기본 리소스 준수\(호스트\)](#) (페이지 351)

[CA Access Control 그룹 권한](#) (페이지 352)

[그룹별 CA Access Control 리소스 액세스](#) (페이지 352)

[사용자별 CA Access Control 리소스 액세스](#) (페이지 352)

[CA Access Control 사용자 권한](#) (페이지 353)

CA Access Control 기본 리소스 준수(호스트)

CA Access Control 기본 리소스 준수(호스트) 보고서는 지정된 리소스에 대한 기본 설정되지 않은 액세스 권한이 있는 사용자 계정을 표시합니다. 이 보고서에는 기본 설정되지 않은 액세스가 허용된 호스트 수와 기본 설정되지 않은 액세스 권한이 있는 총 사용자 계정 수가 표시된 요약 파이형 차트가 제공됩니다. 기본 설정되지 않은 액세스 권한이 있는 각 사용자 계정의 액세스 권한에 대한 호스트별 세부 정보도 제공됩니다.

CA Access Control 그룹 권한

CA Access Control 그룹 권한 보고서는 사용자 그룹이 액세스할 수 있는 모든 리소스 목록을 표시하며 다음 항목을 확인할 수 있는 리소스 이름별 상세 목록을 표 형식으로 표시합니다.

- 호스트 ID
- 액세스 권한
- 액세스 권한이 기본적으로 부여되는지 또는 프로그램을 사용하여 부여되는지 여부
- 적용 가능한 달력 이름이나 기타 시간 제한 같은 모든 제한
- 리소스를 소유하는 사용자 그룹이기 때문에 액세스 권한이 부여되었는지 여부

이 보고서를 사용하여 기업 전체 또는 특정 호스트에 대해 정의된 리소스에 액세스할 수 있는 사용자 그룹을 확인할 수 있습니다. 검토 후 액세스 권한을 보안 정책에 맞게 변경할 수 있습니다.

그룹별 CA Access Control 리소스 액세스

그룹별 CA Access Control 리소스 액세스 보고서는 지정된 리소스에 대해 사용자 그룹에 부여된 액세스 권한을 표시합니다. 이 보고서에는 호스트 ID, 액세스 권한, 기본 액세스 권한 부여 여부 및 기타 제한 사항(예: 요일 및 시간) 지정 여부를 포함하여 리소스에 액세스할 수 있는 모든 사용자 그룹에 대한 상세 목록이 제공됩니다.

사용자별 CA Access Control 리소스 액세스

사용자별 CA Access Control 리소스 액세스 보고서는 지정된 리소스에 대해 사용자 계정에 부여된 액세스 권한을 표시합니다. 이 보고서에는 호스트 ID, 액세스 권한, 기본 액세스 권한 부여 여부 및 기타 제한 사항(예: 요일 및 시간) 지정 여부를 포함하여 리소스에 액세스할 수 있는 모든 사용자 계정에 대한 자세한 목록이 제공됩니다.

CA Access Control 사용자 권한

CA Access Control 사용자 권한 보고서는 사용자에게 대한 액세스 권한을 리소스별로 표시합니다. 사용자가 액세스할 수 있는 각 리소스에 대해 보고서는 사용자의 액세스 유형, 기본 액세스, 사용자가 리소스에 액세스하기 위해 사용할 수 있는 프로그램, 리소스에 대한 사용자의 액세스 시간 제한을 제공합니다. 이 보고서는 또한 사용자가 리소스 소유자인지 여부를 지정합니다.

기타 보고서

표준 기타 보고서는 모니터링되는 파일, 모니터링되는 프로그램, 시스템을 다시 부팅하지 않고 CA Access Control 커널을 언로드하기 위한 UNIX 호스트의 준비 상태에 대한 정보를 제공합니다.

참고: 보고서 제목은 BusinessObjects InfoView 에 나타나는 이름입니다.

다음은 표준 기타 보고서의 목록입니다.

[CA Access Control 모니터링되는 파일](#) (페이지 353)

[CA Access Control 모니터링되는 프로그램](#) (페이지 354)

[언로드 고려 사항이 있는 CA Access Control UNIX 호스트](#) (페이지 354)

[CA Access Control UNIX 언로드 준비](#) (페이지 355)

CA Access Control 모니터링되는 파일

CA Access Control 모니터링되는 파일 보고서는 기업 전체에서 호스트의 중요한 시스템 파일 상태를 표시합니다. 이 보고서에는 파일이 모니터링되지 않는 호스트, 파일이 모니터링되지만 수정된 호스트 및 파일이 모니터링되고 트러스트된 상태로 유지되는 호스트를 나타내는 요약 파이형 차트가 제공됩니다. 또한 해당 호스트의 파일에 대한 정책을 검토하거나 권한 있는 사용자가 파일을 수정했는지 여부를 검토할 수 있도록 파일의 세부 정보(예: 호스트 ID)가 제공됩니다.

데이터 무결성을 보호하려면 중요한 시스템 파일을 반드시 모니터링해야 합니다. 파일이 변경된 시간을 파악하면 감사 추적을 통해 권한 있는 사용자가 보안 정책에 따라 변경을 수행했는지 확인할 수 있습니다.

CA Access Control 모니터링되는 프로그램

CA Access Control 모니터링되는 프로그램 보고서는 기업 전체에서 호스트의 중요한 프로그램 상태를 표시합니다. 이 보고서에는 프로그램이 모니터링되지 않는 호스트, 프로그램이 모니터링되지만 수정된 호스트 및 프로그램이 모니터링되고 트러스트된 상태로 유지되는 호스트를 나타내는 요약 파이형 차트가 제공됩니다. 또한 해당 호스트의 프로그램에 대한 정책을 검토하거나 권한 있는 사용자가 프로그램을 수정했는지 여부를 검토할 수 있도록 프로그램의 세부 정보(호스트 ID)가 제공됩니다.

데이터 무결성을 보호하려면 중요한 프로그램을 반드시 모니터링해야 합니다. 프로그램이 변경된 시간을 확인하면 감사 추적을 통해 권한 있는 사용자가 보안 정책에 따라 변경을 수행했는지 확인할 수 있습니다.

언로드 고려 사항이 있는 CA Access Control UNIX 호스트

언로드 고려 사항이 있는 CA Access Control UNIX 호스트 보고서는 CA Access Control 커널의 언로드를 방해하는 차단된 시스템 호출이 있는 UNIX 호스트를 표시합니다. 이러한 호스트에서는 커널을 언로드하고 CA Access Control 을 업그레이드하려면 먼저 컴퓨터를 다시 시작해야 합니다.

이 보고서는 언로드 고려 사항이 있는 각 호스트에 대해 프로세스 및 부모 프로세스 ID, 프로그램 이름, 차단 시간, 임계값 시간을 나열합니다. 이 보고서는 또한 각 시스템 호출이 블로킹 호출인지 여부를 지정합니다.

보고서는 다음 범주로 호스트를 그룹화합니다.

- **준비되지 않음(오버플로)** - 시스템 호출 테이블이 크기를 초과했으며 커널을 언로드하기 위해 재부팅이 필요합니다.
- **준비되지 않음(블로킹 시스템 호출)** - 블로킹하는 차단된 시스템 호출이 있으며 커널을 언로드하기 위해 재부팅이 필요합니다.
- **가능성 높음(비블로킹 시스템 호출)** - 블로킹하지 않는 차단된 시스템 호출이 있으며 커널을 언로드하기 위해 일반적으로 재부팅이 필요하지 않습니다.

CA Access Control UNIX 언로드 준비

CA Access Control UNIX 언로드 준비 보고서는 시스템 재부팅 없이 CA Access Control 커널을 언로드하고 CA Access Control 을 업그레이드하기 위한 UNIX 호스트의 준비 상태를 표시합니다.

이 보고서는 커널을 언로드할 준비가 된 호스트, 준비가 되었을 가능성이 높은 호스트, 준비가 되지 않은 호스트의 비율을 원형 차트로 요약 표시합니다. 이 보고서는 또한 각 호스트에 대해 차단된 시스템 호출 및 블로킹하지 않는 시스템 호출의 수를 표시합니다.

보고서는 다음 범주로 호스트를 그룹화합니다.

- **준비되지 않음(오버플로)** - 시스템 호출 테이블이 크기를 초과했으며 커널을 언로드하기 위해 재부팅이 필요합니다.
- **준비되지 않음(블로킹 시스템 호출)** - 블로킹하는 차단된 시스템 호출이 있으며 커널을 언로드하기 위해 재부팅이 필요합니다.
- **가능성 높음(비블로킹 시스템 호출)** - 블로킹하지 않는 차단된 시스템 호출이 있으며 커널을 언로드하기 위해 일반적으로 재부팅이 필요하지 않습니다.
- **준비** - 차단된 시스템 호출이 없으며 커널을 언로드하기 위해 다시 부팅할 필요가 없습니다.
- **해당 없음** - 호스트가 UNIX 호스트가 아닙니다.
- **알 수 없는 상태** - 호스트에 대한 정보가 없습니다.

정책 관리 보고서

표준 정책 관리 보고서는 CA Access Control 엔터프라이즈 관리 정책에 대한 정보를 제공합니다.

참고: 보고서 제목은 BusinessObjects InfoView 에 나타나는 이름입니다.

다음은 표준 정책 관리 보고서의 목록입니다.

[CA Access Control 정책 할당](#) (페이지 356)

[CA Access Control 정책 배포 스코어카드](#) (페이지 357)

[CA Access Control 호스트별 정책 배포 스코어카드](#) (페이지 357)

[CA Access Control 호스트 그룹별 정책 배포 스코어카드](#) (페이지 358)

[CA Access Control 호스트별 정책 배포 상태](#) (페이지 358)

[CA Access Control 호스트 그룹별 정책 배포 상태](#) (페이지 358)

[CA Access Control 정책 인벤토리](#) (페이지 359)

[CA Access Control 정책 규칙](#) (페이지 359)

[CA Access Control 정책 버전](#) (페이지 359)

[CA Access Control 호스트별 규칙 위반](#) (페이지 359)

[CA Access Control 호스트 그룹별 규칙 위반](#) (페이지 360)

CA Access Control 정책 할당

CA Access Control 정책 할당 보고서는 지정된 DMS 에 정의된 호스트 및 호스트 그룹에 배포된 정책의 할당 세부 정보를 표시합니다. 이 보고서에는 다음과 같은 정보가 표시됩니다.

- 정책 이름
- 할당 유형(호스트 또는 호스트 그룹)
- 정책이 배포된 호스트 또는 호스트 그룹의 이름

CA Access Control 정책 배포 스코어카드

CA Access Control 정책 배포 스코어카드 보고서는 지정된 정책에 대한 배포 정보를 표시합니다. 이 보고서는 다음 정보를 원형 차트로 요약하여 표시합니다.

- 정책이 올바르게 배포된 호스트의 수
- 정책이 배포되었지만 오류 또는 위반이 발생한 호스트의 수
- 위험한 상태(정책이 호스트에 할당되었지만 정책이 호스트에 배포되지 않음)인 호스트의 수

이 보고서는 또한 정책 배포에 대한 모든 문제를 호스트별로 자세히 표시합니다.

CA Access Control 호스트별 정책 배포 스코어카드

CA Access Control 호스트별 정책 배포 스코어카드는 정책에 대한 배포 정보를 호스트별로 표시합니다. 이 보고서는 다음 정보를 원형 차트로 요약하여 표시합니다.

- 정책이 올바르게 배포된 호스트의 수
- 정책이 배포되었지만 오류 또는 위반이 발생한 호스트의 수
- 위험한 상태(호스트 또는 호스트가 구성원으로 속해 있는 호스트 그룹에 정책이 할당되었지만 정책이 이 호스트에 배포되지 않음)인 호스트의 수

이 보고서는 또한 정책 배포에 대한 모든 문제를 호스트별로 자세히 표시합니다.

CA Access Control 호스트 그룹별 정책 배포 스코어카드

CA Access Control 호스트 그룹별 정책 배포 스코어카드는 정책에 대한 배포 정보를 호스트 그룹별로 표시합니다. 이 보고서는 다음 정보를 원형 차트로 요약하여 표시합니다.

- 정책이 올바르게 배포된 호스트 그룹의 호스트 수
- 정책이 배포되었지만 오류 또는 위반이 발생한 호스트 그룹의 호스트 수
- 호스트 그룹에서 위험한 상태(정책이 호스트 그룹에 할당되었지만 정책이 호스트에 배포되지 않음)인 호스트 수

이 보고서는 또한 정책 배포에 대한 모든 문제를 호스트 그룹별로 자세히 표시합니다.

CA Access Control 호스트별 정책 배포 상태

CA Access Control 호스트별 정책 배포 상태 보고서는 정책에 대한 상태 정보를 호스트별로 표시합니다. 이 보고서는 다음을 포함하여 각 정책의 버전 정보를 제공합니다.

- 위반 상태
- 배포 시간
- 정책을 배포한 사용자의 이름

CA Access Control 호스트 그룹별 정책 배포 상태

CA Access Control 호스트 그룹별 정책 배포 상태 보고서는 정책에 대한 상태 정보를 호스트 그룹별로 표시합니다. 이 보고서는 다음을 포함하여 각 정책의 버전 정보를 제공합니다.

- 위반 상태
- 배포 시간
- 정책을 배포한 사용자의 이름

이 보고서는 또한 정책이 배포된 호스트 그룹 내의 호스트를 나열합니다.

CA Access Control 정책 인벤토리

CA Access Control 정책 인벤토리 보고서는 다음을 포함하여 DMS에 저장된 정책의 스냅샷을 표시합니다.

- 각 정책이 마지막으로 업데이트된 시간
- 정책을 마지막으로 업데이트한 사용자의 이름
- 정책의 배포된 버전 수
- 정책의 최종 완료된 버전
- 정책이 종속된 다른 정책의 이름

참고: 정책이 다른 정책에 종속된 경우 종속된 상위 정책이 배포될 때까지 정책을 배포할 수 없습니다.

CA Access Control 정책 규칙

CA Access Control 정책 규칙 보고서는 정책에 있는 각 규칙의 배포 및 배포 취소 스크립트를 정책 이름별로 표시합니다. 이 보고서는 규칙이 마지막 업데이트된 날짜와 규칙을 마지막으로 업데이트한 사용자의 이름을 제공합니다. 이 보고서는 또한 정책이 최종 완료되어 배포할 준비가 되었는지 여부를 지정하고 정책 버전 번호를 지정합니다.

CA Access Control 정책 버전

CA Access Control 정책 버전 보고서는 각 정책에 대한 버전 정보를 정책 이름별로 표시합니다. 각 정책에 대해 보고서는 다음 내용을 표시합니다.

- 현재 버전 번호
- 버전이 배포된 날짜
- 현재 버전을 배포한 사용자의 이름

이 보고서는 또한 현재 버전이 최종 완료되었는지 여부도 지정합니다.

CA Access Control 호스트별 규칙 위반

CA Access Control 호스트별 규칙 위반 보고서는 정책 상태 및 규칙 위반을 호스트별로 표시합니다. 이 보고서는 각 호스트에 있는 정책의 목록 및 각 정책의 상태, 버전, 위반 상태를 제공합니다. 정책에 대한 규칙 위반이 있으면 이 보고서는 위반에 대한 세부 정보(즉, 위반이 적용되는 리소스 및 속성에 대한 세부 정보)를 제공합니다.

CA Access Control 호스트 그룹별 규칙 위반

CA Access Control 호스트 그룹별 규칙 위반 보고서는 정책 상태 및 규칙 위반을 호스트 그룹별로 표시합니다. 이 보고서는 각 호스트 그룹에 있는 정책의 목록 및 각 정책의 상태, 버전, 위반 상태를 제공합니다. 정책에 대한 규칙 위반이 있으면 이 보고서는 호스트 그룹에 있는 각 호스트 구성원의 위반에 대한 세부 정보(즉, 위반이 적용되는 리소스 및 속성에 대한 세부 정보)를 제공합니다.

암호 정책 보고서

암호 정책 보고서는 CA Access Control 에 정의된 암호 정책에 대한 정보를 제공합니다.

다음은 표준 암호 정책 보고서의 목록입니다.

[CA Access Control 암호 정책별 권한 있는 계정](#) (페이지 360)

[CA Access Control PUPM 암호 정책](#) (페이지 361)

CA Access Control 암호 정책별 권한 있는 계정

이 보고서는 시스템에 있는 모든 권한 있는 계정과 각각의 암호 정책을 표시합니다. 이 보고서를 사용하여 암호 정책과 연계할 권한 있는 계정을 결정할 수 있습니다. 보고서를 검토한 이후에 암호 정책이 올바르게 할당되었는지 여부와 수정 조치가 필요한지 여부를 파악할 수 있습니다.

이 보고서에는 다음과 같은 정보가 표시됩니다.

- 스냅샷 시간
- 암호 정책 이름
- 끝점 유형 및 이름
- 계정 이름
- 마지막 체크 아웃 날짜
- 마지막 암호 변경

CA Access Control PUPM 암호 정책

이 보고서는 복잡성별로 현재 암호 정책을 표시합니다. 이 보고서를 사용하여 기존 암호 정책의 최소/최대 길이 및 기타 정책 매개 변수가 회사의 보안 표준에 부합하는지 여부를 파악할 수 있습니다.

이 보고서는 다음 정보를 표시합니다.

- 스냅샷 날짜
- 암호 정책 이름 및 설명
- 최대 길이
- 최소 길이
- 암호 정책 매개 변수

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](#) (페이지 362)

[CA Access Control 사용자별 PUPM 역할 및 권한 있는 계정](#) (페이지 362)

[CA Access Control 끝점별 권한 있는 계정 요청](#) (페이지 363)

[CA Access Control 승인자별 권한 있는 계정 요청](#) (페이지 364)

[CA Access Control 요청자별 권한 있는 계정 요청](#) (페이지 365)

[CA Access Control 권한 있는 계정별 PUPM 사용자](#) (페이지 366)

[CA Access Control 역할별 PUPM 사용자](#) (페이지 366)

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.

- 스냅샷 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.

- 스냅샷 시간
- 사용자 ID
- 끝점 시간 및 이름
- 역할 이름 및 설명
- 계정 이름
- 예외
- 마지막 암호 변경

참고: 이 보고서를 생성할 때는 완료될 때까지 시간이 오래 걸릴 수 있습니다.

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.

- 스냅샷 시간
- 끝점 유형 및 이름
- 호스트 이름
- 계정
- 요청자
- 요청 정당화
- 요청 시간
- 승인 시간
- 유효 기간(시작)
- 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.

- 스냅샷 시간
- 승인자 사용자 ID
- 끝점 유형 및 이름
- 호스트 이름
- 계정
- 요청자 이름 및 ID
- 요청 정당화
- 요청 시간
- 승인 시간
- 유효 기간(시작)
- 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.

- 스냅샷 이름
- 승인자 사용자 ID
- 끝점 유형 및 이름
- 호스트 이름
- 계정
- 요청 정당화
- 요청 시간
- 승인 시간
- 유효 기간(시작)
- 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.

- 스냅샷 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.

- 스냅샷 시간
- 역할 이름
- 구성원 수
- 사용자 이름
- 사용자 ID
- 전자 메일 주소

UNIX 인증 브로커 보고서

UNAB 보고서는 UNAB 관리 작업의 세부 정보를 제공합니다.

다음은 표준 UNIX 인증 브로커 보고서의 목록입니다.

[CA Access Control 호스트별 UNAB 엔터프라이즈 사용자 액세스](#) (페이지 367)

[CA Access Control 엔터프라이즈 사용자별 호스트에 대한 UNAB 액세스](#)
(페이지 368)

[CA Access Control UNAB 엔터프라이즈 사용자](#) (페이지 368)

[CA Access Control UNAB 엔터프라이즈 사용자 작업](#) (페이지 368)

[CA Access Control UNAB 엔터프라이즈 그룹](#) (페이지 368)

[CA Access Control 호스트 그룹별 UNAB 호스트](#) (페이지 368)

[CA Access Control UNAB 로컬 그룹 마이그레이션 상태](#) (페이지 369)

[CA Access Control UNAB 로컬 그룹 요약](#) (페이지 369)

[CA Access Control UNAB 로컬 사용자 요약](#) (페이지 370)

[CA Access Control 그룹별 UNAB 로컬 그룹 마이그레이션 상태](#) (페이지 370)

[CA Access Control 호스트별 UNAB 그룹 마이그레이션](#) (페이지 370)

[CA Access Control UNAB 로컬 사용자 마이그레이션 상태](#) (페이지 370)

[CA Access Control 호스트별 UNAB 로컬 사용자 마이그레이션 상태](#) (페이지 371)

[CA Access Control 사용자별 UNAB 로컬 사용자 마이그레이션 상태](#) (페이지 371)

[CA Access Control 그룹별 UNAB 비표준 로컬 그룹](#) (페이지 371)

[CA Access Control 사용자별 UNAB 비표준 로컬 사용자](#) (페이지 371)

CA Access Control 호스트별 UNAB 엔터프라이즈 사용자 액세스

이 보고서는 UNAB 호스트에 액세스한 엔터프라이즈 사용자의 목록을 호스트별로 표시합니다. 이 보고서는 각 호스트에 액세스한 엔터프라이즈 사용자, 이러한 사용자의 마지막 로그인 시도, 호스트에 대한 액세스 권한이 부여된 대상(사용자 또는 그룹)에 대한 정보를 제공합니다. 이 보고서를 검토한 다음에는 엔터프라이즈 사용자의 호스트에 대한 액세스 권한을 변경할 수 있습니다.

CA Access Control 엔터프라이즈 사용자별 호스트에 대한 UNAB 액세스

이 보고서는 UNAB 호스트에 액세스한 엔터프라이즈 사용자의 목록을 사용자별로 표시합니다. 이 보고서는 각 호스트에 액세스한 엔터프라이즈 사용자, 이러한 사용자의 마지막 로그인 시도, 호스트에 대한 액세스 권한이 부여된 대상(사용자 또는 그룹)에 대한 정보를 제공합니다. 이 보고서를 검토한 다음에는 엔터프라이즈 사용자의 호스트에 대한 액세스 권한을 변경할 수 있습니다.

CA Access Control UNAB 엔터프라이즈 사용자

이 보고서는 호스트에 액세스할 수 있는 엔터프라이즈 사용자의 목록을 표시합니다. 이 보고서는 현재 엔터프라이즈 사용자의 계정, ID, 홈 디렉터리, 셸 유형을 표시합니다. 이 보고서를 검토한 다음 사용자 속성을 변경하고 엔터프라이즈 사용자를 추가 또는 제거할 수 있습니다.

CA Access Control UNAB 엔터프라이즈 사용자 작업

이 보고서는 마이그레이션되거나 부분 마이그레이션된 엔터프라이즈 사용자 계정의 작업 목록을 표시합니다. 이 보고서를 사용하여 UNIX 호스트에 있는 엔터프라이즈 사용자의 작업을 검토할 수 있습니다. 이 보고서를 통해 가장 최근의 성공/실패한 로그인 시도, 사용자에게 의한 마지막 성공한 암호 변경 등의 정보를 확인할 수 있습니다.

CA Access Control UNAB 엔터프라이즈 그룹

이 보고서는 엔터프라이즈 그룹의 특성을 표시합니다. 이 보고서는 엔터프라이즈 그룹의 세부 정보(예: 그룹 ID)를 제공합니다.

CA Access Control 호스트 그룹별 UNAB 호스트

이 보고서는 호스트 그룹별로 UNAB 호스트를 표시합니다. 이 보고서를 사용하여 현재 그룹화된 UNAB 호스트의 개요를 볼 수 있습니다.

이 보고서에는 다음 속성이 포함됩니다.

- 호스트 그룹
- 호스트 이름
- 총 수

CA Access Control UNAB 로컬 그룹 마이그레이션 상태

이 보고서는 각 그룹의 각 끝점에 대한 마이그레이션 프로세스의 상태를 표시합니다. 이 보고서를 사용하여 모든 호스트에서 마이그레이션 프로세스의 현재 상태를 검토할 수 있습니다.

이 보고서는 다음 정보를 표시합니다.

- 호스트 이름
- 마이그레이션 상태
- 그룹 이름
- 그룹 ID
- 이름 충돌
- GID 충돌
- 구성원 충돌
- Active Directory 그룹 충돌 없음
- 항목 수

CA Access Control UNAB 로컬 그룹 요약

이 보고서는 로컬 그룹 속성의 요약 정보를 표시합니다. 이 보고서를 사용하여 각 UNAB 호스트에서 동일한 그룹의 인스턴스 수를 파악할 수 있습니다.

이 보고서는 다음 정보를 표시합니다.

- 호스트 수
- 그룹 이름
- 그룹 ID
- 인스턴스 수

CA Access Control UNAB 로컬 사용자 요약

이 보고서는 로컬 사용자 매개 변수의 요약을 표시합니다. 이 보고서 안의 정보는 하나의 사용자 계정이 UNIX 호스트에 표시되는 인스턴스의 수를 표시합니다.

이 보고서는 다음 정보를 표시합니다.

- 호스트 수
- 사용자 이름
- 사용자 ID
- 그룹 ID
- 홈 디렉터리
- 로그인 셸
- 항목 수

CA Access Control 그룹별 UNAB 로컬 그룹 마이그레이션 상태

이 보고서는 그룹별로 로컬 그룹의 마이그레이션 프로세스의 상태를 표시합니다. 이 보고서를 사용하여 각 그룹의 마이그레이션 프로세스에 대한 현재 상태를 검토할 수 있습니다.

CA Access Control 호스트별 UNAB 그룹 마이그레이션

이 보고서는 호스트별로 로컬 그룹의 마이그레이션 상태를 표시합니다. 이 보고서를 사용하면 각 호스트의 그룹에 대한 마이그레이션 상태를 자세히 볼 수 있습니다.

CA Access Control UNAB 로컬 사용자 마이그레이션 상태

이 보고서는 로컬 사용자의 마이그레이션 상태를 표시합니다. 이 보고서를 사용하면 각 사용자의 마이그레이션 상태를 보고 로컬 사용자 특성과 엔터프라이즈 사용자 특성을 서로 비교할 수 있습니다.

CA Access Control 호스트별 UNAB 로컬 사용자 마이그레이션 상태

이 보고서는 호스트별로 로컬 사용자의 마이그레이션 상태를 표시합니다. 이 보고서를 사용하면 각 호스트의 사용자에 대한 마이그레이션 상태를 볼 수 있습니다.

CA Access Control 사용자별 UNAB 로컬 사용자 마이그레이션 상태

이 보고서는 사용자별로 로컬 사용자의 마이그레이션 상태를 표시합니다. 이 보고서를 사용하면 각 로컬 사용자의 마이그레이션 상태를 볼 수 있습니다.

CA Access Control 그룹별 UNAB 비표준 로컬 그룹

이 보고서는 그룹별로 비표준 로컬 그룹에 대한 정보를 표시합니다. 이 보고서를 사용하면 로컬 특성이 엔터프라이즈 특성과 다른 로컬 그룹에 대한 세부 정보를 볼 수 있습니다.

CA Access Control 사용자별 UNAB 비표준 로컬 사용자

이 보고서는 사용자별로 비표준 로컬 사용자에게 대한 정보를 표시합니다. 이 보고서를 사용하면 로컬 특성이 엔터프라이즈 특성과 다른 사용자에게 대한 정보를 볼 수 있습니다.

CA Enterprise Log Manager 보고서

CA Enterprise Log Manager 보고서는 CA Access Control 및 UNAB 계정 작업, 리소스 관리 등에 대한 자세한 정보를 표시합니다.

CA Enterprise Log Manager 보고서에 대한 자세한 내용은 CA Enterprise Log Manager 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.

제 11 장: 예제 및 모범 사례 정책 배포

이 섹션은 다음 항목을 포함하고 있습니다.

[예제 정책](#) (페이지 375)

[예제 정책이 저장되는 위치](#) (페이지 376)

[예제 정책 스크립트](#) (페이지 377)

[컴플라이언스 및 모범 사례 정책](#) (페이지 381)

[컴플라이언스 및 모범 사례 정책이 저장되는 위치](#) (페이지 382)

[컴플라이언스 및 모범 사례 정책 스크립트](#) (페이지 383)

[정책 배포](#) (페이지 386)

예제 정책

CA Access Control 에 포함된 예제 정책은 운영 체제와 응용 프로그램 리소스를 보호하기 위해 권장되는 권한 분리 및 최상의 방법론을 제공합니다. 각 정책은 정책의 용도와 포함된 규칙에 대해 설명하는 주석이 포함된 `selang` 스크립트입니다.

예제 정책은 CA Access Control 을 사용하여 시스템의 보안을 유지하기 위한 기초를 제공합니다. 예제 정책을 실제 정책의 기초로 사용하면 조직을 위한 정책 생성 프로세스를 간소화할 수 있습니다. 예제 정책은 실제 보안 정책 및 환경(운영 체제 정책은 설치한 실제 OS 패키지에 의존)에 맞게 사용자 지정해야 합니다.

예제 정책을 사용자 지정한 이후에 CA Access Control 엔터프라이즈 관리를 사용하여 끝점에 정책을 배포합니다.

예제 정책은 다음과 같은 일반적인 응용 프로그램 및 운영 체제용으로 제공됩니다.

- 응용 프로그램:
 - Apache
 - JBoss Application Server
 - CA Access Control 웹 서비스
 - Microsoft SQL Server 2005
 - Oracle Database 10g

- 운영 체제:
 - AIX
 - HP-UX
 - Red Hat Enterprise Linux
 - SuSe Linux Enterprise Server
 - Sun Solaris
 - Windows 2003
- 가상화 시스템:
 - VMware ESX Server
 - Hyper-V
 - Solaris 10 Zones

예제 정책이 저장되는 위치

CA Access Control 은 예제 정책을 다음 디렉터리에 설치합니다.

ACInstallDir/samples/Policies/

ACInstallDir

CA Access Control 이 설치된 디렉터리를 정의합니다.

이 위치에는 다음과 같은 세 개의 하위 디렉터리가 있습니다.

- **Applications** - 응용 프로그램 관련 정책이 들어 있습니다.
- **OS** - 운영 체제 정책이 들어 있습니다.
- **Virtualization** - 가상화 시스템 정책이 들어 있습니다.

CA Access Control 은 정책을 실행하는 **selang** 스크립트가 수록된 텍스트 파일로 정책을 제공합니다. 또한 각 정책에는 보호 정책을 배포 취소하는 데 사용할 수 있는 일치하는 정책이 있습니다. CA Access Control 엔터프라이즈 관리에서 정책을 배포 및 배포 취소합니다.

예제 정책은 **OS_ACTION** 과 같은 명명 규칙을 사용합니다.

OS

정책이 설계된 대상 운영 체제를 정의합니다.

ACTION

스크립트가 수행하는 정책 작업을 지정합니다.

값: deploy 및 undeploy

예를 들어, 다음 파일은 Red Hat Enterprise Linux 4.0 에 대한 예제 배포 정책을 수록하고 있습니다: `_LINUX40_deploy.txt`

참고: 응용 프로그램 정책은 배포 취소 스크립트가 없습니다.

예제 정책 스크립트

각 정책은 정책의 용도와 포함된 규칙에 대해 설명하는 주석이 포함된 **selang** 스크립트입니다. 예제 정책 스크립트는 모범 사례를 보여주기 위해 작성되었습니다.

■ 설명

예제 정책의 각 섹션에서 달성할 목표를 쉽게 이해할 수 있도록 예제 정책에는 설명이 첨부되어 있습니다.

■ 컨테이너

예제 정책은 관련 리소스를 하나의 컨테이너 리소스로 그룹화합니다. 이 방법을 사용하여 공용 정책은 모든 관련 리소스에 한 번 적용됩니다. 정책 규칙(ACL)은 개별 리소스에 적용할 필요가 없습니다. 예를 들어, 정책은 컨테이너를 사용하여 시스템의 모든 구성 파일을 그룹화할 수 있습니다.

정책 컨테이너는 **POL_container_name** 과 같은 명명 규칙을 사용합니다. 이러한 컨테이너는 하위 정책과 같은 역할을 합니다. 예를 들어, OS 예제 정책은 **POL_SYS_CONF** 컨테이너를 사용하여 OS 구성 파일을 보호합니다.

■ 역할

쉽게 사용자를 관리할 수 있도록 예제 정책은 역할에 ACL 을 적용합니다. 각 역할은 실제 사용자를 추가할 수 있는 CA Access Control 사용자 그룹을 사용합니다.

정책 역할은 `ROL_role_name` 과 같은 명명 규칙을 사용합니다. 예를 들어, 예제 정책은 기본 제공되는 `adm` 및 `lp` 와 같은 시스템 사용자에게 `ROL_SYSTEM` 그룹을 사용합니다. 많은 정책은 이러한 사용자에게 적절한 시스템 운용을 위해 폭넓은 사용 권한을 할당하지만 로그인에 사용할 수 없도록 권한의 사용 기간을 제한합니다.

■ 변수

배포할 때 적용할 변경 내용을 최소화하기 위해 예제 정책은 CA Access Control 변수를 사용합니다. 예제 정책은 기본 제공되는 변수를 사용하여 로컬 호스트에 대한 터미널 규칙과 같은 로컬 시스템 리소스를 보호합니다. 예제 정책은 또한 사용자 정의된 변수를 사용하여 간편하게 정책을 변경할 수 있게 합니다. 예를 들어, 사용자 정의된 변수는 관리 사용자의 홈 디렉터리를 포함할 수 있습니다. 관리 사용자가 다른 홈 디렉터리를 사용하는 경우 이 디렉터리만 한 번 변경하면 영향을 받는 모든 규칙이 자동으로 변경됩니다.

예: 정책 스크립트 주석

Solaris SPARC 9 예제 정책에서 가져온 다음 코드 조각은 예제 정책에 주석을 추가하는 방법을 설명합니다. `selang` 구문 규칙을 사용할 때 해시 기호(`#`)로 시작하는 줄은 주석입니다.

```
#
# * 홈 디렉터리 보호 정책 *
# *****
#
# 이 정책은 FILE 클래스를 사용하여 각 디렉터리의
# 소유자만 액세스할 수 있도록 중요한 사용자의 홈
# 디렉터를 보호합니다.
#
# 필수 구성 요소:
# ____없음
#
# 규칙:
# ____없음
#
# 컨테이너:
# ____POL_HOME_DIR____ - 중요한 사용자의 홈 디렉터리
#
```

```
# 컨테이너 POL_HOME_DIR 정의
# 홈 디렉터리 보호
editres CONTAINER POL_HOME_DIR audit(<!POLICY_AUDIT_MODE>) owner(+nobody)
comment("AC 예제 - 홈 디렉터리 보호")
authorize CONTAINER POL_HOME_DIR uid(*_undefined) access(NONE)
editres ACVAR ("HOME_OS_ADMIN") value("/root") type(static)
editusr (<!USER_OS_ADMIN>)
# 특정 FILE 리소스를 정의하고 POL_HOME_DIR 와 연결
editres FILE ("<!HOME_OS_ADMIN>/*") audit(<!POLICY_AUDIT_MODE>) owner(+nobody)
defaccess(NONE) <!POLICY_WARNING_MODE> comment("AC 예제")
authorize FILE ("<!HOME_OS_ADMIN>/*") uid(<!USER_OS_ADMIN>) access(ALL)
chres CONTAINER POL_HOME_DIR mem+("<!HOME_OS_ADMIN>/*") of_class(FILE)
```

예: 예제 정책의 컨테이너

다음 selang 출력은 POL_SYS_FILES 의 속성을 표시합니다. AIX 예제 정책은 시스템 파일을 보호하는 하위 정책을 포함하고 있습니다.

```
AC> sr container POL_SYS_FILES
컨테이너 'POL_SYS_FILES'의 데이터
-----
ACL_____ :
___접근자_____ 액세스
___ROL_SYSADMIN__(GROUP__)_All
___ROL_SYSTEM__(GROUP__)_All
___*(USER__)_R, Chdir
___undefined__(USER__)_R, Chdir
구성원_____ :
___/boot/*_____(FILE__)
___/dev/kmem____(FILE__)
___/dev/mem____(FILE__)
___/dev/port____(FILE__)
감사 모드_____ : 실패
소유자_____ : +nobody_____(USER__)
작성 시간_____ : 2008-12-10 10:32
업데이트 시간_____ : 2008-12-10 10:35
업데이트한 사람_____ : root_____(USER__)
설명_____ : AC 예제 - OS 시스템 파일 보호
```

예: 예제 정책의 변수

Red Hat Enterprise Linux 5 예제 정책에서 가져온 다음 코드 조각은 예제 정책이 변수를 사용하는 방법을 설명합니다. 이 코드 조각에서 예제 정책은 로컬 호스트 및 관리 사용자 `root` 의 홈 디렉터리에 대한 가능한 이름을 정의합니다.

```
#
# * AC 변수 정의 *
# *****
#
# 이 섹션의 규칙은 정책이 사용하는 변수를 정의합니다.
# 변수:
#     LOCALHOST           : 로컬 호스트의 가능한 이름 목록
#     POLICY_AUDIT_MODE   : 정책 감사 모드 설정
#     POLICY_DEFACCESS     : 정책 리소스의 defaccess 설정
#
editres ACVAR ("LOCALHOST") value("localhost") type(static)
editres ACVAR ("LOCALHOST") value+("127.0.0.1")
editres ACVAR ("LOCALHOST") value+("0.0.0.0")
editres ACVAR ("POLICY_AUDIT_MODE") value("FAILURE") type(static)
editres ACVAR ("POLICY_DEFACCESS") value("ALL") type(static)
```

추가 정보:

[사용자 정의된 변수](#) (페이지 109)

[기본 제공되는 변수](#) (페이지 110)

[변수 사용 지침](#) (페이지 111)

[끝점이 변수를 해석하는 방법](#) (페이지 114)

컴플라이언스 및 모범 사례 정책

컴플라이언스 및 모범 사례 정책은 끝점에 컴플라이언스 및 모범 사례 정책을 신속히 배포할 수 있게 해 줍니다. 각 정책은 정책의 용도, 포함하는 규칙, 사용하는 변수를 설명하는 주석이 포함된 `selang` 스크립트입니다.

이 정책은 지급 카드 업계 데이터 보안 요건 및 보안 평가 절차(PCI DSS) 표준과 VMWare VSphere Hardening 요건을 따릅니다.

컴플라이언스 및 모범 사례 정책은 다음 운영 체제 및 가상화 플랫폼에 대해 사용할 수 있습니다.

- 운영 체제
 - Red Hat Advanced Server Linux
 - SuSE Linux
 - SLES
 - AIX
 - HP-UX
 - Solaris
 - Windows 2003 R2
 - Windows 2008 R2
- 가상화 플랫폼
 - VMWare Server ESX
 - Solaris 10 의 Solaris 영역
 - Hyper-V

컴플라이언스 및 모범 사례 정책이 저장되는 위치

엔터프라이즈 관리 서버는 설치 중 컴플라이언스 및 모범 사례 정책을 DMS 에 저장합니다. 이 작업은 엔터프라이즈 관리 서버를 처음 설치할 때 자동으로 수행됩니다.

컴플라이언스 및 모범 사례 정책은 CA Access Control 엔터프라이즈 관리의 정책 관리 섹션에서 관리합니다.

CA Access Control 을 새로 설치할 때마다 컴플라이언스 및 모범 사례 정책은 다음 위치에 저장됩니다.

`ACInstallDir/samples/Policies/OutOfTheBox`

ACInstallDir

CA Access Control 이 설치된 디렉터리를 정의합니다.

CA Access Control 은 정책을 실행하는 `selang` 스크립트가 수록된 텍스트 파일로 정책을 제공합니다. 또한 각 정책에는 보호 정책을 배포 취소하는 데 사용할 수 있는 일치하는 정책이 있습니다. CA Access Control 엔터프라이즈 관리에서 정책을 배포 및 배포 취소합니다.

예제 정책은 다음 명명 규칙을 사용합니다: `REGULATION_ACTION`

REGULATION

정책이 고안된 대상 규정의 이름을 정의합니다.

ACTION

스크립트가 수행하는 정책 작업을 지정합니다.

값: `deploy` 및 `undeploy`

예를 들어, 다음 파일은 PCI DSS 섹션 7.1.1 에 대한 예제 배포 정책을 포함하고 있습니다: `pci_dss_7.1.1_deploy.txt`

참고: 컴플라이언스 및 모범 사례 정책은 OS 에 독립적이며 Windows 및 UNIX 시스템에 적용할 수 있습니다.

컴플라이언스 및 모범 사례 정책 스크립트

각 정책은 정책의 용도와 포함된 규칙에 대해 설명하는 주석이 포함된 `selang` 스크립트입니다.

- 설명

예제 정책의 각 섹션에서 달성할 목표를 쉽게 이해할 수 있도록 예제 정책에는 설명이 첨부되어 있습니다.

- 변수

컴플라이언스 및 모범 사례 정책은 운영 체제에 독립적입니다. 하지만 리소스 그룹은 시스템마다 차이가 있습니다. 이 문제를 극복하기 위해 리소스 목록은 변수를 사용하고 ACL은 이 변수를 정책에 사용합니다. 끝점이 엔터프라이즈 관리 서버에 연결할 때 운영 체제 시스템과 끝점에 배포된 정책에 따라 일치하는 호스트 그룹에 끝점이 추가됩니다.

- 역할

쉽게 사용자를 관리할 수 있도록 예제 정책은 역할에 ACL을 적용합니다. 각 역할은 실제 사용자를 추가할 수 있는 CA Access Control 사용자 그룹을 사용합니다.

정책 역할은 `ROL_role_name`과 같은 명명 규칙을 사용합니다. 예를 들어, 예제 정책은 기본 제공되는 `adm` 및 `lp`와 같은 시스템 사용자에게 `ROL_SYSTEM` 그룹을 사용합니다. 많은 정책은 이러한 사용자에게 적절한 시스템 운용을 위해 폭넓은 사용 권한을 할당하지만 로그인에 사용할 수 없도록 권한의 사용 기간을 제한합니다.

예: 컴플라이언스 및 모범 사례 정책 주석

PCI_DSS_7.1.1 컴플라이언스 정책의 다음 코드 조각은 컴플라이언스 및 모범 사례 정책에 주석을 다는 방법을 설명합니다. `selang` 구문 규칙을 사용할 때 해시 기호(`#`)로 시작하는 줄은 주석입니다.

```
#
# * 2. <!USER_OS_ADMIN> 로그인 및 Access Control 관리 보호 *
# *****
#
# 이 섹션은 administrator 사용자가 직접 로그인하지 못하도록(읽기 액세스)
# TERMINAL 클래스를 사용합니다. Access Control 관리도 또한
# 차단됩니다(쓰기 액세스).
#
# 보안 관리와 시스템 관리를 분리하기 위해 정책은
# 이러한 특수 터미널에만 READ 액세스를 설정합니다.
#
editres    TERMINAL ("<!HOSTNAME>") audit(ALL) warning
authorize  TERMINAL ("<!HOSTNAME>") uid("<!USER_OS_ADMIN>") deniedaccess(READ)
# UNIX에서는 TERMINAL 클래스에 대한 쓰기 액세스에 경고 모드를
# 사용할 수 없으므로 다음 줄이 주석 처리되었습니다.
#authorize TERMINAL ("<!HOSTNAME>") uid("<!USER_OS_ADMIN>") deniedaccess(WRITE)
```


예: 컴플라이언스 및 모범 사례 정책 정책 역할

PCI_DSS_7.1.1 컴플라이언스 정책의 다음 코드 조각은 정책이 역할에 ACL 을 적용하는 방법을 설명합니다.

```
#
# * 1. 역할 정의 *
# *****
#
# 이 섹션의 규칙은 정책이 사용하는 역할을 정의합니다.
#
# * 논리적 속성을 사용하여 기본 제공 OS 사용자를 정의합니다. 이렇게 하면 사용자가 시스템에
# 로그인하지
# 못하도록 방지합니다.
# * CA Access Control 에서만 사용자 +nobody 를 만드십시오. CA Access Control 은
# 이 사용자를 여러 리소스의 소유자로 설정합니다(소유권 바이패스를
# 비활성화하기 위해). 네이티브 OS 에서는 이 사용자를 만들 수 없습니다.
# * ROL_AC_ADMIN 에서 하나 이상의 사용자를 만드십시오. 이 사용자가 없으면
# CA Access Control 에 로그인할 수 없습니다.
# 참고: 기본적으로 이 규칙은 superuser 계정을 ROL_AC_ADMIN 에 추가합니다.
# 이 사용자를 제거하고 이 그룹에
# 보안 관리자를 추가할 것을 권장합니다.
# 규칙:
# ROL_SYSTEM : 기본 제공 OS 사용자
# ROL_SYSADMIN : 시스템 관리자
# ROL_RESTRICTED : 특정 작업에 대한 권한을 갖는 제한된 사용자
# ROL_AC_ADMIN : CA Access Control 관리자
# ROL_AC_AUDITOR : CA Access Control 감사자
# ROL_AC_OPERATOR : CA Access Control 운영자
# ROL_AC_SERVICE : CA Access Control 서비스 관리자
# ROL_AC_PWMANAGER : CA Access Control 암호 관리자
#

editgrp (ROL_SYSTEM ROL_SYSADMIN ROL_RESTRICTED ROL_AC_ADMIN ROL_AC_AUDITOR
ROL_AC_OPERATOR ROL_AC_SERVICE ROL_AC_PWMANAGER)
chgrp (ROL_SYSADMIN ROL_AC_ADMIN) audit(LOGINSUCCESS LOGINFAILURE FAILURE)
editusr (+nobody) comment("AC OOTB - Resource owner used for disabling ownership
bypass")
chusr (+nobody) owner(+nobody)
join ("<!USER_OS_ADMIN>") group(ROL_SYSTEM)
join ("<!USER_OS_ADMIN>") group(ROL_AC_ADMIN)
```

정책 배포

CA Access Control 정책을 배포할 때는 정책이 오류 없이 예상한 대로 배포 및 수행되도록 다음과 같은 일부 일반 단계를 따라야 합니다. 다음 섹션에서는 예제 정책을 배포하기 전 및 후에 수행해야 하는 작업에 대해 설명합니다.

정책 배포를 위한 끝점 준비 방법

정책을 구현하기 전에 정책에 대해 끝점을 준비해야 합니다. 이렇게 하면 나중에 이 정책과 특별히 관련된 문제를 파악할 수 있습니다.

정책 배포를 위해 끝점을 준비하려면

- 운영 체제 또는 응용 프로그램의 신규 설치 사용

OS 정책에 대해 제조업체에서 제공하는 최신 OS 버전 및 패치를 사용하십시오. 이렇게 하면 수정에 따른 잠재적 손상으로부터 시스템을 보호할 수 있습니다. 정책은 시스템이 고의 또는 사고로 인해 변경되지 않도록 보호하므로 정책을 적용한 다음에는 패치를 적용하고 시스템을 필요한 대로 구성할 수 있습니다. 응용 프로그램에도 동일한 논리가 적용됩니다.

- 권한 분리 적용

정책 규칙을 검토하여 필요한 경우 규칙을 추가하십시오. 역할, 사용자, 사용자의 관계(역할 구성원 자격)를 정의하는 정책을 새로 만드십시오. 그러면 이 정책을 예제 정책 이전 또는 이후에 배포할 수 있습니다.

한 사용자에게 너무 많은 권한을 부여하지 않도록 주의하십시오. 예를 들어, 기본적으로 `superuser` 는 CA Access Control 관리 권한을 제공하는 `ROL_AC_ADMIN` 에 추가되어 있습니다. 하지만 이 사용자를 그룹에서 제거한 후 대신 보안 관리자를 추가하는 것이 좋습니다.

- 새 CA Access Control 데이터베이스 생성 및 기존 데이터베이스 백업

정책을 배포하기 전에 새 데이터베이스를 만드십시오. 이렇게 하면 정책 규칙이 충돌하거나 데이터베이스의 기존 규칙이 변경되는 것을 방지할 수 있습니다. 새 데이터베이스를 만들 수 없는 경우 정책을 적용하기 이전 상태로 복원할 수 있도록 데이터베이스를 백업해야 합니다.

- 적절한 관리 역할(시스템 관리, 보안 관리, 응용 프로그램 관리)이 있는 사용자를 할당하십시오.
- 새 감사 로그 파일 사용
기존 감사 로그 파일을 백업한 후 먼저 파일을 제거하십시오. 이렇게 하면 CA Access Control 이 새 이벤트를 로깅할 때 새 감사 로그 파일을 만듭니다. 감사 로그 파일이 배포하는 정책에 대한 이벤트만 수록하고 있으므로 이 정책과 관련된 문제를 보다 신속하게 파악할 수 있습니다.
- CA Access Control 사용자 정의된 변수 설정
미리 설정된 CA Access Control 변수 값("AC 변수 정의" 섹션)을 확인하고, 사용하는 환경에 맞게 조정하고, 필요한 경우 값을 추가 또는 수정하십시오.

단계적으로 정책을 배포하는 방법

정책을 배포할 때 정책이 오류 없이 예상한 대로 배포 및 수행되도록 수행할 수 있는 일부 작업이 있습니다. 정책 배포를 위해 끝점을 준비한 다음에는 단계적으로 정책을 배포하는 것이 좋습니다.

먼저 테스트 환경에서 정책을 배포하고 필요에 따라 정책을 조정한 이후에 실제 환경에서 정책을 배포하는 것이 좋습니다.

단계적으로 정책을 배포하려면

1. 경고 모드에서 정책을 배포합니다.

이제 정책이 활성화되었지만 규칙을 시행하지는 않습니다. 그런 다음 감사 로그를 검토하여 원하는 정책을 적용하기 전에 해당 정책 결과를 미리 볼 수 있습니다.

참고: 기본적으로 예제 정책의 스크립트는 모든 정책 규칙에 대해 경고 모드를 설정합니다.

2. CA Access Control 감사 로그에서 경고 메시지를 검토합니다.

정책을 배포한 이후에는 정책 규칙이 경고 모드를 사용하는 경우 감사 로그에 모든 정책 위반이 경고로 표시됩니다.

3. 실제 시나리오에서 시스템을 사용하고 감사 로그를 다시 분석합니다.

컴퓨터에서 일상적인 운영 절차(로그인, 서비스/응용 프로그램 시작/중지 등)를 수행하여 정책을 효과적으로 테스트할 수 있습니다. 그런 다음 감사 로그를 다시 분석하여 새 경고가 나타나는지 확인할 수 있습니다.

4. 필요한 경우 정책을 수정합니다.

감사 로그에서 얻은 정보를 사용하여 사용하는 환경에서 예상대로 작동하도록 정책을 수정할 수 있습니다.

5. 정책을 활성화하기 위해 경고를 제거합니다.

정책이 실제 업무 환경에서 규칙을 시행할 준비가 되었다고 확신하면 경고 모드를 제거하여 정책을 활성화할 수 있습니다.

정책이 이제 시행됩니다.

참고: 정책을 수정하려면 먼저 정책 시행을 비활성화하고(경고 모드 사용) 정책을 수정한 다음 변경 내용이 원하는 대로 작동한다고 확신할 때 정책을 다시 활성화해야 합니다.

추가 정보:

[정책 배포](#) (페이지 389)

[사용하는 환경에 맞게 정책을 사용자 지정하는 방법](#) (페이지 390)

[예제 정책 시행 활성화](#) (페이지 391)

정책 배포

예제 정책 및 모범 사례 정책은 CA Access Control 변수를 포함하므로 고급 정책 관리 방법을 사용하여 배포해야 합니다.

참고: 예제 정책 파일은 끝점의 `selang` 에서 직접 실행할 수 없습니다.

CA Access Control 엔터프라이즈 관리를 사용하여 예제 정책을 DMS 에 저장한 다음 필요할 때 여러 끝점에 할당하십시오.

추가 정보:

[고급 정책 관리](#) (페이지 72)

[정책 생성 및 배포 방법](#) (페이지 91)

사용하는 환경에 맞게 정책을 사용자 지정하는 방법

예제 정책 및 모범 사례 정책은 사용하는 보안 정책을 위한 기초로서 제공됩니다. 정책을 배포하려면 사용하는 환경에 맞게 사용자 지정해야 합니다.

사용하는 환경에 맞게 정책을 사용자 지정하려면

- CA Access Control 및 시스템 로그 파일을 검토합니다.

배포 프로세스 중 발생한 경고 또는 오류를 파악하여 적절히 정책을 수정합니다.

- 사용자를 정책 규칙에 조인합니다.

정책은 권한 부여를 위해 역할을 사용합니다. 조직의 사용자를 이 역할에 할당해야 합니다.

중요! 정책의 배포를 취소할 때는 만든 사용자 또는 그룹을 삭제하지 마십시오. 삭제하는 경우 동일한 사용자 및 그룹을 사용하는 다른 정책에 있는 접근자 연관 관계 및 ACL 목록의 동작에 영향을 줄 수 있습니다.

- (Windows에만 해당) 공존 유틸리티 eACoexist.exe를 실행합니다.

이 유틸리티는 CA Access Control과 설치된 다른 프로그램 사이의 충돌을 식별하고, 해당 프로그램에 대한 바이패스를 만들어 이 충돌을 해결합니다.

예제 정책 시행 활성화

기본적으로 샘플 정책 스크립트는 모든 정책 규칙에 대해 경고 모드를 설정합니다. 정책을 배포하면 정책이 활성화되지만 규칙이 시행되지는 않습니다. 정책에 익숙해지고 필요한 대로 정책을 사용자 지정할 수 있게 되면 정책 규칙이 시행되도록 정책을 활성화할 준비가 되었습니다.

참고: 이 절차는 하나의 정책에 대해 정책 시행을 활성화하는 방법을 설명합니다. 시스템 유지 관리를 수행한 이후 여러 정책에 대해 정책 시행을 활성화하는 방법을 보려면 사용하는 운영 체제용 *끝점 관리 안내서*를 참조하십시오.

예제 정책 시행을 활성화하려면

1. 정책 스크립트를 편집하여 **warning**의 각 인스턴스를 **warning-**으로 변경합니다.

리소스 또는 접근자에 대해 **warning-**를 설정하는 규칙을 실행하면 CA Access Control은 해당 리소스 또는 접근자의 경고 모드를 제거합니다.

2. 편집된 정책을 배포합니다.
정책 시행이 활성화됩니다.

예: Windows 샘플 정책 시행

다음은 Windows용 샘플 JBoss 정책에서 가져온 코드 조각입니다. 이 정책은 "warning"이 "warning-"으로 변경되었으므로 활성화되었습니다.

```
# Protect JBoss files
# -----

# Protect JBoss files in the application directory.
# These rules apply protection to files that are not protected by other rules.
editfile ("<!JBoss_HOME>\\*") owner(nobody) defaccess(NONE) warning- comment ("AC
Sample - JBoss base dir")
authorize FILE ("<!JBoss_HOME>\\*") id(ROL_JBoss_ADMIN) access(ALL)
via(pgm("<!JBoss_HOME>\\bin\\*"))
authorize FILE ("<!JBoss_HOME>\\*") id(jboss_pgm) access(READ,CHDIR)
via(pgm("<!JBoss_HOME>\\bin\\*", "<!JBoss_HOME>\\java\\pgm\\*"))
```

예제 정책 시행 비활성화

기본적으로 샘플 정책 스크립트는 모든 정책 규칙에 대해 경고 모드를 설정합니다. 정책 시행을 활성화할 때 경고 모드를 제거합니다. 정책 시행을 비활성화하려면 경고 모드를 다시 사용해야 합니다.

참고: 이 절차는 하나의 정책에 대해 정책 시행을 비활성화하는 방법을 설명합니다. 시스템 유지 관리를 수행할 때 여러 정책에 대해 정책 시행을 비활성화하는 방법을 보려면 사용하는 운영 체제용 *끝점 관리 안내서*를 참조하십시오.

예제 정책 시행을 비활성화하려면

1. 정책 스크립트를 편집하여 **warning-**의 각 인스턴스를 **warning** 으로 변경합니다.

리소스 또는 접근자에 대해 **warning** 을 설정하는 규칙을 실행하면 CA Access Control 은 해당 리소스 또는 접근자에 대해 경고 모드를 설정합니다.

2. 편집된 정책을 배포합니다.
정책 시행이 비활성화됩니다.